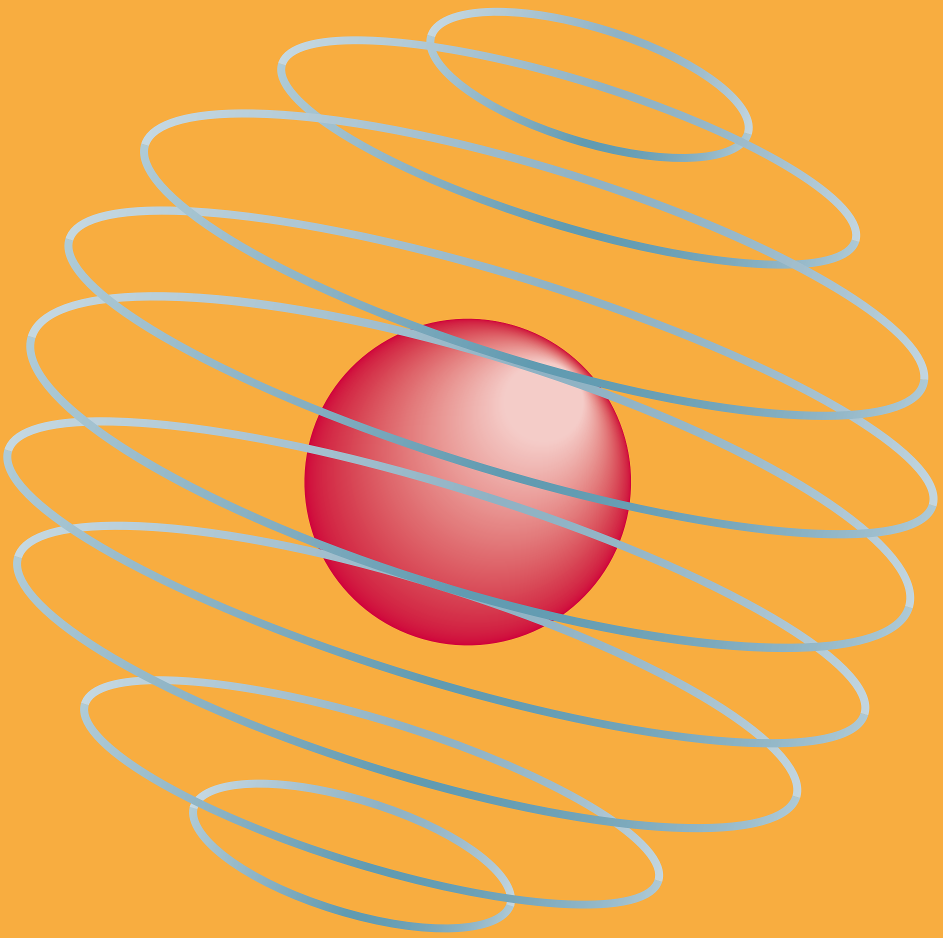
2019 YEARBOOK



UNIVERSITY OF OXFORD

CENTRE *for* DOCTORAL TRAINING *in* CYBER SECURITY

EPSRC
Engineering and Physical Sciences Research Council

Contents

Editorial Board:
Katherine Fletcher
David Hobbs
Martin Kraemer
Andrew Martin
Romy Minko,
Arianna S.
Anjuli R. K. Shere

Design:
Suvarna Designs

All details correct as of August 2019

Alumni

The CDT Team

Director's Preface

The CDT in Cyber Security is now in its sixth year of operation, and here is our biggest and most diverse Yearbook yet. It paints a very broad picture of the incredible range of activity that falls within this discipline. No one should under-estimate the value of setting up some intelligent and diverse students with a few resources: it is a thrill to see them go off and innovate, individually and together. You will read here of a wide range of theses already complete, and many more still in progress, contributing impact in systems design, political theory, understanding the social consequences of security decisions, building better businesses, and many more areas of endeavour. Other articles describe how our students are also active in contributing to and helping to lead cyber security competitions and their own conference, in collaboration with their peers in the CDT in Cyber Security at Royal Holloway University of London.

Of course, this is a team endeavour. We are grateful for support from the National Cyber Security Programme through EPSRC, as well as time and resources from our many external partners who make possible data sharing, internships, Deep Dive Days, and give much encouragement and insight along the way. The support of the University of Oxford is essential to our existence, as is the hard work of nearly 40 supervisors in thirteen academic departments of the University. As well as saying farewell to an increasing number of graduating students, we also mark at the end of the academic year the departure of our Centre Administrator Maureen York to a new adventure in a new phase of life (see page 34). Our admin team is vital both for ensuring the smooth running of the CDT and as the provider of all kinds of student support. I'm very pleased that David Hobbs will stay with the CDT in an expanded role.

It's striking that many of the articles presented here are written by groups of students – some from a mixture of cohorts – as they have taken the initiative to pursue extra research together outside their core areas of interest. This is the strength of the CDT model, especially in the area of Cyber Security, where collaborative teams from multiple disciplines are absolutely crucial. That understanding is becoming commonplace in the wider world today – even if it was much more rare when we began the *Cyber Security Oxford* venture. We are proud of each of our CDT graduates able and ready to take their places in these complex environments of today – whether in research, or business, or the public service. Cyber Security is crucial to everyone – and it's a delight to see our students making a difference.

Andrew Martin
Professor of Systems Security
Director, CDT in Cyber Security

The CDT in numbers

Student Departments*:

Department of Computer Science	42
Faculty of Law	4
Department of Politics and International Relations	3
Oxford Internet Institute	3
Saïd Business School	2
Department of Education	1
Department of Engineering	1
Department of Sociology	1
Department of Statistics	1
Mathematical Institute	1
School of Geography and the Environment	1

Lecture hours in 2018–19 across 11 core modules and 17 electives **321**

4.63 **Average lecturer feedback score (out of 5)**

"Satisfied" or "Very satisfied" in the latest student barometer **96%**

* Numbers do not include CDT18 who are yet to confirm their main departments

69%

In-flight

9%

Submitted

11%

Graduated

11%

Other

276

Student publications to date

49

Conference talks, papers and posters

40 academic supervisors support our CDT students

USA is the most visited 2018-19 conference destination followed by Germany and France

4,700 recyclable coffee pods consumed in 2018-19.

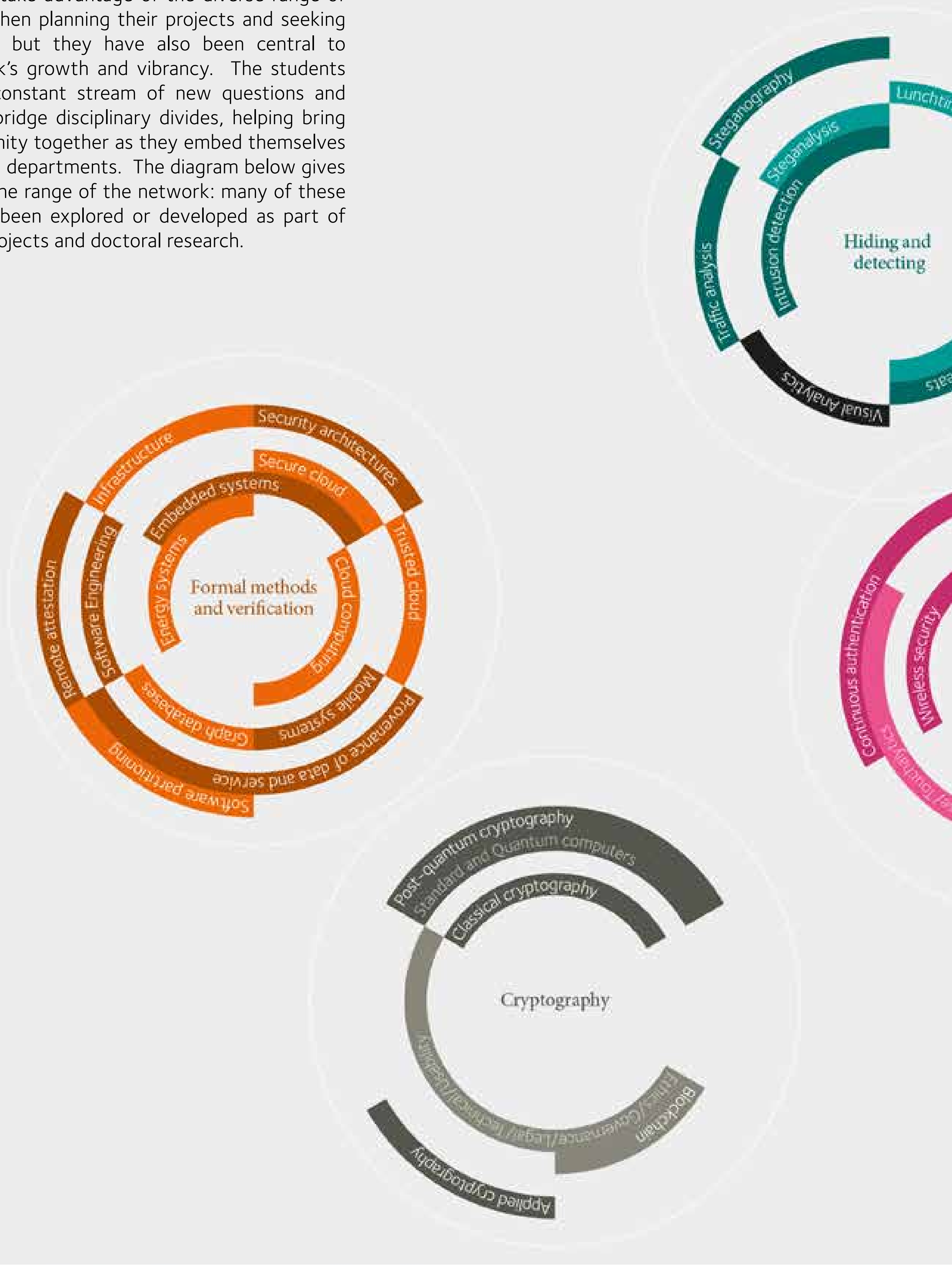
150 reusable water bottles provided to members of the CDT to reduce the need for thousands of single-use plastic cups, since 2018.

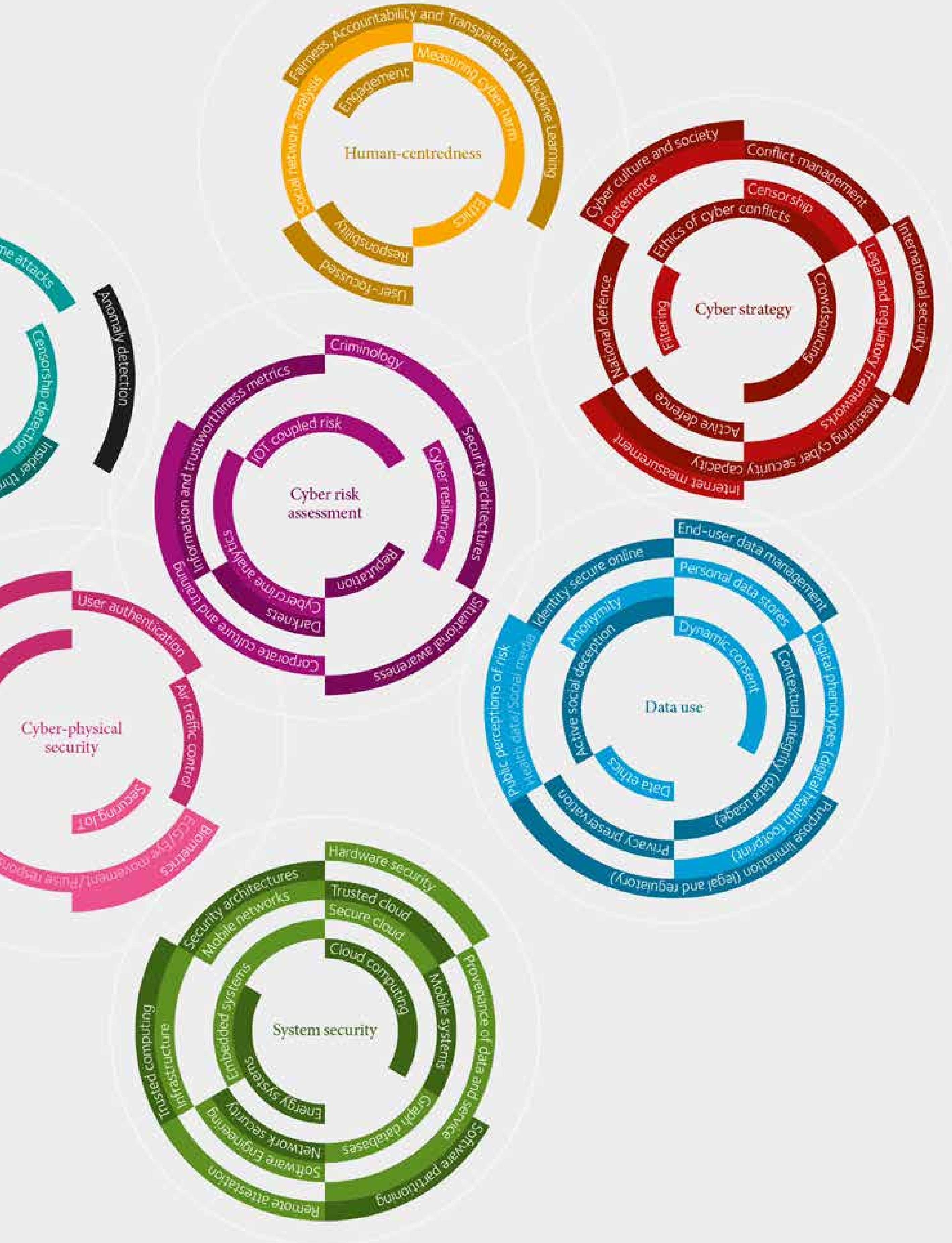
Current Year of Study:

Year 4+	37%
Year 3	21%
Year 2	21%
Year 1	21%

Cyber Security Oxford – The Wider Network

The CDT is part of a wider network of cyber security researchers and practitioners at the University. Cyber Security Oxford (www.cybersecurity.ox.ac.uk) has over 300 members across 26 Departments, in all four Divisions of the University. CDT students are able to take advantage of the diverse range of expertise when planning their projects and seeking supervision, but they have also been central to the network's growth and vibrancy. The students provide a constant stream of new questions and ideas that bridge disciplinary divides, helping bring the community together as they embed themselves in their host departments. The diagram below gives an idea of the range of the network: many of these areas have been explored or developed as part of CDT mini projects and doctoral research.




Human-centredness
Fairness, Accountability and Transparency in Machine Learning
Measuring cyber harm
Engagement
Social network analysis
Ethics
Responsibility
User-focussed
Cyber strategy
Cyber culture and society
Conflict management
Deterrence
Censorship
Ethics of cyber conflicts
International security
Legal and regulatory frameworks
National defence
Filtering
Crowdsourcing
Active defence
Measuring cyber security capacity
Internet measurement
ne attacks
Anomaly detection
Censorship detection
Insider thr
Cyber risk assessment
Criminology
Information and trustworthiness metrics
IOT coupled risk
Cyber resilience
Security architectures
Cybercrime analytics
Reputation
Darknets
Corporate culture and training
Situational awareness
Data use
End-user data management
Identity secure online
Personal data stores
Anonymity
Dynamic consent
Public perceptions of risk
Health data/Social media
Active social deception
Contextual integrity (data usage)
Digital phenotypes (digital health footprint)
Data ethics
Privacy preservation
Purpose limitation (legal and regulatory)
Cyber-physical security
User authentication
Air traffic control
Securing IoT
Biometrics
ECG/Eye movement/Pulse respons
System security
Hardware security
Security architectures
Mobile networks
Trusted cloud
Secure cloud
Cloud computing
Embedded systems
Mobile systems
Provenance of data and service
Trusted computing
Infrastructure
Energy systems
Graph databases
Network security
Software Engineering
Software partitioning
Remote attestation

Submitted Theses

LOUISE AXON

Supervisors: Sadie Creese and Michael Goldsmith, Department of Computer Science

Sonification for Network-Security Monitoring

In the face of increasingly frequent, sophisticated and varied cyber-attacks, organisations must continuously adapt and improve their network defences. In many organisations, maintaining network security is the role of the security operations centre (SOC), in which security practitioners work, aided by security-monitoring tools, to detect and mitigate cyber-attacks. There is a need for effective tools to help security practitioners to engage with and understand the data communicated over the network, and the outputs of automated attack-detection methods. Over the last few years, a number of novel approaches have been examined, with the aim of aiding in various aspects of the network-security monitoring work of security practitioners. This thesis explores one of these approaches in particular: sonification.

Sonification is the representation of data as sound; more specifically, it is widely accepted to be "the use of non-speech audio to convey information". Sonification has been shown to have advantages for presenting data to humans in other fields, such as medicine and astronomy, for monitoring data and for anomaly detection. In theory, some of the known properties of sonification make it a promising data-presentation approach for SOCs. It has been shown that sound can be comprehended peripherally, enabling monitoring as a non-primary task, which may aid busy security practitioners, for example. Prior literature indicates the potential of network-traffic sonification systems for signalling network-security information, but does not evaluate its utility or explore its application in SOCs. The aim of this research is to explore the utility of sonification systems to the security-monitoring tasks carried out in SOCs.

In order to address this aim, we proposed a model to underpin approaches to sonification design for network-security data. We tested the ability of humans to detect network attacks and understand network-security events by listening to a sonification prototype, and found that the approach was effective in an experimental setting, indicating the viability of sonification as an approach to conveying network-security information. In order to understand the design requirements and potential contexts of use for sonification in SOCs, we surveyed and interviewed security practitioners working in SOCs. Finally, we explored the utility of sonification, by studying the use of a sonification system by security practitioners in a set of SOC tasks, in an experimental setting.

We found that using sonification systems could complement existing monitoring practice in SOCs (particularly in contexts in which it is advantageous to be able to monitor network security peripherally), subject to a range of challenges related to the integration of such systems into the SOC environment. While our findings indicate that sonification may be a useful technology for security practitioners, it is important to recognise that our results were obtained in experimental settings. To validate these findings, future longitudinal studies in which sonification systems are deployed in operational SOCs will be key to understanding their true utility and the severity of the challenges posed to integration.

Bio

Louise has completed her DPhil with the CDT in the past academic year, and also holds a BA in Mathematics and Music from Cardiff University, and an MSc in Mathematics of Cryptography and Communications from Royal Holloway University of London. Her DPhil thesis explored solutions for network-security monitoring in Security Operations Centres (SOCs). The focus was on investigating the use of sonification (the representation of data as sound) for network-security monitoring.

Publications

Axon, L., Happa, J., Goldsmith, M. and Creese, S., 2019. Hearing Attacks in Network Data: an Effectiveness Study. Computers & Security, vol. 83, pp. 367-388.

Axon, L., Alahmadi, B., Nurse, J.R., Goldsmith, M. and Creese, S., 2018. Sonification in security operations centres: what do security practitioners think? Workshop on Usable Security (USEC) at Network and Distributed System Security Symposium (NDSS)

Axon, L., Goldsmith, M. and Creese, S., 2019. Sonification Mappings: Estimating Effectiveness, Polarities and Scaling in an Online Experiment. Journal of the Audio Engineering Society, vol. 66(12), pp. 1016-1032.

Axon, L., Nurse, J. R. C., Goldsmith, M. and Creese, S., 2017. A Formalised Approach to Designing Sonification Systems for Network-Security Monitoring. International Journal on Advances in Security

Axon, L., Creese, S., Goldsmith, M. and Nurse, J. R. C., 2016. Reflecting on the Use of Sonification for Network Monitoring. International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE)

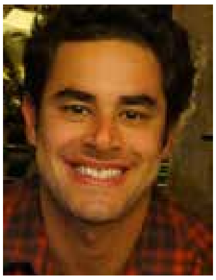
Williams, M., Axon, L., Nurse, J.R. and Creese, S., 2016. Future scenarios and challenges for security and privacy. In Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), 2016 IEEE 2nd International Forum on (pp. 1-6). IEEE.

Axon, L. and Goldsmith, M., 2017. PB-PKI: A Privacy-Aware Blockchain-Based PKI. International Conference on Security and Cryptography (SECRYPT)

Axon, L., Goldsmith, M. and Creese, S., 2018. Privacy Requirements in Cybersecurity Applications of Blockchain. Advances in Computers.

L. Axon, 2019. Sonification for Network-Security Monitoring. University of Oxford (DPhil thesis)

RODRIGO CARVALHO



Supervisors: Sadie Creese and Michael Goldsmith, Department of Computer Science

Investigating Malware Campaigns with Semantic Technologies

IMalware-campaign investigation is a major factor in fighting cybercrime. Most of the research in this area comes from commercial companies, so potentially there is a greater emphasis on detection rather than malware attribution. Aiming at a better balance between human reasoning skills and computer processing capabilities, my project is investigating how semantic technologies could help the insight-generation process of the analyst when investigating the malware ecosystem. My prototype allows for the analyst to assess different investigation hypotheses by facilitating the creation of bespoke clusters, relationships and tags, in addition to integrating and querying distinct datasets in a graph.

Bio

Rodrigo is a Computer Forensics Analyst for the Brazilian Federal Police since 2006 and a member of the National Institute of Forensic Sciences in Brazil. He joined the CDT in Cyber Security at University of Oxford to research about technologies that could make cybercrime investigation more efficient.

Prior to that, he worked at Accenture as a Consulting Analyst in a telecom project. His main role was programming. Rodrigo has a BSc. in Computer Science from University of Brasilia (2005), and completed a Masters in Computer Forensics and Information Security, at the same university, in 2012.

Publications

Visual Analytics for Open Source Intelligence. Rodrigo Carvalho. In Brazilian Journal of Police Science (RBCP). 2014. Journal Article.

Online banking malware ontology. Rodrigo Carvalho, Michael Goldsmith and Jason R. C. Nurse. In International Crime and Intelligence Analysis Conference (ICIA). 2015. Poster.

Applying semantic technologies to fight online banking fraud. Rodrigo Carvalho, Michael Goldsmith and Sadie Creese. In European Intelligence and Security Informatics Conference (EISIC). 2015. Conference proceedings.

Semantic technologies applied to digital forensics analysis and evidence modelling. Rodrigo Carvalho. In 20th European Symposium on Research in Computer Security (ESORICS). 2015. PhD consortium presentation.

Malware investigation using semantic technologies. Rodrigo Carvalho, Michael Goldsmith and Sadie Creese. In Intelligent Exploration of Semantic Data (a workshop at the International Semantic Web Conference). 2016. Workshop proceedings.

Investigating Malware Campaigns with Semantic Technologies. Rodrigo Carvalho, Michael Goldsmith and Sadie Creese. In IEEE Security & Privacy, special issue on Digital Forensics. To appear. Journal article.

JAMIE COLLIER

Supervisor: Lucas Kello, Department of Politics and International Relations

Cyber Security Assemblages

Traditional state-provided security paradigms traditionally deployed in international relations literature are less applicable in the context of cyber security. Instead, a range of actors provide cyber security, leading to assemblages that transcend traditional global-local and public-private distinctions.

If traditional state-centric paradigms do not capture the reality cyber security provision, it is therefore vital to understand which actors provide cyber security in addition to states, (including private sector firms, activist groups, academia, etc.). From there, it is possible to understand how various actors interact and whether such the dynamics between different actors are collaborative or competitive. Having understood the empirical reality of cyber security provision, it is then possible to determine the implications of these altogether new security models. For example, by considering whether the security of individuals is actually prioritised as well as how alternative models or visions of security clash (as seen in disputes between Apple and the FBI over the issue of encryption for example).

Bio

Having previously studied International Relations at the University of Nottingham, Jamie is interested in the strategic and political aspects of cyber security. Surrounded by techies and mathematicians in the first year of the DPhil, Jamie was somewhat overwhelmed and predictably fled to safe waters. He is now based at the Department of Politics and International Relations although can be seen in the Robert Hooke building for CDT parties and to make use of the free printing. Within Oxford, Jamie is active as a Research Affiliate with the Centre for Technology and Global Affairs Studies Programme and as a Research Associate with the Changing Character of War Programme. For the first half of 2017, Jamie was based at MIT as a Fulbright Scholar. Outside of the university, Jamie enjoys hiking, getting lost on bike rides and attempting to read highbrow books that are perhaps beyond his faculties.

Publications

"Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision" Politics and Governance (2018).

Written Evidence submitted to the UK Joint Committee on Cyber Security: Critical National Infrastructure Inquiry (February 13, 2018). http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/written/76828.html

"Bashing Facebook Is Not the Answer to Curbing Russian Influence Operations" Council on Foreign Relations (September 18, 2017). Co-authored with Monica Kaminska. https://www.cfr.org/blog/bashing-facebook-not-answer-curbing-russian-influence-operations

"Proxy Actors in the Cyber Domain: Implications for State Strategy," St Antony's International Review 13, no.1 (2017)

"Strategies of Cyber Crisis Management: Lessons from the Approaches

of Estonia and the United Kingdom," in Ethics and Policies for Cyber Operations, ed. Mariarosaria Taddeo and Ludovica Glorioso, vol. 124 of Philosophical Studies Series. (Springer, 2017), 187-212.

"Cyber Security Assemblages" (paper presented at the International Studies Association's 58th Annual Convention, Baltimore, Maryland, February 22-25 2017).

"Getting Intelligence Agencies to Adapt to Life Out of the Shadows." Council on Foreign Relations (April 5, 2017). https://www.cfr.org/blog-post/getting-intelligence-agencies-adapt-life-out-shadows

"Security Dichotomies in Cyber Security" (paper presented at British International Studies Association 41st Annual International Conference 2016, Edinburgh, UK, June 15-17, 2016). Co-authored with Jantje Silomon.

Richard Dearlove, Christopher Andrew, Stefan Halper, Peter Martland, Alan Dawson, Alfred Rolington and Jamie Collier "Cash is King. The Digital Revolution: The Future of Cash" Cambridge Security Initiative Report (2016).

ANDREW DWYER

Supervisors: Beth Greenhough and Derek McCormack, School of Geography and the Environment

Malware Ecologies: A Politics of Cybersecurity

Computation, in popular imaginations, is at perennial risk of infection from the tools of nefarious hackers, commonly referred to as malware. Today, malware pervade and perform a crucial and constitutive role in the insecurities of contemporary life from financial transactions, to 'critical national infrastructures' – such as electricity, water, and transportation – to devices in our 'smart' homes and cities, and even to potential 'cyberwar.' Yet, critical security research has rarely turned its attention to malware itself. In contrast, I explore malware and its politics, situated and extended beyond, an (auto) ethnographic study of the malware analysis laboratory of the UK endpoint protection business, Sophos. I argue that malware are currently processed through a patho-logic that conflate organic and non-organic materialities, permitting analogies between biology and computation, and are generative of particular forms of security that relegate malware to the intent of their authors. I explore how endpoint protection businesses are imbibed with these logics in order to attend to how malware are analysed, detected, and curated beyond them. By drawing on my method of 'becoming-analyst,' I critically reflect on how malware become known, are responded to by ad hoc political groups, and can assist in rethinking the role of computational agency in geography, international relations, security studies, and beyond. I instead conceive of malware as performative political actors making limited choices in broader computational ecologies. I therefore advocate for an eco-logical repositioning of malware, where cyberspace is not simply a neutral domain; but is central to the formation of choice that gives space for malware to be political. With four case studies – Conficker, Stuxnet, the Dukes, and WannaCry / (Not)Petya – I write new stories on how malware is encountered and dealt with in the twenty-first century. In doing so, I challenge contemporary discourses of cybersecurity to ask if conventional notions of who and what (per)form security are adequate, and how these are reconfigured through a radical 'more-than-human' politics, where malware are not just objects of security, but are active participants in its production and negotiation.

Bio

Andrew's interests in cybersecurity cut across computer science, geography, and international relations. For his substantive DPhil research, Andrew is at the University's School of Geography and the Environment developing a project on malicious software through of an exploration of malware ecologies. This draws upon a range of concepts from geography and computer science to explore how we interact with malware through analysis and detection, and how this is disseminated into broader domains of international relations and politics. In addition, Andrew has been active in policy hackathons, and was part of the Oxford team at Cyber 9/12 in London who won the 'Best Policy Brief' in February 2018. In addition, he has also been a visiting fellow at the German transdisciplinary SFB-TRR 'Dynamics of Security' project between Philipps-Universität Marburg and Justus-Liebig-Universität Gießen between January and June 2019 and is now a research affiliate with the Centre for Technology and Global Affairs at the University of Oxford In his first year, Andrew completed two mini-projects between May and September 2014. The first concerned the commercialisation of academic cyber security research with sponsorship from the former UK Department for Business, Innovation and Skills. The second investigated implantable medical devices and cybersecurity, questioning core concepts such as 'security by default' through the philosophical device of security atmospheres.

Prior to joining Oxford, Andrew gained a BA (Hons) in Geography from Durham University where he focused on security, philosophy and geopolitics. After his undergraduate degree, he worked for the technology consultancy, Accenture, as both a market maker in the products division and as a management consultant in financial services.

Papers

Lorimer, J., Hodgetts, T., Grenyer, R., Greenhough, B., McLeod, C. and Dwyer, A., 2019. Making the microbiome public: Participatory experiments with DNA sequencing in domestic kitchens. Transactions of the Institute of British Geographers, [online]. Available at: https://doi.org/10.1111/tran.12289

Dwyer, A. C. (2018). 'The NHS cyber-attack: A look at the complex environmental conditions of WannaCry.' RAD Magazine, 44, 25–26.

Greenhough, B., Dwyer, A., Grenyer, R., Hodgetts, T., McLeod, C. and Lorimer, J., 2018. Unsettling antibiosis: how might interdisciplinary researchers generate a feeling for the microbiome and to what effect? Palgrave Communications, 4(1), p.149. https://doi.org/10.1057/s41599-018-0196-3]

Hodgetts, T., Grenyer, R., Greenhough, B., McLeod, C., Dwyer, A. and Lorimer, J., 2018. 'The microbiome and its publics: A participatory approach for engaging publics with the microbiome and its implications for health and hygiene.' EMBO reports. [online] Available at: <http://embor.embopress.org/content/early/2018/05/18/embr.201845786.abstract>.

Reports

Dwyer, A. C. (2015). 'UK Academic Cyber Security Commercialisation: Short Report [for the UK Department for Business, Innovation and Skills].' https://ora.ox.ac.uk/objects/uuid:74e7289a-745f-4508-aa6e-fb4b9285e41d.

Exhibits

Dwyer, A. C. (2015). 'Future Fossils: The Pacemaker.' Society and Space (Open Site). Available at: http://societyandspace.org/2015/08/20/the-pacemaker-andew-dwyer/.

Conferences

Dwyer, A. C. (2019). '(Re)Cognizing War.' Global Politics in the Era of Disruptive Technologies: New Scenarios in an Old World? Standing Group di Relazioni Internazionali (SGRI) Conference, Società Italiana di Scienza Politica: Trento, Italy. 13 June 2019.

Dwyer, A. C. (2019). '(Re)Cognising Computation: New Political Actors in Security Studies.' Guest Lecture at SFB-TRR 138 'Dynamics of Security.' Marburg, Germany. 28 May 2019.

Dwyer, A. C. (2019). "Anomalous Structures." Finance, Security, Infrastructure: Hegemonies in Generative Practices. Justus-Liebig-Universität Gießen; Gießen, Germany. 21 March 2019.

Dwyer, A. C. (2018).'Approaching Computation in Political Geography.' New Frontiers in Political Geography. University of Oxford; Oxford, UK. 25 September 2018.

Dwyer, A. C. (2018). 'Negotiating maliciousness: The (Auto)Ethnographic "Becoming-Analyst."' 12th Pan-European Conference on International Relations (EISAPEC18). Prague, Czech Republic: 12 – 15 September 2018.

Dwyer, A. C. (2018). 'Automating the laboratory? Folding securities of malware.' RGS-IBG International Annual Conference. Cardiff, UK: 29 August 2018.

Dwyer, A. C. (2018). 'Rethinking Space in Cybersecurity.' Smart Cities. CDT in Cyber Security Student Conference. Royal Holloway, University of London, Egham, UK: 4 May 2018.

Dwyer, A. C. (2018). 'The Malicious Transience: a malware ecology.' Machinic Encounters. Transient Topographies: Space and Interface in Literature and Art Conference. NUI Galway, Ireland: 21 April 2018.

Dwyer, A. C., and Shaw, J. (2017). 'Place-faking: fermenting resistance through digital productions of space.' RGS-IBG International Annual Conference. London: 1st September 2017.

Dwyer, A. C. (2017). 'Maliciously corrupting spaces of the (non)object.' RGS-IBG International Annual Conference. London: 31st August 2017.

Dwyer, A. C. (2017). 'A More-than-Human Security: Performances of a Malware Politics.' Association of American Geographers Annual Conference. Boston, USA: 8th April 2017.

Dwyer, A. C. (2016). 'A model for future security cooperation: ICANN and the Conficker Working Group.' ICANN 56. Helsinki, Finland: 26th July 2016.

Dwyer, A. C. (2016). 'W32.Stuxnet: An Olympic Games.' Moving Together Postgraduate Conference - Durham University. Durham: 4th May 2016.

Dwyer, A. C. (2015). 'The Pacemaker: Tracing Cyber (Re)Territorialisations.' RGS-IBG International Annual Conference. Exeter: 3rd September 2015.

Symposia

Dwyer, A. C. (2017). 'Situating Cyberspace(s): Ethnography as Depth.' Royal Holloway CDT 'Of Other Cybersecurities' Workshop. Egham: 15th June 2017.

Dwyer, A. C. (2016). 'The Kiss of Death: the curse of the algorithm.' Living with Algorithms - Royal Holloway, University of London. London: 9th June 2016.

Dwyer, A. C. (2015). 'Diffusing Cyber Security Atmospheres: Implantable Medical Devices.' Oxford Cybersec Early Careers Symposium. Oxford: 30th September 2015.

Outreach

Quoted in BBC News (Online) on the Magecart hack of British Airways (2018) and also in the New Scientist on Huawei (2019).

June 2017: Talk on the 'NHS Cyber Attack' to the UK Radiological and Radiation Oncology Congress (UKRCO) in Manchester, UK.

November 2015: BBC Radio 4 'You & Yours' guest answering cybersecurity questions

OLIVER FARNAN

Supervisors: Joss Wright, Oxford Internet Institute and Andrew Martin, Department of Computer Science

Internet security: Censorship, privacy, anonymity, tracking

Many countries perform internet censorship in an attempt to control the information and material that its population can access. With no standard way that this is performed, most countries build a bespoke platform to carry out their aims. Information targeted for censorship is set at the state level, and then this is enforced by technical controls implemented either directly by the national government or by Internet Service Providers.

The details of these systems are rarely made public. As they each target information on the internet in different ways it can be difficult to gather details on what exactly they block, or how exactly they do it. This lack of knowledge can lead to situations where we experience unknown behaviour on the internet.

Lack of understanding can lead to unpredictable behaviour on the internet. Network traffic can be interfered with in ways that wasn't intended. In some cases this can happen in situations where neither the sender or receiver are under the direct jurisdiction of the censorship regime affecting them.

Unlike surveillance which can be passive, for censorship an observable action must take place. This gives us an opportunity to study these actions. We can observe when network connections are reset, packets are dropped, or incorrect results are given to queries. These actions allow us to study how such systems are implemented, and the nature of the content that they're blocking.

My work focuses on the technical implementation of these internet censorship systems. How have they been implemented, and how do they go about blocking unwanted content? I initially focused on the Great Firewall of China, but eventually branch out to look at other internet censorship systems.

I also looked at censorship avoidance technologies. Users in censorious regimes turn to technologies such as Tor or VPNs in an attempt to access information they would not otherwise be able to access. I explored how users use these technologies to access censored information, and whether the use of these technologies themselves can be correlated with internet censorship.

Bio

Before going back to academia for his DPhil, Oliver was a penetration tester and security consultant. He's tested, audited or advised for a large part of the FTSE 100, including Banking and Finance, Energy and Oil, and the

Defence and Intelligence sectors. He has an MPhil from the Cambridge Computing Lab looking at anonymity on the web, with Professor Jon Crowcroft, and has spoken on cyber security matters for several news organisations, including the BBC, The Guardian, Sky News and Wired.

Publications

Oliver Farnan, Alexander Darer, and Joss Wright. "Analysing Censorship Circumvention with VPNs via DNS Cache Snooping." Proceedings of the 2019 IEEE Workshop on Traffic Measurements for Cybersecurity. IEEE, 2019.

Wright, J. A. E., A. Darer, and O. Farnan. "On identifying anomalies in Tor usage with applications in detecting internet censorship." Web Science Conference. 2018.

Darer, Alexander, Oliver Farnan, and Joss Wright. "Automated Discovery of Internet Censorship by Web Crawling." Web Science Conference. 2018.

Darer, Alex, Oliver Farnan, and Joss Wright. "FilteredWeb: A Framework for the Automated Search-Based Discovery of Blocked URLs". Network Traffic Measurement and Analysis Conference. 2017.

Farnan, Oliver, Alexander Darer, and Joss Wright. "Poisoning the Well - Exploring the Great Firewall's Poisoned DNS Responses". Workshop on Privacy in the Electronic Society. 2016.

Farnan, Oliver J., and Jason RC Nurse. "Exploring a Controls-Based Assessment of Infrastructure Vulnerability." International Conference on Risks and Security of Internet and Systems. Springer International Publishing, 2015.

ALASTAIR JANSE VAN RENSBURG

Supervisors: Michael Goldsmith and Jassim Happa, Department of Computer Science

Attack-Parametrised Attack Graphs

The complexity of computer network attacks requires a sophisticated understanding of network security. Attackers combine seemingly inconsequential vulnerabilities into damaging attacks. Attack graphs compactly represent the possible ways exploits can be combined in the network by attackers. Armed with an accurate, up-to-date and sufficiently-detailed attack graph model, network defenders could straightforwardly select the most critical vulnerabilities and weaknesses in their network, allowing them to perform the necessary actions to optimally mitigate the threat.

But attack graphs suffer from a number of problems that stand in the way. They rely heavily on data sources that were not intended to be used for this purpose, and have not been demonstrated to be reliable enough. Graphical models frequently suffer from complexity problems, and attack graphs are no exception. Once an attack graph is constructed, it requires analysis methods that are hard to verify, making any conclusions hard to justify.

In this thesis, I address each of these problems through a variety of theoretical methods. I begin by establishing a clear definition of attack graph, based on template-matching methods. This is used to provide a set of comparisons by which attack graph analysis techniques can be verified theoretically, demonstrating that some common analysis methods perform unreasonable assessments. From this basis, I examine the assumptions that underlie attack graph models, and propose two novel assumptions, the single-precondition assumption and the partitioned-preconditioned assumption. I also provide a motivating smart home example, together with a dataset of vulnerabilities.

I provide two independent contributions towards the generation and analysis of attack graphs; the first is a method to construct attack graphs without vulnerability data, making them easier to construct and allowing them to model zero-day vulnerabilities. The second is a method to parametrise attack graphs, enabling analysis to incorporate characteristics of the attacker and decisions of the defender, so that analysis can be performed across the full spectrum of possible attackers and defender decisions. Finally, these techniques are combined and presented with a collection of possible analysis methods, and applied to the smart home use case through a software implementation.

Bio

Alastair grew up in Cambridgeshire before going to the University of Warwick to study for a Masters in Mathematics. His research focus is on applying mathematical techniques to practical applications. Through his DPhil, Alastair aims to connect theoretical techniques to real cyber defence and create new methods that can be readily used by practitioners.

While at Oxford, Alastair has participated in a number of cyber Capture-the-Flag contests, and helped to found the Oxford Competitive Computer Security Society.

Publications

Janse van Rensburg, A., Nurse, J.R.C. and Goldsmith, M., 2016, Attacker-Parametrised Attack Graphs, Securware '16

Janse van Rensburg, A., Happa, J. and Goldsmith, M., 2015, Stereoscopic Cyber Visualisations

Janse van Rensburg, A., Nurse, J.R.C. and Goldsmith, M., 2015, Quantified Network Security

JANTJE SILOMON

Supervisor: Bill Roscoe, Department of Computer Science and Lucas Kello, Department of Politics and International Relations

Software as a Weapon

This thesis addresses the topic of 'Software as a Weapon' (SaaW) using a mixed methods approach, bringing together elements of Computer Science, International Relations, and Strategic Studies. To aid the public's understanding of the rapidly evolving concepts of cyber security, a multi-disciplinary approach is needed to define its fundamental notions, and place them in the context of existing theories The thesis therefore first addresses the nature of software, malware, and weaponised software via questionnaire-based public solicitation, with three groups of respondents: military officers, academics, and others. The results show that there is consensus among participants regarding the importance of defensive software capabilities for state security. However, depending on the training and background of respondents, questions pertaining to the nature of software exhibit statistically significant differences. For example, when deciding whether software should be treated like a physical object, or whether malware is a weapon. Yet, there is also consensus, such as that defensive software capabilities are vital to a state's security.

The second part of the thesis investigates the factors that contribute to an actor pursuing SaaW. It explores the proliferation debate and examines similarities and differences to traditional weapon domains, including nuclear, biological, and chemical weapons, as well as small arms and light weapons. These factors are then used to create a Bayesian Network model representing an actor's source of impetus. From such a model, it is possible to reason about the interplay of complementary and competing forces. By accounting for restraining and motivating elements, the model introduces objectivity to the debate on actor motivation in the cyber domain, giving a variety of stakeholders a tool to evaluate actors' software weaponising probabilities. To showcase and evaluate this model, three different actors are used, representing terrorists, state powers, and generic attackers. Quantitative data is combined with qualitative interviews, populating network nodes with prior probabilities and relative weightings of observed dependencies. An approach of weighting relative parent-nodes' influence strength is implemented, creating a linearly growing set of probability distributions. The results show that the probability of the generic actor pursuing SaaW is uncertain, which captures the nature of this scenario well. The state actor also shows ambivalence, but in this case high restraints are being countered by almost equally high capabilities, whilst motivating forces are low. The terrorist actor on the other hand has a medium to low probability, driven by a lack of capabilities and limited motivations despite very low retraining factors.

Overall, this thesis emphasises the multi-disciplinary nature of cyber security, and provides novel tools and concepts from Computer Science, International Relations, and Strategic Studies to understand SaaW.

Bio

Jantje completed her Bachelor's Degree in Computer Science, before spending some time in South East Asia, predominantly China. Upon returning to London, she worked in academia and industry, whilst also gaining an Master's Degree in International Security and Global Governance.

Publications

Silomon, J.A. and Roscoe, A.W., 2017, July. Attitudes Towards Software as a Weapon. In MCCSIS ICT, Society and Human Beings, 2017 International Conference on (pp. 119-126).

Silomon, J.A. and Roscoe, A.W., 2017, September. Software and Malware Capabilities: Opinions on (Inter) national Security. In Cyberworlds (CW), 2017 International Conference on (pp. 96-102). IEEE.

Silomon, J.A. and Roeling, M.P., 2018. Assessing Opinions on Software as a Weapon in the Context of (Inter) national Security. In Transactions on Computational Science XXXII (pp. 43-56). Springer, Berlin, Heidelberg.

Silomon, J.A.,2018. Factors Contributing to the Proliferation of Software as a Weapon. In Cyber Warfare and Security (ECCWS), 2018 European Conference on.

MATTHEW SMITH

Supervisor: Ivan Martinovic, Department of Computer Science

Measuring Operational Realities of Security and Privacy for Deployed Avionics

One of the fundamental components of modern aviation is communication between the ground and an aircraft. This is usually facilitated by electronics on board an aircraft, known as avionics. Such communication allows for the safe operation of airspace with aircraft kept sufficiently far apart. This is done with voice and data links, both of which are designed for efficiency, safety and reliability. Recent research has shown that some key aviation data communications – namely new air traffic control surveillance mechanisms - are insecure.

My thesis aimed to expand upon this research by looking at the security of other widely used avionics. The work is broadly divided into two sections: first is a measurement study on security and privacy in the Aircraft Communications Addressing and Reporting System (ACARS), with the second part looking at pilot response to theoretical attacks on safety-critical systems.

ACARS can be described as form of text messaging for aircraft. It has grown beyond its original intention by some margin, with passenger aircraft now using it for a range of purposes including weather updates, airport information and maintenance messages. Anyone can collect ACARS messages with cheap, off-the-shelf hardware. In light of this, my work identified and measured the leakage of sensitive information by privacy-sensitive aircraft operators due to their usage of ACARS. Often, this would involve state or business jets attempting to hide from Flightradar24 but transmitting course- or fine-grained location data via ACARS.

Moving to look at more speculative radio-based attacks, the second part of my thesis considers the impacts of attacks on safety-critical systems and whether normal flight crew behaviours will mitigate them. We assessed this by inviting professional airliner pilots to fly scenarios in our flight simulator, in which we implemented three attacks on landing, collision avoidance and ground proximity warning systems. Our results indicate that attackers would struggle to heavily erode safety but could cause disruption with significant economic and logistical consequences.

Although such attacks on avionics have considerable consequences, addressing them is a much greater challenge than patching security in. Until new, secure systems can be designed, certified and deployed – a process which could take decades – other approaches will be needed in the near term. We briefly consider these with the primary methods including crowd-sourced attack detection, phasing out insecure systems and training on how to identify when systems are under attack.

Bio

Matt is part of the System Security Lab lead by Prof. Ivan Martinovic. His work looks at cyber security in aviation, focussing on the security challenges in avionic communications. This comes at a time when aviation is undergoing a period of change, pushing towards safer, more efficient and faster travel - of which avionic communications form a critical component.

Before studying as part of the CDT, he received a MEng in Computer Science from the University of Warwick. Since he finished his DPhil, he has continued to work in the area of aviation security, taking up a role as a Postdoctoral Research Associate at Oxford.
Outside of work, Matt enjoys all things cycling, outdoors and finding new music.

Publications

Schäfer, M.; Strohmeier, M.; Smith, M.; Fuchs, M.; Lenders, V. & Martinovic, I. (2018) 'OpenSky Report 2018: Assessing the Integrity of Crowdsourced Mode S and ADS–B Data' in 'Digital Avionics Systems Conference (DASC), 2018 IEEE/AIAA 37th'.

Smith, M.; Moser, D.; Strohmeier, M.; Lenders, V. & Martinovic, I. (2018), 'Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS)', Proceedings on Privacy Enhancing Technologies 2018(3), 105--122.

Strohmeier, M.; Smith, M.; Lenders, V. & Martinovic, I. (2018), The real first class? Inferring confidential corporate mergers and government relations from air traffic communication, in 'IEEE European Symposium on Security and Privacy (EuroS&P) 2018'.

Schäfer, M.; Strohmeier, M.; Smith, M.; Fuchs, M.; Lenders, V.; Liechti, M. & Martinovic, I. (2017), OpenSky Report 2017: Mode S and ADS-B Usage of Military and other State Aircraft, in 'Digital Avionics Systems Conference (DASC), 2017 IEEE/AIAA 36th'.

Strohmeier, M.; Smith, M.; Schäfer, M.; Lenders, V. & Martinovic, I. (2017), Crowdsourcing security for wireless air traffic communications, in 'Cyber Conflict (CyCon), 2017 9th International Conference on', pp. 1--18.

Smith, M.; Moser, D.; Strohmeier, M.; Lenders, V. & Martinovic, I. (2017), 'Analyzing Privacy Breaches in the Aircraft Communications Addressing and Reporting System (ACARS)', arXiv preprint arXiv:1705.07065.

Smith, M.; Moser, D.; Strohmeier, M.; Lenders, V. & Martinovic, I. (2017), Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS, in 'International Conference on Financial Cryptography and Data Security', pp. 285--301.

Schäfer, M.; Strohmeier, M.; Smith, M.; Fuchs, M.; Pinheiro, R.; Lenders, V. & Martinovic, I. (2016), OpenSky report 2016: Facts and figures on SSR mode S and ADS-B usage, in 'Digital Avionics Systems Conference (DASC), 2016 IEEE/AIAA 35th', pp. 1--9.

Smith, M.; Strohmeier, M.; Lenders, V. & Martinovic, I. (2016), On the security and privacy of ACARS, in 'Integrated Communications Navigation and Surveillance (ICNS), 2016', pp. 1--27.

Strohmeier, M.; Schäfer, M.; Smith, M.; Lenders, V. & Martinovic, I. (2016), Assessing the Impact of Aviation Security on Cyber Power, in 'Cyber Conflict (CYCON), 2016 8th International Conference on', pp. 223--241.

Strohmeier, M.; Smith, M.; Moser, D., Schäfer, M.;Lenders, V. & Martinovic, I. (2018), Utilizing Air Traffic Communications for OSINT on State and Government Aircraft, in 'Cyber Conflict (CYCON), 2018 10th International Conference on', pp. 299--317

CHRISTIAN VAAS

Supervisor: Ivan Martinovic, Department of Computer Science

Physical phenomena as proof for authentication

For centuries, methods to obtain location information were crucial for our economic success. While initially requiring expert training and cumbersome tools like astrolabes and compasses, advances in material and engineering sciences have brought the ability to determine one's position on Earth to our fingertips. Devices as small and mobile as smart phones can now acquire and process location information.
Fuelled by this new data source, social media companies immediately realised the potential to enhance their users' experience and embedded location-based features into their products. Simultaneously, platforms which allow users to use location information as triggers for automation tasks emerged.

Beyond these use cases for entertainment and convenience, recent advances in academic and industrial research have started to leverage location information for security and safety purposes. While the advantages of location-aware mobile systems to improve security are undisputed, methods to ensure the reliability of location information and minimise the impact on user privacy still require further research.

In this dissertation, we aim to extend the knowledge about security and privacy implications of location information. To achieve this, we first analyse the different paths a mobile system can come in contact with this type of information. Based on these insights, we identify threats associated with the acquisition and processing of location claims. We recognise that in many cases, the absolute location of mobile devices is not needed but rather their constellation is sufficient. For example, the proximity of two devices can aid to validate location claims before relying on them for security or safety critical applications. We propose to use the trajectory a device takes to approach a location as that location's fingerprint. To show the feasibility of this idea and its potential applications, we evaluate two scenarios: user authentication and collective awareness in future intelligent transportation systems.

Finally, we analyse the consequences of data sharing for user privacy. More specifically, we investigate Vehicular Ad-hoc Networks (VANETs) as an open network where location information is essential to ensure its safe operation but also vastly available to malicious actors. We develop solutions to improve passenger privacy while providing more fine grained accountability in these networks which are a cornerstone in the future of intelligent transportation systems.

Bio

Christian started his academic career in Germany at the Technical University of Munich where he graduated with a Bachelor in Computer Science. Led by his interest in Software Engineering, he joined the Elite Graduate Program at the University of Augsburg pursuing a M.Sc. he completed his DPhil as part of the system's security lab, his research focuses on authentication using cues from the physical world. At the moment he is working on location verification to enable the secure platooning of vehicles in cities.

Publications

Vaas, C., Juuti, M., Asokan, N. and Martinovic, I., 2018, April. Get in Line: Ongoing Co-Presence Verification of a Vehicle Formation Based on Driving Trajectories. In Security and Privacy (EuroS&P), 2018 IEEE European Symposium on (pp. 199-214). IEEE.

Juuti, M., Vaas, C., Sluganovic, I., Liljestrand, H., Asokan, N. and Martinovic, I., 2017, June. STASH: Securing transparent authentication schemes using prover-side proximity verification. In Sensing, Communication, and Networking (SECON), 2017 14th Annual IEEE International Conference on (pp. 1-9). IEEE.

Juuti, M., Vaas, C., Liljestrand, H., Sluganovic, I., Asokan, N. and Martinovic, I., 2017, June. Implementing Prover-Side Proximity Verification for Strengthening Transparent Authentication. In Sensing, Communication, and Networking (SECON), 2017 14th Annual IEEE International Conference on (pp. 1-2). IEEE.

Vaas, C. and Happa, J., 2017, April. Detecting disguised processes using application-behavior profiling. In Technologies for Homeland Security (HST), 2017 IEEE International Symposium on (pp. 1-6). IEEE.

MEREDYDD WILLIAMS

Supervisors: Sadie Creese and Jason Nurse, Department of Computer Science

The Privacy Paradox and Smartwatch Educational Games

In opinion polls and surveys, the public claim concern for their privacy. However, we often fail to act to protect our data. This disparity between claim and behaviour is known as the Privacy Paradox. As emerging technologies are unfamiliar, interactive and data-hungry, this issue is likely to only increase. Therefore, our research seeks to: a) identify those devices most at risk; b) uncover those factors which are most influential; and c) implement/evaluate techniques to encourage privacy-protective behaviour. Through initial work, we found that Internet-of-Things (IoT) products faced the greatest threat. Wearable devices were at particular risk, since users rarely used their privacy settings. We then conducted in-depth interviews with product owners, discovering that a lack of awareness is the main issue. Since awareness campaigns are frequently ineffective, we turned our attention to interactive educational games. Our online prototype was successful in a trial with 504 wearable owners. Based on this, we developed the first smartwatch privacy game. Through a 52-day longitudinal study, our Android Wear app encouraged individuals to change their behaviour. With the game proving influential, we recommend such apps as a low-cost and interactive alternative to awareness campaigns.

Bio

Meredydd is conducting research for a PhD in Cyber Security at the University of Oxford. He focuses specifically on privacy, behaviour change and Internet-of-Things devices. Prior to joining Oxford, he completed an MPhil with Distinction in Advanced Computer Science at Christ's College, University of Cambridge. He specialised in security for his Master's thesis, researching Denial-of-Service attacks with Dr Robert N M Watson. He received his undergraduate degree from Aberystwyth University, completing a First-Class BEng (Hons) in Software Engineering. His dissertation also pursued a security theme, as he developed a cryptographic application alongside Prof Reyer Zwiggelaar. He was awarded Aberystwyth's Evan Morgan Scholarship for Computer Science on admittance (2008), and received their best Computer Science Graduate award on completion (2012).

Alongside his research, Meredydd has been the lead Teaching Assistant for the Computer Security and Advanced Security practicals. He also tutored the Computer Security Major Tutorial for the Worcester College Visiting Student Programme. He is a departmental Student Ambassador, a member of their Equality and Diversity Committee (EDC) and a Computer Science author for the Oxplore initiative. Outside of academia, he enjoys sports, politics and history. He is due to complete in September 2018 and is favouring consultancy roles in industry.

Publications

Williams, M., Nurse, J. R. C. and Creese, S., 2018. (Smart)watch out! Encouraging privacy-protective behavior through interactive games. International Journal of Human-Computer Studies (under review).

Housley, W., Webb, H., Williams, M., Procter, R., Edwards, A., Jirotka, M., Burnap, P., Stahl, B.C., Rana, O. and Williams, M., 2018. Interaction and transformation on social media: the case of Twitter campaigns. Social Media + Society, 4(1). Sage.

Williams, M., Nurse, J. R. C. and Creese, S., 2017. "Privacy is the boring bit": User perceptions and behaviour in the Internet-of-Things. In Proceedings of the 15th International Conference on Privacy, Security and Trust (PST).

Williams, M., Yao, K. K. K. and Nurse, J. R. C., 2017. ToARist: Creating an augmented reality tourism app through user-centred design. In Proceedings of the 2017 British HCI Conference. BCS.

Nurse, J. R. C., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., Goldsmith, M. and Creese, S., 2017. An assessment of the security and transparency procedural components of the Estonian Internet voting system. Human Aspects of Information Security, Privacy, and Trust in Lecture Notes in Computer Science, 10292 (pp. 366-383). Springer.

Williams, M., Nurse, J. R. C. and Creese, S., 2016. Privacy salience: Taxonomies and research opportunities. IFIP Advances in Information and Communication Technology 498 (pp. 263-278). Springer.

Williams, M., Nurse, J. R. C. and Creese, S., 2016. The perfect storm: The privacy paradox and the Internet-of-Things. In 2016 11th International Conference on Availability, Reliability and Security (ARES), (pp. 644-652). IEEE.

Williams, M. and Nurse, J. R. C., 2016. Perspectives on privacy in the use of online systems. In Proceedings of the 2016 British HCI Conference. BCS.

Williams, M., Axon, L., Nurse, J. R. C. and Creese, S., 2016. Future scenarios and challenges for security and privacy. In 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry (RTSI). IEEE.

Williams, M. and Nurse, J. R. C., 2016. Optional data disclosure and the online privacy paradox: A UK perspective, Human Aspects of Information Security, Privacy, and Trust in Lecture Notes in Computer Science, 9750 (pp. 186-197). Springer.

Williams, M., 2015. A study of society's perception of online privacy. In Proceedings of the 1st Interdisciplinary Cyber Research Workshop.

Presentations and Academic Posters

Smartwatches and information privacy: Do users practice what they preach? 2018. 2018 Connected Life Conference.

Evaluating smartwatch privacy games through a longitudinal study. 2018. 2018 Oxford Computer Science Conference.

Encouraging protective behaviour through smartwatch privacy games. 2018. 2018 Oxford Computer Science Conference. (Poster, Best poster award).

Privacy in the Internet-of-Things: Perceptions and behaviour. 2017. The 13th Symposium on Usable Privacy and Security. (Poster).

"Privacy is the boring bit": User perceptions and behaviour in the Internet-of-Things. 2017. 2017 Oxford Computer Science Conference.

A taxonomy of privacy salience research. 2016. 2016 IFIP Summer School.

The privacy paradox and the Internet-of-Things. 2016. 2016 Oxford Computer Science Conference. (Best abstract prize).

An interactional analysis of Twitter collective action. 2016. 2016 Connected Life Conference.

"We have much more fighting to do": Analysis of twitter-based online campaigns. 2015. Social Media, Activism, and Organisations 2015.

DANIEL WOODS

Supervisor: Andrew Simpson, Department of Computer Science

The economics of cyber risk transfer

Markets selling formal promises about cyber risk are booming. The cyber insurance market collects $4 billion in premiums and vendors have started to attach warranties to InfoSec products. If prices reflect information as Hayek argued, then these products could improve cyber risk management decisions. This DPhil investigates three different mechanisms to do so.

We first study these markets empirically. A quirk of insurance regulation provided access to 26 different cyber pricing schemes from insurers in California. We provide empirical observations on how premiums vary by coverage type, amount, firm characteristics, and over time. A separate study uses mixed methods to explore how underwriters in the Lloyd's of London market assess risk.
Perversely, a cyber insurance market exists before cyber loss data has been collected in earnest, unlike say the first life insurance policies that were built using historical mortality data. We developed a method to infer cyber loss distributions from insurance prices. Our approach provides probability estimates for cyber losses of different amounts. These estimates can be tailored to firm size, industry or incident type.

A different contribution considers how insurers might use claims data to improve their understanding of cyber risk. We introduce an economic model using Monte Carlo simulations. The results suggest the market tilts towards monopoly when uncertainty about risk controls is high. This could explain why a few firms sell the majority of cyber insurance at present.

Finally, we introduced a model to explore how consumers can use warranties to identify higher quality InfoSec products. The model derives a number of inferences that can be made based on the warranty offered. Further, warranties can create separating a equilibrium pushing the market towards more effective products. However, collecting cyber warranties suggests these products are more marketing tricks than a market fix at present.

Publications

The county fair cyber loss distribution: Drawing inference from insurance prices. Daniel W Woods, Tyler Moore, and Andrew C Simpson. In Proceedings of The 18th Workshop on the Economics of Information Security (WEIS 2019), 2019.

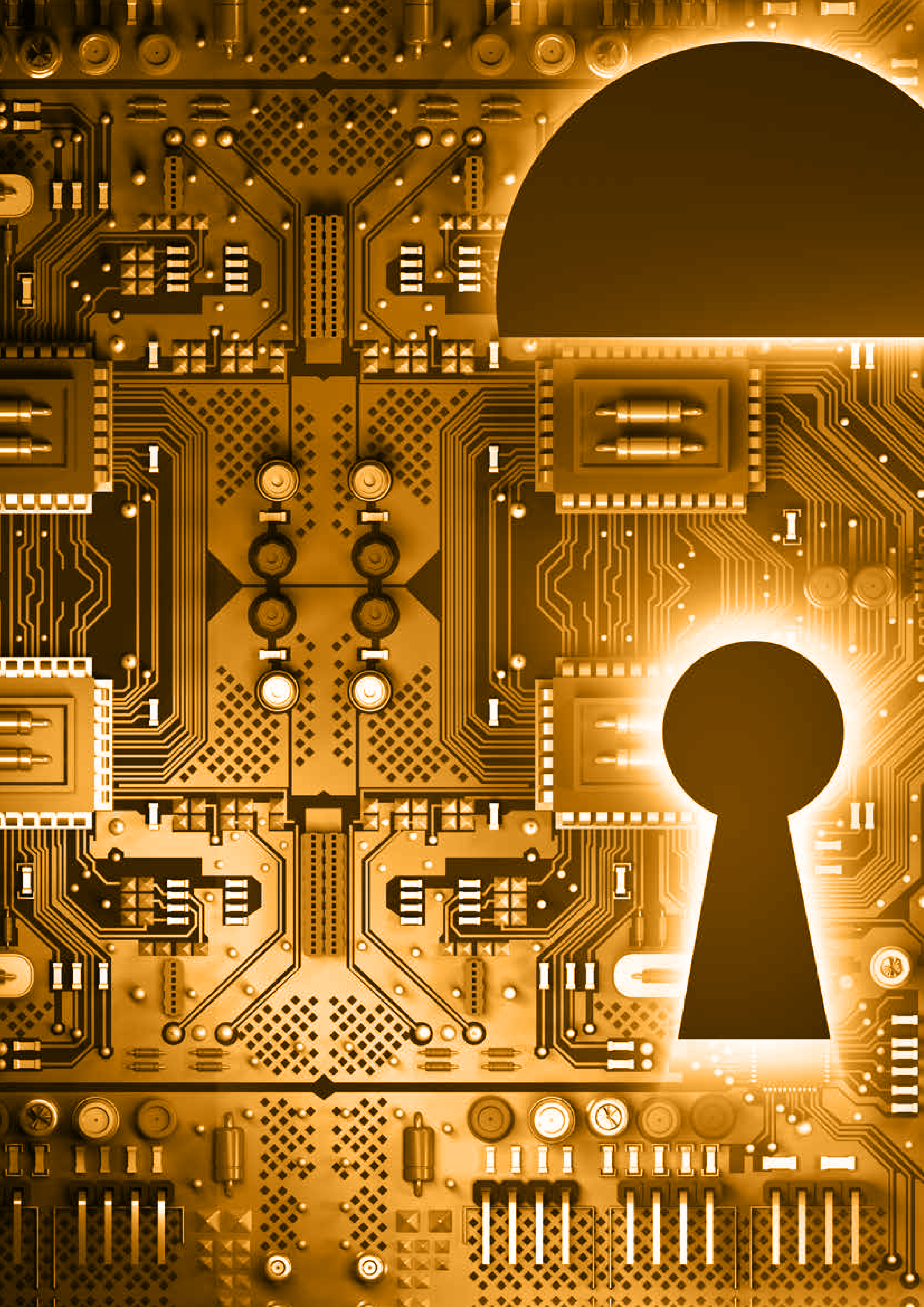
Cyber-warranties as a quality signal for information security products. Daniel W Woods and Andrew C Simpson. In International Conference on Decision and Game Theory for Security, pages 22–37. Springer, 2018.

Monte Carlo methods to investigate how aggregated cyber insurance claims data impacts security investments. Daniel W. Woods and Andrew C. Simpson. In Proceedings of The 17th Workshop on the Economics of Information Security (WEIS 2018), 2018.

Mapping the coverage of security controls in cyber insurance proposal forms Daniel W. Woods, Ioannis Agrafiotis, Jason RC Nurse and Sadie Creese. In Journal of Internet Services and Applications. Vol. 8. No. 1. Pages 8. 2017.

Policy measures and cyber insurance: A framework. Daniel Woods and Andrew C. Simpson. In Journal of Cyber Policy, 2(2):209 - 226, 2017.

Daniel W Woods and Tyler Moore. Does insurance have a future in governing cybersecurity?. IEEE Security & Privacy.



ICO Funded Research on Data Protection in Smart Homes

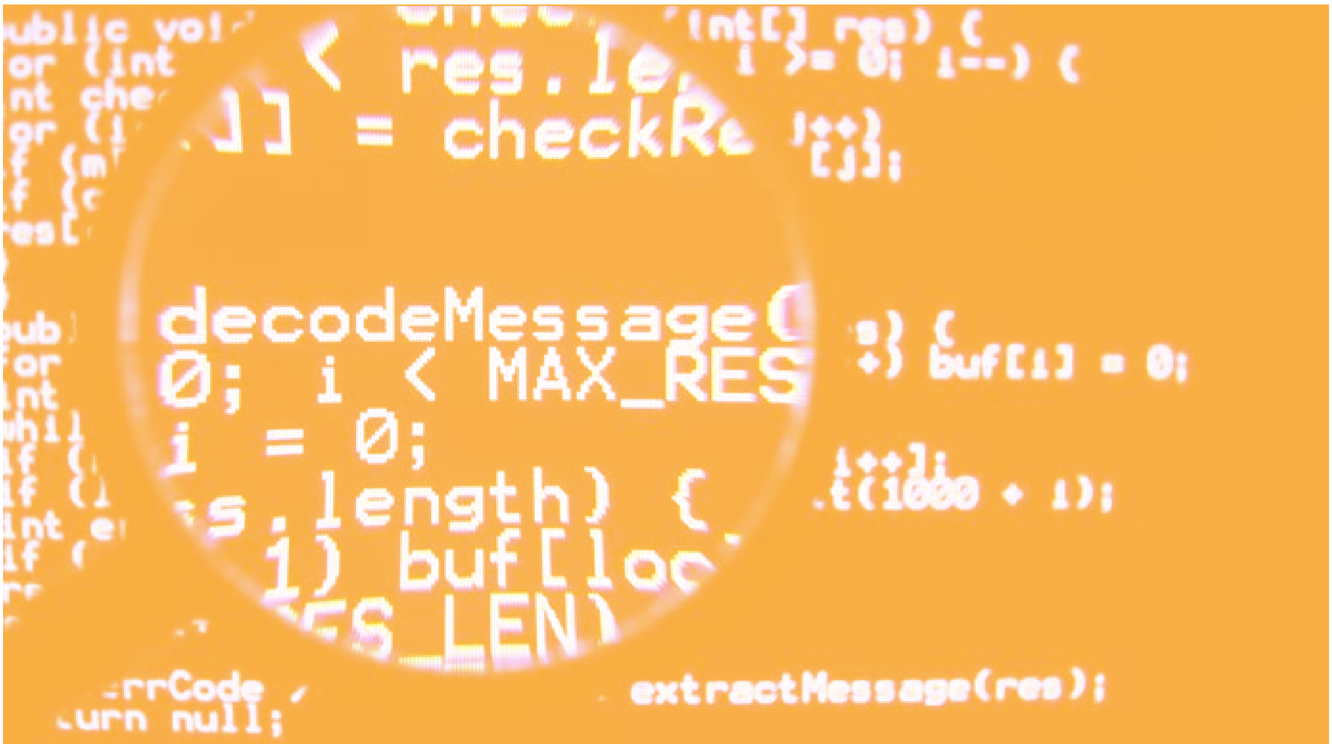
William Seymour and Martin Kraemer discuss their new project 'Informing the Future of Data Protection in Smart Homes'

The rollout of the European General Data Protection Regulation (GDPR) has had a big impact in the cyber security world, with many organisations moving to update their practices in time for the end of May. Our DPhil projects to date have been investigating privacy and security generally applied to smart homes, but this project provides an opportunity to learn from the mistakes of the past and explore the ways in which we might design new devices that integrate data protection principles from the beginning.

Funded by the UK Information Commissioner's Office, we will be undertaking a long-term ethnographic study into how households cope with data protection when adopting new smart home technologies. This involves initial considerations related to purchase and setup smart devices in the home. As households become more familiar with the intricacies of their technology and its use, they will begin to form preferences; our goal is to employ insights and experiences of this work, ultimately to create new (speculative) design patterns, features, and envision interfaces which support householders throughout the process. The project also includes designers and product developers of smart home devices in this project, aiming for usable design artefacts.

Article 25 of the GDPR states that organisations should consider "data protection by design and by default" when designing devices and services. A simple example of this might be a kettle that allows users to opt out of sending analytics data in exchange for not having the kettle learn when to turn on in the morning. But for smart cameras, voice assistants, and thermostats that have more complex data collection practices (and often business models that rely on data collection), it is not always clear what form this would take. We aim to make this requirement more relatable through our ethnographic work, and we support the work of product designers and developers with new design artefacts. A more detailed overview of the project can be found in a position paper we published at the 2019 CHI Conference on Human Factors in Computing Systems.

The six month ethnographic study begins in July, with 8 households taking part. Speculative design and practitioner interviews are scheduled to take place from Q4 2019 onwards. If you'd like to learn more or participate in expert focus groups and interviews, please contact william.seymour@cs.ox.ac.uk or martin.kraemer@cs.ox.ac.uk.



5th Annual Inter-CDT Conference: Cyber Espionage

Anjuli R. K. Shere, CDT18

This year's Inter-CDT conference between Royal Holloway, University of London (RHUL) and the University of Oxford put an interdisciplinary twist on its 'Cyber Espionage' theme, à la Bletchley Park. The two-day event, hosted at Worcester College, Oxford, brought together public and private sector experts for a holistic review of the state of the art of digital spy work.

After extensive deliberation, our theme was chosen because of its relevance to a variety of contemporary issues affecting every stratum of society, from the distressing prevalence of domestic spyware apps to massive data leaks of state secrets online. In contrast, Prof. Andrew Martin, welcomed us to the conference with a short keynote reminding us of the positive historic implications of cyber espionage and of the impact that events such as ours could have on policy.

To begin, Liam Gearon, Associate Professor at the University of Oxford's Department of Education, introduced us to the concept of the "Universities-Security-Intelligence Nexus", which describes the intellectual exchange between academia, national security communities and intelligence agencies. He emphasised that the days of students being tapped on the shoulder in shadowy Oxbridge corridors are behind us; now, figureheads of security and intelligence institutions speak openly at university conferences, such as former FBI Director James Comey's speech at the 2017 Boston Conference on Cyber Security. While academics have recently embraced the study of "security", previously solely the domain of military and intelligence organisations, Gearon inferred that these agencies exploit perceptions of universities as liberal bastions of free speech and knowledge-sharing. Foreign academics on campus present opportunities to monitor and profile potential industrial or state-sanctioned spies, and multi-stakeholder reports advancing security-related theories are rife. This kind of activity, of which university boards and staff must surely be aware, stands in stark contrast to critical student countercultures of the 20th century, notably the anti-military protests that resulted in the 1970 Kent State shootings. Rather than coveting the "secret knowledge" that characterised espionage communities of the past, Gearon stressed that researchers in the field of cyber security work at the novel and "ethically fraught" interface of security and academia; and that they must use their unique perspective of the nexus to assess the threats both opposed and posed by national security and intelligence agencies.

Elaborating on this new dearth of secrecy, Niamh Healy of Ridgeway Information then spoke on the challenges and benefits of open-source intelligence gathering (OSINT). This is a skillset that relies on scrutinising publicly available data to unearth truths that were hidden in plain sight and to debunk lies propagated by powerful people. Unlike traditional intelligence analysis, OSINT is often practiced by civilians as its tools and techniques – and most importantly, its subject matter – are freely and widely available. Significantly, this makes OSINT vital for verification of state-level commitments, such as nuclear non-proliferation. Government capabilities and their professed lack of nuclear ambition may not align, a fact which would previously have been discovered by human intelligence operatives, endangered by virtue of their physical presence in such highly sensitive spaces. Today, Healy told us, eagle-eyed OSINT investigators around the world can recognise the structures that are indicative of a secret nuclear processing facility and can decry governments for violating international norms and agreements, corroborated by many of their peers. This avoids states having to initiate condemnation of each other, so that they can claim that any escalation of tensions is necessary and publicly induced. There are even examples of global open-source investigative journalist collectives combing through barely accessible multilingual online records to supplement state-sanctioned cyber espionage, notably Bellingcat's unmasking of the GRU operatives responsible for the 2018 Skripal poisoning.

While there are many applications of cyber espionage methods, RHUL's Executive Director of the Institute for Cyber Security Innovation, Rob Carolina discussed with us the legal and political implications of spy-work. Talking us through the difficulty of legislating on dual use technologies and the principles laid down by the Tallinn Manual (and subsequently Tallinn 2.0), Carolina argued that "cyberspace does not legally exist" and as such cyber espionage is simply an extension of conventional spy work. In practice, in spite of the convoluted web of cyber activity that is spun by separating actors and servers by state borders, assessments of the legality of any cyber-attack boil down to whether the actions taken were legal in the countries from which they were effected and in which they had an effect. Offensive cyber operations can be classed as a violation of state sovereignty, which remains of paramount importance in international relations. However, Carolina was quick to inform us that cyber espionage "per se" (i.e. conceptually) is not illegal. Rather, it is certain invasive actions undertaken to enable said espionage that are prohibited by law, such as taking down a secure communication network to coerce adversaries into revealing their plans on an insecure channel. This distinction is crucial, as it encourages states' strategies to rely on the obfuscation of those responsible for the mass collection or manipulation of information through cyber espionage.

Conversely, one situation in which the perpetrators of cyber spying are not anonymous but are still difficult to effectively prosecute is that of intimate partner espionage. Leonie Tanczer, Lecturer in International Security and Emerging Technologies at University College London (UCL), closed day one of the conference with a workshop intended to link research and the socio-technical practices necessary to eradicate technology-enabled domestic abuse. In a world where individuals are connected to society through social media networks accessible on personal devices, controlling someone's devices is often a gateway to (and sometimes synonymous with) controlling their existence. Tanczer introduced her audience to the "Gender and Internet of Things (IoT)" project that studies the way that smart technologies can exacerbate domestic abuse that is overwhelmingly targeted against women because of gendered conventions such as men managing the choice and settings of household devices. The IoT not only expands the attack surface for abusers, but also increases the range of ways in which they can stalk and harass their targets. Attackers no longer simply passively observe their victims' activity, e.g. by monitoring the movements of their GPS-enabled phones. Now, they can legally purchase any number of "spyware" apps that allow complete surveillance and control of a device – from activating live audio and video capabilities without warning the user to allowing abusers to both screen and spoof messages. This is a very different scenario to that of a long-distance adversary, but technology-enabled intimate partner abuse is much more pervasive and difficult to challenge. These "hidden" apps are distressingly easy to find online, usually advertised as a way for concerned parents to check that their children are not engaging in dangerous activities, but do not appear visibly on the target device. However, despite their flimsy legal disclaimers, many consumers are adults who use the apps to flout the right to privacy of their unwitting partners or employees. To counter this trend and mitigate its devastating effects on victims, Tanczer's team use the limited information available from shelters and social workers to craft feasible and useful recommendations for both those living with abuse and national policymakers addressing the issue. Tanczer ended her talk on much the same note as that in which Gearon had concluded his: urging us, as researchers, to centre our work around restoring the security of marginalised communities.

Our opening speaker for the final day of the conference, RHUL Professor of information security, Stephen Wolthusen also emphasised the ease with which modern devices may be co-opted for nefarious means. Taking a much more technical perspective on the issue of "cyber intelligence and offensive operations", Wolthusen spoke about the deep-rooted fundamental vulnerabilities that can allow device hardware and firmware to be compromised and the systemic failings resulting from a culture of externalisation and convoluted supply chains that provide ample opportunities for devices to be hacked while under the purview of negligent third-parties. Although there is an awareness of the risks resulting from outsourcing production of electronic communications equipment, even the NSA's attempts to manufacture hardware and software in-house were short-lived due to market pressures and associated financial constraints. Thus, the trustworthiness of devices and software cannot be guaranteed, even when it is officially verified. Exploitation of such vulnerabilities can lead to mass intelligence gathering, but still less data deluge than would be expected by commandeering online channels of communication. Wolthusen explained that conventional intelligence communities, like signals intelligence (SIGINT) analysts, are currently processing innumerable exabytes of data due to the vastness of the internet – a challenge that is only intensifying as time goes on. Improved cryptography and a societal trend towards stronger end-to-end encryption have increased the difficulty of intercepting and decoding intelligence, causing issues with international signalling of capabilities and intentions. Utilising the fundamental vulnerabilities discussed is therefore necessary to ensure that state-mandated espionage activities "yield operationally relevant insights" and avoid inadvertent escalation. As all states engage in cyber espionage, anonymity and plausible deniability are crucial, which occasionally means not publicly reacting to revelations of a 6-month Border Gateway Protocol (BGP) hijacking of internet traffic from Toronto (rerouted via Beijing) to Seoul in 2018.

To vary the pace of the event, Wolthusen's presentation was followed by four student lightning talks, two given by Amy Ertan and Dray Agha of Royal Holloway, and two by Freddie Barr-Smith, Fatima Zahrah and Julia Slupska of the University of Oxford. Ertan's talk deconstructed the new term "algorithmic warfare", as it has been given various definitions. Agha then discussed Russian conflict doctrine regarding the weaponisation of information and physical territory. Shifting to a focus on organisational rather than national security, Barr-Smith advocated for a more widespread acceptance of penetration testing as a mechanism for establishing the current state of defences against skilled adversaries. Finally, Zahrah and Slupska spoke about their project on how modern technology is abused to facilitate intimate partner violence. The talks highlighted the broad range of potential subjects that can be affected by cyber security concerns and gave a brief but very informative glance at some of the research that is being conducted at both universities.

Our final speaker was David Pickard, an independent cyber security researcher with experience working for both the UK government and in industry. To avoid rehashing the international relations angle that had already been explored throughout the conference, Pickard educated us on the operational considerations relevant to cyber espionage (without divulging any classified information). He emphasised the interdisciplinary nature of cyber security work, relative to the specific psychological profiles that are typically attracted to and chosen for purely human intelligence (HUMINT) or SIGINT work. As he had observed all the preceding sessions, Pickard was able to recognise and fill in gaps in our understanding of how cyber espionage collaborations differ from the traditional handler-operative relationship, due to the necessity of analysts being aware of both large amounts of intelligence and the strategic overview. Logistical considerations are key, as ensuring that the guidance given to ministers travelling abroad is followed means acknowledging the feasibility of the advice and explaining to them the reality of foreign capabilities. Key to effective analysis is recognising anomalous behaviour that points to adversaries' methods of communication or patterns of activity, said Pickard. Whether this is noticing that members of a drugs-running operation are all active on a particular ride-sharing app or being aware that lots of pizza being ordered to a military hub might be indicative of significant meetings being held, operational security measures all have weaknesses.

This advice was the perfect inspiration for our closing activity, A Capture the Flag (CTF) competition designed and hosted by three Oxford CDT researchers, Richard Baker, Alastair Janse van Rensburg and Yashovardhan Sharma. Framed as an opportunity to exploit security failures within a fictitious embassy, the CTF involved a plethora of hands-on challenges that ranged from highly technical (e.g. decoding an audio message in the form of recorded dual-tone multi-frequency signalling (DTMF) tones) to purely physical (e.g. lockpicking) and even to a combination of both, such as wiretapping a communications cable and then using specialist software to capture and interpret the data collected. Nothing could have better encapsulated the message of the conference: that both cyber espionage and cyber security require a confluence of perspectives and skills to be effective, and that researchers have a responsibility to put our brains and hands to ethical use.

UNIVERSITY OF OXFORD
CENTRE FOR DOCTORAL TRAINING in CYBER SECURITY
ROYAL HOLLOWAY UNIVERSITY OF LONDON

INTER-CDT CONFERENCE: CYBER ESPIONAGE

How: To attend the conference, please register at **https://cdtconference-2019.eventbrite.com** or scan the QR code below:

What: Two days of interdisciplinary expert talks on cyber espionage

When: Thursday 2nd – Friday 3rd May 2019

Where: Worcester College, University of Oxford

Who: Open to all members of the Centres for Doctoral Training in Cyber Security at both the University of Oxford and Royal Holloway, University of London

Why: Annual Inter-CDT conference, organised by Oxford and RHUL's newest Cyber Security doctoral cohorts

The French Cyber Security & Defence Model: Political principles, strategic goals and threat perception

Arthur Laudrain, CDT18

From Ministries to national agencies or cyber commands, the amount of public institutions involved in cyber defence and security matters is multiplying in most states, in a trend that reflects the pervasive nature of the domain. France is no exception. From the Paris Call to a fully-fledged offensive doctrine, we have seen in recent months a revival of its efforts to secure its citizens and interests in cyber space. This short paper attempts to summarize the French cyber security and defence model, by analysing its main political concepts and principles, its states strategic goals and the evolution of its threat perception, over the last decade.

Political concepts, principles and goals

a) France' sovereignty, national and European strategic autonomy

France has a conceptualisation of sovereignty that makes it stand out of its peers. Baezner and Robin found in their comparative analysis that "France was unique among the states examined in that it used the word "sovereignty" more frequently and in different contexts."[1] Sovereignty, in its French understanding, cannot be restrained to hard sovereignty, i.e. the protection of its citizens, borders and other existential interests.[2] French sovereignty is a wide spectrum that implies strategic autonomy, a concept entailing 1) a high level of industrial and technological autonomy, and 2) an operational autonomy.[3] The latter is the ability to reach an informed decision and to take action, in particular in the context of political or military crises.

French strategic autonomy can be best described as neo-Gaullist, which relies on self-reliance. The perceived need for self-reliance played a major role in driving De Gaulle to transform France into a nuclear power and to leave NATO command in 1966. Some key historical events such as the 1940 surrender or the intelligence frustrations of the 1992 Gulf War further fuelled perceptions that France needed respectively a credible nuclear arsenal, and autonomous intelligence capabilities.[4]

This spirit of autonomy remains today, but with a wider pragmatic recognition of the need for cooperation and integration. France re-joined NATO command in 2009 for mainly pragmatism and influence reasons.[5] However the French nuclear arsenal remains outside of NATO and its intelligence apparatus outside of the 5-Eyes community. France' strategic autonomy is also reliant on a European strategic autonomy, which it seeks to develop. The Hubert Védrine report recommended that the country's return into NATO is accompanied by a strengthening of European defence integration and cooperation, especially in research and development.[6] It encourages the development of mutual interdependence with entities who share critical interests, particularly within the EU. This policy shift initiated in 1992 with the EU Common Foreign and Security Policy was confirmed in the 2008 White Paper, placing the EU as "a central tenet of [France's] security policy".[7] This central place was reaffirmed ever since, including in the last cyber strategy document.[8]

b) Domestic apparatus: Offense / defence separation

Domestically, the French approach contrasts with that embraced by the United States or the United Kingdom. Most notably, France assumes a clear separation between offensive and defensive cyber operations. This means that, contrary to the NSA or the GCHQ, France's leading agency for cybersecurity is exclusively dedicated to defensive operations and not part of the intelligence community. This is a defining element of the Cyber Strategy Review and infuses the whole structure of French cyberdefence. The rational is that having a distinct defensive agency separate from offense-oriented military intelligence agencies "facilitates the acceptance of state intervention [...] whether in public administration or the economic sphere".[9]

c) A counter-threat model based on direct communication rather than public attribution

[1] Marie Baezner and Patrice Robin, "Trend Analysis: Cyber Sovereignty" (Zurich: Center for Security Studies (CSS), ETH Zürich, 2018).

[2] Existantial interests are not clearly defined so that there remains strategic uncertainty, in the context of France's nuclear deterrence. See para. 159 of the 2017 Strategic Review.

[3] See Para. 157. "Revue stratégique de défense et de sécurité nationale," La Documentation Française (Paris: Présidence de la République, October 2017), http://www.ladocumentationfrancaise.fr/rapports-publics/174000744/index.shtml.

[4] The Military Intelligence Agency was created in the aftermath of the Gulf War. Claude Faure, "Bref historique des services de renseignement et de sécurité français contemporains," Revue historique des armées, no. 247 (June 15, 2007): 70–81, http://journals.openedition.org/rha/1843.

[5] André Dumoulin, "La France et l'OTAN : vers la normalisation ?," Courrier hebdomadaire du CRISP n° 2005, no. 20 (2008): 5–47, https://doi.org/10/d6rrtq.

[6] "The Védrine Report" (Paris: Présidence de la République, November 14, 2012), https://otan.delegfrance.org/The-Vedrine-report.

[7] Défense et Sécurité Nationale: Le Livre Blanc (Paris: O. Jacob : Documentation française, 2008).

[8] "Revue Stratégique de Cyberdéfense" (Paris: Secrétariat Général pour la Défense et la Sécurité Nationale, February 12, 2018), http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

[9] "Revue Stratégique de Cyberdéfense."

Peculiarities of the French model are not limited to its conceptualisation of sovereignty. On the diplomatic stage, France has also adopted a different stance than most of its counterparts.[10] A number of NATO allies are increasingly inclined to "name and shame" states involved in cyber attacks. One telling example can be found in October 2018, when the U.S., U.K., Canada and the Netherlands denounced Russian attempts at disrupting the Organization for the Prohibition of Chemical Weapons.[11] Paris expressed its solidarity but fell short of blaming Moscow.[12] Already in 2015, when what then-seemed-to-be ISIS took down TV5Monde in a major hack, no official attribution was made. ANSSI however briefed four dozen media outlets with details of its forensic investigation and indicators of compromise. These details were then analysed by private security firms which pointed the finger at persistent threat actor (APT) 28.[13] More recently, in the case of the #MacronLeaks, France did not issue any kind of attribution either. At the unveiling of the offensive cyber doctrine, Minister Parly revealed that an APT targeted email accounts of high-ranking officials between 2017 and 2018, with the objective of uncovering the navy's oil supply chain.[14] Though the Minister stopped short of explicitly recognizing the group's affiliation with the Russian Federation, she indirectly attributed the attacker's mode of operation to a specific group known as Turla.

France favours red phones over the megaphone

This does not mean that it does not have attribution capabilities. Attributing cyber-attacks is one of the main missions of the French cyberdefence apparatus. But even when it knows, France prefers forthright bilateral dialogues with Russia and other cyber powers.[15] In other words, it favours red phones over the megaphone,[16] in an overall counter-threat model.[17]

Objectives in cyber security and defence: Evolution and granularisation

Following the election of Emmanuel Macron to the Presidency and the creation of a new government, the new Prime Minister requests the SGDSN to write a new defence white paper. The Strategic Review for Defence and National Security, as it is then known, is released in 2017. It promotes digital sovereignty and cybersecurity to top priorities of national defence.[18]

In February 2018, the country's first National Strategy for Cyber Defence clarified both the organization and integration of cyber operations among all government entities[19] as well as the national and international legal framework surrounding their use.[20] It sets-out goals and processes as part of a "robust national cyber security and defence apparatus".[21]

The seven principles underpinning the Strategy are:

- To make the security of French information and communication systems a priority,
- To embrace a policy of active discouragement[22] and coordinated response,
- To fully exercise its digital sovereignty,
- To bring an efficient judicial response to cybercriminality,
- To promote a shared cybersecurity culture,
- To contribute to a trusted and safe digital Europe,
- To act internationally for a collective governance of cyberspace.
- To achieve said goals, the Strategy sets-out a number of policy-making and coordination processes. In practice, three main themes appear: Active discouragement, risk limitation and multilateralism.

Active discouragement

France has adopted a posture of active discouragement against advanced threats. It relies on direct communication with the adversary, as we have detailed earlier, and on an increasingly explicit declaratory strategy.

In January 2019 Minister Florence Parly unveiled the offensive and defensive cyber operations doctrines of the armed forces. The announcement is the latest and strongest step taken by the country as part of its declaratory strategy.[23] In response to cyber and other threats, France is "not afraid" of using cyber weapons.[24] The country did

[10] "Russian Cyber-Chill between DGSE and NSA," Intelligence Online, March 20, 2019, https://www.intelligenceonline.com/grey-areas/2019/03/20/russian-cyber-chill-between-dgse-and-nsa,108349805-art.

[11] "Canada, Western Allies Rebuke Russia over Alleged Global Hacking Campaign," accessed May 6, 2019, https://www.theglobeandmail.com/politics/article-canada-western-allies-rebuke-russia-over-alleged-global-hacking/.

[12] "France Diplomatie : Ministère de l'Europe et Des Affaires Étrangères, 'Royaume-Uni - Cyberattaques," October 4, 2018, https://www.diplomatie.gouv.fr/fr/dossiers-pays/royaume-uni/evenements/article/royaume-uni-cyberattaques-04-10-2018.

[13] Emmanuel Paquette, "Piratage de TV5 Monde: l'enquête s'oriente vers la piste russe," LExpress.fr, June 9, 2015, https://www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe_1687673.html.

[14] Florence Parly, "Stratégie Cyber Des Armées (Speech)," January 18, 2019, https://www.defense.gouv.fr/english/content/download/551517/9394183/20190118%20-%20Stratégie%20cyber%20des%20Armées.pdf.

[15] "Cyberattaques : Paris et Moscou en tête à tête," Libération.fr, November 11, 2018, https://www.liberation.fr/planete/2018/11/11/cyberattaques-paris-et-moscou-en-tete-a-tete_1691473.

[16] Florian Egloff, "The Politics of Publicly Attributing Cyber Incidents | Centre for Technology and Global Affairs," March 6, 2019, https://www.ctga.ox.ac.uk/article/florian-egloff-speaks-politics-publicly-attributing-cyber-incidents.

[17] Egloff.

[18] "Revue Stratégique de Cyberdéfense."

[19] "Revue Stratégique de Cyberdéfense."

[20] "France's Cyberdefense Strategic Review and International Law," Lawfare, March 23, 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

[21] In French as « Dispositif national de protection et de défense informatique robuste ». "Revue Stratégique de Cyberdéfense."

[22] France reserves its concept of deterrence (dissuasion) to the nuclear domain.

[23] Stéphane Taillat, "Signaling, Victory, and Strategy in France's Military Cyber Doctrine," War on the Rocks, May 8, 2019, https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/.

[24] Parly, "Stratégie Cyber Des Armées (Speech)."

not wait until then to perform offensive operations or even to publicly admit doing so. Such operations were first mentioned in the 2008 White Paper[25] and then again with more details in 2013. The case for proportional reprisals in response to a major attack was also made clearly by then-Defence Minister Jean-Yves Le Drian:

"In times of war, cyber weapons may be the response, or part of our response, to an armed attack [aggression armée], being of a cyber nature or otherwise."[26]

Risk limitation and infrastructure sanctuarisation

Risks that are inherent to cyberspace and operations are a recurrent topic in policy documents.

The offensive doctrine places great emphasis on the consideration and mitigation of political, legal and military risks.[27] It mandates a risk balancing exercise in the preparation and conduct of offensive operations: against the risk of escalation in an asymmetric environment, or against the risk of collateral or indirect damage on civilian infrastructures.

In terms of international law, the document recognizes not only the applicability of international humanitarian law to cyberspace, but of international human rights and customary international law more broadly as well. Another key theme of the document is the importance of protecting individuals and critical infrastructures from harm. The document presses to safeguard the "public core of the Internet" from hostile actors. This is a clear demonstration of support for a package of norms unveiled by the Global Commission for the Stability of Cyberspace on Nov. 8 in Singapore.[28]

Multilateralism and stakholderism

On the international stage, one of France's goals relates to the diplomatic process itself. The country seeks to maintain a form of inclusive multilateralism,[29] and in parallel to open-up debates on cyberspace governance to non-state actors. Its International Digital Strategy puts great emphasis into promoting an "open, diverse and trusted" cyberspace in which it envisions the EU as a key player.[30]

Approaching the issue from various stakeholders' perspectives, the Paris Call is an attempt to move away from the deadlock at the UN. Macron made the case for rebuffing what he described as a binary choice between "a Californian Internet and a Chinese Internet."[31] So far, he argued, these two opposite narratives have monopolized the debate and imposed two radically different yet unsatisfactory alternatives: either a model of mere technical governance led by Silicon Valley, or an overwhelming regulation led by authoritarian regimes. While the former does not address issues of privacy and malicious actors, the latter cracks down on human rights and could lead to a "balkanisation" of internet and of wider cyberspace.[32]

Among the 64 state signatories, European countries are the most heavily present. However, almost every continent is represented: among them we find Qatar, South Korea, Mexico, Japan, Canada, Colombia, Morocco, Senegal and New-Zealand. While the U.S., China and Russia are unlikely to join, the Call will rely on support from states like India and Brazil in order to gain traction within international institutions, primarily the United Nations.

The document has already drawn support from influential non-governmental groups (World Leadership Alliance, Chatham House, the WWW Foundation) and technical governance bodies, such as the Number Resource Organization. Powerful business lobbies are another prominent group of signatories. In total, as many as 300 universities, NGOs and professional associations have committed to the Call.

In the industrial landscape, France succeeded in attracting both major initiatives: The Tech Accord and the Charter of Trust represent a significant share of the private-sector signatories, as together they represent 85 powerful corporations such as Airbus, Cisco and Facebook. But the call is not a mere shell for existing groups. Notable newcomers include Google, Samsung Electronics, Intel Corporation, Kaspersky Lab, Thales and many other companies, ranging from the banking and insurance industries, to law, commerce and defence.

While the Paris Call is far from a silver bullet, it offers a fresh starting point and framework for further negotiations on values and norms of behaviour in cyberspace.

Threat perception

A state's perception of threats is based on a variety of factors: strategic goals, history and precedent, one's perception of its own weaknesses and dependencies.[33] While France approached cybersecurity issues from a dominantly technical perspective at its beginnings, Desforges argues, it shifted towards a model that goes

[25] Défense et Sécurité Nationale.

[26] LE DRIAN Jean-Yves, "Déclaration de M. Jean-Yves Le Drian, ministre de la défense, sur la cyberdéfense, à Bruz le 12 décembre 2016.," text, http://www.defense.gouv.fr, le 13 décembre 2016, December 12, 2016, http://discours.vie-publique.fr/notices/163003632.html.

[27] Ministère des Armées, "Éléments Publics de Doctrine Militaire de Lutte Informatique Offensive," January 2019, https://www.defense.gouv.fr/content/download/551555/9394645/Eléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf.

[28] "Global Commission Introduces Six Critical Norms Towards Cyber Stability," Global Commission for the Stability of Cyberspace, accessed May 6, 2019, https://cyberstability.org/research/singapore_norm_package/.

[29] A. Cattaruzza et al., "Sovereignty in Cyberspace: Balkanization or Democratization," in 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, 1–9, https://doi.org/10/gftt4z.

[30] Ministère de l'Europe et des Affaires étrangères, "Stratégie internationale de la France pour le numérique," France Diplomatie : : Ministère de l'Europe et des Affaires étrangères, December 15, 2017, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/strategie-internationale-de-la-france-pour-le-numerique/.

[31] Anonymous, "IGF 2018 Speech by French President Emmanuel Macron," Text, Internet Governance Forum, November 14, 2018, https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron.

[32] Cattaruzza et al., "Sovereignty in Cyberspace."

[33] Raymond Cohen, "Threat Perception in International Crisis," Political Science Quarterly 93, no. 1 (1978): 93, https://doi.org/10/d95kwg.

beyond security and defence issues.[34] The Snowden leaks, the rise of jihadist propaganda and the increasingly geopolitical impact of major attacks pushed France to consider broader societal challenges and actors in defining its strategies and policies.

Threat realisation centred around technology and intelligence (2008-2013)

The Defence and National Security White Paper 2008[35] mentions Internet in its first chapter, but first as an example of a positive trend, highlighting the rise in connectedness of people around the world. The other side of the coin, it later states, is the challenge of keeping up with the high-paced spread of information and ideas, in other words information control and propaganda. The Paper also dedicates a full-page box to serious cyber-attacks detailing the full CIA spectrum. While it does not mention the DDoS attacks on Estonia, the Paper foresees such attacks will be multiplying in the following 15 years and considers the risk of a large-scale attack on its critical infrastructures a major threat. It mentions "cyberwar" as one of the scenarios which could involve the Atlantic Alliance. In consequence, the Paper mandates 1) a switch from a passive to active defence model, 2) the development of offensive cyber capabilities, strategy and doctrine all focusing on adversarial military systems.

It is the very first time France acknowledges cyber threats and decides to act on them in a national public policy document. The Paper also creates a new strategic role for the armed forces known as "knowledge and anticipation".

Broadening to societal challenges and capabilities build-up (2013-2015)

The 2013 White Paper mandated the creation of a national doctrine for major cyber threats response: a coordinated defensive posture mixed with a graduated response from diplomatic, judicial and law enforcement powers to military means when vital interests are at stake. The strategic mission "knowledge and anticipation", created in 2008, now includes information control in its widest sense (maîtrise de l'information), from trends in cryptography to intelligence gathering and critical infrastructure security. Most critically, the Paper contains France's official recognition of cyberspace as an operational domain by stating that "cyberspace is now a battlefield of its own". This is two years after the United States[36] and three years before NATO.[37]

In 2015, the Digital Security Strategy stated that a serious threat ("atteinte significative") to French citizens data could constitute a national security matter, notably in the context of espionage, propaganda or political destabilisation.[38]

Institutional and doctrinal military structuring (2017-2019)

The 2017 Review emphasises the increasing role of Internet and digital giants (GAFAM, Baidu) on geopolitics and sovereignty, as well as on "strategic intimidation" facilitated by the combination of economic, military and informational pressures such as territorial fait-accompli and mass social network trolling.mThe Cyberdefence Review dedicates a significant part (32 pages) to the evolution of the threat landscape. It relies on the "new normal"[39] scenario to highlight the risks brought by quantum computers, Internet of Things and artificial intelligence. The next LPM (2019-2025) reflects this evolution of French threat perception and the impetus granted to the "knowledge and anticipation" mission of the armed forces. The defence budget for 2019 amounts to 35,9 billion EUR, or 1.82% of GDP, pensions excluded.[40] It is planned to increase over the next four years, reaching 44 billion EUR and 2% of GDP in 2023.[41]

Conclusion

Over the past decade, France went through three main major evolution stages in its cyber security and defence structuring: threat realisation (2008-2011), capabilities build-up (2013-2015) and an institutional and doctrinal military structuring accompanied by a strong diplomatic impetus (2017-2019). The recently released offensive doctrine is the culmination of this deep transformation. It particularly represents a turning point for the armed forces, breaking offensive operations from their intelligence silo. The wording of the document and of the accompanying speech by Minister Parly also represents a less veiled signal to Russia, a message France had previously been reluctant to send publicly. The Paris Call, in parallel, is an unprecedented attempt at bringing states, major corporations and the civil society together around key values and principles. Overall, France aims to promote international rules and stability in the cyber domain to prevent escalation of crises, yet seeks room to manoeuvre to support conventional operations, deterrence and retorsion. Such balance is and will remain delicate, which reinforces the need for a better understanding of actors' rationales and policy coordination.

[34] Alix Desforges, "Approche Géopolitique Du Cyberespace, Enjeux Pour La Défense et La Sécurité Nationale, l'exemple de La France" (Université Paris 8 - Vincennes / Saint-Denis, 2018).

[35] Défense et Sécurité Nationale.

[36] David Alexander, "Pentagon to Treat Cyberspace as 'Operational Domain,'" Reuters, July 14, 2011, https://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

[37] Herb Lin, "NATO's Designation of Cyber as an Operational Domain of Conflict," Lawfare, June 15, 2016, https://www.lawfareblog.com/natos-designation-cyber-operational-domain-conflict.

[38] Services du Premier Ministre, "Dossier de Presse - Stratégie Nationale Pour La Sécurité Du Numérique" (Paris, October 16, 2015), https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/.

[39] "Scenario One - The New Normal," CLTC UC Berkeley Center for Long-Term Cybersecurity (blog), accessed June 20, 2019, https://cltc.berkeley.edu/scenario/scenario-one/.

[40] "Communiqué du ministère des Armées_ Budget 2019 : LPM année 1," accessed April 29, 2019, https://www.defense.gouv.fr/actualites/communaute-defense/communique-du-ministere-des-armees_-budget-2019-lpm-annee-1.

[41] "Communiqué du ministère des Armées_ Budget 2019."

Ministry of Justice Internship

Ministry of Justice

Aaron Ceross, CDT16

As with much of the research within the wide remit of cybersecurity, my doctoral work is decidedly interdisciplinary. In my case, the research crosses a range of subjects including computational linguistics, machine learning, economics, requirements engineering, and legal theory. From within the academic environment, it can sometimes be difficult to understand how the DPhil research (and associated skills) are applicable to the what sometimes might seem to be the mythical "real-world". However, during Hilary Term 2019, I had the opportunity to undertake an internship within the Ministry of Justice (MoJ) to do just that.

The UKRI supports an internship programme that enables doctoral students funded through any of its research councils to join a government department. Given my DPhil's focus on privacy, the quantification of legal analysis, and requirements engineering, I applied to the MoJ, as they are currently undertaking an ambitious reform programme by which extensive portions of the legal infrastructure will be digitised. This includes online civil claims, responses to certain criminal offenses. The goal is to not only widen access to legal remedies by providing quick, easy-to-understand processes but ensure that results are consistent.

I worked for three months within HM Courts and Tribunal Services (HMCTS). I worked within different teams including User Experience, Operations, and Data Analysis. The tasks were quite interdisciplinary involving software development, computational sociological analysis, and. It was a unique education not only on how large-scale IT services are designed and delivered, but also on the considerations of digitisation of public services. This latter point is a question that sometimes does not receive enough discussion, with much of the discourse focused on the security of the information gathered and scope of public participation.

Overall, I am grateful to have been selected for the internship as the opportunity broadened my understanding of the inner workings of government, the digitisation of public services. While only indirectly related, the experience has also helped contextualise my own DPhil research.

The Workshop on the Economics of Information Security 2019

Daniel Woods, CDT16

The Workshop on the Economics of Information Security is a multidisciplinary venue attended by criminologists, lawyers, computer scientists, business researchers, and even philosophers. All attendees believe security outcomes can be usefully studied using economic concepts. This year it was hosted by Bruce Schneier at Harvard University.

The keynote speaker, Peter Swire, argued that the OSI model should be extended to include corporations, national governments, and supranational entities. This set the tone for a conference that looks beyond purely technical explanations for why security breaches and privacy violations continue to occur.

My favourite paper from the conference was a study of ad-blocking technology. Advertisers argue that contextual ads, such as displaying clothes products to a user searching for clothes online, increase consumer welfare by providing users with information about available products. The authors designed an experiment (N=212) to understand how contextual ads affect the price, satisfaction, and time spent by a user in making an online purchase.

The results showed no statistically significant difference between users who were randomly assigned an ad-blocker and those who were not. This suggests contextual online advertisements do not help consumers with online purchasing. While this makes sense intuitively, it is important to collect evidence about advertiser's claims given the societal cost resulting from the industry's existence in terms of lost privacy and human potential that might be better applied elsewhere.

I presented our paper in a session on "Mitigating Threat". We identified limitations in existing cyber loss estimates due to weak data. We argued that the price of insurance products covering cyber security events should reflect all available information about potential cyber losses, drawing an analogy with the Efficient Markets Hypothesis. Our main contribution was developing a novel method to infer cyber loss distributions from insurance prices. This flipped a problem – how to derive prices from loss data – that actuarial science has been trying to solve since the field came into existence.

We collected over six thousand cyber insurance prices and inferred a series of distributions. These were combined to derive the County Fair Cyber Loss Distribution. It builds on Francis Galton's observation that, in a competition to guess the weight of an ox at a county fair, the median guess came within 1% of the correct weight even though individual guesses were wildly inaccurate. This research was also presented to a number of insurance firms either side of the conference and they provided many useful suggestions for further work.

Negotiation Transparency in Configurable Protocols

A Case Study on the TLS Protocol and the Forward Secrecy Property

Eman Salem Alashwali, CDT15

Negotiation, always perceived as a critical phase in politics and business protocols, is just as important in communication security protocols. In the latter, the term "negotiation" usually refers to the process of exchanging security-related parameters between the communicating parties (e.g. client and server) in order to reach a mutual agreement on an optimal set of parameters that are supported by both communicating parties. These sensitive parameters include the protocol version, and the set of algorithms (ciphersuite) that will be used for the key-exchange, encryption, and hash, to secure subsequent messages of the protocol.

Such a negotiation phase is commonly used in protocols that support multiple versions and multiple algorithms, and are widely deployed on various types of platforms that vary in their capabilities such as personal computers and embedded (IoT) devices. The Transport Layer Security (TLS) and The Secure SHell (SSH) protocols are two notable examples of such widely used protocols.

Experience shows that the negotiation of security parameters is an attractive phase for downgrade attacks, where an active man-in-the-middle attacker interferes with the exchanged messages by the communicating parties, leading them to agree on a mode weaker than they support and prefer. This allows the attacker to perform subsequent attacks that would not have been possible in the strong mode.

It has become clear that ensuring the integrity (i.e. the messages have not been tampered with) and authenticity (i.e. the messages are coming from the intended party) of the exchanged parameters is of paramount importance in the negotiation phase, in order to prevent downgrade attacks.

While the literature has looked at negotiation integrity and authenticity in the active man-in-the-middle attacker model, we look at the problem from a new perspective: we consider transparency, as a result of a novel attacker model that we propose, which we call the "discriminatory" adversarial model. To the best of our knowledge, transparency and discrimination in security protocols negotiation have not been discussed in the existing literature. We are the first to observe and write about them [1][2][3].

In our research, we made an observation pertaining to parameters negotiation in security protocols. That is, certain client-server negotiation models, which we call "server-dominant", result in an imbalanced power between the communicating parties, the client and server. To illustrate, as shown in Figure 1, in the TLS protocol case, the protocol performs the parameters negotiation as follows: the client proposes a set of parameters such as the protocol versions and ciphersuites, ordered by preference, to the server. The server selects one of them and imposes its choice

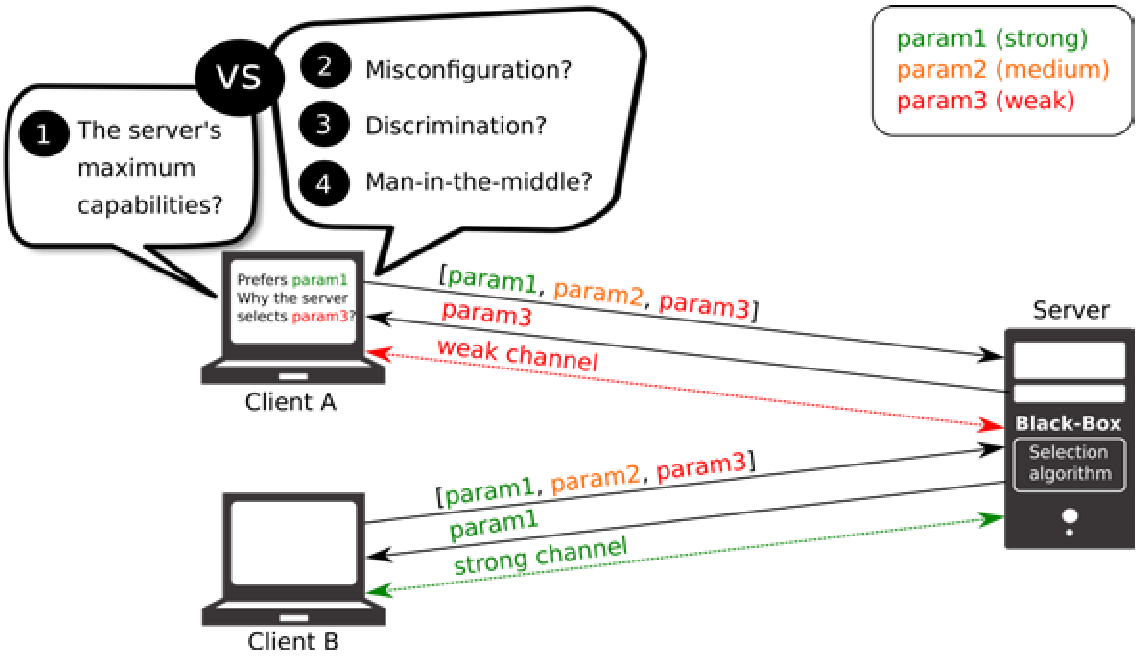


Figure 1: Illustration of our newly introduced discriminatory adversarial model in parameters negotiation in security protocols with server-dominant negotiation model such as the TLS protocol. The term "Param" denotes parameter.

to the client. The client does not necessarily receive its most preferred choice. This can be due to several reasons, such as: server's lack of support for the client's most preferred parameter, server's misconfiguration, server's bad implementation, or a man-in-the-middle attacker that tampered with the messages. However, it can also be due to the server's discrimination against its clients for a powerful third party's advantage (e.g. government intelligence) with minimum liabilities related to the server's involvement. This is a realistic assumption. In fact, it is inspired by past real-life events such as "export-grade" cryptography, a US (deprecated) law, which used to enforce weak cryptography to products (including software) exported outside the US, in addition to Edward Snowden's allegations about the "PRISM" program, for mass surveillance in collaboration with giant cloud service providers.

In the server-dominant negotiation model, the client does not have the means of verifying the server's choice, i.e. justifying the server's decision if it is not optimal, or against the client's preference order. While the server's parameters selection algorithm is known in the protocol specifications, the selection algorithm implementation along with the server's actual supported parameters, are a black-box from the client's perspective.

There is currently no way for the client to verify that the server has behaved correctly, and its selected parameters are optimal. *Figure 1* illustrates our observation which applies to the TLS protocol.

To prove the realism of our model, and most importantly, that our proposed adversarial model can go unnoticed in most mainstream clients today such as web browsers, we consider the case of the TLS protocol and the Forward Secrecy (FS) property. We conduct an empirical analysis on over 10M TLS server addresses, including top domains, random domains, and random IPv4 addresses.

FS is a highly desirable property nowadays, which guarantees that a compromise in the secrecy of the server's long-term key does not compromised the secrecy of past session keys. Therefore, if a passive adversary has been collecting traffic today, the adversary can not decrypt past traffic if the server's private-key is compromised at some point in the future. Some key-exchange algorithms such as ECDHE provide this property, while other key-exchange algorithms such as RSA do not provide it. Experience has shown that it is possible for servers' long-term private-keys to become compromised. For example, RSA long-term private-keys have been compromised through prime factorisation, due to advancement in computing power, or due to low entropy during keys generation. Furthermore, long-term private-keys can be compromised through implementation bugs such as in the Heartbleed bug, through social engineering, or other attacks. While the latest version of TLS, TLS 1.3, mandates FS by design, FS is not mandated in pre-TLS 1.3 versions, which are still widely used by most mainstream TLS clients and servers today, and still support non-FS algorithms. Pre-TLS 1.3 versions (mainly TLS 1.2) may continue to be used for decades to come.

Our empirical study aims to answer the following question: *Do servers that select non-FS key-exchange support a FS one?* That is, are there servers that choose a weaker key-exchange algorithm while they are capable of choosing a stronger one?

To this end, we developed a TLS client that mimics a Chrome browser's proposed versions and ciphersuites, but we implement a heuristic procedure. That is, when the server selects a non-FS key-exchange as a result of our client's default proposal, the client immediately repeats the client's offer to the same server, but with a new set of parameters that proposes FS-only algorithms. This allows us to test if the server is indeed incapable of FS key-exchange algorithms or not.

Our results show that 5.37% of top domains, 7.51% of random domains, and 26.16% of random IPs do not select FS key-exchange algorithms. Surprisingly, 39.20% of the top domains, 24.40% of the random domains, and 14.46% of the random IPs that do not select FS, nevertheless do support FS.

We have studied the case of TLS and FS. However, the discriminatory adversarial model and transparency as a requirement in protocol negotiation models can be generalized to any negotiation of any parameters in security protocols with a semi-trusted party who can gain advantage from discrimination.

This article provided a summary of some of our novel insights and contributions in the area of communication security protocols. Our study, which also provides an extensive discussion regarding possible paths towards forward secure internet, has been accepted for publication in the 15th International Conference on Security and Privacy in Communication Networks (SecureComm 2019), Orlando, US. *For more details about our research, please check the on-line pre-print*[3] *which is available at Google Scholar.*

Acknowledgment

Thanks to Andrew Martin for feedback on this article.

References

[1] Alashwali, E.S. (2016). "On Downgrade Attacks in the TLS Protocol". CDT Mini-Project Report, University of Oxford

[2] Alashwali, E.S. (2017). ""Negotiation-Transparency" as a Property in Configurable Protocols".

DPhil. Transfer of Status Report, University of Oxford

[3] Alashwali, E.S., Szalachowski, P., Martin, A. (2019). "Towards Forward Secure Internet Traffic". In: Security and Privacy in Communication Networks (SecureComm), Orlando, US

On Trustworthiness and Trust

Arianna S. and Sean Sirur CDT17

This summer, CDT students Sean Sirur and Arianna S. attended IFIPTM 2019, the 13th IFIP Working Group 11.11's International Conference on Trust Management. Held this July at the Technical University of Denmark, Copenhagen, the conference's mission is to "share research solutions to problems of Trust and Trust Management... and to identify new issues and directions for future research... on any topic related to the themes of trust, security and privacy".

Speakers for this year's conference spanned the international scene, travelling from Israel, France, Denmark, Japan, China, Austria, Norway, Spain, Slovenia, Italy, the Netherlands and the UK. Topics ranged from authentication libraries and blockchain-based verification, to GDPR modelling for log-based compliance and sourcing trustworthiness for negative trust assessment.

Sean presented his paper on "The Reputation Lag Attack". Selected for publication by IFIPTM 2019, this research built on earlier work and ideas presented at this year's CDT showcase event. The paper focused on information propagation through reputation systems (networks which use opinions as a basis for trust e.g. electronic marketplaces and social networks). The transmission of these opinions can be subject to delays which enable "reputation lag attacks". This is analogous to being stabbed in the back by a trusted individual only to discover afterwards that a mutual friend was similarly accosted before you. Due to the delays, the news of this earlier attack failed to reach you in time, thus leaving you vulnerable. His talk was very well received, with questions running over time and discussion moving out of the metaphorical frying pan and into the coffee break.

Arianna talked to the assembly about "Why We Trust Dynamic Consent to Deliver on Privacy", describing the fundamental tenets of her thesis as a work-in-progress paper. A format new to the 2019 conference, work-in-progress papers made up around 15% of submissions accepted this year. In an engaging and thoughtfully crafted presentation about the importance of trustworthy behaviour in researchers to encourage research participation, Arianna discussed a normative privacy model and how that needs to dictate what "good" data protection looks like in research practice. Dynamic consent, she argued, lets those who collect and store personal information to show compliance with the privacy preferences of the people they collect information from. This mechanism also provides participants with control as and when they require it. Arianna's expertise and focus on better data and privacy practices were notably welcomed not only during her talk but throughout the event, particularly during the panel discussion on the trustworthiness of AI.

A non-governmental organisation recognised by the United Nations, the International Federation for Information Processing (IFIP) brings people together to create high quality research and standards for information sharing and use. Active for over 50 years, IFIP works across 13 technical committees (IFIPTM this year being run under the auspices of the Security and Protection in Information Processing Systems committee) and strongly advocate open access. By sending two students, the CDT is being represented in a field that is only gaining in prominence. Trust in information technology, identity management, socio-technical and sociological problems and emerging technologies are becoming a focal point for researchers in this Digital Age.

Encouraging students to engage with communities like IFIPTM provides the CDT with two key benefits. The first is representation in a growing community of like-minded researchers. The other is the academic rigour brought in through the incorporation of ideas that question the foundational assumptions of trust on which security research is based.

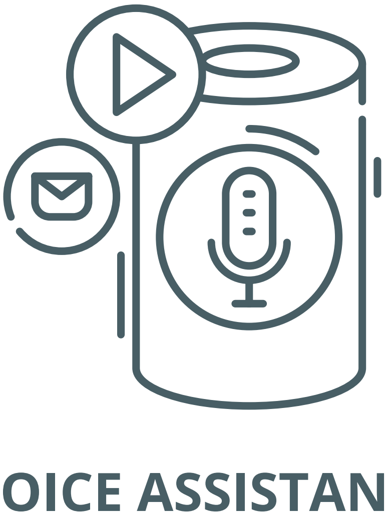
Cyber Security and the Speech Interface – some thoughts on my DPhil and beyond

Mary Bispham, CDT16

The initial idea for my DPhil was the somewhat vague one of 'something to do with speech and language processing in cyber security'. After exploring some possibilities in the two mini-projects at the end of my first year, I eventually settled on the topic of the security of voice control. I have now been researching this topic for nearly three years.

Control of computer systems by voice was for a long time largely limited to the realms of science fiction and academic research. However, in recent years, voice-controlled systems have become commercially available for general use in various environments, including the home, government services and banking. There is something almost eerie about the prospect of being able to affect an increasing range of virtual and cyber-physical actions through an act of natural speech. A speech interface dissolves the boundaries between the natural and the cyber world. This points to new types of security concerns in relation to voice control as a mode of human-computer interaction. Amplifying these concerns is the fact that an attack on a system by sound alone is likely to be impossible to retrospectively attribute to an individual attacker. Being a member of the CDT has given me the opportunity to investigate this new area of cyber security, whilst also gaining a broader knowledge of the field, which has enabled me to ground my research in a wider context.

My DPhil project has focussed on the speech interface as a new attack surface for malicious actors seeking to gain unauthorised access to systems. The most obvious vulnerability of speech interfaces is a lack of access control on account of the difficulty of controlling the acoustic environment in which voice-controlled devices may be deployed. Preventing access to a system by sound is far more challenging than preventing physical or internet access. Whilst physical access may be controlled by physical measures such as locks, and internet access may be controlled by technical measures such as firewalls, controlling the flow of sound through the air is impractical in most environments. A less obvious factor also affecting the security of speech interfaces is the existence of various types of acoustic signals that are interpreted by voice-controlled systems as commands to execute an action, but that are unrecognisable to human listeners. This space of unexpected acoustic input to voice-controlled systems has yet to be comprehensively mapped. Previous research has demonstrated the possibility of hiding voice commands in inaudible frequencies and in white noise. In my own research, I have demonstrated that nonsensical word sounds and utterances of apparently unrelated meaning may be interpreted by voice-controlled digital assistants as valid commands. Currently available defence measures, such as voice biometrics, do not provide an adequate solution for securing the speech interface against all types of potentially malicious input to a system by sound at present. The last phase of my DPhil project looks at prospects for the development of new defence measures.



Aside from the security of voice control as investigated in my DPhil project, there are also other implications for cyber security research from developments in speech and language technology. The privacy implications of 'listening' devices have been the subject of much debate. We have long become accustomed to the notion that the privacy of our written digital communications cannot be assured. The increasingly wide-ranging adoption of speech interfaces presents the frightening prospect of a world in which even our verbal communications cannot be assumed to be either private or transitory.

Another security issue arising from advances in speech and language technology is the increase in potential for social engineering via synthesised voices. In 2018, a qualitative shift in speech synthesis was seen with the public debut of Google's Duplex technology, which was shown to be indistinguishable from a real human voice in phone conversations. Whilst manipulation of humans using bot-generated language is nothing new, the ability to perpetrate such manipulation in verbal rather than written form, using artificial voices which are perceived by humans as real, is likely to make such manipulation far more effective. This will be the case particularly if it becomes possible to generate convincing imitations of individual voices which are known to a victim. As any player of the children's game 'Simon Says' will know, the human response to instruction by voice is partly instinctive, and hence difficult to control in a time-pressured situation. This is especially the case with respect to familiar individual voices, such as those of a family member or authority figure, which can have powerful emotional impact. Social engineering via synthesised voice is a clear example of an area of cyber security in which technical and human factors become inseparable.

A further area of speech and language technology which may become a focus of future cyber security research is machine translation. Developments in spoken machine translation in particular offer vast potential for international communication in real-time across current language barriers. However, an increasing reliance on machine rather than human translators also implies that the integrity and security of machine translation processes will be of paramount importance.

It is even possible that speech and language technology may begin to affect the development of language itself, with implications for cyber security amongst many other fields. A hint of this was seen in a recent experiment conducted by Facebook, which had the aim of training two bots to negotiate an optimal outcome in an exchange of items, using natural English. In the course of the training process, the bots were observed to eschew the use of natural English in favour of a self-generated language, which was presumed to be more efficient than the human one for negotiation purposes. The implications of such developments for the evolution of human language use are interesting to consider, in that they raise the prospect of humans beginning to adapt their own language use to bots, rather than just teaching bots to imitate human language. A further possibility is that voice-controlled devices may begin to influence language learning in young children. It has been suggested that voice-controlled digital assistants could be used to enable young children to learn the native languages of earlier generations of their family, despite living in a different geographical location, by interacting with the voice-controlled device as they would with a live native speaker[1]. Such technology might in fact make it possible for young children to become 'authentic' native speakers of any language, regardless of their place of residence or family environment. Notwithstanding the huge opportunities offered by such developments, it needs also to be recognised that any manipulation or undermining of these technologies for malicious purposes may have far-reaching consequences, which are currently difficult to envisage fully.

[1] Quartz magazine, 13th September 2017, "Echoing the Echo: Want your kid to be bilingual? Alexa could help", https://qz.com/1074540/want-your-kid-to-be-bilingual-alexa-could-help/

CDT's Double Blue

Hayyu Imanda (CDT2018) has secured a full 'Blue' for the second time in lawn tennis (2017, 2019). She played at number 3 at this year's Varsity against Cambridge and also helped the team maintain their place at the BUCS Premier league. Inda has been crucial in developing the positive attitude and competitive spirit within the team, something which she has brought to her CDT cohort as well. When not playing tennis, Inda is a PADI and SSI qualified scuba diver and passionate about the ocean environment.

¡Buena suerte! Maureen

A key figure in the CDT, after 6 years as Centre Administrator, Maureen York will be departing for her new exciting life in Spain (with husband and Sun Conures Rudy and Rio). Maureen's calm and professional attitude along with the love of everything purple, glitter balls and rainbow Slinkys have made her an essential part of the CDT. Maureen is an invaluable asset to the CDT, Department of Computer Science and University; her departure will be felt by all. We wish her great success in her new venture, supporting those who have been diagnosed with cancer and their families. We have no doubt that Maureen will make a massive positive impact with her effervescent personality and deeply caring perspective on life.

Oxford's Competitive Computer Security Society continues to impress

Alistair Janse van Rensburg, CDT14

Oxford's Competitive Computer Security Society, founded and run by CDT students, enjoyed a successful year of both running and competing in capture-the-flag (CTF) competitions. Capture-the-flag competitions allow participants to practice hacking techniques in a controlled (and legal!) environment. In teams of around four, participants are presented with a set of distinct challenges, each designed to require a different skillset, from cryptography to remote binary exploitation. Solving a challenge results in a flag, which can be turned over for points.

This year, in addition to continued support from the CDT, the society received a grant from the Oxford Foundry, allowing us to run a series of events designed to get new participants involved in this exciting and educational activity. Our first event saw students from across the university compete to solve challenges and help fictional intelligence agencies from across the world. Challenges included fixing virtual plumbing and taking control of a passport application page. Many participants had never experienced capture-the-flag contests before and left keen to participate in more. These challenges enable people to get hands-on experience with the practical side of security, beneficial to those studying security and to those who just want to better understand modern cyber risks. We followed this with participation in a real event: the Google Capture-the-Flag. While some challenges were so difficult no team solved them, there was a wide variety, enabling everyone to get involved.

While the ever-popular Inter-ACE contest was not running this year, we were happy to see a spiritual successor in the Higher Education Cyber Challenge (HECC). This event was run by the University of Southampton to replace Inter-ACE and give UK universities an opportunity to compete against each other. The event proved highly enjoyable, featuring guest challenges from some of the sponsors and one challenge that included hunting-down a real location within the university. We eagerly await news of the return of HECC next year!

Practicing practical security through the society has also enabled other benefits, with members using their newfound skills to go on to penetration-testing internships and others participating in other qualifications. We have also had the opportunity to present CTF-inspired teaching to students at a variety of levels throughout the university. Most notably, this year we provided a well-received week long course to first-year students of the CDT, coupling traditional CTF challenges with taught sections covering relevant skills and a series of group challenges, where students joined together to attempt to break into a realistic system – from getting tickets to a dream holiday, to determining the identity of a criminal to stealing a wallet full of Bitcoins.

The society is, as ever, grateful to the CDT for their continued support, enabling us to fund participants to go to events across the UK, including Southampton, Manchester and Liverpool.

From #002147 to #00356B: 5 Months in New Haven

Ilias Giechaskiel, CDT14ish

As anyone who knows me can tell you, I will do anything to remain a student. I was originally planning on joining the workforce after my 4 years of undergraduate courses were over, but getting a master's degree soon put those plans to rest. Then, despite having sworn that I would *never* pursue a PhD just two years prior, I started a 4-year programme in Cyber Security. As if that weren't enough, I took three summers off for internships, making me an honorary member of CDT15 (the "D" in "DPhil" apparently stands for "Dragging on"). My latest annual escape from Oxford life took me to Yale University, where I spent the first half of 2019 as a Visiting Assistant in Research.

At Yale, I worked with Professor Jakub Szefer, whom I had met through my security courses at Princeton. His research on FPGA security spoke to my academic interests, and after a three-way discussion with him and my Oxford supervisor, Professor Kasper Rasmussen, we decided on a project for my visit. As is always the case with research, contingency-planning is key, so after pivoting on the research topic a bit, I started investigating covert-channel attacks on cloud FPGAs. The academic environment was very conducive to successful research: I had positive results within a few weeks of being at Yale, and one of the projects I undertook has already been accepted for publication at the 29th International Conference on Field-Programmable Logic & Applications (FPL). Besides the guidance by my supervisors, I attribute part of this success to the shear amount of resources available at the students' fingertips. Whether purchased through research grants, or donated through industrial partnerships, the equipment to which I had access made me feel like a kid in a toy store.

The equipment wasn't there just for research purposes either: the Yale Center for Engineering Innovation & Design (CEID) offered CNC mills, routers, lathes, and band saws among other dangerous-yet-fascinating machinery. And after some basic safety training, they were all free to use—some even 24/7! I made extensive use of their 3D printers and laser cutter, and although I won't be winning the Red Dot Award for Design anytime soon, I had fun trying to engrave the Oxford crest on wood. In general, I felt quite at home: I immediately joined the Paracleats soccer team (though my allegiance remains with the Oxford University Greek Society!), and quickly discovered all the good lunch spots near campus. My fond memories of the Gloucester Green market and the Osney Food Shed were thus slowly replaced by the food trucks on Sachem street, and deconstructed sushi in the form of Hawaiian poke. I even attended a workshop on AI, Ethics, and Society—the CDT interdisciplinary spirit seems to have followed me here.

Other highlights of my trip include a visit to the Reconfigurable Computing Group at the University of Massachusetts, Amherst; delicious lobster rolls in Boston; and, of course, the Princeton reunions P-rade and fireworks. Overall, despite the bureaucracy involved in officially applying to the Yale graduate school and getting a US J1 visa, the whole experience has been very rewarding—especially as a last foray into academic research before I join the private sector (or, unexpectedly, stumble my way back into student life *yet again*). So, as a final note, I would like to thank the CDT and my Yale and Oxford supervisors for this opportunity, which was only made possible through their financial and academic support.

Yale University

Princeton University

If you squint hard enough, you can see a poorly-engraved Oxford crest between the vanity.

Untangling the Radical Mind: A Computational look at ISIS propaganda

Mariam Nouh, CDT15

The Internet and Online Social Networks (OSN) in particular have changed the way that terrorist and extremist groups can influence and radicalize people. Recent reports show that the mode of operation of these groups starts by exposing a wide audience to extremist propaganda online, before migrating them to less open online platforms for further grooming and radicalization. To limit the reach of cyber-terrorist and extremist groups, several private and governmental organizations are policing online content and utilising big data technologies to minimize damage and counter the spread of such information. For example, the UK launched a Counter Terrorism Internet Referral Unit in 2010 aiming to remove unlawful Internet content and it supports the police in investigating terrorist or radicalizing activities online. The Unit reports that among the most frequently referred links were those coming from several OSNs, such as Facebook and Twitter[1]. Similarly, several OSNs are constantly working on detecting and removing users promoting unlawful and extremist content. Big tech companies such as Facebook, Google and Twitter have established dedicated teams to develop policies and tools to counter terrorism and extremist content and their use of the corresponding platforms. For example, in 2017, Twitter announced that they suspended around 300,000 accounts globally that were linked to terrorism[2]. In addition, an establishment of the Global Internet Forum to Counter Terrorism (GIFCT)[3] by a collection of tech companies with the vision of preventing terrorist from exploiting platforms is a major step towards creating a safe online environment. The GIFCT initiative announced the commitment to invest in technology and improve the existing capabilities to detect and remove terrorist and violent extremist content online.

Realizing the danger caused by the spread of violent extremism and radicalization content online, and how it is becoming a major challenge to societies worldwide, many researchers have attempted to study the online behaviour of a number of extremist and terrorist groups. The Islamic State in Iraq and Syria (ISIS) is one of the leading terrorist groups that utilize social media platforms and invest huge resources in creating digital media to spread their ideology and propaganda[4]. This is achieved by regular publications of a number of propaganda magazines, namely, Dabiq and Rumiyah, as well as a number of high-end quality videos and images promoting their activities[5]. In this study, we aim to untangle the radical mind by exploring linguistic (syntax and semantics) and psycho-linguistic (psychological traits) dimensions of the online propaganda produced by ISIS to recruit and influence people.

Data and Methods

Our dataset consists of 14-issues of Dabiq magazine, which is published by the ISIS group. The aim of these magazines is to spread their ideology, recruit, and reach their target audience. The magazines were published between 2014 and 2016, and consist of around 400,000 words, and 2 million characters. In order to be able to analyze the text in an automated way, we transform the text into a format that we can computationally process and analyze. To do so, each magazine issue is transformed to a vector of words (Bag of Words). We perform a set of pre-processing steps and convert all words to lower-case, remove all stop-words (e.g., and, or, the) and punctuation marks (e.g., . , ! ?). We then perform lemmatization aiming to remove inflectional endings and return words to their roots in order to avoid duplicates of the same word. For example, words with different endings (e.g., shooting) will be mapped to a single word (e.g., shoot).

Semantic Extraction through word Embeddings:

In order to identify the context in which the words are used and their associated semantics, we use word vector embeddings. Word embeddings[6] are used to transform text into meaningful vector representation while preserving the relationship between them. Research in Natural Language Processing (NLP) has compared the effectiveness of word embedding methods for encoding semantic meaning and found that semantic relationships between words are best captured by word vectors within word embedding models. Moreover, converting words into vector embeddings would allow us to create meaningful semantic queries. For

[1] Edwards, C., and Gribbon, L. 2013. Pathways to violent extremism in the digital era. The RUSI Journal 158 (5) : 40– 47

[2] Adam Satariano. 2017. Twitter Suspends 300,000 Accounts Tied to Terrorism in 2017. https://www:bloomberg:com/news/articles/2017-09-19/twitter-suspends-300-000-accounts-in-2017-for-terrorism-content

[3] Global Internet Forum to Counter Terrorism. https://www.gifct.org/

[4] Allendorfer, W. and Herring, S., 2015. ISIS vs. the US government: A war of online video propaganda. AoIR Selected Papers of Internet Research, 5.

[5] Ingram, H.J., 2016. An analysis of Islamic State's Dabiq magazine. Australian Journal of Political Science, 51(3), pp.458-477.

[6] Hamilton, W. L.; Leskovec, J.; and Jurafsky, D. 2016. Diachronic word embeddings reveal statistical laws of semantic change. In Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers) , 1489–1501. Association for Computational Linguistics

example, we would be able to ask the following query from a well-trained model: “King” is to “Queen” as “Man” is to X, and the result value for X would be “woman”.

We use the issues from the Dabiq magazine to create domain-specific word embedding for ISIS propaganda. By training a word embedding model on this corpus, we are able to learn the domain terminology and model the semantic context of terms used in ISIS propaganda. We train word2vec model[7] on our corpus to build the lexical semantic aspects of the text using vector space models. We then build a semantic network of the 3000 top scoring words (tf-idf score), such that a given word is connected to the words close to it in the vector-space. Similarly, every other word in the network is also connected to its vector-neighbours.

Extracting the Psychological traits

Research in fields such as linguistics, social science, and psychology suggests that the use of language and the words choices we make in our daily communication can act as a powerful signal to detect our emotional and psychological states[8]. Several psychological properties are unintentionally transmitted when we communicate. It can be detected in the way we speak or express ourselves in writing. For example, research in the field of psychology has found relations between the choices of words and symptoms such as depression, suicide and anxiety[9]. Moreover, previous research has studied the social psychology of online interaction and investigated the extent to which principles of social psychology carry over into the online domain.

Different text analysis tools and dictionaries have been developed and used in the literature to identify psychological properties from written text. One of the very first tools to achieve this is LIWC[10]. The tool focuses on counting the frequencies of words occurring in a given text and mapping these to a set of pre-defined lexical categories, such as emotions (e.g., anger, fear), social interests (e.g., family, friends), and cognitive processes (e.g., certainty, tentative). These categories together can paint a picture of the author’s interests, personality and emotional states as conveyed in the analyzed text.

We extract psychological properties from text written with the intention of recruiting and influencing people to adopt extremist ideology. We assume that such text will appeal to those who share similar traits. Thus, we analyze the text of the Dabiq magazine from a psychological angle, in order to understand the personality, emotions and the different interests exhibited by their authors. We analyze the text in our corpus and calculate the frequencies of words that map to the different psychological categories. Mainly, we look at the following properties: (1) Big-Five psychological properties, which measures five psychological properties (OCEAN), namely Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism; (2) Emotional analysis, which measures the positive emotions conveyed in the text and the negative emotions (including anger, sadness and anxiety). (3) Personal Pronouns counts the number of 1st (I, we), 2nd (you) and 3rd (she, he, they) personal pronouns used.

Results

In our analysis, we found several common themes that appear across different issues. These themes are obtained through manual investigation and using topic modelling with Latent Dirichlet Allocation (LDA) algorithm[11], which is used to discover the main topics present in the corpus. The main themes are religion, war/violence, and people/places. Given that the group is using religion to legitimize their action, the articles contain a heavy religious tone that is apparent through the excessive use of words such as *Allah* (God), and references to several religious figures and scholars. In the second theme, the war/violence theme, the top words appearing in the ISIS articles consist of words such as *crusade* and *jihad*, which correspond to religiously motivated wars. An interesting finding is that while words such as *war* and *army* have high weights, other related words like *kill* and *blood* have lower weights. This may be a conscious strategy to legitimize the activities of the ISIS group in the eyes of the reader by giving their action an official state-like lawful impression (war instead of kill). As for the final theme of people/places, we can see that places including *Iraq* and *Syria* have high weights which aligns with the origins of the group and their geopolitical standings. Similarly, there are high references to locations where ISIS operations and attacks were carried out, such as Brussels and Paris.

Furthermore, we query the radical word embedding model to show some examples of words and their most similar semantic neighbours in the context of Dabiq magazine. For example, the word ‘taghut’ (tyranny) is most similar to some political figures such as ‘Erdogan’ and ‘Saddam’ which gives an indication that ISIS view those politicians as evil. The word ‘Kuffar’ (infidel) is mostly associated with ‘weak’, ‘tawaghit’, and ‘secular’.

[7] Mikolov, T.; Sutskever, I.; Chen, K.; Corrado, G. S.; and Dean, J. 2013. Distributed representations of words and phrases and their compositionality. In Advances in neural information processing systems , 3111–3119

[8] Tausczik, Y. R., and Pennebaker, J. W. 2010. The psychological meaning of words: LIWC and computerized text analysis methods. Journal of Language and Social Psychology 29(1):24–54.

[9] Al-Mosaiwi, M., and Johnstone, T. 2018. In an absolute state: Elevated use of absolutist words is a marker specific to anxiety, depression, and suicidal ideation. Clinical Psychological Science 6(4):529–542.

[10] Pennebaker, J.; Boyd, R.; Jordan, K.; and Blackburn, K. 2015. The development and psychometric properties of LIWC 2015. Technical report, University of Texas at Austin

[11] Blei, D. M.; Ng, A. Y.; and Jordan, M. I. 2003. Latent dirichletiliev2015automated allocation. Journal of machine Learning research 3(Jan):993–1022

Our psychological analysis of the Dabiq magazine issues revealed a number of properties that complement what is published in the terrorism literature regarding the psychology of extremist groups (Figure. 1). Our analysis shows that they reflect confidence and formal logical thinking style. Adopting this style of writing for the propaganda material may reflect why they have been successful in their recruitment campaigns. Additionally, looking at the big five personality properties, we find that they exhibit high conscientiousness which is typically associated with being focused. Also, of the five factors, they show high levels of neuroticism. As for the emotional analysis, the magazines exhibit both positive and negative emotions. However, they show more negative emotions, manifested mainly through the anger emotion. In terms of the use of personal pronouns, we can see that it reflects the dichotomy mentality of us-vs-them, which is a strategy adopted by extremist groups. They focus more on the 3rd person pronouns (they, she, he) as opposed to less focus on the use of 1st person pronouns (I, we). Also, it is interesting to note that the use of the second person pronoun (you) is higher than 1st person pronouns (I, we), which shows the strategy of these magazines in making the focus on the reader.

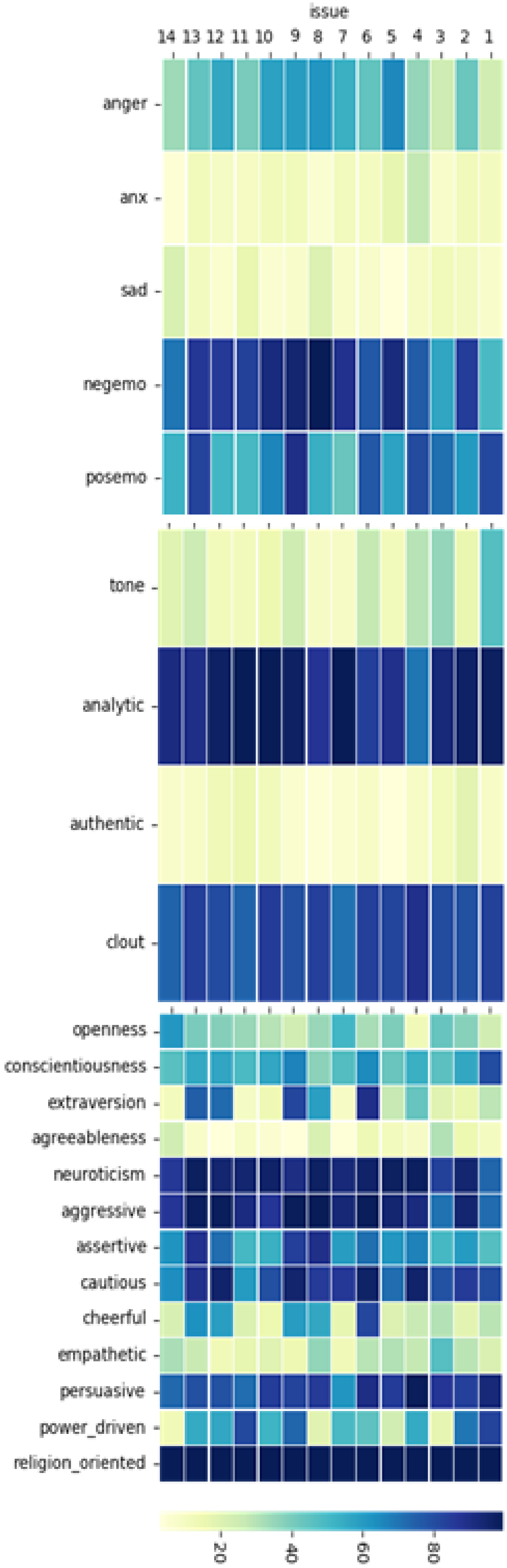


Figure 1: Psychological analysis of 14 Dabiq issues

Losing the Car Keys

Richard Baker, CDT15 and Sebastian Köhler, CDT18

In the Systems Security Lab, CDT students are examining the security and privacy implications of using powerline communication in industrial and automotive scenarios – particularly for charging electric vehicles. Communications technologies originally designed for small-scale home LAN use are being adapted to suit new use cases that exhibit more serious consequences upon system failure.

Electric mobility is a prime example. Electric vehicles (EVs) are proliferating quickly, along with a great swath of new charging infrastructure for them. Charger technologies are evolving, handling more sensitive data and undertaking more complex interactions, while using the charging cable as the communication channel.

In an upcoming USENIX Security 2019 paper, CDT student Richard Baker shows a practical, wireless eavesdropping approach that can extract plaintext messages from the in-cable communication between a vehicle and a charger. The technique was tested in the wild and successfully recovered messages from real cars, in real car parks around the south of England.

The Work so Far

The rise of electric vehicles (EVs) has been swift in recent years and it only continues to accelerate, helped by prevailing attitudes, technological advances and notable personalities contributing in the area. The UK government is already planning a nationwide ban on the sale of fossil fuel vehicles by 2040. Meanwhile Paris plans to ban petrol and diesel vehicles as soon as 2030.

The availability of charging infrastructure has become a major challenge for users, who require access both to private charging points at home and public ones on longer journeys. The lack of sufficient charging points is often noted as a slowing influence on adoption of electric mobility and this has prompted endeavours to expand the infrastructure, both from governments recognising the potential public good and from competing EV manufacturers who understand that having the best infrastructure makes their vehicles more appealing to purchasers. There are already multi-billion-dollar public deployment plans in progress and predictions of worldwide numbers exceed 50 million chargers by 2025 if private systems are included.

A new generation of charger technologies is emerging and bringing a far more complex communication channel to the charging cable itself. This channel is used not only for charging control, but will soon handle billing, vehicle-to-grid operation, internet access and provide a platform for third-party apps — all with a public interface to the world. Against this backdrop, we sought to discover how a malicious person might try to interfere with the charging system. Of the several competing charging systems, we selected the Combined Charging Standard (CCS), in part because of its dominance in the EU and in part due to its use of powerline communication to provide a high-bandwidth channel between vehicle and charger. We were interested in the capabilities of an entirely passive attacker, who only eavesdrops on communication and does not interfere with the process. Given the well-documented tendency of powerline communication to radiate some of the transmitted signal out of the cabling, we chose in particular to investigate whether an attacker could eavesdrop wirelessly on the charging channel.

We undertook a data collection campaign with three fully-electric vehicles: a BMW i3, a Jaguar I-PACE and a Volkswagen e-Golf. The campaign comprised over 800 miles of driving and spanned six major administrative regions of the UK. A total of 54 unique charging sessions were conducted, at locations including service stations, highway rest stops, superstores and hotels.

Due to their already widespread deployment, we tested solely using high-power public chargers, but there are already similar examples available that are intended for private use. In keeping with our passive attacker model we did not modify or interfere with the vehicle, charger or associated cabling in any way.

To collect the signal we simply used an off-the-shelf antenna and a software-defined radio device. An optimised antenna for the low-frequency powerline communication would be over 20m in length, but even our old Wi-Fi antenna was capable of detecting the emissions. The equipment for our experiments cost approximately £700, although equivalent setups are now available for less than £300.

Every site we tested displayed some form of wireless leakage from the charging communication. The weakest signal still showed clear of the background noise by 9dB and spanned a bandwidth of 4.5MHz (out of a maximum of 26MHz). In the best case 25MHz could be seen, up to a peak of 35dB. While there was notable variation from site to site, the behaviour did seem to be consistent across vehicles and chargers from different manufacturers.

With such a clear channel, it was possible to recover the transmitted messages in most of the cases, with hundreds of complete messages captured even in short sessions. In the best case, close to the charging cable at one site, 100.0% of detected packets were received as messages and validated their CRC32 checksums. More surprisingly, the eavesdropper was able to receive 91.8% of messages correctly, even when the antenna was located in the next parking bay.

We also tested whether multiple simultaneous charging sessions caused interference that affected the wireless channel quality. Two vehicles (a Jaguar I-PACE and a VW e-Golf) charged simultaneously in 5 charging sessions at 2 locations. In each case, one vehicle initiated charging first and then the second did so. The eavesdropper's antenna was located between the two vehicles and attempted to listen to both. In all cases, the eavesdropper was able to listen to traffic from both vehicles, albeit with varying success. At worst, 24.3% of messages were received with correct CRC32, at best 94.8% (mean 59.7%).

Where we were able to capture the start of a charging session, we were able to examine the initial key exchange to form an encrypted network. In line with the ISO 15118 standard, every SLAC interaction we observed operated in insecure form. As such, the master Network Membership Key (NMK) could be eavesdropped. With a single vehicle, we were able to intercept the message in 31 cases and acquire the NMK. With two vehicles side-by-side, we received the NMK for a single vehicle in 4 sessions and on one occasion extracted the NMK for both vehicles at the same time. With this key we were able to decrypt the rest of the key exchange and then perform passive eavesdropping of all subsequent PHY-layer traffic over the connection.

We proposed a new initialisation routine that allows the network membership key to be agreed in a secure manner, by applying an Elliptic Curve Diffie Hellman exchange. In the short-term however, it seems that any developers building atop CCS communication should not assume the connection is protected. All findings were disclosed to the relevant manufacturers.

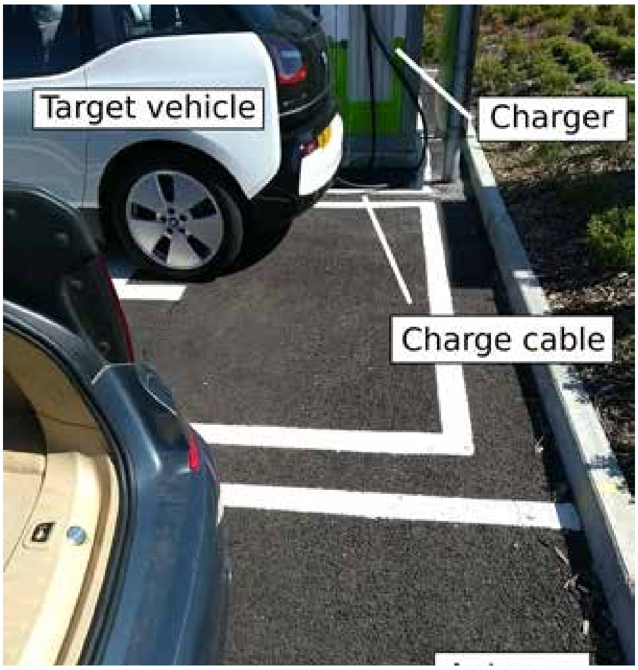
The Future

Further work is now underway to fully map the capabilities of an attacker. An early-stage project, with CDT student Sebastian Köhler and research associate Dr Riccardo Spolaor is currently exploring the impact of jamming and message injection upon the charging communication. The results are expected to have an impact on the design of future EV charging systems, as well as implications for the use of powerline communication in industrial contexts generally.

References

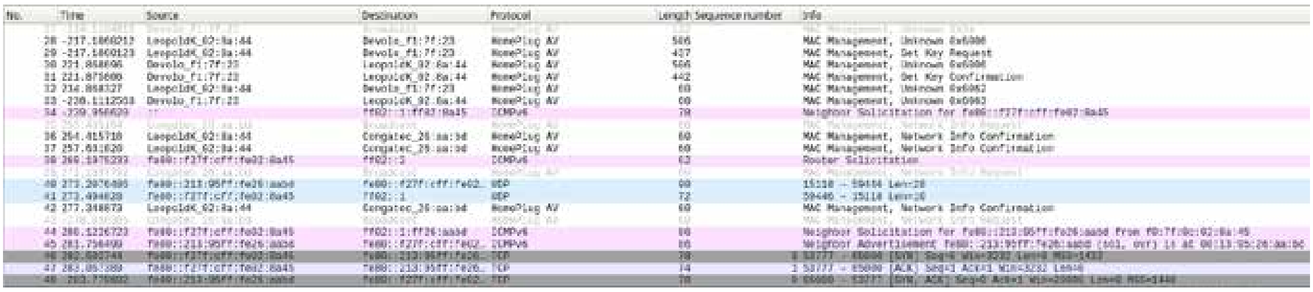
Richard Baker and Ivan Martinovic. “Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging”. In 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, 2019. USENIX Association.

Sébastien Dudek et al. “V2G Injector: Whispering to cars and charging units through the Power-Line”. In Symposium sur la sécurité des technologies de l’information et des communications (SSTIC) 2019.



Capturing messages from the next parking bay

Capturing from two vehicles charging simultaneously



```
No.  Time          Source                      Destination              Protocol     Length Sequence number Info
27   [illegible]   Devolo_f1:7f:23             Broadcast                HomePlug AV  [illegible]            MAC Management, Unknown [illegible]
28   -217.1860212  LeopoldK_62:8a:44           Devolo_f1:7f:23          HomePlug AV  566                    MAC Management, Unknown 0x6008
29   -217.1860123  LeopoldK_62:8a:44           Devolo_f1:7f:23          HomePlug AV  437                    MAC Management, Set Key Request
30   221.858696    Devolo_f1:7f:23             LeopoldK_62:8a:44        HomePlug AV  566                    MAC Management, Unknown 0x6008
31   221.875600    Devolo_f1:7f:23             LeopoldK_62:8a:44        HomePlug AV  442                    MAC Management, Set Key Confirmation
32   234.858327    LeopoldK_62:8a:44           Devolo_f1:7f:23          HomePlug AV  60                     MAC Management, Unknown 0x6062
33   -238.1112568  Devolo_f1:7f:23             LeopoldK_62:8a:44        HomePlug AV  60                     MAC Management, Unknown 0x6063
34   -239.956629   ::                          ff02::1:ff02:8a45        ICMPv6       78                     Neighbor Solicitation for fe80::f27f:cff:fe02:8a45
35   [illegible]   Congatec_26:aa:3d           Broadcast                HomePlug AV  60                     MAC Management, Network Info Request
36   264.415718    LeopoldK_62:8a:44           Congatec_26:aa:3d        HomePlug AV  60                     MAC Management, Network Info Confirmation
37   257.631620    LeopoldK_62:8a:44           Congatec_26:aa:3d        HomePlug AV  60                     MAC Management, Network Info Confirmation
38   269.1875233   fe80::f27f:cff:fe02:8a45    ff02::2                  ICMPv6       62                     Router Solicitation
39   [illegible]   Congatec_26:aa:3d           Broadcast                HomePlug AV  60                     MAC Management, Network Info Request
40   273.2076405   fe80::213:95ff:fe26:aabd    fe80::f27f:cff:fe02…     UDP          90                     15118 → 59446 Len=28
41   273.494628    fe80::f27f:cff:fe02:8a45    ff02::1                  UDP          72                     59446 → 15118 Len=10
42   277.348873    LeopoldK_62:8a:44           Congatec_26:aa:3d        HomePlug AV  60                     MAC Management, Network Info Confirmation
43   [illegible]   Congatec_26:aa:3d           Broadcast                HomePlug AV  60                     MAC Management, Network Info Request
44   280.1226723   fe80::f27f:cff:fe02:8a45    ff02::1:ff26:aabd        ICMPv6       86                     Neighbor Solicitation for fe80::213:95ff:fe26:aabd from f0:7f:0c:02:8a:45
45   281.758400    fe80::213:95ff:fe26:aabd    fe80::f27f:cff:fe02…     ICMPv6       86                     Neighbor Advertisement fe80::213:95ff:fe26:aabd (sol, ovr) is at 00:13:95:26:aa:bd
46   282.880748    fe80::f27f:cff:fe02:8a45    fe80::213:95ff:fe26…     TCP          78                   0 53777 → 65000 [SYN] Seq=0 Win=3232 Len=0 MSS=1432
47   283.05[illegible] fe80::f27f:cff:fe02:8a45 fe80::213:95ff:fe26…    TCP          74                   1 53777 → 65000 [ACK] Seq=1 Ack=1 Win=3232 Len=0
48   283.775802    fe80::213:95ff:fe26:aabd    fe80::f27f:cff:fe02…     TCP          78                   0 65000 → 53777 [SYN, ACK] Seq=0 Ack=1 Win=20000 Len=0 MSS=1440
```

Recovered messages, including the key exchange

Cyber Security in Context

Arianna S., CDT16, Alastair Jane Van Rensburg, CDT15 and Richard Baker, CDT15

Last year, students from CDT'16 ran a "cyber-crisis simulation" for the fresh-faced first years of CDT'18. This year, Arianna S., Alastair Janse van Rensburg and Richard Baker developed and rolled out an entire module based on a similar idea: in order to appreciate cybersecurity you are going to have to get elbow-deep in 1s and 0s at some point.

"Cybersecurity in Context" was a four-day class designed to teach technical skills using Capture-The-Flag (CTF) exercises, and develop an appreciation for the wider impact of the application of these skills; exploring the causes of and responses to cybersecurity events. Three days were themed (forensics, binary exploitation and web) while the fourth focused on medical devices and was our take on the cyber-crisis simulation that made use of skills built up throughout the week.

For days one, two and three, students attempted a series of technical challenges with each challenge representing a particular cybersecurity concept – on "web day" for example, they had to carry out SQL injection attacks on a simple website. The cohort was divided into small groups that put together students from mixed backgrounds. Each group was presented with the same challenges, which they could tackle in any order, and were asked to keep a logbook of solutions they came up with.

Designed to accommodate a variety of skillsets, exercises were meant to enable students of all backgrounds to get hands-on with the theoretical concepts being presented. After the attempting the day's CTF activities, teams came back together to discuss the challenges and place the technical component within the wider context of cybersecurity. We did this by looking at the role these technical elements played in real-world examples.

During "binary exploits", the technical tasks were based around practical experience in subverting software, understanding why these exploits are used (and how to mitigate them) and learning about what they look like "in the wild". Malware research and analysis was the context for these discussions and the three groups were given scenarios in which they were part of an organisation that had experienced an attack (parallels were drawn to Shellshock, Spectre and Triton cases respectively), and needed to brief themselves on the situation, presenting mitigation recommendations accordingly. The "dual-use dilemma" was hotly contested, as to whether or not hacking tools should be used to protect and defend when the potential for their use can have negative consequences. When focusing on web exploits, teams were encouraged to consider the role of regulation in outlining data protection obligations. They needed to review a data breach, discover which exploit had been used, identify the impact or impacts this had and deliver key lessons learned, as well as how this might change their security position moving forward. Further discussion developed ideas around the different levels at which to exploit, such as individual, organizational and state level, while teams presented some excellent ideas regarding how these could be mitigated with very different approaches – preemptive technical solutions at the physical, network and application layers alongside the specification and enforcement of policy, regulation and law.

CDT'19 needed to apply their (in some cases, newly discovered) technical skills to handle their cyber-security crisis, and they did an excellent job. A hospital had been hacked via a vulnerability in one of their medical devices. Students were divided into three teams: Hospital, Manufacturer and Regulator, and given separate briefings. Their objective? To attribute the attack and provide recommendations at the end of the day on how they might respond to or mitigate similar situations.

Feedback received indicates "such an enjoyable course" and that the week was "very valuable". Teams needed to share information but had limited access to each other, so they needed to negotiate the situation as well as with each other. What made the exercise even more challenging was that while each team had their own objectives, attribution needed to be done by the group as a whole. By having to consider organisational behaviour, secure development practice, responsible disclosure, forensic information gathering and regulatory compliance in addition to information gleaned from their technical tasks, students needed to work together to pare down a wealth of data into useful knowledge.

One of the strengths of this Centre for Doctoral Training in Cyber Security is that many students collaborate across departments, and there is a great deal of work that is carried out across multiple disciplines. By running this module the organisers aimed to give both hands on security experience, and stimulate discussion around the impact of technology. The positive engagement and feedback received during and after this class suggest that this exercise is a valuable one, with further potential for future cybersecurity training.

UN-Trusty Co.

Initial Briefing Note

CONFIDENTIAL

Situation

[illegible]

Objective

[illegible]

Tasks

[illegible]

The Computer Misuse Act 1990: the history and context of developing the section 1 offence

Kristopher Wilson, CDT14

The criminal law has consistently grappled with new forms of technology: in that sense, computers are not unique. What makes computers particularly challenging, however, is their ability to intermediate conduct, making possible a wide variety of results from a core set of interactions. This separation between a given computer-mediated act and its effect necessitates serious consideration of the *target* and *focus* of criminality within the construction of criminal offences.

A focus on specifically criminalising the act of making *use* of a computer could result in proscribing otherwise benign conduct. A focus on criminalising the *effect* produced by such use might not sufficiently disincentivise behaviour perceived as risky or harmful. Further, this might result in reliance on general (or pre-existing) offences to prosecute behaviour, only to have those prosecutions fail due to the rigidity of definitional interpretations constructed and conceived by both the legislature and the Courts in the absence of computers. This latter possibility was the problem that in fact arose during early attempts to prosecute individuals who had 'caused damage' to computers,[1] or had obtained the use of a network subscription service by use of another's access credentials.[2] This prompted consideration of creating new offences to respond to 'hacking'.

The Law Commission, in the context of heightened political and public attention to the misuse of computers, released a Working Paper for public consultation in 1988.[3] The central question presented in the Working Paper was '[s]hould the obtaining of unauthorised access to a computer be a criminal offence?'[4] The overwhelming view of the submissions received on this point was that 'hacking by unauthorised entry (or attempted entry) is sufficiently widespread to be of major concern to computer system users'.[5] 'Hacking' was presented as both a threat to the confidentiality or value of information stored on a computer, and a broader threat to the integrity and trust in computer systems. The Law Commission accepted this view noting further that hacking may be undertaken as a preliminary step to committing further general offences, and that the permissibility of *any* form of hacking would result in a feeling of 'insecurity' by computer owners.[6]

The Law Commission rejected the few arguments put forward that the underlying activity of 'hackers' in certain contexts could be beneficial to improving the security of computer systems. Taking a property-based conception of ownership of the system, the Law Commission argued that '[i]t is for those operators to decide how their system shall be tested. If they *invite* outside attack ... that is irrelevant to the uninvited and unauthorised intrusions with which most system owners are concerned'.[7] No consideration appears to have been placed on the difference in 'ownership' of a hardware and 'ownership' of software, the ownership of the former being transferred at purchase, with ownership of the latter remaining with the creator with a transfer of a *license* to use that software being created.

Questions over the enforcement of any such offence were also set aside. The Law Commission was convinced that with full cooperation by the owners of 'victim' computers, law enforcement would face a relatively simple task to identify the source of an 'incoming connection'. Active enforcement would thus remove 'the present aura, if not of acceptability then at least of fun, that surrounds hacking'[8] which would work to persuade 'young people not to enter into, or to be instructed in, hacking'.[9] The efficacy of this view and approach was supported by 'informants' from police forces and industry.[10]

The Law Commission thus concluded that an offence of 'unauthorised access' was both justified and necessary, and, while it would not totally eliminate hacking, it would go a long way toward reducing the overall incidence of 'hacking' and thus increase confidence in the integrity of computer systems.[11] The Law Commission believed a broad offence with a 'comparatively moderate penalty' would serve the aims of deterring all forms hacking, with an additional offence for those who hack in furtherance of an intention to commit a general offence which would carry a more serious sentence (such as fraud).[12] The Law Commission thus recommended a hierarchical approach to dealing with hacking: a summary offence to deal with 'general mischief', and an indictable offence for hacking with *ulterior intent*.[13]

[1] Cox v Riley (1986) 83 Cr App R 54; R v Whiteley (1991) 93 Cr App R 25.

[2] R v Gold and Anor [1988] 2 All ER 186.

[3] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988).

[4] Law Commission, 'Computer Misuse' (Working Paper No 11 Cm 186, 1988) [8.4].

[5] Law Commission, 'Criminal Law: Computer Misuse' (Report no 186 Cm 819, 1989) [2.10].

[6] Ibid [2.14].

[7] Ibid [2.17].

[8] Ibid [2.23].

[9] Ibid.

[10] Ibid.

[11] Ibid [2.24].

[12] Ibid [3.10].

[13] Ibid [3.11].

In relation to the 'basic access offence', it was proposed that such an offence should require that the person 'caused a computer to perform any function with intent to secure access to or obtain information about a program or data held on the computer'. Further, the accused must know the intended access was unauthorised.[14] The potential breadth of this offence was not of concern to the Law Commission who noted that cases where a hacker does not successfully *gain access* to a target system or data would be rare as they would likely not be detected. But they went further, arguing that if the offence required successfully *gaining access*, rather than attempting to, an accused who was in fact detected at an early stage 'might claim that he was only interested in testing the system's defences ... [but they] would still in our view be someone whom the law should seek to discourage.'[15] It was argued that the *mens rea* requirement of intent to gain access would serve a suitable limiting function.

In considering the construction of 'authorisation', the Law Commission noted that while it would be clear that a remote access by an *outsider* would clearly fall within scope, so too should employees of a company who consciously and deliberately access a computer owned by their employer.[16] In such circumstances the burden should be on the prosecution to prove that the employee had knowledge of the extent of their authority and this would be the case where the employer had 'clearly defined limits' which 'should be laid down as a matter of good management practices'.[17] Thus the Law Commission recommended what would essentially be an incentive for computer owners to create a clear chain of authority, supported by policy and other internal documents, that could provide adequate notice to employees of acceptable computer use. Such a requirement was deemed sufficient to negate suggestions that it might be prudent to introduce a possible defence of honest belief.[18]

The Law Commission then turned to the connected issue of *an authorised use for an unauthorised purpose*, that is where an individual or employee does not exceed their scope of authorisation in respect to *accessing* the computer itself but instead undertakes conduct which would fall *outside* their normal duties. It was recommended that such conduct should **not** fall within the scope of the offence.

The final observations made in respect of the basic access offence were to confirm that the term 'computer' should be left undefined, noting that the submissions received agreed that it would unnecessary to attempt to define it. It was then recommended that offence would be triable summarily only with a maximum penalty of three months' imprisonment, a fine up to Level 4 on the scale (at the time £500), or both.[19] While initially considering a six month maximum, the Law Commission was concerned to avoid the impression that the basic offence would be so serious as to warrant a custodial sentence in *most cases*.[20]

With government backing, Michael Colvin MP introduced the Bill that would establish the *Computer Misuse Act 1990* ('CMA'). The Bill navigated the House of Commons and the House of Lords relatively smoothly, with a number of amendments proposed at the Standing Committee stage.[21] It contained the three offences recommended by the Law Commission while also providing additional provisions to deal with jurisdictional issues, as well as some interpretative guidance as to the definition of 'access' and 'authorisation'.

The need for the offences, or the suitability of their framing (as protection of computer integrity) was not seriously challenged during the debate. Indeed, some contributions to the debate were not particularly useful. Hackers were described as members of 'a twisted culture'.[22] This culture was suggested to include those 'who spend all night hacking, and lose their job because of poor performance, or they might have been sacked for hacking whilst at work ... consequently that are often poor',[23] although according to other contributions hacking was lucrative because '[t] hey make a great deal of money out it and the German hackers, at any rate, support a drug-based lifestyle on their activities' and 'because drugs are expensive, hackers need to make a great deal of money'.[24] It was further lamented that '[a]t one time, computers were used only by a few professors and very disciplined professionals, but the tremendous growth in microcomputing has meant the entry into the arena of the unspeakable'.[25] These 'unspeakables' were also said to be motivated by 'a profound sexual inadequacy'.[26] Unsurprisingly, then, the Bill was passed, and the CMA came into force on 29 August 1990.

The basic access offence was constructed in line with the recommendations of the Law Commission, incorporating the focus on 'causing a computer to perform a function' when undertaken with an 'intent to secure access' where the accused 'knows' that the access would be unauthorised. Section 1 thus provided:

A person is guilty of an offence if:

> – he causes a computer to perform a function with intent to secure access to any program or data held in a computer;

[14] Ibid [3.14].

[15] Ibid [3.18].

[16] Ibid [3.35].

[17] Ibid [3.37].

[18] Ibid.

[19] Ibid [3.45].

[20] Ibid.

[21] Notably the proposal to introduce a defence to the section 1 offence where it could be established that the owner of the computer had not taken 'such care as in all the circumstances, was reasonably required to prevent the access in question'. This would effectively be making contributory negligence a defence to a criminal charge, and the amendment was ultimately withdrawn on that basis. This would, however, have brought the section 1 into line with the data protection principles in the Data Protection Act 1984. See, further, Stefan Fafinski, 'Computer Use and Misuse: The Constellation of Control' (PhD Thesis, University of Leeds, September 2008) 39.

[22] HC Deb 9 February 1990, vol 166, col 1137.

[23] HC Deb 9 February 1990, vol 166, col 1177.

[24] HC Deb 9 February 1990, vol 166, col 1154.

[25] HC Deb 9 February 1990, vol 166, col 1151.

[26] HC Deb 9 February 1990, vol 166, col 1156.

- the access he intends to secure is unauthorised; and
- he knows at the time when he causes the computer to perform the function that this is the case.
- The intent a person has to have to commit the offence under this section need not be directed at:
  - any particular program or data;
  - a program or data of any particular kind; or
  - a program or data held in any particular computer.

While the Law Commission's argument that the breadth of the offence might indeed be counterbalanced by the relatively low penalty in their proposal (being in most cases the proverbial slap on the wrist), this was not what was implemented. Instead, the offence provided for a maximum sentence of six months imprisonment, a fine fixed at the statutory maximum (£1000 at the time), or both.[27] The offence retained its summary nature, and was to operate as a lesser-alternative-offence for both sections 2 and 3.[28] This position wouldn't last.

The scope of the offence itself has since been expanded. By leaving computer undefined, the courts have provided the definition as being 'a device for storing, processing and retrieving information'.[29] This potentially now includes all manner of devices including lightbulbs, fridges, cars and watches.[30]

The scope of 'authorisation' has similarly expanded. Take the example of employees. While the Law Commission was of the view that those employees ought not be prosecuted for authorised access for unauthorised purposes, the court, relying on the interpretive guidance provided in the CMA, expanded the offence to cover that very sitation in the case of *R v Bow Street Metropolitan Stipendiary Magistrate and Allison, ex parte United States (No. 2)* ('Allison').[31] *Allison*, involved an employee of American Express who used their access to the American Express computer system to obtain the credit card details of customers and provided those to a number of third parties in the United States, and to Mr Allison who resided in London. These would be used to create fraudulent credit cards. Lord Hobhouse, providing the majority judgement in the House of Lords, rejected the view that authorisation was associated to a 'kind of data', rather it was linked to 'specific data' and 'specific purposes'. The decision in *Allison* thus meant not only that authorisation can, and should, be limited to the specific data in question, but by interpreting the scope of any authority with respect to the 'kind' of access secured as a *separate* and *additional* consideration, the court opened the door for the offence to apply to situations where an accused may have authority to access the data but did so by way of a method that was not itself authorised. Breaches of everyday terms of service agreements might constitute an offence.

While the courts have expanded the scope the offence, the legislature has also increased the penalties. The *Police and Justice Act 2006* modified the sentences available for the section 1 offence. As part of the broader package to ensure the CMA 'kept up' with computing technologies, the character of the section 1 offence was changed from that of a summary offence, to an offence triable either way (that is, also as an indictable offence).[32] On summary conviction, the offence carried a maximum term of imprisonment of 12 months, the statutory maximum fine (£5000), or both.[33] On conviction on indictment the section 1 offence can attract a maximum imprisonment term of two years, the statutory maximum fine, or both.[34] The conversion of the offence from summary to indictable also renders the section 1 offence subject the *Criminal Attempts Act 1981*. It is thus now possible to be prosecuted for attempting to cause a computer to perform a function.[35] These increasingly severe penalties came despite the Law Commission initially arguing that a custodial sentence should be a last resort. Further, with the passing of the *Legal Aid, Sentencing and Punishment of Offenders Act 2012 (Fines on Summary Conviction) Regulations 2015* there is no longer a maximum limit on fines for offences committed under section 1.

These subsequent amendments were made without due consideration for the initial justifications put forth for the creation of the offence in the first place, and that's despite the inherent weaknesses in the arguments accepted by the Law Commission at the time. The section 1 offence casts a wide net and has morphed throughout its 27-year history to become a clear example of over-criminalisation. Most recently, in 2018 the Information Commissioner's Office appears to have discovered this, electing to prosecute an individual for accessing personal information from the Audatex platform (used to process insurance claims) under the CMA rather than pursue charges under the *Data Protection Act 2018*.[36] Time will tell if the cat is now well and truly out of the bag.

[27] Computer Misuse Act 1990 s 1(3) [as originally enacted].

[28] Computer Misuse Act 1990 s 12 [as originally enacted].

[29] DPP v McKeown, DPP v Jones [1997] 2 Cr App R 155, at 163 per Lord Hoffman in the context of admissibility of evidence.

[30] While no such prosecutions have seemingly occurred yet, conduct that would qualify for prosecution has occurred and has been prosecuted in the United States, albeit via fraud offences and then for conspiracy in respect of conduct contravening the Computer Fraud and Abuse Act 18 USC § 1030(a)(5)(A) and (s)(4)(A): see the Mirai Internet of Things Botnet that launched the largest scale Distributed Denial of Service attack observed to date by installing malware in thousands of home 'smart' devices to seize control of their network connection and target the website of cyber security specialist Brian Krebs in July 2016. Brian Krebs, Mirai IoT Botnet Co-Authors Plead Guilty (17 December 17) Krebs on Security <https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/>.

[31] R v Bow Street Metropolitan Stipendiary Magistrate and Allison, ex parte United States (No. 2) [2000] 2 AC 216.

[32] Amended pursuant to Police and Justice Act 2006 ss 35(3), 53.

[33] Computer Misuse Act 1990 s 1(3)(a).

[34] Computer Misuse Act 1990 s 1(3)(c).

[35] Criminal Attempts Act 1981 ss 1(1), 1(4).

[36] See, eg, Jill Lorimer, 'ICO Secures First Prosecution Under Computer Misuse Act', Kingsley Napley (15 November 2018) < https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/ico-secures-first-prosecution-under-computer-misuse-act >.

Tackling the cyber security skills shortage with ENISA

Tommaso de Zan, CDT17

When I realized there was the possibility to do my summer mini-projects at the European Union Network and Information Security Agency (ENISA), I did not hesitate. I have always had the desire to conduct my research embedded in a policy institution like an EU agency, and if you are dealing with cyber security, ENISA is the right place to be.

From a professional/research viewpoint, ENISA delivered and I could not ask for more. Since my arrival in Athens, I was part of COD2, the Data Security and Standardization Unit of ENISA. This meant that I had to attend weekly meetings and participate to the unit's overall activities. It was great to be part of a team since the very beginning as it really helped me to integrate faster in the organization. The best part of my arrangement with ENISA was that I could do my research, but I could also be involved in some of the Agency's projects. Because of my interest in cyber security education and awareness, I asked to be included in the European Cyber Security Month (ECSM) and European Cyber Security Challenge (ECSC) projects. It was fascinating to realize how my research could develop from the high-level concept to something with more concrete policy implications. In fact, for the remainder of my DPhil, I will investigate how capture-the-flag competitions such as the ECSC affect students' interest in a cyber security career. Being involved in the ECSC gave me a comprehensive understanding of the main stakeholders involved in competitions at the national level and how my research could be useful to answer some of the analytical challenges that practitioners in the field have.

The mini-projects went really well, mainly because I had the time to interview many of ENISA's experts. Despite doing interviews in a single organization, the variety of backgrounds – both geographic and academic/professional (I interviewed former heads of national certs, Microsoft's employees, professors and NATO officers just to tell you a few) – helped me to achieve a depth of insights that I would have hardly gathered in any other organization.

Besides work, going to the office everyday was a pleasure. Possibly influenced by the warmth of the southern European sun, people were smiley and kind since day one. I distinctively remember thinking on the day of arrival "why is everyone so smiley?" In the end, ENISA was great to get some (good) work done, but also have more relaxed chats with experts who will always remain good connections for the rest of my life.

On top of all that, I spent spring and summer in Greece!!! I was not expecting it, but I completely fell in love with Athens. What a remarkable city, there is everything you could possibly want: history, amazing food & wine, beaches and welcoming locals! The best part of Athens was going off the traditional tourist pathway and try to do what the Greeks do. Among the best things I have done, besides trying a new Greek taverna every weekend, was to watch one of the final games of the Greek national basketball championship. Believe me, it was intense!

One year later, I am very much missing ENISA and Athens, but I am determined to make our paths cross again in the future! Kalispera!

Panellist’s view of US Cyber Command’s Annual Symposium

Graham Fairclough, CDT13

For the past two years I have been fortunate to be invited to attend US Cyber Command’s annual symposium, the first, held in 2018 as a participant and as a panelist at the 2019 event. The symposium, held at the National Defence University, Washington brings together 200 participants drawn from Cyber Command and other areas of the US Department of Defence (DoD), the US Government, its Five-Eyes allies and academia. Its purpose is to discuss key issues faced by the Command, which the Commander feels would benefit from wider community consideration. The opening address being given by the incumbent Commander, currently Major General Paul Nakasone and previously Admiral Mike Rodgers.

The focus of the initial symposium was to consider the then forthcoming DoD cyber security strategy and Cyber Commands role within it.[1] A focus, simplified in early discussion by asking the question of how the Command will fulfil its central mission of ‘Defend the Nation’ in cyberspace. In answering this question three themes emerged. Firstly, a deep sense of frustration that despite the resources available to the US it seemed unable to mitigate the threat posed by its adversaries in the cyber domain, principally Russia and China, closely followed by North Korea and Iran. Secondly, how the Command should configure itself to conduct its mission and how its role should be integrated across the wider DoD operating model. Thirdly, what policy framework and power of authority was needed to allow the Command to enable mission success. On reflection the symposium represented a ‘shaking-out’ of the themes central to the command’s future operations.

For the second symposium in 2019, the focus was on the operationalisation of the 2018 strategy, concentrating on its key concepts of Persistent Engagement, Defend Forward and their enablement through Partnership and Innovation. The focus of my panel being on the relationship between the role of partnerships in the delivery of Defend Forward. Sharing the stage with Commander US Army Cyber Command, a deputy director of the CIA and the CEO of a financial services company the discussion concluded that partnerships between Cyber Command and its allies, the private sector and academia were not just a requirement but a necessity. Thus, recognising that neither Cyber Command or the wider US government had the resources, principally skilled manpower, knowledge and technical capacity, to deliver Defend Forward on a global scale. A finding that also surfaced in two of the other, four panels.

Attendance at these events has been a great benefit to my studies. The opportunity to meet leading edge cyber security strategists from government, the private sector, and importantly academia alongside engaging in conversation with practitioners who are operating on the front line of cyberspace provided unique insights and alternative positions of relevance to my work. Furthermore, attendance has opened doors to participate in other equally important and challenging events. My only hope now is to receive an invitation to next year’s symposium.

By United States Cyber Command - The Commander’s Vision and Guidance for US Cyber CommandUS-Cyber-Command-Commanders-Vision

[1] An unclassified summary of the strategy, Strategy to Achieve and Maintain Cyberspace Superiority, was published in September 2018.

Cyber Security, Tech Abuse, and Intimate Threats

Julia Slupska, CDT18, Marine Eviette, CDT18, Fatima Zahrah, CDT18, Romy Minko, CDT17 and Zach Tan, Oxford Internet Institute

As technology further intertwines with daily life, perpetrators of intimate partner abuse (IPA) are exposed to more sophisticated means of controlling their targets – leading to a rise in technology-facilitated abuse, or "tech abuse."

Tech abuse describes the use of digital technology to coerce and control someone in the context of an intimate relationship. IPA is a highly prevalent, although often unacknowledged, problem in the UK: one third of all violent crimes recorded by the police in the year ending March 2018 were domestic abuse related.[1]

UK national statistics show women are disproportionately targeted; 8% of adult women and 4% of adult men have experienced abuse.[2] Minoritized women also tend to be the most vulnerable IPA targets due to language barriers, negative experiences with law enforcement, and economic difficulty.[3]

85% of IPA survivors reported experiencing tech abuse as part of a broader pattern of controlling behaviour.[4] Abusers use the following strategies for coercion and control:[5]

- Restricting access to the internet as a form of punishment
- Monitoring devices and accounts
- Forcing targets to disclose passwords
- Guessing passwords or recovery questions
- Private and public harassment, such as threats of violence or self-harm
- Doxxing (exposure of private information)
- Non-consensual pornography

Problem landscape

Our report applied Lessig's framework of the "pathetic red dot". By thinking of human actions as a "dot" acted on by four forces – social norms, the law, the market, and 'architecture' (including information architectures) – we parse out key interactions and understand the problem of tech abuse through a systems approach (see Figure 1).[6]

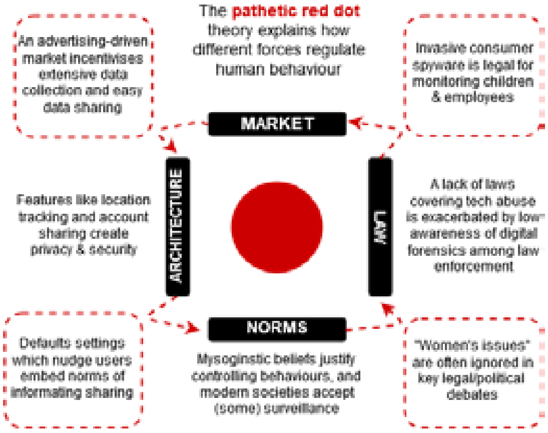

The pathetic red dot theory explains how different forces regulate human behaviour
An advertising-driven market incentivises extensive data collection and easy data sharing
Invasive consumer spyware is legal for monitoring children & employees
MARKET
ARCHITECTURE
LAW
Features like location tracking and account sharing create privacy & security
A lack of laws covering tech abuse is exacerbated by low awareness of digital forensics among law enforcement
NORMS
Defaults settings which nudge users embed norms of informating sharing
Mysoginstic beliefs justify controlling behaviours, and modern societies accept (some) surveillance
"Women's issues" are often ignored in key legal/political debates

Figure 1: Lessig's pathetic red dot theory of governance applied to the problem of tech abuse

Social Norms

Economic and social dependence on the abuser makes it extremely difficult to leave abusive relationships.[8] Furthermore, misogynistic views and beliefs encourage and justify social control and coercion of women.[9] Violence that is disproportionately targeted at women, like IPA, is often taken less seriously. Even after significant efforts made through legal reforms, reports of domestic abuse are still often dismissed in police stations as "just a domestic".[10]

Similar dynamics of exclusion are replicated in cybersecurity. Existing practices rarely consider gendered offences like revenge porn or social-media stalking as "real" cybersecurity vulnerabilities,[11] Furthermore, societal acceptance of paternalistic surveillance practices – such as the widespread monitoring of children or employees – contribute to the continued legality and accessibility of abuse vectors such as commercial spyware applications.[12] Society lacks robust ethical

Note: This paper reports on a research project for Map the System 2019, a competition which asks participants to apply systems level thinking to a social or environmental problem. This is a short summary, please contact us if you have questions.

[1] ONS, "Domestic Abuse in England and Wales: Year Ending March 2018," Office for National Statistics, 2018, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2018.

[2] ONS, ibid.

[3] "The Nature and Impact of Domestic Abuse," Women's Aid, 2018.

[4] "Online and Digital Abuse," Women's Aid, 2018, https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/.

[5] Diana Freed et al., "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 2018, https://doi.org/10.1145/3173574.3174241.

[6] Lawrence Lessig, Code: And Other Laws of Cyberspace, Version 2.0, New York, 2006.

[7] Lessig.

[8] "The Nature and Impact of Domestic Abuse."

[9] Janemaree Maher, Jude Mcculloch, and Kate Fitz-Gibbon, "New Forms of Gendered Surveillance? Intersections of Technology and Family Violence," in Gender, Technology and Violence, ed. Marie Segrave and Laura Vitis, 1st ed. (Routledge, 2017).

[10] "Transforming the Response to Domestic Abuse, Consultation Response and Draft Bill" (2019).

[11] Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity," St. Anthony's International Review, no. Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace (2019).

[12] Rahul Chatterjee et al., "The Spyware Used in Intimate Partner Violence," in Proceedings - IEEE Symposium on Security and Privacy, 2018, https://doi.org/10.1109/SP.2018.00061.

and moral frameworks for recently developed digital technology. Consequently, the burden of protection is placed primarily on the user so that individuals are held solely responsible for their activity and posts, even if they are misused by others without consent.

Law

Rapid technological change in abuse methods often obfuscates the definition of what constitutes 'abuse'. For example, the language of restraining orders does not cover the misuse of smart home technologies for gaslighting.[13] Although computer misuse laws are sometimes sufficient for prosecution, technological advancement means that their applicability is inconsistent at best, and unrecognised at worst.[14] Consequently, IPA advocates often rely on stalking and harassment laws instead of computer misuse laws. Incomplete legal coverage is often exacerbated by technical unfamiliarity among law enforcement officials, prosecutors, and targets.[15] The effective handling and interpretation of digital evidence by forensic investigators poses several challenges for prosecution. Although the vast volume of data being collected and retained as evidence by law enforcement increases potential lines of inquiry, its use must also be matched by relevant and continuous training.[16]

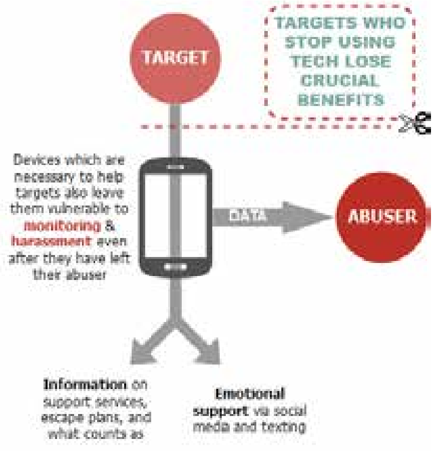

TARGET
TARGETS WHO STOP USING TECH LOSE CRUCIAL BENEFITS
Devices which are necessary to help targets also leave them vulnerable to monitoring & harassment even after they have left their abuser
DATA
ABUSER
Information on support services, escape plans, and what counts as
Emotional support via social media and texting

Figure 2: Dependence on information technology poses problems for targets of IPA

Market forces

Technology companies are motivated to collect, process, and monetise user data as a viable business model at the expense of privacy and security. Under the free-user paradigm, social-media platforms attract and retain users through providing free access while generating profit by monetizing user data for advertising products. Adjacent markets for secondary data processing, commercial location monitoring software and "Internet of Things" (IoT) devices stretch and sometimes violate the principle of "informed consent".[17]

Furthermore, application design and marketing often treat families as a single unit for privacy and security. By incentivising the commodification and portability of user data between products, market forces enable abusers to access data about their target.

Architecture

Seemingly neutral design decisions can facilitate tech abuse. Since data collection, portability, and sharing is typically a default functionality built into applications, an abuser with access to their target's personal data can make it exponentially more difficult for a target to escape, be it physically or from digital monitoring and control.[18]

The failure to acknowledge serious security risks resulting from shared use (by partners or families), provides loopholes for IPA abusers to exploit. Technical functions designed for security, such as remote access tools, have been, and still are, re-appropriated by IPA abusers. For instance, the Find My Friends functionality in iOS products is easily subverted for tracking and monitoring.

Even when explicitly stated, permission settings may simply offer the illusion of choice, and applications will sometimes limit their services if a user attempts to increase their security and privacy settings. This presents a potential 'lose-lose' situation if an IPA target relies on that application to contact family and friends, or to find ways out of abusive situations (see Figure 2). Additionally, applications rarely check or carry over settings previously defined by the user between updates or shared uses, and default app permissions are usually skewed towards enabling data sharing. Although proactive users can update permissions, this still represents an unfair responsibility for IPA targets – who already face significant cognitive, emotional and financial strains - to continuously check settings between a multitude of applications and updates.

[13] Nellie Bowles, "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," The New York Times, 2018.

[14] Kaofeng Lee, "Technology Abuse: It's Still About Power & Control," Women's Media Center, 2016.

[15] Hadeel Al-Alosi, "Technology-Facilitated Abuse: The New Breed of Domestic Violence," The Conversation, 2017.

[16] Owen Bowcott, "Justice System at 'breaking Point' over Digital Evidence," The Guardian, 2018.

[17] H Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," Law and Philosophy, 1998, https://doi.org/10.2307/3505189.

[18] Freed et al., "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology."

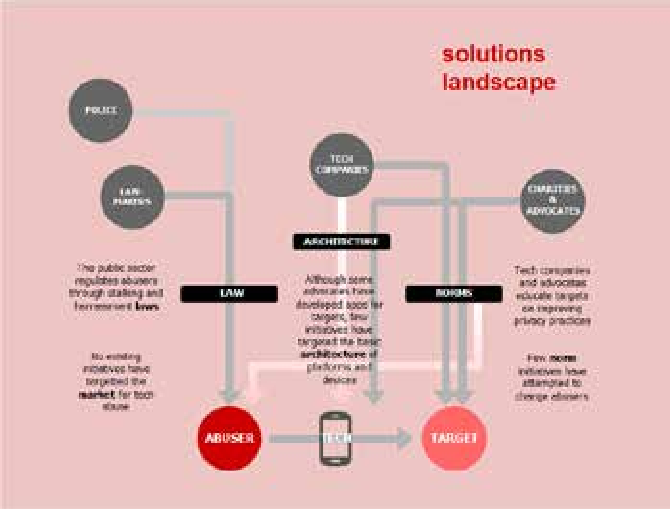

solutions landscape
POLICE
LAW MAKERS
TECH COMPANIES
CHARITIES & ADVOCATES
ARCHITECTURE
LAW
NORMS
The public sector regulates abusers through stalking and harrassment laws
Although some advocates have developed apps for targets, few initiatives have targeted the basic architecture of platforms and devices
Tech companies and advocates educate targets on improving privacy practices
No existing initiatives have targeted the market for tech abuse
Few norm initiatives have attempted to change abusers
ABUSER
TECH
TARGET

Figure 3: Solutions landscape

Solutions landscape

Multiple actors from the public, private, and social sectors are attempting to address tech abuse in IPA. Though our findings reflect a growing awareness of tech abuse, these solutions typically operate in, and are constrained by their specific sectors. Most also do little to affect change in the behaviour of abusers, and instead continue to place further responsibilities on targets.

Public sector

Recent efforts to expand the legal definition of IPA are reflected in a current draft of the Domestic Abuse Bill, which includes controlling or manipulative non-physical abuse.[19] Additionally, the consultation on the draft bill recognised new abuse vectors by including limited references to the role of technology in IPA, both in terms of how it can be misused and as a means of providing effective solutions, which they are working on with charities.[20] (Ministry of Justice, 2018). Furthermore, the "Internet Safety Green Paper" outlines new measures such as "Online Safety" courses in schools to enhance digital literacy among children.[21]

Private Sector

The private sector has introduced a variety of apps for IPA survivors. "SafeTrek" and "Blackbox" facilitate rapid contact to emergency services when an IPA target faces imminent threats. Applications such as "Smart-Safe", "Bright Sky" or the "Tech Safety App" provide advice and enable targets to record, photograph, and store files to the Cloud to prevent discovery. Some applications utilise covert presence, disguising themselves as mundane calculator or weather applications. Unfortunately, such solutions rely on targets of abuse realising that these tools are available to them. Raising awareness can help abusers identify these tools, creating more risks for targets.

Social media platforms, often the source and most prevalent means of tech abuse, struggle to deal with overwhelming occurrences of online harassment, presenting solutions that still place responsibility on targets.[22] Apple and Google have been responsive to IPA research on spyware on their app stores by banning such overtly tagged applications. However, affected developers responded by simply changing the way their products were marketed. As a result, search terms like "find girlfriend", and "monitor family" still return spyware or dual-use results in the app stores.[23]

Social Sector

IPA support services are at the forefront of countering tech abuse in innovative ways. Many domestic violence charity websites provide the following resources:
An 'escape button' that allows users to immediately exit the site;
Instructions on clearing browser history to avoid detection;
"Technology toolkits" containing best practices for online safety and privacy
Aid workers often feel that they do not possess the technical skills to handle sophisticated threats, such as mobile spyware and the subversion of IoT devices.[24] The

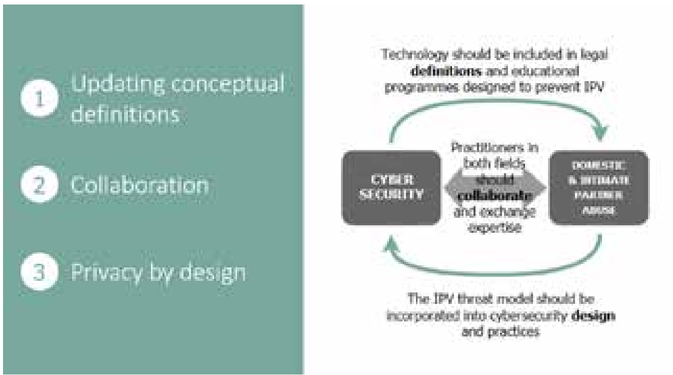

1 Updating conceptual definitions
2 Collaboration
3 Privacy by design
Technology should be included in legal definitions and educational programmes designed to prevent IPV
CYBER SECURITY
Practitioners in both fields should collaborate and exchange expertise
DOMESTIC & INTIMATE PARTNER ABUSE
The IPV threat model should be incorporated into cybersecurity design and practices

Figure 4: Report recommendations

[19] Marian Duggan, "Domestic Abuse Bill: Proposed Changes to Protect Victims Explained," The Conversation, 2019.

[20] Transforming the Response to Domestic Abuse, Consultation Response and Draft Bill.

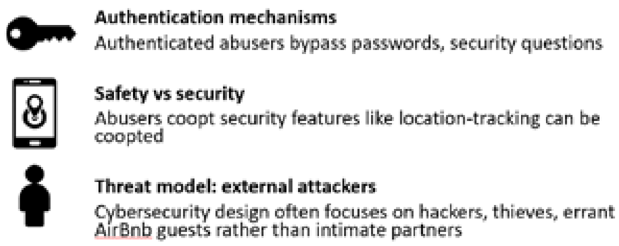
[21] "Internet Safety Strategy - Green Paper." (2017).

[22] Caitlyn Gribbin, "Revenge Porn: Facebook Teaming up with Government to Stop Nude Photos Ending up on Messenger, Instagram," ABC News, 2017.

[23] Chatterjee et al., "The Spyware Used in Intimate Partner Violence."

[24] Isabel Lopez-Neira et al., "'Internet of Things': How Abuse Is Getting Smarter," SSRN Electronic Journal, 2019, https://doi.org/10.2139/ssrn.3350615.

detection of spyware amongst targets is generally ad-hoc and inconsistent, relying on changes in phone behaviour like unusual battery drain, strange notifications and texts, or abusers demonstrating knowledge they would not have otherwise.[25] Spyware removal can be problematic, as targets might be unwilling to remove it for fear of escalating violence.



Authentication mechanisms
Authenticated abusers bypass passwords, security questions

Safety vs security
Abusers coopt security features like location-tracking can be coopted

Threat model: external attackers
Cybersecurity design often focuses on hackers, thieves, errant AirBnb guests rather than intimate partners

Figure 5: Tech abuse challenges many cybersecurity assumptions

Updating conceptual frameworks

Legislators must explicitly recognise the role that technology can play in facilitating IPA and address new threat vectors, such as IoT devices, in the immediate future.[26] Including more specific references to tech abuse within the statutory definition of domestic abuse would increase the level of awareness on this emerging risk vector for both targets and law enforcement.

Education programs can raise awareness of tech abuse. By focusing on early-age education, young adults and teenagers can help clarify social norms as to what is and isn't acceptable online behaviour. Even if there is room for debate, classroom discussions can prompt reflective thinking on whether certain actions – like browsing through a friend's messages or following their location – are acceptable.

Privacy by design

The IPA threat model needs to be incorporated into the product design process. At the design stage, product managers should conduct a domestic violence security review, brainstorm ways in which different features of their products could be subverted, and attempt to mediate these before they hit the market. After products are released, companies should conduct audits and investigate whether their products are being misused.

Design process interventions need to be supported by economic incentives to motivate a shift in industry norms. A useful example is potentially found in Environmental Social Governance (ESG) investing, which provided a framework to incentivise socially responsible investing. ESG treats businesses' approaches to environmental, social, and governance concerns as financially valuable criteria.[27] Investors should evaluate new tech products not just on their usability, but also on whether the design process accounts for the potential of misuse.

Greater Collaboration

We need greater cooperation between cybersecurity professionals and domestic violence charities on the frontlines of tech abuse. Although trainings to 'upskill' charities are useful, they are a highly costly solution given the large number of workers and the constantly changing technology landscape. Given that these charities are already strained for time and money, we suggest that the National Cyber Security Centre establish a *dedicated support line which support workers* can contact for expert opinions. This would allow one dedicated team to research best practices and distribute them to charity workers. The government should investigate the prevalence and legality of consumer spyware and implement both technical as well as legal and regulatory means to prevent the misuse of such tools. Similarly, training specific to tech abuse should be provided to law enforcement officers to help them recognize such instances of abuse.

As technology increasingly mediates our homes and relationships, opportunities for abuse will multiply. The current solutions landscape shows many actors from various sectors addressing this issue, but we firmly believe that more could be done. Tech abuse should be at the forefront of discussions of both intimate partner violence and cybersecurity. As a result, we will be able to address exiting practices more holistically and create social norms, laws, market structures and digital architectures which better serve targets of tech abuse.

We must create social norms, laws, market structures and digital architectures which better serve tragets of tech abuse

[25] Chatterjee et al., "The Spyware Used in Intimate Partner Violence."

[26] Leonie Tanczer et al., "Gender and IoT Research Report: Technology-Facilitated Abuse," November (2018).

[27] Amir Amel-Zadeh and George Serafeim, "Why and How Investors Use ESG Information: Evidence from a Global Survey," Financial Analysts Journal 74, no. 3 (July 2018): 87–103, https://doi.org/10.2469/faj.v74.n3.2.

Life after the CDT

Meredydd Williams, CDT14

A doctorate is often seen as a vehicle for academic progression. However, it is easy to forget the range of opportunities in the private sector. I completed my Cyber Security doctorate in December 2018. But since September, I have worked as a Technology Consultant for Roke Manor Research. Therefore, I've composed this article to outline my experience over the past year. As will become clear, it's possible to marry a full-time job with academic research.

When commencing my doctorate, my sights were set on long-term research. And throughout my four years at Oxford, I relished academia. But, when the thesis was completed, I was placed at a crossroads. Research was a known quantity with a healthy work-life balance. However, I recognised that academic experience can be undervalued. Therefore, as I wished to explore the market, this was the best time.

There's a friendly rivalry between academia and the private sector. While stereotypes are often exaggerated, there are key differences between the environments:

- Travelling. While at Oxford, my commute consisted of a 20-minute walk through University Parks. My commute is now a 90-minute journey, preceded by an alarm clock at 06:30. With this comes costs, inconvenience and the nightmare of rail strikes.
- Deadlines. There is a misconception that the private sector is more driven than academia. The workload is similar in both environments, but the nature of deadlines tends to differ. During a PhD, you might have a large submission every three months. No commercial deliverables are that complex, but they might be due by 5pm.
- Balance. An academic day never really ends. To study, publish and teach, the laptop often emerges on weekends. Days are more defined in the private sector, posing both advantages and challenges. You may reclaim your evenings but miss the freedom of managing your time.
- Freedom. Academics can research their interests, though this is dependent on funding. While the private sector lacks such flexibility, it does provide certainty. Although your workload is selected by others, there is less likelihood that it will disappear.
- Progression. In academia, you can showcase your work on a global stage. But with international exposure comes international competition. There are fewer lecturers than PhDs and advancement has become increasingly challenging. In contrast, companies are unlikely to provide worldwide fame. However, progression and promotion might be more straightforward.

It was not until my final year that I considered the opportunities in the private sector. And because of this, I was rather unprepared! If this article has not deterred you from industry, I have three tips:

- Contacts. Employers will care that you possess a PhD from Oxford. However, they are less likely to care about your publications. Some jobs will align with your research, and these are great opportunities. But most will not, and this can place us in a strange limbo. While few would appreciate a graduate role, we lack the record of an experienced hire. This can lead to (frustrating) automatic filtering from online applications. To ensure your talent is recognised, I suggest making the most of your contacts.
- Skills. While a PhD demonstrates intelligence, employers often perceive academia as lacking realism. For this reason, it is important to develop your transferrable skills. If you're delivering practicals, this demonstrates leadership. If you've spoke at a major conference, you've got international presentation experience. These abilities can be more desirable than the doctorate itself.
- Relax. Don't worry – you'll still receive leave in the private sector. However, it's unlikely to be as frequent or flexible as during your PhD. Therefore, if moving into industry, ensure you take a good holiday first! This should also help to get the thesis nightmares out of your head.

There's some final good news – you can have your cake and eat it too! The division between academia and industry is a false dichotomy. Even if you leave university, this does not preclude you from conducting research. While at Roke, I have continued publishing with my doctoral colleagues. I have also written project bids to collaborate with Oxford academics. And under the auspices of networking, I've even attended conferences at other universities. Do not be afraid to swap sub fusc for a work tie. Your PhD is not an ending, but a beginning.

CDT13 Bios

Bushra AlAhmadi

Supervisor: Ivan Martinovic,
Department of Computer Science

Bushra is in her final year as a PhD student at the Centre for Doctoral Training in Cyber Security, University of Oxford. Prior to starting her PhD, she received an MSc degree with distinction in Computer Science and Engineering with concentration on Network and Information Assurance from Santa Clara University, USA. She was then appointed as a lecturer in the College of Computer and Information Sciences at King Saud University (KSU), Saudi Arabia and received a government scholarship to pursue her doctoral degree. Her previous work experience includes working at the Ministry of Culture and Information in Saudi Arabia, lecturer at King Saud University, Cisco Systems and the Internet Services Operation Security team at Apple in Silicon Valley. Her research involves classification and detection of malware using Machine Learning, improving the security monitoring in Security Operation Centres (SOCs), network security, and the detection of insider threats using Natural Language Processing. Bushra received numerous awards such as the Google Anita Borg Scholarship in 2016, Klaus Brunnstein Award 2016, and Kellogg College Anne McLaren Award for Excellence in 2017. Bushra is also passionate about volunteering, co-founding an initiative inspireHer with support from Google to encourage girls to code in an early age. She also organised workshops at the Annual Hay festival in the United Kingdom to teach children to code using robotics. Bushra is also a member of Hemaya, the leading cyber security professionals community in Saudi Arabia and the Centre of Excellence in Information Assurance in Saudi Arabia.

DPhil Thesis: Applying Software Defined Networking (SDN) Capabilities for Active Malware Detection

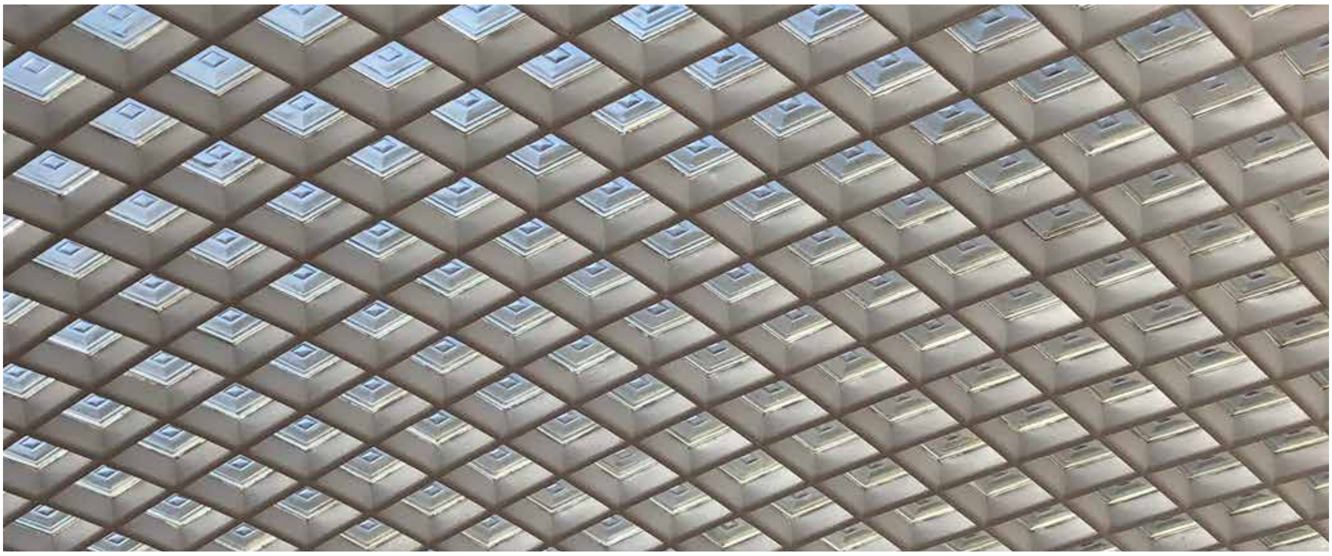
Sophisticated cyber-attacks leverage malware that could have financial, privacy, or human life consequences. Current network intrusion detection solutions are often incapable of detecting malware, as they are built on the assumption that threats are observed as they enter the network at specific perimeter points: an assumption that is no longer valid in modern networks. Attacks have also grown in sophistication and use stealthy malware that are very discrete, traversing the network slowly, taking days, weeks or months to accomplish their objectives to avoid detection. Although Security Information and Event Management (SIEM) systems help deliver a comprehensive analysis, the huge amount of data makes searching for malicious activities like 'looking for a needle in a haystack'. It requires large amounts of storage and processing to perform the required data correlations. To overcome these limitations, we propose to leverage Software Defined Networking (SDN) for the active monitoring, detection and response to malware. We believe that an SDN-based malware detection system offers centralized network-wide visibility. This allows incremental network events correlation, active evidence collection, and supports fast detection and reaction to malware attacks.

Publications

AlAhmadi, B.A. and Martinovic, I., 2018, May. MalClassifier: Malware family classification using network flow sequence behaviour. In APWG Symposium on Electronic Crime Research (eCrime), 2018 (pp. 1-13). IEEE.

Alahmadi, B.A., Legg, P.A. and Nurse, J.R., 2015, April. Using Internet Activity Profiling for Insider-threat Detection. In ICEIS (2) (pp. 709-720).

Axon, L., Alahmadi, B., Nurse, J.R., Goldsmith, M. and Creese, S., 2018. Sonification in security operations centres: what do security practitioners think?. Internet Society.



Ranjbar Balisane

Supervisor: Andrew Martin, Department of Computer Science

Ranjbar has a First Class B.Sc. (Hons) in Ethical Hacking & Network Security and M.Sc. with Distinction in Forensic Computing. Prior to joining the CDT in Cyber Security at Oxford, he worked as an eCampus project manager for Soran University, Kurdistan, initiating the first large scale eCampus in Iraq, working in collaboration with LS Cables (LG). He has experience in vulnerability discovery, penetration testing, programming, networking, and protocol design.

DPhil Thesis: Engineering Secure, Usable, and Privacy Preserving Identity Management System using Trusted Computing.

Researching systematic approach to enhancing authentication privacy and security using trusted computing with Professor Andrew Martin.

While a lot of research is focused on enhancing a particular method of authentication such as enhancing hashing algorithms, or ways which fingerprint templates are stored, or finding new and more secure ways to authenticate a user. This research focuses on the underlying architecture and instead of asking the user to comply with complex policies and change with technology, it changes the underlying architecture using the advances made in technology to provider better privacy protection, security and more usable security.

Publications

R. A. Balisane and A. Martin (2016). Trusted Execution Environment-Based Authentication Gauge

(TEEBAG). In Proceeding of the New Security Paradigms Workshop (NSPW), Colorado, USA, 2016. ACM.

Atamli-Reineh, R. Borgaonkar, R. A. Balisane, G. Petracca, and A. Martin (2016). Analysis of Trusted

Execution Environment usage in Samsung KNOX. In Proceedings of the Workshop on System

Software for Trusted Execution (SysTex), Trento, Italy, 2016.

Mini-Project: OpenSky – Towards Secure Next Generation Air Traffic Communication Protocols

Mini-Project: Trusted Computing versus Identity

Alex Darer

Supervisors: Joss Wright, Oxford Internet Institute and Andrew Martin, Department of Computer Science

Alex is a computer scientist with a MSc from the University of Birmingham where he studied under Dr Tom Chothia and Dr Flavio Garcia. While there he worked on motion based key-logging on smartphones and a practical relay attack for contactless credit cards along with a review of the Visa Paywave protocol. Upon joining the CDT for Cyber Security, he has worked closely with Dr Joss Wright and co-DPhil candidate Oliver Farnan to research various areas of Internet Censorship. In general, his interests lie around censorship, networking security and practical attacks on systems and their associated functions.

DPhil Thesis: New Approaches For Monitoring Internet Censorship

Monitoring Internet Censorship remains a complex research task. Censors around the world employ sophisticated measures to enforce policies of censorship, and there are often repercussions for those who access sensitive material within an area under a censorship regime. For these reasons, we as researchers must be careful about how we test and measure censorship within certain countries. One cannot ethically monitor for filtered content if it puts another individual or group at risk of harm.

A major area within censorship research is building and maintaining URL filter lists for different countries. Alex's work is building this capability by developing automated methods for discovering and monitoring blocked URLs that don't rely on human interaction or local knowledge of censored regions. An important part of this research is performing measurements on infrastructure rather than using volunteers to determine if certain content is filtered.

Publications

Alexander Darer, Farnan, Oliver and Joss Wright. "FilteredWeb: A Framework for the Automated Search-Based Discovery of Blocked URLs." Proceedings of the 2017 Network Traffic Measurement and Analysis Conference (TMA). TMA, 2017.

Farnan, Oliver, Alexander Darer, and Joss Wright. "Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses." Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society. ACM, 2016.

Joss Wright, Alexander Darer and Oliver Farnan. "Filterprints: Identifying Localised Usage Anomalies in Censorship Circumvention Tools."

Graham Fairclough

Supervisors: Victoria Nash, Oxford Internet Institute and Robert Johnson, Faculty of History

Prior to coming up to Oxford Graham served in the British Army, reaching the rank of Colonel. Operational tours included Northern Ireland, Belize, The Balkans, Iraq and Cyprus serving in intelligence and counter-intelligence roles. Senior appointments include a tour in the United Kingdom's Permanent Joint Headquarters (PJHQ), responsible for the delivery of operational intelligence architecture and capability globally, including Iraq and Afghanisatan, during the period 2007-2010, and between 2010-2013, he was the first Chief of Staff to the UK's Chief of Defence intelligence, within the Ministry of Defence. He has served on several occassions with the Government Communications Headquarters (GCHQ) and worked closely with other elements of the United Kingdom's intelligence community and its international partners.

Graham is a graduate of the United Kingdom's Staff College where he gained a MA in Defence Studies from Kings College, London and also holds a MSc in Knowledgement Management Systems from Cranfield University. He participates in NATO's Urbanisation Programme, the 5 Eyes' Contested Urban Environment (CUE) experiement and contributes to the development of United Kingdom military doctrine through a number of work streams where he advises on information manoeuvre and the challenge of operating in a future information led environment. Graham is an associate reseacher with the Changing Character of War Programme at the University of Oxford, working on the impact of the cyber environment on warfare, how cyber security challenges are understood by senior decision makers, and the role of strategic partnerships in delivering national cyber security strategy.

DPhil Thesis: The Emergence of Offensive Cyber in National Cyber Security Strategy: From the Secret State to the Public Space – A United Kingdom Perspective.

Achieving a safe and secure cyber environment is an issue of national security for states. The consequences of not attaining this objective are significant: the denial of critical infrastructure, financial cost, loss of intellectual property, the compromise of personal security and reputational damage. For the United Kingdom, cyber security is considered to be a Tier 1 security concern. United Kingdom government statements concerning the challenges faced in delivering a secure cyber environment indicate a recognition that its current approach to delivering cyber security is no longer valid: 'Getting cyber security right requires new thinking'. A changing threat landscape has led to the acknowledgment of the role and necessity of offensive cyber capability in achieving cyber security, 'We will defend ourselves, but we will also take the fight to you'. This emphasis on the offensive, represents a major shift in the strategic underpinnings on which the United Kingdom's national cyber security strategy has historically been founded. Placing, alongside the existing pillars of a strong defence and a high level of resilience, a third pillar of a strong offence. The requirement exists to understand the nature of this strategic change in policy and its impact on how the United Kingdom implements its national cyber security strategy to meet the challenge of the competitive cyber environment.

Publications

The Mouse, the Tank and Hybrid War: Understanding the Battlespace. G Fairclough. Presented at ICMSS 2016 Conference, Istanbul, Turkey.

A Model to Facilitate Discussions about Cyber Attacks. J Happa, G Fairclough, M Goldsmith and S Creese. Presented at CYCON 2015 and to be published in forthcoming Ethics and Politics for Cyber Warfare.

"Rolling ODD DICE: Operations in Future Urban Warfare". G J Fairclough. Presented at ISSS – ISAC 2015 Conference, Springfield, MA, USA. Published in NATO Urbanisation Experiment 2030. ACT, NATO.

The Truth is Out There – Intelligence in the Cyber Age

The United Kingdom and Japanese Approaches to Cyber Security: Themes for Global Cyber Security Capacity Building in the Future

Elizabeth Phillips

Supervisors: Sadie Creese and Michael Goldsmith, Department of Computer Science

Elizabeth is originally from Carmarthenshire in South Wales where she studied her GCSE's in the medium of welsh at Ysgol Dyffryn Aman in Ammanford. Elizabeth then gained a scholarship to study Mathematics, Further Mathematics, Chemistry, Psychology and Biology at A Level in St Michael's School, Llanelli. Elizabeth completed her undergraduate degree and Masters in Mathematics and Computer Science at Worcester College, Oxford University in June 2013.

DPhil Thesis: Extracting Social Structure and hierarchy from Dark Web Forums using Metadata

Following on from the research undertaken as part of my first mini project entitled "Applying Social Network Analysis to Security", the DPhil will investigate to what extent we can apply social network analysis techniques to various types of communication data in order to identify influential players within a network. This in turn will allow us to identify any potential insiders within an organisation by highlighting those individuals that have greater influence than their role entails and the results can be combined with other indicators obtain from other means, including both technical and psychological metrics. The end result will be an expansion of the tool support created as part of the mini project which will allow users to navigate their way through a communication network and highlight individuals of interest.

Publications

Mini-Project 1: Applying Social Network Analysis to Security

Mini-Project 2: Creating a Cyber Skills Framework for South Africa

Eduardo dos Santos

Supervisors: Andrew Simpson, Department of Computer Science and Dominik Schoop (Esslingen University, Germany)

Eduardo is a fifth year D.Phil (Ph.D) student in the Cyber Security Centre for Doctoral Training at Oxford University. He comes from a Computer Science background. Eduardo is interested in cyber-security aspects of cars due to the impact that autonomous vehicles will have on transport in the near future. His background in cyber-security alongside hearing and visual impairment motivates Eduardo to work towards making driverless cars a reality, as transport should be accessible to everyone.

DPhil Thesis: A Framework for the Automated Security Testing of Autonomous Cars

His research focuses on cyber-security testing of modern cars —- particularly, on how the testing process can be automated. Cyber-threats may arise from inside and outside of the car. In the former, rogue embedded control units (ECUs), may be installed by evil mechanics and interfere with the car's behaviour at random or at an attacker's request. In the latter, outsider threats take the form of interference being sent to an autonomous car's sensors (e.g. camera blinding, and radar spoofing). Both kinds of threats have the potential to fool the car into making the wrong decision. Whenever possible, contributions of this research are supported by industry engineering tools. The ever-growing complexity of automotive systems — in regards to number and type of interacting sensors and systems —- make it unfeasible for a thoroughly framework to be developed in the scope of a single D.Phil thesis. Therefore, case studies are done with a well-selected and representative set of systems.

Publications

dos Santos, E., & Schoop, D. (2018). Towards a Simulation-based Framework for the Security Testing of Autonomous Vehicles (p. 15). Presented at the 6th Embedded Security in Cars USA, Ypsilanti, MI, USA.

dos Santos, E., Simpson, A., & Schoop, D. (2017). A Formal Model to Facilitate Security Testing in Modern Automotive Systems. Electronic Proceedings in Theoretical Computer Science, 271, 95–104. https://doi.org/10.4204/EPTCS.271.7

dos Santos, E. (2017). Poster: A Security Testing Framework for Modern Cars. Presented at the Engineering Secure Software and Systems (ESSoS), Bonn, Germany.

dos Santos, E., Schoop, D., & Simpson, A. (2016). Formal models for automotive systems and vehicular networks: Benefits and challenges. In 2016 IEEE Vehicular Networking Conference (VNC) (pp. 1–8). Columbus, OH, USA. https://doi.org/10.1109/VNC.2016.7835940

Gregory Walton

Supervisor: Joss Wright, Oxford Internet Institute

Greg is researching advanced threats targeting civil society networks, and has worked extensively with Tibetan NGOs in the field in South Asia. He coordinated the primary field-based research for the GhostNet and the ShadowNet investigations in the Dalai Lama's Office and the Tibetan Government-in-Exile in Dharamsala, India, where he worked with a team that uncovered global cyber espionage botnets operating out of China, and penetrating the United Nations, NATO, governments, diplomatic missions, and civil society computers. He is a Fellow of the SecDev Foundation in Ottawa, was formerly a Fellow at the Citizen Lab based at the Munk Centre, University of Toronto, and is a graduate of the Department of Peace Studies, University of Bradford (International Relations and Security Studies).

DPhil Thesis: The Cyber Security of Civil Society Organisations

This project will investigate how high risk/low capacity Civil Society Organisation (CSOs) respond to digital threats from their external environment. The primary attack vector being considered is 'spear phishing': targeted malicious code delivered as email attachments or hyperlinks, through the 'social engineering' of organisational social graphs, or 'social malware'. The analytic focus is on theory construction to mitigate this threat through Socio-Technical organisational learning practices. These practices will support decision-making to manage operational risk within collaborative knowledge management systems within the conceptual framework of the Data-Information-Knowledge-Wisdom (DIKW) hierarchy.. This theory building will be applied to the development of digital threat intelligence sharing practices, both tacit and explicit, and training models delivered via digital dashboards, emerging in the implementation of a sustainable 'Cyber Security Audit and Remediation project' (CyberSAR).

The SecDev Foundation has been awarded a grant by the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL) Internet Freedom (IF) portfolio fund. The grant is to develop and implement a methodology to measurably improve the digital security of 25 Civil Society Organisations in the former Soviet Union through a combination of software, hardware, and training: the 'Cyber Security Audit and Remediation' ('CyberSAR') methodology. The award follows two pilot projects to operationalise the CyberSAR methodology in the Syrian and Tibetan exile diasporas. These three research populations – CSOs in the Syrian conflict space, PRC diasporic networks, and post-Soviet Eurasia – will facilitate in-depth, qualitative comparison of the CyberSAR methodology across varied geo-political and cultural contexts.

The research question posed is: how successful are organisational responses to evolving socio-technical threats, specifically targeted malware attacks?

Publications

Strategic thought in Asian cyberspace: The People's Liberation Army in the 'fifth domain'

Using big data and in-field ethnography to combat advanced threats Tracking the attack lifecycle of an APT campaign targeting Tibetan civil society.

100%
50%
30%
50%
Time
TEAM work
100%
Diagram
40%
Loading
16
20
76
81
% 100
100
200
300
400
yes
Yes
No
STOP
CLOUD

Richard Baker

Supervisor: Ivan Martinovic, Department of Computer Science

Richard is a lifelong computer scientist, having first broken the family computer aged four – long before his MEng at Imperial College London. Since then he has held various technical jobs within finance, insurance and public health; both in the UK and abroad. His broad technical interests include the use of side-channels both for attackers and defenders, the latter where there are sorely underused, the incorporation of physical properties into security and monitoring systems, the economisation of cybercrime, qualifying the impact of security risks and where security common-sense comes from, if anywhere. He is a member of the Systems Security Lab, with a software-defined radio speciality. He is also a proud member of Oxford's Ox002147 CTF team and a founding member of the Competitive Computer Security Society.

DPhil Thesis: Exploiting the Physical in Cyber-Physical Systems

Cyber-Physical systems are a particular worry in the security world because compromises can immediately have real, physical effects. They also present new opportunities for attackers, who can not only exploit the logical behaviour of the system, but also affect the physical phenomena it relies upon. Yet there are opportunities for new security designs that exploit the physical behaviour too; creating challenges that an attacker acting purely at the logical level cannot overcome. The exploitation of physical phenomena is explored in the context of aviation security, drone detection, rogue network monitoring and electric-vehicle security.

Publications

Conferences

Baker, R. and Martinovic, I., 2019. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. To appear USENIX Security 2019.

Baker, R. and Martinovic, I., 2018. EMPower : Detecting Malicious Power Line Networks from EM Emissions. IFIP-Sec 2018.

Birnbach, S., Baker, R. and Martinovic, I., 2017. Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones. NDSS 2017.

Workshops

Baker, R. and Martinovic, I., 2016, October. Secure Location Verification with a Mobile Receiver. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (pp. 35-46). ACM.

Outreach

Baker, R. 2018, April. UAV-ing a laugh?!. Oxford CompSoc Talk.

Baker, R. 2016, May. The Drones Club: Consumer UAVs, their (ab)uses and some countermeasures. 'Research Uncovered' Talk.

Richard Everett

Supervisors: Stephen Roberts and Michael Osborne, Department of Engineering Science

Richard is a DPhil student at Oxford University and is part of the machine learning research group lead by Stephen Roberts. After graduating from UCL with a Masters degree in Computer Science, he moved to Oxford to start applying machine learning to complex multi-agent problems. His work focuses on using game theory and agent-based modelling to study how agents do, and should, interact in the real-world. In the past, he has applied his research to advertising, finance, and cybersecurity, and has also worked with the airline Emirates.

DPhil Thesis: Behaviour Modelling and Exploitation with Machine Learning

A large number of problems in the real-world contain multiple agents who are trying to achieve their goal, and do so through the interaction with not only their environment but also with the other agents in it. Examples include negotiating trades, playing board games, and allocating resources to protect locations.

Be it negotiating a trade, playing a board game, or allocating resources to protect important locations, having an accurate model of how the other participants will behave is crucial to performing well. For this reason, this project combines deep reinforcement learning and game theory to create agents which can reason about the behaviour of others, and exploit that knowledge to maximise their performance.

Publications

A. Cobb, R. Everett, A. Markham, S. Roberts. "Identifying Sources and Sinks in the Presence of Multiple Agents with Gaussian Process Vector Calculus" Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2018.

R. Everett, S. Roberts. "Learning Against Non-Stationary Agents with Opponent Modeling and Deep Reinforcement Learning" AAAI Spring Symposium Series on Learning, Inference, and Control of Multi-Agent Systems, 2018.

R. Everett. "Opponent Modelling of Non-Stationary Agents with Deep Reinforcement Learning" NIPS Workshop on Learning in the Presence of Strategic Behavior, 2017.

D. Hendricks, A. Cobb, R. Everett, S. Roberts. "Inferring Agent Objectives at Different Scales of a Complex Adaptive System" NIPS Workshop on Learning in the Presence of Strategic Behavior, 2017.

R. Everett, J. Nurse, and A. Erola. "The anatomy of online deception: what makes automated text convincing?." Proceedings of the 31st Annual ACM Symposium on Applied Computing. ACM, 2016.

A Distributed Cyber Analytics System for Streaming Anomaly Detection

Ilias Giechaskiel

Supervisor: Kasper Rasmussen, Department of Computer Science

Ilias studied Mathematics at Princeton University and Advanced Computer Science at the University of Cambridge, before joining the CDT in Cyber Security at the University of Oxford. His research focuses on embedded systems security, primarily as it relates to Analog-to-Digital Converters (ADCs) and Field-Programmable Gate Arrays (FPGAs). Ilias's interests took him to Yale University for the first half of 2019, where he investigated covert channel attacks on cloud FPGAs as a Visiting Assistant in Research. During his undergraduate and graduate studies, Ilias completed six internships, namely in the Data License team at Bloomberg, the Windows Security team at Microsoft, the Product Abuse team at Dropbox, the Embedded Systems team at Microsoft Research, and the Hardware/FPGA team at Jump Trading (twice). Ilias also co-founded the Competitive Computer Society and was the captain and co-founder of Oxford's security Capture-the-Flag (CTF) team 0x002147, frequently participating in CTF contests individually and with 0x002147.

DPhil Thesis: Leaky Hardware: Modeling and Exploiting Imperfections in Embedded Devices

Traditionally, computer security has focused on the mathematical properties of protocols, and the correctness of their software implementations. However, the underlying hardware on which code runs is imperfect. In my thesis, I investigate the effects of these imperfections on the security of embedded systems. In researching attacks on the integrity of data processed by embedded systems, I focus on out-of-band signal injection attacks targeting interfaces that transform physical quantities to analog properties. These attacks can cause a mismatch between the physical property being measured and its digitized version, despite the adversary's lack of physical access to the device under attack. After a comprehensive survey and taxonomy of out-of-band electromagnetic, conducted, acoustic, and optical attacks, I investigate the security of several Analog-to-Digital Converters (ADCs), and propose a framework for evaluating the vulnerability of systems to out-of-band signal injection attacks. This framework formalizes the effects of out-of-band attacks (from mere disruptions of sensor outputs to precise control over them) through mathematical definitions, and uses a high-level system model to abstract away from engineering concerns.

My thesis also investigates confidentiality attacks on embedded systems, with a focus on covert- and side-channel attacks on Field-Programmable Gate Arrays (FPGAs). I show that certain routing resources within FPGAs, called long wires, leak information about their state. This information leakage can be measured entirely on-chip to create a high-bandwidth covert channel, and a side channel that can recover cryptographic keys. I demonstrate that the leakage persists across seven families of FPGA devices, and characterize the leakage across various parameters such as the on-device location of the long wires, the presence of multiple competing circuits, etc. The long-wire leakage can be detected even in cloud FPGAs due to novel ring oscillator structures, bypassing currently-deployed countermeasures.

In researching defense mechanisms against remote attacks on FPGAs, I focus on physical isolation between different users to separate FPGA dies (Super Logic Regions, or SLRs). However, I demonstrate that current FPGA architectures are not well-suited for multi-tenant setups, since power-based cross-SLR covert channels can break confidentiality assumptions. Even assigning different users to separate FPGA boards is not enough: leakage through shared Power Supply Units (PSUs) makes cross-FPGA communication possible. Specifically, I introduce the first FPGA-to-FPGA, CPU-to-FPGA, and GPU-to-FPGA covert channels between physically distinct circuit boards, making use of a novel receiver design and classification metric. Overall, my thesis highlights the dangers of remote attacks on embedded devices, and therefore a fundamental need for new approaches to embedded device security.

Publications

I. Giechaskiel, Y. Zhang, and K. B. Rasmussen. "A Framework for Evaluating Security in the Presence of Signal Injection Attacks". In 24th European Symposium on Research in Computer Security (ESORICS), 2019: 10.1007/978-3-030-29959-0_25.

I. Giechaskiel, K. B. Rasmussen, and J. Szefer. "Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs". In 29th International Conference on Field-Programmable Logic & Applications (FPL), 2019.

I. Giechaskiel, K. Eguro, and K. B. Rasmussen. "Leakier Wires: Exploiting FPGA Long Wires for Covert- and Side-Channel Attacks". ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 12, no. 3, pp. 11:1–11:29, August 2019 : 10.1145/3322483..

I. Giechaskiel, K. B. Rasmussen, and K. Eguro. "Leaky Wires: Information Leakage and Covert Communication Between FPGA Long Wires". In 13th ACM Asia Conference on Computer and Communications Security (ASIACCS), 2018. DOI: 10.1145/3196494.3196518.

I. Giechaskiel, C. Cremers, and K. B. Rasmussen. "When the "Crypto" in Cryptocurrencies Breaks: Bitcoin Security Under Broken Primitives". IEEE Security & Privacy, vol. 16, no. 4, pp. 46–56, July/August 2018. DOI: 10.1109/MSP.2018.3111253.

I. Giechaskiel, C. Cremers, and K. B. Rasmussen. "On Bitcoin Security in the Presence of Broken Cryptographic Primitives". In 21st European Symposium on Research in Computer Security (ESORICS), 2016. DOI: 10.1007/978-3-319-45741-3_11.

Mariam Nouh

Supervisors: Sadie Creese, Michael Goldsmith and Jason Nurse, Department of Computer Science

Mariam is doing a DPhil in Cyber Security as part of the Computer Science department. Her research focus is on cybercrimes, intelligence gathering, and online radicalization. She completed her MSc. in Information Systems Security at Concordia University, Canada, where she researched methods for automatic integration of security concepts into software design models. She completed her BSc. degree in Information Technology at King Saud University, Saudi Arabia. In her graduation project she developed a speech recognition program named AraDict, which is an Arabic dictation system.

Before joining Oxford, she worked as a security analyst in the banking sector conducting security compliance reviews and penetration testing. She then developed interest in research and joined King Abdulaziz City for Science and Technology, the national research labs of Saudi Arabia, as a research associate working on multiple research projects in collaboration with MIT University.

Mariam's research interest spans multiple areas including cyber-crimes, social network analysis, natural language processing, and machine learning. During her time at Oxford, she has been an active member of the Oxford Women in Computer Science Society (OxWoCS) aiming to promote and support women in Tech. In her down time, Mariam enjoys participating in CTF competitions, playing squash, and doing street photography.

DPhil Thesis: Cybercrime Intelligence Framework for Detection and Analysis of Cyber-criminals.

With the wide spread of the Internet and the increasing popularity of social networks that provide prompt and ease of communication, several criminal and radical groups have adopted it as a medium of operation. Similarly, crimes committed nowadays generate huge amounts of complex data which makes it a burden on law enforcement to analyse manually. Thus, there is a strong need for automated tools that are able to collect, process, and analyse these large amounts of complex data in a timely manner.

The objective of this doctoral project is to focus on this problem and build a framework, and supporting toolset, that are able to automatically identify online criminal activities. This is achieved using techniques such as natural language processing, social network analysis, and machine learning. The framework is mainly informed by a set of requirements gathered from interviews with law-enforcement and security analysts, in order to assist them in handling big data content, gathering intelligence, and expand on existing analytical technologies.

Publications:

M. Nouh and J. R. C. Nurse, "Identifying Key-Players in Online Activist Groups on the Facebook Social Network," 2015 IEEE International Conference on Data Mining Workshop (ICDMW), Atlantic City, NJ, 2015, pp. 969-978. doi: 10.1109/ICDMW.2015.88

M. Nouh, J. R. C. Nurse and M. Goldsmith, "Towards Designing a Multipurpose Cybercrime Intelligence Framework," 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2016, pp. 60-67. doi: 10.1109/EISIC.2016.018

M. Nouh, J. R. C. Nurse and M. Goldsmith. "POSTER: Detection of Online Radical Content Using Multimodal Approach", 2017 IEEE European Symposium on Security and Privacy (EuroSP2017), Paris, 2017.

M. Nouh, J. R. C. Nurse and M. Goldsmith, "CCINT: The Cyber-Crime INTelligence Framework for Detecting Online Radical Content, Grace Hopper Celebration Conference (GHC), Orlando, USA. October 2017. (3rd prize award, ACM Student Research Competition)

M. Nouh, J. R. C. Nurse and M. Goldsmith, Applying Machine Learning to Detect Evidence of Online Radical Behavior. Artificial Intelligence at Oxford conference (AI @Oxford), 2018. (Poster)

M. Nouh, J. R. C. Nurse, Helena Webb, and M. Goldsmith, Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. Workshop on Usable Security and Privacy (USEC) Internet Society, San Diego, California, Feb 24, 2019. ISBN 1-891562-57-6

M. Nouh, J. R. C. Nurse, and M. Goldsmith, Understanding the Radical Mind: Identifying Signals to Detect Extremist Content on Twitter. IEEE International Conference on Intelligence and Security Informatics (ISI), 2019

Reports and Presentations:

On Understanding Online Radicalism: A Case Study on ISIS Propaganda Using Computational Methods. At the International Terrorism and Social Media Conference (TASM Conf), Swansea, 2019

Towards Expanding the Frontiers of Traditional Policing of Cybercrimes. At Chatham House, The Royal Institute of International Affairs. Workshop on Understanding Cybercrime for Better Policing: Regional and Global Challenges. London, 2019

Understanding the Radical Mind Using Linguistic and Psychological properties. 2018 Behavioral and Social Sciences in Security (BASS).

Identifying Signals to Detect Radicalism on Twitter. Vox-Pol Conference on Violent Extremism, Terrorism, and the Internet: Present and Future Trends, 2018.

Identifying influential users in activist groups on Facebook. Social Networking in cyberspace (SNIC) conference, 2015.

Structural and Behavioural Analysis of the University's Spear-Phishing Emails", CDT Mini-Project report, 2015.

Kristopher Wilson

Supervisor: Rebecca Williams, Faculty of Law

Kris graduated with a Bachelor of Laws (Honours) at Flinders University in Adelaide, South Australia. He then undertook a Master of Laws at the University of New South Wales in Sydney, specialising in Media and Technology Law. He has worked at Flinders University teaching Public Law, Advanced Legal Research, Criminal Law, Intellectual Property Law, and Law in a Digital Age. He has also worked at the University of Reading, teaching LLM modules on Internet Law, Data Protection and Privacy Law, and Intellectual Property Law. Additionally, Kris has provided services in relation to legal policy development at the South Australian Attorney General's Department, the South Australian Law Reform Institute, and delivered a number of Professional Development seminars.

DPhil Thesis: 'What's Wrong with the CMA? Computer Misuse and the Criminal Law'

The introduction of any new criminal law is accompanied by a series of justifications. The CMA was justified by the Law Commission based on five considerations: fair labelling and deterrence; that it would serve a supplementary role to existing offences by criminalising conduct on their periphery; that the ultimate harm of malicious uses of computers was the access to, and impairment of, computer operations and this fell outside the experience of the criminal law; that 'hacking' served a criminogenic function; and that other jurisdictions had enacted similar provisions.

Since the introduction of the CMA, the operation of computing and network technologies has continued to evolve. As such, this thesis aims systematically to revisit the justifications set out to support the creation of the computer specific offences contained in the Act. It will argue that these justifications no longer support the CMA, if indeed they ever did so. The evolution of computing technology, well beyond that contemplated by lawmakers at the time, means the problems computers presented to the criminal law are better served by reconsidering the structure and operation of general offences, rather than creating new specific offences. The notion of 'computer crime' as being a subject for the substantive criminal law has, in most cases, turned out to be illusory.

Publications

Kristopher Wilson, 'As Brexit dominates news, Investigatory Powers Bill sneaks in under the radar', The Conversation, 1 July 2016 <https://theconversation.com/as-brexit-dominates-news-investigatory-powers-bill-sneaks-in-under-the-radar-61780>.

Kristopher Wilson, 'The Computer Misuse Act 1990 (UK) and Responding to the Evolving Cybercrime Threat Landscape', CDT Working Paper 2015.

Kristopher Wilson, 'Virtual Private Networks and 'Geo-Blocked' Works: Service Users as Unwitting Cyber Criminals', CDT Working Paper 2015.

Kristopher Wilson, 'Computer-Related Crime' in David Caruso et al South Australian Criminal Law and Procedure (3rd edition, Lexis Nexis) (forthcoming 2019)

Kristopher Wilson, 'Future Proof Your Legal Career: The Future of Legal Practice' at South Australian Legal Services Commission Conference 29 June 2018

Tina Wu

Supervisor: Andrew Martin, Department of Computer Science

Tina completed her MSc in Forensic Computing and Security at the University of Derby. She then joined Airbus Group as a Research Engineer focusing on research in cyber security and forensics in industrial control systems. Her research interests are in Forensics and monitoring of industrial control systems with a focus on live memory forensics, novel attack detection methods, malware analysis, side channel attacks and the Internet of Things (IoT). Now she is a DPhil student at Oxford's CDT in Cyber Security, her research focuses on developing and improving the digital forensic process in the IoT.

DPhil Thesis: IoT Security and Digital Forensics

In Tina's DPhil project she is working to improve the digital forensic procedures required to carry out investigations in the IoT environment. The first part of the digital forensic investigation process involves identifying the number and the type of devices on the network, with the number of IoT devices being connected to networks, increasing, an investigator may miss hidden devices. Exploring practical methods to automatically fingerprint IoT devices on the network will speed up the identification process in an investigation.

Beside the technical challenges in IoT forensics, Tina has explored non-technical challenges such as; definitions, experience and capability in the analysis of IoT data/devices and current/future challenges. Tina has also been exploring using Bluetooth Low Energy (BLE) to extract evidential data from IoT consumer medical devices.

Publications

Wu, Tina and Jason R. C. Nurse. "Exploring The Use Of PLC Debugging Tools For Digital Forensic Investigations On SCADA Systems." JDFSL 10 (2015): 79-96.

Wu, T. and Martin, A., 2018,""Bluetooth Low Energy used for Memory Acquisition from Smart Health Care Devices". Accepted at The 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 1256-1261.

Tina Wu, Frank Breitinger, and Ibrahim Baggili. 2019. "IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions". In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom

Olusola Akinrolabu

Supervisor: Andrew Martin, Department of Computer Science and Steve New, Said Business School

Olusola graduated with a BSc. (Honours) in Computer Science from Babcock University, Nigeria and also holds a Master's degree in Mobile and High-Speed Telecommunications Networks from Oxford Brookes University.

His industry experience spans over 15 years, where he has worked in both network and security-related roles. He has been involved in the planning, implementation and support of global networks at this time.
His last role was as a Security Technical Lead of a team of six for a Global publishing firm. He currently holds various industry certifications including CISSP-ISSAP, CISA, CCSP, GSEC, GSNA, and CNSE.

As part of the first year of the CDT, Olu completed two mini-projects, the first titled supply chain risks in cloud computing and the other is on detecting sophisticated attacks in security operation centres (SOC). He has since continued his research looking into the risks in the Cloud's supply chain and how cloud stakeholders can assess these dynamic risks.

DPhil Thesis: Cyber Supply Chain Risks in Cloud Computing - The Effect of Transparency on the Risk Assessment of SaaS.

In this research, we address the supply chain transparency gap in cloud risk assessment. We proposed the application of a Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model that is supported by supplier security assessment and supply chain mapping in the identification, analysis, and evaluation of cloud risks. Designed for cloud providers, the CSCCRA model follows a systematic approach to cloud risk assessment, and decomposes a cloud service into its component services (managed by different suppliers), while using a multi-criteria decision support tool to assess each of these suppliers. We followed a 3-staged validation process, which included conducting case studies with SaaS providers to confirm the applicability of the model to assessing cloud risks and risks of other composite systems.

Publications

Can improved transparency reduce supply chain risks in cloud computing? Akinrolabu, O. and New, S. Operations and Supply Chain Management Journal, 10(3), pp.130-140, 2017.

Cyber supply chain risks in cloud computing– bridging the risk assessment gap. Akinrolabu, O., New, S. and Martin, A. Open Journal of Cloud Computing (OJCC), 5(1), pp 1-19, 2017.

The challenge of detecting sophisticated attacks: Insights from SOC Analysts. Akinrolabu, O., Agrafiotis, I. and Erola, A. 1st International Workshop on Cyber Threat Intelligence Management (CyberTIM 2018), 2018.

CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. Akinrolabu, O., New, S. and Martin, A. 15th European, Mediterranean, and Middle Eastern Conference on Information Systems (EMCIS2018), (pp. 177-184). Springer, 2018.

Cloud Service Supplier Assessment: A Delphi Study. Akinrolabu, O., New, S. and Martin, A. In Proceedings of the 8th International Conference on Innovative Computing Technology (INTECH 2018), 2018.

Assessing the security risks of multicloud SaaS Applications: A Real-world case study. Akinrolabu, O., New, S. and Martin, A. In Proceedings of the 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2019), 2019.

Eman Alashwali

Supervisor: Andrew Martin, Department of Computer Science

Eman holds MSc. in Information Security from University College London (UCL), UK, and BSc. in Computer Science from King Abdulaziz University (KAU), Saudi Arabia. Her research interests are in the theory and practice of network security protocols. In her spare time, Eman enjoys reading, drawing, and photography.

DPhil Thesis: Negotiation Transparency in Configurable Protocols

My Dphil. project focuses on a class of attacks known as "Downgrade Attacks". These attacks are mainly associated with multi-versions, multi-layer, and agile cryptographic protocols. In such attacks, an adversary leads the communicating parties to operate in a mode that is weaker than the one that those parties preferred. As a result, the adversary can exploit the weak mode's flaws to break main security guarantees the protocol provides.

I pay a particular attention to the Transport Layer Security protocol (TLS) that is used to secure internet communications. I examine some innovative methods to reduce the downgrade attacks surface. Additionally, using measurement-based approaches, I analyse real-world data to better understand the current state.

Publications

Alashwali, E., Szalachowski P., and Martin A. (2019). "Towards Forward Secure Internet Traffic". In: the 15th International Conference on Security and Privacy in Communication Networks (SecureComm), Orlando, US.

Alashwali, E., Szalachowski P., and Martin A. (2019). "Does "www." Mean Better Transport Layer Security?". In: the 14th International Conference on Availability, Reliability and Security (ARES 2019), Canterbury, UK.

Alashwali, E. and Szalachowski P. (2018). "DSTC: DNS-based strict TLS configurations". In: the 13th International Conference on Risks and Security of Internet and Systems (CRiSIS), Arcachon, France.

Alashwali, E. and Rasmussen, K. (2018). "On the Feasibility of Fine–Grained TLS Security Configurations in Web Browsers Based on the Requested Domain Name". In: the 14th International Conference on Security and Privacy in Communication Networks (SecureComm), Singapore, Singapore.

Alashwali, E. and Rasmussen, K. (2018). "What's in a Downgrade? A Taxonomy of Downgrade Attacks in the TLS Protocol and Application Protocols Using TLS". In: the 6th International Workshop on Applications and Techniques in Cyber Security 2018 (ATCS), in conjunction with SecureComm, Singapore, Singapore.

Mini-Project 1: Secure Verifiable Remote Attestation of Embedded Devices

Mini-Project 2: On Downgrade Attacks in the TLS Protocol

Mary Bispham

Supervisors: Michael Goldsmith and Ioannis Agrafiotis, Department of Computer Science

Mary holds a first degree in Latin, and also holds several Master degrees, including an MA in Copyright Law and an MSc in Bioinformatics. Prior to joining the CDT Mary worked for some years in intellectual property administration. Her DPhil project relates to speech and language processing in a cyber security context, focussing on the security of speech interfaces and of speech-controlled devices.

DPhil Thesis Security Aspects of Human-Computer Interaction by Speech

This project seeks to investigate the security of human-computer interaction via a natural spoken language interface. The use of speech interfaces to interact with smartphones, PCs and smart home devices is becoming more widespread. Such interfaces are frequently given the persona of a friendly digital assistant, with the aim of creating a sense of communication with a human-like conversation partner which acts as a 'broker' between users and the vastly complex, often intimidating cyber world. Whilst speech-based digital assistants offer great potential advantages in terms of usability, there are clearly also significant security concerns arising from an increasingly pervasive presence of speech-based agents which provide a single gateway to their users' interactions with their devices as well as with the Web and the Internet of Things. A speech interface potentially enables an attacker to gain access to a victim's system without needing to obtain physical or internet access to their device. The security of spoken language interfaces has yet to be comprehensively investigated. This project seeks to close this gap, focussing in particular on the security implications of mismatches between machine and human understanding of spoken language.

Publications

Mini-Project 1: Linguistic Features of Impersonation in Online Discourse

Mini-Project 2: Security Vulnerabilities in Speech Recognition Systems

M. K. Bispham, I. Agrafiotis, and M. Goldsmith, "A taxonomy of attacks via the speech interface", Proceedings of Third International Conference on Cyber-Technologies and Cyber-Systems, 2018.

M. K. Bispham, I. Agrafiotis, and M. Goldsmith, "Nonsense attacks on Google Assistant and missense attacks on Amazon Alexa", Proceedings of International Conference on Information Systems Security and Privacy, 2019.

M. K. Bispham, I. Agrafiotis, and M. Goldsmith, "Attack and defence modelling for attacks via the speech interface", Proceedings of International Conference on Information Systems Security and Privacy, 2019.

(forthcoming) M. K. Bispham, I. Agrafiotis, and M. Goldsmith, "The speech interface as an attack surface: An overview", International Journal On Advances in Security, v 12 n 1 & 2, 2019.

Aaron Ceross

Supervisor: Andrew Simpson, Department of Computer Science

Aaron has a background in law and prior to joining the CDT, he worked as a researcher in data protection, privacy, and surveillance at the University of Groningen in the Netherlands as well as the University of Malta. Aaron recently completed the MSc in Computer Science from the University of Bristol in order to expand his technical abilities as well as be able to engage in more multidisciplinary research.

DPhil Thesis: Metrics and models for privacy engineering.

His research proposes to investigate how privacy risks can be more effectively articulated to information system designers. The goal is to be able to establish a link between a systems-level risk analysis and regulatory outcomes. This entails the following questions: (i) what are the challenges faced by information system designers with regards to privacy, as both a broad concept and multilevel values? (ii) what information needs to be made available in order for these challenges to be overcome? (iii) is this information drive measurably effective privacy practices for systems design? This research seeks to match the causes of regulatory liability to specific system design implementation, focusing on being able to accurately link normative regulatory values to a system's operational metrics. This results in measures which may inform organisations of the risks to personal data. One of the means by which empirical data may be gathered for privacy failures within information systems is from events such as data breaches, and other events recorded by authorities. These data may be used as ground truth from which to develop objective, generalisable metrics for privacy risk. This thus provides a more quantitative measures for privacy risk analysis, which hitherto has been largely qualitative, subjective measures. This would therefore better inform the information systems engineering process.

Publications

Mini-Project 1: Understanding threats to anonymisation: Gap-analysis and research directions

Mini-Project 2: Exploring Liabilities and Remedies for Data Breach

Presented "Examining data protection enforcement actions through qualitative interviews and data exploration" at the 37th annual conference of the British and Irish Legal, Education and Technology Association (April 2017), and will be published in the International Review of Law, Computers and Technology.

- Presenting "The use of data protection enforcement actions as a data source for privacy economics" at the 3rd International Workshop on Technical and Legal Aspects of Data Privacy and Security (September 2017), to be published in the SAFECOMP 2017 Workshop Proceedings in Lecture Notes in Computer Science

Jacqueline Eggenschwiler

Supervisor: Rebecca Williams, Faculty of Law

Jacqueline Eggenschwiler is a Swiss-born DPhil Candidate in Cyber Security at Oxford's Centre for Doctoral Training in Cyber Security. She completed her undergraduate studies in International Affairs at the University of St. Gallen and holds three master's degrees in International Affairs and Governance, International Management, and Human Rights from the University of St. Gallen and the London School of Economics and Political Science. Her current research interests revolve around cyberspace governance and regulation.

DPhil Thesis: Non-State Actors and Norms of Responsible Behaviour in Cyberspace

Despite the fact that academic publications pertaining to cybersecurity generally, and norm making processes specifically have surged over the course of the past two decades, the inputs of non-state actors to global cybersecurity governance endeavours have remained under-theorised. Jacqueline's research examines the roles and contributions of non-state actors to processes concerned with developing norms of responsible behaviour for the virtual realm. Specifically, it analyses how, in which capacity, and with which effects non-state protagonists engage in global norm cultivation endeavours by surveying different exploratory case studies.

Triangulating different qualitative means and methods of data collection and analysis, her thesis suggests that non-state actors exert discernible political and discursive influence over discussions about rules of the road for global information and telecommunications infrastructures. It demonstrates that non-state actors have to be taken seriously as key contributors to global cybersecurity steering efforts, and that their activities have important implications for accountability and legitimacy structures. Their normative undertakings also have significant consequences for how authority relationships are restructured and normative agency is shared between governmental and non-governmental entities.

Publications

2018: Blog Entry: Three Measures That Could Pave the Way to Building Successful Cyber Norms: https://www.cfr.org/blog/three-measures-could-pave-way-building-successful-cyber-norms;

2019: Policy Paper: International Cybersecurity Norm Development: The Roles of States Post-2017: https://eucyberdirect.eu/content_research/1064/

John Galea

Supervisor: Daniel Kroening, Department of Computer Science

John Galea completed his B.Sc. undergraduate degree in Computer Science and Artificial Intelligence at the University of Malta (First Class Honours) in 2013. He continued his studies and was awarded a Master's degree in Computer Science (Distinction) in 2015. He is currently reading for a DPhil in Cyber Security at the Department of Computer Science, University of Oxford. John's main interests include program analysis and software verification.

DPhil Project: Enhancing Automatic Vulnerability Analysis with the use of Software Verification Techniques

Software vendors must give priority to patching exploitable bugs from those that are less serious. However, to show that a bug is exploitable, it is often required to manually construct an exploit as a proof-of-concept. Automatic Exploit Generation (AEG) is one solution to assess the severity of vulnerabilities. Overall, John Galea's work aims to investigate the techniques pertaining to AEG, as well as extend the state-of-the-art in this research area..

Publications

Mini-Project 1: The Verser protocol: Verifying Services of IoT Devices Based on Their Capabilities

Mini-Project 2: ROPEX: Towards the Circumvention of Data Execution Prevention via Automatic Exploit Generation

Dennis Jackson

Supervisors: Andrew Simpson, Department of Computer Science and Cas Cremers, CISPA Helmholtz Center for Information Securit

After growing up in the Lake District (England), Dennis studied Mathematics at the University of Warwick, with a particular focus on Graph Theory and Dynamical Systems, culminating in a Master of Mathematics. He also took a number of modules in high performance computing and parallel algorithms from the Department of Computer Science. Dennis's primary research interest is the formal verification of security protocols.

Publications

Seems Legit: Automated Analysis of Subtle Attacks on Protocols that use Signatures. Dennis Jackson, Katriel Cohn-Gordon, Cas Cremers, Ralf Sasse. At ACM Conference on Computer and Communications Security 2019 (CCS 2019)

Prime, Order Please! Revisiting Small Subgroup and Invalid Curve Attacks on Protocols using Diffie-Hellman. Cas Cremers, Dennis Jackson. Distinguished Paper at IEEE Computer Security Foundations Symposium 2019 (CSF 2019)

Internships

Privacy, Networking & Security Research Internship with Mozilla. Mountain View, Summer 2019.

Nicholas Moore

Supervisor: Cas Cremers,
Department of Computer Science

Nicholas is a computer scientist, with degrees from the Universities of Durham and Bristol, which focussed on artificial intelligence and machine learning, with a strong emphasis on logic. He spent six years working for the UK Government as a software developer and big data expert, primarily on cyber security topics, before leaving in 2015 to join the CDT.

MRes Project

Computer network protocols are increasingly being asked to provide much higher levels of security than they had ever been asked previously. Whilst simple concepts like authentication and secrecy still remain very much in scope, it is now becoming more common that a protocol is expected to be resilient to attacks, sometimes even after a breach of security has happened.

In response to these demands, protocol designers have rapidly moved to using more and more participant state - that is, knowledge that each participant in a session must store in order to verify that the session remains secure, and must be kept accurate to continue the session further. However, the automated symbolic analysis and verification of such protocols is harder than traditional stateless protocols, since many tools have been built with assumptions about how state is handled. These assumptions often result in either under-approximating how state will be used - and hence any security proofs found may be incorrect, or makes it more likely that the tool is unable to terminate - and no security proof can be found.

Nicholas's DPhil is on the improving the state-of-the-art for automated verification of stateful security protocols, using his knowledge of logic and software development to help improve the tamarin-prover tool, and its underlying formal basis, as well as developing new models for stateful security protocols. His approach is two-fold, in that he will be looking at existing models of stateful protocols to understand where they struggle, but also attempting to improve the tooling available to protocol modellers so they can more easily see potential issues. His end goal is to make such protocols easier to automatically verify, and thus improve the level of security and trust end-users can have in network communications.

Publications

Mini-Project 1: Tamarin's Injective Facts Constraint-Reduction Rule

Mini-Project 2: Evaluating software packages for attacks against elliptic curve cryptography

William Osborn

Supervisors: Felix Reed-Tsochas, Said business School and Andrew Martin, Department of Computer Science

After graduating high school in Albuquerque, New Mexico, William joined the U.S. Military where he served as a paratrooper in Afghanistan with the 82nd Airborne Division, in support of the NATO-led International Security Assistance Force. Following his military service he received a Bachelors of Science from Penn State University in Security and Risk Analysis, focusing on Intelligence Analysis and Modelling. William then received a Masters Degree from Duke University focusing in Information Science and Information Studies. William is currently conducting research at the Saïd Business School, focusing on offensive cyber security measures as well as Corporate Cyber crime and Harm Analysis. He plans to work with corporate partners in developing offensive cyber security strategies and help them structure their physical security measures.
DPhil Thesis: Offensive Cyber Strategies for Medium to Large Corporations

He is interested in looking at the current and seemingly weak cyber security infrastructure of corporations. He will be looking at past cases of cyber incidents, fraud and attacks, response times as well as autopsies of the attacks. Given the data, he hopes to develop a new non-static strategy that evolves with the needs of corporations based off of their specific needs.

Publications

Harvard Business Review: https://hbr.org/2016/10/companies-should-understand-where-cybercrime-thrives

Mini-Project 1: How does geopolitical relevance and foreign investment impact a small island nation's cyber security strategy?

Mini-Project 2: The Ecosystem of Cybercrime: A Comparison of cybercrime in Brazil and Russia

Michal Piskozub

Supervisor: Ivan Martinovic, Department of Computer Science

Michal has been interested in Computer Science (and technology related topics) since his childhood friend introduced him to it at the age of 7. He continued this passion by doing BSc in Computer Science at King's College London and MSc in Computer Science at the University of Oxford. In the Cyber Security CDT in Oxford he completed two projects titled: On The Way To Adaptive Honeypots, and Dynamic Re-Planning For Cyber-Physical Situational Awareness. His DPhil project is titled Network Traffic Analysis For Malware Detection. Topics he is interested in include network security, malware analysis and data visualisation.

DPhil Thesis: Network Traffic Analysis For Malware Detection

Due to the fact that malware detection by analysing an executable is challenging and ineffective on a large scale, this project approaches the problem from a different perspective. Almost all modern malicious programs connect back to their authors to either ask for commands or send data from an infected computer. This is accomplished by using the Internet and more precisely by using computers' networking capabilities.

The aim of this project is to detect malware based on network traffic data. All network connections use packets as fundamental units that carry data. On the lowest level malware that communicates back to its origin creates and sends packets which constitute part of the behaviour of malware. The objective of this project is to perform a behavioural analysis of malicious programs by analysing network interactions.

While there are a number of papers that propose methods to detect malware based on their network behaviour, they concentrate on doing so manually and work with small datasets. The project will explore ways of automatic creation of features that are associated with known and new malware activities and will create a platform that will allow to work with datasets on the scale of big data.

Publications

Mini-Project 1: On The Way To Adaptive Honeypots

Mini-Project 2: Dynamic Re-Planning For Cyber-Physical Situational Awareness

Michal Piskozub, Riccardo Spolaor, and Ivan Martinovic. 2019. MalAlert: Detecting Malware in Large-Scale Network Traffic Using Statistical Features. SIGMETRICS Perform. Eval. Rev. 46, 3.

Michal Piskozub, Riccardo Spolaor, Mauro Conti, and Ivan Martinovic. 2019. On the Resilience of Network-based Moving Target Defense Techniques Against Host Profiling Attacks. In Proceedings of the 6th ACM Workshop on Moving Target Defense (MTD '19).

Mark Patrick Roeling

Supervisor: Geoff Nicholls, Department of Statistics

Mark Patrick Roeling (Dutch) studied psychology (BSc), behaviour genetics (MSc) and genetic epidemiology (MSc) and worked as a junior researcher in the Erasmus MC Rotterdam (Netherlands). He worked as data scientist for Capgemini, where he focused on detecting fraud in e-channels in the banking sector. So far, his work has been strongly statistical and at Oxford he aims to use his background to combine methods and models from (genetic) epidemiology to improve the detection of anomalies in the cyber domain. In his first year, he has studied the vulnerability of state estimation algorithms to false data injection in an aerospace setting, and the possibility to detect fraudulent credit application by systematically comparing residuals from regression analyses to detect dishonest clients. His second year focused on the unsupervised detection of botnets and illustrated the merit of Stochastic Blockmodels.

DPhil Thesis: Applying statistical and machine learning techniques to improve the detection of anomalies and increase veracity of data in cyberspace.

This is a DPhil project at the University of Oxford in cybersecurity with a strong focus on statistical analyses. Increasing amounts of transactions occur in the cyber domain, and this results in a need to create new methods capable of detecting anomalies in large and highly unbalanced datasets. The overarching aim of this project is to improve, develop, and apply statistical and machine learning algorithms to understand cybersecurity problems. These algorithms are typically capable of clustering and classifying observations (individuals, computers, etc.) with high accuracy.

Publications

Annual CDT Showcase: Anomaly detection collaboration [ING netherlands BV Amsterdam] Lie detection in big data: comparing residuals from regression analyses to detect deceptive scores in 219.810 credit applications.

Stochastic Blockmodels as an unsupervised approach to detect botnet infected clusters in networked data. Proceedings of the Data Science for Cyber-Security workshop.

Detection of abnormal data provided by fraudsters: a new approach to using residuals from regression models to improve fraud classification. FINE annual conference; Data Science for Fraud Detection, The Hague.

Mini-Project 1: False data injection in Kalman Filters in an aerospace setting; ADS-B data with simulated noise

Mini-Project 2: Lie detection in big data: comparing residuals from regression analyses to detect abnormal or deceptive scores in 219.810 consumer credit applications.

Internet of Things CDT annual conference with Royal Holloway

GCHQ data science seminar Alan Turing Institute

Thomas Spoor

Supervisor: Andrew Martin, Department of Computer Science

Thomas is a British student who completed a masters degree in Mathematics and Computer Science from Oxford before joining the CDT. During his time there he spent a summer working for the games developer Rebellion, and participated in a couple of security-themed projects during his studies – most notably winning an award for a group work designed to help a user detect attacks on a network.

Recently he has been working on malicious uses for Trusted Computing architecture and the security of short-range communications used by "Internet of Things" devices.

Publications

Mini-Project 1: Trusted Malware

Mini-Project 2: Investigating the Feasibility of Intercepting Personal Information from Internet of Things Devices

Adam Zibak

Supervisor: Andrew Simpson, Department of Computer Science

After obtaining his bachelor's degree in Computer Science, Adam completed the MSc in IT Law and Management from King's College London (Distinction) where he gained a grounding in the areas of Law which are most relevant to Information Technology as well as an understanding of business management techniques used within industry. Prior to joining the CDT, Adam worked as an open-source intelligence researcher and Arabic linguist for the International Centre for Security Analysis at King's College London.

Adam's primary research interest is cyber threat intelligence sharing, with an emphasis on evaluating the efficacy of current threat sharing initiatives and systems. Adam is the President of the Oxford University Strategic Studies Group (OUSSG). During his tenure, the Group paid special attention to Cyber Security topics, which included inviting high-profile field experts such as the Technical Director of NCSC, the former Director of GCHQ and NATO's Assistant Secretary General for Emerging Security Challenges.

DPhil Thesis: A Holistic Framework for Evaluating the Efficacy of Cyber Security Information Sharing Efforts

Cyber security information sharing is increasingly regarded as a crucial element in improving national and organisational cyber security posture. Growing efforts in the public and private sectors to foster cyber security information sharing have resulted in today's complex constellation of sharing centres, organisations, platforms and tools in various industries and government agencies, but have brought inconsistent observed improvement in security outcomes. A growing body of evidence from the academic and grey literature suggests that focus is shifting from creating interoperable sharing solutions to generating value. However, despite the growing interest and the proliferation of sharing efforts, the literature on the ability to fairly and accurately measure the value of these efforts remains limited.

In this research proposal we lay out the motivation for an empirical study that explores several aspects of information sharing in order to develop evaluation metrics and frameworks. A qualitative-dominated methodological approach will be utilised to develop more nuanced insights into the stakeholders' attitudes and understandings. The contribution will be in threefold: developing a taxonomy for cyber security information sharing as well as design goals; assessing the needs and determining the requirements for an information sharing evaluation framework; and assembling a suite of evaluation metrics within a holistic evaluation framework.

Publications

Adam Zibak and Andrew Simpson. 2018. Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts?. In Proceedings of the 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA 18). IEEE.

Adam Zibak and Andrew Simpson. 2019. Towards Better Understanding of Cyber Security Information Sharing. In Proceedings of the 2019 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA 19). IEEE.

Adam Zibak and Andrew Simpson. 2019. Cyber Threat Information Sharing: Perceived Benefits and Barriers. In Proceedings of The 14th International Conference on Availability, Reliability and Security (ARES 2019). ACM.

M-P1: When You Lose, Do Not Lose the Lesson: A Case Study on The Sony Pictures Entertainment 2014 Data Breach

M-P2: Conceptual Pipelines for the Access-data Centric Approach to Open Source Intelligence (in collaboration with Horus Security Consultancy)

CDT16 Bios

Angeliki Aktypi

Supervisor: Kasper Rasmussen, Department of Computer Science

Angeliki holds a Diploma in Electrical and Computer Engineering from Democritus University of Thrace in Xanthi, Greece and a M.Sc. in Communications & Computer Security from Telecom ParisTech, studied at campus Eurecom, in Sophia Antipolis, France. During her studies, she has pursued her undergraduate and postgraduate internships at BT (UK) and Thales (France) companies, respectively. Her main research interests focus on the deployment of security infrastructures in connected environments (IoT), the human aspects of security and privacy, the defence against network cyber-attacks and the cybercrime detection by using forensics tools.

DPhil Thesis: Discovery of and Access to Resources between Entities within IoT Systems

The rapid increase in the use of connected devices (e.g., wearables, smart locks) and cloud applications (e.g., collaboration platforms, big data tools) established trends for a fully programmed and distance manageable lifestyle and shifted the character of the society to be open and network-oriented. The proliferation on connectivity combined with the increase in cyber-crime and the terrorism expansion in cyber space have created an urgent need to rapidly advance our security countermeasures and re-think of traditional approaches. Recognising this need, this DPhil thesis is going to explore and propose the deployment of security infrastructures in connected environments, many times referred to as the Internet of Things. In particular, the objective is to develop secure and resilient to attacks protocols that enable effective discovery and access to resources between entities within IoT systems. Entities include devices (such as sensors, actuators, embedded systems), but also include software-only virtual entities (such as virtual service instances in a cloud or fog computing context).

Publications

Mini-Project 1: Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks

Mini-Project 2: A Secure P2P Protocol to Promote Collaboration between Internet of Things (IoT) Devices

John Gallacher

Supervisors: Joss Wright, Oxford Internet Institute

John is a DPhil student within the University of Oxford's Cyber Security Centre for Doctoral Training. His research focuses on investigating the causes of online polarisation, ranging from aggressive intergroup contact, the spread of extremist material and hostile interference from foreign states. He is based within the Oxford Internet Institute and the Department for Experimental Psychology under the supervision of Dr Joss Wright, Dr Jonathan Bright and Dr Marc Heerdink.

John's work combines analytic methods drawn from computer science (machine learning, natural language processing and network science) with insights from experimental psychology and open source information from social media in order to measure how groups interact online, and how this relates to real world events.

He holds a BA in Experimental Psychology from the University of Oxford, and worked previously as a security consultant.

DPhil Thesis: The Security Implications of Online Intergroup Contact

Publications

Gallacher, J.D., & Heerdink, M., (2019) Measuring the effect of hostile information operations: a case study of Russian Internet Research Agency interference in online conversations Defence Strategic Communications, 6, 155-198

Gallacher, J.D., Heerdink, M. & Hewstone, M., (2018) Online engagement between opposing extremist political groups predicts physical violence of offline encounters Under Review – Nature Human Behaviour

Gallacher, J.D., & Fredheim, R., (2018) Division aboard, cohesion at home: How the Russian troll factory works to divide societies overseas whilst spreading pro-regime messages to domestic audiences. Responding to Cognitive Security Challenges, Chapter 5, NATO Strategic Communications Centre of Excellence

Fredheim, R., & Gallacher, J.D., (2018) Robotrolling 3/2018. NATO Strategic Communications Centre of Excellence

Gallacher, J.D., Barash, V., Howard, P.N., & Kelly, J,. (2017) Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans. Data Memo 2017.9. Oxford, UK: Project on Computational Propaganda

Gallacher, J.D., (2019) Automated Detection of Terrorist and Extremist Content. Extreme Digital Speech: Contexts, Responses, and Solutions. VoxPol Network of Excellence for Research in Violent Online Political Extremism (In press)

Mini-Project 1: Information Warfare and Computational Propaganda

Mini-Project 2: Violent Political Extremism and Intergroup Contact Online

Munir Geden

Supervisor: Kasper Rasmussen, Department of Computer Science

Before steering into a research-based career, Munir worked for more than five years as a software engineer in financial IT industry, after receiving his BSc in Computer Engineering followed by MSc in Engineering and Technology Management from Bogazici University (Istanbul). He came to the UK for pursuing another master's degree in Software Systems Engineering at UCL with a research and security focus which brought him to Oxford to gain a better understanding of cyber-security by employing an interdisciplinary perspective.

In addition to previous interest in malware analysis via both static and dynamic techniques, he is currently working on the detection of runtime attacks exploiting memory bugs in a remote context.

DPhil Thesis: Remote Attestation of Runtime Behaviours

Most remote attestation techniques ensure only the load-time integrity of applications by applying checksum functions on static code regions. However, these static techniques cannot catch runtime attacks (e.g., code-reuse, non-control data attacks) that operate on dynamic memory regions such as stack or heap areas. To take the runtime attestation a step forward, I am working on an attestation scheme that checks the compliance of dynamic properties collected at runtime with the static features extracted from the code in advance.

Publications

"Ngram and Signature Based Malware Detection in Android Platform", Master's thesis supervised by Dr. Jens Krinke, UCL

Geden, M. and Happa, J., 2018, October. "Classification of Malware Families Based on Runtime Behaviour". In 11th International Symposium on Cyberspace Safety and Security (pp. 33-48). Springer, Cham.

Geden, M. and Rasmussen, K., 2019, August. "Hardware-assisted Remote Runtime Attestation for Critical Embedded Systems. In 2019 17th Annual Conference on Privacy, Security, and Trust (PST), IEEE.

Faisal Hameed

Supervisors: Sadie Creese, Michael Goldsmith and Ioannis Agrafiotis, Department of Computer Science

A seasoned cybersecurity professional with a track record of (15 years +) experience spanning various engineering, consulting and management CISO entities. Working in diverse environments from promising start-ups to international organizations (The World Bank Group, ExxonMobil, E&Y, HP, Unilever, UK Gov) to. B.Sc in CS, M.Sc in Information Security and Assurance from the States.

Faisal's research interests are in national and international security capacity building and maturity models.

The cohort based Oxford PhD programme at the CDT is an outstanding bouquet of cross-disciplinary disciplines that will uniquely position Faisal for thought leadership at the national and international arena.

DPhil Thesis: Formalising an outline around risk assessments for national critical infrastructures.

Most remote attestation techniques ensure only the load-time integrity of applications by applying checksum functions on static code regions. However, these static techniques cannot catch runtime attacks (e.g., code-reuse, non-control data attacks) that operate on dynamic memory regions such as stack or heap areas. To take the runtime attestation a step forward, I am working on an attestation scheme that checks the compliance of dynamic properties collected at runtime with the static features extracted from the code in advance.

Publications

Mini-Project 1: Disrupting Trust in CyberCriminal Marketplace

In publication: What Really Works: Analysing Trends and Success Factors in International Cybersecurity Capacity Building Initiatives

Manuel Hepfer

Supervisors: Thomas Powell and Thomas Lawrence, Said Business School

Manuel's academic background combines the areas of computer science and business administration. After graduating in 2015 from Reutlingen University (Germany) with a bachelor's degree in Business Informatics, he pursued his education at the London School of Economics, where he graduated in 2016 with a master's degree in Management, Information Systems, and Digital Innovation.

After gaining experience during practical placements in management consultancies (PricewaterhouseCoopers, Audi Consulting) and large corporations (Porsche Financial Services, Robert Bosch GmbH), Manuel's inquisitiveness and his desire to ascertain "whatever holds the world together in its inmost folds" (Goethe, 1808) convinced him to embark on his doctoral journey.

Given Manuel's background that combines social sciences with computer science, his particular research interests are located at the juncture where cyber security meets business. During the first year at the CDT, Manuel exploratorily examined how organisations adapt differently to cyber-security breaches and why differences in firm performance following a cyber-breach are observed. This research output will hopefully be published in a practitioner journal in the management domain.

DPhil Thesis: Explaining firm success and failure following a cyber-security breach

Currently, Manuel is working on an empirical research project with two professors (Thomas Powell, Tom Lawrence) from Said Business School that explores how management cognition shapes the preparedness of organisations for cyber-attacks, and how that preparedness contributes to an organisation's resilience. By comparing how multiple organisations have prepared and countered a severe cyber-attack in the past, the project aims to contribute to cyber-security and strategic management theory and practice.

Monica Kaminska

Supervisor: Lucas Kello, Department of Politics and International Relations

Monica studied International Relations at LSE for her bachelor's degree and, during this time, undertook internships at the Foreign and Commonwealth Office and in the business intelligence sector. She then moved to Cambridge to pursue an MPhil in Geographical Research. After graduating she worked in the financial sector, advising private equity funds and strategy consultancies. Given her background in the social sciences, she is particularly interested in the impact of cyber threats on international security. During her first year at the CDT, Monica undertook a mini-project at the Oxford Internet Institute where she co-authored two research memos on computational propaganda and social media activity during the 2017 UK General Election. She also presented the research at the Global Legislative Openness Conference in Kiev, Ukraine and the International Bar Association Conference in Sydney, Australia.

DPhil Thesis: Restrained responses: explaining the puzzle of lack of meaningful and proportionate punishment for major offensive cyber operations.

States struggle to punish cyber actions that are highly damaging to national interests yet fail to meet the threshold of armed attack. The "risk society" perspective in international relations theory raises questions about whether deterrence via punishment is the rationally effective recourse in such situations. Western policymakers have used risk management to evaluate the emerging security environment and security risks of the cyber domain – including the properties of complex adaptive systems, the ease of proliferation, and collateral damage – leading to policies that seem to privilege responses other than punishment. Risk management involves reducing likelihoods of scenarios to a level deemed tolerable or as low as can reasonably be achieved; thus it often neglects punishment considerations. This thesis analyses and explains this Western policy attitude. It argues that the prevailing risk management framework underlies the failure to apply proportionate punishment and potentially more effective deterrent responses to cyberattacks.

Publications

Gallacher, J. D., Kaminska, M., Kollanyi, B., & Howard, P. N. (2017) Junk News and Bots during the 2017 UK General Election: What Are UK Voters Sharing Over Twitter? Data Memo 2017.5. Oxford, UK: Project on Computational Propaganda

http://comprop.oii.ox.ac.uk/2017/05/31/junk-news-and-bots-during-the-2017-uk-general-election/

Kaminska, M., Gallacher, J.D., Kollanyi, B., Yasseri, T., & Howard, P. N. (2017). Social Media and

News Sources during the 2017 UK General Election. Data Memo 2017.6 Oxford, UK: Project on Computational Propaganda

http://comprop.oii.ox.ac.uk/2017/06/06/social-media-and-news-sources-during-the-2017-uk-general-election

Gallacher, J. D., & Kaminska, M., (2017) Facebook needs to be more open about its effect on democracy. The Guardian

https://www.theguardian.com/commentisfree/2017/jun/12/general-election-social-media-facebook-twitter?CMP=soc_3156

Collier, J., & Kaminska, M., (2017) Bashing Facebook is not the answer to curbing Russian influence operations. Council on Foreign Relations.https://www.cfr.org/blog/bashing-facebook-not-answer-curbing-russian-influence-operations

Mini-Project 1: Computational Propaganda and the 2017 UK General Election

Mini-Project 2: Why is retaliation against offensive Russian cyber actions generally so difficult? A comparison of past responses from Estonia, Germany and the US.

Martin Kraemer

Supervisor: Ivan Flechais
Co-supervisor: Helena Webb,
Department of Computer Science

Martin is a 3rd year DPhil student at the Department of Computer Science working on home user privacy with Ivan Flechais. He graduated with an MSc in Computer Science (distinction) from The University of Edinburgh, has previously worked as consultant with SAP and holds a BSc in Business Information Systems from Duale Hochschule Badenwurttemberg (Mannheim).

Martin's research at Edinburgh was supervised by Prof David Aspinall and focussed on the security and privacy of eHealth devices. His work with SAP focussed on mobile solutions for enterprise processes and helped him realise that cyber security was not only one of his customers' biggest concerns but also an incredibly interesting subject to study.

DPhil Thesis: Empowering Users' Privacy Practices in Smart Homes

The increase in data collection in our homes is fuelled by the emergence of internet-connected devices. These devices are designed to transfer, process, and disseminate data which becomes a pivotal part of the relationship between technology providers and households. However, reactions to events revealing manufacturers' practices and attitudes show a misalignment of expectations. Ultimately damaging the relationship, these issues are often referred to in the context of privacy.

Previous empirical privacy research has been carried out in other technological contexts or from risk management, system, and network perspectives in the home. Most of these studies were limited to temporary accounts of individuals. In the home, traditionally considered as one of the most private spaces, technology overlaps established social structure and related practices. Technology becomes communal, to some extent used by the community of the household rather than a single individual.

This thesis disentangles communal privacy practices in smart homes in three steps: an initial mixed method exploration of communal smart home technology use; a longitudinal, ethnographic study of communal privacy practices with 8; and the development of design artefacts for smart homes to share our insights but also as a tool for future design practice.

Publications

Kraemer, M.J., Seymour, W., Binns, R., Van Kleek, M., & Flechais, I. (2019). Informing the future of data protection in smart homes. Presented at the CHI'19 Workshop on New Directions for the IoT: Automate, Share, Build, and Care.

MJ Kraemer. Preserving Privacy in Smart Homes: A Socio-Cultural Approach. Proceedings of Conference Extended Abstracts on Human Factors in Computing Systems (CHI), ACM, 2018

MJ Kraemer, I Flechais. Researching Privacy in Smart Homes: A Roadmap of Future Directions and Research Methods. Living in the Internet of Things: Cybersecurity of the IoT Conference, IET, 2018.

MJ Kraemer, J Happa, S Creese. Exploring the Relationship between Residual Risk

Awareness and Cyber Security Posture - A qualitative study on the state of cyber security in large enterprises. Technical Paper. 2018.

Krämer, Aspinall, Wolters. POSTER: Weighing in eHealth Security - A Security and Privacy Study of Smart Scales. Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016

Andikan Otung

Supervisor: Andrew Martin,
Department of Computer Science

Andikan studied Electronic & Electrical Engineering (MEng) at UCL, where he graduated on the Dean's list. After graduation, Andikan began a career in telecommunications, working in London as a Sales Engineer for Ciena – a multibillion dollar networking-infrastructure vendor. As well as (officially) becoming an inventor, Andikan developed an increasing interest in Security, through his work on the government side of sales operations.

As the more perceptive of readers may have already gathered, Andikan is both technically and commercially minded. His interests reflect this and include: IoT Security, Trusted Computing, DDoS, Cryptography, Multi-factor (including location-based) Authentication as well as commercial strategies enabling the fast creation and adoption of new technologies.

Arianna S.

Supervisor: Sadie Creese, Michael Goldsmith and Helena Webb, Department of Computer Science and Harriet Tear, Centre for Health, Law and Emerging Technologies

Arianna is a DPhil student working within the Cyber Analytics Group under Professor Sadie Creese, supervised by Professor Michael Goldsmith. Her work on dynamic consent and data protection compliance is co-supervised by Dr Harriet Teare, Deputy Director of HeLEX (the Centre for Health, Law and Emerging Technologies), and Dr Helena Webb, whose focus lies with Human Centred Interaction in the Department of Computer Science.

Her work focuses specifically on how to "inform" consent choices by developing an approach that combines technical controls with user engagement to allow individuals to have more control over the data they share, and to outline good practice for those who collect, store, use and share that information.

DPhil Thesis: Dynamic Consent as a mechanism for data minimisation.

Arianna's research describes a problem with consent as it is implemented at the moment and presents a solution to this. Personal information is collected and shared for further uses than it was originally collected for. This "secondary" data-use may occur without an individual's knowledge or permission and under recent data protection legislation like the General Data Protection Regulation (GDPR) and recent iteration of the Data Protection Act (DPA18) can be illegal. Dynamic consent offers a solution to this, resting on principles of revocation, engagement and persistence. A mechanism that accommodates current "blanket approaches to giving consent, it also extends functionality to place control in the hands of the individual. This thesis interrogates the importance of such a paradigm shift in how we conceptualise consent and explores its potential impact, with a view to contributing to the conversation around how to build new systems and implement change in the ones we currently have.

Publications

Schuler Scott, A., Goldsmith, M. and Teare, H., 2018. Wider Research Applications of Dynamic Consent. In IFIP International Summer School on Privacy and Identity Management (pp. 114-120). Springer, Cham.

Schuler Scott, A., Goldsmith, M., Teare, H., Creese, S. and Kaye, J., 2018. Dynamic Consent in Cybersecurity for Health. In Int'l Conf. Health Informatics and Medical Systems (HIMS'18). CSREA Press.

Recent projects:

(2019) Developed, coordinated and ran "Cybersecurity in Context" at the CDT, a module designed to teach technical skills and explore causes/responses to cybersecurity events. Topics covered were forensics, binary exploitation, web attacks and a cyber crisis simulation.

Upcoming:

Schuler Scott, A., Goldsmith, M., Teare, H., Creese, S. and Webb, H., 2019. Why We Trust Dynamic Consent to Deliver on Privacy. A work-in-progress paper at the 13th IFIP International Conference on Trust Management (IFIPTM 2019).

William Seymour

Supervisor: Max van Kleek, Department of Computer Science

William's research uses speculative design to create and prototype solutions to privacy and security problems in the smart home. Rooted in philosophy, he examines how accounts of respect, from Kant through to those of contemporary philosophers, might inform the design of future smart home devices. His main work on voice assistants uses familiar technology in unfamiliar ways to prompt learning, discussion, and self reflection on topics where traditional research approaches struggle to drive engagement.

DPhil Thesis: Making Sense of Smart Devices in the Home.

There is a prevailing sense of confusion surrounding smart IoT devices in the home, particularly around the data they collect and how it is processed. This research aims to empower users to make meaningful decisions about how they interact with the technology in their daily lives by exploring two mechanisms which can be communicate device boundaries and help the formation of accurate mental models: sensemaking and the portrayal of devices as (bounded) social actors.

Publications

Van Kleek, M., Seymour, W., Binns, R., and Shadbolt, N., 2018. Respectful Things: Adding Social Intelligence to 'Smart' Devices. In the Living in the Internet of Things Conference, London.

Seymour, W., Van Kleek, M., Binns, R., and Shadbolt, N., 2019. Aretha: A Respectful Voice Assistant for the Smart Home. In the Living in the Internet of Things Conference, London.

Van Kleek, M., Seymour, W., Binns, R., Zhao, J., Karandikar, D., and Shadbolt, N., 2019. IoT Refine: Making Smart Home Devices Accountable for Their Data Harvesting Practices. In the Living in the Internet of Things Conference, London.

Workshops:

Seymour, W., and Van Kleek, M., 2019. The Internet of Kant: Respect as a Lens for IoT Design. In Standing on the Shoulders of Giants: Exploring the Intersection of Philosophy and HCI workshop at the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow.

Kraemer, M., Seymour, W., Binns, R., Van Kleek, M., and Flechais, I., 2019. Informing The Future of Data Protection in Smart Homes. In New Directions for the IoT: Automate, Share, Build, and Care workshop at the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow.

Van Kleek, M., Seymour, W., Binns, R., and Veale, M., 2018. The Need for Sensemaking in Networked Privacy and Algorithmic Responsibility. In Sensemaking in a Senseless World Workshop at the 2018 CHI Conference on Human Factors in Computing Systems, Montreal.

Seymour, W., 2018. Social Acceptability and Respectful Smart Assistants. In (Un) Acceptable!?! – Re-thinking the Social Acceptability of Emerging Technologies Workshop at the 2018 CHI Conference on Human Factors in Computing Systems, Montreal.

Research Competitions:

Seymour, W., 2019. Privacy Therapy with Aretha: What If Your Firewall Could Talk? In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, ACM, Glasgow.

Seymour, W., 2018. How loyal is your Alexa?: Imagining a Respectful Smart Assistant. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, Montreal.

Marcel Stolz

Supervisors: Michael Goldsmith, Department of Computer Science and Lucas Kello, Department of Politics and International Relations

Marcel first became aware of security and defence matters during his military service in the Swiss army, serving as an officer (first lieutenant) in the electronic operations unit. During Marcel's Bachelor's and Master's studies at the University of Bern, he gained insights into political work as member of the university's TUX party, discussing topics such as privacy. Marcel subsequently worked with Swisscom, Switzerland's national phone operator, in the Big Data Mobility Insights Squad.

Marcel's current interest lies in combining his technical knowledge with his interests in politics and history. He explores aspects of state and net neutrality, how it can be implemented in cyberspace, and what capabilities a neutral nation should build up in cyberspace.

DPhil Thesis: State Neutrality and Cyber Defence

Publications

Mini-Project 1: Neutrality and Cyber Defence

Mini-Project 2: Assessing Risks from Wearable IoT Devices in a Military Context (currently being prepared for publication in a Journal)

Oleh Stupak

Supervisors: Greg Taylor, Oxford Internet Institute and Aleksei Parakhonyak, Department of Economics

Oleh holds MSc in Economics from Paris 1 Pantheon-Sorbonne (France) and BSc, MA degrees in International Economics from Taras Shevchenko National University of Kyiv (Ukraine).

Alongside with academia, he obtained more than six years of experience in private sector. Three of which, Oleh held a CEO position in the self-founded company "thelamp". The company was a projection of his curiosity to the innovative technologies. It provided a full range of IT services and specialised on the tailoring of unique software solution for commercial and governmental purposes.

His MSc thesis in Paris 1 was devoted to the research on DDoS (distributed denial-of-service) attack risk for industries. The model developed during that period is capable of calculating the enterprises' chance of being the subject of DDoS attack considering 25 economic and technical parameters.

Oleh is convinced that the future stands in interdisciplinary approaches and cooperation among schools. His desire for knowledge and world outlook brought him to Oxford's CDT in Cyber Security. Currently, Oleh focuses on the emerging cyber security threats for enterprises. His broad area of interests includes: enterprises behaviour and unfair competition in the information environment, cyber security risks.

Publications

MSc Thesis: Determination of DDoS enterprises` risks

Supervised by Sergei Guriev (Professor of Economics, Science PO)

Mini-Project 1: Unfair Competition in the information environment. Industrial information leakage

Supervised by Alexei Parakhonyak (Associate Professor, Univeristy of Oxford)

Mini-Project 2: Unfair Competition in the information environment. The DDoS attack

Supervised by Greg Taylor (Associate Professor, Univeristy of Oxford)

Jack Sturgess

Supervisor: Ivan Martinovic, Department of Computer Science

Jack graduated from the University of Surrey with a BSc (Hons) in Mathematics and an MSc (Dist.) in Information Security. He worked as a software engineer at Accenture for 1 year and at IBM for 5 years; he also co-founded a video games company, while at IBM, that released two titles on PlayStation Network and one on Steam.

An avid traveler, Jack volunteered as a conservationist in Arizona and California after his first degree, camping and working in the middle of nowhere while enjoying fantastic landscapes! His interests also include programming, board-gaming, hiking, and number theory.

Jack's research interests include authentication, cryptography, steganography, and the Internet-of-Things. Being part of the CDT has proven to be an excellent way to study the interweave of these subjects and to understand their implications across other disciplines.

Publications

Sturgess, J., & Martinovic, I., "VisAuth: Authentication over a Visual Channel using an Embedded Image", Cryptology and Network Security (CANS) 2017

Sturgess, J., Nurse, J. R. C., & Zhao, J., "A Capability-oriented Approach to Assessing Privacy Risk in Smart Home Ecosystems", PETRAS 2018

Olivia Sturrock

Supervisor: Andrew Martin, Department of Computer Science

With a background in Economics, Olivia first studied computer science at Liverpool University graduating with a MSC in Advanced Computer Science and Internet Economics. Her dissertation for this, in ontological meaning negotiation between agents, led to key interests of multi-agent systems, agent negotiations and how these subjects can be applied to cybersecurity.

DPhil Thesis: Smart Cities: Security Implications of Smart Critical Infrastructure

Looking at how the development of Smart Cities and the related technology could affect the security of the city.

Publications

Mini-Project 1: The Changing Security Needs for Distributed Energy Generation in the UK

Valentin Weber

Supervisors: Lucas Kello, Department of Politics and International Relations and Joss Wright, Oxford Internet Institute

Valentin is a Research Affiliate with the Centre for Technology and Global Affairs, University of Oxford. Previously, he was an Open Technology Fund Senior Fellow in Information Controls at the Berkman Klein Center for Internet & Society, Harvard University. He also worked for the International Security Department at Chatham House. Valentin is interested in how the cyber domain is changing conflicts and state strategies. His current research focuses on the integration of cyber and grand strategy, as well as on the role of information controls in state strategies.

DPhil Thesis: The Diffusion of Cyber Norms and Its Implication for Power

My thesis studies the proliferation of cyber norms, and in particular of information control and freedom. It researches the United States, China, and Russia, which are one of the main norm promoters in cyberspace.

Publications

Vasilis Ververis, Marios Isaakidis, Valentin Weber, and Benjamin Fabian. "Shedding Light on Mobile App Store Censorship." In Proceedings of the 27th Conference on User Modelling, Adaptation and Personalization Adjunct. June 2019. Larnaca, Cyprus. ACM, New York, NY.

Valentin Weber and Vasilis Ververis. "Measuring Censorship on Mobile App Stores." OxPol. 3 May 2019.

"Finding a European Response to Huawei's 5G Ambitions." Norwegian Institute of International Affairs. March 2019.

"A Bold Proposal for Fighting Censorship: Increase the Collateral Damage." Net Politics - Council on Foreign Relations. 31 January 2019.

"Understanding the Global Ramifications of China's Information Controls Model." in AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives. White Paper for the Joint Chiefs of Staff. January 2019.

"Linking Cyber Strategy with Grand Strategy: The Case of the United States." Journal of Cyber Policy. 2018.

"States and Their Proxies in Cyber Operations." Lawfare. 15 May 2018.

"The Rise of China's Security-Industrial Complex." Net Politics - Council on Foreign Relations. 17 July 2018.

"Why China's Internet Censorship Model Will Prevail Over Russia's." Net Politics - Council on Foreign Relations. 12 December 2017.

CDT17 Bios

Thomas Burton

Supervisor: Kasper Rasmussen, Department of Computer Science

Thomas studied an MComp in Computer Science (with Security and Resilience) for four years at Newcastle University. His current areas of interest include secure localisation, misusing localisation schemes for attacks, and mesh networking. At Newcastle he studied a range of topics from system security and information security and trust to high integrity software development and the challenge of developing highly dependable systems. His third and fourth year dissertation projects covered the security related topics of biometric security and authentication, and cryptographic, specifically zero-knowledge proofs. He has also spent several summers working with a health sciences and bioinformatics group. With them he has worked on a range of projects ranging from website development to algorithm development. During this work, he experienced working with people from a range of academic departments and fields.

DPhil Thesis: Secure Urban Audio Localisation

I am looking at the use of smartphones for urban search and rescue. Specifically I am working on secure protocols for using audio to locate smartphone devices to assist in an urban disaster environment. This type of localisation has a number of potential challenges to overcome as a result of limited low level hardware access, the scale over which the protocols are being used, and how easily an attacker can interfere as the cost of mounting at attack is low. Attackers also have several key advantages, such as, being able to transfer information at the speed of light using normal radio communication which is much faster than the sound used for the localisation.

Erin Chapman

Erin is a Canadian-New Zealander with a Bachelor of Science majoring in Computer Science from the University of Auckland and a Masters of Computer and Information Sciences (hons, first class) from Auckland University of Technology. Her Masters' thesis focused on the design of cryptographic fundamentals. She has also been involved in inter-disciplinary research into random number generation, which explores the use of radio telescopes for generating true random numbers. Erin's areas of interest are in cryptography and machine learning, particularly the ways in which evolutionary computing methods, such as genetic programming and neural networks, can be applied to developing secure systems.

Selina Yoon Cho

Supervisors: Ivan Flechais, Department of Computer Science and Jonathan Lusthaus, Department of Sociology

Selina is interested in understanding how cybercrime intersects with online social entertainment. Her current work explores the behavioural and social factors involved in manipulating online game tools, and the interplay between cheaters and non-cheaters within collaborative team play and resource gathering.

Selina holds an MSc (Distinction) in Information Security and a BA in Economics. Her masters dissertation elaborated on the concept of security through obscurity through its designs in cryptographic obfuscations and image steganography. Prior to joining the CDT, Selina worked as a security consultant in a power plant.

Selina is the President of the Oxford Fintech and Legaltech Society, a platform for sharing interdisciplinary ideas in finance and law through seminars, hackathons, and research collaborations. She has helped establish the Society's partnership with Deep Tech Dispute Resolution Lab in the Faculty of Law to investigate automated negotiation methods.

DPhil Thesis: The Implications of Cheating in Online Multiplayer Games on Skills Development and User Experience

Online gaming is one of the most common ways teenagers and young technology adapters become familiarised with the use of the online world. Its experience extends the mundane interactions that occur in real-life such as bonding, rivalry, and transaction, to a broader audience. Whilst it primarily serves as a source of naïve entertainment, the cheating activities it is frequently associated with are said to be, or on the periphery of, perpetrating forms of conventional cybercrime. The covert nature of cheating and its associated markets have meant that there lacks depth in understanding the pervasiveness and extent of unwanted behaviours in the gaming platforms.

With a focus on competitive multiplayer online games, this research seeks to address these challenges by exploring the types of strategies commonly discussed and sold in external communities, and simulating the interplay between cheaters and victims of cheating on the virtual platform.

Outputs

S. Y. Cho and J. Wright (forthcoming), "Into the Dark: A Case Study of Banned Darknet Drug Forums," in 11th International Conference on Social Informatics, Springer International Publishing, 2019.

Tommaso De Zan

Supervisors: Ewart Keep and Liam Gearon, Department of Education; Andrew Martin, Department of Computer Science.

Tommaso is a DPhil student in Cyber Security at the University of Oxford, where he is analyzing policies to reduce the cyber security skills shortage. In the context of his research, he conducted six months of fieldwork at the European Union Network and Information Security Agency. In Oxford, he is also a Research Associate with the Centre for Technology and Global Affairs at the Department of Politics and International Relations and he is a member of the Working Group on Cyber Security Culture and Skills of the Global Forum on Cyber Expertise.
Prior to his DPhil, he was an Associate Fellow at the European Union Institute for Security Studies in Brussels and a Researcher at the International Affairs Institute (IAI) in Rome. Before joining IAI, he interned at the Geneva International Peace Research Institutein Geneva.
He holds a Master's degree in International Relations from the University of Bologna and was an exchange student at the University of Denver and Université catholique de Louvain.

DPhil Thesis: Do competitions affect students' interest in cyber security career? The cyber security skills shortage and public policy interventions

Employers have been lamenting for several years the lack of cyber security professionals in the labour market, the so-called cyber security skills shortage. The shortfall of information security workers means that our data, networks and systems are less secure, which might undermine economic development and national security. Governments have scrambled to redress this trend and have designed and implemented policies to increase the pipeline of cyber security professionals. Among these policies, cyber security competitions have sprouted and received the support of governments and industry alike. Nonetheless, it is generally unknown whether skills shortage policies such as cyber security competitions work and how. This dissertation project investigates the outcomes of these competitions, especially whether they affect students' career interest in cyber security.

Publications:

De Zan T., Giacomello G., Martino L. (forthcoming), "Italy", Routledge Handbook of Global Cybersecurity, edited by Manjikian M. and Romaniuk S. N., Routledge, New York;

De Zan T. (forthcoming), "The Italian Cyber Security Skills Shortage in the International Context", Global Cyber Security Center, Rome

De Zan T. (2019), "Much Ado About the Cyber Skills Shortage", Net Politics, Digital and Cyberspace Policy Program, Council on Foreign Relations, New York, https://on.cfr.org/2tHwSTx;

De Zan T. (2019), "Cybersecurity, what we (really) need to close the cyber security skills shortage, (in Italian), Formiche, https://bit.ly/2TWnAyF;

De Zan T. (2019), "Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions", Global Cyber Security Center, Rome, https://bit.ly/2tpedvs;

CDT17 Bios continued

Seb Farquhar

Supervisor: Yarin Gal, Department of Computer Science

Seb is interested in cyber security within machine learning and artificial intelligence. This includes technical work on robust deep learning systems that are able to recognize and safely handle unexpected or adversarial inputs as well as privacy-preserving machine learning and policy questions related to the safe adoption of AI systems. Before beginning this DPhil, Seb worked at the Future of Humanity Institute at the University of Oxford, was Director of the Global Priorities Project, a think tank focusing on global catastrophic risk management, and worked for McKinsey & Co. as a consultant focusing on public sector clients. He has a Master's degree in Physics and Philosophy from the University of Oxford.

DPhil Thesis: Foundations for secure deep learning

In this research project I explore foundations for safe and secure deep learning including:

-Systems capable of detecting anomalies/out-of-distribution behaviour using Bayesian deep learning methods and ensembles.

-Differentially private deep learning systems for learning over extended periods of time or across related simultaneous contexts with managed privacy leakage.

-Deep learning architectures optimized for secure multi-party computation.

Jack Kenny

Supervisors: Catherine Redgwell and Efthymios Papastavridis, Faculty of Law

Jack's background is in public international law. He holds an LL.B degree in Law with European Study and an LL.M degree in International and European Law. Jack is supervised by Professor Catherine Redgwell and Dr. Efthymios Papastavridis at the Faculty of Law. In addition to his DPhil research Jack is a Post-Doctoral Research Fellow at the Hebrew University of Jerusalem on The Prospects for an International Attribution Mechanism for Cyber Operations project. He has several years of research experience including positions at the International Law Programme at Chatham House, the British Institute of International and Comparative Law, and the Amsterdam Centre for International Law. Prior to commencing his doctorate, he held the post of Research Assistant with teaching responsibilities at the Institute for Public International Law, University of Bonn, under Professor Stefan Talmon. Jack has worked on cases involving issues of international and EU law. Current research interests include the relationship between customary law and treaty law, state responsibility, use of force, and the applicability of these topics to new and emerging areas governed by international law such as cyber operations.

DPhil Thesis: Establishing state responsibility for cyber operations

My research considers how existing frameworks of public international law apply to cyber operations. Specifically, the thesis focuses on establishing state responsibility for cyber operations by analysis of applicable primary and secondary rules of international law. The thesis aims to identify and examine primary rules and their application to cyber operations with an analysis of state responsibility and attribution, and discuss possible remedies and forms of restitution.

Klaudia Krawiecka

Supervisor: Ivan Martinovic, Department of Computer Science

Klaudia graduated from the NordSecMob programme in 2017, obtaining a Master's degree in Security and Mobile Computing from two universities: Aalto University and Norwegian University of Science and Technology. Her adventure with computer science began in primary school. She continued to develop her passion during high school and in college. During the second year of her Bachelor's studies, she took an internship in the ICT security office where she was introduced to computer forensics and cyber security fields; in addition, she had a great opportunity to conduct trainings for police officers on NFC technology and the risks arising from its use. She also worked as a Research Assistant at Aalto University in Secure Systems Group. Her research project, which developed into her Master's dissertation, concerned developing SafeKeeper, a system that secures users' passwords on the web. This project received two prestigious awards from the Finnish Information Security Association and the Finnish Computer Science Society.

Furthermore, she actively engage in other activities, including volunteering (e.g., OxfordHack, InspireHer!) and student societies such as Oxford Women in Computer Science Society. Guided by a passion for the spread of education in the area of new technology among children, youth, and adults, and the alignment of this area with opportunities and education for people with disabilities and people socially excluded, she set up a foundation that aims to teach programming and electronics in the form of hands-on workshops.

DPhil Thesis: Authenticating Internet of Things (IoT) devices using out-of-band channels

The amount of Internet of Things (IoT) devices available on the market increases significantly every year. Many such devices are integral parts of smart buildings, which are equipped with modern systems and technologies designed to increase the safety and comfort of their users. Many devices are not equipped with displays or do not allow users to verify their operation. Out-of-band channels such as visual channels (e.g. Augmented Reality) may provide a novel way of authenticating various sensors and give the users an appropriate feedback. The research focuses on designing, implementing, examining and assessing different out-of-band authentication channels and to determine which ones provide stronger security guarantees and fulfill usability, deployability and performance requirements.

Dennis Malliouris

Supervisor: Andrew Simpson, Department of Computer Science

Dennis D. Malliouris started the DPhil in Cyber Security programme in 2017. He has an MRes in Management (Distinction) for which he studied at London Business School and University College London. He was awarded the SoM Full Scholarship for the duration of his studies. Priorly, he graduated first in his class with an MSc in Management & Finance from UCL. During his studies at UCL, he was an elected student representative. He organised trips and events, worked on projects to improve student experience, and mediated conflicts between faculty and students. Dennis also obtained a BA in Management (first-class), has a certificate in financial valuation from Saïd Business School (OCVP), and is a qualified management accountant (IHK). Dennis worked on multidisciplinary in-house consultancy-type projects at Siemens in Germany and the UK, at a technology-driven hedge fund, and in financial research & valuation.

His research at the CDT explores financial, strategic, and organizational implications of cyber security for firms. Specifically, his research projects explore executives' activities around security breaches and information security investments.

Dennis grew up multilingually and speaks English, German, Greek, and French. He represents Oxford University in regional and national competitions, and New College on university-level, in multiple sports. He gratefully acknowledges CDT/EPSRC funding, New College's 1379 Society Old Members Scholarship, and New College's Sporting and Cultural Award.

DPhil Thesis: Strategic and financial implications of Cyber Security: Understanding decisions to invest in cyber security, market reactions, and corporate executives' approaches to and reactions subsequent to security breaches.

Publications:

D. D. Malliouris & A. C. Simpson (2019). The stock market impact of information security investments: the case of security standards. In: The 2019 Workshop on the Economics of Information Security (WEIS 2019).

Romy Minko

Supervisors: Artur Ekert and Christophe Petit, Maths Institute

Romy's background is primarily in Mathematics, although she also holds a BSc in Chemistry from the University of Melbourne. Romy first became interested in cryptography while at secondary school in Australia and subsequently went on to complete the MSc in the Mathematics of Cryptography and Communications at Royal Holloway, graduating with Distinction. Her research interests lie in post-quantum cryptography and quantum computation; she is currently focussed on supersingular isogeny-based cryptosystems and has previously conducted research in blind quantum computing. Romy is also a 2018 Policy Fellow with the Department of Prime Minister and Cabinet of Australia, where she experienced drafting cybersecurity policy at a government level.

DPhil Thesis: Post-quantum cryptography using multivariate polynomial systems

Multivariate public-key cryptography (MPKC) is one of the four most common branches of post-quantum cryptography, describing cryptosystems based on solving systems of multivariate polynomials. An important step in the cryptanalysis of MPKC system is finding a Gröbner basis for the system. My research focusses on adapting generic Gröbner Basis algorithms to families of multivariate polynomial systems with specific structures. I am currently looking at multivariate linearised polynomials, which have not been studied in great detail.

Additionally I am exploring applications of the HHL quantum algorithm for solving systems of multivariate polynomials, in particular Boolean systems.

James Pavur

Supervisor: Ivan Martinovic, Department of computer Science

James hails from Atlanta, Georgia (USA) and holds a BSFS in Science, Technology, and International Affairs from Georgetown University in Washington, DC. He is at Oxford on a Rhodes Scholarship (Georgia and Wolfson, 17). His thesis revolves around the security and privacy aspects of satellites and space-based systems with his most recent research focusing on satellite telecommunications and broadband services.

He has dabbled in cybersecurity through a variety of professional experiences – including functioning as the principle cyber decision maker at a 500 employee non-profit (Students of Georgetown Incorporated). His internship experiences include working as a Reverse Engineer for Embedded Systems at Booz Allen Hamilton, auditing building control and SCADA systems as a contractor for the US General Services Administration, and investigating computer crimes with the US Postal Service's Office of the Inspector General. He has also contributed to telecommunications and privacy policy research through Georgetown's Software and Security Engineering Research Center.

His language of choice is python, although (with generous use of Google) he is also proficient in C/C++, JavaScript, C#, PHP, and Visual Basic.He enjoys hackathons and CTF competitions, collecting (and sometimes consuming) tea, flying kites, and pretending he knows how to play squash.

DPhil Thesis: On Space Cyber-Security

This project focuses on cyber-security concerns for satellite systems. On going experimental research includes the investigation of privacy and security properties for modern satellite broadband connections over the Digital Video Broadcasting for Satellite (DVB-S) protocol, and the integrity and authenticity of space situational awareness data for flight control and orbit determination. The project also considers the strategic and political effects of Cyber-ASAT (Anti-Satellite Weapon) capabilities.

Longer term, the thesis will focus on providing core security principles and best practices to enable the secure operation of critical space missions. These principles will be derived from experimental research and strategic analysis

Publications:

James Pavur, Daniel Moser, Vincent Lenders, and Ivan Martinovic. 2019. Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband. In WiSec '19: Conference on Security and Privacy in Wireless and Mobile Networks, May 15– 17, 2019, Miami, FL, USA. ACM, New York, NY, USA. https://doi.org/10.1145/3317549.3323418

James Pavur and Ivan Martinovic. 2019. The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In 2019 11th International Conference on Cyber Conflict - Silent Battle, May 28-31, 2019, Tallinn, Estonia. NATO CCD COE Publications, Tallinn, Estonia.

James Pavur. 2018. Cyber Security and AI (Seminar). Rhodes Artificial Intelligence Laboratory - Speaker Series. November 07, 2018, Oxford, United Kingdom.

Mark Quinlan

Supervisor: Andrew Simpson,
Department of Computer Science

Mark Quinlan has gained a mixture of industry experience and academic knowledge prior to starting a DPhil in Cyber Security, his industry experience including BAE Systems where he worked within the cyber field in both commercial and government projects. His consultancy business designed and built manufacturing resource planning systems, as well as systems security strategy consultancy for companies ranging from British racing teams to Japanese Tier One suppliers. Mark lives with his partner, and when not pursuing his academic passions he enjoys restoring classic cars, driving karts and said cars, hiking, non-fiction, and enjoying good food and company. Once upon a time Mark was a Dutchman, but has lived in the UK since 2004.

DPhil Thesis: Cyber Continuum; towards a security engineering framework incorporating legacy systems

Mark is looking into privacy and security of Internet of Things devices, and their wider infrastructural landscape. Current work includes a privacy and security analysis of connected cars through the examination of the data-gathering systems of a production vehicle, to ascertain some of the privacy-related threats to which such systems give rise.

Future work: With the lifecycle of an average car being approximately nine years, a connected car has a longer lifespan than the typical IoT device. In addition, it is significantly more likely to be re-sold over its lifetime. When looking at embedded devices across the IoT spectrum, more and more devices are falling outside traditional consumer devices such as speakers and home security, increasingly being used within city infrastructure, and in private and commercial transportation such as cars, the need for security management over longer lifecycles becomes more apparent.

The high-level research objectives are as follows;

1. What is the current state of the literature on the management of legacy embedded systems, and their associated infrastructure?
2. What is the current state of manufacturers providing security updates to their products?
3. What would a theoretical framework incorporating the long-term management of legacy IoT devices look like?

Lonie Sebagh

Supervisors: Jonathan Lusthaus and Federico Varese, Department of Sociology

Following her first year classes and projects Lonie is now researching the disruption of online criminal marketplaces combining sociology, criminology, and economics perspectives. Her focus is on bringing a new research method to the field of cybercrime, laboratory and online experiments, in order to better evaluate traders' behaviours on these platforms following disruption operations such as slander, Sybil, and website takedowns.

Prior to joining the CDT Lonie was a student in Business and Management at the Universities of St Andrews and Edinburgh. Her interest in Cyber Security stems from her work experience in the IT Security department of a private bank in Geneva in 2014, which inspired her to make the transition from Business to Information Technology through a PG Diploma (Distinction) with an emphasis on Computer Security and Critical software engineering.

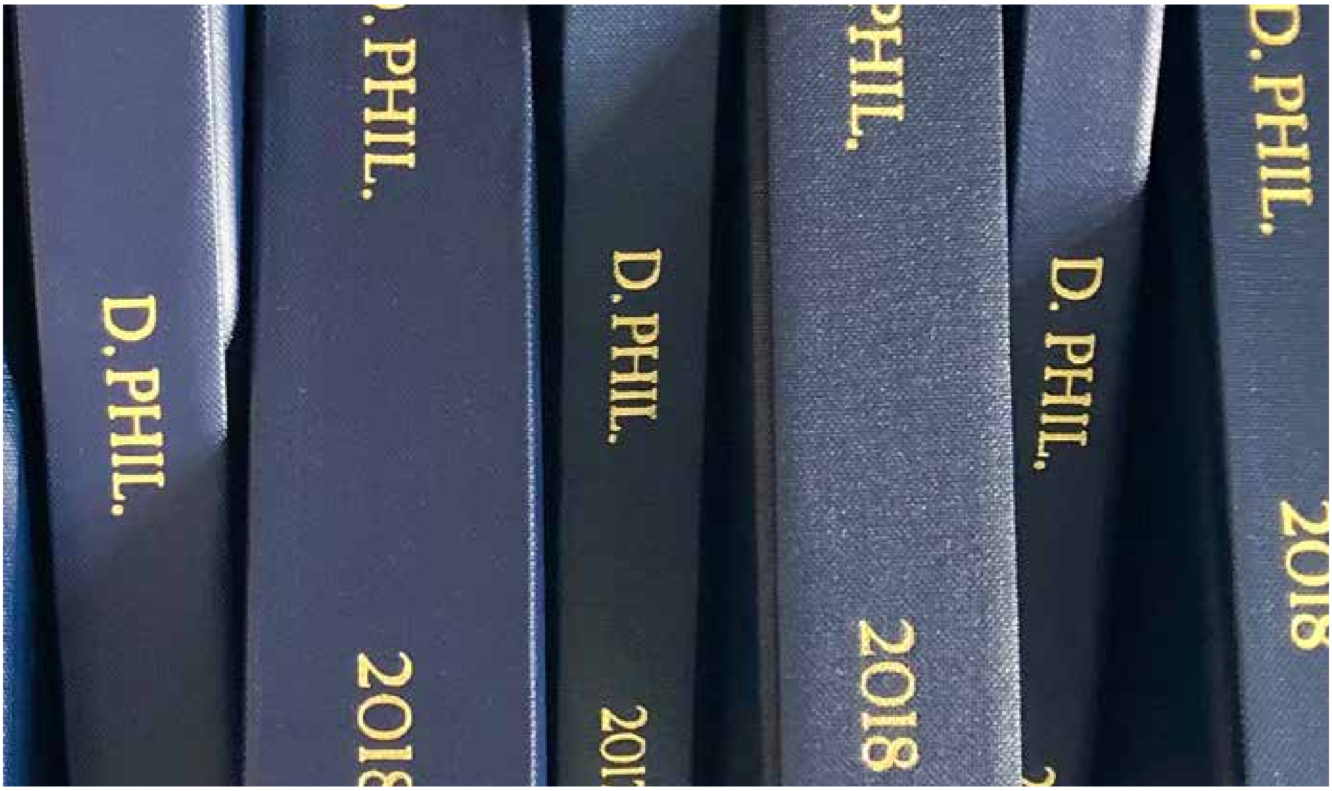
In her spare time Lonie can be found in the yoga studio where she has has recently become a certified yoga instructor and in her College where she is working as an IT Assistant.

DPhil Thesis: The disruption of Dark Net Markets – the impact of slander, Sybil, and platform takedown operations

This research will use social laboratory and online experiments, never before used in the field of cybercrime, to better understand cybercriminal networks' responses to Law Enforcement disruption operations in darknet markets. Operations currently performed in the wild will be replicated in controlled settings in order to test their respective effectiveness in lowering product quality and increasing price, therefore rendering these markets less attractive. Participants' behaviours during trading games when subjected to certain disruption operations will inform policies about which operations to use, when to use them, whether to use them individually or simultaneously, and what 'breaking points' Law Enforcement should act upon in order to disrupt these markets more efficiently. The insights from these experiments will be combined with interviews of Law Enforcement agents and forum data where platform users discuss their experiences in these markets.

Publications:

Lonie Sebagh, Jonathan Lusthaus, Federico Varese, 2019. Responses to Slander and Sybil Disruption Operations in Online Criminal Marketplaces – a Laboratory Experiment. In: 2019 European Economic Science Association (ESA) Meeting, September 5-8, Dijon, France.



Sean Sirur

Supervisor: Kasper Rasmussen, Department of Computer Science, Tim Muller, University of Nottingham

Sean has been involved with security and formal methods for the majority of their academic career. In their Computer Science and Physics BSc from Edinburgh, these two areas were their primary focus, in addition to quantum and statistical physics.

While Sean wishes to maintain a strong connection to their formal background, they are also intent on drawing inspiration for their research from sociological issues. Their move into formal trust research is particular ideal as it also incorporates their experience of physics through network dynamics and information theory. Sean's primary focus in trust is formalising the exploitation of trust systems, particularly in systems were there is a delay in information transmission between users. In addition to this, they will be working on research around trust dynamics on the dark web.

Sean has worked part-time as a teaching assistant for three courses at Oxford (Network Security and Cloud Security with the Software Engineering Program and Computer Security with the Department of Computer Science) and as a tutor and lab demonstrator for Computer Security at UoEdinburgh. Their hobbies include hiking, reading, music, spending time around animals and playing games.

DPhil Thesis: The Reputation Lag Attack

Reputation-based trust systems are increasingly common on digital platforms; this includes any model where the trustworthiness of an actor is derived from how other actors judge their interactions with that entity. Common examples include review and ratings systems as often used on electronic marketplaces. In any such system, the propagation of reputation suffers from delays of various kinds e.g. network connectivity, reporting delays and rating-update delays. There is very little existing research on the exploitation of this lag, known as a reputation lag attack. Furthermore, there is no robust theoretical framework for the definition, discussion and evaluation of such attacks. Current research is a first step towards constructing a suitable theoretical framework of reputation lag attacks. Future research includes investigating techniques with which attackers can increase their profit so as to provide an insight into attack patterns. The findings of this future research can then be used to validate and improve upon the framework; construct mitigations against the attack; and to aid investigations into whether the attack is already occurring in the wild and with what frequency.

Publications

Sirur, S., & Muller, T. (2019). The Reputation Lag Attack. In Proceedings of the 13th IFIP WG 11.11 International Conference on Trust Management July 17 - July 19, 2019, Copenhagen, Denmark

Sirur, S., Nurse, J.R. and Webb, H., 2018, October. Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (pp. 88-95). ACM

Eva Stanková

Supervisor: Justine Pila, Faculty of Law

Eva is reading for a DPhil in Cyber Security at the University of Oxford within the CDT 2017 cohort. Her DPhil thesis is devoted to the legal implications of computational creativity of artificial intelligence-driven systems deployed in cyber defence. During her studies at the Law Faculty of Charles University in Prague, Eva worked as a Research Assistant at the Department of Politics and Sociology (Law Faculty) and she served as an Intern at criminal and business law sections of courts in Prague. After graduation Eva practiced law in Prague-based law firms as an Associate in corporate, IP/IT, media and telecommunication legal teams. In 2015, her interest in intersection of intellectual property law and competition law brought her to the Munich Intellectual Property Law Centre (MIPLC). Thanks to the MIPLC LL.M. programme she acquired insights into IP and IT law topics related to cyber security such as software patents or copyright. Eva also dealt with policy coordination in internal market at the Secretariat General of the European Commission in Brussels. In her mini-projects she focused on evolution of data protection regulation in Europe and legal implications of AI-driven creativity in cyber security.

DPhil Thesis: AI-Driven Defence Systems and the Limits of Copyright and Patent Law

This research deals with computational creativity in the context of the current state of the art artificial intelligence algorithms deployed in network defence. It features a legal assessment of whether objects generated by AI-driven systems qualify for copyright and patent protection under the current legal regimes in Europe and in the United Kingdom. In order to examine the eligibility for the legal protection, a human creativity requirement will be analysed, and it will be determined how it is applied to computer-generated objects. This project will conclude with recommendations towards such a legal regime for AI-generated objects which would be ideal for incentivising innovation in the field of cyber security.

Henry Turner

Supervisor: Ivan Martinovic, Department of computer Science

Henry comes from Colchester, Essex and holds a MEng from Imperial College London in Computing. His thesis examines security aspects of biometric systems, with a particular focus on voice processing systems and their resilience to realistic attacks, as well as developing ways to better protect users of these systems.

During his time at Imperial College London he completed his thesis on security schemes in body sensor networks and facilitating secure communication in embedded medical devices. He has interned as a software engineer at Intel Security (McAfee) working on corporate network monitoring products. Prior to this he also ran a small enterprise publishing iPhone and Android applications during his teenage years, distributing more than 250,000 copies of his applications during the project's lifespan.

DPhil Thesis: Improving the Security of Voice Interface Systems

Voice interfaces have become common on modern devices, and increasingly support complex interactivity, as well as authentication mechanisms to provide personalised (and sensitive) functionality to users.

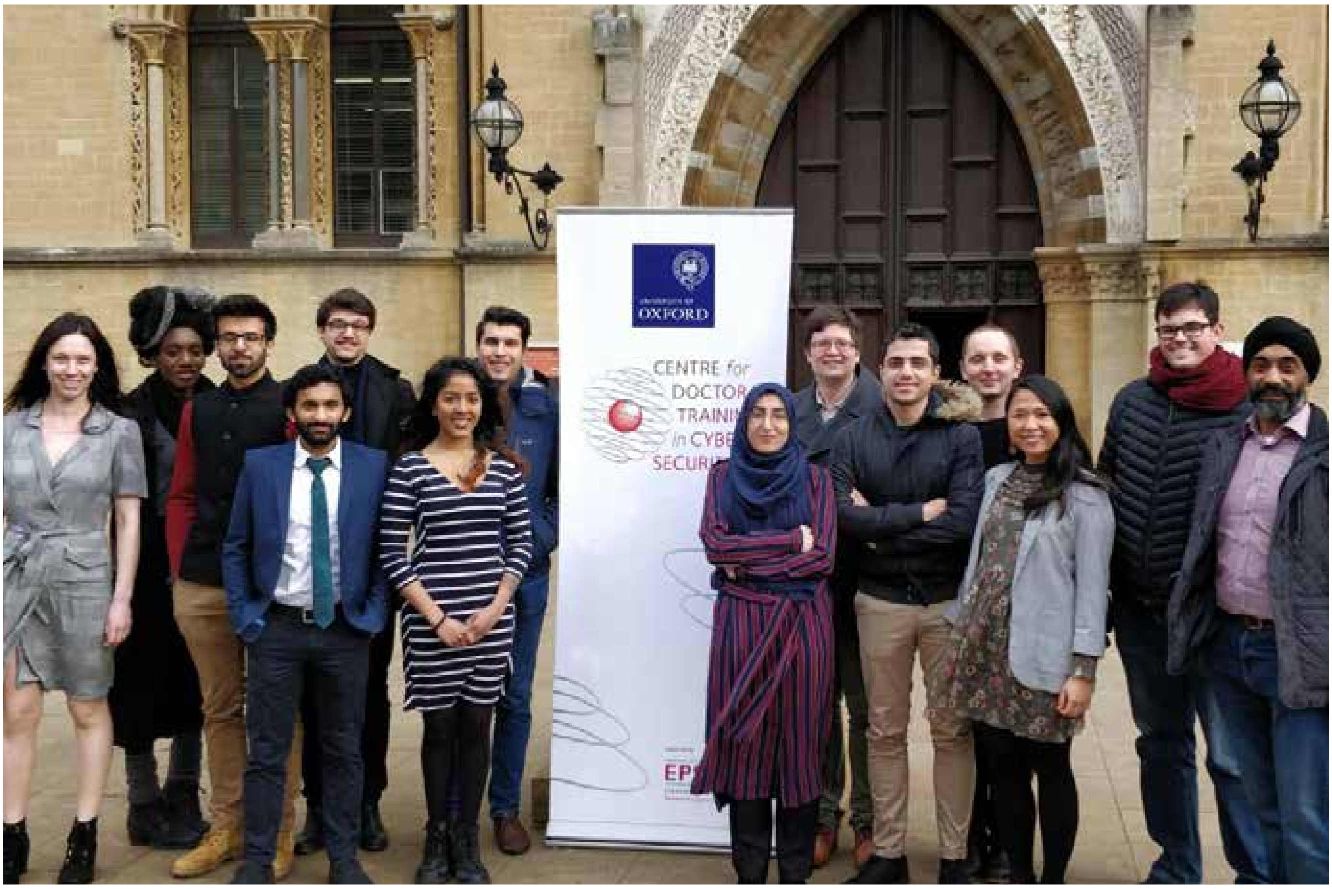
We focus on such voice interfaces, and in particular improving their performance in adversarial situations. We do this through the testing of attacks against such systems and through the development of tools to analyse security properties. In turn these allow us to identify flaws and weaknesses in voice systems.

We then design improved voice interface systems to combat weaknesses and flaws we identify, to improve their overall security properties.

In addition to work on voice interface systems, we intend to try and translate some of our attacks and tooling to other biometric systems, to see if they suffer from similar weaknesses and can be improved in similar ways.

Publications:

Turner, H., Lovisotto, G. and Martinovic, I. Attacking Speaker Recognition Systems with Phoneme Morphing, European Symposium on Research in Computer Security 2019, 23-27 September 2019, Luxembourg



CDT18 Bios

Freddie Barr-Smith

Freddie holds a BSc in Computer Science and Business Management (First) and an MSc in Software and Systems Security (Distinction). He also has held positions in infrastructure and security roles in multiple sectors.

He is very interested is penetration testing, digital forensics, malware analysis and exploit development. In this regard he holds several relevant certifications.

Although principally a technical specialist, there is also an interest in the wider societal scope of security, such as the intersection between cybersecurity, international relations and strategy, particularly how this affects cyberwarfare and the phenomena of influence operations. There is also a longstanding fascination with criminology and forensics, particularly how it intersects with cybersecurity via cybercrime.

Mini-Projects

Mini-Project 1: Phishing With a Darknet - Imitation of Onion Services

Mini-Project 2: Malware Anti-Forensic and Evasion Techniques

George Chalhoub

George Chalhoub (georgechalhoub.com) is a doctoral researcher in cybersecurity at Pembroke College, Oxford. He holds a BS in Computer Science (First) from the Lebanese American University and an MSc in Computer Science (Distinction) from the University of Southampton. During his master thesis at Southampton, he has developed a 3D information system for ship pump systems in coordination with Lloyd's Register. George is also the CEO of GC Group LLC, a startup specialising in web hosting and security. His research interests mainly surround User Experience (UX) and security.

Mini-Projects

Mini-Project 1: Anomaly-Based Network Intrusion Detection System through Convolutional Neural Network and Stochastic Gradient Descent Algorithm

Mini-Project 2: "Alexa, are you spying on me?": User Experience factors affecting privacy and security in Smart Home Assistants

Anirudh Ekambaranathan

Anirudh holds an MSc in Computer Science and Education from Twente University in the Netherlands. His research focuses on applied machine learning in the context of cyber security. Currently he is researching anomaly based intrusion detection systems. His previous research projects focused on Wi-Fi tracking and stylometric linkability in darknet markets. Before joining the CDT he worked as a part-time math teacher in secondary school and had his own cyber security startup.

Mini-Projects

Mini-Project 1: GAN Based Anomaly Detection Using Protocol Conditioning and Feature Corruption

Mini-Project 2: Developer Practices surrounding Security and Privacy of Family Oriented Apps

Marine Eviette

Marine is a Radcliffe scholar with interests in Privacy and Cryptography-having undertaken prior research in Post Quantum Cryptography, Cryptanalysis of Historical Ciphers and Online Privacy. The latter of which she is choosing to pursue further by completing projects concerning unintentionally-created personas as well as concerning design approaches that encourage privacy-averse behaviour. Besides this she previously completed a Masters thesis which sought to help prevent the propagation of Cyber Attacks by utilising ZKP verified Distributed Ledger Technology.

Publications:

Upcoming: The emergence of the online shadow identity: Investigating the unsolicited creation of online identity profiles

Connected Life 2019 Conference: Cybersecurity, Tech Abuse, and Intimate Partner Violence

Map the System Oxford semi-finalist.

Martin Georgiev

Martin holds a BEng degree from the University of Edinburgh which incorporated an exchange year at University of California, Irvine (UCI). During his stay abroad, he developed an interest in cyber security and published a joint paper with the SPROUT (Security and Privacy Research OUTfit) group at ESORICS 2018. He has various internship experiences ranging from the banking industry with Royal Bank of Canada to developing systems to enhance the experience of his fellow students. At Oxford, Martin is interested in areas where cyber security intersects with machine learning such as biometric based continuous authentication and adversarial machine learning.

Mini-Projects

Mini-Project 1: Towards continuous touch-based mobile authentication using neural networks

Mini-Project 2: Adversarial noise injection into digital images through electromagnetic interference

Hayyu Imanda

Inda (@indaimanda) is an Indonesian Jardine Scholar at Exeter College. She grew up in Jakarta before pursuing her BSc in Mathematics at Edinburgh, and her MSc in Mathematics and Foundations of Computer Science at Oxford. Her MSc dissertation covered the security of the supersingular isogeny key exchange when used with the parameters submitted to NIST Call for Post-Quantum Cryptography Algorithms.

In her year after finishing her master's degree, she was a software developer for a FinTech company and later an intern for the forensics team at a consultancy in Jakarta. In her first year of the CDT, she co-organised the joint CDT conference with Royal Holloway, themed Cyber Espionage. Her current research interests include the post-quantum cryptography, differential privacy, and cybersecurity of conservation and citizen science.

She has a full Blue in tennis and an AOW scuba diver certification, and when possible, she spends time away from Oxford travelling across her diverse home country. You will also find her baked goods during a Cyber Cafe or two!

Mini-Projects

Mini-Project 1: Location Privacy in Conservation

Mini-Project 2: Mass Surveillance and Isogeny-Based Post-Quantum Cryptography

CDT18 Bios continued

Jack Jackson

Jack is currently a DPhil Researcher at the University of Oxford, where he resides within the Centre for Doctoral Training in Cyber Security. Jack has previously held roles as a Chief Technology Officer, Principal Technology Consultant, Research Scientist, Cryptographer, and Cognitive Engineer; across a number of Europe's most prolific Startups. For his work, Jack has been honoured with a number of accolades, including a Europe-wide entrepreneurship award. He has also acted as both a keynote and guest speaker at several prolific conferences, including the International Workshop on the Future Perspective of Decentralized Applications, held in conjunction with the 24th International European Conference on Parallel and Distributed Computing – where he also sat as a Program Committee member.

Before joining Oxford, Jack made a name for himself within both the Startup and Blockchain communities across Europe. This stemmed from his researching into privacy-enabling blockchain technologies, where he explored the application of advanced cryptographic mechanisms, such as: homomorphic encryption, differential privacy and secure multiparty computation – to distributed ledger ecosystems. In recognition for his efforts, Jack was invited to act as an Associate Editor at Frontiers Open Access Journal, where he curated his own section on the Fourth Industrial Revolution. In this role, Jack leads a team of seasoned academics, consisting of established professors and postdoctoral researchers.

Whilst at Oxford, Jack has been invited to act as an Expert Consultant on Blockchain Technologies by United Nations (UN) entities. As of 2019, Jack has committed to conducting research into a number of areas, including: cyber insurance, social engineering, and the development and application of deep fake technologies. To these ends, he is utilising his rich and diverse background, which branches across a broad array of areas within: insurance, artificial intelligence, cryptography and distributed ledger technologies.

Mini-Projects

Mini-Project 1: Understanding the Impediments of Creating a Precompetitive Dataset for Cyber Risk

Mini-Project 2: Deep Phishing

Sebastian Köhler

Sebastian started his research in Cyber Security during his undergraduate studies in Computer Science at the University of Applied Sciences Würzburg-Schweinfurt, Germany. Due to his interests in the security of cars, he completed his bachelor's degree with a dissertation at the research and development centre of the Dr. Ing. h.c. F. Porsche AG. Before his doctorate, he received a master's degree in Computing & Security and got awarded the prize for the best overall performance on the MSc in Computing & Security for the academic year 2017/18 from King's College London.

As a doctoral researcher in the Centre for Doctoral Training in Cyber Security at the University of Oxford, he focuses on automotive and embedded systems security. Currently, he is researching possible attacks against the communication between an electric vehicle and the charging station.

Sebastian's interest in Computer Science is not limited to his studies, he also likes to improve his knowledge and skills in his spare time by taking part in Capture the Flag Challenges, Hackathons and conferences.

Mini-Projects

Mini-Project 1: Interrupting the CCS Charging Communication using Radio Frequency Interference

Mini-Project 2: 2 Fast & 2 Furious: Exploiting High-Power Charging to Disrupt the Power Grid.

Arthur Laudrain

Arthur P.B. Laudrain (@APB_Laudrain) is a Rotary Global Scholar for Peace and a doctoral researcher in cybersecurity at Wolfson College. His current interests relate to norms of behaviour, defence policies and assessing states' military capabilities in cyberspace. In 2019, he joined the French Strategic Research Institute (IRSEM, Paris) as a Visiting Research Fellow and the International Institute for Strategic Studies (IISS, London) as a Research Assistant. He is part of the executive committee of Oxford's Strategic Studies Group. Arthur was educated at Université de Montréal (BSc), King's College London (MA) and Universiteit Leiden (LLM). His work has been cited by Martin Libiki and Barrie Sander, among others.

Publications:

Forthcoming and in progress

- *"Autonomous Weapons and the Law of Targeting: Categorising Use-Cases to Map Operational Constraints", International Review of the Red Cross, Digital Technology and War Special Edition. Revised and resubmitted.*
- *"Mapping the Known Unknowns of Cybersecurity Education: A Review of Syllabi on Cyber Conflict and Security", Journal of Political Science Education. With Trey Herr and Max Smeets. Revised and resubmitted.*
- *"French Cyber Security and Defence: Strategy, Policy-Making and Coordination", SSRN Working Paper Series. Available at: https://papers.ssrn.com/abstract=3432338*

Conference

"Military Cyber Operations: Comparative Approach of France and the UK", National Research Agency Cyber Studies Seminar, Université de Bordeaux, June 6th 2019.

"The French Counter-Disinformation Strategy and its Defence Toolkit", Oxford Policy Exchange Network (OPEN) Fellowship Series, St-Anthony's College, March 11th 2019.

Non-scientific articles

"France's New Offensive Cyber Doctrine", Cybersecurity and Deterrence, Lawfare, Washington DC, February 26th 2019. Available at https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace

"Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace", DayZero Cybersecurity Law and Policy, Lawfare, Washington DC, December 4th 2018. Available at https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

Media appearance

"Tactical Cyber Weapons For Future French Battlefield Ops?", Breaking Defense, June 2019. Available at: https://breakingdefense.com/2019/06/tactical-cyber-weapons-for-future-french-battlefield-ops/

"France Bolsters Cyber Capabilities and Commitment through New Doctrine", Jane's Intelligence Review – Military & Security Assessments Intelligence Centre, London, March 2019. Available at https://www.janes.com/images/assets/179/87179/France_bolsters_cyber_capabilities_and_commitment_through_new_doctrine.pdf

Mini-Projects

Mini-Project 1: French Cyber Security and Defence: Strategy, Policy-Making and Coordination

Mini-Project 2: Assessing Military Cyber Capabilities: Methodology, Challenges and Benefits to International Peace and Security

Matthew Rogers

Matthew is a 2018 Rhodes Scholar with a degree in software engineering from Auburn University. His experience includes work with Dynetics, an engineering firm, doing malware analysis and reverse engineering APT malware. Additionally he has spent time at the Defense Digital Service, bolstering their cyber capabilities. He has spoken at several conferences on malware analysis and cyber security education. His research focuses on creating cheap intrusion detection systems for serial data bus networks, primarily J1939. From this he hopes to build out mission assurance research for critical transportation and military systems.

Publications:

Speaker at the Association of Old Crows 55th Symposium panel on "Preparing EMS Superiority" : "Electronic Sheepdogs : Providing the Hacker's Mindset to Everyone"

Mini-Projects

Mini-Project 1: A State-Based Rules Framework for Serial Data Bus Networks

Mini-Project 2: Using Offensive Techniques for good on Serial Data Bus Networks

Yashovardhan Sharma

Yashovardhan has been fiddling with computers ever since he was a toddler. A penchant for testing the limits of what was possible given a computer system made him naturally inclined towards computer security.

He completed his MPhil in Advanced Computer Science from the University of Cambridge and his BTech (Honours) in Computer Science and Engineering from IIIT-Delhi. Having worked on projects ranging from Healthcare to Artificial Intelligence to Human Computer Interaction, his focus recently has been on the area of Privacy and Security, with an emphasis on Cryptography. During his sojourn at Oxford he hopes to design and build trusted systems that leak minimal information and are reasonably resistant to compromise.

The interdisciplinary and collaborative nature of the CDT is a key reason for Yashovardhan to have come to the "other place". Born and raised in India, he is also known for his ability to enjoy non-spicy food.

Mini-Projects

Mini-Project 1: Exploring the Impact of Availability in Secure Enclaves

Mini-Project 2: Analysing the Safety of Collision Avoidance Protocols for Aviation

Anjuli R. K. Shere

Anjuli (@AnjuliRKShere) is an analyst, writer, and researcher, with experience of journalistic and security-related investigations. While attending 'Particle Summer School' at CERN, she was inspired by the scientific progress created by global collaboration. She has since studied a BA (Hons) in Politics and International Relations at the University of Nottingham, and spent a year gaining a Certificate in Social Sciences and Humanities at Sciences Po, Paris.

During her master's degree in Science and International Security in the Department of War Studies at King's College London, Anjuli began reporting on current affairs for the New Statesman. She specialised in strategic security threats posed by emerging technological concerns, and wrote her dissertation on the extent to which machine learning could protect the NHS from cyber-attacks. Following this, Anjuli's professional roles included working as a conference and research analyst for the Association for International Broadcasting and as part of the SwiftTrace team, improving the quality of the analytical tools available for intelligence operations.

While enjoying her first year studying for her doctorate in Cyber Security at the University of Oxford, Anjuli has co-organised and emceed the CDT conference on Cyber Espionage and is also a member of the yearbook committee. However, her proudest recent achievements are being part of the team that topped the Capture The Flag leaderboard during a practical module and learning how to tap a communications cable. Currently, Anjuli has returned to her work as an intelligence analyst on Channel 4's fugitive simulation, 'Hunted'. She is also conducting cross-disciplinary research projects within the faculties of Law and Computer Science.

Publications:

https://www.newstatesman.com/writers/321610

Spoke at and reported on the 2018 International Political and Media Conference on Achieving Sustainability in Asia-Pacific (ASAP), http://asap90.rti.org.tw/wp-content/uploads/2018/09/CONFERENCE-WITH-NOTES-20SEPT2018-0926.pdf

Mini-Projects

Mini-Project 1: Now You [Don't] See Me: How have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations?

Mini-Project 2: Securing a Free Press inside a Networked Panopticon: The case of the Internet of Things

Julia Slupska

Julia Slupska is a Research Associate at the Digital Ethics Lab at the Oxford Internet Institute. Her research focuses on the ethical implications of conceptual models of cybersecurity. Currently, she is studying cybersecurity in the context of intimate partner violence and the use of simulations in political decision-making. Previously, she completed the MSc in Social Science of the Internet on the role of metaphors in international cybersecurity policy. Before joining the OII, Julia worked on an LSE Law project on comparative regional integration and coordinated a course on Economics in Foreign Policy for the Foreign and Commonwealth Office. She also works as a freelance photographer.

Publications:

Slupska, Julia and Mariarosaria Taddeo "Generative Metaphors in Cybersecurity Governance" (forthcoming), Yearbook of the Digital Ethics Lab 2019.

Slupska, Julia. "Safe at Home: Towards a Feminist Critique of Cybersecurity", St. Anthony's International Review, Whose Security is Cybersecurity?Authority, Responsibility and Power in Cyberspace, Volume 15, Issue 1, May 2019.

Chalmers, Damian and Julia Slupska. "The Regional Remaking of Trade and Investment Law." European Journal of International Law, Volume 30, Issue 1, February 2019, Pages 169–197, https://doi.org/10.1093/ejil/chz004

Presentations:

Slupska, Julia. "Designing IoT Security for Intimate Threats," (21 May 2019), London IoT Meetup Group.

Slupska, Julia, Romy Minko, Zhi Tan, Fatima Zahra and Marine Eviette. "Cybersecurity and Intimate Partner Violence" (2019) Map the System Research Competition. Also presented at Connected Life Conference 2019.

Slupska, Julia. "Towards a Feminist Critique of Smart Home Security Analysis" (9 March 2019), Oxbridge Women in Computer Science Conference.

Mini-Projects

Mini-Project 1: "We're All Happily Married Here!": Understanding Intimate Partner Abuse as a Cybersecurity Issue

Mini-Project 2: Simulations and Cybersecurity Policy-making

Claudine Tinsman

Claudine received her BA in Political Science (magna cum laude) from UC San Diego. During her time in California, she worked in a legal clinic, city government, and an international immigration law firm.

She holds a Master of Law (MLaw) in Legal Issues, Crime and Security of Information Technologies from the University of Lausanne. Her master's thesis examined the potential implications of treating intelligent agents as legally liable actors.
Her current research interests include the detection and prevention of cyber-enabled child sexual exploitation, as well as cyber harm propagation arising from threat intelligence sharing between organisations.

Publications:

Tinsman, Claudine. "Book Review: Bruce Schneier, Click Here to Kill Everybody: Security and Survival in a Hyper-connected World." St. Anthony's international Review, May 2019.

Forthcoming and in Progress

Tinsman, Claudine, Amaya Silva, Javier, New, Steven. Supply Chain Cyber Security Challenges in Industry 4.0. Manuscript in preparation.

Talks

"Social Engineering Attacks", Cyber Security Awareness Week, HSBC, May 20, 2019.

Mini-Projects

Mini-Project 1: A Universal Security Rating System for Mobile Apps: Preventing Today's Fraud From Becoming Tomorrow's Nightmare

Mini-Project 2: Personal Data: Implications for organisational threat intelligence communication under the GDPR

Fatima Zahrah

Fatima received a First Class BSc (Hons) degree in Computer Science from the University of Bradford. During her undergraduate studies, Fatima has worked on a variety of projects including an IBM project to create a smart house greeting system by using emerging cognitive technologies, including IBM Watson. For her DPhil, Fatima's research interests focus around online radicalisation. Her first mini-project will explore the comparability between the social engineering techniques used by different groups of extremists online, and investigate whether similar de-radicalisation strategies can be applied to different forms of radicalisation processes. Her second mini-project will aim to profile pro-extremist posts on Twitter through semantic analysis. This will be used to further investigate how counter-extremism campaigns can be made more effective by directly addressing the personality traits of those currently targeted and thus potentially more likely to fall victim to online radicalisation.

Mini-Projects

Mini-Project 1: Social Engineering in Online Extremism: A Comparison of Violent Jihadi and Far-right Radicalisation

Mini-Project 2: A computational analysis of extremist and counter-extremist content on social media

Alumni

Katriel Cohn Gordon

Katriel is a mathematician-turned-computer-scientist studying the theory of security protocols. His research has lately focused on messaging protocols, and in particular secure messaging as used by WhatsApp, Google Allo, Signal, Wire, and many other apps. For example, it turns out that WhatsApp's encryption lets you send secret messages even if your phone was compromised in the past; this isn't captured by traditional models, which consider that scenario to be a lost cause.

He's also interested in the public key infrastructure that powers the modern secure Internet, and has spent some time working with Google's Certificate Transparency team, as well as spending summers during his PhD interning with Google and Facebook. Before joining the CDT he did a masters' degree at Oxford, and worked as a data programmer in a hedge fund.

When not working (which is of course hardly ever), he enjoys fiddling with gadgets, reading the Internet, and -- when he can drag himself away from a computer -- fencing with the University team.

Katriel has joined Facebook as a Research Scientist, working on tools to improve users' privacy

Florian Egloff

Florian joined the DPhil in Cyber Security programme in 2013 as a Clarendon Scholar, and completed his DPhil in 2018. Florian was hosted at the Department of Politics and International Relations and supervised by Dr. Lucas Kello. His main research interest lies in the realm of cyber security in international relations. He researches non- and semi-state actors involved in cyber security and their impact on international politics. In his DPhil he explored a historical analogy to mercantile companies, privateers, and pirates, shedding light onto the blurred boundaries between state and private interests. Whilst at Oxford, in the technical domain Florian investigated malware, which had been delivered to the University of Oxford's network. He focused on what can be learnt about attackers' targeting behaviour.

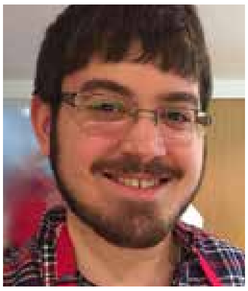
Florian now works as a Senior Researcher in Cybersecurity at the Center for Security Studies at ETH Zurich, Switzerland. Florian's current research projects focus primarily on the politics of public attribution, the role of non- and semi-state actors in cyber security, and the use of cyber intrusions for political purposes. In addition to his teaching and research activities, Florian provides strategic consultancy, expert advice, and training, including on cyber foreign policy, attribution, and cyber security, to public and private sector entities.

David Mellor

David is now a Senior Lecturer in Sociology at the University of South Wales. He also undertakes review and evaluation work for the European Commission for projects involving AI and robotics, and more generally in areas of technological innovation with potential social impacts.

David's research is about the moral, ethical, social and cultural aspects of developments in digital technologies. Current work looks at: AI and social policy; bias, exclusion and standardization in the automated revolution; social life with robots; theories of global technicity and how technology shapes the human. In addition to publishing from his Oxford research he is part of an EU consortium working on research involving citizens assemblies, with young people and experts in various fields, that bridge open science and democratic debate concerning the future of responsible AI.

Kevin Milner



Kevin is a Canadian with a BSc in computer science at the University of Alberta and an MSc in quantum information theory from McGill University. His DPhil work was with Cas Cremers, improving the tools used in formal analysis of protocols, as well as designing and formally analysing protocols that provide security guarantees even after key compromise.

Yudhistira Nugraha

Yudhistira Nugraha is an Indonesian civil servant for the Directorate of Information Security at the Directorate General of Informatics Applications, the Ministry of Communications and Information Technology.

After his study leave where he did his Doctoral work in Cyber Security at Oxford, Yudhistira is appointed as the Acting Head of Institutional Cybersecurity Section. He is currently working with European Union for GDPR Compliance and Awareness in Indonesia. He's actively involved in drafting Indonesia's proposed Personal Data Protection Law. He is also appointed as the member of TELSOM's working group on ASEAN Framework on Digital Data Governance.

His previous role before joining the Oxford Centre Doctoral Training in Cyber Security was Head of Information Security Management Section, where he oversaw Cybersecurity Governance and Policy in Indonesia. He had been worked as a delegation member for different regional and international forums, including ITU, ASEAN, ASEAN-Japan Information Security Policy Meeting, ASEAN Network Security Action Council, ASEAN Regional Forum on Cybersecurity/Cybercrime-related issues and the Asia Pacific Computer Emergency Response Team.

Before work for the government, he started his career as a Radio Access Network Engineer with the vendor and telecommunication operator in Indonesia. Yudhistira received a B.Eng. in Telecommunications Engineering from Telkom University, Bandung – Indonesia and a Master's Degree in Information and Communication Technology Advanced from the School of Computing and Information Technology at the University of Wollongong, Australia.

Emma Osborn

Emma's doctoral project focused on small-scale cyber security – cyber security for small organisations and individuals.

The growing concern over the standard of cyber security of individuals and small organisations highlights an imbalance in the way cyber security has developed to favour government and large companies. The project evaluated the small-scale cyber security ecosystem, who the stakeholders are and how they interact to achieve a level of security. The aim was to understand the different drivers within the system: establish what the need for cyber security is, where that need isn't being met and what measures might be best suited to improving the security of this sector.

Emma has started a training and Consultancy company, OCSRC Ltd., focussing on SMEs.

Vincent Taylor

Vincent is currently a Cyber Developer at Mishcon de Reya LLP. His job mainly involves consulting on cyber security matters, cyber threat intelligence and software engineering, but also includes digital forensics and research to a lesser extent. Vincent primarily works with the cyber intelligence analysts and cyber security consultants within MDR Cyber, but also consult for solicitors of Mishcon de Reya LLP when they are working on cyber-related cases.

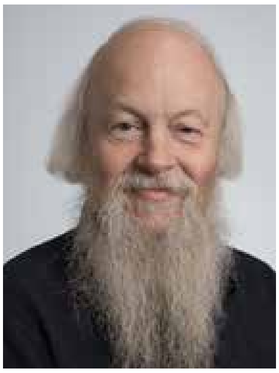
The Alumni network is continuing to expand – please see **www.cybersecurity.ox.ac.uk/alumni** for further details

The CDT Team

Andrew Martin – CDT Director

Professor of Systems Security, Department of Computer Science
An Oxford graduate, Andrew worked as a Software Engineer at Praxis in Bath, where he first encountered some of the challenges of information security and secure systems engineering in the late 1980s. After a DPhil back in Oxford, he escaped to the other side of the world to be a Research Fellow at the Software Verification Research Centre in the University of Queensland. Eventually the excellent weather and relaxed way of life got the better of him, and so he returned to the UK, and entered his current post in 1999.

The core of his research interest here has been in the security in distributed systems. Mostly of late that's been explored through looking at applications of hardware-based security controls – often described as Trusted Computing technologies - particularly as applied to cloud, mobile, and embedded applications (now known as the Internet of Things). His research group has been looking for the architectural elements and design patterns necessary to make trusted clouds and secure IoT a reality. These ideas have the potential to transform how we think about distributed systems and the security of the information they process.



Michael Goldsmith – CDT Co-Director

Senior Research Fellow, Associate Professor, Department of Computer Science
Michael Goldsmith is a Senior Research Fellow at the Department of Computer Science and Worcester College, Oxford. With a background in Formal Methods and Concurrency Theory, Goldsmith was one of the pioneers of automated cryptoprotocol analysis. His research work has investigated a range of Technology Strategy Board and industrial or government-funded projects ranging from highly mathematical semantic models to multidisciplinary research at the social-technical interface. He is an Associate Director of the Cyber Security Centre, Co-Director of the newly launched Centre for Doctoral Training in Cybersecurity and is active in the IAAC Academic Liaison Panel.

Lucas Kello – CDT Co-Director

Associate Professor of International Relations, Director of the Centre for Technology and Global Affairs, Department of Politics and International Relations
Lucas serves as Director of the Centre for Technology and Global Affairs, a major research initiative exploring the impact of modern technology on international relations, government, and society. His recent publications include The Virtual Weapon and International Order (Yale University Press), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft" in International Security, and "Security" in The Oxford Companion to International Relations (Oxford University Press).

Joss Wright – CDT Co-Director

Senior Research Fellow, Oxford Internet Institute

Joss Wright is Senior Research Fellow at the Oxford Internet Institute, where his research focuses on the analysis of information controls and their global development, and on the design and applications of privacy enhancing technologies.

Joss' work focuses on interdisciplinary approaches to the measurement and analysis of technologies that exert, subvert, or resist control over information. He has a particular interest in bridging the gaps between technically-focused analyses of security and privacy technologies, and their broader social and political implications.

In addition to his work on internet censorship, Joss also co-directs the Oxford Martin School's Programme on the Illegal Wildlife Trade, in which he researches the trade in illegal and unsustainable wildlife products online.

Maureen York – CDT Centre Administrator

Maureen has worked at the University since 1994, supporting and managing graduate training programmes. Maureen set up and managed the very first CDT programme in the UK in 2002 (Life Sciences Interface DTC) and has now set up five such programmes, the latest being the CDT in Cyber Security.

In addition to her work at the University, Maureen runs her own coaching, mentoring and retreat business and is a qualified mindset coach, specialising in the area of intuitive thinking and the nature of thought and how it impacts your experience of life.

Katherine Fletcher – CDT Industry Liaison Officer

Katherine is the Coordinator of Cyber Security Oxford, the University-wide network of cyber security researchers and practitioners. Her role in the CDT is to help connect students to the wider community of Oxford researchers, and to support matchmaking for research projects with industry or other external partners. Katherine has over 10 years' experience as a Project / Programme manager largely based in Oxford, specialising in large-scale, multidisciplinary research projects spanning academia and industry. Recent experience includes managing research projects in biomedical/computer science (linking pharma industry and academia), open-source software development projects (academic data management) and cybersecurity (multiple business sectors and academia).

Katherine received a BA in International Relations from William Jewell College (Liberty, Missouri, USA; 2001), and an MA in Global Political Economy from the University of Sussex (2004).

David Hobbs – CDT Programme Administrator

David joined the CDT in September 2013, just before the first cohort of students arrived. He is responsible for the day to day administration of the programme and acts as a first point of contact for admissions enquiries, on course students and our new alumni network. David has over 12 years of experience within Higher Education in several UK universities. Prior to moving to Oxford, David studied and worked at the University of York for a number of years.

Centre for Doctoral Training in Cyber Security
Dept of Computer Science
Wolfson Building
Parks Road
Oxford
OX1 3QD

cdt@cybersecurity.ox.ac.uk
01865 610644

UNIVERSITY OF OXFORD

CENTRE *for* DOCTORAL TRAINING *in* CYBER SECURITY

EPSRC
Engineering and Physical Sciences Research Council