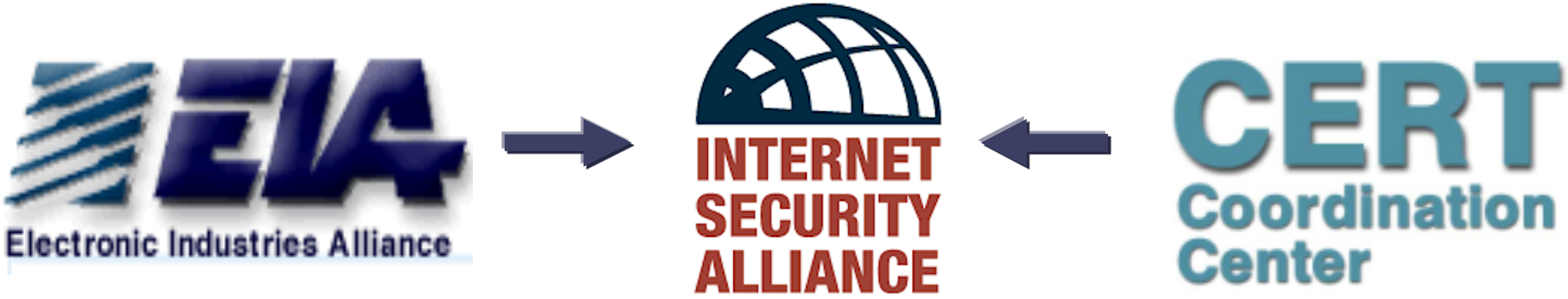
The Internet Security Alliance



The **Internet Security Alliance** is a collaborative effort between Carnegie Mellon University's ***Software Engineering Institute (SEI)*** and its ***CERT Coordination Center (CERT/CC)*** and the ***Electronic Industries Alliance (EIA***), a federation of trade associations with over 2,500 members.

INTERNET
SECURITY
ALLIANCE

Sponsors

AIG

Booz | Allen | Hamilton

CERIDIAN

CABLE & WIRELESS

IBM®

ITT Industries
Engineered for life

Mellon

NAM
National Association
of Manufacturers

NORTHROP GRUMMAN

NASDAQ

NORSK TIPPING

NORTEL
NETWORKS

Raytheon

redsiren
Security. Integrity. Trust.™

Russell

SONY

SINTEF
Telecom and Informatics

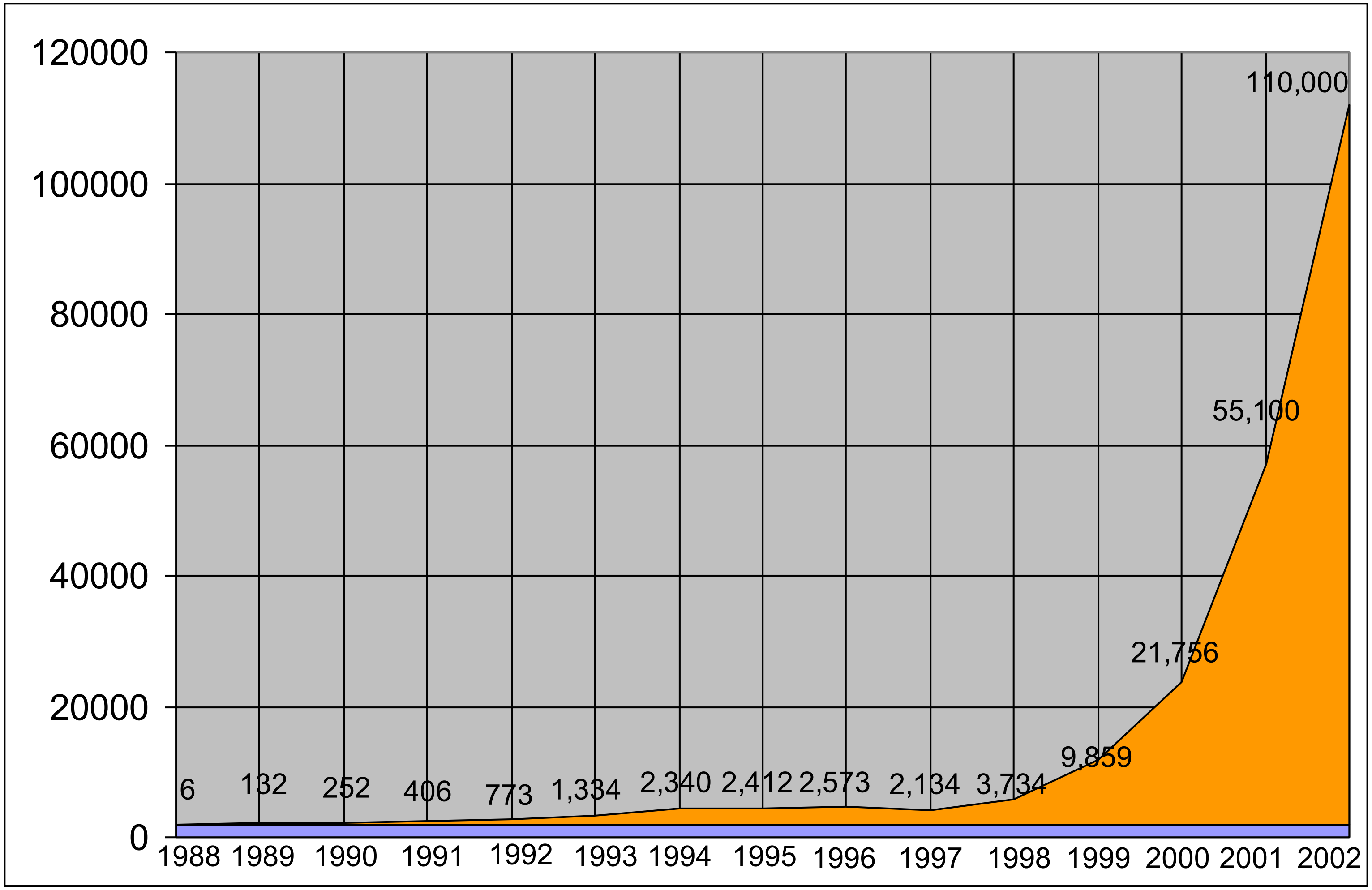
TATA

VISA

VeriSign®

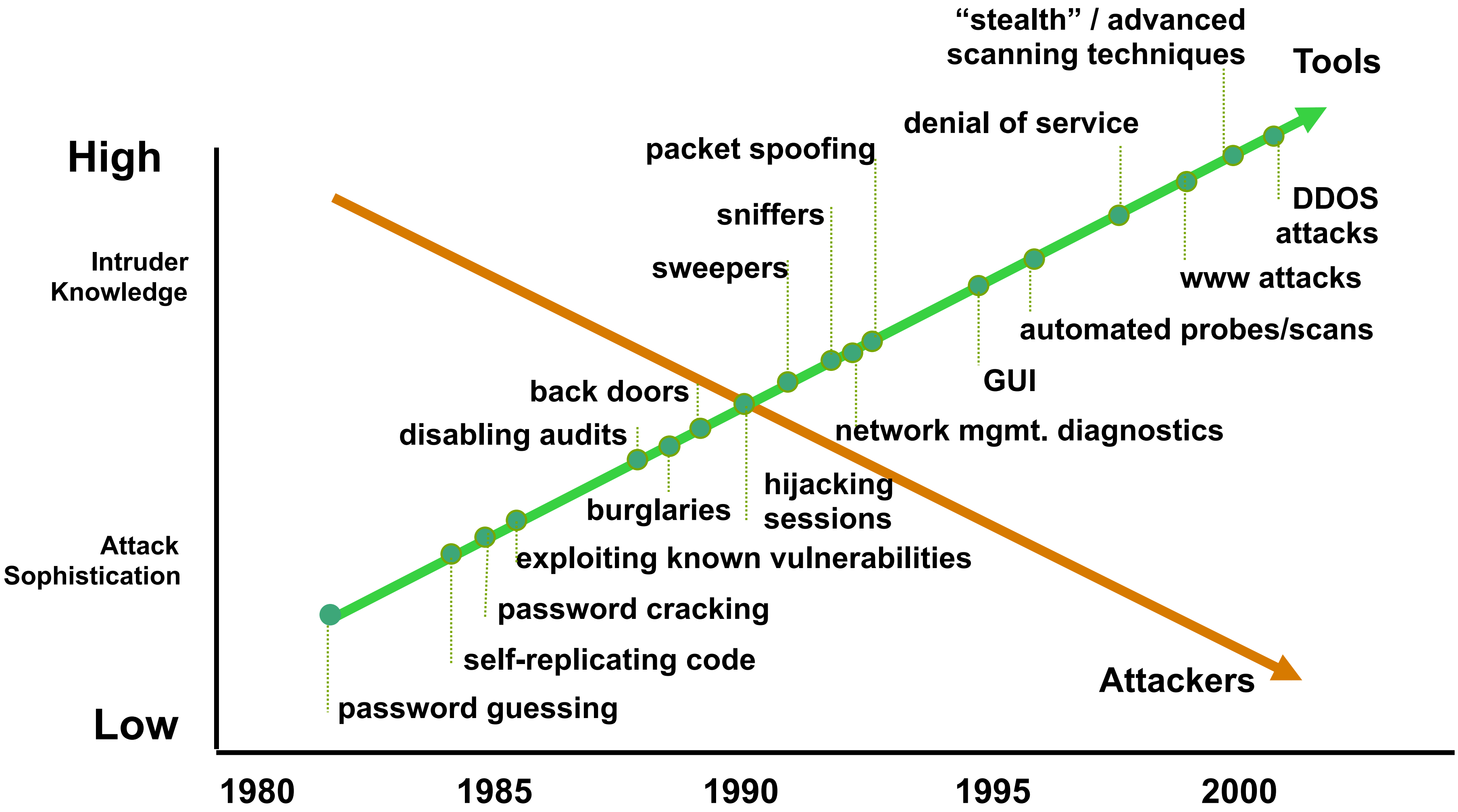
verizon

Growth in Incidents Reported to the CERT/CC



INTERNET SECURITY ALLIANCE

Attack Sophistication v. Intruder Technical Knowledge



INTERNET SECURITY ALLIANCE

Financial Impacts of Attacks

- Klez virus:
  - Clean up and lost productivity: $9 billion
- Code Red: 1 million computers affected
  - Clean-up and lost productivity: $2.6 billion
- Love Bug: 50 variants, 40 million computers affected
  - Clean-up and lost productivity: $8.8 billion
- Nimda
  - Clean-up and lost productivity: $1.2 billion
- Slammer
  - Clean up and lost productivity: $1 billion +

Won’t Advanced Technology Protect Us?

“Installing a network security device is not a substitute for a constant focus and keeping our defenses up to date… There is no special technology that can make an enterprise completely secure.”

– *National Plan to Secure Cyberspace, 2/14/03*

Step 1 Invest in Cyber Security

- US Government increasing spending 64 % for cyber security.

*****

For Business there is a 21% ROI for early incorporation of security

- *CSO Magazine* 12/02

INTERNET SECURITY ALLIANCE

Step 2. Adopt and Implement Best Practices

- Cited in US National Draft Strategy to Protect Cyber Space (September 2002)
- Endorsed by TechNet for CEO Security Initiative (April 2003)
- Endorsed US India Business Council (April 2003)

Common Sense Guide for Senior Managers

INTERNET SECURITY ALLIANCE

Top Ten Recommended Information Security Practices

1st Edition - July 2002

INTERNET SECURITY ALLIANCE

Common Sense Guide Top Ten Practice Topics

- Practice #1: General Management
- Practice #2: Policy
- Practice #3: Risk Management
- Practice #4: Security Architecture & Design
- Practice #5: User Issues
- Practice #6: System & Network Management
- Practice #7: Authentication & Authorization
- Practice #8: Monitor & Audit
- Practice #9: Physical Security
- Practice #10: Continuity Planning & Disaster Recovery

Step 3. Risk Mitigation/Cyber Insurance

1. Are you covered?

Many policies no longer cover cyber

2. Should you be covered?

ISAlliance Cyber-Insurance Program

- Free cyber check up provided by AIG for members
- Market incentive for increased security practices
- 10% discount for ISAlliance members
- Additional 5% discount for implementing ISAlliance Best Practices (July 2002)
- Discounts more than offset sponsorship dues
- Audit program to be announced soon

Step 4 Join ISAlliance

Join and participate in a cyber-security information sharing organization

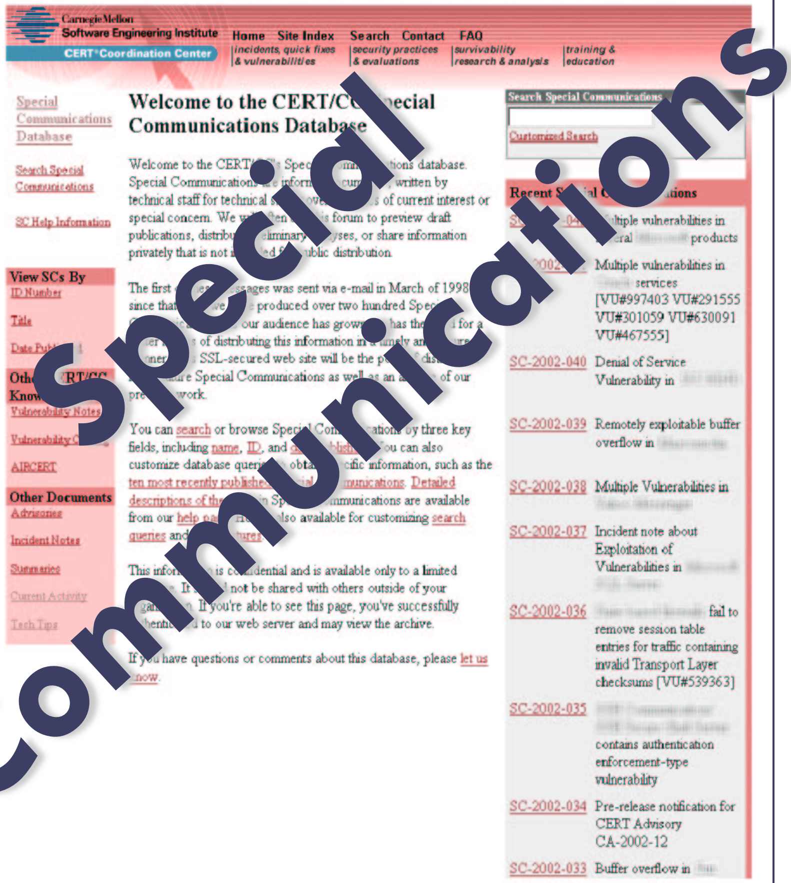
Benefits

- Share critical information across industries and across national boarders
- Provide secure setting to work on common problems
- Provide economic incentive programs
- Develop model industry programs
- Give policy makers an alternative to regulatory models

CERT Knowledgebase Examples

CERT Coordination Center

Figure 3: Special Communications index page



Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center
Home
Site Index
Search
Contact
FAQ
incidents, quick fixes & vulnerabilities
security practices & evaluations
survivability research & analysis
training & education
Special Communications Database
Search Special Communications
SC Help Information
View SCs By
ID Number
Title
Date Published
Other CERT/CC Know[illegible]
Vulnerability Notes
Vulnerability Catalog
AIRCERT
Other Documents
Advisories
Incident Notes
Summaries
Current Activity
Tech Tips
Search Special Communications
Customized Search

Welcome to the CERT/CC Special Communications Database

Welcome to the CERT/CC's Special Communications database. Special Communications are informal documents, written by technical staff for technical staff, covering topics of current interest or special concern. We will often use this forum to preview draft publications, distribute preliminary analyses, or share information privately that is not intended for public distribution.

The first of these messages was sent via e-mail in March of 1998; since that time, we have produced over two hundred Special Communications. As our audience has grown, so has the need for a better means of distributing this information in a timely and secure manner. This SSL-secured web site will be the point of distribution for future Special Communications as well as an archive of our previous work.

You can search or browse Special Communications by three key fields, including name, ID, and date published. You can also customize database queries to obtain specific information, such as the ten most recently published Special Communications. Detailed descriptions of the [illegible] in Special Communications are available from our help page. Help is also available for customizing search queries and [illegible]tures.

This information is confidential and is available only to a limited audience. It should not be shared with others outside of your organization. If you're able to see this page, you've successfully authenticated to our web server and may view the archive.

If you have questions or comments about this database, please let us know.

Recent Special Communications

SC-2002-04[illegible]	Multiple vulnerabilities in several [redacted] products
SC-2002-0[illegible]	Multiple vulnerabilities in [redacted] services [VU#997403 VU#291555 VU#301059 VU#630091 VU#467555]
SC-2002-040	Denial of Service Vulnerability in [redacted]
SC-2002-039	Remotely exploitable buffer overflow in [redacted]
SC-2002-038	Multiple Vulnerabilities in [redacted]
SC-2002-037	Incident note about Exploitation of Vulnerabilities in [redacted]
SC-2002-036	[redacted] fail to remove session table entries for traffic containing invalid Transport Layer checksums [VU#539363]
SC-2002-035	[redacted] contains authentication enforcement-type vulnerability
SC-2002-034	Pre-release notification for CERT Advisory CA-2002-12
SC-2002-033	Buffer overflow in [redacted]

Special Communications

Benefits of Information Sharing Organizations

- May lesson the likelihood of attack

"Organizations that share information about computer break ins are less attractive targets for malicious attackers." – *NYT 2003*

- Participants in information sharing have the ability to better prepare for attacks

Benefits of Information Sharing Organizations/Examples

- SNMP vulnerability
  - CERT notified Alliance members Oct. 2001
  - Publicly disclosed Feb. 2002
- Slammer worm
  - CERT notified Alliance members May 2002
  - Worm exploited Jan. 2003