MTR140021

MITRE TECHNICAL REPORT

MITRE

Supply Chain Attack Framework and Attack Patterns

Sponsor: DASD SE
Dept. No.: Z610
Contract No.: W15P7T-13-C-F600
Project No.: 0713D050-AA

McLean, VA

John F. Miller
December 2013

Acknowledgments

The author would like to acknowledge and thank Peter Kertzner, a MITRE colleague whose active collaboration throughout FY13 provided many meaningful contributions to this product.

The author also appreciates the useful data, suggestions, and insight provided during the course of this study by other technical staff at MITRE and the project sponsoring office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD SE).

Table of Contents

List of Figures

1 Introduction

1.1 Objective

During FY13, MITRE conducted an effort on behalf of the Office of the Assistant Secretary of Defense for Systems Engineering (DASD SE) to address supply chain attacks relevant to Department of Defense (DoD) acquisition program protection planning. The objectives of this work were to:

- Pull together a comprehensive set of data sources to provide a holistic view of supply chain attacks of malicious insertion that, to date, has not been available.
- Generate a catalog of attack patterns that provides a structure for maturing the supply chain risk management (SCRM) aspects of system security engineering (SSE), together with potential application approaches for assessing malicious insertion in critical components of DoD systems being acquired or sustained.

1.2 Background and Motivation

Although SSE has traditionally been viewed as a specialty engineering area, it has become increasingly evident that implementing SSE to address emergent adversarial threats must be tightly integrated within a systems engineering (SE) approach. Yet, the security risks for large, complex systems are neither fully understood nor adequately addressed by the systems engineers responsible for system specification, design, implementation, and integration. To address this situation, DASD SE has engaged in a number of efforts to assure trusted systems and networks (TSN), including the development of an SSE methodology (Baldwin et al. 2012; Popick and Reed 2013) that is built upon standard SE processes (e.g., requirements definition and risk management) as well as traditional security practices (e.g., threat analysis and vulnerability assessment).

This SSE methodology provides a defined set of activities and analyses to be carried out by a multidisciplinary team led by systems engineers in order to identify and protect mission-critical system components. Successful implementation, however, depends on the availability of adequate data and procedures to carry out the defined activities; e.g., threat analysis and vulnerability assessment. Ongoing efforts by engineers and security professionals within several sub-disciplines of system security address threats, vulnerabilities, and attacks at various levels. Building on these sources, DASD SE has sponsored efforts to examine the supply chain and software development lifecycle contexts of threat activity (Reed 2012) and to develop associated attack vector understanding (Miller 2013).

The general nature of the threat is malicious exploitation of vulnerabilities in fielded systems. In addition to cyber attacks initiated during system operation, emergent, more complex threat-actor involvement can occur early in and throughout the acquisition lifecycle. By inserting malicious software and counterfeit components during system design and development and across the supply chain, adversaries can gain system control for later remote exploitation or plant “time bombs” that will degrade or alter system performance at a later time, either preset or event-triggered. The threat of malicious insertion and tampering throughout the development and supply of critical system components is thus a broad SE concern.

1.3 Approach and Results

Given the extensive push to strengthen the SCRM aspects of SSE and program protection over the past several years, MITRE undertook an effort to build on the previous attack vector understanding. This effort brought together various sources of information, gathered it into a supply chain attack framework that leverages it to be useful, and developed a catalog of specific supply chain attack patterns of malicious insertion of hardware (HW), software (SW), firmware (FW), and system information/data.

The framework and catalog were compiled to assist acquisition programs in understanding the nature and potential extent of supply chain attacks. The attack patterns cover a broad scope, but can be filtered and structured into views to help programs in their consideration of specific types of supply chain attacks.

2 Supply Chain Attack Framework and Attack Patterns

2.1 Description

This effort addressed SCRM in system acquisition and, specifically, the topic of supply chain attacks. The goal was to elaborate an understanding of attack patterns used to exploit vulnerabilities in the system-acquisition supply chain and throughout the system-development lifecycle. The early results of this work were published as an article on supply chain attack vectors (Miller 2013); and, the matured work and results covered in this report were the topic of a recent conference paper (Miller and Kertzner 2013).

2.1.1 Focus

The focus of this work was to gather a wide range of supply chain attack information and structure it in a useful framework to meet the cross-cutting needs of a diverse SCRM community. The goal was to provide a comprehensive view of supply chain attacks of malicious insertion across the full acquisition lifecycle that, to date, has not been available. The framework structures and codifies supply chain attacks using attack patterns that include associated threat and vulnerability information.

2.1.2 Expected Outcome

It is anticipated that the resulting catalog of attack patterns will:

- Help DoD programs acquire and sustain systems that are less vulnerable to supply chain attacks by addressing malicious insertion within the supply chain.
- Provide information to focus supply chain threat analyses and vulnerability assessments executed by acquisition program engineers as they perform a TSN analysis (DoD 2012).

2.2 Research Sources and Results

This section covers the research that provided the basis for the framework development and attack data-gathering effort. A broad scope of research sources was included initially, in order to analyze the problem space from a SE perspective, which included attacks of malicious insertion via the supply chain, network-based attacks against fielded systems, the connection between supply chain vulnerabilities that allow malicious insertion and the vulnerabilities implanted by malicious insertion that allow attacks during fielded operations, and the potential mitigations and risk-cost-benefit tradeoffs necessary to select countermeasures to effectively accomplish security risk mitigation.

While the focus of this effort was on the supply chain attack space, the broader awareness described above provided fruitful context information for shaping the attributes important to an elaboration of supply chain attacks. Accordingly, some of the sources focused on the countermeasure space, but also provided perspectives on the attack space being secured. For example:

- A Software Engineering Institute technical report (Dougherty et al. 2009) describes 15 secure design patterns in 3 categories. They provide general (reusable) solutions as implementable design guidance. The report includes a general reference to eliminating the introduction of vulnerabilities into code and mitigating the consequences of such vulnerabilities. Specific attack information is discussed for each design pattern, albeit indirectly and in an un-normalized, unstructured manner.

- Various research efforts at the University of Virginia describe 4 security practices, termed “smart, reusable security services,” intended to reduce the success of cyber attacks (Bayuk and Horowitz 2011; Jones and Horowitz 2012; Horowitz and Pierce 2013; Jones, Nguyen, and Horowitz 2011; Babineau, Jones, Horowitz 2012). These research papers contain a general reference to the threat of cyber attacks, particularly with regard to the use of commercial off-the-shelf (COTS) HW and SW.
- A MITRE Corporation Cyber Resiliency Engineering Framework describes 14 security practices/techniques intended to reduce the success of cyber attack (Bodeau and Graubart. 2011). These techniques are coordinated to different architectural layers that are susceptible to attack vector exploit (12 architectural layers are itemized).

While the above sources focused primarily on protections against fielded system attacks, other sources of countermeasures included protection against malicious insertion via the supply chain. Most notable among these is the SCRM Key Practices Guide (DoD-SCRM 2010) which describes 32 key practices (KPs) as risk mitigations for supply chain threats.

There are other, more directly related and ongoing efforts by engineers and security professionals within several sub-disciplines of system security. Those efforts address threats, vulnerabilities, and attacks at various levels. For example:

- The National Institute of Standards and Technology (NIST) recently updated and enhanced its guide for conducting information security risk assessments (NIST 2012). The guide describes threat events targeted at information systems and provides a compilation of representative examples of adversarial threat events.
- The Department of Homeland Security is sponsoring an ongoing effort to grow and maintain a publicly available catalog that provides a common attack pattern enumeration and classification (CAPEC) of typical methods for exploiting SW (MITRE Corporation 2012). The CAPEC attack patterns capture and communicate the SW attacker’s perspective, derived from the concept of design patterns applied in a destructive rather than constructive context and generated from in-depth analysis of real-world SW exploits.
- The MITRE Corporation has developed a Threat Assessment and Remediation Analysis (TARA) methodology to identify and assess cyber and supply chain threats and to select effective countermeasures (Wynn et al. 2011). The TARA methodology relies on a catalog of adversarial tactics, techniques, and procedures (TTPs) that has been built primarily from engagements with information system programs.

Building primarily on these three sources (i.e., NIST, CAPEC, and TARA), together with the above and other sources, this effort culminated in a robust catalog of supply chain attacks of malicious insertion (see Appendix A) and an initial set of potential countermeasures to mitigate those attacks (see Appendix B).

The SCRM Key Practices Guide, together with a generic, end-to-end supply chain system mapping, were used to help ensure that the catalog encompassed a broad set of supply chain attack patterns. Each of the 32 KPs tracks to at least one attack. And there are at least 8 attack patterns identified for each of the points of attack within the supply chain map (see paragraph 2.3 for further discussion).

The SCRM Key Practices Guide and the other sources mentioned above were also used to compile an initial set of countermeasures as a proof of concept for the overall process of tracing supply chain attacks to actionable guidance for risk reduction. The countermeasures that were identified by this effort (but not further elaborated) are:

- Secure Configuration Management of Software
- Prevent or Detect Critical Component Tampering
- Security-Focused Programming Languages
- Security-Focused Design and Coding Standards and Reviews
- Supply Chain Red Teaming
- Trusted Shipping
- Hardened Delivery Mechanisms
- Tracking Tags and Security Tags
- Pedigree Established Across the Supply Chain
- Bulk Spares Inventory
- Multiple Suppliers
- Trusted Suppliers
- Acquirer Anonymity
- Electromagnetic / Thermal Analysis
- Network Traffic Restriction
- Visual Inspection
- Cryptography
- Supply Chain Visibility
- Personnel Trust
- Software Update Security

2.3 Supply Chain Attack Framework Scope

Examples of supply chain attacks include the insertion of malicious SW into open-source libraries and the substitution of counterfeit HW components in a receiving department at a lower tier of the supply chain. The former exploits an acquisition process in order to create a design vulnerability (associated with open-source code) and the latter exploits a receiving department process weakness. With such broad-reaching concerns in mind, it is useful to consider exactly what was determined to be in scope for this effort and what was determined to be out of scope.

This effort generated a catalog of specific supply chain attack patterns, scoped as follows:

- The object of the attacks considered is:
    - Information and communications technology (ICT)[1] components of a weapon system (or ICT system) being acquired or sustained
- The types of supply chain attacks considered are:
    - Malicious insertion (which includes substitution, alteration, and malware insertion) of HW, SW, or FW in critical ICT components
    - Malicious insertion within any system related data or information (which includes requirements, design, manuals, architectures, and roadmaps)
- The timeframe of attacks considered includes:
    - Any time during the system acquisition lifecycle, including pre-acquisition, acquisition, or sustainment
- The points of attack within the supply chain are:

[1] ICT: "Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT)…" (DoD 2012)

- Locations (see Fig. 1): System and software development locations and their internal processes and environments; e.g., integrated development environments (IDEs)
  - Malicious activity that occurs at any location in the supply chain, including development tools and processes owned/used by that site/facility
  - Supply chain locations include the program office, prime contractor, and all tiers of sub-contractors/sub-suppliers and integrators (Included in these categories are the field support activities; e.g., parts depots and software support activities; and their suppliers)
- Between locations (see Fig. 2): Supply chain linkages
  - Malicious activity that occurs within the physical flow between supply chain locations (i.e., acquirer and supplier logistics networks)
  - Malicious activity that occurs within the information and data flow of the supply chain (i.e., acquirer and supplier external ICT/IDE environments)

Given this scope, the goal was to gather, structure, and elaborate the attack patterns used for malicious insertion in critical components across the full system-acquisition lifecycle by identifying exploitable weaknesses in the system-acquisition supply chain, using a generic, end-to-end supply chain system as illustrated in Figs. 1 and 2.

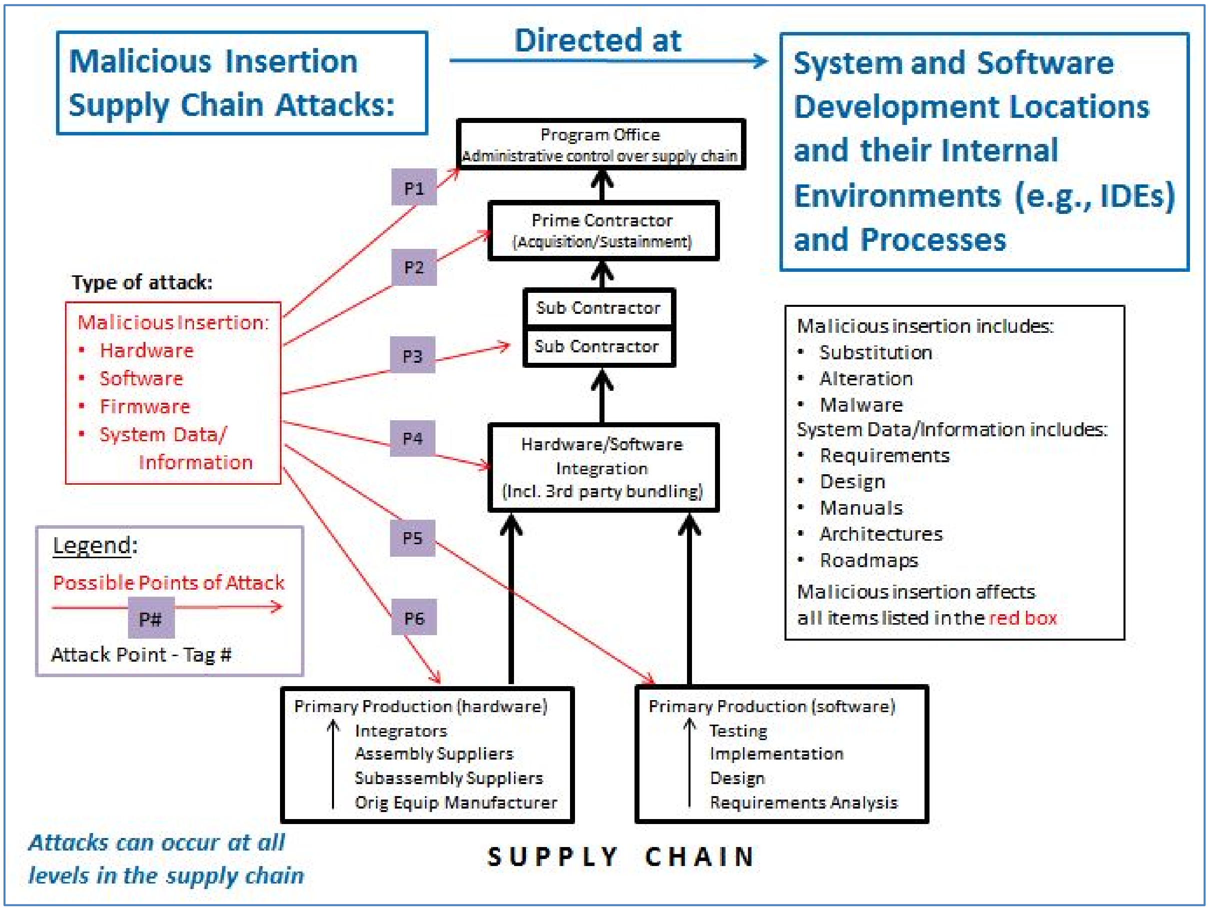


Figure 1. Points of Attack – Supply Chain Locations.

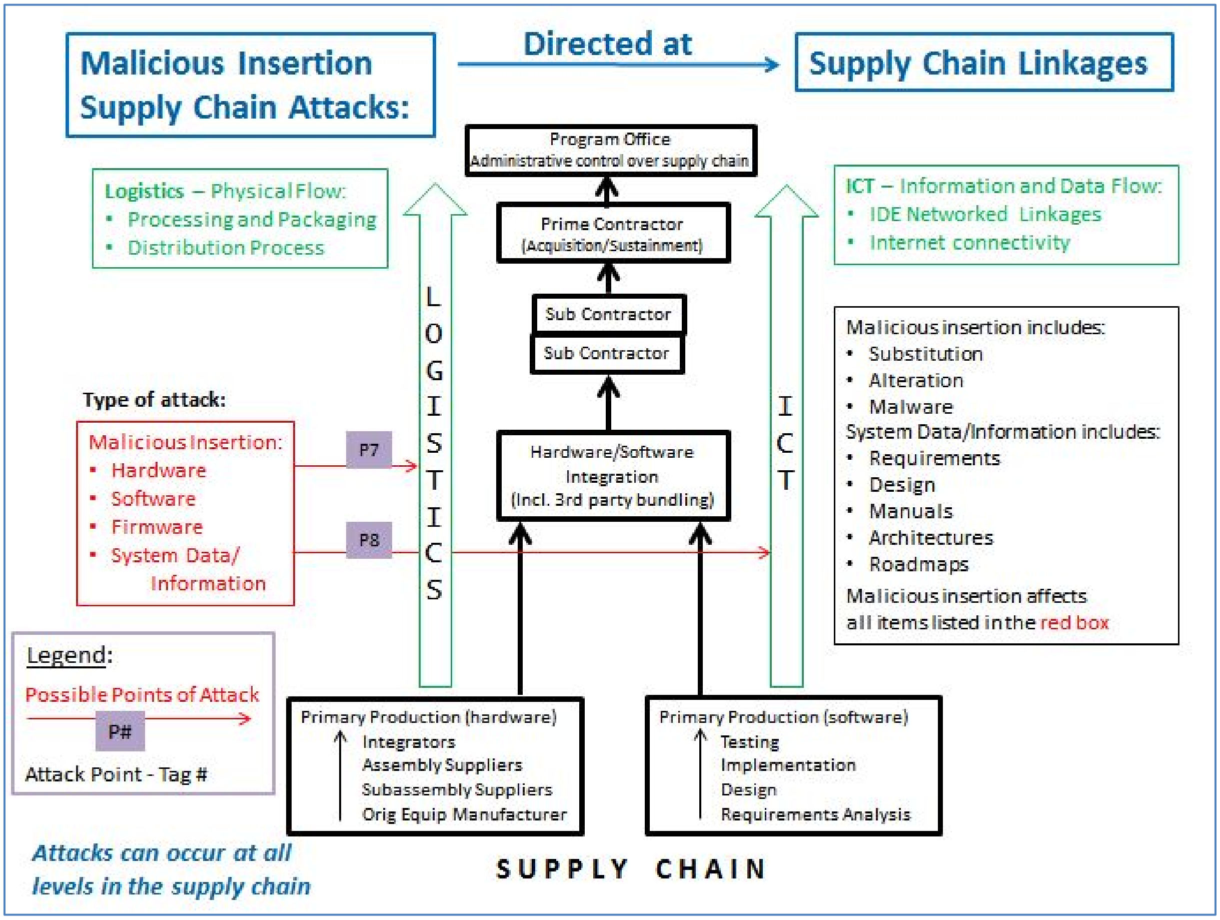


Figure 2. Points of Attack – Supply Chain Linkages.

The following example attacks provide further clarity with respect to scope:

- Supply chain vs. a fielded system:
  - In Scope: Supply chain attacks against the system being acquired/sustained
    - Example: Implantation of a backdoor in system SW during development or maintenance
  - Out of Scope: Network-based, insider, or physical attacks against a fielded system during operations
    - Example: Exploitation of a backdoor in system SW that was implanted during development or maintenance
- Support systems:
  - In Scope: Supply chain attacks against "first-order" (directly related to system development) support systems for the acquisition
    - Examples: Maliciously altered compilers; malicious SW inserted in a HW development environment; maliciously altered field-programmable gate array (FPGA) programming tools
  - Out of Scope: Supply chain attacks against "second-order" support systems for the acquisition
    - Example: Malicious insertion of code into a shipping and receiving system to subvert distribution processes

Supply chain threats other than malicious insertion are also out of scope for the current work (although they could be accommodated by a framework expansion). Out-of-scope examples include:

- Malicious extraction in the supply chain, including loss of:
  - Advanced technology
  - Intellectual property
  - Unclassified controlled technical information
- Considerations of non-attack based security threats and vulnerabilities
  - Example 1: Existing system design weaknesses (e.g., unintentional SW vulnerabilities) which could potentially be mitigated by supply chain countermeasures
  - Example 2: The contractor's use of a supplier for a critical-function application-specific integrated circuit (ASIC) different from the known/trusted supplier that was previously indicated in the contractor's procurement plans

2.4 Attack Pattern Catalog Details

The attack pattern catalog (see Appendix A) was created by using various sources of supply chain data and information and building on the TTPs of TARA, the supply chain elements of CAPEC, and the adversarial threats compiled by NIST (see the discussion and references in paragraph 2.2). The resulting collective body of attacks brings what has already been captured in TARA and CAPEC for the supply chain to a refined level of detail. The NIST data was mined and translated for its relevance and applicability to DoD system acquisition.

Adversarial attacks are composed of many attributes, including the adversarial threat source, the method used by the adversary, the action that causes malicious insertion, and the adversary's goal. This effort developed a supply chain attack framework to structure and describe supply chain attack patterns where each pattern is elaborated by context data – provided in the form of 12 specific attributes that structure and codify the attack pattern. The catalog provides the content for 41 attack patterns that can be analyzed in various ways to support threat analyses and vulnerability assessments.

The 12 attack attributes that frame each of the 41 attack patterns are:

- *Attack ID* (unique ID number)
- *Attack Point* (supply chain location or linkage)
- *Phase Targeted* (acquisition lifecycle phase)
- *Attack Type* (malicious insertion of SW, HW, FW, or system information/data)
- *Attack Act* (the "what")
- *Attack Vector* (the "how")
- *Attack Origin* (the "who")
- *Attack Goal* (the "why")
- *Attack Impact* (consequence if successful)
- *References* (sources of information)
- *Threat* (adversarial event directed at supply chain)
- *Vulnerabilities* (exploitable weaknesses)

A short description of each attribute is given in parentheses above. The detailed descriptions are provided in Fig. 3. The *Attack Point* tag ("P#") designations listed in Fig.3 are graphically illustrated in Figs. 1 and 2.

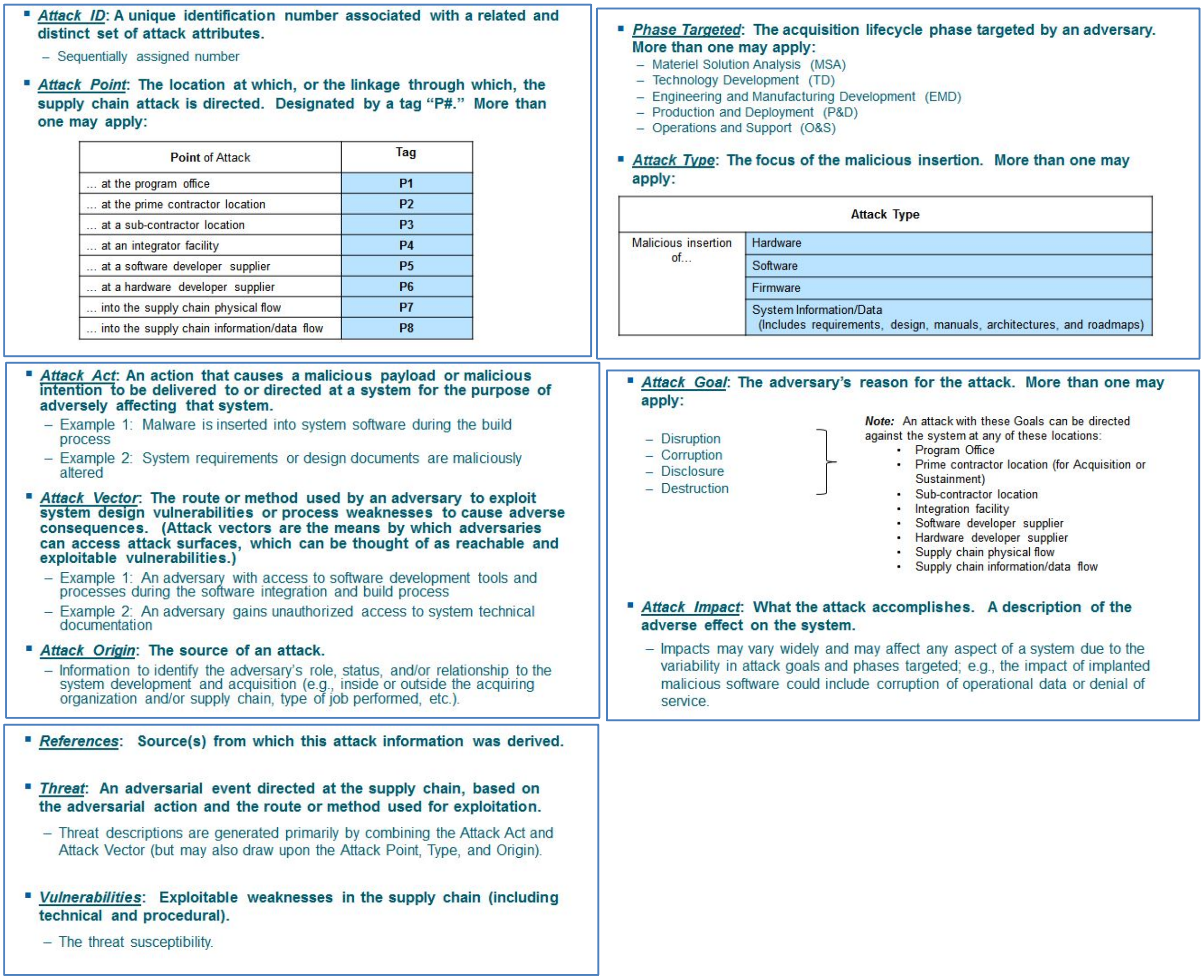


Figure 3. Attack Attributes Defined.

The attack patterns were built by populating the attack attributes in the framework with attack information gathered and structured from the various sources. It was often helpful to construct a graphic representation of the key attributes of an attack as it was being developed. For example, Fig. 4 illustrates an attack of malicious insertion of SW in any of the SW engineering environments of SW developers/contractors during any lifecycle phase after Milestone-B. (This is attack A3 in the catalog.)

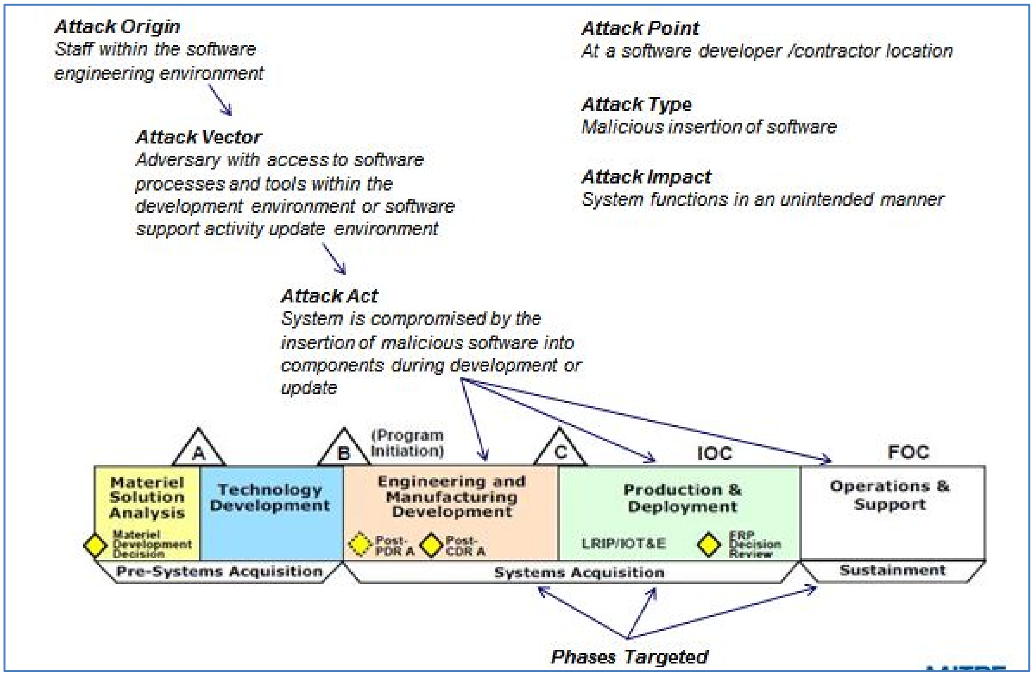


Figure 4. A Pictorial View of the Key Attributes for Attack A3.

The key attack information illustrated in Fig. 4 is what, how, and who. The *Attack Act* tells you what type of malicious insertion is targeted. The *Attack Vector* describes the how part – the route or method used by the adversary. The *Attack Origin* is the who part – the adversary's status, role, or relationship to the program.

Building on this information, the rest of the attributes for attack A3 were developed, and Fig.5 provides a snapshot of the attack from the final catalog.

Attack Identifier: A3

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): System is compromised by the insertion of malicious software into components during development or update.

Attack Vector: Adversary with access to software processes and tools within the development environment or software support activity update environment.

Attack Origin: Staff within the software engineering environment.

Attack Goal: Disruption: Yes Disclosure: Yes
Corruption: Yes Destruction:

Attack Impact: System may function in a manner that is unintended.

References: Based on NIST SP 800-30; page E-4

Threat: An adversary with access to software processes and tools within the development or software support environment can insert malicious software into components during development or update/maintenance.

Vulnerabilities: The development environment or software support activity environment is susceptible To an adversary inserting malicious software into components during development or update.

Attack Points: Program Office: Software Developer: Yes
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support: Yes

Figure 5. Attack Pattern A3.

Appendix A includes the fully elaborated attack patterns for all 41 supply chain attacks.

2.5 Utility

The most significant points concerning the utility of this work are:

- As previously mentioned, it pulls together a comprehensive set of sources to provide a holistic view of supply chain attacks that was previously not available.
- It provides a structure for maturing the SSE discipline (see paragraph 2.5.1).
- It can be used as a decision support tool by acquisition programs for the SCRM aspects of program protection (see paragraph 2.5.2).

2.5.1 Maturing the SSE Discipline

The structure and content of the catalog can be analyzed in various ways to provide insight into the understanding of current supply chain attacks. There are various ways in which the catalog will support supply chain attack analysis and evaluation. For example, Fig. 6 shows the distribution of the 41 attack patterns across both the types of critical components that need to be protected and the lifecycle phases targeted by the attacks. There is a fairly even distribution between HW and SW; and, malicious insertion in FW and system information/data are also important.

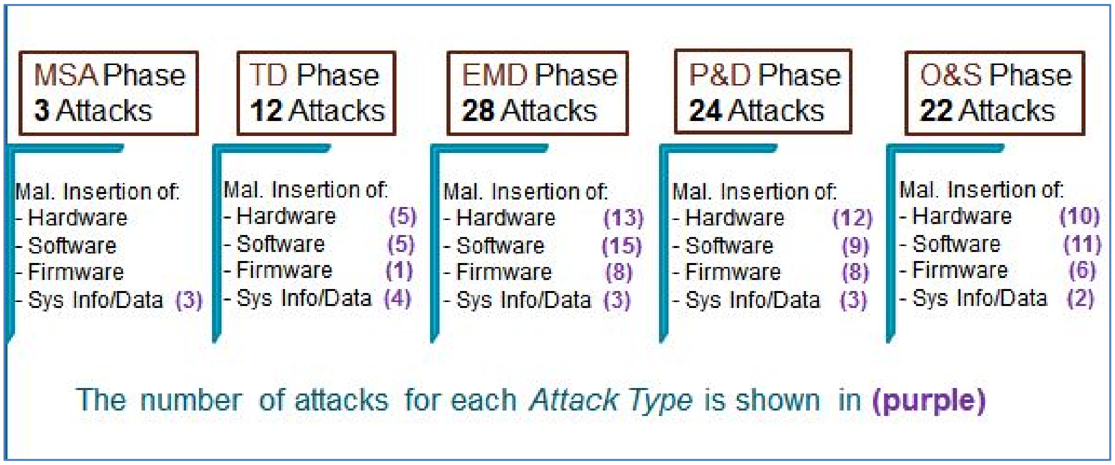


Figure 6. Analysis of Attack Types by Phase.

While it is no surprise that the EMD phase is susceptible to the greatest number of attacks (cf. Fig. 6), it is insightful to examine how some of these attacks are applicable across the lifecycle. Figure 7 illustrates that many attacks are applicable across multiple phases.

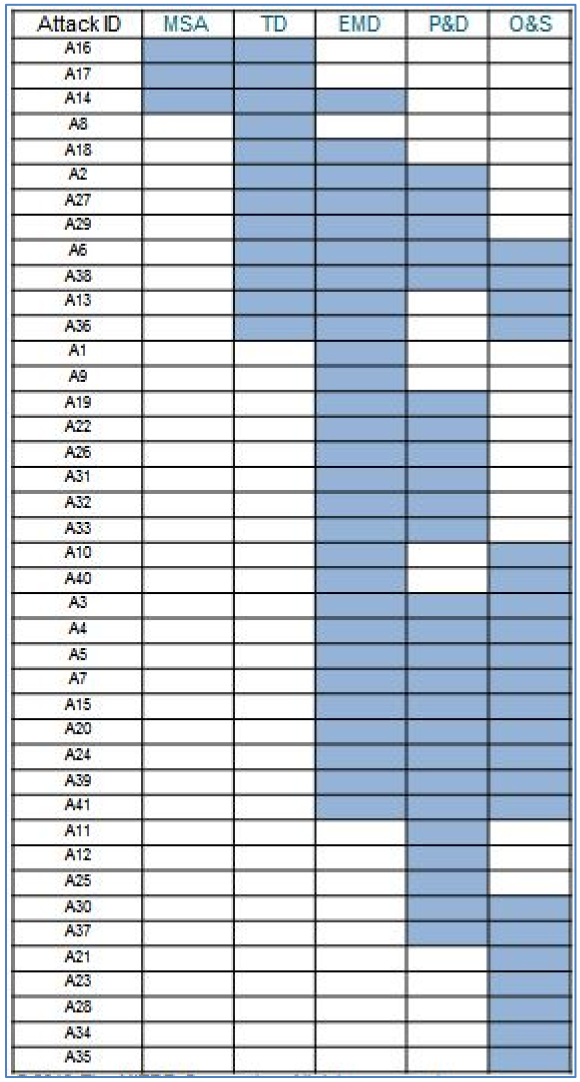


Figure 7. Analysis of Phase Applicability Based on Current Attack Understanding.

Several conclusions can be drawn from this analysis:

- Most attacks are applicable across multiple phases
- There are a significant number of TD phase attacks
    - (Planning for these attacks should occur during the MSA phase)
- Early mitigation planning should aim to leverage cost-effective protection across the lifecycle
- Over 2/3 of the attacks are applicable to the EMD phase
- Most attacks applicable to P&D are applicable in earlier phases as well
- There are important attacks that target only the sustainment supply chain

The analysis shown in Fig. 8 demonstrates what can be learned about the potential points of attack for each attack.

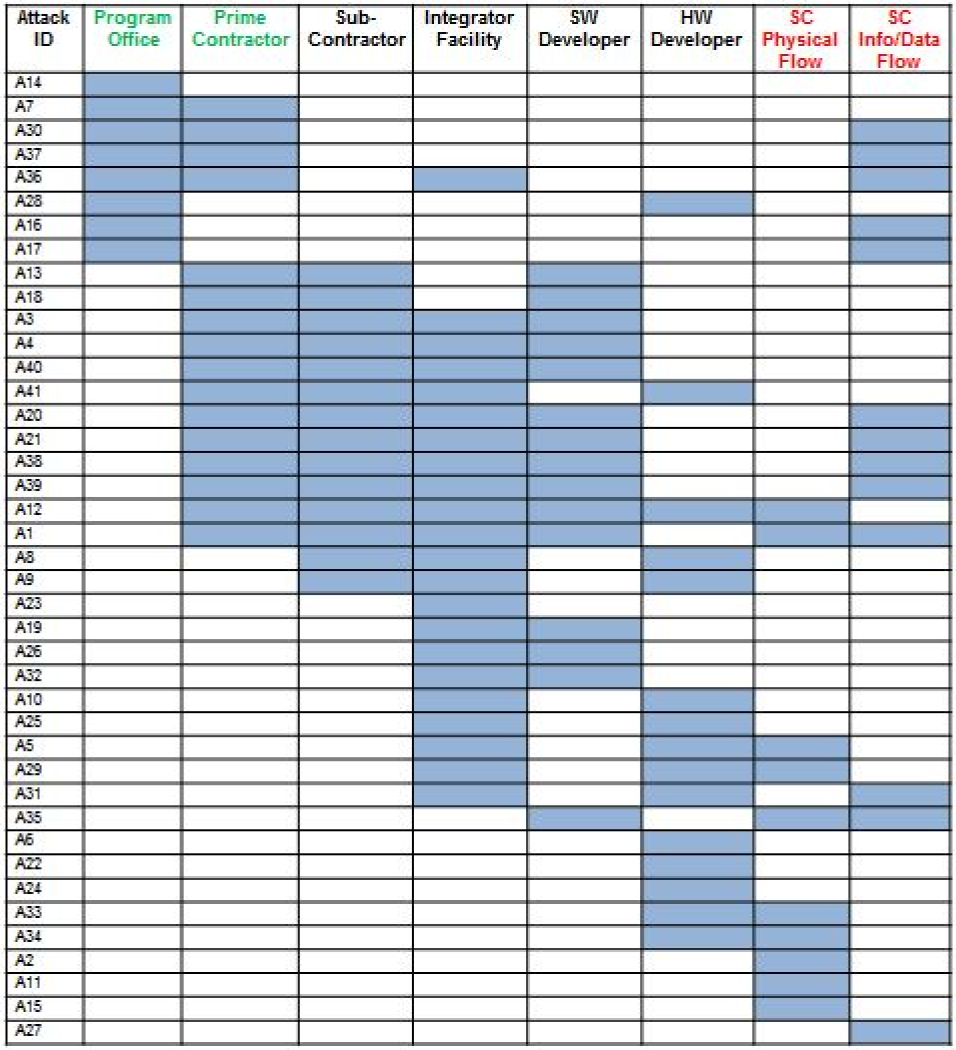


Figure 8. Analysis of Attack Point Applicability.

Conclusions from this analysis include:

- About half of the attacks can occur at either the program office or prime contractor locations
- Most attacks applicable to primes are also applicable to lower tiers
- Most attacks applicable to sub-contractors are also applicable to integrator facilities
- SW developer suppliers and HW developer suppliers are targeted by the same number of attacks

While this paragraph has provided several basic analyses, the attack patterns can be filtered and structured into other views to support program-specific consideration of specific types of supply chain attacks.

2.5.2 Concept of Use as a Decision Support Tool

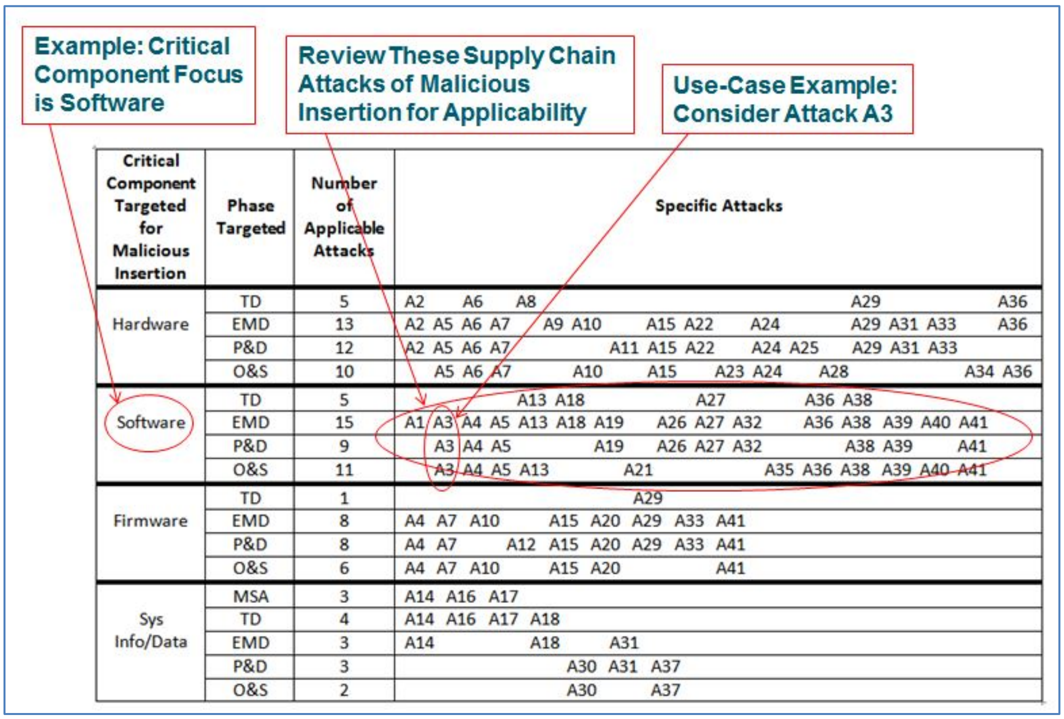
The attack pattern catalog provides an elaboration of malicious insertion of HW, SW, FW, and system information and data into critical components of a DoD system being acquired or sustained. Acquisition programs may find this compilation useful for:

- Estimating and establishing program protection and SSE resourcing levels
- Guiding the TSN analysis

- Selecting and validating countermeasures
- Supporting abuse case analysis
- Performing supply chain penetration testing to verify how secure the supply chain really is against malicious insertion

This paragraph focuses on a potential application approach for supporting acquisition program engineers as they perform a TSN analysis. As a decision support tool, the framework content can be analyzed and applied in various ways to zero in on specific types of supply chain attacks and inform, from a technical and procedural point of view, the supply chain threat analyses and vulnerability assessments across the full lifecycle.

As an example scenario to illustrate how the framework might be used, suppose that your mission-critical system components have been identified through a criticality analysis and you want to use the catalog to identify potential attacks of malicious insertion. You have many mission-critical SW components, so your current focus is on potential SW attacks that might occur during the EMD phase and beyond. Figure 9 filters and sorts all the attack patterns according to the types of critical components and phases targeted.



Critical Component Targeted for Malicious Insertion	Phase Targeted	Number of Applicable Attacks	Specific Attacks
Hardware	TD	5	A2 A6 A8 A29 A36
	EMD	13	A2 A5 A6 A7 A9 A10 A15 A22 A24 A29 A31 A33 A36
	P&D	12	A2 A5 A6 A7 A11 A15 A22 A24 A25 A29 A31 A33
	O&S	10	A5 A6 A7 A10 A15 A23 A24 A28 A34 A36
Software	TD	5	A13 A18 A27 A36 A38
	EMD	15	A1 A3 A4 A5 A13 A18 A19 A26 A27 A32 A36 A38 A39 A40 A41
	P&D	9	A3 A4 A5 A19 A26 A27 A32 A38 A39 A41
	O&S	11	A3 A4 A5 A13 A21 A35 A36 A38 A39 A40 A41
Firmware	TD	1	A29
	EMD	8	A4 A7 A10 A15 A20 A29 A33 A41
	P&D	8	A4 A7 A12 A15 A20 A29 A33 A41
	O&S	6	A4 A7 A10 A15 A20 A41
Sys Info/Data	MSA	3	A14 A16 A17
	TD	4	A14 A16 A17 A18
	EMD	3	A14 A18 A31
	P&D	3	A30 A31 A37
	O&S	2	A30 A37

Figure 9. Use-Case Scenario Attacks for Consideration.

For this use-case, you might want to review all the attacks that are circled in the large red oval in Fig. 9 (i.e., A1, A3, A4, A5, A13, etc.) in order to get a holistic sense of the potential attacks of malicious insertion targeting SW.

Most of the attacks are applicable across multiple lifecycle phases. Dealing with such attacks early can limit the costs of securing the supply chain later. Some of the attacks are applicable during the TD phase and, although your immediate interest is in the EMD phase and beyond, it may prove useful to consider what might have been done for protection during the TD phase and whether this type of attack is still a significant concern for your program.

Selecting attack A3 to continue this use-case example, you next examine the key attributes of that attack pattern (which were graphically presented in Fig. 4 and discussed in paragraph 2.4).

Based on that analysis, you determine the applicability of attack A3 to your program-specific supply chain structure and your SW engineering environment(s) with a consideration of how they will change over time across the EMD, P&D, and O&S phases of acquisition.

Each attack pattern in the catalog includes specific threat and vulnerability information associated with that attack. Figure 5 provided a snapshot of attack A3 from the catalog. By examining the *Threat* and *Vulnerabilities* attributes for attack A3, it can readily be seen that the *Attack Act* and *Attack Vector* (with supporting information from the *Attack Origin*) are primarily what feed into describing the *Threat* and *Vulnerability* that A3 delivers.

For attack A3, the following information from the catalog may prove useful to the TSN analysis and to the subsequent development of the Program Protection Plan (PPP) (DASD SE 2011):

- *Threat*: An adversary with access to software processes and tools within the development or software support environment can insert malicious software into components during development or update/maintenance.
- *Vulnerabilities*: The development environment or software support activity environment is susceptible to an adversary inserting malicious software into components during development or update.

In summary, the anticipated uses and benefits of the supply chain attack framework and catalog include the following:

- Users can zero in on specific types of supply chain attacks that can harm their systems, whether in acquisition or in the field
- The attack pattern data can be sorted on any of the attributes as deemed relevant by the user (e.g., the *Attack Type*, the *Phase Targeted*, or the *Attack Point*)
- Users include DoD programs (and their contractors) charged with performing a TSN analysis to protect critical components
- Results can inform specific sections of the PPP; e.g., sections 5.1 (Threats in Table 5.1-2) and 5.2 (Vulnerabilities in Table 5.2-1)

3 Potential Next Steps

When used across programs or domains, this supply chain attack framework and catalog might improve consistency and uniformity in SCRM related analyses and reports. This catalog of information could form the basis of future supply chain attack characterization. Potential next steps could include:

- Program engagements
  - Walk through use-cases and/or support abuse case development with selected programs
  - Use the engagements to inform implementation concepts and improve the framework and its content (e.g., to inform TSN analysis and improve PPP)
- Partnerships
  - Form partnerships, to include Microelectronics and Software Assurance interests, to ensure broadest possible coverage of supply chain attacks
  - Ensure supply chain attack and countermeasure work meets the cross-cutting needs of a diverse set of constituents
- Transition strategy
  - Determine how this work can be structured and institutionalized to maximize usability and benefit
  - Examine alternative approaches and strive to have this work brought into existing/developing catalogs and guidance

4 References

Babineau, G.L., R.A. Jones, and B.M. Horowitz. 2012. "A System-Aware Cyber Security Method for Shipboard Control Systems," IEEE Homeland Security Conference 2012.

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, BC, 19-23 March.

Bayuk, J.L. and B.M. Horowitz. 2011. "An Architectural Systems Engineering Methodology for Addressing Cyber Security," Systems Engineering, 14, 294-304.

Bodeau, D.J. and R. Graubart. 2011. *Cyber Resiliency Engineering Framework*. The MITRE Corporation Technical Report MTR 110237. September.

DoD (Department of Defense). 2012. DoD Instruction (DoDI) 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)." 5 November.

DoD (Department of Defense) SCRM Program Management Office (PMO). 2010. *Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program*. 25 February.

DASD SE (Deputy Assistant Secretary of Defense for Systems Engineering). 2011. *Program Protection Plan Outline & Guidance, Ver 1.0*. July.

Dougherty, C., K. Sayre, R.C. Seacord, D. Svoboda, and K. Togashi. 2009. *Secure Design Patterns*. Software Engineering Institute (SEI) Technical Report CMU/SEI-2009-TR-010. October.

Horowitz, B.M. and K. Pierce. 2013. "The Integration of Diversely Redundant Designs, Dynamic System Models and State Estimation Technology to the Cyber Security of Physical Systems," Systems Engineering Volume 16, No. 3.

Jones, R.A. and B.M. Horowitz. 2012. "A System-Aware Cyber Security Architecture," Systems Engineering, Volume 15, No. 2.

Jones, R.A., T.V. Nguyen, and B.M. Horowitz. 2011. "System-Aware Security for Nuclear Power Systems," IEEE Homeland Security Conference 2011.

Miller, J.F. 2013. "Addressing Attack Vectors Within the Acquisition Supply Chain and the System-Development Lifecycle." INSIGHT Vol. 16, Issue 2, July.

Miller, J.F., and P.D. Kertzner. 2013. "A Supply Chain Attack Framework to Support Department of Defense Supply Chain Security Risk Management." Paper presented at the 16th Annual NDIA Systems Engineering Conference, Crystal City, VA, 28-31 October.

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

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

Popick, P.R., and M. Reed. 2013. "Requirements Challenges in Addressing Malicious Supply Chain Threats." INSIGHT Vol. 16, Issue 2, July.

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, 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.

Appendix A Supply Chain Attack Pattern Catalog

****

This catalog contains the supply chain attack patterns that target the malicious insertion of Hardware, Software, Firmware, and/or System Information and Data.

Attack Identifier: A1

Target (Attack Type): Hardware: Firmware:

Software: Yes Sys Information or Data:

Description (Attack Act): "Targeted" malware (e.g., specifically designed to later take control of system, identify and exhilarate data or information, and conceal these actions) is introduced into system software during development.

Attack Vector: An adversary uses common delivery mechanisms (e.g., email attachments or removable media) to infiltrate the IDE or other development environment tools.

Attack Origin: An outsider with knowledge of the development environment, staff, and/or procedures.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the "targeted" capability of the malware. System may function in a manner that is unintended.

References: Based on NIST SP 800-30; page E-2

Threat: During software development, an outsider with knowledge of the development environment, staff, and/or procedures can breach the security of the IDE and/or other software development environment tools for unauthorized insertion of malware.

Vulnerabilities: The IDE and/or other software development environment tools are susceptible to an outsider (with knowledge of the development environment, staff, and/or procedures) inserting malware.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Yes Hardware Developer:

Sub-Contractor: Yes Physical Flow: Yes

Integrator Facility Yes Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment:

Operations and Support:

Attack Identifier: A2

Target (Attack Type): Hardware: Yes Firmware:
Software: Sys Information or Data:

Description (Attack Act): Legitimate hardware is replaced with faulty counterfeit or tampered hardware in the supply chain distribution channel.

Attack Vector: Adversary intercepts hardware from legitimate suppliers en route to contractor/integrator (in order to modify or replace it).

Attack Origin: Supply chain distribution personnel (packaging, shipping, receiving, or transfer).

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the counterfeit or tampered hardware.

References: Based on NIST SP 800-30; page E-3(Also based on TARA)

Threat: Adversarial supply chain distribution channel personnel (e.g., packaging, shipping, receiving, or transfer) can intercept and replace legitimate critical hardware components with malicious ones.

Vulnerabilities: The distribution channel (e.g., packaging, shipping, receiving, or transfer) is susceptible to adversarial personnel intercepting and replacing legitimate critical hardware components with malicious ones.

Attack Points: Program Office: Software Developer:
Prime Contractor: Hardware Developer:
Sub-Contractor: Physical Flow: Yes
Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development: Yes
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A3

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): System is compromised by the insertion of malicious software into components during development or update.

Attack Vector: Adversary with access to software processes and tools within the development environment or software support activity update environment.

Attack Origin: Staff within the software engineering environment.

Attack Goal: Disruption: Yes Disclosure: Yes
Corruption: Yes Destruction:

Attack Impact: System may function in a manner that is unintended.

References: Based on NIST SP 800-30; page E-4

Threat: An adversary with access to software processes and tools within the development or software support environment can insert malicious software into components during development or update/maintenance.

Vulnerabilities: The development environment or software support activity environment is susceptible To an adversary inserting malicious software into components during development or update.

Attack Points: Program Office: Software Developer: Yes
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support: Yes

Attack Identifier: A4

Target (Attack Type): Hardware: Firmware: Yes

Software: Yes Sys Information or Data:

Description (Attack Act): Malicious logic (e.g., a back-door Trojan) is programmed into software or microelectronics (e.g., FPGAs) during development or an update.

Attack Vector: An adversary with access privileges within the software or firmware configuration control system during coding and logic-bearing component development.

Attack Origin: A software or firmware programmer during coding and integration.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the malicious logic.

References: Based on CAPEC: Attack ID 441 (c/o Bob Martin)

Threat: A software or firmware programmer with access to the configuration control system can introduce malicious logic into software or microelectronics during coding and/or logic-bearing component development or update/maintenance.

Vulnerabilities: The configuration control system is susceptible to the introduction of malicious logic into software or firmware/microelectronics during coding, integration, and/or logic-bearing component development or update/maintenance.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Yes Hardware Developer:

Sub-Contractor: Yes Physical Flow:

Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support: Yes

Attack Identifier: A5

Target (Attack Type): Hardware: Yes Firmware:

Software: Yes Sys Information or Data:

Description (Attack Act): Malware is embedded in a replacement server motherboard (e.g., in the flash memory) in order to alter server functionality from that intended.

Attack Vector: An adversary with access to the procurement, maintenance, and/or upgrade of servers, during the server procurement or hardware update process.

Attack Origin: A software-savvy adversary with hardware procurement control deep in the supply chain.

Attack Goal: Disruption: Disclosure: Yes

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the malware.

References: Based on web post by Slashdot: Dell Ships Infected Motherboards July 21, 2010(c/o Rick Dove)

Threat: An adversary with access to hardware procurement, maintenance, or upgrade control can embed malware in a critical component server motherboard.

Vulnerabilities: The control processes and mechanisms for hardware procurement, maintenance, and/or upgrade are susceptible to embedded malware in a critical component server motherboard.

Attack Points: Program Office: Software Developer:

Prime Contractor: Hardware Developer: Yes

Sub-Contractor: Physical Flow: Yes

Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support: Yes

Attack Identifier: A6

Target (Attack Type): Hardware: Yes Firmware:

Software: Sys Information or Data:

Description (Attack Act): A microprocessor (or other chip) with a secret backdoor is substituted for a legitimate hardware component, where the backdoor is in the actual chip itself rather than in the firmware installed on it.

Attack Vector: An adversary with the ability to introduce malicious microelectronics components into the commodity procurement process without independent testing of those devices.

Attack Origin: A microelectronics manufacturer deep in the supply chain.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the backdoor.

References: Based on web post by samzenpus (protect-ya-neck dept.)(c/o Rick Dove)

Threat: An adversary with access to the hardware commodity procurement process can insert improperly vetted or untested malicious critical microelectronics components into the system during development.

Vulnerabilities: The hardware commodity procurement process is susceptible to insertion of improperly vetted or untested malicious critical microelectronics components during system development.

Attack Points: Program Office: Software Developer:

Prime Contractor: Hardware Developer: Yes

Sub-Contractor: Physical Flow:

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development: Yes

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support: Yes

Attack Identifier: A7

Target (Attack Type): Hardware: Yes Firmware: Yes

Software: Sys Information or Data:

Description (Attack Act): A microelectronics component (e.g., an FPGA) containing malicious logic (e.g., a back-door) is substituted for an approved, delivered component by direction from the program office or the prime contractor.

Attack Vector: An adversary positioned to direct program activity to cause the inclusion of compromised microelectronics components in the system being acquired or sustained.

Attack Origin: A program office or prime contractor engineer ("trusted insider").

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the malicious logic.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary positioned to direct program activity can cause the inclusion of compromised microelectronics components in the system being acquired or sustained.

Vulnerabilities: Trusted-insider processes for directing program activity are susceptible to an adversary positioned and able to direct the inclusion of compromised microelectronics components in the system being acquired or sustained.

Attack Points: Program Office: Yes Software Developer:

Prime Contractor: Yes Hardware Developer:

Sub-Contractor: Physical Flow:

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support: Yes

Attack Identifier: A8

Target (Attack Type): Hardware: Yes; Firmware: ; Software: ; Sys Information or Data:

Description (Attack Act): A maliciously altered hardware component is substituted for a baseline component at the PDR timeframe.

Attack Vector: An adversary with access to system components during allocated baseline development.

Attack Origin: Assembly sub-contractor engineers and technicians.

Attack Goal: Disruption: Yes; Disclosure: ; Corruption: ; Destruction:

Attack Impact: System may function in a manner that is unintended, leading to disruption of the acquisition program and system design process.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component in the PDR timeframe.

Vulnerabilities: Access to system components during allocated baseline development is susceptible to substitution of a maliciously altered hardware component for a baseline component in the PDR timeframe.

Attack Points: Program Office: ; Software Developer: ; Prime Contractor: ; Hardware Developer: Yes; Sub-Contractor: Yes; Physical Flow: ; Integrator Facility: Yes; Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development: Yes
Engineering and Manufacturing Development:
Production and Deployment:
Operations and Support:

Attack Identifier: A9

Target (Attack Type): Hardware: Yes Firmware:
Software: Sys Information or Data:

Description (Attack Act): A maliciously altered hardware component is substituted for a legitimate component during system test and integration.

Attack Vector: An adversary with access to system components during system test and evaluation.

Attack Origin: Test engineers and hardware integrators at a lower tier in the supply chain.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: System may function in a manner that is unintended.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to system components during system test and evaluation can substitute a maliciously altered hardware component for a legitimate component during system test and integration.

Vulnerabilities: Access to system components during system test and evaluation is susceptible to substitution of a maliciously altered hardware component for a legitimate component during system test and integration.

Attack Points: Program Office: Software Developer:
Prime Contractor: Hardware Developer: Yes
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment:
Operations and Support:

Attack Identifier: A10

Target (Attack Type): Hardware: Yes; Firmware: Yes; Software: ; Sys Information or Data:

Description (Attack Act): A counterfeit component is supplied from a lower-tier component supplier to a sub-system developer or integrator, which is then built into the system being acquired or sustained.

Attack Vector: An adversary with the ability to introduce counterfeit components into the procurement process in such a way that they are not thoroughly tested or otherwise verified for security. Includes hardware and firmware acquired through a commodity purchase, system acquisition, or sustainment process.

Attack Origin: A small-company component supplier feeding into the acquisition or sustainment supply chain.

Attack Goal: Disruption: Yes; Disclosure: ; Corruption: Yes; Destruction:

Attack Impact: System may function in a manner that is unintended.

References: Based in part on Slashdot, March 09, 2010; as well as a web post by kdawson (do-not-get-too-close-to-the-viewfinder dept.)(c/o Rick Dove)

Threat: An adversary with access to the procurement process can introduce counterfeit hardware and firmware components that have not been thoroughly tested or verified for security.

Vulnerabilities: The supply chain lower-tier component procurement process is susceptible to the introduction of counterfeit hardware and firmware components that have not been thoroughly tested or verified for security.

Attack Points: Program Office: ; Software Developer: ; Prime Contractor: ; Hardware Developer: Yes; Sub-Contractor: ; Physical Flow: ; Integrator Facility: Yes; Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment:
Operations and Support: Yes

Attack Identifier: A11

Target (Attack Type): Hardware: Yes | Firmware: | Software: | Sys Information or Data:

Description (Attack Act): A maliciously altered hardware component is substituted for a tested and approved component.

Attack Vector: An adversary with access to production component supplier shipping channels during transfer of system components.

Attack Origin: Component transfer personnel (e.g., shipping, receiving, and transferring) at a lower tier in the supply chain, including transportation companies.

Attack Goal: Disruption: Yes | Disclosure: | Corruption: Yes | Destruction: Yes

Attack Impact: System may function in a manner that is unintended, including destruction.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to production component supplier shipping channels during transfer of system components can substitute a maliciously altered hardware component for a tested and approved component.

Vulnerabilities: The supplier shipping channels, during transfer of system components, are susceptible to the substitution of maliciously altered hardware components for tested and approved components.

Attack Points: Program Office: | Software Developer: | Prime Contractor: | Hardware Developer: | Sub-Contractor: | Physical Flow: Yes | Integrator Facility: | Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development:
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A12

Target (Attack Type): Hardware: Firmware: Yes

Software: Sys Information or Data:

Description (Attack Act): A counterfeit firmware component is substituted for an authentic component.

Attack Vector: An adversary with access to production component supplier shipping channels during transfer of system components.

Attack Origin: Component transfer personnel (e.g., shipping, receiving, and transferring) at a lower tier in the supply chain, including transportation companies.

Attack Goal: Disruption: Yes Disclosure:

Corruption: Yes Destruction: Yes

Attack Impact: System may function in a manner that is unintended, including destruction.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to supplier shipping channels during transfer of system components can substitute a counterfeit firmware component for an authentic component.

Vulnerabilities: Access to supplier shipping channels during transfer of system components is susceptible to the substitution of counterfeit firmware components for authentic components.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Yes Hardware Developer: Yes

Sub-Contractor: Yes Physical Flow: Yes

Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development:

Production and Deployment: Yes

Operations and Support:

Attack Identifier: A13

Target (Attack Type): Hardware: Firmware:

Software: Yes Sys Information or Data:

Description (Attack Act): Malicious code (e.g., a logic bomb) is hidden in custom software during coding, integration, or test, either directly during the release or update processes, or via installation programs and device drivers (support systems) and/or development tools (e.g., a compromised compiler).

Attack Vector: An adversary with access privileges within the software development environment and associated tools, including the software unit/component test system, software configuration management system, and/or other software support and development tools.

Attack Origin: Software engineers and test engineers at any custom software developer facility.

Attack Goal: Disruption: Yes Disclosure:

Corruption: Yes Destruction: Yes

Attack Impact: Can vary widely, depending on the capability of the malicious code.

References: Based in part on various news stories; e.g., http://www.theregister.co.uk/2010/06/25/spanish_logic_bomb_probe(c/o Rick Dove)

Threat: An adversary with access privileges within the software development environment and to associated tools, including the software unit/component test system and the software configuration management system, can hide malicious code in custom software.

Vulnerabilities: Access privileges within the software development environment, including associated access to software support and development tools (e.g., the software unit/component test system and the software configuration management system), are susceptible to allowing hidden malicious code in custom software.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Yes Hardware Developer:

Sub-Contractor: Yes Physical Flow:

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development: Yes

Engineering and Manufacturing Development: Yes

Production and Deployment:

Operations and Support: Yes

Attack Identifier: A14

Target (Attack Type): Hardware: Firmware:
Software: Sys Information or Data: Yes

Description (Attack Act): Advanced technology and critical component architecture (including design and interface) descriptions are altered to circumvent dial-down functionality requirements associated with Defense Exportability Features (DEF).

Attack Vector: An adversary with access to DEF considerations within the program office's acquisition documents that include descriptions of advanced technology and/or specific components' criticality.

Attack Origin: Program office staff ("trusted insider").

Attack Goal: Disruption: Disclosure: Yes
Corruption: Destruction:

Attack Impact: Unintended release, distribution, or disclosure of advanced technology.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to DEF considerations contained in a program office's acquisition documents, considerations that include descriptions of advanced technology and/or specific components' criticality, can alter documents to circumvent dial-down functionality requirements for DEF.

Vulnerabilities: Access to DEF considerations contained in a program office's acquisition documents (including descriptions of advanced technology and/or specific components' criticality) are susceptible to malicious alteration to circumvent dial-down functionality requirements for DEF.

Attack Points: Program Office: Yes Software Developer:
Prime Contractor: Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis: Yes
Technology Development: Yes
Engineering and Manufacturing Development: Yes
Production and Deployment:
Operations and Support:

Attack Identifier: A15

Target (Attack Type): Hardware: Yes; Firmware: Yes; Software: ; Sys Information or Data:

Description (Attack Act): A hardware or firmware component is intercepted by an adversary for the purpose of substitution or manipulation.

Attack Vector: The distribution channel of a system component being transferred between supplier and acquirer, either in transit or at a transfer point.

Attack Origin: Any supplier personnel with undue access privileges.

Attack Goal: Disruption: Yes; Disclosure: ; Corruption: Yes; Destruction:

Attack Impact: Can vary widely, depending on the adversary's goal.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: A hardware or firmware component can be intercepted by an adversary while in transit between supplier and acquirer, for the purpose of substitution or manipulation.

Vulnerabilities: The distribution channels are susceptible to hardware or firmware components being intercepted while in transit between supplier and acquirer, for the purpose of substitution or manipulation.

Attack Points: Program Office: ; Software Developer: ; Prime Contractor: ; Hardware Developer: ; Sub-Contractor: ; Physical Flow: Yes; Integrator Facility: ; Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support: Yes

Attack Identifier: A16

Target (Attack Type): Hardware: Firmware:
Software: Sys Information or Data: Yes

Description (Attack Act): Descriptions of system capabilities in the ICD and/or the CDD are misrepresented or altered, intending to cause errors in derived system requirements.

Attack Vector: Program Office domain of acquisition activities associated with potential submissions into the JCIDS document development and review processes.

Attack Origin: DOD Components and other "Sponsors" of JCIDS documents ("trusted" insiders).

Attack Goal: Disruption: Disclosure:
Corruption: Yes Destruction:

Attack Impact: JCIDS documents that do not reflect capability gaps or associated needed capability requirements.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: Within program office acquisition activities associated with potential Joint Capabilities Integration and Development System (JCIDS) submissions, descriptions of system capabilities in the ICD and/or the CDD can be misrepresented or altered, intending to cause errors in derived system requirements.

Vulnerabilities: The program office acquisition processes associated with Joint Capabilities Integration and Development System (JCIDS) submissions and descriptions of system capabilities in the ICD and/or the CDD are susceptible to malicious alteration or misrepresentation.

Attack Points: Program Office: Yes Software Developer:
Prime Contractor: Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis: Yes
Technology Development: Yes
Engineering and Manufacturing Development:
Production and Deployment:
Operations and Support:

Attack Identifier: A17

Target (Attack Type): Hardware: Firmware: Software: Sys Information or Data: Yes

Description (Attack Act): Mission data, for example the mission threads and Concept of Operations (CONOPS), and/or requirements in the System Requirements Document (SRD) or the Technical Requirements Document (TRD) are altered, in order to cause errors in system development.

Attack Vector: Program Office domain of acquisition activities associated with mission data integrity and stakeholder and system requirements development.

Attack Origin: Systems engineers ("trusted" insiders).

Attack Goal: Disruption: Disclosure: Corruption: Yes Destruction:

Attack Impact: Faulty or inadequate system specification and design.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: Within program office acquisition activities, mission data (e.g., mission threads and CONOPS) and/or requirements in the SRD or the TRD can be altered in order to cause errors in system development.

Vulnerabilities: The program office acquisition processes are susceptible to allowing malicious alteration of mission data (e.g., mission threads and CONOPS) and/or requirements in the SRD or the TRD.

Attack Points: Program Office: Yes Software Developer: Prime Contractor: Hardware Developer: Sub-Contractor: Physical Flow: Integrator Facility: Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis: Yes
Technology Development: Yes
Engineering and Manufacturing Development:
Production and Deployment:
Operations and Support:

Attack Identifier: A18

Target (Attack Type): Hardware: Firmware:

Software: Yes Sys Information or Data: Yes

Description (Attack Act): The requirements allocated to software are corrupted or the software design documents are altered, in order to cause errors in system design.

Attack Vector: An adversary with access to the requirements allocation processes and tools, and/or with access to the software design processes and tools.

Attack Origin: Systems engineers and software engineers at a software contractor location.

Attack Goal: Disruption: Disclosure:

Corruption: Yes Destruction:

Attack Impact: Faulty or inadequate system design.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to requirements allocation and/or software design processes and tools can corrupt or alter either, in order to cause errors in system design.

Vulnerabilities: Requirements allocation and/or software design processes and tools are susceptible to malicious insertion in the software requirements or design.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Yes Hardware Developer:

Sub-Contractor: Yes Physical Flow:

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development: Yes

Engineering and Manufacturing Development: Yes

Production and Deployment:

Operations and Support:

Attack Identifier: A19

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): Malicious software is implanted in a system during the hardware-software integration phase.

Attack Vector: An adversary with access to 3rd party bundling processes and tools during the integration of system components for delivery to a higher-level supply chain contractor.

Attack Origin: A system integrator at a lower tier in the supply chain.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: System can function in a manner that is unintended.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to 3rd party bundling processes and tools can implant malicious software in a system during the hardware-software integration phase.

Vulnerabilities: 3rd party bundling processes and tools are susceptible to implantation of malicious software during the hardware-software integration phase.

Attack Points: Program Office: Software Developer: Yes
Prime Contractor: Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A20

Target (Attack Type): Hardware: Firmware: Yes

Software: Sys Information or Data:

Description (Attack Act): A BIOS containing known vulnerabilities is installed for future exploitation.

Attack Vector: An adversary with access to download system software and update associated firmware with versions containing vulnerabilities.

Attack Origin: Hardware/ software integrators at lower tier in supply chain.

Attack Goal: Disruption: Disclosure:

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the inserted vulnerabilities.

References: Based on TARA; AV ID 003

Threat: An adversary with access to download and update system software installs a BIOS containing known vulnerabilities for future exploitation.

Vulnerabilities: Processes and tools for access to download system software and update associated firmware are susceptible to malicious installation.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Yes Hardware Developer:

Sub-Contractor: Yes Physical Flow:

Integrator Facility: Yes Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support: Yes

Attack Identifier: A21

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): A software update containing malicious code is applied to the system being sustained.

Attack Vector: An adversary leverages an automated process to download and install malicious code that is believed to be a valid and authentic software update or patch.

Attack Origin: Software integrators and maintainers at lower tier in supply chain.

Attack Goal: Disruption: Yes Disclosure: Yes
Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the malicious code.

References: Based on TARA; AV ID 024

Threat: An automated software update/patch downloader/installer can be corrupted to download malicious code and apply it to systems being sustained.

Vulnerabilities: Access to an automated software update/patch downloader/installer is susceptible to corruption for downloading malicious code.

Attack Points: Program Office: Software Developer: Yes
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development:
Production and Deployment:
Operations and Support: Yes

Attack Identifier: A22

Target (Attack Type): Hardware: Yes | Firmware: | Software: | Sys Information or Data:

Description (Attack Act): The design and/or fabrication of hardware components is compromised.

Attack Vector: An adversary compromises the design and manufacture of critical hardware at targeted suppliers.

Attack Origin: Hardware design and manufacture engineers at lower tier in supply chain.

Attack Goal: Disruption: Yes | Disclosure: | Corruption: Yes | Destruction:

Attack Impact: Faulty or inadequate system design.

References: Based on TARA; AV ID 121

Threat: The design and manufacture of critical hardware at targeted suppliers can be compromised.

Vulnerabilities: Processes and tools for the design and manufacture of critical hardware are susceptible to compromise.

Attack Points: Program Office: | Software Developer: | Prime Contractor: | Hardware Developer: Yes | Sub-Contractor: | Physical Flow: | Integrator Facility: | Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A23

Target (Attack Type): Hardware: Yes | Firmware: | Software: | Sys Information or Data:

Description (Attack Act): During sustainment, legitimate faulty hardware or firmware is replaced by hardware into which malicious subcomponents have been placed.

Attack Vector: An adversary with access to intercept replacement hardware or firmware from a legitimate supplier and substitute components that have been maliciously altered.

Attack Origin: Technician with knowledge of and access to systems within the support supply chain.

Attack Goal: Disruption: Yes | Disclosure: | Corruption: Yes | Destruction: Yes

Attack Impact: Can vary widely, depending on the capability of the malicious subcomponents.

References: Based on TARA; AV ID 122

Threat: During sustainment, legitimate faulty hardware/firmware can be replaced by hardware/firmware into which malicious subcomponents have been placed.

Vulnerabilities: Access to systems within the sustainment supply chain are susceptible to unauthorized substitution of replacement hardware or firmware components.

Attack Points: Program Office: | Software Developer: | Prime Contractor: | Hardware Developer: | Sub-Contractor: | Physical Flow: | Integrator Facility: Yes | Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development:
Production and Deployment:
Operations and Support: Yes

Attack Identifier: A24

Target (Attack Type): Hardware: Yes Firmware:

Software: Sys Information or Data:

Description (Attack Act): An ASIC for the system being acquired or maintained is designed and produced with malicious functionality built in.

Attack Vector: An adversary gains access to the hardware design and development processes within a DMEA accredited "trusted supplier" facility.

Attack Origin: Hardware designer or fabricator at a lower tier in the supply chain.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the capability of the maliciously designed ASIC.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An application-specific integrated circuit (ASIC) for a system being acquired or maintained can be designed and produced with malicious functionality built in.

Vulnerabilities: Access to the hardware design and development processes within a DMEA accredited "trusted supplier" facility is susceptible to the design and/or production of an application-specific integrated circuit (ASIC) with malicious functionality built in.

Attack Points: Program Office: Software Developer:

Prime Contractor: Hardware Developer: Yes

Sub-Contractor: Physical Flow:

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support: Yes

Attack Identifier: A25

Target (Attack Type): Hardware: Yes Firmware:
Software: Sys Information or Data:

Description (Attack Act): A counterfeit hardware component is implanted in the system being acquired.

Attack Vector: An adversary produces counterfeit hardware components and includes them in product assembly.

Attack Origin: Engineers and technicians at an assembly sub-contractor site.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: The assembly containing counterfeit components (e.g., counterfeit routers, switches, LAN, or WAN cards) results in a system specifically designed for malicious purposes.

References: Based on TARA; AV ID 163

Threat: A counterfeit hardware component can be implanted in a system being acquired. (This is different from: A counterfeit hardware component can end up in a system being acquired.)

Vulnerabilities: Processes and tools at an assembly or sub-assembly site are susceptible to the implantation of a counterfeit hardware component.

Attack Points: Program Office: Software Developer:
Prime Contractor: Hardware Developer: Yes
Sub-Contractor: Physical Flow:
Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development:
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A26

Target (Attack Type): Hardware: Firmware:

Software: Yes Sys Information or Data:

Description (Attack Act): Malicious software is implanted in the system being integrated.

Attack Vector: An adversary includes unsecured 3rd party components in a technology, product, or code-base, packaging a potentially malicious component with the product before shipment to the acquirer.

Attack Origin: Software developers/ integrators at lower tier in supply chain.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction: Yes

Attack Impact: Can vary widely, depending on the adversary's goal.

References: Based on TARA; AV ID 181

Threat: Unsecured, potentially malicious 3rd party components of a technology or code-base can be packaged with a product before shipment to an acquirer.

Vulnerabilities: Processes and tools for software integration are susceptible to the implantation of unsecured, malicious 3rd party software components.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Hardware Developer:

Sub-Contractor: Physical Flow:

Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support:

Attack Identifier: A27

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): Malicious code is inserted into open source software used for math libraries.

Attack Vector: An adversary with access to open source library code and knowledge of its particular use for the system being acquired.

Attack Origin: An outsider (or insider) with knowledge of the software development plans for acquisition.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: Can vary widely, depending on the adversary's goal.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to open source code and knowledge of its particular use for the system being acquired can insert malicious code into open source software used for math libraries.

Vulnerabilities: Access to open source software and/or the processes and tools for including it in system math libraries are susceptible to malicious code insertion.

Attack Points: Program Office: Software Developer:
Prime Contractor: Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development: Yes
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A28

Target (Attack Type): Hardware: Yes Firmware:

Software: Sys Information or Data:

Description (Attack Act): Insertion of maliciously altered hardware components into the gray market.

Attack Vector: During lifecycle sustainment, spare components (from original suppliers) will often become unavailable. As a result, the obsolescence program to find replacements introduces a potential avenue for attack by adversaries who offer the necessary replacement parts, but with malware incorporated.

Attack Origin: The gray market or “bogus” components intended to be accepted as genuine from reputable, trusted sources.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Yes Destruction: Yes

Attack Impact: Can vary widely, depending on the adversary's goal.

References: Based on TARA; AV ID 124

Threat: A gray market adversary can exploit an obsolescence program to introduce replacement hardware with malware incorporated.

Vulnerabilities: Use of the gray market for hardware replacement components is susceptible to the introduction of malware-infested components.

Attack Points: Program Office: Yes Software Developer:

Prime Contractor: Hardware Developer: Yes

Sub-Contractor: Physical Flow:

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development:

Production and Deployment:

Operations and Support: Yes

Attack Identifier: A29

Target (Attack Type): Hardware: Yes; Firmware: Yes; Software: ; Sys Information or Data:

Description (Attack Act): Rogue processes in an integration facility are established in order to clandestinely insert maliciously altered components into the system.

Attack Vector: An adversary with access to critical components as they are being integrated into the acquired system.

Attack Origin: Organization with the ability to establish deceptive processes.

Attack Goal: Disruption: Yes; Disclosure: ; Corruption: Yes; Destruction:

Attack Impact: System may function in a manner that is unintended, which can vary widely.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to critical components as they are being integrated into the acquired system can insert maliciously altered hardware or firmware into the system.

Vulnerabilities: Processes in an integration facility are susceptible to the insertion of maliciously altered hardware.

Attack Points: Program Office: ; Software Developer: ; Prime Contractor: ; Hardware Developer: Yes; Sub-Contractor: ; Physical Flow: Yes; Integrator Facility: Yes; Information Flow:

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development: Yes
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A30

Target (Attack Type): Hardware: Firmware:
Software: Sys Information or Data: Yes

Description (Attack Act): During the system build process, the system is deliberately misconfigured by the alteration of the build data.

Attack Vector: An adversary with access to the data files and processes used for executing system configuration and performing the build.

Attack Origin: Engineers who are performing the system build and configuration activities.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction: Yes

Attack Impact: Compromise of the external mission load, which can lead to a variety of final impacts.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with access to the data files and processes used for executing system configuration and performing the build can deliberately misconfigure the build data.

Vulnerabilities: Access to system configuration data files and build processes are susceptible to deliberate misconfiguration of the system.

Attack Points: Program Office: Yes Software Developer:
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development:
Production and Deployment: Yes
Operations and Support: Yes

Attack Identifier: A31

Target (Attack Type): Hardware: Yes; Firmware: ; Software: ; Sys Information or Data: Yes

Description (Attack Act): Manipulation of design specifications to produce malicious hardware (e.g., the modification of transistor specifications for an integrated circuit).

Attack Vector: An adversary with access to design specifications during the hardware manufacturing process.

Attack Origin: Hardware engineers at a lower-tier to whom the manufacture of key components has been outsourced.

Attack Goal: Disruption: ; Disclosure: ; Corruption: Yes; Destruction:

Attack Impact: Faulty hardware manufactured to compromised design specifications.

References: Based on CAPEC: Attack ID 438 (c/o Bob Martin)

Threat: An adversary with access to design specifications during the hardware manufacturing process can manipulate the design specifications to produce malicious hardware.

Vulnerabilities: Access to design specifications during the hardware manufacturing process are susceptible to allowing production of malicious hardware.

Attack Points: Program Office: ; Software Developer: ; Prime Contractor: ; Hardware Developer: Yes; Sub-Contractor: ; Physical Flow: ; Integrator Facility: Yes; Information Flow: Yes

Applicable Life Cycle Phases:
Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support:

Attack Identifier: A32

Target (Attack Type): Hardware: Firmware:

Software: Yes Sys Information or Data:

Description (Attack Act): Malware is embedded into a sub-assembly via a linked library or by directly pre-installing it in a software file.

Attack Vector: An adversary with access to software being integrated into a system during a "sub-assembly" manufacturing process.

Attack Origin: Software engineers at a lower-tier to whom software integration of key components has been outsourced.

Attack Goal: Disruption: Yes Disclosure: Yes

Corruption: Destruction:

Attack Impact: Can vary widely, depending on the capability of the malware.

References: Based on CAPEC: Attack ID 438 (c/o Bob Martin)

Threat: An adversary with access to software being integrated into a system during a "sub-assembly" manufacturing process can embed malware into a sub-assembly.

Vulnerabilities: Access to software and associated integration processes during sub-assembly manufacturing are susceptible to insertion of malware via linked libraries and/or pre-installed software.

Attack Points: Program Office: Software Developer: Yes

Prime Contractor: Hardware Developer:

Sub-Contractor: Physical Flow:

Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support:

Attack Identifier: A33

Target (Attack Type): Hardware: Yes Firmware: Yes

Software: Sys Information or Data:

Description (Attack Act): A malicious component is substituted for a legitimate component during the packaging and distribution processes.

Attack Vector: An adversary with access to services provided from a manufacturer to a supplier during packaging and distribution.

Attack Origin: Technical and non-technical staff at an Original Equipment Manufacturer (OEM) facility.

Attack Goal: Disruption: Yes Disclosure:

Corruption: Yes Destruction: Yes

Attack Impact: Can vary widely, depending on the capability of the malicious component.

References: Based on CAPEC: Attack ID 439 (c/o Bob Martin)

Threat: An adversary with access to critical components during packaging and distribution can substitute a malicious component for a legitimate component.

Vulnerabilities: Packaging and distribution processes at an OEM are susceptible to insertion of malicious hardware or firmware.

Attack Points: Program Office: Software Developer:

Prime Contractor: Hardware Developer: Yes

Sub-Contractor: Physical Flow: Yes

Integrator Facility: Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development: Yes

Production and Deployment: Yes

Operations and Support:

Attack Identifier: A34

Target (Attack Type): Hardware: Yes; Firmware:; Software:; Sys Information or Data:

Description (Attack Act): Malicious hardware is substituted for a legitimate component during lifecycle maintenance.

Attack Vector: An adversary with access to the fielded operational system that is offline for scheduled maintenance and/or with access to parts depot logistics.

Attack Origin: Technical and non-technical staff at a field support activity.

Attack Goal: Disruption: Yes; Disclosure:; Corruption: Yes; Destruction: Yes

Attack Impact: Can vary widely, depending on the capability of the malicious hardware.

References: Based on CAPEC: Attack ID 440 (c/o Bob Martin)

Threat: An adversary with access to a fielded operational system that is offline for scheduled maintenance and/or with access to parts depot logistics can substitute malicious hardware for a legitimate component during lifecycle maintenance.

Vulnerabilities: A fielded operational system offline for scheduled lifecycle maintenance and/or access to parts depot logistics are susceptible to the insertion of malicious hardware.

Attack Points:

Program Office:

Software Developer:

Prime Contractor:

Hardware Developer: Yes

Sub-Contractor:

Physical Flow: Yes

Integrator Facility:

Information Flow:

Applicable Life Cycle Phases:

Materiel Solution Analysis:

Technology Development:

Engineering and Manufacturing Development:

Production and Deployment:

Operations and Support: Yes

Attack Identifier: A35

Target (Attack Type):	Hardware:	Firmware:
	Software: Yes	Sys Information or Data:

Description (Attack Act): Malicious software is substituted for a legitimate component during a software upgrade.

Attack Vector: An adversary with access to software support activity upgrades.

Attack Origin: Technical and non-technical staff at a field support activity.

Attack Goal:	Disruption:	Disclosure:
	Corruption: Yes	Destruction:

Attack Impact: Can vary widely, depending on the capability of the malicious code.

References: Based on CAPEC: Attack ID 440 (c/o Bob Martin)

Threat: An adversary with access to a software support activity can substitute malicious software for a legitimate component during a software upgrade.

Vulnerabilities: Software support activity upgrade processes and tools are susceptible to the introduction of malicious software.

Attack Points:	Program Office:	Software Developer: Yes
	Prime Contractor:	Hardware Developer:
	Sub-Contractor:	Physical Flow: Yes
	Integrator Facility:	Information Flow: Yes

Applicable Life Cycle Phases:	Materiel Solution Analysis:
	Technology Development:
	Engineering and Manufacturing Development:
	Production and Deployment:
	Operations and Support: Yes

Attack Identifier: A36

Target (Attack Type): Hardware: Yes Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): An adversary manipulates any of the following hardware and/or software baselines during Acquisition; functional baseline; allocated baseline; product baseline; or the product baseline updates during sustainment.

Attack Vector: An adversary with access to configuration control tools and processes during the establishment and/or update of system baselines.

Attack Origin: Configuration management personnel.

Attack Goal: Disruption: Disclosure:
Corruption: Yes Destruction:

Attack Impact: This configuration management breach will likely produce a faulty baseline with unquestioned integrity. The final impacts could vary widely.

References: Based on TARA: Several AV IDs

Threat: An adversary with access to configuration control tools and processes can manipulate any of the hardware and/or software development baselines during acquisition, or product baseline updates during sustainment.

Vulnerabilities: Processes and tools for hardware and software baseline creation and updates are susceptible to manipulation and corruption.

Attack Points: Program Office: Yes Software Developer:
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Yes Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development: Yes
Engineering and Manufacturing Development: Yes
Production and Deployment:
Operations and Support: Yes

Attack Identifier: A37

Target (Attack Type): Hardware: Firmware:
Software: Sys Information or Data: Yes

Description (Attack Act): An adversary corrupts critical operational data by injecting false but believable data into the system during configuration.

Attack Vector: An adversary with access to the data files and processes used for providing operational data loads during system configuration.

Attack Origin: Engineers or technicians who are loading operational data during system configuration.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: Suboptimal system performance (at varying degrees of degradation) during operations, with an associated loss of confidence.

References: Based on NIST SP 800-30; pages E-5 and E-6

Threat: An adversary with access to the data files and processes used for providing operational data loads can corrupt critical operational data by injecting false but believable data into the system during configuration.

Vulnerabilities: Data files, processes, and tools for configuring the system and establishing operational data loads are susceptible to malicious tampering.

Attack Points: Program Office: Yes Software Developer:
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Physical Flow:
Integrator Facility: Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development:
Production and Deployment: Yes
Operations and Support: Yes

Attack Identifier: A38

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): Maliciously altered commercial off-the-shelf (COTS) software is introduced into a primary support system (e.g., system design tools, a compiler, or a configuration management system).

Attack Vector: An adversary with the ability to subvert web-based delivery and/or on-site software updates.

Attack Origin: Technical or non-technical staff at a support system vendor location or with access to its distribution process.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: Faulty support system operation which could delay or degrade the system acquisition processes, or if undetected, the operational system itself.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with the ability to subvert web-based delivery and/or on-site software updates can introduce maliciously altered COTS software into a primary support system (e.g., system design tools, a compiler, or a configuration management system).

Vulnerabilities: Web-based delivery and/or on-site software update processes are susceptible to the introduction of maliciously altered COTS software into a primary support system (e.g., system design tools, a compiler, or a configuration management system).

Attack Points: Program Office: Software Developer: Yes
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development: Yes
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support: Yes

Attack Identifier: A39

Target (Attack Type): Hardware: Firmware:
Software: Yes Sys Information or Data:

Description (Attack Act): Maliciously altered COTS software is introduced into the system being acquired or sustained.

Attack Vector: An adversary with the ability to subvert web-based delivery of COTS software and/or the ability to access on-site insertion of COTS software into the system being acquired or sustained.

Attack Origin: Technical or non-technical staff at a software supplier or integrator location or with access to their COTS distribution process.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction: Yes

Attack Impact: Can vary widely, depending on the capability of the malicious COTS code.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with the ability to subvert web-based delivery of COTS software and/or the ability to access on-site insertion of COTS software into the system being acquired or sustained can introduce maliciously altered COTS software into the system.

Vulnerabilities: Web-based delivery and/or on-site software update processes are susceptible to the introduction of maliciously altered COTS software into the system being acquired or sustained.

Attack Points: Program Office: Software Developer: Yes
Prime Contractor: Yes Hardware Developer:
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow: Yes

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support: Yes

Attack Identifier: A40

Target (Attack Type):	Hardware:	Firmware:
	Software: Yes	Sys Information or Data:

Description (Attack Act): Software development tools are maliciously altered. Such tools include requirements management and database tools, software design tools, configuration management tools, compilers, system build tools, and software performance testing and load testing tools.

Attack Vector: An adversary with the ability to manipulate components of primary support systems and tools within the software development environment.

Attack Origin: Staff charged with the installation, management, and/or maintenance of primary support systems for software development.

Attack Goal:	Disruption: Yes	Disclosure:
	Corruption: Yes	Destruction:

Attack Impact: Faulty operation of a primary acquisition support system.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with the ability to manipulate components of primary support systems and tools within the software development environment can maliciously alter those software development tools (which include, e.g., requirements management and database tools, software design tools, configuration management tools, compilers, system build tools, and software performance testing and load testing tools).

Vulnerabilities: Access to components of primary support systems and tools within the software development environment are susceptible to malicious alteration.

Attack Points:	Program Office:	Software Developer: Yes
	Prime Contractor: Yes	Hardware Developer:
	Sub-Contractor: Yes	Physical Flow:
	Integrator Facility: Yes	Information Flow:

Applicable Life Cycle Phases:

- Materiel Solution Analysis:
- Technology Development:
- Engineering and Manufacturing Development: Yes
- Production and Deployment:
- Operations and Support: Yes

Attack Identifier: A41

Target (Attack Type): Hardware: Firmware: Yes
Software: Yes Sys Information or Data:

Description (Attack Act): Malicious software is inserted within the hardware development environment (e.g., malware inserted in a robotic control system) or within the firmware development environment (e.g., a maliciously altered FPGA programming tool).

Attack Vector: An adversary with the ability to manipulate components of primary support systems and tools within the hardware and/or firmware development and production environments.

Attack Origin: Staff charged with the installation, management, and/or maintenance of primary support systems for hardware and/or firmware development and production.

Attack Goal: Disruption: Yes Disclosure:
Corruption: Yes Destruction:

Attack Impact: Faulty operation of a primary acquisition support system.

References: Derived from multiple sources, including interviews with SCRM practitioners.

Threat: An adversary with the ability to manipulate components of primary support systems and tools within the development/production environments can insert malicious software within the hardware development environment (e.g., malware inserted in a robotic control system) or within the firmware development environment (e.g., a maliciously altered FPGA programming tool).

Vulnerabilities: Access to components of primary support systems and tools within the hardware development and/or firmware production environments are susceptible to malicious insertion of software and firmware.

Attack Points: Program Office: Software Developer:
Prime Contractor: Yes Hardware Developer: Yes
Sub-Contractor: Yes Physical Flow:
Integrator Facility: Yes Information Flow:

Applicable Life Cycle Phases: Materiel Solution Analysis:
Technology Development:
Engineering and Manufacturing Development: Yes
Production and Deployment: Yes
Operations and Support: Yes

Appendix B Initial Potential Countermeasures Catalog

****

This catalog contains the initial set of potential countermeasures for supply chain attacks of malicious insertion focused on: Hardware, Software, Firmware, and/or System Information and Data.

Countermeasure (CM) ID: CM-1

CM Name: Secure Configuration Management of Software

CM Focus: Software + Sys Info/Data

Mitigation Approach: Implement configuration management security practices that protect the integrity of software and associated data.

CM Description: Include security enhancements in the Software Configuration Management system that: monitor and control access to the configuration management system, harden centralized repositories against attack, establish acceptance criteria for configuration management check-in to assure integrity, plan for and audit the security of the configuration management administration processes, and maintain configuration control over operational systems.

CM Goals (Prevent, Detect, Respond): Prevent + Detect + Respond

Earliest Implementation Phase: MSA

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff + Equipment

CM Type (Process, Technical, Device): Process + Device

Expected Risk Reduction (Limited, Significant): Significant

References: TARA pilot catalog entry: C000022; NSA draft document on configuration management process; NIST Special Publication 800-128, August 2011

Countermeasure (CM) ID: CM-2

CM Name: Prevent or Detect Critical Component Tampering

CM Focus: Hardware + Firmware

Mitigation Approach: Prevent or detect tampering with critical hardware or firmware components while in transit, across all lifecycle phases, through use of state-of-the-art anti-tamper devices.

CM Description: Plan for, use, and monitor anti-tamper techniques and devices to prevent and/or detect tampering (unauthorized interference to cause damage), in order to safeguard shipments, transfers, and deliveries of critical hardware and firmware across the system's full lifecycle. Use tamper-resistant and tamper-evident packaging (e.g., plastic coating for circuit boards, tamper tape, paint, sensors, and/or seals for cases and containers) and inspect received system components for evidence of tampering.

CM Goals (Prevent, Detect, Respond): Prevent + Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Equipment

CM Type (Process, Technical, Device): Device

Expected Risk Reduction (Limited, Significant): Significant

References: TARA pilot catalog entry: C000011

Countermeasure (CM) ID: CM-3

CM Name: Security-Focused Programming Languages

CM Focus: Software

Mitigation Approach: Choose programming languages (and support tools) that counter software vulnerabilities and minimize the potential for exploitable weaknesses.

CM Description: Choose programming languages that protect against both unintentional and intentional software vulnerabilities. Select languages and support tools that reduce the likelihood of exploitable weaknesses and/or provide constructs that make software weakness and vulnerabilities easier to avoid.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: TD

Timeframe to Implement: Between Milestone A and Milestone B

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Technical

Expected Risk Reduction (Limited, Significant): Significant

References: TARA pilot catalog entry: C000021SCRM; Key Practices Guide-2010-02-25.pdf

Countermeasure (CM) ID: CM-4

CM Name: Security-Focused Design and Coding Standards and Reviews

CM Focus: Software

Mitigation Approach: Establish the use of security-focused design and coding standards/guidelines and use them for inspections and reviews.

CM Description: Establish the use of design and coding standards and guidelines to improve security (in addition to quality, readability, and maintainability) of software components. Use them as part of the criteria for design inspections to ensure integrity (and traceability) of allocated software requirements and design and to ensure minimized attack surfaces in the architecture. Conduct manual source code reviews on all critical software components to discover exploitable weaknesses and vulnerabilities.

CM Goals (Prevent, Detect, Respond): Prevent + Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: TARA pilot catalog entries: C000020 and C000062; DASD-SE Generic Contract Language (6 Feb 2013); https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices; http://cwe.mitre.org/top25/index.html; www.cert.org/archive/pdf/09tr010.pdf - 2009-10-23; SafeCode referenced from the TSN Analysis Tutorial: http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf

Countermeasure (CM) ID: CM-5

CM Name: Supply Chain Red Teaming

CM Focus: Hardware + Software + Firmware + Sys Info/Data

Mitigation Approach: Use red teams to perform supply chain penetration testing.

CM Description: A supply chain red team conducts penetration testing to assess specific vulnerabilities as well as the overall security of the supply chain, by simulating various potential attack actions of an adversary; e.g., by penetration testing of the hardware development environment. In so doing, they identify potential vulnerabilities in the supply chain.

CM Goals (Prevent, Detect, Respond): Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process + Device

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000017; SCRM Key Practices Guide-2010-02-25.pdf

Countermeasure (CM) ID: CM-6

CM Name: Trusted Shipping

CM Focus: Hardware + Firmware

Mitigation Approach: Utilize trusted shipping to protect deliveries.

CM Description: The contractors and sub-suppliers use trusted means of shipping (e.g., bonded/cleared/vetted and insured couriers) to ensure that the critical components, once purchased, are not subject to compromise during their delivery.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000010

Countermeasure (CM) ID: CM-7

CM Name: Hardened Delivery Mechanisms

CM Focus: Hardware + Software + Firmware

Mitigation Approach: Harden supply chain delivery mechanisms.

CM Description: Ensure that critical component delivery mechanisms (both physical and logical) used by all supplier tiers do not provide opportunities for unauthorized access to the component or information about its uses (including the identities of end users). Unauthorized access includes unauthorized modification which could lead to malicious substitution and subversion). This practice covers the entire lifecycle, including the delivery of system components to integrators, delivery of the system itself to users, and system maintenance (including repair and delivery of replacement parts or software). This practice also includes inventory management for the system and its elements.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Centers + Staff + Equipment

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000069; SCRM Key Practices Guide-2010-02-25.pdf

Countermeasure (CM) ID: CM-8

CM Name: Tracking Tags and Security Tags

CM Focus: Hardware + Firmware

Mitigation Approach: Use optical tags and/or RFID tagging to track shipments. Embed security tags into hardware and firmware components.

CM Description: 1. Incorporate optical tags onto the surface of critical components. (The tag, which is very small, is validated at point of receipt.) 2. Use RFID tagging to track transit of shipped components at each leg of the distribution channel. 3. Incorporate "security tag" technology into a system that can be used to verify the authenticity of semiconductor devices and detect falsely marked "ghost" chips. Such a tag could take the form of a small digital circuit which is added to the chip design and communicates through the package with an external sensor.

CM Goals (Prevent, Detect, Respond): Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): High

Resources Needed (Centers, Staff, Equipment): Equipment

CM Type (Process, Technical, Device): Technical + Device

Expected Risk Reduction (Limited, Significant): Significant

References: Based on the following TARA pilot catalog entries: C000015 for optical tags, C000059 for RFID tagging, and C000064 for embedded tags; http://cs.ucsb.edu/~koc/ccs130h/2011/00-hw-trojans/05.pdf

Countermeasure (CM) ID: CM-9

CM Name: Pedigree Established Across the Supply Chain

CM Focus: Software + Sys Info/Data

Mitigation Approach: Identify and assess trustworthiness of software and information, from the lowest levels/tiers of the supply chain up to system deployment.

CM Description: Critical software and information is identified. For each, information concerning the design, development, maintenance, and delivery is known and assessed for its trustworthiness. For example, the developers, maintainers, and distributors of critical software are known, and have been assessed in terms of their trustworthiness. This pedigree and lineage of software is monitored to ensure that trust is maintained. Similarly, critical and sensitive information is monitored from origination, to storage, to delivery to ensure that the integrity of the information is maintained.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000006

Countermeasure (CM) ID: CM-10

CM Name: Bulk Spares Inventory

CM Focus: Hardware + Firmware

Mitigation Approach: Maintain a large spare parts inventory/depot.

CM Description: Bulk purchases of spare parts for critical ICT components are made early on, usually at the same time the critical component is acquired. Doing so, instead of purchasing them as needed, mitigates the threat of an adversary replacing the spare parts with substandard or malware infected components.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: P&D

Timeframe to Implement: Between Milestone B and Milestone C

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Centers

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Limited

References: Based on TARA pilot catalog entry: C000009

Countermeasure (CM) ID: CM-11

CM Name: Multiple Suppliers

CM Focus: Hardware + Software + Firmware

Mitigation Approach: Use multiple suppliers for key critical components.

CM Description: Use multiple suppliers of critical components and critical-component assemblies to limit the chance that an adversary may compromise some of the components during design, development, manufacturing, and/or integration at one of the supply chain locations.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: EMD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Technical

Expected Risk Reduction (Limited, Significant): Limited

References: Based on TARA pilot catalog entry: C000007

Countermeasure (CM) ID: CM-12

CM Name: Trusted Suppliers

CM Focus: Hardware + Software + Firmware

Mitigation Approach: Use trusted foundries for critical hardware or software components.

CM Description: Use or develop trusted components to protect functions that are so critical that their exploitation would cause severe harm to the system/mission. For critical hardware that may be susceptible to supply chain attacks, trusted foundries or more stringent controls around design, development, and distribution of these components should be used. For critical software assets, trust may be increased through the use of TPM, HAP, and trusted OSs.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: EMD

Timeframe to Implement: After Milestone B

Cost to Implement (High, Medium, Low): High

Resources Needed (Centers, Staff, Equipment): Centers

CM Type (Process, Technical, Device): Process + Technical

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000008

Countermeasure (CM) ID: CM-13

CM Name: Acquirer Anonymity

CM Focus: Hardware + Firmware

Mitigation Approach: Utilize anonymous, bulk purchase of stock components and blind buy acquisition of custom components.

CM Description: When possible, avoid acquisition/purchase of custom configurations of critical components and purchase stock components instead. When custom configurations are necessary, implement a blind-buy contractual arrangement early in the acquisition lifecycle. The purpose of such procedures is to limit activities that might reveal to a potential attacker the end user of critical components.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000012

Countermeasure (CM) ID: CM-14

CM Name: Electromagnetic (EM) / Thermal Analysis

CM Focus: Hardware + Firmware

Mitigation Approach: Conduct EM/thermal emanations analysis.

CM Description: Use electromagnetic and/or thermal analysis to detect any changes that have been made to hardware (or counterfeit hardware). These analyses can allow detection of gold-standard circuits as well as tampered circuits.

CM Goals (Prevent, Detect, Respond): Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): High

Resources Needed (Centers, Staff, Equipment): Staff + Equipment

CM Type (Process, Technical, Device): Technical + Device

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000016

Countermeasure (CM) ID: CM-15

CM Name: Network Traffic Restriction

CM Focus: Software + Sys Info/Data

Mitigation Approach: Restrict traffic on all supply chain networks and integrated development environments (IDEs).

CM Description: Specify "deny all" or "permit by exception" for both inbound and outbound network traffic on all supply chain networks and integrated development environments (IDEs) over which critical software and sensitive data and information will be delivered and/or maintained. This includes the program office and all contactor tiers of the supply chain.

CM Goals (Prevent, Detect, Respond): Prevent

Earliest Implementation Phase: MSA

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000030

Countermeasure (CM) ID: CM-16

CM Name: Visual Inspection

CM Focus: Hardware + Firmware

Mitigation Approach: Use visual inspection to detect counterfeit components and tampering.

CM Description: Visually inspect ICT component for tampering, anomalies, defects, or counterfeits.

CM Goals (Prevent, Detect, Respond): Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Limited

References: Based on TARA pilot catalog entry: C000058

Countermeasure (CM) ID: CM-17

CM Name: Cryptography

CM Focus: Software + Firmware + Sys Info/Data

Mitigation Approach: Use cryptography to authenticate sources of software and information/data.

CM Description: Require and use digital signatures, encryption, checksums, and/or other cryptographic techniques to verify sender authenticity of all information and data received, including software and firmware.

CM Goals (Prevent, Detect, Respond): Prevent + Detect

Earliest Implementation Phase: MSA

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process + Technical

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000061

Countermeasure (CM) ID: CM-18

CM Name: Supply Chain Visibility

CM Focus: Hardware + Software + Firmware

Mitigation Approach: Maximize the acquirer's visibility into all tiers of the supply chain.

CM Description: Acquirers should seek to maximize visibility into all suppliers and their supporting tiers (including both custom and OTS products) to understand how elements are created, tested, delivered, and supported throughout the lifecycle, and to assess potential supply chain structures (suppliers and linkages). This visibility enables acquirers to evaluate the supply chain sufficiently to manage supply chain risks and protect the integrity and availability of critical components.

CM Goals (Prevent, Detect, Respond): Prevent + Detect

Earliest Implementation Phase: TD

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Medium

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000067; SCRM Key Practices Guide-2010-02-25.pdf

Countermeasure (CM) ID: CM-19

CM Name: Personnel Trust

CM Focus: Hardware + Software + Firmware + Sys Info/Data

Mitigation Approach: Ensure trustworthiness of key personnel.

CM Description: Acquirers and suppliers should evaluate all staff for trustworthiness to the extent that these individuals occupy key roles or perform tasks that if not done correctly will cause the system or mission to degrade or fail. Identify roles or positions where opportunities to access critical components and information could lead to malicious insertion. Evaluate key personnel for competency and trustworthiness. Conduct periodic reevaluation of key personnel. Consider supplier past performance as part of source selection requirements.

CM Goals (Prevent, Detect, Respond): Prevent + Detect

Earliest Implementation Phase: MSA

Timeframe to Implement: Ongoing

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Process

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000076; SCRM Key Practices Guide-2010-02-25.pdf

Countermeasure (CM) ID: CM-20

CM Name: Software Update Security

CM Focus: Software

Mitigation Approach: Minimize supply chain risks during software update processes.

CM Description: Software updates and patches can change the system in ways that create new vulnerabilities. On the other hand, failing to update or apply a patch may leave a known vulnerability in place that an attacker could exploit. Treat each patch as a new element in the system. Authenticate patch sources. Examine patch delivery approaches. Test patches to ensure that they are "as produced." Apply patches and updates in a way that permits rollback.

CM Goals (Prevent, Detect, Respond): Prevent + Detect + Respond

Earliest Implementation Phase: O&S

Timeframe to Implement: After Milestone C

Cost to Implement (High, Medium, Low): Low

Resources Needed (Centers, Staff, Equipment): Staff

CM Type (Process, Technical, Device): Technical

Expected Risk Reduction (Limited, Significant): Significant

References: Based on TARA pilot catalog entry: C000078;SCRM Key Practices Guide-2010-02-25.pdf

Appendix C Acronym List

ASIC	Application-Specific Integrated Circuit
CAPEC	Common Attack Pattern Enumeration and Classification
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
DASD SE	Deputy Assistant Secretary of Defense for Systems Engineering
DEF	Defense Exportability Features
DoD	Department of Defense
DoDI	Department of Defense Instruction
EM	Electromagnetic
EMD	Engineering and Manufacturing Development
FPGA	Field-Programmable Gate Array
FW	Firmware
FY	Fiscal Year
HW	Hardware
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IDE	Integrated Development Environment
KP	Key Practice
MSA	Materiel Solution Analysis
MTR	MITRE Technical Report
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
O&S	Operations and Support
P&D	Production and Deployment
PMO	Program Management Office
PPP	Program Protection Plan
SCRM	Supply Chain Risk Management
SE	Systems Engineering
SEI	Software Engineering Institute
SRD	System Requirements Document
SSE	System Security Engineering
SW	Software
TARA	Threat Assessment and Remediation Analysis
TD	Technology Development
TRD	Technical Requirements Document
TSN	Trusted Systems and Networks
TTP	Tactics, Techniques, and Procedures