Rethinking Cybersecurity from the Inside Out

An Engineering and Life Cycle-Based Approach for Building Trustworthy Resilient Systems

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

The current landscape.

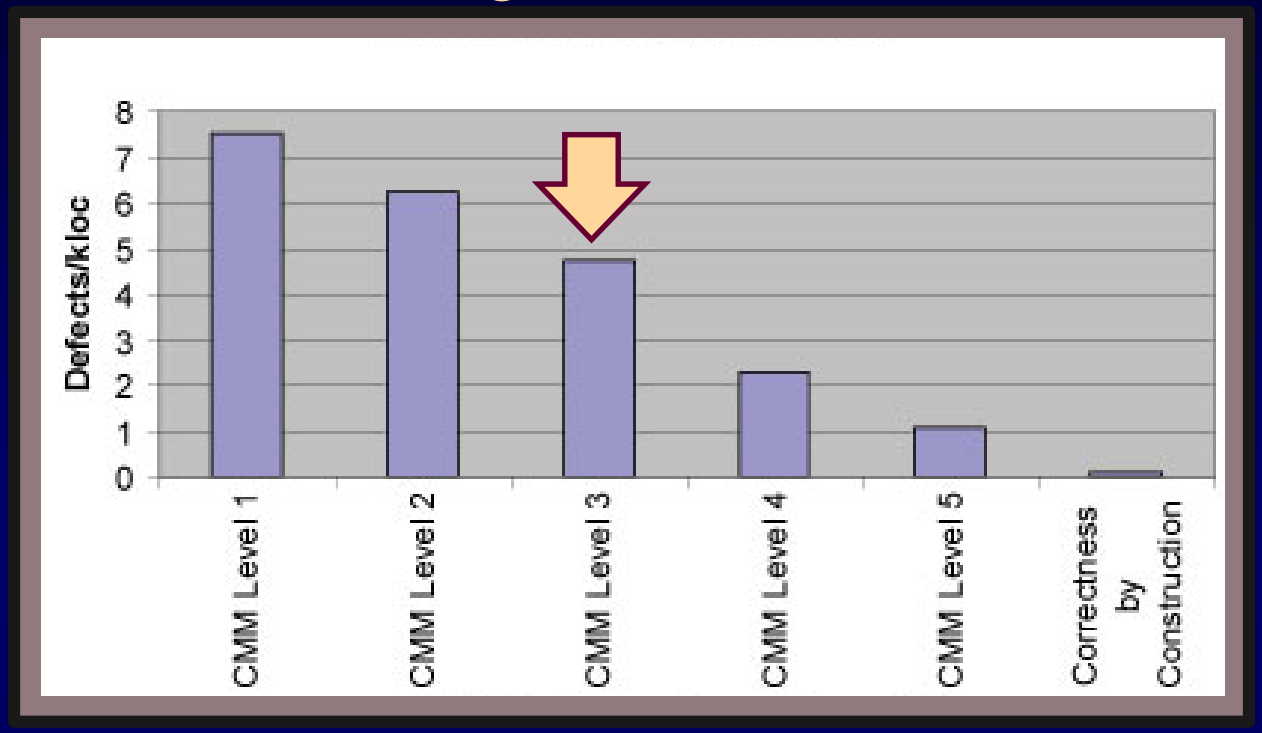
Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

Complexity.

An adversary's most effective weapon in the 21st century.

One organization's IT product *feature* is another organization's *attack surface*.

Estimating Number of Vulnerabilities



Between 1% and 5% of software flaws are security vulnerabilities.

Source: *Software Assessments, Benchmarks, and Best Practices*, C. Jones.

So, 50mLOC / 1kLOC * 4.9 Flaws / 1kLOC ≅ 245,000 flaws
Or approximately 2,400 to 12,200 potential security vulnerabilities.

Source: *Security Vulnerabilities in Software Systems - A Quantitative Perspective*, O.H. Alhazmi.

The n + 1 vulnerabilities problem.

Unconstrained due to increasing attack surface.

When culture clashes with science…

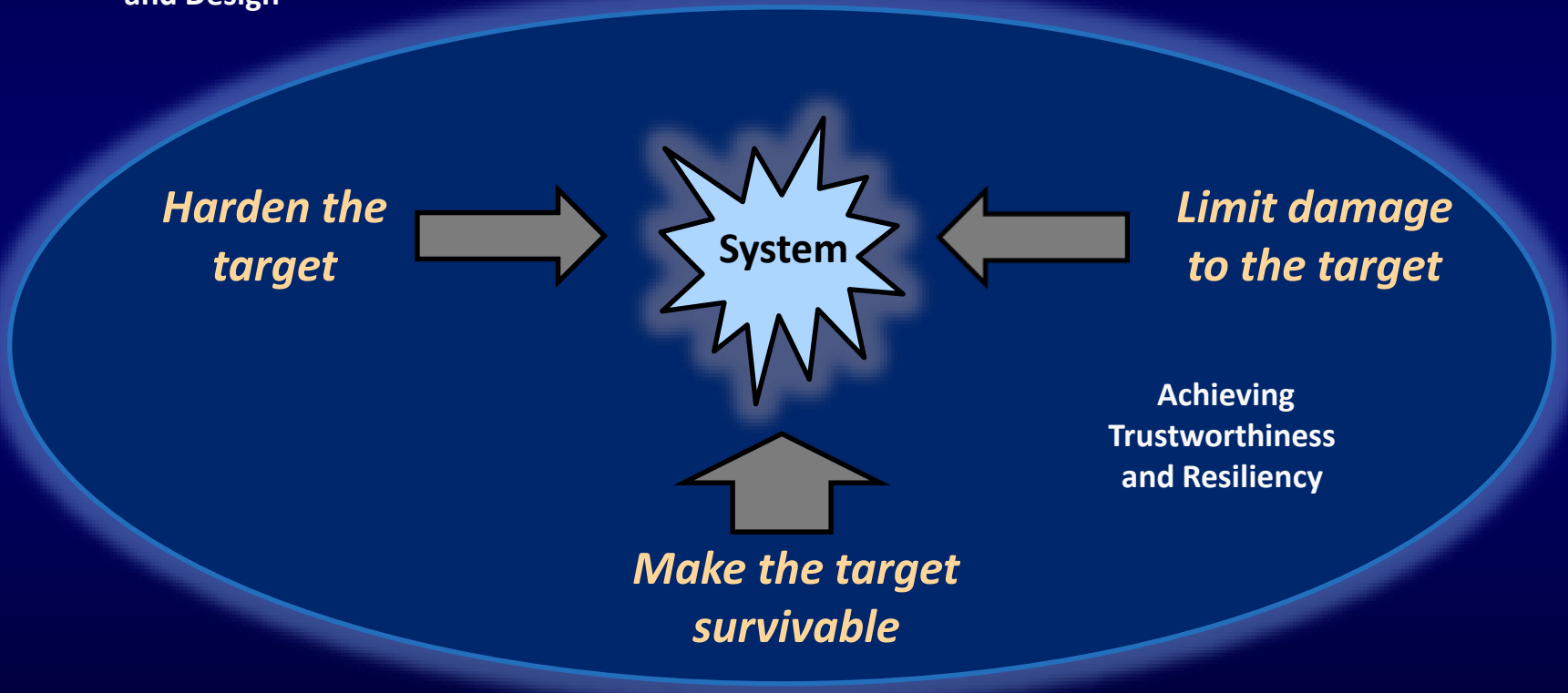
Science wins.

The hard cybersecurity problems are buried below the water line…

In the hardware, software, and firmware.

Security Architecture and Design

Reducing susceptibility to *cyber threats* requires a multidimensional systems engineering approach.



How we do security today…

Bottom up, instead of top down.
Outside in, instead of inside out.
Tactical instead of strategic.

We are managing the trees, but not the forest.

The road ahead.

Institutionalize.

The ultimate objective for security.

Operationalize.

On the Horizon…

NIST Special Publication 800-160

Systems Security Engineering

An Integrated Approach to Building Trustworthy Resilient Systems

Multidisciplinary integration of security best practices.

Command and control of the security space.

Technical Processes

- 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

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

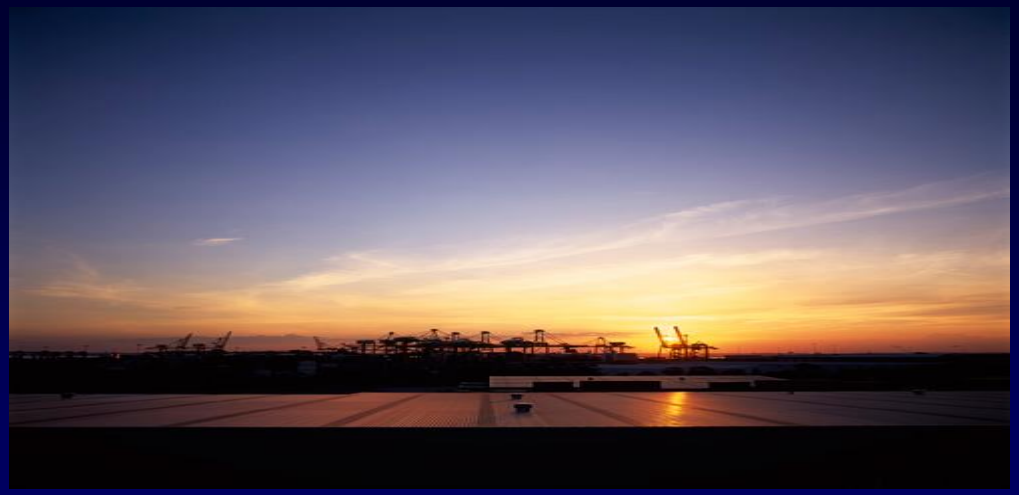
Nontechnical Processes

- Project planning
  - Project assessment and control
    - Decision management
      - Risk management
        - Configuration management
          - Information management
            - Measurement
              - Quality assurance
            - Acquisition and Supply
          - Life cycle model management
        - Infrastructure management
      - Portfolio management
    - Human resource management
  - Quality management
- Knowledge management

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

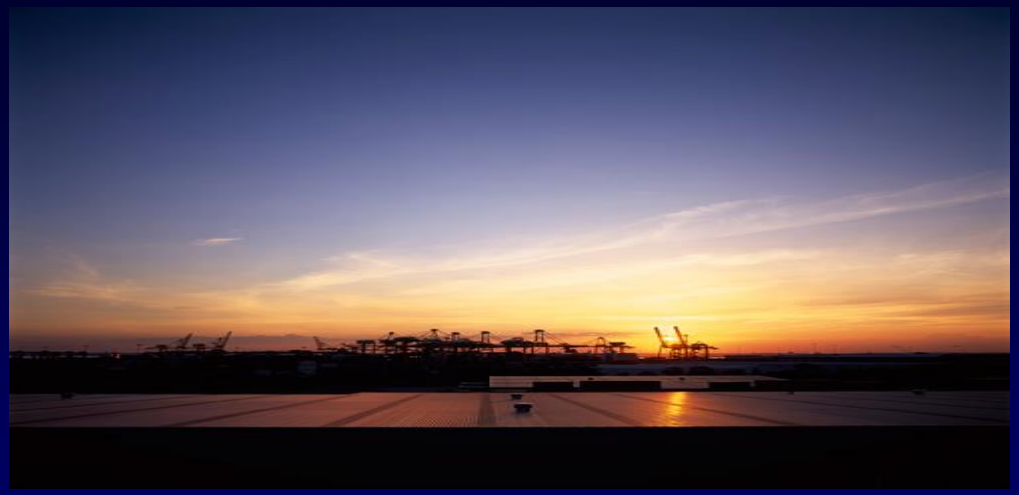
An example.



Human Resource Management Process

Systems Engineering View

"The purpose of the Human Resource Management process is to ensure the organization is provided with necessary human resources and to maintain their competencies, consistent with business needs."



Human Resource Management Process

Systems Security Engineering View

"Systems security engineering, as part of the Human Resource Management process, defines the criteria for qualification, assessment, and ongoing training of individuals that apply scientific, engineering, and information assurance principles to deliver trustworthy and resilient systems that satisfy stakeholder needs and requirements within their established risk tolerance."

-- NIST Special Publication 800-160.

Systems Security Engineering

HR Management Process Outcomes

- Required system security engineering skills are identified.
- System security engineering skills are developed, maintained or enhanced.
- Individuals with system security engineering skills are provided to projects.
- System security engineering knowledge, skills, and information are collected, shared, reused and improved throughout the organization.

Human Resource Management Process

Security-Related Activities and Tasks

- **HR-1 IDENTIFY SYSTEMS SECURITY ENGINEERING SKILLS**

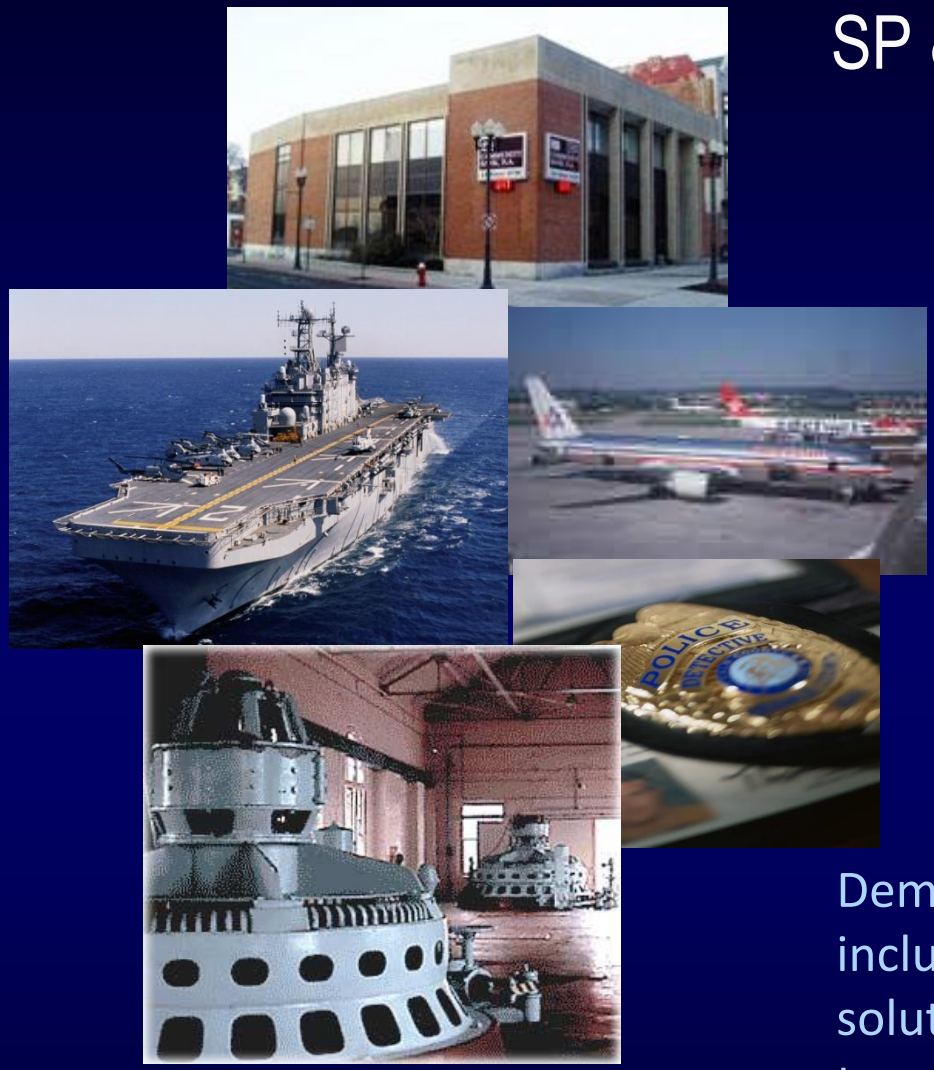
  HR-1.1 Identify systems security engineering skills needed based on current and expected projects.

  Supplemental Guidance: The National Cybersecurity Workforce Framework defines various categories and specialty areas of cybersecurity work including systems security engineering and also identifies common tasks and knowledge, skills, and abilities (KSA's) associated with each specialty area. The framework can be used by government, industry, and academia to describe cybersecurity work and workforces, and related education, training, and professional development. The cybersecurity categories include: securely provision; operate and maintain; protect and defend; investigate; collect and operate; analyze; and oversight and development.

  HR-1.2 Identify systems security engineering skills of organizational personnel and conduct a skills gap analysis.

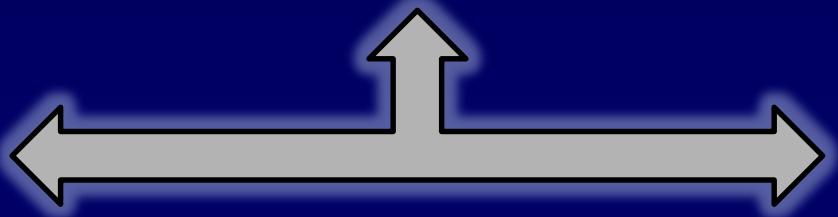
  Supplemental Guidance: Comparing the systems security engineering skills of organizational personnel with the skills needed to support current and expected projects can serve to inform training and education requirements and activities.

  References: National Cybersecurity Workforce Framework: http://csrc.nist.gov/nice/framework. Cybersecurity Framework, *Identify Function*: http://www.nist.gov/cyberframework.



SP 800-160 References Section

Incorporating by reference and aligning, national and international security standards, guidelines, frameworks, and best practices.



30 ISO/IEC/IEEE 15288 Engineering Process Steps

Demonstrating in a transparent and inclusive manner, that multiple security solutions and approaches can be employed to achieve trustworthy resilient systems.

SP 800-160 Structure and Content

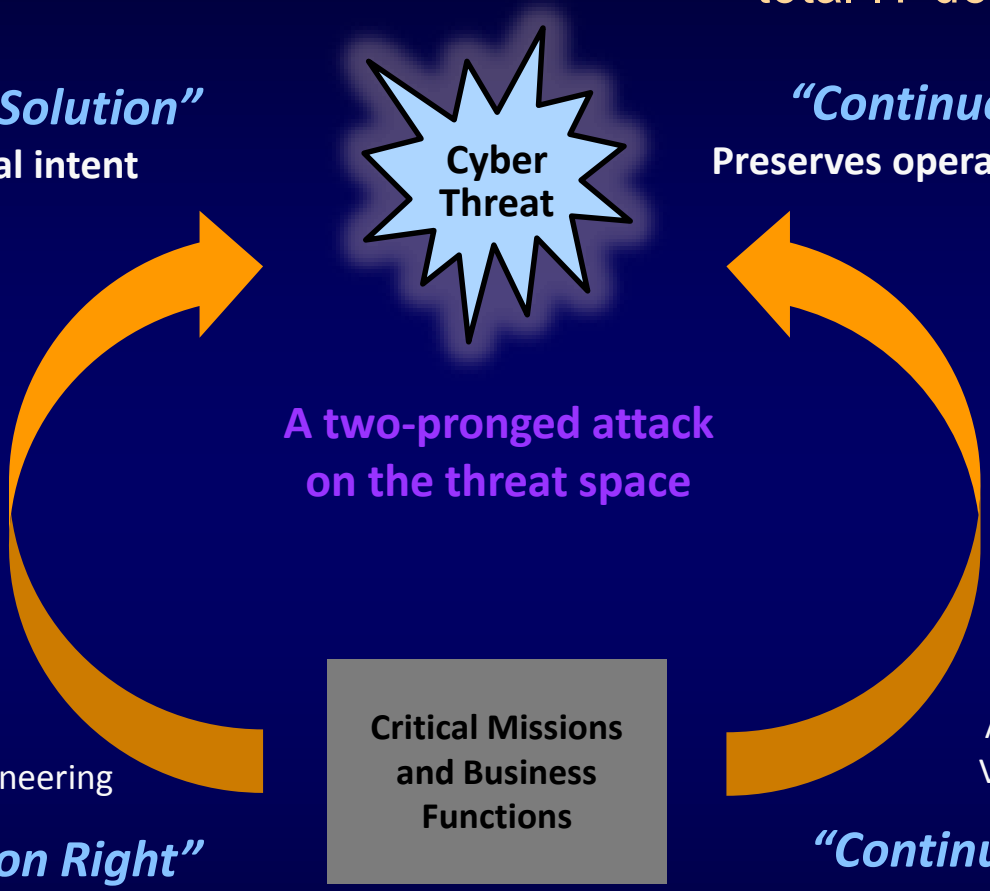
- *Chapter 1 INTRODUCTION*
- *Chapter 2 THE FUNDAMENTALS*
- *Chapter 3 THE PROCESSES*

- *Appendix A REFERENCES*
- *Appendix B GLOSSARY*
- *Appendix C ACRONYMS*
- *Appendix D SUMMARY OF ACTIVITIES AND TASKS*
- *Appendix E ROLES AND RESPONSIBILITIES*
- *Appendix F SECURITY DESIGN PRINCIPLES*
- *Appendix G HARDWARE, SOFTWARE, AND SYSTEM ASSURANCE*
- *Appendix H INFORMATION SECURITY RISK MANAGEMENT*
- *Appendix I SYSTEM AND CYBER RESILIENCY*
- *Appendix J ENTERPRISE ARCHITECTURE INTEGRATION*
- *Appendix K DOD ENGINEERING SUPPLEMENT*

Some final thoughts.

A Winning Strategy

To survive in the digital age of total IT dependence…



"Build the Right Solution"

Meets operational intent

Systems Engineering
Software Assurance
System Life Cycle
Testing/Evaluation
Trustworthiness
Resiliency
Design
Architecture
Acquisition
Secure Coding
Static Code Analysis
Systems Integration
Systems Security Engineering

"Continuously Monitor"

Preserves operational intent over time

Security Configurations
Ongoing Authorization
Separation of Duties
Software Patching
Traffic Analyses
Security State
Asset Inventory
Network Sensors
Incident Response
Threat Assessment
Situational Awareness
Administrative Privileges
Vulnerability Assessment

"Build the Solution Right"

Meets design intent

"Continuously Maintain"

Preserves design intent over time

Foundation of Components, Systems, Services

Be *proactive*, not *reactive* when it comes to protecting your organizational assets from cyber threats.

Security should be a by-product of good design and development practices—integrated throughout the organization.

Government

Academia

Security is a team sport.

Industry


We The People

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

LinkedIn
http://www.linkedin.com/in/ronrossnist

Senior Information Security Researchers and Technical Support

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Web: csrc.nist.gov

Comments: sec-cert@nist.gov