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

Exercise Exemplars

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 10/09/2012, SR Case # 13-S-0074 applies.

Criticality Analysis (CA) Exemplar

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Criticality Analysis Exercise Possible Solution

Use these results for future exercises:

#	Critical Function	Level
1	**Search** -Conduct a search in the area assigned using onboard sensors at standoff distances required for survival purposes based on pre-mission intelligence as well as in-flight intelligence updates	I
2	**Detect** - Analyze sensor systems responses for possible surface contact	I
3	**Locate** -Establish target position and vector (course and speed); quality of position and vector within the strike platform engagement requirements	I
4	**Classify -** Use onboard sensors combined with multi-intelligence data obtained from non-organic systems to determine if contact is: friendly, neutral, hostile or unknown; if hostile – determine type	**II**
5	**Communicate -** Pass surface ship contact information and video feed via tactical data link back to airborne E-2D; receive intelligence and tasking updates via tactical data link or secure voice	**I**
6	**Track -** maintain surface contact plot of area of interest; once enemy surface group is located, maintain track until directed otherwise; provide target updates location and vector at X frequency via tactical data link	**II**

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Vulnerability Assessment (VA) Exercise I Exemplar

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Vulnerability Assessment Exercise
Part I - White Board Discussion Exemplar

Supply Chain 1

Critical Component: *EO/IR FPGA*	Critical Component: *Tracking Algorithm Code*
Supply Chain Vulnerability	**SW Development Vulnerability**
OEM Manufacture Process	SW Configuration Management Repository
Vendor FPGA fabrication process	SW development facility
Vendor FPGA parts supplier	SW developer design activity
OEM design process	

Supply Chain 2

Critical Component: *Sensor Control SW*	Critical Component: *Custom Tracking Algorithm SW*
Supply Chain Vulnerability	**SW Development Vulnerability**
Open source math libraries	SW development facility
SW Configuration Management repository	SW developer design activity
SW development facility	SW developer baseline
	Open source math libraries

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Vulnerability Assessment (VA) Exercise II Exemplar

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Vulnerability Assessment Exercise Part II Results – for future Exercises

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

FPGA: Sub HIJ	Custom Tracking Algorithm: Sub SSS	
Y	N	1. Does the Contractor have a process to establish trusted suppliers ?
Y	N	2. Require suppliers to have similar processes for the above questions?
N	N	3. Has the prime contractor vetted suppliers of critical function components (HW/SW/Firmware) based upon the security of their processes?
Y	Y	4. Are secure shipping methods used to ship? How are components shipped from one supplier to another
Y	Y	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.)?
Y	N	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?
N	N	7. Does the supplier have controls to limit access to critical components?
Y	N	8. Can the contractor identify everyone that has access to critical components?
N	N	9. Are Blind Buys Used to Contract for Critical Function Components?
N	Y	10. Are Specific Test Requirements Established for Critical Components?
N	N	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 10/09/2012, SR Case # 13-S-0074 applies.

Vulnerability Assessment Exercise Part II Results – for future Exercises

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

FPGA: Sub HIJ	Custom Tracking Algorithm: Sub SSS	
N	Y	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?
N	N	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)
Y	N	3. Are Static Analysis Tools Used to Identify violations of the secure design and coding standards?
N	N	4. Are design and code inspections used to identify violations of secure design and coding standards?
Y	N	5. Does the Software Contain Fault Detection/Fault Isolation (FDFI) and Tracking or Logging of Faults?
N	N	6. Do the Software Interfaces Contain Input Checking and Validation?
N	N	7. Is a separation kernel used to control communications between lvl I critical functions and other critical functions
N	N	8. Is Access to the Development Environment Controlled With Limited Authorities and Does it Enable Tracing All Code Changes to Specific Individuals?
Y	N	9. Are Specific Code Test-Coverage Metrics Used to Ensure Adequate Testing?
Y	Y	10. Are Regression Tests Routinely Run Following Changes to Code?

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Vulnerability Assessment Exercise Part II Results – for future Exercises

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

FPGA: Sub HIJ	Custom Tracking Algorithm: Sub SSS
N/A	N/A
N	Y
N	N
N	N
N	N/A
Y	N/A
N	N
Y	N
N	N

1. Will the development tools undergo acceptance testing before installation in the development facility
2. Is red team testing planned for the supply chain and development facility each component ?
3. Does the UAV zero memory if system is brought down outside of US control
4. Does UAV have anti-tamper to protect technology intellectual property?
5. Does the FPGA utilize encryption for loading bit streams onto the component?
6. Are custom designed ASICs sourced from a trusted supplier?
7. Has the maintenance port on the classification / sensor processor been disabled to prevent backdoor access
8. Does the configuration management system require two authenticated users to process a change?
9. Is a code review done on all open source software used by the component

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Initial Risk Assessment (RA) Exemplar

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Risk Assessment Possible Solution

Overall risk likelihood exemplar for use in determining the risk rating:

Component	Threat Assessment Likelihood	Supply Chain VA Likelihood	Software Developme nt VA Likelihood	Program Generated Questions	Overall Likelihood
FPGA (Sub HIJ)	H	L (45%)	M(60%)	M(50%)	M
Custom Tracking Algorithm SW (Sub SSS)	M	M (72%)	H(80%)	H(83%)	H

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Risk Assessment
Possible Solution

Overall risk rating exemplar:

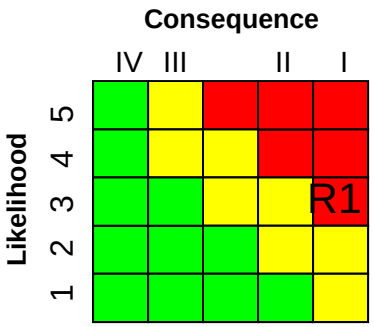
Component	Overall Likelihood	Consequence (from Criticality Analysis)	Risk Rating
R1 - FPGA (Sub HIJ)	M (3)	H(5)	H(3,5)
R2 - Custom Tracking Algorithm SW (Sub SSS)	H (4)	H(4)	H(4,4)

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

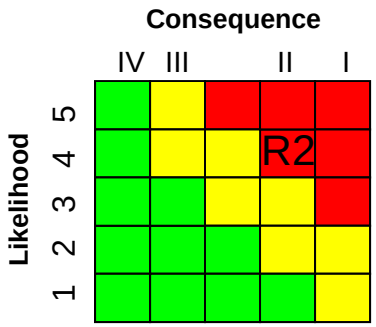
Risk Assessment Exercise

Initial Risk Posture for two or more selected Critical Components

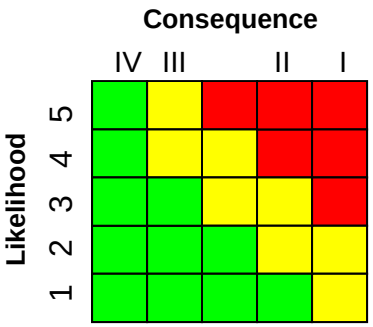
FPGA: R1



Track: R2



CC3:



Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Countermeasures Selection (CS) Exemplar

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.

Cost-Benefit-Risk Trade Study Exemplar

Component	Risk Rating	Countermeasures	Cost impact	Risk reduc-tion	Residual Risk Rating
Custom Tracking Algorithm SW (Sub SSS)	H (4,4)	Secure design and coding stds	L	-1	M (3,4)
		Wrappers	M	-2	M (2,4)
		Separation Kernel	H	-2	M (2,4)
FPGA (sub HIJ)	H (3,5)	Anonymity plan that	H	-2	L (1,5)
		Access control	M	-2	L (1,5)
Math Lib (open source)	H (4,4)	Static analyzer	M	-1	M (3,4)
		Manual inspection	L	-2	M (2,4)

Distribution Statement A – Approved for public release by OSR on 10/09/2012, SR Case # 13-S-0074 applies.