Hyper Contextual Software Security Knowledge Management

Shao-Fang Wen

Faculty of Computer Science and Media Technology
Norwegian University of Science and Technology, Norway

1. Introduction

Open source software (OSS) has become increasingly important and has attracted developers from both public and private sectors. In the 2015 Future of Open Source Survey [9], 78% of companies run operations on open source, and 55% of respondents said open source delivers superior security [5]. This reputation arises from the community development model and the resulting purview by the "many eyes" of developers worldwide. Yet, of the 8,000-13,000 vulnerabilities detected annually, about 40% impact open source software [8].

Nations and security communities have spent enormous efforts in emphasizing security awareness and building security principles, like ISO/IEC 15026, Common Criteria (CC), SSE-CMM, NIST SP 800-160, and many others. Why have these software security policies in OSS faced continuous failure? While there are several possible reasons, it is noteworthy that secuity has not been fully discussed in the development of the software in open source communities, and it is necessary to examine why software guidelines and principles have not been effective despite efforts by policy makers. As Scacchi [13] points out, the meaning of open source in the socio-technical context is broader than its technical definition, and includes communities of practice, social practices, technical cultures, and uses. As the software industry evolves and enters into the era of the Internet of Thing (IoT), moreover, the meaning of OSS is becoming broader and the needs for contextual software analysis are increasing.

In light of this problem, in this research we address the security problems of software products released and maintained by open source communities. Specifically, we apply a socio-technical systems perspective, which systematically and holistically takes into account the social context as well as technological aspects. Based on the socio-technical model and context, we then examine the main factors that were once disproportionately considered in the development of software security principles and make suggestions for designing a more effective and productive security knowledge management system for securing OSS. It is worthwhile to focus on security knowledge management in OSS, given that previous studies of the evaluation of software security mostly considered general software [3, 10-12]. We propose the notion of Hyper Contextual Knowledge Management that requires security knowledge to be described at a conceptual level, called hyper-contextual, shared by all contexts, and thus allows the non-linearly correlated knowledge between contexts to be identified and transferred. With the proper understanding of the common characteristics of software security, we believe that, software communities, project teams and software engineers can use them to understand, explain, predict, control and create software security with a degree of certainly.

2. Objectives

The research goal is to provide a hyper contextual security knowledge management system that would facilitate open source communities to effectively offer appropriate secure software products. We seek to examine the hypothesis: *Hyper Contextual Knowledge Management can improve security quality of software product that are delivered and maintained by open source communities.* We expect the research process and the resulting framework that should be helpful for those who seek to examine how technical and non-technical security issues are related in the open source environment.

3. Research Question

The issues raised in the previous sections motivate the following research question:

Whether hyper contextual security knowledge management system can improve the security quality of software products that are produced and maintained by open source communities?

Given the multi-faceted aspects of both socio-technical context and knowledge model design, we choose to break this research question into the following four smaller questions.

- (RQ1) What are the strengths and weaknesses, technical and non-technical, of software security management defined in the open source communities?
- (RQ2) What is the knowledge meta-model of software security domain that consists of conceptual security knowledge?
- (RQ3) How can the proposed knowledge model be integrated into open source communities to form a knowledge management system for securing software products?
- (RQ4) How can the proposed knowledge management system be evaluated to meet the demands for software products in the studied communities?

4. Methodology

The research methodology to pursue the main objective of this work comprises several steps. First, we will make an interpretive inquiry in the context of OSS evaluation using a socio-technical modeling approach provided by Kowalski [7] to be able to comprehensively model the identified OSS security problems, in relation to security principles and guidelines. Necessary data were collected using expert interviews, industry reports, software security standards, and other materials to analyze software-related security issues.

Since the main goal of this research is to produce an artifact, the design science appears as a natural methodology of our research. We plan to have 3 iterations of DSR to complete the research work. Figure 1 represents the research iterations. The research iterations are linked to the research studies and research questions as following:

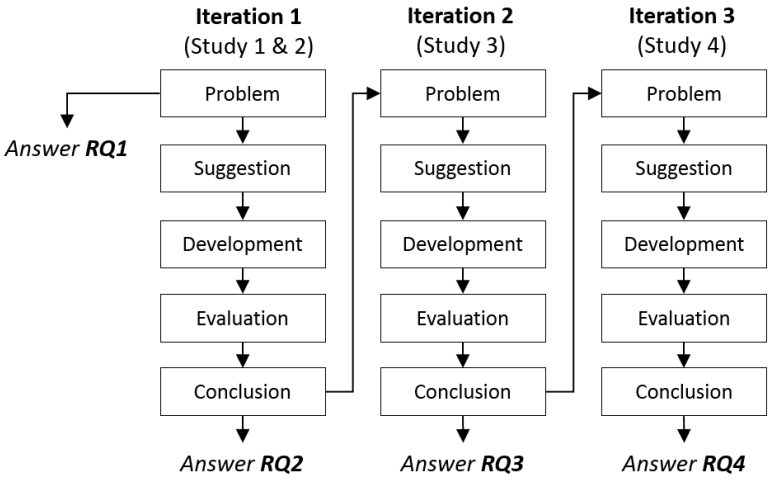

Figure 1: Research iterations

Reference

[1] Al Sabbagh, B. and S. Kowalski (2013). "A socio-technical framework for threat modeling a software supply chain". The 2013 Dewald Roode Workshop on Information Systems Security Research, October 4-5, 2013, Niagara Falls, New York, USA, International Federation for Information Processing.

[2] Alan, R. H., S. T. March, J. Park and S. Ram (2004). "Design science in information systems research." MIS quarterly. volume 28, issue 1, pages 75-105.

[3] Aurum, A., F. Daneshgar and J. Ward (2008). "Investigating Knowledge Management practices in software development organisations–An Australian experience." Information and Software Technology. volume 50, issue 6, pages 511-533.

[4] Bider, I. and S. Kowalski (2014). A framework for synchronizing human behavior, processes and support systems using a socio-technical approach. Enterprise, Business-Process and Information Systems Modeling, Springer: 109-123.

[5] Hoepman, J.-H. and B. Jacobs (2007). "Increased security through open source." Communications of the ACM. volume 50, issue 1, pages 79-83.

[6] Karokola, G., S. Kowalski and L. Yngström (2011). "Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View". HAISA.

[7] Kowalski, S. (1994). "IT insecurity: a multi-discipline inquiry." PhD Thesis, Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden. ISBN: 91-7153-207-2.

[8] Martin, B., C. Sullo and J. Kouns. (2015). "OSVDB: open source vulnerability database." Electronic document. https://blog.osvdb.org/category/vulnerability-statistics/.

[9] NorthBridge (2015). "2015 Future of Open Source Survey." Electronic document. http://www.northbridge.com/open-source

[10] Nunes, F. J. B. and A. B. Albuquerque (2010). A Secure Software Development Supported by Knowledge Management. Innovations and Advances in Computer Sciences and Engineering, Springer: 291-296.

[11] O'Connor, R. and S. Basri (2014). "Understanding the role of knowledge management in software development: a case study in very small companies." International Journal of Systems and Service-Oriented Engineering. volume 4, issue 1, pages 39-52.

[12] Rus, I. and M. Lindvall (2002). "Knowledge management in software engineering." IEEE software. volume 19, issue 3, pages 26.

[13] Scacchi, W. (2002). "Understanding the requirements for developing open source software systems". IEE Proceedings--Software, IET.

[14] Vaishnavi, V. and W. Kuechler (2004). "Design research in information systems." Electronic document. http://desrist.org/design-research-in-information-systems/.