System & Network Security Introduction

Incidents

I will go over only some of these, but leave the rest for you to read.

April 1998

"*Masters of Downloading/2016216*" broke into key computer in Dept. of Defense

Hackers claimed that the information that they acquired would be of interest to international terrorists.

DoD’s public comments

- *Acknowledged that there had been an intrusion*
- *Never commented on hacker’s claim*

January 2000*

Over the Internet hackers broke into files of *CD Universe*

- *Stole over 25,000 of credit card numbers with associated names*
- *Tried to blackmail company by threatening to publish the numbers*
  - Sort of dumb; should have used the numbers and bought stuff
- *Company refused, and some of the names & numbers were published*
- *Thousands of credit card numbers had to be changed*
- *CD Universe sales dramatically decreased because customers lost confidence in company*
- *Tracked through multiple foreign sites*

February 2000

Yahoo, Amazon, E*Trade, Buy.com, CNN, eBay were denied service by DDoS *(Distributed Denial of Service)* attacks

Targeted web sites were overloaded with traffic

Traffic was generated from many other machines that had been broken into earlier

Estimated explicit cost: several million $ in revenue

Incalculable implicit costs

July 2001: Code Red

Code Red worm infected > 250,000 Windows hosts in less than 9 hours

Too short a time for security and system administers to respond

Used infected hosts to launch DDoS attacks

Initially attacked the White House web server with DDoS attack

Machines of U.S. Government, ATT, Microsoft, FedEx, and others were affected for several weeks

Some of the Code Red worm variants had installed remote control back doors for later attacks

Code Red (continued)

The vulnerability that allowed the infection was identified in June 2001 and Microsoft quickly issued a patch

A month before the DDoS attack

But few installed the patch

Cost of recovering has been estimated at several billion dollars

Some DDoS victims considering suing owners of infected hosts

Negligence because known vulnerability was not fixed

September 2001: Nimda

Infected > 100,000 hosts in 8 hours

Security administrators and sysadmins didn't have time to do much

Nimda attacked both clients and servers of all Windows OSs

The worm had several infection vectors (i.e., mechanisms)

Cost of recovering has been estimated at 1.5 billion dollars

January 2003: SQL Worm

January 24 & 25, 2003

Exploits two of three vulnerabilities in the Resolution Service of Microsoft’s SQL Server 2000

Self-propagating worm

Caused

- *Internet degradation worldwide*
- *Compromised vulnerable hosts*

2011: Stuxnet

Targeted Siemens *WinCC* industrial control software running on Windows OSs

First known malware that

- *Spied on and harms industrial systems*
- *Had a PLA rootkit*

Exploited several vulnerabilities

- *Windows shortcut icon*
- *Special RPC that causes a buffer overflow*
- *Others*

Can be remotely controlled by a browser

2012: Flame

Flame, sKyWIper

Attacks Windows OS

Spread via LANs or USB sticks

Can record ksystrokes, screen, network activity, skype…

Most of attacks in Near East including Iran

Remotely controlled by a number of computers in Europe and North America

Some attacks in U.S. and Canada

Can remove all traces of itself

2012: Flame

Scatters malicious code into multiple Windows DLLs

Evades detection

- *Via rootkits*
- *Detects AV software that is running and configures itself to minimize detection by that AV software*

After initial infection, remote access is opened

- *Used to download additional modules*
- *Used to upload collected data*

May have been developed by CIA or NSA as part of effort to determine state of Iranian nuclear activity

SQL Worm
Vulnerability Details

Vulnerability 1

- *Buffer overflow that allowed insertion and execution of arbitrary code on SQL server*
  - Allowed worm to be inserted in SQL servers

Vulnerability 2

- *While different than vulnerability 1, it also allowed insertion and execution of arbitrary code*

Vulnerability 3

- *Keep-alive function in SQL server allowed*
  - DDoS attacks against other hosts
  - Congestion on the Internet

SQL Worm
Network Traffic Details

Large amount of traffic

UDP port 1434

Small datagrams: 376-410 bytes

Source IP addresses spoofed

IP addresses seemed random

Note

Some of the above details could have been used to filter datagrams at firewalls

SQL Worm
Fixes

Vulnerabilities were known for over 6 months prior to attack

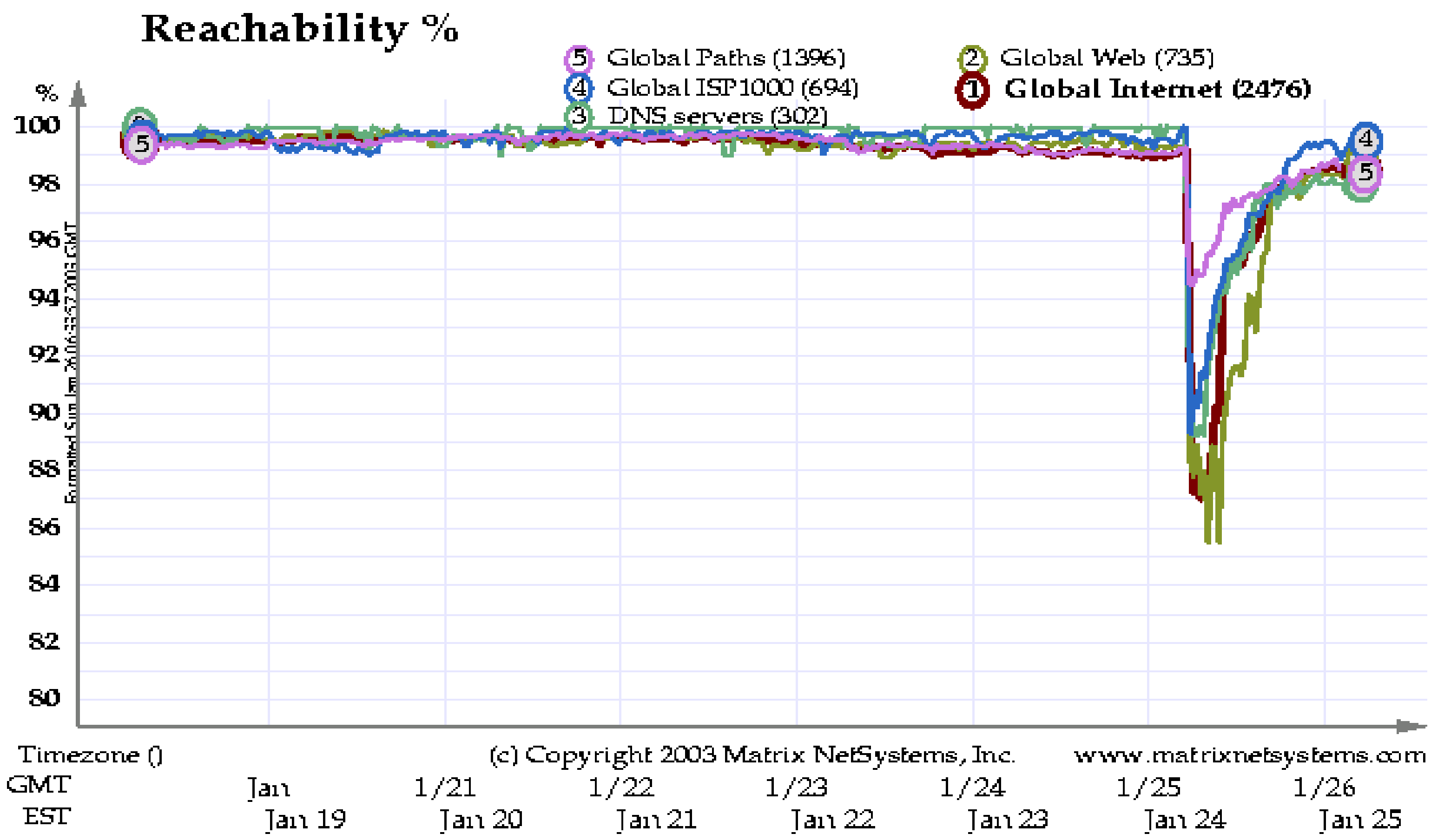
Microsoft issued patches about 5 months before attack

Worldwide, many patches were never installed

- *Various IIT organizations ran Microsoft SQL Servers*
- *Apparently most did not have the patches installed*
- *e.g., IIT On-Line had 3 or 4 SQL Servers running at the Rice campus.*
  - Apparently none were patched
- *Even Microsoft did not patch all of its SQL servers*

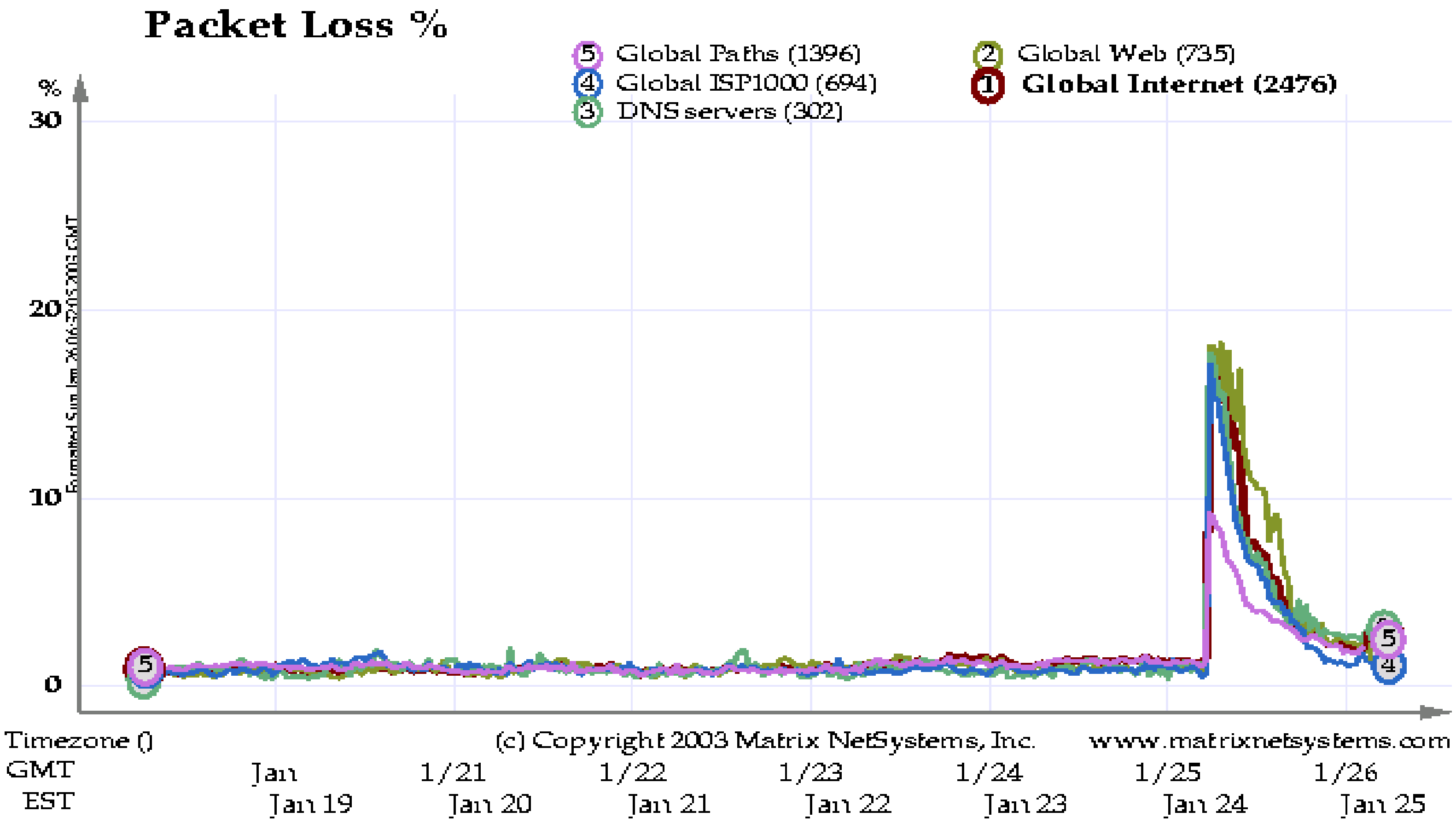
SQL Worm

% Reachability Over 6 Days



SQL Worm

% Packet Loss Over 6 Days



August 2003: W32 Blaster Worm

All Windows NT, 2000, and XP operating systems were vulnerable

DDoS Worm

Exploited a vulnerability in the operating systems' DCOM RPC interface

W32 Blaster Worm

Operation

Worm enters via DCOM RPC

Once in the OS, the worm retrieves a copy of the file `msblast.exe` from the compromising host

`msblast.exe` then uses the compromised system to scan for other vulnerable systems to compromise in the same manner

- *Uses TCP session on port 135 with involvement of ports 139 & 445*
- *Names used other than* `mblast.exe`
  - `teekids.exe` and `penis32.exe`
- *Even after patches Win2K OSs were still somewhat vulnerable via their DCOM RPC*

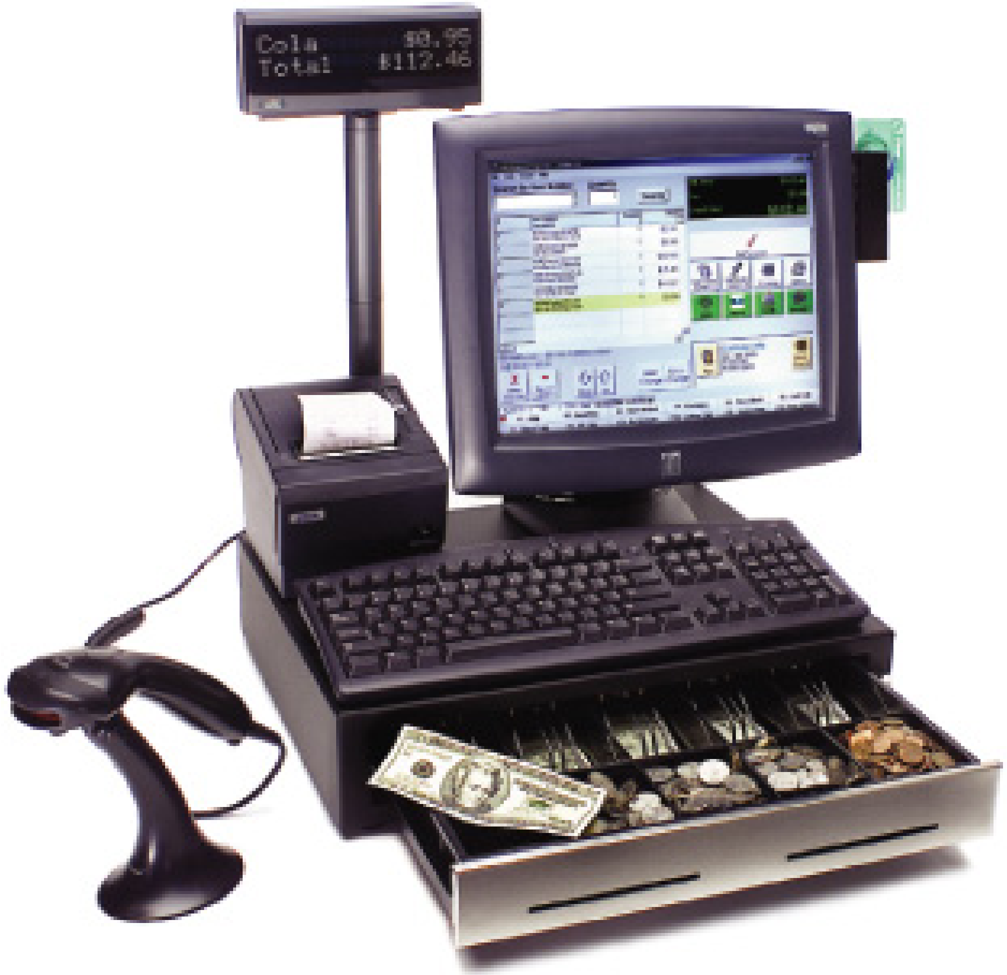
W32 Blaster Worm
A Clever Twist

Launched a SYN flood attack targeting *windowsupdate.com*

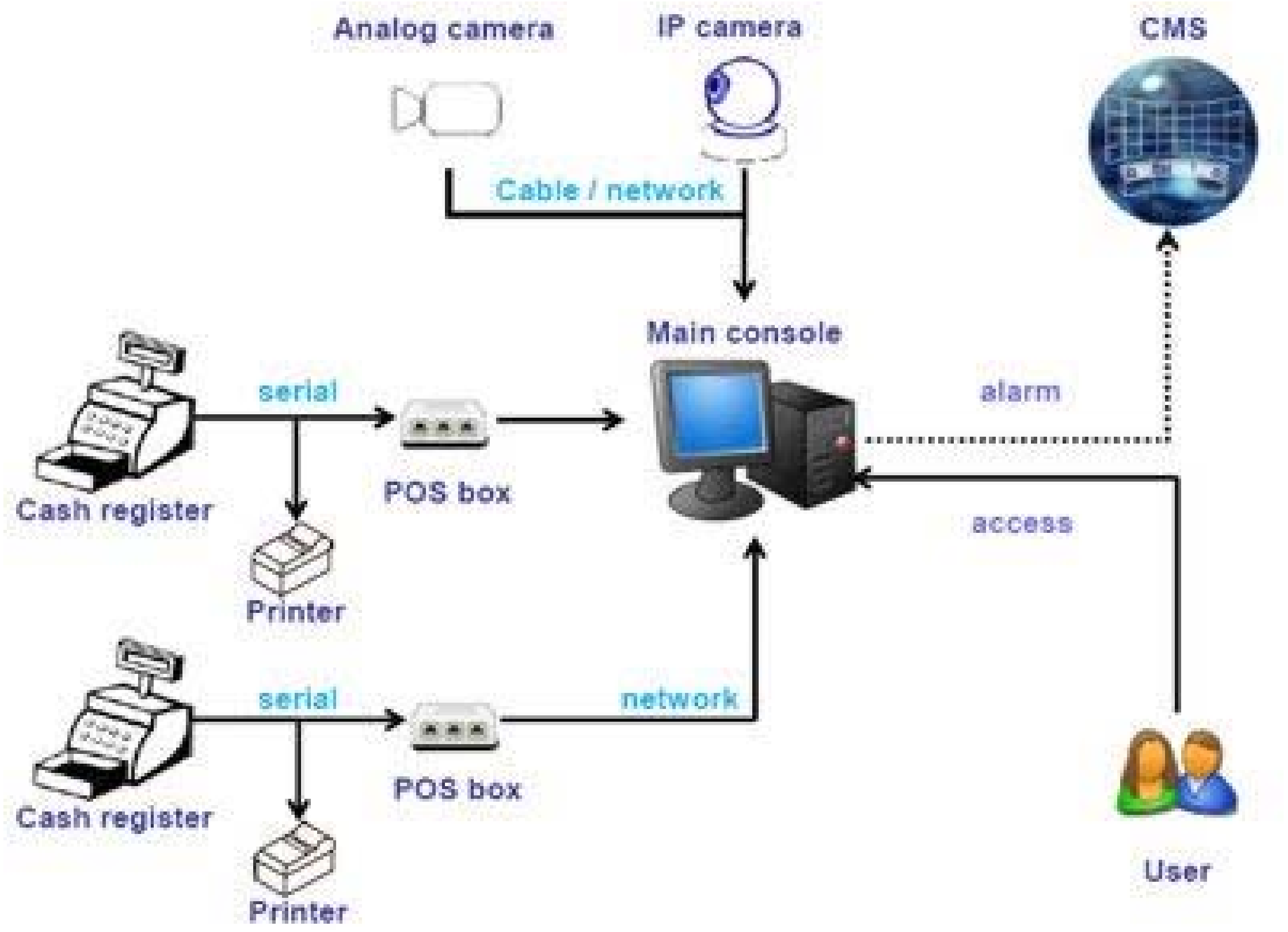
The Microsoft patch to fix the vulnerability was retrieved through this web site

Thus the DDoS attack on *windowsupdate.com* prevented computers from downloading the corrective patch

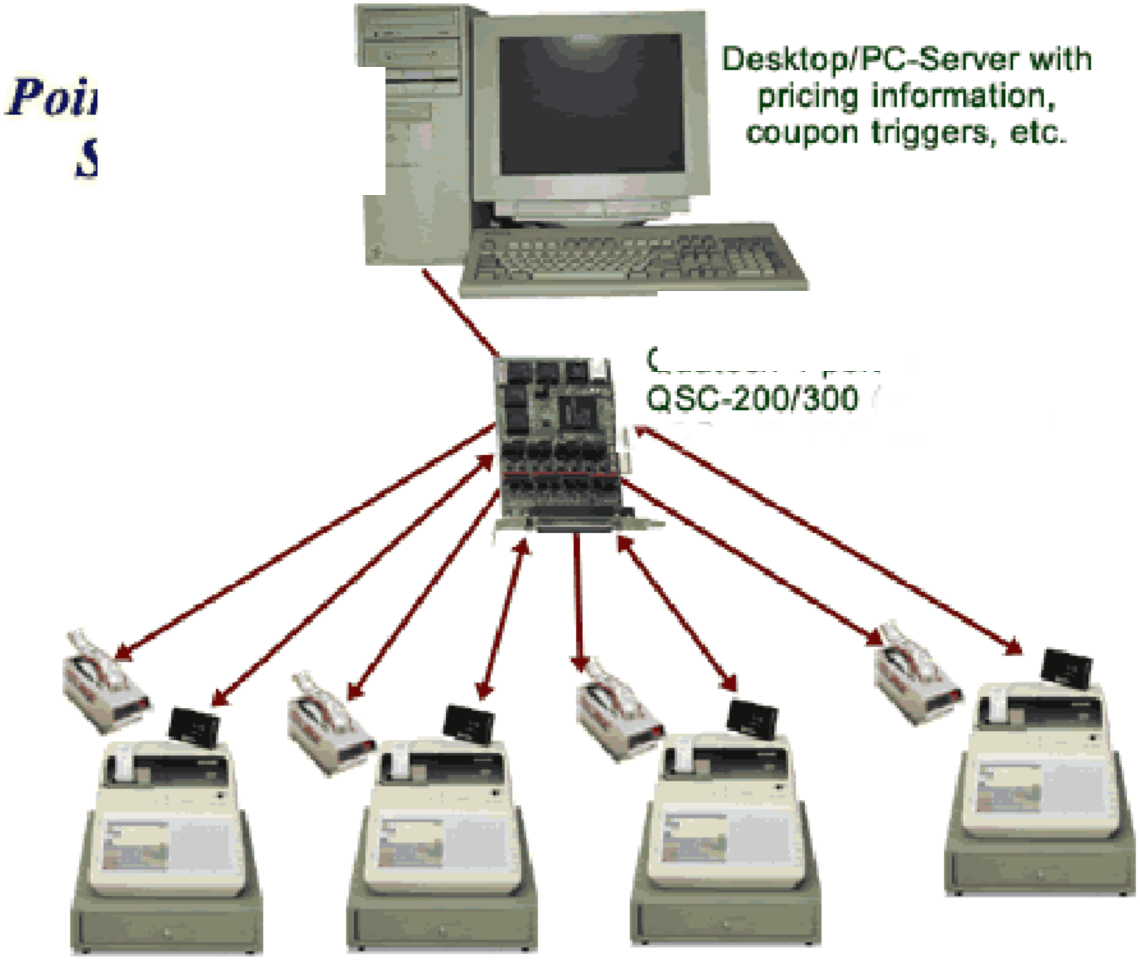
Point of Sale (PoS) Terminal



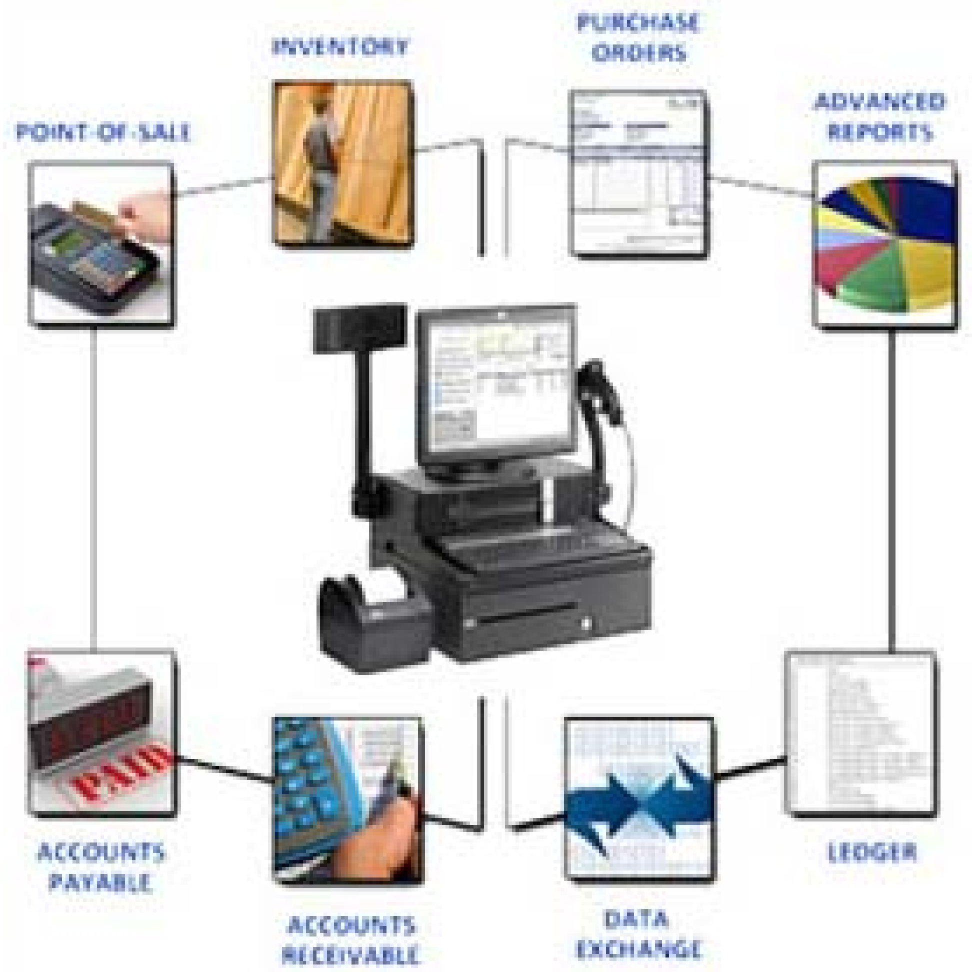
Point of Sale (PoS) System



Point of Sale (PoS) System


Poi
S
Desktop/PC-Server with pricing information, coupon triggers, etc.
QSC-200/300

Point of Sale (PoS) System



Mag. Stripe Payment Cards

The magnetic stripe on the back of your payment card contains 3 lines (called "Tracks") of information

Track 1: CardNumber, Name, ExpirationDate, Optional, CRC

Track 2: CardNumber, ExpirationDate, Optional, CRC

Track 3: Effectively not used

This is enough information to duplicate a payment card

Target

Target stores had data systems that were largely autonomous

- *A processor center in each store managed multiple PoS terminals, inventory, store databases, pharmacy…*

Two servers were in processor center at each store

- *Multiple virtual machines, mostly Windows based*
- *VMs ran applications that separately support the different functions*
- *Actually pharmacy applications ran on a Linux VM*

But payment card authentication, PoS monitoring and updating were done in Target Corp. central system

Target

Updates were done when the stores are closed

- *Updates were transferred to each store's processor center from Target Corp's central system*
  - VMs were updated
- *VMs then updated peripheral devices such a PoS terminals*

Target Breach

Holiday season, 2013 *(late Nov – mid Dec)*

40 million payment card records were stolen from customers who made in-store purchases

Information on 70 million "guests" were also stolen

> *Guest: Anyone who shared some personal info with Target*

How it Was Done

Target Corp’s central servers were likely hacked

Malware was sent to the store’s processor center, which forwarded it to the PoS terminals

Malware was RAM Scraping *malware*

But payment card information was encrypted

Except that it can’t be encrypted all the time

It must be briefly decrypted to plaintext to be able to read it

Done in RAM memory

How it Was Done

RAM Scraping malware in the PoS terminals watched for decryption of card info as plaintext in RAM

When it existed as plaintext in RAM, it was copied into the *RAM Scraper* database

Periodically the database was sent to an external server

Chip & PIN Payment Cards

A Chip & PIN payment card:

- ***No*** *magnetic strip that is read*
- *An integrated circuit (chip) that contains all the needed information, strongly encrypted*
- *A PIN, strongly encrypted*

The PoS reads the info from the chip and does pretty much the same thing that is done for mag. strip cards

CREDIT CARD
4215 3156 0372 5493
4524
VALID THRU
01/19
FIRSTNAME LASTNAME

Chip & PIN Payment Cards

But the user must manually enter the PIN

The PIN is immediately encrypted the same as the encrypted PIN from the card

Both encrypted PINs are sent to the verification server

If

The encrypted values of the two PINs agree and

The other info is OK,

Then the transaction is approved

Notice that the encrypted PIN from the card is <u>never</u> decrypted.

Chip & PIN Payment Cards

Will chip & PIN cards “solve” PoS breaches such as Target’s?

Incident Summary

These examples are all too typical

Representative of the many incidents that occur

We’ll revisit some of these incidents later and in more detail

But before we move on, lets try to make some general observations

Some General Observations*

(Intentionally left blank. Fill in the observations made by the class.)

Challenges for Security

Challenges for Cyber Security

Computer security not simple

Must secure the users, content and system

Potential attacks on the security features must be considered

Procedures used to provide particular services are often counterintuitive

Attackers only need to find a single weakness, the developer needs to find all weaknesses

Users and system managers tend to not see the benefits of security until a failure occurs

Security requires regular and constant monitoring

Security is often an afterthought to be incorporated into a system after the design is complete

Gets in the way of using systems

Challenges for Cyber Security

Challenge of keeping networks and computers both secure and operational has never been greater

A number of trends illustrate why security is becoming increasingly difficult

Many trends have resulted in security attacks growing at an alarming rate

Some Useful Web Sources

Internet Storm Center

- *Updated information on attacks and trends*
- *http://isc.sans.org/*

milw0rm

- *List of exploits sorted in various ways*
  - Vulnerable platforms, local (e.g., privilege escalation) or remote…
- *Some shellcode*
- *www.milw0rm.com*

Some Useful Web Sources

CERT (Computer Emergency Readiness Team)

- *Software Engineering Institute @ Carnegie Mellon Univ.*
- *Much information on attacks*
- *http://www.cert.org   http://www.cert.org/advisories/*
- *Advisories moved to US-CERT in 2005, but they still exist at CERT*

US-CERT

- *U.S. Dept of Homeland Security*
- *http://www.us-cert.gov*
- *http://www.us-cert.gov/cas/techalerts/*

Some Useful Web Sources

Mitre *(http://www.cve.mitre.org)*

- *Classifies vulnerabilities and exploits, giving each a CVE-ID (CVE Identifiers)*
  - CVE: Common Vulnerabilities & Exposures
- *Links to many other security sites*

Hackerstorm *(http://www.hackerstorm.com)*

- *Has the OSVDB (Open Source Vulnerability Tool)*
- *View and lookup vulnerabilities for thousands of vendors offline*

Some Useful Web Sources

Many other very useful free web sites

But be careful

- *Many offer software tools to download and use*
- *Some of these sites have malicious intent, clothed in a patina of respectability*
- *You may get infected if you use their software tools*

Protect Yourself

If you use a tool from a web site of which your are uncertain:

- *Scan the tool in question with 2 or 3 truly different AV softwares*
- *Run the tool in a controlled environment from which you can recover*
- *Monitor the tool's activities*
  - Network sniffer (e.g., tcpdump) to look for strange network traffic
  - Check on changes to Registry and specific files
    - *MS Sysinternals tools* filemon *and* regmon -- *they detect changes*
    - *Tripwire*

Some Exploit Trends

2012 Exploit Trends

Exploit vulnerabilities are moving from OSs and systems to applications

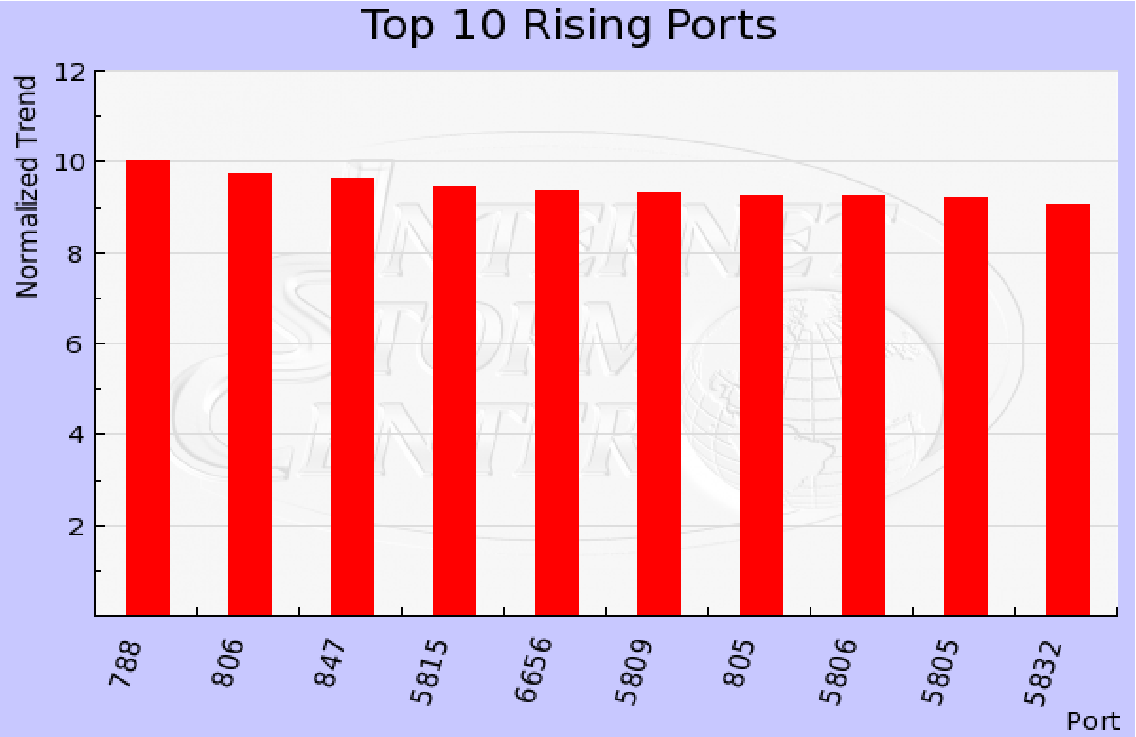
The applications targeted most tend to change over time because of

- *Application popularity*
- *Inability to effectively patch an application*
- *Emergence of new malware*

Browsers and browser-invoked client-side applications are being targeted because

- *Trusted web servers are being compromised*

Ports for Which Attacks Seem to be Rising - July 2013



The “ Normalized Trend" is an attempt to assign a number to the increase in activity for a given port

Trend = sqrt[$(S-s)^2/s + (T-t)^2/t$)]

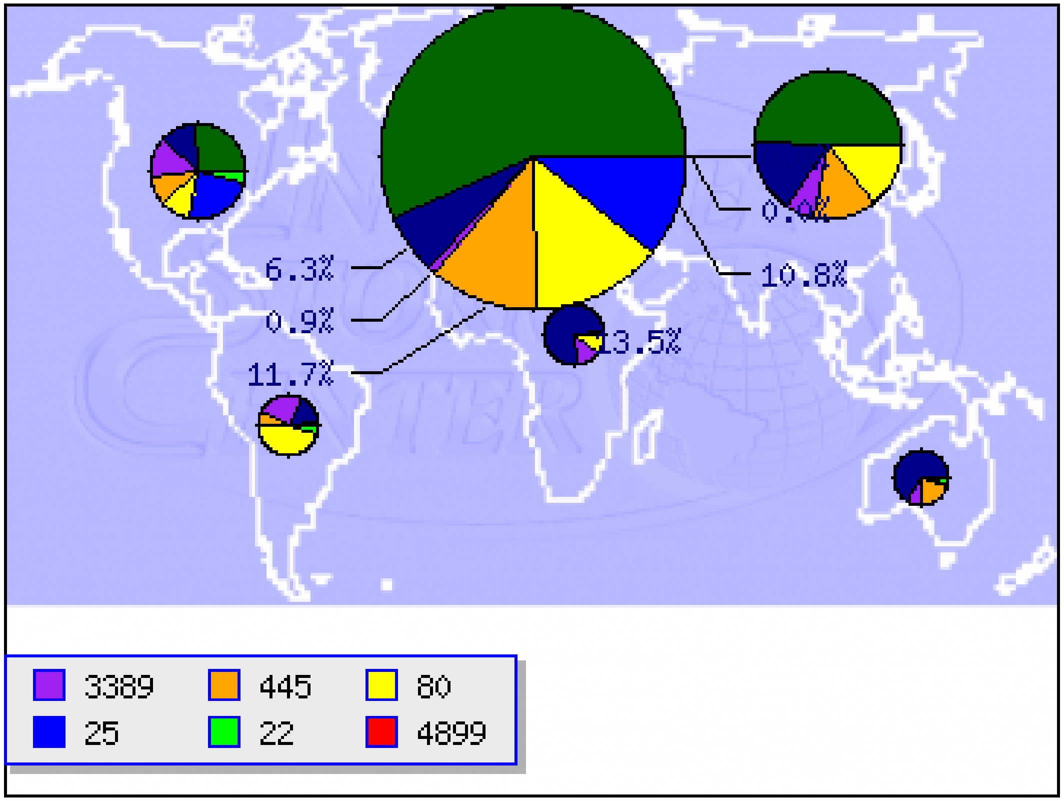
S = number of source IPs hitting this port last 24 hrs.

s = average number of source IPs hitting this port each day for last 30 days

T = number of target IPs getting hit from this port last 24 hrs.

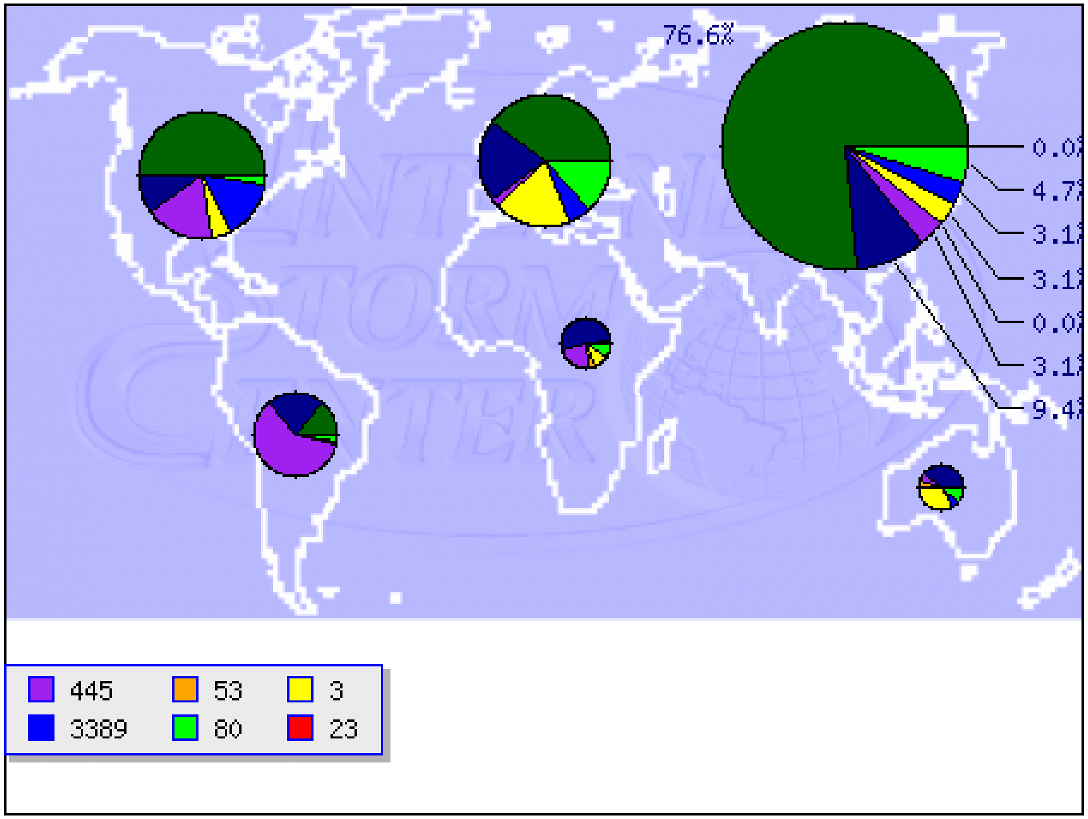
t = average number of target IPs getting hit from this port each day for last 30 days

Ports Being Used for Probes or Attacks by Continent – July 2013*



The green area means that the port usage is OK.

Ports Being Used for Probes or Attacks by Continent – June 2014*



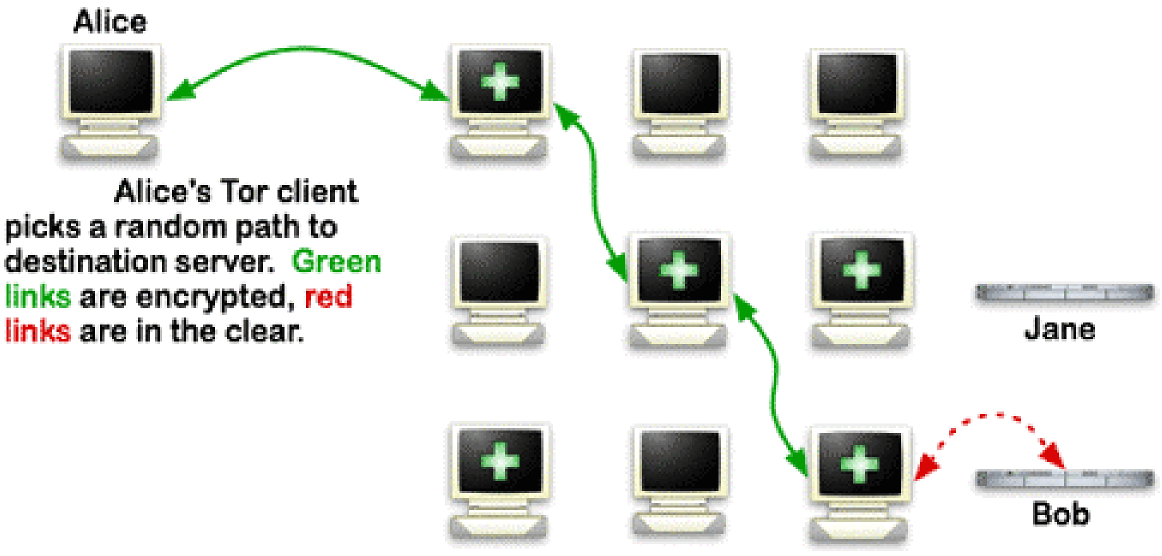
The green area means that the port usage is OK.

TOR

TOR ***(The Onion Router)***

- *Free software for enabling online anonymity*
- *Internet traffic travels through a free, worldwide volunteer network consisting of more than three thousand relays*
- *Helps conceal a user's location or usage from anyone conducting network surveillance or traffic analysis*
- *More difficult to trace Internet activity*
  - e.g., visits to web sites, online posts, instant messages and other communication forms back to the user
- ***Stated goal****: Protect users' personal privacy, freedom, and ability to conduct confidential business by keeping their internet activities from being monitored*

How TOR Works



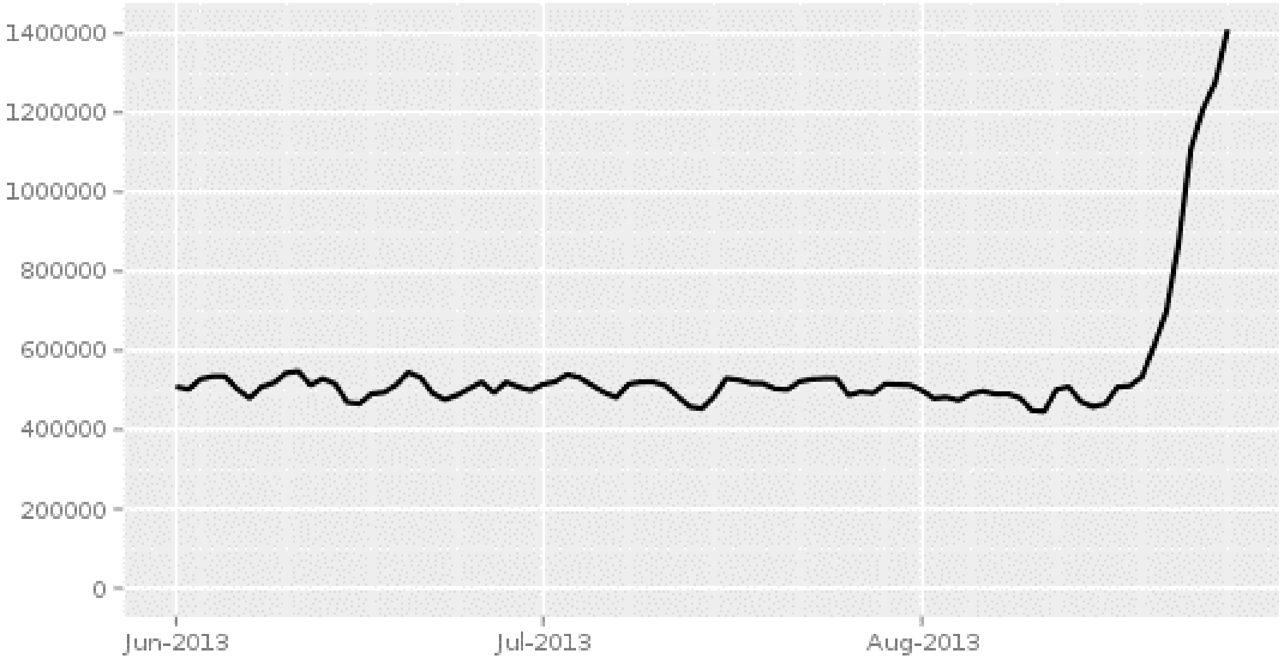
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

TOR Directly Connected Users
Recent Worldwide Information

An interesting reported TOR curve

Number of users directly connected to TOR

What's going on?



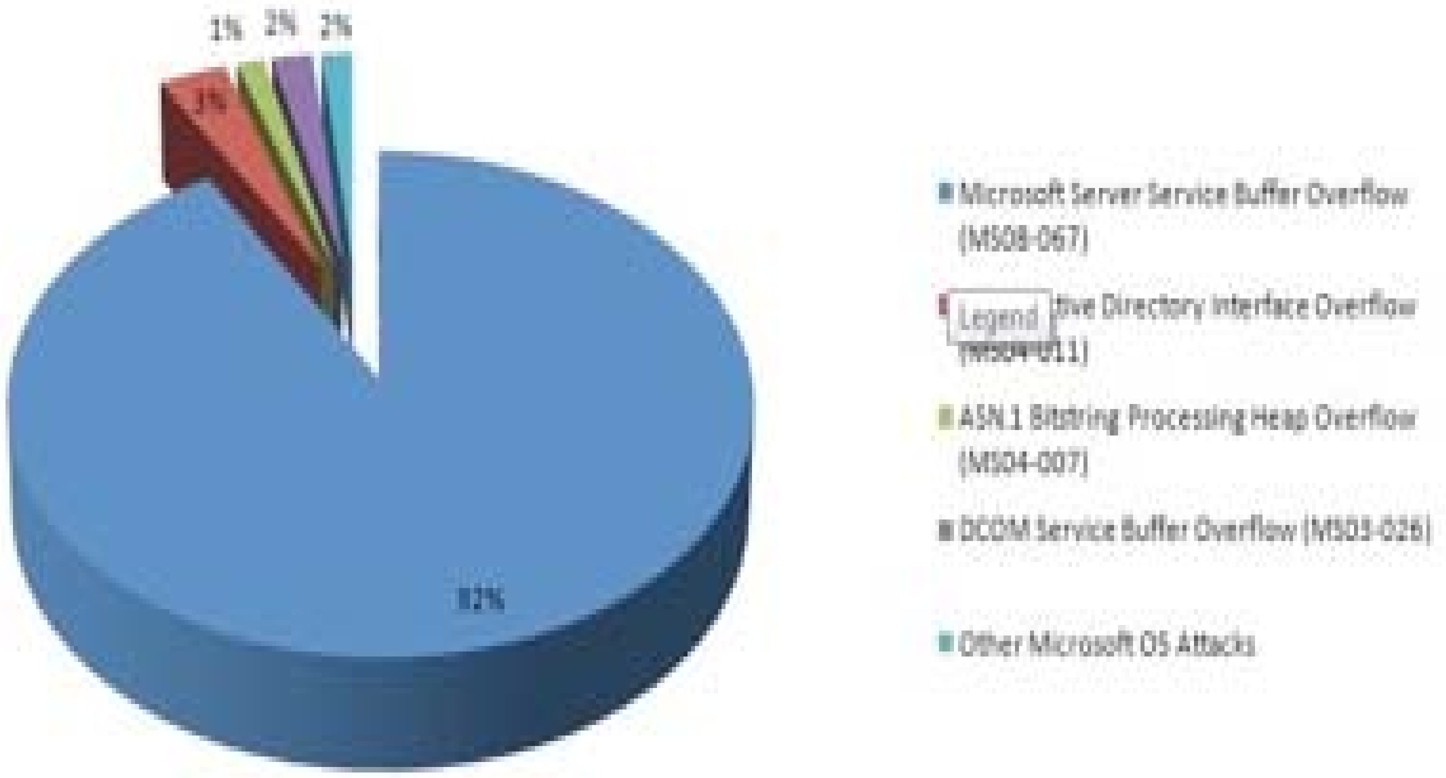
Some hypotheses

New malware?

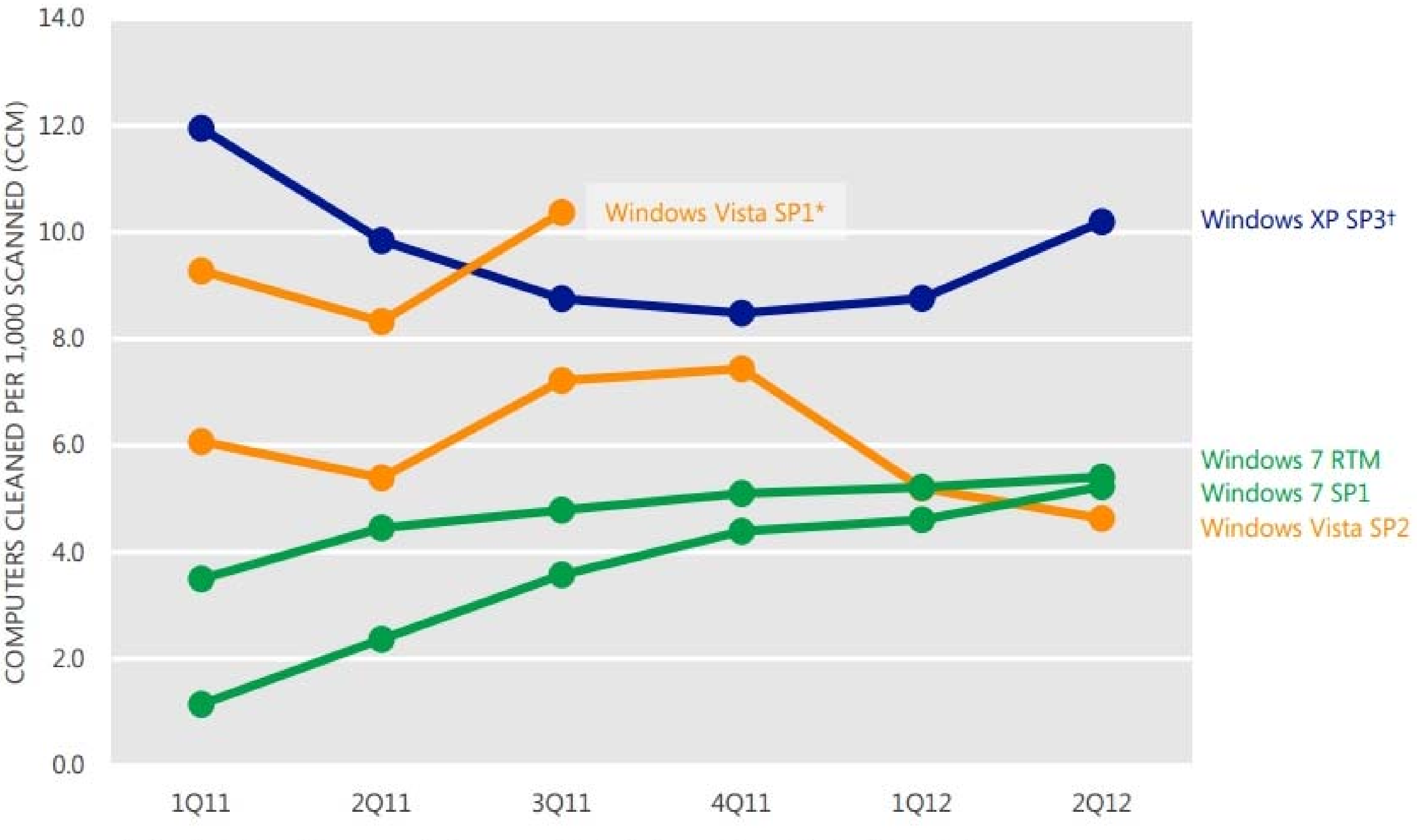
People responding to news of government surveillance?

A reporting error?

Microsoft OS Attacks

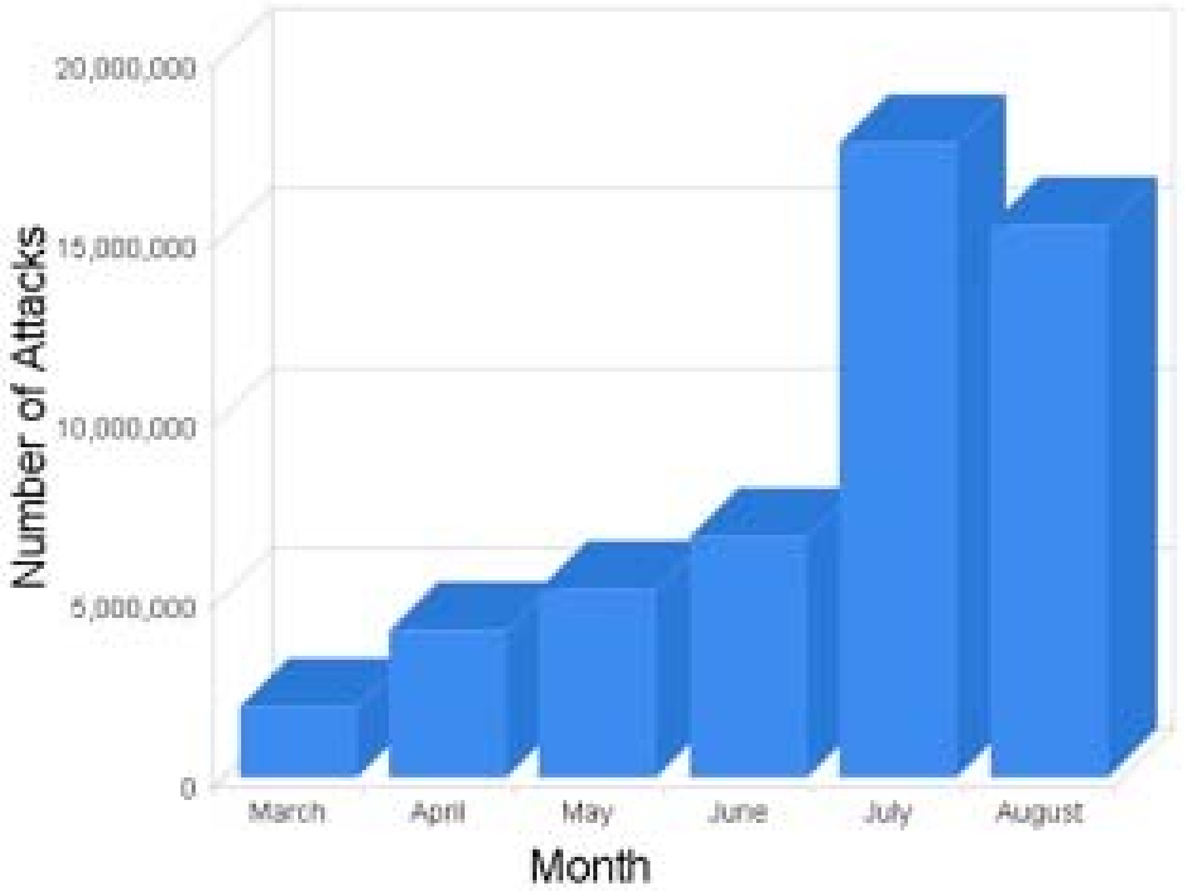


Windows Infection Rate Trends

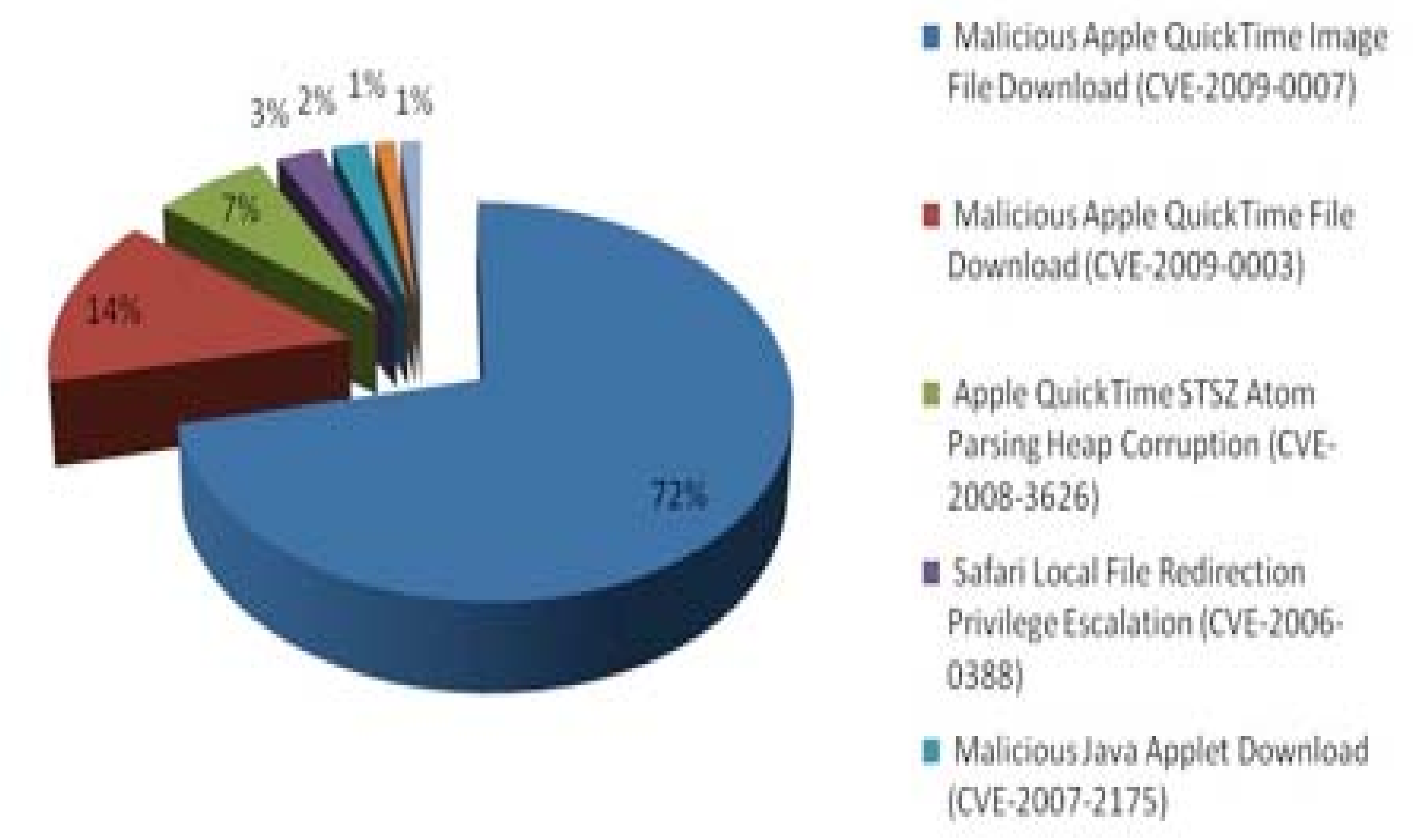


* Support ended July 12, 2011. †Extended support for Windows XP ends April 8, 2014.

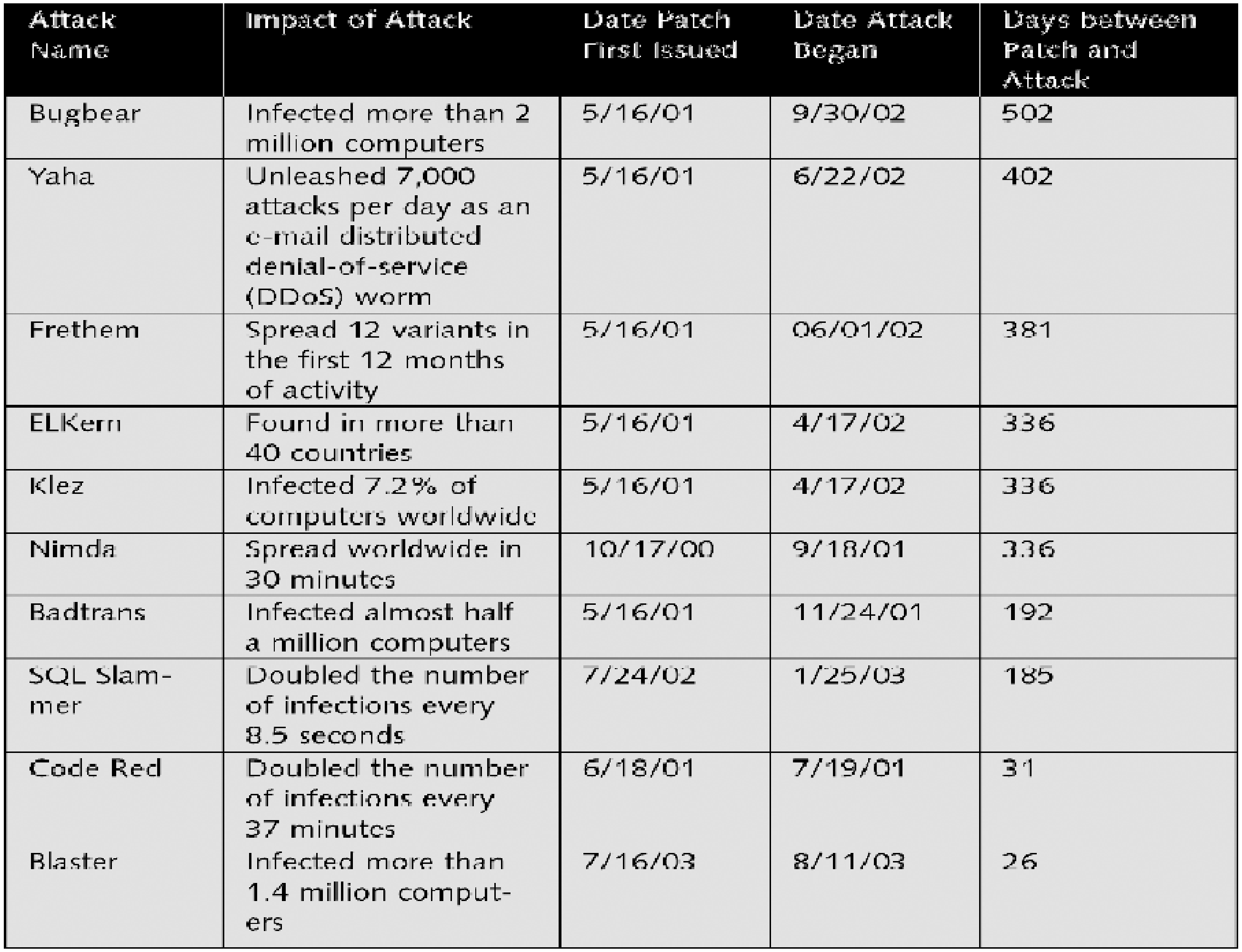
Number of Microsoft Attacks
March-August 2011



Apple Attacks



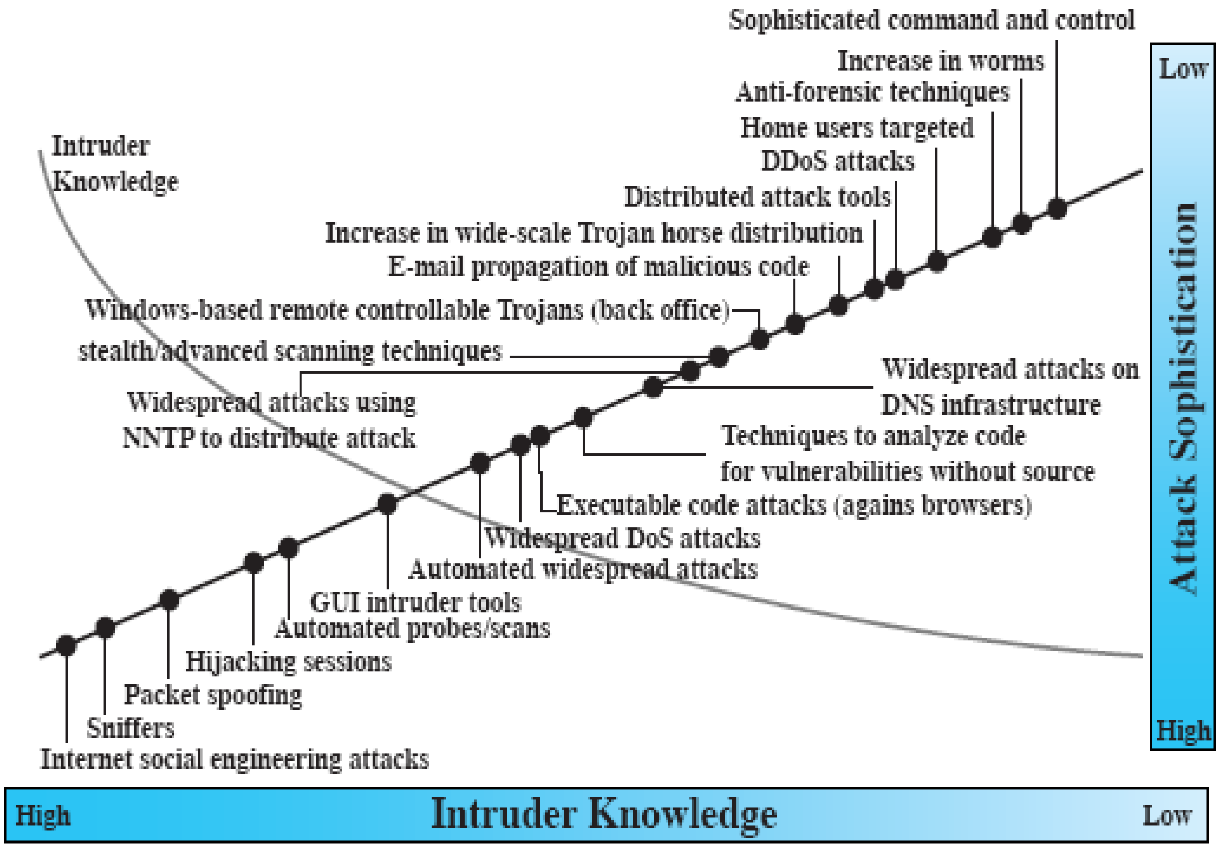
Delay Between Patches & Attacks



Attack Name	Impact of Attack	Date Patch First Issued	Date Attack Began	Days between Patch and Attack
Bugbear	Infected more than 2 million computers	5/16/01	9/30/02	502
Yaha	Unleashed 7,000 attacks per day as an e-mail distributed denial-of-service (DDoS) worm	5/16/01	6/22/02	402
Frethem	Spread 12 variants in the first 12 months of activity	5/16/01	06/01/02	381
ELKern	Found in more than 40 countries	5/16/01	4/17/02	336
Klez	Infected 7.2% of computers worldwide	5/16/01	4/17/02	336
Nimda	Spread worldwide in 30 minutes	10/17/00	9/18/01	336
Badtrans	Infected almost half a million computers	5/16/01	11/24/01	192
SQL Slammer	Doubled the number of infections every 8.5 seconds	7/24/02	1/25/03	185
Code Red	Doubled the number of infections every 37 minutes	6/18/01	7/19/01	31
Blaster	Infected more than 1.4 million computers	7/16/03	8/11/03	26

Hacker's use of patch information to mount attacks

Trends in Attack Sophistication and Intruder Knowledge



Source: CERT

The increasing straight line indicates types of tools readily available to attackers.

The decreasing curved line indicates relative amount of knowledge attacker must have to launch a successful attack.

Source: CERT

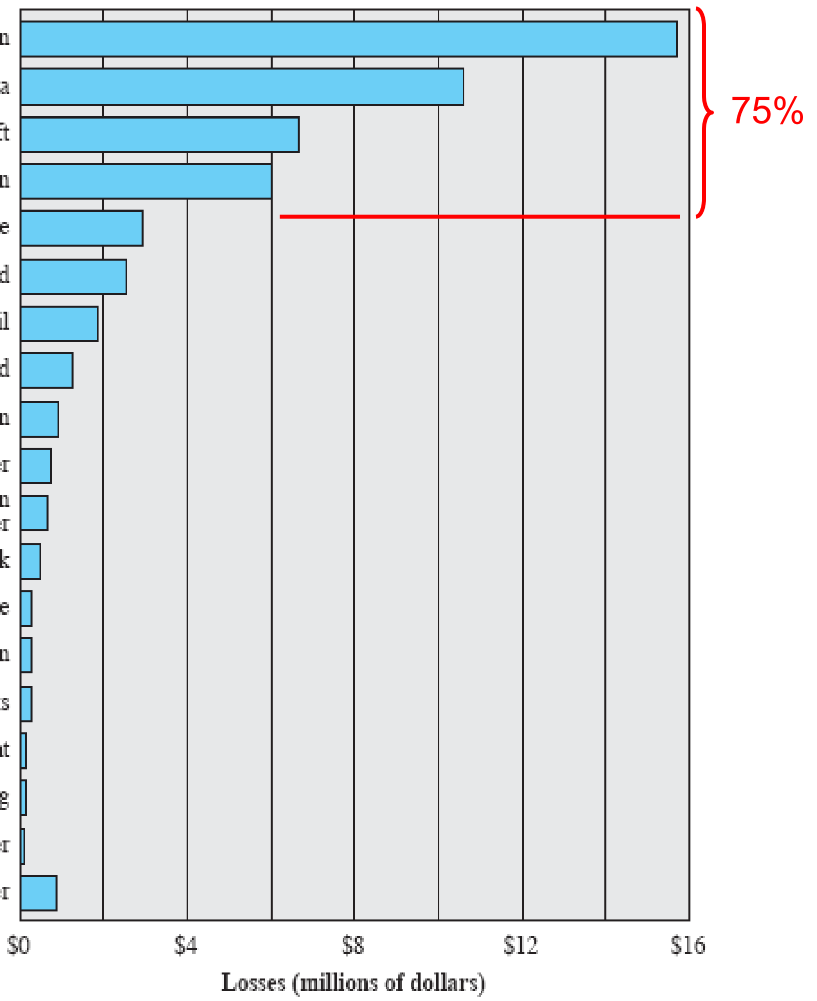
So increasingly sophisticated tools are available that can be easily used without the user having much knowledge.

$ Losses by Type of Attack

FBI 2008 Crime Survey

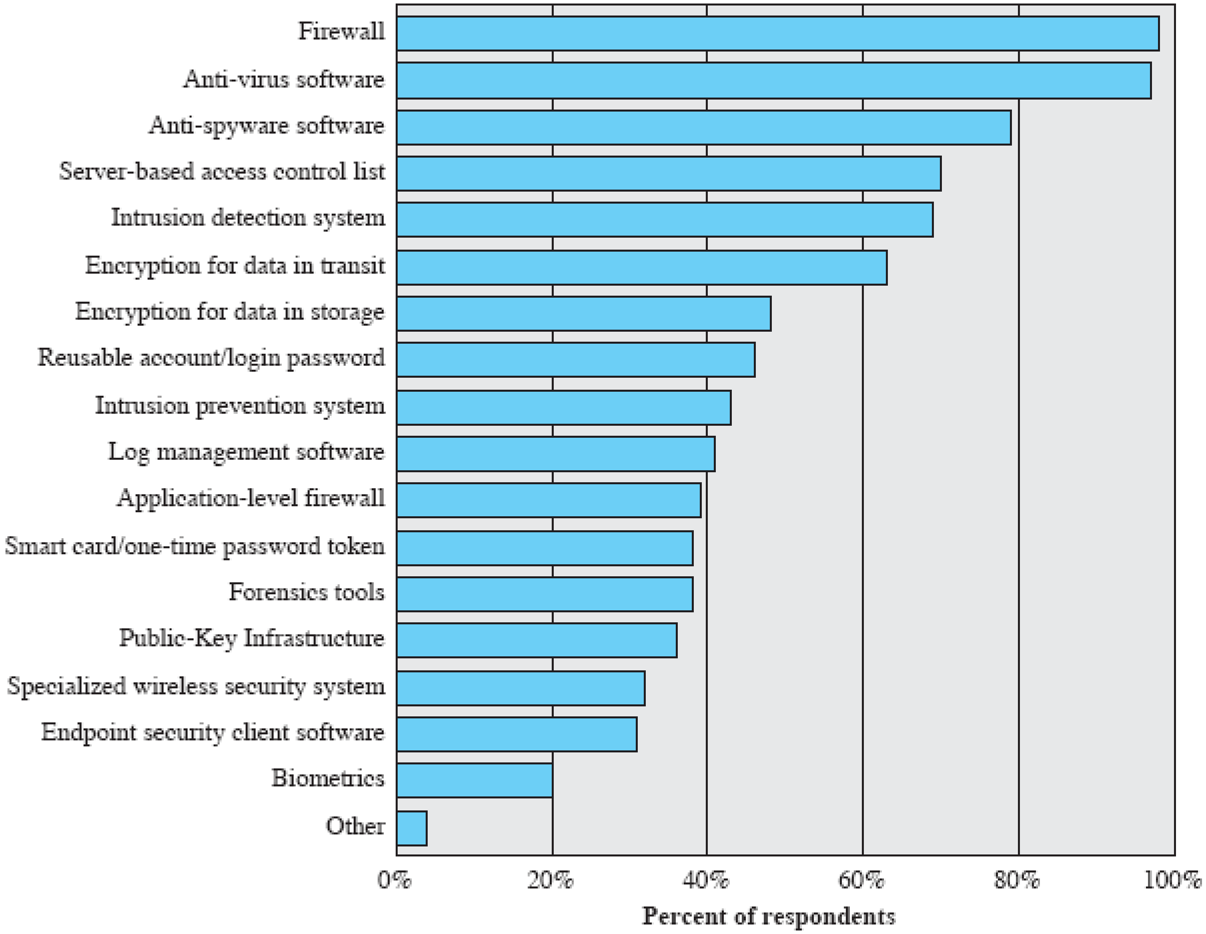
	Other	Physical	Tech.
Virus contamination			X
Unauthorized access to data			X
Laptop or mobile hardware theft		X	
Theft of proprietary information		X	X
Denial of service			X
Financial fraud			
Intruder abuse of net access or email		X	X
Telecom fraud			
Bots (zombies) within the organization			
System penetration by outsider			
Phishing in which your organization was fraudulently represented as sender			
Abuse of wireless network			
Instant messaging misuse			
Misuse of public Web application			
Sabotage of data or networks			
Web site defacement			
Password sniffing			X
Exploit of your organization's DNS server			
Other			

Countered by:



Security Technology Used
FBI 2008 Crime Survey

- Almost everyone uses ***firewalls*** and ***anti-virus*** software.
  - *Oldest. Mature and familiar.*
  - *Many vendors reduces cost.*
  - *Many threats can be defeated with these two.*
- The use of anti-spyware has increased since 2006.



Security Technology Used

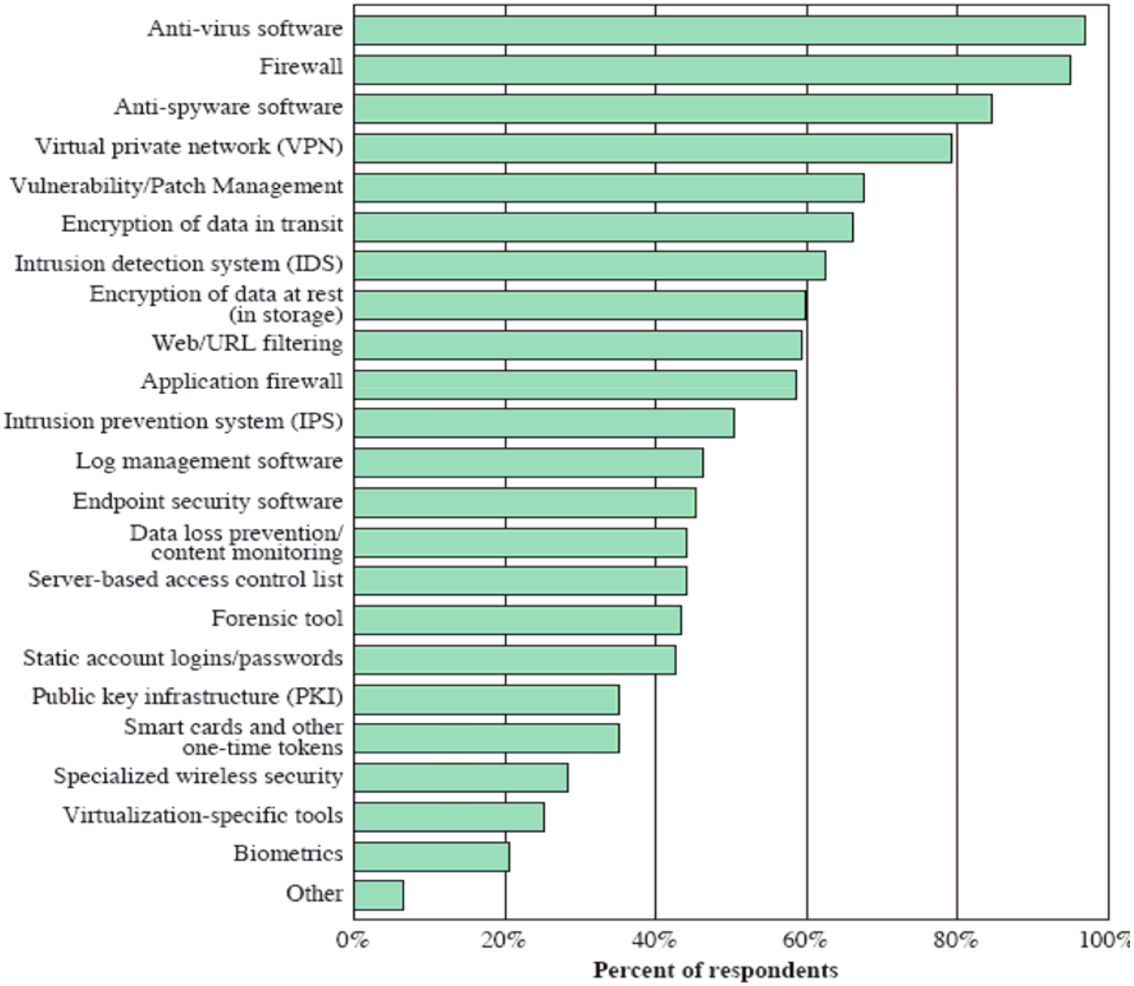
FBI 2010-2011 Crime Survey

Firewalls and ***anti-virus*** software still lead, but have switched places

The use of anti-spyware has increased since 2008.

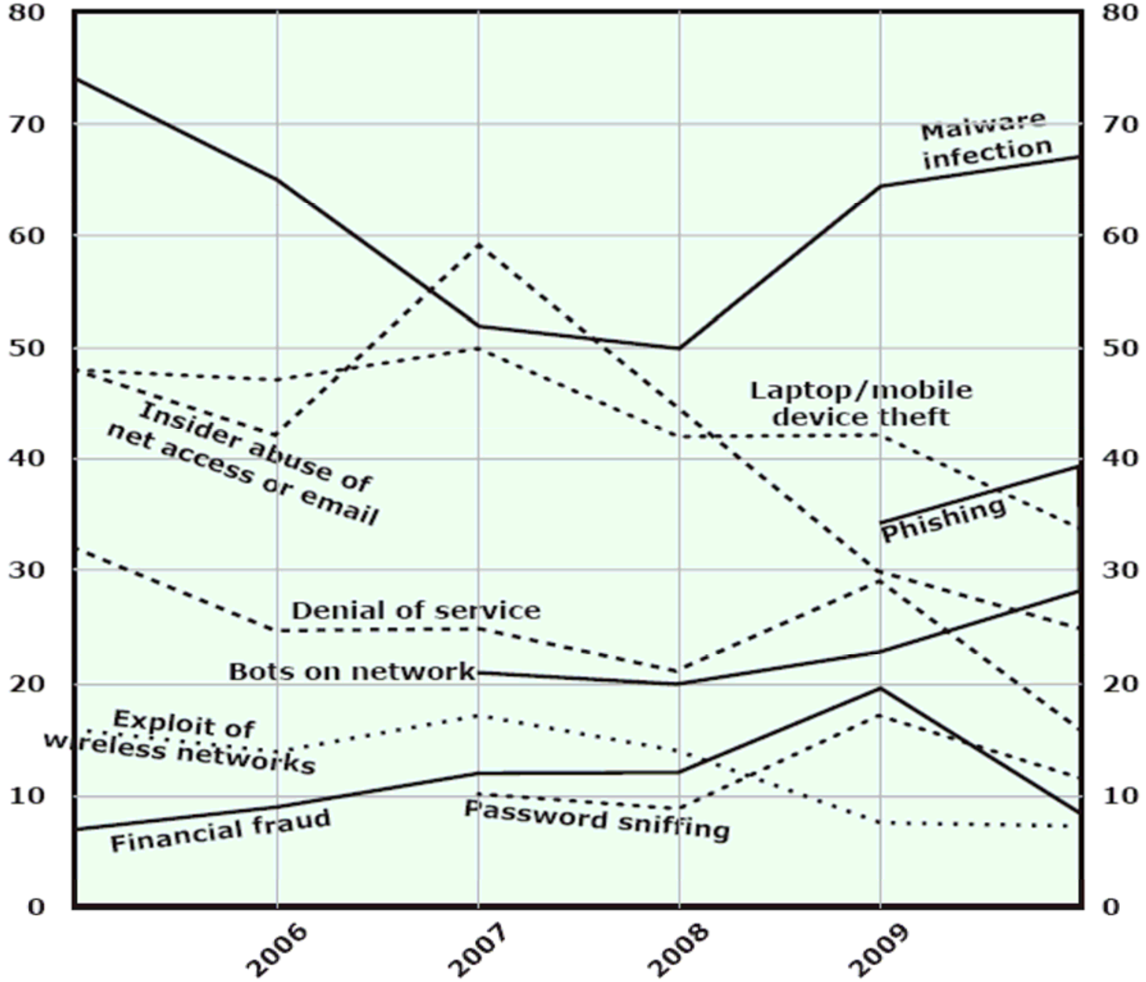
VPNs are now 4th. They weren't on the chart in 2008.

Virtualization now exists; weren't on chart in 2008



Attack Trends

FBI 2010-2011 Crime Survey



What is Computer Security

Defining Computer Security

Tasks of guarding digital information, which is typically:

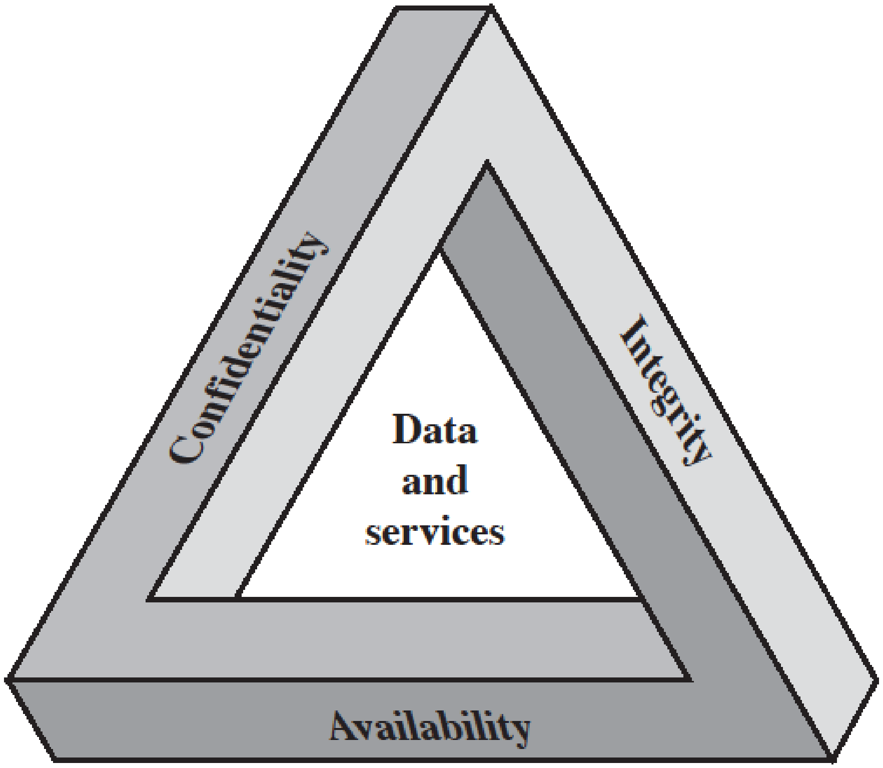
- *Processed by computers (such as a personal computers),*
- *Stored on magnetic or optical storage devices (such as a hard drives or DVDs), and*
- *Transmitted over networks*

Task of guarding the above computers, storage devices networks and security systems in order to keep them in reliable operation

So it's guarding

- *Information*
- *Systems*
- *Hardware*

Security Triad



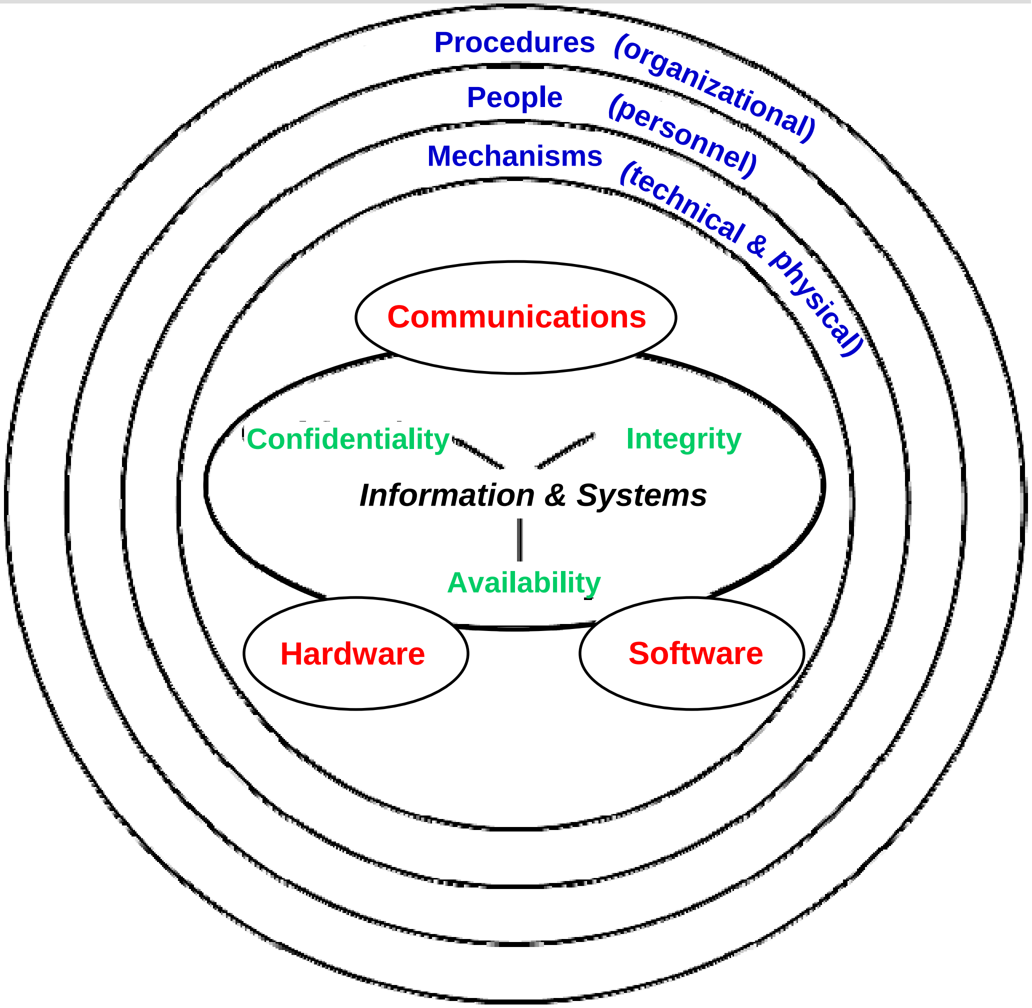
Defining Security

What needs protection?

What characteristics achieve this protection?

Protection is achieved via a combination of 3 technologies

Entities employing the 3 technologies



Confidentiality

Data

Assures that information is not available to unauthorized persons

Privacy

Assures that individuals control the information related to them

Who may collect and store it

To whom it is disclosed

Integrity

Data

Assures that information and software are changed only in a specific and authorized manner

Systems

Assures that a system performs its intended function in an unimpeded manner

Assures absence of deliberate or inadvertent unauthorized system manipulation

Availability

Assures that systems work promptly and that service is not denied to authorized users

Two Additional Characteristics

Authenticity (sometimes included as part of Integrity)

- *Verifiability genuine and trusted*
- *Confidence in validity of a transmission*
- *Confidence in the accuracy of the source*

Accountability

- *Ability to trace the actions of an entity uniquely to that entity*
- *Non-repudiation, after-action recovery & legal action*
- *Causes systems to keep records of activities*

Security and Data Theft

Security often associated with theft prevention

Drivers install security systems on their cars to prevent the cars from being stolen

Same is true with information security—businesses cite preventing data theft as primary goal of information security

Theft of data is the largest explicit cause of financial loss due to a security breach

One of the most important objectives of information security is to protect important business and personal data from theft

Legal Consequences

Businesses that fail to protect data may face serious penalties

Laws in the USA include:

- *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)   [health insurance & privacy for people changing jobs]*
- *The Sarbanes-Oxley Act of 2002 (SOX)   [accounting & investor protection]*
- *The Gramm-Leach-Blilely Act (GLBA) [consumers' personal financial]*
- *USA Patriot Act 2001*
  - “Sunsetted”
- *Domestic Security Enhancement Act of 2003*
  - Revision of Patriot Act of 2001

Productivity
Cost of Attacks

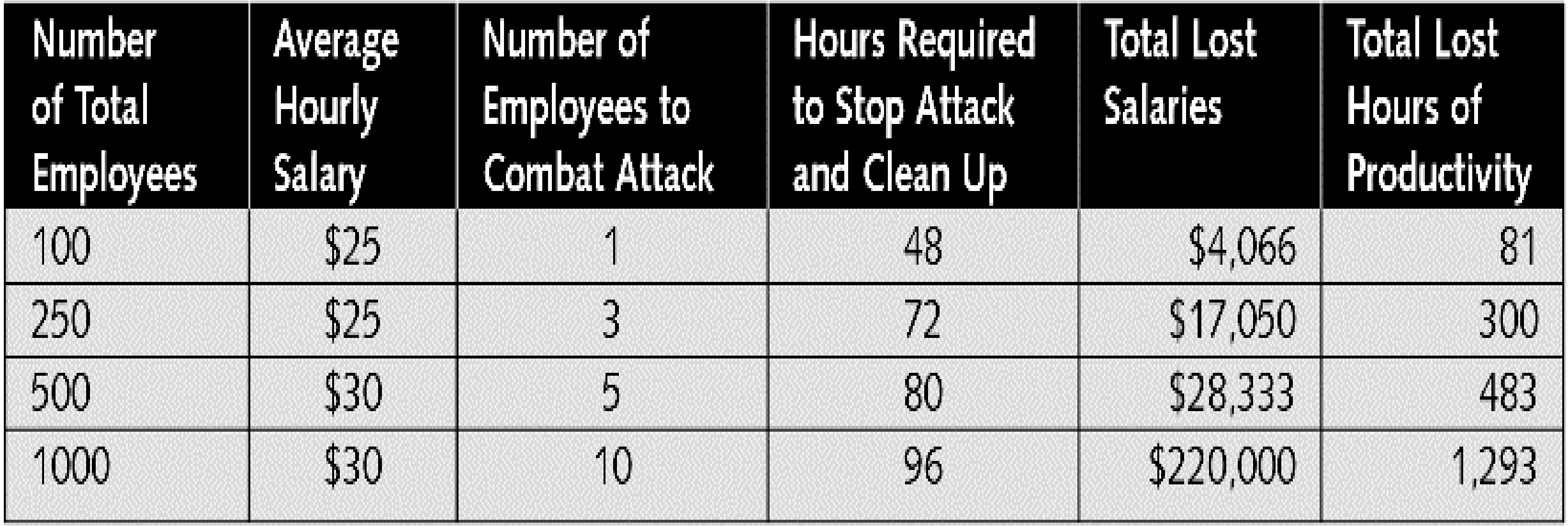
After an attack on information security, clean-up efforts divert resources, such as time and money away from normal activities

A Corporate IT Forum survey of major corporations showed:

- *Each attack costs a company an average of $213,000 in lost man-hours and related costs*
- *One-third of corporations reported an average of more than 3,000 man-hours lost*

Productivity

Cost of Attacks



Number of Total Employees	Average Hourly Salary	Number of Employees to Combat Attack	Hours Required to Stop Attack and Clean Up	Total Lost Salaries	Total Lost Hours of Productivity
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1000	$30	10	96	$220,000	1,293

Cyberterrorism

An area of growing concern among defense experts are surprise attacks by terrorist groups using computer technology and the Internet (cyberterrorism)

These attacks could cripple a nation’s electronic and commercial infrastructure

Our challenge in combating cyberterrorism is that many prime targets are not owned and managed by the federal government

Cyberwarfare

Another area of increasing concern is cyberwarfare

Cyberterrorism and cyberwarfare are sometimes used synonymously

What's the difference?

Identity Theft

Identity theft involves using someone’s personal information, such as social security numbers, to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating

National, state, and local legislation continues to be enacted to deal with this growing problem

The Fair and Accurate Credit Transactions Act of 2003 is a federal law that addresses identity theft

Identity theft has become a huge problem

e.g., Target Corp in late 2013

An Aside of Interest

What Takes 20 Minutes?

Watch an entire sitcom on TV if you fast forward through the commercials

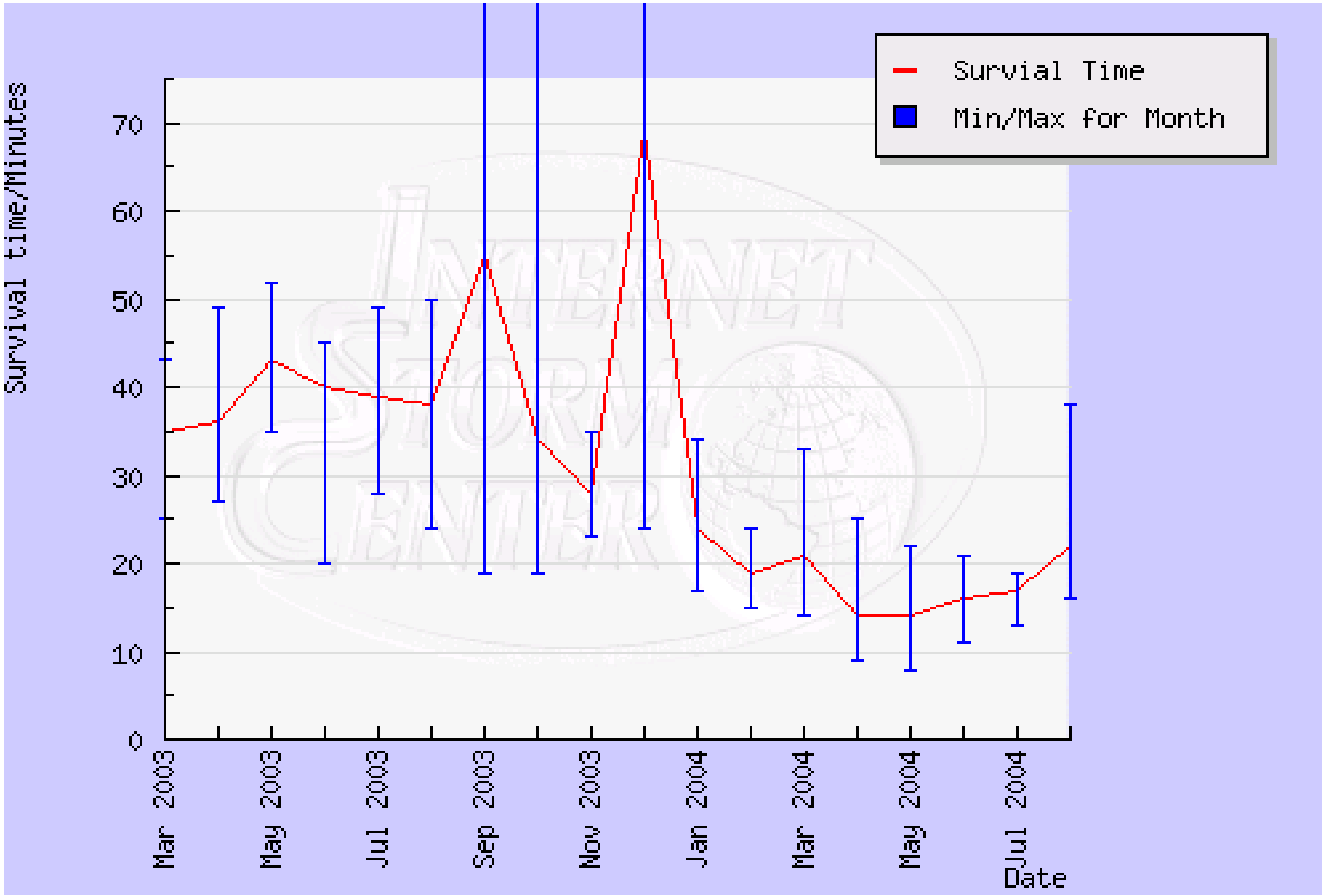
Drive to my home from IIT after class at night.

A class break

The time to infect an average unprotected computer running poorly patched Windows once it's connected to the Internet.

SANS Institute

SANS Institute Study Results



Implications of 20 Minutes

20 minutes is not enough time to download the security patches from Windows Update

Most people will

- *Take their new computer out of the box*
- *Plug it in and connect it to their Internet connection*
- *Turn it on*

A very few will immediately try to get the patches

This use to be an overwhelming problem

Implications of 20 Minutes

Fortunately with versions of windows from XPsp3 and beyond and also Linux

- *The firewall is on by default*
- *This helps*

Also most reputable ISPs

- *Block ports often used by viruses and worms*
- *Filter known email viruses and some spam*
- *Result: Survival time is longer*

Some Accepted Truths and Goals

Truth #1

Complete security doesn’t exist.

- *The goal is to reduce the probability of a successful attack to some acceptable minimum*
- *Acceptable minimums are different for different organizations and people*

Truth #2

Cryptography is necessary but not sufficient.

- *Some people look to cryptography as* ***<u>the</u>*** *answer to security*
- *But real-world systems are incredibly complex with myriad unknown and unintended functionality*
- *Cryptography is just one of a number of preventive technologies*
- *Good encryption secures most information as it traverses an open Internet*
- *Doesn't handle domain, zone, or organization compromises*
  - These handled by firewalls, audits, detection, reaction**…**

Truth #3

Security is a pain

- *Security involves tradeoffs among the following:*
  - Confidentiality
  - Integrity
  - Authenticity and Accountability
  - Availability
- *e.g., Home intrusion systems change the way you do things*
  - Must set intrusion system when you leave
  - Must quickly disable intrusion system when you return
  - Cannot walk around at night after arming motion detectors

Our New World

Internet Has Changed Almost Everything

It has changed us

- *The way we shop*
- *The way we communicate with others*
- *The way we do work*
- *With smartphones, were always connected*

Internet Has Changed Almost Everything

It has changed lives of criminals, terrorists, & publicity seekers

- *Enhances their ability to act*
- *Amplifies ability to attack*
- *Can attack from a distance, anonymously, and with automation*
- *Enhances their ability to act together*
  - There are growing ties among multinational underworld cartels and terrorist organizations

Internet Has Changed Almost Everything

- Changed the way governments can do things
  - *Enhanced ability of different arms of government to act and to keep records*
  - *Enhanced ability of different arms of government to act together*
    - e.g., Common databases
  - *But this also enhanced government's ability to probe into our privacy and to keep records on us*
- Changed the way business (and especially big business) does things
  - *Easier to be geographically spread out*
  - *Enhanced business's ability to probe into our privacy and to keep records on us*

Cyber Crime

In some ways much the same as POC (Plain Old Crime)

POC tools included

- *Lock picks*
- *Double sets of account books*
- *Dynamite*

Cyber crime tools include

- *Networking*
- *Worms, trojan horses, viruses, port scanners…*
- *Computers*
- ***Automation*** *This is new!*

Crime Example: Rob Bank*

POC	***Cyber***
Gun	Computer Internet Obtainable hacking software
Mask *Anonymity difficult especially with video monitoring cameras…*	Laundered IP addresses Viruses in other computers *Anonymity much easier*
Must go to bank to rob it	Can do it remotely
High physical risk	Zero physical risk
Average "take": ~$1500 *Nationwide average in FY2000*	Average "take": Very large *Every day banks transfer billions of dollars over networks to & from networked databases*

Example: Privacy Invasion
(may or may not be crime)

More Conventional	*Cyber*
Parabolic microphones, camera, infrared & night vision detectors... *Sniffers, chat relay masqueraders...*	Computer, Internet Obtainable hacking software *Sniffers, chat relay masqueraders...*
Must hide antennas; avoid being seen. Neighbors might know who you are.	Can lie about who you are. Chat relay is transparent to users.
Locate equipment nearby *Parked van, neighbor's house...*	In some cases can be half a world away.
High physical risk.	Zero physical risk.
Listen to your conversations. See what your doing. Know better your activities.	Remotely accesses your files. Monitor your private chatting. Record the web sites you visit.

Attacker Motivation

Use to be mostly

- *Bragging rights or trophy collecting*
- *Thrill seeking*
- *Fun and sport*

Now there is more of

- *Financial gain*
- *Collection of intelligence and proprietary information*
- *Political activism*
- *Terrorism*
- *Warfare*

Future

Attacks will likely be

More sophisticated, common & widespread
Harder to track, capture, and convict attackers
Effects can be more devastating

Why?

Future

Why?

- *A network is the criminal's friend*
  - Can act at a distance -- maybe many countries away
  - Successful attack schemes can be propagated widely and instantly
- *A computer is the criminal's friend*
  - Successful attack schemes can be replicated
    - *Only the original designer of the attack scheme need be skilled*
    - *Others copycats can be sort of dumb: "script-kiddies“*
      - DDoS software and scripts are well publicized
      - Virus, worm, and trojan horse software is available
      - Detailed user instructions exist
  - Attack schemes can take advantage of automation

What’s The Problem?

Why can’t we just make networks and computers secure?

Software is Very Complex

Really there are 3 sources of software problems

Complexity

Mobility

Connectivity

Software is Very Complex

Operating Systems

Solaris 7:	*400 thousand lines of code*
Linux:	*1.5 million*
Win95:	*5 million*
Win2K:	*35 million*
WinXP:	*40 million*
Vista:	*50 million*

Other Systems By Contrast

Space Shuttle:	*10 million*
Space Station:	*40 million*
Boeing 777:	*7 million*

Software is Very Complex

MSWORD

1983: 27K lines of code

1995: 2 million

2000: >2.5 million

Measuring Software Complexity

Computer Science is replete with thousands of PhD theses on measuring software complexity

There are hundreds of books on the subject

Yet the only measure that seems to have wide acceptance and correlates well with numbers of bugs is lines of code (LOCs)

Bugs per KLOCs range from 50 down to 5 per KLOC

The number of 5 is achieved after extensive code reviews and testing

And still there are bugs left that seem to never come out

Numbers of Windows Bugs

So WinXP, at best, was likely to have initially

$$\frac{40x10^6}{10^3} KLOCs \ \ x \ \frac{20bugs}{KLOC} = 800{,}000\, bugs$$

After XP sp3, if we're lucky, maybe we're now down to

$$\frac{40x10^6}{10^3} KLOCs \ \ x \ \frac{5bugs}{KLOC} = 20{,}000\, bugs$$

Vista sp1

$$\frac{50x10^6}{10^3} KLOCs \ \ x \ \frac{25bugs}{KLOC} = 125{,}000\, bugs$$

Make you feel good?

Reuse & Code Sharing

Components such as functions, DLLs and classes are shared by multiple applications

For instance if a DLL is changed after an application that uses it is coded, the application might be made vulnerable by the changed DLL

Applications interact directly with each other

This bypasses operating system control and logging

Protocol stacks are implemented differently by different vendors

OSs must depend on the protocol stacks being secure

Device Drivers

Device drivers are developed by different vendors

- *Often not developed well or controlled*
- *How many time have you downloaded a driver off the Internet and installed it without investigating it?*

Usually run in a privileged mode

- *So if they malfunction they can mess up the entire system*
- *Or if they contain malware, the attacker will have elevated privileges*

Mobile Code

When you use a web browser, code moves from a server into your computer and executes in your computer

Sometimes called *mobile* or *extensible* code

Examples

Java

.NET

OSs support mobile code by providing for the dynamic loading of code at runtime

Mobile Code

Applications support extensibility via scripting

- *e.g., Browsers, word processors, spreadsheets...*

Mobility and extensibility make security much harder

- *Software even more complex*
- *How can you determine the security of code that has not yet arrived at your computer?*
  - Certificates?
  - Hashes?

Mobile Code

Many worms and viruses are themselves types of mobile code

- *They don't just propagate*
- *They install backdoors, keyboard & screen monitors, event loggers and trojans for later use*

A Quote

“Life was simple before World War II.
After that, we had systems.”

Grace Hopper, Admiral, USN

And she said this before there was an Internet.

Internet Added Yet More Complexity

Computers are directly connected together via LANs

LANs are connected to other LANs, MANs & WANs

The different LANs, MANs and WANs, ISPs are controlled and administered by different organizations

The WANs cross international boundaries

And the network software (that we've already discussed) is also so very complex

- *And new network software is sometimes not well tested*
  - Things have gotten better here

Internet Added Yet More Complexity

The various parts of the Internet interconnect

- *Form systems which in turn form even larger systems…*

The various parts of the Internet interact

- *Interactions are both intended and unintended*

The Internet is very complex

- *Even the system components are very complex*
  - e.g., a Computer millions of lines of code

Components and subsystems fail or partially fail, sometimes in obscure ways

- *Failures are usually unknown to other parts of the Internet*
- *Failures are sometimes unknown to the component itself*

Internet Added Yet More Complexity

The Internet and its subsystems & components are so complex that they can exhibit unintended operation even if they are bug free

React in unexpected ways to pathological sets of circumstances

The Internet also has unintended bugs that cause additional unintended operations

Both the unintended operation and the bugs might or might not be repeatable

More Terminology

I will now go through some of the terms

But review and understand all of them.

Computer vs. Network Security

Computer Security

The process of securing a single, stand-alone computer,

Network Security

The process of securing an entire network of computers and the network devices that constitute the network

Computer vs. Network Security
NSA Definition

Computer security

Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer.

Network security

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects. Network security includes providing for data integrity.

Comments on Terminology

Network security has a set of terminology that needs to be defined and understood

We’ll now consider a number of definitions

Be aware of them

We will revisit most of them as we move through the topics of this course

Three Related Definitions

Authentication

To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Non-repudiation

Sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Inability of sender to deny either the sending or contents of whatever is sent

Three Related Definitions

Digital Signature

Data that has been encrypted by a user's private key.

Too restrictive. Often private keys are used, but the above is an implementation of a digital signature; not its definition

Any scheme whereby the sender provides to the receiver something that assures the receiver that indeed the stuff sent has been sent by the sender and that it is accurate

Some Security Devices

Network Firewall

A system or combination of systems that enforce a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.

Resident Firewall

Software running resident on a computer system that acts as a guard, inspecting entities that enter and leave the system, passing or blocking the entities based upon a set of rules reflecting the system security policy.

Some Security Devices

Intrusion Detection Systems (IDS)

Systems which use various techniques to attempt detection of intrusion into a computer or network by observation of actions, security logs, or auditing data. Detection of break-ins or attempts via software systems that operate on logs or alert information.

Intrusion Prevention System

An IDS linked to firewalls that can dynamically change the firewall rules based upon detected intrusions in order to stop the intrusion.

Demilitarized Zone (DMZ)

A part of a network that is connected to both a secure and insecure network (sometimes referred to as the intranet and Internet respectively).

Some Attack and Hacking Definitions

Denial of Service (DoS)

- *An attack with the motivation of disruption, not theft. The DoS attack is designed to make a system, network, or service perform poorly or become unavailable to those users that legitimately have a right to that function.*
- *Usually makes a system perform poorly or become unavailable by overloading it so that it cannot service legitimate users*
  - e.g., I-88 at 5pm performs poorly
- *DoS is one of the most simple ways to damage a system. Denying legitimate users access to a resource is the general goal of DoS attacks.*

Some Attack and Hacking Definitions

Distributed Denial of Service

A DoS attack that comes from multiple places concurrently.

The "seed" attacker recruits additional attackers.

Then all the attackers start at the same time.

Some Attack and Hacking Definitions

Hacking

Def1: Unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network.

Def2: Authorized use or attempts to circumvent or bypass the security mechanisms of an information system or network. (Ethical hacking)

Cracking

Unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network.

Script Kiddies

Hackers or crackers who use pre-made tools for hacking and cracking information systems and network, and who generally have no knowledge of the function of the tools that are being used.

Some Attack and Hacking Definitions

Spoofing

- *Pretending to be someone or something other than who or what you are. Impersonating, masquerading, and mimicking are forms of spoofing.*
- *Spoofing is usually associated with IP addresses, where an attacker will use a false source IP address as the source of packets. This makes the investigation of an incident more difficult, as the true IP address of the attacker is not visible*
  - But the attacker cannot received information back because the source IP address is not that of the attacker

Some Attack and Hacking Definitions

Smurf

A type of DDoS attack in which a network is swamped with replies to a stimulus that is magnified by the network

e.g., Replies to ICMP echo requests (PINGs)

A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim.

All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Cryptographic Definitions

Cryptography

The science of the methodology of rendering plaintext unintelligible, and for decrypting encrypted messages into intelligible form.

Cryptography is one of the more complex areas of information security

One popular implementation of cryptography is securing email using applications such as encrypted email or PGP (Pretty Good Privacy).

Cryptographic Definitions

Public Key Infrastructure (PKI)

Infrastructure allowing users to securely exchange data using encrypted key pairs, while confirming the identity of the users involved in the data exchange.

The implementation of a full-scale PKI in a large environment can take an organization as long as a year or more. When a PKI is implemented, the initial stage is known as a Pilot and is run in a controlled portion of the network to test continuity.

Much more on this and other related definitions in the cryptography section of this course

Misc. Definitions

Biometrics

The science of measuring unique physical characteristics of the human body and using them as methods of identification verification.

Examples

- Fingerprint scanners
- Hand scanners
- Voice recognition
- Retinal scanners
- Iris scanners
- Facial recognition

Misc. Definitions

Auditing

The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend and indicate changes in controls, policy, or procedures.

To systematically view the log files of network devices scanning for details that can identify use of network resources.

Misc. Definitions

Scanning

The (usually automatic) interrogation of a set of networked computers and other network devices to determine their state, nature, and vulnerability.

Real-time Auditing

Ongoing scanning for the purpose of detecting and quickly correcting host vulnerabilities.

Misc. Definitions

Network Forensics

The process of determining how an attack was executed and the amount of damage caused by the attack, along with the process of gathering evidence to prove damage and/or financial loss.

Misc. Definitions

Security Analysis

The analysis of the security needs of an organization in order to guide in establishing a security policy.

Security Policy

A set of rules, laws, and practices that regulate how an organization man-ages, protects, and distributes sensitive information.

These are important first steps!

Misc. Definitions

Layered Defense

The process of reliance on multiple technologies and systems in the defense of a network or computer system.

Most organizations who are serious about security will have implemented a layered approach to their security.

By presenting multiple obstacles for the attacker, the overall defense level of the network increases.

Misc. Definitions

Root

The name of the user account on UNIX/Linux systems that has system-level control.

Also used at times to indicate a Windows ***Administrator*** *account.*

Generally, when an attacker is trying to gain control over a computer, ***Root*** *or* ***Administrator*** *access is a goal.*

When the attacker has gained Root access, the whole system is subject to compromise.

Misc. Definitions

Social Engineering (two definitions)

1. *The process of gaining access to otherwise unavailable information via human-to-human contact.*

   Often done by an attacker who calls up someone in an organization asking them questions to learn the inner details of the organization. This information would be otherwise unavailable to the attacker through “normal” means of access.

2. *The process of teaching and convincing members of an organization of the need to adopt certain actions for the sake of security.*

   Often done by an organization through security policy and subsequent training.

Misc. Definitions

Countermeasures

An action, device, procedure, technique, or other measure that reduces the vulnerability of a computer system or network

Countermeasures designed for a specific threat and vulnerabilities involve more sophisticated techniques as well as activities traditionally perceived as security.

Summary

The challenge of keeping computers and networks secure is becoming increasingly difficult

Attacks can be launched without human intervention and infect millions of computers in a few hours

Security protects

- *The integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information*
- *The integrity and availability of computers and networks*

Assign02
slide 1 of 1

Read S&B, Chap 1

Answer Problems 1.1, 1.3 and 1.4

Special Problem 02-1:

> *The 1st part of this lecture describes several cyber attacks*
>
> *Write a ¾ to 1 page document that specifically contains the following two sections:*
>
> 1. General Observations (100±50 words)
> 2. Attack Amelioration (200±50 words)
>
>   *Discusses what can be done to ameliorate such attacks*

Submit entire Assign02 in .doc format, 12 point type single spaced lines

> *Follow the Homework Process slides from class session 01 so that you don't loose points*