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

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Introduction
Why Security Culture

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

Method

1. Grounded Theory [Corbin and Strauss, 2008] analysis from existing literature.
2. Comparative model derived from empirical data.
3. Theoretical and empirical models applied to a secure design process.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results

Cases
What is Security
Culture?
Guidelines

Future work

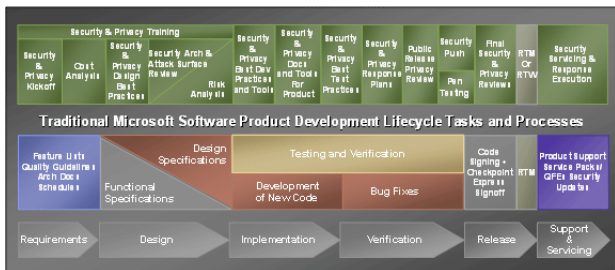Summary

References

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.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results

Cases
What is Security
Culture?
Guidelines

Future work

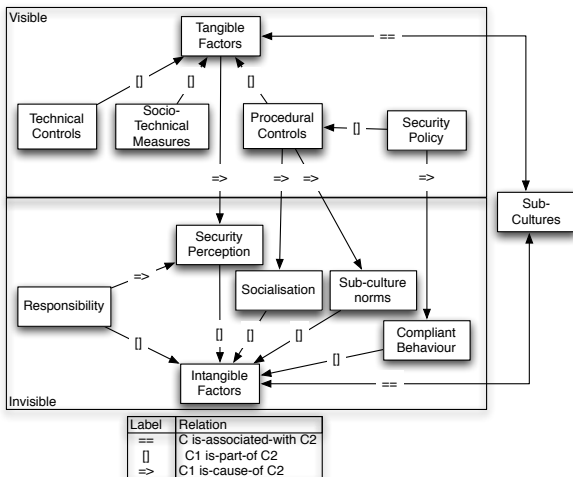Summary

References

Case Studies
Security Development Lifecycle

- A software development process for developing secure software [Howard and Lipner, 2006, Microsoft Corporation, 2008].
- Pragmatic : based on Microsoft's experience securing Windows 2000, .NET and Windows Server 2003.
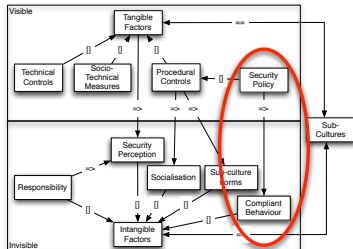- Prescriptive: guidance for all stages of the secure software development lifecycle.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

What is Security Culture?

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

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

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Guideline 1
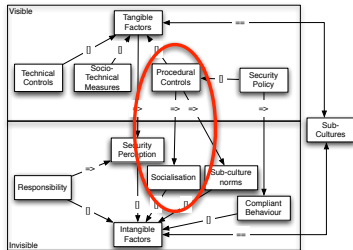## Have a single, visible, security policy

- Statements of management intent.
- Multiple forms of procedural control lead to multiple security perspectives.
- Reliance on social networks in lieu of visible policies.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Guideline 2
Leverage socialisation

- *Socialisation* is the
  process of developing
  culturally acceptable
  beliefs, values and
  behaviours
  [Brown, 1998].

- Certificate installation as
  a rite of passage.

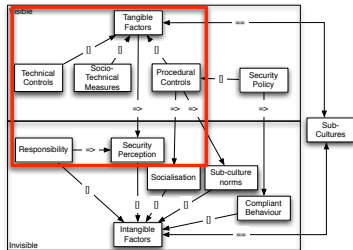- Compliance and
  socialisation
  synonymous in the SDL.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Guideline 3
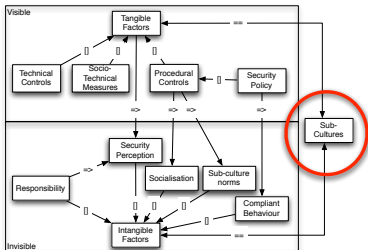Model lines of responsibility

- 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.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Guideline 4
Know your subcultures

- Evident in NeuroGrid
  when asking users to
  describe how data was
  handled.

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

- Understanding values
  helps to determine
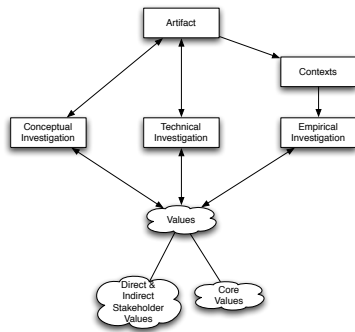 whether security will be
  sacrificed for operational
  goals.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Future work

Value Sensitive Design and the design process

- Identifies *impacting human values* and integrates them into the design process.

- Conceptual, Empirical and Technical Investigation.

- Supplements existing design processes.

- Precedents in secure and usable design [Friedman et al., 2002, Friedman et al., 2005, Friedman et al., 2006]

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

Future work
Augmenting Value Sensitive Design

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

Guideline	Value
Have a single, visible security policy	Compliant Behaviour
Leverage socialisation	Socialisation
Model lines of responsibility	Responsibility
Understand your subcultures	Sub-culture norms

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.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

References I

📄 Brown, A. (1998).
Organisational Culture.
Prentice Hall, 2nd edition.

📄 Corbin, J. M. and Strauss, A. L. (2008).
Basics of qualitative research : techniques and procedures for developing grounded theory.
Sage Publications, Inc., 3rd edition.

📄 Darley, J. M. and Latané, B. (1970).
Norms and normative behaviour: field studies of social interdependence.
In Berkowitz, L. and Macaulay, J., editors, *Altruism and Helping Behaviour*. Academic Press.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

References II

📄 Friedman, B., Howe, D., and Felten, E. (2002).
Informed consent in the mozilla browser: implementing
value-sensitive design.
*System Sciences, 2002. HICSS. Proceedings of the
35th Annual Hawaii International Conference on*, pages
10 pp.–.

📄 Friedman, B., Lin, P., and Miller, J. K. (2005).
Informed consent by design.
In Cranor, L. F. and Garfinkel, S., editors, *Security and
Usability: Designing Secure Systems that People Can
Use*. O'Reilly Media.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

References III

📄 Friedman, B., Smith, I., Kahn Jr., P. H., Consolvo, S., and Selawski, J. (2006).
Development of a privacy addendum for open source licenses: Value sensitive design in industry.
In Dourish, P. and Friday, A., editors, *Ubicomp 2006*, LNSC 2006, pages 194–211. Springer-Verlag Berlin Heidelberg.

📄 Geddes et al (2006).
The challenges of developing a collaborative data and compute grid for neurosciences.
Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on, pages 81–86.

Making the
invisible
visible

S. Faily,
I. Fléchais

Introduction

Method

Results
Cases
What is Security
Culture?
Guidelines

Future work

Summary

References

References IV

📄 Howard, M. and Lipner, S. (2006).
The security development lifecycle: SDL, a process for developing demonstrably more secure software.
Microsoft Press, Redmond, Wash.

📄 Microsoft Corporation (2008).
Microsoft Security Development Lifecycle (SDL) - version 3.2.
http://msdn.microsoft.com/en-gb/library/cc307748.aspx.