CQSDI
Cyber Physical System Security Panel

System Security Perspective
March 2019

Holly Dunlap
Raytheon
NDIA SSE Committee Chair
Holly.Dunlap@Raytheon.com
Agenda

• Observations as the NDIA SSE Committee Chair
• Where we’ve been, where we are, and where we are heading
• King for a Day
Cyber is everyone’s responsibility

.... what is your responsibility?
Winter (Cyber) is Coming….

Pretty sure its here.

HELLO BEAUTIFUL

https://www.ourmovielife.com/2017/08/15/game-thrones-prediction-5-will-wall-fall/

https://www.youtube.com/watch?v=GsEBezKmuFA
Key DoD Protection Activities to Improve Cyber Resiliency

Program Protection & Cybersecurity
DoDI 5000.02, Enclosure 3 & 14

Technology
What: A capability element that contributes to the warfighters’ technical advantage (CPI)

Key Protection Activity:
• Anti-Tamper
• Defense Exportability Features
• CPI Protection List
• Acquisition Security Database

Goal: Prevent the compromise and loss of CPI

Components
What: Mission-critical functions and components

Key Protection Activity:
• Software Assurance
• Hardware Assurance/Trusted Foundry
• Supply Chain Risk Management
• Anti-counterfeits
• Joint Federated Assurance Center (JFAC)

Goal: Protect key mission components from malicious activity

Information
What: Information about the program, system, designs, processes, capabilities and end-items

Key Protection Activity:
• Classification
• Export Controls
• Information Security
• Joint Acquisition Protection & Exploitation Cell (JAPEC)

Goal: Ensure key system and program data is protected from adversary collection

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

System security engineering evaluates, integrates, and manages the risks of security specialties: hardware assurance, software assurance, anti-tamper, supply chain risk management, and cybersecurity, to provide a security perspective within the system architecture and throughout the system development lifecycle.
Trending towards convergence…

2011
- Technology
- Information
- Components

2015
- Technology
- Information
- Components

+2019
- Safety
- Technology
- Information
- Components
- Reliability
- Quality
- Cyber Resilient & Secure Systems
Readily Available Clear System Security Trade (Risk, Cost, Performance) Based Options

Why is this important?

Customer Requirement Example: Trusted, Cyber Resilient, & Secure System
Customer Requirement Example: Implement Risk Management Framework

How do we get from here to here?!

Trusted, Cyber Resilient, & Secure System

Technical Requirements

Tends to be ambiguous & hard to measure, hard to prove, hard to compete for contracts....
System Security Engineering King for the Day Wish…..

Start with the high level operational Systems of Systems Concept to understand what is critical to the success of the mission

Decompose the system and identify system mission critical functions

Further decompose the system mission critical function into system mission critical components (hardware, software, firmware).

Select components with the right risk, cost, and performance to meet the customers requirements.

Provide an assurance case to prove the customer requirements have been met.

• Tiers of Assurance
  (Confidence Levels)
  – Architecture
  – Hardware
  – Software
  – Supply Chain
  – Protection of Critical Program Information (CPI)

• Assurance Case
  – Claim - Assertion to be proven
    – Argument – How evidence supports the claim
      – Evidence – Documented proof.
Prove Why Your System Should be Trusted

- Assurance cases includes the collection of things you do to increase confidence that the system and all of the integrated components (hardware, software, firmware) will work as designed and only as intended. Some of these actions may also be considered to be countermeasures or risk mitigations.
  - People (Expertise. Critical thinking.)
  - Processes (Standard operating procedures. Reducing variation. Analysis)
    - Testing
  - Technology
    - Design Features
    - Tools
    - Capabilities

Prove the System is safe.
Prove the System is reliable.
Prove the System is secure.
Prove the System is trustworthy.
Prove the System is resilient while under attack.

Would you bet your life on it?
Would you bet your family’s life on it?