Boeing Defense and Security

Strike Surveillance and Mobility

The Value of Using Systems Engineering to Sharpen the Spear against the Cyber Threat

Richard Massey Technical Fellow CISSP®

APPROVED FOR RELEASE: Request for Release of Information, number 18-00520-BDS

Cybersecurity Engineering Architecture and Design

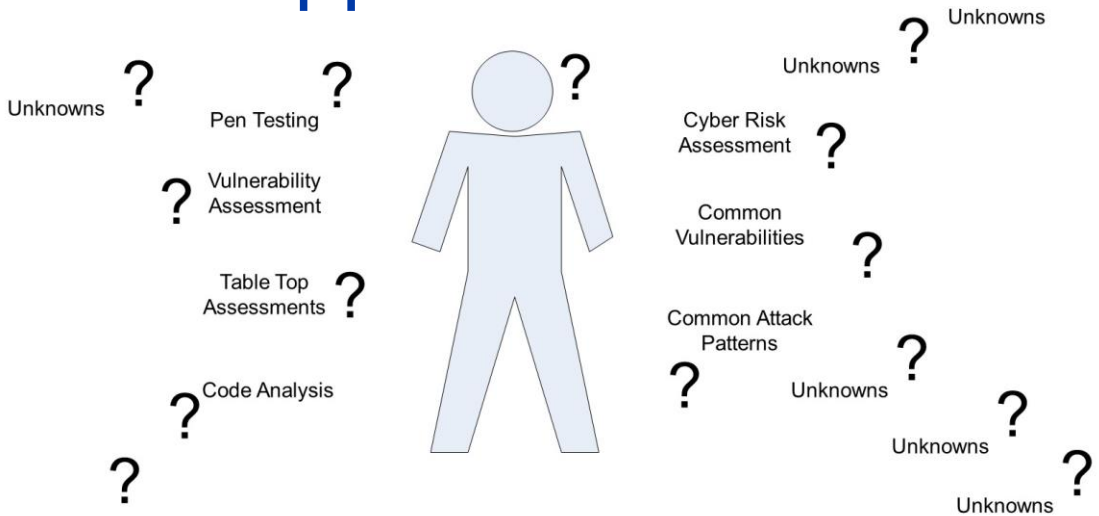
- Cybersecurity can and should be considered at all layers of a system and operations of a system throughout its life cycle
- As such architecture, design and implementation (hardware and software) changes can have a positive or negative effect on the Cybersecurity posture and risk of our delivered products
- We should consider the security objectives in the development and maintenance of an architecture
- How best can we integrate this into our systems processes?

DODi 5000.2 E14: 3.b. Design for Cyber Threat Environments.

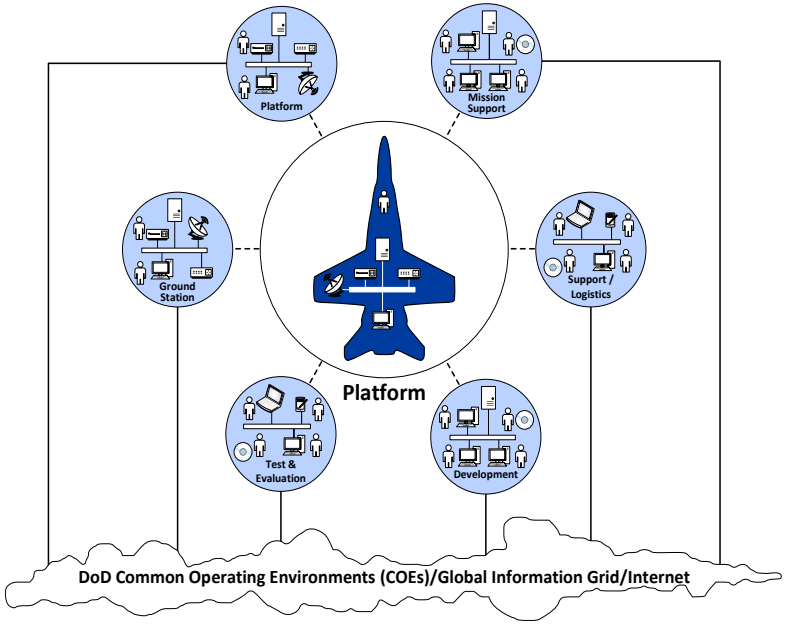
Systems Security Engineering and Architecture Definition

- Risk Management Framework TASK 2-2: Select the security controls for the information system and document the controls in the security plan.
  - Primary Responsibility: Information Security Architect; Information System Owner.
  - Supporting Roles: Authorizing Official or Designated Representative; Information Owner/Steward; Information System Security Officer; Information System Security Engineer." (NIST 800-37)
- The RMF Process (800-37) does little to recognize the architecture, except as embedded in organizational control PL-8 to integrate security architecture with information architecture and an assurance requirement (SA-17). These do not drive architecture solutions to meet risks
- System Security Engineering (IAW NIST SP-800-160 (Section 3.4.4)):
  - Informs selection of one or more alternatives thru the analysis of security views of each architecture
  - Vulnerability and susceptibility to disruptions, hazards, and threats across all *architecture views*.
  - Analysis informs risk assessments, risk treatment, and engineering decision making and trades.
  - Synchronize *System Requirements Definition* and *Design Definition* processes.
  - Iterates with the *Business and Mission Analysis* and *System Requirements Definition* processes
  - Achieve a negotiated understanding of the particular security concerns and associated characteristics of the problem to be solved and the proposed solution to the problem.
  - Emergent system security properties and behavior begin to form as a result of system architecture definition.

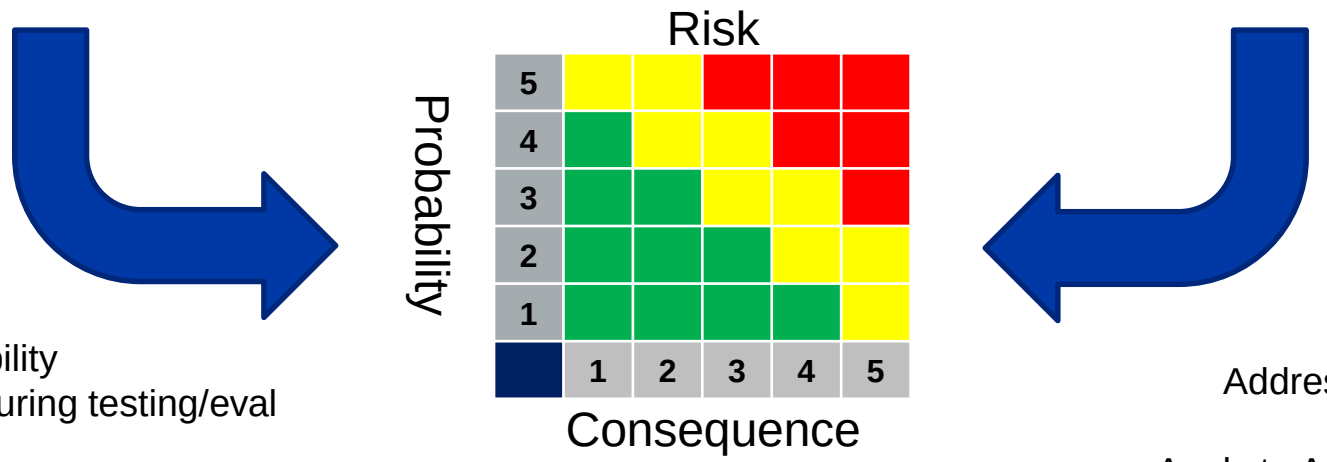
Systems Approach



Susceptibilities, Weakness and Issues



Attack Surface

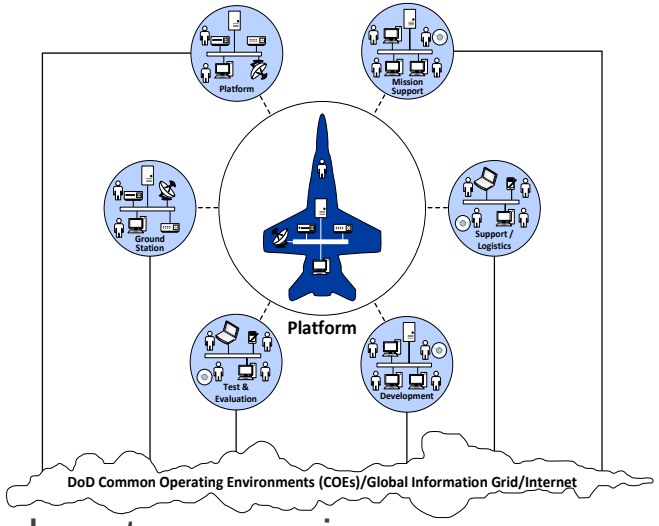


Knowns
Limited Intel of adversary capability
Limited to issues and findings during testing/eval

Unknowns:
Adversary intent / future capability
Address unknowns by understanding system
Define weakness / strengths
Apply to Attack Patterns –> Operational / System

Probability== (Attack Surface with a susceptibility)
Consequence == f(loss of Aircraft, loss of mission capability (full, partial, none) etc)

Resources and Body of Knowledge Sources



Understanding Impact, Threat Vectors

- System SMEs that understand the systems and its dependencies
- Users that understand the operational context
- Attack Patterns/ Threat Vectors
  - MITRE CAPECs, CWEs
  - Body of Knowledge / Taxonomy based on the SMEs, users and security minded systems engineers
  - Safety Criticality Analysis
  - Mission Function Criticality Analysis
  - Functional System Architecture
  - Operational CONOPs
- Understanding of Likelihood
  - Known Intel
  - Subjective Assessment based on relative known capabilities
  - Objective Criteria
    - Based on an understanding of risk factors against the efforts required by an adversary

Measure risk against known criteria about the system through out its life-cycle

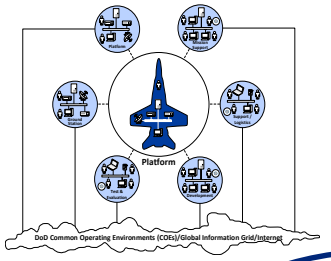
Objective Risk Determination

Risk Factors

System and operational criteria which evaluate the attack surface

Cybersecurity Risk

Attack Surface Characteristics



Probability Standard Criteria

$f\,(Threat + Sus)$

Consequence Standard Criteria

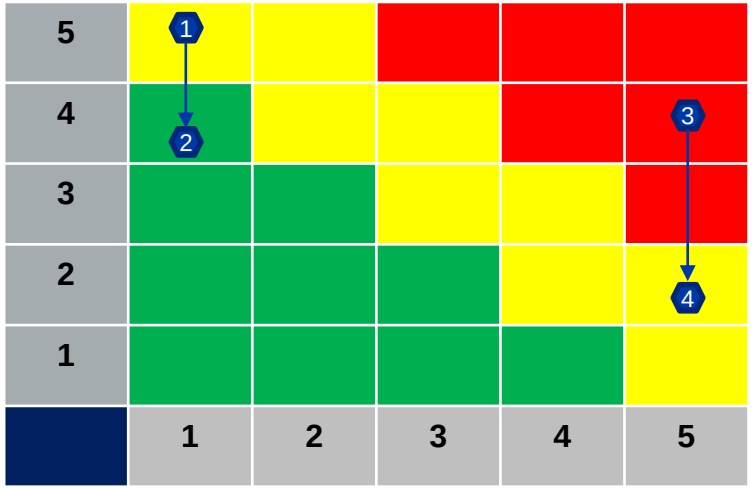
$f\,(Mission\ Eff)$

Measureable risk against mission and capabilities based on an understanding of the threat surface applied to objective standards

Value and Cost of Ownership

Understand What is Important/Security Challenges

- Normalize Issues, findings, perceived weaknesses into risk
- Prioritize based on assessed risk against mission objectives
- Trade architecture, design, implementation for cost vs benefit
- Trace to Architecture/Design/Implementation
- Incorporate into Systems Requirements



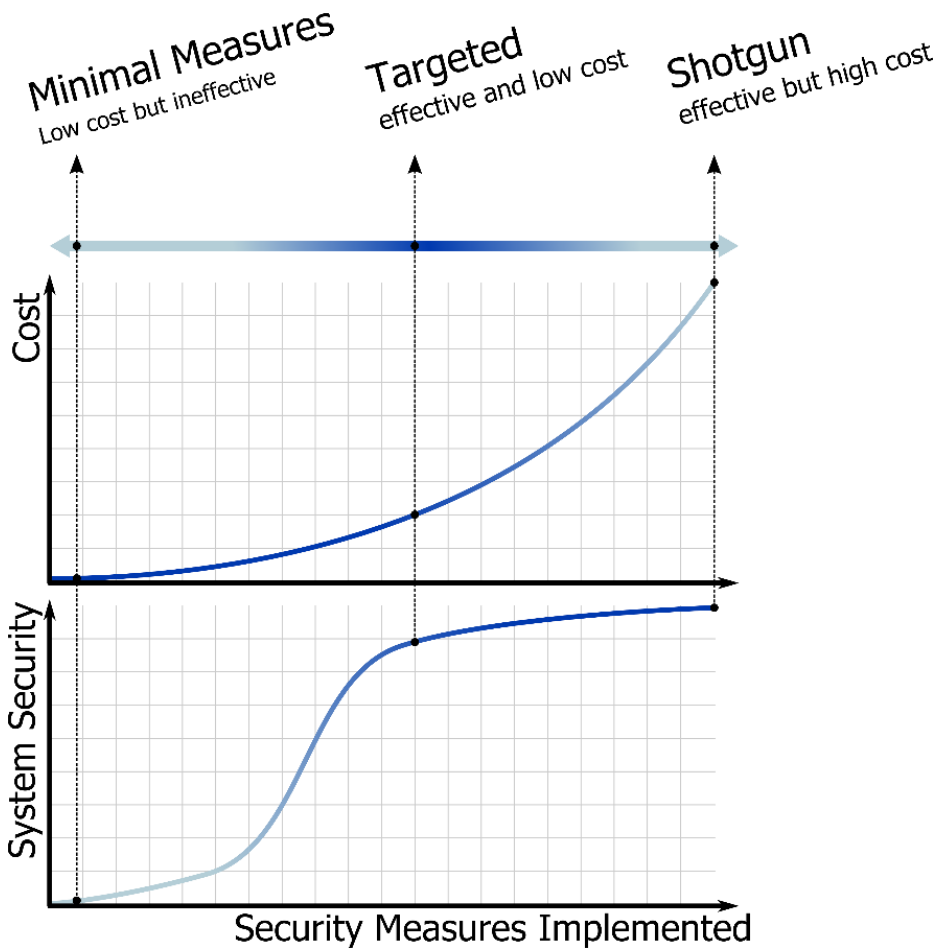
1->2 $$$$

3->4 $$

Cannot afford to apply all best practices or address all issues and findings

Why Perform Threat Assessment?

- Threat Assessments systematically identify and evaluate threats that are most likely to affect the platform's mission effectivenes
  - Informed with a solid understanding of the platform architecture, how it's used and who has access.
  - Address threats with appropriate countermeasures in a logical order, starting with the threats that present the greatest risk to the platform.
- Avoid applying security in a "shotgun" approach.
  - Applying security indiscriminately adds unnecessary cost to the platform.
  - Knowing the threats that are most applicable to the platform, enables the application of only those security features that protect against these applicable threats.



SSE

Level	SSE Analysis/Activity Ex	Artifacts Ex
Mission	Ops Analysis System Theory Analysis	Security Objectives Threats Acceptable Risk
System of System	Architecture Trades Access Controls Information Flow Needs Risk Assessment	Attack Surface Security Functional Analysis Information Flow System Requirements
Design	Design Trades Architecture Validation Security Policy	Implement Security Policy Design Requirements Verification
Implementation	Trusted Development Component Evaluation Code Inspection/Analysis Pen Testing	Component Certifications Code Weakeness/Vulnerabilities Design Issues Security Proofs

Assurance Arguments

- NIST 800-160 SSE (assurance via SSE)
  - Integration of Security Controls into the SSE effort focused on Risk
  - Develop assurance arguments that the system is secure (2.4)
    - SWA Risk mitigated, Supply Chain Risk mitigated, Specific Threats Mitigated
      - vs
    - SWA Plan, Supply Chain Risk Mitigation Plan, SCTM & SSP Package
- Assurance Arguments are matured to address the primary security objectives for the mission
  - Keeps the conversation during trades in focus
  - Helps balance and inform risk
  - Maturation will lead to better body of evidence to support informed risk decisions

Accomplishments & Results

- Program Acceptance of the Benefits to Change/Add Security Controls for Segregation of Software Development Environment
- Validated Trades on Security Objectives for a Mission Computer Redesign
- Identified Supply Chain Risk and Identifying Effective Opportunities to Product Work Flow
- Platform Risk Assessments
  - Measureable Risks to improve System Integrity

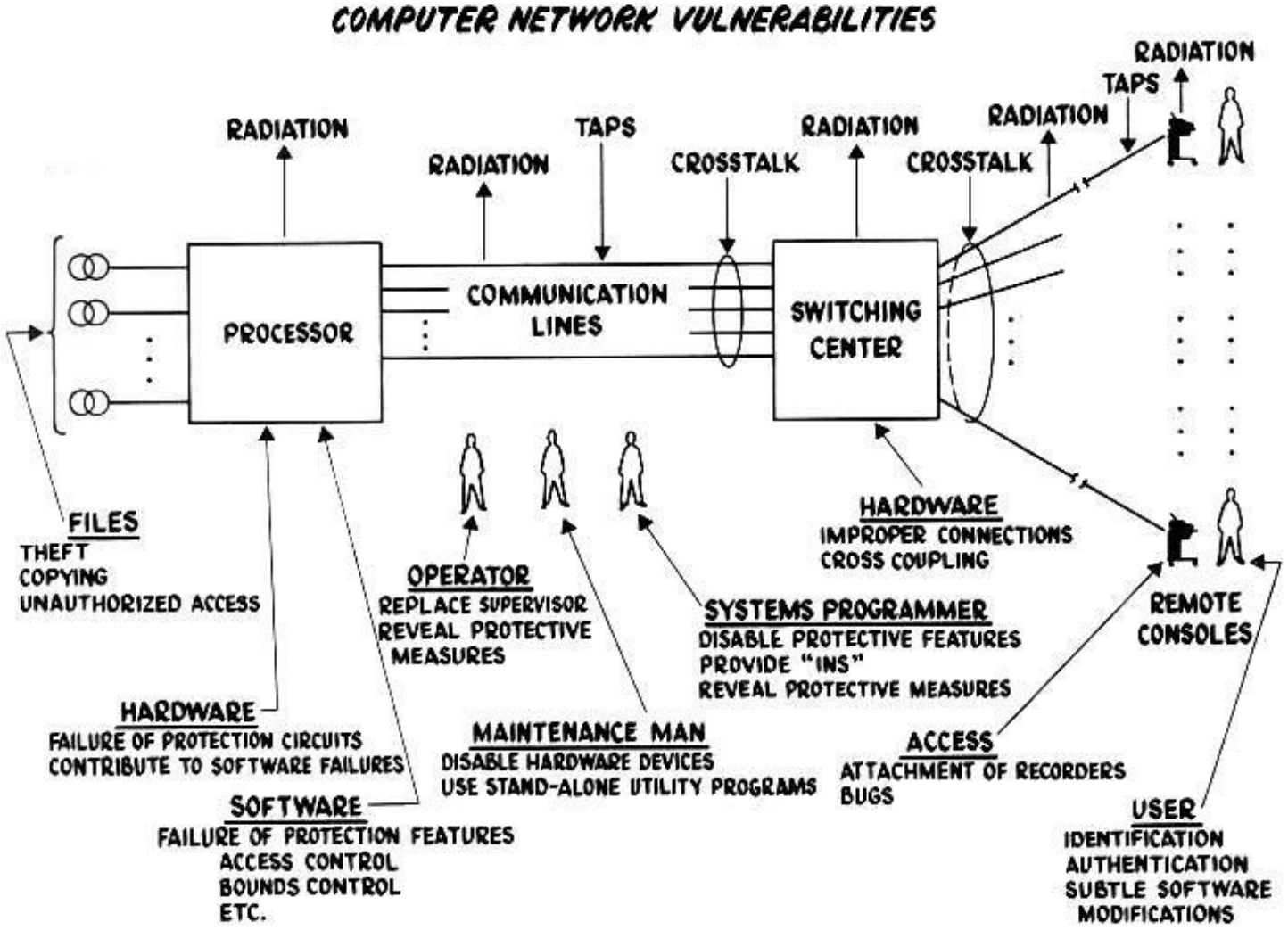
Skills Required

- Systems thinking
- Present engineers with an objective they will provide a solution
- Systems Engineering
- Software Engineering/Electrical/Embedded Engineering

- Successes
  - Threat Assessments effective tool to express security concerns to a solution
  - Attack Patterns mapped to countermeasures help tailor security controls
  - Mix of seasoned embedded engineers, senior security engineers and new recruits

FYE: A Look Back in time

Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1 circa 1969



Focus was on confidentiality

Today we are ALSO concerned about the disruption of the computer systems that operate our weapon systems.

The attack surface begins with this view, it has greatly expanded into the development of the system

RAND CORP APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED