Securing the Ecosystem

The Need for Multidimensional Protection in the 21st Century

Ron Ross
Complexity

Millions, Billions, and Trillions of Everything
The Ecosystem

Ubiquitous Connectivity Produces Shared Risk
The Ecosystem

*Systems Engineering View*

Critical interdependencies and relationships among internal system elements, systems within enterprise environments, and systems in external environments that affect security solutions.
Systems Security Engineering

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

Courtesy: NIST Special Publication 800-160, Volume 1
Key Concerns

• Architecture
• Assurance
• Behavior
• Cost
• Criticality
• Design
• Effectiveness
• Emergence
• Ergonomics
• Exposure
• Fit-for-purpose
• Human performance
• Life cycle concepts
• Penetration resistance
• Performance

• Privacy
• Protection needs
• Requirements
• Risk
• Security objectives
• Strength of function
• Security performance
• Threat
• Trades
• Training
• Uncertainty
• Vulnerability
• Verification
• Validation
Multidimensional Protection Strategy

- Penetration-resistant architecture
- Damage-limiting operations
- Designs to achieve cyber resiliency and survivability

Stop the incursion...
Limit the damage after the incursion has occurred...
Continue to operate even in a degraded or debilitated state.
The Vision

Framework for Securing the Ecosystem

Mission/Business - Processes - Technology - Communications - Production

BizOps

DevSecOps

Supply Chain Security

Systems Security Engineering

Transparency - Traceability - Trust - Assurance - Integrity - System Resilience
Objectives

• Apply system security engineering concepts to agile, DevOps, and DevSecOps processes to create a “lean SSE” process

• Expand DevSecOps approaches from software components to “systems”

• Incorporate “security” into product and system development, implementation, operation, sustainment, and compliance
Objectives

• Develop a “holistic” risk management approach for systems and organizations
• Use BizOps to drive technology and security solutions
• Implement a multidimensional protection strategy to create cyber resilient systems
• Increase system and component assurance by maximizing life cycle testing and evaluation
• Focus on supply chain security
What are you building?
Ron Ross

Email: ron.ross@nist.gov
Mobile: (301) 651-5083
Web: http://csrc.nist.gov
Twitter: https://twitter.com/ronrossecure
LinkedIn: https://www.linkedin.com/in/ronrossecure