Stevens Institute Security Research

- National Center for Secure and Resilient Maritime Commerce
- Naval Security Infrastructure Technology Laboratory
- Center for the Advancement of Secure Systems and Information Assurance
  - National Cybersecurity Center of Excellence in Information Assurance Education
  - National Cybersecurity Center of Excellence in Information Assurance Research
- Leader of the DoD University Affiliated Research Center for Systems Engineering Systems Security Core Research Topic

Why new focus on Systems Engineering Security?
SERC Security Engineering Research Roadmap

1. Define systems security
2. Measure systems security
3. Devise system security frameworks
4. Improve the proficiency of the security engineering workforce
1. Define systems security

- Reassess periphery models
- Focus on whole systems
- Examine interfaces and interactions
- Understand similarities and differences across domains
2. Measure systems security

- Achievable and comparable security attributes
- Outcome-based rather than vulnerability-based
- Identify systemic value of currently available control standards
- Identify and measure trade-offs with respect to security features
3. Devise systems security frameworks

- Include policy, process and technology
- Provide basis for evaluation
- New classes of system-level solutions
- Security-receptive architectures
4. Improve the proficiency of the security engineering workforce

- Encourage and educate workforce
- Operational security requirements
- Community force multipliers
- Engage stakeholders
Example:
Systemic Security

Security
- facilitates governance process
  - thwarts perpetrators
  - informs enact
  - engages audit
  - reports to vulnerabilities

Governance process
- produces policy
  - observes policy
  - provides requirements for rules and regulations
  - establishes systems

Systems
- systems
  - enterprises
  - management
  - infrastructures

Infrastructures
- information attributes
  - availability
  - integrity
  - confidentiality

Information attributes
- when degraded may reduce
  - produce and manage

Production and manage
- produces and manages value
  - assets
  - intangibles
  - mission

Value
- disrupted
  - data corruption
  - data breach

Disruption
- disrupts damage
  - data
to exploit
  - permit

Damage
- protects

Protection
- monitors

Monitor
- detects harm to recovery alternatives
  - preserves
  - restore

Recovery alternatives
- provides access controls
  - authorizes

Access controls
- provides monitors

Monitors
- observes monitors
  - provides

Observes
- observes

Detect harm to

Detect harm to
- detect

Detect
- provides

Provides
Example System

1. User logs in to desktop.
2. Desktop connects to webserver through open firewall ports.
3. Desktop sends information request to webserver.
4. Webserver peer connects to database and sends user credentials.
5. Webserver executes user credential lookup and comparison.
6. Database accepts credentials (may reject but not in this example).
7. Database sends information query.
8. Database sends query result to webserver.
9. Webserver reformats information and sends to desktop through open firewall ports.
10. Desktop sends information screen through open firewall ports.
11. Desktop executes display menu.
13. Desktop executes display information and stores locally.
Metaphorical Construct
Discovery

ISO 27005:2008
Security Risk Assessment
Task Order:
1. Identification of assets
2. Identification of threats
3. Identification of existing controls
4. Identification of vulnerabilities
5. Identification of consequences
Questions? Discussion?

Follow-up:
jenennifer.bayuk@stevens.edu