FAILY, S. 2013. Security patterns considered harmful? In *Proceedings of the 2nd International workshop on cyberpatterns (Cyberpatterns 2013): unifying design patterns with security, attack and forensic patterns, 8-9 July 2013, Abingdon, UK*. Oxford: Oxford Brookes University, pages 108-109.

Security patterns considered harmful?

FAILY, S.

2013

Security Patterns Considered Harmful?

Shamal Faily

Department of Computer Science
University of Oxford
Oxford UK OX1 3QD
firstname.lastname@cs.ox.ac.uk

Abstract. While a useful source of repeatable security knowledge, ambiguity about what security patterns are and how they might be applied call into question their reliability as a design tool. To provoke discussion about their usefulness, this paper claims that security patterns should be considered harmful because (i) they abdicate design responsibility, (ii) their implications are unclear, and (iii) abstractions are still an enemy. We also consider *Strong Concepts* as a more useful alternative for security design.

1 Motivation

Security patterns describe particular, recurring security problems arising in specific contexts, and present a well-proven generic solution for them [1]. By breaking security problems into smaller pieces, security patterns make design complexity easy to manage. However, Schumacher et al's definition for a security pattern is framed in terms of what it does, rather than what it is. At the panel at Cyberpatterns 2012, panelists were asked to define a security pattern. In general, the panelists agreed that patterns are an abstraction of the repetitive, they need to tell their user something interesting, and they need to be analysed in order to determine if they are applicable or not. Yet, panelists also defined security patterns differently, based on their particular cybersecurity stake. While most would agree that security patterns can be useful as a source of repeatable knowledge, we claim that they should also be considered harmful for security design. After all, if a panel of experts are unable to agree on what security patterns are, and how they should be used, why should we expect others to adopt them?

2 Why are Security Patterns harmful?

Our argument that security patterns might be considered harmful runs as follows:

– *Security patterns abdictate design responsibility*: In general, patterns abdicate responsibility to practitioners for understanding both their problem and its context well enough to understand the implications of a security pattern. Because they appear to satisfy relevant requirements, architects may succumb to the temptation of selecting patterns at an early stages of system design, when the context remains unclear. This can have unexpected consequences.

– *The implications of security pattern application are unclear*: The consequence of pattern application is an important element in the original Gang of Four patterns [2]. Yet, not all security pattern templates consider the implications of pattern application; when they do, useful dimensions of their application are omitted. For example, Lobato et al's [3] privacy policy patterns consider their consequences only in terms of user comprehension and confidence; privacy is, however, a much more nuanced value and privacy design implications are much broader.
– *Abstractions are still an enemy*: In their response to Wing's work on the merits of computational thinking [4], Blackwell et al. [5] claim that abstractions have potentially harmful side-effects because dehumanising complexity leads to problems re-establishing their human impact when these are contextualised. This claim appears to hold true for patterns as well as abstractions, particularly where patterns rely on organisational abstractions that are more rigid that computational forms.

3 Strong Concepts as an alternative to security patterns

Some in the HCI community have criticised patterns for being tied to interfaces rather than actual design practice. From a security design perspective, this may also be the case. As a result, *Strong Concepts* [6] have been proposed as an alternative. Strong concepts, such as *social navigation* and *seamfulness* are softer than design patterns while still affording a useful design vocabulary; they also afford evaluation criteria that experienced designers can adopt. As such, many incomplete security patterns in the wild might be more usefully employed as strong concepts to provide better heuristics for security designers.

4 Acknowledgements

The research described in this paper was funded by the EU FP7 *webinos* project (FP7-ICT-2009-05 Objective 1.2).

References

1. Schumacher, M., Fernandez, E., Hybertson, D., Buschmann, F.: Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons (2005)
2. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design patterns: elements of reusable object-oriented software. Addison-Wesley (1995)
3. Lobato, L., Fernandez, E., Zorzo, S.: Patterns to support the development of privacy policies. In: Availability, Reliability and Security, 2009. ARES '09. International Conference on. (2009) 744–749
4. Wing, J.M.: Computational thinking. Communications of the ACM **49**(3) (2006) 33–35
5. Blackwell, A.F., Church, L., Green, T.: The Abstract is 'an Enemy': Alternative Perspectives on Computational Thinking. In: Proceedings of 20th Annual Workshop of the Psychology of Programming Interest Group. (2008) 34–43
6. Höök, K., Löwgren, J.: Strong concepts: Intermediate-level knowledge in interaction design research. ACM Trans. Comput.-Hum. Interact. **19**(3) (October 2012) 23:1–23:18