Making the invisible visible

a theory of security culture for secure and usable grids

Shamal Faily

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford, OX1 3QD, UK

What is a security culture and why is it useful? There is no straight answer to the first question, but there is an argument for the second, especially for grid environments. Nurturing safety culture is an important factor in enhancing perceptions of safety and reducing the number of accidents, but is security culture equally useful? Values people hold about assets, controls, security and usability may conflict. Ignoring this conflict and the role culture plays in exposing assets to risks can lead to consequences ranging from the loss of an asset, through to loss of life. The picture painted of security culture by the literature is largely based on single organisations and ignores the cultural diversity, disparate needs and interests found in large, heterogeneous environments. By analysing what security culture is and how it is manifested in a grid environment, we can glean insights which inform the process of designing secure and usable grids.

In order to derive some meaning about security culture, we performed analytical induction on a sample of the peer-reviewed literature on security culture, to generate theory from observed, real-world phenomena. Grounded Theory [1] was selected as the methodology for this approach. The induced model was used to identify a number of areas which might suggest divergence should the framework to be applied to grid environments.

This theory was validated using two cases. Firstly, a comparative theory of security culture was developed, grounded in empirical data from a contemporary e-Science project, namely NeuroGrid [3]. The empirical data was elicited from qualitative interviews, the design of which was informed by the divergence highlighted in the literature derived model. Secondly, both the theoretically and empirically derived frameworks were applied to literature on the Security Development Lifecycle [6], to determine whether the main tenets of the security culture theory continued to hold.

The literature indicates that security culture is often described as something which can be mentally perceived, such as security awareness or obedient behaviour. Our research found that these viewpoints fail to explain the larger picture. Like a number of other writers on security culture, we take inspiration from the work of Schein and his layered model of organisational culture [7]. We also consider the work of those who consider culture less as a hierarchy and more as an ordered system of symbols where meaning is based on individual participants, rather than the organisation as a whole [4, 5].

We define security culture as a combination of *tangible factors* and *intangible factors* within both an organisation's culture and its subcultures ; prominent elements of this model are illustrated in figure 1. Tangible factors are visible artifacts of a culture or subculture and are represented by technical controls, procedural controls or socio-technical measures. Intangible factors are invisible assumptions, norms and values of a culture's participants. Security culture may nest other sub-cultures which vary between organisational units. Not only can security perception vary between these sub-cultures, but members of the sub-cultures can affect security controls based on their perception of other sub-cultures' security perceptions.

Our analysis yielded several practical guidelines which, when adopted, lead to a security culture more in-tune with the security needs of a grid environment. Some of these guide-

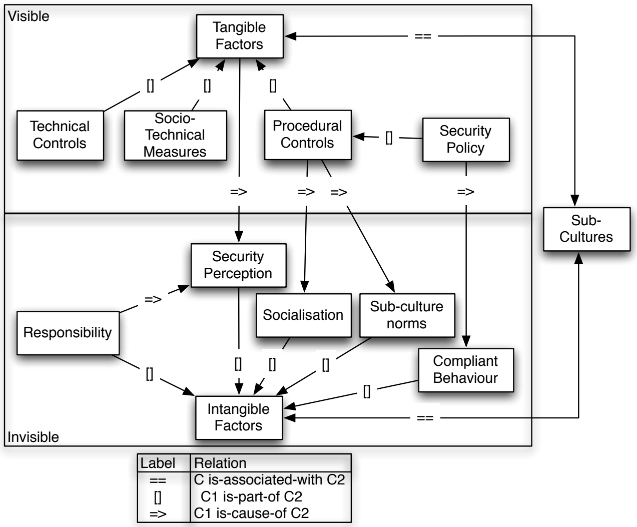

Fig. 1. security culture network diagram

lines point to a need to understand models of responsibility, and the values and norms of subcultures. This begs the question of how to incorporate these insights into the secure design process? The fact that many of the intangible factors of security culture are values suggests that incorporating Value-Sensitive Design [2] may be useful. Value-Sensitive Design attends to the human values impacting a potential system and integrates these into the design process. This approach consists of three forms of investigation : conceptual, empirical and technical.

Future work will involve augmenting Value-Sensitive Design with insights from this work, to determine factors relating to the socio-technical environment, which impact security and secure systems design.

References

1. Corbin, J. M., and Strauss, A. L. *Basics of qualitative research : techniques and procedures for developing grounded theory*, 3rd ed. Sage Publications, Inc., 2008.
2. Friedman, B., Peter H. Kahn, J., and Borning, A. Value sensitive design and information systems. In *Human-Computer Interaction and Mangement Information Sytesms : Foundations*, P. Zhang and D. Galletta, Eds. M. E. Sharpe, 2006.
3. Geddes et al. The challenges of developing a collaborative data and compute grid for neurosciences. *Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on* (2006), 81–86.
4. Geertz, C. Thick description: Towards an interpretive theory of culture. In *The interpretation of cultures: selected essays.* Basic Books, New York, 1973, pp. 5–30.
5. Hirschheim, R., and Newman, M. Symbolism and information systems development: Myth, metaphor and magic. *Information Systems Research 2*, 1 (1991), 29–62.
6. Microsoft Corporation. Microsoft Security Development Lifecycle (SDL) - version 3.2. *http://msdn.microsoft.com/en-gb/library/cc307748.aspx* (2008).
7. Schein, E. H. *Organizational Culture and Leadership*, 2nd ed. Jossey-Bass, 1992.