



# Survivability –

## A New Security Paradigm for Protecting Highly Distributed Mission-Critical Systems

**Howard F. Lipson, Ph.D. <hfl@cert.org>**  
**CERT<sup>®</sup> Coordination Center, SEI-CMU**

**Workshop on Electricity Security and Survivability**  
**November 28-29, 2001**  
**Carnegie Mellon University**

**This work was sponsored in part by the U.S. Department of  
Defense and the Advanced Technology Institute**

**© 2000, 2001 by Carnegie Mellon University**

CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office



# Outline

**Survivability Concepts**

**Research Approaches**

**Research Issues**



# What does Internet survivability have to do with protecting electric power systems?

- 1. Electric power systems are becoming increasingly dependent on open, unbounded, networked information systems, such as the Internet.**
  
- 2. Characteristics of the electric power system are becoming more like those of the Internet.**



# The Problem

**We are increasingly dependent upon large-scale highly distributed systems**

- defense
- telecommunications
- banking and finance
- transportation
- e-commerce
- ***energy: electric power***



## The Problem (2)

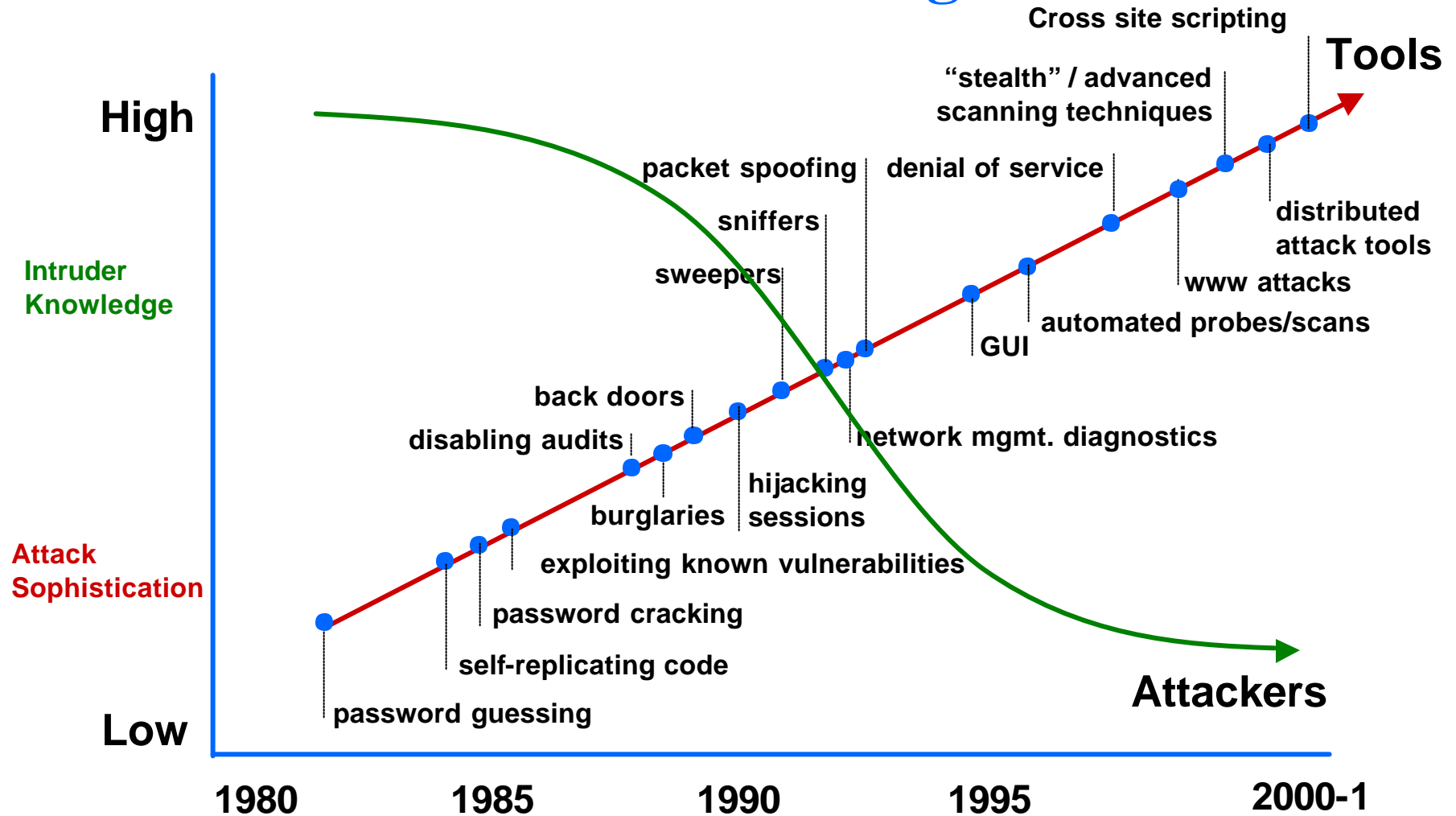
**Large-scale highly distributed systems cannot be totally isolated from potential intruders.**

**No amount of system “hardening” can guarantee that such systems are invulnerable to attack.**

**Serious consequences of system compromises and failures**

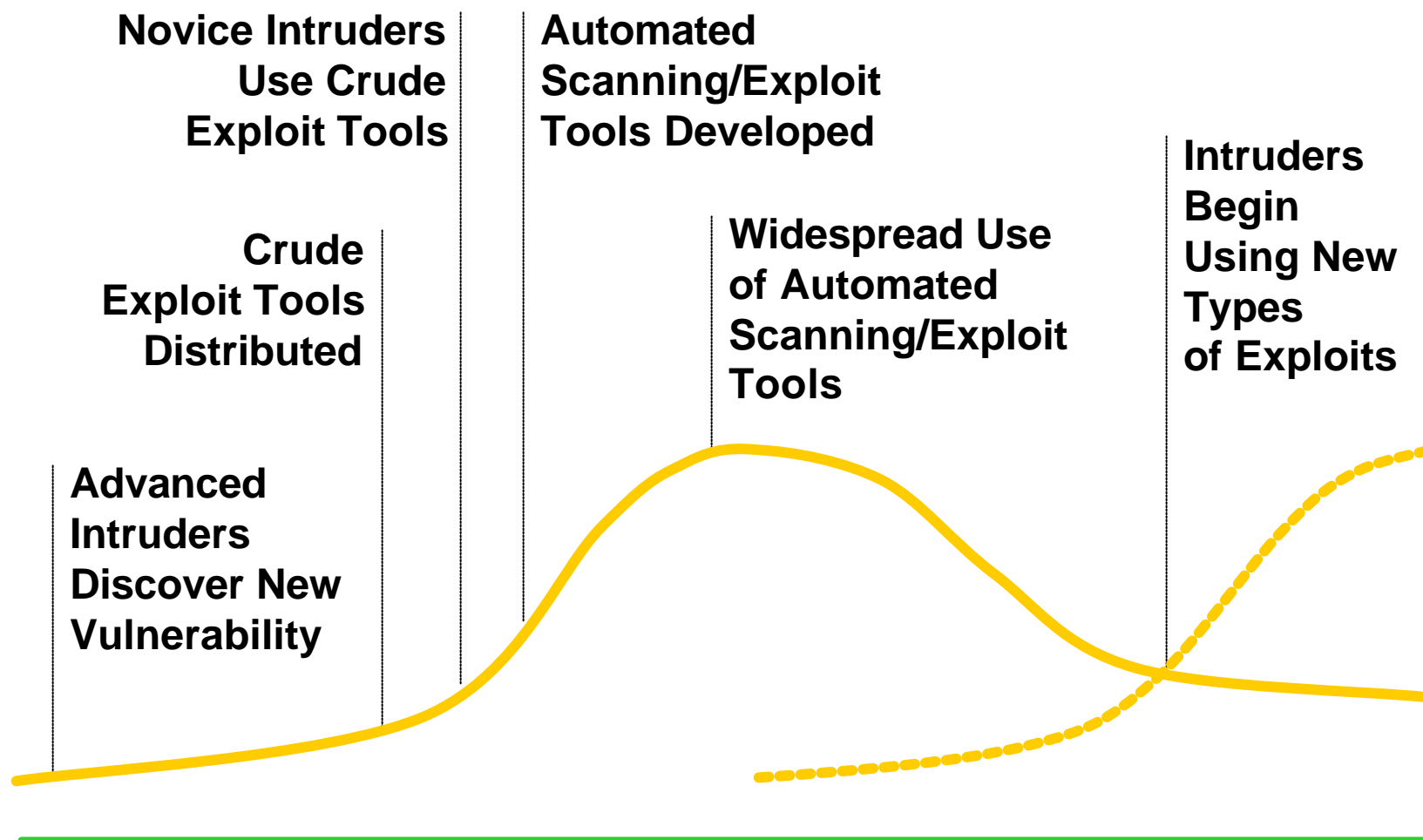


# Attack Sophistication vs. Intruder Technical Knowledge





# Vulnerability Exploit Cycle





## In the beginning . . .

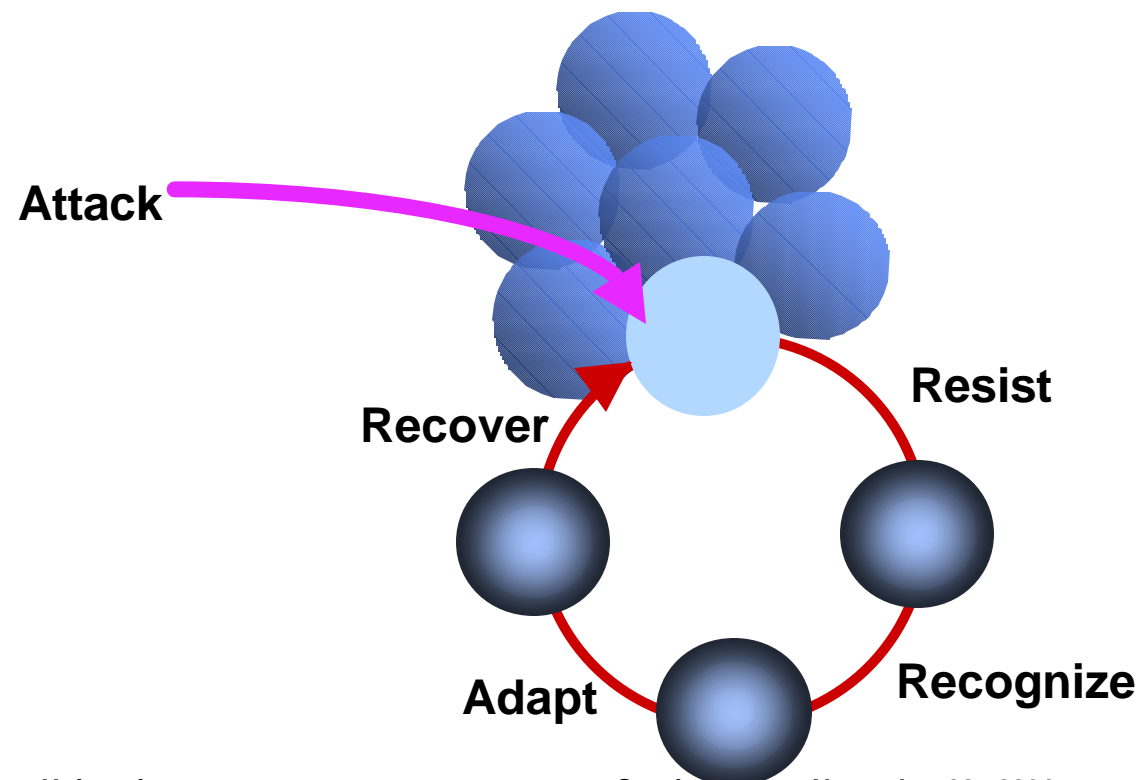
**“Can we build DoD systems that will continue to operate despite a successful cyber-attack?”**

**DARPA (Survivability Program)  
Late 1995, early 1996**



# Survivability

***Survivability*** is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.





## 3 R's of Survivability

### **Resistance**

**ability of a system to repel attacks**

### **Recognition**

**ability to recognize attacks and the extent of damage**

### **Recovery**

**ability to restore essential services during attack, and recover full services after attack**



## For Short-term Survivability

Deal with the effects of a crisis: **Car rounding a sharp curve is about to veer off cliff.**

A guardrail is a “survivability solution”, whether the underlying cause is:

- Ice on the road
- Drunken driver
- Brakes have been tampered with

For long-term survivability: **Do the forensics!**



# For Long-term Survivability

**System adaptation and evolution is essential,  
because ...**

- **New vulnerabilities are discovered**
- **New attack patterns appear**
- **Continual attacker-defender escalation**
- **Underlying technologies change**
- **Collaborators become competitors**
- **Political, social, legal changes**
- **Missions evolve, or change drastically**



# Traditional Assumptions for Information Security

- **Clearly defined boundaries**
- **Central administrative control**
- **Global visibility**
- **Trustworthy insiders**



# The New Computing Environment Changes Everything

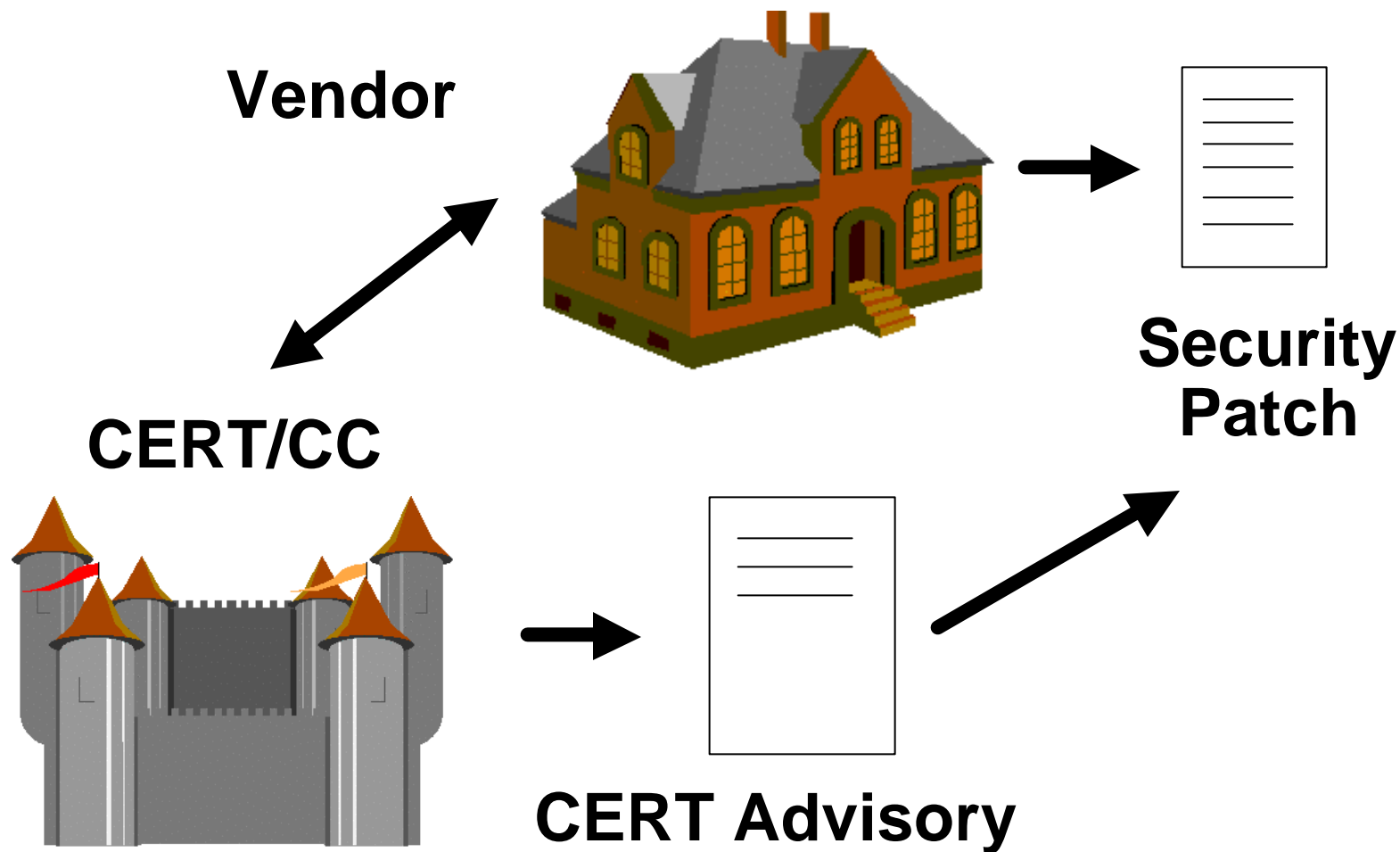
- **Open, highly distributed systems**
- **Boundaries are ill-defined (complex physical and logical perimeters)**
- **No central (or unified) administrative control**
- **No global visibility**
- **Untrustworthy insiders**
  - **includes incomplete and imprecise information about software: COTS, Java applets, Active X controls, etc.**
- **Unknown participants**
- **Large scale, coordinated attacks**
- **Survival at risk**



# **An Example of the Security Impact of the New IT Environment**

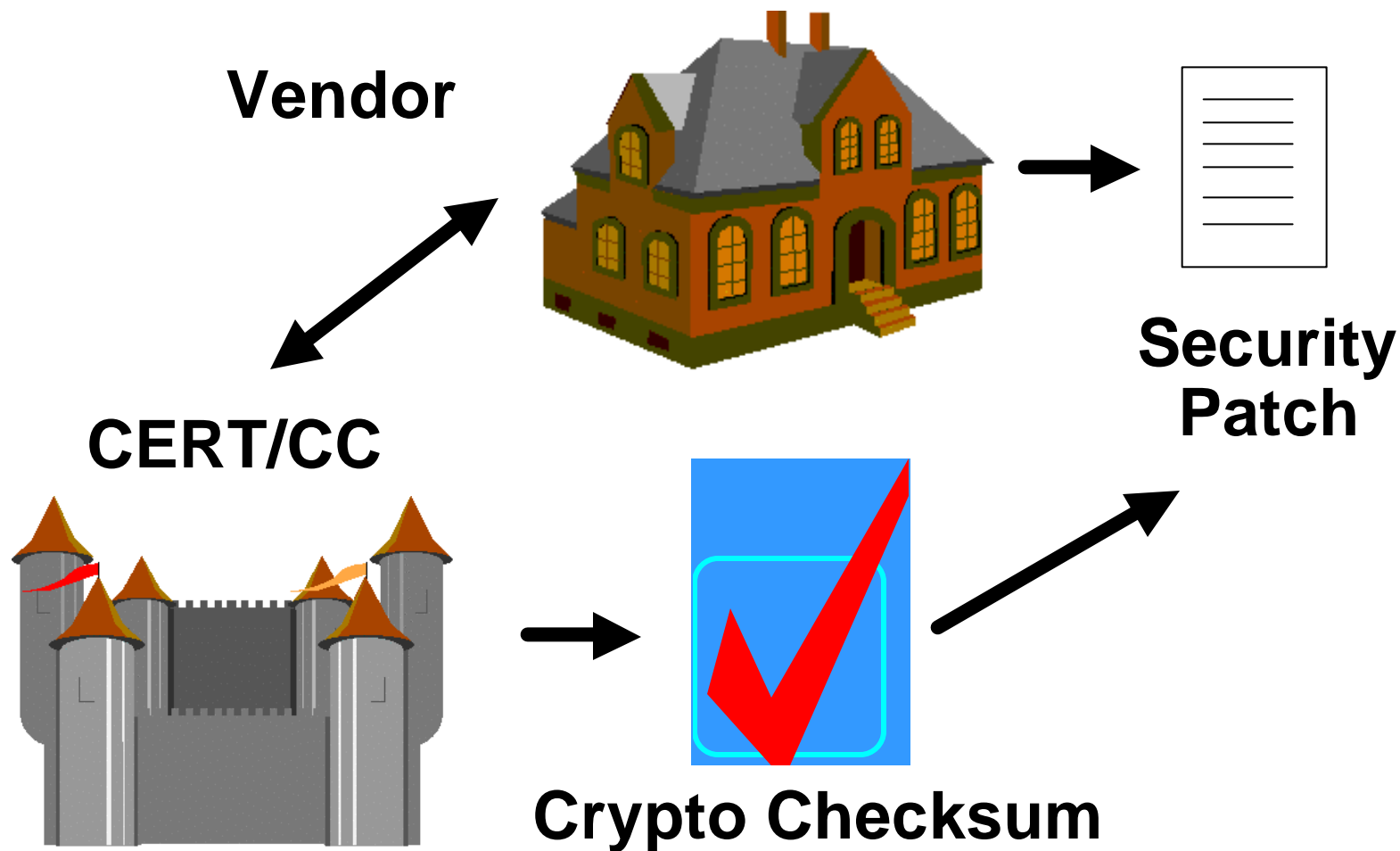


# Security Advisory Process



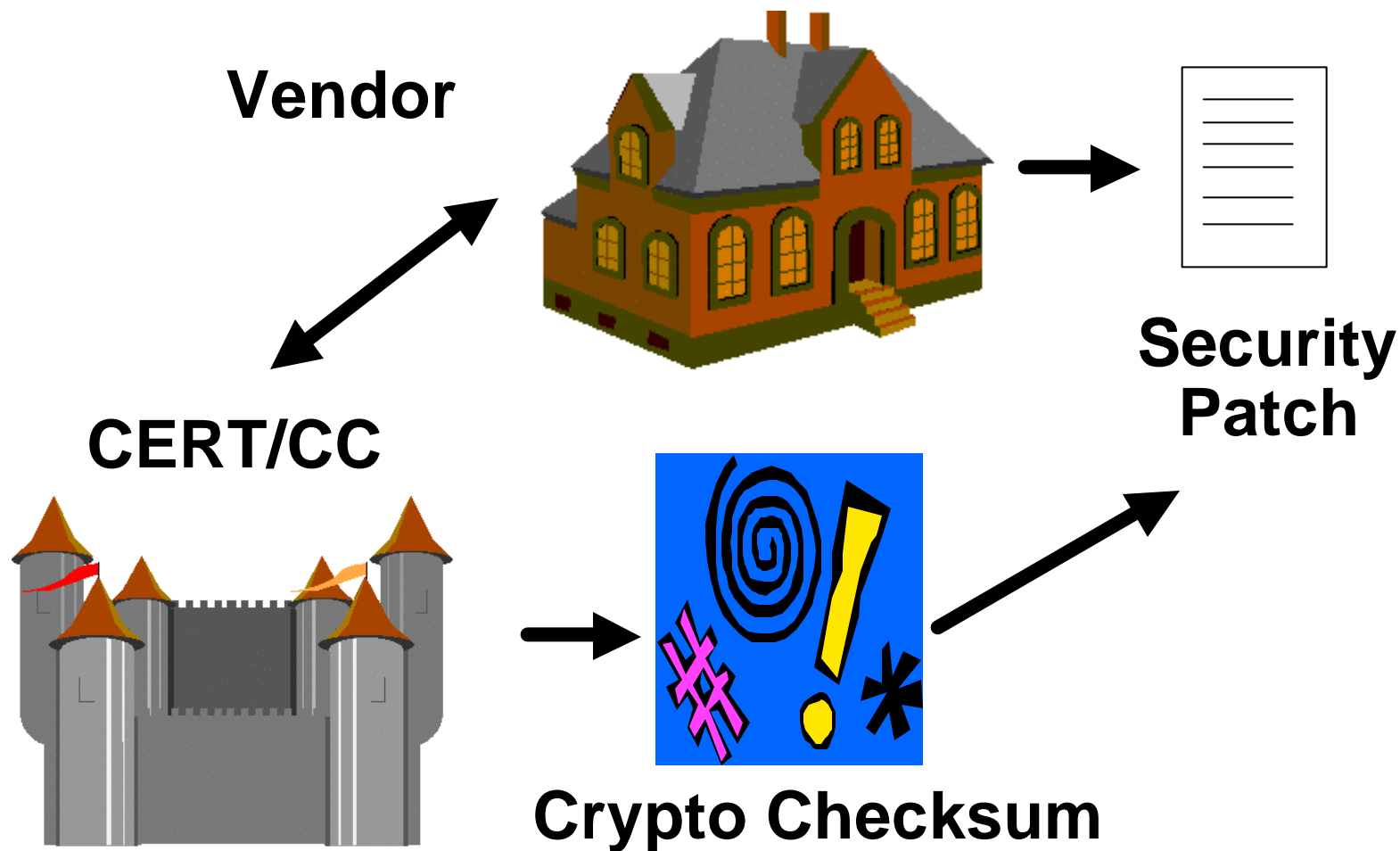


# Security Advisory Process



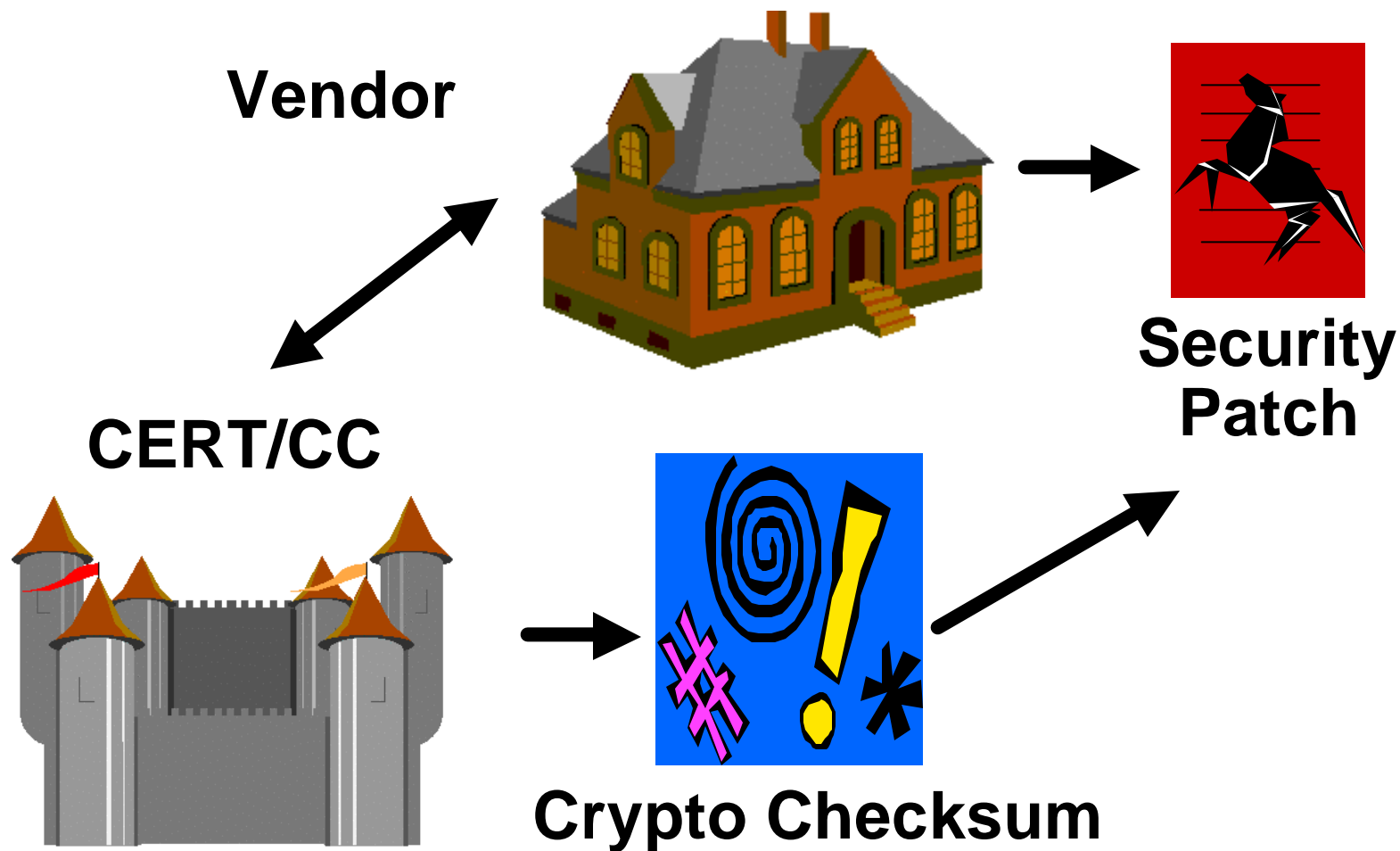


# Security Advisory Process





# Security Advisory Process





# Unbounded Systems

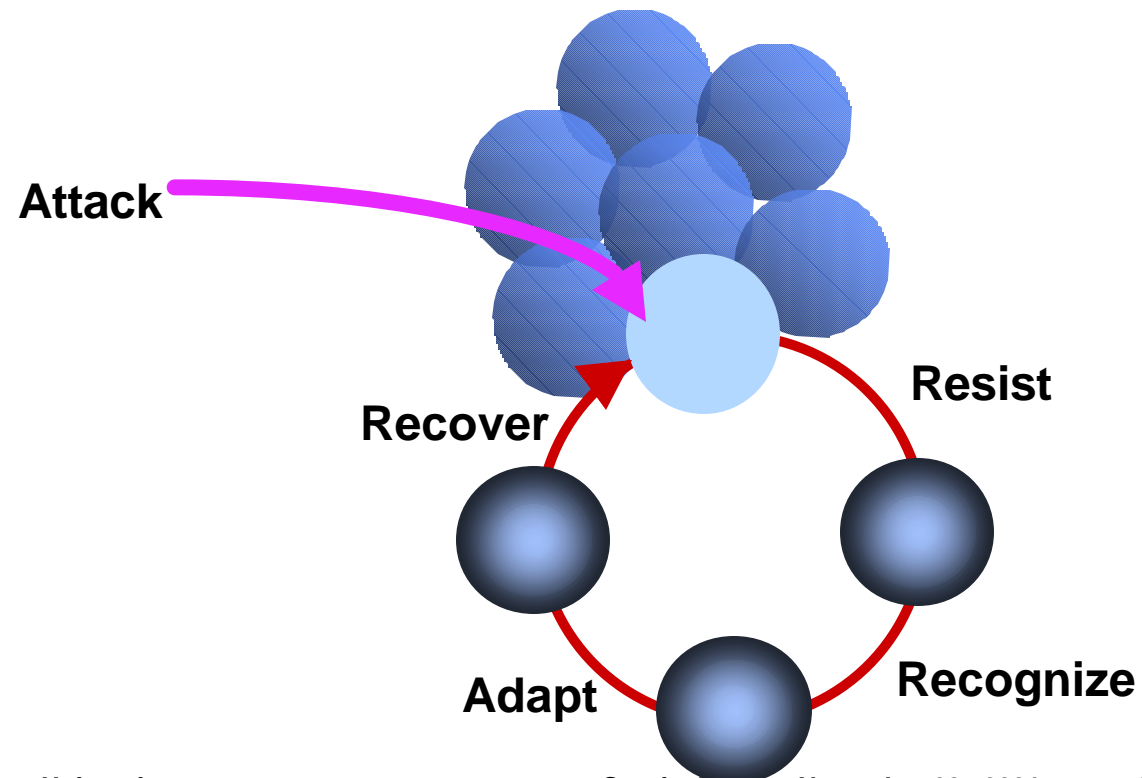
- **No unified administrative control**
- **No global visibility**
- **Untrustworthy insiders**
- **Lack of complete, timely information**

**Sound like the U.S. electric power system?**



# Survivability

***Survivability* is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.**





# Fundamental Assumption

**No individual component of a system is immune to all attacks, accidents, and design errors.**



## Fundamental Goal

**The mission must survive.**

- **Not any individual component.**
- **Not even the system itself.**



# Mission

**A very high level statement of  
context-dependent requirements:**

- (1) Req'ts under normal usage**
- (2) Req'ts under stress**



# Example: Mission of the Titanic

**Under normal conditions:**

**Luxurious transatlantic transportation**

**Under stress:**

**Buoyancy**



# Mission of the US Electric Power Industry **Under Deregulation**

**Reliably and profitably**  
generate and supply electricity wherever and  
whenever it is needed in North America.



## Other Definitions of Survivability

**What's wrong with the following definitions?**

- **A survivable system is one that functions correctly despite attacks.**
- **A survivable system is one that continues to operate in the presence of a successful attack.**
- **Survivability is the ability of a system to maintain a set of essential services despite the presence of abnormal events such as faults and intrusions.**



# Survivability Requirements

## Mission-critical functionality

- (alternate sets of) minimum essential services
- graceful degradation of services

## Mission-critical software quality attributes

- security, safety, reliability,  
performance, usability

## Requirements for the 3 R's and evolution



# Management Perspective

## Security

**Increase the cost of compromise beyond the value to an attacker**

**Industry standard practices**

**What's it gonna cost me?**



## Management Perspective (2)

### Survivability

**No individual component of a system is immune to all attacks accidents, and failures.**

**Business risk management**

**Allocate budget across the 3 R's**



# The New Paradigm – Survivability versus Security

**Security is a technical specialty that provides generic solutions that are largely independent of the mission being protected.**

**Survivability is a blend of security and mission-specific risk management.**

**Survivability solutions require participation from all aspects of an organization: technical and business.**



# Some Techniques & Methods

## Security

- **Fortress model: firewalls, security policy**
- **Authentication, access control (insider trust)**
- **Encryption**
- **Intrusion detection (recovery secondary)**
- **Auditing, integrity checking, monitoring**
- **Success criteria:**
  - **binary: attack succeeds or fails**
  - **follow industry standard practices**



## Some Techniques & Methods (2)

### Survivability

- Security techniques where applicable
- Diversity, redundancy
- Trust validation
- Recovery (largely automated)
- Mission-specific risk management
  - includes contingency (disaster) planning
- Emergent algorithms
- Success criterion:
  - mission fulfillment
    - graceful degradation
    - essential services maintained
- Solutions can transcend the system



# Characteristics of Survivability

**Survivability is an *emergent property* of a system.**

**Desired system-wide properties “emerge” from local actions and distributed cooperation.**

**An emergent property need not be a property of any individual node or link.**



# Survivability Research Approaches

**Survivable Network Analysis Method**

**Emergent Algorithms**

**Survivable Systems Simulation**

**Survivability Requirements of Critical Infrastructures**

**Flow-Service Quality / Intrusion Awareness / V-RATE**

**Information Survivability Workshops**



# Survivable Network Analysis

- **Understand survivability risks for your system:**
  - What system services must survive attacks, accidents, and failures?
  - What architectural elements aid in resistance, recognition, and recovery?
- **Identify mitigating strategies:**
  - What architecture changes can improve survivability
  - Which changes have the highest payoff?



# Survivable Network Analysis Map

Intrusion Scenario	Softspot Effects	Architecture Strategies for →	Resistance	Recognition	Recovery
(Scenario 1) ...		Current			
		Recommended			
(Scenario n)		Current			
		Recommended			

Defines survivability strategies for the three R's based on intrusion softspots

Relates survivability strategies to the architecture

Makes recommendations for architecture modifications

Provides basis for risk analysis, cost-benefit trade-offs



# Vigilant Healthcare System – Survivability Map (Case Study)

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
An unauthorized user corrupts the DB leading to loss of trust in all validated TPs by all providers.	<b>Current:</b> Security model in DB protects TPs against corruption.	<b>Current:</b> None, except when a provider happens to recognize a corrupted TP.	<b>Current:</b> Locate an uncorrupted backup or reconstruct TPs from scratch.
<b>Softspot:</b> Treatment Plans	<b>Recommended:</b> Implement live replicated DBs that cross check for validity (supported by many DBs) [5]	<b>Recommended:</b> Add and check crypto-checksums on TPs in the DB. [3, 4]	<b>Recommended:</b> Reduce the backup cycle to quickly rebuild once a corrupted DB is detected. [5]



**Our next approach is based on our  
earlier observation . . .**

**Survivability is an *emergent property* of a system.**



# Emergent Algorithms

**Simple Local Actions**

**+ Simple Near Neighbor Interactions**

**=> Complex Global Properties**

**Autonomous distributed agents**

**such that if sufficiently many act as intended,  
desired global properties will emerge.**

**Distributed computations**

**that fulfill mission requirements by exploiting  
the characteristics of unbounded systems.**



## Emergent Algorithms (2)

### Produce emergent properties

- exist globally, but not necessarily locally

### Self-stabilizing

- converge to required functionality and non-functional global properties, even when corrupted

### Genetic

- can self-optimize for survivability and efficiency



## Emergent Algorithms (3)

### Cooperation with little coordination

- make best use of available information and resources
- anticipate needs of others
- no central control nor global visibility

### Holographic

- all parts contribute wherever needed
- no individual part is essential



## **Emergent Algorithms (4)**

**Produce global effects through cooperative local actions distributed throughout a system.**

**Provide solutions to survivability problems that cannot be achieved by conventional means.**

**Are well suited to**

- **systems with highly dynamic structure**
- **systems that must adapt or evolve in response to changing conditions**
- **unbounded networks**



## Emergent Algorithms (5)

**Early results with an emergent algorithm for message routing in an unbounded network:**

- **demonstrate feasibility**
- **demonstrate cost-effectiveness with respect to performance and storage costs per node.**



# Survivable Systems Simulation

## Easel — Emergent Algorithm Simulation Environment and Language

### Research Goals:

- **Advance scientific knowledge of survivable systems**
- **Improve survivability of mission-critical systems**
- **Provide tools and methods for survivability engineering**



## Easel Objectives

- **Create a testbed for mission-critical applications and systems.**
- **Allow stakeholders to visualize the effects of specific cyber-attacks, accidents, and failures on a given system or infrastructure.**
- **Allow stakeholders to visualize and study cascade effects.**

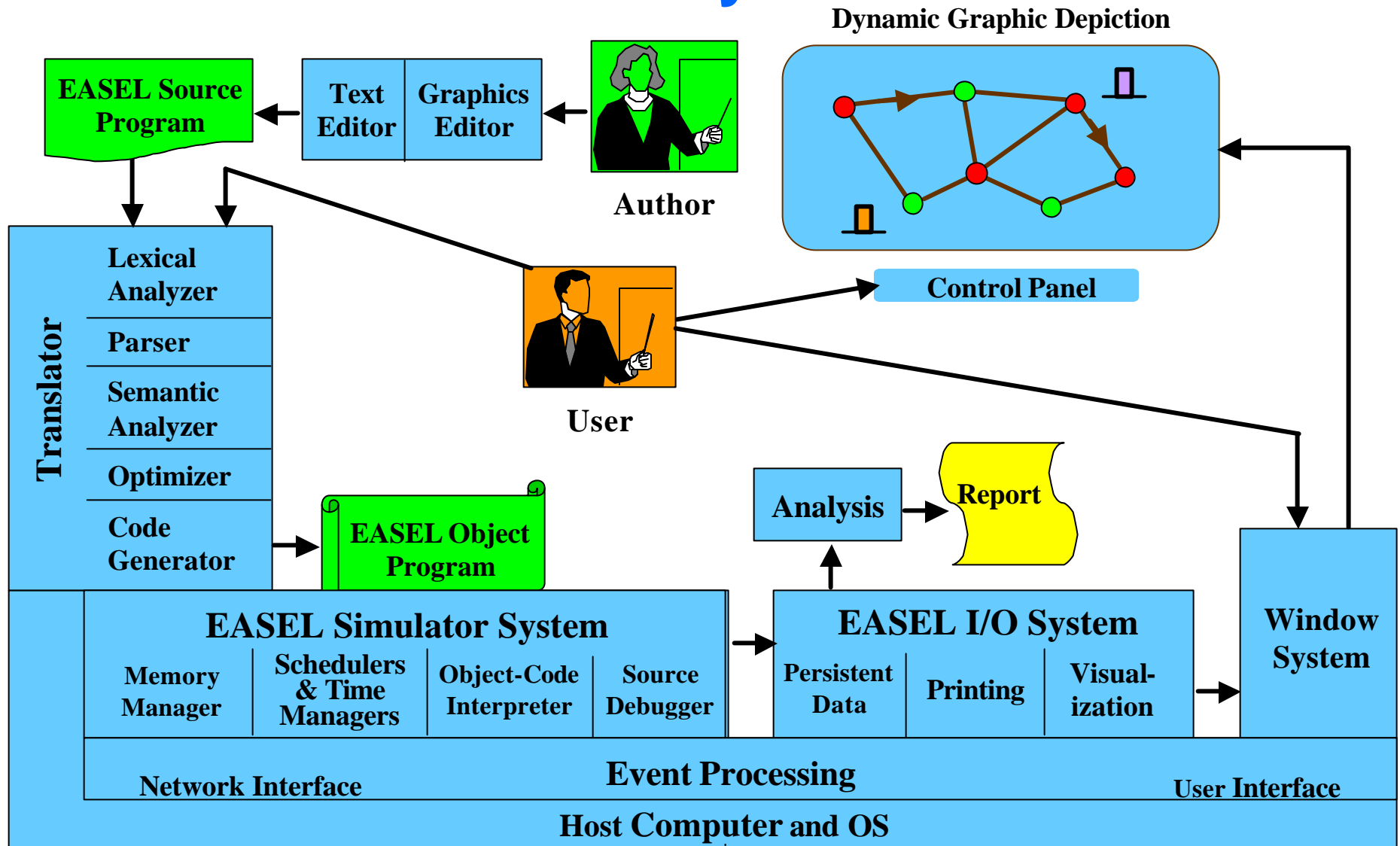


## Easel Objectives (2)

- **Enable analysis and validation of proposed survivability strategies, methods, and architectures.**
- **Enable “what-if” analyses and contingency planning based on simulated walk-throughs of survivability scenarios.**



# Easel Simulation System





## Easel Characteristics

- **Discrete simulation at multiple levels of abstraction.**
- **Enables simulated execution of 1000s of parallel “actors” (e.g. nodes), but is hosted on uniprocessor machines.**
- **Supports loosely coupled network semantics**
  - **no shared memory**
  - **concurrent scheduling (no shared global clock)**



## Easel Characteristics (2)

- **Actors**
  - software, physical, electronic, human
- **Observers and facilitators**
- **Neighbor relationships**
  - direct comm link, proximity, line-of-sight
  - multiple simultaneous neighbor relationships allow the simulation of coordinated physical and electronic network assaults.



# Study Survivability Requirements of Critical Infrastructures

**Three master's theses (at SEI/Carnegie Mellon) on survivability requirements:**

**U.S. Electric Power Industry**

**U.S. Healthcare System**

**Banking and Finance Infrastructure**



## New Research Areas

- **V-RATE: Vendor Risk Analysis & Threat Evaluation**
  - **Survivability assessment of critical COTS-based systems**
  
- **FSQ: Flow-Service Quality**
  - **Mission dependency analysis of information flows**
  
- **IAD: Intrusion-Aware Development**
  - **Mission risk reduction through tolerant architectures, that incorporate intrusion analysis into existing processes**



# IEEE Information Survivability Workshops

**Provide a forum for the exchange of research results in survivability**

**Foster collaboration between critical infrastructure domain experts and the survivability research community**

**Foster multidisciplinary research approaches and collaboration**

**4th ISW in Vancouver, March 18-20, 2002**



# Survivability Research Issues

**How do you assess and measure survivability?**

- mean time between successful attacks 😊

**What architectural approaches are best?**

- context (scenario) dependent
- must be capable of rapid evolution
- survivability degrades over time

**How do you effectively model, simulate, and visualize survivability?**



## Survivability Research Issues (2)

**What engineering methodologies support the design and maintenance of survivable systems?**

**How do you manage the risks and tradeoffs to design affordable survivable systems (i.e., meet their functional and non-functional requirements)?**

**How do you design systems that can sustain their survivability in the face of ever-escalating attacker capabilities?**



# Survivability and Dependability

## What can we learn from dependability?

- rigorous analysis vs. ad-hoc tools
- metrics
- tradeoffs among software quality attributes
- fault tolerance vs. intrusion tolerance

## How can survivability return the favor?

- mission-based, context-sensitive approach
- sharp focus on intelligent adversaries
- preparing for attacks can strengthen a system against accidents and failures.



# Survivability Research Areas

**Foundational Concepts**

**Critical Infrastructure Protection**

**Survivability Architectures**

**Risk-Assessment**

**Survivable Systems Analysis and Design**

**Engineering Methodologies and Tools**

**Modeling and Simulation**

**Evaluation and Testing**

**New Threats to Survivability & Threat Taxonomies**

**Automated Recovery**



## **Survivability Research Areas (2)**

**Survivability Metrics**

**Formal Methods for Survivability Analysis**

**Requirements and Tradeoffs**

**Dependability Despite Malicious Faults**

**Mobile Code and Intrusion Tolerance**

**Human Factors to Enhance Survivability**

**Public Policy Planning, Legal Aspects, Insurance**

**Costs to Society of Non-survivable Systems**

**Internet Standards and Survivability**



## For more information ...

**Howard F. Lipson and David A. Fisher,  
“Survivability—A New Technical and Business  
Perspective on Security,” *Proceedings of the 1999  
New Security Paradigms Workshop*, Caledon Hills,  
ON, Sept. 21–24, 1999, Association for Computing  
Machinery, New York, NY.**

**Available at: <http://www.cert.org/research/>  
along with lots more on survivability research.**



## Contact Information

**Howard F. Lipson    [hfl@cert.org](mailto:hfl@cert.org)**

**+1-412-268-7237**

**<http://www.cert.org/research/>**

**CERT<sup>®</sup> Coordination Center  
Software Engineering Institute  
4500 Fifth Avenue  
Pittsburgh, PA 15213 USA**