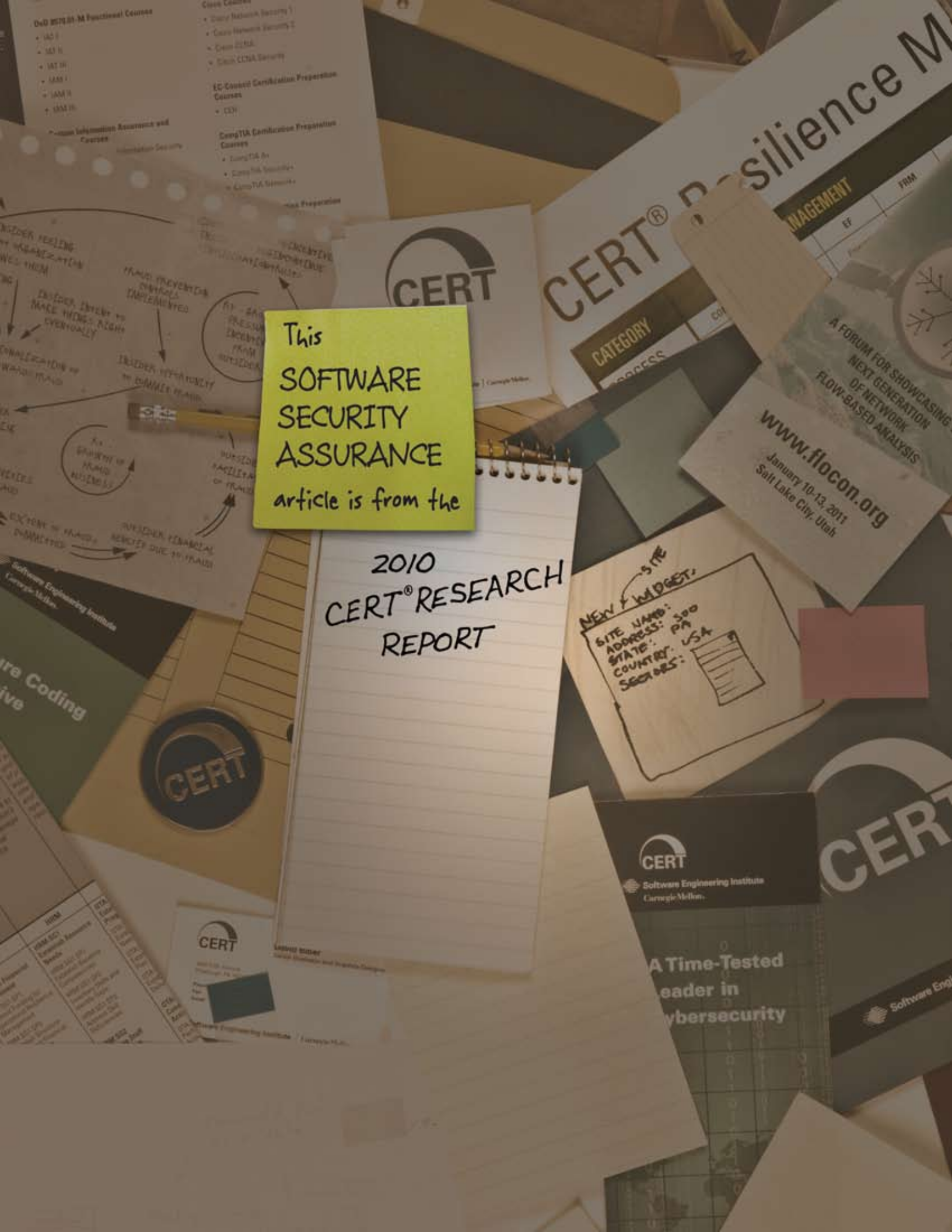
This
SOFTWARE
SECURITY
ASSURANCE
article is from the
2010
CERT® RESEARCH
REPORT
CERT
www.flocon.org
January 10-13, 2011
Salt Lake City, Utah
A FORUM FOR SHOWCASING
NEXT GENERATION
OF NETWORK
FLOW-BASED ANALYSIS
CERT
Software Engineering Institute
Carnegie Mellon
A Time-Tested
eader in
ybersecurity

Software Security Assurance Overview

The Software Security Assurance (SSA) team focuses on addressing security in the early life-cycle phases of acquisition and software development. Building security into software requires considerations beyond basic authentication/authorization and mandated operational compliance to identify and address the threat environment in which the resulting operational system must function. With greater security preparation, organizations have seen major reductions in operational vulnerabilities resulting in reductions in software patching. For example, Microsoft's own data shows that the patch levels for versions of Windows that were developed after the security "push" are half of what they were for earlier versions.[1]

Current approaches for software engineering apply a blend of training, frameworks, methods, tools, assessments, and best practices. Engineering software for effective security requires addressing all of these aspects to provide the ability to incorporate security as needed. The SSA team has developed frameworks, methods, assessments, and tools to support measurements and best practices identified to improve operational security and provide program management the ability to monitor software engineering to ensure effective consideration of security. A major gap in the security education of software engineers is being addressed through the development of curricula for colleges and universities. Transitioning the results of this research is a critical focus for SSA.

One unexpected finding of the team's research is that developing additional practices won't enable more organizations to implement software assurance into their life cycle. Instead, there's a critical need for better integration into the way software is designed and built. Wholesale change is difficult for organizations. So the SSA team has been developing practical guidelines and techniques and then piloting them to show results that are able to be replicated. If organizations can see it works, there's a better chance they'll implement it.

"It's like creating a cookbook," says Carol Woody, technical manager for SSA. "You build the recipe and then someone has to figure out how to cook it in their kitchen. We're developing customizable frameworks, methods, and techniques that organizations can tailor to their existing software acquisition and engineering practices."

The team worked on the following major research projects in 2010, collaborating with researchers in other SEI teams, at CMU, and at other universities and organizations world-wide.

Building Assured Systems Framework (BASF)

The SSA team developed the BASF, which provides a meaningful context and structure within which to describe, compare, and contrast research and development methods for building assured systems. It can also be used to identify gaps, prioritize new research projects, and stop or decommission current research projects that are not contributing useful results.

Supply Chain Assurance

Researchers developed an approach for assessing software supply chains and identifying the associated software assurance risks. SSA collaborated with members of the SEI's Acquisition team on this work.

Survivability Analysis Framework (SAF)

The SAF was a major area of research in fiscal year 2009 that informed Software Security Assurance research in fiscal year 2010. SSA researchers documented the SAF, an analysis technique for analyzing complexity and integration issues throughout the development life cycle for project management and stakeholders to ensure that development is proceeding toward an expected operational solution, for public release. The SAF was piloted for Joint Battle Mission Command and Control (JBMC2) in the analysis of a Time Sensitive Targeting mission thread for the Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (OUSD [AT&L]). A second pilot analysis was completed for Time Sensitive Targeting information assurance for Electronic Systems Center, Cryptologic Systems Group, and Network Systems Division (ESC/CPSG NSD). The pilot results were documented in special reports for the U.S. Department of Defense.

---

[1] *http://www.microsoft.com/security/sdl/learn/measurable.aspx*

Software Security Measurement

This research focused on how to establish and specify a level of security and then how to measure, at each phase of the life cycle, whether that level of security has been achieved. The SSA team collaborated with members of the CERT Resilience Management team and the SEI Measurement and Analysis team.

Security Requirements Engineering

Several authoritative studies have shown that requirements engineering defects cost 10 to 200 times as much to correct once fielded than if they were detected during requirements development. The SSA team collaborated with other researchers and led several teams of CMU students in developing processes and tools to help organizations build security into the requirements engineering process.

Trusted Hardware for Cyber Security

This research evaluated the promise and limitations of using trusted hardware as a foundation for achieving demonstrably high assurance of end-to-end security properties of applications executing in extreme adversarial environments. It laid the groundwork for future work that will explore and exploit the concepts of trust and trustworthiness and provide a scientific basis for understanding the relationships among hardware, software, security, and trust.

Catastrophe Analysis

Along with researchers from the SEI Acquisition and System Design teams, SSA researchers analyzed key dynamics that take place and how they affect the country's technical infrastructure when catastrophes occur. The goal of this research is to understand complex failure in order to better build and operate technologies and address today's complex, software-dependent networked systems.

Complexity Modeling and Analysis

The SSA team partnered with SEI experts from Systems of Systems, Acquisition, and CERT Insider Threat teams to apply modeling techniques to analyze software assurance solutions for the increasingly complex, highly interconnected, rapidly changing state of software systems. The team created a modeling framework to examine the gaps, barriers, and incentives that affect the development and implementation of assurance solutions for complex systems.

The SSA team also supported the Department of Homeland Security (DHS) Processes and Practices, Measurement, and Workforce Education and Training Working Groups. This work informs the software engineering community about software assurance best practices and is available on the Build Security In (*https://buildsecurityin.us-cert.gov/bsi/home.html*) and Software Assurance Community Resources and Information Clearinghouse (*https://buildsecurityin.us-cert.gov/swa/*) websites.

Through their research and transition efforts, the SSA team has led the way for addressing security early in the software life cycle.