CS-3002: Information Security

Lecture # 1: Security Goals, History of Attack and Underground Economy

Prof. Dr. Sufian Hameed
Department of Computer Science
FAST-NUCES

What is This Class About ?

Learn About Security

Make a Difference

How Can You Make a Difference?

- Be a more security-- aware user
  - Make better security decisions
- Be a more security– aware developer
  - Design & build more secure systems
- Be a security practitioner & researcher
  - Identify security issues
  - Propose new security solutions

Computer Security Today

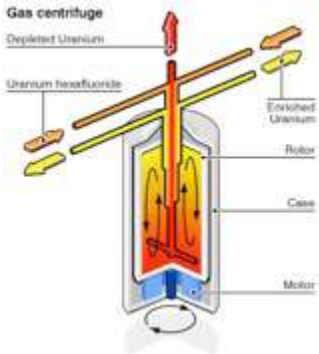
Why Computer Security ?

Computer systems are ubiquitous in our daily life

- Computers store and process our data and information
- Computers access and control our resources

Valuable Data

Private Data

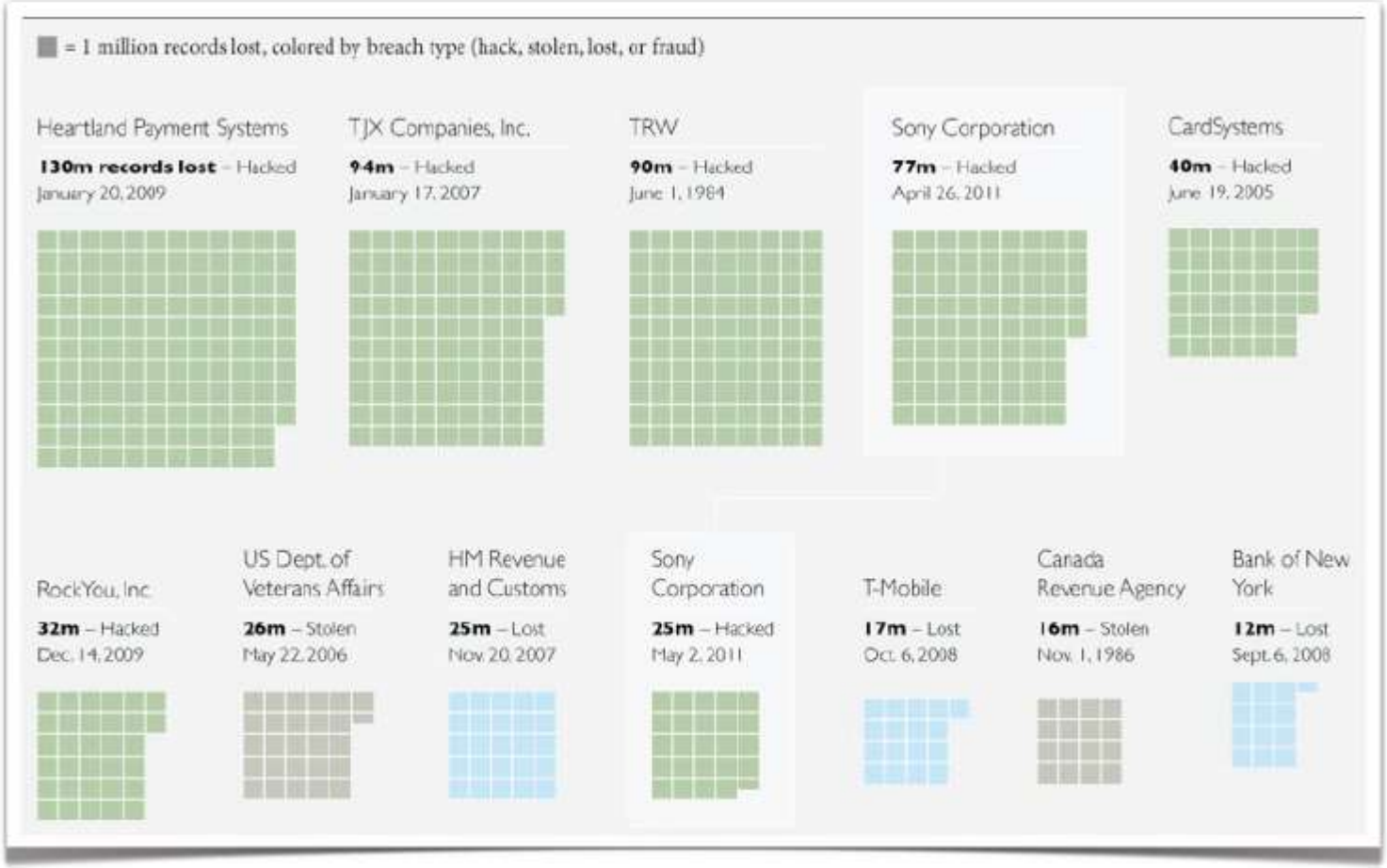


Dangerous Data

The Sony Breach

- **An Example:The Playstation Network (PSN) Attack**
  - Illegal intrusion into network around April 2011
  - Severe consequences for users and companies
  - Financial damage of over 24 billion dollars

Top Data Breaches



(Nathan Yau, http://flowingdata.com)

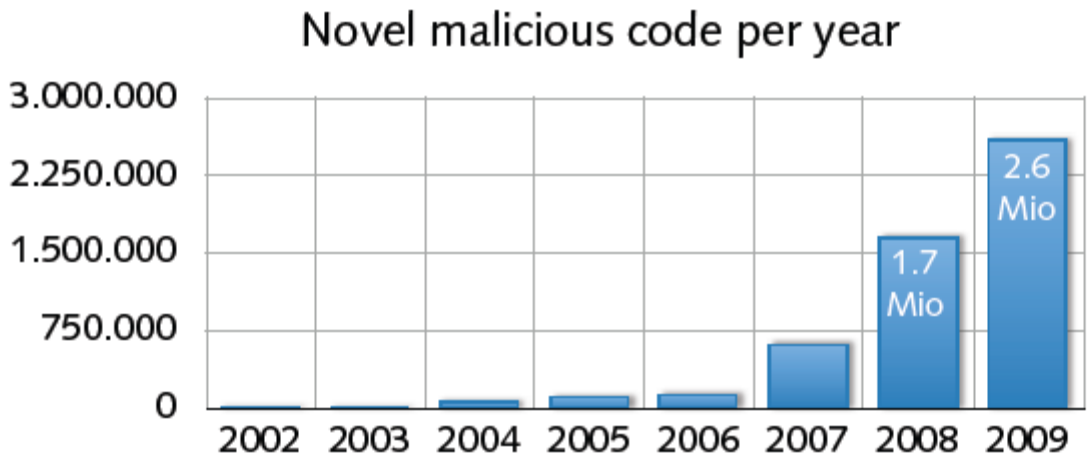
Further Example

- **Stuxnet Worm**
  - Computer worm detected in January 2010
  - Initially spread via MS Windows and targets Siemens industrial software and equipment (SCADA)
  - Spies on and disrupts industrial systems
  - Possible sabotage against uranium enrichment infrastructure in Iran

- **Rustock Botnet**
  - Network of 1.7 million infected systems (zombies)
  - Capability of sending 22 million spam messages per day
  - Active from around 2007 to March 2011
  - Taken down by Microsoft, U.S. Fed Agents and University of Washington
  - On July 18, 2011, Microsoft put a bounty of US$ 250 K on the individual behind Rustock botnet.

… more trouble ahead

- **Cyberspace — a dangerous place**
  - Omnipresence of computer attacks, viruses and worms
  - Persistent underground economy (worth billions of dollars)
  - Soon cyber-terrorism and cyber-warfare?



(Symantec, 2010)

Who is who ?

Informal terminology of attackers

Oldschool	Newschool	Description
Phreaker	—	Someone manipulating telephone systems
Hacker	Cracker	Someone breaking into computer systems
—	Hacker	Computer enthusiast
Cracker	Reverser	Someone reverse engineering programs
Lamer	Script kiddie	Unexperienced and naive attacker
—	Bot herder	Maintainer of a bot network
—	Spammer	Someone sending unsolicited emails
—	Hacktivist	Politically motivated attacker

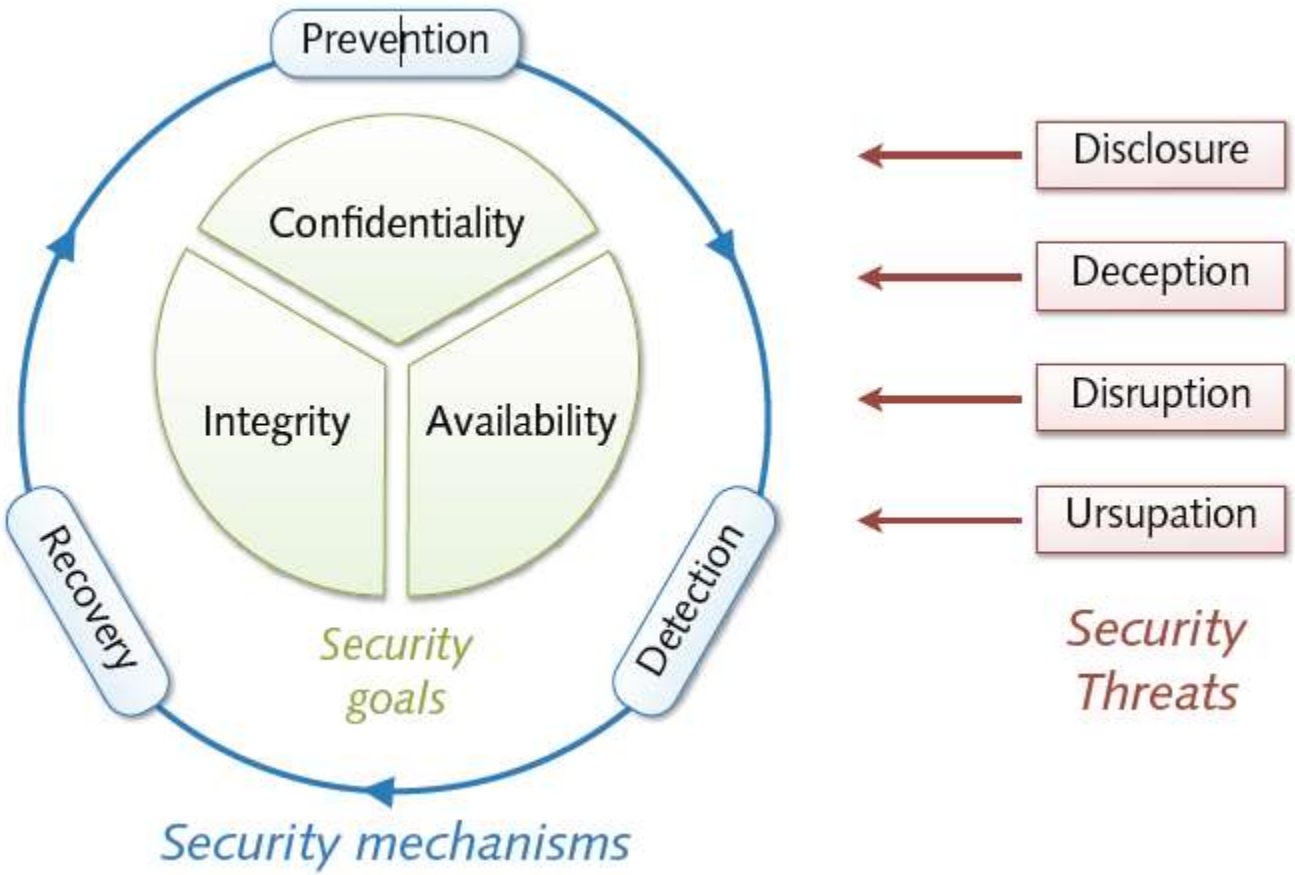
Various other types of attackers, e.g. crime, military, agencies, ...

Security is fun too!

- **Security is different from other disciplines**
  - Established concepts are put into questions
  - Intersection with many areas of computer science
  - Often, it’s a game of good and evil players
- **Practice and theory of security are often fun**
  - Monitoring, detection and analysis of real attacks
  - Reasoning about limits of attacks and defenses

Security Goals and Mechanisms

A Formal View



Security Goals

- **Security goals (memory hook: "CIA")**
  - *Confidentiality* of information and resources
  - *Integrity* of information and resources
  - *Availability* of information and resources
- **Basic definitions**
  - *Threat* = potential violation of a protective goal
  - *Security* = protection from intentional threats
  - *Safety* = protection from accidental threats

Confidentiality

Confidentiality

Protection of resources from unauthorized disclosure

Check: *Who* is authorized to access *which* resources?

- **Security measures**
  - Encryption of data, resource hiding
- **Examples**
  - An attacker eavesdrop a telephone conversation
  - An attacker reads the emails on your computer

Integrity

Integrity

Protection of resources from unauthorized manipulation

Check: *Who* does *what* on *which* resources?

- **Security measures**
  - Authorization, checksums, digital fingerprints
- **Examples**
  - An attacker changes the receipt of a bank transaction
  - An attacker tampers with files on your computer

Availability

Availability

Protection of resources from unauthorized disruption

Check: *When* and *how* are *which* resources used?

- **Security Measures**
  - Restriction, redundancy, load balancing
- **Examples**
  - An attacker crashes the web server of a company
  - An attacker formats the hard disk of your computer

Threats & Attacks

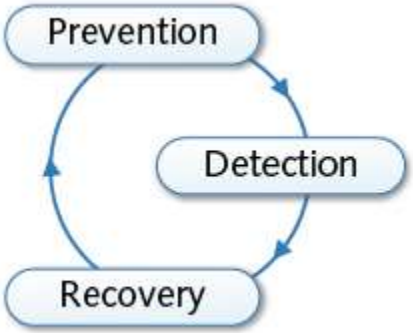
- **Basic classes of threats**
  - *Disclosure* = unauthorized access to information
  - *Deception* = acceptance of false data (e.g. masquerading)
  - *Disruption* = interruption or prevention of correct operation
  - *Usurpation* = unauthorized control of resources
- **Attack** = attempt to violate a security goal (intentional threat)
  - Often combinations of different threat classes

Examples of Attacks

- *Snooping* = passive eavesdropping of information
  → disclosure
  ✸ network sniffing, keyboard logging
- *Manipulation* = active modification of information
  → deception, disruption and usurpation
  ✸ redirection of control flow, man-in-the-middle attacks
- *Spoofing* = impersonation of one entity by another
  → deception and usurpation
  ✸ address spoofing, phishing attacks

Security Mechanisms

- **Security policies and mechanisms**
  - *Policy* = statement of what is and what is not allowed
  - *Mechanism* = method or tool enforcing a security policy
- **Strategies for security mechanisms**
  - *Prevention* of attacks
  - *Detection* of attacks
  - *Recovery* from attacks



- Bruce Schneier: *Security is a process, not a product!*

Prevention

- **Prevention of attacks**
  - Prevention of attacks *prior to violation of security goals*
- **Examples**
  - *Data reduction and separation*

    Removal or separation of information and resources
  - *Authentication and encryption*

    Restriction of access to information and resources
- **Limitations**
  - Inapplicable in many settings, e.g. open services

Detection

- **Detection of attacks**
  - Detection of attacks *during violation of security goals*
- **Examples**
  - *Anti-virus scanners*

    Detection of malicious code on computers
  - *Network intrusion detection*

    Detection of attacks in computer networks
- **Limitations**
  - Ineffective against unknown and “invisible” attacks

Recovery

- **Recovery**
  - Recovery from attacks *after violation of security goals*
- **Examples**
  - *Computer forensics*

    Investigation and analysis of security incidents
  - *Malware analysis*

    Observation and analysis of malicious software
- **Limitations**
  - Severe damage might have already occurred

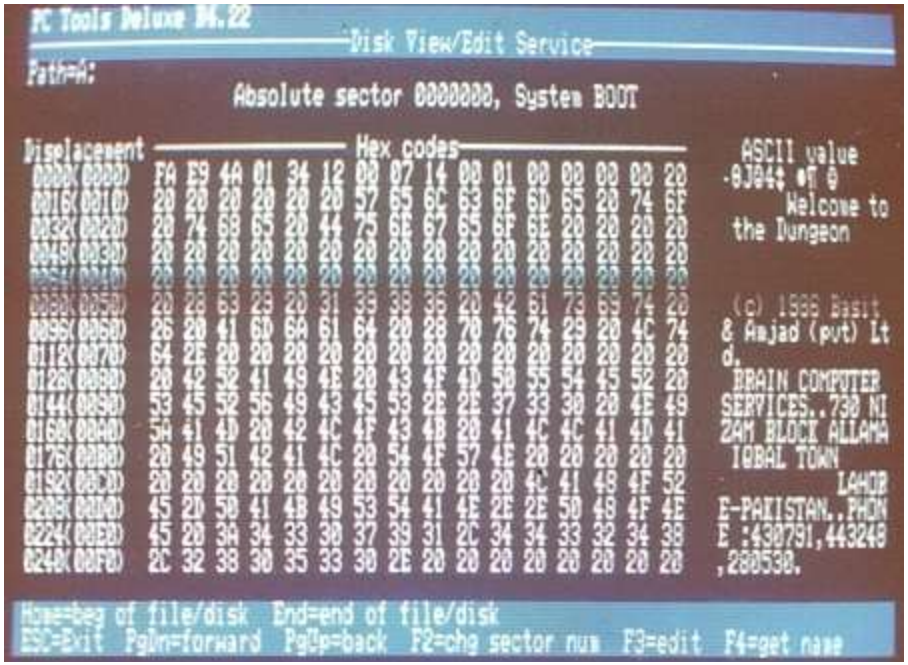
Further Concepts

- *Authenticity* = truthfulness of information and resources
  - May be viewed as an aspect of integrity
- *Accountability* = linking of actions and users
  - Realization of non-repudiation in computer systems
- *Privacy* = Security and control of personal information
  - Property of individuals and not of data

History of Attacks

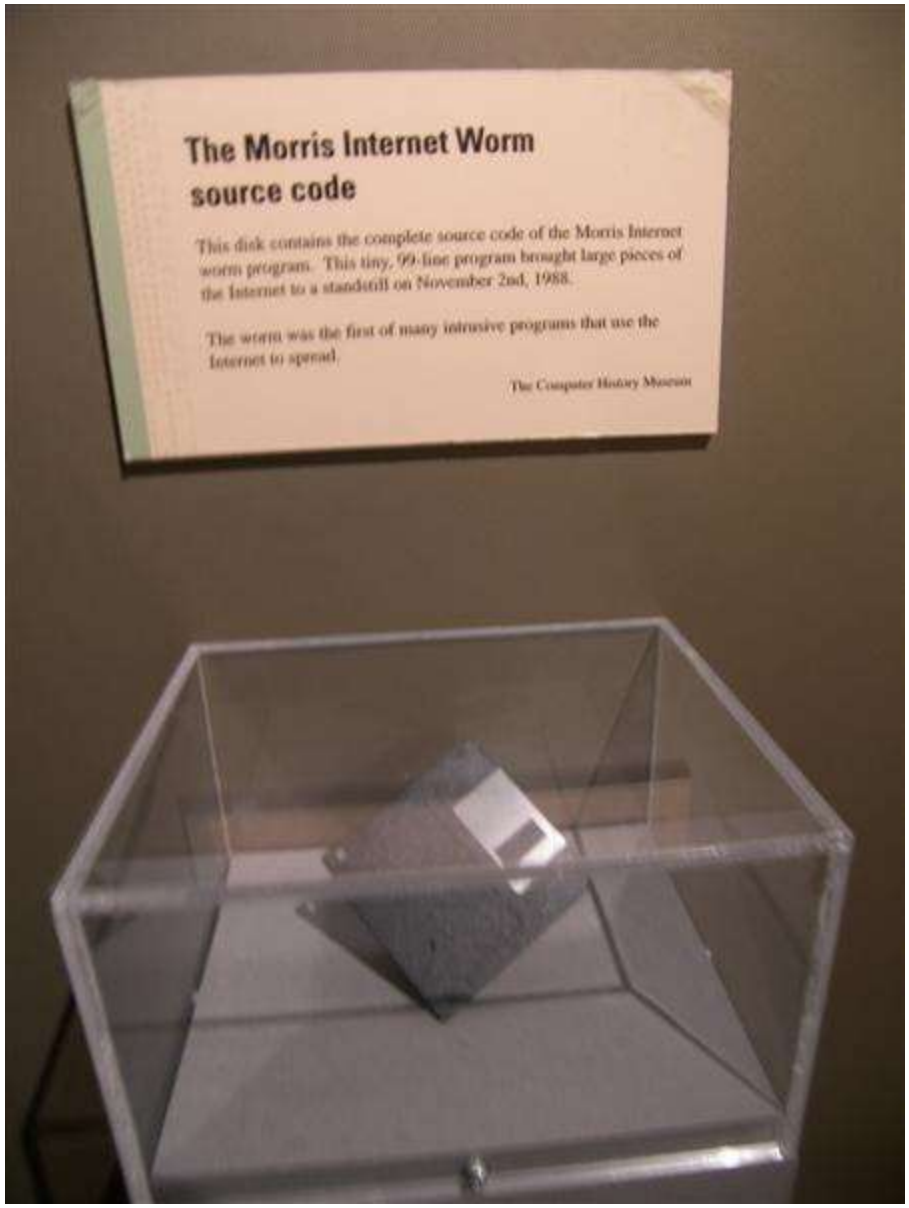
Brain: Where it all started …..

- **Brain** released in January 1986, is considered to be the first computer virus for MS-DOS.
- Infects the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system.
- Written by two brothers, Basit Farooq Alvi and Amjad Farooq Alvi from lahore.



Morris

- The **Morris worm** (November 2, 1988) was one of the first computer worms distributed via the Internet.
- It was written by a student at Cornell University, Robert Tappan Morris.
- The small program disables roughly 6,000 computers (10% of the internet) by flooding their memory banks with copies of itself.
- He is fined $10,000 and sentenced to three years' probation.



Melissa

- Melissa virus, created by David L Smith, was reported in 1999
- Exploited MS-Word, Outlook
- The virus was attached along with emails which had a message: “Here is that document you asked for, don’t show it to anybody else”
- On activation, it sends the same to the top 50 people in the contacts list
- Caused a heavy damage due to heavy traffic and it lead to the shutting down of email gateways of companies like Intel Corp., Alcatel Lucent, Microsoft .etc

ILoveLetter worm

- The "I Love You" virus (5 may 2000) infects millions of Windows PC overnight
- Started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs“
- Opening the attachment activated the Visual Basic script
- The worm did damage on the local machine, overwriting image files, and sent a copy of itself to the first 50 addresses in the Windows Address Book used by Microsoft Outlook.
- Also sends passwords and usernames stored on infected computers back to the virus's author.
- Authorities trace the virus to a young Filipino computer student, but he goes free because the Philippines has no laws against hacking and spreading computer viruses.

CodeRed

- The Code Red worm, released on 13th July, 2001, attacked Microsoft's IIS web servers
- Sneaked through the server via a patch in the indexing software with IIS
- Used the buffer overflow technique (a long string of repeated character 'N' was used to overflow a buffer)
- A fix was found in a month's time which limited the damage to $2.5 billion.

The affected sites were defaced with the message

HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

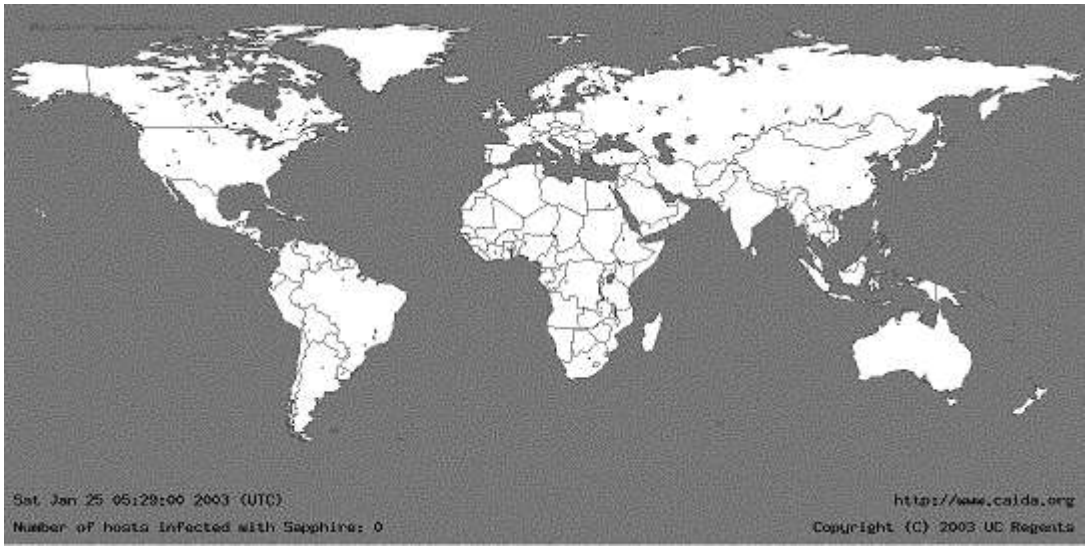
Nimda

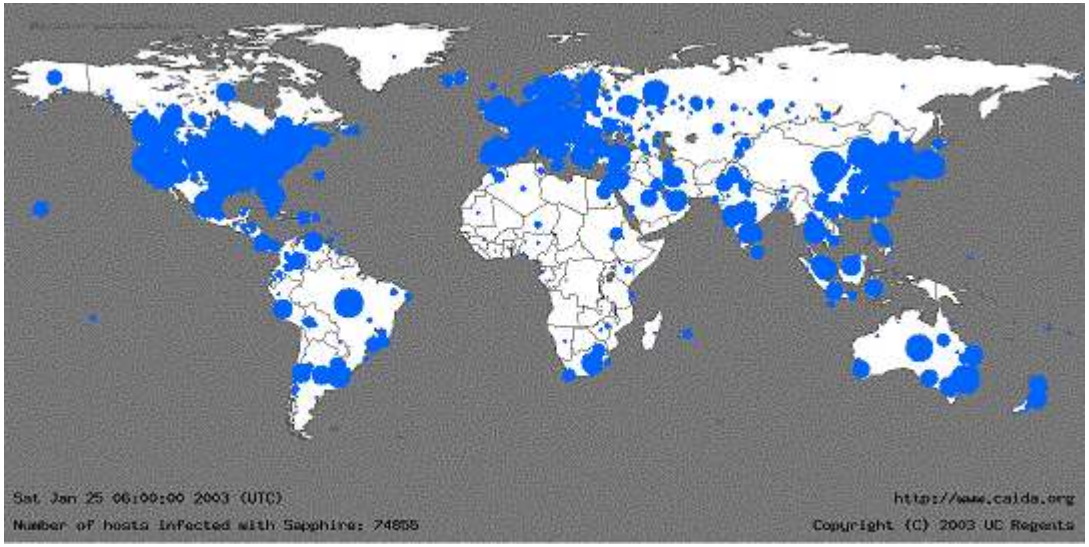
- Nimda was a file infector worm released on September 18, 2001,
- Spread through out the world in 22 minutes
- It used different methods for propagation i.e. emails, open network shares, backdoor left by other viruses
- Nimda spelled backwards is “Admin”
- Damage caused by Nimda : $ 635 million!

SQL Slammer aka Sapphire worm

- **SQL Slammer or the worm that ate the internet** (January 25, 2003) caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic
- Exploits the vulnerability in the Microsoft SQL servers and uses the buffer overflow bug to slow down the servers
- Slows down the entire Internet.
- Infects hundreds of thousands of computers in less than three hours
- *The fastest-spreading worm ever knocking cash machines offline and delaying airline flights*

SQL Slammer


Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents


Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

Current Trends

Historical hackers (prior to 2000)

- Profile:
  - Male
  - Between 14 and 34 years of age
  - Computer addicted
  - No social life




No Commercial Interest !!!

Source: Raimund Genes

Historical Hackers

- 1990s:
  - Phone phreaking, Free calls
- Early 2000s:
  - Email worms
  - CodeRed, Nimda

Financially Motivated

- Shift in late 2000s
- Spam
  - Pharmaceuticals
  - Fake products
- Carding/Fraud
  - Identify theft, credit fraud

Politically Motivated

- Stuxnet

Politically Motivated

Typical Botherder: *0x80"* *(pronounced X-eighty)*

High school dropout

- "…most of these people infect are so stupid they really ain't got no business being on the Internet in the first place."

Working hours: approx. 2 minutes/day to manage Botnet

Monthly earnings: $6,800 on average

Daily Activities:

- Chatting with people while his bots make him money
- Recently paid $800 for an hour alone in a VIP room ….

Job Description:

- Controls 13,000+ computers in more than 20 countries
- Infected Bot PCs download Adware then search for new victim PCs
- Adware displays ads and mines data on victim's online browsing habits.
- Bots collect password, e-mail address, SS#, credit and banking data

Washington Post: ***Invasion of the Computer Snatchers***

Some things in the news

- Nigerian letter (419 Scams) still works:
  - Michigan Treasurer Sends 1.2MUSD of State Funds !!!
- Many zero-day attacks
  - Google, Excel, Word, Powerpoint, Office …
- Criminal access to important devices
  - Numerous lost, stolen laptops, storage media, containing customer information
  - Second-hand computers (hard drives) pose risk
- Vint Cerf estimates ¼ of PCs on Internet are bots

Texas CISO, Feb 2010

Trends since 2010

- Malware, worms, and Trojan horses
  - spread by email, instant messaging, malicious or infected websites
- Botnets and zombies
  - improving their encryption capabilities, more difficult to detect
- Scareware – fake/rogue security software
- Attacks on client-side software
  - browsers, media players, PDF readers, etc.
- Ransom attacks
  - malware encrypts hard drives, or DDOS attack
- Social network attacks
  - Users' trust in online friends makes these networks a prime target.
- Cloud Computing - growing use will make this a prime target for attack.
- Web Applications - developed with inadequate security controls
- Budget cuts - problem for security personnel and a boom to cyber criminals.

Same list in Oklahoma Monthly Security Tips Newsletter

Monetization of Exploits

Marketplace for Vulnerabilities

Option 1: Bug Bounty Programs

- Google vulnerability reward program: 3K $
- Mozilla big bounty program: 500 $
- Pwn2Own competition: 15K $

Option 2:

- ZDI, iDefense purchases: 2K-10K $
  - Zero Day Initiative | 3Com | TippingPoint, a division of 3Com, http://www.zerodayinitiative.com/
  - Vulnerability Contributor Program // iDefense Labs, http://labs.idefense.com/vcp/

Marketplace for Vulnerabilities

- **Option 3: Black Market**

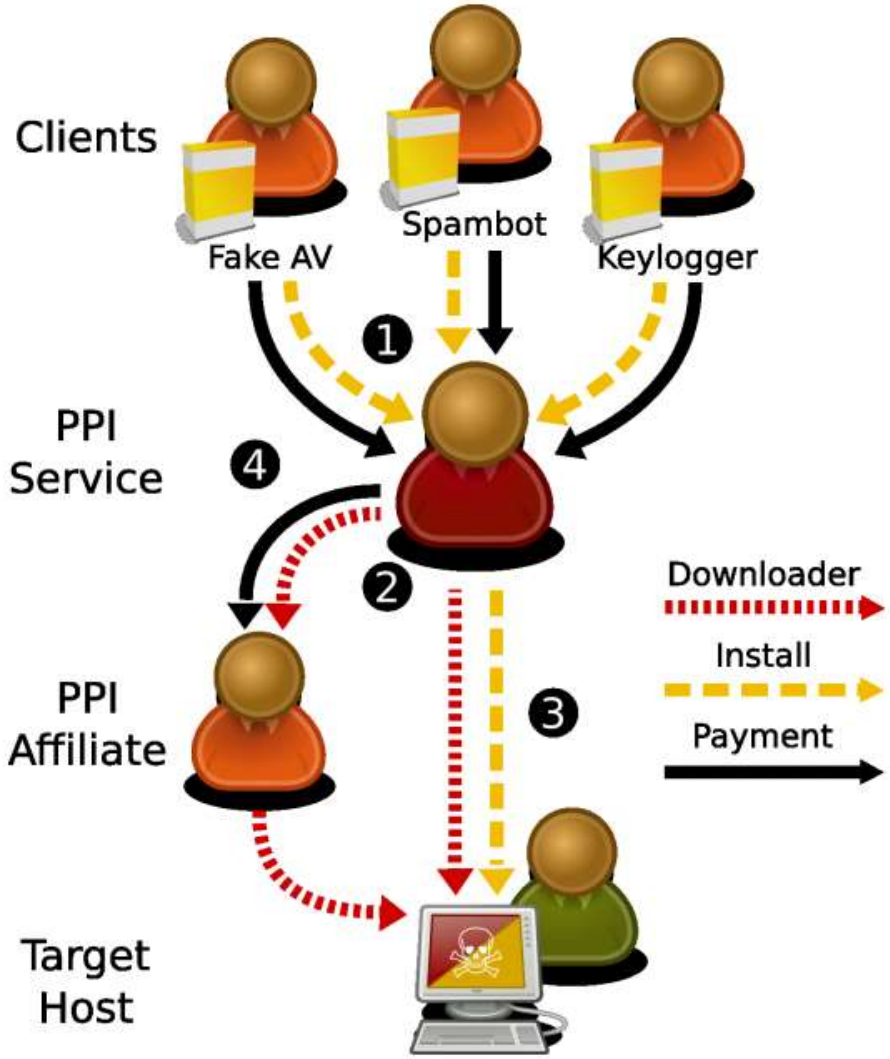
Vulnerability/Exploit	Value	Source
"Some exploits"	$200,000 - $250,000	A government official referring to what "some people" pay [9]
a "real good" exploit	over $100,000	Official from SNOsoft research team [10]
Vista exploit	$50,000	Raimund Genes, Trend Micro [8]
"Weaponized exploit"	$20,000-$30,000	David Maynor, SecureWorks [11]

Source: Charlie Miller (http://securityevaluators.com/files/papers/0daymarket.pdf). This is a very good read, also discussed the challenges involving legitimate buyers.

Underground Economy

- **Spam service**
- **Rent-a-bot**
- **Cash-out**

Marketplace for Pay-Per-Install (PPI)



Credit: Zulfikar Ramzan

Installs4Sale.net - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://installs4sale.net/

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Progra...

Google Search Sidewiki Bookmarks Translate AutoLink Sign in

Installs4Sale.net

Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

КОНТАКТЫ

560869831

550525933

info [at] installs4sale.net

ПРИЕМУЩЕСТВА

- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!

Convert Installs to Cash with High Rates

GoldInstall

Main | Sign up | Login | Rates | Contacts | Terms of service | FAQ

Prices

Goldinstall Rates for 1K Installs for each Country.

Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$
DK	20$
ES	30$
AU	55$
FR	30$
NL	20$
NO	20$
PT	30$
LB	6$

Earning4u.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://earning4u.com/index.php?l=en

Most Visited Getting Started Latest Headlines Exchange - GraBBerZ ... GraBBerZ CoM http://www.sysnet.ucs... GraBBerZ CoM Cyber Genome Progra...

Google "underground economy" blackhat Search Sidewiki Bookmarks Translate stefan...

Earning4u.com

EARNING4U.COM

ENTER STATS

BETTER RATES! NO HOLD!
ONLY REAL ONLINE STATISTIC!

REGISTER TODAY

MAIN | ABOUT US | CONDITIONS | RATES | FAQ | CONTACTS

The partnership program «Earning4u» is the easiest way to earn money.
All you need to do to start working with us is register.

You will earn from 6$(Asia) to 180$(USA) per 1000 installs. You can view all prices in the «Rates» section.

Key Features

Thanks to an individual approach to each client when you work with our system you have:

- Online statistics updated in real time
- A 24-hour support service ready to answer all your questions
- Absolutely no shaving and total independence of your statistics from other system users
- Stable weekly payments on virtually all payment systems: Fethard, WebMoney, Wire, e-gold, Western Union (WU), MoneyGram, Anelik and ePassporte, and PayPal
- For regular clients and for those making more than 5000 installs per day – higher rates for all countries and special working conditions

We have more than 8 years' experience in working with installs. Our regular clients include more than 1000 webmasters who are all pleased to work with us.

Find: Next Previous Highlight all Match case

Done

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.pay-per-install.com/ Go Links

PAY PER INSTALL AFFILIATE PROGRAMS

Today is: Tuesday 16. November 2010

CLICK HERE TO VISIT OUR BEST SPONSOR.

WE WORK
Even when you sleep!

One of the best PPI programs. Up to $180 per 1000 Installs.

Affiliate Program NewsLetter Get new programs via email

Insert your Email Address: Subscribe

JOIN MAKE MONEY FORUM

Learn How to make money with PPN Gateway

Free guide to teach you how to make $7000 per day

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates.

BOOKMARK US

MAKE MONEY CATEGORIES
- Pay Per Click
- Pay Per Impression
- Bid Search Engines
- Pay Per Lead
- Pay Per Install

OTHERS
- CONTACT

GET PAID from each toolbar install

Best Pay-per-install affiliate programs on the net. Earn money with any traffic, these ActiveX affiliates will convert anything and make you rich. Payments are up to $1.50 per install. You usualy distribute installation of toolbar and making cash. You can also make loads of money with content sites such are movies, games, mp3 and protect your content with Content Gateways which are paying most, to unlock the content user needs to install simple adware application and than he can get content for free.

All

Pages: [0] [1] [2] [3] [4]

Make money with these BEST AFFILIATE PROGRAMS

BOOKMARK US

Last 10 Reviews
- CPALead - November/13/2010
- SexSearch - October/31/2010
- LoudMo - October/28/2010
- SexSearch - October/18/2010
- SexSearch - October/18/2010
- ioXes - October/12/2010
- Earning4u - September/09/2010
- Earning4u - August/30/2010

Recommended reading

- The Underground Economy of the Pay-Per-Install (PPI) Business by Kevin Stevens
- Measuring Pay-per-Install: The Commoditization of Malware Distribution by Juan Caballero (Usenix Sec 2011)

Why are there security vulnerabilities?

- Lots of buggy software...
  - Why do programmers write insecure code?
  - Awareness is the main issue

- Some contributing factors
  - Few courses in computer security
  - Programming text books do not emphasize security
  - Few security audits
  - C is an unsafe language
  - Programmers have many other things to worry about
  - Legacy software (some solutions, e.g. Sandboxing)
  - Consumers do not care about security
  - Security is expensive and takes time

If you remember only one thing from this course:

A vulnerability that is “too complicated for anyone to ever find” will be found !

I hope you remember more than one thing

Summary

Summary

- Threat landscape is *highly dynamic* as it is driven by economic motivation, and especially organized crime
- No *"final state of security"*
- Prevention not always possible; intelligent response mechanisms are strongly needed.

Acknowledgements

Material in this lecture are taken from the slides prepared by:

- Prof. Dr. Konrad Rieck (Uni-Göttingen)