Development of a Master of Software Assurance Reference Curriculum

Nancy R. Mead, Carnegie Mellon University, USA

Julia H. Allen, Carnegie Mellon University, USA

Mark Ardis, Stevens Institute of Technology, USA

Thomas B. Hilburn, Embry-Riddle Aeronautical University, USA

Andrew J. Kornecki, Embry-Riddle Aeronautical University, USA

Rick Linger, Carnegie Mellon University, USA

James McDonald, Monmouth University, USA

ABSTRACT

Modern society is deeply and irreversibly dependent on software systems of remarkable scope and complexity in areas that are essential for preserving this way of life. The security and correct functioning of these systems are vital. Recognizing these realities, the U. S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD) enlisted the resources of the Software Engineering Institute at Carnegie Mellon University to develop a curriculum for a Master of Software Assurance degree program and define transition strategies for implementation. In this article, the authors present an overview of the Master of Software Assurance curriculum project, including its history, student prerequisites and outcomes, a core body of knowledge, and curriculum architecture from which to create such a degree program. The authors also provide suggestions for implementing a Master of Software Assurance program.

Keywords: *Curriculum Architecture, Software Assurance, Software Assurance Curriculum, Software Assurance Education, Transition Strategies*

Software has become the core component of modern products and services. It has enabled functionality, business operations, and control systems critical to our way of life. However, software's race to ubiquity has outpaced security advances commensurate with software's vital role in our society. Consequently, as our dependence on software and software-intensive systems grows, we find ourselves exposed to an increasing number of risks.

The complexity of software and software-intensive systems, for instance, poses inherent

DOI: 10.4018/jsse.2010100102

risk. It obscures the essential intent of the software, masks potentially harmful uses, precludes exhaustive testing, and introduces problems in the operation and maintenance of the software. This complexity, combined with the interdependence of the systems we rely on, also creates a weakest link syndrome: attackers need only take down the most vulnerable component to have far-reaching and damaging effects on the larger system. What's more, anywhere-to-anywhere interconnectivity makes the proliferation of malware easy and the identification of its source hard.

The rising number of vulnerabilities compounds risk and—gives attackers even more targets of opportunity—as shown by the rising number of incidents targeting software vulnerabilities (Bosworth, 2002).

In this environment, the threats are large and diverse, ranging from independent, unsophisticated, opportunistic hackers to the very technically competent intruders backed by organized crime (Anderson, 2008). Malicious actors are increasingly acquiring information technology skills that allow them to launch attacks designed to steal information for financial gain, and to disrupt, deny access to, degrade, or destroy critical information and infrastructure systems. Technical sophistication is no longer a necessary requirement: increasingly sophisticated attack methods, thanks to the growing underground trade in productized attack tools, no longer require great technical savvy to execute.

Recognizing these realities, the U. S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD) enlisted the resources of the Software Engineering Institute (SEI) at Carnegie Mellon University to develop a curriculum for a Master of Software Assurance degree program and define transition strategies for future implementation. For the purposes of this curriculum, the discipline of software assurance is targeted specifically to the security and correct functioning of software systems, whatever their origins, application domain, or operational environments.

As noted in our curriculum report, the need for a master's level program in this discipline has been growing for years (Mead, 2010a).

- At the Knowledge Transfer Network Workshop in Paris in March 2009, cybersecurity education was recognized as part of the information security, privacy, and assurance roadmap vision. Cyber security education was also identified as one of the workshop's lines of development (LSEC, 2009).
- A study by the nonpartisan Partnership for Public Service points out that "[President Obama's] success in combating these threats [to cyber security] and the safety of the nation will depend on implementing a comprehensive and coordinated strategy—a goal that must include building a vibrant, highly trained and dedicated cyber security workforce in this country." The report found that "The pipeline of new talent [with the skills to ensure the security of software systems] is inadequate. . . . only 40 percent of CIOs [chief information officers], CISOs [chief information security officers] and IT [information technology] hiring managers are satisfied or very satisfied with the quality of applicants applying for federal cyber security jobs, and only 30 percent are satisfied or very satisfied with the number of qualified candidates who are applying (PPS, 2009).
- The need for cyber security education was emphasized by The New York Times in quoting Dr. Nasir Memon, a professor at the Polytechnic Institute on New York University: "There is a huge demand, and a lot more schools have created programs, but to be honest, we're still not producing enough students" (Drew, 2009).
- Carnegie Mellon University and CERT have been active in this area for years, particularly in the Survivability and Information Assurance (SIA) Curriculum and the Scholarship for Service program