Transitioning to Engineering-based Cybersecurity
Applying Design Principles to Develop Trustworthy Secure Systems
Complexity

Millions, Billions, and Trillions of Everything
The Current Landscape...

Little or no understanding of what’s in the “black box.”
Today’s systems...

• Present a uniform attack surface
• Rely on a single-dimension protection strategy based on penetration resistance
• Are susceptible to destructive cyber-attacks
“Security is embedded in systems. Rather than two engineering groups designing two systems, one intended to protect the other, systems engineering specifies and designs a single system with security embedded in the system and its components.”

-- Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundational Concepts, 2021 INCOSE International Symposium
The Ecosystem

Framework for Securing Organizational Systems and Assets

Mission/Business - Processes - Technology - Communications - Production

BizOps - DevOps - Supply Chain

Systems Security Engineering

Transparency - Traceability - Trust - Assurance - Integrity - Resilience - Reliability
Multidimensional Protection Strategy

- Penetration-resistant architecture
- Damage-limiting operations
- Designs to achieve trustworthy secure systems

What is a System?

• An arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. Systems can be physical or conceptual, or a combination of both. [ISO/IEEE 15288] [INCOSE]
System of Systems

ENVIRONMENT OF OPERATION

Enabling System

System Element

System Element

Enabling System

SYSTEM OF INTEREST

Interoperating System

Interoperating System

Interoperating System

NON-OPERATIONAL ENVIRONMENT
Security Engineering Focuses on Asset Loss
Requirements Engineering

- Stakeholder Security Requirements
- System Security Requirements
- Asset Protection Needs
- Mission and Business Needs
- Life Cycle Concepts
- Constraints
- Risk Tolerance and Loss

Validation: Was the correct system built?

Verification: Was the system built correctly?
Characteristics

- Disciplined and structured development process
- Integrates security into the system life cycle
- Applied to all elements in the system stack
- Can be tailored and implemented in agile development processes
- Provides needed traceability of requirements and transparency into development processes leading to greater trust in systems and system elements
No system can provide *absolute* security due to the limits of human certainty, the uncertainty that exists in the life cycle of every system, and the constraints of cost, schedule, performance, feasibility, and practicality.

As such, trade-offs made routinely across contradictory, competing, and conflicting needs and constraints are optimized to achieve *adequate* security, which reflects a decision made by stakeholders.
As secure as reasonably practicable...

The set of identified alternatives resides in this portion of the parameter space.

A: Large increases in system security can be achieved by addressing basic security issues. Little cost, schedule, or technical impact.

B: Basic security issues have been addressed but significant security can still be "bought" without failing to meet cost, schedule, or technical performance requirements.

C: Limit of ASARP regime has been reached but significant increases in security can be "bought" without exceeding tolerable limits of cost, schedule, or technical performance requirements.

D: Limit of achievable security has been met. Increased security cannot be "bought" at any cost.

Adapted from NASA.
An assurance case is a reasoned, auditable artifact that is created to support the contention that a top-level claim is satisfied.

An assurance case contains:

- One or more claims about properties
- Arguments that logically link the evidence and any assumptions
- A body of evidence
- Justification of the choice of a top-level claim and the method of reasoning
Assurance and Rigor

Key Issues for Building Trustworthy Secure Systems
Systems and software engineering — System life cycle processes

“Secure By Design”

Business or mission analysis
  • Stakeholder needs and requirements definition
    • System requirements definition
    • Architecture definition
    • Design definition
    • System analysis
      • Implementation
      • Integration
    • Verification
    • Transition
    • Validation
  • Operation
  • Maintenance
  • Disposal

NIST SP 800-160 Volume 1
Next Generation Development Processes

Credit: Network Intelligence

DevSecOps

AGILE DEVELOPMENT
SECURE ARCHITECTURE
APPLICATION SECURITY
CODE REVIEW/TESTING
SECURE CONFIGURATION
SECURE OPERATIONS

Security Integration

Transparency
Traceability
Visibility
Assurance
Ron Ross
Email: ron.ross@nist.gov
Mobile: (301) 651-5083
Web: http://csrg.nist.gov
Twitter: https://twitter.com/ronrossecure
LinkedIn: https://www.linkedin.com/in/ronrossecure