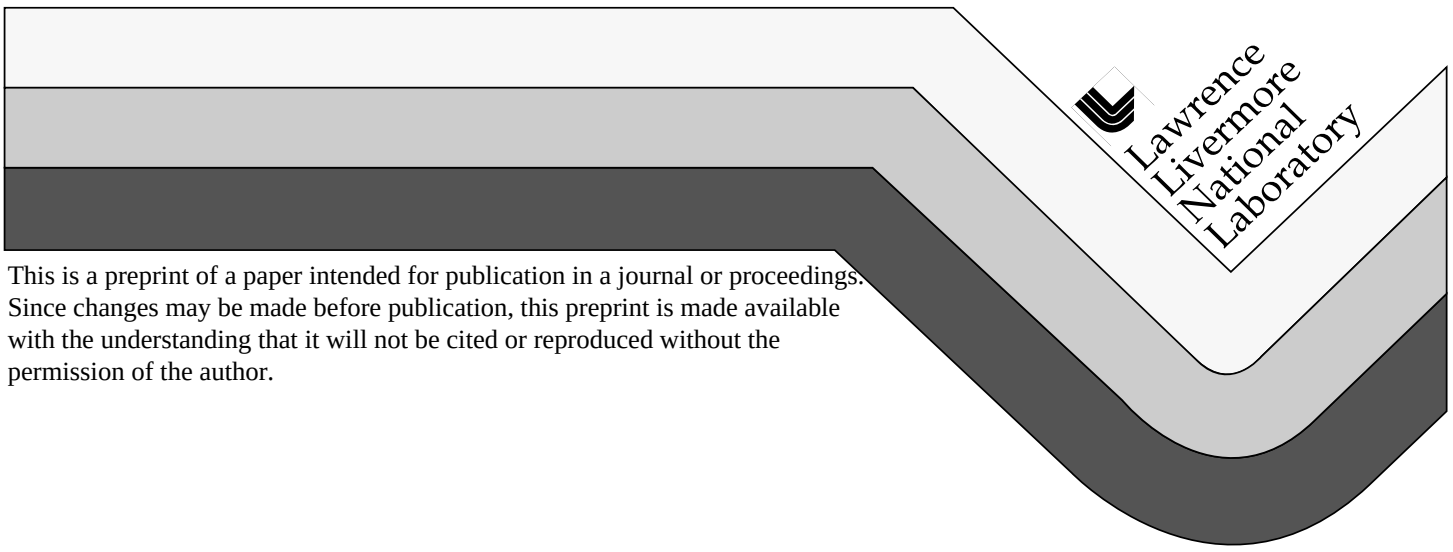
UCRL-JC-128061
Preprint

Tools for 21st Century Infrastructure Protection

S. R. Trost

This paper was prepared for submittal to
Workshop on Protecting and Assuring Critical National Infrastructure
Setting the Research and Policy Agenda
Palo Alto, CA
July 21-22, 1997

July 1997



Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

Tools for 21st Century Infrastructure Protection

Abstract

The President's Commission on Critical Infrastructure Protection (PCCIP) was formed under Executive Order 13010 to recommend a national strategy for protecting and assuring critical infrastructures. Eight critical infrastructure elements have been identified.

This paper provides an overview of tools necessary to conduct in depth analysis and characterization of threats, vulnerabilities, and interdependencies of critical infrastructure subsystems, and their interaction with each other. Particular emphasis is placed on research requirements necessary to develop the next generation of tools.

In addition to tools, a number of system level research suggestions are made including developing a system architecture, data flow models, national level resources, and a national test bed.

Introduction

Imagine the following events, occurring within a 24 hour period:

> On a hot summer day, power generation equipment in the Pacific Northwest is approaching capacity. Several momentary power disruptions occur, but power is restored using standard operating procedures. Suddenly, a major outage occurs on the main feeds from the Bonneville Power authority. Prior load sharing agreements result in power being added from adjacent grids; power disruptions suddenly occur on these as well. After a period of time, operators are slowly able to restore power to the bulk of customers.
>
> Shortly thereafter, a bank card processing facility in Delaware loses power. Emergency generators start to kick in, but they suddenly fail. The facility cannot process credit authorizations from retailers, resulting in financial loss of millions of dollars per hour.
>
> A freight train carrying toxic chemicals derails in Texas; clouds of toxic fumes rise into the air and a nearby town must be evacuated.

The FBI is called in and must make a number of determinations:

> Are these isolated events, or are they related?
>
> Are they a result of natural failure, or have they been orchestrated by a terrorist group or nation state?
>
> If they are the result of a deliberate act, what means can be used to identify and locate the perpetrators?

To conduct an analysis, the FBI will need a set of tools to augment their traditional methods. For example, would an "information attack" leave a forensic pattern that could be analyzed (like fingerprints, or residual chemicals)?

More importantly, how could an attack be avoided? Or if the result of faulty design, or natural hazard, how could system designs be hardened so that failures become increasingly rare. The purpose of this paper is to discuss the need for advanced tools for infrastructure protection.

The subject area is vast; this paper approaches the discussion by providing a general overview, develops a number of high level models, and then moves to a specific set of recommendations.

The example above identifies tools for law enforcement. Tools research must encompass a broader set of stakeholders including system designers, infrastructure operators, and the research community.

On the Need for Critical Infrastructure Protection

We are rapidly moving into an information based society; much of the nation's infrastructure is becoming dependent on information technology for both planning and operation. Concerns over the vulnerability of the infrastructure led to formation of the President's Commission on Critical Infrastructure Protection.

The Commission's charter is to examine eight identified infrastructure elements and to recommend protection strategies. The Commission recognizes that increased reliance on computer and communication systems exposes the infrastructure to new vulnerabilities. Of particular concern is the possibility of an orchestrated information attack. According to Commissioner Tom Marsh:

> "Technology is a bigger part of the problem — and the solution — than we originally thought. The main problem is a lack of tools with which to detect, identify, characterize and defend against attack, especially cyber attack."

The entire critical infrastructure is a complex, interdependent system of subsystems. The Department of Defense has developed an extensive methodology and set of tools for dealing with systems of systems; the current challenge is to draw on, improve, and develop new tools for application to the critical infrastructure.

A number of approaches to improving the critical infrastructure are being considered; the purpose of this paper is to examine the requirements for new and improved tools.

The nation's infrastructure is huge, ever changing, and has many interdependencies. This paper gives examples in many infrastructure areas; actual research emphasis will depend on prioritization determined from simplifying assumptions, architectural decomposition, and consequence analysis.

Lessons From the Pacific Northwest Power Outage

As an example of advanced tools requirements, consider lessons learned from a major power outage. Major outages occurred in the "Western System" on July 2 and August 10, 1996. Gerald Cauley and Karl Stahlkopf, in a report titled "Technical Issues Raised by the Western System Outages", examine reasons for the system failure and offer suggestions for follow up.

Cauley's and Stahlkopf's analysis suggests a number of causes of the outage. Among them they noted that while worst case analysis had been done, the particular scenario had not been studied. They also suggest that operators did not have all the data they needed to make proper decisions. Particularly notable was that no one could see the big picture across the entire system. The authors suggest that there is substantial improvement needed to the modeling process. For example, models used for planning are different than models used for online monitoring and control. Finally, there are thousands of system components, and as many problems waiting to occur.

Based on these observations, the authors suggest the following:

On line dynamic security assessment tools, and security indices.

Wide area communication network and system monitoring process.

National standards for operations and engineering.

Improved system planning and risk assessment methods.

Standard system planning and operating data models.

Validated data in simulation models.

Wide area measurement and controls.

A Proposed Taxonomy for Critical Infrastructure Tools

To develop a structured approach to analyzing tools needs, we postulate a set of analytic tools to assist in analysis and synthesis of critical infrastructures. Tool sets need to progress from component tools, to subsystem tools, to system tools to intersystem tools, as illustrated in Figure 1.

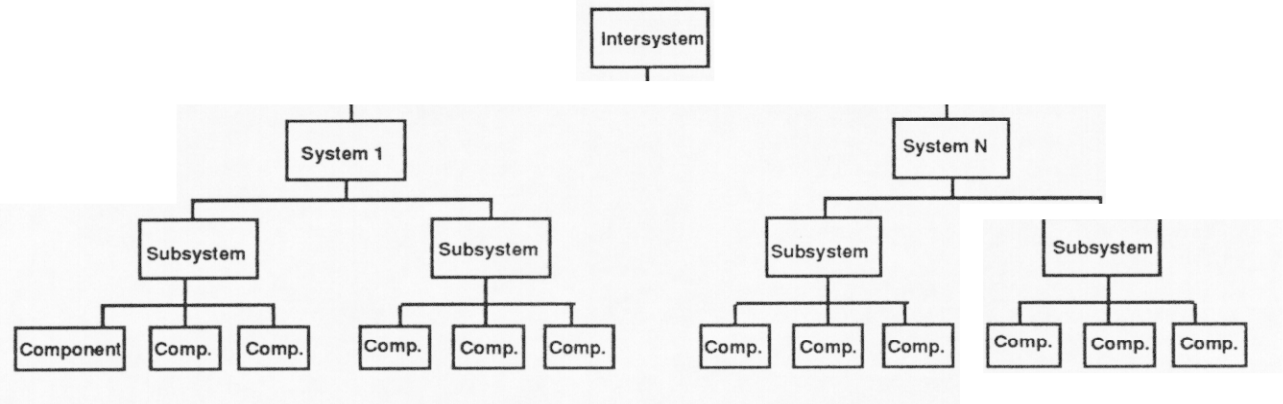


Figure 1 – Tool Taxonomy

In this taxonomy, we have taken the view of specific analytic tools to support each of the infrastructure elements. The notion of intersystem tools takes the taxonomy one step further, by postulating interactions among subsystems.

Returning to the example at the beginning of this paper, consider the tools necessary to detect an information attack. Table I below casts the proposed taxonomy in tabular from, and indicates tool requirements.

Major Area	Example	Tools
Intersystem	Electric power/communications	High fidelity simulation
System	Regional power grid	Electric fault analysis
Subsystem	Generation subsystem	Cooling system analysis
Component	Turbine control system	Control system security tools

Table 1

A Framework for Analysis

To meet the goal of having a robust set of tools for analyzing the critical infrastructure, it is useful to have a framework for analysis. One useful framework looks at system vulnerabilities, threats that can exploit these vulnerabilities, and consequences if the vulnerabilities are attacked.

For example, consider a water supply that is dependent on an open reservoir. The vulnerabilities in this system include bacterial and toxic contamination, reservoir leaks, and failure of the downstream water supply system. Threats that might exploit these vulnerabilities include both natural effects, natural disasters, and terrorist actions. Consequences of contamination could range from minor to severe depending on the population served, detectability, and availability of back up supplies.

What kind of tools are required? In the case above, an analyst needs to model how a bacterial or toxic contaminant would spread in the water supply, and in the reservoir. Required calculations include diffusion and lifetime.

The above material examines the vulnerability of a particular water supply. In the national context, the water system is a highly distributed system made up of independent subsystems. There appears to be no single point in which to attack the country's water supply. In the national context, the water supply is less vulnerable than the banking system (due to reliance on the communication infrastructure). Clearly, a prioritization based on national level consequences will be an important element in determining a research strategy.

Returning to the taxonomy of Figure 1, we are now in a position to expand the taxonomy. For example, at the system level a variety of tools are needed as illustrated in Figure 2.

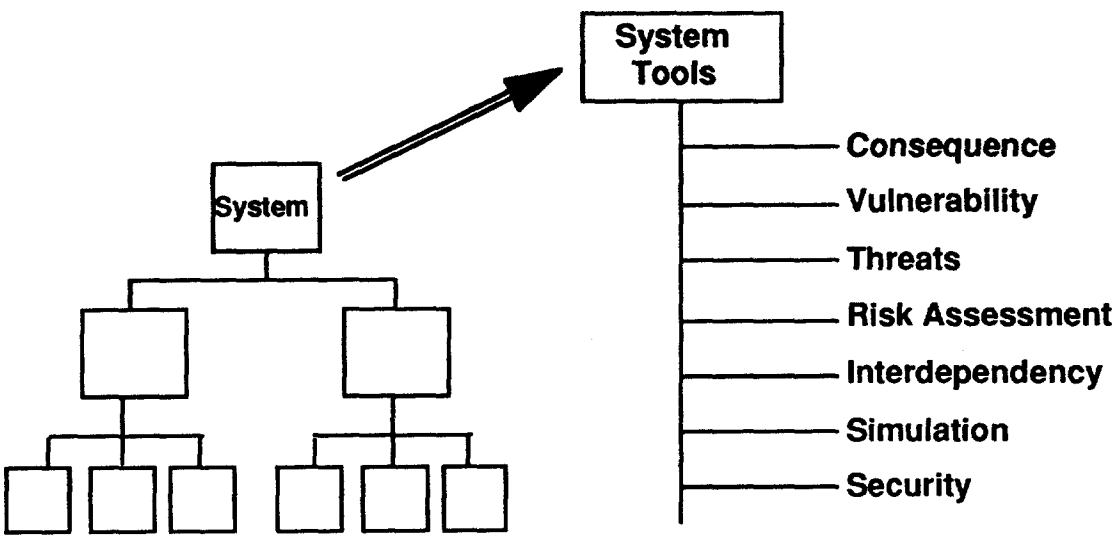


Figure 2 — Expanded Tool Taxonomy

Developing a System and Data Architecture

Viewing the nation's critical infrastructure requires understanding of the system architecture and the data flows. While there are many interdependencies, a rigorous decomposition can help identify critical dependencies and eliminate ones of little consequence.

Unfortunately, the infrastructure grew rather than being designed. More important, the infrastructure is not static, but undergoes continuous change.

An adaptable, as built, system architecture must be developed. A method of identifying critical nodes, links, and dependencies is required. This architecture must be used to develop a common language, thus enabling the research, operational, legal, and other communities to communicate.

Further, a set of standards will be required to understand data flows, communications, interfaces, and models. While a challenging task, architecture development will simplify and standardize many other research tasks.

Tools Research -- Developing a Strategy

This paper assumes that component and subsystem level tools are under continuing development, and will continue to be improved as necessary. The focus of new tools research should be on high payoff technical and policy tools that will help strengthen the critical infrastructure.

One method of approaching this problem is to examine the issues from back to front. (In all likelihood, the process described here needs to be fully automated, a true research challenge.)

Consequences: Begin by looking at eight critical infrastructures to determine failure scenarios that have the greatest consequences. Would losing the country's financial transaction system, or the nation's transportation system be more severe? Since electric power is required to operate portions of both of these, would failure of the electric system have the highest consequence. As with all tools described in this paper, they must have the capability to rapidly and automatically update themselves as the infrastructure itself undergoes continuing evolution.

Vulnerability: Next, examine the vulnerabilities of the systems with the highest consequence of loss. Are natural hazards, or weardown from routine use the largest vulnerability? How vulnerable is the system to computer attack? To information overload?

Threats: Next, identify threats that can attack these vulnerabilities. Are the threats natural hazards, or are they human induced? If human (for example, a computer attack), what are the motivations? Are the threats credible?

Risks: Formal risk assessment methods must be used to examine the threats, vulnerabilities, and consequences. This will help develop the high priority research requirements.

The analysis above moves from consequence to vulnerability to threat. A complementary analysis is also required; this starts with threats, examines their credibility, then analyzes vulnerabilities and consequences.

Application of the framework in the manner described above helps prioritize research requirements among the infrastructure elements, and for some scenarios.

Suggestions for Research

The subsections below suggest tools research in a number of subcategories. These suggestions are by no means complete, but are designed to enable a healthy debate.

Component and Subsystem Tools

For the purpose of critical infrastructure protection, we suggest that primary emphasis be on system level tools. Component and subsystem tools need improvement, and are under continuing development. However, efforts at the component and subsystem levels that can address security vulnerabilities and interdependencies should be accelerated.

System Tools

It is likely that tools at the systems level will need improvement. For example, the electric power grid used to be constrained to separate subsystems. Analytical tools (power transient analysis) were capable of dealing with these subsystems. As deregulation causes systems to be interconnected, tools must be improved.

Systems Analysis — A set of advanced, automated, systems analysis tools are needed to understand vulnerabilities, risks and consequences of failure of a component, subsystem, or system. As an example, consider an automobile tunnel as an element of the transportation infrastructure.

Questions to be answered include identifying the vulnerabilities of the tunnel (high explosive attack, fire, electric attack on the ventilators, etc.), determining the risks or probability of attack for the various vulnerabilities, and examining the consequences of each attack. Because the country's infrastructure is so large, tools must be developed that can carry on these analyses in an automated way.

Specific research issues to be addressed:

1) Can an automated mapping process build a high fidelity network model? If so, to what level of detail?

2) How can the specific configuration of a subelement be automatically determined?

3) How can the operating condition of a subelement be determined?

Electric Power — Existing tools must be improved to allow country level modeling of the power grid, with particular emphasis on interconnections and fault analysis. The work of Cauley and Stahlkopf, previously cited, provides an additional insight into requirements.

Security Tools

With respect to other infrastructures, our computer communications systems are relatively immature. Further, the complexities of software, and the difficulty of validating software and hardware combinations, implies an increased need for computer tools of all kinds. Examples of needed research include more robust authentication, intrusion denial and/or detection, and forensics.

The need for advanced security tools is being developed in a number of forums. For example, DARPA is co-sponsoring a workshop "Research for Critical Infrastructure Assurance", July 9-11, 1997. Major research themes examined in this workshop are:

Indications and warnings
Intrusion detection
Probes, monitors, sensors

Preliminary results from the DARPA workshop will be available for further discussion.

Computer security experts suggest that the most important steps in securing systems from attack are to have appropriate authentication mechanisms, coupled with authorization tools. Current systems have rather weak security that works by a user supplying a password, then the system authenticating via this password. Many advanced mechanisms have been developed to strengthen the password schemes (e.g., Kerberos), but they are not in routine use.

Strong authentication must come into common use — employing a biometric will likely form the basis of this technology. Note that while an individual organization may employ strong authentication, there has been little work on hierarchical authentication. For example, Company X may have strong authentication, it may interact electronically with Company Y. But little research has been done on the interconnection of these systems; while certification systems for electronic commerce are coming into use, how will system certification be accomplished for tiered systems interacting with each other?

Once authenticated, users must be authorized for multiple services. Research to strengthen authorization will generate a new set of tools. Methods to authorize over multiple networks are also required.

As evidenced by monthly reports of security flaws in commercial software, there are many security "holes". Further, commercial pressure to release software as quickly as possible has led to rapid product turnover, and less than desirable attention to software quality. What means can be taken to reduce software problems, including introduction of undesirable security holes? How can software be certified secure? How can software releases be synchronized so that security is as up to date as

possible? All of these are challenging solutions, and will require serious work as we attempt to build solid, secure networks.

On a separate track, research is needed on tools for intrusion detection, indications and warnings, and forensics in case of attack. Current indications and warning systems work on known attack patterns. How to move this work forward so that it can keep up with rapid changes is a very important task.

Current information security professionals stress forensics are an essential element in understanding patterns and assessing future trends. Research is needed to automate forensics to be able to handle increasing volumes of data.

Professor Nick Bambos has suggested the following set of high priority research topics:

- Design of security-minded/fault-tolerant/gracefully-degrading network architectures.
- Design "smart firewalls" that provide adaptive, flexible computer network security management.
- Design of expert systems and intelligent software agents for detecting/tracking unauthorized intruders and security holes.
- Develop systematic methodology to allow the evaluation of security risk exposure for distributed/networked/interconnected computer systems and the cost/benefit elasticity of various measures. That requires
    - — Developing engineering and policy concepts and principles for computer network security management.
    - — Developing canonical models for security in computer networks.
    - — Developing analytical methods for studying the models.
    - — Deploying a large scale simulation platform for evaluation of secure network architectures.
- Develop benchmarks for system security.
- Develop standards for secure systems. Set up standard committees.
- Set up national/state centers with teams of experts to record-track-analyze-evaluate reported computer network security breaches.
- Set up national repository of data/information/methods regarding computer network security.
- Deploy large scale physical computer network testbed for research into computer network security.

Intersystem Tools

From a consequence viewpoint, scenarios that result in dire events are the ones that need most attention. Tools must be developed that allow modeling and simulation of the infrastructure, with the goal of obtaining consequences of failure. A ranking methodology that finds likely scenarios with very high consequences can be used to prioritize research.

Infrastructure Simulation and Modeling — A tool that can simulate complex, highly interdependent systems is needed. The tool should be capable of country-wide modeling Underlying models must provide high fidelity. Because the infrastructure is constantly changing, the tool must adaptively reconfigure itself.

The difficulty of this task must not be underestimated; earlier in this paper we noted the need for architectural decomposition and simplification. If undertaken, the overall modeling task will be simplified.

As evident from the discussion above, there are a wealth of component, subsystem, and system level tools available for each of the infrastructure elements. However, there are few, if any, tools that will address the linkages between systems, and provide an analytical capability for systematically investigating interdependencies. As an example, various water supply systems may depend on electricity and computers to operate remote pumps. The computers themselves are dependent on electricity. Computers may have back up power for emergencies, which itself is dependent on fuel reserves. Replenishing the reserves is dependent on the oil and gas distribution system.

Fully analyzing an attack and defense scenario involving the water supply, then depends on the ability to investigate the interdependencies noted above. The interdependency problem requires high priority when developing a critical infrastructure research portfolio.

Databases, Libraries, Resources

A national repository for critical infrastructure tools, models, and data could play an important role in speeding infrastructure protection and reaction. In this repository one would have a validated set of analytical tools, and to the extent possible, a validated set of analytical models. For example, after the World Series earthquake, LLNL was involved in modeling the San Francisco Bay Bridge and the Cypress structure. We considered our codes to be state of the art, but they were not the type employed by the state highway people, thus resulting in distrust of our results. Further, the lack of a validated model resulted in substantial time and effort to build and validate a model.

As another example, there was a "gate" failure at the Folsom Dam within the last year. There was a question directed at finding all like gates at other dams in the country. A national repository could be of great value during the response phase of a national crisis.

The repository must contain many other elements. For example, the need to share "incident" data is often cited. Elements of the national repository might include:

- Validated analytical tools
- Validated analytical models
- Graphical information system (GIS) with location and model information of infrastructure elements
- Threat, vulnerability, consequences models
- Lessons learned data

A Critical Infrastructure Test Bed

Whether employing existing commercial tools, or developing new ones, there is an urgent need to test these tools in a repeatable way. There will be few circumstances when you can afford to test on a live system (e.g. — you don't want to launch a virus on a banking and finance system in order to test virus detection tools).

Ultimately, threats and vulnerabilities need to be tested on a working test bed, and research results that project hardening also need to be evaluated. Due to the expense of such a test bed, consideration must be given to developing a virtual test bed; in addition, there will be a need for several test beds distributed throughout the country that can be accessed by researchers and implementors.

Setting the Research Agenda

This paper discusses a broad range of research topics, essential to providing a long term improvement in protection of the critical infrastructure. From a wealth of research topics, it is essential to focus and prioritize. Extensive discussions with experts from academia, government, industry, and research laboratories suggests three topics of very high priority and with potential of major impact. These topics have been discussed in detail above:

- *Simulation and modeling* – with particular emphasis on complex, highly interdependent systems.

- *Critical infrastructure testbed*

- *National repository* – designed to house validated models and tools

Conclusion

This paper has proposed a tools taxonomy for defining requirements for the critical infrastructure. A number of tools have been discussed with emphasis on modeling and simulation and testing.

The infrastructure is a coupled system of systems. Tools that handle interdependencies will be a critical element.

The paper has postulated a national repository and discussed elements to make it work.

APPENDIX:

Infrastructure Protection Vugraphs

Tools for 21st Century Infrastructure Protection

Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda

Stanford University

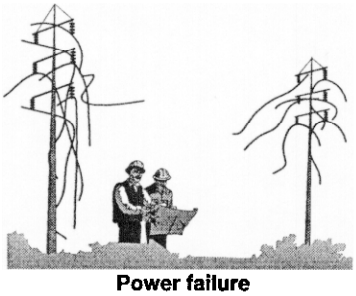
Stan Trost
Lawrence Livermore National Laboratory

July 21, 1997

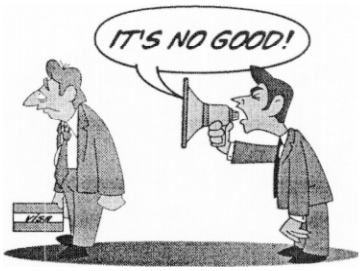
Some views on infrastructure protection

Hardware Vendor	—	**Lid Lock 2000 will prevent your PC's chips from being stolen.**
Hardware Vendor	—	**Secure cable trap prevents theft of mouse, keyboard, speakers, more.**
Firewall Vendor	—	**". . . All functions are denied except those which are allowed."**
Sage	—	**"Why don't we have a market in electronic security that rivals that in physical security?"**
Tom Marsh	—	**"Technology is a bigger part of the problem — and the solution — than we originally thought. The main problem is a lack of tools with which to detect, identify, characterize and defend against attack, especially cyber attack."**

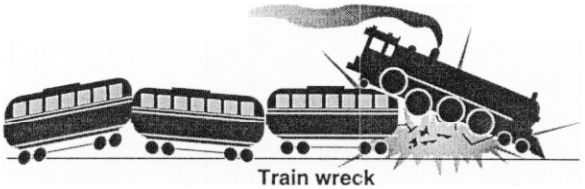
Infrastructure failures can have a wide rage of consequences.



Power failure



Bank processing center

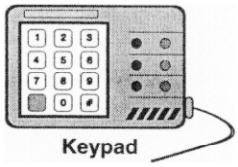


Train wreck

Page 3

How will we change our tools to meet new challenges?

Locks



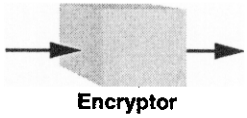
Keypad

Fences

Firewall

Chains

Old



Encryptor

New

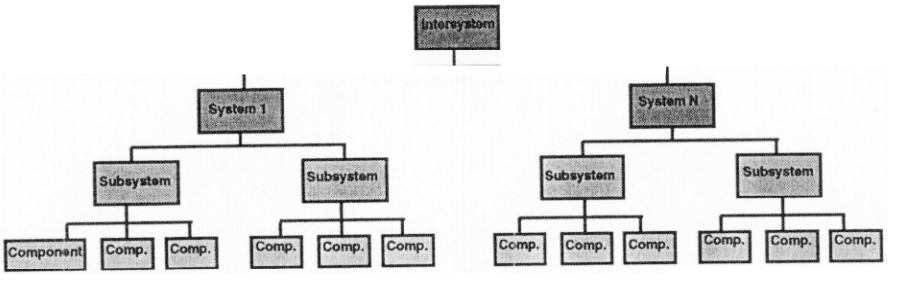
Page 4

Lessons learned are an important element in future planning

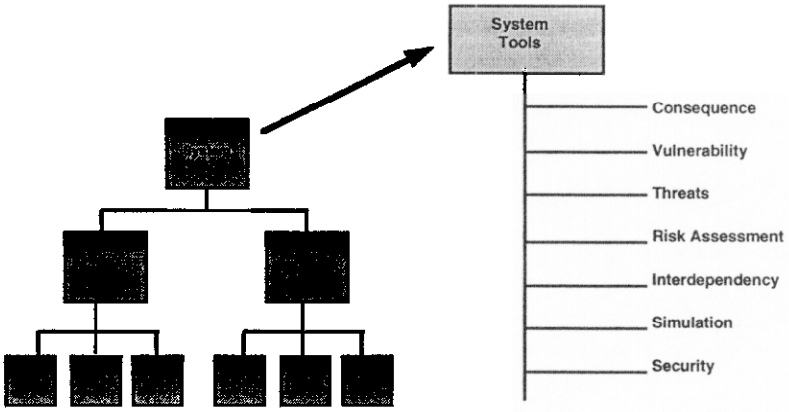
Example: Pacific Northwest power outage

- On line dynamic security assessment tools, and security indices.
- Wide area communication network and system monitoring process.
- National standards for operations and engineering.
- Improved system planning and risk assessment methods.
- Standard system planning and operating data models.
- Validated data in simulation models.
- Wide area measurement and controls.

A detailed tool taxonomy can highlight research requirements



Research continuously improves subsystem and component level tools. New research should be targeted at the system level



Page 7

Large scale interconnected systems require new analytical tools.

- **Current network tools model performance. Few tools model consequences of failure.**
- **Network topologies are dynamic. Models must reconfigure themselves to match the physical environment.**
- **Risk analysis techniques must handle an unprecedented number of variables.**
- **Complex software is being developed and marketed with inadequate attention to quality.**
- **Security and performance "holes" are de riguer.**

Design, testing, and assurance of large systems is very difficult. Fundamental research is required.

Page 8

Six major areas for high leverage research are proposed.

- **System level tools.**
- **Component and subsystem tools.**
- **Intersystem tools.**
- **Computer network security tools.**
- **A national critical infrastructure repository.**
- **A critical infrastructure test bed.**

Due to workshop time constraints, I focus on the three items in red.

Page 9

Intersystem Tools - research challenges

- **Tools must be developed that allow modeling and simulation of the infrastructure, and its interdependencies, with the goal of obtaining consequences of failure.**
- **Can tools automatically map the physical network to build an accurate model in real time.**
- **Can a tool provide country-wide modeling.**
- **Can tools address the linkages between systems and provide an analytical capability for systematically investigating interdependencies.**

Page 10

Databases, Libraries, Resources

- National repository for tools, models, and data could play an important role in speeding infrastructure protection and reaction.
  - Validated analytical tools
  - Validated analytical models
  - Graphical information system (GIS) with location and model information of infrastructure elements
  - Threat, vulnerability, consequences models
  - Lessons learned data

Key challenge: Can the repository itself be secured??

Page 11

A Critical Infrastructure Test Bed

- Urgent need to test tools in a repeatable way.
- Threats and vulnerabilities need to be tested on a working test bed.
- Research results that project hardening need to be evaluated.
- Consideration must be given to developing a virtual test bed.
- Several test beds distributed throughout the country that can be accessed by researchers and implementors.

Page 12

Conclusion: a wealth of research opportunities exist. Three high priority proposals for this workshop are:

- Intersystem tools.
- A national critical infrastructure repository.
- A critical infrastructure test bed.
- Breakout session questions (for each proposal):
  - Succinct research description
  - Identify research challenges
  - Impact of doing research
  - Suggested approach

Page 13

Conclusion: a wealth of research opportunities exist. Three high priority proposals for this workshop are:

- Intersystem tools.
- A national critical infrastructure repository.
- A critical infrastructure test bed.
- Breakout session questions (for each proposal):
  - Succinct research description
  - Identify research challenges
  - Impact of doing research
  - Suggested approach

Page 13

Technical Information Department • **Lawrence Livermore National Laboratory**
University of California • Livermore, California 94551