Chapter 1

State of Practice in Secure Software: Experts’ Views on Best Ways Ahead

Bill Whyte
Independent Consultant, UK

John Harrison
LanditD, UK

ABSTRACT

The authors present a synthesis of expert views on some important actions to improve the state of practice in secure software. The main conclusions are: the skill base is lacking; business cases for security good practice are poorly developed; choosing between different ‘good practices’ is difficult; research will only have impact if compatible with the commercial environment of developers and their existent skills. The study is grounded on experiences as panel moderators, rapporteurs and report writers involved in drafting the views of experts. Some research directions are indicated.

INTRODUCTION

Although some organisations are proficient in and committed to good-practice software development that promotes resilience against security-attacks, it is widely recognised that they are very much the minority, with a long tail of developers who lack either the skill or motivation to do so. Here we present a synthesis of expert views on some of the most important actions for the medium and long-term in order to improve the overall state of practice in secure software. An important aspect of our study is that it is grounded significantly on our experiences as panel moderators, rapporteurs and report writers involved in drafting the views of a number of experts and submission of these drafts to the experts for approval through a series of iterations. By this means we believe we have identified several areas of expert consensus and disagreement, with minimal interpretation by ourselves. Furthermore these have been crosschecked against other independent sources.

A large majority of the experts involved agreed that a very significant, if not the most significant, positive impact on secure software development would be concentration on measures that improve the overall quality of the ‘state of practice’ rather than the ‘state of the art’ in secure
software development. They further concluded that this necessarily involves not just new research and development in good-practice security life-cycle methodology but also measures to support business-case development. Furthermore, these should take into account the knowledge-base, (professional development and university education), on which any better-practice developments would have to be based. However good in itself is any research activity, clearly its eventual adoption by these segments of the software industry must depend on its clear contribution to their business case and, at the very least, their ability to use and understand it.

This text, therefore, does not attempt a deep analysis of secure software research development in terms of its detailed scientific and technological excellence or its theoretical basis, but rather attempts to identify specific characteristics which it should possess in order to meet the needs particularly of the ‘average’ (and lower than average) development teams and those under significant commercial pressure.

BACKGROUND

Proper selection of methodology for acquiring, authoritative views in the area of applied technology is often insufficiently addressed, with a failure to employ research methods that are properly grounded, with issues such as ‘observation’ versus ‘theory’ [O’HEAR] not separated out. At worst, observation simply consists of an unrepresentative sampling of journal papers or online search, and theory simply the biased views of the enquirer, and in neither case with the investigator’s views subject to proper ‘closed-loop’ feedback. To avoid this as far as possible and although we do make use of open-loop sources, our findings are weighted towards first-hand encounters with a number of peer-reviewed activities involving experts in secure software development. In the course of these encounters we have sometimes been involved in drafting (and redrafting) reports summarizing consensus views on the subject. What is, and what is not, said, and the manner in which the discussions proceed during this consensus building, can give additional insight into the debate.

Prominent among these was participation in a UK Department of Trade and Industry (DTI) Global Watch Initiative, in January 2006 [GWM]. The Global Watch team comprised a small body of experts who met a wide range of influential academic and governmental representatives and senior staff in leading software companies in California and Washington State.

One consequence of the report back from the Global Watch Mission was the setting up in March 2007 of a Special Interest Group on Secure Software Development (SSDSIG). This is one of a number of working groups established by the Cyber Security Knowledge Transfer Network of the UK Department of Business, Enterprise and Regulatory Reform. SSDSIG has as its aims that of identifying the principle barriers to secure software development and to make recommendations to address them. Membership is open to all interested persons and has operated via a number of mechanisms: well-attended, face-to-face meetings of industry and academic practitioners, active email discussions between members and also other interested parties, approaches to outside bodies for information acquisition and knowledge transfer. SSDSIG sponsored a report into the state of undergraduate education on software security, has run a very successful open workshop and published its first White Paper in June 2008 [WHYTE, HARRISON]. SSDSIG’S executive are now concentrating on taking forward the recommendations contained in that paper.

Following on from the above activities, SSDSIG was invited to be represented at a meeting held jointly by the European Research Consortium for Informatics and Mathematics (ERCIM) and the F5 ‘Security Unit’ of the European Commission Directorate for the Information Society. The
Related Content

A Look Behind Conceptual Modeling Constructs in Information System Analysis and Design
www.igi-global.com/article/look-behind-conceptual-modeling-constructs/40954?camid=4v1a

A Survey of Web Services Provision
An Liu, Hai Liu, Baoping Lin, Liusheng Huang, Naijie Gu and Qing Li (2010). International Journal of
Systems and Service-Oriented Engineering (pp. 26-45).
www.igi-global.com/article/survey-web-services-provision/39097?camid=4v1a

AIWAS: The Automatic Identification of Web Attacks System
Toan Huynh and James Miller (2012). International Journal of Systems and Service-Oriented Engineering
(pp. 73-91).
www.igi-global.com/article/aiwas-automatic-identification-web-attacks/64200?camid=4v1a

Design-Based Research with AGILE Sprints to Produce MUVES in Vocational Education
Todd Cochrane, Niki E. Davis and Julie Mackey (2018). Application Development and Design: Concepts,
Methodologies, Tools, and Applications (pp. 607-624).
www.igi-global.com/chapter/design-based-research-with-agile-sprints-to-produce-muves-in-
vocational-education/188226?camid=4v1a