Carnegie Mellon University
Software Engineering Institute

Survivability –

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

Howard F. Lipson, Ph.D.
CERT® Coordination Center
Pittsburgh, PA USA

IFIP WG 10.4
Summer 2000 Meeting, 28 June – 2 July

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

Outline

Survivability Concepts

Research Approaches

Research Issues

The Problem

We are increasingly dependent upon large-scale highly distributed systems

- **defense**
- **energy**
- **telecommunications**
- **transportation**
- **banking and finance**
- ***e-commerce***

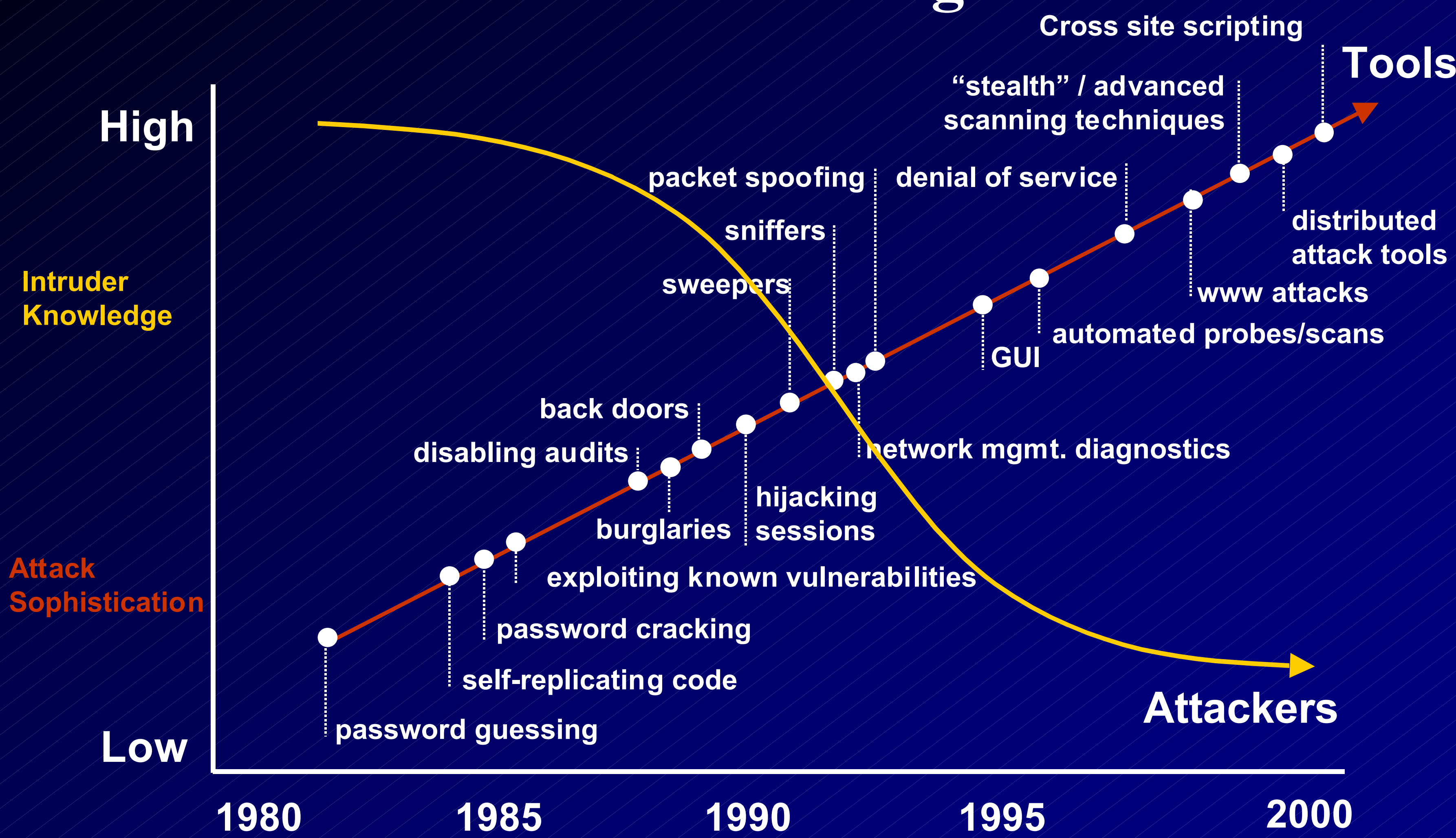
The Problem (2)

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

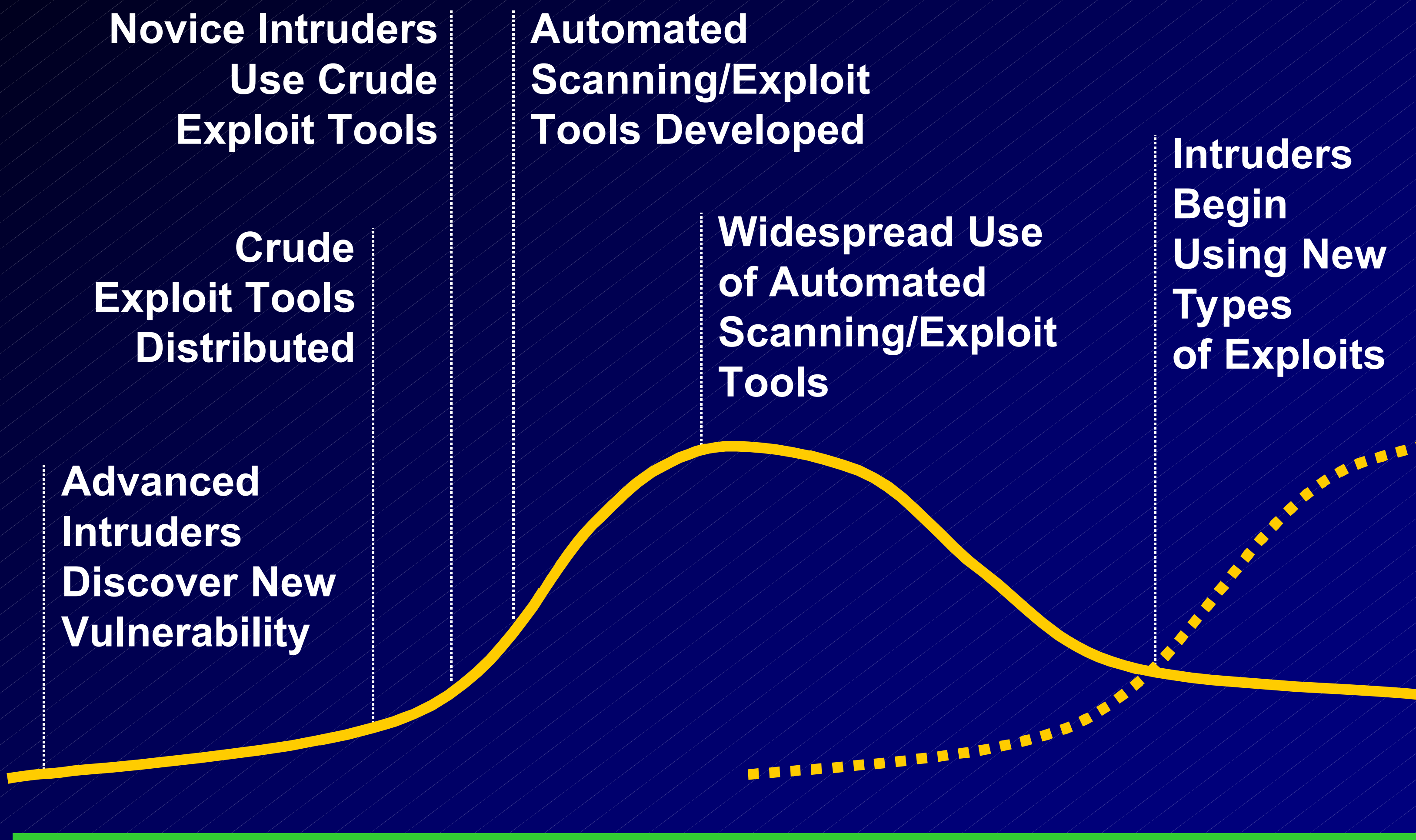
No amount of system “hardening” can guarantee that such systems are invulnerable to attack.

Serious consequences of system compromises and failures

Attack Sophistication vs. Intruder Technical Knowledge



Vulnerability Exploit Cycle



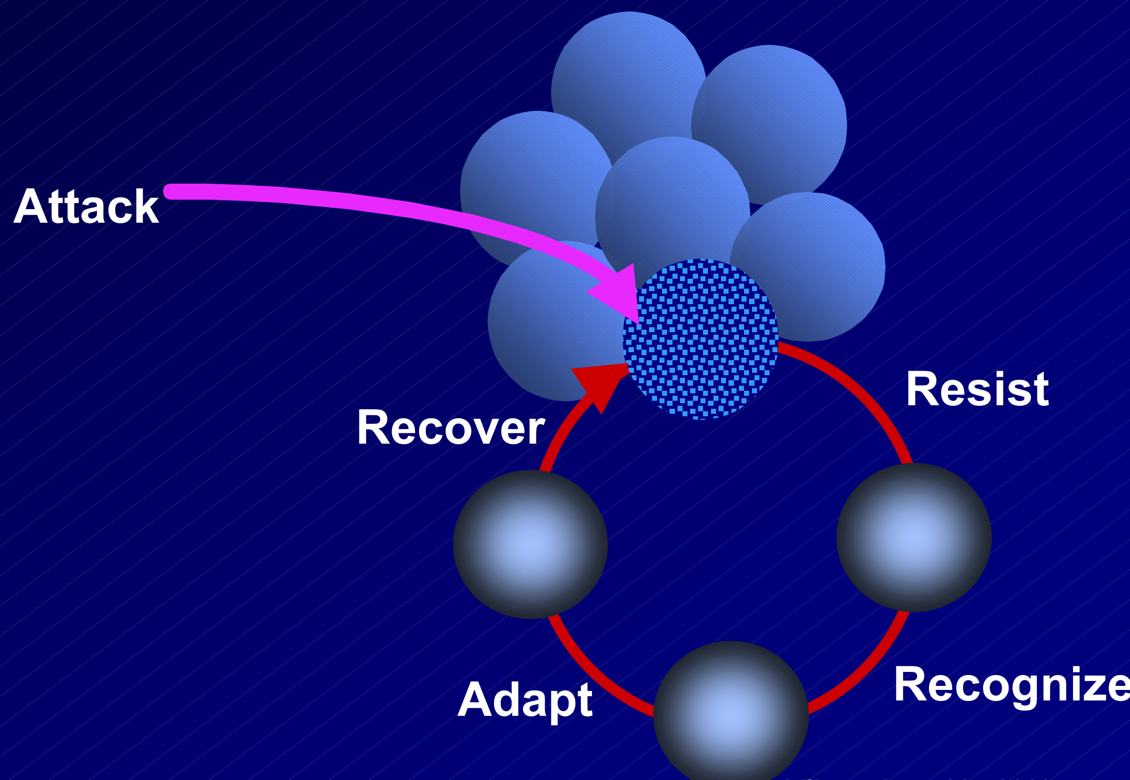
In the beginning . . .

"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 Long-term Survivability

System adaptation and evolution is essential, because …

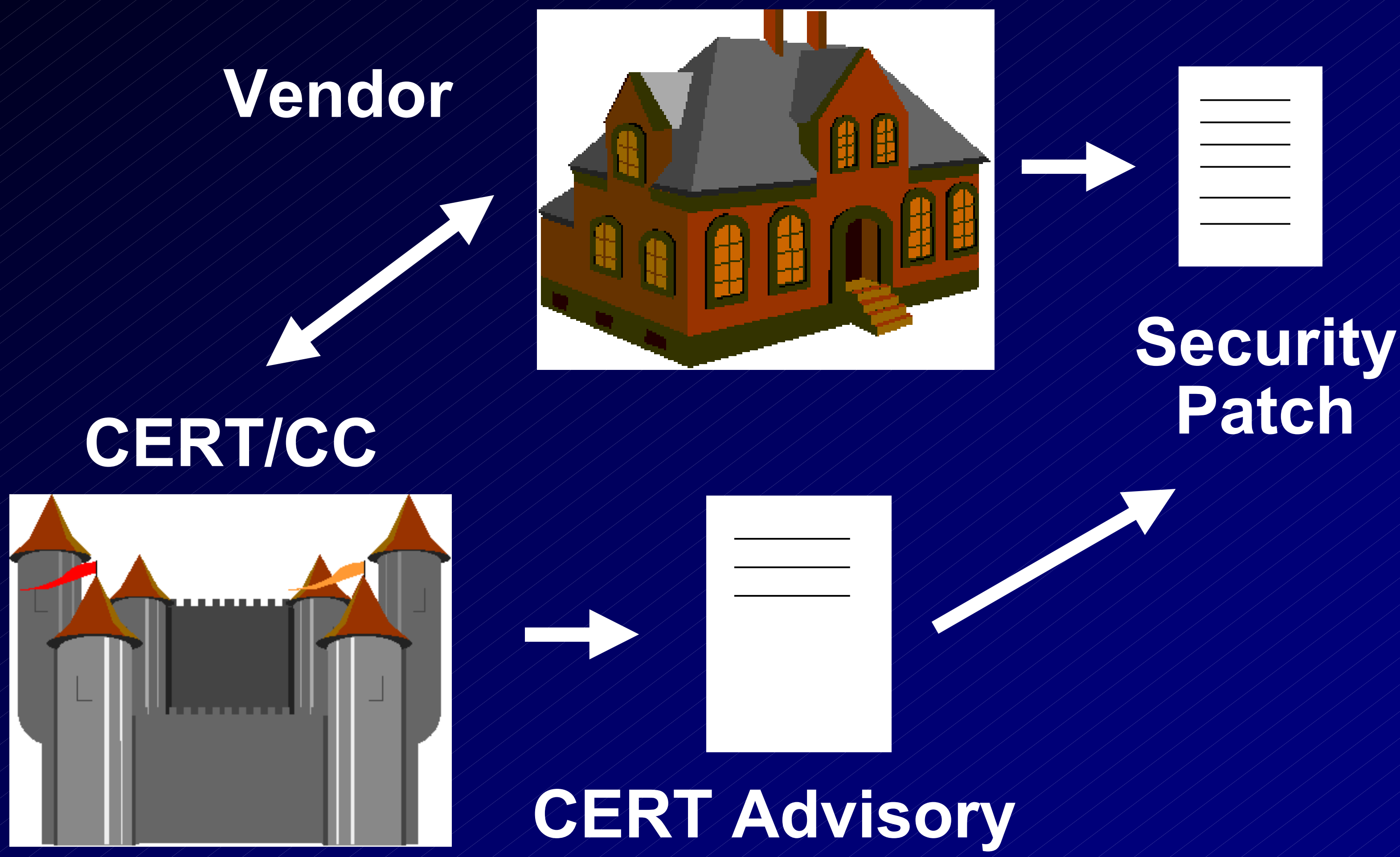
- Missions evolve, or change drastically
- Underlying technologies change
- New attack patterns
- Continual attacker-defender escalation
- Political, social, legal changes
- Collaborators become competitors
- Survivability lifecycle

The New Computing Environment Changes Everything

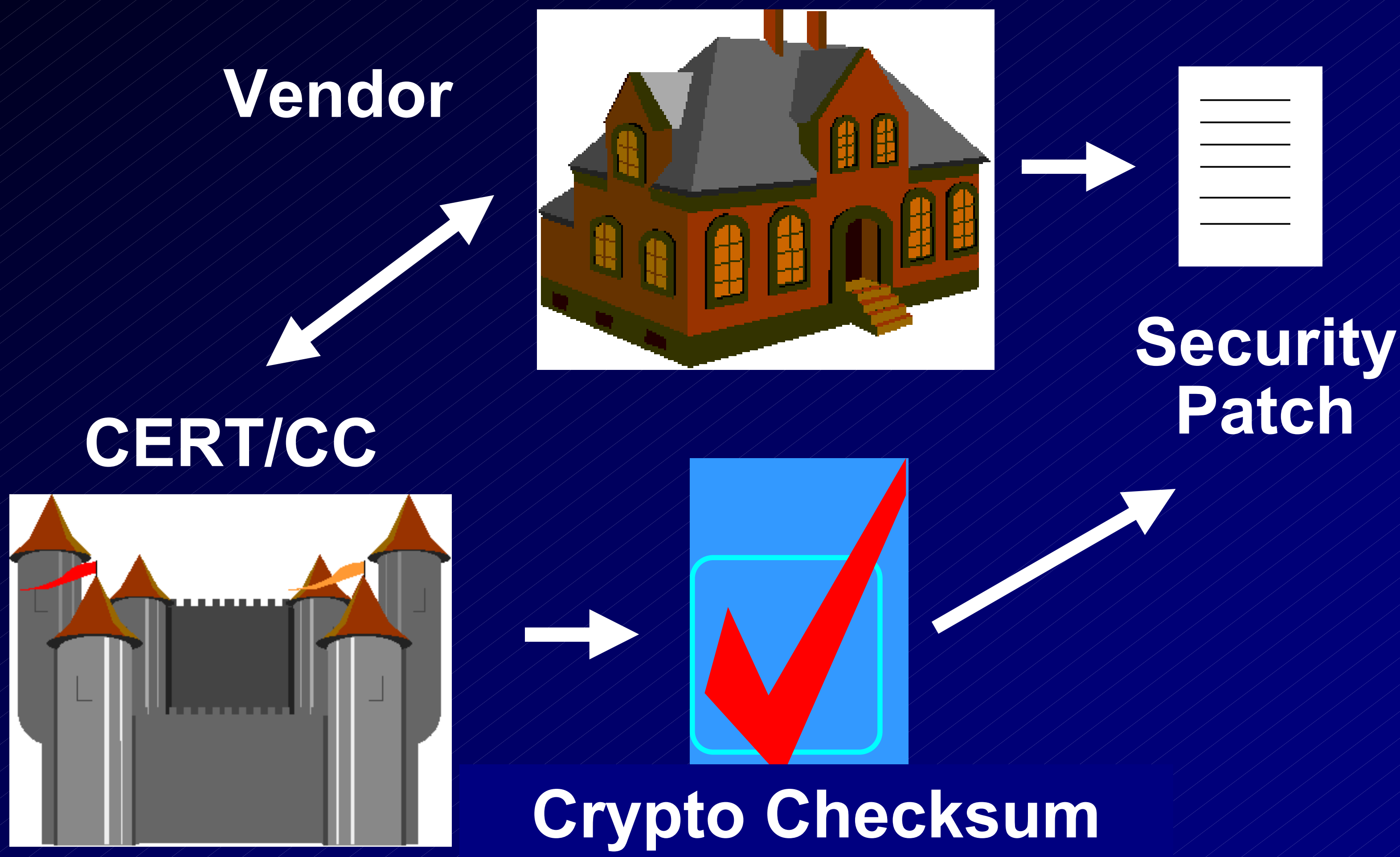
- Open, highly distributed systems
- No central administrative control
- No global visibility
- Untrusted insiders
- Unknown participants
- Unknown perimeters (physical and logical)
- Unknown software components
  - COTS, Java applets, ActiveX controls, etc.
- Large scale, coordinated attacks
- Survival at risk

An Example of the Security Impact of the New IT Environment

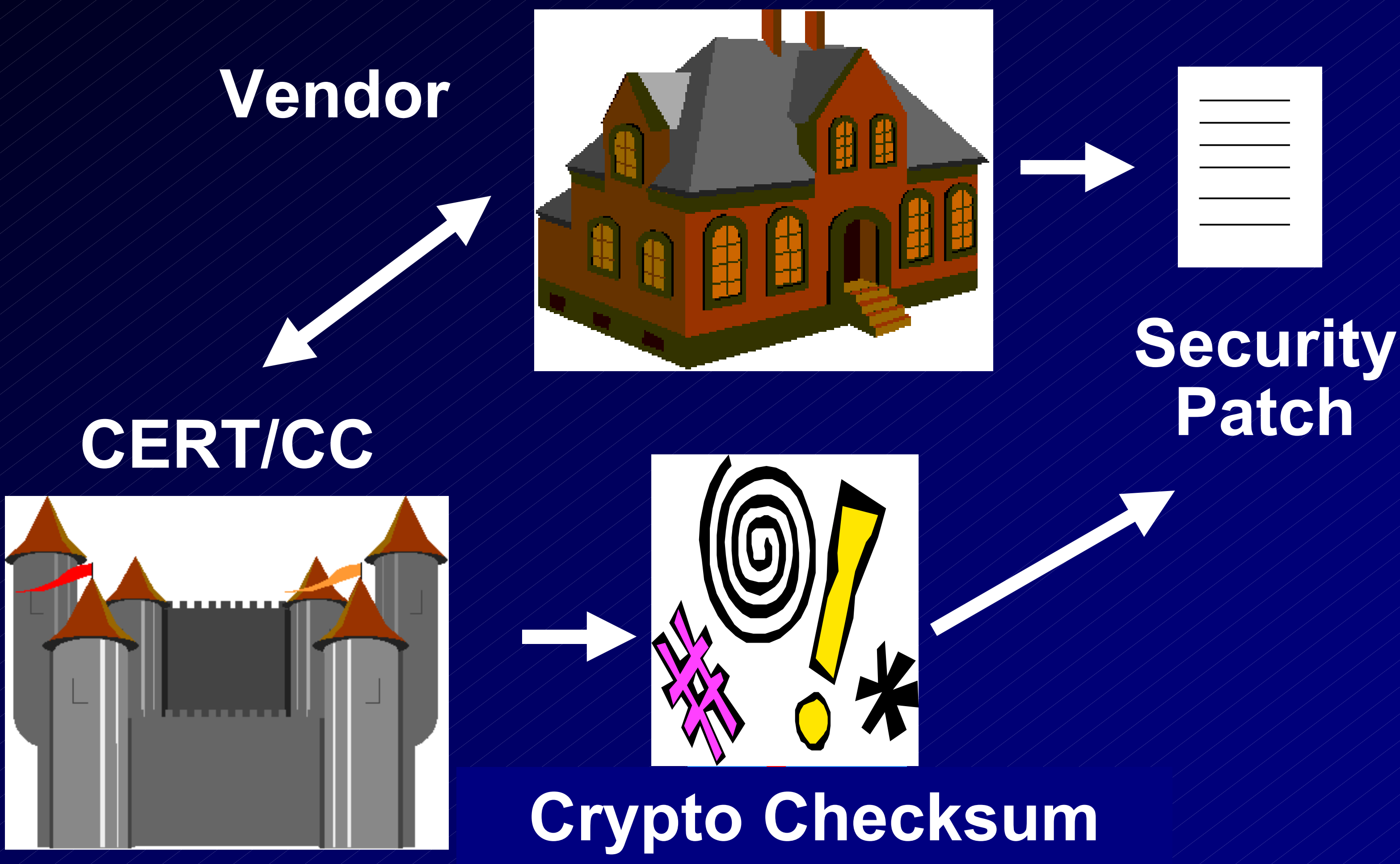
Security Advisory Process



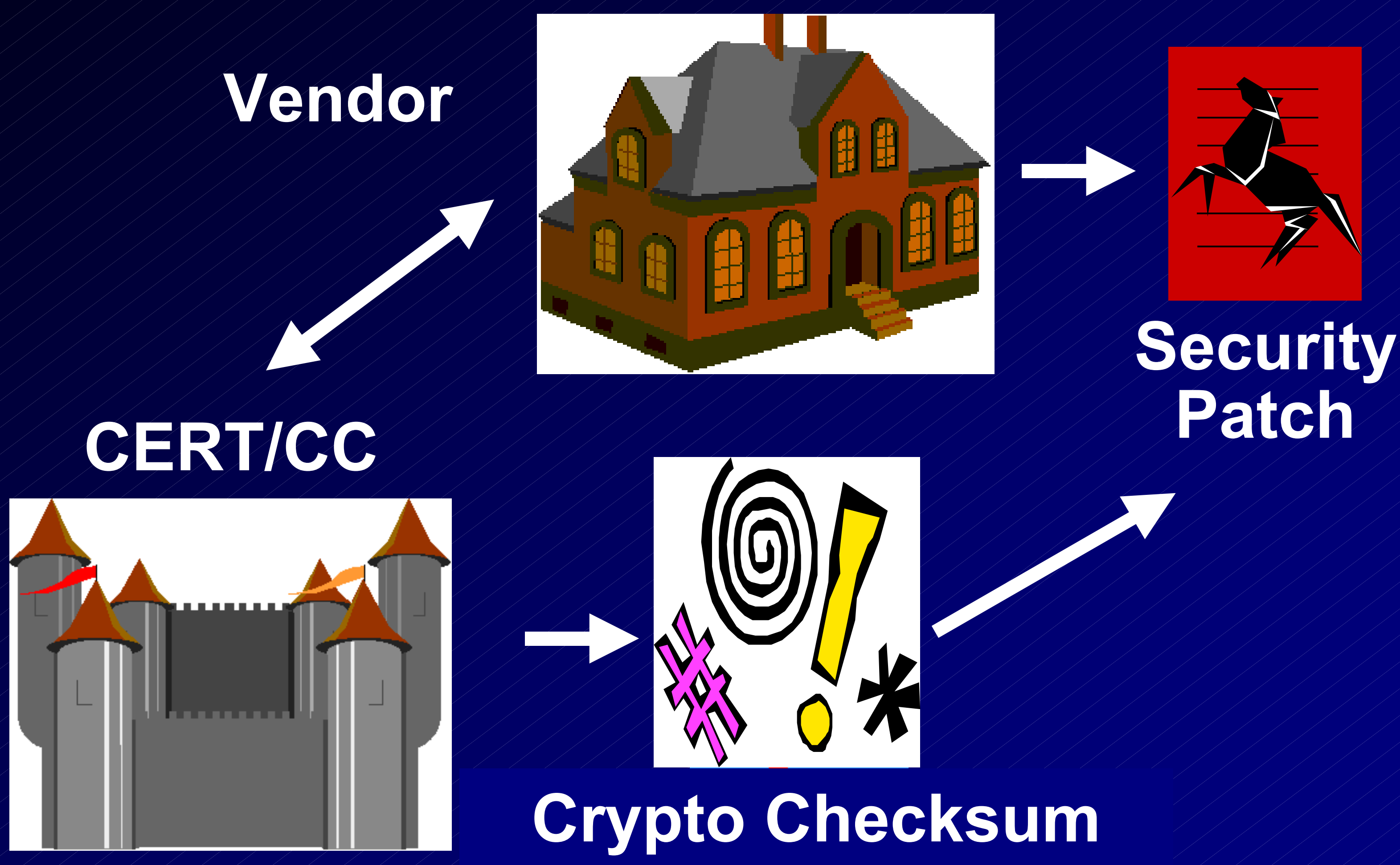
Security Advisory Process



Security Advisory Process



Security Advisory Process

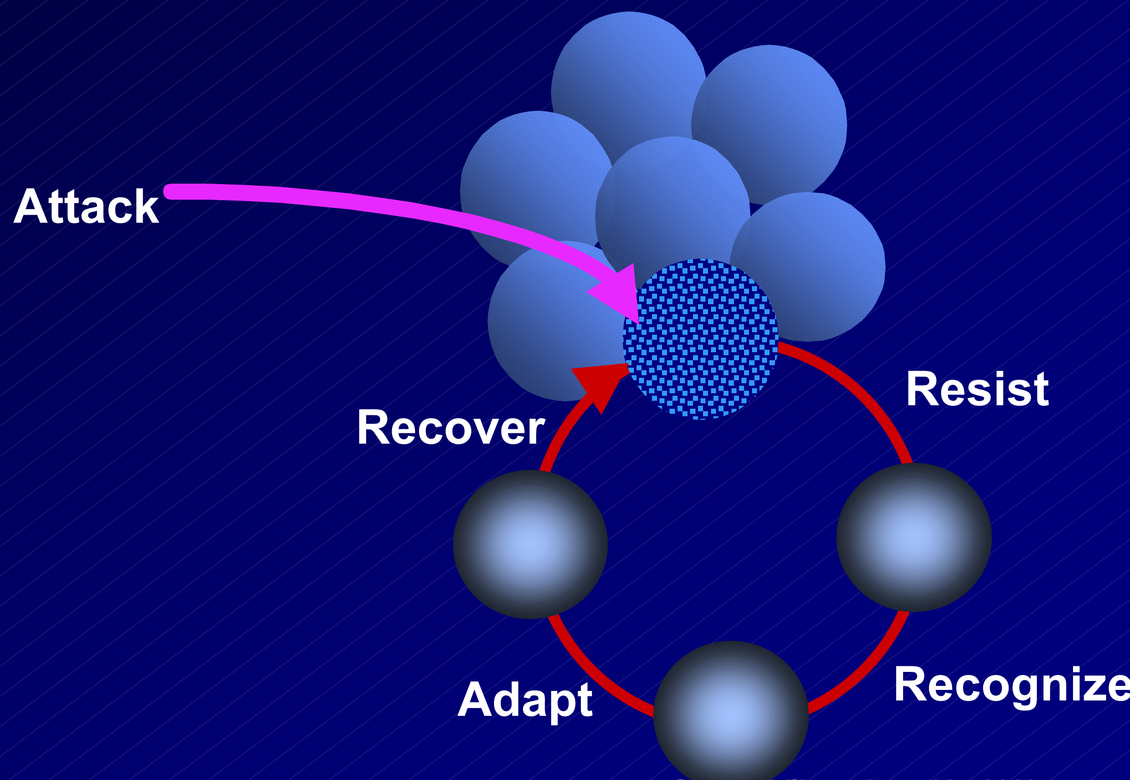


Unbounded Systems

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

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

Survivability Requirements

Mission-critical functionality
- 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.

Techniques & Methods

Security

- Fortress model: firewalls, security policy
- Insider trust
- Encryption, authentication, access control
- Intrusion detection (Recovery secondary)
- Success criterion: binary:
  - Attack succeeds or fails

Techniques & Methods (2)

Survivability

- Security techniques where applicable
- Diversity, redundancy
- Trust validation
- Recovery (largely automated)
- Mission-specific risk management
- Contingency (disaster) planning
- Success criteria:
  - 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

Formal Methods

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 ⑧	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. **Softspot:** Treatment Plans	**Current:** Security model in DB protects TPs against corruption.	**Current:** None, except when a provider happens to recognize a corrupted TP.	**Current:** Locate an uncorrupted backup or reconstruct TPs from scratch.
	Recommended: Implement live replicated DBs that cross check for validity (supported by many DBs) [5]	**Recommended:** Add and check crypto-checksums on TPs in the DB. [3, 4]	**Recommended:** 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

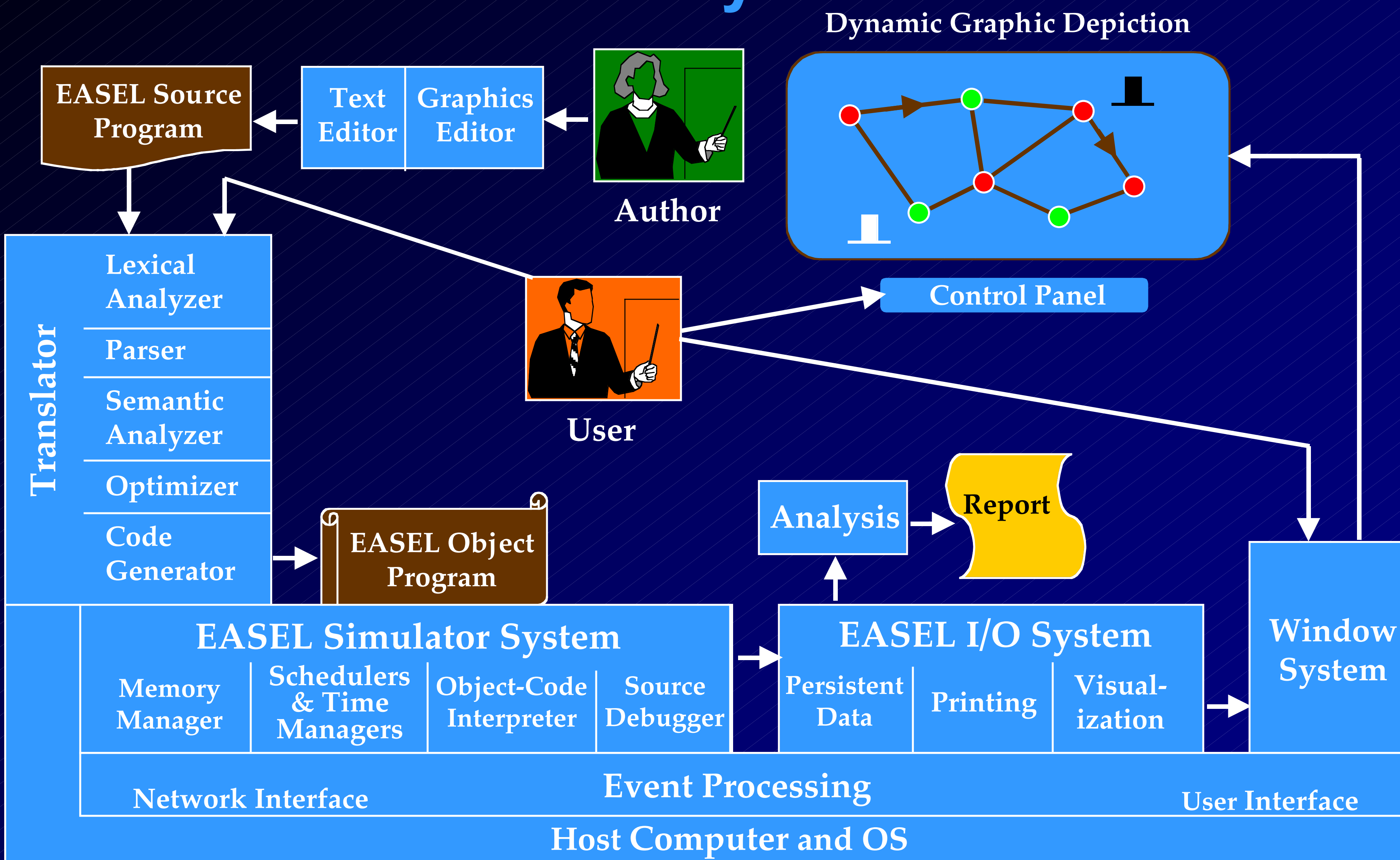
Easel Objectives

- 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

Formal Methods

Survivability Working Group

- Carnegie Mellon School of CS
- SEI-CERT/CC

First Project:

Using model checking to investigate the survivability of inter-bank transactions

Dependability Despite Malicious Faults Workshop:
"Analyzing Survivability Properties of Specification of Networks"

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

ISW-2000 has a special focus on dependability

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

Contact Information

Howard F. Lipson   hfl@cert.org

+1–412–268–7237

http://www.cert.org/research/

CERT® Coordination Center
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213 USA