

Context-Sensitive Requirements and Risk Management with IRIS

Shamal Faily and Ivan Fléchais
 Computing Laboratory, University of Oxford
 Email: {shamal.faily, ivan.flechais}@comlab.ox.ac.uk

The Problem Many secure systems are not designed for their environments; defending against attacks in one context does not guarantee success in another. Risk analysis can supplement security requirements, but reasoning about assets, threats, and vulnerabilities in different contexts of use is hard.

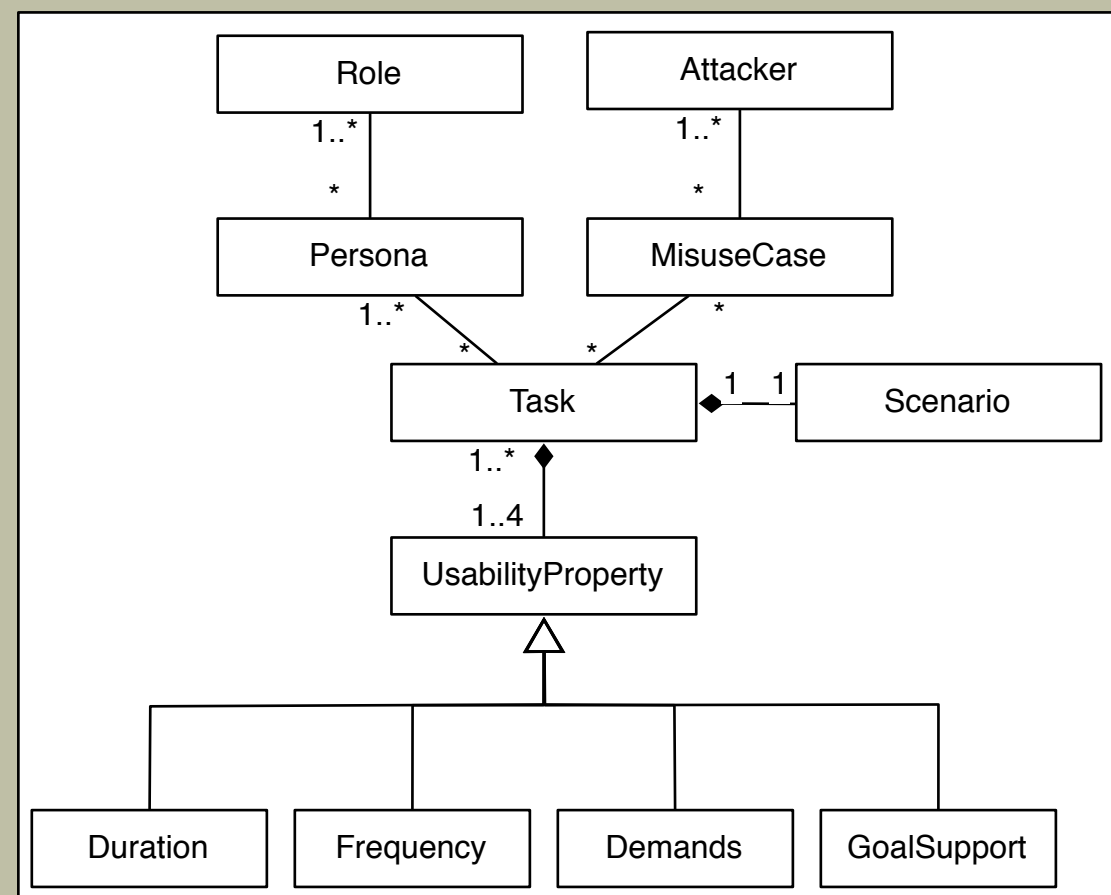
Our Approach IRIS (Integrating Requirements and Information Security) is a framework for designing secure and usable systems. IRIS consists of a meta-model integrating the notion of environment with concepts from requirements and risk management, together with tool-support.

- The IRIS meta-model consists of 4 sub-models, bound together in a common environment.
- Each sub-model relates to a different view of the context of use.

The IRIS Meta-Model

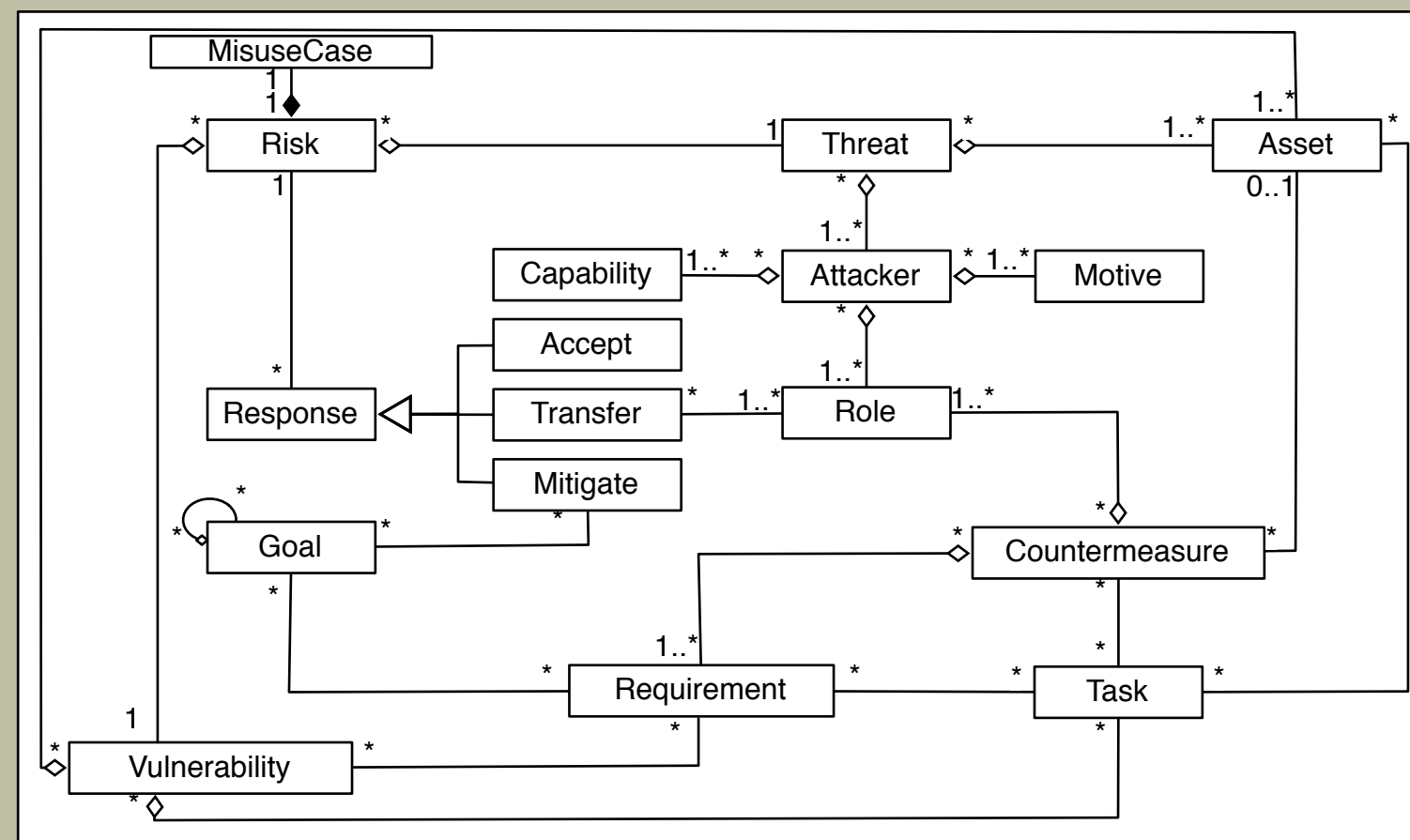
Task Sub-Model

- Tasks and scenarios model work performance.
- Properties relate task usability to *personas*.
- Misuse cases* [6] validate rather than elicit risks.



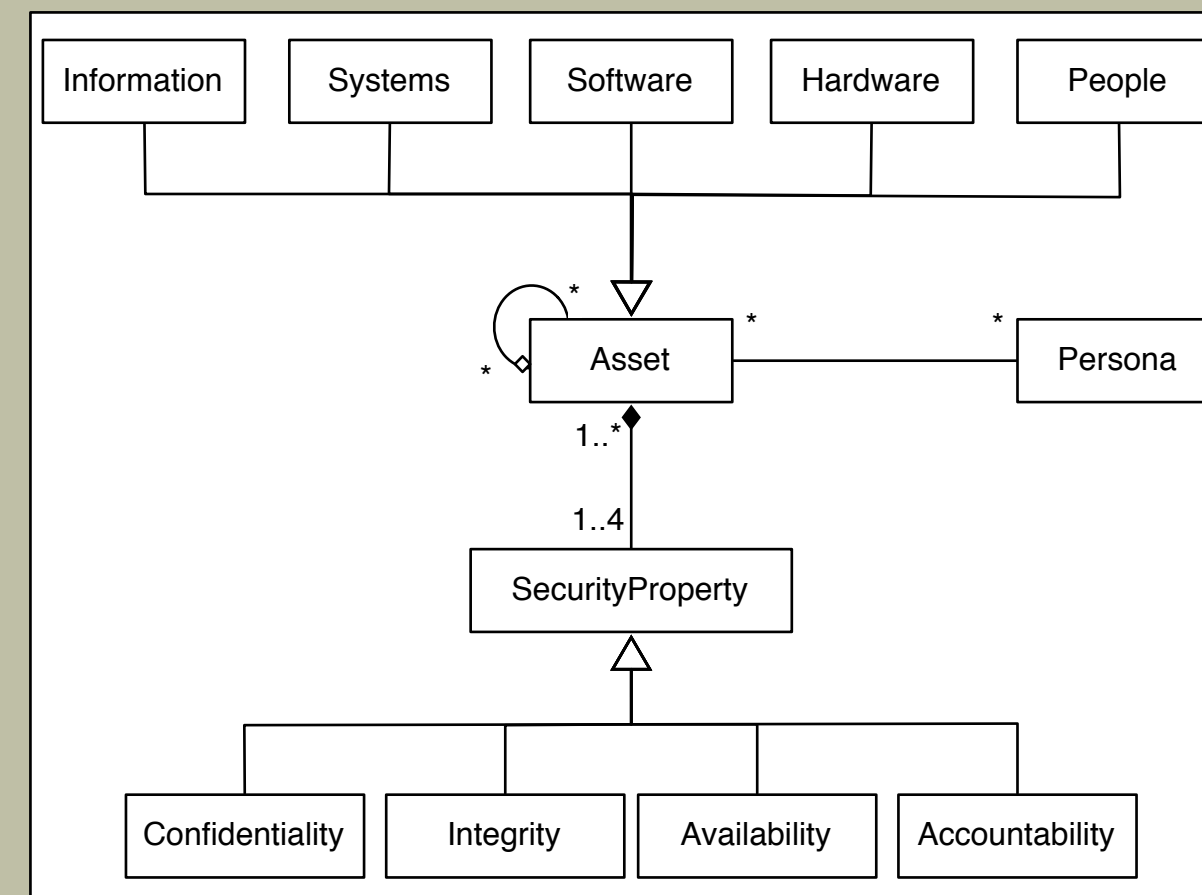
Risk Analysis Sub-Model

- Attackers are modelled as well as threats.
- Asset, threat, and countermeasure properties facilitate risk scoring.
- Roles capture responsibilities.



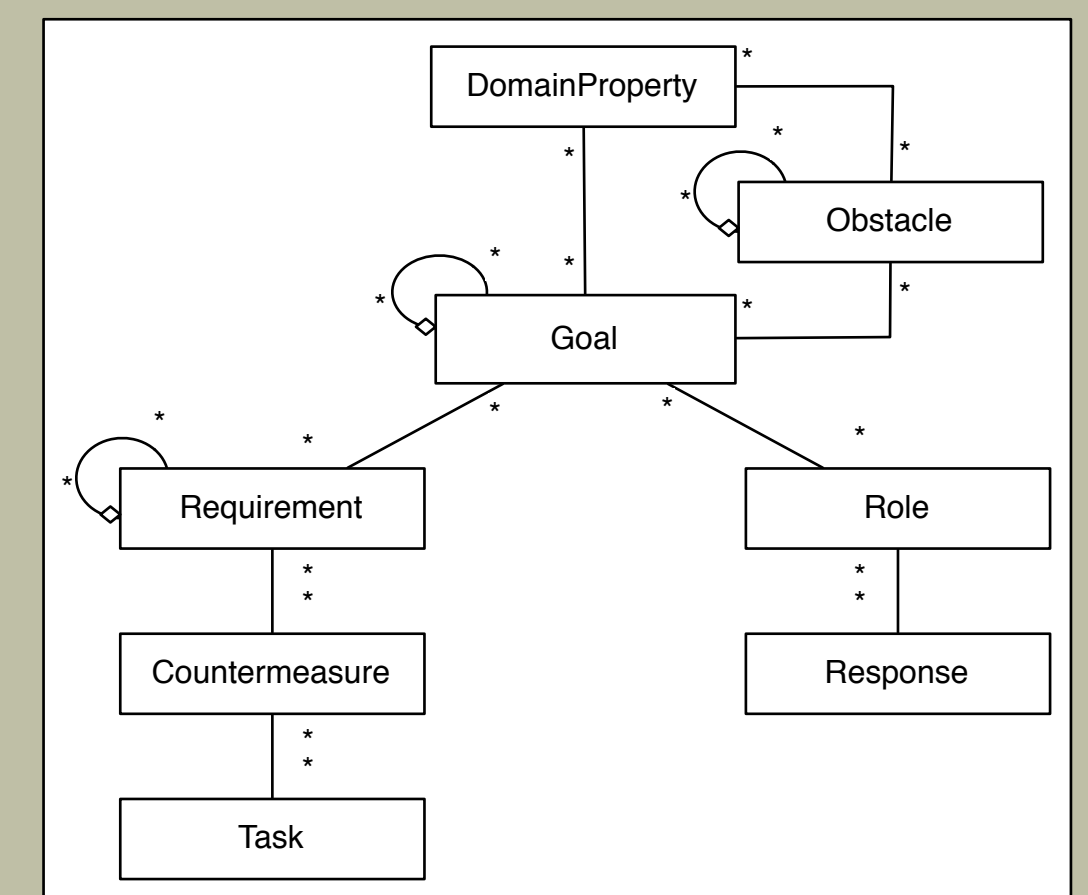
Asset Sub-Model

- Asset types inspired by OCTAVE [1].
- Multiple security properties explore asset values.
- Assets used by *personas* rather than users.



Goal Sub-Model

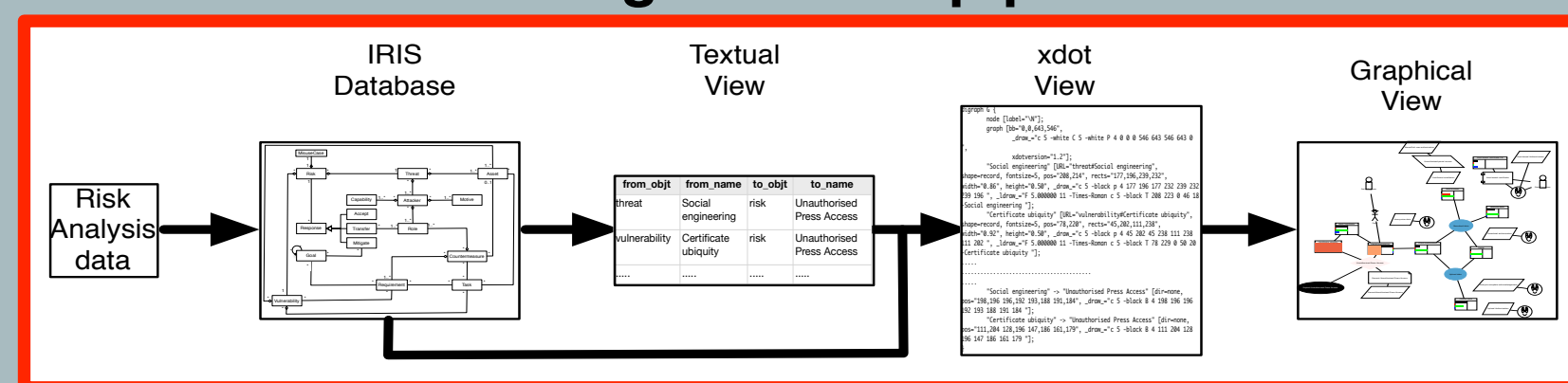
- Goals are boundary objects.
- Goal and *obstacle* refinement elicit risks and their responses.
- Goal sub-model based on KAOS [2].



- IRIS also includes a requirements & risk management tool.
- Provides explicit support for usable security design.
- Asset, Task, Goal, and Risk Analysis models automatically generated.

Tool-Support

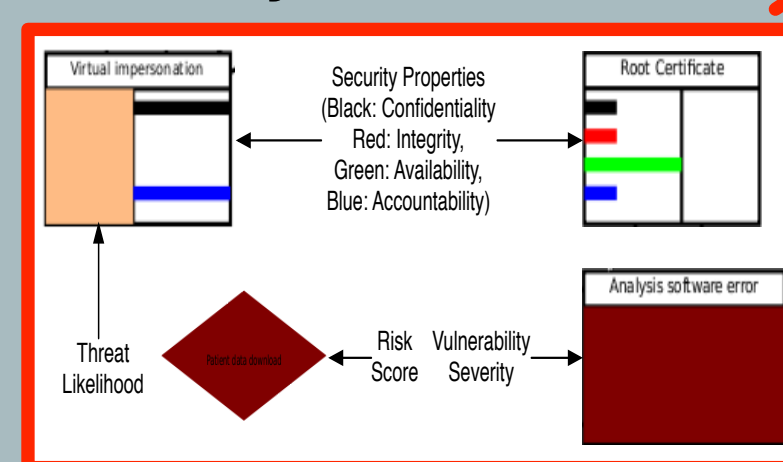
Model generation pipeline



IRIS User Interface

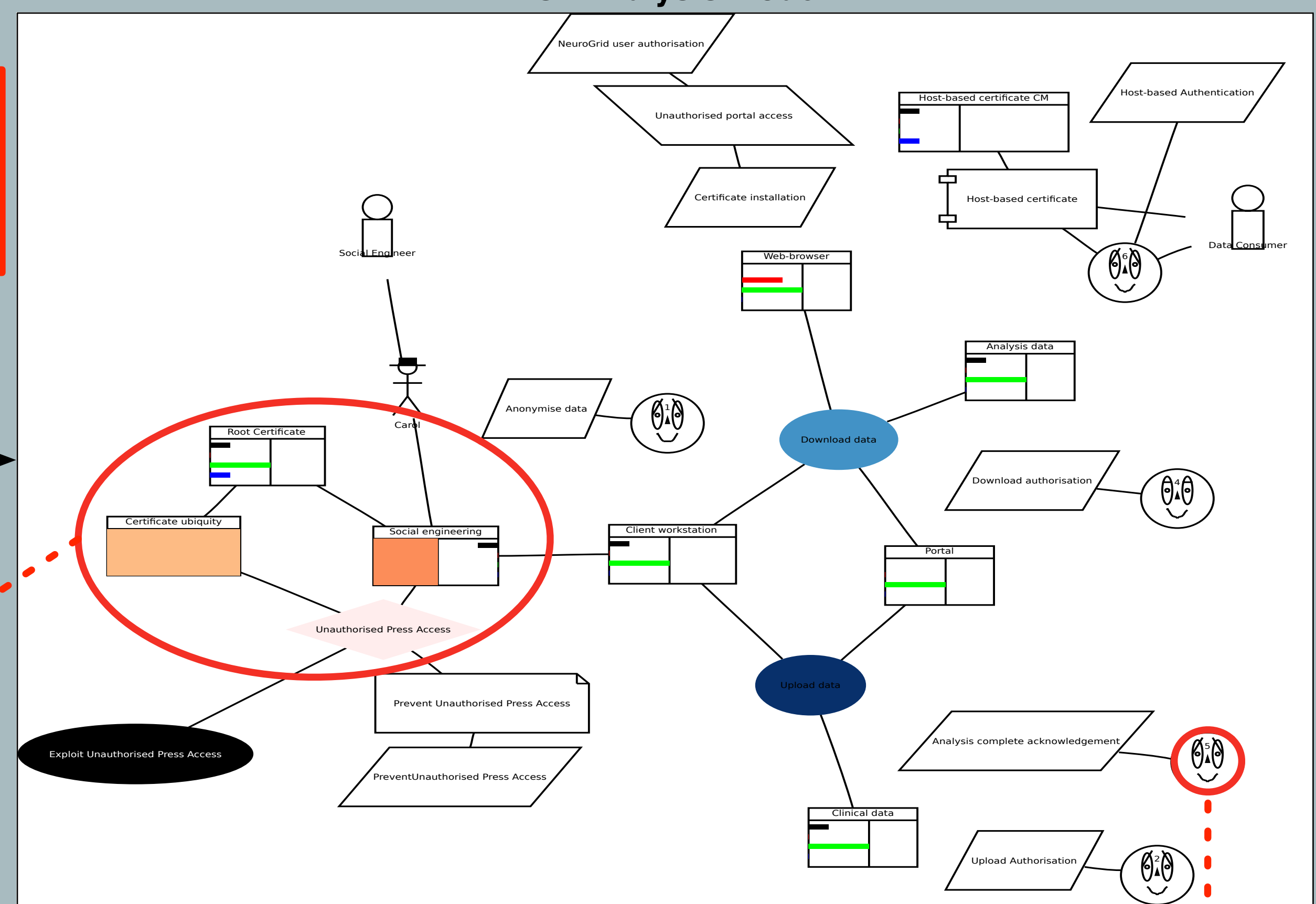
Description	Priority	Rationale	Fit Criterion	Originator	Type
All data destined for NeuroGrid shall be anonymised according to external...	1	Patient and volunteer confidentiality.	A sample of data on NeuroGrid shall be anonymised according to external...	Goal model	Security
Data submitters shall be registered as such on the access control policy for the...	1	Data integrity	Not possible for guest users to upload data.	Goal model	Security
Access to the NeuroGrid shall only be permitted if a root certificate has been...	1	Only authorised users can access NeuroGrid.	Not possible to access NeuroGrid from a workstation where a root certificate isn't...	Goal model	Security
Data downloaders shall be registered as such on the access control policy for the...	1	Only authorised users can access analysis data.	TBC	Goal model	Security
When data analysis is complete, an email shall be sent to the data submitter informing...	1	Useful reminder for submitters.	Email acknowledgement received after a simple job completes.	Goal model	Functional
A host-based authentication method shall supplement root key access to the...	1	Provide defence in depth if a root certificate is...	Attempts to login to the NeuroGrid portal with credentials not possible from any...	Goal model	Security

Security artifact colours



- The Risk Analysis Model is a quick-look view of the current risk analysis.
- Nodes and associations are generated automatically.
- Risk analysis artifacts are colour coded to quickly visualise their properties.

Risk Analysis Model



- Requirement quality is visualised by Chernoff Faces [3].
- Quality is assessed by:
 - requirements completeness,
 - the presence of an imperative mood phrase,
 - lack of ambiguity [7].

	😊	😐	😞	😡
Complete	✓	✗	✗	✗
Imperative	✓	✓	✗	✗
Unambiguous	✓	?	?	✗

References

[1] Alberts, C.J., Dorofee, A. J., *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley, Boston, 2002

[2] Dardenne, A., van Lamsweerde, A., Fickas S., Goal-Directed Requirements Acquisition. *Science of Computer Programming* 20, 1993, pp. 3 - 50

[3] Chernoff, H., The Use of Faces to Represent Points in K-Dimensional Space Graphically. *Journal of the American Statistical Association* (1973), p. 68

[4] Fléchais, I., Mascolo C., Sasse, M.A., Integrating Security and Usability into the Requirements and Design Process. *International Journal of Electronic Security and Digital Forensics* 1, 2007, pp. 12-26

[5] van Lamsweerde, A., Letier E., Handling Obstacles in Goal-Oriented Requirements Engineering. *IEEE Transactions on Software Engineering* 26 (10), 2000, pp. 978-1005

[6] Sindre, G., Opdahl L., Eliciting Security Requirements with Misuse Cases. *Requirements Engineering* 10 (1), 2005, pp. 34-44

[7] Wilson, W., Rosenberg, L., Hyatt L., Automated Quality Analysis of Natural Language Requirement Specifications. *Proceedings of Fourteenth Annual Pacific Northwest Software Quality Conference*. 1996

Acknowledgements

This research was funded by the EPSRC CASE Studentship R07437/CN001.

We are also grateful to Qinetiq Ltd for their sponsorship of this work.