

Corporate and Personal Information Protection

...at the PC level

Given to DB Professionals, Inc. on February 22nd 2003
By Patrick Miller, CISSP SSCP TCP

Overview

- Who am I, and why am I an expert on Information Security?
- FUD (Fear Uncertainty and Doubt) slides, a.k.a. scary stuff to motivate you
- Real dangers
- How they do it – hacker/fraud tactics
- Protection 101
 - Software
 - Hardware
 - Humans
- Self-tests and Resources
- ID theft tips
- Demonstrations – if time permits

Interaction

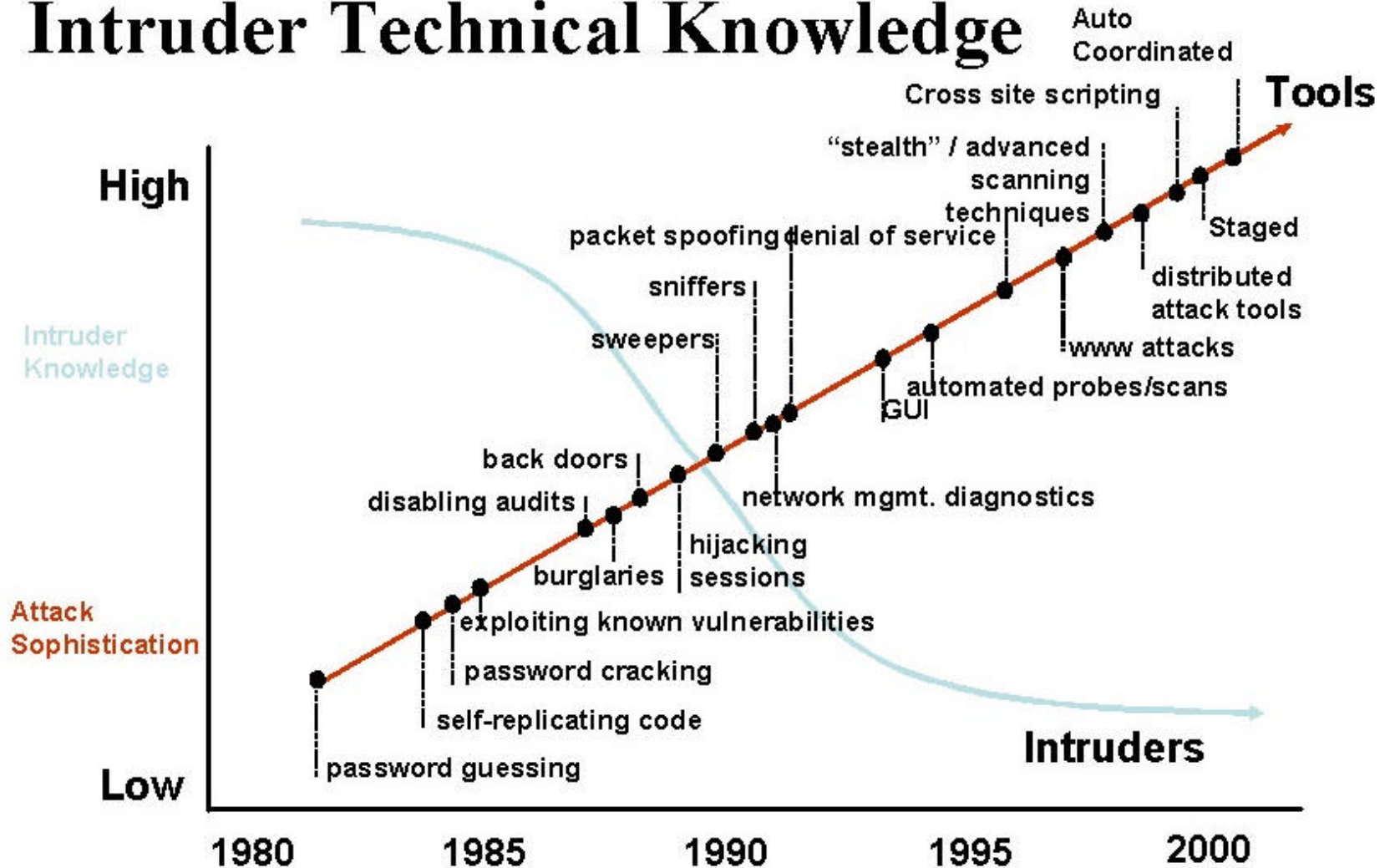
- Please ask questions as we go, others may benefit from your query
- No such thing as a stupid question – this is a complicated subject
- Let's *try* to stay on-topic, but side discussions are welcome

The Current Situation

- Hackers (and terrorists, etc.) are actively looking for vulnerable systems to use
- Point-and-click tools for scanning and hacking systems are freely available on the Internet
- Importance/Herd Factor misconception (there is no safety in numbers – automated scans will find you)
- New systems connected to the Internet will be scanned and potentially hacked within 15 minutes
- The “Honeynet Project” and other coordinated efforts

Attack Sophistication vs. Intruder Technical Knowledge

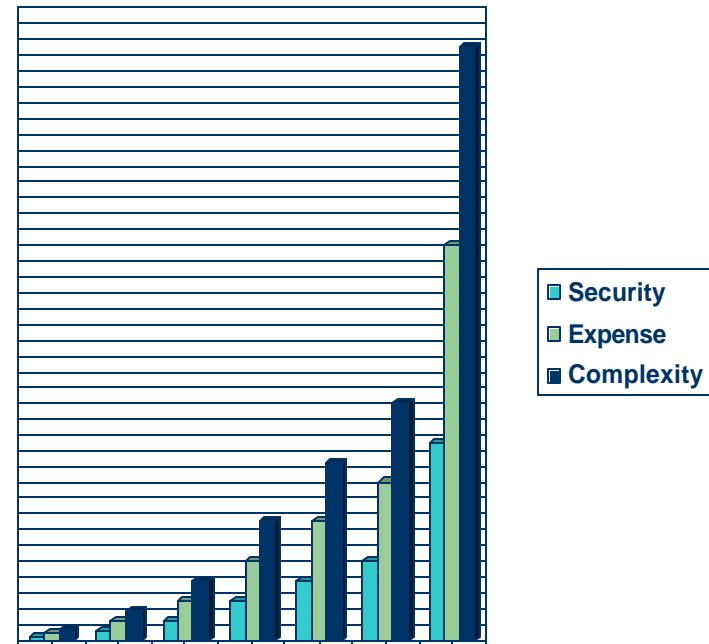
Source: Carnegie Mellon



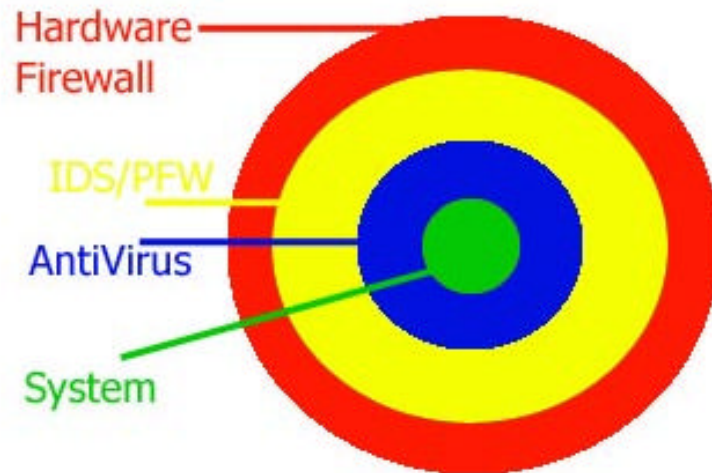
Security vs. Reality

- No “Silver Bullet”
- Requires constant vigilance
- Nothing is truly “Secure”
- Insider damage is much worse than outsider damage
- Security is not obscurity
- Tradeoff of functionality
- More security = higher cost at a higher level of complexity

- You don’t have to “outrun the bear”



The Ring/Fortress Model



- Think of walls around a fortress or castle
- Other models are “the organism” or “holistic”
- Never put an unprotected system on the Internet – you are an incident waiting to happen
- Not protecting systems appropriately may become a crime - DHS

Real Dangers - Corporate

- Direct or indirect leakage of confidential or proprietary information
- Loss or corruption of data
- Internal launch point for external hacks
- Eavesdropping or “sniffing” credentials
- Denial of service (DoS and DDoS)
- Shareholder perspectives are fragile

Real Dangers - Personal

- ID Theft - #1 crime
- Loss of time while cleaning up credit situation
- Loss of time while cleaning up bank and Internet accounts
- Loss of time while cleaning/rebuilding affected personal systems
- Loss of job if found to be the source of a corporate security breach
- Criminal treatment and investigation for crimes committed from your systems or network space

How They Do It - The Web

- Rule of thumb: don't click on it if you don't have to...
 - Use the “Stop” button in your browser instead
- Pop-Ups
 - Clock isn't accurate?
 - Exposing IP address?
 - Color isn't right?
- Cookies
 - Account harvesting
 - So called “customization” features or required cookies
- Cross Site Scripting
 - Malicious or otherwise unauthorized scripts that run within the context of the “Trusted” site
- Redirects
 - Form submission that goes to more than the intended recipient
- Rogue Web Servers
 - IE and Windows are hooked very deeply together

How They Do It - Email

- Outlook and Outlook Express
 - The dreaded “preview” window exploit
 - OE is not as secure as Outlook – don’t use it
 - Patch it, but expect problems anyway, it’s Microsoft...
- Web-based email
 - Easy way to send scripts
 - Easy to break into
- HTML email vs. Text
 - Text-based has no web content – much safer
- Pay attention to the file type!!!
 - Executables (.exe, .com, .bat)
 - VB Script (.vbs)
 - Zip files (.zip)

How They Do It - Spyware

- Many “Shareware” or “Adware” installations are fronts for “Spyware”
 - Gator, Real Networks, Game demos are some of the worst
- Always do the “Custom” installation
 - Uncheck (disable) any function that looks suspicious
 - Uncheck (disable) any additional software
- Spyware can have issues other than privacy
- Look for new icons in your system tray or Programs folder that are different from the software you intended to install
- Examine your Add/Remove Programs
- Keep an eye on your “Program Files” folder

Protection 101 - Software

- Windows settings best practices
- Vendor Patches
- Anti-Virus
- Personal Firewall
- HIDS (Host-Based Intrusion Detection Systems)
- Encryption
- History killers, Anonymizers, etc...

Windows Settings

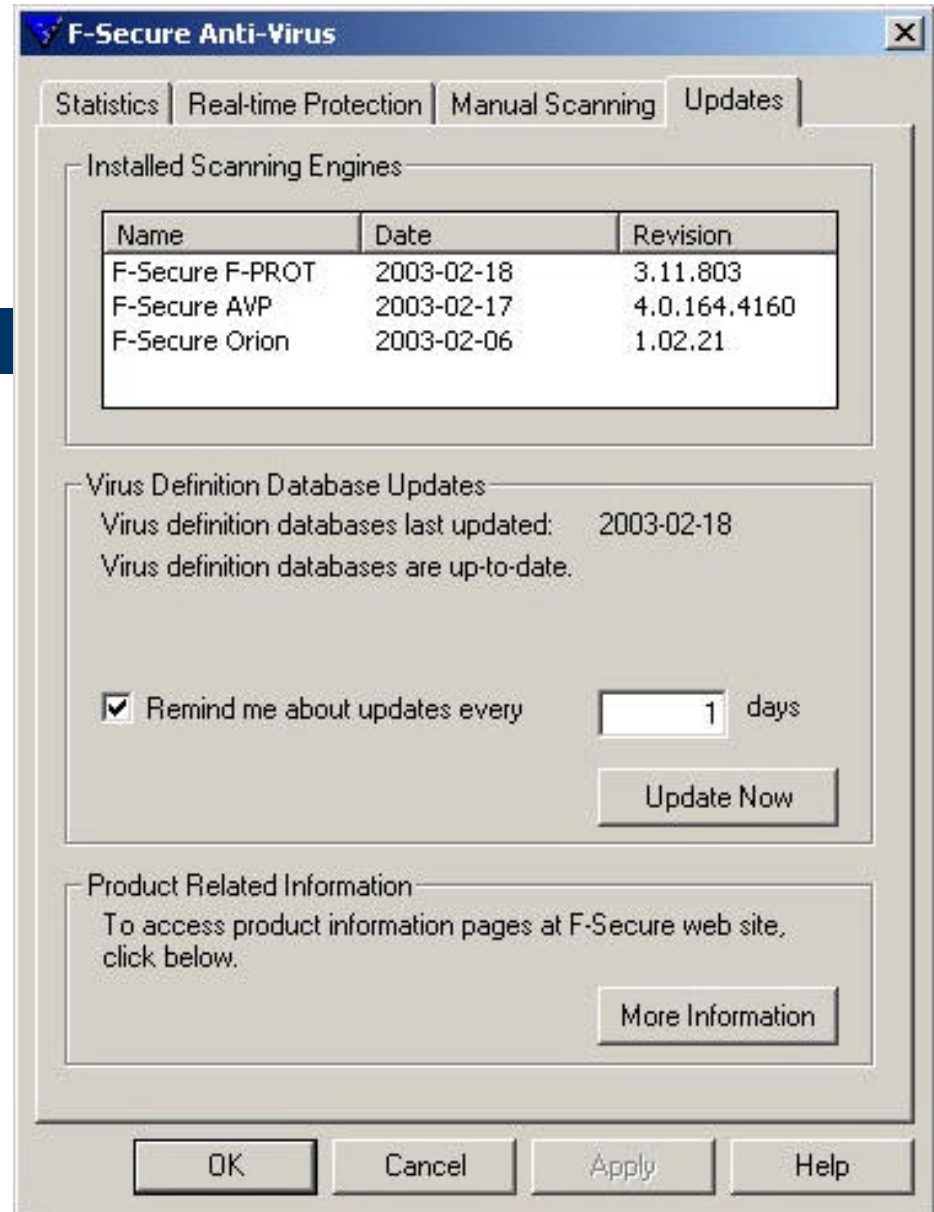
- Accounts and Passwords
 - Different accounts for different users
 - Rename the Administrator and Guest accounts
 - Disable Guest account
 - Don't do everything as "Administrator"
 - Trojans, viruses, scripts, sniffers/keyloggers
 - Audit and recovery is much easier
 - Use STRONG passwords!
 - Create an easy to remember system
 - L33+ #@x0R
 - The "Hand" model: Upper, Lower, Special, Numbers, Length
- The Windows "Local Administrator" hole
 - Use different passwords for the Administrator account on different systems
- Secure-build document – write it all down!

Vendor Patches

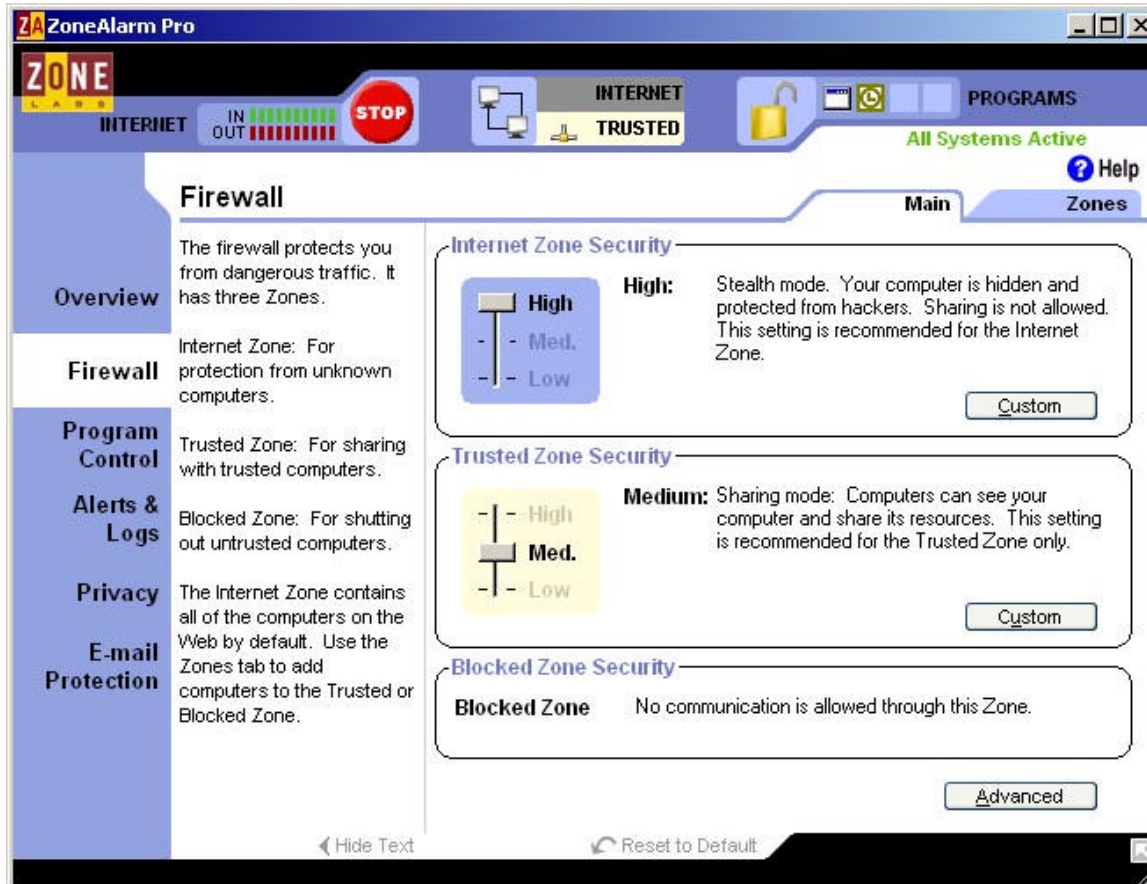
- Check all vendor sites for new patches, especially Microsoft
- Pay particular attention to software that touches the network – especially if you use any Remote Administration utilities (pcAnywhere, etc)
- Don't forget firmware or flash updates
- Most common reason for virus outbreaks
- Can cause new issues or break software
- **Backup all critical files before applying patch**

Anti-Virus

- Enabled (running)
- Real-time scans
- Manual scans
- Regular updates
- Try to disinfect - delete if necessary



Personal Firewall - ZoneAlarm



Personal Firewall - ZoneAlarm

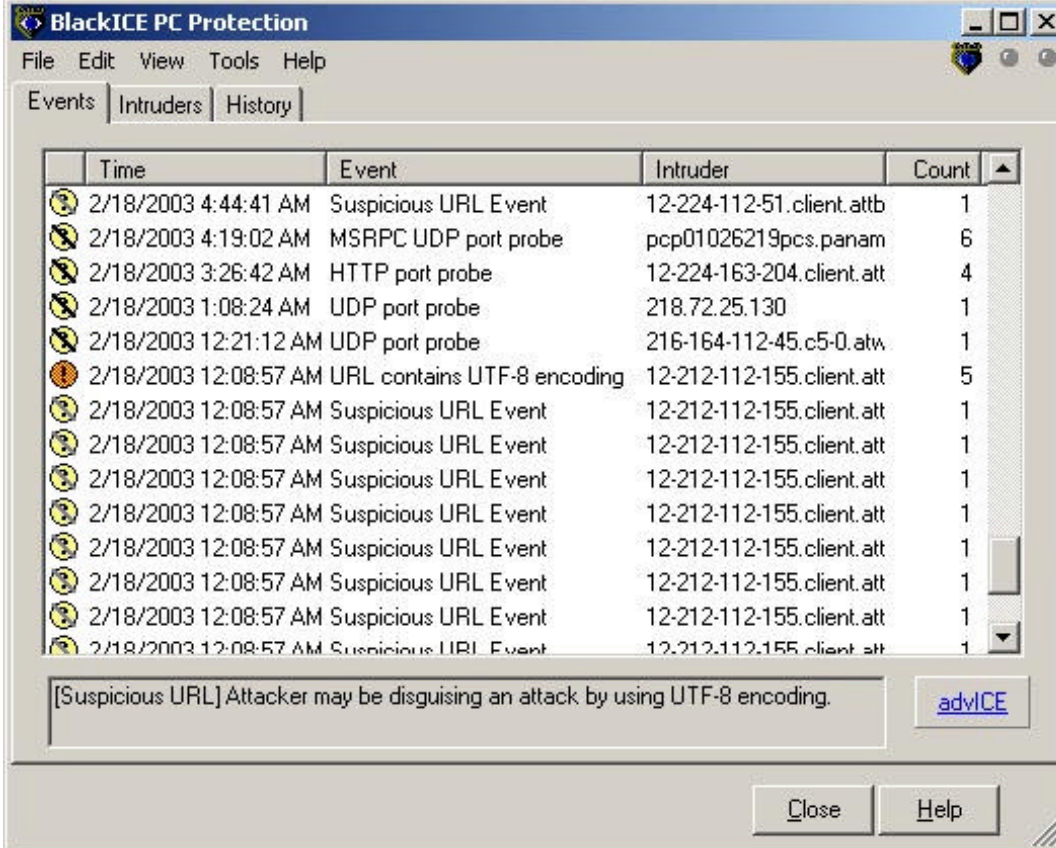
Pros:

- Blocks both inbound and outbound traffic
- Pop-up killer
- Cookie filter
- Email attachment filter
- Tracking (attack source detection)

Cons:

- Can be very “noisy”
- Steep learning curve
- Large installation base, due to the free ZA product line
- Many viruses/trojans target ZA

H.I.D.S. and Firewall – Black ICE



The screenshot shows the BlackICE PC Protection interface. The window title is "BlackICE PC Protection" and it has a menu bar with "File", "Edit", "View", "Tools", and "Help". Below the menu bar are three tabs: "Events", "Intruders", and "History". The "Events" tab is active, displaying a table of intrusion events.

	Time	Event	Intruder	Count
?	2/18/2003 4:44:41 AM	Suspicious URL Event	12-224-112-51.client.atb	1
X	2/18/2003 4:19:02 AM	MSRPC UDP port probe	pcp01026219pcs.panam	6
X	2/18/2003 3:26:42 AM	HTTP port probe	12-224-163-204.client.att	4
X	2/18/2003 1:08:24 AM	UDP port probe	218.72.25.130	1
X	2/18/2003 12:21:12 AM	UDP port probe	216-164-112-45.c5-0.atw	1
!	2/18/2003 12:08:57 AM	URL contains UTF-8 encoding	12-212-112-155.client.att	5
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
?	2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1

Below the table, there is a message box: "[Suspicious URL] Attacker may be disguising an attack by using UTF-8 encoding." with a blue "advICE" button. At the bottom right, there are "Close" and "Help" buttons.

H.I.D.S. and Firewall – Black ICE

Pros:

- HIDS and Firewall working together
- Detailed advice with support group
- Easy configuration
- Very small footprint
- Attack source detection
- Robert Graham

Cons:

- Only blocks inbound traffic by default
- Application protection is “noisy” – requires skill
- Requires add-on (ClearICE) to make sense of the logs

Hybrids vs. Stand-alone

- Security through layers is best
- Multiple stand-alone packages are best, but they are harder to manage overall
- Personal Firewall and Content Filtering (ZA)
- Personal Firewall and IDS (BlackICE)
- Personal Firewall and Antivirus (McAfee)
- All-in-one packages (Symantec)

Encryption Tools

- Password Safes (Counterpane)
 - Store all passwords in one safe location accessed by a single password
 - Hold multiple safes in one application
- File encryption (ACrypt, PGP)
 - Encrypt specific files
 - Encrypt entire drives or partitions
- Email encryption (PGP)
 - Encrypt content attached to email
 - Encrypt entire email - text and all

Other Software

- History Killers
- Anonymizers
- Cookie Crushers
- Spam Filters
- Content and URL Filters

- ***Watch out for security “snake-oil”***

Protection 101 - Hardware

- Routers
- Firewalls
- VPN (Virtual Private Network)
- Wired vs. Wireless
 - Telephones
 - LANs/Ethernet
- Old Hardware

Routers and Firewalls

- Routers only control traffic between networks
 - Control is typically based on IP address
 - Level of sophistication is relatively low
- Firewalls actually inspect the content and state of the traffic
 - Control is down to the port/protocol level
 - Can filter content such as scripts
 - High degree of sophistication

BlackICE behind a hardware firewall

Inside

The screenshot shows the BlackICE PC Protection interface with the 'Events' tab selected. The table below lists the events recorded from the inside of the firewall.

Time	Event	Intruder	Count
2/13/2003 10:15:12 AM	BlackICE detection started	0.0.0.0	1
2/13/2003 10:13:15 AM	BlackICE detection stopped	0.0.0.0	1
1/24/2003 1:15:48 PM	HTTP attack	164.109.92.167	1

At the bottom of the window, a status bar displays: [Unauthorized Access] Suspicious traffic seen [advICE](#)

Outside

The screenshot shows the BlackICE PC Protection interface with the 'Events' tab selected. The table below lists the events recorded from the outside of the firewall.

Time	Event	Intruder	Count
2/18/2003 4:44:41 AM	Suspicious URL Event	12-224-112-51.client.atlb	1
2/18/2003 4:19:02 AM	MSRPC UDP port probe	pcp01026219pcs.panam	6
2/18/2003 3:26:42 AM	HTTP port probe	12-224-163-204.client.att	4
2/18/2003 1:08:24 AM	UDP port probe	218.72.25.130	1
2/18/2003 12:21:12 AM	UDP port probe	216-164-112-45.c5-0.atw	1
2/18/2003 12:08:57 AM	URL contains UTF-8 encoding	12-212-112-155.client.att	5
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1
2/18/2003 12:08:57 AM	Suspicious URL Event	12-212-112-155.client.att	1

At the bottom of the window, a status bar displays: [Suspicious URL] Attacker may be disguising an attack by using UTF-8 encoding. [advICE](#)

VPNs (Virtual Private Networks)

- Inexpensive way to extend a network without purchasing leased (private) lines
- Point to point encryption of traffic between two systems over an untrusted network
- Only protects the information in transit - data is not encrypted on either end of the VPN “tunnel”
- Can be integrated with personal firewall and anti-virus technologies
- Watch out for “split tunneling”

Wired vs. Wireless - Telephone

- Encrypted handset-to-base is the only secure wireless (cordless – not cell/mobile) phone
- Wireless/cordless traffic is easy to intercept with a scanner
 - Digit grabbers can capture touchpad entries
- Mobile/cell phone traffic is also easy to intercept
- Telephone cable is harder to manage and more expensive to run, but very secure in comparison
- TIP: Lock your Demarcation Box... It *can* happen!

Wired vs. Wireless - Ethernet

- Wireless is **insecure**, use it at your own risk
- Use of LEAP/EAP is very complex, but it is currently the best way to secure wireless
- Consider VPN if you have the technology
- Running Cat-5 cable is expensive and hard to manage, but much more secure
- WiFi-Glyphs

Wireless Insecurity – War Driving

- Wireless NIC (Network Interface Card)
- Wireless Access Point
- The “tennis-ball can” antenna
- Wireless sniffers
 - Email (web and smtp/pop)
 - User IDs and passwords
 - LAN scanning for Windows shares (easy to break into)
 - Money/Quicken files
 - Other sensitive personal information

Old Hardware

- Donating a system to a charity?
 - Giving your old computer to the schools?
 - Giving a hard drive to your friend's kids?
-
- It is *very easy* to reconstruct data from an old hard drive using freely available software on the Internet – **degauss or “scrub” it!**
 - **EraserD** is highly recommended...

Protection 101 – Humans

- Social Engineering
 - Via the Internet
 - Give fake information when possible
 - Via the telephone
 - The “Yes and No” voice recording scam
- Dumpster Diving
 - Use a cross-cut shredder for everything with any account information whatsoever
 - Shred all “Free Offers” that you don’t use
- Current Address
 - Credit card companies
 - Consumer credit agencies (The Big Three)

Self Tests

- Gibson Research Center (www.grc.com)
 - Many different tools
- Vulnerability Scanners
 - Pick one... (I prefer ISS)
 - Microsoft Baseline Analyzer
 - GFI LANGuard Network Scanner
- Microsoft HFNetCheck (for the guru in you)
- Microsoft Update Center (frequent visits)

Keep Informed - Lists

- **X-Force** - <https://atla-mm1.iss.net/mailman/listinfo/alert>
- **SecurityTracker** -
http://www.securitytracker.com/signup/signup_now.html
- **Crypto-Gram** – <http://www.counterpane.com/crypto-gram.html>
- **NTBugTraq** - <http://www.ntbugtraq.com/>
- **Microsoft Security Bulletins** -
<http://www.microsoft.com/technet/security/bulletin/notify.asp>
- **Other Vendors**
 - Who makes your Cable/DSL router?
 - Do you use any Instant Messaging software?
 - What audio/video software do you use?

Keep Informed - News

- **SANS** – <http://www.sans.org>
- **CERT** – <http://www.cert.org>
- **Internet Storm Center** – <http://isc.incidents.org>
- **ISS Internet Threat Level** - <https://gtoc.iss.net/>
- **Department of Homeland Security Threat Level** - <http://www.whitehouse.gov/homeland/>
- **National Infrastructure Protection Center Daily Reports** - <http://www.nipc.gov/dailyreports/dailyindex.htm>
- **SARC Virus Info** - <http://www.sarc.com/>
- **Trend-Micro World Virus Map** - <http://wtc.trendmicro.com/wtc/wmap.html>
- **SecurityFocus** – <http://www.securityfocus.com>

Resources

- **BlackICE** - http://blackice.iss.net/product_pc_protection.php
- **ZoneAlarm** - <http://www.zonelabs.com/store/content/home.jsp>
- **F-Secure** - <http://www.f-secure.com/products/anti-virus/pe/>
- **Symantec** - http://www.symantec.com/product/index_homecomp.html
- **McAfee** - <http://www.mcafee.com/myapps/vs7/default.asp>
- **PasswordSafe** - <http://www.counterpane.com/passsafe.html>
- **ACrypt** - <http://www.acrypt.com/>
- **PGP** - <http://www.pgp.com>
- **GFI LANGuard** - <http://www.gfisoftware.com/lannetscan/>
- **EraserD** - <http://download.sourceforge.net/eraser/eraser53s.zip>
- **Robert Graham** – <http://www.robertgraham.com>

Resources - Microsoft

- **Microsoft Office Updates** –
<http://office.microsoft.com/productupdates>
- **Microsoft Update Center** -
<http://v4.windowsupdate.microsoft.com/en/default.asp>
- **Microsoft HFNetCheck** –
<http://www.microsoft.com/technet/security/tools/tools/hfnetchk.asp>
- **Microsoft Baseline Security Analyzer** -
www.microsoft.com/TechNet/Security/tools/tools/MBSAHome.ASP
- **Microsoft Security Center** - <http://www.microsoft.com/security/>
- **Microsoft Security Bulletin Service** -
<http://www.microsoft.com/technet/security/bulletin/notify.asp>
- **Microsoft Security Tools and Checklists** -
<http://www.microsoft.com/technet/security/tools/tools.asp>

Tips for ID Theft Victims

- Create a checklist and log
 - Which agencies/companies have been contacted
 - Document exactly what they are going to do to remedy your issue and when they expect to have it done (verify)
 - Get name of contact person you speak with every time you call – it may change
 - Record every number you call
 - If you get transferred, write down the new number
 - Record time and duration of all calls
 - Take extensive notes or record conversation
 - Be persistent! Don't take no for an answer unless you absolutely have to.

More Tips for ID Theft Victims

- Contact all creditors – *immediately*
 - Change account information
 - Remove SSN as identifier
 - Establish a password
- Contact Credit Bureaus and get a Fraud Alert
 - Experian
 - Equifax
 - Trans Union
- Contact local FBI headquarters
- Contact local Secret Service representative
- Contact Oregon State Police
- **Monitor all accounts very closely**

The End...

Contact Information:

*This presentation can be found at
<http://www.pcmill.com/presentations/>*

Patrick Miller, CISSP SSCP TCP
patrick_miller@ureach.com
877.581.1601