PERFORMANCE TECHNOLOGIES

Securing Windows – A Monumental Task!

IIT Network Security Conference and Expo

March 2008

Michael A. Fekety

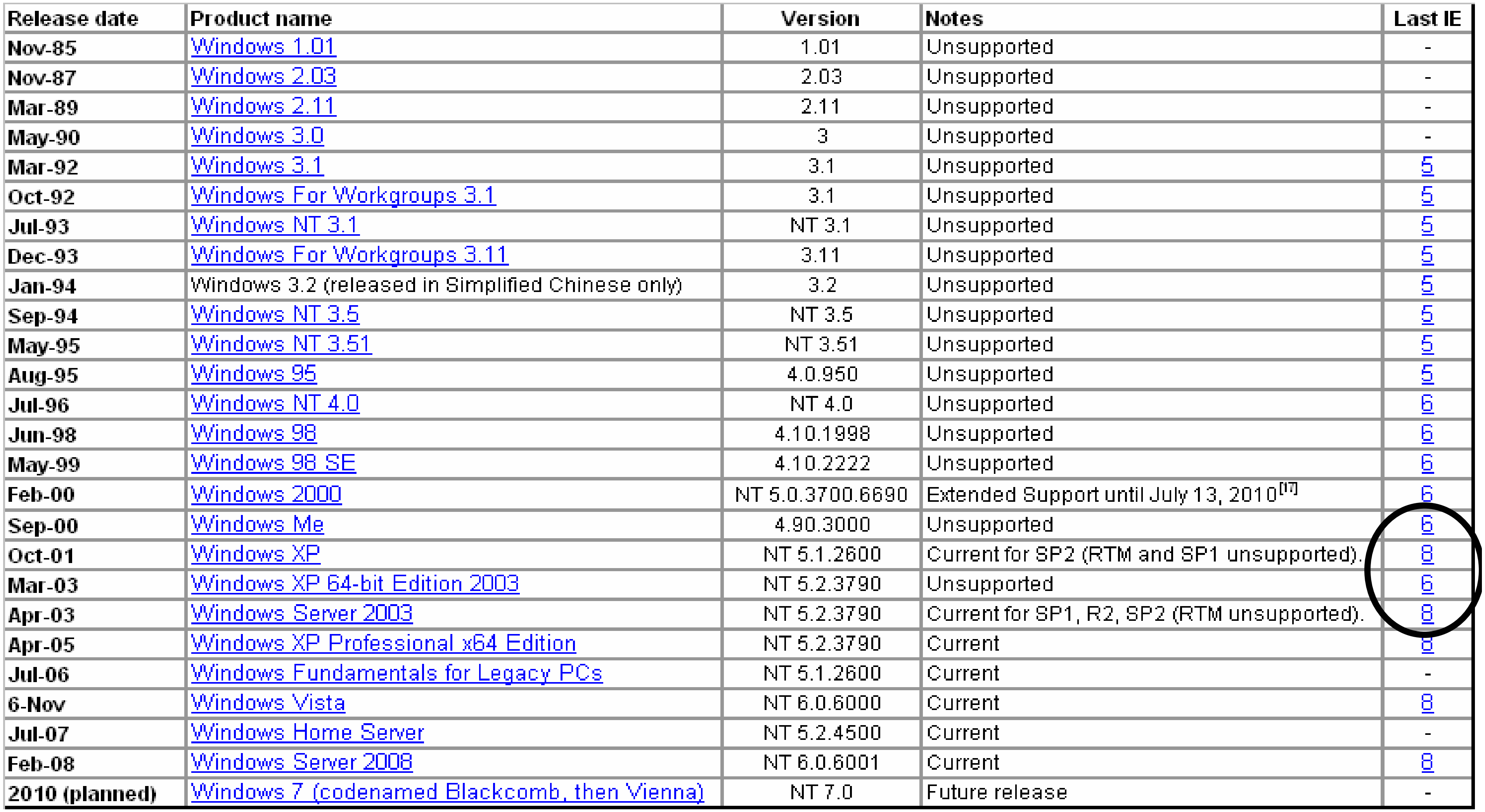
CELEBRATING 25 YEARS PERFORMANCE TECHNOLOGIES

www.pt.com

Purpose of this Presentation…..

- ◆ Provide a brief history of Windows
- ◆ Characterize the Windows market
- ◆ Compare / contrast Windows security to other OS's
- ◆ Describe Windows vulnerabilities
- ◆ Suggest ways to secure Windows
- ◆ Discuss PC-based SIP Security
- ◆ Q & A

Windows Release Schedule…..



Release date	Product name	Version	Notes	Last IE
Nov-85	Windows 1.01	1.01	Unsupported	-
Nov-87	Windows 2.03	2.03	Unsupported	-
Mar-89	Windows 2.11	2.11	Unsupported	-
May-90	Windows 3.0	3	Unsupported	-
Mar-92	Windows 3.1	3.1	Unsupported	5
Oct-92	Windows For Workgroups 3.1	3.1	Unsupported	5
Jul-93	Windows NT 3.1	NT 3.1	Unsupported	5
Dec-93	Windows For Workgroups 3.11	3.11	Unsupported	5
Jan-94	Windows 3.2 (released in Simplified Chinese only)	3.2	Unsupported	5
Sep-94	Windows NT 3.5	NT 3.5	Unsupported	5
May-95	Windows NT 3.51	NT 3.51	Unsupported	5
Aug-95	Windows 95	4.0.950	Unsupported	5
Jul-96	Windows NT 4.0	NT 4.0	Unsupported	6
Jun-98	Windows 98	4.10.1998	Unsupported	6
May-99	Windows 98 SE	4.10.2222	Unsupported	6
Feb-00	Windows 2000	NT 5.0.3700.6690	Extended Support until July 13, 2010[17]	6
Sep-00	Windows Me	4.90.3000	Unsupported	6
Oct-01	Windows XP	NT 5.1.2600	Current for SP2 (RTM and SP1 unsupported).	8
Mar-03	Windows XP 64-bit Edition 2003	NT 5.2.3790	Unsupported	6
Apr-03	Windows Server 2003	NT 5.2.3790	Current for SP1, R2, SP2 (RTM unsupported).	8
Apr-05	Windows XP Professional x64 Edition	NT 5.2.3790	Current	8
Jul-06	Windows Fundamentals for Legacy PCs	NT 5.1.2600	Current	-
6-Nov	Windows Vista	NT 6.0.6000	Current	8
Jul-07	Windows Home Server	NT 5.2.4500	Current	-
Feb-08	Windows Server 2008	NT 6.0.6001	Current	8
2010 (planned)	Windows 7 (codenamed Blackcomb, then Vienna)	NT 7.0	Future release	-

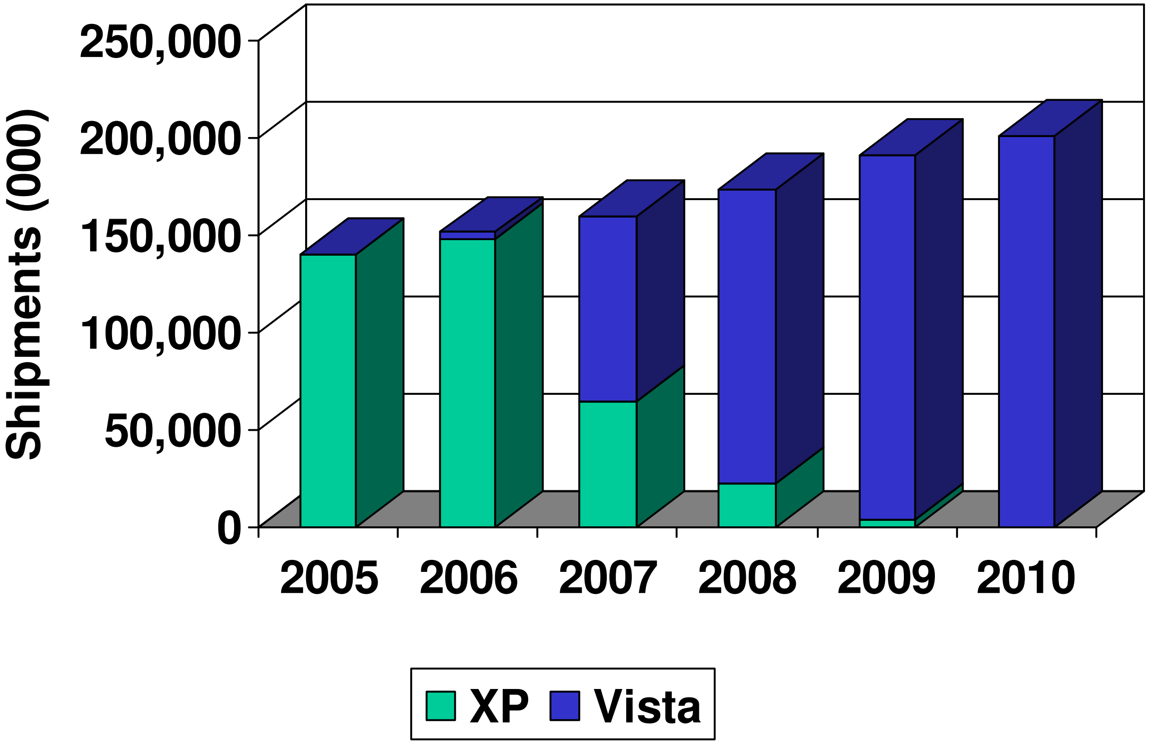
http://en.wikipedia.org/wiki/Microsoft_Windows

PERFORMANCE TECHNOLOGIES

www.pt.com

Windows Shipments…..

It is forecast there will be 1B Windows Users by Mid-2008

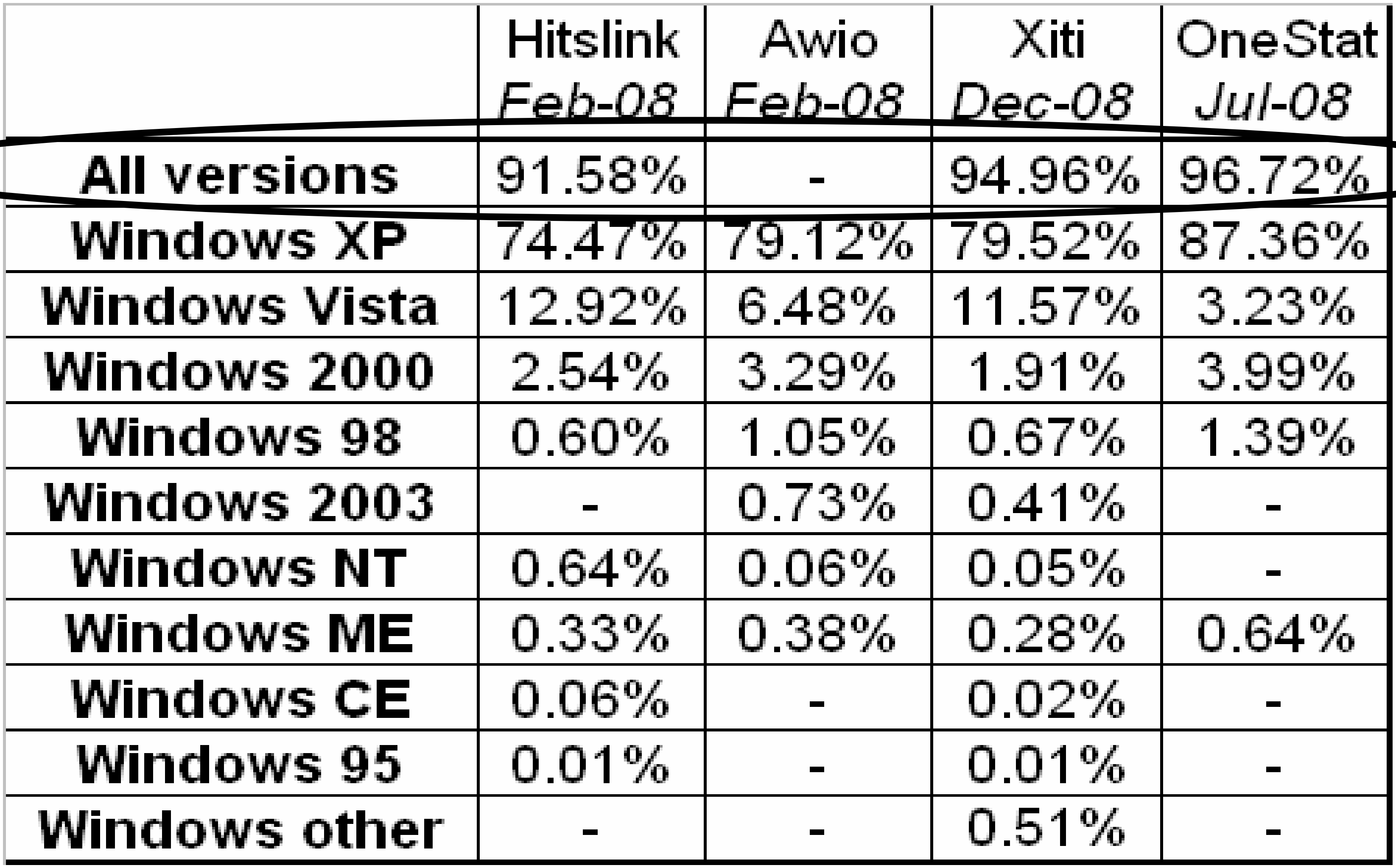


The vast majority are Windows XP

http://blogs.zdnet.com/microsoft/?p=596

http://www.microsoft.com/presspass/itanalyst/docs/IDCVistaEcoImpactDec2006.pdf

Windows Deployed Base…..

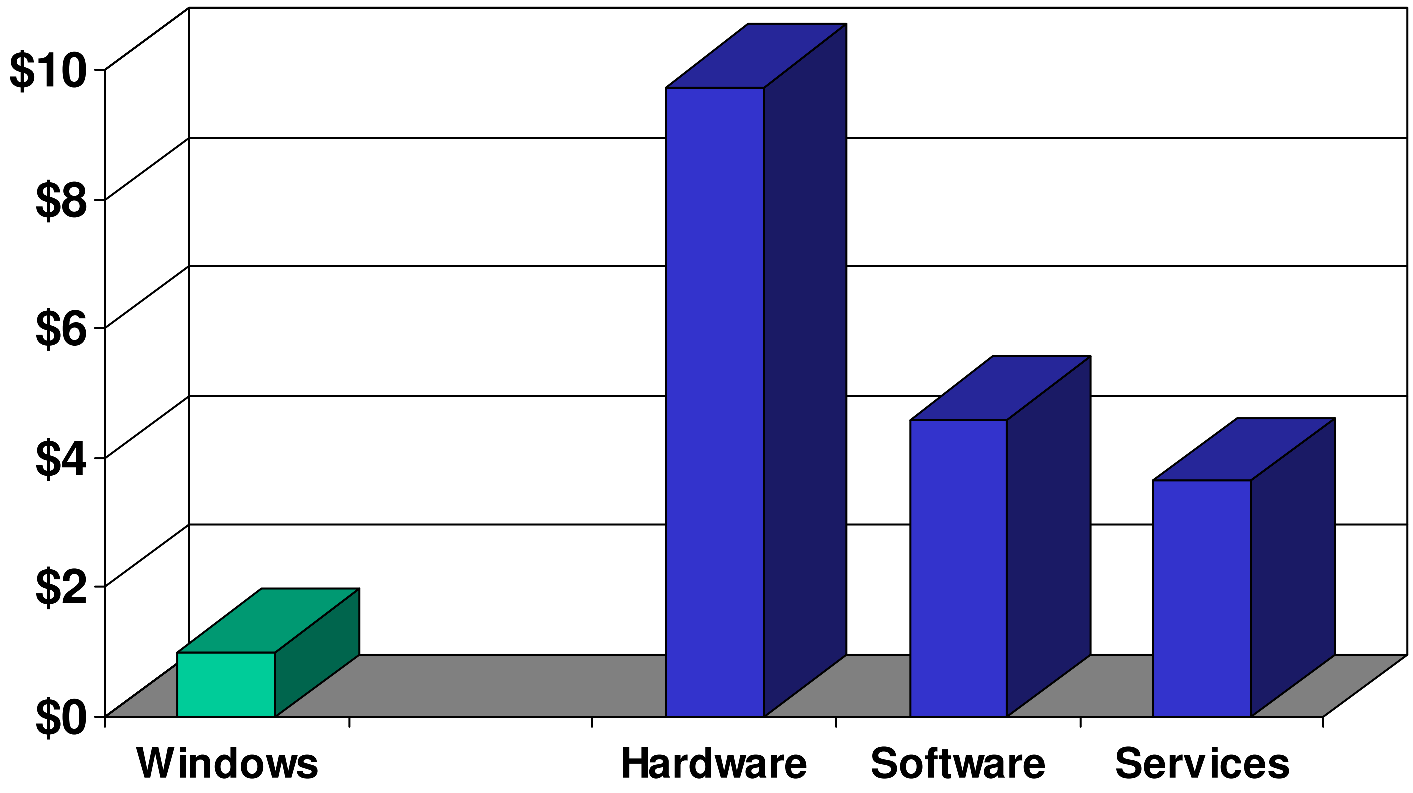


	Hitslink *Feb-08*	Awio *Feb-08*	Xiti *Dec-08*	OneStat *Jul-08*
All versions	91.58%	-	94.96%	96.72%
Windows XP	74.47%	79.12%	79.52%	87.36%
Windows Vista	12.92%	6.48%	11.57%	3.23%
Windows 2000	2.54%	3.29%	1.91%	3.99%
Windows 98	0.60%	1.05%	0.67%	1.39%
Windows 2003	-	0.73%	0.41%	-
Windows NT	0.64%	0.06%	0.05%	-
Windows ME	0.33%	0.38%	0.28%	0.64%
Windows CE	0.06%	-	0.02%	-
Windows 95	0.01%	-	0.01%	-
Windows other	-	-	0.51%	-

http://en.wikipedia.org/wiki/Microsoft_Windows

Windows Ecosystem…..

For every $1 spent on Windows there is an additional $18 spent in the Ecosystem



http://www.microsoft.com/presspass/itanalyst/docs/IDCVistaEcoImpactDec2006.pdf

Windows Statistics…..

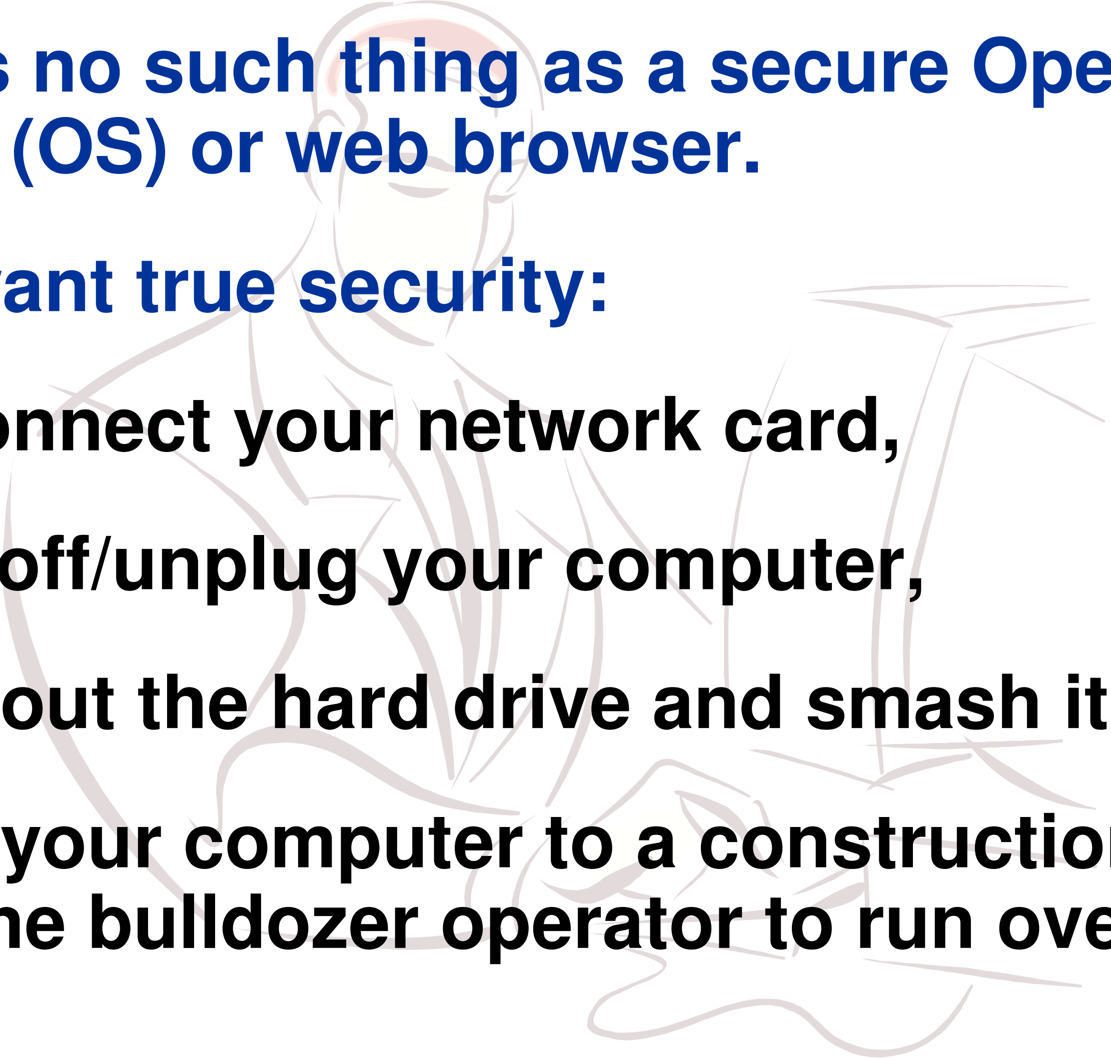
- Windows has been available 22 years
- There have been 25 versions released
- The vast majority of the world uses it
- There is a LARGE ecosystem supporting it

Why is it so hard to secure?

PERFORMANCE TECHNOLOGIES

www.pt.com

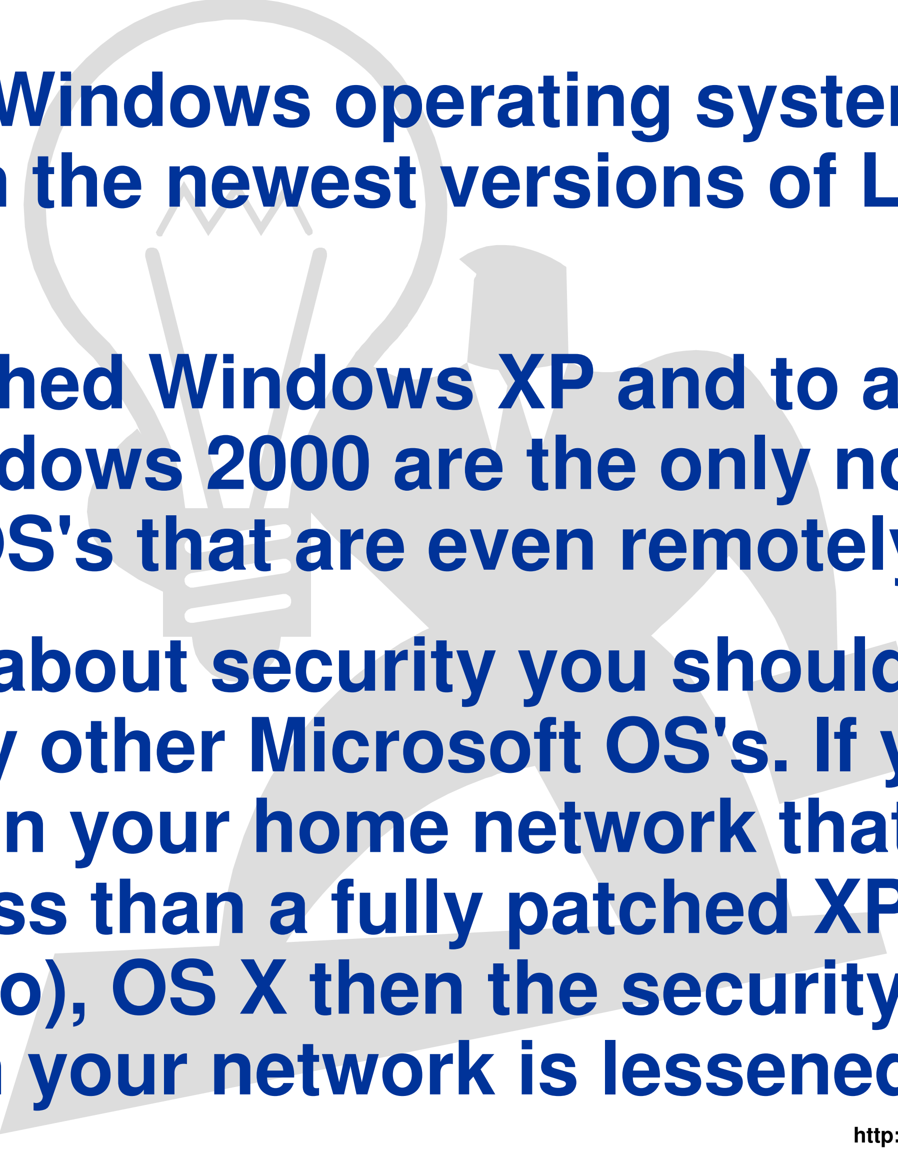
Is Your Windows-based PC Secure…..



- There is no such thing as a secure Operating System (OS) or web browser.
- If you want true security:
  - Disconnect your network card,
  - Turn off/unplug your computer,
  - Take out the hard drive and smash it to bits,
  - Take your computer to a construction site and ask the bulldozer operator to run over it.

http://tweakhound.com/xp/security/page_1.htm

What if you Want to Connect.....



- In general, Windows operating systems are less secure than the newest versions of Linux and Mac OS.
- A fully patched Windows XP and to a lesser degree Windows 2000 are the only non-server Microsoft OS's that are even remotely secure.
- If you care about security you shouldn't be running any other Microsoft OS's. If you have machines on your home network that run anything less than a fully patched XP, 2000, Linux (distro), OS X then the security of any machine on your network is lessened.

http://tweakhound.com/xp/security/page_1.htm

Definitions…..

A “port” is the doorway from which computers communicate with each other

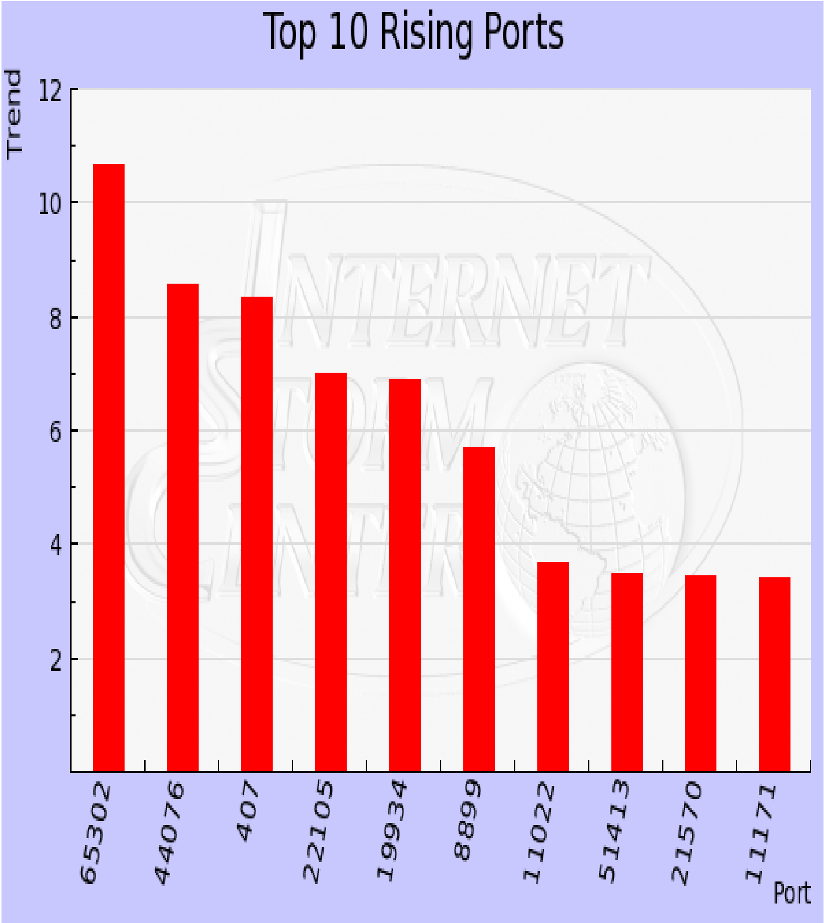
- For TCP/UDP protocols, a port is a special number present in the data packet header
- Ports are used to map data to a particular process running on a computer:
  - IP address is the “street address”
  - Port Number is the “apartment”
    - Range from 0 – 65535
      - Port 80 – HTTP
      - Port 443 – HTTPS
      - Port 5060 – SIP
  - For TCP / UDP a packet header specifies a 16-bit source and destination port
  - A “socket” consists of an IP address and TCP/UDP port

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

http://tweakhound.com/xp/security/page_1.htm

Security Threats.....

- A "port scan" takes place with programs called “port scanners”
  - Hackers use port scanners to identify open ports on your system
  - Once an open port is found there will be attempt to enter your system to collect data or place malicious programs on it
- DSHIELF.ORG tracks port scans in real time
  - Reports on attempted port scans from participating companies and individuals are sent to DShield on a real time basis
  - The number of reported entry attempts is averaging over 1.1 BILLION per month (these represent only the attacks reported)

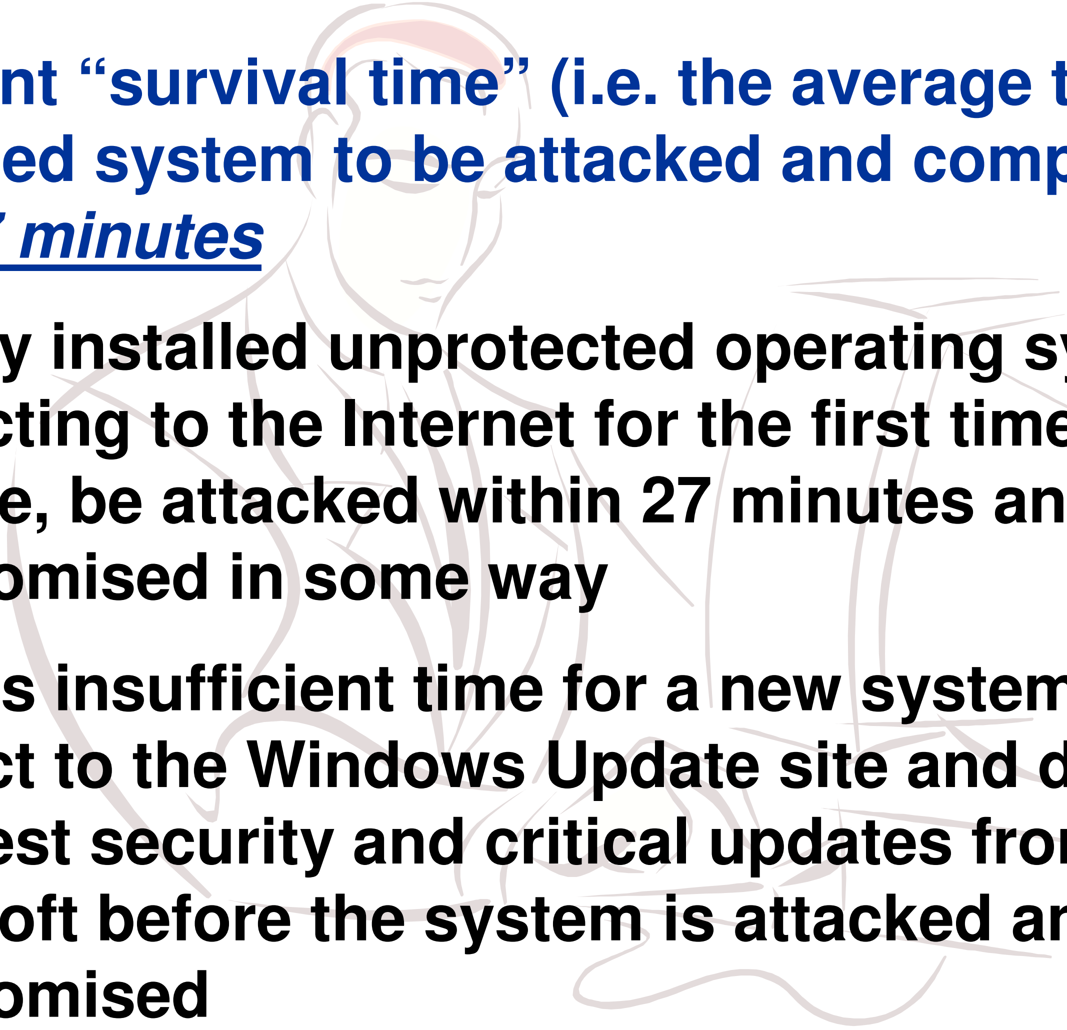


The "Trend" attempts to put a number to the increase in activity for a given port. It compares the last 24 hours to the last 30 days. If there is a rise in activity compared to the last 30 days, the trend is high.

http://www.dshield.org/trends.html

http://tweakhound.com/xp/security/page_1.htm

New Windows Version Survival Time…..



The current “survival time” (i.e. the average time for an unprotected system to be attacked and compromised) is only ***27 minutes***

- A newly installed unprotected operating system connecting to the Internet for the first time will, on average, be attacked within 27 minutes and compromised in some way
- There is insufficient time for a new system to connect to the Windows Update site and download the latest security and critical updates from Microsoft before the system is attacked and compromised

http://tweakhound.com/xp/security/page_1.htm

Windows Updates…..

In 2007 alone, Microsoft has released multiple updates for Internet Explorer:

- Cumulative Security Update for Internet Explorer (939653) (MS07-057)
- Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127) (MS07-050)
- Cumulative Security Update for Internet Explorer (937143) (MS07-045)
- Cumulative Security Update for Internet Explorer (933566) (MS07-033)
- Vulnerabilities in GDI Could Allow Remote Code Execution (925902) (MS07-017)
- Cumulative Security Update for Internet Explorer (931768) (MS07-027)
- Cumulative Security Update for Internet Explorer (928090) (MS07-016)
- Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969) (MS07-004)

Internet Explorer is by far the weakest Windows security link!

(minimally, you should be running SP2 / IE7)

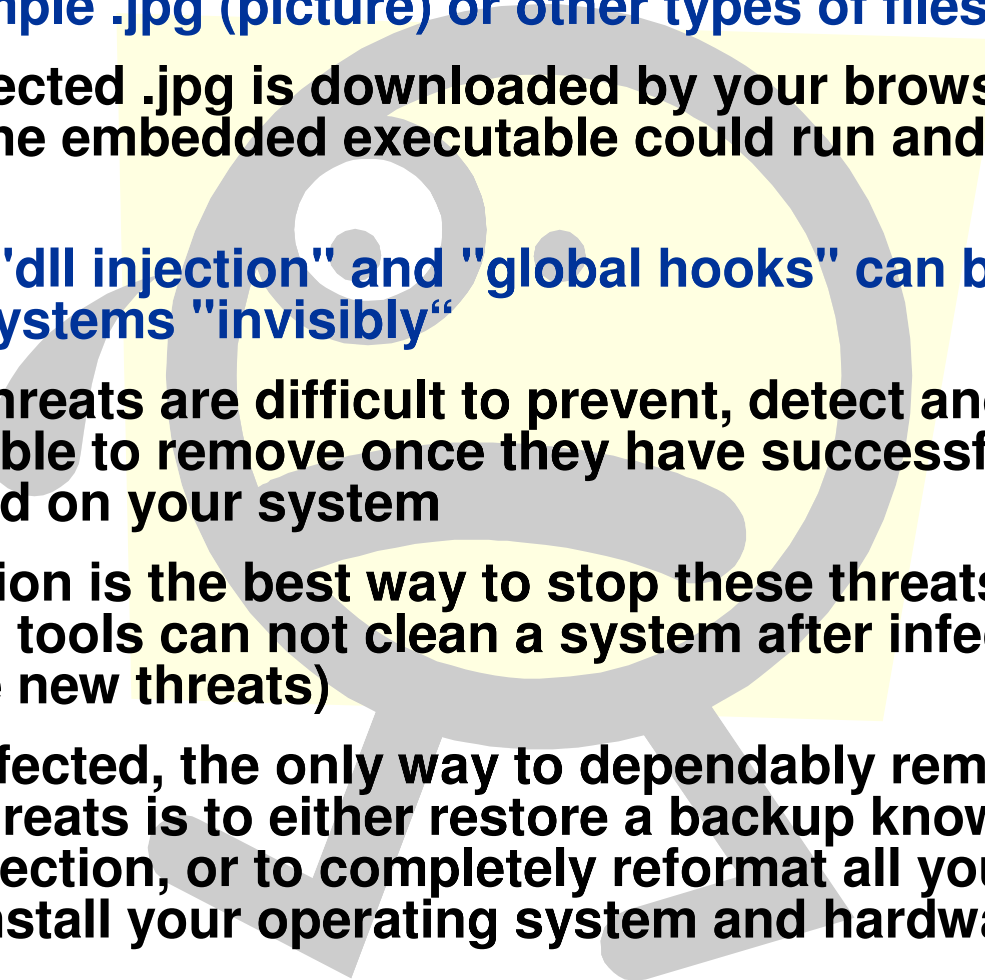
http://www.sans.org/top20/#c1

Internet Explorer…..

- If you are using Internet Explorer YOU MUST upgrade to Windows XP Service Pack 2
  - Users should upgrade to version 7 (or 8) of Internet Explorer (KB926874)
- Keep your system updated with all the latest patches and service packs by enabling AUTOMATIC UPDATES
- Prevent vulnerable ActiveX components from running inside Internet Explorer
- Many spyware programs are installed as Browser Helper Objects (a small program that runs automatically every time Internet Explorer starts and extends the browser's capabilities - Browser Helper Objects can be detected with Antispyware scanners)
- Use intrusion prevention/detection systems, anti-virus, anti-spyware and malware detection software to block malicious HTML script code
- Windows 98/ME/NT are no longer supported for updates – users should consider upgrading to Windows XP
- Consider using other browsers such as Mozilla Firefox that do not support ActiveX technology

http://www.sans.org/top20/#c1

Other Security Threats…..

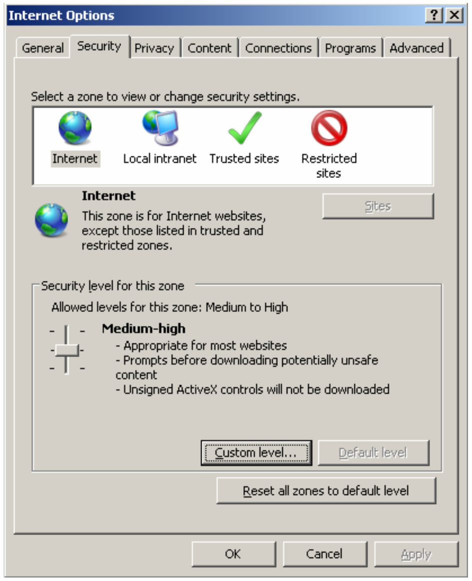


- Viruses, trojans and other executable files can be embedded within a simple .jpg (picture) or other types of files
  - If an infected .jpg is downloaded by your browser or email client, the embedded executable could run and install a Trojan or virus
- "rootkits", "dll injection" and "global hooks" can be injected and take over systems "invisibly“
  - These threats are difficult to prevent, detect and almost impossible to remove once they have successfully been deployed on your system
  - Prevention is the best way to stop these threats (many removal tools can not clean a system after infection from one of these new threats)
  - Once infected, the only way to dependably remove one of these threats is to either restore a backup known to be made prior infection, or to completely reformat all your hard drives and reinstall your operating system and hardware

http://tweakhound.com/xp/security/page_1.htm

A Quick IE Configuration Update…..

- Select “Internet Options” under the “Tools” menu
- Select “Security”, then “Custom Level” for the “Internet” zone
- Many of the flaws in IE are exploited through Active Scripting or ActiveX Controls.
- Under Scripting, select Disable for “Allow Scriptlets” to prevent content from being exposed from your clipboard. Note: Disabling Active Scripting may cause some web sites not to work properly. ActiveX Controls are not as popular but are potentially more dangerous as they allow greater access to the system.
- Select Disable for “Download unsigned ActiveX Controls”, then Disable for “Initialize and script ActiveX Controls not marked as safe”
- Java applets typically have more capabilities than ActiveX scripts, to control, under “Scripting”, Prompt for “Scripting of Java Applets” to properly sandbox the Java applet and prevent privileged access to your system.
- Ensure that no un-trusted sites are in the Trusted sites or Local intranet zones as these zones have weaker security settings than the other zones.
- *Microsoft has published a “Internet Explorer 7 Desktop Security Guide” to enhance Internet Explorer security. It examines the new features and setting that can be modified to provide a more "locked down" security configuration for Internet Explorer 7.*



Select a zone to view or change security settings.

Internet

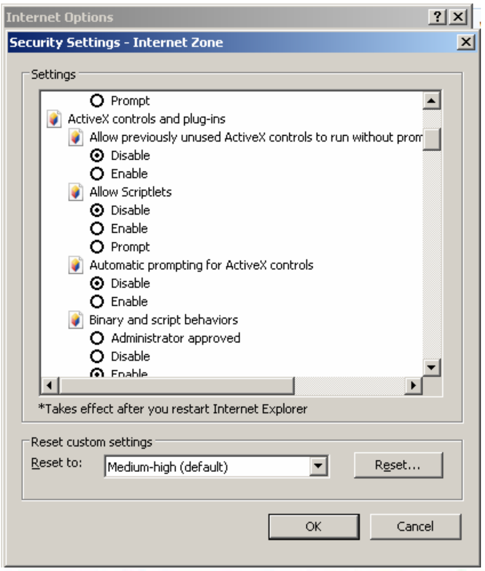
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded



Settings

○ Prompt
ActiveX controls and plug-ins
Allow previously unused ActiveX controls to run without prom
● Disable
○ Enable
Allow Scriptlets
● Disable
○ Enable
○ Prompt
Automatic prompting for ActiveX controls
● Disable
○ Enable
Binary and script behaviors
○ Administrator approved
○ Disable
● Enable

*Takes effect after you restart Internet Explorer

Reset custom settings

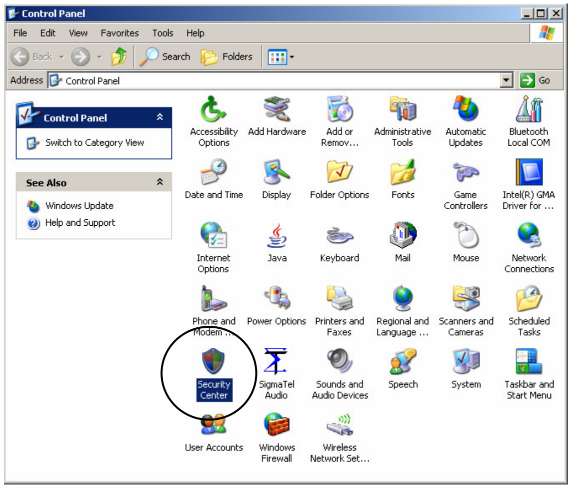
Reset to: Medium-high (default)

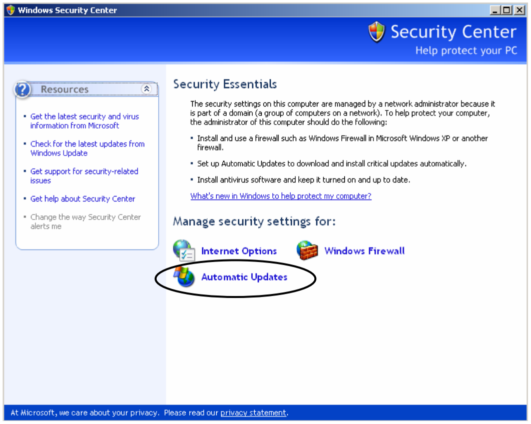
http://www.microsoft.com/downloads/details.aspx?FamilyID=6AA4C1DA-6021-468E-A8CF-AF4AFE4C84B2&displaylang=en

http://www.sans.org/top20/#c1

Security Recommendations…..

- Secure Internet Explorer
- Ensure AUTOMATIC UPDATES is ON
- Utilize a Firewall (ALWAYS)!
- Minimize the use of Softphones




Windows Security Center

Security Center
Help protect your PC

Resources

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security Essentials

The security settings on this computer are managed by a network administrator because it is part of a domain (a group of computers on a network). To help protect your computer, the administrator of this computer should do the following:

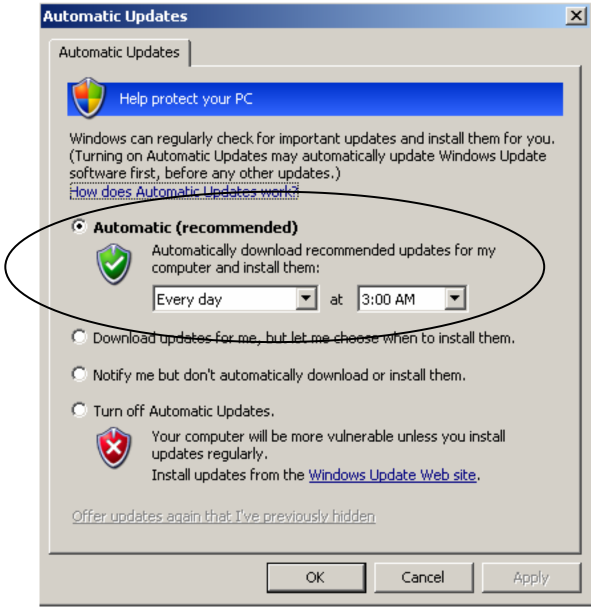
- Install and use a firewall such as Windows Firewall in Microsoft Windows XP or another firewall.
- Set up Automatic Updates to download and install critical updates automatically.
- Install antivirus software and keep it turned on and up to date.

What's new in Windows to help protect my computer?

Manage security settings for:

Internet Options
Windows Firewall
Automatic Updates

At Microsoft, we care about your privacy. Please read our privacy statement.


Automatic Updates

Automatic Updates

Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)
How does Automatic Updates work?

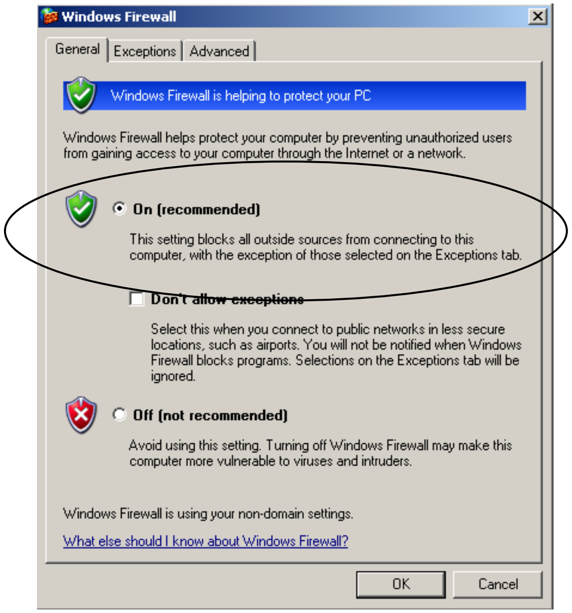
● Automatic (recommended)
Automatically download recommended updates for my computer and install them:
Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.
Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden


Windows Firewall

General | Exceptions | Advanced

Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

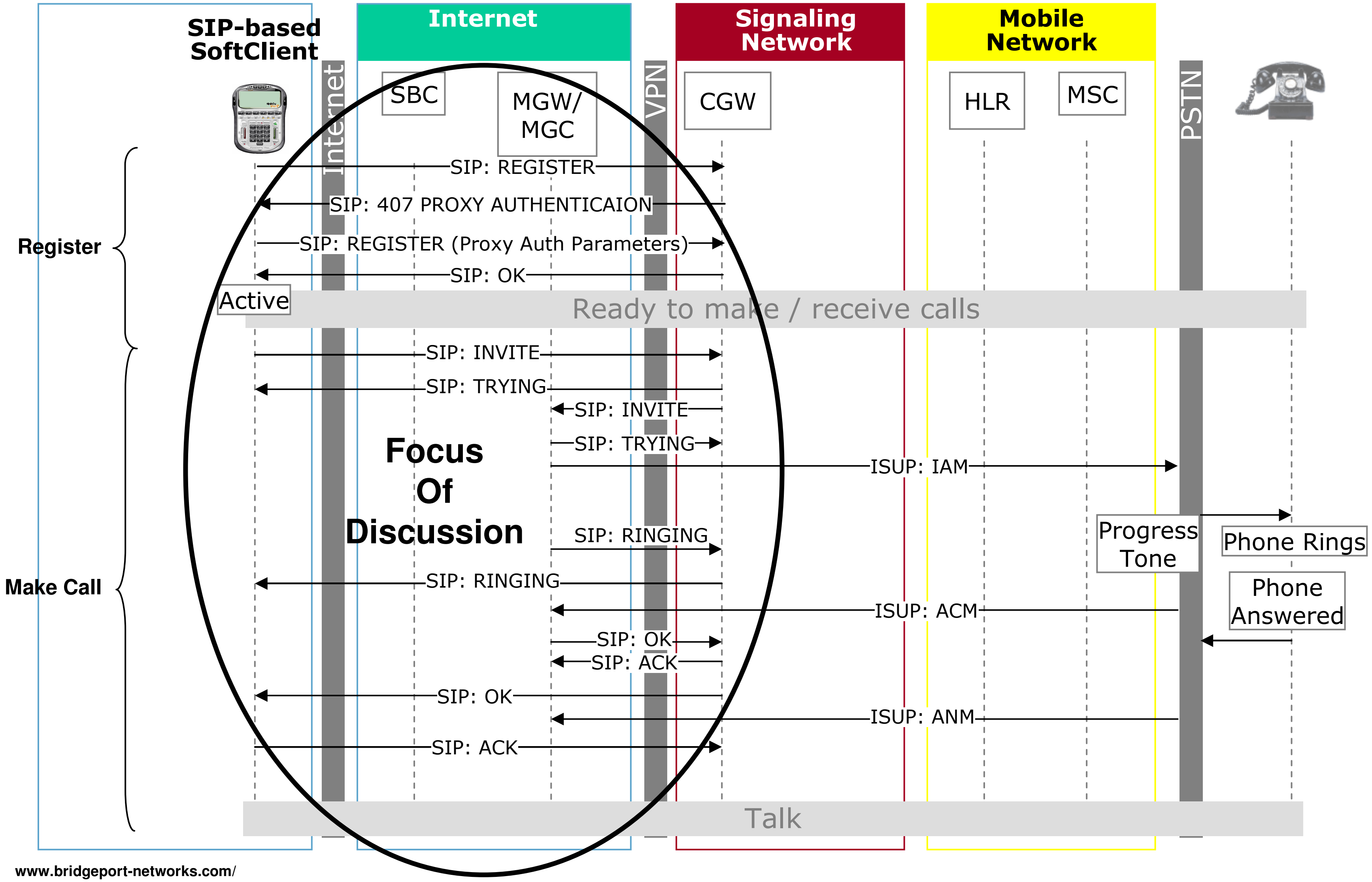
○ Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Windows Firewall is using your non-domain settings.
What else should I know about Windows Firewall?

Changing Gears…..

Windows-based SIP Security

Call Model – Ladder Diagram…..



www.bridgeport-networks.com/

VoIP Security Challenges…..

Security is breached when an individual is able to compromise a signaling packet by reading / modifying call setup information without authority to perform one or more of the following:

- Spoofing – pose as someone else,
- Repudiation – claim a call wasn't made or resources weren't utilized (instead, a spoof occurred),
- Tampering – when an individual is able to modify the SIP call flow and send sessions to rogue locations,
- Phreaking – improperly utilizing unauthorized services and charging to someone else.
- Denial of Service (DOS) – when an individual floods / bombards a server / network so service is denied to authorized users.

Why The VoIP Security Concern…..

- TDM analog and digital phones are non-intelligent – the network / PBX contains all of the intelligence
- TDM circuits are essentially a closed system
  - Devices are physically hardwired (whereas in a VoIP system devices are virtual and can be moved anywhere)
- In VoIP systems the calling SIP device has lots of intelligence
  - Softphones are no more secure than any other PC application (and can access the network via wireline or wireless)
- As a result – VoIP has opened voice devices to more security problems and attacks than encountered in TDM-based environments

Spoofing – Example…..

VoIP hackers gut Caller ID - Numbers spoofed, ID blocking cracked

By Kevin Polsen

VoIP networks, currently outside FCC regulation, place those capabilities in the hands of ordinary netizens. In a telephone interview with SecurityFocus, 21-year-old phone hacker "Lucky 225" ***demonstrated how he could spoof his Caller ID*** to appear to be phoning from the reporter's office. In another demonstration, the reporter phoned Lucky's associate "Natas" from a residential phone ***with Caller ID blocked. Natas was able to rattle off the unlisted phone number***.

As described by Lucky, much Caller ID chicanery can be accomplished by taking advantage of implementation quirks in Voice over IP networks that try, but fail, to implement Caller ID properly. "There are little exploits that you can do," says Lucky. But ***the most powerful tool for manipulating and accessing CPN data is the open-source Linux-based PBX software Asterisk, used in combination with a permissive VoIP provider***. "It's fully configurable, you can pretty much do anything you want with it," says Lucky. "That's why Voice over IP is changing things.“

Natas used Asterisk in conjunction with the XXXXXX Network for his demonstration of Caller ID unmasking

SIP Proxies / Gateways Need Time to Mature!

http://www.theregister.co.uk/2004/07/07/hackers_gut_voip/

Spoofing – Services Available…..

Rates

Enjoy low rates for all calls with XXXXXXXXX. There are never any hidden costs or monthly fees with XXXXXXXXX! All rates include toll free access, web based access, optional call recording, and customer service support. When you're low on minutes, simply login to XXXXXXXXX.com to recharge your card!

60 Minutes of Talk Time	$10.00	Buy Now
120 Minutes of Talk Time	$20.00	Buy Now
240 Minutes of Talk Time	$40.00	Buy Now
480 Minutes of Talk Time	$80.00	Buy Now

Our service is intended for business professionals within the U.S. including, but not limited to: Private Investigators, Skip Tracers, Law Enforcement and Lawyers, giving them freedom to choose any number as the Caller ID. XXXXXXXXX allows you to be whoever you want to be.

Repudiation – Point to Ponder…..

Definition – "*Refuse to acknowledge, ratify or recognize as valid*"

What Happens When Someone Repudiates a Claim They Made a Call (there is not a lot of legal background)? Are the VoIP Networks Secure / Auditable Enough to Prove Who Made the Call in a Court of Law?

http://www.wordwebonline.com/en/REPUDIATE

Ramifications of Spoofing / Repudiation…..

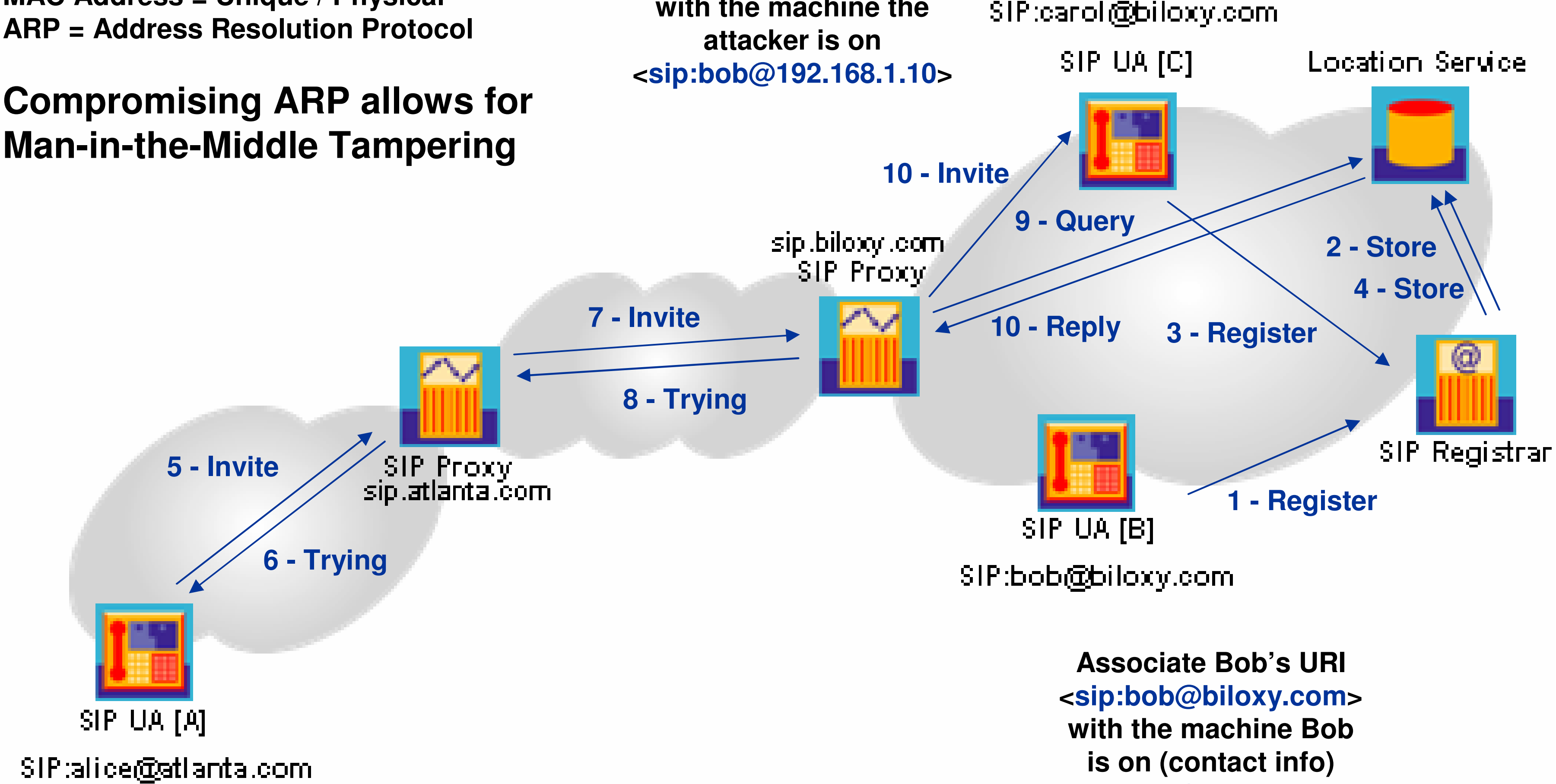
- **Fraud – Falsely identifying oneself to:**
  - ❑ Companies that utilize Caller ID (e.g. credit card companies, banks, ticket brokers, etc.) – for personal or financial gain
  - ❑ A business, law enforcement agency, etc – to gather information
  - ❑ Friends / Enemies / …. for some devious reason
  - ❑ Commit a crime in general
- **Repudiation – How do Law Enforcement agencies prove who did what?**

Tampering – Example…..

IP Address = Logical
MAC Address = Unique / Physical
ARP = Address Resolution Protocol

Compromising ARP allows for Man-in-the-Middle Tampering

Re-associate Bob’s URI <sip:bob@biloxy.com> with the machine the attacker is on <sip:bob@192.168.1.10>



Associate Bob’s URI <sip:bob@biloxy.com> with the machine Bob is on (contact info) <sip:bob@192.168.1.5>

http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt#86

http://www.intoto.com/product_briefs/Converged%20Network%20Security%20White%20Paper%20061405.pdf

Phreaking – Example…..

Security Threats In VoIP

By Nadeem Unuth

Service theft can be exemplified by phreaking, which is ***a type of hacking that steals service from a service provider***, or use service while passing the cost to another person. ***Encryption is not very common in SIP, which controls authentication over VoIP calls, so user credentials are vulnerable to theft.***

Eavesdropping is how most hackers steal credentials and other information. Through eavesdropping, a third party can obtain names, password and phone numbers, allowing them to gain control over voicemail, calling plan, call forwarding and billing information. ***This subsequently leads to service theft***.

A phreaker can change calling plans and packages and add more credit or make calls using the victim's account. He can of course as well access confidential elements like voice mail, do personal things like change a call forwarding number.

Use of Encryption Needs to Increase!

http://voip.about.com/od/security/a/SecuThreats.htm

Phreaking – Ramification…..

VoIP phreakers establish thriving black market

By John Levden

Telephone systems hackers have established a thriving black market in reselling stolen VoIP minutes.

Hackers are breaking into gateway servers used to connect a carrier's phone network to the internet and reselling this access to smaller, unscrupulous operators, sometimes via web-based wholesale minutes markets. Wholesale purchasers of the purloined access are often small telco operations who resell access to ordinary punters via printed phone cards.

These telephone ***phreakers steal 200m minutes a month, worth $26m***, estimates New York telecom firm Stealth Communications. Telecoms fraud is a well known, if under-reported problem, that pre-dates the internet by years. It is a multimillion-dollar business, with ***estimates of direct damages resulting from fraud varying from $35bn to $40bn a year.***

VoIP Utilization Will Continue to Increase!

http://www.theregister.co.uk/2007/03/22/voip_fraud/

Denial of Service (DoS) Attack…..

How VoIP is changing the network security equation

By – Philip Bednarz

VoIP denial of service attacks are of two kinds: ones that ***exploit software bugs*** to bring down routers and servers and those caused by a ***distributed bandwidth attack.***

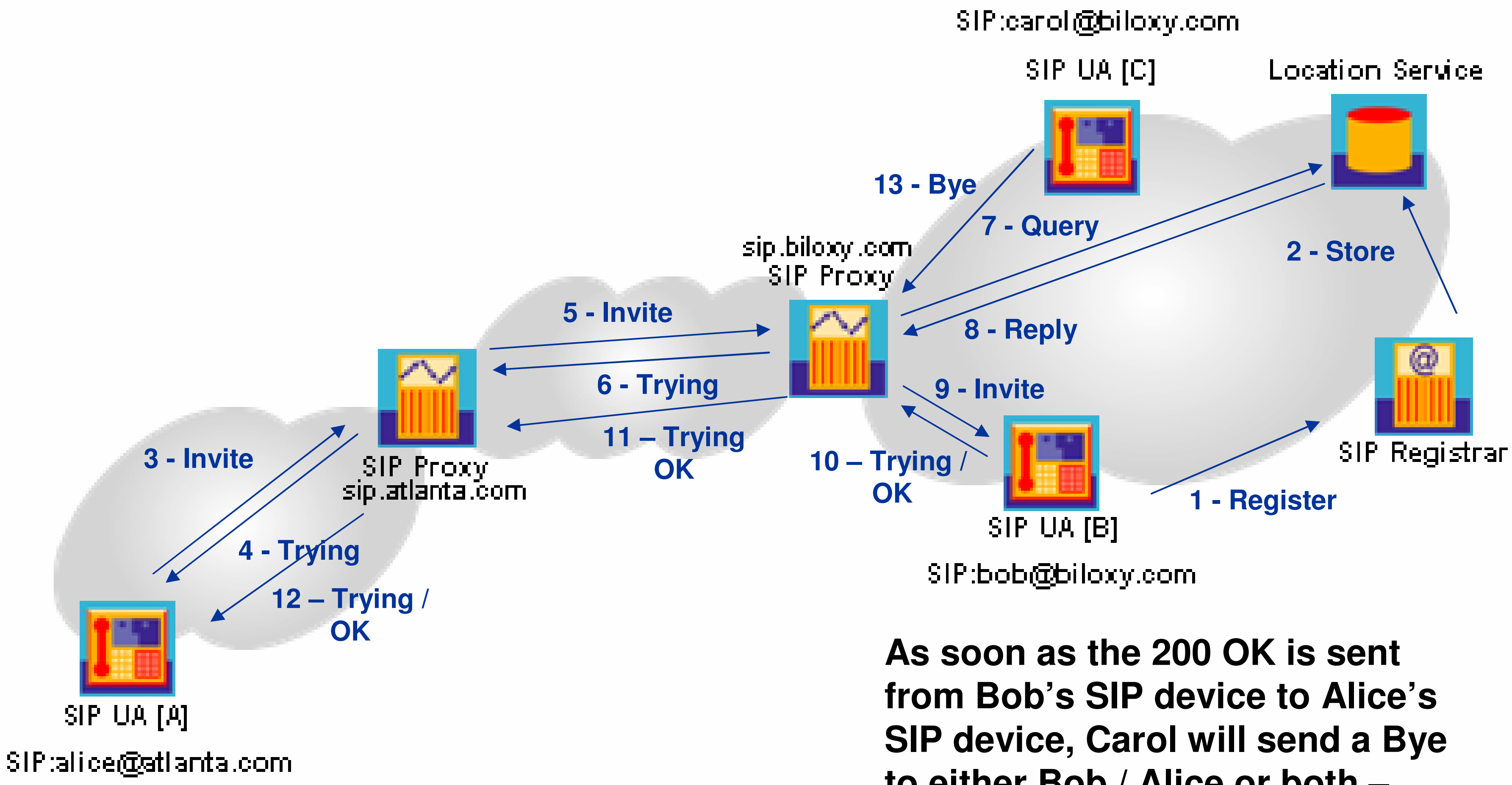
In one scenario for a distributed denial of service (DDoS) attack, the hacker prepares a number of unwitting hosts in advance of the actual attack. A "sniffing" program roams the network looking for poorly protected and hence vulnerable hosts.

A very desirable host would be a computer with a high bandwidth connection to the Internet such as a home PC connected via a cable modem. When a likely host is found the program installs software sometimes referred to as a "bot." The bot, once installed, logs on to a clandestine chat server account, posts its identity and awaits instructions from a master. The master attack program sends a message to all its compromised hosts' bots to send a barrage of traffic directed at a specific victim.

A great deal of work still needs to be done in this area. The most effective means are ***filtering programs that are installed at Internet service providers' servers*** that look for suspicious packets and block them before they reach the victim.

http://www.eetimes.com/story/OEG20021014S0072

Denial of Service Attack – Example…..



As soon as the 200 OK is sent from Bob's SIP device to Alice's SIP device, Carol will send a Bye to either Bob / Alice or both – preventing service

http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt#81

Security Recommendations…..

- Utilize Intrusion Detection Systems to monitor internal traffic
- Minimize the use of Softphones
- Put a firewall in front of your SIP Server – lock down administrative interface IP / MAC addresses
- Encrypt your voice payload and signaling (no defacto standard yet – nor for keys)
  - S-RTP (payload)
  - S-SIP (signaling)
  - Transport Layer Security (TLS) (signaling / configuration)
  - IP-SEC (tunneling versus transport)
- Plan for the day of a DoS attack by designing redundancy into the network

S-RTP		
RTP	RTCP	TLS
Unreliable / UDP		Reliable / TCP
Network / IP, Network Security / IPSec		
Link Layer		
Physical Layer		

http://www.voiplowdown.com/2007/voip-security-challenges-25-ways-to-secure-your-voip-network/

Where Can You Go For Help…..

There are two sites that discuss the software security threats to the data functions. These sites now include information on VoIP vulnerabilities. Both sites are funded by the federal Homeland Security Administration:

http://cve.mitre.org/

http://nvd.nist.gov/

Concluding Thoughts…..

Are there any security concerns???

Can they be handled adequately???

Will implementation be easy???

What are your next steps???

Performance Technologies - Our Business

- Performance Technologies develops communication solutions for network equipment developers and defense / aerospace integrators worldwide

- Markets served:
  - Telecommunications
  - Defense and Homeland Security
  - Commercial

Questions?

(Thank You)

Mike Fekety
Sales Director
Performance Technologies Inc
630-430-2843 (Cell)