IDA

Institute for Defense Analyses

4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Systems Security Engineering: A Framework to Protect Hardware Down to the Last Tactical Inch

Brian Cohen, bcohen@ida.org

703-845-6684

October 28, 2015

This material represents ongoing technical work and the views of the author and does not represent any policies or positions of the government

Outline

- The Last Tactical Inch
- Formulating Risk at the Component Level
- Framework for Managing Component Risk
- Scenario
- Gaps
- Next Steps

- Many thanks to the Trustworthy Supplier Framework Team; Catherine Ortiz (DBS), Huan Zhang (IDA), Michele Moss (BAH), Sydney Pope (DAC), and Tracee Gilbert

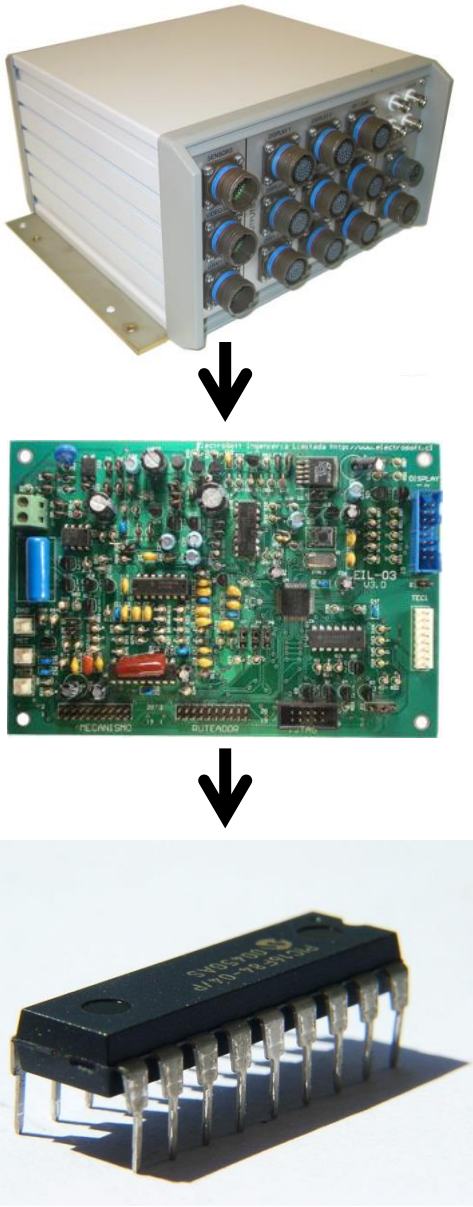
Objective

- Goals
  - Enable the definition of component-level mitigations that will enable system and mission requirements to be met
    - We will call those mitigations “controls”
  - Enable buyers to select appropriate controls
  - Enable buyers to select appropriate implementations for those controls
  - Support the evaluation of the cost and effectiveness of those implementations
- The result can be thought of as a toolbox
  - This is the “Framework”

The initial emphasis is on electronic components

The Last Tactical Inch

- This is mostly about Supply Chain Risk Management (SCRM) (and counterfeits)
- We have significant visibility and control of the contracted supply chain
- We don't have visibility and control over commercial products
- Commercial products are moving "up" the DOD supply chain
- The Last Tactical Inch is what you have to do to understand and manage risk when buying a commercial product
  - In this case a "component"



What is Component-Level Risk?

- It is the risk that some weakness or vulnerability in a component can lead to a system-level security consequence
- Risk is generally a function of the consequences, vulnerabilities, and threats
- For a given situation, the component-level risk is primarily a function of the vulnerabilities, since the consequences and threats are essentially fixed

Developed Definitions

- "Trustworthiness" is the way in which component-level risk is characterized
  - Based on how product security weakness ("vulnerabilities") may impact security aspects of system performance and mission success
  - Trustworthy products depend on trustworthy suppliers
- *Trustworthiness is a basis for knowing a product is free of "vulnerabilities" that could compromise system or mission security*
  - This definition is for "product trustworthiness"
  - "Supplier trustworthiness" is a basis for knowing that a supplier is not likely to introduce such vulnerabilities
- Adopted definition: "*Controls,"* which are safeguards or countermeasures to avoid, counteract, or minimize security risks (we will use this at times synonymously with mitigation)

Motivation in the DOD Context

- DoDI 4140.67
  - Requires R&E to collaborate with DOD services and agencies to establish technical anti-counterfeit qualification criteria for suppliers.
- DoDI 5200.44
  - For Critical Components:
    - Requires the use of the protection of custom application specific integrated circuits (ASICs) for which a military end use can be identified (DMEA accredited Trusted Supplier process flow)
    - *"Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use."*
    - *"Detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions."*
    - *"Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing."*

Component Vulnerabilities

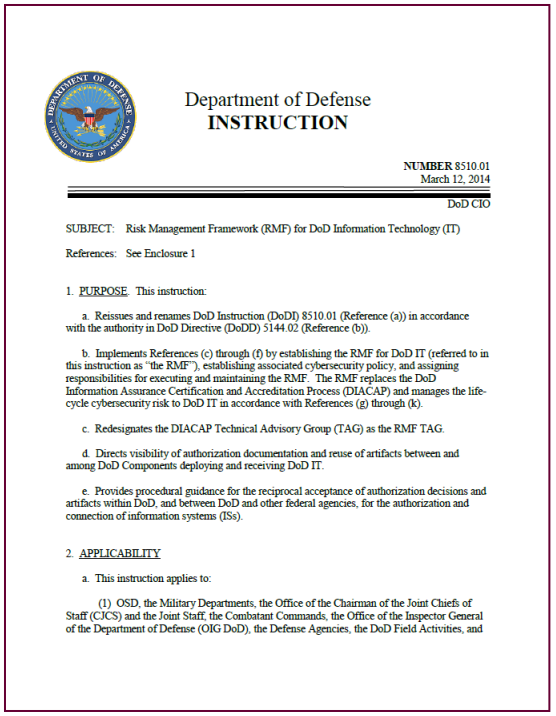
- Non-uniform and/or non-random premature failure
- Inappropriate communication channels
- Input–output ports that provide greater access/visibility than required to perform specified functions
- Component security feature defects
- Loss of access to supply
- Performs functions beyond those in the specification
- Component has falsified (or unknown) provenance
- Intended component features are security hazards
- Component contains functional defects (design/specification flaws)
- Component itself may contain information or technology that creates a system security issue
- Component supplier may know and reveal customer confidential information

IDA | Current Standards, Practices and Regulations

- DMEA Trusted Suppliers
- DLA Qualified Suppliers List for Distributors (QSLD)
- QTSL Program (Qualified Testing Suppliers List)
- DLA Qualified Manufacturers List (QML)
- DLA Qualified Products List (QPL)
- NASA/JPL Approved Supplier List
- MDA Distributor Qualification Program
- ISO 9000
- NISTIR-7622
- Open Group O-TTPS
- ISO/IEC 27036
- SAE/G19 – AS5553, AS6171(Draft), AS6174, AS6496, ARP 6178
- IDEA 1010
- NDAA 2015 818c
- Section 2319 of Title 10
- FAR Subpart 9.2
- **NIST SP 800-161, SP 800-53 R4 - This was identified as a foundation for the Framework**

IDA | Trustworthiness Framework Approach

- DOD's approach is based on a Risk Management Framework for Cyber
  - DODI 8510.01 issued 3/12/14
  - Employs NIST controls as described in NIST SP-800-53
- NIST has adapted SP-800-53 to SCRM as NIST SP-800-161[1]
  - The Trustworthiness Framework is based on 800-161
- Revised Risk Management (RM) Guide issued[2]
  - Team evaluated the guide to harmonize these efforts with the new RM guide



Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.

d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.

e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and

[1] NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Boyens et al, April 2015

[2] Department of Defense Risk Management Guide for Defense Acquisition Programs, 7th Edition (Interim Release), December 2014

NIST SP 800-161 Controls Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Planning
- Program Management
- System and Services Acquisition
- Personnel Security
- Provenance
- Risk Assessment
- System and Communication Protection
- System and Information Integrity

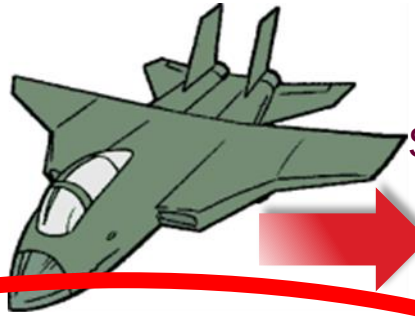
- Of 236 controls in NIST SP800-161, only 78 were considered relevant to acquisitions of components.

How the Framework was Developed

- Each of the NIST SP 800-161 controls was reviewed
  - Selected those that were relevant to being a Trustworthy Supplier
  - Name and descriptions were interpreted in the context of component acquisitions and the hardware context
- A map between component vulnerabilities and relevant NIST SP 800-161 controls was developed
- A map between relevant NIST SP 800-161 controls and standards, practices and regulations was developed
  - This is a cross reference indexing control into specific sections of various standards and practices
- The Framework is a series of detailed spreadsheets that form a toolbox

IDA | Scenario - SCRM Support for the Buyer

Covered system is threatened by counterfeits (either criminal or nation-state)



Buyer performs SCRM criticality and vulnerability analyses

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)	Exposure
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II	Low Low
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I	High Low Medium Low
SW Algorithm A	None	Very Low	II	Very Low
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I	High High

Buyer decides to reduce residual risk by employing controls that relate to the supplier and/or product

Determines that certain critical components are at risk (counterfeits could result in grave consequences)

Buyer employs systems integrator controls but residual risk may still be present

This scenario is a generic version of a threat scenario presented in NIST SP 800-161 in the context of how DOD implements SCRM (i.e., DODI 5200.44 and PPPs)

In this scenario we use the term "buyer" to refer to a PM or subordinate purchaser

Scenario (cont'd)

The Framework helps the Buyer identify how to articulate security requirements and translate those to controls and down to actionable implementations at the component level

Buyer makes candidate selections of standards and practices to be employed

Buyer evaluates measures of effectiveness and cost for the standards and practices

Buyer chooses standards and practices that will manage the risk

Methods for evaluation of effectiveness and cost are outside the scope of this effort and need further work

Scenario (cont'd)

- Telecommunication Example based on Scenario 1 in Appendix D of NIST SP 800-161
  - *If an inferior quality element was inserted into the system, it would likely fail more often than expected, causing reduced functionality of the system. In the event a large number of counterfeit products were mixed in with genuine parts and integrated into the system randomly, the number and severity of unexpected outages could grow significantly. The agency and integrator decided that the chances a counterfeit product could be purchased to maintain the system and the estimated potential impact of such an event were high enough to warrant further evaluation.*

Scenario (cont'd)

Buyer assesses identifies vulnerabilities exposing the highest risks to critical components

- Non-uniform and/or non-random premature failure
- Component has falsified (or unknown) provenance

Based on that assessment, buyer selects appropriate controls

- Applies the map between component vulnerabilities and relevant NIST SP 800-161 controls
  - Appropriate controls are those that reduce the likelihood of the component vulnerabilities

Scenario (cont'd)

- Buyer selected controls:

To be done by supplier:

1. Require developers to perform security testing/evaluation at all post-design phases of the SDLC [Ref. SA-11]
2. Validate that the information system or system component received is genuine and has not been altered [Ref. SA-12(10)]

To be done by systems integrator:

3. Incorporate security requirements into the design of information systems (security engineering) [Ref. PL-8, SC-36]
4. Employ supplier diversity requirements [PL-8(2)]

Buyer employs systems integrator controls but residual risk is present

These controls are from the Telecom Scenario in NIST SP 800-161

Scenario (cont'd)

Buyer chooses standards and practices that will manage the risk

Apply the map between relevant controls and the standards and practices

Buyer selects either AS5553 or AS6174 as addressing the needed controls and having the needed cost and effectiveness

Control Description	AS5553	OTTP-S	AS6174A	ISO9001	MIL-PREF-38535 (QML/QPL)
Security testing/evaluation	Section 4.1.4 Verification of Purchased Product	PD_MPP: Well-defined Development/Engineering Method Process and Practices	D.1.1 – Recommended Contract Pass-Down Clauses & D.3.1 – Contracts Issued To Independent Distributors	7.4.3 – Verification of purchased product & 7.5.3 – Identification and traceability	A.3.3.1 Certification of conformance and acquisition traceability
Genuine and unaltered	Section 4.1.4 Verification of Purchased Product		E.1 Counterfeit Material Detection		

Identified Gaps

- NIST SP 800-161 has some areas that need improvement
  - Organization improvement – controls overlap and are duplicative in some areas
  - Needs more strength in the tier that supports the component buyer
  - Harmonizing terminology of the controls to be more concise for diverse set of users of the standard
- Still don't have a good evaluation of product vulnerabilities
  - A good direction would be to harmonize with the CVE/CWE efforts
- We still have literally no idea about how to measure and evaluate the cost and effectiveness of controls and the applications of these practices and standards
- Existing standards and practices only partly cover the identified NIST SP 800-161 controls

Gaps in Existing Standards and Practices

- Minimizing Component Functionality
- Reviewing and controlling the release of information to the public (i.e., ITAR/Export)
- Treating Critical Components as Configuration-Parts Managed Items
- Reviewing available Subordinate Supplier Threat and Vulnerability Information
- Centralized and Automated Inventory Control for Horizontal Protection
- Assuring supply chain security across the product life cycle
- Avoidance of Custom Configurations and Single Suppliers
- Concealing Buyer End Use
- High levels of protection as afforded by the DMEA accredited trusted suppliers program are currently only required for ASICs

Summary

- This briefing:
  - Showed how to use component vulnerabilities to articulate system security requirements at the component level
    - Applies to SCRM and Counterfeits
  - Defined a Framework for controls that:
    - Helps in the selection of appropriate controls
    - Provides a mapping to relevant implementations using existing standards and practices
  - Suggest using the Framework as a “toolbox”
  - Demonstrates the Framework on a Scenario

More work to be done:

- Involving a broader community to refine the work
- Development of more tools for the toolbox
- Figuring out how to assess effectiveness and cost