Resilience Assessment of CI: challenges and promising directions

Bill Sanders

Smart Grid Security Efforts @ Illinois

TCIPG: Trustworthy Cyber Infrastructure for the Power Grid (www.tcipg.org)

- Drive the design of an resilient cyber infrastructure electric power which operates through attacks
- $18.8 M over five year, started Oct. 1, 2009
- Univ. Illinois, Cornell, Dartmouth, U.C. Davis, Wash. State Univ.
- Funded by DOE and DHS
- Follow-on to $7.5 M NSF CyberTrust Center

Illinois's Singapore Adv. Digital Sciences Center Smart Grid Subprogram

~$15M effort / 5 years

Projects in Microgrids, DERs, and HANs

Korean National Smart Grid TestBed on Jeju Island.

Project concerning tesbed and cyber security research (DDSOS)

CACAIS

Testbed

Products tested & validated in CACAIS testbed: $1.2M FY10 funding from ONR

Illinois Center for a Smarter Electric Grid

Validation & Compliance Services

- $2.5M, YR1 DCEO funding
- Test bed & lab equipped with HW/SW to perform validation of Smart Grid systems
- Critical Infrastructure Protection (CIP): pre-audit check for compliance to NERC standards
- Prepare for NERC reliability compliance audits

4 New DOE Office of Electricity Security Projects with:

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Entergy THE POWER OF PEOPLE

GRID PROTECTION ALLIANCE

DTE Energy

Telcordia

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Pacific Northwest NATIONAL LABORATORY

pjm

GRID PROTECTION ALLIANCE

ALSTOM

Honeywell

INL

Security Metrics

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

Limitations of 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, 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.

Stochastic Security Metrics Challenge

Create a

scientific foundation, methods, and tools

for stochastic assessment of security metrics

that can be applied to critical infrastructure systems

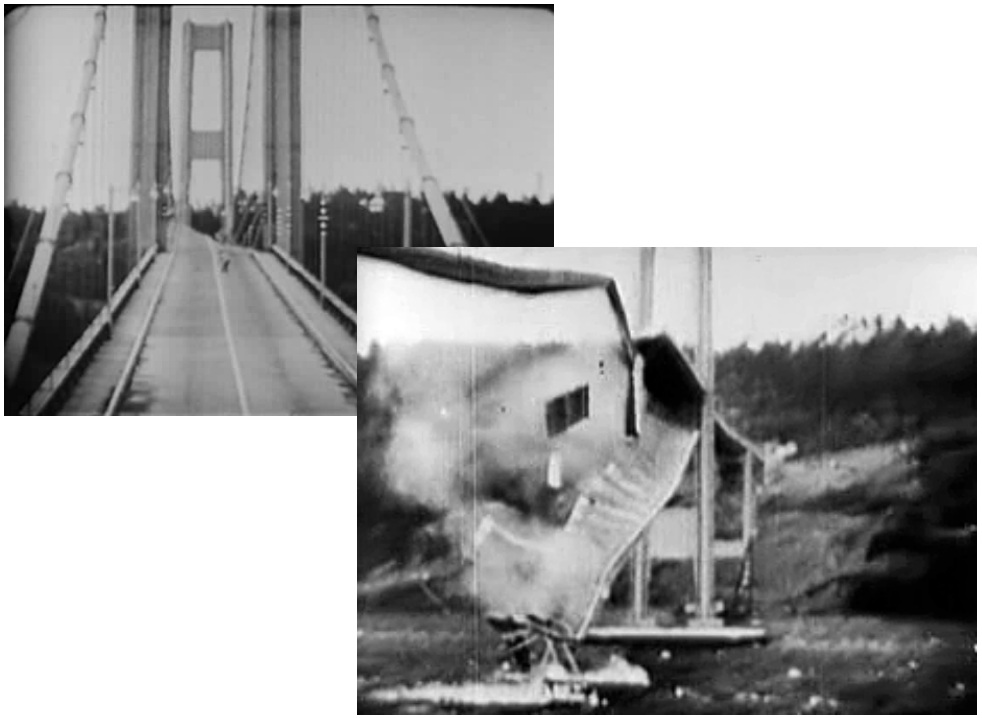
throughout their lifecycle.

Characteristics of Dream Stochastic Security Metric Analysis Method

- Be a predictive rather than lagging indicator
- Model a wide variety of adversaries
- Account for user behavior (e.g., degree of compliance with security policy)
- Express state-dependent behavior differences
- Support a wide variety of security metrics
- Be efficient in its computation (space, time, and or number of samples required)

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!***

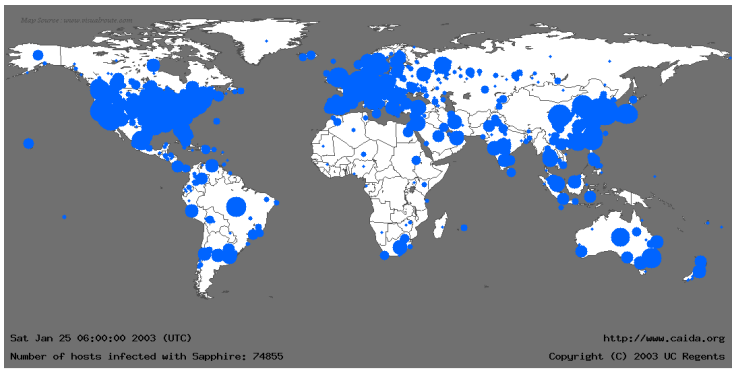


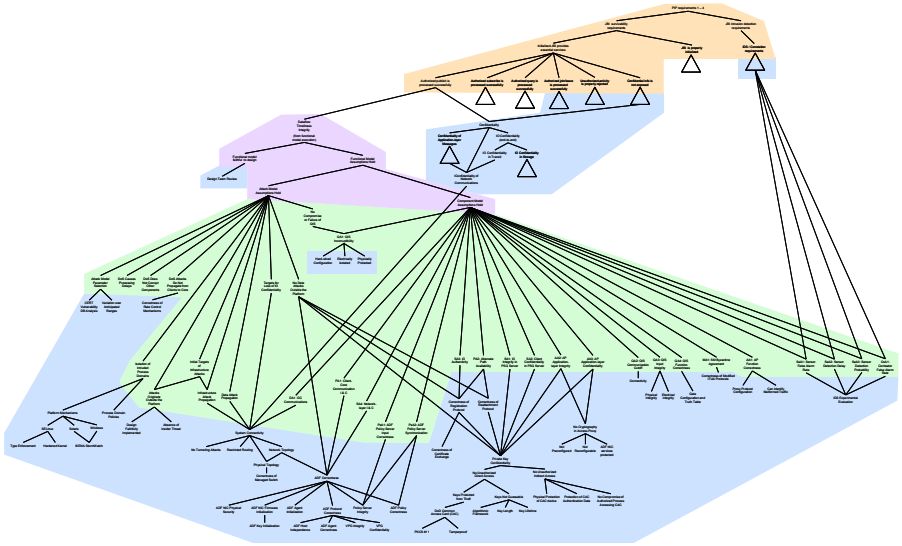
Challenge 2: Develop Security Argument Methodology linking Organizational and Technical Security Metrics

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 3: 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

Recap: Stochastic Security Metric Challenges

- Define appropriate quantitative security metrics
- Develop Security Argument Methodology linking Organizational and Technical Security Metrics
- Building Effective Stochastic Security Metric Evaluation Tools