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

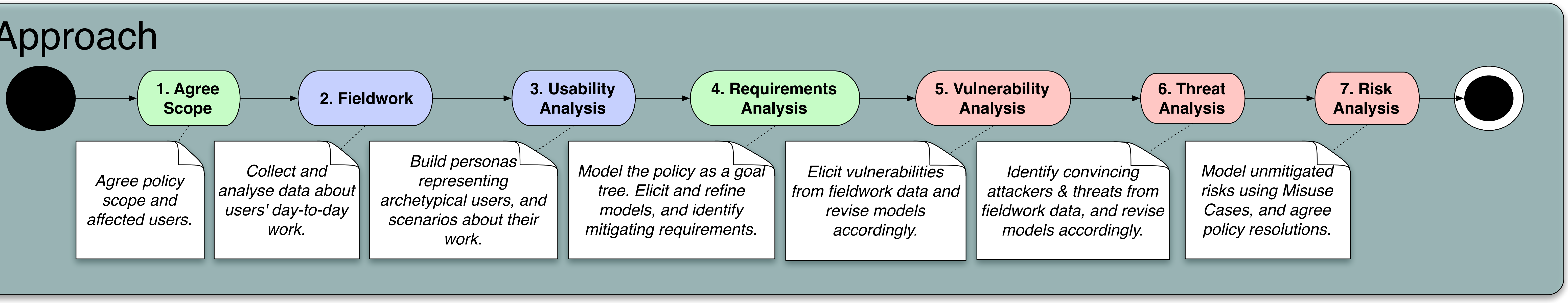
The Problem

- 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.

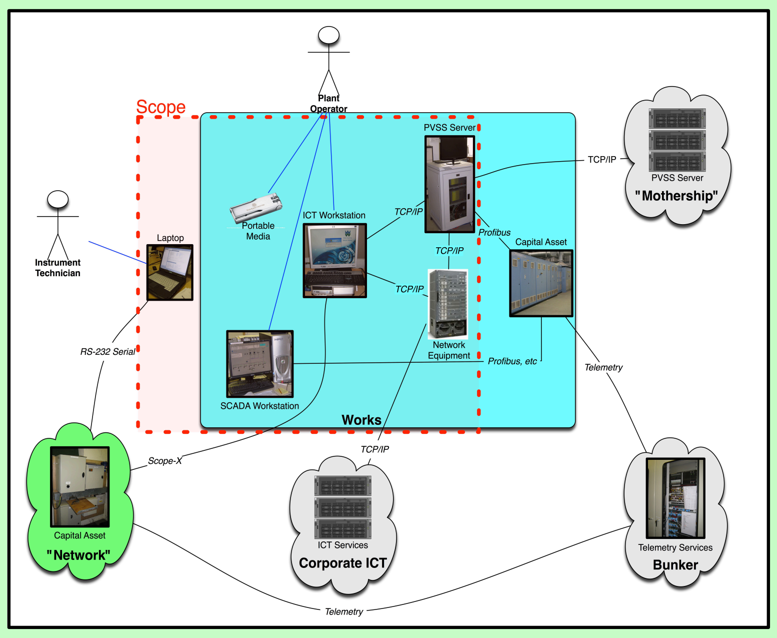
6. Threat Analysis: Identify convincing attackers & threats from fieldwork data, and revise models accordingly.

7. Risk Analysis: Model unmitigated risks using Misuse Cases, and agree policy resolutions.

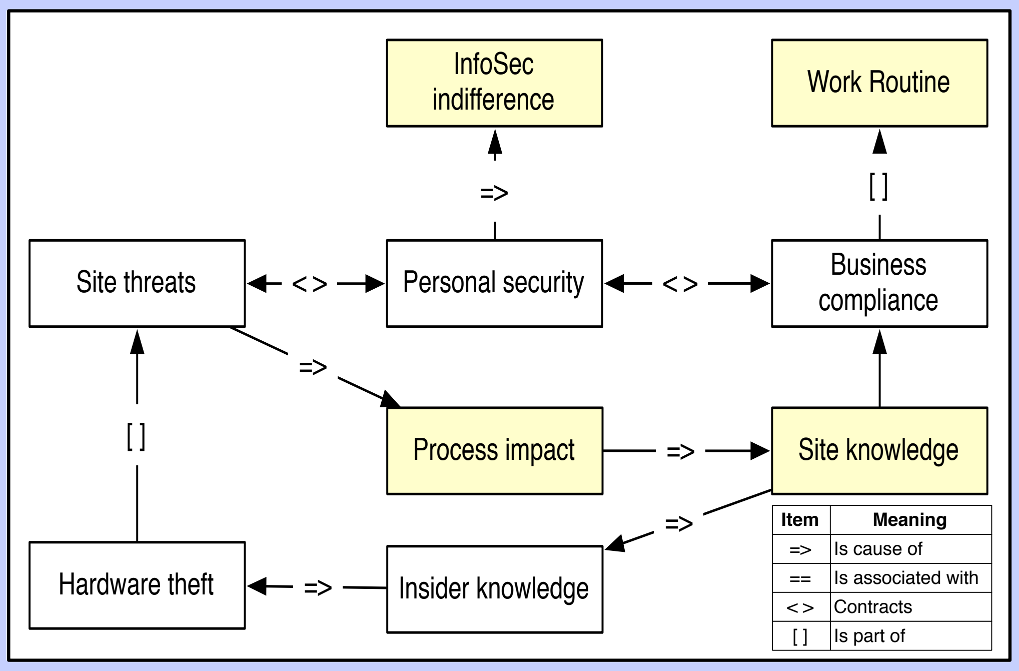
Preliminary Results

✓ 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.

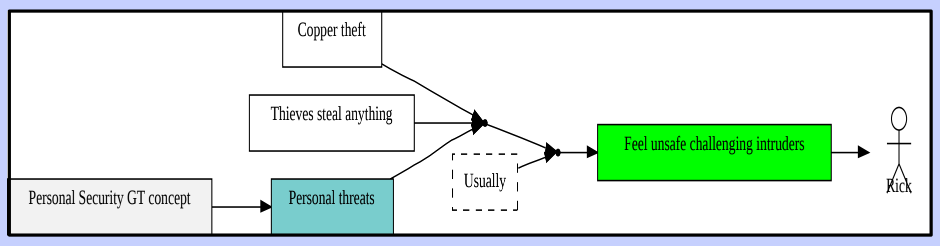


2. We visited 4 different water treatment plants, interviewing plant operators, and other staff. A conceptual model of plant security was developed from a qualitative data analysis of the collected data.



Item	Meaning
=>	Is cause of
==	Is associated with
< >	Contracts
[ ]	Is part of

3. Using the results of the qualitative data analysis, a plant operator persona (Rick), and several task scenarios were elicited.

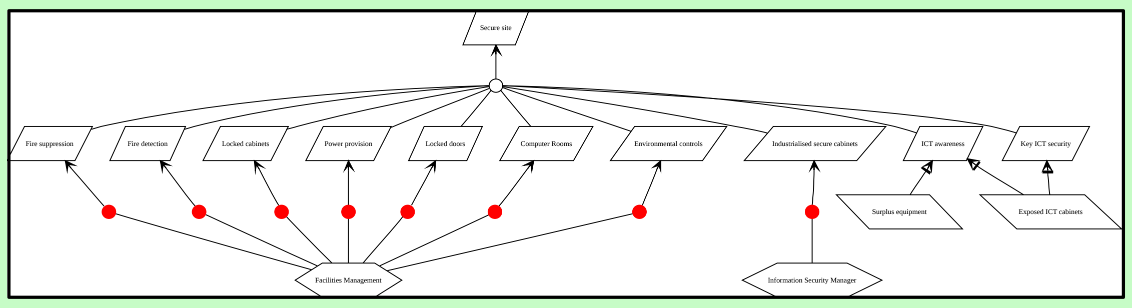

Copper theft
Thieves steal anything
Personal Security GT concept
Personal threats
Usually
Feel unsafe challenging intruders
Rick

Although information security doesn't phase Rick too much, personal security does. Potentially facing off a scrap metal thief is a big worry for Rick.
"The police don't respond to intruder alarms at a nearby pumping station any more due to false alarms", says Rick.
"Because of this, we've been told not to go out to these places on our own.
We have a lone-worker system when people call us when we get to a particular station, but what happens if we get problems on the way?"

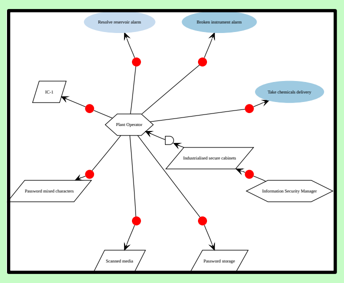
Motivation details about Rick, a plant operator persona.

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.

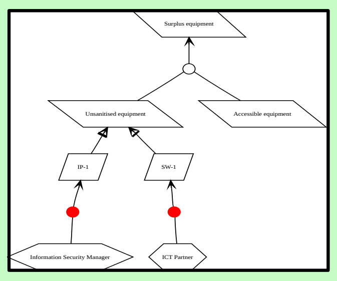
Goal Models



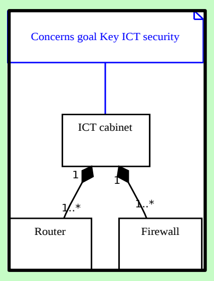
Responsibility Models



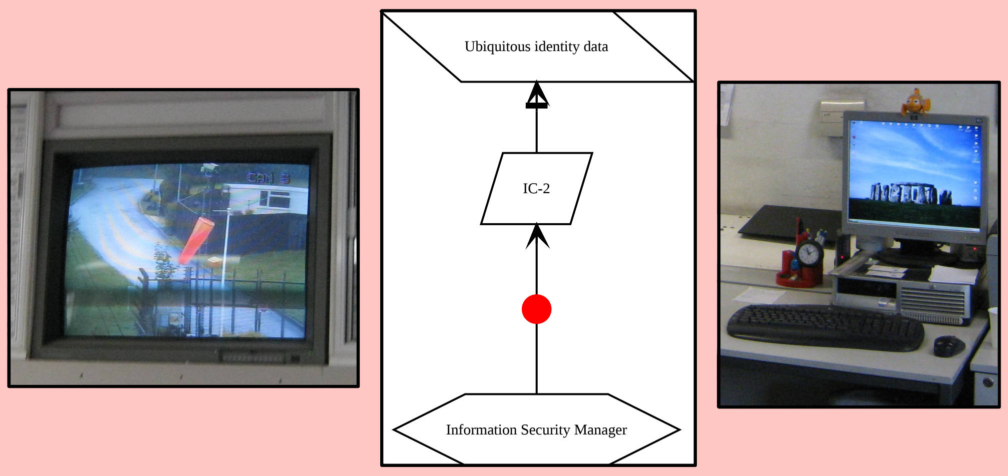
Obstacle Models



Asset Models

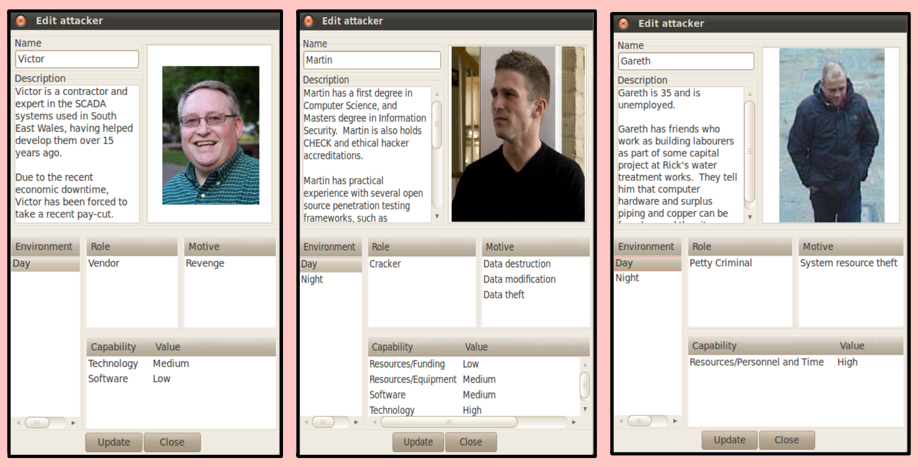


5. Based on the usability analysis data, 8 vulnerabilities were identified, 3 of which were mitigated at this stage.



Data contributing to ubiquitous identity vulnerability, and mitigating requirement.

6. Collected and open-source data helped identify 4 convincing attackers, and 8 possible threats.



Edit attacker
Name: Victor
Description: Victor is a contractor and expert in the SCADA systems used in South East Wales, having helped develop them over 15 years ago.

Due to the recent economic downtime, Victor has been forced to take a recent pay-cut.

Environment	Role	Motive
Day	Vendor	Revenge

Capability	Value
Technology	Medium
Software	Low

Edit attacker
Name: Martin
Description: Martin has a first degree in Computer Science, and Masters degree in Information Security. Martin is also holds CHECK and ethical hacker accreditations.

Martin has practical experience with several open source penetration testing frameworks, such as

Environment	Role	Motive
Day Night	Cracker	Data destruction Data modification Data theft

Capability	Value
Resources/Funding	Low
Resources/Equipment	Medium
Software	Medium
Technology	High

Edit attacker
Name: Gareth
Description: Gareth is 35 and is unemployed.

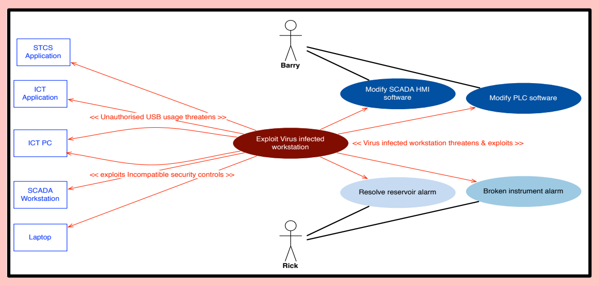
Gareth has friends who work as building labourers as part of some capital project at Rick's water treatment works. They tell him that computer hardware and surplus piping and copper can be

Environment	Role	Motive
Day Night	Petty Criminal	System resource theft

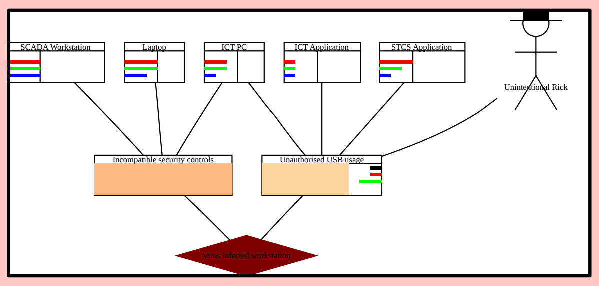
Capability	Value
Resources/Personnel and Time	High

Inside attacker (left), penetration tester (centre), and petty thief attacker profiles

7. Finally, the most topical risks were modelled as Misuse Cases, analysed, and mitigated in participatory design workshops.



Task (left) and Risk Analysis (right) model of virus-infected workstation risk



References

[1] Faily, S., and Fléchais, I. Barry is not the weakest link: Eliciting Secure System Requirements with Personas. *Proceedings of the 24th British HCI Group Annual Conference on People and Computers*, 2010, 113–120

[2] Faily, S., and Fléchais, I. The secret lives of assumptions: Developing and refining assumption personas for secure system design. *Proceedings of the 3rd Conference on Human-Centered Software Engineering* (2010),111–118

[3] Faily, S., and Fléchais, I. Towards tool-support for Usable Secure Requirements Engineering with CAIRIS. *International Journal of Secure Software Engineering* 1 (3), 2010, 56–70

[4] CAIRIS web site. http://www.comlab.ox.ac.uk/cairis

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

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

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.