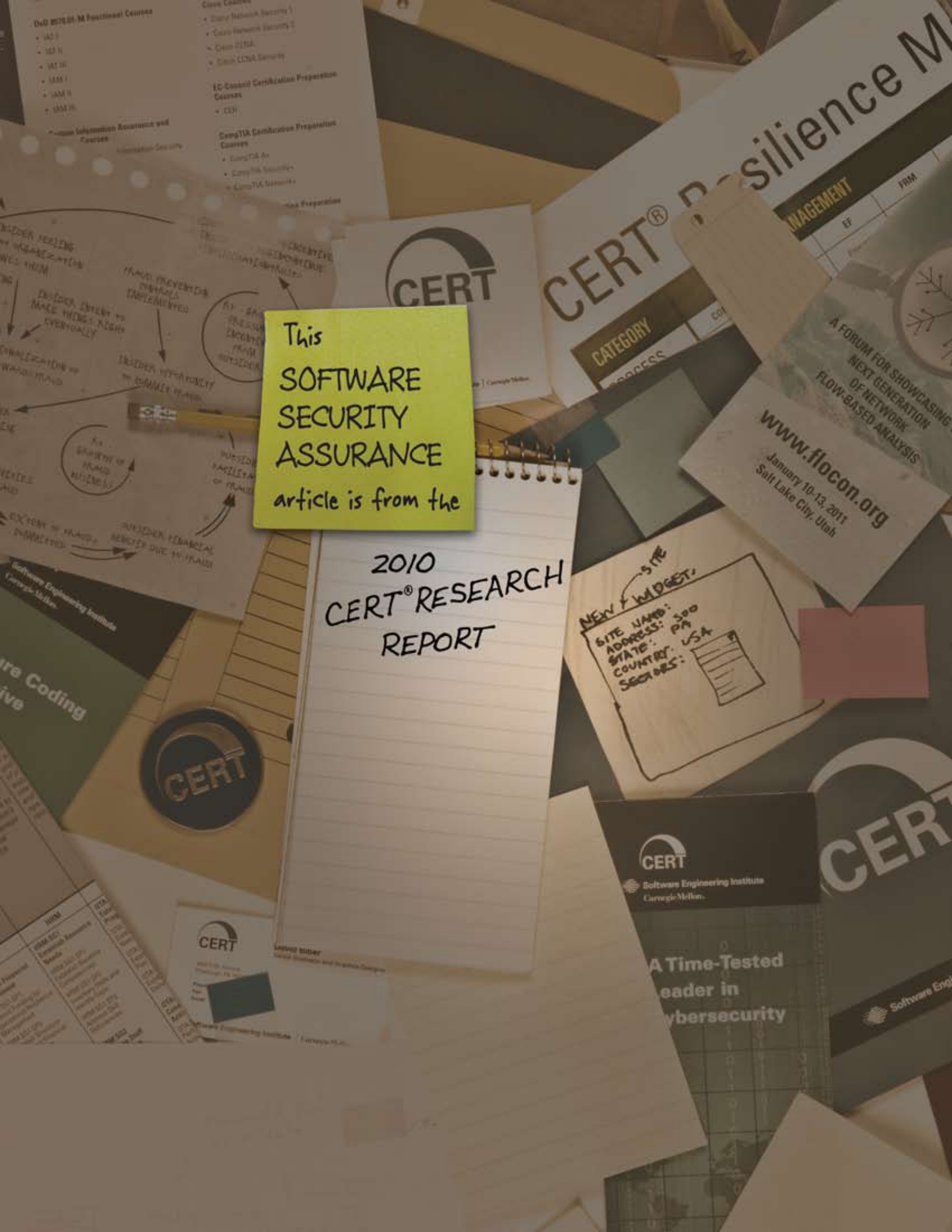
This
SOFTWARE
SECURITY
ASSURANCE
article is from the
2010
CERT® RESEARCH
REPORT
CERT
www.flocon.org
January 10-13, 2011
Salt Lake City, Utah
A FORUM FOR SHOWCASING
NEXT GENERATION
OF NETWORK
FLOW-BASED ANALYSIS
CERT
Software Engineering Institute
Carnegie Mellon
A Time-Tested
eader in
ybersecurity

Building Assured Systems Framework (BASF)


Principal Investigators:
Nancy R. Mead and Julia H. Allen

Problem Addressed

There is no single, recognized framework to organize research and practice areas focused on building assured systems (BAS). Sponsors of the CERT Program's research could use such a framework to help address the following challenges, including customer "pain points" and general research problems:

- How do I decide which security methods fit into a specific life-cycle activity?
- How do I know if a specific security method is sufficiently mature for me to use on my projects?
- When should I take a chance on a security research approach that has not been widely used?
- What actions can I take when I have no approach or method for prioritizing and selecting new research or when promising research appears to be unrelated to other research in the field?

Such a framework could also help organize CERT research efforts.

Some organizations have already begun addressing BAS in research and development including

- organizations participating in the Building Security In Maturity Model [1]
- Microsoft's software development lifecycle (SDL) [2]
- Software Assurance Forum for Excellence in Code (SAFECode) consortium members [3]
- Oracle
- members of the Open Web Application Security Project (OWASP) using the Software Assurance Maturity Model (SAMM)

Efforts to incorporate BAS tend to be stronger in vendor organizations. However, they are weaker in large organizations developing systems for use in-house and integrating across multiple vendors. They are also weaker in small- to medium-sized companies developing products for licensed use. Furthermore, there are a variety of life-cycle models in practice—no single approach has emerged as standard. Even in the larger organizations adopting secure software engineering practices, there is a tendency to select a subset of the total set of recommended or applicable practices. Such uneven adoption of BAS suggests the need for ways to measure results.

Research Approach

To understand previous and current work that could inform BASF development, we started by examining a number of existing software development and acquisition life-cycle process models, models for the development of more secure software, and research frameworks in software security and assurance. With this information, we formed a hypothesis that the recently developed Master of Software Assurance (MSwA2010) body of knowledge (BoK) [4] could serve as our starting point for the BASF. This makes sense given that the curriculum BoK draws extensively from more than 25 sources describing methods, practices, and technologies for software assurance and security (including the software security models considered in this report). Also, as the authors of this report, we led and contributed to the development of the MSwA2010 curriculum.

We tested this hypothesis by assigning "maturity levels" to each area of the MSwA2010 BoK. BoK areas include assurance across life cycles, risk management, assurance assessment, assurance management, system security assurance, system functionality assurance, and system operational assurance. We defined these levels as follows:

- L1—The area provides guidance for how to think about a topic for which there is no proven or widely accepted approach. The intent of the area is to raise awareness and aid the reader in thinking about the problem and candidate solutions. The area may also describe promising research results that may have been demonstrated in a constrained setting.
- L2—The area describes practices that are in early pilot use and are demonstrating some successful results.
- L3—The area describes practices that have been successfully deployed (mature) but are in limited use in industry or government organizations. They may be more broadly deployed in a particular market sector.
- L4—The area describes practices that have been successfully deployed and are in widespread use. Readers can start using these practices today with confidence. Experience reports and case studies are typically available.

To test this hypothesis further, we mapped existing CERT research work to the MSwA2010 BoK to see whether there were corresponding BoK areas for each research project. All major research projects did correspond to one or more BoK areas, either directly or indirectly. This gave us confidence that the BoK areas (and the research from which

they were derived) could be used as our initial framework. Once we mapped the current CERT research projects to the MSwA2010 BoK, we performed an initial gap analysis to identify some promising research areas for CERT.

The BASF helps to address some, but not all, of the four research questions stated previously. Since the BASF naturally covers the development life cycle, mapping a particular security method to the appropriate knowledge area(s) does help to answer the first question (relationship of security method to life-cycle phase). For the second question (security method maturity), considering knowledge area maturity levels in conjunction with examining a specific method provides information to help decide whether the method is sufficiently mature for use. The third question is a bit harder to answer and requires more work on the part of a BASF user. A cost/benefit analysis or risk assessment aids in answering the third question of whether it is worth taking a chance on a method that has not been widely used.

Expected Benefits

From a research perspective, researchers could consider periodically rating the maturity of their methods using the research approach described above. This would assist BASF users in deciding which methods to use. It would also be helpful if researchers and research methods users could begin to collect and provide cost/benefit data. All too often, researchers and research method users decide on a particular method but do not collect any information to determine whether the benefit justified the cost or to help inform future decisions.

We believe the BASF provides a context and structure for CERT's research work in building assured systems and that it can be used to show how various research efforts fit together. The gap analysis that we have done could be used to help in selecting new research and, to some extent, in prioritizing research projects. We anticipate that the BASF could be used in planning and justifying CERT's research program and communicating about it with others.

We expect that the U.S. Department of Defense (DoD) and other sponsors will find the BASF useful for tracking current research and development efforts in building assured systems and possibly in acquiring assured systems.

2010 Accomplishments

In 2010 we performed the research described above and documented the results in a technical report on the BASF [6].

Future Goals

To maximize its usefulness, the BASF needs to be more comprehensive. The BASF helps to address some, but not all, of the customer pain points. It is helpful in addressing the first and second questions, but is limited in its usefulness in addressing the third question. There are some areas of research that do not fit the BASF neatly. The BASF is not intended to exclude these areas, but we recognize that some important research work does not fit the MSwA2010 topics directly. For example, our recent software assurance curriculum work is needed research, but it does not map directly to the MSwA2010 topics. As another example, some of our advanced work in intrusion detection and network analysis also does not map directly to these topics. This may suggest the need for follow-on work to broaden the BASF to provide a framework for a wider range of research activities.

References

[1] McGraw, Gary; Chess, Brian; & Migues, Sammy. Building Security In Maturity Model BSIMM v2.0. *http://www.bsimm2.com/ (Accessed March 2011)*

[2] Lipner, S. & Howard M. "The Trustworthy Computing Security Development Lifecycle." March 2005. *http://msdn.microsoft.com/en-us/library/ms995349.aspx*

[3] Software Assurance Forum for Excellence in Code (SAFECode). SAFECode. *http://www.safecode.org* (2011).

[4] Mead, Nancy R.; Allen, Julia H.; Ardis, Mark; Hilburn, Thomas B.; Kornecki, Andrew J.; Linger, Rick; & McDonald, James. Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum (CMU/SEI-2010-TR-005, ESC-TR-2010-005). Software Engineering Institute, Carnegie Mellon University, 2010. *http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm*

[5] Allen, Julia H.; Barnum, Sean; Ellison, Robert J.; McGraw, Gary; & Mead, Nancy R. Software Security Engineering: A Guide for Project Managers. Addison-Wesley Professional, 2008.

[6] Mead, Nancy R. & Allen, Julia H., Building Assured Systems Framework (CMU/SEI-2010-TR-025). Software Engineering Institute, Carnegie Mellon University, September 2010. *http://www.sei.cmu.edu/library/abstracts/reports/10tr025.cfm*