System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial

Exercises

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

15th Annual NDIA Systems Engineering Conference
San Diego, CA | October 22, 2012

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Criticality Analysis (CA) Exercise

Exercise Time: 15 minutes

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

CA Exercise – Scenario Description

- In this Exercise, you will perform an initial Criticality Analysis. You will determine the Critical Functions of a system, but not the implementing Critical Components.

- You have been assigned to the program office for an acquisition program that has just completed its Analysis of Alternatives (AoA) and has begun the engineering analysis of the **preferred concept** .

- The **preferred concept** is a fixed wing unmanned aircraft system (UAS) to perform an ISR mission. The program office has begun defining and decomposing the preferred concept and assessing the critical enabling technologies.

- The ISR mission thread is the "kill chain" mission thread – to consider search, locate, and track of an enemy surface strike group and pass targeting information back to an airborne E-2D that, in turn, provides information to a carrier strike aircraft.

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Criticality Analysis Exercise – Template for Results

- Divide into teams of 2 to develop an initial Criticality Analysis
- You have been provided with
  - A generic unmanned aerial vehicle operational view (OV-1)
  - A concept of operations
  - A copy of the chart shown below to record your results
- Determine and list 5 to 6 Critical Functions associated with the "kill chain" mission thread. Concentrate on functions that will be implemented with logic bearing hardware, firmware, and software. Assign Criticality Levels.

#	Critical Function	Level
1		
2		
3		
4		
5		
6		

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Case Study – Concept of Operations (CONOPS)

Notional UAS CONOPS

- Operational Employment: The Unmanned Aircraft System (UAS) provides persistent intelligence, surveillance and reconnaissance (ISR) to the fleet to improve battle space situational awareness and enhance the find, fix, and track portions of the sensor-to-shore kill chain including anti-access and access denial operations. The UAS conducts autonomous ISR operations utilizing an Unmanned Aerial Vehicle (UAV) with on-board active and passive sensors to collect, process, and forward sensor data to the UAS Mission Control System (MCS) for further analysis, assessment, and dissemination. The UAV may forward its sensor data to airborne platforms such as the E-2D and P-8 for tactical utilization as required by operational tasking. The UAV is capable of operating either from a carrier (CVN) as an integral part of the Carrier Air Wing (CVW) or from a Naval Air Station (NAS) as part of a CVW detachment ashore. UAV afloat and ashore air operations are autonomous but similar to a manned aircraft, with the added capability of direct intervention by a human operator for CVN flight deck operations, airborne safety of flight actions, and maintenance actions. Mission execution capability resident within the UAV includes the ability to accept in-flight updates to the mission plan from an authorized source, including another MCS or a C2 facility equipped, trained, and certified to provide mission plan updates to the UAV. Specific UAS ISR mission and sensor performance is contained in the UAS Initial Capability Document (ICD).

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Case Study – Concept of Operations (CONOPS)

- Operational Employment (continued): The Mission Control System (MCS) performs the Tasking, Processing, Exploitation, and Dissemination (TPED) functions required for ISR execution through its mission planning, mission execution, sensor data analysis, and dissemination steps. Mission planning takes the air tasking order, develops and validates a mission flight plan from the point of takeoff to the operating area (and return), and generates the UAV mission plan for upload into the UAV. The mission flight plan includes the matching of sensors to ISR tasking received, as well as linking the UAV communications suite capabilities to the line-of-sight (LOS) and beyond-line-of-sight (BLOS) communication plan for sensor data dissemination and flight following. Mission execution is accomplished by a team that includes: Mission Commander, who is responsible for mission execution; UAV operator, trained and certified to conduct autonomous UAV flight operations, who oversees UAV flight operations; and sensor operator, who receives the sensor download from the UAV, conducts data analysis, and makes sensor data dissemination recommendations to the Mission Commander. The MCS operates at a 24x7 pace when ISR missions are conducted and is capable of handling multiple UAS missions simultaneously as stated in the ICD. The MCS is included as part of the CVN-installed ISR and air operations systems or as a mobile facility hosted by a NAS. The afloat MCS exercises Level IV control over the UAV; UAV launch and recovery is integrated into the CVN launch and recovery systems (JFCOM TCS JOINT CONOPS May 2000). The ashore MCS is a Level V facility which includes capability of launching and recovering UAVs.

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Case Study – Concept of Operations (CONOPS)

- Operational Scenario: A US carrier battle group (CBG) is tasked with maintaining situational awareness of all non-US surface warship activities within the South China Sea. The CVW UAS squadron is tasked with providing 24x7 surveillance coverage of the operation area. An airborne E-2D will provide air surveillance coverage and will keep an airborne tactical plot of non-US warship traffic in the South China Sea. The UAS task is to conduct a surface search of the South China Sea and report to the CBG and E-2D any detected suspected surface warships while maintaining Rules of Engagement (ROE) standoff distances from surface warships. The CVN MCS is tasked with planning and executing the tasking, including assessment of UAV sensor data to confirm identification, location, course, and speed of surface warships. The MCS Mission Commander has tactical control over the UAV and is authorized to modify the mission plan as required to complete: 1) surface search of the operational area; and 2) maintain track of designated non-US warships.

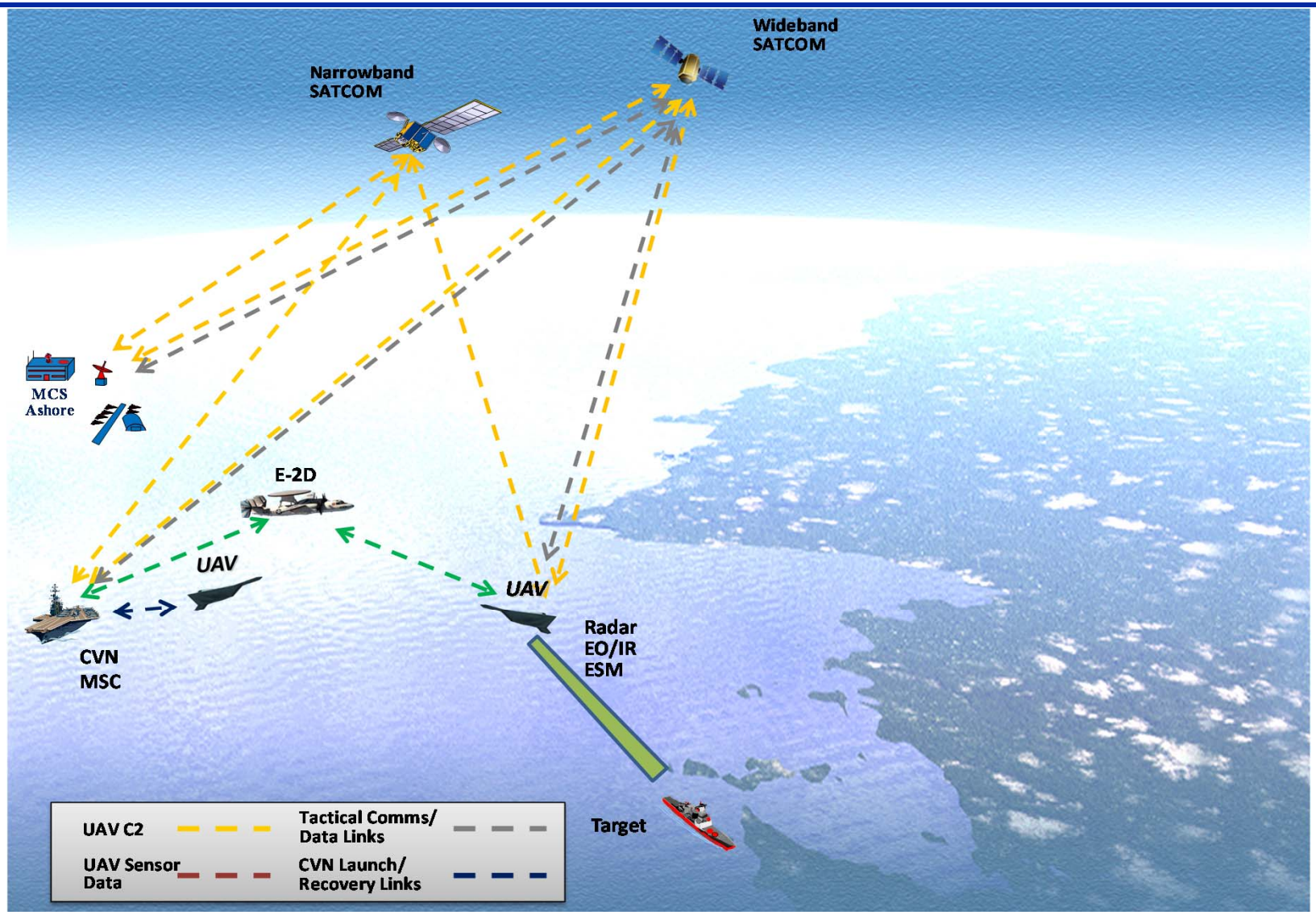
Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Case Study – Concept of Operations (CONOPS)

- Maintenance and Logistics: The UAS maintenance philosophy is Organizational (O-Level) to Depot (D-Level) where O-Level maintenance responsibilities include daily pre-flight, post-flight, turnaround inspections, and system level troubleshooting. Organizational level scheduled and unscheduled maintenance is conducted primarily by Weapon Replacement Assembly (WRA), Shop Replaceable Assembly (SRA), and/or component level "remove and replace" capability. Although there is some Intermediate (I-Level) maintenance (e.g., tire and wheel, hydraulics) leveraging on the existing CVN/NAS infrastructure, the majority of daily maintenance is conducted by O-Level military (organic) personal for both the CVW and ashore detachment locations. D-Level maintenance is anticipated to include airframe, engine, communication, and sensors supported by military, contractor, or a combination of military/contractor maintainers.
- The UAS requires logistic support whether as part of the CVW or stationed ashore at an NAS. A logistic management system integrated with the Naval Aviation Logistic Command information system is the centerpiece of tracking and managing the UAS supply and maintenance activities. The UAS Squadron afloat or ashore has access to the same data residing within the UAS logistic management system to include maintenance actions status, supply management and electronic aircraft discrepancy book information.

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Case Study – High-Level OV-1



Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment (VA) Exercise – Part I

Exercise Time: 20 minutes

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part I

Continuing along on the UAS for maritime surveillance we are going to look at potential supply chains, including software and firmware COTS, and the software development process for tracking and search functions from the preceding criticality analysis.

The end objective is to identify and quantify the potential vulnerabilities so that cost effective "countermeasures" can be incorporated into the system requirements or the statement of work prior to issuing the RFP

Brain storm a list of the possible vulnerabilities to each of the potential supply chain and the software development process chains provided. Also consider UAV specific vulnerabilities

You have been provided with

1. Criticality Analysis Results *in Exemplars*
2. Architecture Handout
   - Generic supply chain and malicious threat vectors
   - A notional architecture that is used to support requirements analysis
   - Two potential supply chains diagrams
   - Two possible software development life cycles

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Detailed Step by Step Vulnerability Assessment

Step 1 – Determine Access Path Opportunities

- Consider the system CONOPS (including OV-1 diagram) and notional architecture to determine design-attribute related attack surfaces
- Consider the SE, SW, and Supply Chain processes for process-activity type weaknesses

Step 2 – Select Attack Scenarios

- Determine the types of attack scenarios that might apply by considering how an adversary could exploit potential software and supply chain weaknesses
- Select a set of attack vectors from the catalog that best fit the attack surface identified by the chosen attack scenarios ("the catalog" is provided by the generic threats in the Architecture Handout and the attack vector catalog in the Tutorial Appendix)
- Consider both intentional and unintentional vulnerabilities (keeping in mind that the exploit will be of malicious intent)

Step 3 -- Determine Exploitable Vulnerabilities

- Select two critical components for each supply chain
- Apply each attack vector against each component and, with engineering judgment, assess if the attack vector is successful
- If successful, then an exploitable vulnerability exists
- Repeat the approach using the next attack vector
- For each critical component, list its vulnerabilities

Step 4 – Inform the Threat Assessment / Vulnerability Assessment Based Risk Likelihood Determination

- This step is part of the next exercise

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part I Output Template

Supply Chain 1

Supply Chain Vulnerability	Software Development Vulnerability

Supply Chain 2

Supply Chain Vulnerability	Software Development Vulnerability

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment (VA) Exercise – Part II

Exercise Time: 30 minutes

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part II – with Heuristic Questions

Continuing along on the UAS for maritime surveillance we are going to look at potential supply chains, including software and firmware COTS, and the software development process for two of the components from the Vulnerability Assessment Part I

The objective of this exercise is to identify and quantify additional potential vulnerabilities for two of the components

1. For two given potential critical components (one from each of the potential supply/development chains provided), answer the questions on the following two charts
2. Add domain specific questions or any questions that you developed during vulnerability brainstorming that are not addressed in the following two charts

You have been provided with

– Two selected potential critical components

– A set of generic supply chain and software assurance vulnerability questions

– Results of participants' brain storming domain specific vulnerabilities

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part II

- **Approach:**
  - Use the following two critical components (from supply chains 1 and 2)
    - CC1: FPGA (Sub HIJ)
    - CC2: Custom Tracking Algorithm SW (Sub SSS)
  - Respond to the questions on the following pages
    - Review each question and determine if the intent of the question applies to your supply chain environment. If it does not, mark it N/A. If it does, continue:
  - Determine if your supply chain vulnerability list addresses the question. If it does, place a "Y" in the corresponding row; if not, place a "N". (This approach assumes that plans to address the identified vulnerability are already in place.)
    - Using Q1 as an example: If one of your CC1 identified vulnerabilities deals with the need for a trusted supplier, then enter a "Y" in that row under the CC1 column. If not, then enter a "N"

Note:

- Do not be surprised if there is a large number of "N"s recorded, as access to a draft SOW, which would address many of these questions, has not been provided

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part II

- **Supply chain vulnerabilities to consider (put a "Y" or "N" next to each question)**

FPGA: Sub HIJ	Custom Tracking Algorithm: Sub SSS

1. Does the Contractor have a process to establish trusted suppliers ?
2. Require suppliers to have similar processes for the above questions?
3. Has the prime contractor vetted suppliers of critical function components (HW/SW/Firmware) based upon the security of their processes?
4. Are secure shipping methods used to ship? How are components shipped from one supplier to another
5. Does receiving supplier 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.)?
6. Does the supplier have controls in place to ensure technical manuals are printed by a trusted supplier who limits access to the technical material?
7. Does the supplier have controls to limit access to critical components?
8. Can the contractor identify everyone that has access to critical components?
9. Are Blind Buys Used to Contract for Critical Function Components?
10. Are Specific Test Requirements Established for Critical Components?
11. Does the Developer Require Secure Design and Fabrication or Manufacturing Standards for Critical Components?

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part II

- **Software vulnerabilities to consider (put a "Y" or "N" next to each question)**

FPGA: Sub HIJ	Custom Tracking Algorithm: Sub SSS

1. Does the Developer Have a design and code inspection process that requires specific secure design and coding standards as part of the inspection criteria?
   - Secure design and coding standards which considers CWE, Software Engineering Institute (SEI) *Top 10* secure coding practices and other sources when defining the standards?
2. Have common Software Vulnerabilities Been Mitigated?
   - Derived From Common Weakness Enumeration (CWE)
   - Common Vulnerabilities and Exposures (CVE)
   - Common Attack Pattern Enumeration and Classification (CAPEC)
3. Are Static Analysis Tools Used to Identify violations of the secure design and coding standards?
4. Are design and code inspections used to identify violations of secure design and coding standards?
5. Does the Software Contain Fault Detection/Fault Isolation (FDFI) and Tracking or Logging of Faults?
6. Do the Software Interfaces Contain Input Checking and Validation?
7. Is a separation kernel used to control communications between level I critical functions and other critical functions
8. Is Access to the Development Environment Controlled With Limited Authorities and Does it Enable Tracing All Code Changes to Specific Individuals?
9. Are Specific Code Test-Coverage Metrics Used to Ensure Adequate Testing?
10. Are Regression Tests Routinely Run Following Changes to Code?

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Vulnerability Assessment Exercise Part II

- **UAV and design specific vulnerabilities to consider from Part I brainstorming (put a "Y" or "N" next to each question)**

	FPGA: Sub HIJ	Custom Tracking Algorithm: Sub SSS
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Initial Risk Assessment (RA) Exercise

Exercise Time: 30 minutes

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Risk Assessment – Likelihood Guidance

- One approach for translating the vulnerability assessment into a risk likelihood input is to use an equal weighted scoring model that calculates the percentage of "No" answers in the groupings of "Y-N" questions from the VA.
- We will use this method for the exercise:

Number of "No" Responses	Risk Likelihood
All "NO"	Near Certainty (VH - 5)
>=75% NO	High Likely (H - 4)
>= 25% No	Likely (M - 3)
<= 25% No	Low Likelihood (L - 2)
<= 10% No	Not Likely (NL - 1)

- Use the table above to determine the risk likelihood for each critical component
  - Develop likelihood calculations for supply chain, software, and domain-specific
- Approaches to combining the Supply Chain Vulnerability Assessment and the Software Vulnerability Assessment
  - Do separate calculations to determine two vulnerability likelihoods and then use the most severe among the threat and the two vulnerabilities as the overall likelihood input
  - ✓ Do separate calculations and average to get a single likelihood calculation
  - Domain specific judgment on weightings to get a single likelihood

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Risk Assessment Exercise

Determine the overall risk likelihood for each of the two selected critical components

- Assume a Likely [M(3)] to Highly Likely [H(4)] threat likelihood for suppliers for which you have no threat information request results
- For the domain-specific "Y-N" VA questions, do one of the following:
  - Separate them and allocate each to either the supply chain or SW group
  - Add another column below and include a domain-specific calculation

Component	Threat Assessment Likelihood	Supply Chain VA Likelihood	Software Development VA Likelihood		Overall Likelihood
FPGA (Sub HIJ)					
Custom Tracking Algorithm SW (Sub SSS)					

Add any others that you'd like to assess

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Risk Assessment Exercise

Using the likelihoods from the previous page and your previous consequence ratings, determine the overall risk rating

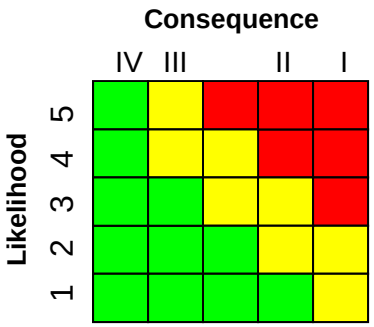
Component	Overall Likelihood	Consequence (from Criticality Analysis)	Risk Rating
FPGA (Sub HIJ)			
Custom Tracking Algorithm SW (Sub SSS)			

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

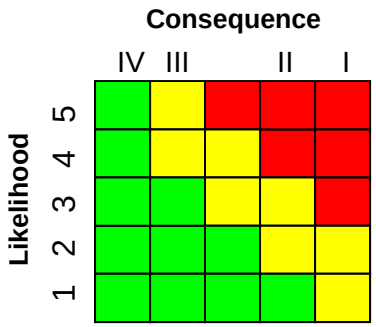
Risk Assessment Exercise

Initial Risk Posture for two or more selected Critical Components

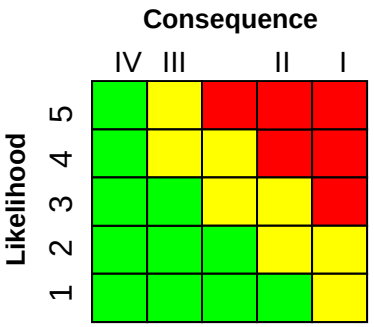
CC1:



CC2:



CC3:



Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Countermeasures Selection (CS) Exercise

Exercise time: 30 minutes

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Examples of Possible Countermeasures

Risk	Cost
-1	M
-2	H
-1	L
-2	L
-1	M
-2	H
-2	M
-1	L

- Possible acquisition process countermeasures for critical functions with risk lowering impact and order of magnitude cost
  - ❑ A supplier management plan
    - supplier selection criteria to reduce supply chain risks
    - Identification functionally equivalent alternate components and sources
    - Evaluates and maintains a list of suppliers and alternates suppliers with respect to the criteria established
  - ❑ An anonymity plan that
    - Protects the baseline design, test and supply chain data
    - Use blinds buys for component procurement
  - ❑ Secure design and coding standards that address the most common vulnerabilities identified in CWE or the CERT.
  - ❑ The use of secure design and coding standards are part of the criteria used for design and code inspections
  - ❑ The use of a static analyzer to identify and mitigate vulnerabilities
  - ❑ Inspection of code for vulnerabilities and malware
  - ❑ Access control that
    - Limits access
    - Logs access and notes specific information changed and accessed
    - Require inspection and approval of changes
  - ❑ A Government provided supply chain threat briefing
- ***Values assigned to risk reduction and cost are for example. Program based team's must develop estimates for their environment for reducing risk likelihood and cost to implement.***

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Examples of Possible Countermeasures

- Possible system design countermeasures for critical functions with risk lowering impact and order of magnitude cost

Risk	Cost
-2	H
-1	M
-1	L
-2	L
-2	M
-2	M
-2	H

- ❑ A separation kernel –
  - hardware and/or firmware and/or software mechanisms whose primary function is to establish, isolate and separate multiple partitions and control information flow between the subjects and exported resources allocated to those partitions
- ❑ Fault detection with degraded mode recovery
- ❑ Authentication with least privilege for interfacing with critical functions
- ❑ Wrappers for COTS, legacy and developmental software to enforce strong typing and context checking.
- ❑ Wrappers for COTS, legacy and developmental software to identify and log invalid interface parameters
- ❑ physical and logical diversity where redundancy or additional supply chain protections are required
- ❑ An on-board monitoring function that checks for configuration integrity and unauthorized access.
  - Examples include honey pots which capture information about attackers, scanners and sniffers that check for signatures of attackers, and monitoring clients which check for current patches and valid configurations

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.

Cost-Benefit-Risk Trade Study Exercise

- **The exemplar critical components are given below**
  - Determine at least two countermeasures to evaluate for each component
  - Estimate the implementation cost impacts and risk reduction achieved by each countermeasure

Component	Risk Rating	Countermeasures	Cost impact	Risk reduc-tion	Residual Risk Rating
Custom Tracking Algorithm SW (Sub SSS)					
FPGA (sub HIJ)					
Math Lib (open source)					

- **Select Countermeasures for Implementation by putting a star next to the ones selected**
- **For this exercise assume that:**
  - A Countermeasure value of -1 reduces likelihood by one band in the risk cube
  - Cost values have the following cost weights: L= $25K; M=$250K; H=$2.5M

Distribution Statement A – Approved for public release by OSR on 10/10/2012, SR Case # 13-S-0072 applies.