Cyber Security—Reality and Perspectives

Universidad Carlos III-SPIN

Ángel Jordán

Madrid, June 24 2004

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.

Outline of the Presentation

- Overview of the SEI
- The Threat of Cyberterrorism and Internet Attacks
- Cyberterrorism?
- The Cyber Environment
- Security and Survivability
- Statistics---Incident Trends
- The Administrative Overload because of the Incident Trends
- Intrusion Detection
- CERT (Computer Emergency Response Team) Advisories (Alerts)
- Cyberterror Vulnerabilities
- The Software Engineering Institute and Cyber Security
- CERT Centers
- CERT Coordination Center
- US-CERT
- AIRCERT (Automatic Incident Response CERT)
- CERT Analysis Center
- Survivable Systems Initiative
- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)
- CSIRT (Computer Security Incident Response Team) Development
- Training
- Survivable Systems Engineering
- Conclusions

Overview of the SEI

Angel Jordan
University Professor Emeritus
Provost Emeritus, Carnegie Mellon University
Acting Director
Software Engineering Institute
ajordan@sei.cmu.edu
www.sei.cmu.edu
412-268-7740

Sponsored by the U.S. Department of Defense

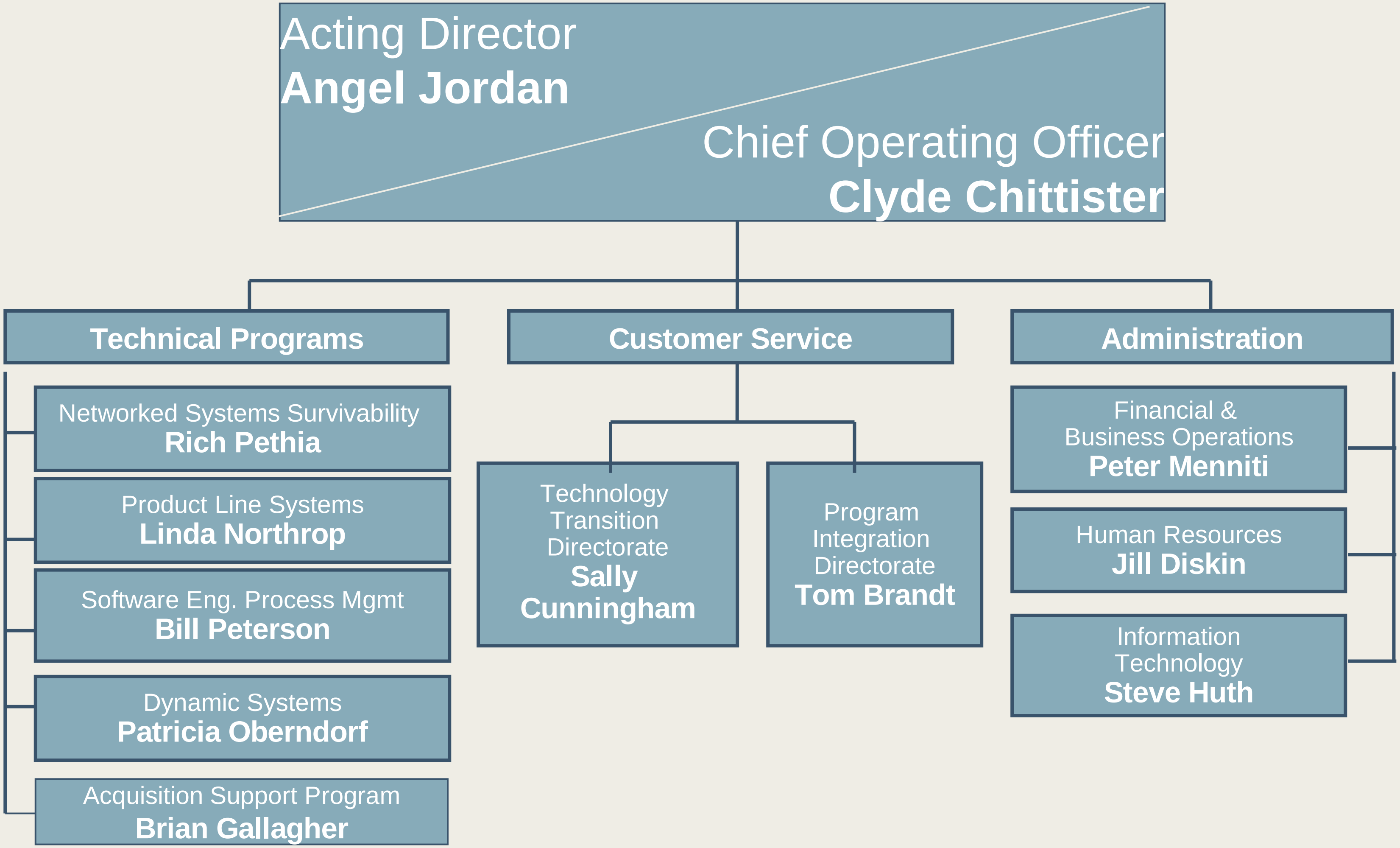
Software Engineering Institute

Applied R&D laboratory, Federally Funded R&D Center, at Carnegie Mellon University, Pittsburgh PA

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

Encouraged to support industry in precompetitive technology and in technology activities

SEI Organization Chart



Acting Director
Angel Jordan

Chief Operating Officer
Clyde Chittister

Technical Programs

- Networked Systems Survivability **Rich Pethia**
- Product Line Systems **Linda Northrop**
- Software Eng. Process Mgmt **Bill Peterson**
- Dynamic Systems **Patricia Oberndorf**
- Acquisition Support Program **Brian Gallagher**

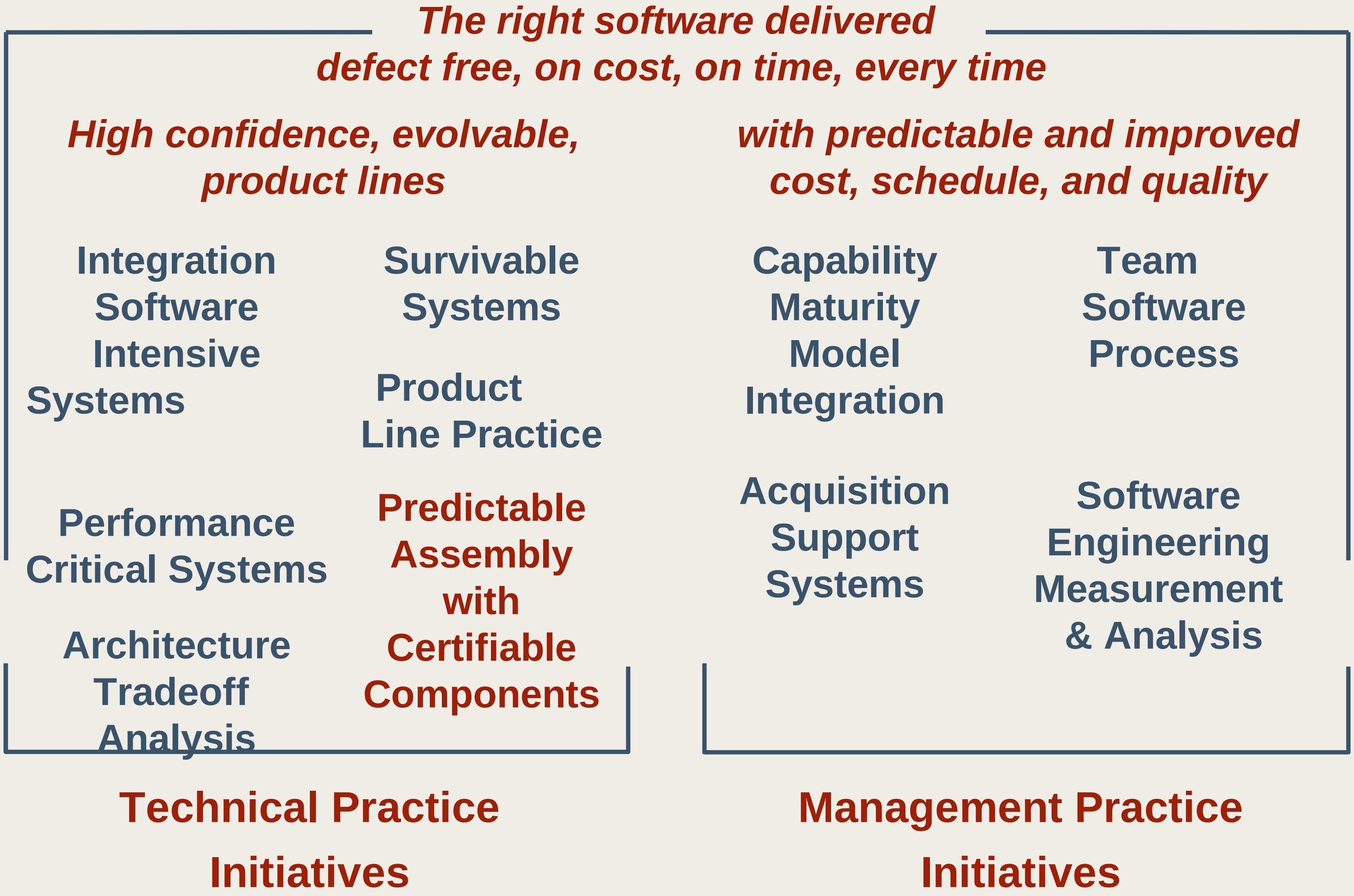
Customer Service

- Technology Transition Directorate **Sally Cunningham**
- Program Integration Directorate **Tom Brandt**

Administration

- Financial & Business Operations **Peter Menniti**
- Human Resources **Jill Diskin**
- Information Technology **Steve Huth**

SEI Technical Program



The right software delivered defect free, on cost, on time, every time

High confidence, evolvable, product lines

with predictable and improved cost, schedule, and quality

Integration Software Intensive Systems

Survivable Systems

Product Line Practice

Performance Critical Systems

Predictable Assembly with Certifiable Components

Architecture Tradeoff Analysis

Capability Maturity Model Integration

Team Software Process

Acquisition Support Systems

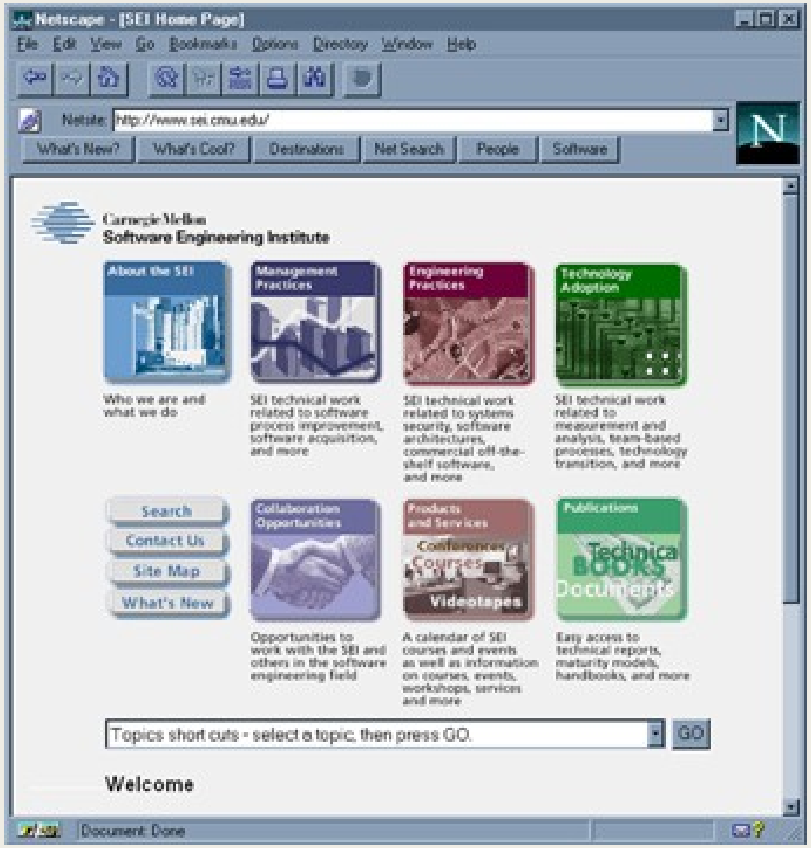
Software Engineering Measurement & Analysis

Technical Practice Initiatives

Management Practice Initiatives

Carnegie Mellon
Software Engineering Institute

Visit Our Web Site


Netscape - [SEI Home Page]
File Edit View Go Bookmarks Options Directory Window Help
Netsite: http://www.sei.cmu.edu/
What's New? What's Cool? Destinations Net Search People Software
Carnegie Mellon
Software Engineering Institute
About the SEI
Management Practices
Engineering Practices
Technology Adoption
Search
Contact Us
Site Map
What's New
Collaboration Opportunities
Products and Services
Conferences
Courses
Videotapes
Publications
Technical
BOOKS
Documents
GO
Welcome
Document: Done

Who we are and what we do

SEI technical work related to software process improvement, software acquisition, and more

SEI technical work related to systems security, software architectures, commercial off-the-shelf software, and more

SEI technical work related to measurement and analysis, team-based processes, technology transition, and more

Opportunities to work with the SEI and others in the software engineering field

A calendar of SEI courses and events as well as information on courses, events, workshops, services and more

Easy access to technical reports, maturity models, handbooks, and more

Topics short cuts - select a topic, then press GO.

For more information contact:

Angel Jordan
ajordan@sei.cmu.edu
412-268-7740

http://www.sei.cmu.edu

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**

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**

The Cyber Environment

“Urban Sprawl” in Cyberspace

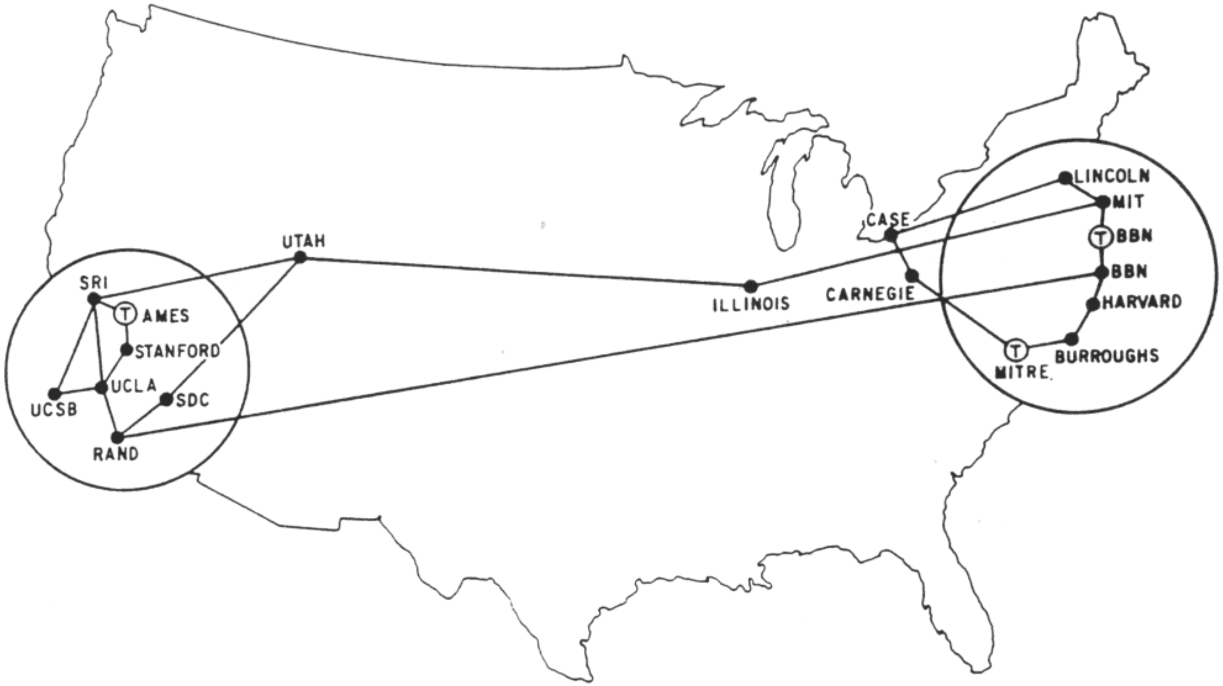
- Cyberspace has grown exponentially in recent years, now especially with wireless technologies

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

The Environment – Old Structure

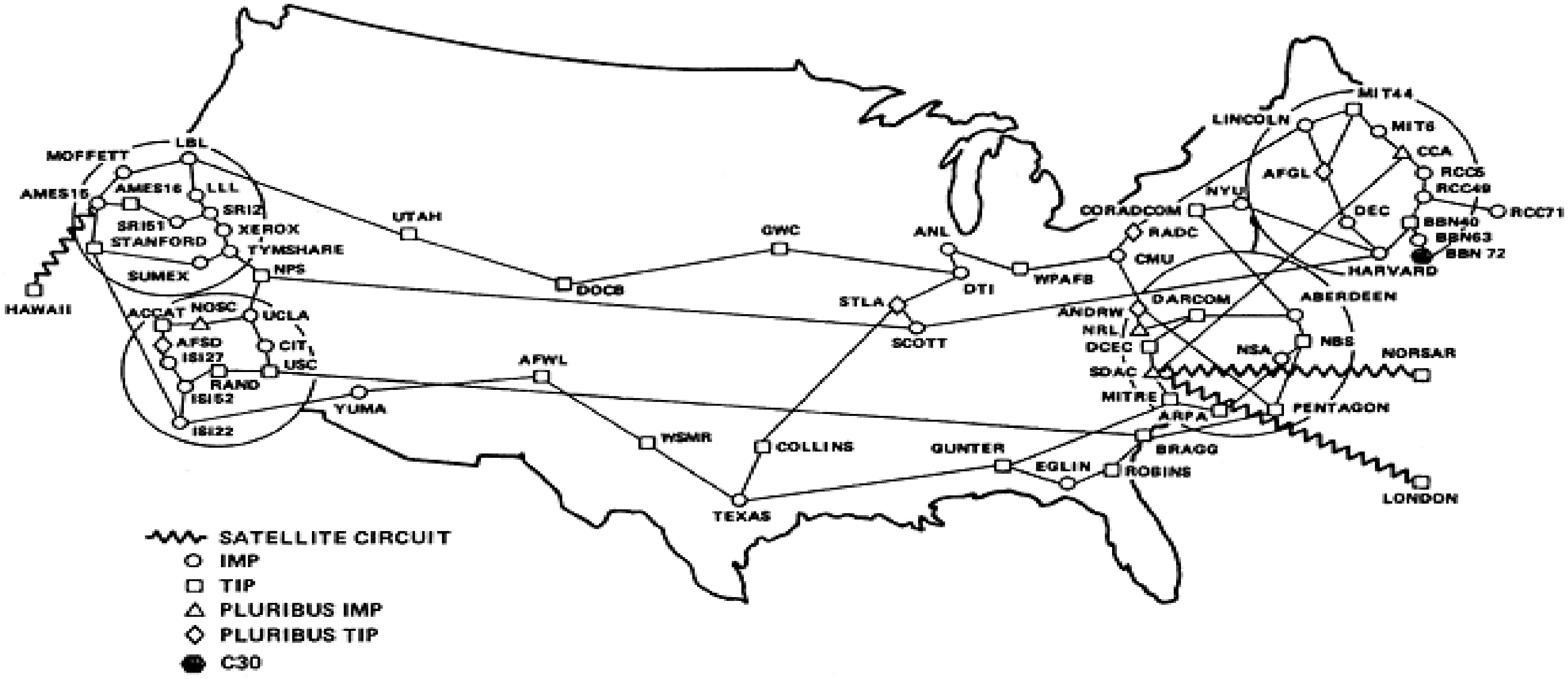
The Net Then – ARPANET 1971



MAP 4 September 1971

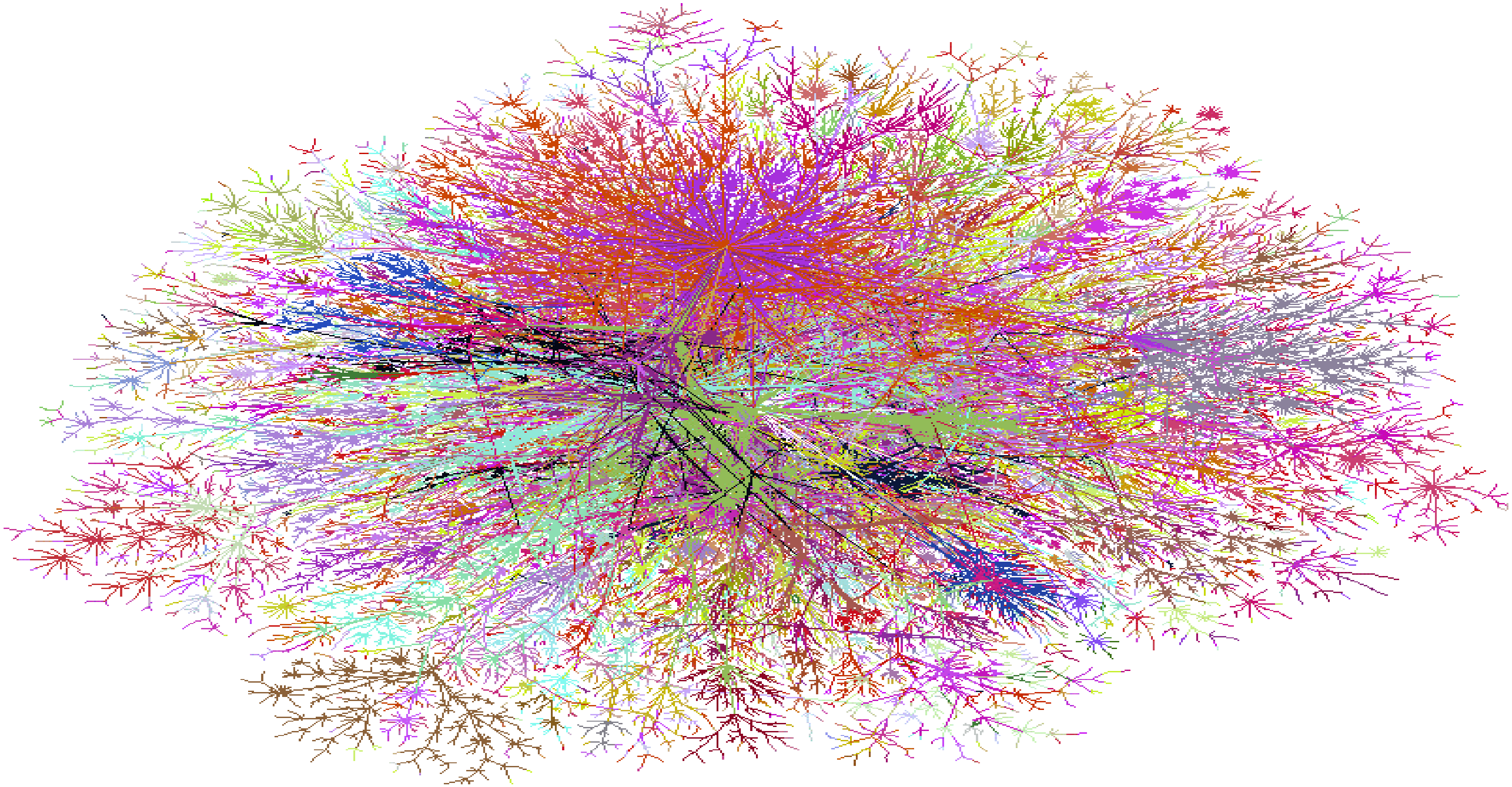
The Old ’Net

ARPANET GEOGRAPHIC MAP, OCTOBER 1980



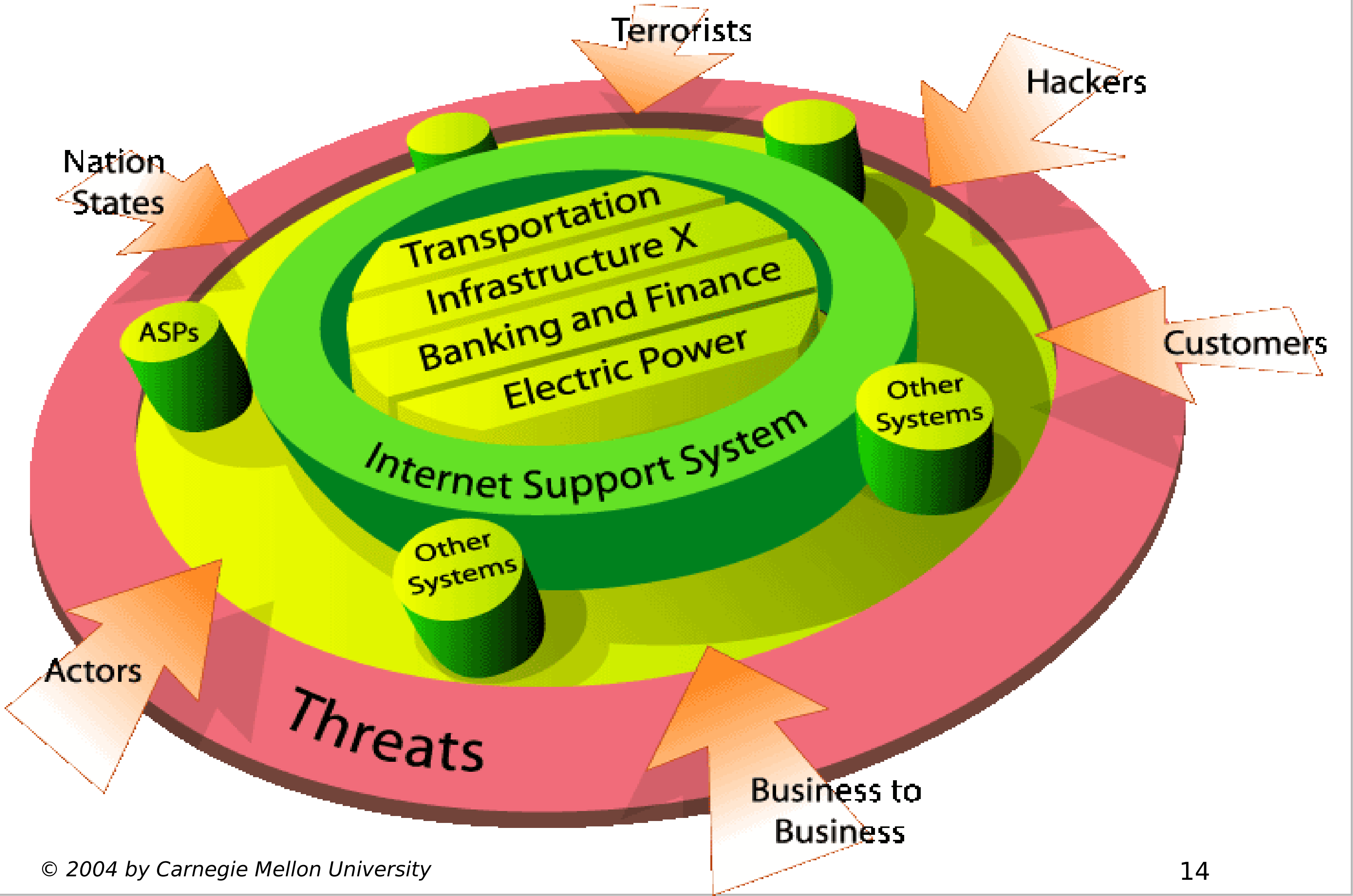
(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

The New Net-Still Growing



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

Internet Integrated Infrastructure Threat Environment



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**

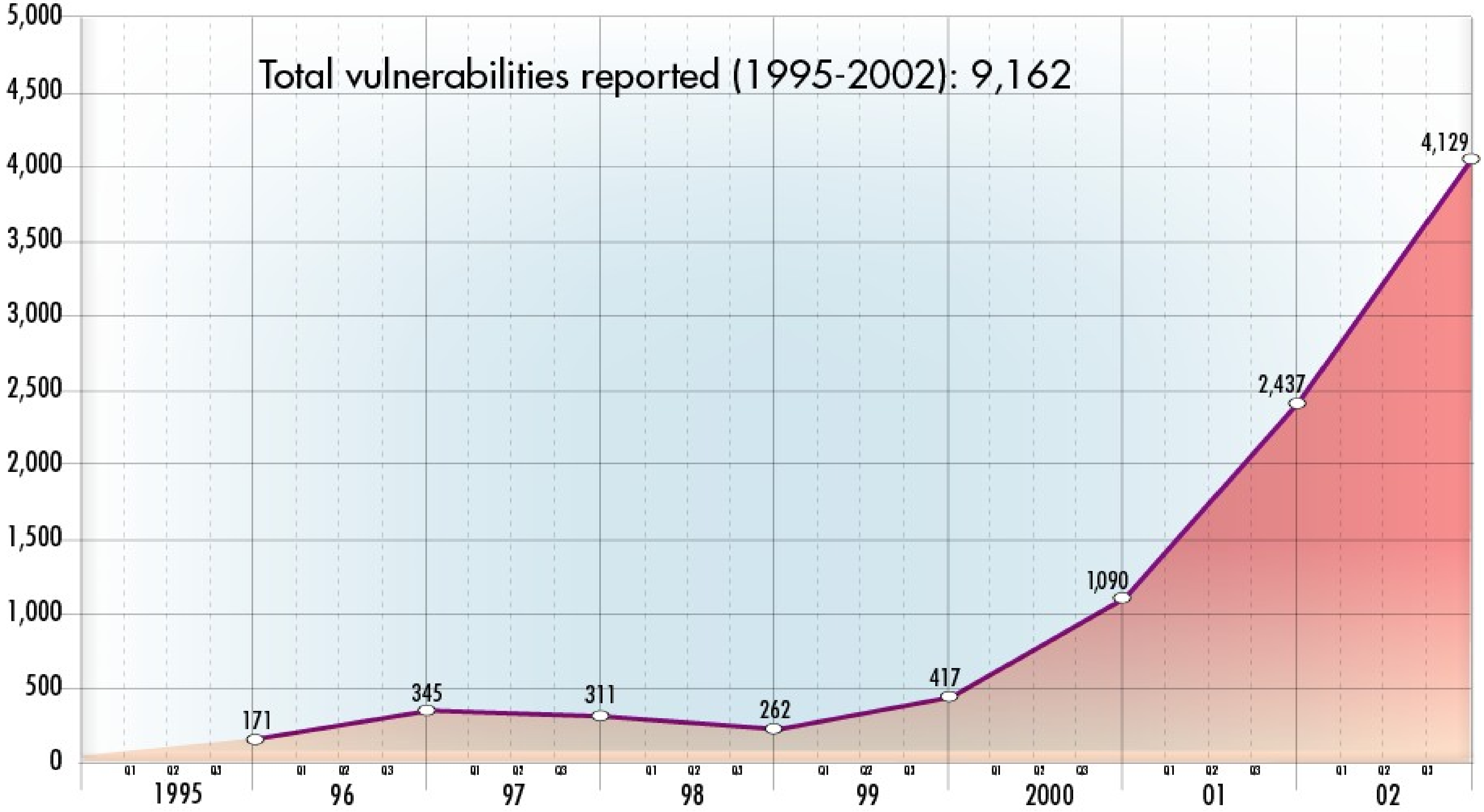
- **The Information Infrastructure is designed for efficiency and functionality, *not* for security or survivability**

The Threat - Statistics

How Real is the Threat – the stats

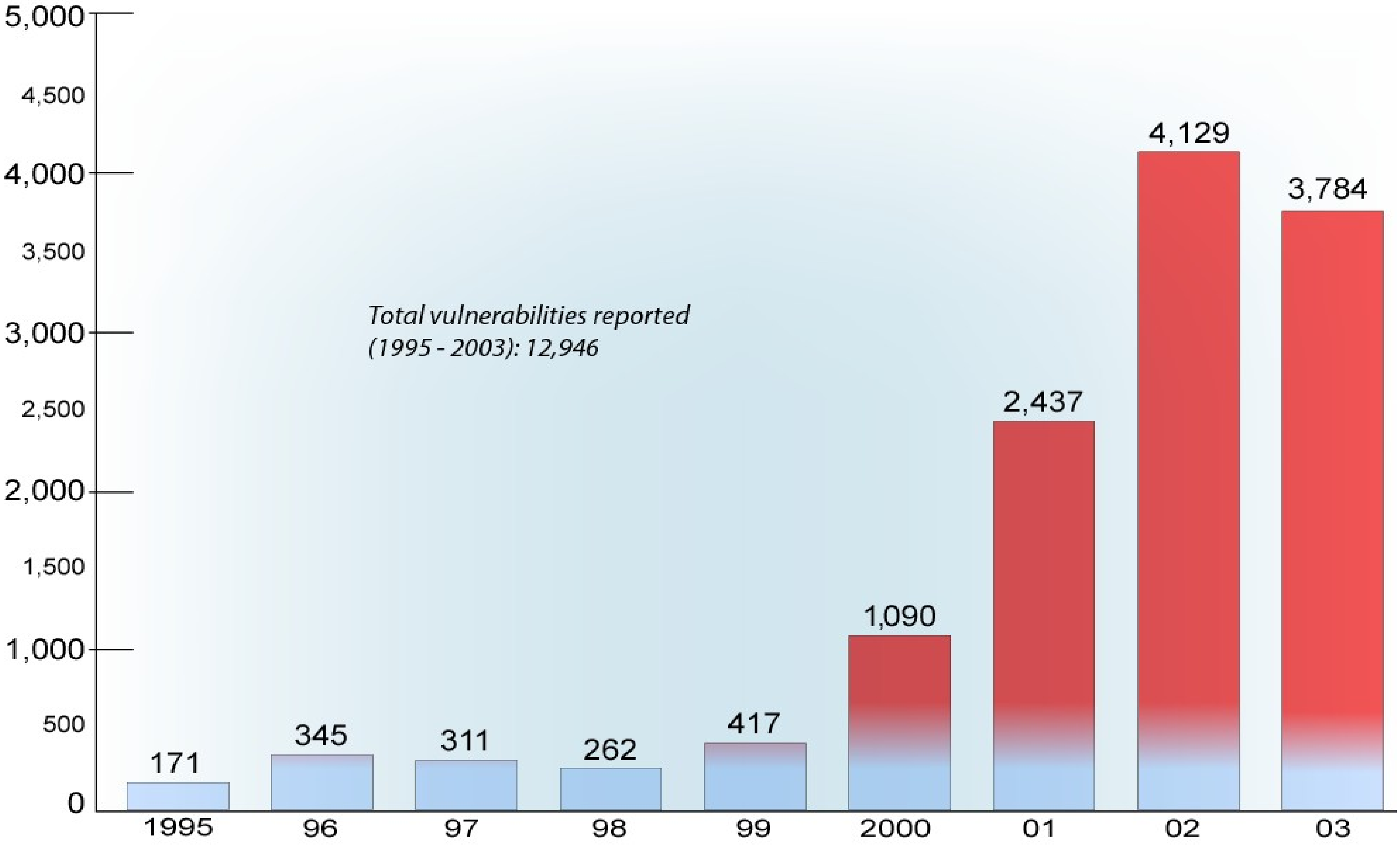
- Incidents and Vulnerabilities reported by the CERT C/C
  - CERT/CC Incident Reports
    - **1988-2000: 47,711**
    - **1999: 9,859**
    - **2000: 21,756**
    - **2001: 52,658**
    - **2002: 82,094**
  - Vulnerabilities Discovered
    - **1995-2000: 2,596**
    - **1999: 417**
    - **2000: 1,090**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

Increasing Vulnerability => Increasing Threat



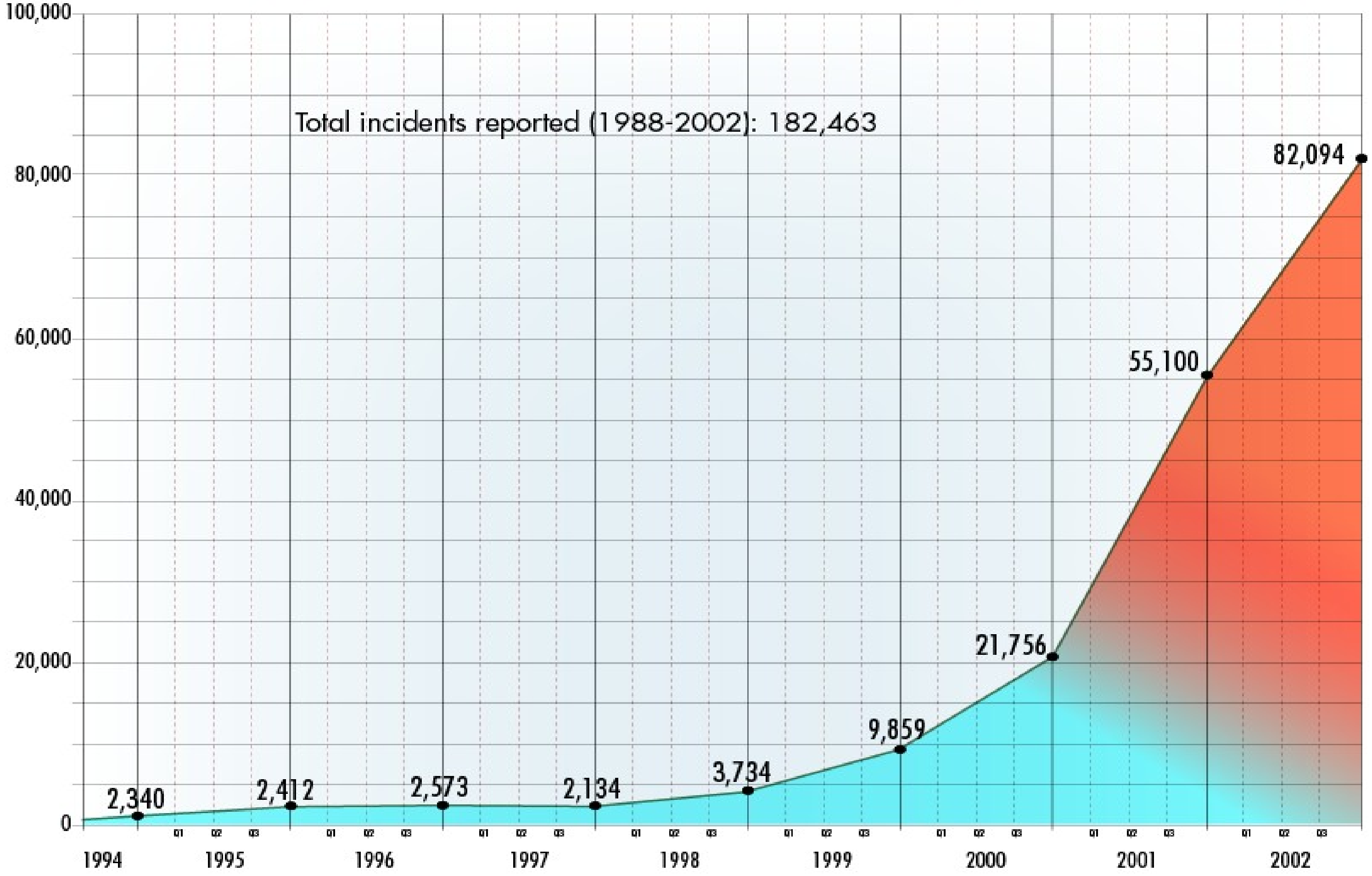
© 2004 by Carnegie Mellon University

Vulnerabilities Reported to the CERT/CC

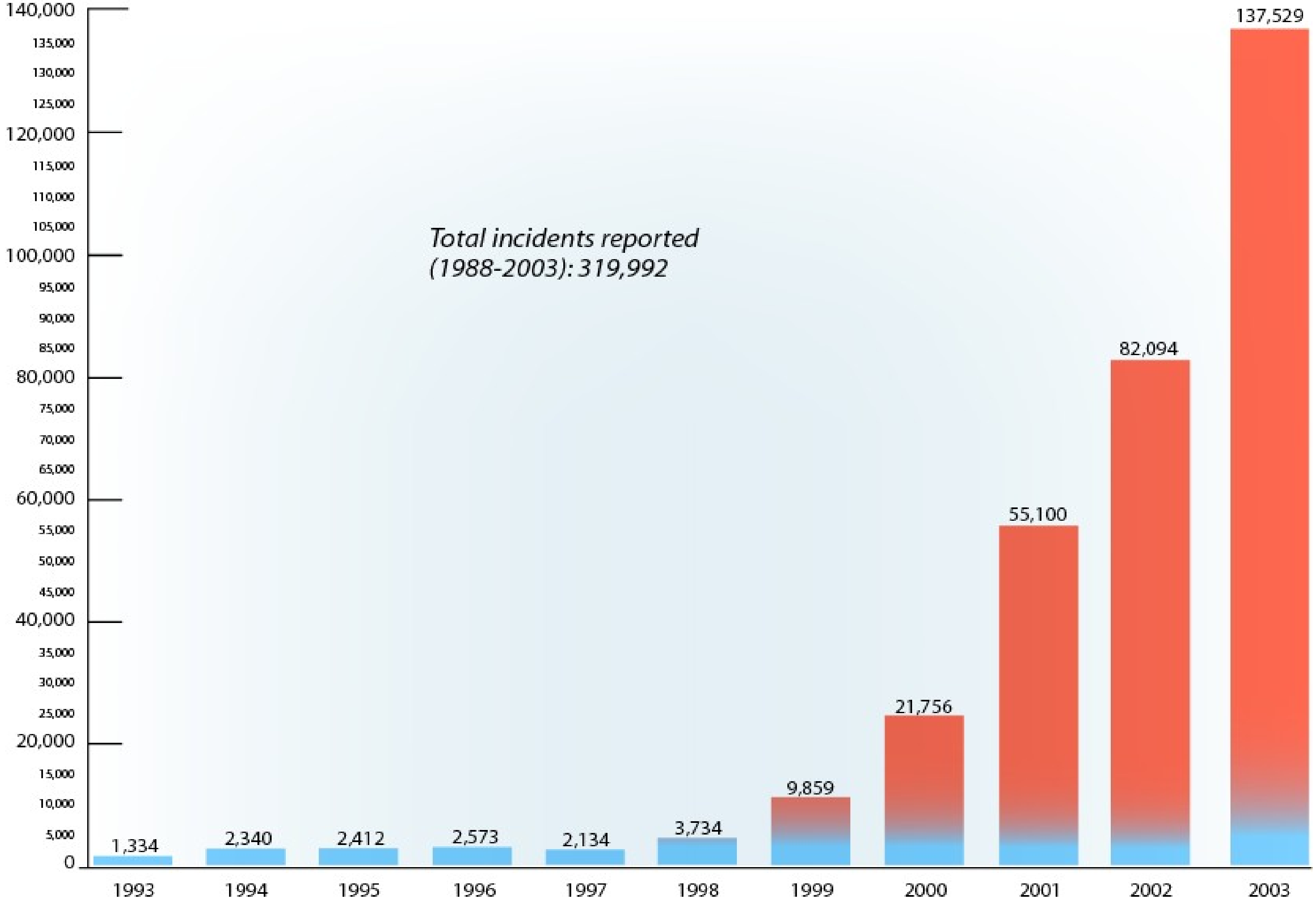


Total vulnerabilities reported (1995 - 2003): 12,946

More Vulnerabilities => More Incidents

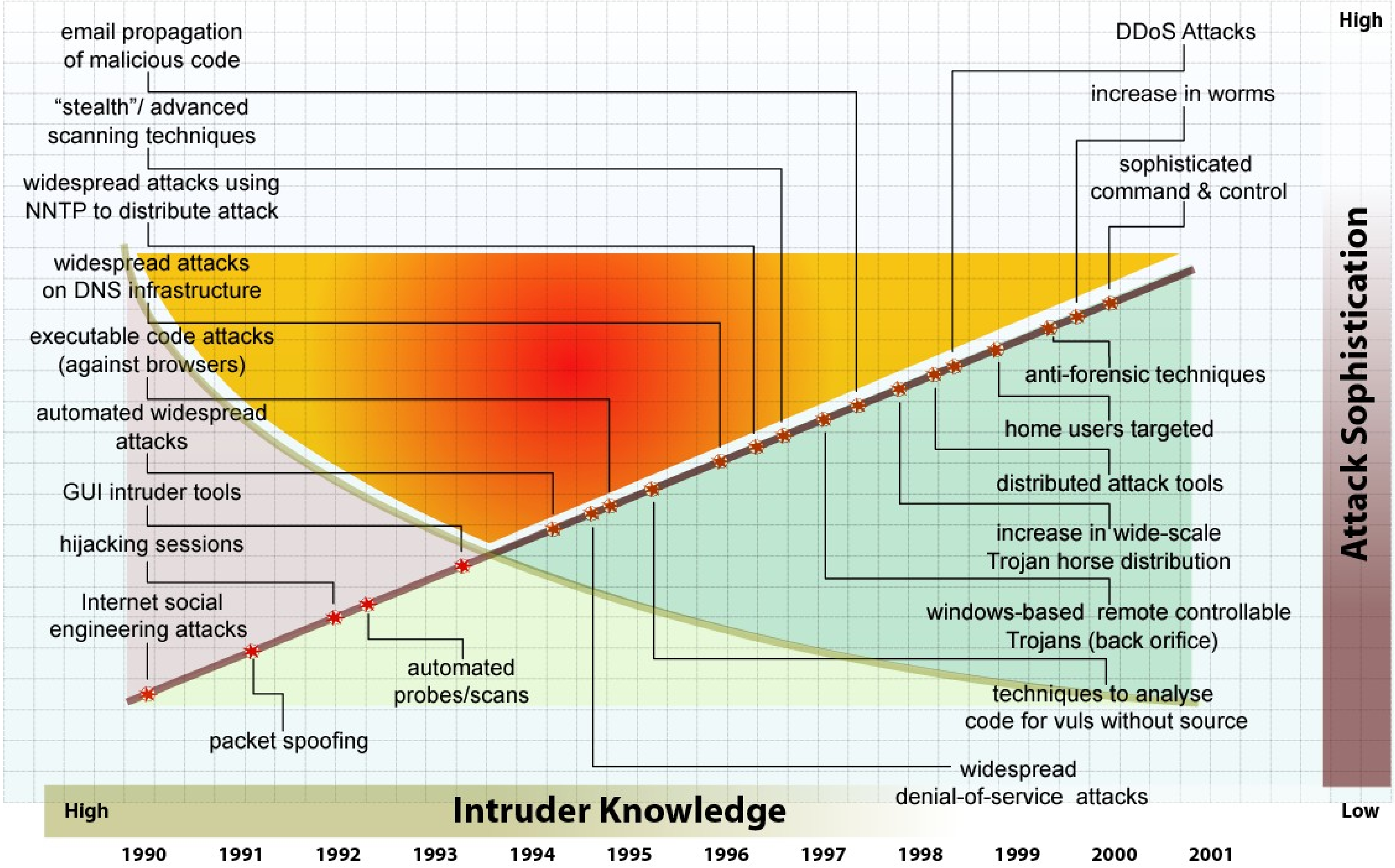


Incidents Reported to the CERT/CC



Total incidents reported (1988-2003): 319,992

Incident Trends are Toward Higher Sophistication



email propagation of malicious code

"stealth"/ advanced scanning techniques

widespread attacks using NNTP to distribute attack

widespread attacks on DNS infrastructure

executable code attacks (against browsers)

automated widespread attacks

GUI intruder tools

hijacking sessions

Internet social engineering attacks

packet spoofing

automated probes/scans

DDoS Attacks

increase in worms

sophisticated command & control

anti-forensic techniques

home users targeted

distributed attack tools

increase in wide-scale Trojan horse distribution

windows-based remote controllable Trojans (back orifice)

techniques to analyse code for vuls without source

widespread denial-of-service attacks

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

Should We Be Concerned?

Attackers well aware of the potential impact of using cyberspace

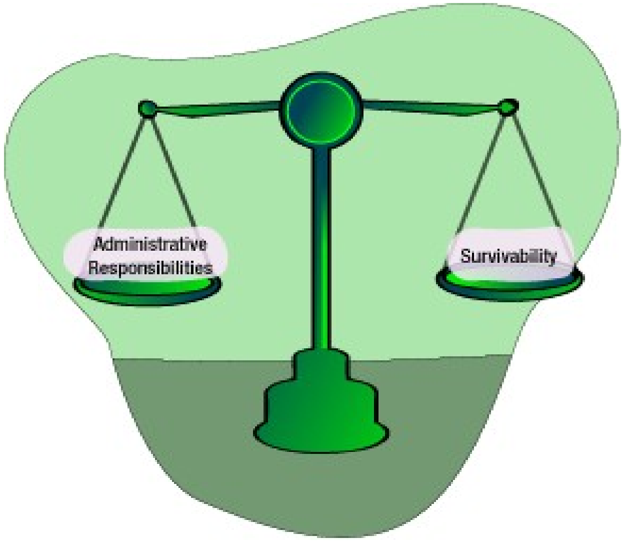
- Nations adding Computer Network Warfare to strategy and doctrine
- Terrorist groups developing cyber capabilities (Al Qaeda)
- Criminal groups have been using cyberspace for years
- Critical Infrastructures prime targets (exploitation and compromise)

We are our own worst enemy

- Websites great source of intelligence

Your Administrative Responsibilities

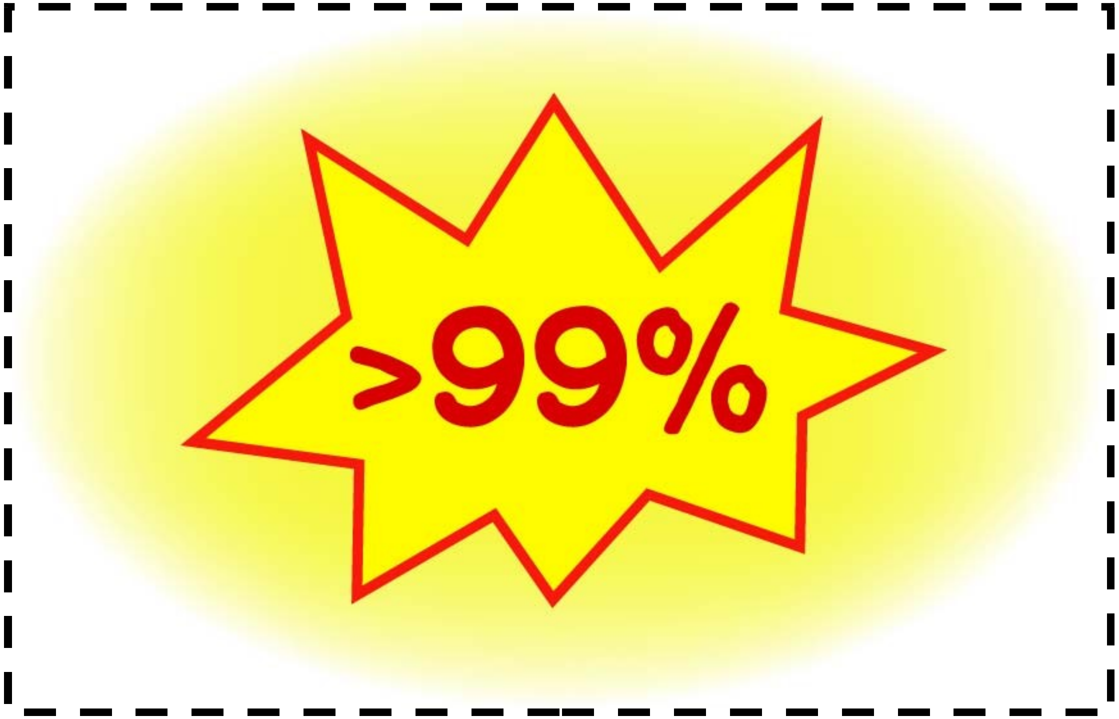
- Monitoring
- Incident response
- Damage assessment and recovery
- Analysis
- System life-cycle management
- Backups, fault tolerance



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

Why Care About Patches



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

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

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)

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

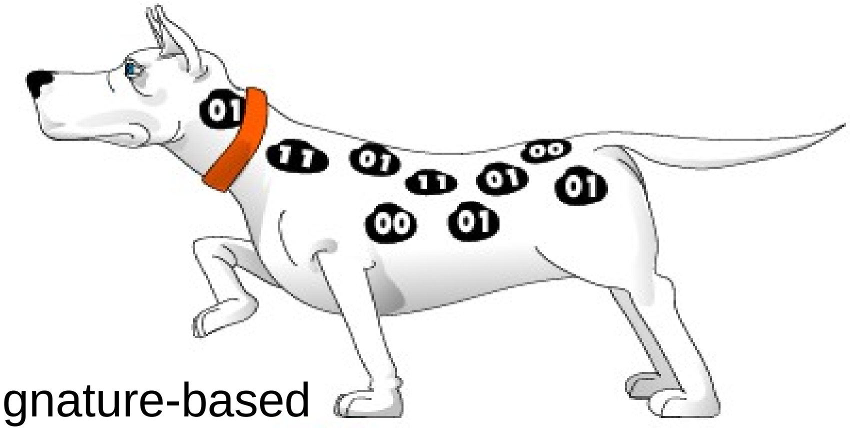
What is an Intrusion Detection System?

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

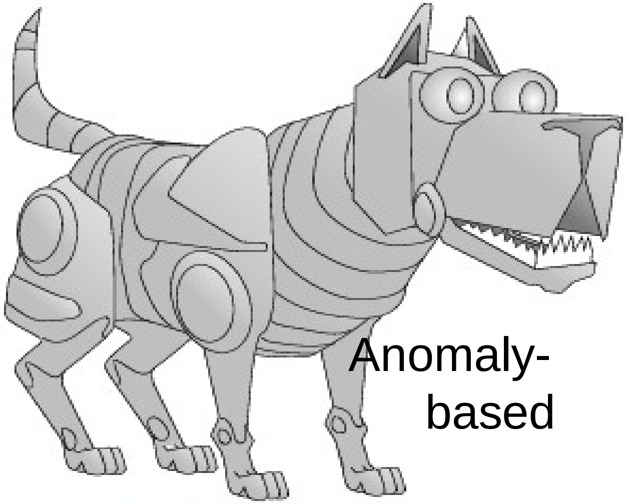
- Malicious traffic, such as attempts to circumvent identification & authorization or other access controls
- Reconnaissance traffic, such as port scans
- Unusual traffic: type, level, source, etc.
- Activity on host systems that is outside of known patterns

Device then logs and reports activity in prescribed manner

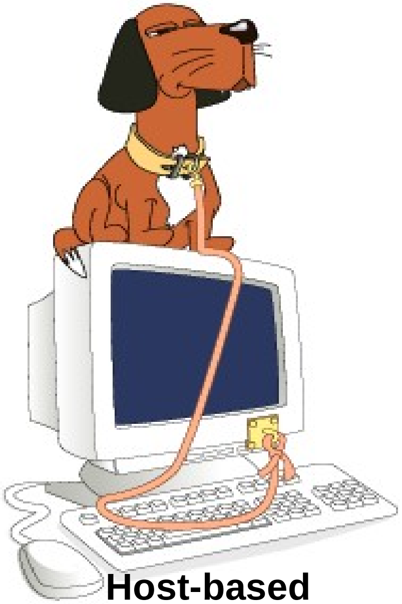
Types of IDS



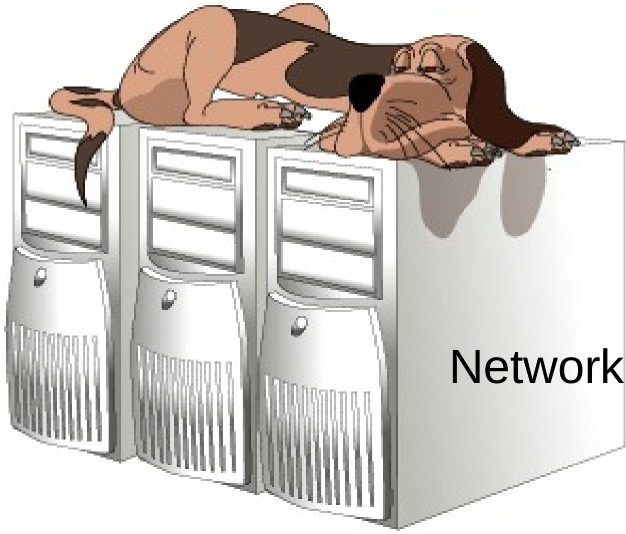
Signature-based



Anomaly-based



Host-based



Network-based

CERT® Advisories (Alerts)

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**

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

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**

Software Engineering Institute

Applied research and development laboratory situated as an integral unit at Carnegie Mellon University

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

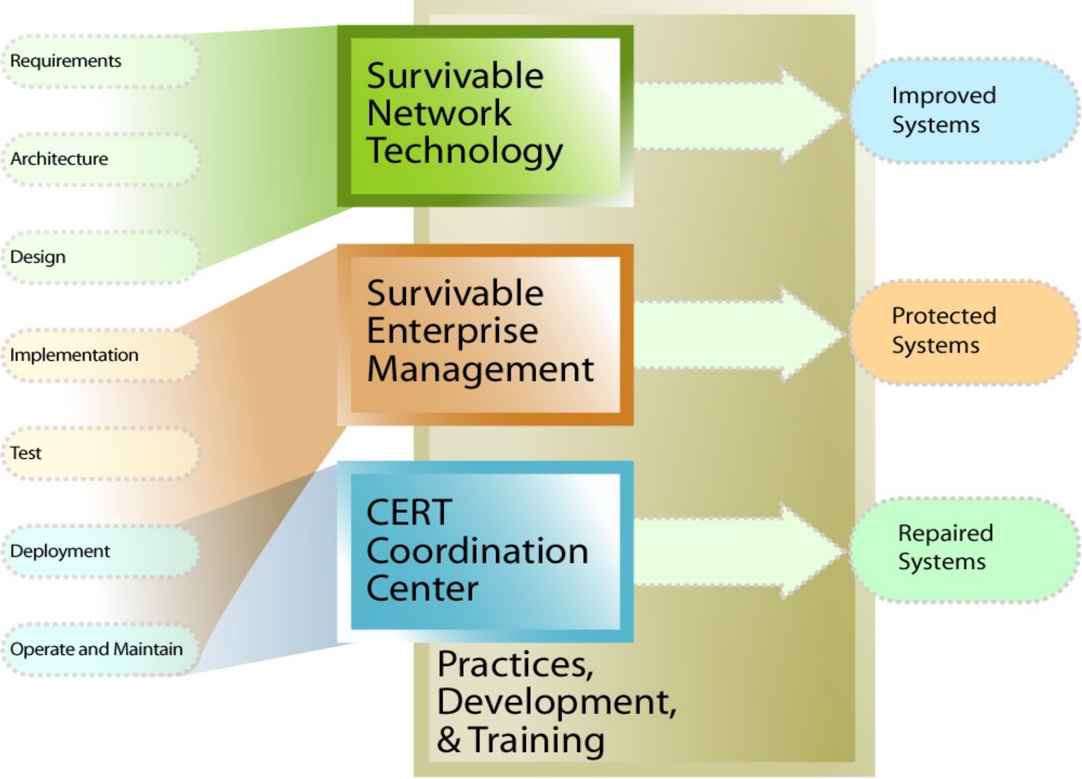
Encouraged to support industry in pre-competitive technology research and development and in technology transition activities

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



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

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

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

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**

US-CERT Focus

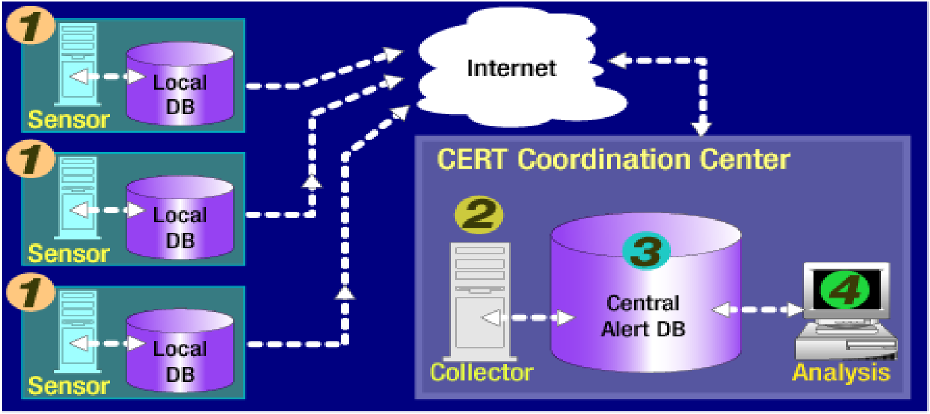
Prevent and mitigate cyber attacks and reduce cyber vulnerabilities by concentrating on four areas:

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

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

AirCERT (Automatic Incident Response CERT)



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

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

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

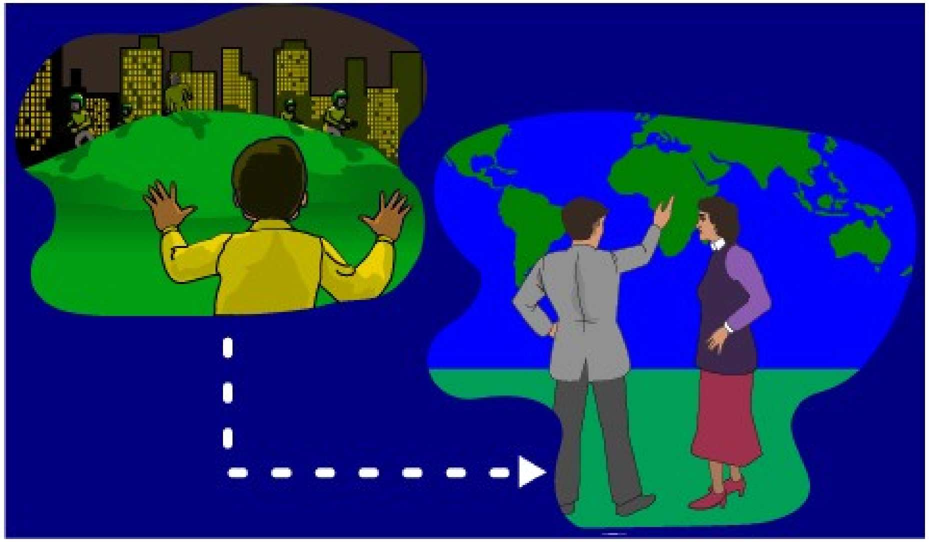
US-CERT: Vulnerability Discovery and Reduction (2)

- 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

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

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

Survivability

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

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

Critical Need for Better Engineering Methods

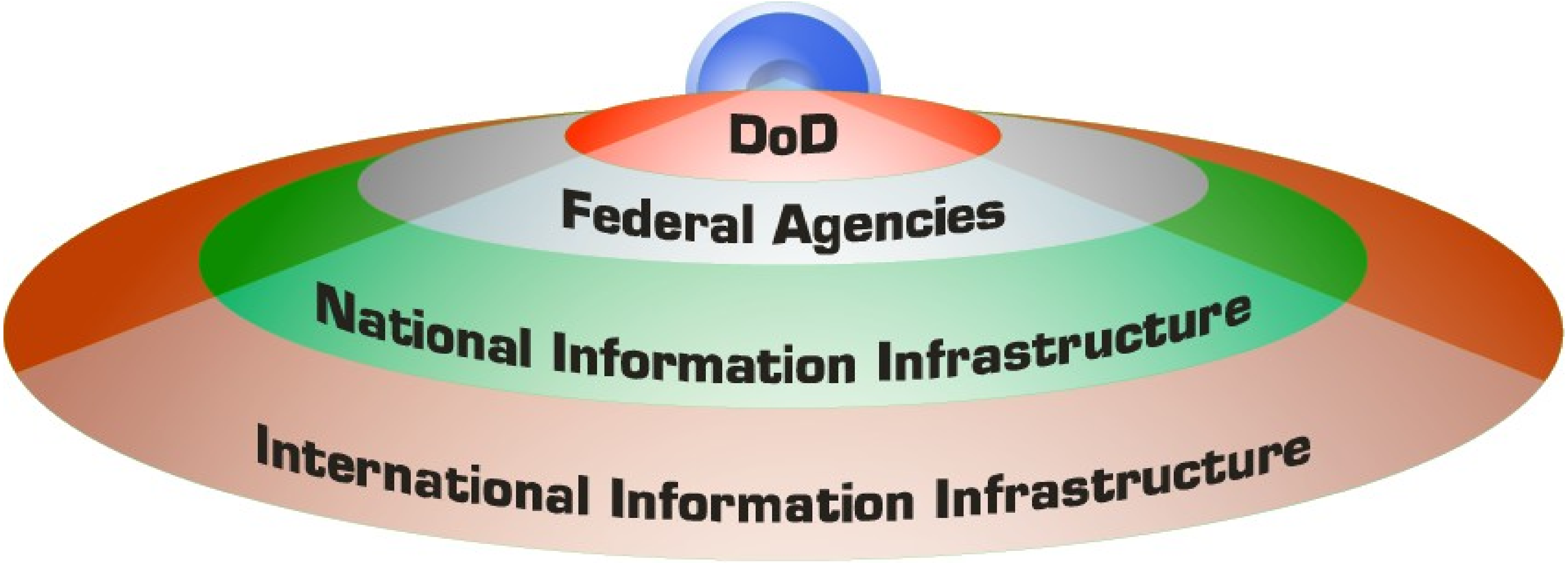
Sophisticated intruders target

- 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

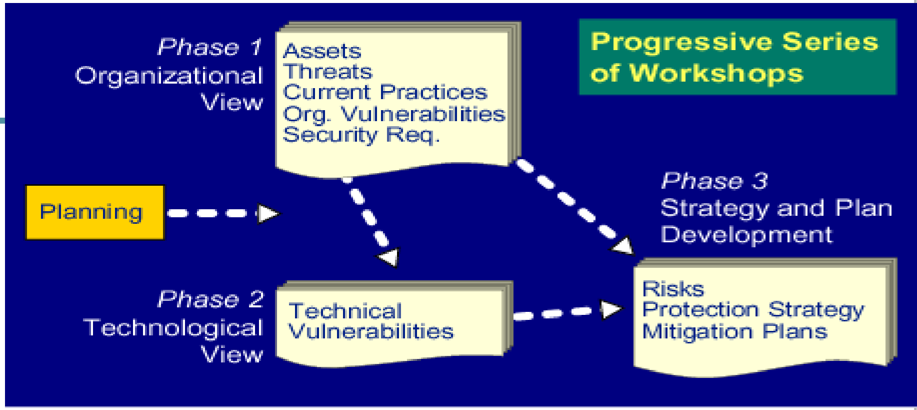
Many organizations rely solely on insufficient boundary control and “bolt-on” mechanisms as defense

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

CERT/CC Field of Vision


DoD
Federal Agencies
National Information Infrastructure
International Information Infrastructure

OCTAVE^{SM}



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

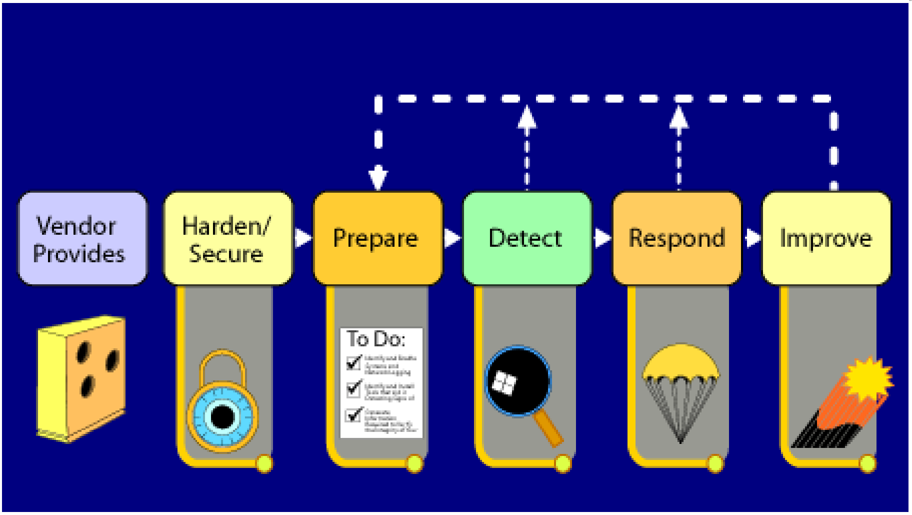
Actively piloting in DoD, government, & industry sectors

Created first derivative method: OCTAVE-S for small organizations

Offering training

Seeking transition opportunities

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

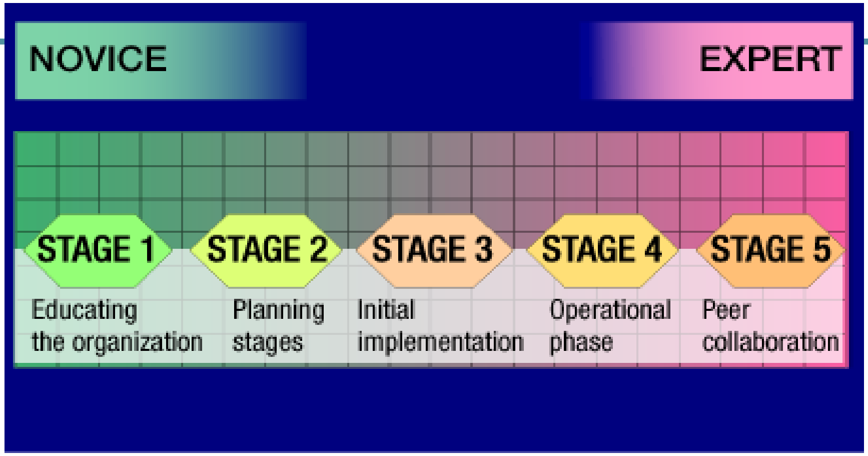
Working on certification standards

Seeking DoD pilot sites & transition opportunities

CSIRT (Computer Security Incident Response Team) 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

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

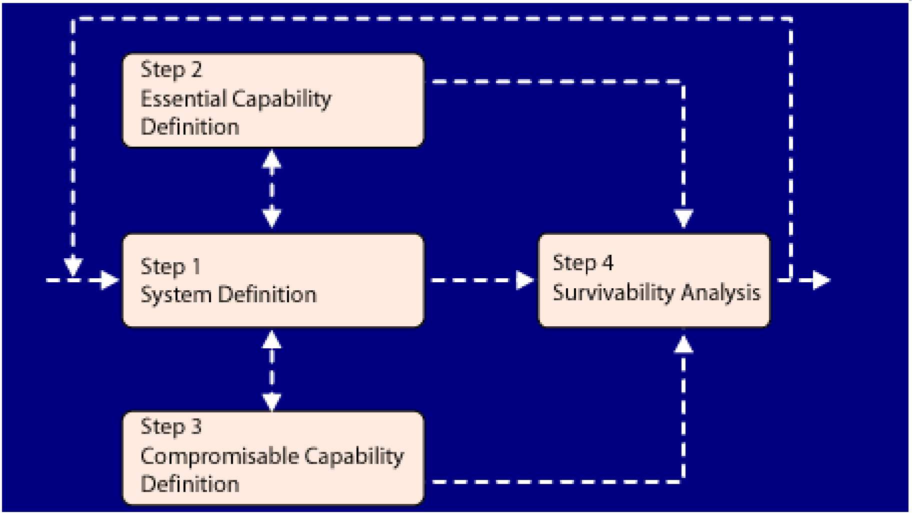
Offering public and customer deliveries

Seeking transition and licensing partners

Survivable System Engineering

Need

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


Step 2
Essential Capability Definition
Step 1
System Definition
Step 4
Survivability Analysis
Step 3
Compromisable Capability Definition

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

Let’s Draw Some Conclusions

- The Internet is growing in an uncontrolled way
- Vulnerabilities and incidents are growing
- Cyberterrorism could happen
- The Overload of System Administrators is growing
- Intrusion Detection Systems are mandatory
- The use of Patches and Workarounds is essential
- CERT Centers play a key role in Cyber Security
- US CERT initiatives promise to play a key role in Cyber Security and in the combat of Cyberterrorism
- Education in Cyber Security is essential
- Systems Survivability has emerged as a new Engineering Discipline

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.