Executive Meeting
Gestão de Riscos em TI
e Segurança da Informação

Cyber Security—Reality and Perspectives

Dr. Angel Jordan
Director of the Software Engineering Institute
Provost Emeritus
Carnegie Mellon University

Brazil, March 2004



MODULO Education Center
21 Embratel
Microsoft

Cyber Security—Reality and Perspectives

Dr. Angel Jordan
Director of the Software Engineering Institute

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

The CERT Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.
© 2004 by Carnegie Mellon University



Overview

- The Cyber Environment
- Statistics
- Implementing Cyber Security
- CERT Advisories
- Cyberterror Vulnerabilities
- The CERT Centers and their Initiatives

© 2004 by Carnegie Mellon University

The Cyber Environment

Cyberspace

- **Borderless**
- **Dynamic**
- **Anonymous**
- **Accessible**

Not limited to the Internet

- **Includes isolated networks**
- **Embedded systems**
- **Wireless technology**
- **Environment expanding to include new technologies**



© 2004 by Carnegie Mellon University

The Cyber Environment

"Urban Sprawl" in Cyberspace

- **Cyberspace has grown exponentially in recent years, now especially with wireless technologies**

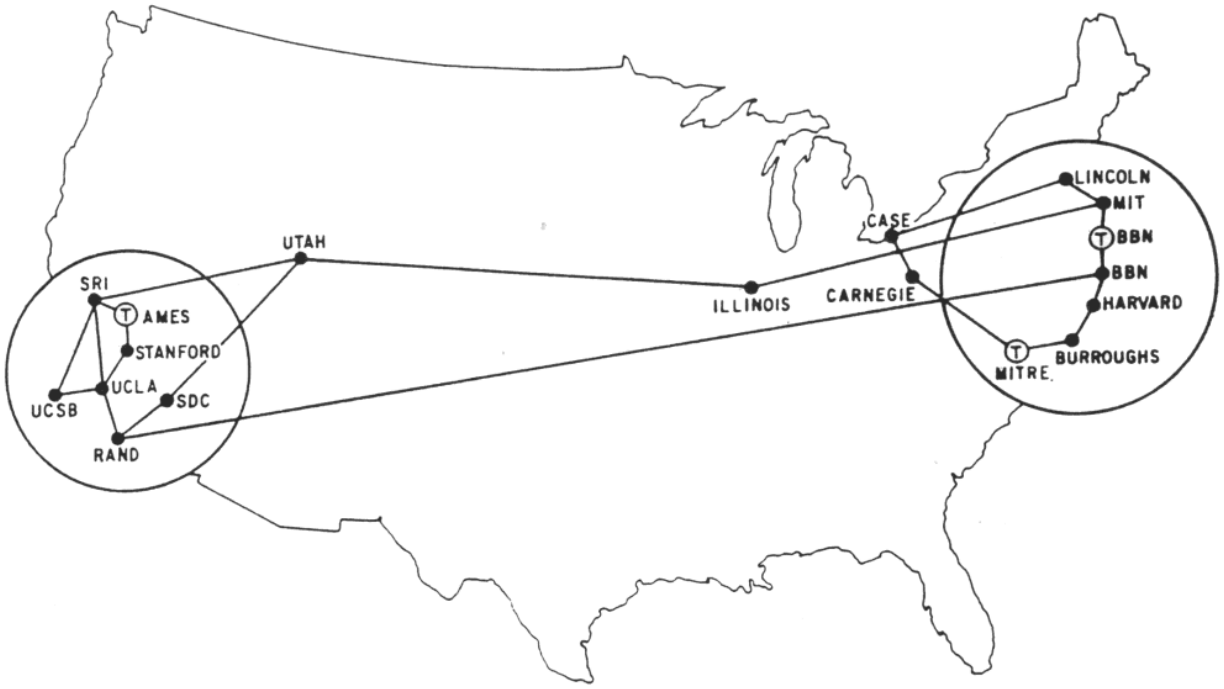
Expansion leads to increased threat

- **More people are aware of the capabilities of cyberspace (including criminals and terrorists)**
- **The cyber and physical environments now overlap and are interdependent**
- **Critical infrastructures now rely on the cyber environment**
- **As networks, systems, and service multiply, so do vulnerabilities**

© 2004 by Carnegie Mellon University

The Environment – Old Structure

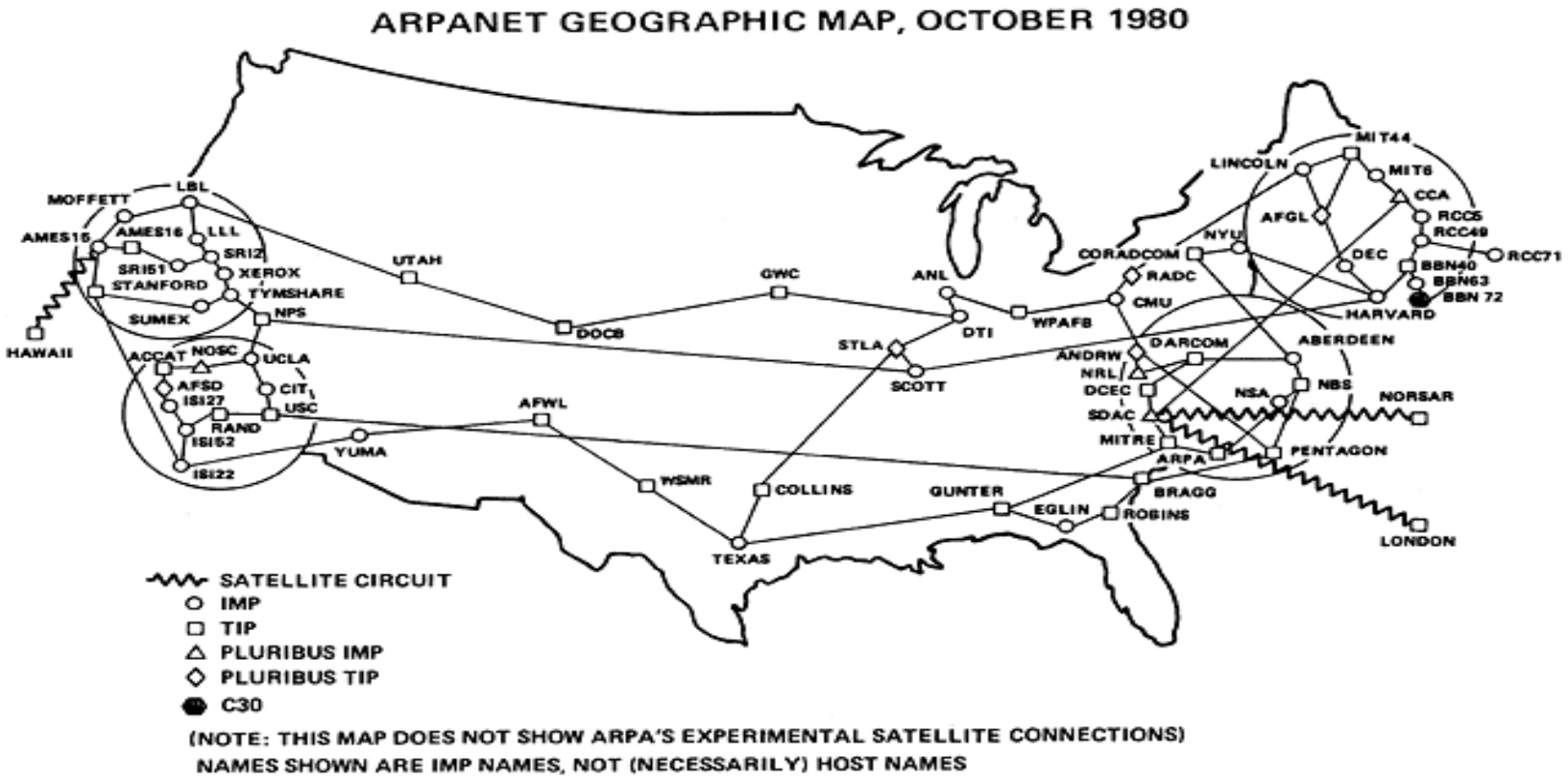
The Net Then – ARPANET 1971



MAP 4 September 1971

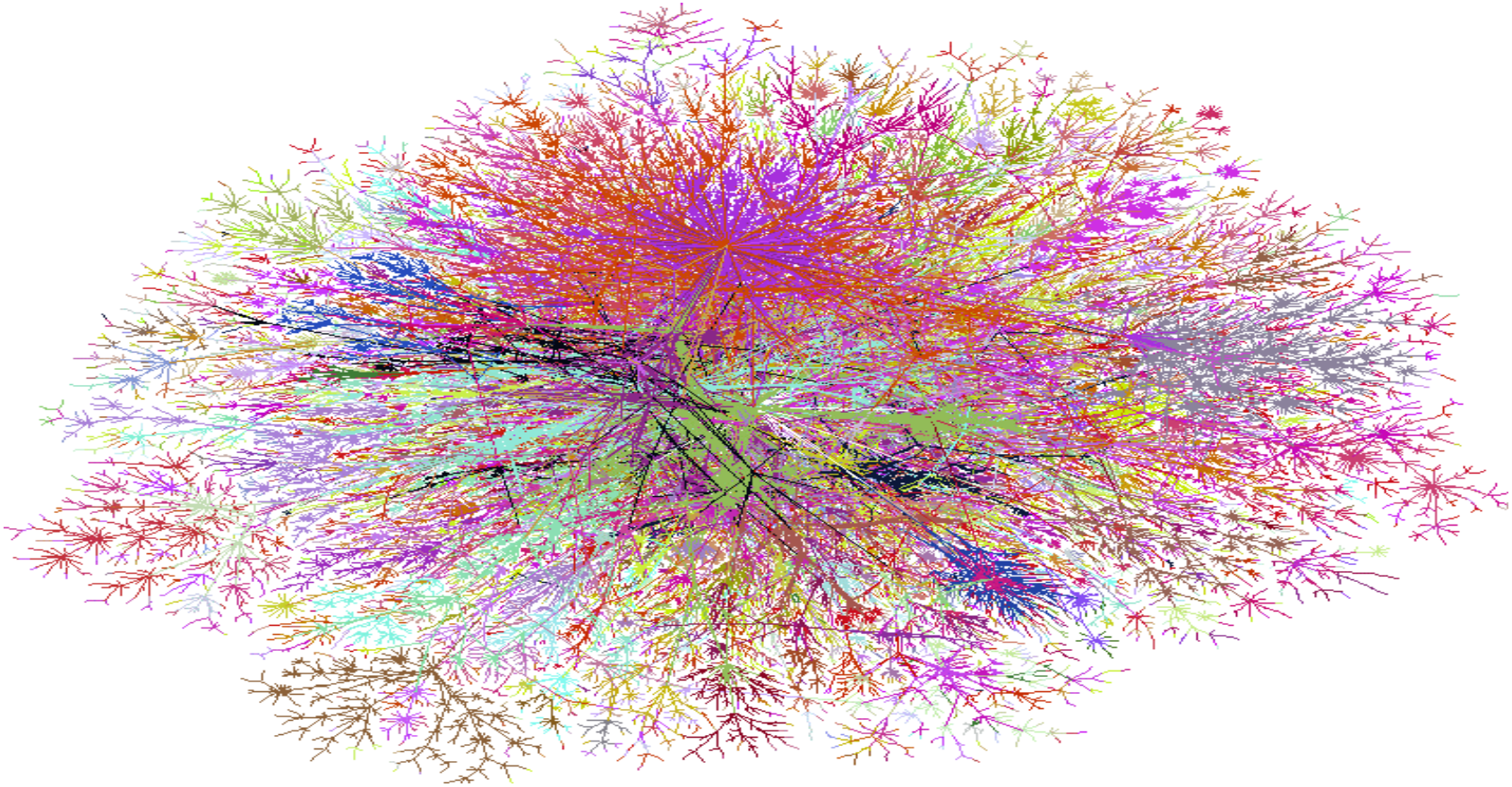
© 2004 by Carnegie Mellon University

The Old 'Net



© 2004 by Carnegie Mellon University

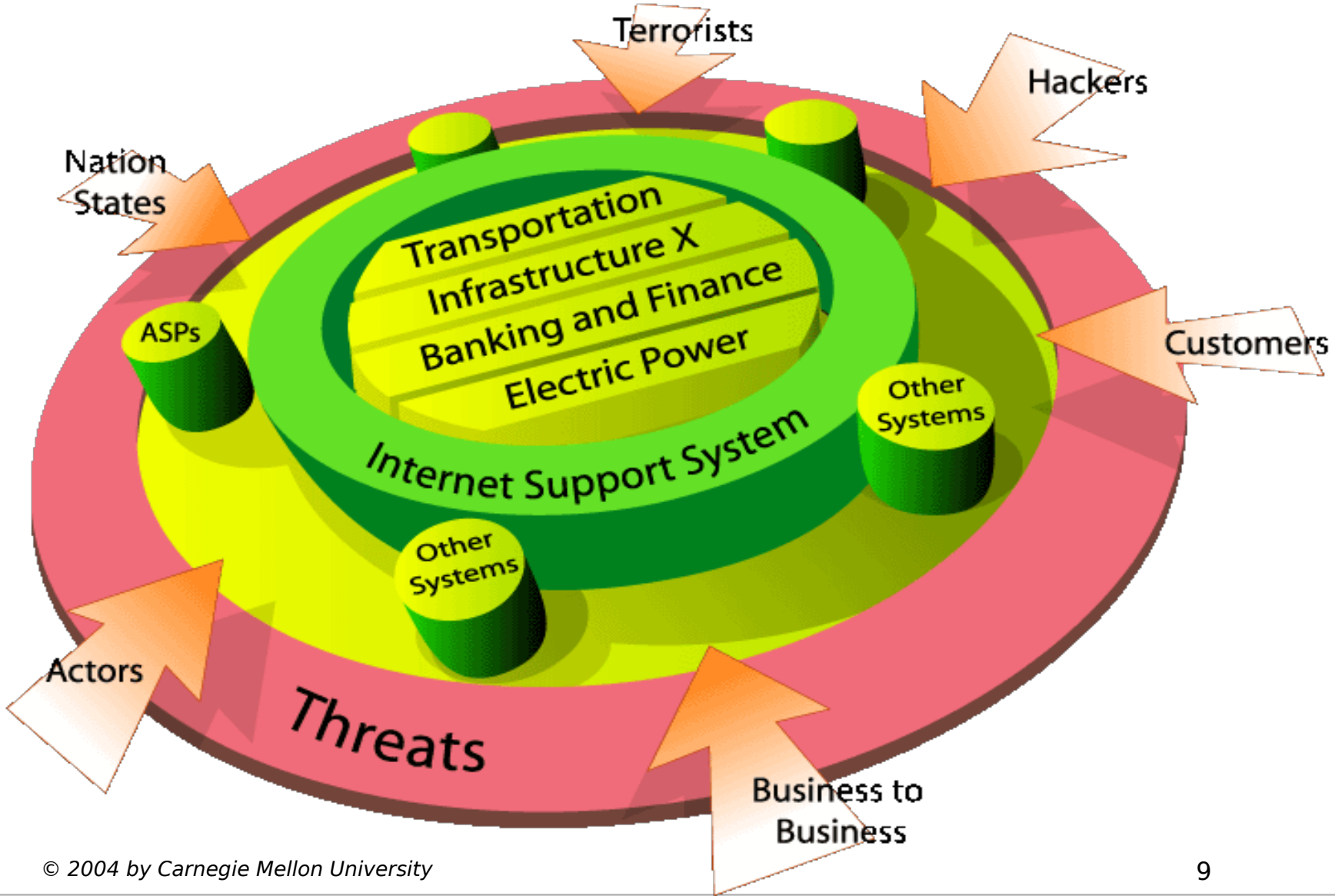
The New Net-Still Growing



Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

© 2004 by Carnegie Mellon University

Internet Integrated Infrastructure Threat Environment



© 2004 by Carnegie Mellon University

Cyberterrorism?

Within the CERT Centers, we have *no* documented cases of cyber terror, however:

- **Crime using Internet technologies is on the rise**
- **Cyber/Physical connectivity increases the threat**
- **Traditional terrorist attacks can have significant cyber impact**

© 2004 by Carnegie Mellon University

The Threat - Reality

How real is the threat?

- **Al Qaeda regularly uses computer technology to pass operational plans & training materials**
- **Osama bin Laden has stated that the Information and Financial Infrastructures of the U.S. are targets for terrorist action**
- **The attack on the World Trade Center had a serious cyber impact on the Financial Infrastructure even though it was not the target of the attack**
- **The Information Infrastructure is designed for efficiency and functionality, *not* for security or survivability**

© 2004 by Carnegie Mellon University

The Threat - Statistics

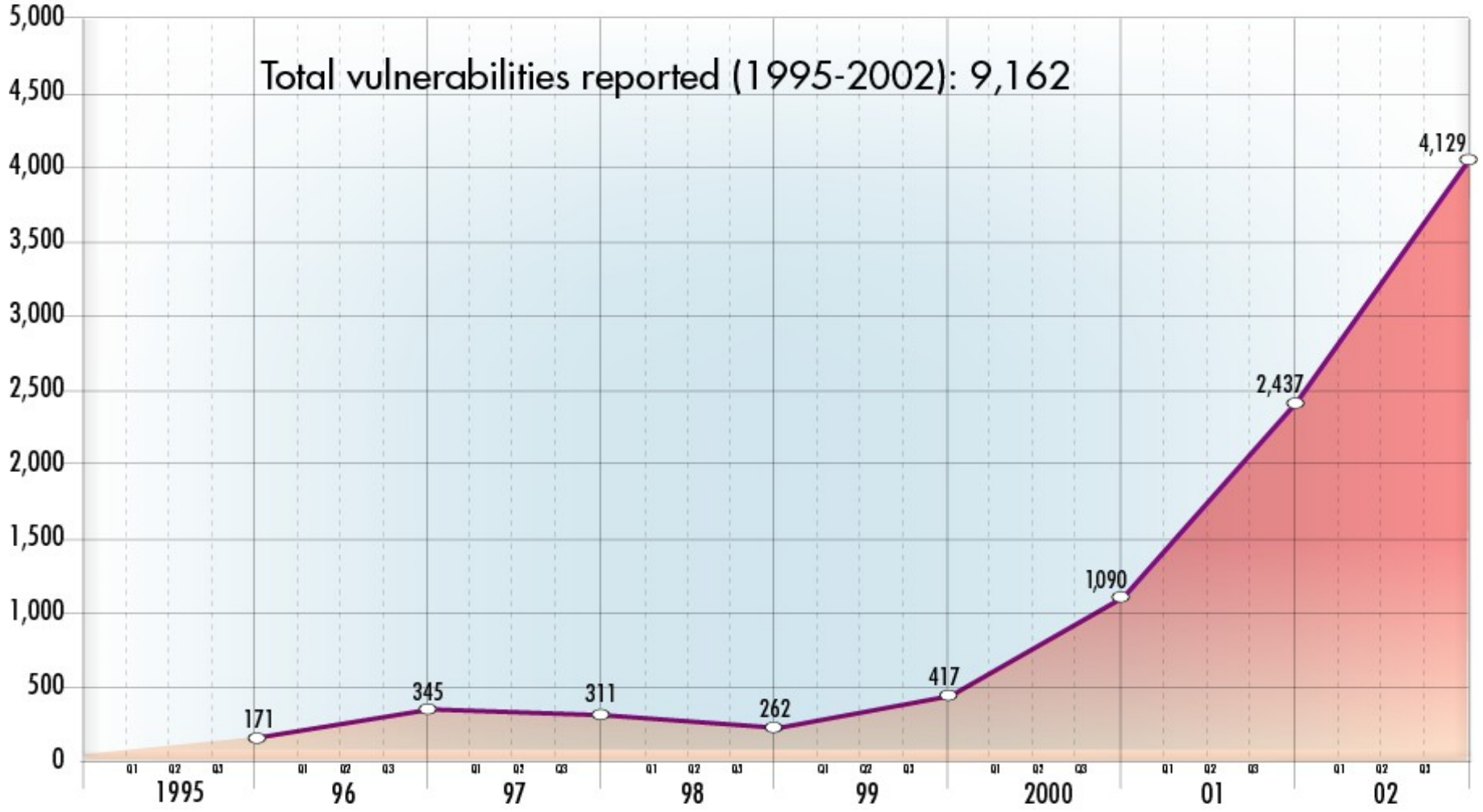
How Real is the Threat – the stats

- Incidents and Vulnerabilities reported by the CERT C/C
  - CERT/CC Incident Reports
    - **1988-2000: 47,711**
    - **1999: 9,859**
    - **2000: 21,756**
    - **2001: 52,658**
    - **2002: 82,094**
  - Vulnerabilities Discovered
    - **1995-2000: 2,596**
    - **1999: 417**
    - **2000: 1,090**
    - **2001: 2,437**
    - **2002: 4,129**



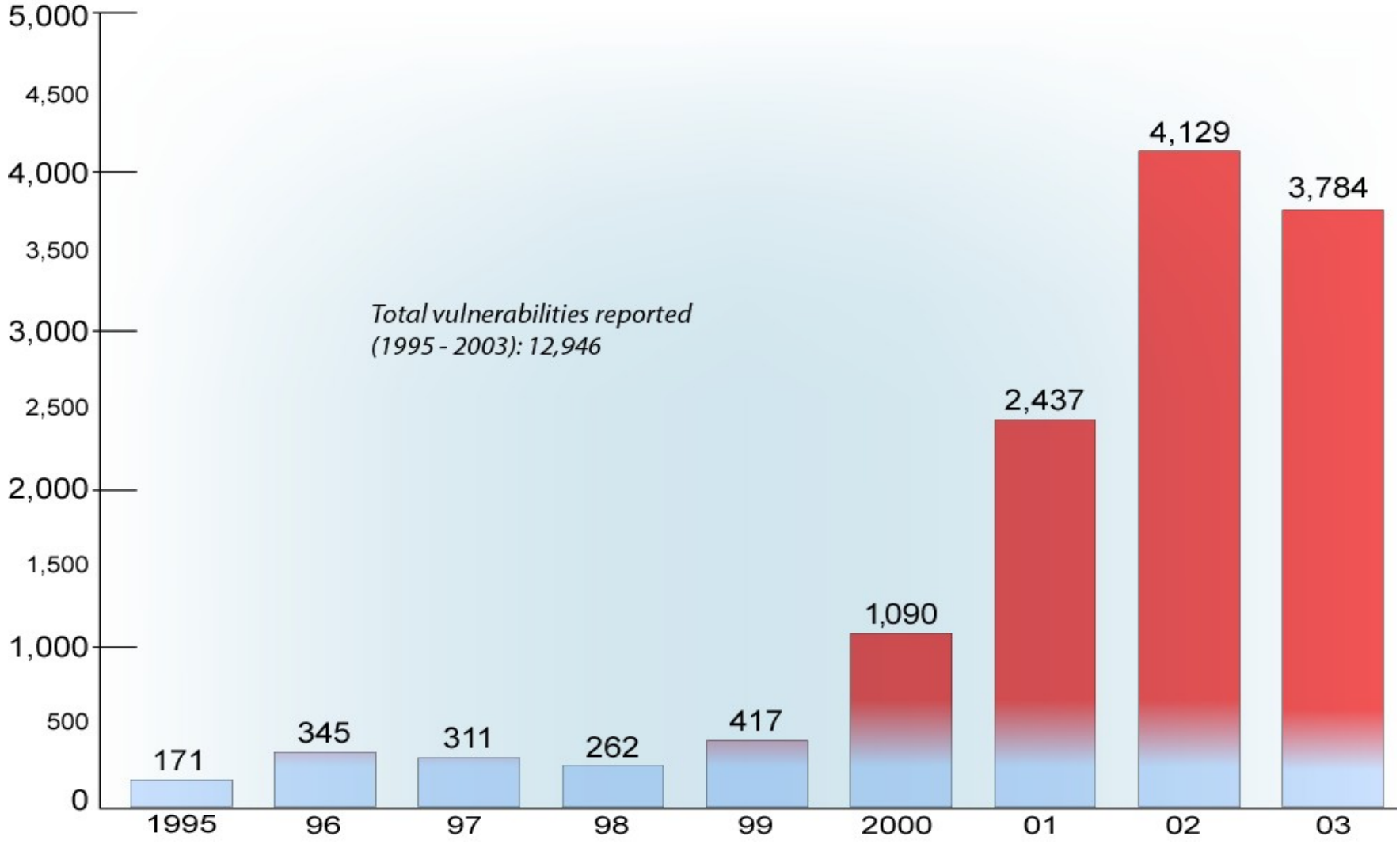
© 2004 by Carnegie Mellon University

Increasing Vulnerability => Increasing Threat



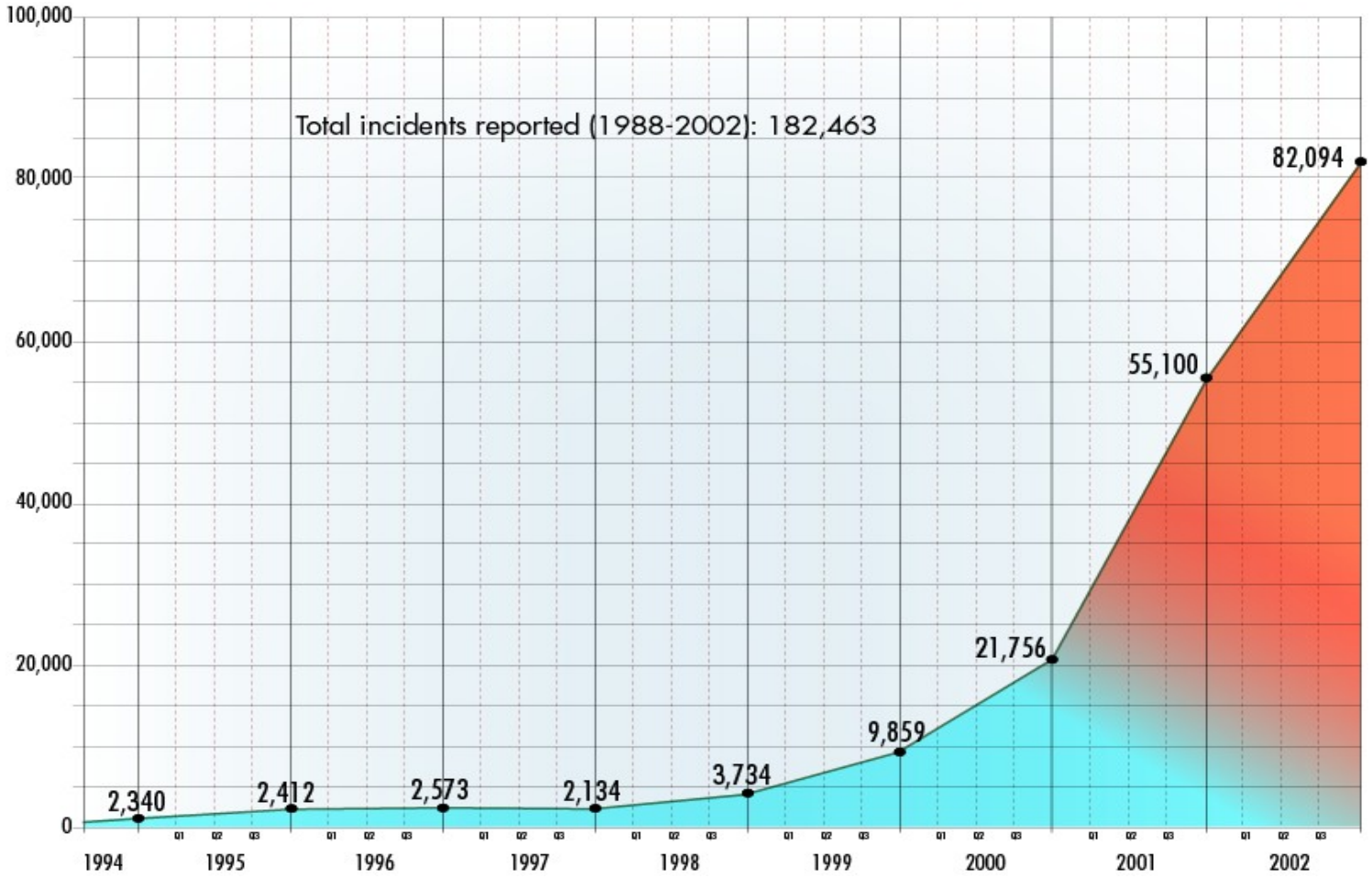
© 2004 by Carnegie Mellon University

Vulnerabilities Reported to the CERT/CC



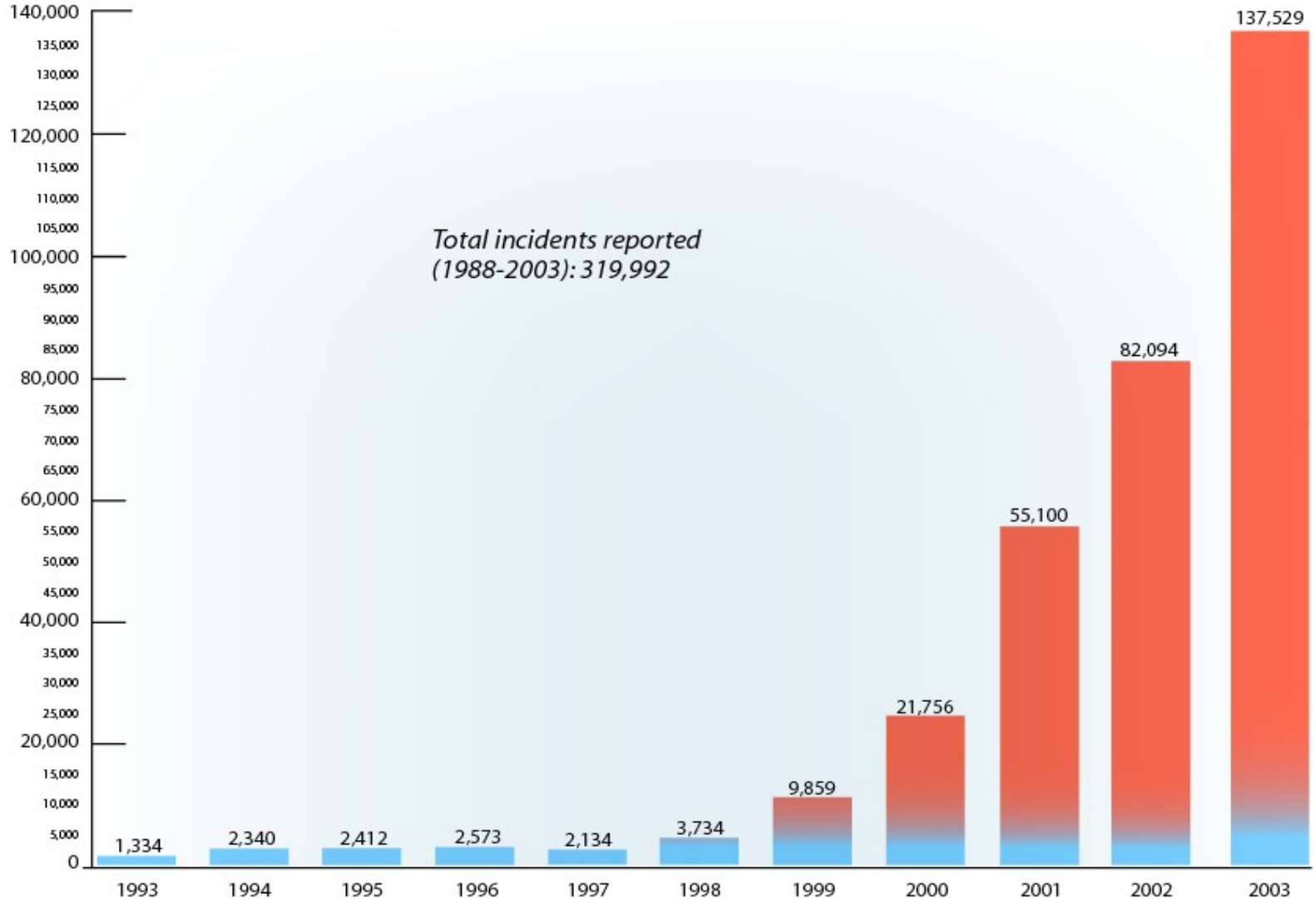
© 2004 by Carnegie Mellon University

More Vulnerabilities => More Incidents



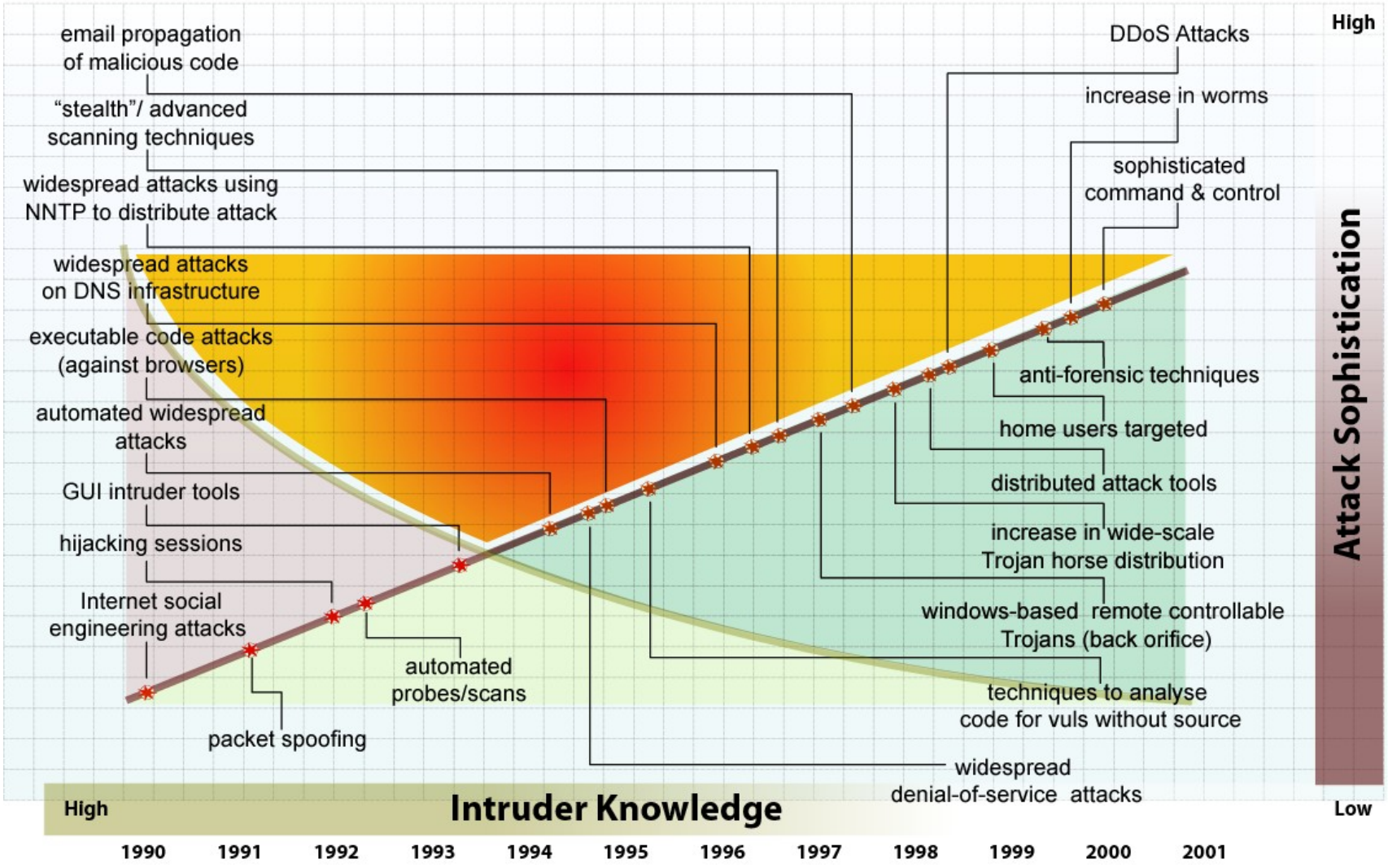
© 2004 by Carnegie Mellon University

Incidents Reported to the CERT/CC



© 2004 by Carnegie Mellon University

Incident Trends are Toward Higher Sophistication



Should We Be Concerned?

The Development and growth of cyber technologies has changed the threat environment forever

Adoption of technology creates dependencies that evolve to interdependency

- **A significant attack on one can directly impact others (Cascade effect)**

Pervasiveness of cyber technologies redefines security

- **Physical attacks have cyber consequences and Cyber attacks have physical consequences**

© 2004 by Carnegie Mellon University

Should We Be Concerned?

Attackers well aware of the potential impact of using cyberspace

- **Nations adding Computer Network Warfare to strategy and doctrine**
- **Terrorist groups developing cyber capabilities (Al Qaeda)**
- **Criminal groups have been using cyberspace for years**
- **Critical Infrastructures prime targets (exploitation and compromise)**

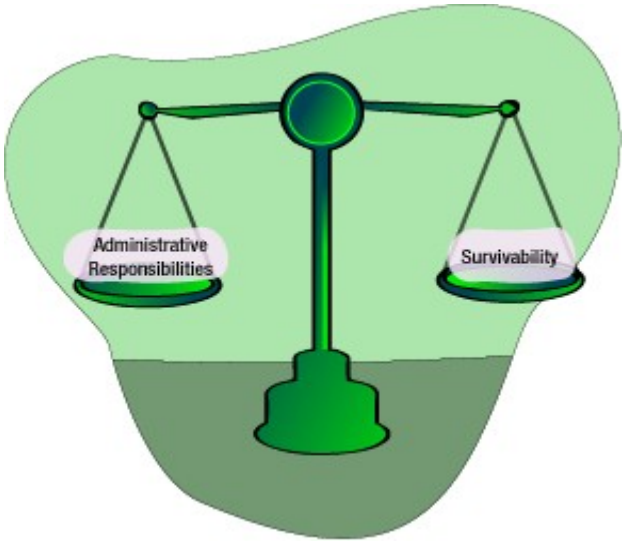
We are our own worst enemy

- **Websites great source of intelligence**

© 2004 by Carnegie Mellon University

Your Administrative Responsibilities

- Monitoring
- Incident response
- Damage assessment and recovery
- Analysis
- System life-cycle management
- Backups, fault tolerance



© 2004 by Carnegie Mellon University

Security Patches and Workarounds

- Stay up-to-date regarding vendor patches and workarounds to address security vulnerabilities
- Verify the integrity and authenticity of all downloaded software before applying it to your systems
- Test patches and workarounds in an isolated, physically secure test environment before deployment
- Deploy security patches and workarounds as soon as possible to reduce exposure to attacks
- Maintain a thorough, up-to-date record of security patches and workarounds that you have applied

© 2004 by Carnegie Mellon University

Why Care About Patches



of intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available.

© 2004 by Carnegie Mellon University

Virus Scanning

Even the most conscientious users can receive a virus

- **Files and media exchanged between employees and with customers or other external contacts**
- **Data downloaded from remote systems**
- **E-mail attachments**

Measures

- **Install and regularly use current virus scanning software**
- **Keep virus scanners data up-to-date on all systems**
- **Raise awareness of current and emerging virus threats**
- **Train users to scan all data received for viruses before use**

© 2004 by Carnegie Mellon University

Host-based Firewalls

Another layer of Defense
- **Becoming commonplace,**

yet still under-utilized

OS specific
- **Free and commercial**
- **Some have IDS too**

Examples:
- **Zone Alarm**
- **Black Ice Defender**
- **Tiny Personal Firewall**
- **Linux Firewalls**
- **Windows XP Firewall**
- **Mac OSX Host Firewall (on by default)**



© 2004 by Carnegie Mellon University

Network Firewalls

One or more components placed at gateways between networks to enforce information security policy

- **Filtering routers**
- **Bastion hosts and application/service proxies**
- **Network switches**
- **Network monitors**

Ensure secure administration of firewall components

Reinforce perimeter defenses with host security

© 2004 by Carnegie Mellon University

What is an Intrusion Detection System?

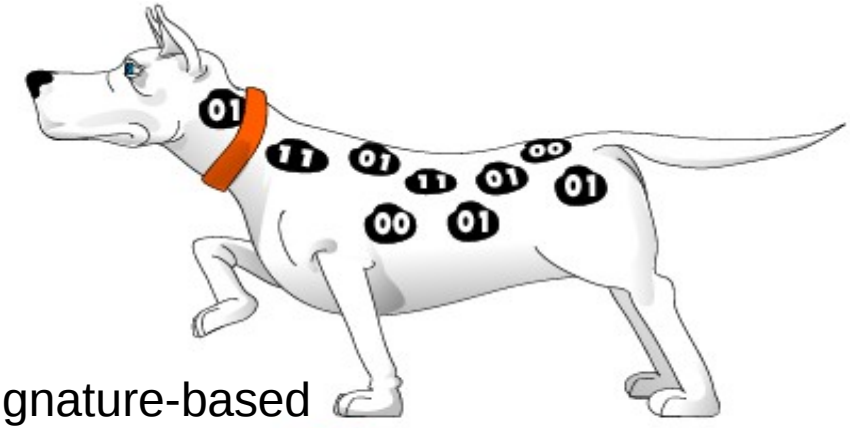
Device on a network that monitors traffic and/or host activity looking for the following:

- **Malicious traffic, such as attempts to circumvent identification & authorization or other access controls**
- **Reconnaissance traffic, such as port scans**
- **Unusual traffic: type, level, source, etc.**
- **Activity on host systems that is outside of known patterns**

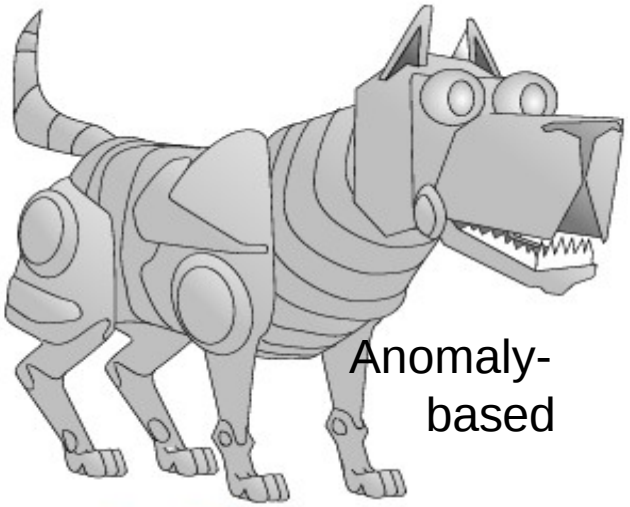
Device then logs and reports activity in prescribed manner

© 2004 by Carnegie Mellon University

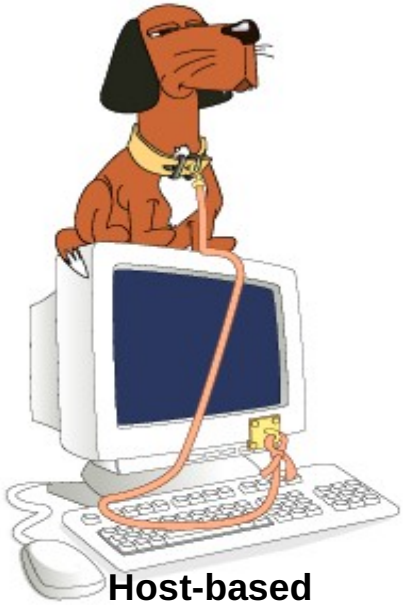
Types of IDS



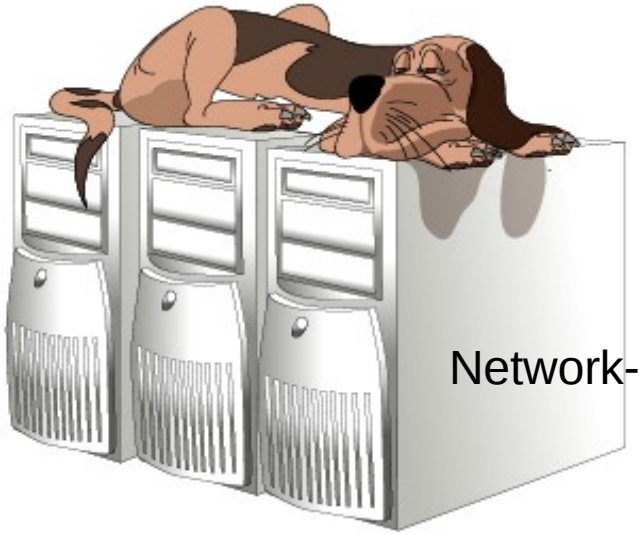
Signature-based



Anomaly-based



Host-based



Network-based

© 2004 by Carnegie Mellon University

CERT® Advisories

CERT® Advisories alert you to vulnerabilities for which you should take immediate action

- **Description of the vulnerability and its scope**
- **Potential impact should the vulnerability be exploited**
- **Solutions or workarounds**
- **Appendices contain details and vendor information**
- **Revision history**
- **PGP signature**

© 2004 by Carnegie Mellon University

Cyberterror Vulnerabilities

Most Infrastructures are Scale-free networks

- Able to survive random attacks, but susceptible to targeted attack
  - Super Hubs (Financial)
  - Considerable redundancy within the system but not *of* the system

Database Compromise

- Ability to Destroy, Disrupt, or Distort critical data
- Information as essential as physical infrastructure

Physical Attack

- Loss of facilities
- Redundancy becomes critical

Physical Security in Cyberspace

- Most physical access is now controlled with Internet technology
- Generation of keys, cards, identity, etc. controlled in cyberspace

© 2004 by Carnegie Mellon University

Strategies & Tactics

Key Points

- Good security administration is all about good systems administration
- Take a conservative approach in configuration management
- Separate, isolate and simplify system and network services
- You're only ever as secure as your weakest link
- Practice vigilance and be prepared for change
- Apply appropriate tactics to sustain and improve security
- Keep systems and network components up-to-date regarding patches and workarounds for security
- Maintain secure backups

© 2004 by Carnegie Mellon University

Software Engineering Institute

Applied research and development laboratory situated as a college-level unit at Carnegie Mellon University

Mission is to provide leadership in software engineering and to transition new software engineering technology

Encouraged to support industry in pre-competitive technology research and development and in technology transition activities

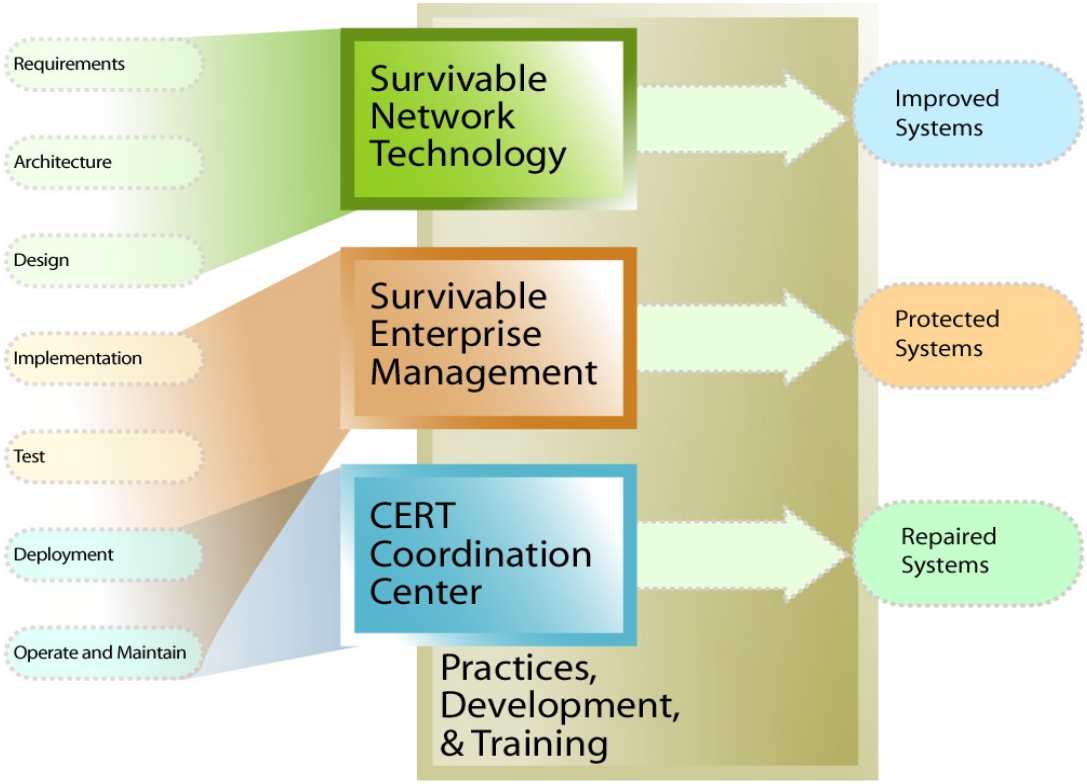
© 2004 by Carnegie Mellon University

CERT Centers

CERT was formed in 1988 in response to the Internet Worm

CERT added research, training, and analysis as the Internet matured

September 15, 2003 CERT Centers is named the US CERT (www.us-cert.gov) in partnership with DHS



© 2004 by Carnegie Mellon University

CERT® Coordination Center

Solving today's security problems

Artifact Analysis

Study intruder code to develop defenses

Developing new techniques for analysis

Vulnerability Handling

Analyze flaws in Internet systems

4,000 vulnerabilities handled each year

Publications available at http://kb.cert.org/vuls/

Incident Handling

Respond to security emergencies on the Internet

Measure exploitation of flaws

100,000 incidents handled each year

Publications available at http://www.cert.org

© 2004 by Carnegie Mellon University

US-CERT

US-CERT is a partnership of

- **The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS)**
- **The CERT Coordination Center**

© 2004 by Carnegie Mellon University

CERT's Areas of Expertise

- Vulnerability analysis
- Artifact analysis
- Insider threats
- Survivable Architectures
- Function abstraction/extraction
- Modeling and simulation
- Dependency and critical infrastructure analysis
- Best practices and methodologies for testing software
- R&D

© 2004 by Carnegie Mellon University

US-CERT Working Relationships

US-CERT will work with organizations involved in watch, warning, and response, including:

- **Private, public, and academic organizations that operate computer security incident response teams (CSIRTs)**
- **Managed security service providers**
- **ISACs**
- **Infrastructure owners/operators**
- **Technology developers**

© 2004 by Carnegie Mellon University

US-CERT Focus

Prevent and mitigate cyber attacks and reduce cyber vulnerabilities by concentrating on four areas:

- **Improving warning of and response to incidents**
- **Increasing coordination of response information**
- **Reducing vulnerabilities**
- **Enhancing prevention and protection efforts**

© 2004 by Carnegie Mellon University

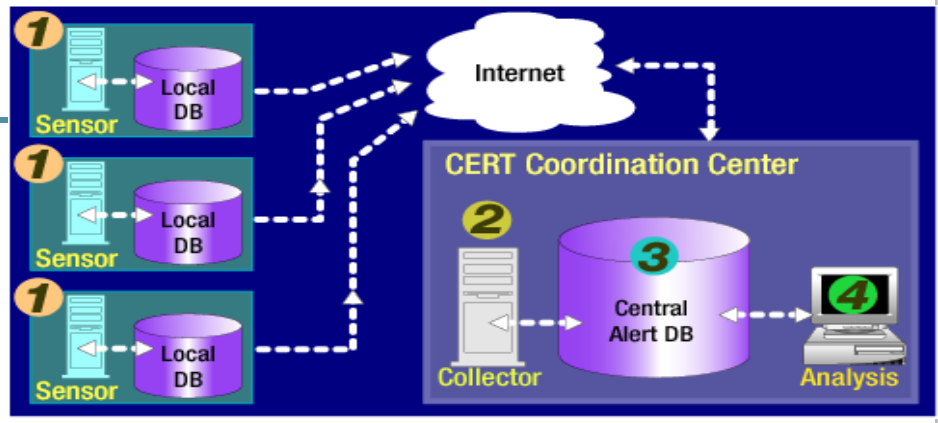
US-CERT: Coordinated Response

- Provide tools and capabilities to share information in a secure manner
- Contact partners regularly and exchange information and make this situational awareness information available to partners
- Facilitate coordination and cooperation in major Internet security events
- Work with vulnerability reporters, partners, and vendors to resolve vulnerabilities
- Provide direct support to response and recovery operations following major cyber failures in national infrastructure

© 2004 by Carnegie Mellon University

AIRCERT

Technology needed to handle exponential growth in incidents & develop systems of indications and warnings



Key Ideas

Open-source infrastructure to automatically gather & report security events from Internet sites to the CERT/CC

Reduce the burden on security analysts by automatically handling well-understood attacks

Spot problems not visible from a local perspective

Use and Status

Gather structured, security incident data for analysis to identify current trends, scope of a specific widespread incident, & predictive indicators for attacks

Completed proof-of-concept prototype; some components being tested by the Internet community, piloting with GSA & agencies

© 2004 by Carnegie Mellon University

US-CERT: Sharing Incident and Sensor Data

- Work to improve capabilities to share incident and sensor data, and monitor and improve the health of the Internet
- Advance standards for incident data exchange
- Encourage vendors to adopt these standards
- Share incident and network sensor data among partners with appropriate sanitization
- Develop better analysis capabilities for analyzing collected data

© 2004 by Carnegie Mellon University

US-CERT: Vulnerability Discovery and Reduction (1)

- Work with partners and the private sector to significantly reduce vulnerabilities in:
  - commercial off-the-shelf software
  - software used by critical infrastructures
- Identify, develop, and promote use of tools that are effective in reducing vulnerabilities in software
- Assemble collection of existing/emerging tools that can strengthen current software quality evaluation schemes
- Test key technologies currently in use, or planned for use, in our critical infrastructures

© 2004 by Carnegie Mellon University

US-CERT: Vulnerability Discovery and Reduction (2)

- **Share best practices for secure programming with software development managers**

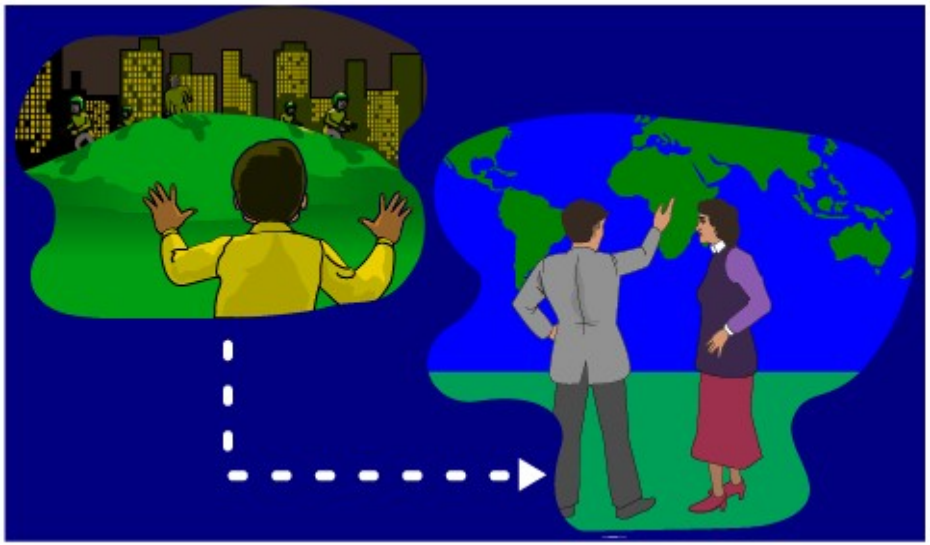
- **Establish a vulnerability discovery lab**
  - **demonstrate the effectiveness of methods and tools**
  - **identify latent vulnerabilities in deployed technologies**
  - **identify vulnerabilities in products under development**

© 2004 by Carnegie Mellon University

CERT® Analysis Center

Need

Attacks occur at Internet speed and cause major damage within reaction cycles; we need predictive and preventative capability



Key Ideas

Augment existing, inadequate, IDS technology

Dynamically adjust for rapid changes in environment

Protection against new threats

Use and Status

Studying feasibility of data collection, reduction & fusion processes

Initial pilot successful at identifying severe operational anomalies & previously undetected probes

© 2004 by Carnegie Mellon University

Survivable Systems Initiative

A major initiative of the SEI as a Federally Funded Research and Development Center (FFRDC) funded by DOD
An important component of this initiative is:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2004 by Carnegie Mellon University

Survivability

The ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, accidents, and failures

© 2004 by Carnegie Mellon University

Initiative Goal

Ensure that appropriate technology, systems management practices, and supporting infrastructures are used to limit damage and to ensure continuity of critical services in the presence of attacks, accidents, and failures

© 2004 by Carnegie Mellon University

Critical Need for Better Engineering Methods

Sophisticated intruders target

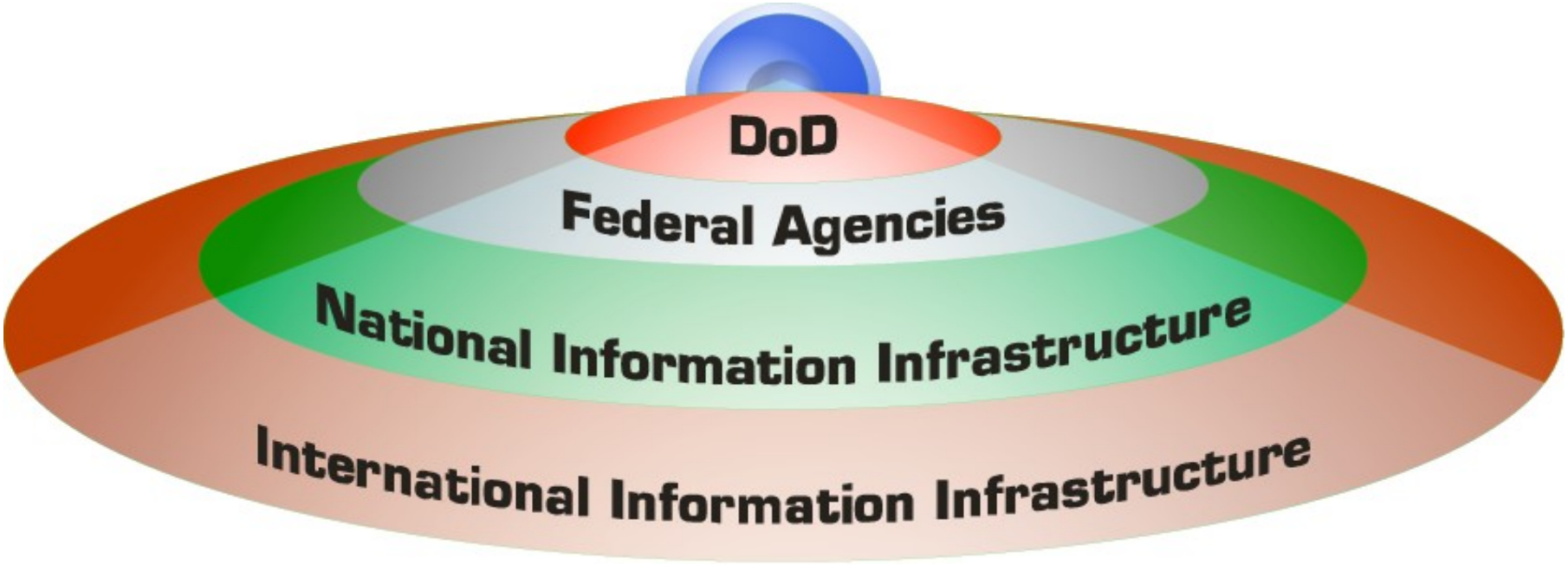
- **distributed user workflows**
- **trust relationships among distributed systems**
- **limited visibility into and control of remote systems**
- **people and the meaning they assign to content**
- **work resources that people rely on**

Many organizations rely solely on insufficient boundary control and "bolt-on" mechanisms as defense

Resistance, recognition, and response must be integrated into the system and application architecture

© 2004 by Carnegie Mellon University

CERT/CC Field of Vision

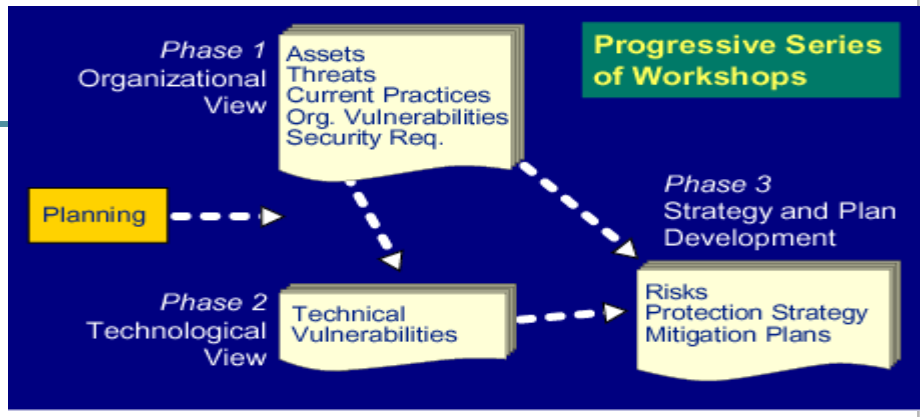


© 2004 by Carnegie Mellon University

OCTAVE℠

Need

Effective security management programs must be sensitive to mission and overall objectives.



Key Ideas

Information security must be linked to an organization's mission & business objectives for effective planning

Enable interdisciplinary teams to perform information security risk evaluations & act as a focal point for improvement efforts

Use and Status

Actively piloting in DoD, government, & industry sectors

Created first derivative method: OCTAVE-S for small organizations

Offering training

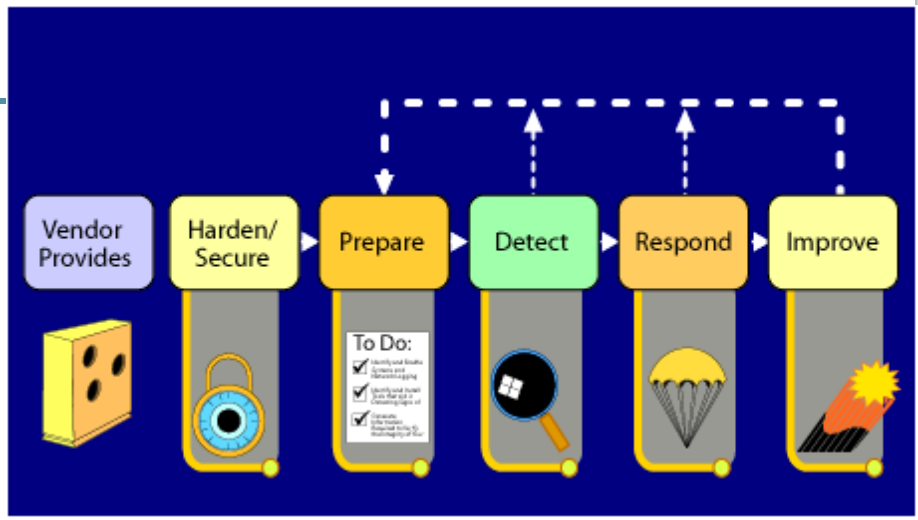
Seeking transition opportunities

© 2004 by Carnegie Mellon University

Security Practices

Need

Pervasive understanding of security policy, management practices and technical practices



Key Ideas

Organizations can improve the security & survivability of networked systems by adopting CERT® security practices

Use and Status

Practices are published on the web & taught in training courses

Working on certification standards

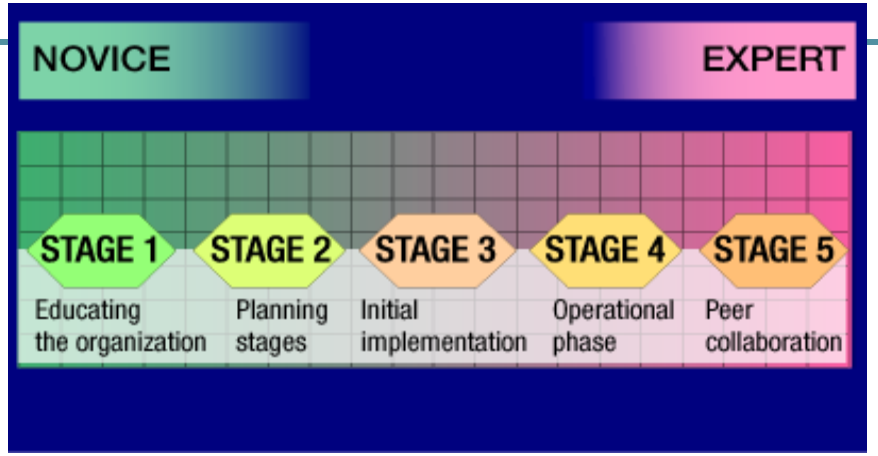
Seeking DoD pilot sites & transition opportunities

© 2004 by Carnegie Mellon University

CSIRT Development

Need

Organizations need teams to respond to computer security incidents



Key Ideas

Develop a community of CSIRTs to share resources and respond to global incidents

Engage organizations as partners depending on the maturity of their CSIRT capability

Use and Status

Assisting DoD and other sectors to develop a certification and accreditation process for CSIRTs

Using CSIRT training courses as a transition mechanism for our knowledge and experience

© 2004 by Carnegie Mellon University

Training

Need

Improve the information security skills of technical staff and managers to address the increasing gap between core competencies required and number of qualified personnel

- Concepts and Trends in Information Security
- Information Security for Technical Staff
- Managing Risks to Information Assets
- Executive Role in Information Security: Risk and Survivability
- Computer Security Incident Handling for Technical Staff
- Computer Security Incident Handling for Technical Staff-Adv
- Managing Computer Security Incident Response Teams
- Creating a CSIRT Team
- Overview of Managing a CSIRT

Key Ideas

Approaches exist to protect critical information assets and systems

All levels of staff need training to facilitate adoption of security practices

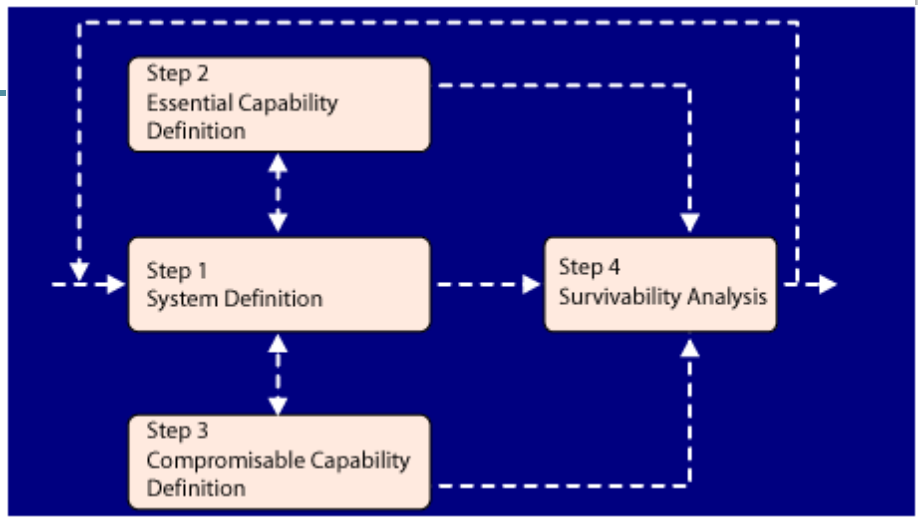
Use and Status

Offering public and customer deliveries

Seeking transition and licensing partners

© 2004 by Carnegie Mellon University

Survivable System Engineering



Need

Structured, repeatable methods to identify architectural & design changes that enhance a system's survivability

Key Ideas

Focus on survivable architectures for loosely coupled & unbounded systems

Support evolution of survivable architectures as requirements & technologies change

Use and Status

Understand survivability risks to a system architecture & identify mitigating strategies

SSE version 1.0 documented; short tutorial developed; pilots ongoing

Seeking transition opportunities

© 2004 by Carnegie Mellon University

How To Contact Us

US mail:	**Networked Systems Survivability** **Software Engineering Institute** **Carnegie Mellon University** **4500 Fifth Avenue** **Pittsburgh, PA 15213-3890 USA**
FAX:	**+1 412 268 6989**
Web site:	**http://www.cert.org** **http://www.us-cert.gov**

CERT/CC Incident Handling

Email:	cert@cert.org
24-hour hotline:	+1 412 268 7090 CERT personnel answer 8:30 AM - 5:00 PM EST(GMT-5)/EDT (GMT-4) Mon.-Fri. On call for emergencies during other hours.

© 2004 by Carnegie Mellon University