The Problem

Many secure systems are not designed for their environment; 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

- 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.
- Task Sub-Model: Tasks and scenarios model work performance. Properties relate task usability to personas.
- 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].

Tool-Support

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

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.

Model generation pipeline

- 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].

References


Acknowledgements

This research was funded by the EPSRC CASE Studentship R074377/ CN001. We are also grateful to Qinetiq Ltd for their sponsorship of this work.