Vulnerability Analysis Techniques to Support Trusted Systems and Networks (TSN) Analysis

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

17th Annual NDIA Systems Engineering Conference

Springfield, VA | October 29, 2014

What Are We Protecting?

Program Protection Planning
DoDI 5000.02

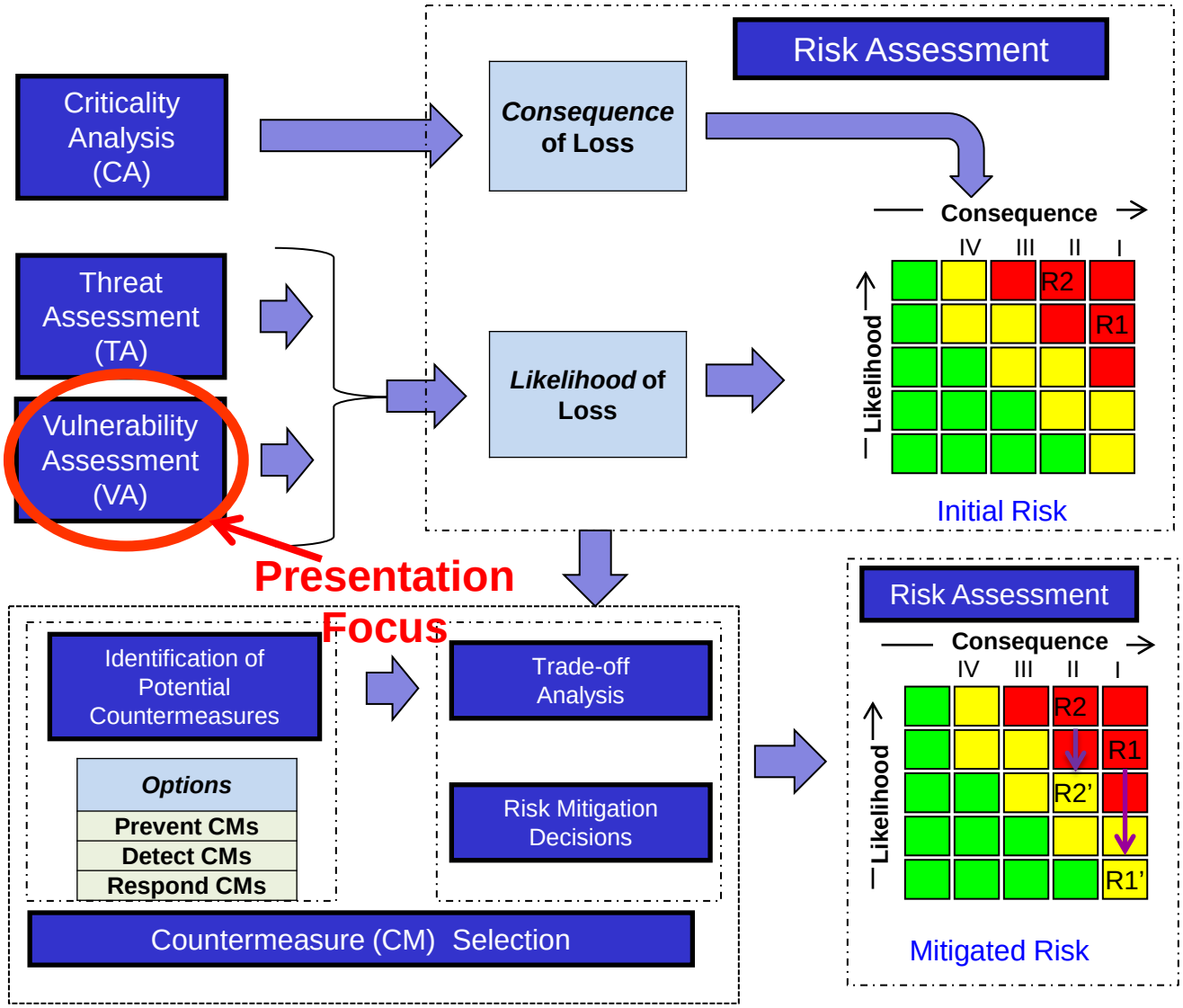
DoDM 5200.01, Vol. 1-4 | DoDI 5200.39 | DoDI 5200.44
DoDI 5230.24 | DoDM 5200.45 | DoDI 8500.01 | DoDI 8510.01

Presentation Focus

Information Analysis	CPI Analysis	TSN Analysis
What: Information about applications, processes, capabilities and end-items	What: A capability element that contributes to the warfighters' technical advantage (CPI)	What: Mission-critical elements and components
Who Identifies: All	Who Identifies: System Engineers with CI/Intel and Security SME support	Who Identifies: System Engineers, Logisticians
ID Process: CPI identification, criticality analysis, and classification guidance	ID Process: CPI Identification	ID Process: Criticality Analysis
Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments	Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence (CI) assessments	Threat Assessment: Defense Intelligence Agency Threat Analysis Center
Countermeasures: Cybersecurity, Risk Management Framework (RMF), Classification, Export Controls, Security, etc.	Countermeasures: Anti-Tamper, Classification, Exportability Features, Security, etc.	Countermeasures: SCRM, Cybersecurity, Anti-counterfeits, RMF, software assurance, Trusted Foundry, etc.
Goal: "Keep critical information from getting out" by protecting data from our adversaries	Goal: "Keep secret stuff in" by preventing the compromise and loss of CPI	Goal: "Keep malicious stuff out" by protecting key mission components

System Security Risk Assessment

Trusted Systems and Networks (TSN) Analysis



Frequent VA Issues:

1. Superficial
2. Lack of objective criteria
3. Application across the life cycle
4. Application to legacy software and components

Vulnerability Assessments

Concerns:

- Superficial - wide variability in results; not repeatable
- Lack of objective criteria more opinion based
- Often not done during Material Solution Analysis (MSA) and early in the Technology Maturation and Risk Reduction (TMRR) phases
- Not applied to legacy software and hardware components

Approach:

- Establish objective criteria that can be adapted by domain and is repeatable with focus on critical functions, components
- Apply methods that encourage analysis to the level of system design
- Ensure that VAs are done for each phase of the acquisition life cycle
- Use a blend of techniques across the life cycle to identify vulnerabilities
- Do sampling of legacy software to estimate vulnerabilities
- Update techniques based upon results

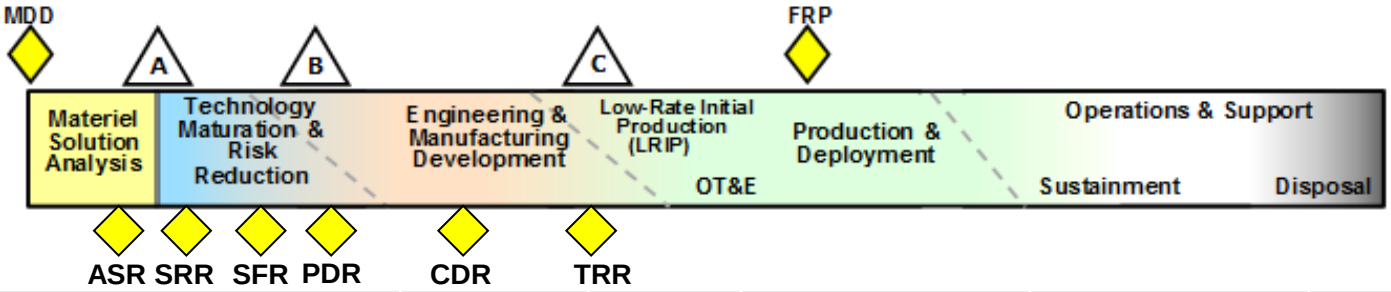
Vulnerability Assessment Techniques

Technique	High Level Description
1. Vulnerability assessment questionnaire	A set of questions that a program answers to identify vulnerabilities that can be mitigated by Statement of Work (SOW) and System Requirements Document (SRD) additions to the RFP
2. Attack Pattern Path Analysis	Using three databases of publicly available information that define attack patterns, vulnerabilities, and weaknesses (CAPEC, CVE, CWE*)
3. Static analysis and other detection techniques	For software systems, static analysis, dynamic analysis, and other testing, tools, and techniques to identify vulnerabilities in software during development, in legacy software, and in open source
4. Component Diversity Analysis	Assess the potential impact of malicious insertion in a component that is used multiple times in one or more critical functions or sub-functions
5. Fault Tree Analysis (FTA)/ Attack Tree Analysis	Commonly used in system safety and reliability, adjusted for used in system security to account for malicious actors introducing intentional system faults, as opposed to random sources of failure
6. Red team penetration testing	Subjecting a system, supply chain, and/or the development environment to a series of attacks, simulating the tactics of an actual threat through the use of misuse cases

Full descriptions of each analysis are available in the *Trusted Systems and Networks (TSN) Analysis* white paper (http://www.acq.osd.mil/se/initiatives/init_pp-sse.html)

* Common Attack Pattern Enumeration and Classification (CAPEC) | Common Vulnerabilities and Exposures (CVE) | Common Weakness Enumeration (CWE)

Vulnerability Assessment Techniques across the Acquisition Life Cycle



	Techniques	Legacy	MSA	TMRR		EMD		P&D	O&S
				SRR	PDR	CDR	SVR		
1	VA Questionnaire		x	x					
2	Attack Pattern Path Analysis	x		x	x	x	x	x	x
3	Static Analysis & Other Detection Techniques	x			x	x	x	x	x
4	Component Diversity Analyzer	x	x	x	x	x			
5	Fault Tree Analysis/ Attack Tree Analysis	x			x	x	x	x	
6	Penetration Test	x				x	x	x	x

Calculating Likelihood

1. **Equally-weighted scoring model**
   - Applies to: Questionnaire, Vulnerability Databases, FTA/ATA,
2. **Weighted scoring model**
   - Applies to: Questionnaire, Vulnerability Databases, FTA/ATA
3. **Success Rates**
   - Applies to: Penetration Test/Red Team, Static Analysis
4. **Likelihood Adjustment (given a likelihood, analysis can lead to an upward or downward adjustment**
   - Applies to: Component Diversity Analysis

Vulnerability Assessment Questionnaire

- **Yes/No questions which indicate potential vulnerabilities**
  - Supply Chain Example: Does the Statement of Work (SOW) require the contractor to have a process to establish trusted suppliers?
  - Software Example: Does the SOW require design and code inspections to identify violations of secure design and coding standards for critical function components?
  - Domain-specific questions can provide more unique insights - attack patterns
- **Questions enable the program to implement cost-effective measures early in the life cycle which reduce the number of vulnerabilities that must be mitigated later in the life cycle**
  - Aids establishment of a base set of protection measures

Optimal Use: Before Milestone A and early in TMRR Phase (or wherever a program enters the acquisition life cycle).

Vulnerability Assessment Questionnaire: Supply Chain Example

1. ___ Does the Statement of Work (SOW) require the contractor to have a process to establish secure suppliers?
2. ___ Does the SOW require the contractor to obtain DoD-specific Application-Specific Integrated Circuits (ASICS) from a Defense Microelectronics Activity (DMEA)-approved supplier?
3. ___ Does the SOW require the contractor to employ protections that manage risk in the supply chain for critical 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?
4. ___ Does the SOW require the contractor to require suppliers to have similar processes for the above questions?
5. ___ Does the SOW require the prime contractor to vet suppliers of critical function components (hardware/software/firmware) based upon the security of their processes?
6. ___ Does the SOW require the contractor to use secure shipping methods for critical components? How are components shipped from one supplier to another?
7. ___ Does the SOW require the contractor to have processes to verify critical function components received from suppliers to ensure that components are free from malicious insertion (e.g., seals, inspection, secure shipping, testing, etc.)?
8. ___ Does the SOW require the contractor to have controls in place to ensure technical manuals are printed by a trusted supplier who limits access to the technical material?
9. ___ Does the SOW require the contractor to have controls to limit access to critical components?
10. ___ Does the SOW require the contractor to identify everyone that has access to critical components?
11. ___ Does the SOW require the contractor to use blind buys to contract for [selected] critical function components?
12. ___ Does the SOW require specific security test requirements to be established for critical components?
13. ___ Does the SOW require the developer to define and use secure design and fabrication or manufacturing standards for critical components?

Vulnerability Assessment Questionnaire Incorporated into RFP

1. Complete questionnaire
2. Program Office analyzes the questions answered 'No' and determines whether a protection measure related to the question provides cost-effective risk reduction
3. For selected questions determined to be valuable, a system specification or SOW requirement can be derived from the question

For example, if the Program Office answered 'No' to:

"Does the SOW require the contractor to obtain DoD-specific Application-Specific Integrated Circuits (ASICS) for a critical function from a Defense Microelectronics Activity (DMEA)-approved supplier?"

Then an SOW statement can be added which says:

"The contractor shall obtain DoD-specific ASICS from a DMEA-approved supplier for a critical function."

Attack Pattern Path Analysis

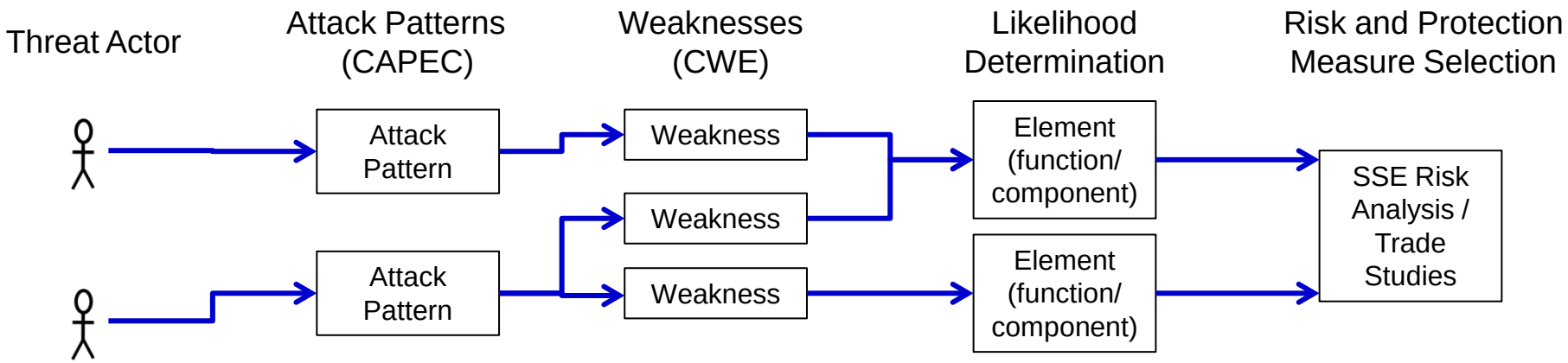
- **Combines publically available information from CAPEC, CWE, and CVE to conduct a vulnerability assessment**
  - Reviewing the types of weaknesses/vulnerabilities that different attack patterns are effective in attacking, a program can identify vulnerabilities in its own system
    - For custom developed components, use a combination of CAPEC and CWE
    - For Commercial Off the Shelf (COTS) components, use a combination of CAPEC and CVE
- **Potential uses**
  - Used to identify attack patterns for security verification, validation and penetration testing
  - Analysis comparing potential COTS components. Gives an understanding of which attacks/vulnerabilities potential COTS components are susceptible to
  - Can be used early in the life cycle to indicate potential vulnerabilities of any preliminary functions or design implementations
  - Assessing product baselines against specific attacks patterns or vulnerabilities
  - Assessment of legacy software

Optimal Use: This technique can be used to evaluate potential COTS products, and development of requirements based upon abuse cases after Milestone A.

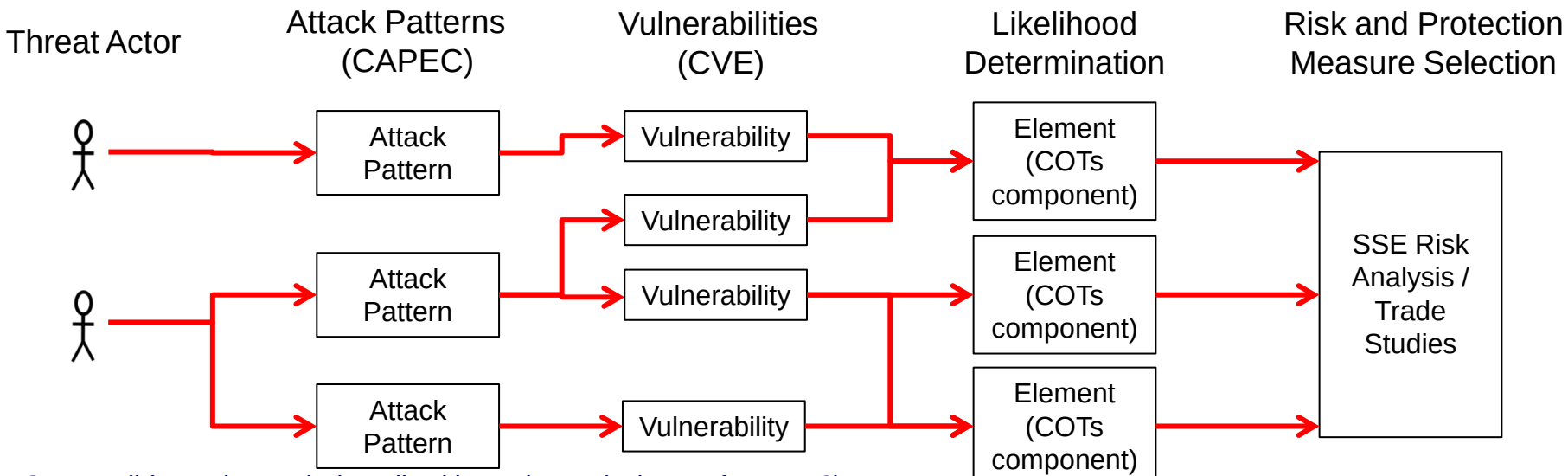
**NOTE: Builds on the work described by Bob Martin (see reference 2)

Attack Pattern Path Analysis Example

Custom Development Application



COTS Component Application



**NOTE: Builds on the work described by Bob Martin (see reference 2)

Attack Pattern Path Analysis Incorporated into RFP

Two alternative approaches:

1. **Program Office identifies a set of attack vectors (CAPEC) which the system must protect against.**

   This becomes a factor in the evaluation of designs by analyzing the vulnerability of the design and adding protection measures. This requirement may be incorporated into the system requirements spec or the SOW. Usually the design evaluation results are presented at the systems engineering technical reviews

2. **SOW and /or Section L language is added to have the contractor propose attack vectors (CAPEC) which the system must protect against.**

   The proposed set is presented to the government sponsor in the proposal or as part of the SRR or SFR for approval .

Component Diversity Analysis

- **Typical Perspective:** Selecting common components is potentially advantageous in terms of maintainability, reliability, and life cycle cost.
- **Security Perspective:** Common components can increase the system security risk.
  - A component used within or across multiple critical functions, the vulnerabilities of that particular component also are common across the functions
  - It makes the component a higher value target for malicious insertion of logic because the impact of exploiting a particular vulnerability is increased.
- **Applying Component Diversity**
  - **To the system:** Adding design and component diversity into the system lowers the impact of exploiting a particular vulnerability
  - **To the supply chain:** Consider using multiple sources to supply the component.
  - Balance the security benefits of diverse components with the potential cost savings of common components

Optimal Use: With notional components early in the life cycle, or as part of trade analyses to determine selection of components later in the design.

Component Diversity Probability

Option 1: Three of component X (X1, X2, X3) are used (Dependent events)

$$P(\text{all fail}) = P(A)*P(B|A)*P(C|A)$$

$$P(\text{all fail}) \approx P(A)$$

≈ 1 because if a vulnerability was exploited in component X1, same exploitation is assumed to effect all of the same component (X2 and X3)

Probability Events:
A – Component X1 fails
B – Component X2 fails
C – Component X3 fails
D – Component Y1 fails

Dependent Events:
A&B = P(A)*P(B|A)

Independent Events:
A&B = P(A)*P(B)

Option 2: Two of component X (X1 and X2) and one of component Y (Y1) are used (Y1 is an Independent Event)

$$P(\text{all fail}) = P(A)*P(B|A)*P(D)$$

$$P(\text{all fail}) \approx P(A)*P(D)$$

≈ 1 because if a vulnerability was exploited in component X1, same exploitation is assumed to effect all of the same component (X2)

If P(D) < 1, then **Option 2 has a lower probability of all three components failing** due to the exploitation of a vulnerability.

Component Diversity Analysis Example

1. **Diversity across the system:** A microprocessor needed in three separate subsystems to implement a critical function in each subsystem
   - Security Issue: Exploitation of a single vulnerability can impact all 3 critical functions
   - Diversity Solution: Selecting at least 2 different microprocessors decreases the likelihood that a single vulnerability can impact all 3 critical functions

2. **Diverse redundancy:** Reliability analysis dictates need for redundant processors to implement a specific function
   - Security Issue: If redundant components are exactly the same, an exploitation may lead both to fail
   - Diversity Solution: Select two different processors to implement the redundancy, ensuring exploitation of a single vulnerability doesn't eliminate the reliability increase of adding redundancy

3. **Consider diversity across systems**

Component Diversity Analysis Incorporated into RFP

- **Key factor to include diversity analysis in the RFP is define the scope of the analysis.**
- **The following are examples of defining the analysis scope:**
  - The contractor shall use diversity analysis during the design of the level I critical functions to determine where to employ component diversity
  - Critical functions for CF1 and CF2 shall employ component diversity

Application to Legacy Components

Issue: Legacy components are incorporated into a system without knowledge of the security risks. Resource limitations typically do not allow for a full security analysis of each legacy component incorporated into the system.

General Solution: Divide legacy components by language type, subsystem and application. Select part (~5%) of each legacy type to analyze using one or more techniques described previously. For legacy software, static/dynamic analyzers are likely the most effective technique

- Assess the risk of the legacy components based on that small selection
  - If the risk is high, consider analysis of a larger portion to determine necessary protections (may specify additional analysis as RFP task)
  - If this risk is low/medium some protections may be warranted, but additional analyses may not be necessary.
- At a minimum the program should have an understanding of the risk being accepted

In Summary

- **Vulnerability Assessments (as part of the TSN Analysis) must be completed to the appropriate level of detail throughout the life cycle to identify and implement cost-effective protection measures**

- **For each program circumstance, a modified application of vulnerability analysis techniques leads to effective assessment of the system**
  - **Early in the Life Cycle:** Techniques which identify cost-effective protection measures through simple analyses should be emphasized
  - **Addressing Legacy:** Analyzing a piece of the legacy code/system allows for an understanding of the risks associated with incorporating legacy components

For Additional Information

Melinda Reed

ODASD, Systems Engineering

571-372-6562 | Melinda.K.Reed4.civ@mail.mil

Paul Popick

ODASD, Systems Engineering

571-372-6467 | Paul.R.Popick.ctr@mail.mil

JeanPaul LeSaint

ODASD, Systems Engineering

571-372-6554 | JeanPaul.R.LeSaint.ctr@mail.mil

Definitions for the Purposes of This Presentation

- **Static Analysis:** An analysis performed on the system without the system in operation. This can include anything from design inspections to software static analyzer applications
- **Penetration Testing:** Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. (NIST SP 800-115)
  - For the purposes of this presentation, applying real-world attack scenarios in any manner, whether the scenario is carried out on paper or through the use of more advanced tools and techniques.
- **Red Teaming:** The use of an independent team to conduct activities similar to those described in penetration testing. This is typically associated with developmental testing.

References

1. Trusted Systems and Networks (TSN) Analysis June 2014 (http://www.acq.osd.mil/se/docs/Trusted-Systems-and-Networks-TSN-Analysis.pdf)
2. Martin, Robert, “Non-Malicious Taint: Bad Hygiene is as Dangerous to the Mission as Malicious Intent, CrossTalk Magazine issue on Mitigating Risks of Counterfeit and Tainted Components, March 2014, (http://www.crosstalkonline.org/storage/issue-archives/2014/201403/201403-Martin.pdf)
3. Reed, Melinda, John F. Miller, and Paul Popick, "Supply Chain Attack Patterns: Framework and Catalog," Office of the Deputy Assistant Secretary of Defense for Systems Engineering, August 2014.
4. Slater, Chris, et al,“ Toward a Secure Systems Engineering Methodology” , http://www.schneier.com/paper-secure-methodology.pdf
5. The MITRE Corporation, “Common Vulnerabilities and Exposures; The Standard for Information Security Vulnerability Names.” Internet: http://cve.mitre.org [Jan. 23, 2012].
6. The MITRE Corporation, “Common Weakness Enumeration; A Community-Developed Dictionary of Software Weakness Types.” Internet: http://cwe.mitre.org [Jan. 23, 2012].
7. The MITRE Corporation, “Common Attack Pattern Enumeration and Classification; A Community Knowledge Resource for Building Secure Software.” Internet: http://capec.mitre.org [Jan. 23, 2012].

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

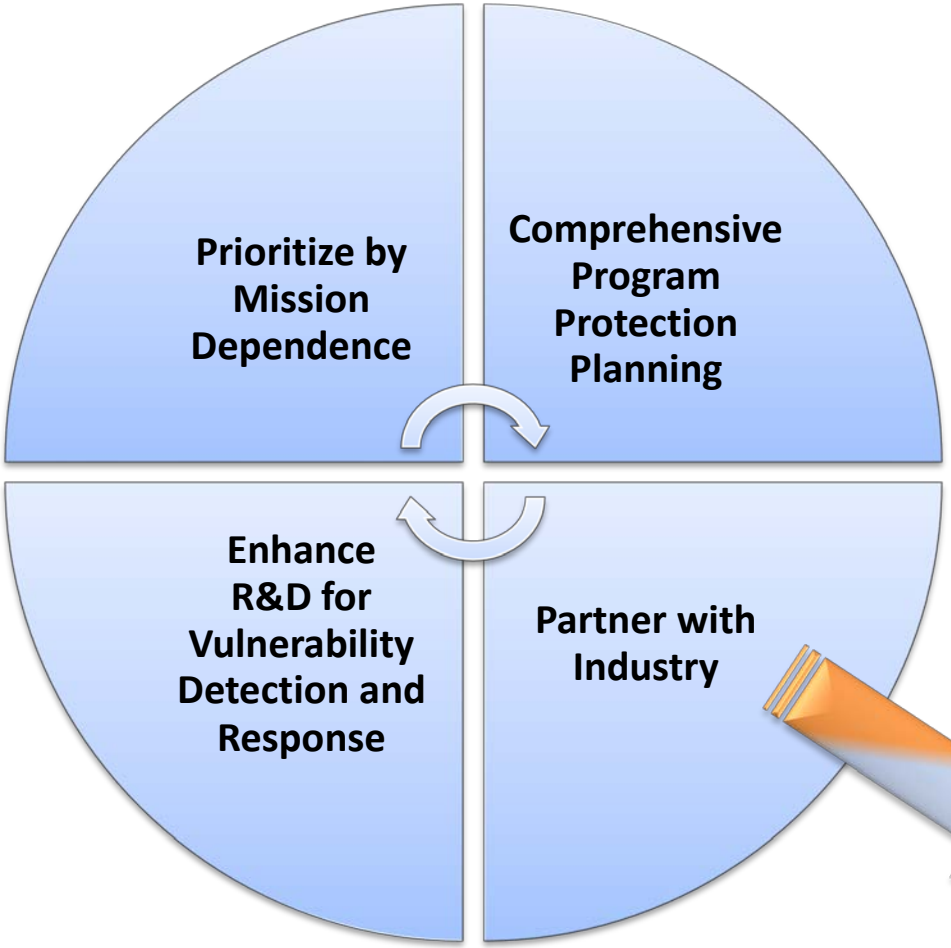
DASD, Systems Engineering
http://www.acq.osd.mil/se

Additional References

Trusted Defense Systems and Networks Strategy

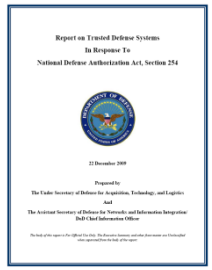
Drivers/Enablers

- National Cybersecurity Strategies
- Globalization Challenges
- Increasing System Complexity
- Intellectual Property Protection



Delivering Trusted Systems

Report on Trusted Defense Systems



USD(AT&L)
ASD(NII)/DoD CIO

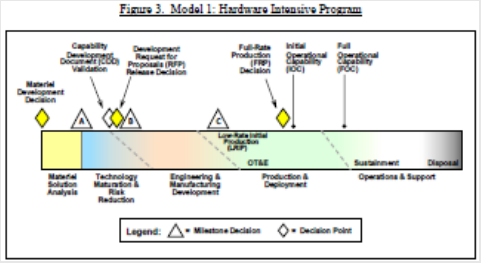
Executive Summary:
http://www.acq.osd.mil/se/pg/spec-studies.html

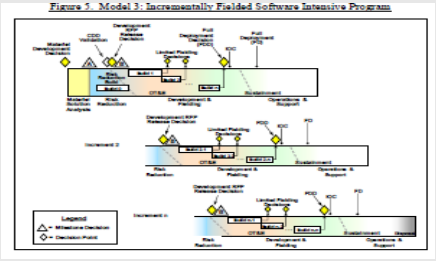
Ensuring Confidence in Defense Systems

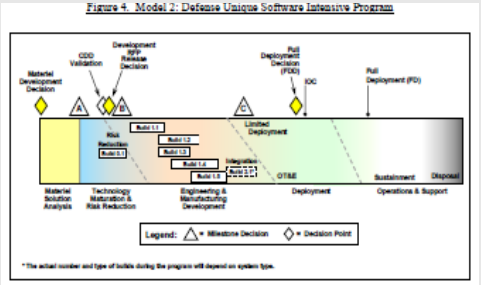
- ***Threat*:**
  - Nation-state, terrorist, criminal, or rogue developer who gain control of systems through supply chain opportunities, exploit vulnerabilities remotely, and/or degrade system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences:***
  - Loss of critical data and technology
  - System corruption
  - Loss of confidence in critical warfighting capability; mission impact

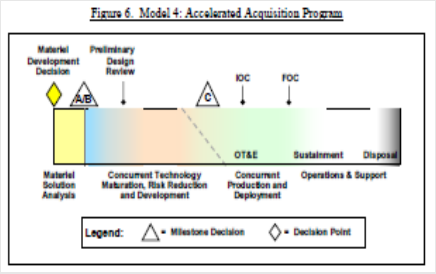
Today's acquisition environment drives the increased emphasis

Networked systems
Software-intensive
Prime Integrator, hundreds of suppliers
Advanced technology and critical components

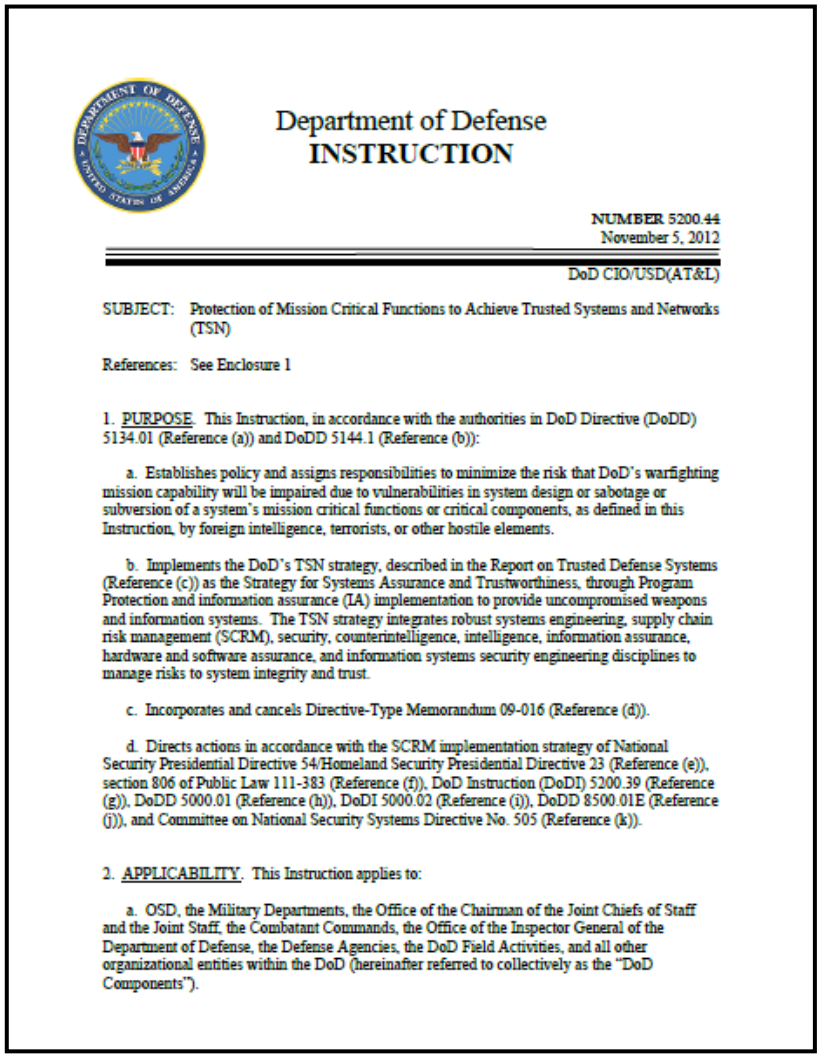








DoDI 5200.44
Trusted Systems and Networks



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout life cycle of key systems by utilizing**
  - Criticality analysis is the process for prioritizing risk management efforts
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
- **Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)**
- **Document planning and accomplishments in program protection and information assurance activities**

Static Analysis and Other Detection Techniques

- **Static analysis, dynamic analysis, and other testing, tools, and techniques to identify vulnerabilities in software during development**
  - Static and dynamic analyzers from different vendors use different testing techniques and internal criteria and often find different weaknesses and vulnerabilities
  - Program defines the categories of defects to be addressed
  - Program Identifies the detection method for each category to be addressed
  - For those capabilities that relate the defects to specific CWE and CVE entries, the results can be combined with the Vulnerability Database technique

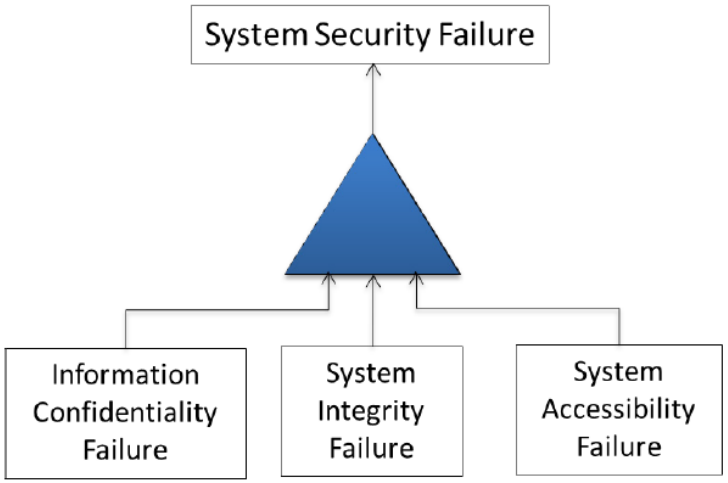
Optimal Use: As early as there is software to be assessed by detection tools. Typically useful legacy assessment in MSA phase and from PDR onward for developmental code

Static Analysis and Other Detection Techniques Incorporated into RFP

- **Incorporate requirements to conduct appropriate analysis techniques into the SOW of the RFP.**
- **Key factors for these requirements include:**
  - Ensure that the requirement scopes the analysis appropriately. One way is to require analysis on critical functions
  - Ensure that requirements state that certain categories of vulnerabilities found must be fixed prior to delivery (just completing the analysis is not sufficient)

Fault Tree Analysis (FTA)/ Attack Tree Analysis

- **Top-down approach that uses Boolean logic to identify potential sources of system failures**
  - Assumes a hypothetical system or mission failure has occurred
  - Traces outcome back through the system to determine contributing component malfunctions or failures



- **Activities for applying FTA to system security:**
  - Establish the set of failure events to be evaluated based upon the list of critical functions.
  - For each failure event, decompose the fault tree to identify the logical dependencies among hypothetical component failures.
  - Identify any "hot spots" of components that represent significant risks because they play a role in multiple failure events.

Optimal Use: FTA can be useful to identify sources of system failures in designs and product baselines, typically useful from PDR through deployment. Also can be applied to legacy systems.

Attack Tree Methodology

An Attack tree is a visualization tool to enumerate and weight different attacks against a system

- The SE creates an attack tree by replicating an adversary to find weak points in a system
  - The root node of the tree is the component being analyzed
  - To form the child nodes, the SE decomposes the node into its life cycle
  - Each life cycle phase breaks down into two access categories; physical security and trust model
  - If appropriate each node is further decomposed in this manner

The above is paraphrased from Salter et al, " Toward a Secure Systems Engineering Methodology" http://www.schneier.com/paper-secure-methodology.pdf

Fault Tree Analysis (FTA)/ Attack Tree Analysis

- **Applying the results of FTA/ATA**
  - Enhancing protections
    - Add protections to the design for any
  - Establishing a detection/response scheme
    - Protections are not practical in some circumstances based on cost or the impact to performance.
    - Detection: there may be more cost-effective measures which detect and log the fault/attack, so that the system or user is aware that it occurred
    - Response: Additionally, there may be a response measure put in place when certain faults/attacks are detected.
- **Adjustments in applying FTA for security**
  - The faults aren't random
    - Typical applications of FTA assume random faults, and independent probabilities of each faults, allowing for Bayesian analysis
    - In security, the faults are not independent or random. Therefore Bayesian analysis cannot be used from a security perspective.

Fault Tree Analysis (FTA)/ Attack Tree Analysis Incorporated into RFP

Key factors to include Fault Tree or Attack Tree Analysis in the RFP SOW or Section L:

- Program Office identifies top-level faults or components to be analyzed based upon the system needs for a protection scheme (to include prevention, detection and response measures)
- Contractors describe their fault tree and / or attack tree methodology
- Contractors propose top-level faults or components and identify a protection scheme (to include prevention, detection and response measures)

Red Team/Penetration Testing

- **Approach for Red Team/Penetration Testing**
  1. Gather data about the system, supply chain and development environment
  2. Define the objectives, type of attacks, and scope of the attacks
     - Types of attacks are a set of abuse or misuse cases that can be defined in a manner similar to use cases
  3. Execute simulation of attacks and record results
- **Impact of the results**
  - Extends the knowledge of the security behavior of the system, supply chain, and development environment
  - Demonstrates what an attacker can accomplish once the system is breached
  - Simulated attack data can be used to determine where more protection measures (if any) are necessary
  - Add attack pattern penetration test criteria to RFP

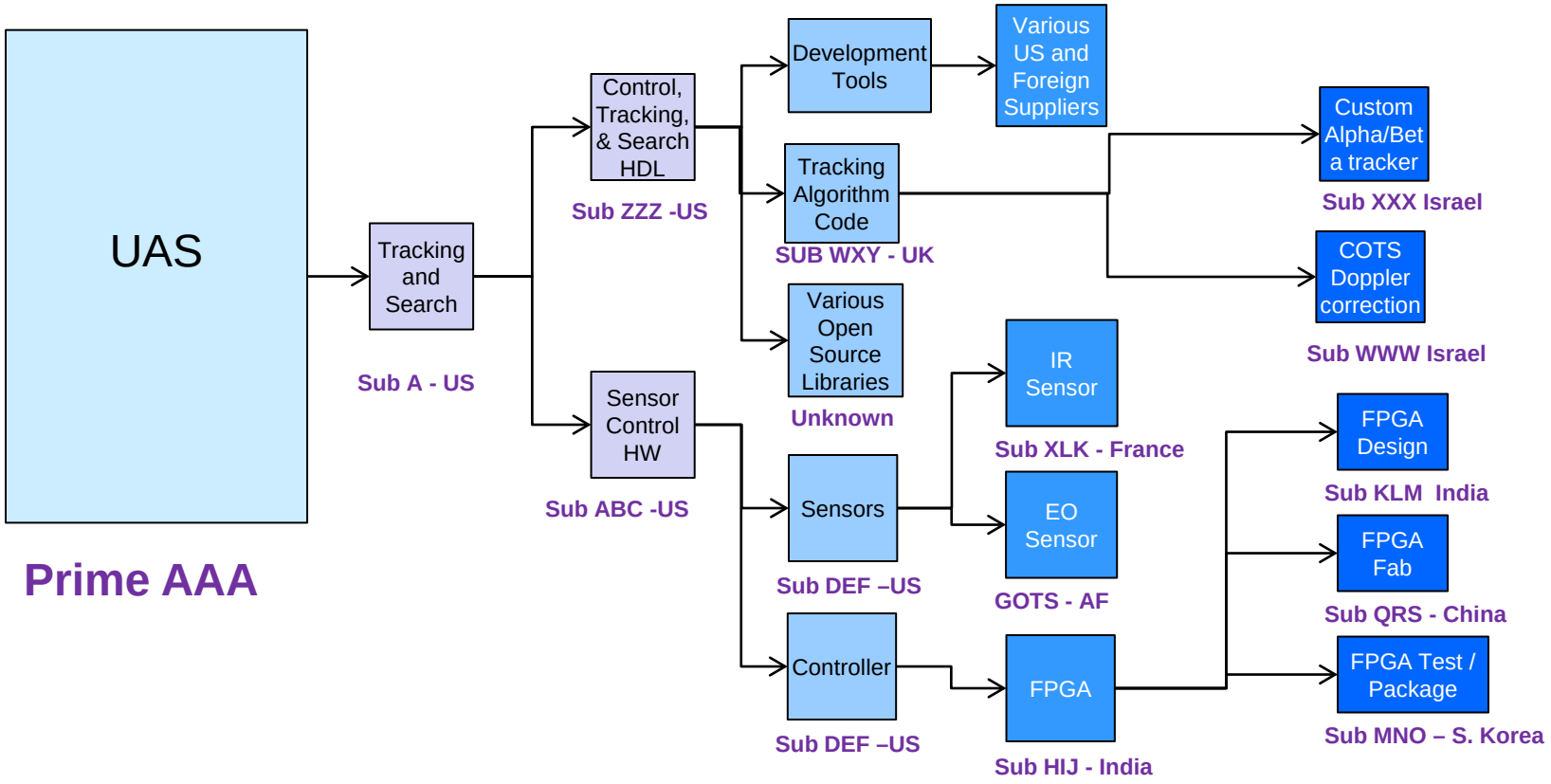
Optimal Use: As soon as the development environment/supply chain is established. For the system, once a system product baseline has been established. Begin defining penetration test scenarios as early as the MSA phase

Red Team/Penetration Testing: Supply Chain Example

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.



Red Team/Penetration Testing: Design Example

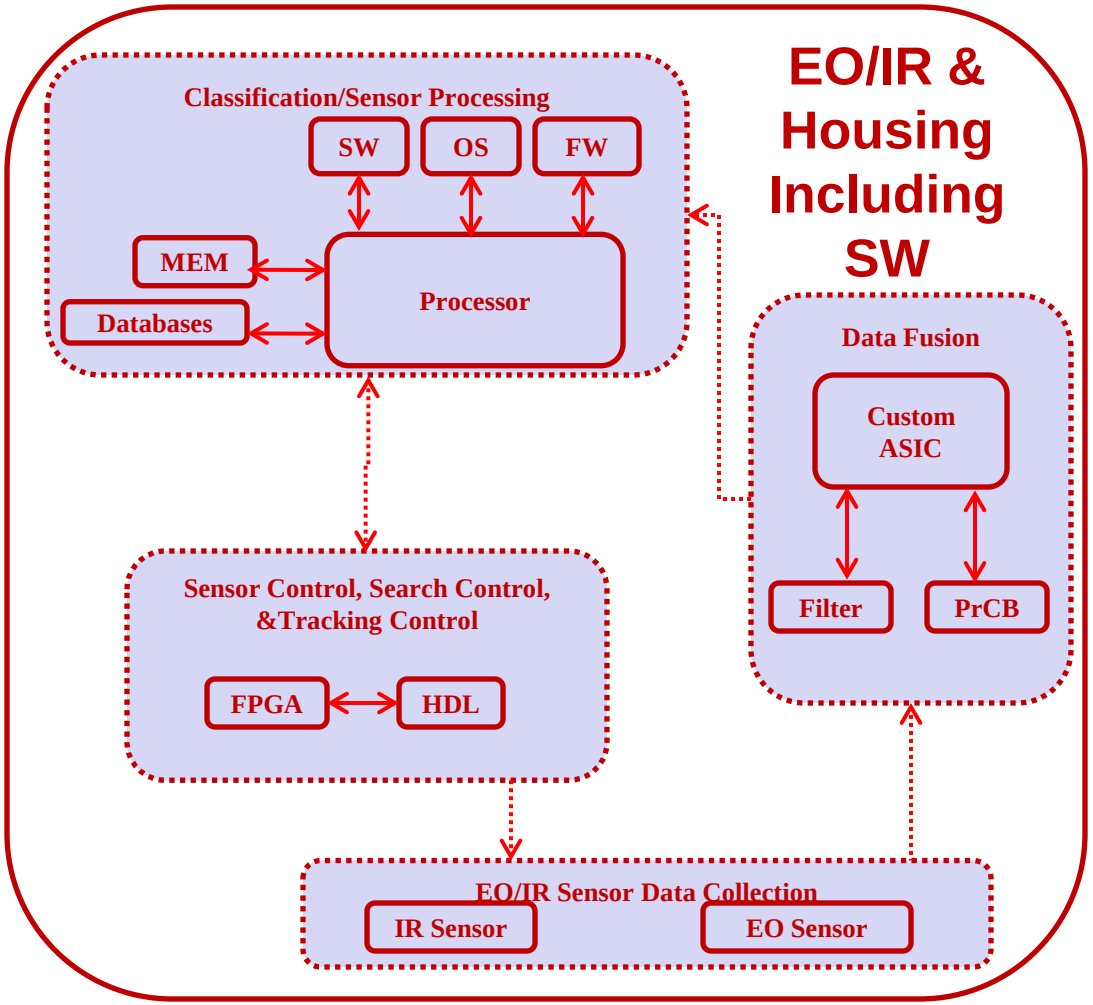
CAPEC-153: Input Data Manipulation

An attacker exploits a weakness in input validation by controlling the format, structure, and composition of data to an input-processing interface. By supplying input of a non-standard or unexpected form an attacker can adversely impact the security of the target. Input Data Manipulation seeks to control how the input is processed.

CAPEC-171: Variable Manipulation

An attacker manipulates variables used by an application to perform a variety of possible attacks. This can either be performed through the manipulation of function call parameters or by manipulating external variables, such as environment variables, that are used by an application.

Apply attack patterns to tracking and search functions



Red Team/Penetration Testing Incorporated into RFP

1. **Program Office would identify in the RFP a set of attack vectors which the system will be subjected to. Some key factors to identify:**
   - Defining the objectives, scope and types of attacks
   - Timing of red teams/penetration tests (could conduct paper one's early in the life cycle and "live" trials after
   - Defining acceptable outcomes and requirements for what to do with the results.