Miller *continued*

gated in systems acquisition and operations. Mapping attack vectors to vulnerabilities in order to determine specific countermeasures adds the dimensions of the supply chain and development lifecycle to the systems engineering-based design trade space and the overall risk-management process.

References

Baldwin, K., J. F. Miller, P. R. Popick, and J. Goodnight. 2012. "The United States Department of Defense Revitalization of System Security Engineering Through Program Protection." Paper presented at the 6th Annual Institute of Electrical and Electronics Engineers (IEEE) International Systems Conference, Vancouver, CA-BC, 19–23 March.

IEEE (Institute of Electrical and Electronics Engineers). 2008. IEEE 5288-2008. *Systems and Software Engineering—System Life Cycle Processes*.

ISO and IEC (International Organisation for Standardisation and International Electrotechnical Commission). 2011. ISO/IEC 15026-2:2011. Systems and Software Engineering—Systems and Software Assurance—*Part 2: Assurance Case*.

MITRE Corporation. 2012. *CAPEC—Common Attack Pattern Enumeration and Classification*. http://capec.mitre.org.

NIST (US National Institute of Standards and Technology). 2012. NIST SP 800-30. *Information Security—Guide for Conducting Risk Assessments*. Rev. 1.

Reed, M. 2012. "System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase with Hands-On Exercises." Tutorial presented at the 15th Annual NDIA Systems Engineering Conference, San Diego, US-CA, 22–25 Oct.

Wynn, J., J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart, and L. Clausen. 2011. MTR 110176. *Threat Assessment & Remediation Analysis (TARA)—Methodology Description*. Version 1.0. http://www.mitre.org/work/tech_papers/2012/11_4982.

Requirements Challenges in Addressing Malicious Supply Chain Threats

Paul R. Popick, paul.popick@incose.org**; and Melinda Reed,** melinda.reed@incose.org

In today's environment of cyber attacks and exploitation of system vulnerabilities, the systems engineer needs to be more aware of security during the system specification and design stage. Recent examples of supply chain attacks include computer motherboards shipping with malware, military chips from China with secret backdoors, and a bank employee inserting malware into the ATM network.

This article discusses the US Department of Defense (DoD) state of practice for incorporating trusted system and network security requirements into the specifications for large, complex systems. The article describes the current environment, the trends that are influencing the need for system security engineering, and the types of system security requirements and analysis techniques the DoD is using. This article updates the system security engineering risk-cost-benefit trade-off analysis described in previous papers (including Baldwin et al. 2012).

The trends that are contributing to the system-security challenges facing major DoD programs include the increasing reliance on commercially available technology, complex supply chains that include thousands of suppliers worldwide (figure 1), system interconnectedness, and the identification and exploitation of the supply chain and commercial off-the-shelf (COTS) vulnerabilities.

The complexity of supply chains and development processes of major acquisition programs (with prime contractors, subcontractors, suppliers, and subsuppliers) makes it difficult for anyone truly to know what is in the system and where it came from. Many of the COTS products have complex supply chains that are not secured to prevent alteration and malicious insertion. In addition, open-source code and code of unknown origin are often incorporated into the system's COTS components and the COTS tools used to develop DoD subsystems. These COTS and open-source

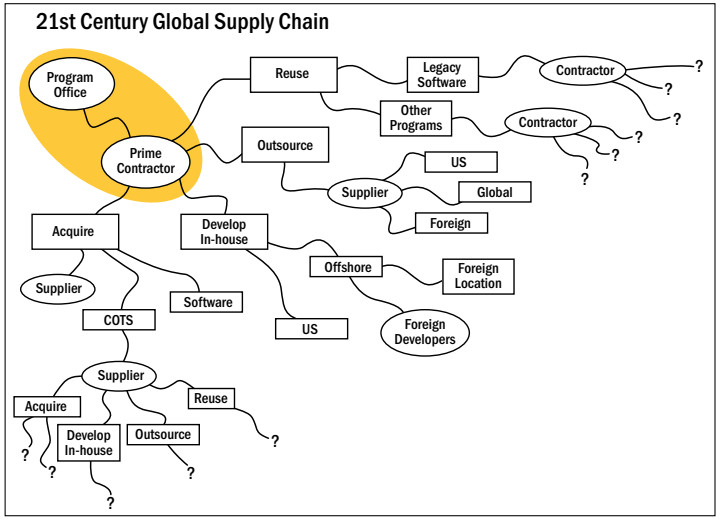

Figure 1. Global complexity of DoD supply chain

products are widely available for study, reverse engineering, and exploitation of vulnerabilities.

The systems engineer and system security engineer must consider not only the security of the system but also the security of the supply chain (see John Miller's article in this issue), the COTS products used in the system, and the information incorporated into the system as much of the development and manufacturing exist outside of traditional controls. In designing and trading off potential components, the systems engineer must consider whether the COTS products are vulnerable to attack within the supply chain, the development environment, the development process, the system maintenance process, and the operational system.

The motivations for exploiting these vulnerabilities include financial gain, exfiltration of data, denial of service, and alteration of mission results. For a further discussion of how attack vectors are linked with the vulnerability assessment and how attack vectors inform the requirements analysis, see John Miller's article.

Stakeholder needs are captured in the system-requirements documents from the sponsor and from applicable DoD directives and instructions (Kendall 2011; DoD 2012). The related DoD directives and instructions require that systems incorporate program protection, information assurance, protections related to the supply chain, counterfeit protections, and anti-tamper. These policies do not describe the details of the protections required, allowing the systems engineer and the systems security engineer the flexibility to define the specific requirements and design.

Security Analysis Trade-Off Method

The systems engineer and system security engineer analyze risk to determine appropriate trade-offs between security protection requirements and technical performance, cost, and schedule requirements. The systems engineer needs to recognize that vulnerabilities will continue to be identified during the system development and operation, and thus the system security requirements will need to be reassessed and updated as system requirements and design decisions are made. Regardless of the robust protection functions a program may incorporate to prevent attacks, the systems engineer and system security engineer also need to consider how to respond to an attack that penetrates the system. The systems engineer and system security engineer will need to incorporate functions that not only prevent but also detect and respond to attacks that exploit vulnerabilities.

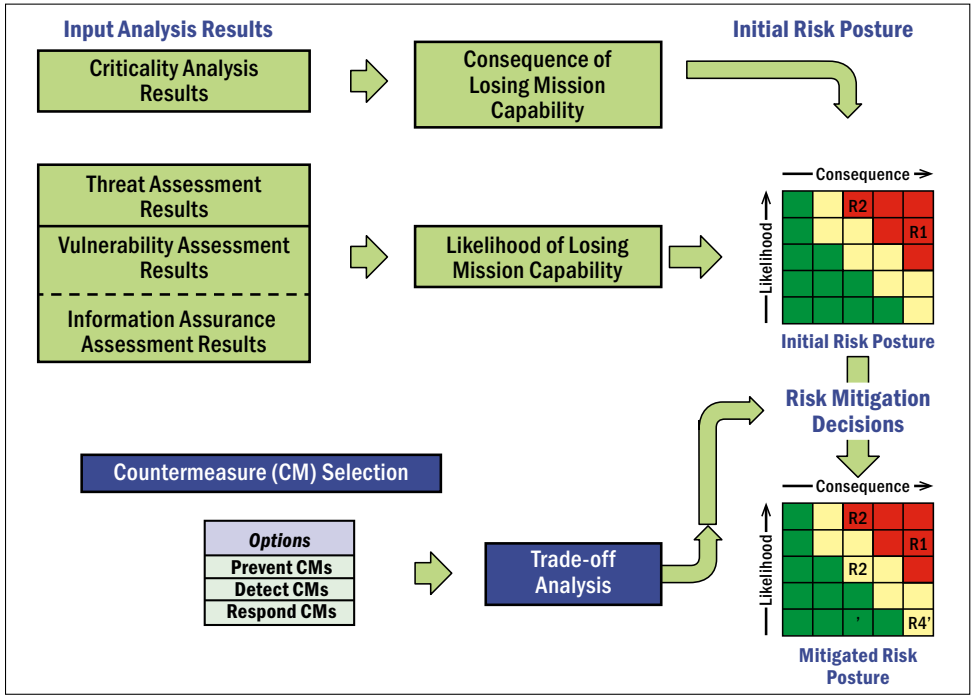

Figure 2. Risk-cost-benefit trade-off analysis method

To aid the systems engineer and system security engineer to analyze system security and to make trade-off decisions, the DoD has begun using an updated risk–cost–benefit trade-off analysis method for trusted systems and network security shown in figure 2. Note that the risk assessment depicted uses the criticality analysis for the consequence factor and a combination of the threat and vulnerability assessment as the likelihood factor.

Program managers and systems engineers apply this system security analysis method before each systems engineering technical review and periodically during the operations and maintenance phase of the DoD acquisition lifecycle. These updates of the system security analysis ensure that the program includes security updates to the system requirements and design characteristics that align with other updates as a result of elaborating the system. The method also promotes consistent system security engineering analysis across DoD programs as well as within a program. Figure 3 shows the points for systems engineering technical review in the DoD lifecycle where the system security analysis updates are incorporated into the requirements and design baselines.

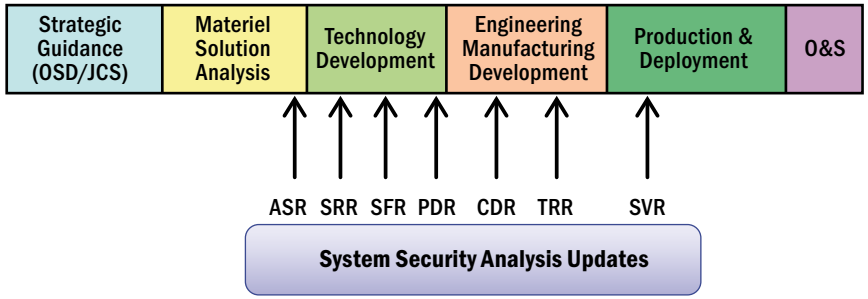

Figure 3. System security analysis updates in the DoD lifecycle

This analysis method requires multiple iterations to create or complete an update to the system security engineering analysis. There is no set sequence among the criticality analysis, threat assessment, vulnerability assessment, and the information assurance assessment steps; each step informs the other. The criticality analysis uses the initial concept description and the mission threads to determine the mission-critical functions and associated components. The criticality of the functions is grouped into the four levels shown in table 1.

Table 1. Protection failure criticality levels

Level I — Total Mission Failure
Level II — Significant Mission Failure
Level III — Partial/Acceptable Mission Failure
Level IV — Negligible Mission Degradation

Threat and Vulnerability Assessments

DoD systems are exposed to threats of malicious insertion and tampering throughout the development and supply of critical components from external and internal sources. This exposure is further exacerbated by the use of a significant number of COTS parts that are obtained through a global supply chain. Examples of malicious insertion threats are widely publicized and include telecommunication switches that exfiltrate data and radar systems that are unable to detect a particular country's planes.

The vulnerability assessment identifies weaknesses in system design, development, production, components, operation, and the supply chain that can be exploited to prevent or degrade the system's operation. During the requirements analysis, systems engineers evaluate potential vulnerabilities to critical function components to determine whether additional security requirements or constraints are needed to mitigate vulnerabilities. Identifying vulnerabilities extends the typical engineering process beyond the system to also consider the protection of the supply chain and the development environment. Systems engineers analyze the potential for the components to be exploited or subverted during development and supply, and they consider the potential to design in resiliency to allow the system to detect exploitation and continue to operate.

Early in the system-acquisition process, systems engineers need to identify potential vulnerabilities by examining the system concepts and critical functions for access paths. One approach is to list common vulnerabilities of the system, supply chain, and development environment, drawn from industry databases (SEI 2012; Mitre Corporation 2012) and the *Defense Acquisition Guidebook* (DAU 2012, chapters 4 and 13). Engineers can use this list to evaluate whether the requirements preclude these vulnerabilities. Another approach is to draw upon information-assurance and systems-security-engineering expertise to identify possible attack vectors and then use the attack vectors to determine whether the requirements prevent the attack. A vulnerability is listed for those attacks that are not prevented by the current set of requirements.

An analysis tool that DoD has used with both of these approaches is to draw a map of the movement of a critical component from the original equipment manufacturing through all of the intermediary contractors to the prime contractor showing the company name and the site location (figure 4).

This map helps the program identify vulnerabilities with each link in the supply chain. The vulnerability analysis results are used as part of the risk assessment to determine the likelihood of losing mission capability (figure 2).

The information-assurance assessment is a specialized vulnerability assessment that uses the system categorization along with the required baseline controls to identify confidentiality, integrity, and availability vulnerabilities to the system and the critical functions that are not prevented by the baseline controls. The results of the information-assurance assessment are combined with those from the vulnerability assessment to inform the risk assessment and assist with determining the strength of implementation required, tailoring of the control set, and translating the controls into requirements. The systems engineer and system security engineer need to ensure that threat, vulnerability, and information assurance assessments examine the findings from one another to avoid missing or duplicating vulnerabilities. Any previously identified vulnerabilities are used as part of each of the assessments. The systems engineer and system security engineer examine the system concept and requirements to determine the set of potential baseline and additional information assurance controls necessary to mitigate these risks to an acceptable level. The information assurance controls are defined by requirements and specific design details necessary to ensure they mitigate the identified confidentiality, integrity, and availability vulnerabilities. These mitigation requirements are captured in the system requirements, functional baselines and process requirements in the Statement of Work.

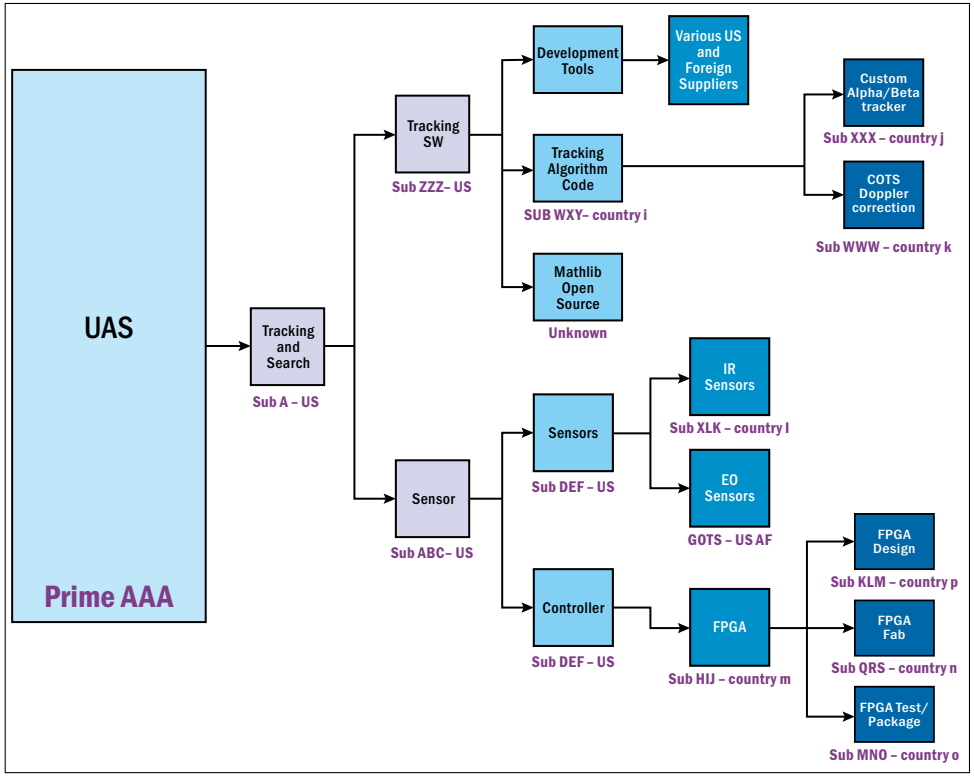

Figure 4. Supply-chain analysis map

The results of the criticality analysis, vulnerability assessment, threat assessment, and information-assurance assessment contribute to the risk assessment. Countermeasures are cost-effective activities and attributes to mitigate or neutralize threats to and vulnerabilities of the system-critical functions and associated components. They vary from process requirements to system requirements, constraints, and design attributes. Although potential countermeasures are often identified as part of each of the assessments, during this step the systems engineer develops a comprehensive list of potential countermeasures. The potential countermeasures list needs to include countermeasures that detect and respond to attacks as well as prevent the attacks.

For example, a system-detection countermeasure may be a function that is built into the system that identifies when a critical function is behaving in an unauthorized manner. It sends an alert and logs relevant data to allow for later forensic analysis. Similarly, a process-detection countermeasure may be one that limits update or insertion of software code, sends alerts about unauthorized access attempts, and logs data for later forensic analysis. A "respond" countermeasure determines how the system or the supply chain process reacts to an attack. The "detect" and "respond" countermeasures ensure that awareness and response capability are built into the system and its supporting processes.

Risk-Cost–Benefit Trade-Off

The risk–cost–benefit trade-off analysis includes two levels of trade-off analysis. The program conducts an analysis within the security domain to trade off the potential countermeasures to identify a cost-effective set of system security requirements. The other trade-off level considers the broader system functional and nonfunctional performance requirements and design characteristics to ensure a balanced trade-off of system security requirements versus performance and cost impacts. For example, a security countermeasure to monitor a critical function's behavior may lead to an unacceptable decrease in the function's throughput or response time. Similarly affordability of the system requirements may also necessitate examination of alternatives requirements. This leads to a dynamic environment in which systems engineering trade-off results outside the security domain trigger a need to update the system security engineering analysis and trade-offs.

Risk, cost, and benefit factors influence these two levels of trade-offs. The systems engineer may explore alternative designs to evaluate the new or revised requirements. The output of this step is a set of affordable countermeasure requirements to be incorporated into the system requirements baseline and acquisition-process requirements from the Statement of Work.

Future Plans

The defense department is just beginning to use this trusted systems and network analysis method for system security engineering. The method provides an objective way of analyzing and quantifying the system security and developing the system security requirements. Extending the system security engineering trade-off analysis into the supply chain, development processes, and the development tools requires systems engineering interactions with procurement and acquisition processes that are not normally employed during the system specification and design.

The need to address global supply-chain threats and development threats has made it necessary to implement in parallel with the development of system security engineering methods and tools. This concurrency leads to some confusion by the system security engineers as the methods and tools are continuously upgraded. DoD is developing an outreach and training program to ensure that the systems engineers and system security engineers are trained to perform this work.

Programs are finding it challenging to respond to changing supply-chain threats, development threats, and uncovered vulnerabilities. Using this method before each of the systems engineering technical reviews and periodically during operations may assist programs to respond to this challenge. This method emphasizes the affordability considerations through the cost–benefit trade-off to ensure that system security requirements are part of the overall acquisition and fielding of secure operational systems. In order to fully address supply-chain issues, the systems engineering community needs a comprehensive outreach approach to increase leadership awareness and to train program managers, systems engineers, and system security engineers. Professional societies, industry associations, and industrial firms have an important role to play in this outreach.

The Department of Defense has developed guidance for the *Defense Acquisition Guidebook* chapters 4 and 13 (DAU 2012) and has prepared awareness briefings for the acquisition community. This guidance has increased awareness of the need for system security engineering training for systems engineers and system security engineers. The DoD is developing training material and will incorporate it into courses at the Defense Acquisition University as well as continuing education courses offered through industry and professional organizations.

Information-assurance controls are documented and have been in use within the DoD for a number of years (US DoD 2003). The information-assurance control policy is currently being updated and will be issued in the near future to include supply-chain controls and a risk-management framework for cybersecurity (DoD, forthcoming). In systems engineering terms, the information-assurance controls need to be refined into system requirements because these controls are not described in sufficient detail to evaluate their effectiveness with respect to specific

» continues on next page

attack vectors or to specify a system for acquisition. Unfortunately in the past the information-assurance controls have not always been refined and incorporated into the system requirements. This can result in missing or overlapping requirements. The DoD is emphasizing the role of the system security engineering to ensure that the information-assurance controls are refined and incorporated into the system and process requirements.

The Systems Engineering Research Center and other federally funded research-and-development centers have initiated research into secure design methods for the operational system (SERC 2012; SEI 2009). Research is also needed to define secure design methods and process descriptions for the supply chain similar to those for the operational system. To date, the acquisition community has engaged in limited activity (DoD 2010) that has broadly defined the secure supply-chain approaches but has not defined them to the level of detail necessary distinguish between implementations. The DoD is sponsoring activities to begin developing catalogs of these supply-chain methods and is encouraging more industry research into secure supply-chain and software-assurance techniques.

References

Baldwin, K., J. F. Miller, P. R. Popick, and J. Goodnight. 2012. "The United States Department of Defense Revitalization of System Security Engineering through Program Protection." Paper presented at the IEEE Systems Conference, Vancouver, CA-BC, March.

DAU (US Defense Acquisition University). 2012. *Defense Acquisition Guidebook*. Fort Belvoir, US-VA: DAU. https://acc.dau.mil/ communitybrowser.aspx?id=332951.

DoD (US Department of Defense). 2003. DoD Instruction 8500.02. *Information Assurance Implementation*.

———. 2010. *Key Practices and Implementation Guide for the DoD Comprehensive National Cyber Initiative 11 Supply Chain Risk Management Pilot Program*. Washington, US-DC: Supply Chain Risk Management Program Management Office, Global Task Force.

———. 2012. DoD Instruction 5200.44. *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*.

———. In preparation. DoD Instruction 8500.01. *Cybersecurity*. Draft.

Kendall, F. 2011. "Document Streamlining–Program Protection Plan (PPP), Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics." Washington, US-DC: Under Secretary of Defense for Acquisition, Technology, and Logistics.

Mitre Corporation. 2012. *Common Weakness Enumeration: A Community-Developed Dictionary of Software Weakness Types*. http://cwe.mitre.org/.

SEI (Software Engineering Institute). 2009. CMU/SEI-2009-TR-010. *SEI Secure Design Patterns*. Pittsburg, US-PA: Carnegie-Mellon University, Software Engineering Institute.

———. 2012. "Top Ten Secure Coding Practices." Website of the Software Engineering Institute at Carnegie-Mellon University, Pittsburgh, US-PA. https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices.

SERC (Systems Engineering Research Center). 2012. SERC-2012-TR-028. *Security Engineering*.

July 2013 | Volume 16 Issue 2

A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING

INCOSE
International Council on Systems Engineering

INSIGHT

What's Inside

What's Inside

Special Feature

Systems Engineering Is Responsible for System Security