Building Better Systems Security Engineers

Benjamin Winter & Jason Puckett

27th Annual Systems & Mission Engineering Conference

29 October 2024

9/27/2024

Who We Are

- **Benjamin Winter**
  - Associate Director, Systems Engineering
  - Cybersecurity Lead Systems Engineer
  - M.S. Information Security, James Madison University

- **Jason Puckett**
  - Senior Principal Systems Engineer
  - Product Family Cybersecurity Lead Systems Engineer
  - M.S. Applied Mathematics, University Minnesota, Duluth

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Outline

- What is Systems Security Engineering (SSE)
- Product Landscape
- SSE Failures
- Where Are the Qualified SSEs
- Ideal Skillset of an SSE
- Cybersecurity Education
- Professional Training
- Solutions

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

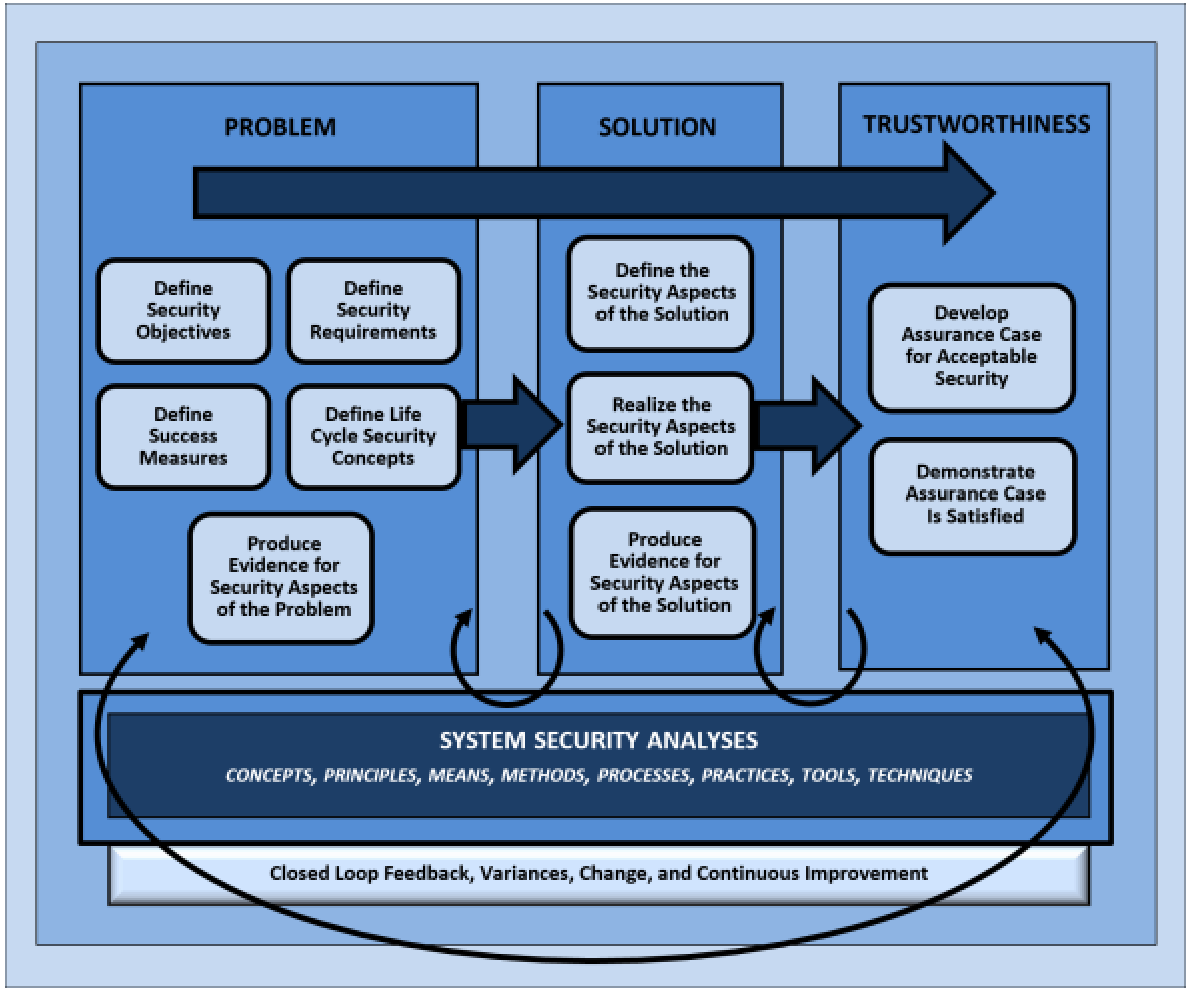
What is Systems Security Engineering

NIST SP 800-161v1r1

Developing trustworthy systems for contested operational environments

Adopt an engineering-based approach that addresses the principles of trustworthy secure design and apply those principles throughout the system life cycle

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE


PROBLEM
SOLUTION
TRUSTWORTHINESS
Define Security Objectives
Define Security Requirements
Define Success Measures
Define Life Cycle Security Concepts
Produce Evidence for Security Aspects of the Problem
Define the Security Aspects of the Solution
Realize the Security Aspects of the Solution
Produce Evidence for Security Aspects of the Solution
Develop Assurance Case for Acceptable Security
Demonstrate Assurance Case Is Satisfied
SYSTEM SECURITY ANALYSES
CONCEPTS, PRINCIPLES, MEANS, METHODS, PROCESSES, PRACTICES, TOOLS, TECHNIQUES
Closed Loop Feedback, Variances, Change, and Continuous Improvement

Source: Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1.

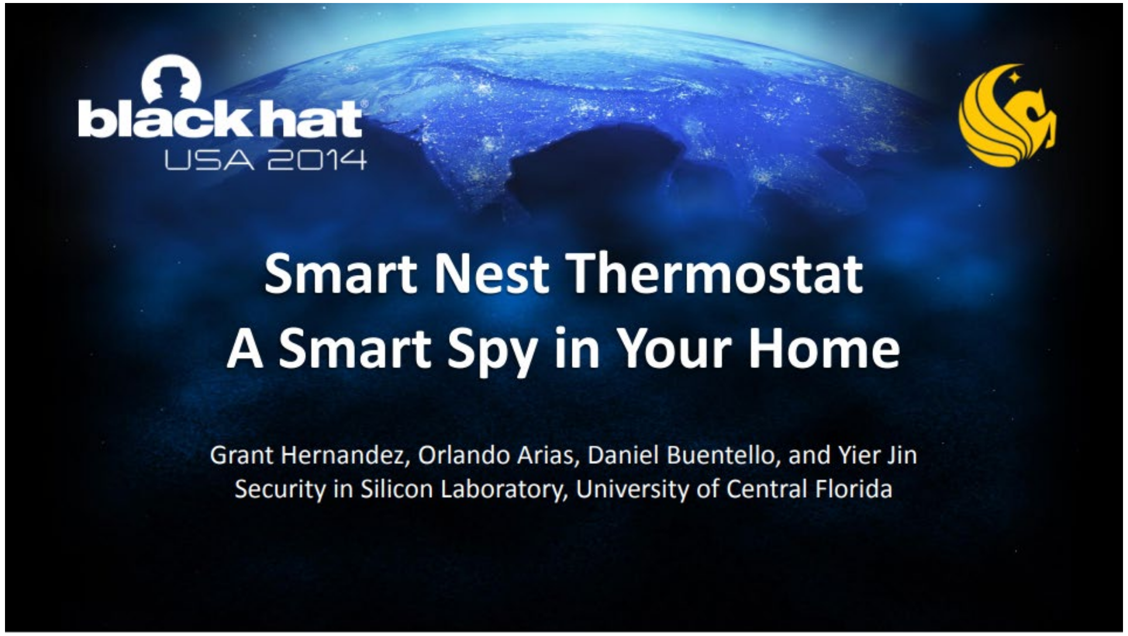
Product Landscape

Every product needs Systems Security Engineering

images: Flaticon.com

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Systems Security Engineering Failures



blackhat
USA 2014

Smart Nest Thermostat
A Smart Spy in Your Home

Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin
Security in Silicon Laboratory, University of Central Florida

Source: https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home.pdf

- **Early Nest Thermostat Flaws**
  - Client on botnet
  - Backdoor to network
  - Spy on network

- **Google Commitment to Security**

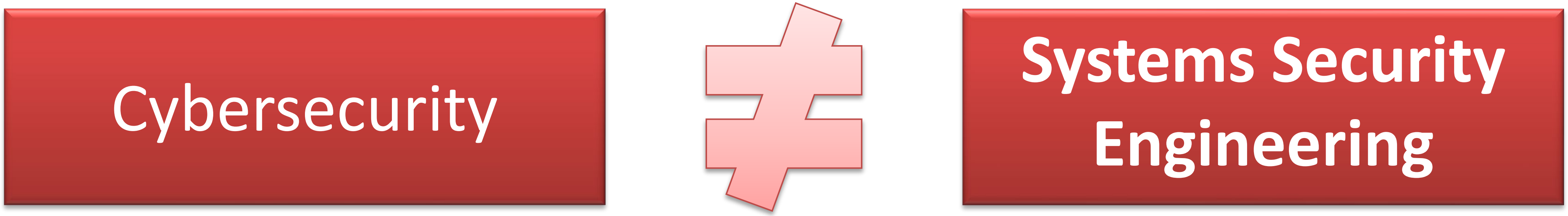
  We protect our users with industry-leading security, responsible data practices, and easy-to-use privacy controls

images: Flaticon.com

Where are you sourcing your products today and to what level of security are they designed?

The Challenge

Cybersecurity without Engineering does not provide an adequate background in Systems Security Engineering



Cybersecurity ≠ Systems Security Engineering

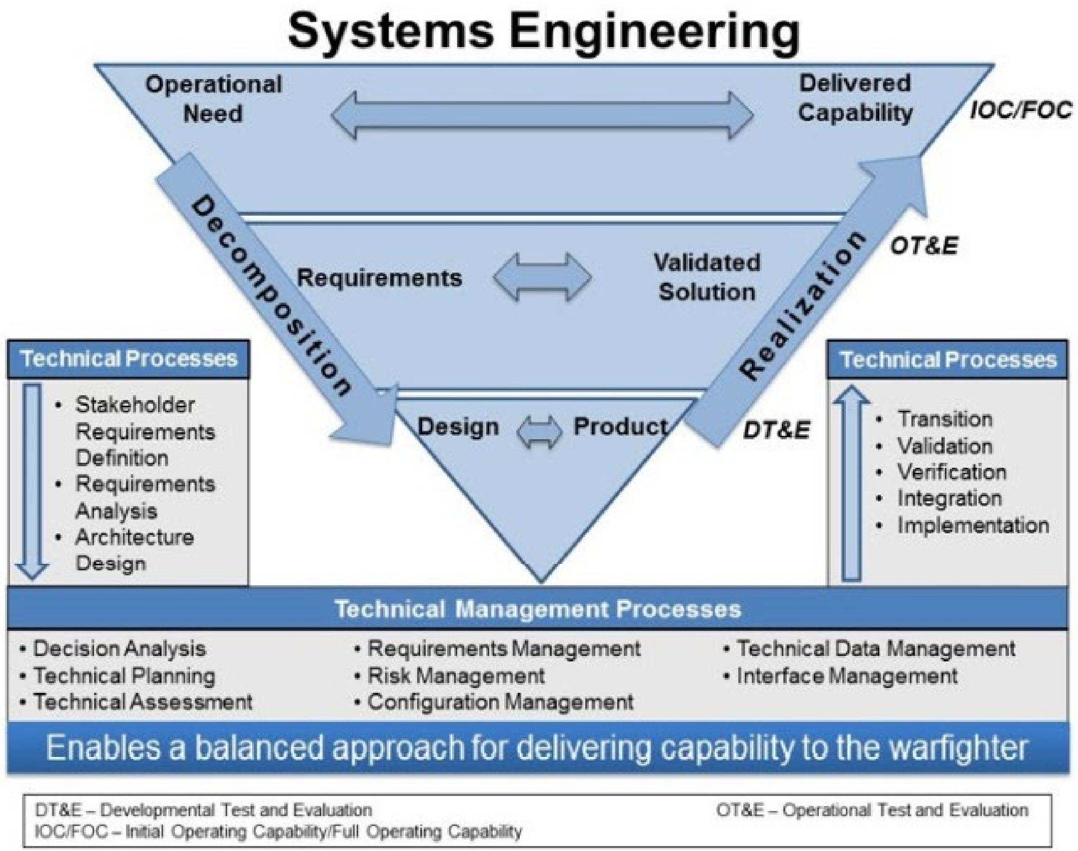
What makes up the ideal SSE skillset?

Who is guiding aspiring cybersecurity candidates into Systems Security Engineering?

Ideal Skillset of an SSE

- **Engineering mindset with skills across multiple disciplines**
  - computer science, software engineering, information technology, and cybersecurity.

- **Identifying both security risk and opportunity for improvement when it is easiest**



Systems Engineering

Operational Need ⟷ Delivered Capability

IOC/FOC

Requirements ⟷ Validated Solution

OT&E

Design ⟷ Product

DT&E

Decomposition

Realization

Technical Processes
- Stakeholder Requirements Definition
- Requirements Analysis
- Architecture Design

Technical Processes
- Transition
- Validation
- Verification
- Integration
- Implementation

Technical Management Processes
- Decision Analysis
- Technical Planning
- Technical Assessment
- Requirements Management
- Risk Management
- Configuration Management
- Technical Data Management
- Interface Management

Enables a balanced approach for delivering capability to the warfighter

DT&E – Developmental Test and Evaluation
IOC/FOC – Initial Operating Capability/Full Operating Capability
OT&E – Operational Test and Evaluation

“Systems Engineering Guidebook”, Office of the Deputy Director for Engineering Office of the Under Secretary of Defense for Research and Engineering, February 2022. https://ac.cto.mil/wp-content/uploads/2022/02/Systems-Eng-Guidebook_Feb2022-Cleared-slp.pdf

Where Are The Qualified Systems Security Engineers

- **Cybersecurity career interest is exploding**
  - As of August 2022 there were over 700,000 open roles in cybersecurity in the U.S.
  - Cybersecurity jobs are expected to grow 32% from 2022 to 2032
  - College enrollment in cybersecurity programs has increased 19% from 2016 to 2021
  - Many high schools incorporate cybersecurity as part of their STEM programs
  - Many adults are turning to cybersecurity as a midlife career change

How many bring an engineering mindset?

Hellmann, K. (2023, Sept 22). See Yourself in Cybersecurity. U.S. Department of Labor Blog. Available https://blog.dol.gov/2023/09/22/see-yourself-in-cybersecurity
Rowles, E. (2023, Sept 14). When Bad News Is Good News: Cyber Breaches Drive Demand For Cybersecurity Programs. Gray DI [Online]. Available https://www.graydi.us/blog/graydata/when-bad-news-is-good-news-cyber-breaches-drive-demand-for-cybersecurity-programs

Cybersecurity Education -
A comparison of two top tier cybersecurity programs

- **University A**
  - Top tier cyber program
  - Focus: cyber policy, attacks, risk management, incident response
  - Ideal for cyber analysts, corporate IT, CISOs
- **Vast majority of colleges follow this model**
- **Does not adequately educate in SSE principles**

- **University B**
  - Top tier cyber program
  - Focus: computer science and engineering with cybersecurity
  - Ideal for SSE
  - M.S. Cyber-Physical Systems is specifically SSE focused
- **Limited number of colleges follow this model**
- **Provides a solid SSE foundation**

Double majors and internships can help bridge the gap to SSE

Are Professional Certifications Helpful?

- **Short comings**
  - Not focused on the system as a whole
  - Domain specific knowledge (servers, networks)
  - Broad but not deep
- **Exceptions**
  - ISSAP – Information Systems Security Architecture Professional
  - ISSEP – Information Systems Security Engineering Professional
- **Can fill gaps but won’t create a “complete” SSE**

CompTIA Security+

CompTIA Linux+

ISSAP – Information Systems Security Architecture Professional

ISSEP – Information Systems Security Engineering Professional

Solutions for consideration

- **Rotations**
  - Rotational programs within organizations enables engineers to gain exposure to diverse facets of SSE

- **In House Training**
  - Training can be developed to bridge the gap for individuals who may possess some portion of the ideal skill set skill but not all

- **R&D Initiatives**
  - Delve deeper into cutting-edge technologies and methodologies while also walking the engineering lifecycle

- **Influence Education**
  - Employers have long partnered with universities to shape programs and then steered employees take those programs

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Examples

- **Rotations**
  - Rotational programs within organizations enables engineers to gain exposure to diverse facets of SSE

- **In House Training**
  - Training can be developed to bridge the gap for individuals who may possess some portion of the ideal skill set skill but not all

- **R&D Initiatives**
  - Delve deeper into cutting-edge technologies and methodologies while also walking the engineering lifecycle

- Formal rotational program help employees gain experience across functional areas
- “Informal” rotation where the SSE team may help cross-train engineers from other disciplines
- Supported with mentoring

Examples

NDIA

- **Rotations**
  - Rotational programs within organizations enables engineers to gain exposure to diverse facets of SSE

- **In House Training**
  - Training can be developed to bridge the gap for individuals who may possess some portion of the ideal skill set skill but not all

- In-house developed training that all SSEs are encouraged to take
  - Cybersecurity Bootcamp
  - Embedded Systems Security
- Tuition reimbursement program to help employees achieve the higher-level SSE certifications like ISC2's ISSAP and ISSEP certifications

Influence Education
- Employers have long partnered with universities to shape programs and then steered employees take those programs

Examples

- **Rotations**
  - Rotational programs within organizations enables enginee to gain exposure to diverse facets of SSE

- Initiatives have included:
  - Building virtual machines (VMs)
  - Developing Security Tools/Dashboards
  - Implementing and automating System Technical Implementation Guides (STIGs)

- **R&D Initiatives**
  - Delve deeper into cutting-edge technologies and methodologies while also walking the engineering lifecycle

- **Influence Education**
  - Employers have long partnered with universities to shape programs and then steered employees take those programs

Examples

- Partner with colleges and universities to shape programs through participation in industry advisory committees
- Recruit and train students through summer internships and COOP assignments
- Partner with students providing mentorship in their engineering capstone project

– Delve deeper into cu e technologies and methodo while also walking the engineering lifecycle

- **In House Training**
  - Training can be developed to bridge the gap for individuals who may possess some portion of the ideal skill set skill but not all

- **Influence Education**
  - Employers have long partnered with universities to shape programs and then steered employees take those programs

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Recruiting SSEs

- **Interviewing Candidates**
  - Focus on engineering experience then security experience
  - Early career vs. Late career

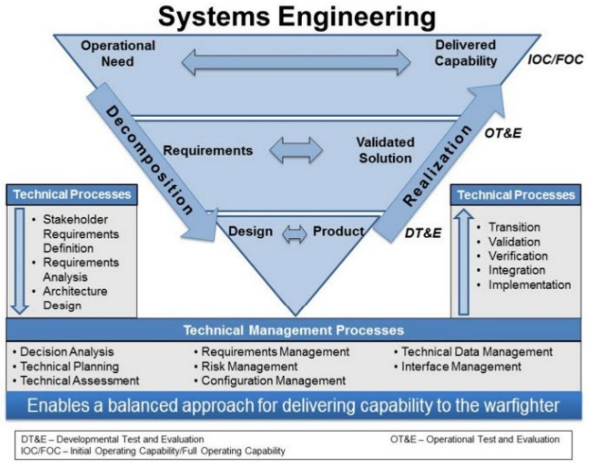
- **Existing staff**
  - R&D
    - Virtual machines (VMs), Security Tools/Dashboards, and implementing System Technical Implementation Guides (STIGs)
  - Rotation and mentoring
    - Allow “incomplete” SSE to join a team and be mentored in areas of need

Raytheon Company - Approved for Public Disclosure
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Conclusion

- **Robust cybersecurity design requires empowered and knowledgeable SSEs across the entire system development life cycle**

- **A strategic view of bolstering SSE support with well-rounded engineers can be realized, ensuring resilience and integrity in the face of evolving cyber threats**


Systems Engineering
Operational Need
Delivered Capability
IOC/FOC
Decomposition
Realization
OT&E
Requirements
Validated Solution
Design
Product
DT&E
Technical Processes
• Stakeholder Requirements Definition
• Requirements Analysis
• Architecture Design
Technical Processes
• Transition
• Validation
• Verification
• Integration
• Implementation
Technical Management Processes
• Decision Analysis
• Technical Planning
• Technical Assessment
• Requirements Management
• Risk Management
• Configuration Management
• Technical Data Management
• Interface Management
Enables a balanced approach for delivering capability to the warfighter
DT&E – Developmental Test and Evaluation
IOC/FOC – Initial Operating Capability/Full Operating Capability
OT&E – Operational Test and Evaluation