Security through Usability: a user-centered approach for balanced security policy requirements

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

The Problem
Information Security policies need to respond to evolving threats without over-specifying security.
There is a noticeable lack of support for writing security policies which balance security and usability.

The Solution
Make policy development user-centric by applying User-Centered Design [1,2].
Augment User-Centered Design with complementary techniques & tools from Information Security and Requirements Engineering [3,4,5,6].

Our Approach
1. Agree Scope
   Agree policy scope and affected users.
2. Fieldwork
   Collect and analyse data about users’ day-to-day work.
3. Usability Analysis
   Build personas representing archetypical users, and scenarios about their work.
4. Requirements Analysis
   Model the policy as a goal tree. Elicit and refine models, and identify mitigating requirements.
5. Vulnerability Analysis
   Elicit vulnerabilities from fieldwork data and revise models accordingly.
6. Threat Analysis
   Identify convincing attackers & threats from fieldwork data, and revise models accordingly.
7. Risk Analysis
   Model unmitigated risks using Misuse Cases, and agree policy resolutions.

Preliminary Results
✓ Eliciting policy requirements for SCADA and Control Systems used by plant operations staff at a UK water company.

1. The policy scope was agreed & modelled using a Rich Picture Context Diagram.
2. We visited 4 different water treatment plants, interviewing plant operators, and other staff. A conceptual model of plant security was developed from a qualitative data analysis of the collected data.
3. Using the results of the qualitative data analysis, a plant operator persona (Rick), and several task scenarios were elicited.
4. Based on the collected data & documentation, 102 policy goals, 8 roles, and 18 assets. Based on obstructing policy goals alone, several vulnerabilities and threats were identified and mitigated.
5. Based on the usability analysis data, 8 vulnerabilities were identified, 3 of which were mitigated at this stage.
6. Collected and open-source data helped identify 4 convincing attackers, and 8 possible threats.
7. Finally, the most topical risks were modelled as Misuse Cases, analysed, and mitigated in participatory design workshops.

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.

References