

System Security Engineering for Safer Systems

John Maziarz, CSEP-Acquisition

Gary Dockall, CSEP

Disclaimer

This presentation comprises the thoughts of the presenter and does not reflect positively or negatively on the presenter's employer, clients, or professional affiliations.

Outline

- Introduction
- What IS System Security Engineering?
- Why Have System Security Engineering?
- Why plan for System Security Engineering?
- So What?
- Conclusion

Outline

- **Introduction**
- What IS System Security Engineering?
- Why Have System Security Engineering?
- Why plan for System Security Engineering?
- So What?
- Conclusion

Introduction

- We live in a very non-secure world today
 - July 2013 INCOSE Insight was dedicated to System Security
 - Countless accounts of damaging, counterfeiting, hacking, etc., of things and information

A Few Examples

- Vice-President Dick Cheney's pacemaker
- Target department store chain identity theft
- U. S F-35 fighter sensitive data
- Possible identify theft via computers implementing U. S. Government's Affordable Care Act
- 2015 Ukraine power outage
- Hypothetical "strategic EMP event"

Doing it Right

- Zenith Electronics Corporation had it right!



- Translating to security: Let's plan security measures the right way, up front, **BEFORE** we do all the cool stuff!

System Security Engineering, aka...

- System security
 - System protection
 - Program security
 - Program protection
-
- Bottom line – all similar terms, all with the same end state in mind

Outline

- Introduction
- **What IS System Security Engineering?**
- Why Have System Security Engineering?
- Why plan for System Security Engineering?
- So What?
- Conclusion

An Obligatory Definition

- National Institute of Standards and Technology Special Publication 800-160 defines system security engineering as:
“...a specialty engineering discipline of systems engineering that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties and other contributing engineering specialties to provide a fully integrated, system-level perspective of system security.”

Or Two...

- Defense Acquisition University's Defense Acquisition Guidebook, Chapter 3, defines Program Protection as:

"...the integrating process for mitigating and managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability, or supply chain exploitation/insertion, battlefield loss, and unauthorized or inadvertent disclosure throughout the acquisition lifecycle."

Anti-Definitions

- System Security Engineering is not JUST:
 - Cybersecurity
 - Anti-Tamper
 - Supply chain protection
 - System security engineering
 - Anti-terrorism / force protection
 - Operations security

Outline

- Introduction
- What IS System Security Engineering?
- **Why Have System Security Engineering?**
- Why plan for System Security Engineering?
- So What?
- Conclusion

U. S. Government Interest Items

Theft of F-35 design data is helping U.S. adversaries:

Pentagon

- Cyber Threat

U.S. Lawmakers Say NASA May Have Given DOD Secrets To China

- Sensitive information presented at public venues

VA laptop goes missing

- Was PII compromised?

U.S. Watchdog Warns That FAA Pilot, Aircraft Information Is At Risk

- Potential to hack registry databases

C-130J Contractor Identifies Counterfeit Parts in Display Units

- Tipped Off by Increased Number of Circuit Board Failures

Espionage and Sabotage

- System Security Engineering is all about keeping the “good stuff” in and the “bad stuff” out!
 - Determine the “good stuff” and figure out how to protect it
 - Determining what are the most important components and figure out how to prevent “bad stuff” from getting in

Outline

- Introduction
- What IS System Security Engineering?
- Why Have System Security Engineering?
- **Why plan for System Security Engineering?**
- So What?
- Conclusion

Current DoD Thinking

- System Security Engineering includes:
 - Cybersecurity
 - Anti-Tamper
 - Supply chain protection
 - System security engineering
 - Anti-terrorism / force protection
 - Operations security

Current DoD Thinking

- System Security Engineering includes:
 - Communications security
 - Physical security
 - Personnel security
 - Industrial security
 - Transportation security

Current DoD Thinking

- System Security Engineering planning:
 - Integrates
 - Balances
 - Defines

Outline

- Introduction
- What IS System Security Engineering?
- Why Have System Security Engineering?
- Why plan for System Security Engineering?
- **So What?**
- Conclusion

So What Does This Mean to Me?

- I don't work in military-related industries.
I work in:
 - Energy
 - SCADA system data (cybersecurity)
 - SCADA system servers (supply chain protection)
 - Power plants and distribution yards (physical security)
 - System Operators (personnel security)
 - Nuclear fuel (transportation security, operations security)
 - Oil and gas pipelines (physical security)
 - Pipeline remote controls (cyber, supply chain protection)

So What Does This Mean to Me?

- I don't work in military-related industries.
I work in:
 - Commercial Aerospace
 - Aircraft and spacecraft avionics (cybersecurity, supply chain protection)
 - National Airspace System (cybersecurity, supply chain protection, personnel security)
 - Space tracking and communications networks (cybersecurity, supply chain protection, personnel security, physical security)

So What Does This Mean to Me?

- I don't work in military-related industries. I work in:
 - Environmental Management
 - Operations security
 - Transportation
 - Rapid transit signaling (cyber, supply chain protection)
 - Rail rights-of-way (physical security)
 - Air traffic control/management (cyber, supply chain protection)
 - Unmanned vehicle data link (cyber)

So What Does This Mean to Me?

- I don't work in military-related industries.
I work in:
 - Health
 - PHI (cyber)
 - Medical hardware (supply chain protection)
 - Finance
 - PII (cyber)
 - Servers (supply chain protection)

Outline

- Introduction
- What IS System Security Engineering?
- Why Have System Security Engineering?
- Why plan for System Security Engineering?
- So What?
- **Conclusion**

Take-aways

- Planning for System Security Engineering is a must-do!
 - Define requirements
 - Facilitate trade studies
 - Engage in system decomposition
 - Engage in integration and test
- All to protect the “good stuff” and keep out the “bad stuff”!

Thank You!

Thanks for your attention and participation