Improving Secure Systems Design with Security Culture

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

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.

Sub Cultures

Perceptions vary between sub-cultures

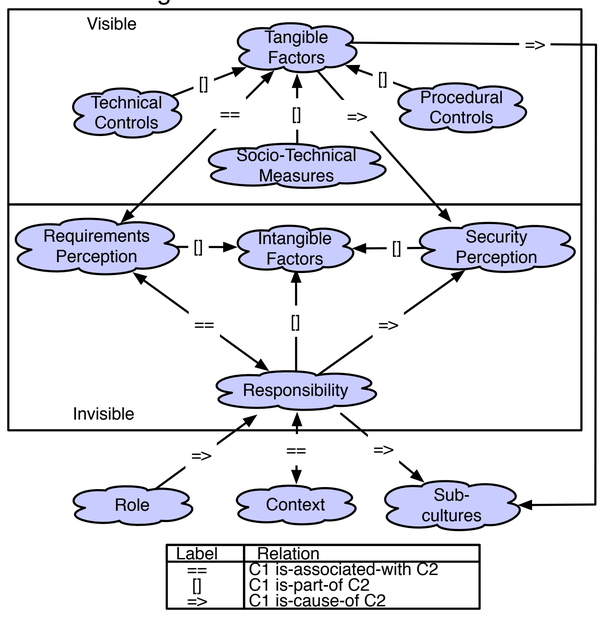
Norms and values evident when describing tasks and controls.

? A system which is secure and usable in one culture may not be in an another.

A conceptual model of Security Culture can provide guidelines for informing secure systems design.

Security Culture

The combination of *tangible* and *intangible* factors within an organisation's culture and its subcultures.



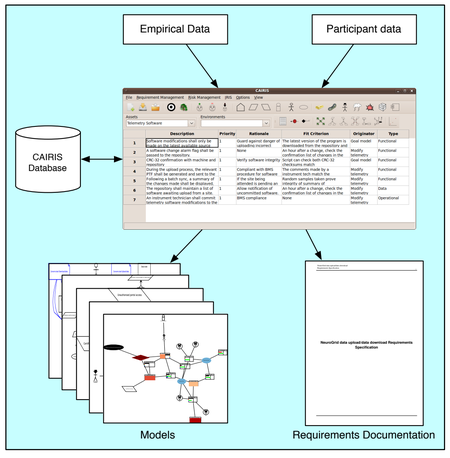
Label	Relation
==	C1 is-associated-with C2
[]	C1 is-part-of C2
=>	C1 is-cause-of C2

Secure Systems Design

IRIS (Integrating Requirements and Information Security) is a framework for usable secure systems design.

This framework incorporates:

- ✓ A user-centered design process
- ✓ Integrated tool-support

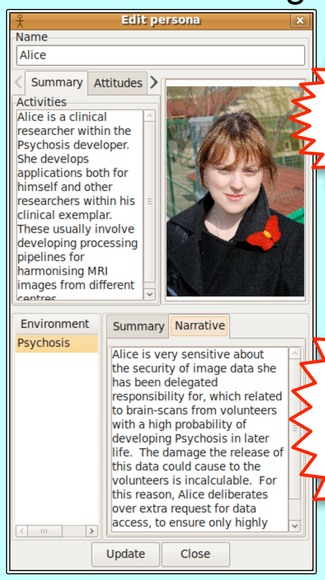


Requirements Perception

Implicit requirements cement security values.

Indifference towards requirements leads to ambiguity

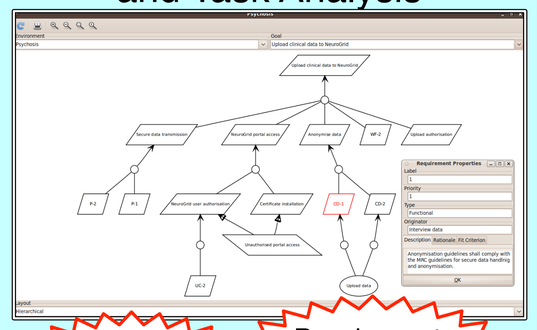
Personas and User-Centered Design



Personas are specifications of archetypical users

Contextual Inquiry used to elicit persona, task, and environment data

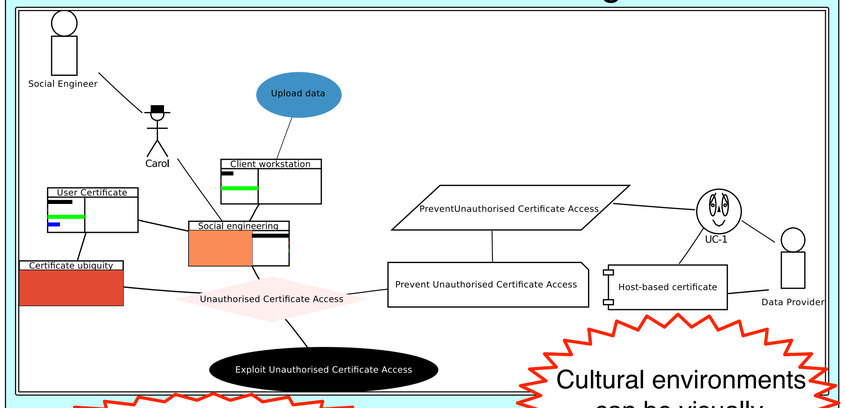
Goal, Requirement, and Task Analysis



Requirements quality validated using Chernoff Faces

Requirements traceable to functional,security, or usability goals

Environment Modelling



Role-Responsibility relationships tracked

Cultural environments can be visually modelled

Roles & Responsibility

Security perceptions strengthen or weaken security culture

Clearly defining responsibilities increases security perception

Elaborate role & responsibility taxonomies

Context

Shaped by controls and values.

Operational and Cultural Contexts

Ambiguous affordances affect security perception