SYSTEMS ENGINEERING
Research Center

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

SERC Security

By
Jennifer Bayuk

Annual SERC Research Review
October 5-6, 2011
University of Maryland
Marriott Inn and Convention Center
Hyattsville, MD
www.sercuarc.org

SERC Security Research Tasks

- RT8 – System Security Roadmap
  - —Our foundation
- RT28 – System Aware Security
  - —Currently active – PI is Barry Horowitz, UVA
- RT32 – System Security Metrics
  - —Proposed – PI is Jennifer Bayuk
  - —If accepted will require multiple security SME collaborators
- RT38 – Cyber Security Decision Support
  - —Proposed – PI is Barry Horowitz
  - —Builds on RT28

RT 8: System Security Roadmap

The SERC system security roadmap was motivated by the fact that current defensive strategies add tremendously to cost and do not respond effectively to the growing sophistication of attacks, as well as the recognition that today's systems engineers are inadequately prepared to address system security requirements.

RT8 was a 8-month effort with representation from the majority of the SERC members, as well as a larger community of invited security subject matter experts.

The final report emphasized that progress in *system security research must follow a scientific process* that includes clear problem statements, thorough problem background descriptions including a full literature review, clearly defined solution criteria, and proposed hypothesis formulated to shed light on a solution and how it may be proven or disproven.

As security luminary and roadmap reviewer Peter G. Neumann said in his email response to the final draft, the roadmap was "*a very worthy step forward*" in security research.

RT 28: System Aware Security

Successful security design patterns should yield metrics that relate increases in security to corresponding impacts on system performance. Such metrics provide much needed information required by the engineering trade-space.

Building on RT8: *Systems Security Engineering Roadmap*, RT28 research in architecture frameworks will devise systems security engineering methods that integrate fault tolerant and automatic control system technologies with cyber security technologies, processes, and tools to develop System-Aware security services that will be transferable between systems with common functionality.

Key Deliverables:

- *Description of system-aware security as an architectural concept, to include a prototype of system-aware security services architecture to demonstrate integration of services to dynamically adapt performance based upon risk and system performance implications.*
- *Design patterns with embedded metrics regarding security/system performance tradeoffs.*

RT 32: System Security Metrics

The state of the art and current practice in security metrics use certification and testing strategies rather than correctness and effectiveness criteria. Security requirements can be *verified* using well known certification techniques in combination with continuous monitoring technologies, but can be *validated* only with respect to system mission and purpose.

Building on RT8: *Systems Security Engineering Roadmap*, RT32 research in security metrics shall provide the *theoretical foundation* to support security requirement analysis and security models for use in both security requirements verification and validation.

Key Deliverables:

- *Security framework that combines both security and systems engineering techniques from other disciplines to combine measurable systems security attributes into a working definition of systems-level security that can be measured (to include output from RT28).*
- *Evaluation report via the framework for DoD-selected case studies.*

RT 38:
Cyber Security Decision Support

The uncertainties and judgment calls surrounding cyber security call for a process through which DOD operators and procurement officers could interact with system designers in exploring the tradeoff space as a precursor to selecting and evaluating final design candidates.

Building on RT28: *Cyber Security Decision Support*, RT-38, will build upon the security scoring system developed in RT-28. RT-38 research will focus on the design of a collaboration environment that addresses the influences of uncertainties in expert judgment and decision-maker preferences and how they influence complex decision making. This work will have a foundation in the mathematics of multi-objective decision theory under uncertainty, and will be tailored to enable practical use.

Key Deliverables:

- *A prototype distributed software system for multi-agent decision support.*
- *Analysis and documentation of results for the use of the prototype in formative experiments, initial evaluations, and technology demonstrations.*

SYSTEMS ENGINEERING
Research Center

Remainder of Session Agenda

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

- Summary of RT28 – Rick Jones, UVA
- Roundtable discussion