A Multidisciplinary Approach to Building Trustworthy Secure Systems

Protecting the Nation's Critical Assets in the 21st Century

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

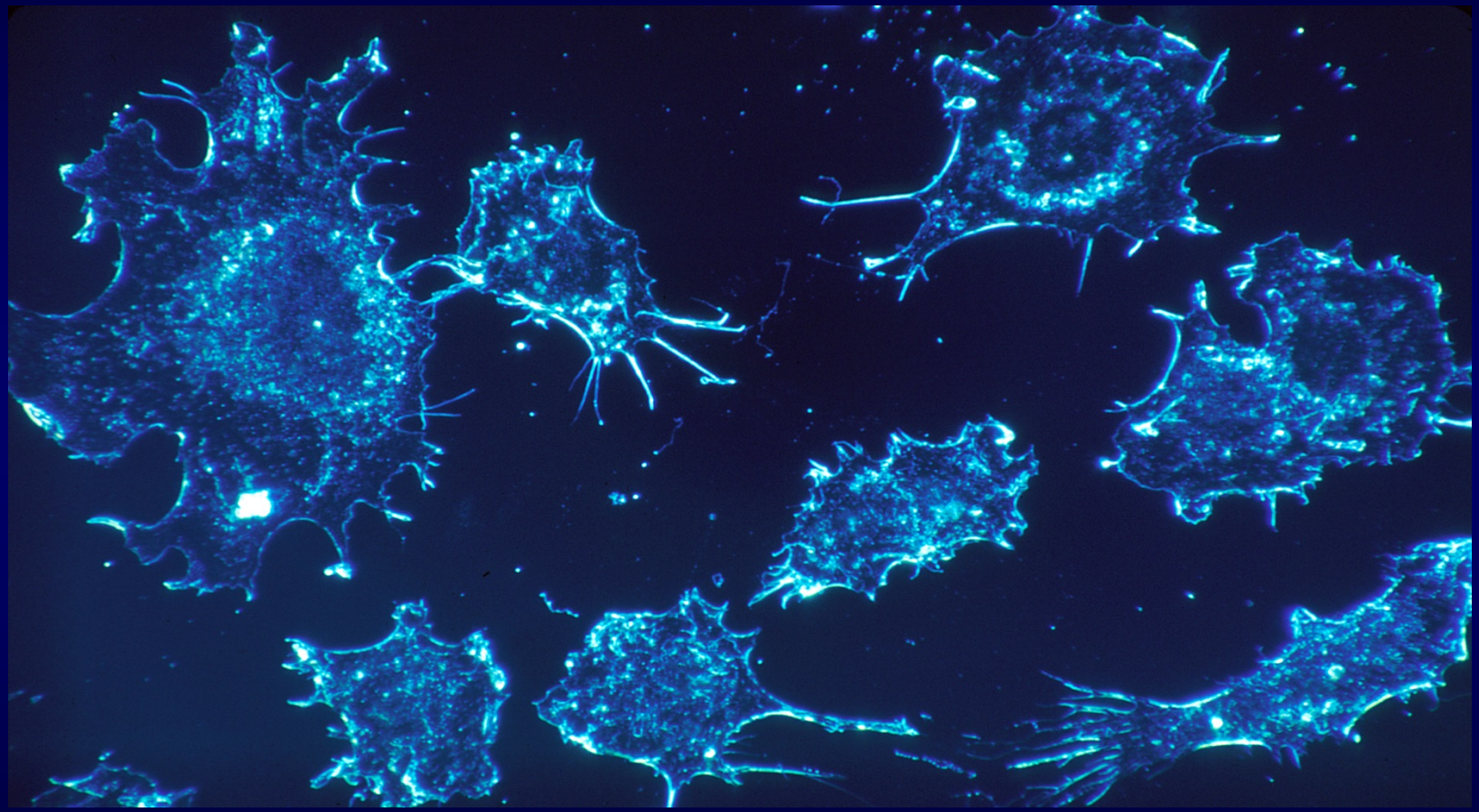
OPM.
Anthem BCBS.
Ashley Madison.

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

Complexity.


Kinetic space.

Cyber space.

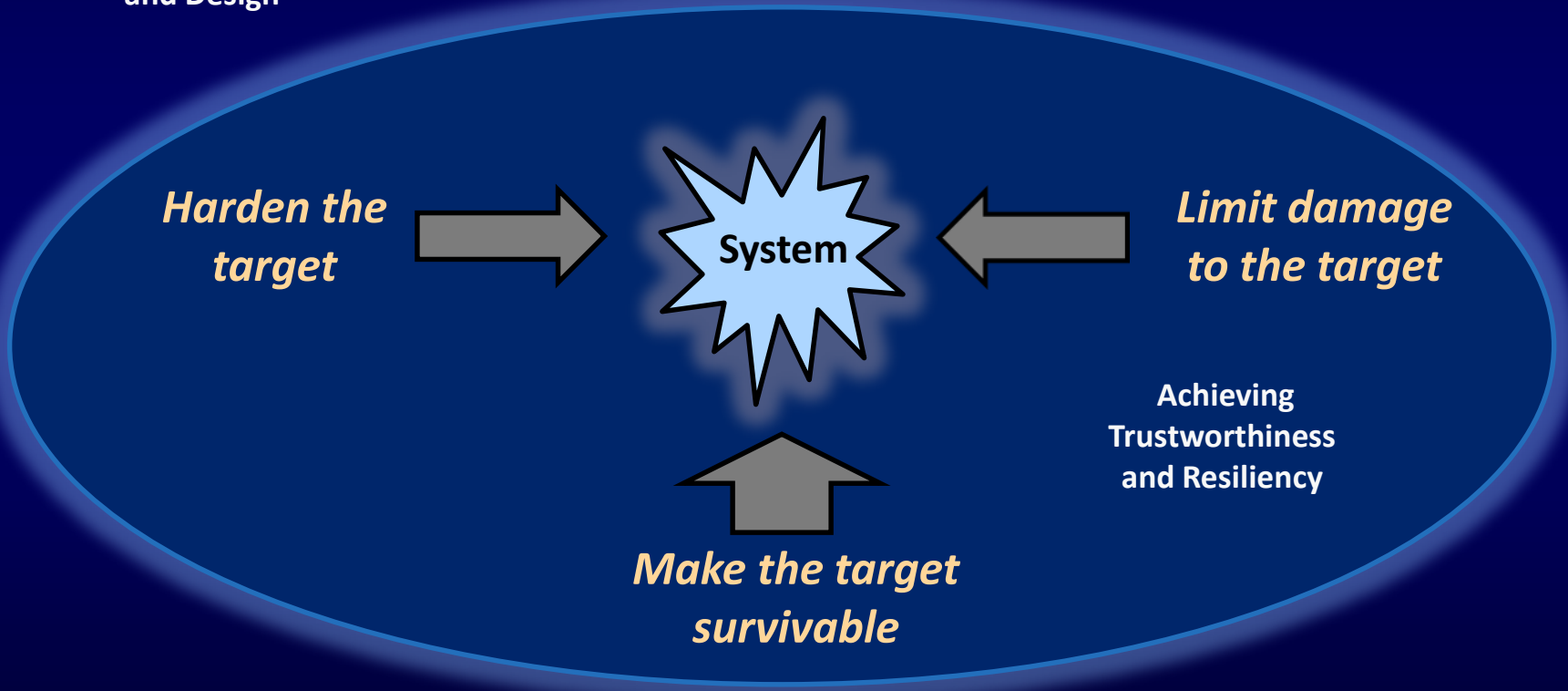


Sharks and glaciers.

The n+1 vulnerabilities problem.

Security Architecture and Design

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



Security.

An emergent property.

Risk assessment.

Assets and consequences.

Engineer up.

05.04.16

NIST Special Publication 800-160

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure 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

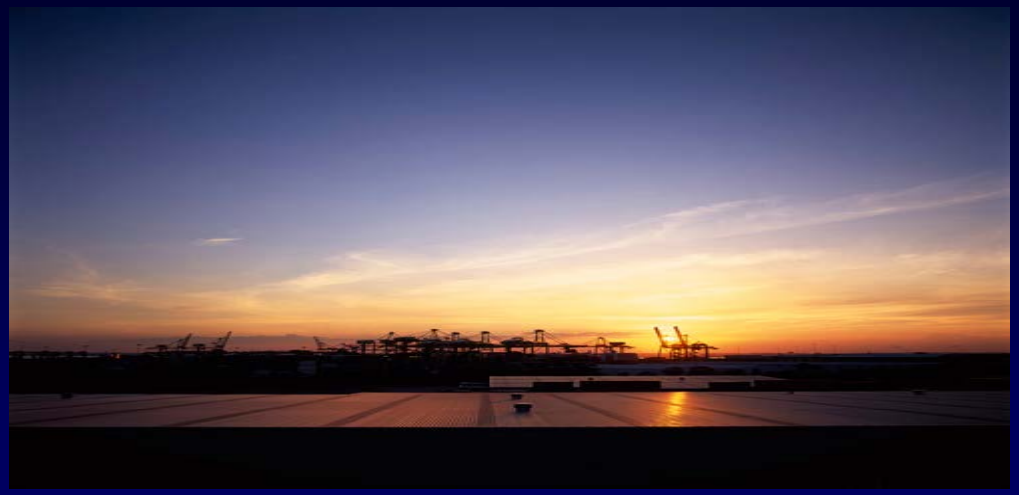
Nontechnical Processes

- 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

A few examples.

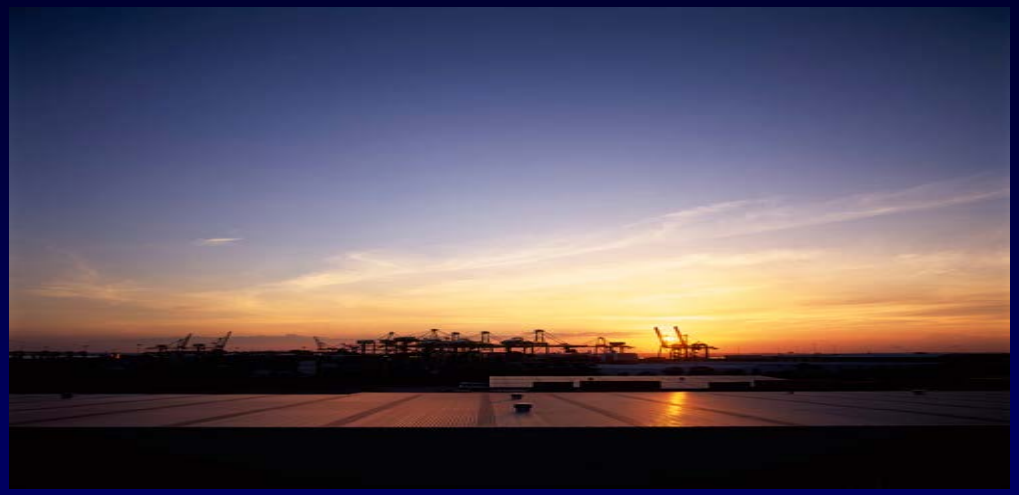


Human Resource Management Process

Systems Engineering View

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

-- ISO/IEC/IEEE 15288-2015.



Human Resource Management Process

Systems Security Engineering View

"Systems security engineering, as part of the *Human Resource Management* process, defines the security criteria for the qualification, assessment, selection, and ongoing training of skilled and experienced personnel qualified to perform the security aspects of life cycle processes to achieve organization, project, and stakeholder security objectives."

-- NIST Special Publication 800-160.

Systems Security Engineering

HR Management Process Outcomes

- Systems security engineering skills required by projects are identified.
- Individuals with systems security engineering skills are provided to projects.
- Systems security engineering skills of personnel are developed, maintained or enhanced.

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.

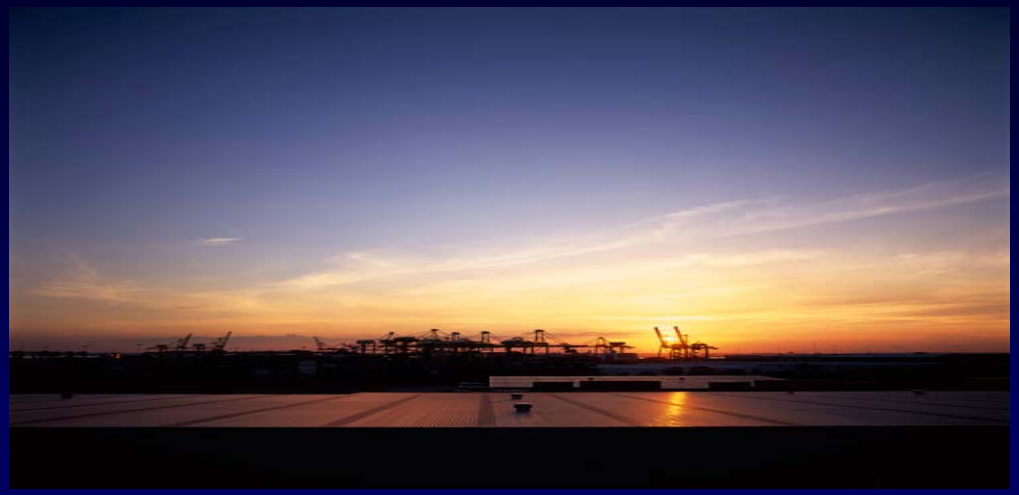
  Elaboration: Systems security engineering skills needed include foundational skills that span systems engineering and security specialties, and security specialty skills determined by current and expected project needs.

  HR-1.2 Identify existing systems security engineering skills of personnel.

  Elaboration: Skills identified include all relevant systems engineering and specialty security engineering, technology, and related skills.

  References: ISO/IEC/IEEE 15288, Section 6.2.4.3 a).

  Related Publications: ISO/IEC 12207, Section 6.2.4.3.1; National Cybersecurity Workforce Framework; DoD Directive 8140.01; ISO/IEC 27034-1, (SDL) Section A.9.1.

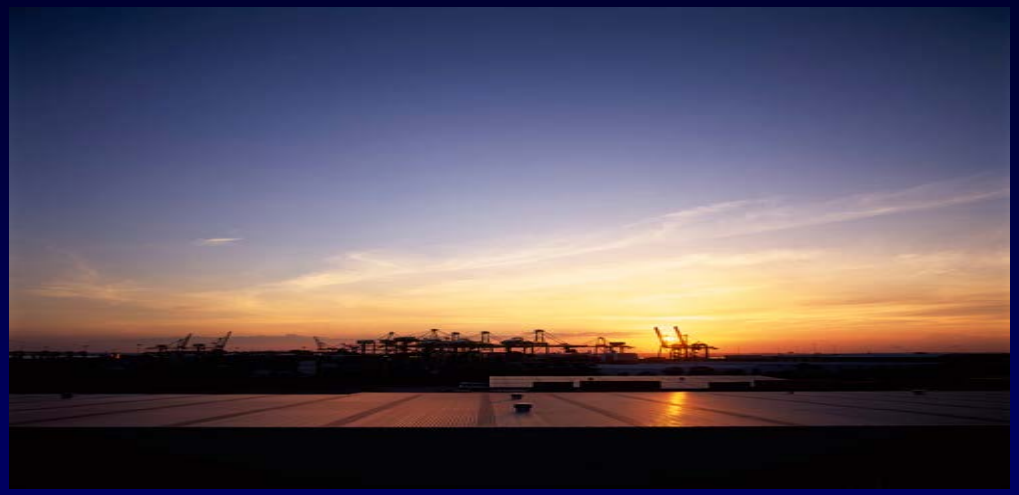


Stakeholder Needs and Requirements Definition Process

Systems Engineering View

"The purpose of the Stakeholder Needs and Requirements Definition process is to define the stakeholder requirements for a system that can provide the capabilities needed by users and other stakeholders in a defined environment."

-- ISO/IEC/IEEE 15288-2015.



Stakeholder Needs and Requirements Definition Process

Systems Security Engineering View

"Systems security engineering, as part of the Stakeholder Needs and Requirements Definition process, defines the stakeholder security requirements that provide the protection capability and security characteristics for the system in satisfaction of all needs of users and other stakeholders…"

-- NIST Special Publication 800-160.

Systems Security Engineering

Stakeholder Needs and Requirements Definition Process Outcomes

- The specific security interests of stakeholders of the system are identified.
- Stakeholder assets and assets classes are identified.
- Asset susceptibility to adversity and uncertainty is determined.
- Asset protection priorities and protection assurances are determined.
- Stakeholder protection needs are defined and prioritized.

Stakeholder Needs and Requirements Definition Process

Security-Related Activities and Tasks

- **SN-2 DEFINE STAKEHOLDER PROTECTION NEEDS**

  SN-2.2 Identify stakeholder assets and asset classes.

  Elaboration: Assets include all tangible and intangible assets. The assets and asset classes are identified in consideration of all stakeholders and all contexts in which assets are used by the system-of-interest. This includes the business or mission; the enabling systems of the system-of-interest; the other systems that interact with the system-of-interest; and stakeholders whose assets are utilized by the business or mission and/or by the system-of-interest.

  SN-2.5 Identify stakeholder protection needs.

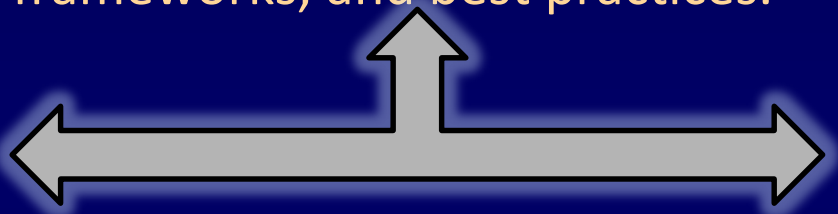
  Elaboration: Stakeholder protection needs are identified in terms of the loss consequences realized by stakeholder relative to assets and the events that produce the loss consequences. Protection needs should be identified in a manner consistent with how stakeholders manage the assets. The protection needs are identified in dimensions that are consistent with the loss concerns (e.g., loss of control, loss of ownership, loss as in destruction) so as to account for varying needs across varying concerns.

  References: ISO/IEC/IEEE 15288, Section 6.4.2.3 b); ISO/IEC 15026; ISO/IEC 25010; ISO TS 18152; ISO/IEC 25063.

  Related Publications: FIPS Publication 199; NIST SP 800-37 (RMF Step 1).

References and Related Publications Sections

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.

Appendices

A Wealth of Trusted Systems Development Principles, Concepts, and Best Practices

- References
- Roles, Responsibilities, and Skills
- Design Principles for Security
- Engineering and Security Fundamentals
- System Resiliency
- Security Requirements Considerations
- Software Security and Assurance
- Hardware Security and Assurance
- System Security Analyses
- RMF Application

Some final thoughts.

The Cold War.

Institutionalize.

The ultimate objective for security.

Operationalize.

Leadership.
Governance.
Accountability.

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

Government

Academia

Security is a team sport.

Industry

Race to the Top

Better Security Through Engineering

Ron Ross

100 Bureau Drive Mailstop 7730
Gaithersburg, MD USA 20899-7730

Email
ron.ross@nist.gov

Mobile
(301) 651.5083

LinkedIn
www.linkedin.com/in/ronrossnist

Twitter
@ronrossecure

Web
csrc.nist.gov

Comments
sec-cert@nist.gov

We are here to help you be more secure…