A Supply Chain Attack Framework to Support Department of Defense Supply Chain Security Risk Management

Dr. John F. Miller
The MITRE Corporation

Peter D. Kertzner
The MITRE Corporation

NDIA 16th Annual Systems Engineering Conference
28 – 31 October 2013

MITRE

Description of the Work

- **Task**
  - Develop a catalog containing a wide range of supply chain attacks of malicious insertion across the full acquisition lifecycle
  - Include threats, vulnerabilities, and associated countermeasures
  - Develop a framework to structure and codify the attacks and link them to associated countermeasures
- **Expected Outcome**
  - Help DoD programs acquire and sustain systems that are less vulnerable to supply chain attacks
    - By addressing malicious insertion across the supply chain
    - By providing a comprehensive view of attacks not previously available
  - Provide information to engineers performing a Trusted Systems and Networks (TSN) Analysis (ref. DoDI 5200.44, Nov 5, 2012)
    - To better focus the supply chain threat analysis, vulnerability assessment, and countermeasures selection

Research Sources for the Supply Chain Framework, Attacks, and Countermeasures

- **Sources for Catalog Research**
  - DASD(SE) Pilot catalog, updated using current Threat Assessment & Remediation Analysis (TARA) database
  - NIST SP 800-30 threat sources and events – key factors in conducting a risk assessment
  - SCRM Key Practices Guide
  - TSN Analysis Tutorial
  - UVA work underway on system-aware security (B. Horowitz, et al.)
  - TSN Roundtable – TSN ICT Risk Mitigation Guidebook (c/o T. Weir); Findings and structure (c/o S. Adams)
  - Common Attack Pattern Enumeration and Classification (CAPEC) data (c/o B. Martin)
  - SEI software template elements in secure design patterns
  - DHS/HS-SEDI – SC Exploit Frame of Reference (SCEFOR) (c/o K. Hill)
  - MITRE Cyber Resiliency Framework (CRF) architectural constructs
  - Relevant supply chain case studies (c/o R. Dove)

Framework Provides a Vehicle to Leverage a Variety of Sources

Development Overview and Status

- **Created catalogs of attacks and countermeasures, implemented as Excel spreadsheets**
  - Attack Catalog – 41 Attacks
    - Generic end-to-end supply chain system mapped to consider possible points of attack
    - Each Key Practice in the SCRM KP Guide will track to at least one attack
    - Catalog significantly builds on the supply chain attack coverage in CAPEC
  - Initial Countermeasures Catalog – 62 Countermeasures (4 final, 58 draft)
  - Each attack and countermeasure is a line-entry in the catalog
    - Each attack is elaborated by context data – 13 specific attributes
    - Countermeasures are similarly elaborated – 15 specific attributes
    - Attacks and countermeasures are cross-referenced
- **Compiling actionable guidance to render countermeasures implementation-ready**
  - Currently, 4 countermeasures have implementation guidance:
    - Secure Configuration Management of Software
    - Prevent or Detect Critical Component Tampering
    - Security-Focused Programming Languages
    - Security-Focused Design and Coding Standards and Reviews
- **Created an initial approach for application**

Supply Chain Attack Catalog Development

Attack Catalog Attributes

- *Attack ID (unique ID number)*
- *Attack Point (supply chain location or linkage)*
- *Phase Targeted (acquisition lifecycle phase)*
- *Attack Type (malicious insertion of SW, HW, etc.)*
- *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)*
- *Applicable Countermeasures (mapped IDs)*

- The early results of this work were published as:
  - Miller, John F., "Addressing Attack Vectors Within the Acquisition Supply Chain and the System-Development Lifecycle," INCOSE Insight 16(2), July 2013
- Detailed descriptions of each Attack Attribute are provided in the Backup section

Supply Chain Attacks and Countermeasures – Catalog Attributes

Attack Catalog

- *Attack ID (unique ID number)*
- *Attack Point (supply chain location or linkage)*
- *Phase Targeted (acquisition lifecycle phase)*
- *Attack Type (malicious insertion of SW, HW, etc.)*
- *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)*
- *Applicable Countermeasures (mapped IDs)*

Mapping to Countermeasures Catalog

Countermeasures Catalog

- *CM ID*
- *CM Name*
- *CM Type*
- *CM Focus*
- *Mitigation Approach*
- *CM Description*
- *CM Goal*
- *Earliest Implementation Phase*
- *Timeframe to Implement*
- *Resources Needed*
- *Cost to Implement*
- *Amount of Risk Reduction*
- *References*
- *Implementation Action*
- *Applicable Attacks*

Points to File with Implementation Guidance

Mapping to Attack Catalog

Concept of Use

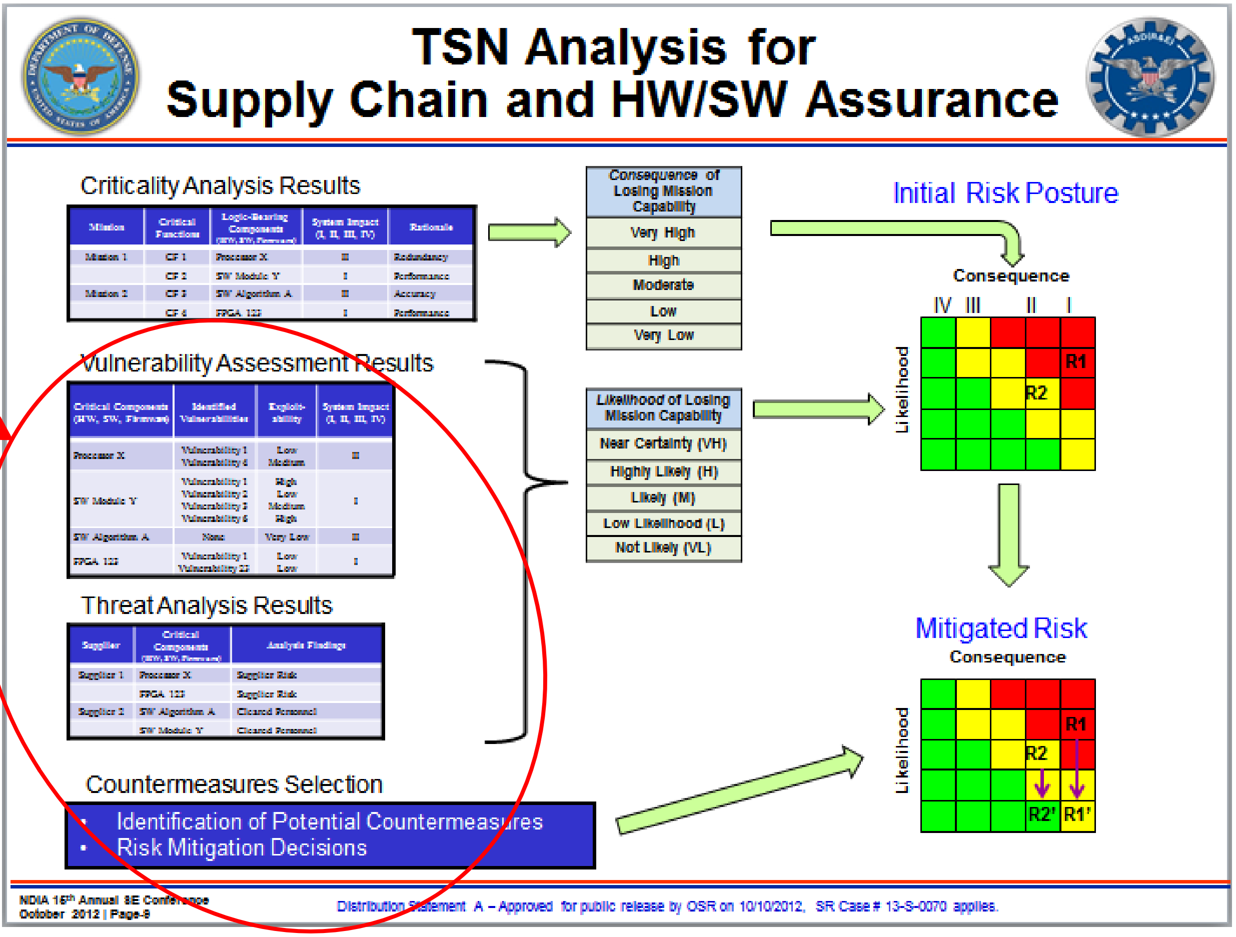
- **Who could use it?**
  - Individuals (programs and contractors) charged with performing a TSN Analysis to protect critical Information and Communications Technology (ICT) components in DoD systems being acquired or sustained
- **How could it be used?**
  - To identify specific supply chain attacks and applicable countermeasures pertinent to a program during specified lifecycle phase(s)
  - To support development of supply chain security requirements for Requests for Proposals (RFPs) and contracts
  - Results can be captured in specific sections of the Program Protection Plan (PPP):
    - 5.1 (Table 5.1-2), 5.2 (Table 5.2-1), and 5.3 (Subsection 5.3.4 and Table 5.3.6-1)
- **What are the potential benefits of using it?**
  - Users can zero in on <u>specific types of supply chain attacks</u> that can harm their systems, whether in acquisition or in the field
  - Users can identify specific, <u>implementation-ready countermeasures</u> linked to relevant particular types of attacks
  - Improved PPPs and RFP contract language leading to more successful programs

Expectation: Inform the TSN Analysis

Help focus these areas of the TSN Analysis using correlated threat, vulnerability, and countermeasure data relevant to malicious insertion in the supply chain

The TSN Analysis is described in:

K. Baldwin, J. F. Miller, P. R. Popick, and J. Goodnight, “The United States Department of Defense Revitalization of System Security Engineering Through Program Protection,” 6th Annual IEEE International Systems Conference, Vancouver, CA, 19–23 March 2012.



TSN Analysis for Supply Chain and HW/SW Assurance

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploit-ability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture

Mitigated Risk

Countermeasures Selection

- Identification of Potential Countermeasures
- Risk Mitigation Decisions

NDIA 16th Annual SE Conference
October 2012 | Page-8

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0070 applies.

Use-Case Scenario

Example: Critical Component Focus is Software

Review These Supply Chain Attacks of Malicious Insertion for Applicability

Use-Case Example: Consider Attack A3

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

Example Supply Chain Attack – A3

Attack Origin
Staff within the software engineering environment

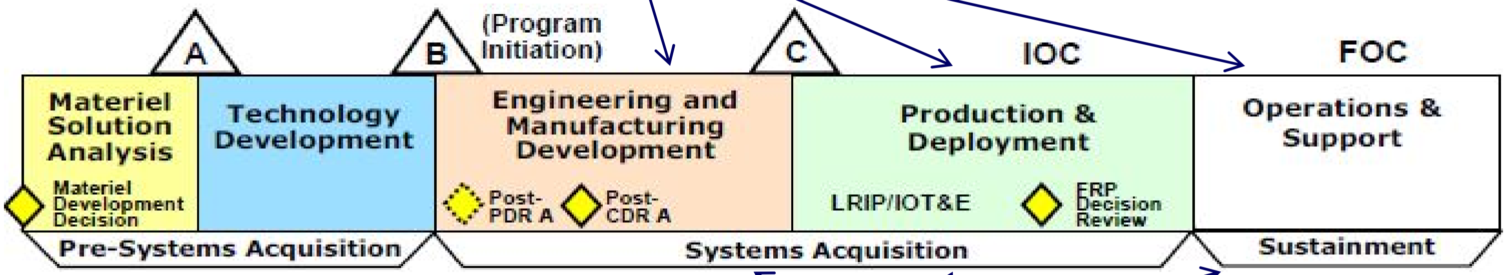
Attack Vector
Adversary with access to software processes and tools within the development environment or software support activity update environment

Attack Act
System is compromised by the insertion of malicious software into components during development or update

Attack Point
At a software developer /contractor location

Attack Type
Malicious insertion of software

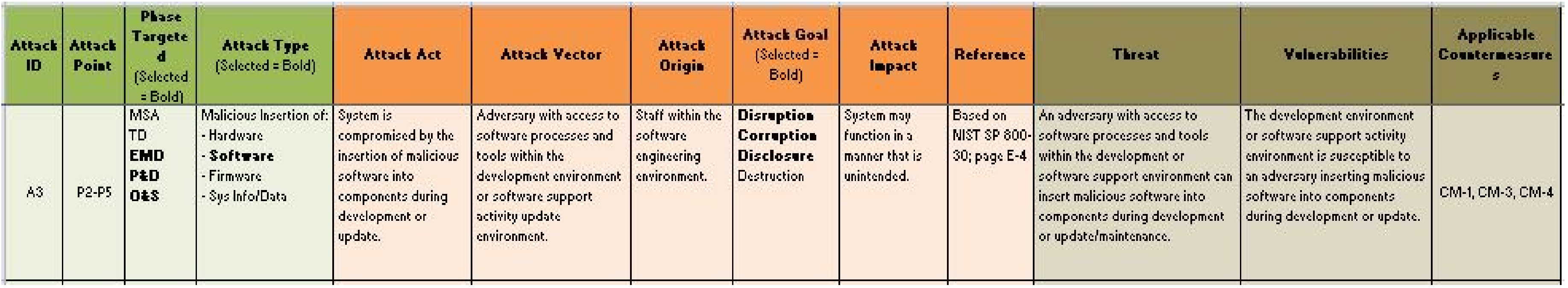
Attack Impact
System functions in an unintended manner



Phases Targeted

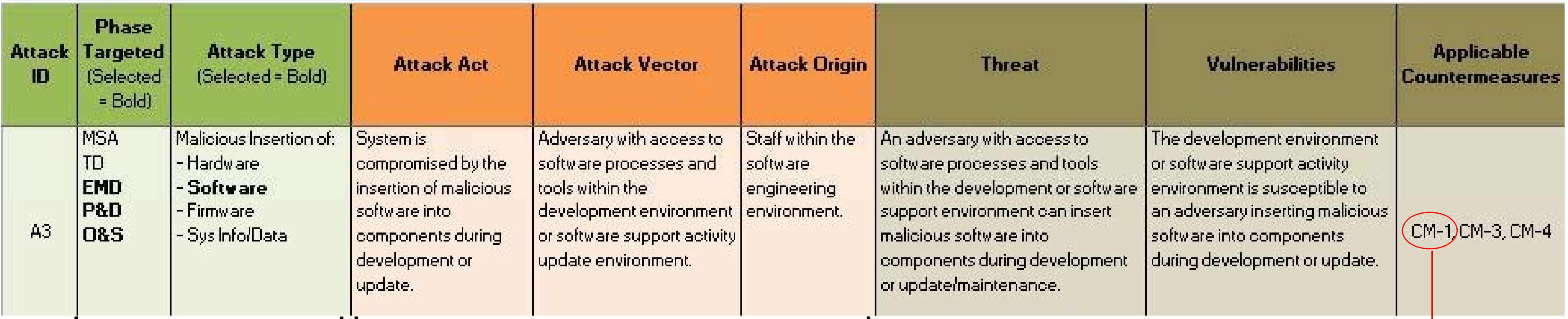
Attack Catalog Usage

The full catalog entry for sample Attack A3:

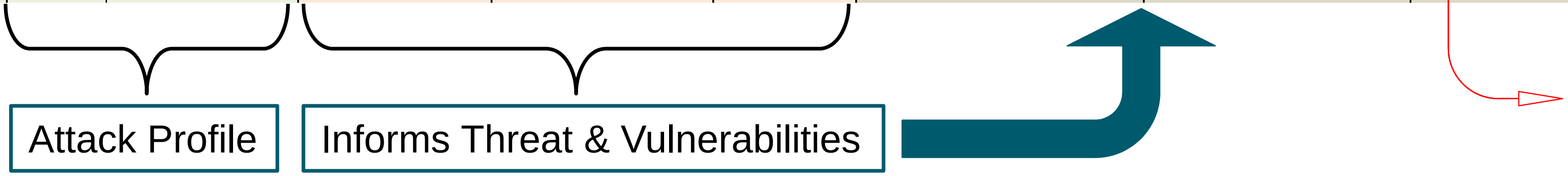


Attack ID	Attack Point	Phase Targeted (Selected = Bold)	Attack Type (Selected = Bold)	Attack Act	Attack Vector	Attack Origin	Attack Goal (Selected = Bold)	Attack Impact	Reference	Threat	Vulnerabilities	Applicable Countermeasures
A3	P2-P5	MSA TD **EMD** **P&D** **O&S**	Malicious Insertion of: - Hardware - **Software** - Firmware - Sys Info/Data	System is compromised by the insertion of malicious software into components during development or update.	Adversary with access to software processes and tools within the development environment or software support activity update environment.	Staff within the software engineering environment.	**Disruption** **Corruption** **Disclosure** Destruction	System may function in a manner that is unintended.	Based on NIST SP 800-30; page E-4	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.	The development environment or software support activity environment is susceptible to an adversary inserting malicious software into components during development or update.	CM-1, CM-3, CM-4

Key attributes for the analysis:



Attack ID	Phase Targeted (Selected = Bold)	Attack Type (Selected = Bold)	Attack Act	Attack Vector	Attack Origin	Threat	Vulnerabilities	Applicable Countermeasures
A3	MSA TD **EMD** **P&D** **O&S**	Malicious Insertion of: - Hardware - **Software** - Firmware - Sys Info/Data	System is compromised by the insertion of malicious software into components during development or update.	Adversary with access to software processes and tools within the development environment or software support activity update environment.	Staff within the software engineering environment.	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.	The development environment or software support activity environment is susceptible to an adversary inserting malicious software into components during development or update.	CM-1, CM-3, CM-4

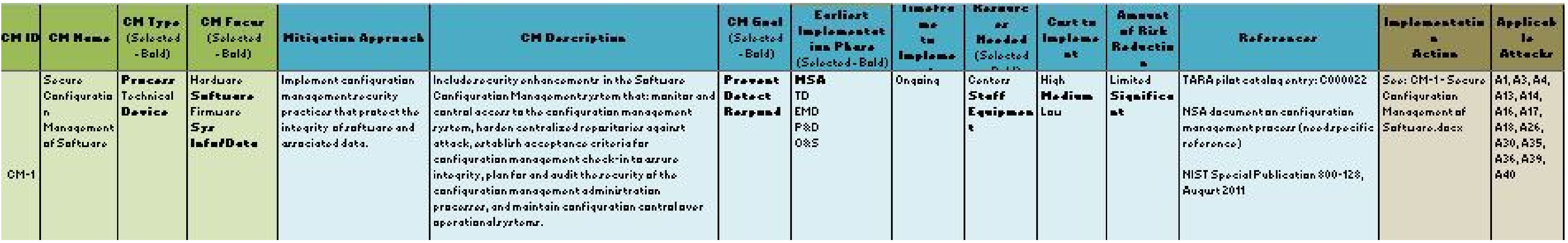


Attack Profile

Informs Threat & Vulnerabilities

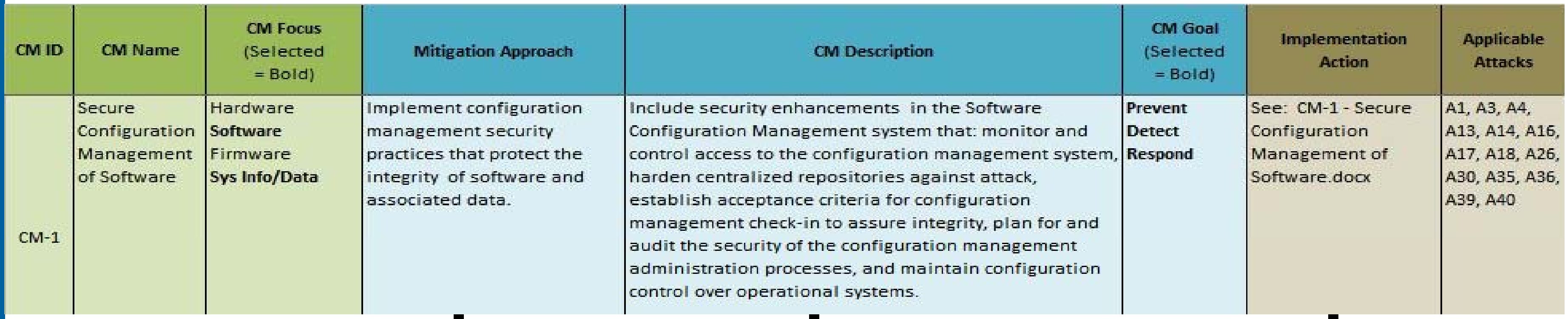
Countermeasures Catalog Usage

The full catalog entry for sample Countermeasure CM-1:



CM ID	CM Name	CM Type (Selected - Bold)	CM Focus (Selected - Bold)	Mitigation Approach	CM Description	CM Goal (Selected - Bold)	Earliest Implementation Phase (Selected - Bold)	Timeframe to Implement	Resources Needed (Selected - Bold)	Cost to Implement	Amount of Risk Reduction	References	Implementation Action	Applicable Attacks
CM-1	Secure Configuration Management of Software	**Process** Technical **Device**	Hardware **Software** Firmware **Sys Info/Data**	Implement configuration management security practices that protect the integrity of software and associated data.	Includes 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.	**Prevent** **Detect** **Respond**	**MSA** TD EMD P&D O&S	Ongoing	Contents **Staff** **Equipment**	High **Medium** Low	Limited **Significant**	TARA pilot catalog entry: C000022 NSA document on configuration management process (needs specific reference) NIST Special Publication 800-128, August 2011	See: CM-1 - Secure Configuration Management of Software.docx	A1, A3, A4, A13, A14, A16, A17, A18, A26, A30, A35, A36, A39, A40

Key attributes for the analysis:



CM ID	CM Name	CM Focus (Selected = Bold)	Mitigation Approach	CM Description	CM Goal (Selected = Bold)	Implementation Action	Applicable Attacks
CM-1	Secure Configuration Management of Software	Hardware **Software** Firmware **Sys Info/Data**	Implement configuration management security practices that protect the integrity of software and associated data.	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.	**Prevent** **Detect** **Respond**	See: CM-1 - Secure Configuration Management of Software.docx	A1, A3, A4, A13, A14, A16, A17, A18, A26, A30, A35, A36, A39, A40

High Level

Mid Level

Implementation-Ready Level

Requirements and Contract Language Can Be Developed From These Sources

Detailed Implementation Actions for CM-1 (1 of 2)

Actions for strengthening security of a configuration management system and its data:

- **Monitor and control access to the configuration management system**
  - Restrict access (including network access) to the configuration management system
    - Allow only specific user identities to access the system and its repositories (e.g., using role based access control and least privilege access for users)
  - Monitor and log all access (and access attempts) to the system, including who made the access (or attempt), when, and the purpose of access
    - Normal, successful logins as well as failed login attempts
    - All specific changes for successful logins
    - Unusual times of configuration management system usage
    - Unexpected locations for remote access to configuration management system
    - Unusual configuration management system activity
    - Unexpected individuals trying to access the configuration management system
    - Someone updating an unusually large number of Configuration Items
  - After a pre-determined number of failed login attempts, whether access is authorized or not, lock out the user and log an alert
  - Use strong authentication (e.g., multi-factor authentication) when authenticating system managers, administrators, and operators
  - Encrypt passwords when stored and when transmitted over a network
- **Harden centralized repositories against attack**
  - Limit the number of other services being run to reduce the risk that these other services could expose the repository to attack
  - Physically and operationally protect the configuration management system and the tools that comprise it
  - Understand who the suppliers of the configuration management system and associated tools are and perform threat assessments when questions of assurance arise
  - Store configuration management tools, source code, binary code, current configurations, and configuration baseline data in a protected manner

Detailed Implementation Actions for CM-1 (2 of 2)

- **Establish acceptance criteria for configuration management check-in to assure integrity**
  - Enforce change management protocols that ensure only authorized changes to software can be made; e.g., through two-person inspection and approval of changes
  - Ensure that configuration management supports traceability and protection of each configuration item
  - Verify that mobile code has been evaluated for acceptable risk (assess the various mechanisms used to verify implementation to support security needs) prior to introducing the code into the system configuration
  - Identify and use adequate industry tools and test cases to test any binary or machine-executable public domain software products (with no support and no source code) being incorporated into the system configuration
- **Plan for and audit the security of the configuration management administration processes**
  - Ensure the configuration management plan includes processes for configuration audits (who, what, and when of each change) and for protection against unauthorized access and changes (including changes for all critical function components and their associated requirements and architectural elements)
  - Audit the access logs and repository updates to determine unexpected or unusual activity
  - Protect audit records
  - Strengthen the security of the configuration management system itself by assuring the integrity of all component updates/upgrades (primarily the software components of the configuration management system)
- **Maintain configuration control over operational systems**
  - Ensure that software support activities for fielded, operational systems include the same security features and attributes for their Configuration Management System as those listed above

Potential RFP and Contract Language

- **Catalog high-level information (Mitigation Approach)**
  - May be suitable for stating proposal "Evaluation Criteria"
- **Catalog mid-level information (Countermeasure Description)**
  - May be appropriate for the RFP Statement of Work (SOW)
- **Catalog detailed level (Implementation Action files)**
  - Could be incorporated into a related Data Item Description (DID) to be put under contract
  - Could be packaged as a white paper that is referenced from the RFP "Instructions to Bidders"
  - Could be used for discussions with related support tool vendors to provide security-focused options

Utility

- **Provides a holistic view of supply chain attacks**
  - Pulls together information from a comprehensive set of sources
  - Provides a structure with context data that was previously unavailable
  - Can support analyses of abuse cases and supply chain penetration testing
- **Provides a decision support tool**
  - Includes potential application approaches for identifying and addressing malicious insertion
    - Across the supply chain
    - Across all lifecycle phases
- **Provides a structure for maturing the SSE discipline**
  - The evolving catalogs will support supply chain attack analysis and evaluation
  - *Provides insight into the understanding of current attacks and countermeasures*

Analysis of Attack Types by Phase

- 41 attacks in the current catalog
- Number of attacks for each Type is shown in **(purple)**

MSA Phase
3 Attacks

Mal. Insertion of:	
- Hardware	
- Software	
- Firmware	
- Sys Info/Data	**(3)**

TD Phase
12 Attacks

Mal. Insertion of:	
- Hardware	**(5)**
- Software	**(5)**
- Firmware	**(1)**
- Sys Info/Data	**(4)**

EMD Phase
28 Attacks

Mal. Insertion of:	
- Hardware	**(13)**
- Software	**(15)**
- Firmware	**(8)**
- Sys Info/Data	**(3)**

P&D Phase
24 Attacks

Mal. Insertion of:	
- Hardware	**(12)**
- Software	**(9)**
- Firmware	**(8)**
- Sys Info/Data	**(3)**

O&S Phase
22 Attacks

Mal. Insertion of:	
- Hardware	**(10)**
- Software	**(11)**
- Firmware	**(6)**
- Sys Info/Data	**(2)**

Analysis of Phase Applicability Based on Current Attack Understanding

Attack ID	MSA	TD	EMD	P&D	O&S
A16	▨	▨			
A17	▨	▨			
A14	▨	▨	▨		
A8		▨			
A18		▨	▨		
A2		▨	▨	▨	
A27		▨	▨	▨	
A29		▨	▨	▨	
A6		▨	▨	▨	▨
A38		▨	▨	▨	▨
A13		▨	▨		▨
A36		▨	▨		▨
A1			▨		
A9			▨		
A19			▨	▨	
A22			▨	▨	
A26			▨	▨	
A31			▨	▨	
A32			▨	▨	
A33			▨	▨	
A10			▨		▨
A40			▨		▨
A3			▨	▨	▨
A4			▨	▨	▨
A5			▨	▨	▨
A7			▨	▨	▨
A15			▨	▨	▨
A20			▨	▨	▨
A24			▨	▨	▨
A39			▨	▨	▨
A41			▨	▨	▨
A11				▨	
A12				▨	
A25				▨	
A30				▨	▨
A37				▨	▨
A21					▨
A23					▨
A28					▨
A34					▨
A35					▨

- There are a significant number of TD phase attacks
- Planning for them should occur during the MSA phase

- Most attacks are applicable across multiple phases
- 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

If you start early, you can plan for the whole lifecycle

Analysis of What can be Learned about Potential Points of Attack

Attack ID	Program Office	Prime Contractor	Sub-Contractor	Integrator Facility	SW Developer	HW Developer	SC Physical Flow	SC Info/Data Flow
A14	■							
A7	■	■						
A30	■	■						■
A37	■	■						■
A36	■	■		■				■
A28	■					■		
A16	■							■
A17	■							■
A13		■	■		■			
A18		■	■		■			
A3		■	■	■	■			
A4		■	■	■	■			
A40		■	■	■	■			
A41		■	■	■		■		
A20		■	■	■	■			■
A21		■	■	■	■			■
A38		■	■	■	■			■
A39		■	■	■	■			■
A12		■	■	■	■	■	■	
A1		■	■	■	■		■	■
A8			■	■		■		
A9			■	■		■		
A23				■				
A19				■	■			
A26				■	■			
A32				■	■			
A10				■		■		
A25				■		■		
A5				■		■	■	
A29				■		■	■	
A31				■		■		■
A35					■		■	■
A6						■		
A22						■		
A24						■		
A33						■	■	
A34						■	■	
A2							■	
A11							■	
A15							■	
A27								■

- 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

- Software developer suppliers and hardware developer suppliers are targeted by the same number of attacks

- Very few types of attacks are specified solely against distribution channels, including either the physical flow or the information/data flow

Next Steps

- Program Engagements
- Partnerships
- Technical Transition/Strategy Analysis

Questions / Comments / Suggestions

Contact:

John F. Miller
The MITRE Corporation
jfmiller@mitre.org
804-448-8578

Backup

Attack Attributes Defined (1 of 5)

- ***Attack ID***: **A unique identification number associated with a related and distinct set of attack attributes.**
  - Sequentially assigned number
- ***Attack Point***: **The location at which, or the linkage through which, the supply chain attack is directed. Designated by a tag "P#." More than one may apply:**

Point of Attack	**Tag**
… at the program office	**P1**
… at the prime contractor location	**P2**
… at a sub-contractor location	**P3**
… at an integrator facility	**P4**
… at a software developer supplier	**P5**
… at a hardware developer supplier	**P6**
… into the supply chain physical flow	**P7**
… into the supply chain information/data flow	**P8**

Attack Attributes Defined (2 of 5)

- ***Phase Targeted***: **The acquisition lifecycle phase targeted by an adversary. More than one may apply:**
  - Materiel Solution Analysis (MSA)
  - Technology Development (TD)
  - Engineering and Manufacturing Development (EMD)
  - Production and Deployment (P&D)
  - Operations and Support (O&S)

- ***Attack Type***: **The focus of the malicious insertion. More than one may apply:**

Attack Type	
Malicious insertion of…	Hardware
	Software
	Firmware
	System Information/Data (Includes requirements, design, manuals, architectures, and roadmaps)

Attack Attributes Defined (3 of 5)

- ***Attack Act***: **An action that causes a malicious payload or malicious intention to be delivered to or directed at a system for the purpose of adversely affecting that system.**
  - Example 1: Malware is inserted into system software during the build process
  - Example 2: System requirements or design documents are maliciously altered
- ***Attack Vector***: **The route or method used by an adversary to exploit system design vulnerabilities or process weaknesses to cause adverse consequences. (Attack vectors are the means by which adversaries can access attack surfaces, which can be thought of as reachable and exploitable vulnerabilities.)**
  - Example 1: An adversary with access to software development tools and processes during the software integration and build process
  - Example 2: An adversary gains unauthorized access to system technical documentation
- ***Attack Origin***: **The source of an attack.**
  - Information to identify the adversary's role, status, and/or relationship to the system development and acquisition (e.g., inside or outside the acquiring organization and/or supply chain, type of job performed, etc.).

Attack Attributes Defined (4 of 5)

- ***Attack Goal***: **The adversary's reason for the attack. More than one may apply:**
  - Disruption
  - Corruption
  - Disclosure
  - Destruction

Note: An attack with these Goals can be directed against the system at any of these locations:

- Program Office
- Prime contractor location (for Acquisition or Sustainment)
- Sub-contractor location
- Integration facility
- Software developer supplier
- Hardware developer supplier
- Supply chain physical flow
- Supply chain information/data flow

- ***Attack Impact***: **What the attack accomplishes. A description of the adverse effect on the system.**
  - Impacts may vary widely and may affect any aspect of a system due to the variability in attack goals and phases targeted; e.g., the impact of implanted malicious software could include corruption of operational data or denial of service.

Attack Attributes Defined (5 of 5)

- ***References***: **Source(s) from which this attack information was derived.**
- ***Threat***: **An adversarial event directed at the supply chain, based on the adversarial action and the route or method used for exploitation.**
  - Threat descriptions are generated primarily by combining the Attack Act and Attack Vector (but may also draw upon the Attack Point, Type, and Origin).
- ***Vulnerabilities***: **Exploitable weaknesses in the supply chain (including technical and procedural).**
  - The threat susceptibility.
- ***Applicable Countermeasures***: **A mapping to all countermeasures that might apply and should be considered, designated by "CM-#" tags.**
  - Each CM-# tag listed provides the # of an applicable countermeasure in the companion countermeasures catalog.