Information Security as a Resource

Oxford University Department of Computer Science, 13 – 16 October, 2011

http://www.cs.ox.ac.uk/ISR11/

Abstracts of Talks

Resources in Cryptography

Ed Blakey

In previous work, the author has developed a framework within which to deal with the resources consumed during computational processes (adding to the familiar resources of *run-time* and *memory space* such non-standard resources as *precision* and *energy*); this framework provides various complexity-theoretic tools and techniques. Here, we seek an analogous treatment not of computational processes but of *cryptographic protocols* and similar, so as to be able to apply the existing complexity-theoretic tools and techniques in the derivation and verification of protocols in a wider information-theoretic context. Accordingly, we advocate a framework in which one may reason about the costs—which may be related to computation, communication, information (including side-channel information), availability of primitives, etc.—incurred when executing cryptographic protocols, coin-tossing schemes, etc.

Why Does Visual Analytics Work and What is the Underlying Theory?

Min Chen

In this speech, the speaker will first give a brief overview of the field of visual analytics, and outline the four dissertations of visual analytics. This is followed by a case study, which illustrates how visual analytics works in practice. The speaker then examines some theoretic frameworks proposed for visual analytics (not many), and discuss the information-theoretic framework in detail.

Structural Resources for Quantum Crypto

Bob Coecke

We investigate which physical properties underpin quantum cryptographic protocols. In particular, while it is often said that mutually unbiased bases are key to those, we show that for many protocols a stronger form is required, which boils down to basis structures forming a scaled bialgebra in the sense of `arXiv:0906.4725`. From a more foundational perspective, this strong form of complementarity seems to be tightly intertwined with quantum non-locality, which distinguished it from protocols such as BB84 which only require ordinary complementarity. This is joint work with Ross Duncan (Université Libre de Bruxelles) and Quanlong Wang (Beihang University, Beijing), and also draws from Anne Hillebrand's MSc thesis here at Oxford.

Creation vs. Conservation of Security

Simon Gay

If information security is a resource, where does it come from? Is it conserved, like energy? In the world of classical security analysis, cryptographic schemes typically derive their security from (unproven) assumptions about computational complexity and results focus on showing that security is conserved during manipulation and communication of keys and messages. Quantum key distribution systems, on the other hand, create secret keys from nothing, and proofs of their correctness have a different character. In my talk I will explore some ideas arising from this contrast.

Security as a Resource in Process-Aware Information Systems

Michael Huth

Process-aware information systems create, change, and maintain their data based on "business" processes and their management. Languages and tools for business processes management have been developed, and are widely deployed in industry and heavily researched in academia.

Up until recently, the emphasis of these models, tools, and their analysis has been on the control flow of processes and its consistency. But it is clear that research now shifts towards the study of data flow and of compliance of processes with regulatory or security policies.

Ideally, one would like to be able to compose control-flow models with resources that capture important constraints for compliance and security. These resources would not only lead to controlling run-time monitors, but they would also inform static analyses that could check the realizability of secure processes or generate repair advise for insecure processes.

We will therefore give an introduction to some security aspects of process-aware information systems. Then we will explore how a view of security as a resource may aid us in developing clean, transparent, and analyzable models of secure, process-aware information systems.

Preliminary results featured in this talk are joint work with Jason Crampton (Royal Holloway) and Jim Huan-Pu Kuo (Imperial College London).

The Expectation Monad

Bart Jacobs

The expectation monad captures measures and plays a role in security in the formalization of a probabilistic programming language for security proofs. In the talk the monad will be re-described via an abstract construction involving effect modules. It will be shown how it gives rise to probabilistic versions of classical results of Manes and Gelfand: algebras of the expectation monad are convex compact Hausdorff spaces, which are dually equivalent to Banach effect modules. Further, they lead to an algebraic re-formulation of Gleason's theorem.

Algebraic Foundations for Quantitative Information Flow

Pasquale Malacaria

Quantitative Information Flow sees confidential information as a resource and aims to measure its change due to possible observations of the system. Several mathematical ideas have been proposed as a basis for Quantitative Information Flow. Information theory, probability, guessability are the main ideas in most proposals. They aim to quantify how much information is leaked, how likely is to guess the secret and how long does it take to guess the secret respectively. We show how the Lattice of Information provides a valuable foundation for all these approaches; not only it provides an elegant algebraic framework for the ideas, but also to investigate their relationship. In particular we will use this lattice to prove some results establishing order relation correspondences between the different quantitative approaches. The implications of these results w.r.t. recent work in the community is also investigated.

From Classical Channels Towards Abstract Models of Computation

Mike Mislove

Logical Complexity in Security

Dusko Pavlovic

Shannon sought security against the attacker with unbounded computational powers: if an information source contains some information, Shannon's attacker will surely find that information. Diffie and Hellman refined Shannon's view of security by taking into account attacker's computational limitations. Computational complexity thus became the foundation of modern cryptography.

However, although the attacker is not viewed as an omnipotent computer any more, he is still viewed as an omnipotent programmer: if there is an attack algorithm that might exploit a vulnerability, the Diffie-Hellman attacker will surely find that algorithm. Indeed, a system is deemed insecure as soon as an attack algorithm exists, not taking into account how hard it may be for the attacker to construct that algorithm. But some algorithms may be computationally easy to run, but logically complex to program. This distinction is abstracted away from the current attacker models. The Diffie-Hellman step from unbounded to bounded computational powers in security models has not been extended into a step from unbounded to bounded logical powers.

Can we formalize a suitable notion of logical complexity, to measure how hard it is to construct an algorithm, and in particular an attack algorithm? Can logical complexity be used as a security tool?

Trust as a Resource

Peter Ryan

Security-critical systems must be trustworthy but they also need to be trusted. This is especially true of secure voting systems, where the entire electorate should, ideally, understand and trust the security mechanisms. Significant progress has been made in recent years in developing verifiable voting systems,

but to date very little uptake. A major obstacle is the lack of understanding of the goals and mechanisms. Paradoxes arise like the fact that verifiable/fully-auditable schemes that are designed to detect any malfunction and corruption may in fact undermine trust. Focus groups suggest that many voters prefer not to even contemplate the idea that things could go wrong. Thus greater trustworthiness may actually run counter to promoting trust.

In this talk I will outline the idea of verifiable voting and discuss how some of the design choices may impact both trustworthiness and trust.

Min-Entropy as a Resource

Geoffrey Smith

The secrecy of certain values (such as sender identities, keys, and nonces) is crucial to the achievement of various security goals. We can view this secrecy as a "resource" that may gradually be "consumed" by information leaks in a system. Let a secret S be modeled as a random variable with some *a priori* distribution, assumed publicly known. *Min-entropy* measures S's secrecy based on its *Bayes vulnerability* to be guessed correctly in one try by an adversary. If a system manipulates S and produces an output O, then the amount of secrecy "consumed" can be defined as the amount by which observing O decreases S's min-entropy. In this talk, we explore the intuition of min-entropy as a resource, in both deterministic and probabilistic systems. We focus on compositionality results that bound the amount of leakage of a compound system based on the leakage of its components, showing for example that n repeated independent runs, using the same value of S each time, leak at most $\mathcal{O}(\log n)$ bits; we apply this result to the scenario of timing attacks against blinded cryptography. We deal mostly with the "static" perspective of leakage averaged over all runs, but also comment on the "dynamic" perspective of leakage in a single run.

Bridging the Gap between Two Views of Security

Bogdan Warinschi

Cryptography can be viewed as a hierarchical structure where complex cryptosystems are built from lesser resources, e.g. cryptographic primitives. Existing approaches for rigorous analysis of cryptographic schemes define the "amount" of security provided by the building blocks in essentially two different ways. In symbolic models security is an all or nothing property that holds against non-deterministic adversaries. In computational models security holds only probabilistically and is assessed against polynomially bounded adversaries. In this talk I will discuss a research direction that attempts to reconcile these two views. It turns out that, under the right assumptions, symbolic models are faithful with respect to the computational models. If time permits I will also discuss some recent progress on compositionality issues that arise naturally within this research area.

Winning Strategies in Concurrent Games

Glynn Winskel

In this talk I will present recent results on concurrent games with winning conditions. These model two-party games in which a Player (or a team of players) compete against an Opponent (a team of opponents), possibly in a highly distributed fashion. As usual the dichotomy Player vs. Opponent stands for a variety of situations such as Process vs. Environment, or Proof vs. Refutation. Both games and nondeterministic concurrent strategies are represented by event structures with an extra function expressing the polarity (the Player/Opponent nature) of each event. Winning conditions specify those plays for which Player wins. Winning strategies compose and conditions are given for copy-cat strategies to be winning. The result is a bicategory rich in structure and (largely unexplored) modelling power.