Making the invisible visible
A theory of security culture for secure and usable grids

S. Faily    I. Fléchais

Computing Laboratory
University of Oxford

UK e-Science All Hands Meeting 2008
Introduction

Why Security Culture

- Values conflict.
- Existing understanding based on inappropriate contexts.
- Tools are value-free and not contextualised.
Method

2. Comparative model derived from empirical data.
3. Theoretical and empirical models applied to a secure design process.
Case Studies

NeuroGrid

• A grid based collaborative research environment [Geddes et al, 2006].
• 3 clinical exemplars: Stroke, Dementia and Psychosis.
• Data both sensitive and distributed.
Case Studies
Security Development Lifecycle

- A software development process for developing secure software [Howard and Lipner, 2006, Microsoft Corporation, 2008].
- Prescriptive: guidance for all stages of the secure software development lifecycle.
What is Security Culture?

A combination of tangible and intangible factors within both an organisation’s culture and its subcultures.

<table>
<thead>
<tr>
<th>Label</th>
<th>Relation</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td>C is-associated-with C2</td>
</tr>
<tr>
<td>[]</td>
<td>C1 is-part-of C2</td>
</tr>
<tr>
<td>=&gt;</td>
<td>C1 is-cause-of C2</td>
</tr>
</tbody>
</table>

- Tangible Factors
  - Technical Controls
  - Socio-Technical Measures
  - Procedural Controls
  - Security Policy

- Intangible Factors
  - Sub-culture norms
  - Socialisation
  - Compliant Behaviour
  - Security Perception
  - Responsibility
Guideline 1
Have a single, visible, security policy

- Statements of management intent.
- Multiple forms of procedural control lead to multiple security perspectives.
- Reliance on social networks in lieu of visible policies.
• Socialisation is the process of developing culturally acceptable beliefs, values and behaviours [Brown, 1998].
• Certificate installation as a rite of passage.
• Compliance and socialisation synonymous in the SDL.
• Literature: organisational and moral responsibility.
• NeuroGrid: various and split between technical controls and assets.
• Ambiguity identified by modelling lines of responsibility before implementing a security policy.
• Evident in NeuroGrid when asking users to describe how data was handled.

• Diffusion of Responsibility [Darley and Latané, 1970].

• Understanding values helps to determine whether security will be sacrificed for operational goals.
Future work

Value Sensitive Design and the design process

- Identifies *impacting human values* and integrates them into the design process.
- Supplements existing design processes.
- Precedents in secure and usable design [Friedman et al., 2002, Friedman et al., 2005, Friedman et al., 2006]
Future work

Augmenting Value Sensitive Design

- Conceptual Investigation.
  - Augment with additional values.
- Empirical Investigation.
  - Responsibility modelling.
- Technical Investigation.
  - Implications of augmenting the approach.

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have a single, visible security policy</td>
<td>Compliant Behaviour</td>
</tr>
<tr>
<td>Leverage socialisation</td>
<td>Socialisation</td>
</tr>
<tr>
<td>Model lines of responsibility</td>
<td>Responsibility</td>
</tr>
<tr>
<td>Understand your subcultures</td>
<td>Sub-culture norms</td>
</tr>
</tbody>
</table>
Summary
Contributions

• Security Culture: what is it and why do we need it.
• Guidelines for a healthy security culture.
• An agenda for incorporating insights into the secure design process.


References III

