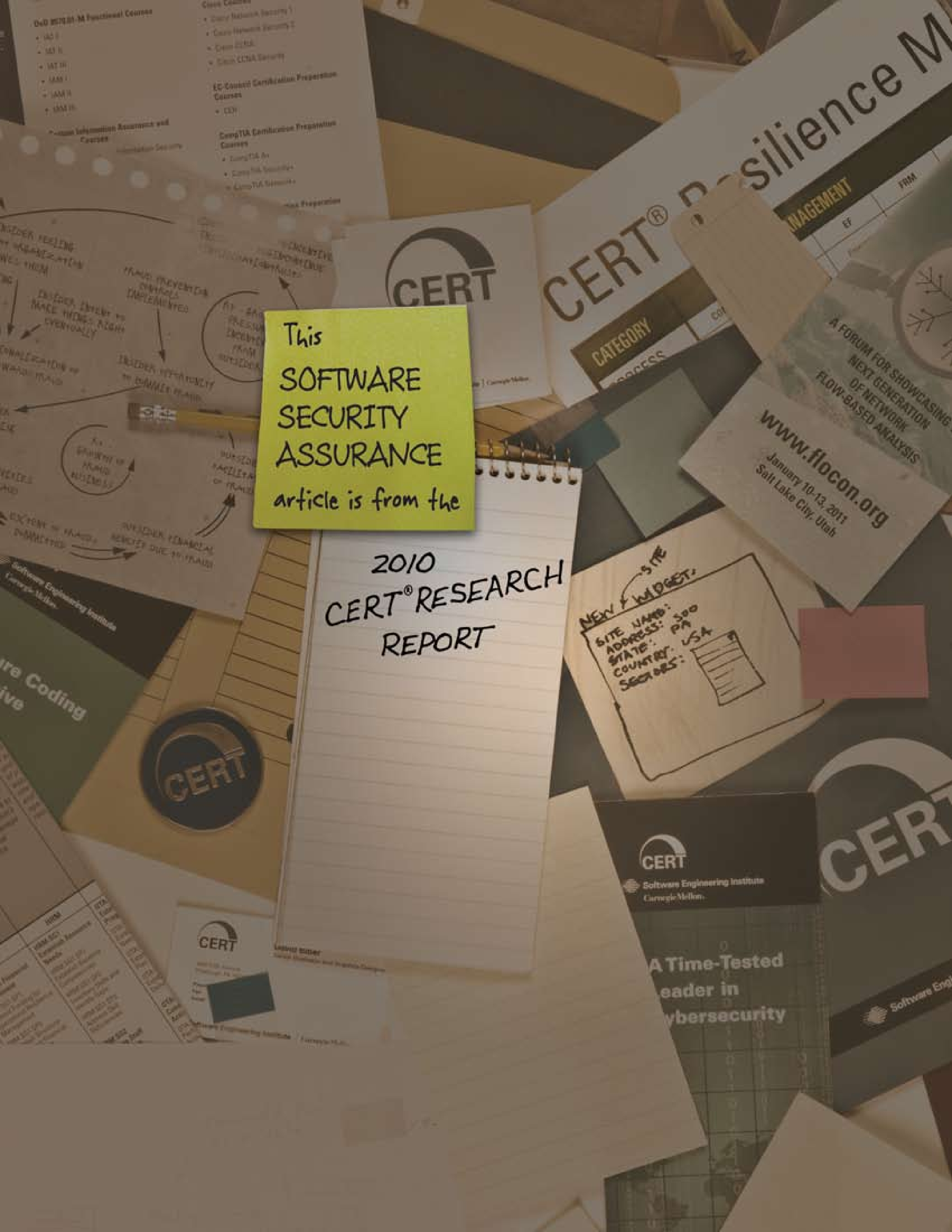

This SOFTWARE SECURITY ASSURANCE article is from the

2010 CERT® RESEARCH REPORT

CERT® Resilience M
CATEGORY
CERT
A FORUM FOR SHOWCASING NEXT GENERATION OF NETWORK FLOW-BASED ANALYSIS
www.flocon.org
January 10-13, 2011 Salt Lake City, Utah
NEW SITE WIDGET
SITE NAME:
ADDRESS: 300
STATE: PA
COUNTRY: USA
SECTORS:
Software Engineering Institute
Carnegie Mellon
A Time-Tested Leader in Cybersecurity
Secure Coding

Supply Chain Assurance

Principal Investigators:
Robert Ellison, Chris Alberts,
Rita Creel, Audrey Dorofee, and Carol Woody

Problem Addressed

The term “supply chain” has a long history in the business community and includes recent trends such as such just-in-time inventory. In the past, the business community considered supply chains as relevant only to the delivery of physical products. Now the business community uses the technology supply chain to develop most IT systems (hardware, software, public and classified networks, and connected devices), which together enable the uninterrupted operations of key government and industrial base actors, such as the Department of Defense, the Department of Homeland Security, and their major suppliers. While we have decades of physical supply chain data that have led to effective management practices, we have limited experience with software supply chains. While no perfect solution exists, much can be done to enable organizations to reduce risk effectively and efficiently while leveraging the significant opportunities afforded by supply chains.

On-time delivery and costs often get the most commercial attention, but some of the most serious risks are associated with system assurance, the confidence that the system behaves as expected. Software defects, such as design and implementation errors, can lead to unexpected behaviors or to system failure. Defects that enable an attacker to purposely change system behavior are often referred to as vulnerabilities. The source of such vulnerabilities is the supply chain, which includes commercial product vendors, custom development and integration contractors, and suppliers and subcontractors to those organizations. This research considers how to better manage the acquisition of software developed through a supply chain to reduce the likelihood of operational vulnerabilities.

Unfortunately, exploitable software defects are widespread. MITRE has analyzed successful attacks and identified more than 600 common software weaknesses, described in its Common Weakness Enumeration (CWE). Many of the CWE defects are widely known, as are the techniques that eliminate them. But those techniques are frequently not applied. For example, countermeasures for SQL injections are well established, yet SQL injections still rank second on the MITRE/SANS list of the top 25 most dangerous software errors. Veracode’s State of Software Security Report released on September 22, 2010 warns that most software is very insecure. Regardless of software origin, 58 percent of all applications submitted to Veracode for testing did not achieve an acceptable security score upon first submission.

Software supply chain security issues do not vanish when an acquisition is completed. Product designers base their decisions on the data available and the threats known at the time of development. Product assessments performed as part of the initial acquisition for a commercial component are valid only at that time.

Some examples of sources of risks that may emerge during deployment include the following:

- New attack techniques and software weaknesses cannot be foreseen.
- Product upgrades that add features or change design can invalidate the results of prior risk assessments and may introduce vulnerabilities.
- Corporate mergers, new subcontractors, or changes in corporate policies, staff training, or software development processes may eliminate expected supply chain risk management (SCRM) practices.
- Product criticality may increase with new or expanded usage.

Research Approach

In an attempt to integrate development and acquisition practices with risk-based evaluation and mitigation of product vulnerabilities, the SEI has begun research that explores the complex dynamics of software supply chain risk and examines techniques, such as systematic risk assessment, based on key drivers [1], use of assurance cases [2], attack surface analysis and threat modeling [3, 4], and consideration of supply chains for systems as well as systems of systems [5].

Taking a systems perspective on software supply chain risks, this research considers current practices in software supply chain analysis and seeks some foundational practices. The role of an acquirer depends on the nature of an acquisition. Product development is completed in advance of an acquirer’s product and supplier assessment. An acquirer seeks evidence that software developers have applied appropriate practices such as threat modeling and security testing. Acquirers need to understand the residual risks they will have to accept and accommodate in their operational implementation.

This research concentrates primarily on the role of the acquirer in software supply chain risk analysis for security. However, both suppliers and acquirers should perform such analysis, and it should consider the three components shown below and in Figure 1.

- attack analysis: factors that lead to successful attacks
- supplier: capability to limit product attributes that enable attacks
- acquirer: tradeoff decisions (desired usage and acceptable business risks)
- business risk assessment: identify attack enablers and possible business risks
- supplier/product assessment in terms of attack enablers and capability of supplier to manage them

Several factors, as shown in Figure 2, affect the occurrence of supply chain risks and the ability of an acquirer to manage them.

- Custom-developed software systems enable the acquirer to monitor and control risks during development. However, systems are increasingly constructed by integrating commercially available software, in which case the only controls might be to accept the risks or not to use a specific product.
- The owner of a system that participates in a system of systems has no control over or knowledge of the security risks of the other member systems.
- Expanded network connectivity and increased interoperability and dependencies among systems can increase the exposure of a system to adverse conditions. For example, a system for a large supplier has interfaces to their purchasers, manufacturers, and their transporters. Retailers, manufacturers, and suppliers are at risk when one of the other participating systems has been compromised.
- End-user software has always been a target for attackers. A large user community increases the likelihood of attack success. When the primary medium of data exchange was the floppy disk, an attacker might have used a Microsoft Word or Excel macro as malware. In 2010 the web is the dominant medium of data exchange, and web pages are used to install malware. Increased end-user connectivity, compromised mobile applications, and misconfigured end-user software increase the likelihood of end-user device compromise.

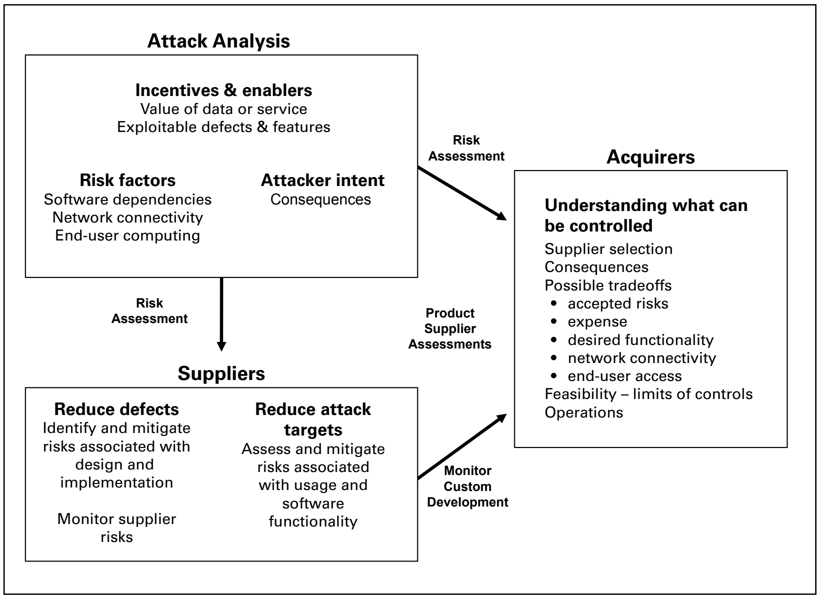

Figure 1

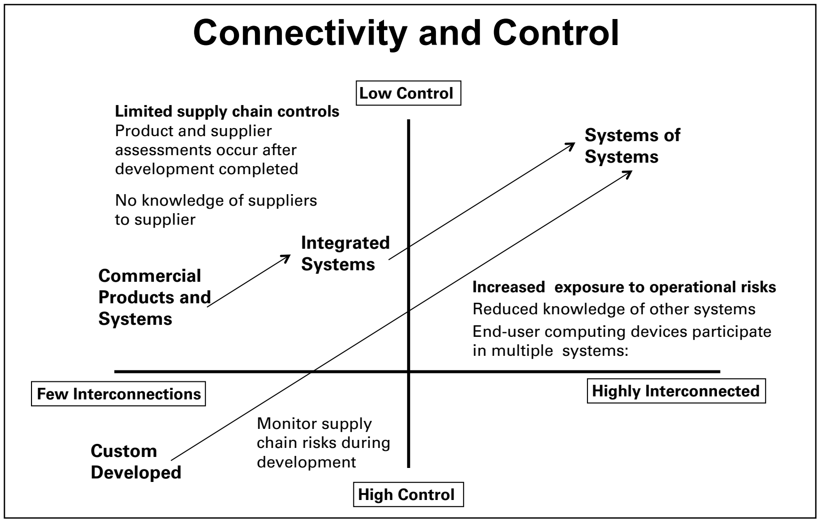
Connectivity and Control
Low Control
Limited supply chain controls
Product and supplier assessments occur after development completed
No knowledge of suppliers to supplier
Systems of Systems
Integrated Systems
Commercial Products and Systems
Increased exposure to operational risks
Reduced knowledge of other systems
End-user computing devices participate in multiple systems:
Few Interconnections
Highly Interconnected
Monitor supply chain risks during development
Custom Developed
High Control

Figure 2

Expected Benefits

The expected acquirer benefits of this research include

- an understanding of the supply chain factors that can be effectively managed to reduce risks and the management of those factors during deployment
- for outsourced development and integration, acquirer practices to monitor and mitigate supply chain risks
- for commercial components, an identification of essential supplier and product attributes appropriate for an acquisition

2010 Accomplishments

In 2010, the SEI

- developed a supply chain risk model [1] and identified supply chain factors based on the type of acquisition [5] funded by the Department of Homeland Security (DHS)
- participated in DHS Software Assurance Working Groups and Forums
- held an internal SEI workshop with participation from members of the SEI Acquisition Support Program to identify supply chain issues that organizations supported by the SEI have encountered and to discuss how those concerns could be addressed
- presented the Supply Chain Risk Management Framework to the DHS Software Assurance Forum, March 2010

Future Goals

The SEI is proposing future work that will help acquirers build the capability to identify software supply chain risks, select mitigation solutions for key risks, and measure the effectiveness of solutions throughout the life cycle, as well as to obtain leading indicators related to software supply chain security.

As noted in the introduction, known software development practices exist that can reduce the occurrence of vulnerabilities. We are seeking organizations interested in helping us establish the risk reduction from incremental incorporation of such demonstrated practices into their acquisitions.

References

[1] Christopher Alberts, Rita Creel, Audrey Dorofee, Robert Ellison, and Carol Woody, "A systemic approach for assessing software supply-chain risk," in *Proc. 44th Hawaii Int. Conf. on System Sciences,* Kauai, HI, 2011. *https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/acquisition/1230-BSI.html*

[2] Robert J. Ellison, John B. Goodenough, Charles B. Weinstock, and Carol Woody, "Evaluating and mitigating software supply chain security risks," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2010-TN-016, 2010. *http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm*

[3] Robert Ellison and Carol Woody, "Supply-chain risk management: Incorporating security into software development," in *Proc. 43rd Hawaii Int. Conf. on System Sciences,* Poipu, Kauai, HI, 2010. *https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/acquisition/1140-BSI.html*

[4] Robert Ellison and Carol Woody, "Considering software supply-chain risks," CrossTalk, vol. 23, no. 5, pp. 9-12, Sep.-Oct. 2010.

[5] Robert J. Ellison, Christopher J. Alberts, Rita C. Creel, Audrey J. Dorofee, and Carol Woody, "Software supply chain risk management: From products to systems of systems," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2010-TN-026, 2010. *http://www.sei.cmu.edu/library/abstracts/reports/10tn026.cfm*