



Information Trust
I N S T I T U T E

Security Metrics: State of the Art and Challenges

Bill Sanders

University of Illinois

January 28, 2009



www.itl.uiuc.edu

Everyone says Security Metrics are Important ...

- Security metrics were an **important problem** in the **2005 INFOSEC Research Council Hard Problems List**
- The Computer Research Association has identified **cyber security risk assessment** as one of four grand challenges
- February 2005 PITAC report placed **quantitative benefit-cost modeling** at number nine on its list of “Cyber Security Research Priorities.”
- **New security metrics that are linked to the business were ranked first** among six key security imperatives developed by over twenty Fortune 500 firms
- **New regulatory requirements of Sarbanes-Oxley and the Basel II Accord have created more urgency for metrics that integrate security risk with overall business risk**
- **Almost every critical infrastructure roadmap lists security metrics as a critical challenge**

The list goes on ...



Recent U.S. Congressional Workshop

- Convened at the request of Senators Lieberman and Collins in Wash. DC, October 3, 2008
- Named security metrics and their quantification as one of 3 key cyber security research areas
- I briefed government leaders on need, and led discussion on possible solutions

JOSEPH L. LIEBERMAN, CONNECTICUT, CHAIRMAN
CARL LEVIN, MICHIGAN
DANIEL K. AKAKA, HAWAII
THOMAS H. CARPER, DELAWARE
MARK L. PRICER, ARKANSAS
MARY L. LANDRIEU, LOUISIANA
BARACK OBAMA, ILLINOIS
CLAIRE McCASKILL, MISSOURI
JOHN TESTER, MONTANA
SUSAN M. COLLINS, MAINE
TED STEVENS, ALASKA
GEORGE V. VONNOVIC, OHIO
ROMAN COSGROVE, MINNESOTA
TOM COBURN, CALIFORNIA
PEB W. DOMENEZ, NEW MEXICO
JOHN WARNER, VIRGINIA
JOHN E. SUNUNU, NEW HAMPSHIRE
MICHAEL L. ALEXANDER, STAFF DIRECTOR
BRANDON L. MCGORR, MINORITY STAFF DIRECTOR

United States Senate
COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

September 18, 2008

Dr. William Sanders
University of Illinois at Urbana-Champaign
451 CSL
1308 W Main, M/S 228
Urbana, IL 61801

Dear Dr. Sanders,


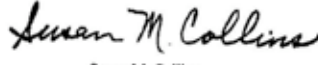
The integrity and reliability of our nation's cyber infrastructure is one of the most pressing security challenges facing the federal government. As the Chairman and Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, we are committed to ensuring that the information stored in our government networks remains protected and the systems running our nation's critical infrastructure are secure. In order to achieve such a lofty goal, we must refocus, enhance, and accelerate the cyber security research and development conducted in this country.

It is time to bring citizens, business, and government together with researchers to provide some new perspective on this important issue. To this end, we are hosting three forums intended to generate a plan for the future of cyber security research and development focused on user needs. Our partner and moderator in this effort, the Institute for Information Infrastructure Protection (I3P), is a national consortium of leading academic institutions, non-profits, and national laboratories, managed by Dartmouth College. The I3P's breadth of experience will ensure that the forums will be focused and effective. We have charged the I3P with delivering to us a report of the forums' key findings which we hope will provide a foundational roadmap for the incoming Administration.

Each forum will focus on one of three key issue areas – economic trade-offs, human behavior, and effective technology – that seem to be preventing the promise of cyber security from becoming reality. Each group will be highly selective and relatively small to ensure that all participants have their voices heard. Because of your experience and insight, we cordially request your presence at the second of these forums, moderated by Rob Cunningham of the MIT Lincoln Laboratory, which will address technology for cyber physical system security. The forum will explore those impediments to a secure infrastructure that result from failure to acquire data sources, to understand threats, to develop useable technology, and to evaluate that technology in a meaningful way.

This forum will be held on Monday, October 6, at the Hyatt Regency on Capitol Hill in Washington, DC beginning at 8am and ending at approximately 5pm. An agenda is attached to this letter.

Please RSVP to Nicole Hewett by September 29 at Nicole.Hewett@Dartmouth.EDU or by phone at (603) 646-0703. We look forward to your participation in this important event.

Sincerely,

Joseph I. Lieberman
Chairman
Honorary Co-Chair, I3P Forums

Susan M. Collins
Ranking Member
Honorary Co-Chair, I3P Forums

Security Truths ...

- Security is no longer (or perhaps never was) **absolute**
- ICT (information and communication technology) systems/networks must operate through attacks, providing proper service in spite of possible penetrations
- If security cannot be shown to be absolute, **quantification of the “amount” of security that a particular approach provides is essential**
- Quantification can be useful in:
 - A **relative** sense, to choose among design alternatives
 - In an **absolute** sense, to provide guarantees to users

Security Metrics

- There is no shortage of security metrics ...
- But, are they the right ones?

Organizational Security Metrics, pt. 1

- Metrics used to describe, and to track the effectiveness of, organizational programs and processes
- Can help plan investment in IT architectures or technologies, as well as creation, sustainment, and termination of security programs and program elements
- Can be broken down into security program metrics and security process metrics
- Security Program Metric Examples:
 - NIST SP 800-26 (Security Self-Assessment Guide for IT Systems) [Swanson 2001]
 - Corporate Information Security Working Group [CISWG 2005] builds on NIST SP 800, and lists metrics that are usually percentages (systems/procedures/personnel) that conform to a given best practice

Organizational Security Metrics, pt. 2

- Security Process Metrics: Security capability maturity models (CMMs):
 - Systems Security Engineering Capability Maturity Model [SSE-CMM 2003],
 - Security Capability Model developed by the *CSO Magazine and CMU's CERT/CC* [Slater 2005],
 - NSA's INFOSEC Assurance Capability Model [NSA 2004],
 - B-Secure Security Maturity Model [Breakwater 2003].
- All of these specify levels of maturity, and definition of specific areas for which assessment is performed.

Technical Security Metrics

- Compare technical objects, e.g., algorithms, specifications, architectures and alternative designs, products, and as-implemented systems.
- Also can support the selection of IT products and technologies, and also serve as inputs to various operational security metrics
- Technical security metrics are the least-developed and most ad hoc

Technical Security Metric Examples

- **Common Evaluation Methodology** (CEM) or “Common Criteria” [CC 2004b] defines the evaluation process for Evaluation Assurance Levels, each of which is a set of assurance requirements
- **Common Vulnerabilities and Exposures** (CVE) list
- **Open Source Testing Methodology Manual** (OSSTMM) [Herzog 2003] enables the computation of **Risk Assessment Values** (RAVs) for products or systems being tested
- Institute for Security and Open Methodologies (ISECOM) defines RAVs [Herzog 2003] for ten areas of security controls assessed using the OSSTMM
- Open Web Security Application Project (OWASP) defines the **DREAD risk metric** (damage, reproducibility, exploitability, affected users, and discoverability) to assess the level of risk associated with a threat to a Web application [OWASP 2005].

Operational Security Metrics

- Used to describe, and hence to manage the risks to, operational environments
- Include measures of
 - operational readiness or security posture (e.g., how well a system can be expected to perform given an assumed threat environment),
 - measures used in risk management (e.g., security compliance), metrics that describe
 - threat environments, metrics that support incident response and vulnerability management, and potentially
 - other metrics produced as a part of normal operations that can be used as input to other security metrics.
- These metrics generally require experimental/empirical measurement for their estimation.

Operational Security Metrics Examples

- **Operational Readiness**

- SCORE (Security Consensus Operational Readiness Evaluation) from SANS Institute
- NIST's Practices and Checklists/Implementation Guide

- **Security Posture**

- Common Vulnerabilities and Exposures (**CVE**) and the Common Vulnerability Scoring System (**CVSS**) [Schiffman 2005].
- [Bernito 2005] lists a small, easily understood set of security metrics that serve as indicators of overall security posture: baseline defenses coverage (antivirus protection, antispymware), patch latency, password strength, platform compliance scores, and legitimate e-mail traffic analysis

Existing Security Metrics Summary

- Most traditional approaches to security validation have focused on and specifying procedures that should be followed during the design of a system.
- When quantitative methods have been used, they have typically either been based on:
 - formal methods (e.g., [Lan81]), aiming to prove that certain security properties hold given a specified set of assumptions, or
 - statistical methods, on specific system components, e.g., intrusion detection systems, or
 - been quite informal, using a team of experts (often called a “red team,” e.g. [Low01]) to try to compromise a system.

Problems with Existing Security Metrics Approaches

- **Process Guidelines** can improve security, but provide NO quantification of the amount of security that has been obtained
- **Formal methods** aim either to prove absolute security (not usually possible), or find problems (useful, but NO quantification).
- **Red Teams** can find problems (useful), but again, NO predictive quantification of security.
- Most existing metrics are **lagging indicators** of performance (and hence not predictive!)
- **Cost** to gain confidence, if possible, is **very high**.

More Security Metrics Problems

- *Existing methods are focus narrowly and exclusively on single aspect of security*
- *Inputs for organizational-level security metric computation are often not available, and difficult to quantify*
- *Organizational-level and technical security metrics are not integrated to provide a comprehensive view*

Security Metrics Challenge

Create a

***scientific foundation, methods, and tools
for quantitative assessment of security
metrics***

***that can be applied to large-scale
information-communication technology
systems***

throughout their lifecycle.

Practical Applications of Security Metrics

Organizational-level Metrics

Questions the CIO cannot answer:

- How much risk am I carrying?
- Am I better off now than I was this time last year?
- Am I spending the right amount of money on the right things?
- How do I compare to my peers?
- What risk transfer options do I have?

(From CRA, Four Grand Challenges in Trustworthy Computing, 2003)

A Question neither can answer:

- How do the technical metrics impact the organizational-level security metrics?



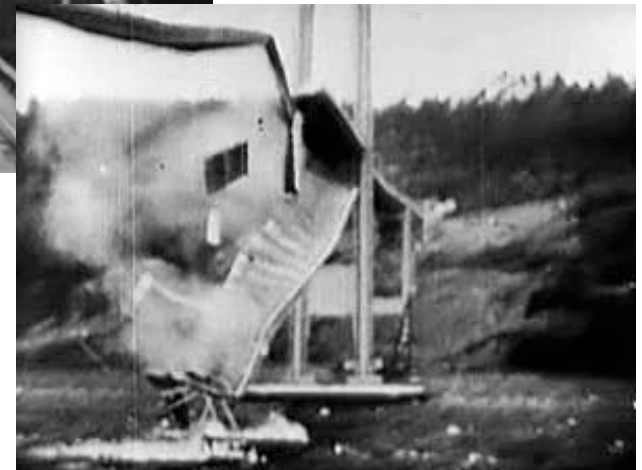
Technical Metrics

Questions the design engineer cannot answer:

- Is design A or B more secure (confidentiality, integrity, availability, privacy)?
- Have I made the appropriate design trade off between timeliness, security, and cost?
- How will the system, as implemented, respond to a specific attack scenario?
- What is the most critical part of the system to test, from a security point of view?

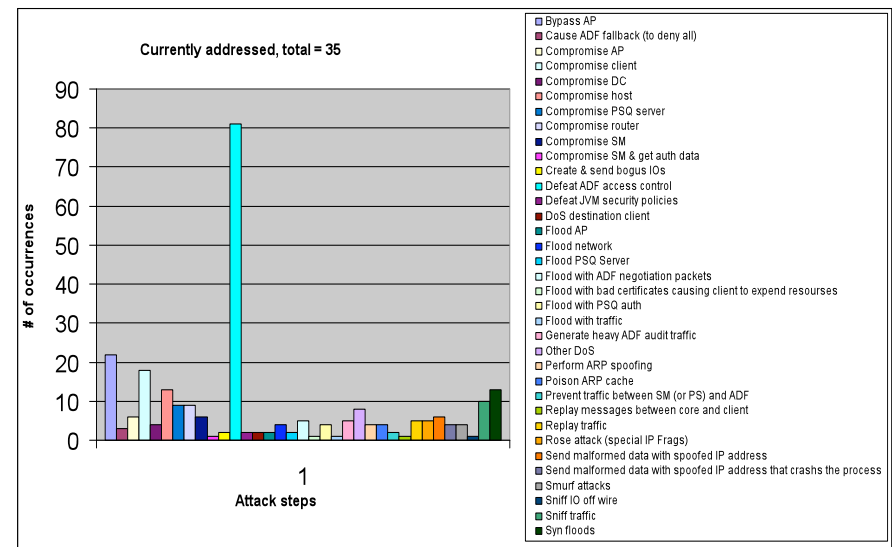
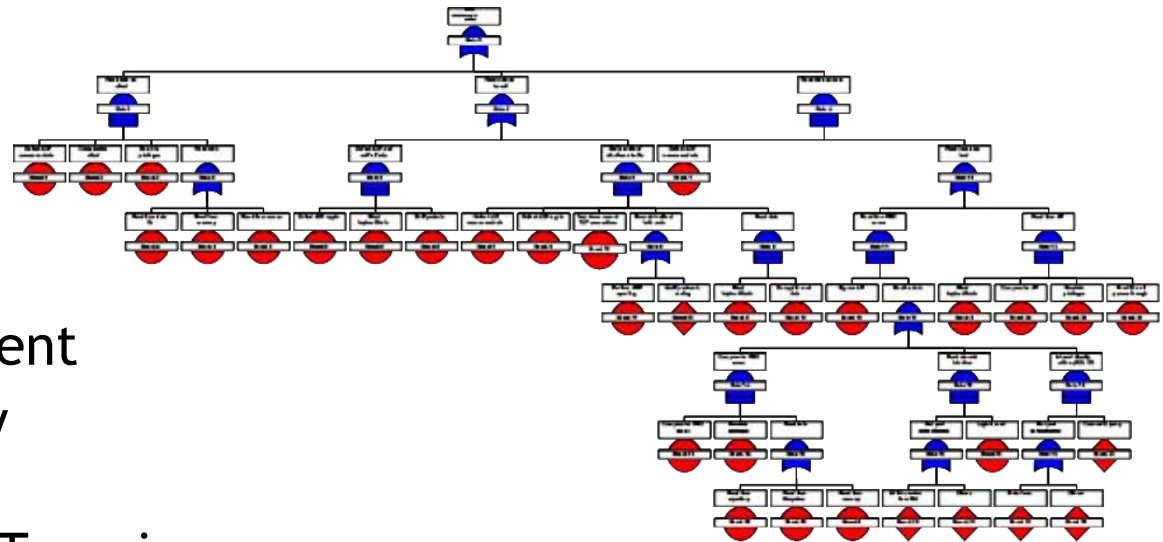
Challenge 1: Define Appropriate Security Metrics

- ***Metrics on multiple levels must be integrated:***
 - Operational-level metrics
 - Technical & Mission oriented metrics
 - Component-level metrics
- ***Metrics must be applied throughout the system lifecycle:***
 - Design, Configuration, Operation, Upgrade/ Evolution
- ***Both Product- and Process-oriented metrics***
- ***Not a single number!***



Challenge 2: Determine Methods for Estimating Metrics

- Formal Methods
- Probabilistic Models
- Benchmarking / Experimentation
- Classical Risk Assessment
- Threat & Vulnerability Assessment
- Whiteboarding & Red Teaming
- Informal and Semiformal Methods
- **Methods must be both model- and experimentally-based**
- **Multiple modeling and experimental methods must be integrated**

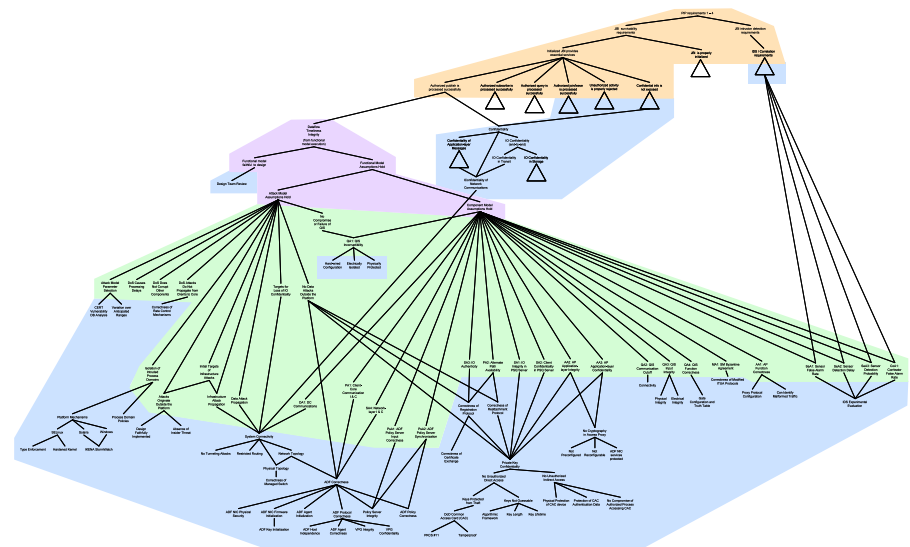
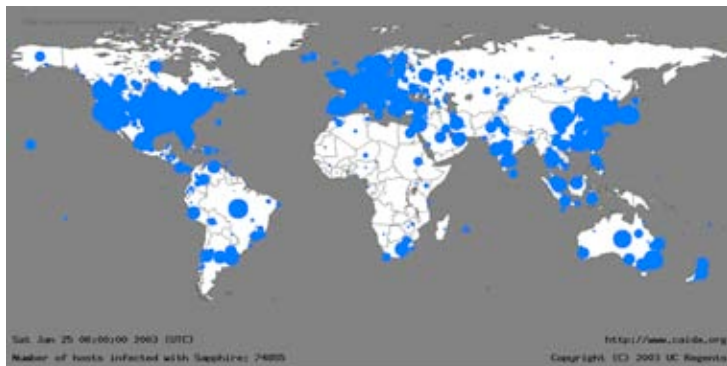


Challenge 3: Develop Security Argument Methodology linking Organizational and Technical Security Metrics

Create overall **security argument** to relate business and technical security metrics to one another and provide convincing overarching assessment of system-level, end-to-end, security

Metric Composition Challenges/Tasks

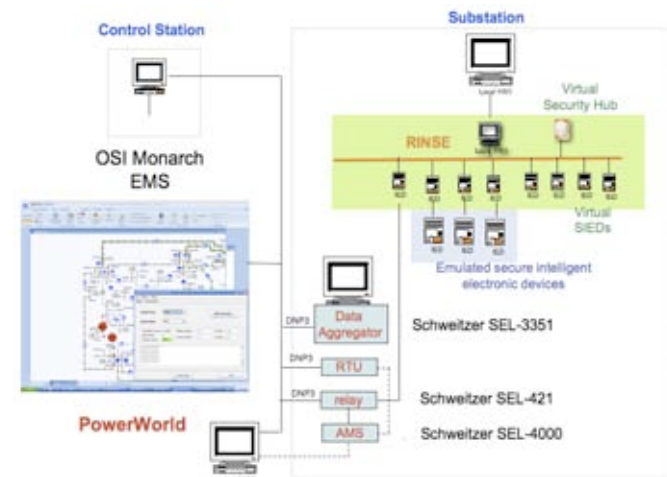
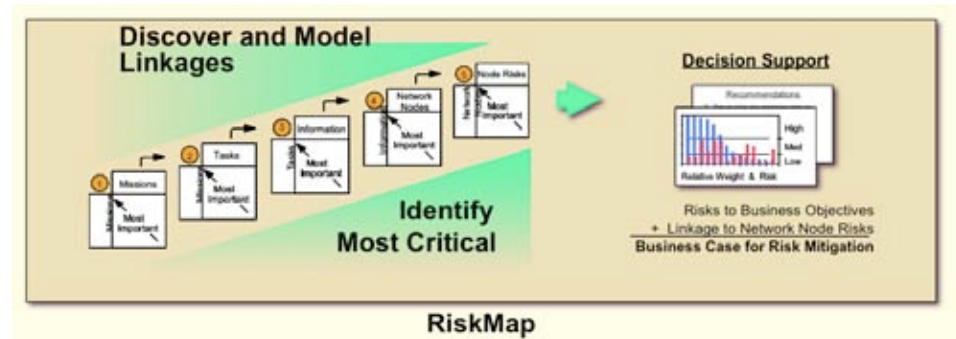
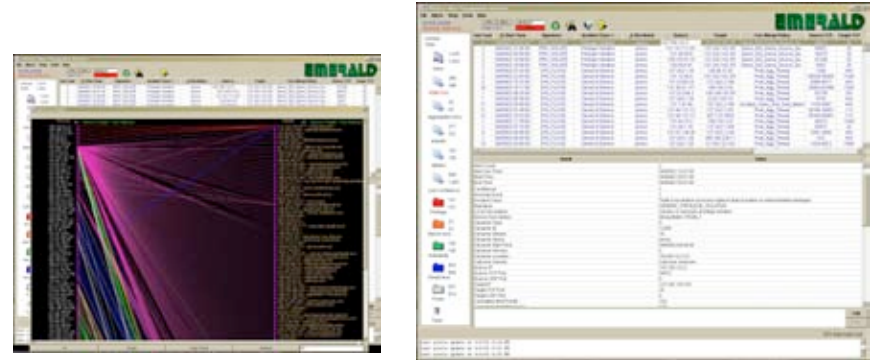
- Understand how to combine seemingly disparate types of evidence into an convincing overall argument.
- Define calculus for decomposing requirements into sub-requirements that can be validated independently
- Develop method for specify relationship between different parts of evidence gathered during the assessment process



Challenge 4: Building Effective Security Metric Evaluation Tools

- **Must put the methods in the hands of practitioners**
- **Must build usable tools that integrate organizational and technical metrics together with multiple metric estimation techniques**

=> Grand Challenge: Construct a methodology and tools that can be demonstrated to provide industry and government with a mechanism for determining accurate, quantifiable, security metrics



Challenge 5: Insure Impact via Legal/Regulatory Policy

- What incentives are necessary to insure that desired security metrics are achieved?
 - Return on Investment
 - Legal recourse (after the fact)
 - Regulation
- Sample Legal/Regulatory Policies:
 - Federal Information Security Management Act (FISMA)
 - NERC-CIP Standard in the Electric Power Industry
 - Basel II - establishes minimum capital requirements for banking organizations to reduce operational risks.
 - Health Insurance Portability and Accountability Act (HIPAA)

Discussion Topics

- What are appropriate organizational and technical security metrics for ICT systems?
- What evaluation methods can be used to develop an overall methodology for quantifying end-to-end security, at each stage of a system's lifecycle?
- What tools and testbeds need to be created to bring the developed methodology to practitioners?
- What policy/regulation should be put in place to insure prescribed security metrics will be achieved?
- What is an appropriate plan (timeline and milestones) for achieving useable & practical security metrics?