NIST ITL Security Metrics Activities

William C. Barker

Chief, Computer Security Division

NIST ITL Security Metrics Activities

- Theoretical foundations of cyber security metrics
  - Individual Measurements in some cases difficult
  - Predicting behaviors under composition still more difficult
- Results-oriented measurement
  - Practical in near term, yields maximum pay-off
  - Supports correlation of security actions and observed exploits
- Controls application statistics
  - Relatively easy to capture
  - Focuses on implementation of C&A controls
  - Correlation with vulnerability reduction not quantifiably demonstrated

NIST FY 2007 Initiative in Cyber Security

Discrete Mathematics, Information Science, and Applications

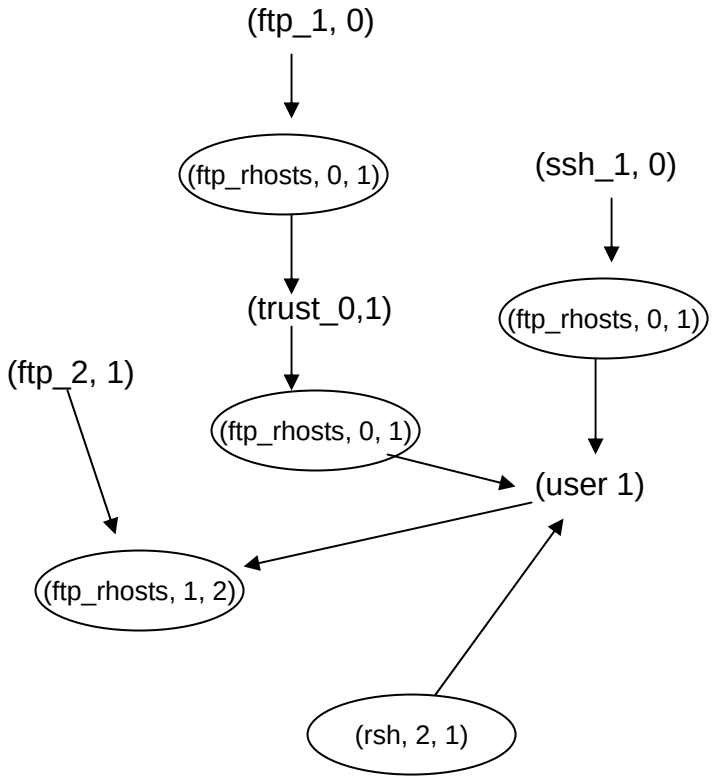
- Math Division has lead
- Begin developing foundations of a measurement science for complex information systems.
- Basis for such work found in the fields of:
  - Discrete mathematics,
  - Theoretical computer science, and
  - The physical sciences.
- Plan to develop and analyze abstract mathematical models of information system structure and information flow.

NIST FY 2007 Initiative in Cyber Security

- Will study:
  - Combinatorial structures (e.g., abstract networks and graphs),
  - Information theory, and
  - Computational complexity theory (central).
- Studies will use:
  - The emerging theory of discrete random systems,
  - The (probabilistic) theory of Markov processes, and
  - Modern Monte Carlo based computational approaches.
- Studies will exploit useful analogies from the study of physical systems, considering infinite (continuous) analogs of information systems utilizing theories of:
  - Pattern formation,
  - Dynamical systems,
  - Bifurcations,
  - Phase transitions, and
  - Chaos.
- Fundamental work will be applied to the study of:
  - Computer networks and computer security and
  - Phenomena such as nanostructures and quantum information systems.

Measuring Network Security Using Attack Graphs

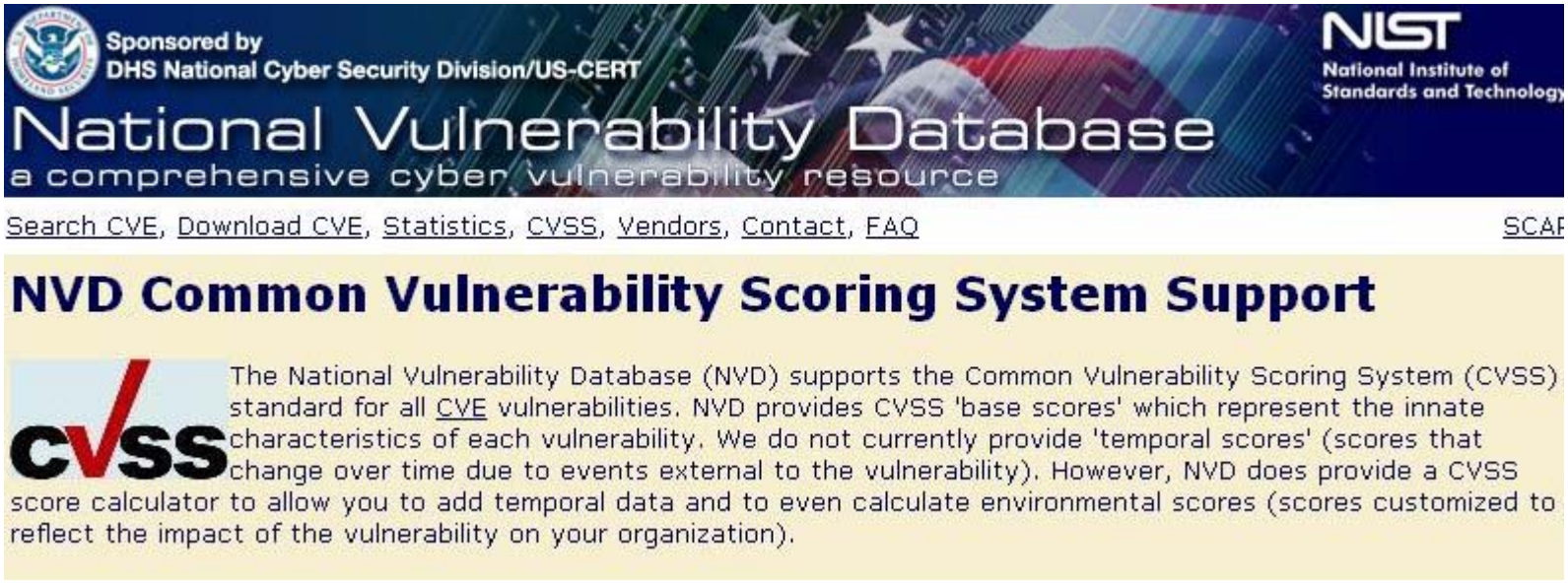
- A Topographical Analysis of Known Critical Resources in a system can yield measurable data on overall system security
- Analysis can Produce an Attack Graph Showing Most Vulnerable Paths to/within systems
- System and Network Hardening can be Applied in a Cost Effective and Appropriate Manner
- System Resistance to Attacks can be Quantified and Measured



Source: Anoop Singhal CSD NIST
Lingyu Wang, CIISE, Concordia University
Sushil Jajodia, George Mason University

Measuring Vulnerabilities

- Establishes Standard Base Scores for Vulnerabilities
- Ability for Organizations to Tailor According to Environment and Risk
- Allows for Generation of Common Vulnerability Vectors
- Can Support and Feed Attack Graph Analysis



NIST Special Publication 800-55

National Institute of Standards and Technology

Technology Administration

U.S. Department of Commerce

Security Metrics Guide for Information Technology Systems

Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo

- ✓ How an Organization, Through the Use of Metrics, Identifies the Adequacy of In-place Security Controls, Policies, and Procedures
- ✓ Providing an Approach to Help Management Decide Where to Invest in Additional Security Protection Resources
- ✓ Explaining the Metric Development and Implementation Process and How it can Also be Used to Adequately Justify Security Control Investments.
- ✓ How Results of an Effective Metric Program can Provide Useful Data for Directing the Allocation of Information Security Resources and Simplify the Preparation of Performance-related Reports.

NIST 800-55 Rev1 update

Revised	New	Remained
• Measures development methodology to tie into enterprise-wide strategic planning process • Measures implementation methodology to integrate continuous monitoring • Measure development template • Mapping to NIST SP 800-53 Rev1 controls • Roles and responsibilities for consistency with FISMA and recent NIST publications	• Measures within SDLC section and examples for quantifying integration of information security into system development and integration process • Touch points with Risk Management Framework • Term ***measures*** • Example measures consistent with the updated template	Types of measures: • Implementation measures to track progress in implementing information security controls (% of trained personnel) • Effectiveness/efficiency measures to track results of security control implementation (% of applicable vulnerabilities that have been remediated) • Impact measures to articulate the impact of information security on the organization's mission (cost of virus attacks)