Social, Security, and Privacy Implications of Computing

PSWP Class Offering

University at Albany, SUNY

February 17, 2006

Sanjay Goel

Computer Security

Agenda

- Computer Crime
- Attacks
  - Buffer Overflow Attacks
  - Password Cracking
  - Session Hijacking
- Conclusions

Computer Security

Hacking

- Every 18 seconds an incident is reported (CSI/FBI Report, 03)
- Every third day a new virus is released (ISCA Report, 12/03)
- Number of Reported incidents has gone up from 52,000 to 140,000 from 2001 to 2003
  - (CERT Report, 2003)
- Unreported Incidents have gone up from 4.1 million to 15.9 million from 2001 to 2003
  - (Aberdeen Report, 03)
- Identity Theft costs have gone up from 8.75 billion to 24 billion in one year (2002 to 2003)
  - (Aberdeen Report, 03)

Computer Security

Key Vulnerabilities

Incidents Reported

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

CERT

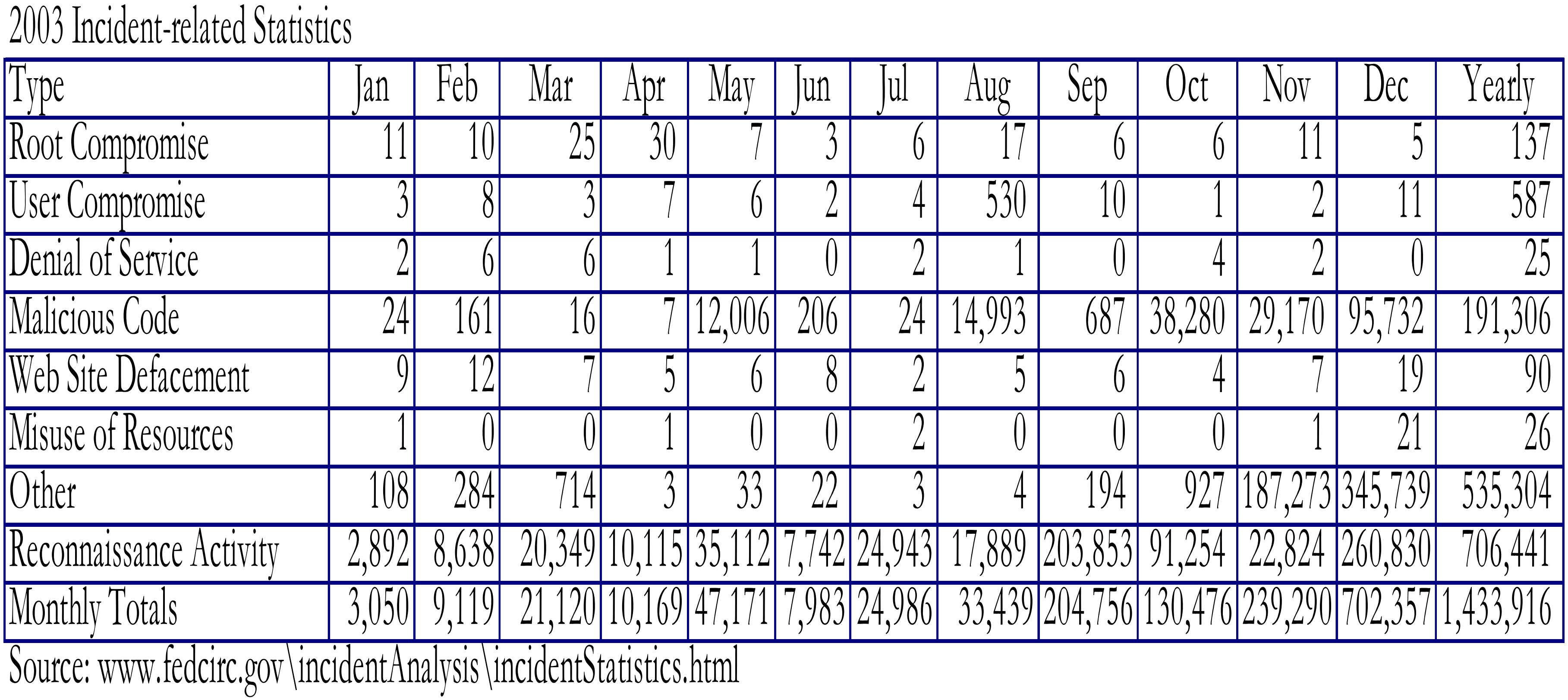
Vulnerabilities Reported

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

- The number of incidents have gone up by more than 6 times
  - An incident may involve one site or hundreds (or even thousands) of sites.
  - some incidents may involve ongoing activity for long periods of time.
- The number of vulnerabilities have gone up more than 3 times

Computer Security

Statistics



2003 Incident-related Statistics

Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Yearly
Root Compromise	11	10	25	30	7	3	6	17	6	6	11	5	137
User Compromise	3	8	3	7	6	2	4	530	10	1	2	11	587
Denial of Service	2	6	6	1	1	0	2	1	0	4	2	0	25
Malicious Code	24	161	16	7	12,006	206	24	14,993	687	38,280	29,170	95,732	191,306
Web Site Defacement	9	12	7	5	6	8	2	5	6	4	7	19	90
Misuse of Resources	1	0	0	1	0	0	2	0	0	0	1	21	26
Other	108	284	714	3	33	22	3	4	194	927	187,273	345,739	535,304
Reconnaissance Activity	2,892	8,638	20,349	10,115	35,112	7,742	24,943	17,889	203,853	91,254	22,824	260,830	706,441
Monthly Totals	3,050	9,119	21,120	10,169	47,171	7,983	24,986	33,439	204,756	130,476	239,290	702,357	1,433,916

Source: www.fedcirc.gov\incidentAnalysis\incidentStatistics.html

Computer Security

Security Incidents

April 08, CNET News.com

NetSky attacks target file–sharing networks.

The main Website of file–sharing network **eDonkey was knocked offline** this week following an attack from NetSky.

Earlier this week, the Kazaa and eDonkey sites, as well as three other file-sharing sites, were bracing for a distributed denial–of–service (DDoS) attack expected to be launched by variants of the NetSky worm.

NetSky.Q, which first appeared March 29, is designed to attack certain Websites that distribute file–sharing clients, as well as sites that distribute hacking and cracking tools. The attack is scheduled to last at least six days.

Source: http://news.com.com/2100–1009_3–5187211.html?tag=nefd.top

February 2004,

According to security experts mi2g, virus activity caused as much as **$83 billion** in economic damage in February. With numerous variants of MyDoom/Doomjuice and NetSky causing havoc over the wires.

Computer Security

Security Incidents

April 09, Mobile Pipeline

Second Cisco WLAN security threat exposed.

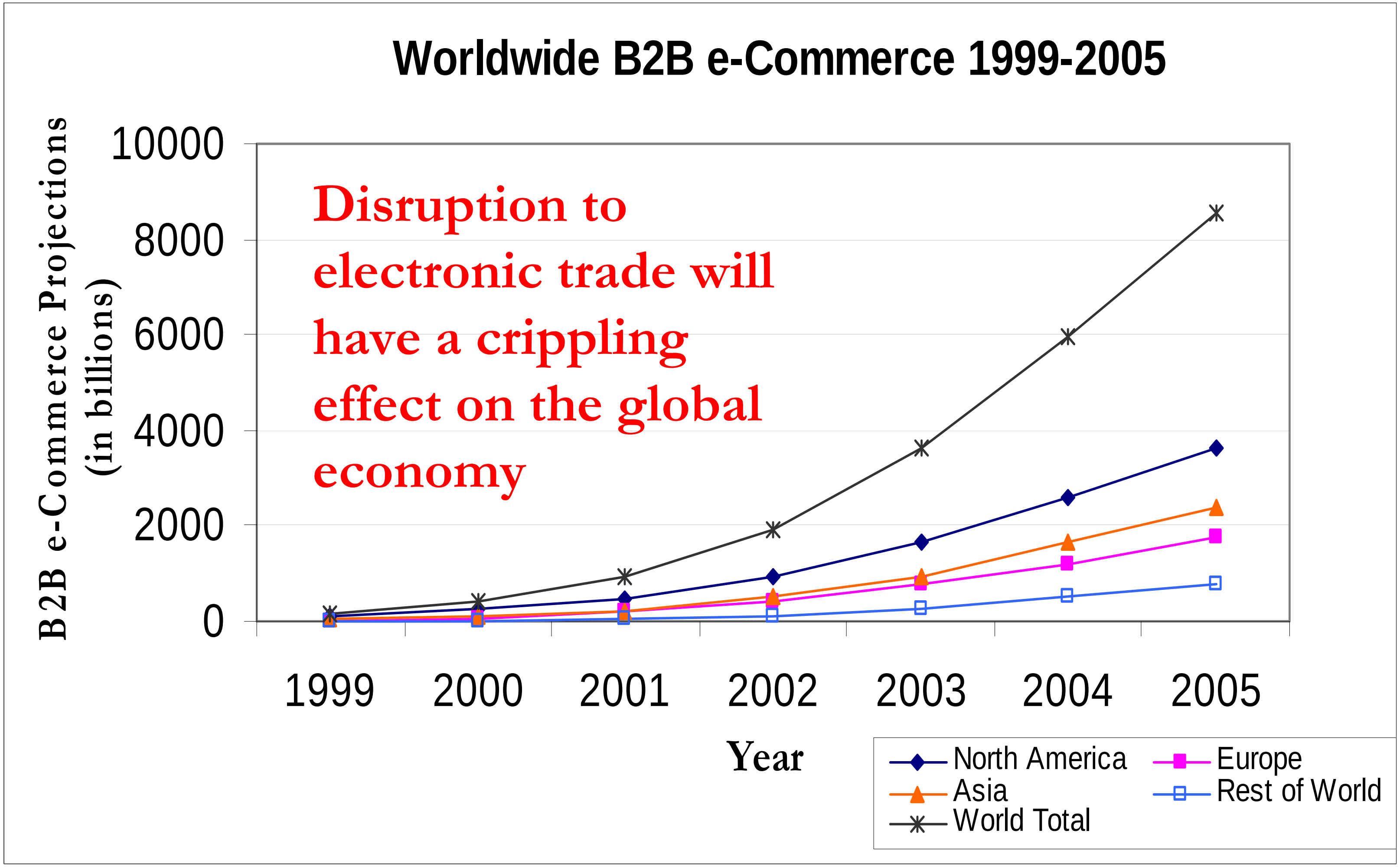
Cisco faced its second serious WLAN security threat last week when a network and security analyst released a tool that attacks the company's proprietary Lightweight Extensible Authentication Protocol (LEAP) wireless authentication system.

Wright strongly urged LEAP users to take alternative measures. "Customers using LEAP should be aware that the usernames and password of their user account are exposed, and should plan for the deployment of alternate authentication mechanisms such as PEAP or TTLS,"

http://www.mobilepipeline.com/news/18900815;jsessionid=3TNL4

Computer Security

Economy Connected to Internet



Disruption to electronic trade will have a crippling effect on the global economy

Computer Security

Financial Losses

- Melissa Virus (1999)
  - Macro virus that exploits MS Outlook security weakness
  - Distributes Infected word files to top 50 users in the address book
  - Over 80 million in damages
- I Love You (May, 2000)
  - Macro virus that exploits MS Outlook security weakness
  - Estimated at over 10 billion dollars in damages
- Klez (April, 2002)
  - Caused $18.9 billion in damages.
- Yaha (June 2002)
  - Caused $11.1 billion worth of damages.

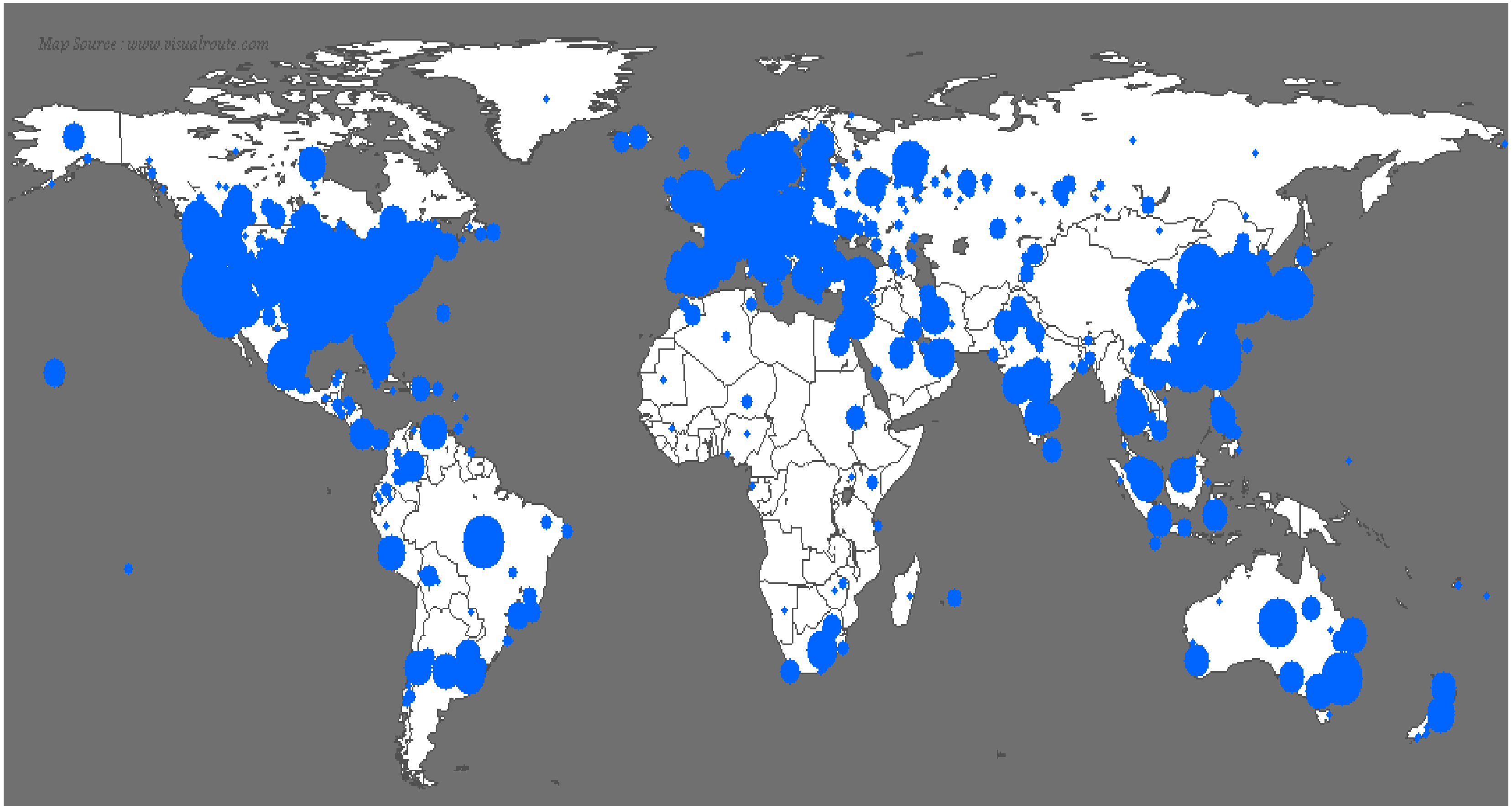
Computer Security

Financial Losses

- Slapper Worm (September 2002)
  - Exploits a buffer overrun vulnerability in SSL 2.0 impacting Linux Apache Web servers
  - Tens of thousands of victims
  - Collected victims in a network for use in DDoS attacks
- SQL Slammer Worm /Sapphire (January 2003)
  - Attacked a vulnerability in SQL Server that was also embedded in other software(75,000 victims in 10 minutes)
  - Disabled ATM machines, 911 systems, airline scheduling systems
  - Caused over 1 billion dollars in losses
- Sobig (August 2003)
  - Caused an estimated $36.1 billion in damages.

Computer Security

SQL Slammer



- Rate of Spread of viruses continutes to grow
  - Within hours the viruses can spread to every part of the world

Computer Security

Critical Infrastructure

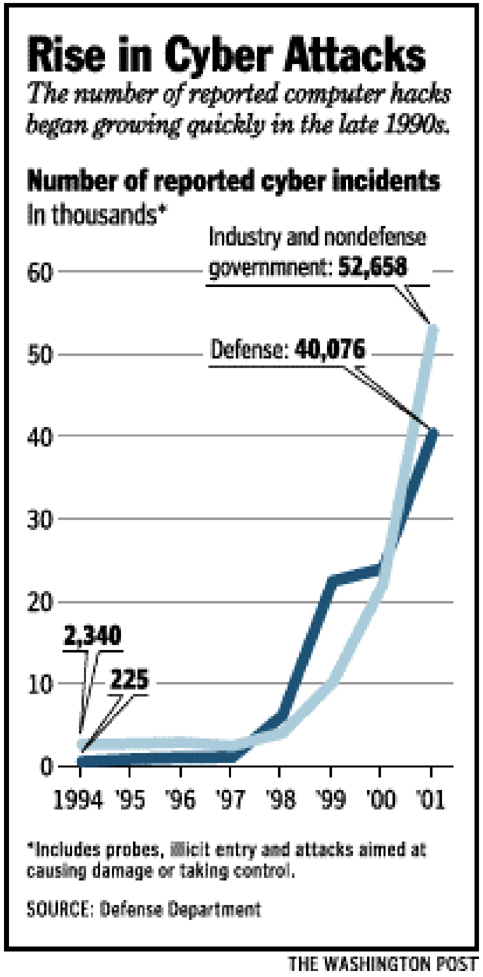
- Technology has made many of our essential services (utilities, banking, transportation, etc.) enormously more productive and reliable
- Virtually every critical service (such as electrical power grids, phone systems, air traffic control, water and sewer service, and medical services) is dependent on computers.
- U.S. analysts believe that by disabling or taking command of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives & property. *(Washington Post June 27, 2002)*

Computer Security

Critical Infrastructure

- The nation’s health, wealth & security depends on the protection of critical infrastructure from various threats
- The defense establishment computers are under constant probe and attack
- Next wave of terrorist attacks are anticipated to be a dual physical and cyber attack

- **The next generation warfare that we may face will be cyber warfare**



Rise in Cyber Attacks

The number of reported computer hacks began growing quickly in the late 1990s.

*Includes probes, illicit entry and attacks aimed at causing damage or taking control.

SOURCE: Defense Department

THE WASHINGTON POST

Computer Security

Security Incidents (Infrastructure)

April 12, Associated Press

LAX airport hit by brief blackout. A brief power–line failure knocked out electricity to the Los Angeles International Airport (LAX) control tower and disrupted air traffic Monday morning, April 12. **Eighty to 100 flights had to hold in the air, circle or stay on the ground at other airports**, Federal Aviation Administration spokesperson Donn Walker said.

All radar, radios and telephones –– essentially everything that controllers use to communicate with aircraft and other control facilities –– were hit by the outage, Walker said.

Source: http://www.usatoday.com/travel/news/2004–04–12–lax–blackout_ x.htm

Computer Security

Security Incidents (Infrastructure)

April 11, Reuters

Top microchip makers suffer minor damage in blackout. A power blackout struck parts of Taiwan's silicon valley and caused minor damage at the world's top two microchip foundries, Taiwan Semiconductor Manufacturing Co (TSMC) and United Microelectronics Corp (UMC), company executives said on Saturday,

April 10.

Back–up generators helped to mitigate losses, which were estimated at up to a few million U.S. dollars by UMC, the world's second–largest contract chipmaker.

TSMC said it was still evaluating its damage. "The damage caused by today's power outage will be no more than tens of million of (Taiwan) dollars," said Sandy Yen, a spokesman for UMC.

Source: http://www.usatoday.com/tech/techinvestor/2004–04–11–taiwan– blackout_x.htm

Computer Security

Security Incidents (Infrastructure)

4/16/01 Insight on the News - Investigative Report

Hackers Attack Sandia Computers

Hackers recently penetrated national-security computer systems at Sandia National Nuclear Laboratory in Albuquerque gaining access to classified information relating to nuclear-weapons design.

02/04/2003, NucNews

London hacker Joseph James McElroy, 18, hacks into 17 computer systems at the Fermi National Accelerator Laboratory near Chicago over a two-week period in June 2002 to store and exchange hundreds of gigabytes worth of computer files with his friends.

09/24/03, IDG News Service

U.S. immigration system hit by virus

The U.S. Department of State struggled Tuesday to quell an outbreak of the W32.Welchia Internet worm on the department's computer systems.

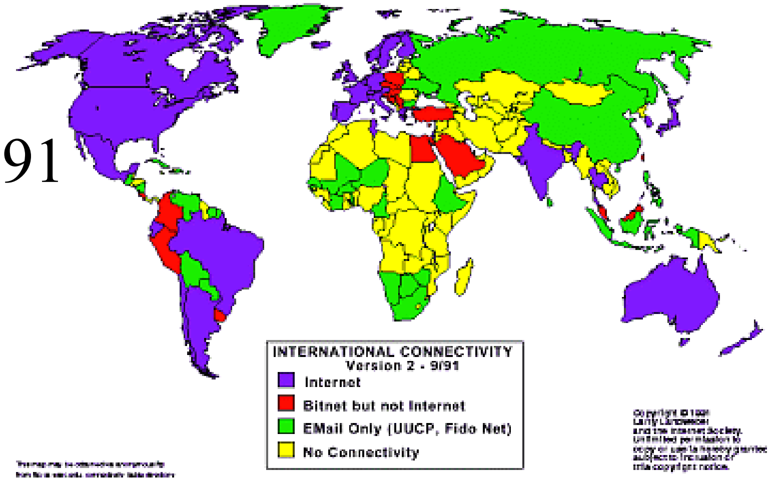
Source: http://www.infoworld.com/article/03/09/24/HNimmigration_1.html

Computer Security

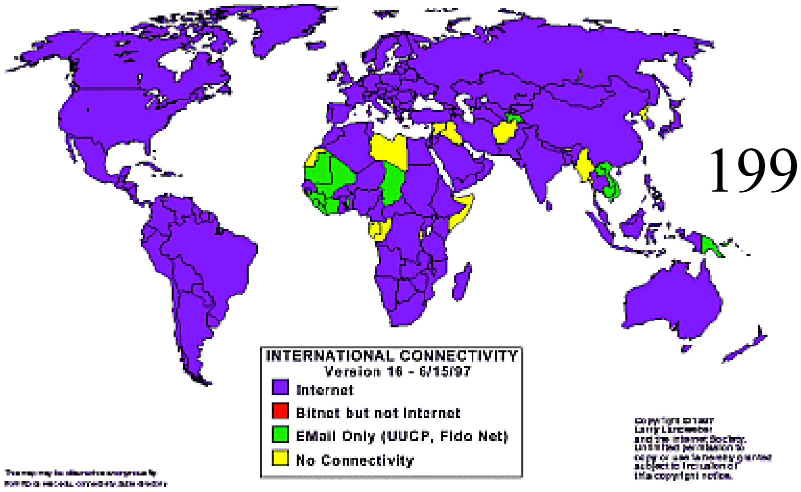
Life Style Depends on Computers

- An employees sends about 22.9 messages each day, recieves 81 messages per day and gets 19.5 spam messages per day.
- The number of instant messaging users will grow to 180 million in 2004 (Gartner Report)
- The world has become globally connected
  - Today each country has connectivity to the Internet

1991



1997



Computer Security

Who Out of These is a Hacker?

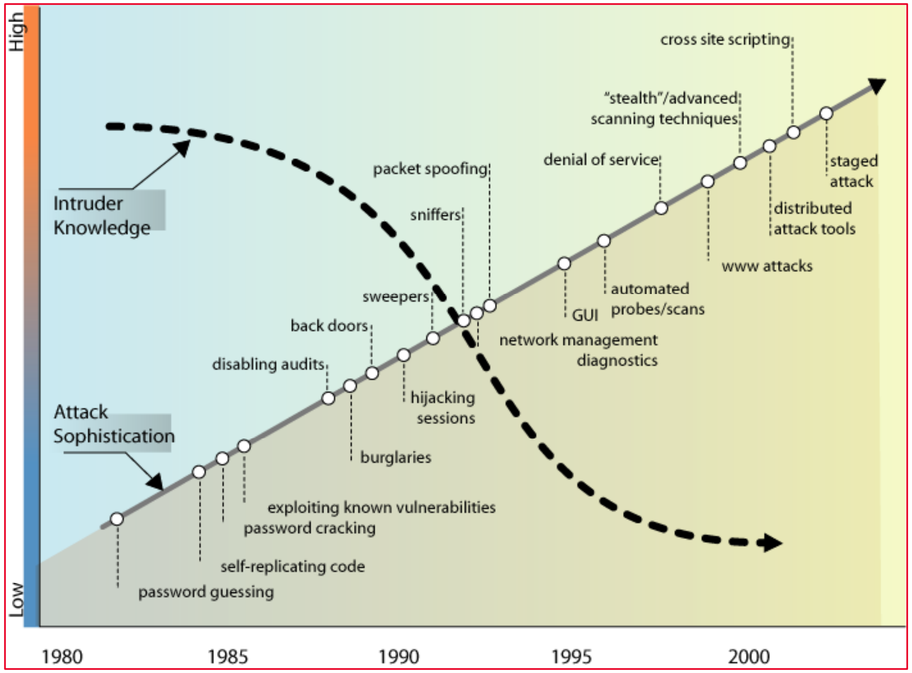
- pictures

Computer Security

Changing profile of the hacker

- In past hackers were geniuses with a deep interest in technology.
- Today hackers can operate with little knowledge network or computers
  - Download code from the Internet
  - Follow recipes
- Number of potential hackers grows from a few to several million
- Hackers of tomorrow will be terrorists with deep evil intent.

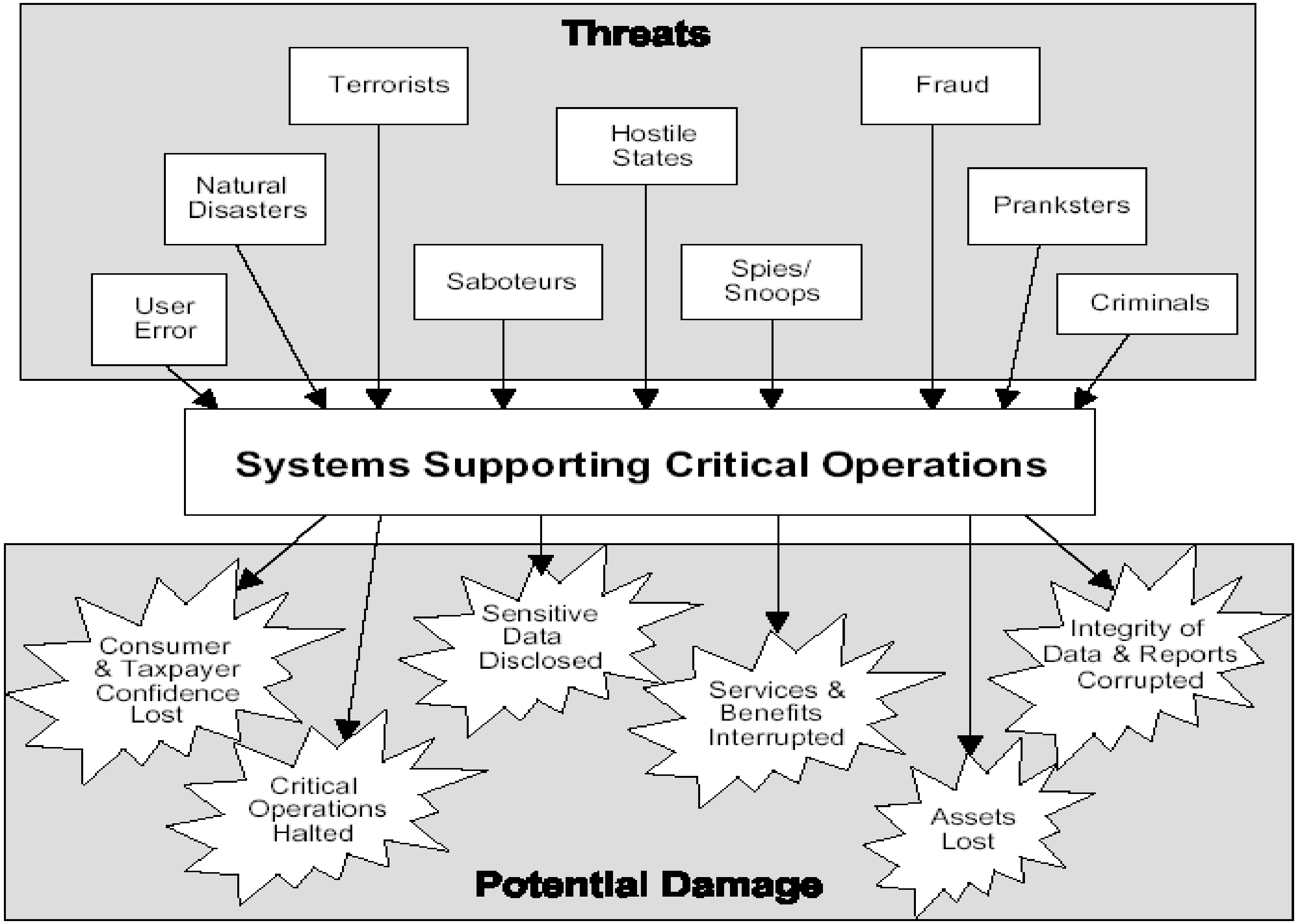
Carnegie Mellon
Software Engineering Institute



'02 Carnegie Mellon University

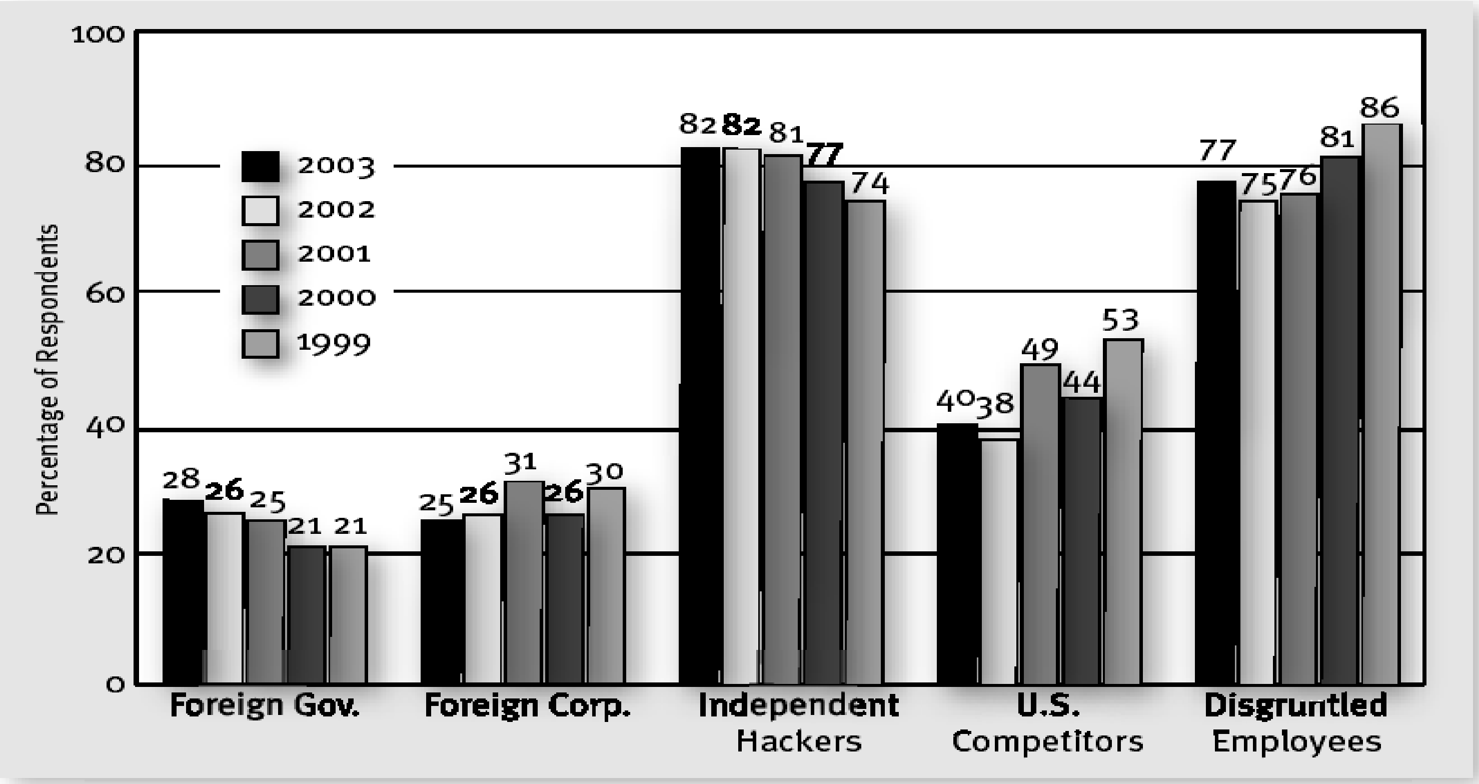
Computer Security

Critical Infrastructure Threats


Threats
Terrorists
Fraud
Hostile States
Natural Disasters
Pranksters
Saboteurs
Spies/ Snoops
Criminals
User Error
Systems Supporting Critical Operations
Consumer & Taxpayer Confidence Lost
Sensitive Data Disclosed
Services & Benefits Interrupted
Integrity of Data & Reports Corrupted
Critical Operations Halted
Assets Lost
Potential Damage

Computer Security

Sources of Attack



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

2003: 488 Respondents/92%
2002: 414 Respondents/82%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%

Attacks on Computers

Types

I. Buffer Overflow Attack

II. Password Cracking

III. Session Hijacking

I. Buffer Overflow Attack

Buffer Overflow Attack

Basics

- OSI Layer: Application.
- Definition: Attacker tries to store more information on the stack than the size of the buffer allows for and manipulates the memory stack to execute malicious code.
- Who is Vulnerable: Programs which do not have a rigorous memory check in the code are vulnerable to this attack.
- Typical Behaviors: Can be used for obtaining privileges on a machine or for denial-of-service.

Buffer Overflow Attack

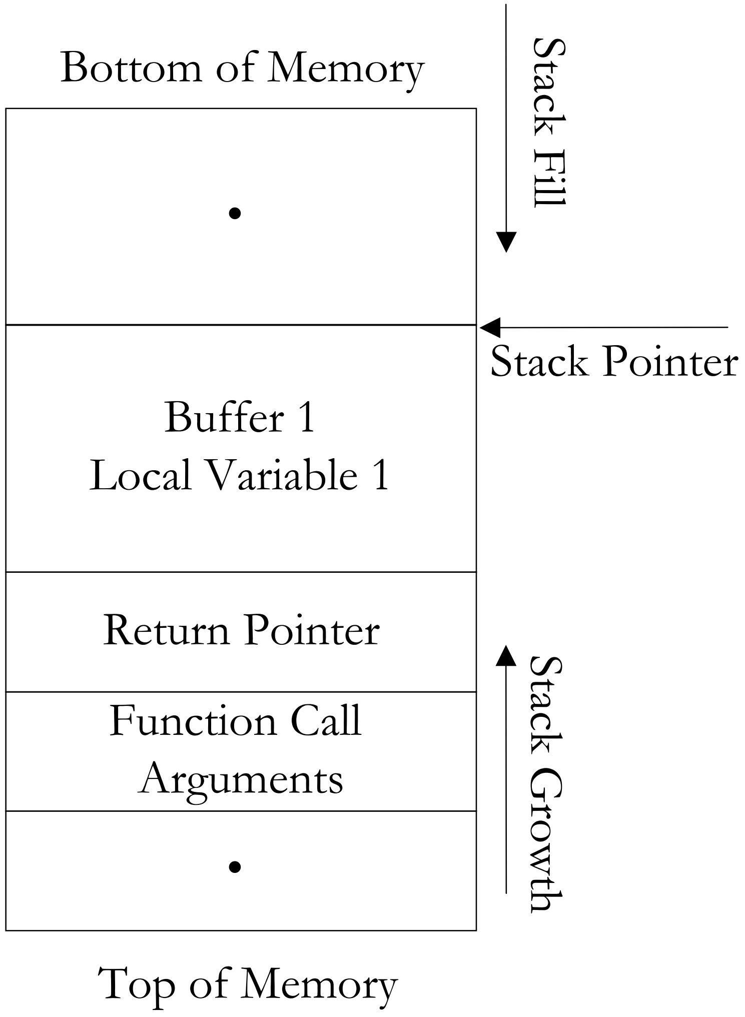
Incidents

- Effectiveness of this attack has been common knowledge since the 1980's:
  - Used by the Internet Worm used in 1988 to gain unauthorized access to networks and systems.
  - Accounts for approximately half of all security vulnerabilities.
- According to a recent survey MS Blaster worm caused:
  - Remediation cost $475,000 per company (median average - including hard, soft and productivity costs) with larger node-count companies reporting losses up to $4,228,000.
  - Entered company networks most often through infected laptops, then through VPNs, and finally through mis-configured firewalls or routers.
  - From TruSecure / ICSA Labs, 29 August 2003.

Buffer Overflow Attack

Creating Execution Stack

- Four bulk operations are performed to call a function in a conventional architecture:
  - The function's parameters are saved onto the stack
  - The return address is saved onto stack
  - Execution is transferred to the called function.
- Once the function completes its task, it jumps back to the return address saved on the stack
- Note that the string grows towards the return address

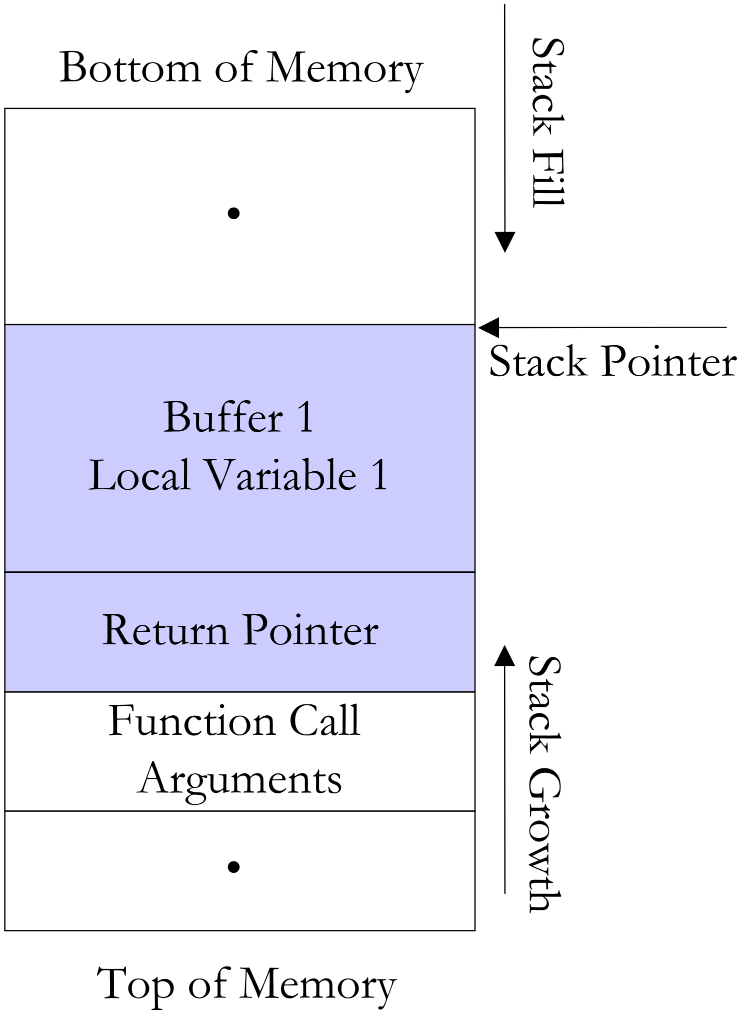


Normal Stack

Buffer Overflow Attack

Vulnerability

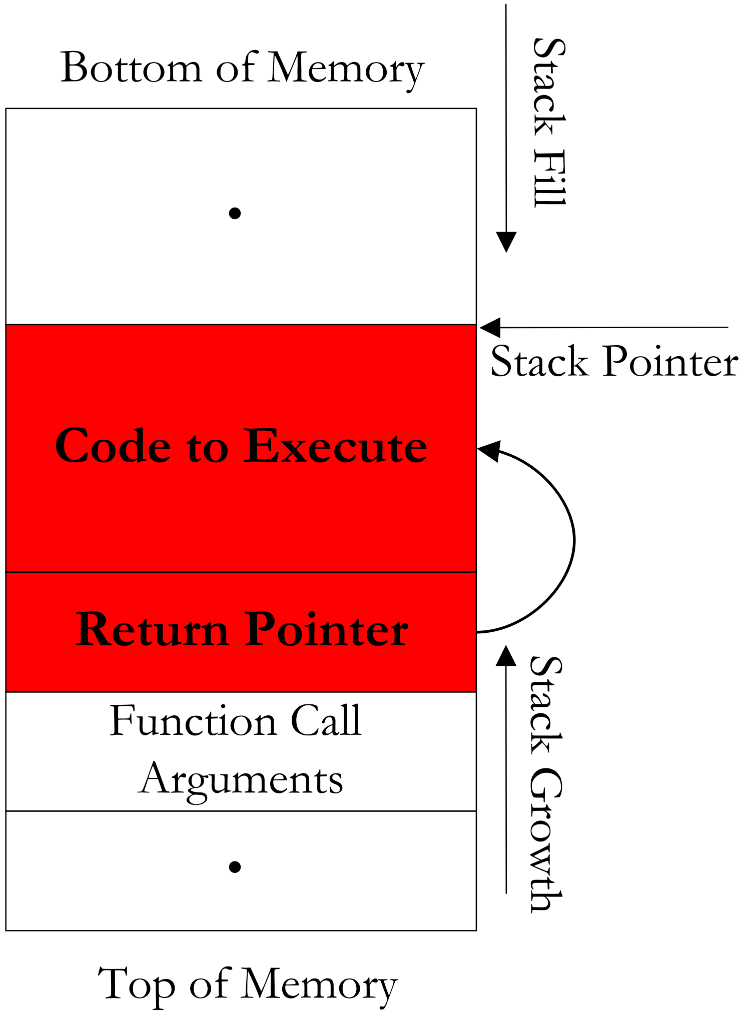
- Buffer overflow vulnerability occurs where an application reads external information such as a character string and and an input string larger than the allocated buffer memory is sent (and the application doesn't check the size).
  - Input will normally come from an environment variable, user input, or a network connection.
  - e.g. if memory allocated for name is 50 characters, and a name of more than 50 characters is input by user
- The return pointer can be overwritten by the user data



Buffer Overflow Attack

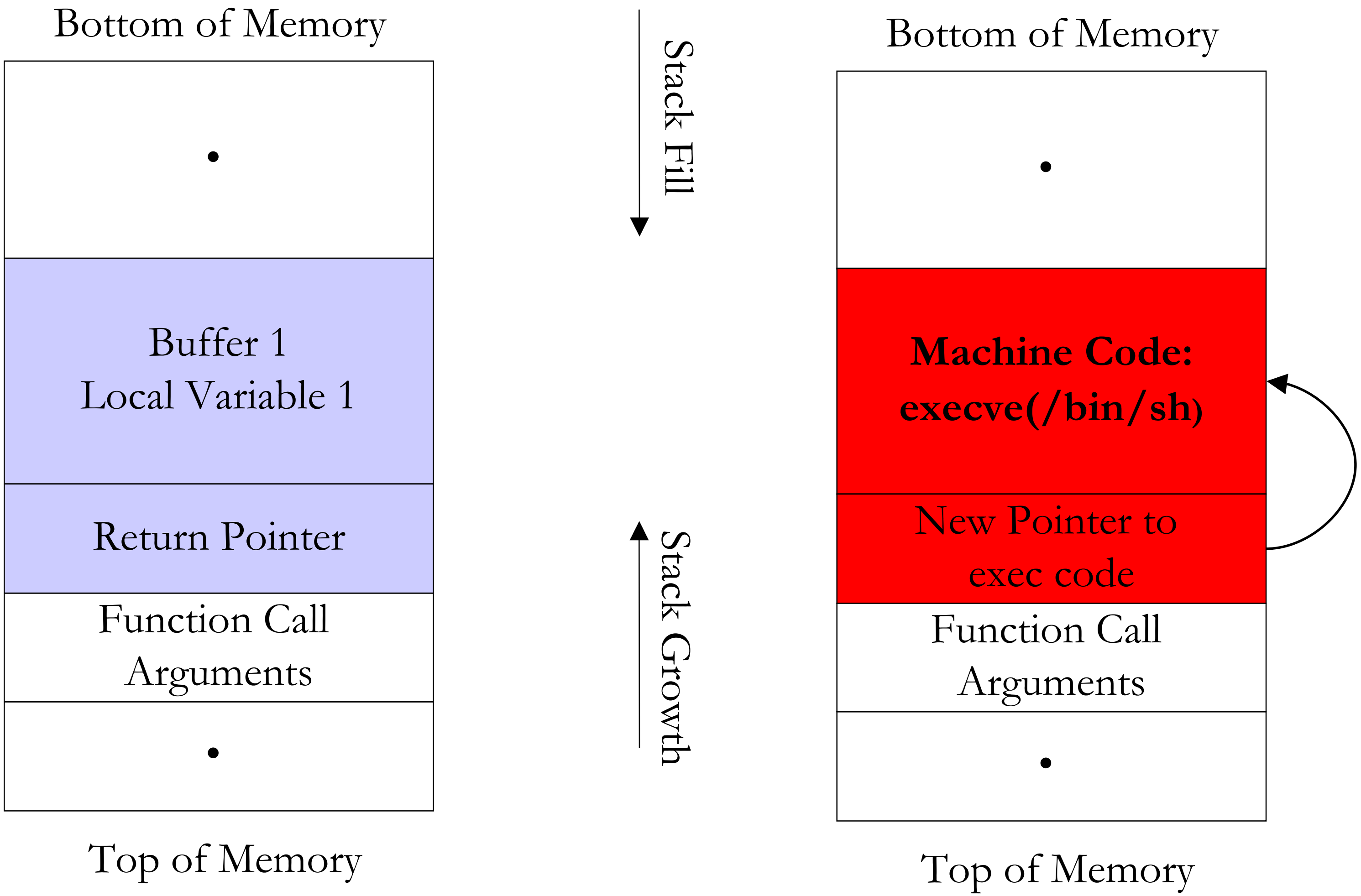
Executing the Attack

- Inject the attack code, which is typically a small sequence of instructions that spawn a shell, into a running process
- Change the execution path of the running process to execute the attack code.
  - Change the value of the return address to the address of malicious code
- Both of the goals must be achieved at the same time to perform a successful attack.



Buffer Overflow Attack

Compare Stack



Buffer Overflow Attack

Protection/Detection

- Avoid programming mistakes.
- **Patch, patch, patch !!!**
  - Does not effectively protect from zero day exploits.
- Keep your AV software up to date.
- Follow layered approach to information security – segment your network, only allow the necessary services, block and log everything else.
- Monitor your network for anomalous activity.
- Deploy Buffer Overflow kernel patches – not 100% effective but may be able to protect your environment the next time your patching process misses a few boxes.

II. Password Cracking

Password Cracking

Issues

- Most common mean of authentication:
  - Compares the token provided by user with stored token
- The weakest link in the security chain.
- On average each person has 8-12 passwords:
  - Different systems impose different requirements on passwords.
  - Passwords need to be changed often.
  - Some passwords are used occasionally (once a year).

Password Cracking

Ten Common Mistakes

1. Leaving passwords blank or unchanged from default value.
2. Use the letters p-a-s-s-w-o-r-d as the password.
3. Use their favorite movie star as the password.
4. Use their spouse's name as their password.
5. Use the same password for every thing.
6. Write passwords on post-it notes.
7. Paste a list of passwords under the key board.
8. Store all passwords in an excel spread sheet on their PDA Insert their passwords in the rolodex.
9. Write all passwords in their personal diary.
10. Give the password to a person who claims to the system administrator.

Password Cracking

Security Levels

🔓 Filing System

Clear text

🔓 Dedicated Authentication Server

Clear text

🔒 Encrypted

Password + Encryption = bf4ee8HjaQkbw

🔒🔒 Hashed

Password + Hash function = aad3b435b51404eeaad3b435b51404ee

🔒🔒🔒 Salted Hash

(Username + Salt + Password) + Hash function = e3ed2cb1f5e0162199be16b12419c012

Password Cracking

Password Encryption

- Typical Registration Scenario
  - User submits username and password
  - A one-way hash of the password is created: 793d5257b65cfcd227f6834e738d8f06
  - Password hash is stored in a database
  - Later, the user types his username and password
  - Password hash is created in memory and is compared to the one stored in the database
  - If Hash value = Hash value → User is allowed into system
- Only way to crack a password is to keep guessing passwords until the correct password is guessed.

Password Cracking

Methods of Attack

- Brute Force Attack
  - Tries all combinations of letters, numbers & symbols
- Dictionary Attack
  - Quick technique that tries every word in a specific dictionary
- Hybrid Attack
  - Adds numbers or symbols to the end of a word
- Popular programs for password cracking
  - LC4
  - Sam Inside
  - Crack
  - John the Ripper (JTR)

Password Cracking

Impact on Security

- What we found on Al Qaeda computers were two things. One, the kind of simple hacking tools that are available to anyone who goes out on the Internet looking for them, **tools such as LOphtCrack that allows you to get into almost anyone's password if they've used a simple eight-digit password.** That kind of tool frightens most people when they learn that if they're using only an eight-digit password with standard numbers and letters that probably anyone can get into your password in less than two minutes by downloading a tool like LOphtCrack, which is available publicly on the Internet. It was that kind of tool which we found, nothing terribly sophisticated

  -- Richard Clark

  Presidents Advisor on Cyber Security (2001-2003)

Password Cracking

Windows Passwords

- Set or change password → Windows generates a LM hash and a NT hash.
- Two hashing functions used to encrypt passwords
  - LAN Manager hash (LM hash)
    - Password is padded with zeros until there are 14 characters.
    - It is then converted to uppercase and split into two 7-character pieces
    - Each half is encrypted using an 8-byte DES (data encryption standard) key
    - Result is combined into a 16-byte, one way hash value
  - NT hash (NT hash)
    - Converts password to Unicode and uses MD4 hash algorithm to obtain a 16-byte value
- Hashes are stored in the Security Accounts Manager database
  - Commonly known as " SAM" or "the SAM file"
- SAM is locked by system kernel when system is running.
  - File location: C:\WINDOWS\SYSTEM32\CONFIG
- SYSKEY
  - Password à (LM/NT hash) à SYSKEY = Twice-Encrypted Password

Password Cracking

Protection/Detection

Protection:

- Disable Storage of LAN Manager Hashes.
- Configure both Local and Domain Account Policies (Password & Account Lockout Policies).
- Audit access to important files.
- Implement SYSKEY security on all systems.
- Set BIOS to boot first from the Hard Drive .
- Password-protect the BIOS.
- Enforce strong passwords!
- Change your passwords frequently.
- Use two or three factor authentication.
- Use one time passwords.

Passwords

Protection

- Weak passwords:
  - Personal Information
  - Dictionary passwords
  - Short in length
  - All UPPER case or lower case
  - Digits only
  - Blank and Default passwords
  - Example: sara

- Strong passwords:
  - 8 or more characters of mixed case
  - Contains at least one special character or digit or both
  - No words, acronyms, names, or dates
  - No personal information
  - Example Ikmy9tt!

III. Session Hijacking

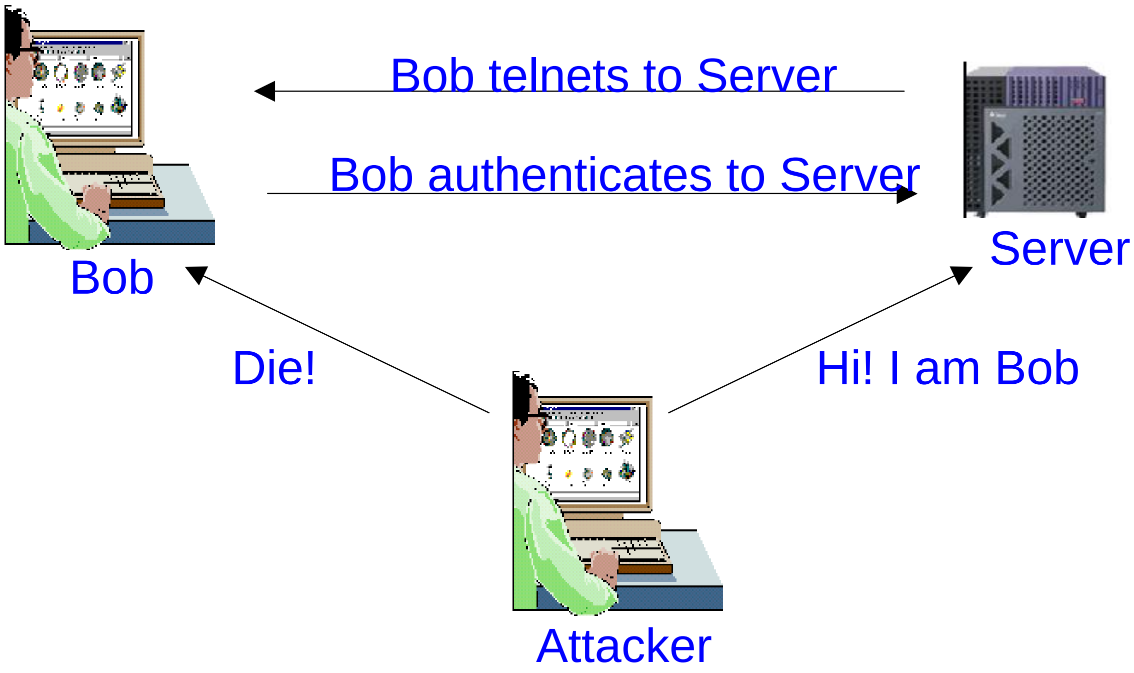
Session Hijacking

Basics

- OSI Layer: Data Link, Network, Session.
- Definition: User takes over an existing active session and exploits existing trust relationship.
- Process:
  - User makes a connection to the remote system by authenticating using her user ID and password.
  - After the user authenticates, she has access to the server as long as the session lasts.
  - Hacker takes the user offline by denial of service.
  - Hacker gains access to the target system by impersonating the legitimate user.
- Typical Behaviors: Attacker usually monitors the session, periodically injects commands into session and can launch passive and active attacks from the session.

Session Hijacking

How Is It Done ?



Bob telnets to Server

Bob authenticates to Server

Bob

Server

Die!

Hi! I am Bob

Attacker

Session Hijacking

Underlying Technology

- Reliable Transport
  - At sending end data stream broken into packets.
  - At receiving end packets reassembled.
- Sequence numbers are 32-bit counters used to:
  - Tell receiving machine the correct order of packets.
  - Tell sender which packets were received and which were lost.
- Receiver and Sender generate their own sequence numbers.

Session Hijacking

Underlying Technology

- Three requirements to hijack non-encrypted TCP communication:
  - There must be non-encrypted session oriented traffic.
  - Attacker must be able to recognize TCP sequence number and predict what the next sequence number will be.
  - Attacker must spoof the hosts MAC or IP address.
- IP & MAC addresses can be easily obtained:
  - Hacker usually has to make educated guess of the sequence number.
  - Once attacker gets server to accept the guessed sequence number he can hijack the session.

Session Hijacking

Protection/Detection

Protection:

- Use encryption.
- Use strong authentication.
- Configure appropriate spoof rules on gateways.
- Monitor for ARP cache poisoning.

Additional protection at the Data Link Layer:

- Use port security feature on Ethernet switches.
- Hard code ARP tables on your critical servers and turn off ARP on your network interfaces.

Conclusions

Computer Security

Layered Approach to Security

- Do not underestimate internal network threats.
- Apply industry best practices in your day to day work.
- Use layered approach to information security.
- Take a proactive approach to information security.
  - Do not wait for an incident to happen and react when it may be a little too late.

Computer Security

Closing Thoughts

- Are we really any better in Information Security than we were a few years ago with all the investments into this area?
- Is Information Security a long term research area or is it a passing fad?
- Are we focusing too much on perimeter defense and need to look at resilient systems?

Additional Material

Tool Index

Tool Name	General Use	OS	Available From
Ettercap	Sniffer	Linux	http://ettercap.sourceforge.net
Hunt	Sniffer/Hijacking	Linux	http://lin.fsid.cvut.cz/~kra
Ethereal	Sniffer	Linux Windows	http://www.ethereal.com/download.html
RPCScan2	Scanner	Windows	http://www.foundstone.com
dcom2_scanner.c	Scanner	Linux	http://packetstormsecurity.com
Netcat	Scanner-Multipurpose	Linux Windows	http://www.hack-box.info/bruteforce.html
John the Ripper	Password Cracker	Linux Windows	http://www.openwall.com
Linux Kernel Patch	Kernel Security Patch	Linux	http://www.openwall.com/linux
BufferShield 1.01a	Kernel Security Patch	Windows	http://www.sys-manage.com/index10.htm
OverflowGuard	Kernel Security Patch	Windows	http://www.datasecuritysoftware.com
StackDefender	Kernel Security Patch	Windows	http://www.ngsec.com/ngproducts
Juggernaut	Sniffer/Hijacking	Linux	http://packetstorm.securify.com
TTY Watcher	Sniffer/Hijacking	Linux	http://www.cerias.purdue.edu
IP Watcher	Sniffer/Hijacking	Linux	http://www.engrade.com

Buffer Overflow Attacks

Available Products for Microsoft Windows OS

Vulnerability	BufferShield	OverflowGuard	StackDefender
Protects stack	Yes	Yes	Yes
Protects heap	Yes	Yes	No
Protects applications	Yes	No	Yes
Protects services	Yes	Yes	Yes
Definition of protection scope	Yes	No	No
Free Edition available	Yes	No	No
Supports Windows 2003	Yes	Yes	No

Note: As published on the http://www.sys-manage.com/index10.htm, on February 21, 2004.

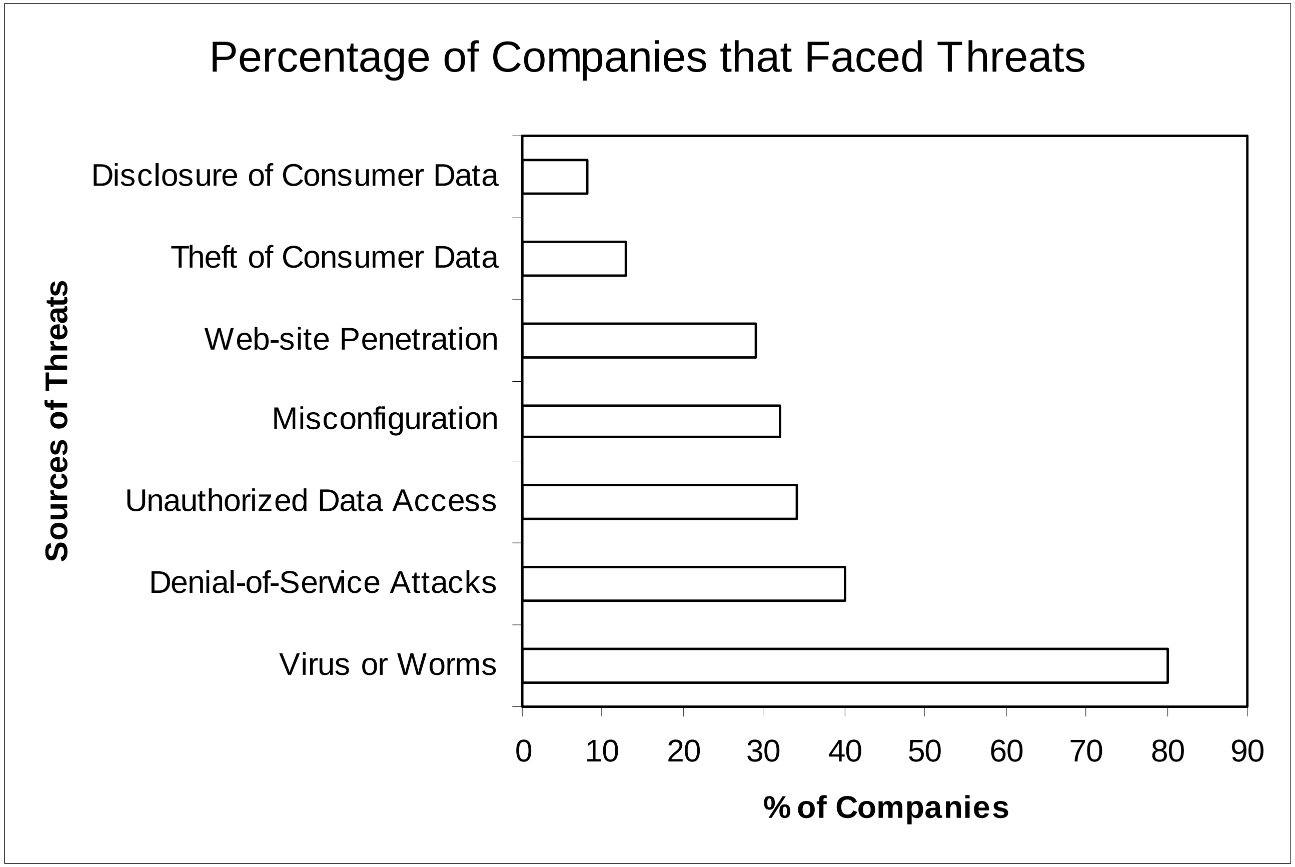
Passwords

Why Do We Use Passwords?

- To prevent unauthorized use of user accounts
- To prevent unauthorized access to important information
- To guarantee security of personal information
- To use various Internet Services securely

Computer Security

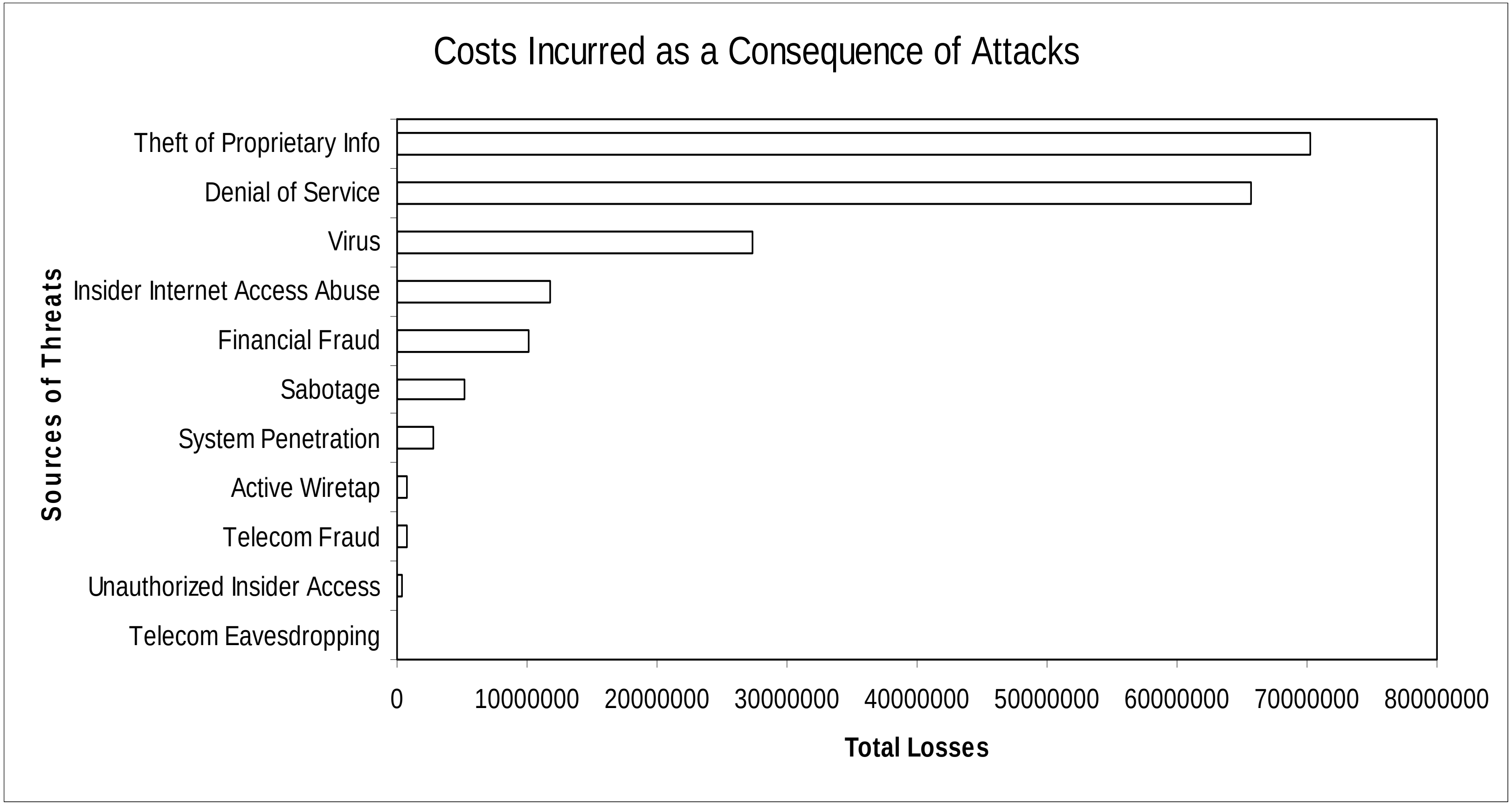
Threats Companies Faced



Information Week, January 5, 2004, p. 59

Computer Security

Threats Companies Faced



CERT

Computer Security

Impact

- U.S. companies spend more than $13 billion in damages caused by Security breaches. (Information Week, August 12, 2002)
- Eight banking web sites in the United States, Canada, Great Britain, and Thailand were attacked (AIG Web Site)
  - 23,000 credit card numbers were stolen.
  - The hackers proceeded to publish 6,500 of the cards online causing third-party damages in excess of $3M.
- In just the first five days of circulation, the I Love You virus cost businesses $6.7 billion. (CSO Magazine, December 2002).