We heard about the worm on 11/2/88


“On the evening of 2 November 1988, someone infected the Internet with a worm program. … This infection eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days.”
...it was the catalyst for the CERT/CC

The SEI established, with DARPA sponsorship, The Computer Emergency Response Team Coordination Center in 1988.

“The CERT/CC’s mission is to respond to security emergencies on the Internet, serve as a focal point for reporting security vulnerabilities, serve as a model to help others establish incident response teams, and raise awareness of security issues.”
The early vision
International cooperation speeds response to Internet security breaches.
But there were ARPAnet attacks in 1986


“The hacker’s code name was “Hunter” – a mystery invader hiding inside a twisting electronic labyrinth, breaking into U.S. computer systems and stealing sensitive military and security information”
Hackers were once a nuisance

Source: Time Magazine, December 12, 1994

Newsday technology writer & hacker critic found:

- Email box jammed with thousands of messages
- Phone reprogrammed to an out of state number where caller’s heard an obscenity loaded recorded message
Then it got more serious


An international group attacked major companies: MCI WorldCom, Sprint, AT&T, and Equifax credit reporters.

- had phone numbers of celebrities (e.g. Madonna)
- Had access to FBI's national crime database.
- Gained information on phones tapped by FBI & DEA
- Created phone numbers for their own use
… and profitable

Source: PBS web site report on Vladimir Levin (1994)

Russian hacker accessed Citibank computers and transferred $10M to his accounts using passwords and codes stolen from Citibank customers

- Citibank & FBI tracked Levin
- all but $400,000 recovered
Software Blamed for Problems

Source: Business Week Cover Story, December 6, 1999

“Software Hell

Bugs, viruses, complexity

Is there any way out of this mess”
DDOS attacks become a reality

Source: Seattle Post-Intelligencer Staff and News Services; February 9, 2000

Operations of major e-commerce & web sites seriously disrupted

- Amazon.com, eBay, CNN, others
Links made with organized crime

Source: Ecommerce Times – March 9, 2001

FBI advises that Eastern European hacker groups stole information from e-commerce & online banking sites

- 40 firms in 20 states, lost over 1M credit card numbers
- credit card information sold to organized crime entities.
- the criminal groups usually try to sell security services to victim sites
The relationships grow


Eastern European Internet sites traffic in tens of thousands of stolen credit-card numbers weekly

- Claims financial loses of over $1B/year
- Cards prices at $.40 to $5.00/card – bulk rates for lots of hundreds or thousands
- Organized crime groups buying from black-hat hackers
Spyware Targets Individuals

Source: The Register, Aug 30 2002

Spyware freely available

- Distributed via email
- Logs keystrokes and copies all email
- Sends recorded information to a specified email address
Extortion


- Oleg Zezev, a/k/a "Alex," a Kazakhstan citizen, sentenced to 51 months in prison following his conviction on extortion and computer hacking charges.

- Convicted of hacking into Bloomberg L.P.'s computer system; stealing confidential information and threatening public disclosure if $200,000 not paid.
Bot Nets for Hire

Source: Technology Review - September 24, 2004

- Rent pirated computers for $100/hour
- Average rate in underground markets
- Used for sending SPAM, launching DDOS attacks, distributing Pornography, etc..
Going “phishing”

Definition

- Phishing: fraudulent email and websites used to lure recipients into divulging sensitive information such as credit card numbers, social security numbers, bank account numbers & PINs, etc.

A rapidly growing problem

- Anti phishing working group (www.antiphishing.org)
  - Dec. 03 – reports increase 400% over holidays
  - Feb. 04 – reports increase 50% in January
  - March 04 – reports increase 60% in February
  - April 04 – reports increase 43% in March
  - May 04 – reports increase 180% in April
  - Jan 05 – 300% increase over May 04
Identity theft flourishes -1

Chronicle, October 21, 2004 – reports on theft of Social Security numbers from UC Berkeley systems; 600,000 Californians effected

Associated Press, November 4, 2004 – reports a former University of Texas student indicted on hacking into UT’s system and stealing Social Security numbers and other personal information from more than 37,000 students and employees.
Identity theft flourishes -2

Los Angeles Times, November 4, 2004 – reports four computers stolen from Wells Fargo; lost Social Security numbers of customers

Computerworld, January 10, 2005 – reports hacker steals names, photos and Social Security numbers of more than 32,000 students and staff at George Mason University
Identity theft flourishes -3

news.com, Feb 15, 2005 – reports ChoicePoint confirmed that criminals accessed its database of consumer records, potentially viewing the data of about 35,000 Californians; at least one case of identity fraud.
A growing electronic crime infrastructure

Source: Baseline Mag, March 7, 2005

- Web mobs named carderplanet, stealthdivision, darkprofits and the shadowcrew
  - Buy and sell millions of credit card numbers, social security numbers and identification documents
  - Often for less than $10 each
  - Build sites and services to create more skilled, like-minded organizations.

- U.S. Secret Service said Shadowcrew had 4,000 members
  - Sold 1.5 million credit card numbers, 18 million e-mail account and other ID documents
  - Sold to highest bidders
With links to terrorist activities

Source: Testimony of Mr. Dennis Lormel, FBI; Senate Subcommittee on Technology, Terrorism and Government Information - July 9, 2002

- Terrorists have used identity theft & Social Security Number fraud to obtain employment and access to secure locations.
- Also used by terrorists to obtain Driver's Licenses, bank and credit card accounts through which terrorism financing is facilitated.
- Terrorist cell in Spain used stolen credit cards in
Vulnerabilities

Vulnerabilities Discovered

Time
Attacks

Time

Attacks
Compromises

Time

Compromises
Damage

Time

Damage
What About the Future?
A continuously changing problem – systems -1

Complex, continuously evolving, interdependent elements – ultra-large scale systems that go far beyond our current “system of systems”

- New design and implementation merge with updates and configuration changes
- Systems that must continuously deliver results while suffering attacks, accidents and failures
- Individual components becoming more secure (e.g. operating systems)
A continuously changing problem – systems -2

- Network connected, embedded systems likely to be vulnerable
  - Firmware vulnerabilities become major problem
  - Current response & recovery practices won’t scale up
- Continued growth in vulnerability caused by increased size & complexity
- Serious entertainment systems will be Internet connected & run serious operating systems with significant memory & disc
  - And you think botnets are a problem now!
Continuously changing threats

More and more of the same plus new challenges

- Dramatic increase in “attacks for profit”
- Continued increases in computer/network facilitated crime – e.g. fraud, identity theft, pornography, pirated IP, extortion
- Shift of attack patterns – from OS to applications, new devices & protocols
- Stealthy, automated attacks aimed at individual companies/industries
- Increased instances of embedded malicious code
- Increase in technical mercenaries
Continuously changing security products and services -1

Key question: How will today’s security solutions evolve, scale to meet new challenges?

- Increased dissatisfaction with effectiveness of perimeter security
- Growing dissatisfaction with Intrusion Detection Systems (limited effectiveness, inability to scale to ultra-large scale systems, weak support for retrospective analysis)
- Growing dissatisfaction with anti-malware products
Continuously changing security products and services -2

- Increased integration of system management & security tools (though with little improvement in effectiveness)
- Emergence of "application centric" security event detection systems
- More hardware to help solve problems – biometrics, encrypting discs, etc
- Increase in risk consulting on insider threats & compliance
Continuously changing victims -1

Globalization and ubiquitous Internet connected systems are changing the fabric of government/business/citizen interactions. The emerging socio-technical ecosystem will bring new targets.

- Increase in espionage as relationships change world-wide
- Increase in industrial espionage as developing countries become major players in world-wide markets
- Increase in attacks on citizens of countries with growing economies
Continuously changing victims -2

- As security in advanced agencies/companies improves, weaker links in contractor/supply chains will be attacked.
- Likely to see at least one concentrated attack on a critical infrastructure (maybe a run-away experiment).
What Can We Do?
Recognize the power of FIRST
Better Understanding

Analysis->Understanding->Informed Action->Improvement

- Today sharing is time consuming and expensive leading to islands of information and little shared understanding
  - FIRST members are in an excellent position to:
    - Work together and with standards groups like IETF on open standards for the capture, storage and transmission of security information and analysis results
    - Form sharing & analysis coalitions to improve understanding and disseminate knowledge
    - Establish global indications and warning systems with predictive capabilities
    - Define requirements for automated support for recognition, response, reconstitution & recovery
Better Software

Low quality software continues as the root cause of most vulnerabilities/incidents

- Good software engineering process solves much of this problem
- Static source code analysis tools are increasingly effective
- Secure out-of-the-box configurations help too

FIRST members can build the case for management attention
Better Systems

Some problems are rooted in system architecture & design
  ▪ Viruses, spam, DDOS, spyware

Today’s reactive solutions are reaching their limits of effectiveness

FIRST members should increase involvement in new technology development forums
  ▪ IETF, standards groups, vendor forums
Better Systems Management

We all know that some organizations are on top of security & others are clueless

We all need to promote security management practices that are:

- Supportive of an organization’s mission & goals
- Focused on risk reduction rather than mere compliance
- Integrated with other key business practices
- Measured, reviewed & updated on a regular basis
Evolving the Security Approach
Better People

Management practice dictates the “what”, but it’s the skills & abilities of the staff that determine the “how well”

Support & promote the development of performance & training standards such as DoD 8530 & 8570.

Encourage your management to invest in the training & skills building needed to stay on top of a constantly changing problem
Goal for Future Vulnerabilities
Goal for Future Attacks
Goal for Future Compromises
Goal for Future Damage