



Introduction to Information Security

Learning Objectives

Upon completion of this material, you should be able to:

- Define key terms and critical concepts of information security.
- List the key challenges of information security, and key protection layers.
- Describe the CNSS security model (McCumber Cube).
- Be able to differentiate between *threats* and *attacks* to information.
- Identify today's most common threats and attacks against information.

Required reading:

Management of Information Security (MIS), by Whitman & Mattord

Chapter 1, pages 1 – 8

Introduction

“In the last 20 years, technology has permeated every facet of the business environment. The business place is no longer static – it moves whenever employees travel from office to office, from office to home, from city to city. Since business have become more fluid, ..., **information security is no longer the sole responsibility of a small dedicated group of professionals, ..., it is now the responsibility of every employee, especially managers.**”

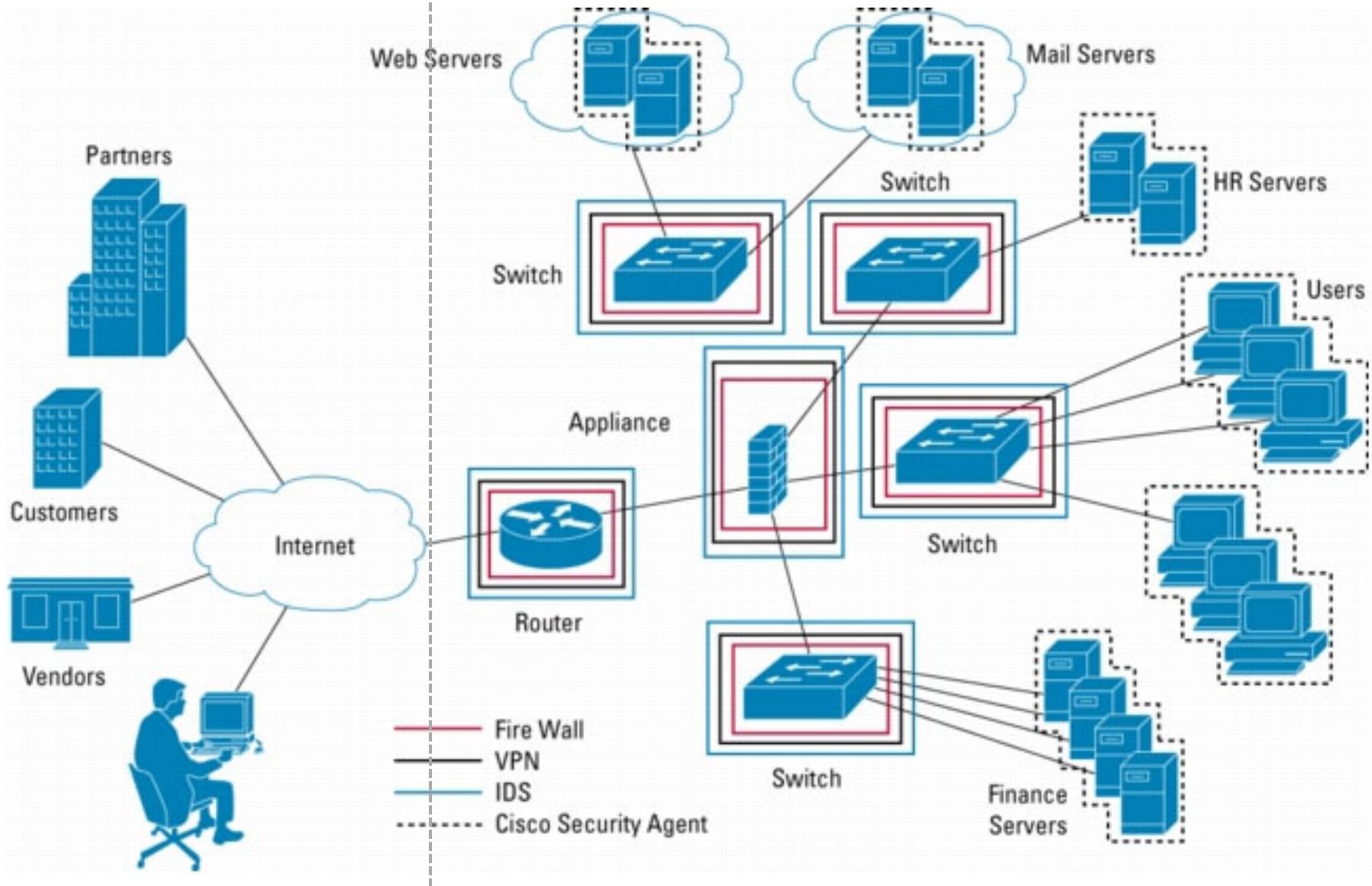


<http://www.businessandleadership.com/fs/img/news/200811/378x/business-traveller.jpg>

<http://www.koolringtones.co.uk/wp-content/uploads/2010/01/mobile-phones.jpg>

Internet

corporation



Organization	Description of security breach	Number of identities exposed
Grays Harbor Pediatrics, WA	A backup tape, stolen from an employee's car, was used for storing copies of paper records; patients may have had their names, Social Security numbers, insurance details, driver's license information, immunization records, medical history forms, previous doctor records, and patient medical records stolen	12,000
Tulane University, LA	A university-issued laptop was stolen from an employee's car. It was used to process 2010 tax records for employees, students, and others; the information included names, Social Security numbers, salary information, and addresses	10,000
Seacoast Radiology, NH	Patient names, Social Security numbers, addresses, phone numbers, and other personal information were exposed by a security breach	231,400
Centra, GA	A laptop was stolen from the trunk of an employee's rental car that contained patient names and billing information	11,982
Stony Brook University, NY	Student and faculty network and student IDs were posted online after a file with all registered student and faculty ID numbers was exposed	61,001
deviantART, Silverpop Systems Inc., CA	Attackers exposed the e-mail addresses, usernames, and birth dates of the entire user database	13,000,000
Twin America LLC, CitySights, NY	An attacker inserted a malicious script on a Web server and stole the customer database that contained customer names, credit card numbers, credit card expiration dates, CVV2 data, addresses, and e-mail addresses	110,000
Ohio State University, OH	Unauthorized individuals logged into an Ohio State server and accessed the names, Social Security numbers, dates of birth, and addresses of current and former students, faculty, staff, University consultants, and University contractors	750,000
Gawker, NY	Attackers gained access to the database and accessed staff and user e-mails and passwords	1,300,000

Introduction (cont.)

Example: Gawker – importance of good passwords

The first thing the Gnosis group does in the synopsis it released of their attack is identify Nick Denton's (founder of Gawker Media) password, and point out that it is the same password he uses for Gawker's Google Apps account and on his twitter account @nicknoted. They go on to provide 16 more Gawker staffer's e-mail addresses, user names, and passwords. The passwords, 15 of which are strings that are either common dictionary words or slight variations thereof and one that is the person's name and 1, indicate that Gawker has no password composition policy (how long passwords should be, that they should contain letters/numbers/special characters) for employees.

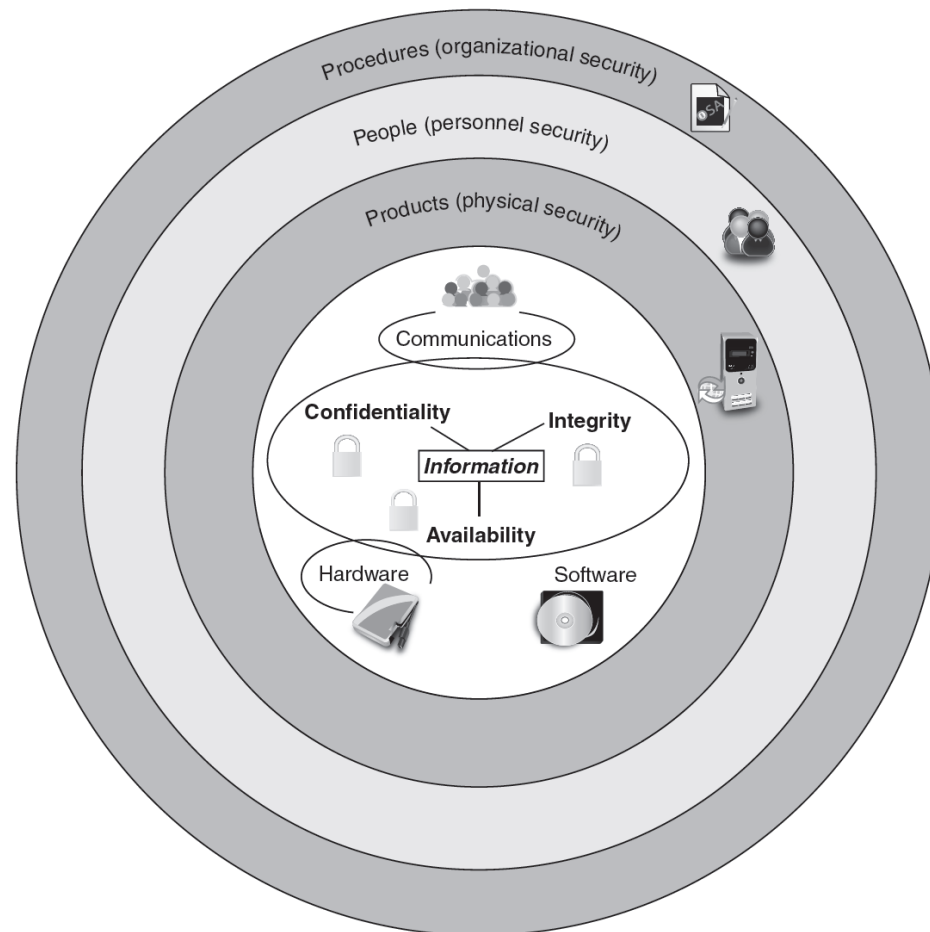
They also determined his password on the campfire team collaboration tool instance used by Gawker (a real time chat utility) and with it extracted 4 gigabytes of Gawker chat logs. From within those chat logs the attackers were able to extract FTP (file transfer protocol) servers, usernames, and credentials for the sites thq.com, valvesoftware, rockstargames, lucasarts, scea, kotaku, and 2kgames.

Information Technology

- **Information Technology** – technology involving development and use of computer systems and networks for the purpose of processing and distribution of data
 - ❖ in many organizations, information/data is seen as the most valuable asset
- **Information System** – entire set of **data**, **software**, **hardware**, **networks**, **people**, **procedures** and **policies** that deal with processing & distribution of information in an organization
 - ❖ each of 7 components has its own strengths, weaknesses, and its own security requirements

Information Technology (cont.)

Information is stored on computer hardware, manipulated by software, transmitted by communication, used by people, etc.
⇒ each of these areas must be adequately protected!

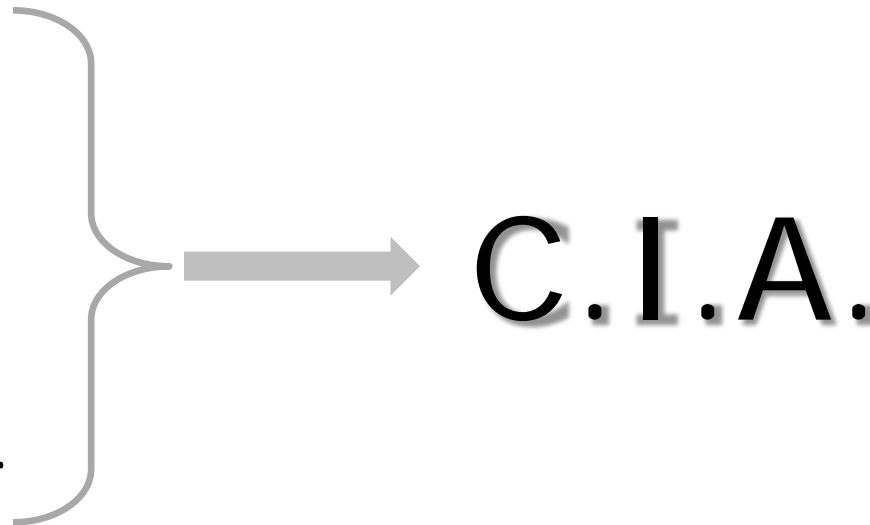


Information Security

**Security = state of being secure,
free from danger.**

- **Information Security** – practice of defending digital information from unauthorized

- ◆ access
- ◆ use
- ◆ recording
- ◆ disruption
- ◆ modification
- ◆ destruction, ...



Information Security (cont.)

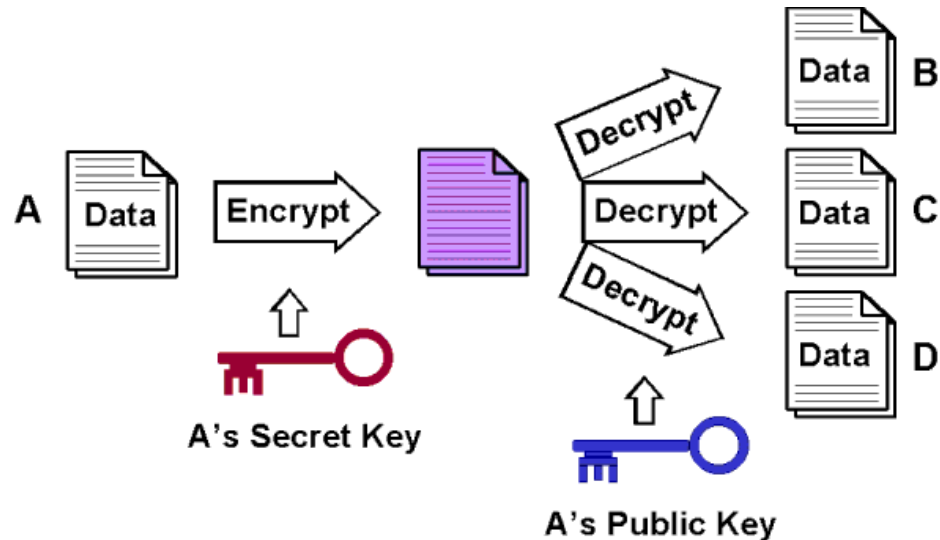
- **C.I.A. triangle** – 3 key characteristics of info. that must be protected by information security:
 - ◊ **confidentiality** - only authorized parties can view information
 - ◊ **integrity** - information is correct and not altered over its entire life-cycle
 - ◊ **availability** - data is accessible to authorized users whenever needed



Information Security (cont.)

Example: How to ensure data confidentiality?

➤ cryptography



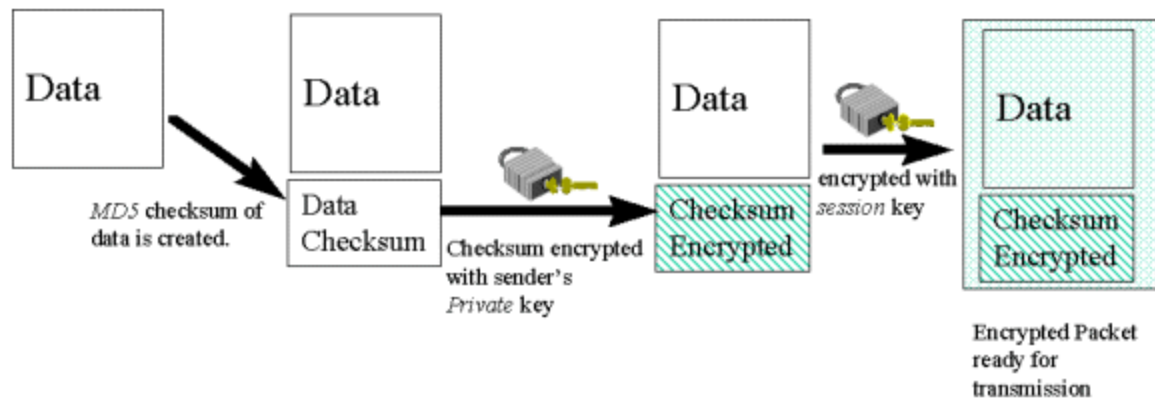
➤ strong user authentication / restricting access

➤ limiting number of places where data can appear
(e.g., read only, cannot be stored on an USB)

Information Security (cont.)

Example: How to ensure data integrity?

- strong user authentication / restricting access
- cryptography

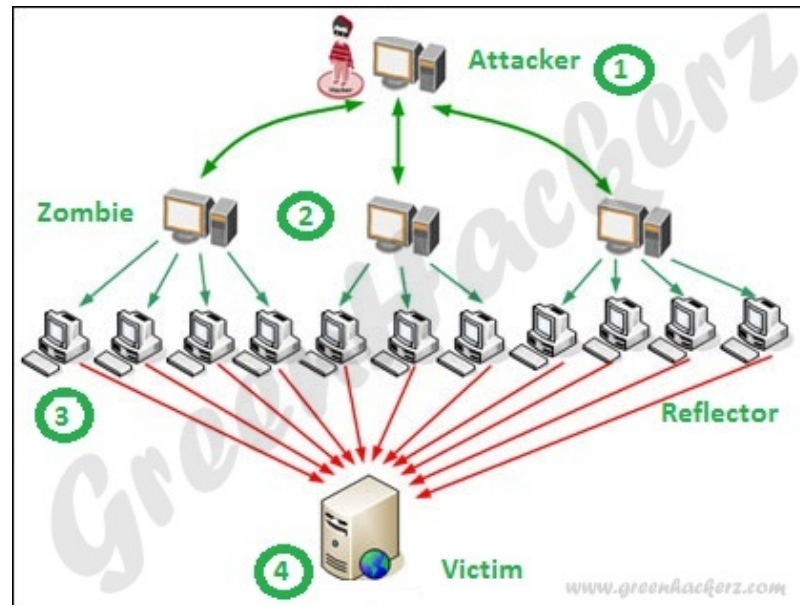


- documenting system activity

Information Security (cont.)

Example: How to ensure data availability?

➤ anti-DDoS system



➤ well established backup procedure

➤ effective data-recovery procedure

Information Security (cont.)

Example: The biggest challenge of information security?

➤ How much of security?

Information security should balance protection & access - a completely secure information system would not allow anyone access, or would be very 'user-unfriendly'!

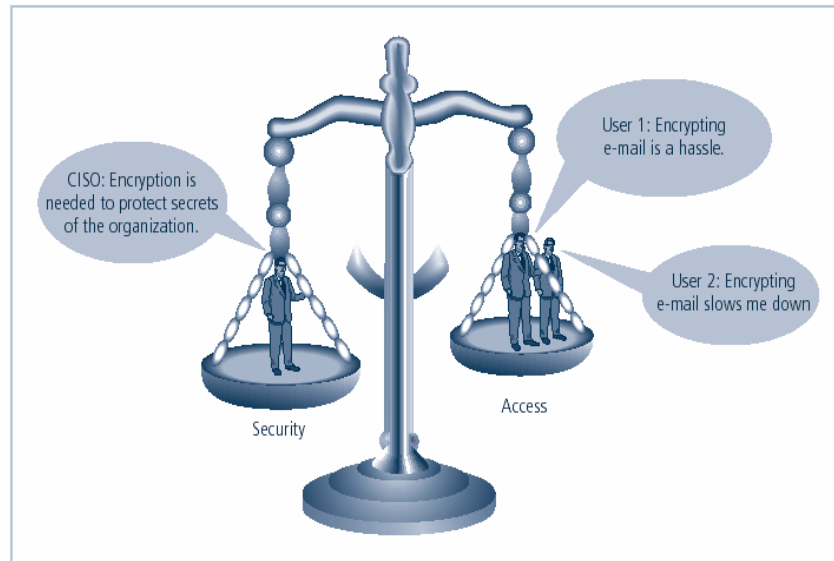


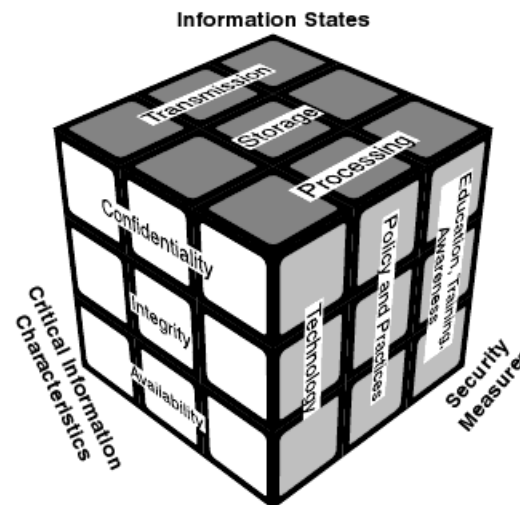
FIGURE 1-7 Balancing Information Security and Access

Information Security (cont.)

**Where/how do we start
building or evaluating
a security system?**

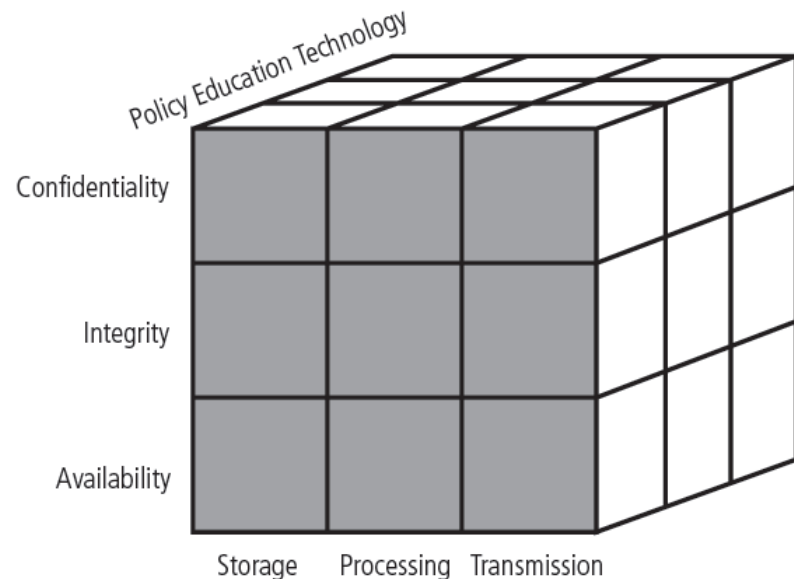
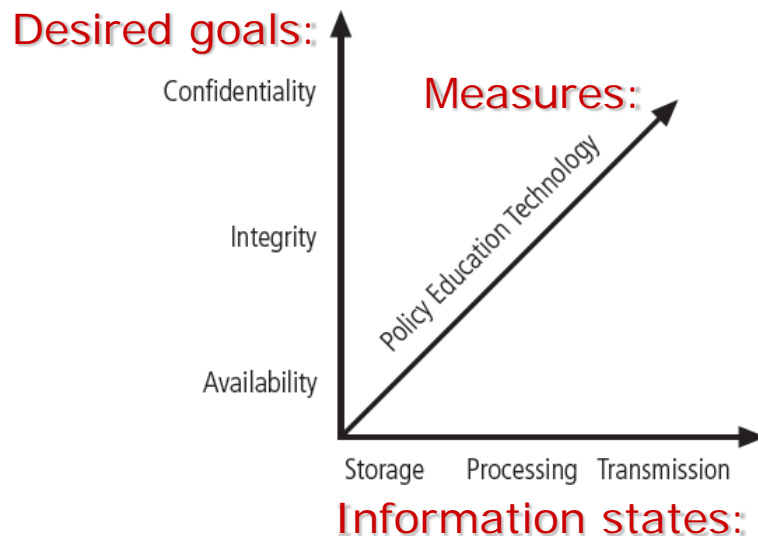
CNSS Security Model

- **CNSS = Committee on National Security Systems**
- **McCumber Cube** – Rubik's cube-like [detailed model](#) for establishment and evaluation of information security
 - ◆ to develop a secure system, one must consider not only key security goals (CIA) but also how these goals relate to various states in which information resides and full range of available security measures



CNSS Security Model (cont.)

- Each of 27 cells in the cube represents an area that must be addressed to secure an information system
 - ❖ e.g., intersection between **data integrity**, **storage** and **technology** implies the need to use technology to protect data integrity of information while in storage
 - solution: host intrusion system that alerts the security administrator when a critical file is modified



**Are all 27 aspects of security
worth examining
at every company?**

Threats

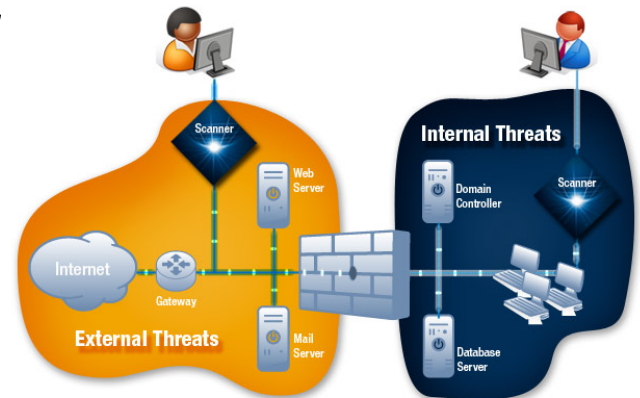
- **Security threat** – any action/inaction that could cause disclosure, alteration, loss, damage or unavailability of a company's/individual's assets
- There are three components of threat:
 - ◆ **Targets**: organization's asset that might be attacked
 - information (its confidentiality, integrity, availability), software, hardware, network service, system resource, etc.
 - ◆ **Agents**: people or organizations originating the threat – intentional or non-intentional
 - employees, ex-employees, hackers, commercial rivals, terrorists, criminals, general public, customers
 - ◆ **Events**: type of action that poses the threat
 - misuse of authorized information, malicious / accidental alteration of information, malicious / accidental destruction of information, etc.

Threats (cont.)

- Each organization must prioritize its threats based on:

- ◆ its business priorities

- e.g. what are the company's main assets:
 - (a) web servers (e-commerce company),
 - (b) data (software company)?



- ◆ conditions under which its key assets operate

- e.g. are there any wireless links / access points?

- ◆ organizational strategy regarding risk

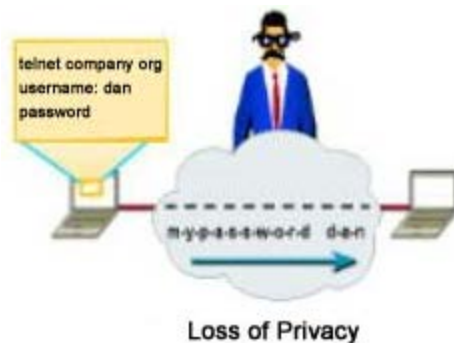
- e.g. cost/time of encrypting every file/email vs. worker's productivity

Threats (cont.)

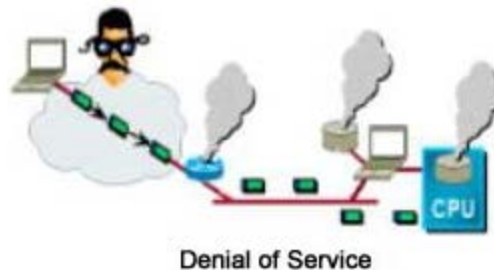
Example: Companies and their threats

Which of the three threats is most critical for which of the three companies?

Amazon



Hospital



TD Bank



Threat Events

- **General groups of threat events:**

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Deviations in quality of service by service providers	Power and WAN quality of service issues from service providers
Forces of nature	Fire, flood, earthquake, lightning
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Threat Events (cont.)

- **Top Threat-Driven Expenses (C-ACM study)**

Top Threat-Driven Expenses	Rating
1. Deliberate software attacks	12.7
2. Acts of human error or failure	7.6
3. Technical software failures or errors	7.0
4. Technical hardware failures or errors	6.0
5. Quality-of-service deviations from service providers	4.9
6. Deliberate acts of espionage or trespass	4.7
7. Deliberate acts of theft	4.1
8. Deliberate acts of sabotage or vandalism	4.0
9. Technological obsolescence	3.3
10. Forces of nature	3.0
11. Compromises to intellectual property	2.2
12. Deliberate acts of information extortion	1.0

Threat Events

Hardware and Software Failures and Errors

- ❖ cannot be controlled or prevented by the organization
- ❖ best defense: keep up-to-date about latest hardware /software vulnerabilities

Forces of Nature

- ❖ fire, flood, earthquake, hurricane, tsunami, electrostatic discharge, dust contamination
- ❖ organization must implement controls to limit damage as well as develop incident response plans and business continuity plans

Threat Events (cont.)

Who is the biggest threat to your organization?



Tom Twostory
convicted burglar



Dick Davis a.k.a.
"wannabe amateur hacker"



Harriet Allthumbs
employee
accidentally
deleted the one copy
of a critical report

Threat Events

Act of Human Error or Failure

- ❖ organization's own employee's are one of its greatest threats
- ❖ examples:
 - entry of erroneous data
 - accidental deletion or modification of data
 - failure to protect data
 - storing data in unprotected areas

outside



inside

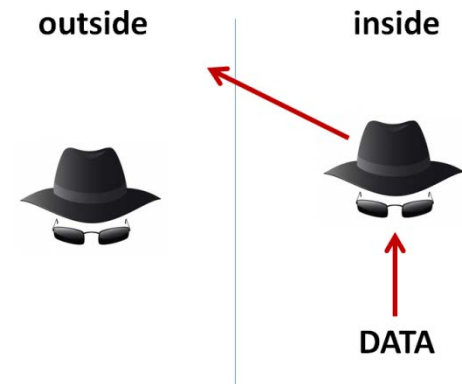


- Much of human error or failure can be prevented
 - ❖ preventative measures:
 - training and ongoing awareness activities
 - enhanced control techniques:
 - ★ require users to type a critical command twice
 - ★ ask for verification of commands by a second party

Threat Events

Compromise to Intellectual Property (IP)

- ❖ IP = ideas or any tangible or virtual representation of those ideas
- ❖ any unauthorized use of IP constitutes a security threat
- ❖ defense measures:
 - use of digital watermarks and embedded code



Example: Peter Morch story – compromise to IP

In 2000, while still employed at Cisco Systems, Morch logged into a computer belonging to another Cisco software engineer, and obtained (burned onto a CD) proprietary information about an ongoing project.

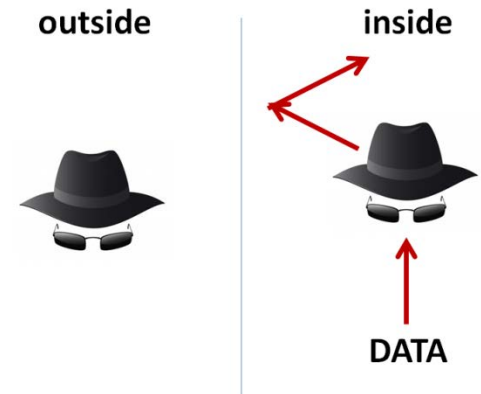
Shortly after, Morch started working for Calix Networks – a potential competitor with Cisco. He offered them Cisco's information.

Morch was sentenced to 3 years' probation.

Threat Events

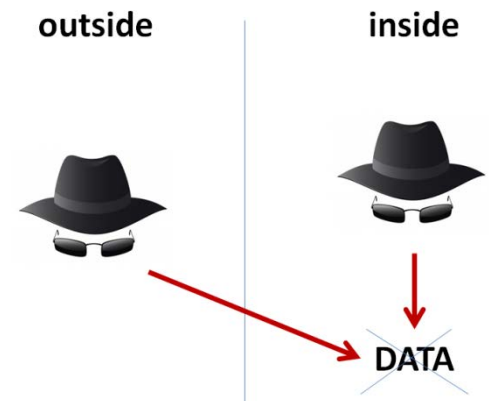
Deliberate Act of Info. Extortion / Blackmail

- ❖ hacker or trusted insider steals information and demands compensation for its return
- ❖ example:
 - theft of data files containing customer credit card information



Deliberate Act of Sabotage or Vandalism

- ❖ acts aimed to destroy an information asset and, ultimately, damage the image of an organization
- ❖ example:
 - hackers accessing a system and damaging or destroying critical data



Threat Events

Example: Maxus story – info. extortion by outsider

In 2000, a mysterious hacker identified as Maxus demanded \$100,000 from CDUniverse company in exchange for not releasing the names and credit card numbers of over 350,000 customers he had obtained from the company website.

After CDUniverse failed to pay him, Maxus decided to set up the site, titled Maxus Credit Cards Datapipe, and to give away the stolen customer data. He announced the site's presence Dec. 25th on an Internet Relay Chat group devoted to stolen credit cards.

Soon after launching his site, Maxus said it became so popular among credit card thieves that he had to implement a cap to limit visitors to one stolen card at a time.

Apprehending Maxus will not be easy, said Richard M. Smith, an online security expert in Brookline, Mass., who helped federal agents track down the author of the Melissa virus, David L. Smith. Maxus appears to move about online using stolen accounts and relays his email through other sites to conceal the originating Internet protocol address ...

www.nytimes.com/2000/01/10/business/thief-reveals-credit-card-data-when-web-extortion-plot-fails.html
www.cyberagecard.com/news/?page=2

Threat Events

Example: Two Kazakhstan employees story – info. extortion by **insider**

In 2002, two employees in a company in Kazakhstan allegedly got access to Bloomberg L.P. financial information database because their company was an affiliate of Bloomberg.

They allegedly demanded \$200,000 from Bloomberg to reveal how they got access to the database.

Bloomberg opened an offshore account with \$200,000 balance, and invited the pair to London to personally meet with Michael Bloomberg.

At the meeting there were police officials who arrested the two alleged extortionists.

NOTE: finding a vulnerability and requiring payment to learn about it may be considered extortion.

<http://www.cybercrime.gov/zezevIndict.htm>

Threat Events

Example: Patrick McKenna story – information vandalism by **insider**

In 2000, McKenna was fired by Bricsnet (software company). As a revenge, he remotely accessed his former employer's computer server, and:

- 1) deleted approximately 675 computer files;
- 2) modified computer user access levels;
- 3) altered billing records;
- 4) sent emails, which appeared to have originated from an authorized representative of the victim company to over 100 clients. Emails contained false statement about business activities of the company.

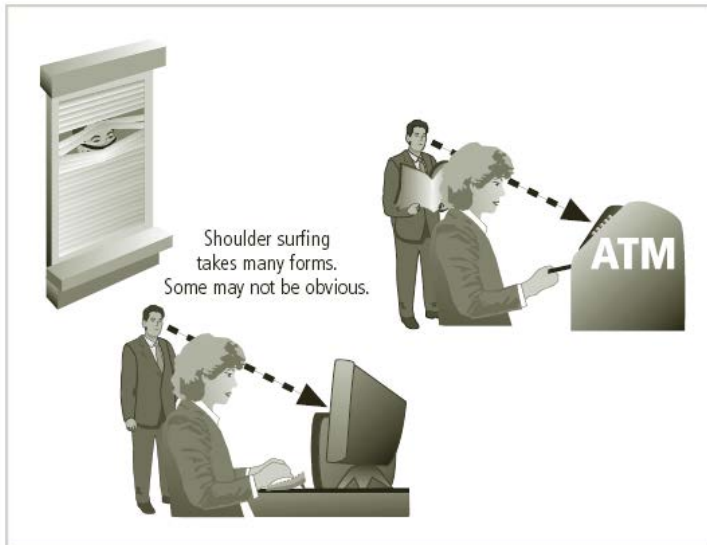
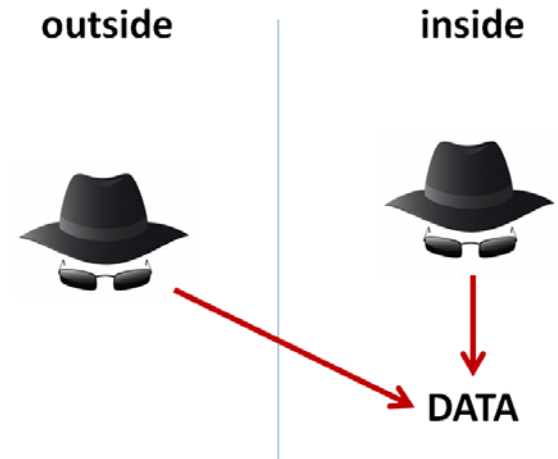
He was sentenced to 6 months in prison, followed by 2-years of supervised release. He was also ordered to pay \$13,614.11 for caused damages ...

<http://www.cybercrime.gov/McKennaSent.htm>

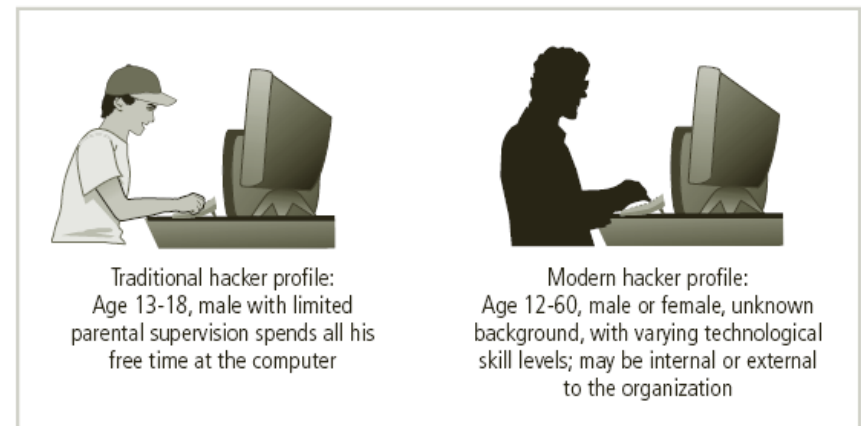
Threat Events

Deliberate Act of Trespass

- ❖ unauthorized access to info. that an organization is trying to protect
- ❖ low-tech: **shoulder surfing**
- ❖ high-tech: **hacking**



shoulder surfing



hacker profiles

Threat Events

Example: Princeton vs. Yale – trespass by outsider

Yale University's admission created a web-based system to enable applicants to check the status of their application on-line. To access the system, the applicants had to prove their identity by answering questions regarding their name, birth date, SIN.

Many of these students also applied to other top universities.

At Princeton, associate dean and director of admissions Stephen LeMenager knew that the private information that Yale used to control access was also in the applications that candidates submitted to Princeton. He used this information to log into the Yale system several times as applicants.

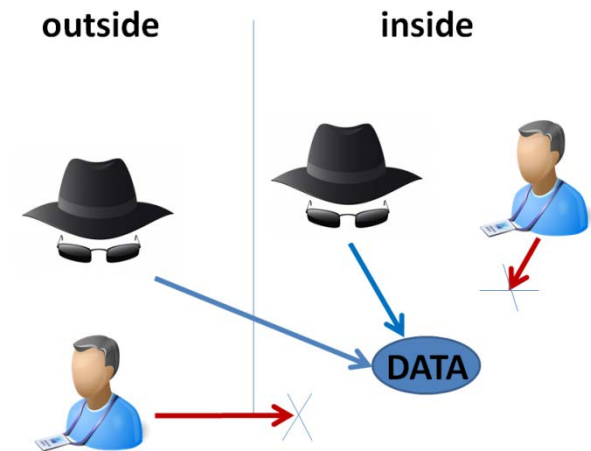
When the word got out, he admitted doing the break-ins but said that he was merely testing the security of the Yale system. Princeton put him on administrative leave.

The case emphasizes that information used to control access must not be generally available ...

Threat Events

Deviations in Quality of Service

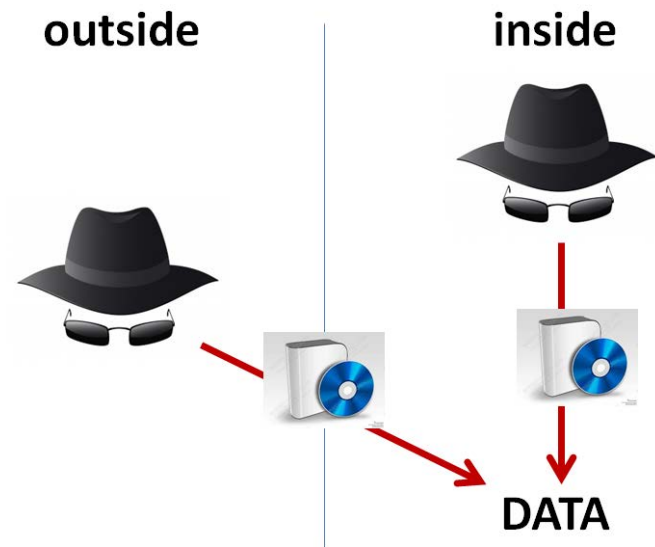
- ❖ in organizations that relies on the Internet and Web, irregularities in **available bandwidth** or **server's CPU** can dramatically affect their operation
 - e.g. employees or customers cannot contact the system



Threat Events: Deliberate Software Attacks

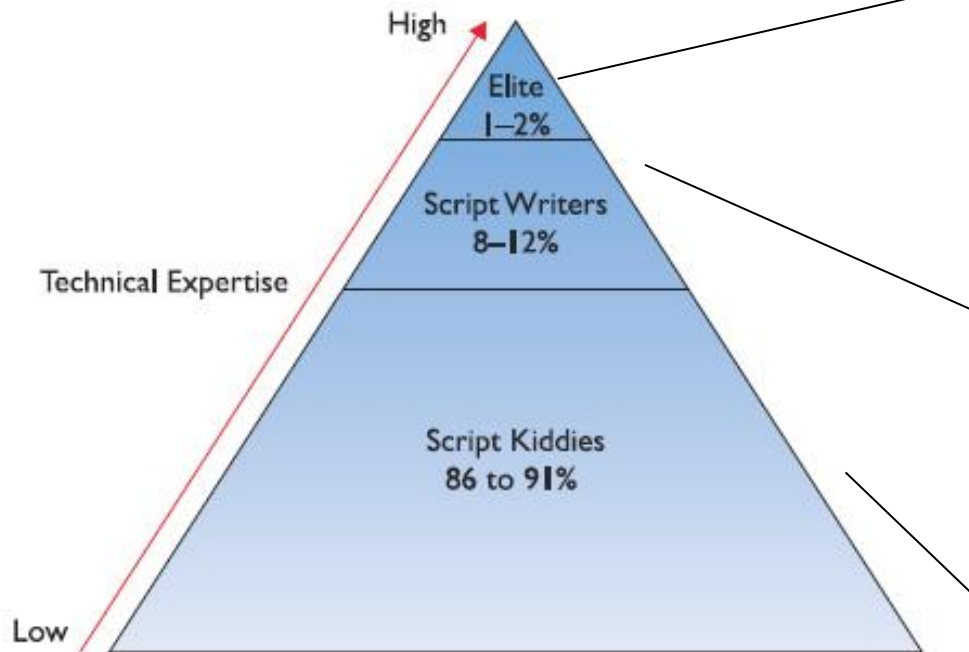
Deliberate Software Attacks

- ◆ a deliberate action aimed to violate / compromise a system's security through the use of software
- ◆ types of attacks:
 - a) Use of Malware
 - b) Password Cracking
 - c) DoS and DDoS
 - d) Spoofing
 - e) Sniffing
 - f) Man-in-the-Middle
 - g) Phishing
 - h) Pharming



Threat Events: Deliberate Software Attacks

Hacker = a person that conduct a deliberate software attack



Elite Hackers: Individuals capable of discovering new vulnerabilities and writing scripts that exploit those vulnerabilities.

Script Writers: Individuals capable of writing scripts to exploit known vulnerabilities.

Script Kiddies: Individuals with (only) enough understanding of computer systems to be able to download and run scripts that others have developed. Vast majority of attack activity on the Internet is carried out by these individuals.

• **Figure 1.1** Distribution of attacker skill levels

Threat Events: Deliberate Software Attacks

a) Use of Malware

- ◆ assumes the use of specialized software (malware) to damage or destroy information, or to deny access to the target system
- ◆ types of malware:
 - VIRUS
 - WORM
 - TROJAN HORSE
 - LOGIC BOMB
 - ROOTKIT
 - SPYWARE
 - ADWARE

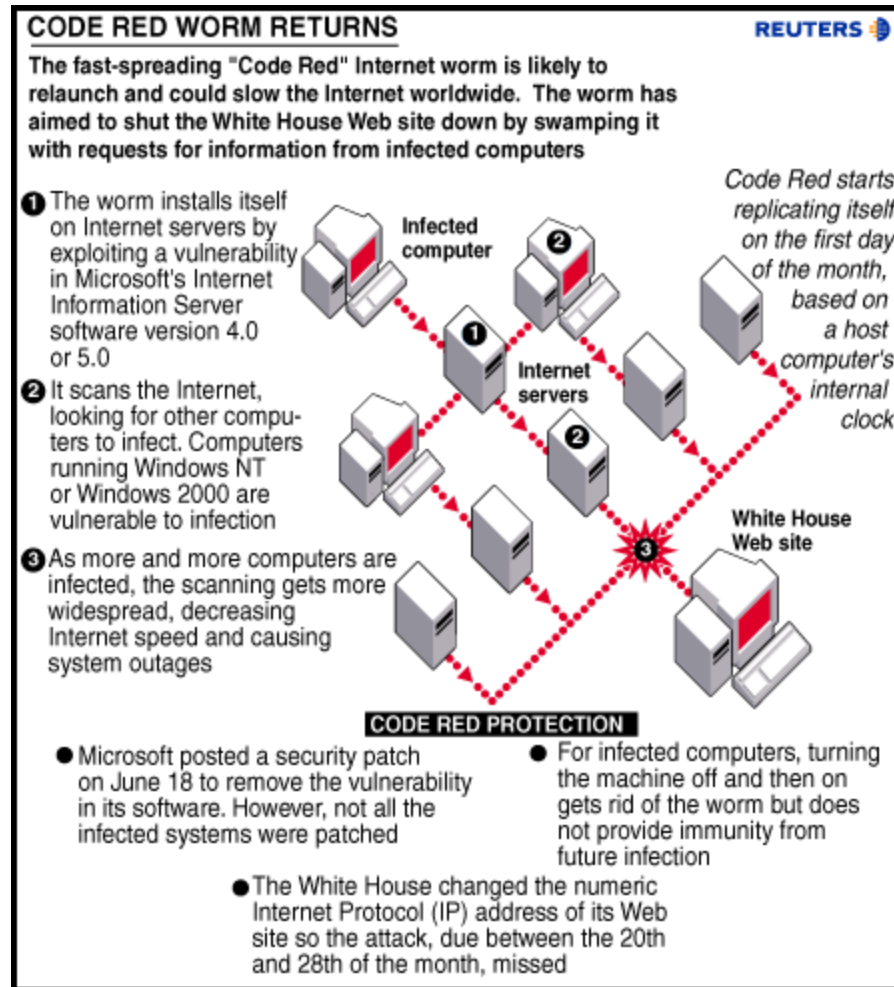
Threat Events: Deliberate Software Attacks

- **VIRUS** – malware that needs a 'carrier' to survive
 - ★ in fact, 2 carriers needed: document/program and user
 - ★ a virus secretly attaches itself to a document, and then executes its malicious payload when that document is opened and respective program launched
 - ★ most viruses rely on actions of users to spread, e.g.:
 - ◆ send/activate an infected file by email
 - ◆ download/activate an infected file from the Internet
 - ◆ download/activate an infected file from a USB drive
 - ★ viruses can cause the following damage:
 - ◆ cause a computer to crash repeatedly
 - ◆ erase files from a hard drive, reformat a hard drive
 - ◆ reduce security settings and allow intruders to remotely access the computer

Threat Events: Deliberate Software Attacks

- **WORM** – malware that uses computer networks & security-holes in applications or OSs to replicate itself
 - ★ once it exploits vulnerability on one system, worm deposits its payload and searches for another computer
 - ★ differences between viruses and worms
 - ◆ viruses need a carrier document/program (must 'attach' itself to something to propagate), are typically delivered by email, and require user action
 - ◆ worms do NOT need a carrier (can 'move' on their own), are typically spread through the Internet/Web, and do NOT rely on user action
 - ★ examples:
 - ◆ **Code Red (2001)** – each copy of the worm scanned the Internet for Windows NT / 2000 servers that did not have the Microsoft Security patch installed; once infecting a system, worm would start scanning random IP addresses at port 80 looking for other servers to infect ...

Threat Events: Deliberate Software Attacks

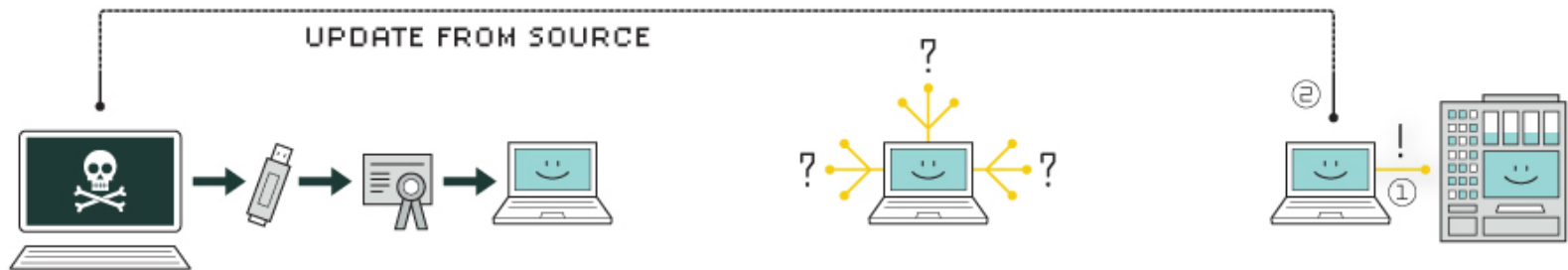


Threat Events: Deliberate Software Attacks

- ♦ **Stuxnet (2010)** – a highly sophisticated worm that used a variety of advanced techniques to spread, including:
 - by the use of shared infected USB drives (spreads even between computers that are not connected to the Internet);
 - by connecting to systems using a default database password;
 - by searching for unprotected administrative shares of systems on the LAN;
 - ...

While it was programmed to spread from system to system, it was actually searching for a very specific type of system – programmable logic controller (PLC) system made by Siemens and run on devices that control and monitor industrial processes. When it found such a system, it executed a series of actions designed to destroy centrifuges attached to the Siemens controller.

HOW STUXNET WORKED



1. infection

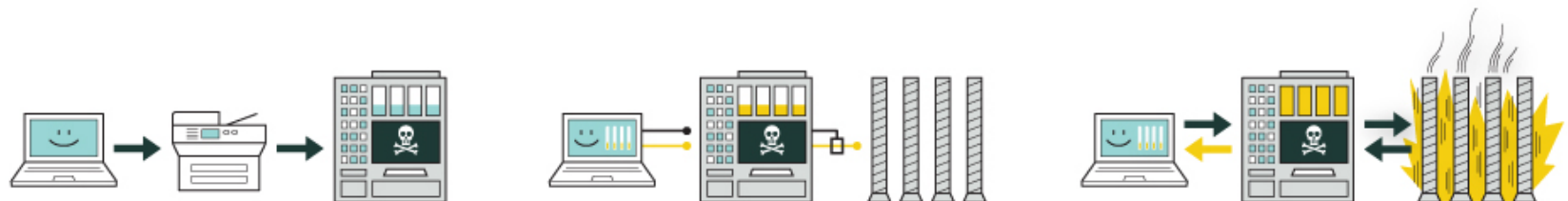
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

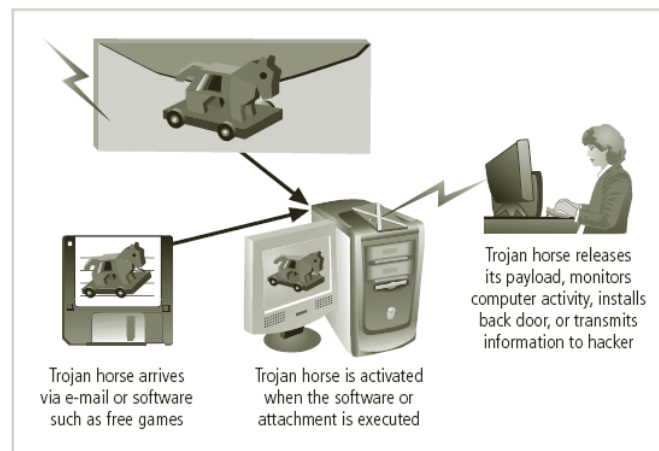
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Threat Events: Deliberate Software Attacks

- **TROJAN HORSE** – malware that looks legitimate and is advertised as performing one activity but actually does something else; it does **NOT** self-replicate
 - ★ can achieve various attacks on the host: irritate the user with pop-ups or changing desktops
 - ★ can create back doors to give malicious users access to the system – needed for DDoS!!!
 - ★ example: **AOL4Free** - advertised free access to AOL Internet Service; would delete hard drive



Threat Events: Deliberate Software Attacks

- **LOGIC BOMB** – malware typically installed by an authorized user; lies dormant until triggered by a specific logical event; once triggered it can perform any number of malicious activities
 - ★ trigger events: 1) a certain date reached on the calendar – check for organization payroll data; 2) a person was fired, etc.

Description	Reason for Attack	Results
A logic bomb was planted in a financial services computer network that caused 1,000 computers to delete critical data.	A disgruntled employee had counted on this causing the company's stock price to drop and he would earn money when the stock dropped.	The logic bomb detonated yet the employee was caught and sentenced to 8 years in prison and ordered to pay \$3.1 million in restitution.
A logic bomb at a defense contractor was designed to delete important rocket project data.	The employee's plan was to be hired as a highly paid consultant to fix the problem.	The logic bomb was discovered and disabled before it triggered. The employee was charged with computer tampering and attempted fraud and was fined \$5,000.
A logic bomb at a health services firm was set to go off on the employee's birthday.	None was given.	The employee was sentenced to 30 months in a federal prison and paid \$81,200 in restitution to the company.

Threat Events: Deliberate Software Attacks

Example: Roger Duronio story – logic bomb

In 2002, disgruntled system administrator for UBS was accused of planting a logic bomb shortly before quitting his job. The bomb had been designed to wipe out 2,000 files on the main servers for UBS, and cripple the company.

His plan was to drive down the company's stock, and eventually profit from that (*put option contract*).

During the downtime caused by the **logic bomb**, brokers could not access the UBS network or make trades. According to one employer: *"Every branch was having problems," she said. "Every single broker was complaining. They couldn't log onto their desktops and [get to] their applications because the servers were down. The brokers might have been able to make some calls to friend brokers, but my understanding was that trading was not doable."*

In 2006, Duronio was convicted and sentenced to 8 years and 1 month in prison as well as \$3.1 million restitution to UBS.

<http://www.securitypronews.com/insiderreports/insider/spn-49-20060608DuronioLogicBombTrialBegins.html>

Threat Events: Deliberate Software Attacks

- **ROOTKIT** – software tools used to break into a computer, modify the operation of the OS in some fashion in order to facilitate a nonstandard/unauthorized functions
 - ★ unlike virus, rootkit's goal is not to damage computer directly or to spread , but to hide the presence and/or control the function of other (malicious) software
 - ★ since rootkits change the OS, the only safe and foolproof way to handle a rootkit infection is to reformat the hard drive and reinstall the OS

Example: Sony story – rootkit

In 2005, Sony included a rootkit program Extended Copy Protection (XCP) on many of its music CDs in an attempt to prevent illegal copying. The software was automatically installed on Windows desktop computers (in a hidden directory) when customers tried to play the CD.

The software would allow only a limited degree of actions over the songs.

Threat Events: Deliberate Software Attacks

- **SPYWARE** – software that spies on users by gathering information without their consent, thus violating their privacy

★ example: Zango – transmits detailed information to advertisers about Web sites you visit



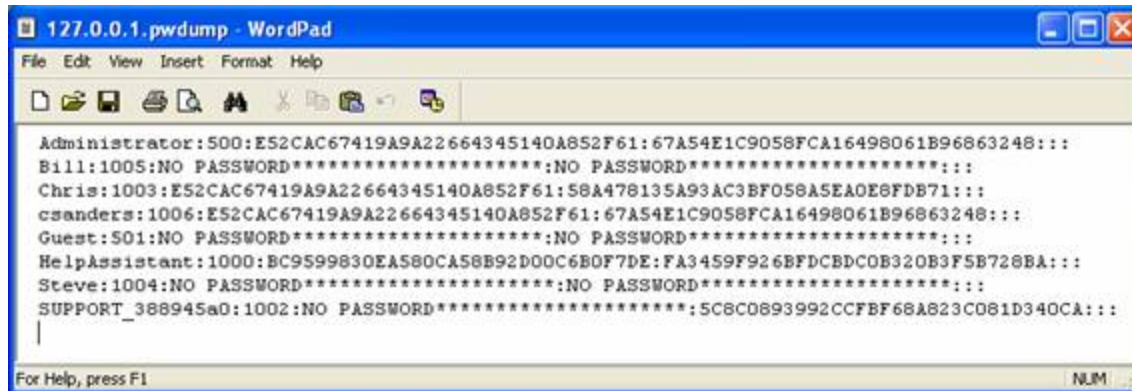
- **ADWARE** – software that delivers advertising content in a manner that is unexpected and unwanted by the user

Threat Events: Deliberate Software Attacks

b) Password Cracking

- ◆ attempt to reverse-calculate a password
- ◆ requires that a copy of Security Account Manager (SAM) - **a registry data file** - be obtained
 - **SAM file** (c:\windows\system32\config\SAM) contains the hashed representation of the user's password – **LM or NTLM hash algorithms** are used
 - **cracking procedure**: hash any random password using the same algorithm, and then compare to the SAM file's entries
 - SAM file is locked when Windows is running: cannot be opened, copied or removed (unless **pwdump** is run by the administrator)
 - off-line copy of SAM's content can be obtained (e.g.) by booting the machine on an alternate OS such as NTFS-DOS or Linux

Threat Events: Deliberate Software Attacks



```
Administrator:500:E52CAC67419A9A22664345140A852F61:67A54E1C9058FCA16498061B96863248:::
Bill:1005:NO PASSWORD:::
Chris:1003:E52CAC67419A9A22664345140A852F61:58A478135A93AC3BF058A5EAOE8FDB71:::
csanders:1006:E52CAC67419A9A22664345140A852F61:67A54E1C9058FCA16498061B96863248:::
Guest:501:NO PASSWORD:::
HelpAssistant:1000:BC9599830EA580CA58B92D00C6B0F7DE:FA3459F926BFDCBDCOB320B3F5B728BA:::
Steve:1004:NO PASSWORD:::
SUPPORT_388945a0:1002:NO PASSWORD:5C8C0893992CCFBF68A823C081D340CA:::
```

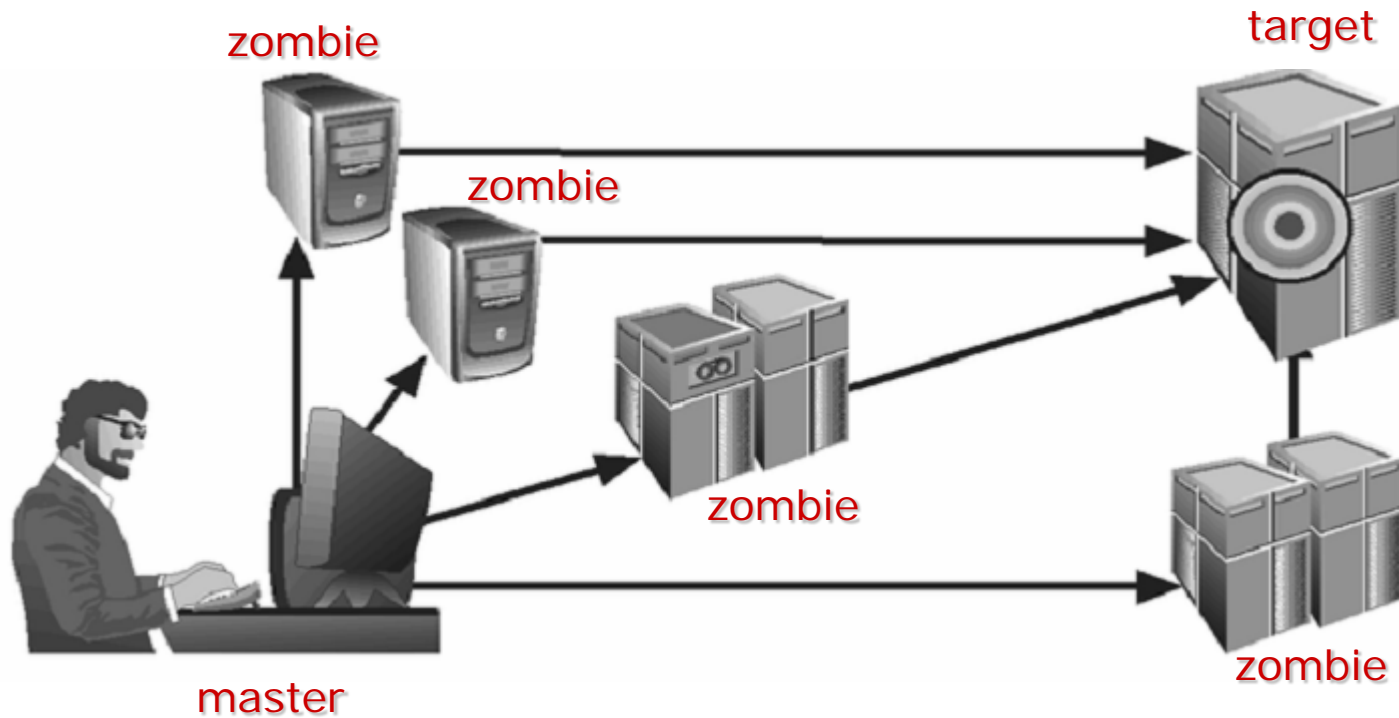
- ◆ types of password cracking attacks
 - **brute force** – every possible combination/password is tried
 - **guessing** – the attacker uses his/her knowledge of the user's personal information and tries to guess the password
 - **dictionary** – a list of commonly used passwords (the dictionary) is used

Threat Events: Deliberate Software Attacks

c) Denial of Service (DoS)

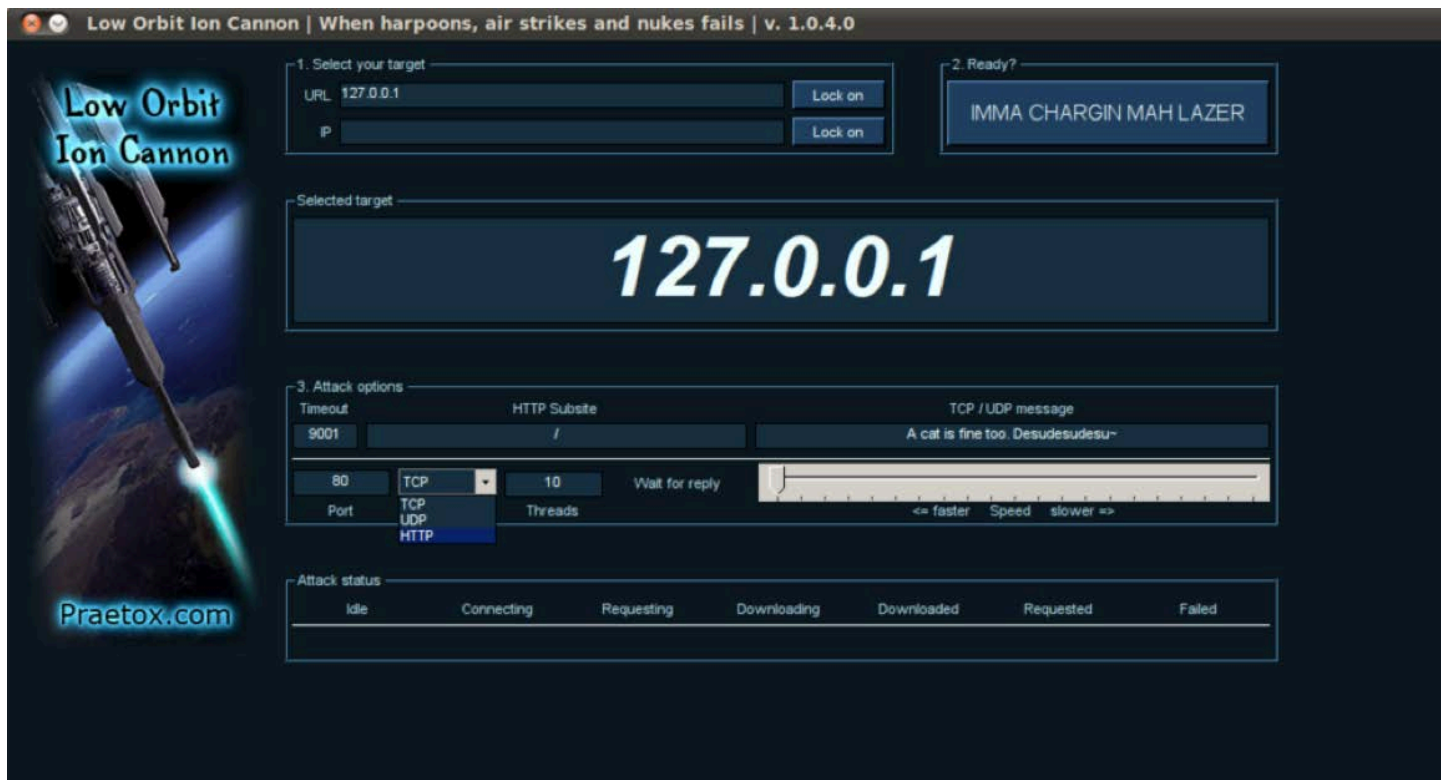
- ◆ attacker sends a large number of requests to a target
 - target gets overloaded and cannot respond to legitimate requests
- ◆ in case of **distributed DoS - DDoS**, a coordinated stream of requests is launched from many locations (zombies) at the same time
 - **zombie**: a compromised machine that can be commanded remotely by the **master** machine
- ◆ organization must ensure that 'minimum service level', as defined by Service Level Agreement (SLA) with the ISP will still satisfy its needs
- ◆ alternative solution: backup ISP

Threat Events: Deliberate Software Attacks



Threat Events: Deliberate Software Attacks

- ❖ Low Orbit Ion Cannon (LOIC)
 - open source network stress testing and DoS attack tool
 - available in Windows, Mac, Linux



Threat Events: Deliberate Software Attacks

Example: Mafiaboy story - DDoS

In 2000, a number of major firms were subjected to devastatingly effective distributed denial-of-service (DDoS) attack that blocked each of their e-commerce systems for hours at a time. Victims of this series of attacks included: CNN.com, eBay, Yahoo.com, Amazon.com, Dell.com, ZDNet, and other firms.

The Yankee Group estimated that these attacks cost \$1.2 billion in 48 hours:

- \$100 million from lost revenue

- \$100 million from the need to create tighter security

- \$1 billion in combined market capitalization loss.

At first, the attack was thought to be the work of an elite hacker, but it turned to be orchestrated by a 15-year-old hacker in Canada.

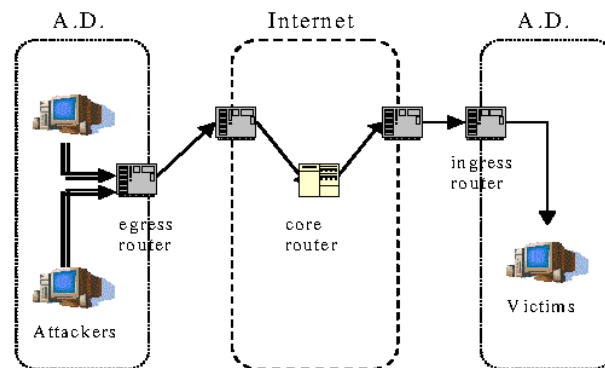
He was sentenced to eight months detention plus one year probation and \$250 fine.

http://journal.fibreculture.org/issue9/issue9_genosko.html

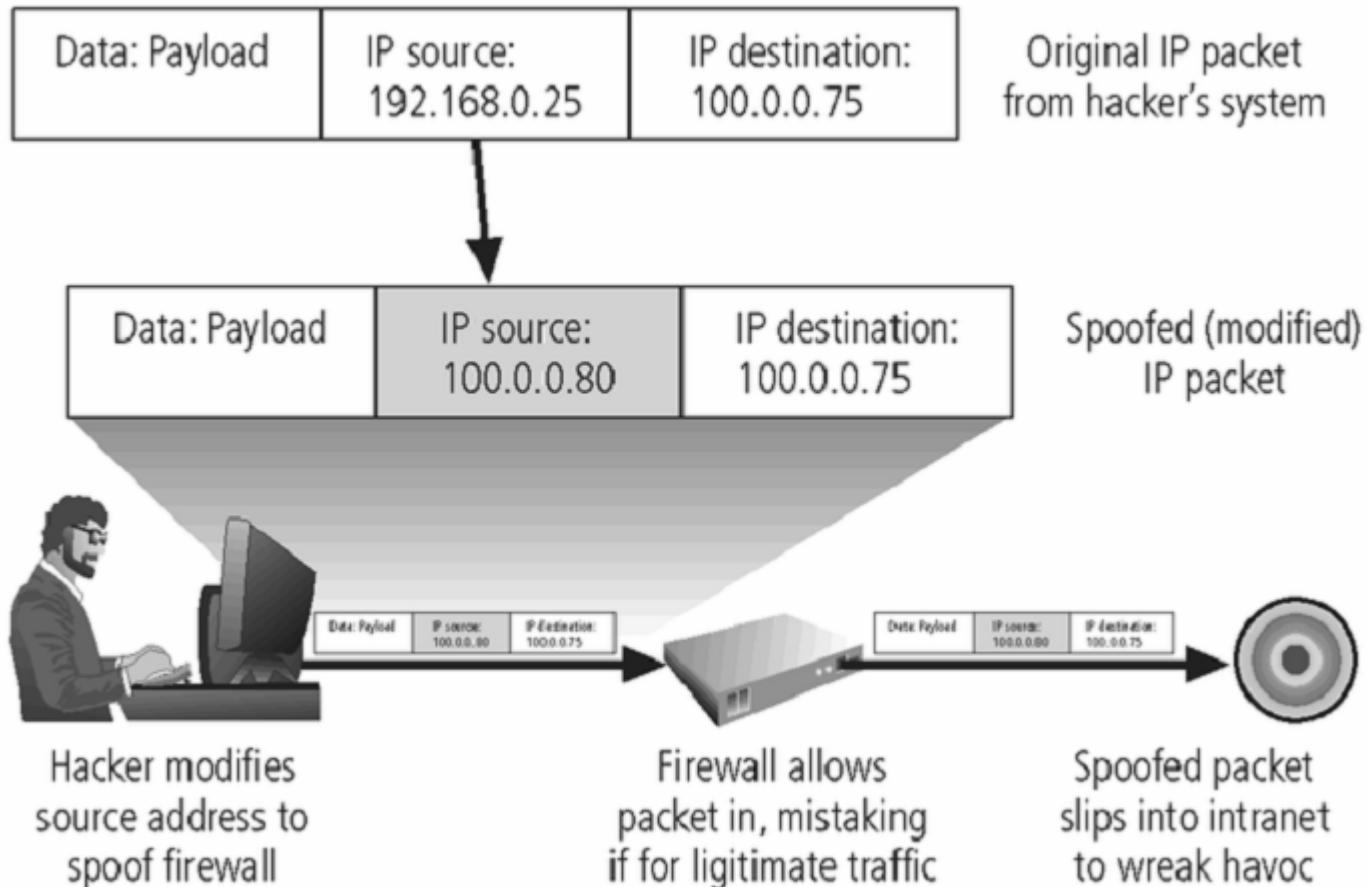
Threat Events: Deliberate Software Attacks

d) Spoofing

- ❖ insertion of forged (but trusted) IP addresses into IP packets in order to gain access to networks/computers
- ❖ new routers and firewalls can offer protection against IP spoofing
 - ingress filtering – upstream ISP discards any packet coming into a network if the source address is not valid, i.e. IP does not belong to any of the networks connected to the ISP
 - egress filtering – organization's firewall discards any outgoing packet with a source addr. that does not belong to that organization



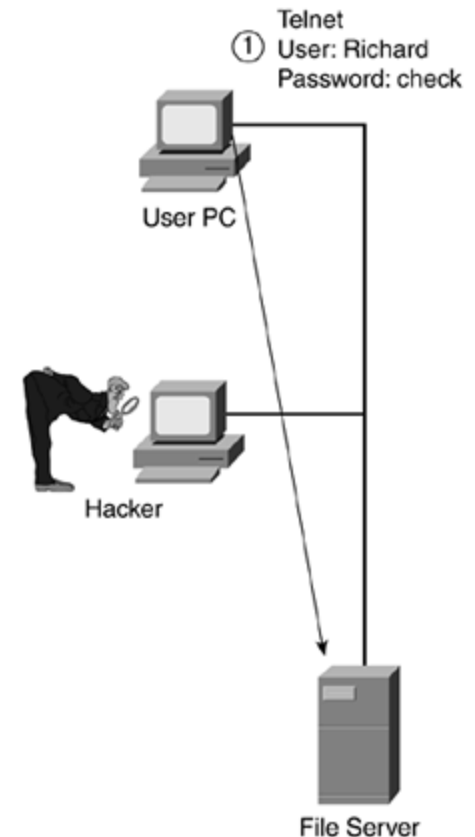
Threat Events: Deliberate Software Attacks



Threat Events: Deliberate Software Attacks

e) Sniffing

- ◆ use of a program or device that can monitor data traveling over a network
 - unauthorized sniffers can be very dangerous – they cannot be detected, yet they can sniff/extract critical information from the packets traveling over the network
 - wireless sniffing is particularly simple, due to the 'open' nature of the wireless medium



Threat Events: Deliberate Software Attacks

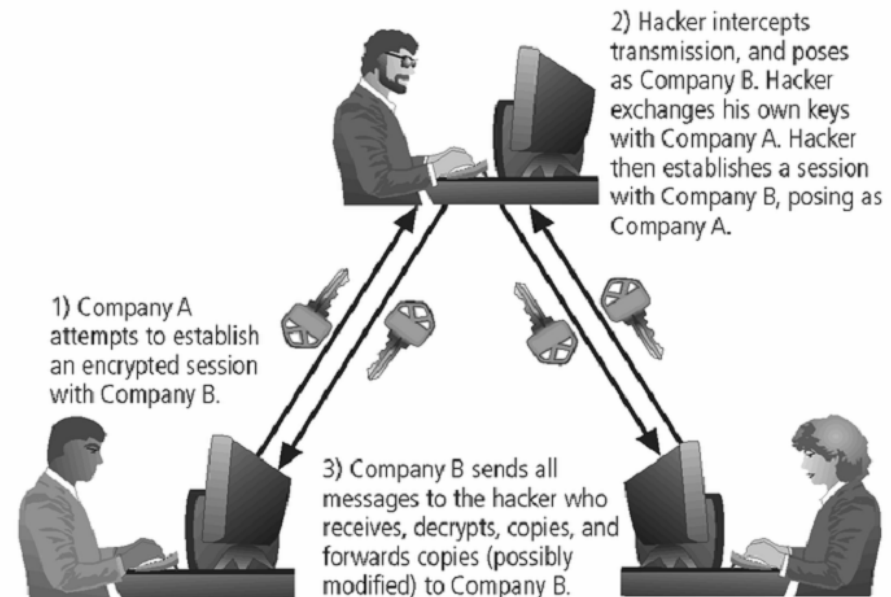
f) Man-in-the-Middle Attacks

- ◆ gives an illusion that two computers are communicating with each other, when actually they are sending and receiving data with a computer between them

- spoofing and/or sniffing can be involved

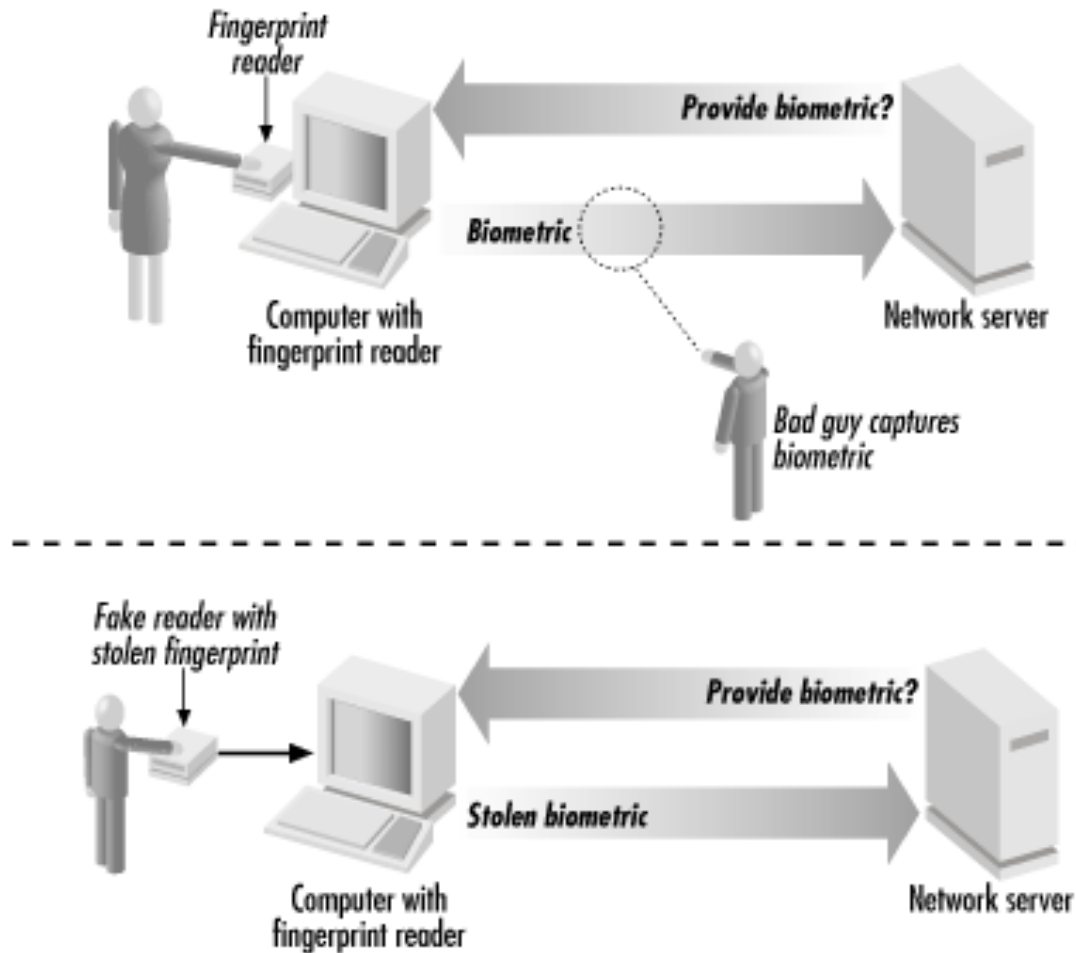
- ◆ examples:

- passive – attacker records, alters and resends data at a later time
- active – attacker intercepts, alters and sends data before the original arrives to the recipient



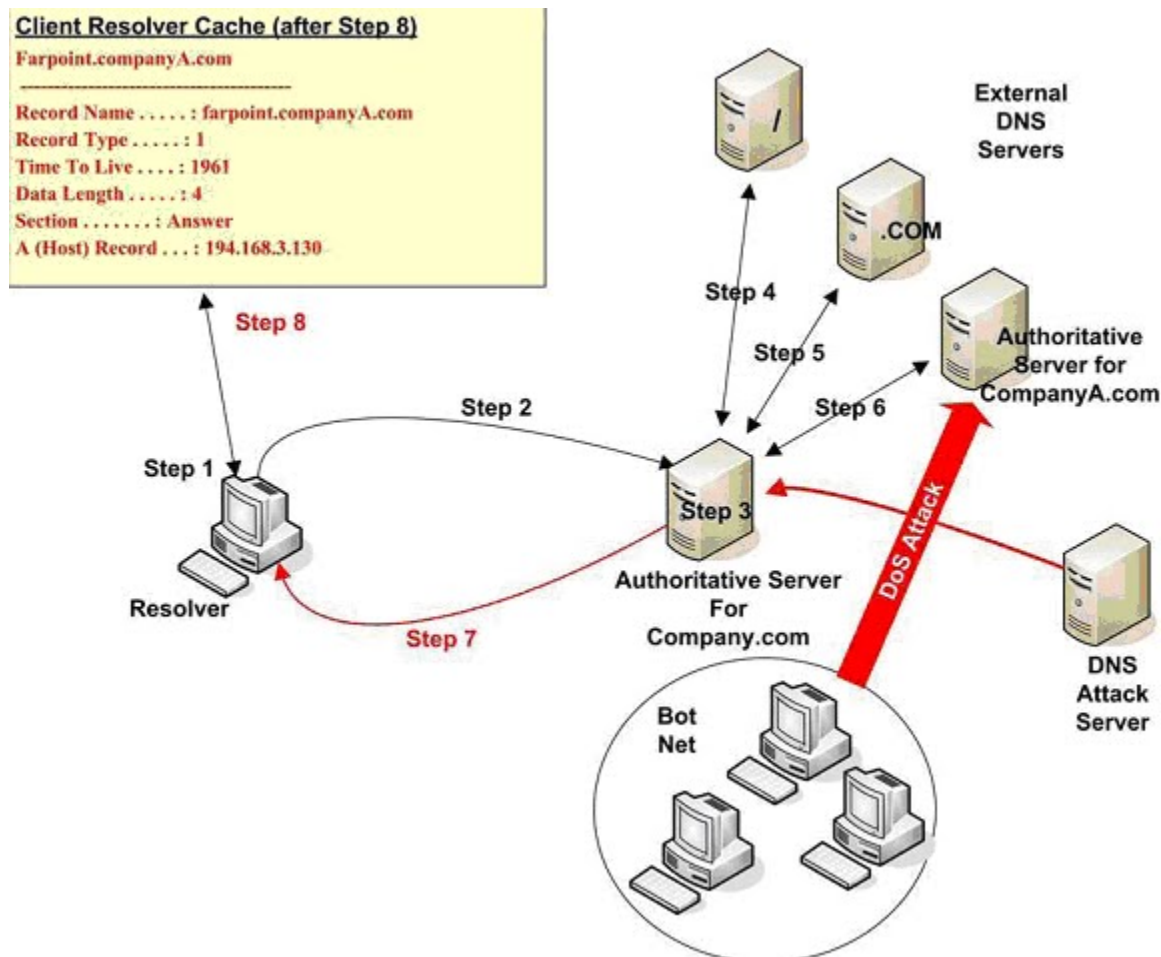
Threat Events: Deliberate Software Attacks

Example: **Replay** (passive Man-in-the-Middle attack)



Threat Events: Deliberate Software Attacks

Example: **DNS Poisoning** (active Man-in-the-Middle attack)



Threat Events: Deliberate Software Attacks

Social Engineering

- ◆ process of using social skills to manipulate people into revealing vulnerable information
 - example: **phishing** and **pharming**

g) Phishing

- ◆ attempt to gain sensitive personal information by posing as a legitimate entity
 - **SIMPLE PHISHING**: an email is sent to the victim informing them of a problem (e.g. with their email or banking account) and asking them to provide their username, password, etc.;

'From' email address is spoofed to look legitimate, 'Reply To' email address is an account controlled by the attacker

Threat Events: Deliberate Software Attacks

- **SOPHISTICATED PHISHING**: an email is sent to the victim containing a link to a bogus website that looks legitimate



Example: Phishing using URL Links Embedded in HTML-based Emails

<http://1example.link.com>

http://53d8b.malicious_phishing_site.com/index.php

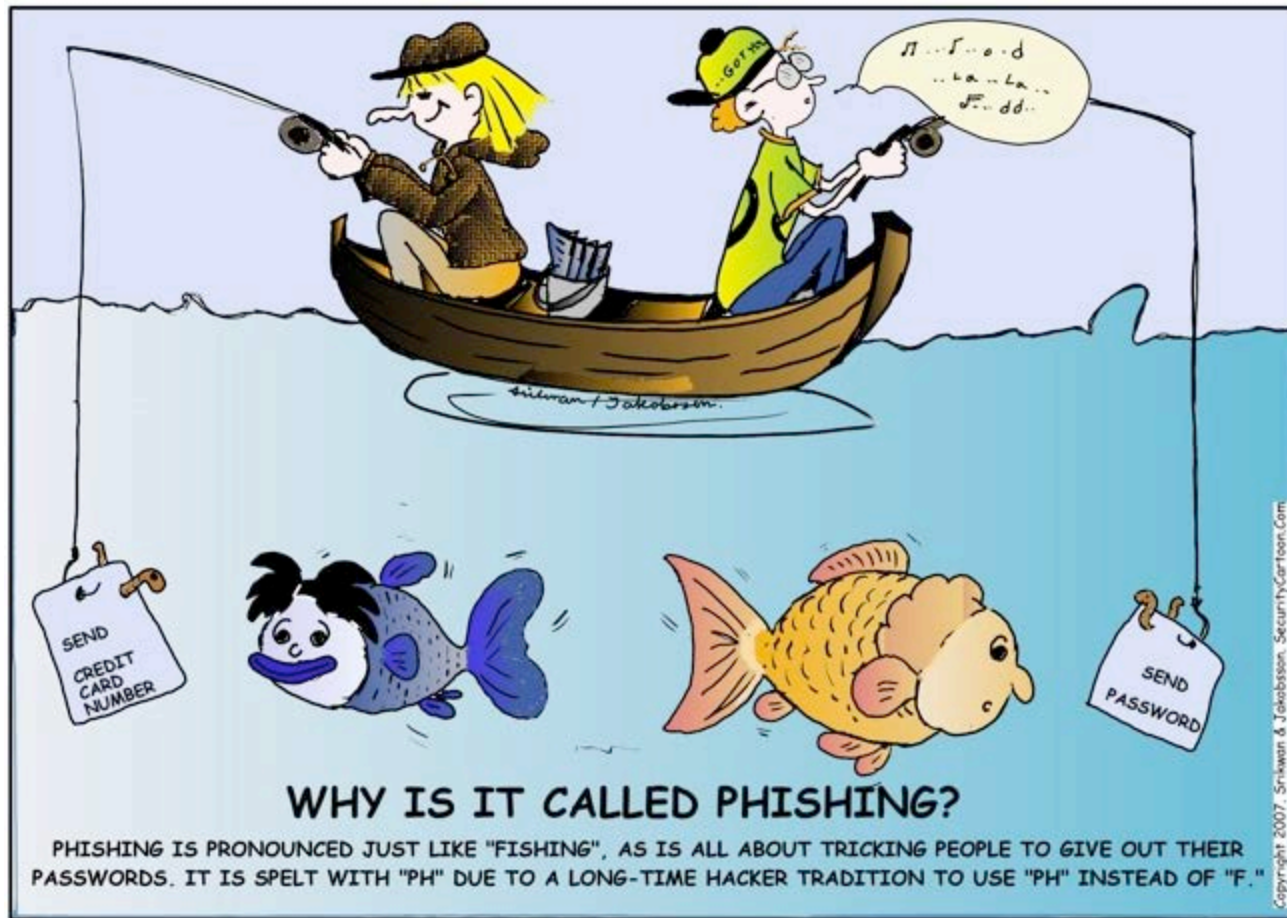
Threat Events: Deliberate Software Attacks

Example: Phishing using URL Links Embedded in HTML-based Emails

The image displays a phishing attack example. On the left, a screenshot of a web browser shows an email from 'online@regions.com' with the subject 'You have 1 new ALERT message'. The email body contains a message from Michael Whitman, dated Friday, January 26, 2007, at 6:53 PM. The message states: 'You have 1 new ALERT message. Please login to your **RegionsNet Online Ban** and visit the **Message Center** section in order to message. To Login, please click the link below: [Go To RegionsNet Online](#)'. Below the link, it says '© 2007 Regions Bank. All rights reserved'.

On the right, a screenshot of the 'RegionsNET - Online Banking - Mozilla Firefox' browser window shows the 'RegionsNET ONLINE BANKING' login page. The URL in the address bar is 'http://alienhub.kg.net.pl/regions/regionsnet/EB/login/index.htm'. The page features the 'RegionsNET' logo and the tagline 'Bank Anytime. Anywhere.'. Below the header, there is a 'Secure Login' section with a login form. The form includes fields for 'Login ID:' and 'Password:', an 'Access Accounts' button, and a 'Password Rules' section stating: 'Must be 8-16 characters and include both numbers and letters (at least one of each). Passwords are case sensitive.' There are also 'Tips' listed: 'If you cannot login or get a disabled message, call 800-395-1856 Monday through Friday 7 a.m. to 7 p.m. CT and 7 a.m. through 2 p.m. CT on Saturday.' and 'Do not use your browser's back button while logged into RegionsNet.' At the bottom of the login section, there are buttons for 'Personal Banking Demo' and 'Enroll in RegionsNet'. A 'Disclaimer' section at the bottom states: 'Sign On Policy: This is a protected data system with monitoring and active security. If you do not consent to monitoring, or do not have a valid account, please exit the system now.' Below the disclaimer, there are links for 'Copyright Information', 'Privacy Pledge', 'Member FDIC', and 'Equal Housing Lender'.

Threat Events: Deliberate Software Attacks



<http://www.informacija.rs/Clanci/Phishing-Obmanjivanje-korisnika.html>

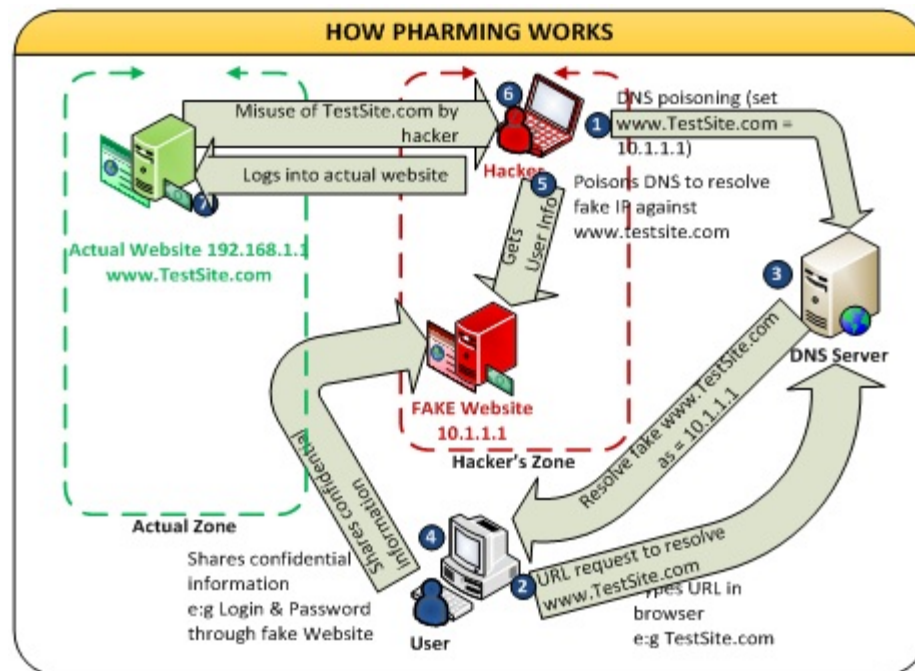
Threat Events: Deliberate Software Attacks



Threat Events: Deliberate Software Attacks

i) Pharming

- ❖ phishing is accomplished by getting users to type in or click on a bogus URL
- ❖ pharming redirects users to false website without them even knowing it – typed in or clicked on URL looks OK



- performed through **DNS poisoning** – user's local DNS Cache or DNS server are 'poisoned' by a virus

Threat Events: Deliberate Software Attacks

Example: Elaborate Pharming Attack on 65 Banks in February 2007

Storyline:

1. Targeted victims, from US and Australia, were lured to a bogus website appearing to be a link to a news story from *The Australian*.
2. When the victim arrived at the website, if the victim's Windows OS wasn't patched, a malware was automatically downloaded into their computer.
3. When a user then went to visit any one of the 65 targeted banks (PayPal, eBay, Discover Card, American Express, Bank of Scotland, ...) their computer was redirected to a false website, even though they typed in the correct URL for the bank.
4. The user then entered in their identity information through the false website which then logged in as the user on the real website.
5. The user then was able to do their banking. However, the criminals were now logged on as the user and could withdraw funds after the user thought they had logged off.