

Safe Surfing

How to surf the Net without getting PWND!

A sincere, "thank you!"

- Thanks to everyone that put this conference together!
- Thanks to all of you for taking the time to attend.
 - No matter how technical something is, it always boils down to people in one way or another.
 - Users, administrators, decision-makers, etc.
 - If nothing else, Layers “Eight and Nine” of the OSI Model
 - Politics & Funding ☺
 - People, process and technology...all working together...over time is what makes the difference.
 - You are the people that are making it happen!

Who am I? I'm Bryce Galbraith.



- A perpetually curious kid who at 10, got a Commodore 64 and a modem (before the Internet!) Now I'm just a bigger kid with a mortgage...
- I've held security positions at global ISPs and Fortune 500 companies.
- I was a senior member of Foundstone's world-renowned attack and penetration team as well as a senior instructor and co-author of Foundstone's "Ultimate Hacking: Hands-On" course series.
- I am a contributing author of the internationally bestselling book, *Hacking Exposed: Network Security Secrets & Solutions*.
- I'm currently one of the SANS Institute's top rated Certified Instructors and a lead penetration tester at Layered Security.
- I've taught the art of ethical hacking and countermeasures to thousands of IT professionals from a who's who of top companies, financial institutions, and government agencies around the globe.
- I'm an active member of several security-related professional organizations, I speak at a variety of conferences, and hold a number of certifications: CISSP, GCIH, GSEC, CEH, CHFI, Security+, and CCNA.

Unique Perspective

- I come from a unique (albeit twisted) perspective...
- My entire career has been focused on offense.
- I am an “Ethical Hacker” (i.e. I have permission).
- My job is to hack into some of the most sensitive and secure networks in the world.
- I use conventional and non-conventional means to accomplish this goal.
- This requires perpetual research and experimentation.
- I’m here to share some of what I’ve learned.
- The more I learn the more I realize I don’t know...

What We're Going To Cover...

- Common Security Myths
 - Hackers *love* our myths.
 - We're going to dispel them...
- The Wiles of The Internet
 - Hackers have amazing capabilities.
 - We are going to explore them...
- Defense
 - Offense is almost always easier than defense.
 - We're going to make them work for it...

Awareness Is Essential!

- The Art of War
 - Written by Sun Tzu in 6th century B.C.
- Considered the definitive work on military strategies and tactics of its time - still a fundamental text today.
- A major theme:
 - Know thy enemy
 - Know thy self
- This is a war – with zeros and ones instead of bullets.
- We cannot expect to effectively defend against an enemy we do not understand...

Common Security Myths

- Hackers *love* our ignorance, arrogance and apathy.
 - Whether conscious or subconscious – doesn't really matter
 - They have no mercy whatsoever...
- The more you learn about technology, the more amazed you become that it works at all.
 - Exponential growth & infinitely complex
- The more you learn about, “information security” the more you realize that the term is really an oxymoron.
 - Virtually impossible to defend against all threats.
 - Unplug? Not gonna happen...
- There is no “silver bullet” – despite what vendors say!
- Myths abound...let's explore a few favorites.

Common Security Myths

- MYTH
 - “I don’t have anything anyone would want.”
- FACT
 - You have an IP address, MAC address, hard drive, CPU, memory and a nice pipe to the Internet that isn’t theirs.
 - Stealth, anonymity and misdirection are *very* valuable to attackers who *do not* want to get caught.
 - Fraud-related activities, purveying illegal pornography, extortion, spam, Distributed Denial of Service (DDoS), etc.
 - They would love to add your machine to their botnet!
 - Guess who the Feds (or rival criminals) come looking for?
 - “It wasn’t me!” – Isn’t that what they all say?
 - Don’t forget about your identity and your money too...

Common Security Myths

- MYTH

- “I use a Mac. They’re *way* more secure than Windows.”

- FACT

- Macs are more *obscure*, not more secure - very important!
 - Don’t be naïve. Hackers go for mass effect – historically Windows.
 - This is changing and hackers are all over it. There is blood in the water.
 - Remember hackers love ignorance, arrogance and apathy.
 - Exploit writers actually *prefer* Macs and their *users*.
 - They are turning their attentions towards Macs with a vengeance.
 - Macs are in some ways easier to hack. Hackers hate Vista/7/2008 right now and as always, are choosing the path of least resistance.
 - Macs have no AV, Apple provides updates insecurely, less attention, lack of GPOs as a rule, no ASLR or stack canaries, misinformed users, and Macs haven’t been subjected to the full-force of the hacking underworld...yet.
 - Apple perpetuates the myth instead of warning their customers.
 - Users tend to believe the myth in mass and may even be arrogant about it.
 - “Pride goeth before the fall”, as they say...

Common Security Myths

- MYTH
 - “I’m good about patching so I should be alright.”
- FACT
 - If only it were that easy. Far from it, however.
 - Many attacks take advantage of *features* of OSs, browsers, network protocols, network devices, common or default configurations, etc. and have nothing to do with patching.
 - The very nature of patching is reactionary.
 - The vulnerability already exists and many times an exploit is available in the wild before a patch is released.
 - Patch Tuesday -> “Exploit Wednesday”
 - Zero-day’s in-the-wild
 - What about client apps and third-party software??

Common Security Myths

- MYTH

- “I don’t use Internet Explorer. I use _____.”

- FACT

- Remember obscurity is not the same as security.
 - No browser is secure – only varying degrees of insecurity
 - Hacker’s routinely release exploits for all of them.
 - Month-of-browser bugs proved the point convincingly
 - <http://browserfun.blogspot.com/>
 - Recent study:
 - Firefox flaws account for 44% of all browser bugs. Apple's Safari takes second, with 35%, IE in third with 15%.
 - Much of the security, or lack there of, still rests on the individual user awareness, actions and discretion as well as the level of attention the hacking world directs at it.

Common Security Myths

- MYTH
 - “I have Product XYZ on my computer to protect me.”
- FACT
 - There is no product that will protect against all the threats. It simply doesn't exist. I wish it did...
 - AV can be bypassed with polymorphic code generators.
 - Encoders, encryption, code-obfuscators, etc.
 - Firewalls/proxies can be bypassed in numerous ways
 - “The truth about personal firewalls”
 - <http://www.rootkit.com/newsread.php?newsid=849>
 - SSL encapsulation
 - Covert channels
 - Riding over trusted connections
 - Invisible IE windows via OLE
 - Steganography



Common Security Myths

- MYTH
 - “No one can guess my password.”
- FACT
 - Your password may not be as strong as you think.
 - LanMan hashes up to 14 characters, alpha-numeric and any of 32 special characters can be cracked within seconds or minutes with Rainbow Tables.
 - They don't actually have to guess it.
 - Key loggers & network interception
 - Replaying/passing credentials
 - Pass-the-hash toolkit or Meterpreter module from Metasploit
 - Memory-based attacks
 - Authentication bypass
 - Insecure storage on hard disk (boot-around attacks)

Common Security Myths

- MYTH
 - “All my stuff is encrypted.”
- FACT
 - Are you absolutely certain? Even so...
 - Many encrypted protocols fall to various attacks
 - SSL, RDP, SSHv1 for example can fall to man-in-the-middle
 - Several protocols are susceptible to downgrade attacks
 - Windows authentication: NTLMv2 -> NTLMv1 -> LM
 - SSHv2 -> SSHv1
 - Attackers often attack where least expected
 - Before encryption or after decryption has been applied.
 - Encryption keys not stored securely (e.g. disk, RAM)
 - Key loggers (physical, SW, acoustic, wireless, Mac keyboard!)

Common Security Myths

- MYTH
 - “Why can’t they get it together and *fix* this stuff!?”
- FACT
 - We (a.k.a. you and I) are still the weakest link.
 - Social engineering *works* – that’s why they do it.
 - Phishing, spear-phishing & whaling works.
 - People go to questionable websites
 - We download all sorts of things
 - Free DVD burning software – “Sweet!”
 - Special CODEC to view that video – “Hmm, it *looks* legit.”
 - Cool widgets – “This will make my life sooo much better.”
 - We click on links in e-mails and open attachments
 - We download, run, grant privileges, and permit things through our firewalls with only cursory investigation into their origins.
 - ...and best of all, we do it all while logged in as super-users!

Most users clicked "Yes" to this...



WARNING!

You are about to install some malware. Malware is bad. By reading this warning through to the end and still clicking yes you're failing the Windows Darwin Test. Don't be that guy, if you're reading this message still then wise up and for the love of your family photos on your hard drive click the 'No' button.

Yes

No



Common Security Myths - Summary

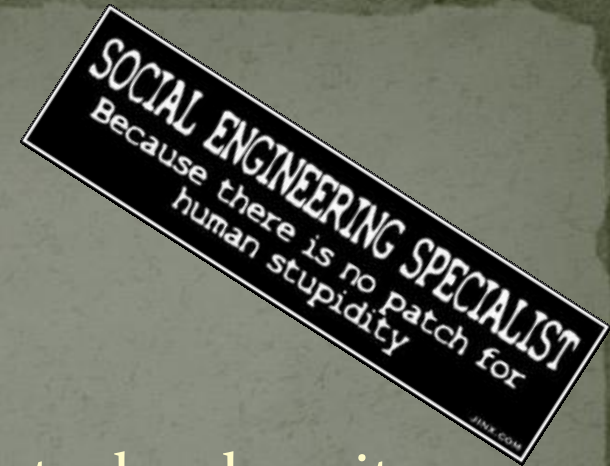
- Ignorance , arrogance and apathy undermine security
 - We need to realize that defense takes real work, not a patch.
- Everyone is a target
 - If nothing else they want your machine and bandwidth.
 - They are likely after much more than that...
- There is no “silver bullet”
 - No OS, browser, firewall, password or product can do it.
- We are all too often the weak link
 - We have to take responsibility too ☺
- The hackers are usually at least one step ahead
 - We need to put up a good fight and make them work for it.

The Wiles of the Internet



- Now let's take a look at some of the more interesting and effective attack vectors attackers have devised to gain access to our most critical information...
- I often refer to the Internet as the Wild, Wild, Web.
- It is a dangerous place...and it's getting worse.
 - Organized crime contingencies
 - Nation-states
 - Increasing numbers of hackers and script-kiddies
 - Sophisticated hacker tools and exploitation frameworks
 - Increasingly advanced exploitation techniques
 - Exponential growth of technologies and user base
 - Proliferation of open wireless networks – free Wi-Fi!
 - Failure to learn from past mistakes...

The Wiles of the Internet



- Social Engineering
 - ‘Cause it works...
 - Never underestimate - combined with technology it can be extremely convincing:
 - Information recon
 - Pipl for starters – <http://pipl.com/>
 - Maltego – <http://www.peterva.com/>
 - Technologies:
 - Caller-ID spoofing, click-jacking, phishing, pop-ups, hidden features, bugs, meta-data in docs/pics, online resumes, etc.
 - Shameless plug for SANS Security 550 – Information Recon
 - The Social Engineering Framework – NEW!
 - <http://www.social-engineer.org/>

The Wiles of the Internet

- Phishing / Spear-phishing / Whaling
 - It just works – extremely well.
 - People are still clicking on links in e-mails
 - People are still giving out personal details at these sites
 - People are trusting e-mail addresses and phone numbers
 - People are still opening up attachments in e-mails
 - People are still not verifying the sites they're going to
 - People are still not verifying that SSL is established
 - People are still accepting certificate warnings
 - Phishing will stop when:
 - People stop biting...not likely
 - Technology prevents them from biting
 - DNSSec, spam filtering, attachment scrubbing, white-lists, black-lists, browser add-ons, OpenDNS, digital sigs, etc. – no easy solution.

The Wiles of the Internet

- Don't forget about physical attacks!
 - **Hardware key loggers**
 - Placed inline between keyboard and computer
 - **OS boot-around attacks (raw file system access)**
 - Insecure password storage, cached domain creds, files, etc.
 - Linux Live distros – BackTrack, Helix, Ubuntu ☺
 - ntpasswd - <http://home.eunet.no/pnordahl/ntppasswd/>
 - Kon-Boot - <http://www.piotrbania.com/all/kon-boot/>
 - **Direct Memory Access (DMA) attacks**
 - Direct access to physical memory (e.g. passwords, settings)
 - **Cold-boot attack and “Evil maid” attacks**
 - Can defeat full disk encryption
 - http://en.wikipedia.org/wiki/Cold_boot_attack
 - <http://theinvisiblethings.blogspot.com/>

The Wiles of the Internet

- Traffic Interception (a.k.a. sniffing)
 - A hacker favorite!
 - Passwords, clear-text HTTP, instant messaging, DNS, SNMP, telnet, FTP, most web-mail apps and social networking sites are clear-text after the login, etc.
 - Strong authentication but weak transport – pwnd!
 - Wireless makes is easier than ever (more on this later)
 - Sniffing on switches? No problem.
 - Gratuitous ARP-replies that poison ARP caches
 - Victims forward Ethernet frames to hacker (i.e. mitm)
 - Cable networks
 - Many cable networks are essentially giant hubs
 - Just need an older modem or firmware in many cases
 - Brings a whole new meaning to having a snoop neighbor!

The Wiles of the Internet

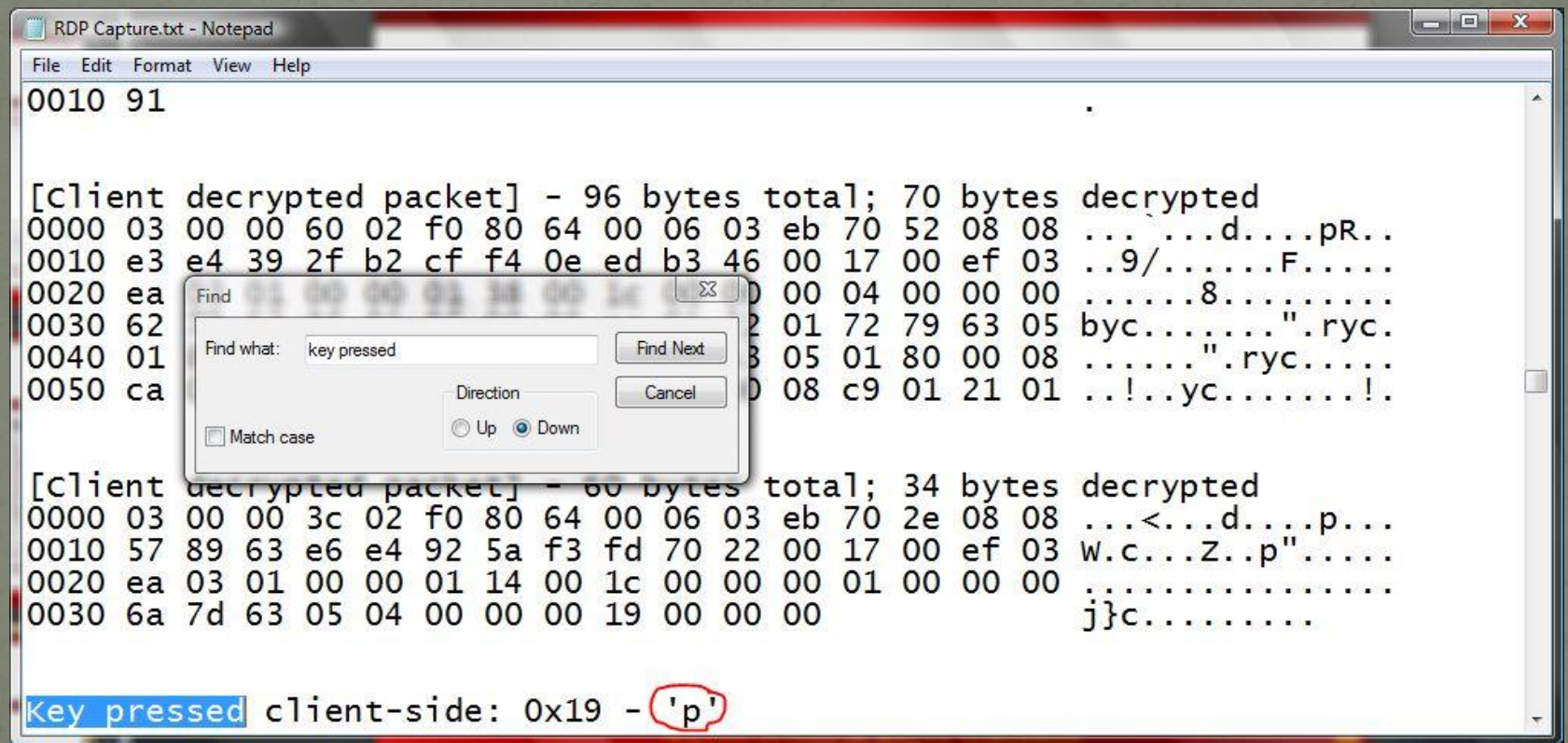
- Default Protocols & Application Behavior
 - Too much information (TMI)
 - Many default protocols and applications broadcast all sorts of sensitive information
 - Bonjour service (e.g. Macs, iTunes, etc.)
 - Windows Media Center
 - Universal Plug-n-Play
 - Bluetooth – person's name or computer name
 - IPv6 – enabled by default on current OSs.
 - Etc.

The Wiles of the Internet

- Man-in-the-middle Attacks
 - Enables control over OSI Layers
 - ARP cache-poisoning is a favorite
 - Gratuitous ARP-replies to poison ARP caches
 - Can be used to:
 - Spoof DNS, capture credentials, inject commands, hi-jack sessions, side-jack connections, bypass strong authentication (e.g. RSA SecurID)
 - Defeat encryption: SSL, RDP, POP₃S, IMAPS, LDAPS, PPTP, some SSL VPNs
 - Downgrade protocols: NTLMv2 -> NTLMv1 -> LM
 - I have entire presentation on this – just e-mail me.

The Wiles of the Internet

- Man-in-the-middle Attacks



```
RDP Capture.txt - Notepad
File Edit Format View Help
0010 91

[Client decrypted packet] - 96 bytes total; 70 bytes decrypted
0000 03 00 00 60 02 f0 80 64 00 06 03 eb 70 52 08 08 ...d....pR..
0010 e3 e4 39 2f b2 cf f4 0e ed b3 46 00 17 00 ef 03 ..9/.....F....
0020 ea 00 04 00 00 00 01 72 79 63 05 byc.....".ryc.
0030 62 08 c9 01 21 01 ..!..yc.....!
0040 01
0050 ca

[Client decrypted packet] - 60 bytes total; 34 bytes decrypted
0000 03 00 00 3c 02 f0 80 64 00 06 03 eb 70 2e 08 08 ...<...d....p...
0010 57 89 63 e6 e4 92 5a f3 fd 70 22 00 17 00 ef 03 w.c...Z..p".....
0020 ea 03 01 00 00 01 14 00 1c 00 00 00 01 00 00 00 .....
0030 6a 7d 63 05 04 00 00 00 19 00 00 00 j}c.....


Key pressed client-side: 0x19 - 'p'
```


CNN.com - Breaking News, U.S., World, We
File Edit View History Bookmarks Tools Help
http://www.cnn.com/

CNN.com
Web CNN News CNN Video
HOME WORLD U.S. POLITICS CRIME ENTERTAINMENT HEALTH TECH
Hot Topics » Susan Boyle • Mexico • Torture • Money & Main St. • Commentary

Set your CNN.com Edition

updated 1:48 p.m. EDT, Fri April 17, 2009



Latest News

- Small plane crashes in Flori
- If Chavez talks, Obama wou
- Navarrette: Obama treats M
- Singer 'gobsmacked' by ove
- Illegal immigrants detained,
- Transgender murder trial m
- iReport.com: Your tributes t
- Cops track tot mom's move
- Ticker: Governor under fire
- 'Crack was my friend,' ex-a
- Commentary: Memo may hi
- Dad finds daughter he thoug
- Forgotten nut could save liv

Done

Victim - XP
http://www.google.com/

YAHOO!
Web Images Video Local Shopping more
Search:

Featured




CARLOS VILLALON/REDUX

MitM attacks rock!
Heat waves shimmer over the desert. A team of forensic experts clad in white overalls excavate

Virtually any page element or
DNS request...

The Wiles of the Internet

- Malicious Browser Content
 - Modern web pages utilize active web content extensively
 - JavaScript, ActiveX, Java, Flash, embedded AV, etc.
 - Code downloaded and run within your browser's context
 - What could go wrong? ☺
 - It's a free-for-all:
 - XSS, XSRF, session cookie stealing, session hi-jacking, malware installation, complete control of victim
 - Flash cookies – hidden tracking cookies
 - Browser Exploitation Framework (BeEF)
 - <http://www.bindshell.net/tools/beef/>
 - Hooks the browser with nasty JavaScript
 - Deployed via web site, phishing e-mail, forum posts, mitm.



BeEF

Autorun
Disabled

Zombies

	10.0.0.6
	10.0.0.6
	10.0.0.10
	10.0.0.4
	10.0.0.10
	10.0.0.10

Browser Exploitation Framework

Module

Metasploit Browser Autopwn

This module creates a Metasploit listener using a backend server, and then sends the client code which creates an iframe connecting to the waiting exploit.

Setup MSF to allow BeEF access (settings in /beef/ui/msf.php):

```
sudo ./msfconsole
msf > load xmlrpc Pass=BeEFMSFPass
```

LHOST (Required)

LPORT

SRVHOST (Required)

SRVPORT (Required)

URIPATH

Log Summary

[Refresh Log] [Clear Log] [Display Raw Log]

```
[17/09/09 06:41:47 10.0.0.6]
Zombie connected: Safari 531.9 - Intel Mac OS X 10_5_8
[17/09/09 06:39:50 10.0.0.4]
Module Result:
Tor is NOT being used
[17/09/09 06:39:49 10.0.0.6]
Module code sent
[17/09/09 06:39:24 10.0.0.6]
Module Result:
Default Plugin
Java Embedding Plugin 0.9.7.1
QuickTime Plug-in 7.6.4
Shockwave Flash
Flip4Mac Windows Media Plugin 2.2.2
iPhotoPhotocast
[17/09/09 06:39:22 10.0.0.6]
Module code sent
[17/09/09 06:39:03 10.0.0.10]
Module Result:
Adobe Reader 9.0
Windows Pinball
Windows Movie Maker
MSN
Paros
[17/09/09 06:39:03 10.0.0.6]
Module code sent
[17/09/09 06:38:35 10.0.0.4]
Zombie connected: Firefox 3.0.14 - Linux i686
[17/09/09 06:38:29 10.0.0.6]
Zombie connected: Safari 531.9 - Intel Mac OS X 10_5_8
[17/09/09 06:38:04 10.0.0.6]
Zombie connected: Firefox 3.5.3 - Intel Mac OS X 10.5
[17/09/09 06:37:57 10.0.0.10]
Zombie connected: Internet Explorer 8.0 - Windows NT 5.1
[17/09/09 06:37:51 10.0.0.10]
Zombie connected: Firefox 3.0.10 - Windows NT 5.1
[17/09/09 06:37:36 10.0.0.10]
Zombie connected: Chrome 3.0.195.21 - Windows NT 5.1
```


The Wiles of the Internet

- SSL/TLS Attacks
 - Many sites don't use SSL/TLS at all or only at logon
 - Webmail, social networking sites, etc.
 - Sniffing, injecting and side-jacking ensues
 - When used, we rely heavily on it to:
 - Verify the authenticity of the site we're visiting
 - Encrypt our data in transit
 - Normally this works pretty well – if they use it.
 - Hacker's have learned how to attack it.
 - Interception before encryption
 - Spoofed certificates
 - SSL man-in-the-middle
 - sslstrip

The Wiles of the Internet

- SSL/TLS Attacks
 - **Interception before encryption**
 - This essentially renders SSL/TLS completely impotent.
 - Several modern malware tools utilize this technique.
 - Many of them target specific sites and their users.
 - Not much else to say – game over...

The Wiles of the Internet

- SSL/TLS Attacks
 - Spoofed certificates
 - Md5 hash collisions
 - Allows the creation of spoofed certs that will verify correctly due to hash collisions in the MD5 hashing algorithm.
 - Translation – NO BROWSER WARNING!
 - Wild card certificate spoofing
 - In the commonName field, list the site as *\o.example.com.
 - This creates a certificate that tricks many programs into authenticating virtually every address on the internet.
 - Translation - NO BROWSER WARNING!

The Wiles of the Internet

- SSL/TLS Attacks
 - SSL/TLS man-in-the-middle
 - Attacker gets in the middle (e.g. ARP-poisoning)
 - Hacker intercepts and keeps real cert from site
 - Duplicates cert except the Public key (most important part)
 - Sends spoofed cert to user
 - USER GETS BROWSER CERTIFICATE WARNING!
 - Possibly combine with previous attack and no warning?
 - No matter, user promptly ignores warning regardless 😊
 - All traffic can be decrypted on-the-fly
 - Attacker can see, manipulate and/or inject any element!
 - Hacker wins again...

The Wiles of the Internet

- SSL/TLS Attacks

- **ssltrip**

- “It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon.” – Moxie Marlinspike
 - End result - SSL from site to hacker, clear-text from hacker to you, icon in URL shows a lock, user thinks SSL is established and proceeds.
 - Hacker wins again...

The Wiles of the Internet

- Exploitation Frameworks
 - There are an increasing number frameworks that bring very advanced exploits and payloads to anyone...
 - Browser Exploitation Framework (just covered)
 - <http://www.bindshell.net/tools/beef/>
 - Web App Attack and Audit Framework
 - <http://w3af.sourceforge.net/>
 - Metaphish Phishing Framework
 - <http://www.attackresearch.com/>
 - Metasploit Framework
 - <http://www.metasploit.com/>
 - They just need a big red button ;)



The Wiles of the Internet

- Exploitation Frameworks
 - Metasploit Framework
 - Huge exploit collection (frequent updates)
 - db_autopwn, browser autopwn, karmasploit (wireless)
 - Advanced Payload collection
 - Shells, reverse shells, the ability to disable firewalls on victim
 - Add an Admin user to victim, PassiveX, VNC dllinject, etc.
 - Meterpreter
 - hashdump, timestomp, pass-the-hash, remote command execute
 - Full file system, registry, networking control, pivoting support
 - Memory resident – injects itself as a DLL into victim process (can migrate)
 - Inline Ruby scripting, screenshots, disable keyboard/mouse, etc.
 - Payloads can be deployed through a variety of means
 - Stand-alone EXE, JavaScript, Visual Basic scripts (macros ☺), C, Perl
 - Advanced encoders to evade AV/IDS/IPS/HIDS/HIPS.
 - “Shikata ga nai” – Japanese for, “nothing can be done about it”



The Wiles of the Internet

- Wireless Networks
 - Now let's add the joy and freedom of wireless to the mix and what could possibly go wrong? ☺
 - All these attacks and more work just as well on wireless
 - Traffic interception is actually easier
 - ARP-cache poisoning mitm attacks work the same
 - If anything, it provides *more opportunities* for attackers
 - Stealth, easier access, long distance with proper equipment
 - Denial of Service (RF-based and logical attacks)
 - Opens up wireless mitm attacks at Layer 1 as well
 - Client-duping with fake Aps
 - MAC-spoofing – allows hacker to ride trusted connections

The Wiles of the Internet

- Wireless Networks
 - Wireless encryption mechanisms have issues
 - 802.11-based networks
 - Encryption protocols
 - Wired Equivalent Privacy (WEP) – IEEE
 - Wi-Fi Protected Access (WPA) – Wi-Fi Alliance
 - 802.11i – IEEE
 - Wi-Fi Protected Access 2 (WPA2) – Wi-Fi Alliance
 - Some of the better attack tools
 - Aircrack-ng – WEP, LEAP, WPA/WPA2-PSK, etc.
 - Wepbuster – totally automated WEP cracking
 - WPA/WPA2 rainbow tables for PSK mode
 - Extensible Authentication Protocol (EAP)
 - Over 40 different kinds (LEAP, PEAP, etc.)
 - Attacks vary depending on the version of EAP deployed

The Wiles of the Internet

- Wireless Networks

- KarmaSploit

- Attacks any wireless device configured to automatically connect to preferred networks or whenever a user manually tells their wireless client to connect to a network.
 - Wherever and whenever your wireless card is on
 - Even on airplanes! Hacking the friendly skies...
 - How does it work?
 - Attacker passively monitors RF in the area
 - Victim wireless clients send probes looking for their network(s)
 - Attacker responds *as* the network(s)
 - Victim associates, gets an IP address from KarmaSploit
 - Attacker delivers exploits via Metasploit integration (e.g. autopwn)
 - Client gets pwnd! Even if they didn't *mean* to connect.

The Attacks

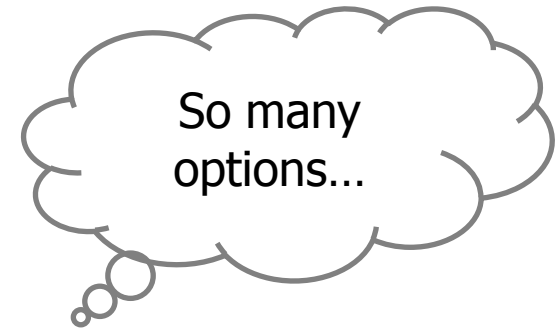
- Portable AP w/ Internet



- Internet Connection Sharing
- Built-in wireless assoc to AP
- Running Cain (Windows)



- BackTrack in a VM or on a second laptop w/ another wireless card.



→ Internet

- Wireless broadband (e.g. EV-DO, EDGE, 3G)
- Built-in to many laptops today

The Wiles of the Internet

- Wireless Networks
 - Bluetooth isn't immune either – far from it.
 - Discover “non-discoverable” devices
 - Crack the encryption (fixed PIN of 0000) on headsets
 - Sync up to headset
 - Record *and play* arbitrary audio – “Can you hear me now?”
 - Check out Joshua Wright's work at:
 - <http://www.willhackforsushi.com/>
 - <http://www.youtube.com/watch?v=1c-jzYAH2gw>
 - Numerous other phone-specific bugs and attack vectors

The Wiles of the Internet

- Client-side Attacks
 - An increasingly popular attack vector
 - Straight to the inner sanctum
 - Can evade firewalls/proxies/NIDS/NIPS
 - Encoders help with evasion
 - Metasploit & Metaphish helpful in creation process
 - Virtually all client apps have issues
 - All popular browsers on all popular OSs
 - Adobe Reader, QuickTime, Flash, Java
 - iTunes, Windows Media Player, WinAmp ☺
 - Office documents (file format flaws – MS can't fix)
 - Mail clients, instant messaging clients, etc.
 - Pretty much all the client software we use...

The Wiles of the Internet

- Malicious Software Updates
 - Clearly, keeping our software up-to-date is crucial.
 - Hackers know this too...
 - Malicious updates? Oh my!
 - Hack into site and plant backdoored version
 - Deploy modified versions on file sharing networks
 - Utilize MD5 hash collisions to spoof verification process
 - <http://www.doxpara.org/> (Fire & Ice)
 - ISR-Evilgrade
 - Many vendors use insecure update mechanisms
 - Mac OS X (say it ain't so!), iTunes, - Java plugin, Winzip, Winamp, Open Office, Linkedin Toolbar, DAP [Download Accelerator], notepad++, speedbit
 - Modular framework can easily be extended...

The Wiles of the Internet

- Malicious Software Updates
 - While we're on the topic of updates, what about cell phones?
 - The browsers are actually useable now.
 - How often do updates come out?
 - Attackers reverse the firmware updates and find exploits within hours or days after their release.
 - Users sit vulnerable for weeks/months.
 - iPhone apps run as root (similar on other phones)
 - Hacker can run anything they want with root privileges
 - "There's an app for that" takes on a whole new dimension

The Wiles of the Internet

- The first iPhone worm
 - Rickrolls jailbroken iPhones!
- Sing it with me now...1,2,3

Never gonna give you up,
Never gonna let you down,
Never gonna run around and desert you,
Never gonna make you cry,
Never gonna say goodbye,
Never gonna tell a lie and hurt you...



The Wiles of the Internet

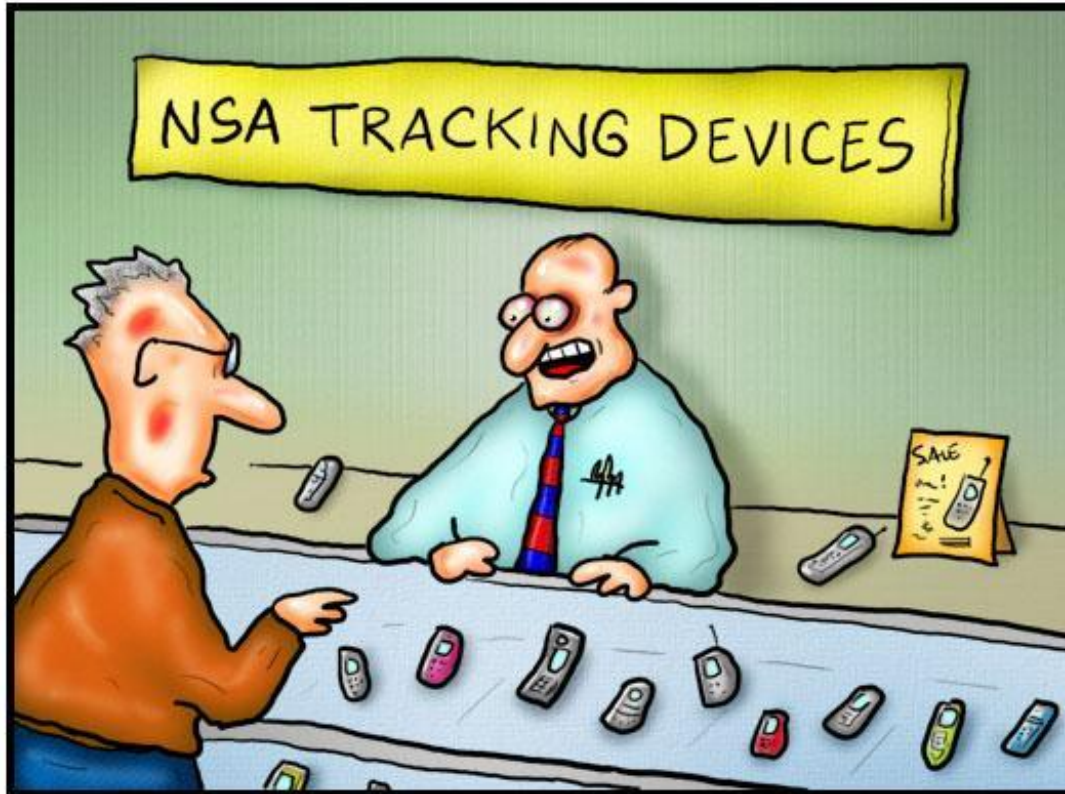
- “Can you track me now!?”
 - Mobile phone tracking goes mainstream
 - As the phones get smarter, so does the malware...
 - Current features include:
 - GPS tracking to within feet
 - Stealth call monitoring/recording (inbound & outbound)
 - All text messages, call logs and e-mails
 - Stealth bugging (enable phone mic remotely when not in call)
 - Popular software
 - <http://www.mobile-spy.com/>
 - <http://www.flexispy.com/>
 - Can be deployed locally or via exploit (no cables required)
 - Not just for the Governments anymore! 😊



The Wiles of the Internet

DOCTOR FUN

17 May 2006



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

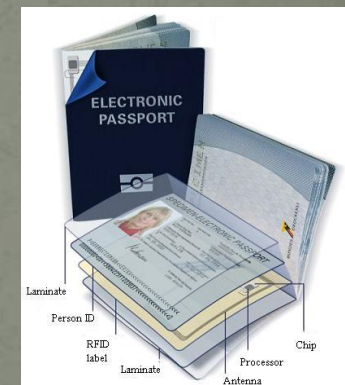
"Yeah - we used to call them cell phones."

The Wiles of the Internet

- Some Interesting iPhone “Features”
 - The iPhone is just awesome...but it has some issues.
 - All apps run as root (where did these come from again?)
 - PIN can be bypassed with physical access
 - Photos are geo-tagged (embedded GPS coordinates)
 - Every time you press the Home key it takes a screenshot of whatever you’re looking at and saves it to the flash drive
 - A forensics dream feature – hmm, wait a minute ;)
 - Has awesome mic pickup...for the attacker to use
 - New version has Voice Control
 - Works when phone is locked – hold down the Home key
 - Say, call so-and-so or just speak a number to dial – doh!
 - Capture biometrics from touch screen? Working on it...

The Wiles of the Internet

- Radio-Frequency Identification (RFID)
 - Historically (as well as currently) used to in supply-chain management arena primarily
 - Likely in your wallet right now...
 - Increasingly being used to track people
 - All new Passports (e-Passport) as of 2007
 - New driver's licenses in some States
 - Many newer credit cards
 - Other contactless payment systems
 - ExxonMobil Speedpass (1997)
 - Contactless smartcards
 - Building access cards
 - Babies, patients, the dead??
 - DoD CAC – coming soon



The Wiles of the Internet

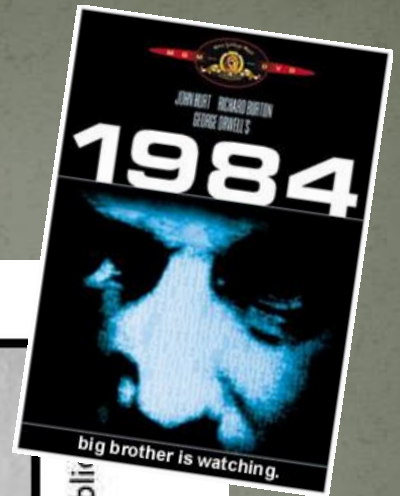
- Radio-Frequency Identification (RFID)
 - Hackers are already cloning and “skimming”.
 - Cloning building access cards
 - Skimming credit card and e-Passport information
 - Hackers put Elvis Presley's information on an e-Passport
 - Big plans for the future
 - ID info (photo, name, country, etc.) – done
 - Crypto keys (PKI smartcard) – done
 - Cell phones with RFID readers in them –done
 - First cell/satellite phone combo unit – done
 - Global PKI system managed by the ITU of the UN – in progress...
 - US just relinquished control of the ICANN organization recently.
 - Mobile IPv6 global routing with a single IPv6 address – done
 - IPv6 address on chip is you on the grid? For your safety...
 - *Required* human implantable RFID chips?? Not me ☺



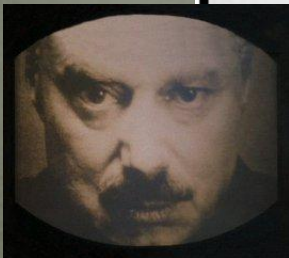


The Wiles of the Internet

DOCTOR FUN



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>



The Wiles of the Internet



Conspiracy??

Is it paranoia or a “heightened sense of awareness?”
I never can tell...

The Wiles of the Internet

- Radio-Frequency Identification (RFID)
 - Conspiracy or not, expect hackers to increase their onslaught on these technologies as we continue to rely on them to help us:
 - Public-Key Infrastructure (PKI)
 - Confidentiality, Integrity, Availability (CIA)
 - Authentication, Authorization, Accounting (AAA)
 - Non-repudiation (“It wasn’t me” won’t cut it)
 - Positively identify/track people
 - Identity theft, online fraud, ATM scams, etc.
 - Illegal immigrants, terrorists, “undocumented workers”, etc.
 - Sex offenders, parolees, people out on bail, etc.
 - Newborns, Alzheimer’s patients, mentally ill, etc.
 - Tragedy victims (e.g. hurricane Katrina victims)
 - Travelers, public transportation, financial transactions
 - Internet activity (e.g. child pornography, rebels, etc.)
 - Everyone and everything? Search Google for “Internet of Things”
 - Btw, your search will be tracked too ☺

The Wiles of the Internet

- All of this *will* increase security, right?
 - E-passport - PWND! “Elvis’ has *left* the country...”



Defense

- So how in the world do we defend against all this??
 - **First step – awareness!**
 - You don't know what you don't know...and what you don't know can most definitely hurt you.
 - Educate yourself - perpetually. Rapidly developing...
 - This is just the beginning...
 - You may find my blog helpful - <http://blog.layeredsec.com/>
 - Knowing the hacker's capabilities puts you a long way down the road to effective defense.
 - **Now let's look at some practical steps to raise the bar...**

Defense

- Yes - even on your Mac! ☺
 - New Metasploit module takes control of iSight camera
 - It's game on folks. Don't get caught with your pants down...figuratively or literally.



Defense

- A Bottom Up Approach
 - BIOS password
 - Full disk encryption (FDE) - preferably multi-factor auth
 - If Windows, SYSKEY boot password
 - Strong passphrase (more in a bit)
 - Patches (OS *and* applications)
 - Personal Software Inspector - <http://psi.secunia.com/>
 - Careful when updating on public networks (e.g. ISR-Evilgrade)
 - Verify signatures (if they provide them – come on Apple!)
 - Secure configuration
 - <http://www.cisecurity.org/>
 - Encrypted volumes once booted (FDE no help then)
 - <http://www.truecrypt.org/>
 - Granular firewall (ingress *and* egress)
 - Anti-malware (AV/HIDS/HIPS/etc.) – even on Macs ☺

Defense

- OpenDNS
 - <http://www.opendns.com/>
 - Even if you click, it won't resolve – brilliant!
 - Existing malware may not be able to either
- Helpful Firefox Add-ons
 - NoScript – <http://noscript.net/> (remember BeEF?)
 - FlashBlock - <http://flashblock.mozdev.org/>
 - Web of Trust (WOT) - <http://www.mywot.com/>
 - Adblock Plus - <http://adblockplus.org/>

Defense

- A Note on Passphrases
 - Not derived from a word - at all
 - Hackers pretty much invented l33t \$p3@k, btw...
 - Un-guessable, never re-used, lengthy (15+)
 - Password managers make this possible – careful!
 - <http://keepass.info/>
 - <http://passwordsafe.sourceforge.net/>
 - <http://1password.com/> (Mac and iPhone only)
 - I even use bogus answers to security questions
 - Mother's maiden name? “Humperdink”
 - Different for each app
 - Keep track in password manager
 - Keep your password manager safe 😊
 - All your eggs in one place...
 - Separate TrueCrypt volumes?



Defense

- Avoid clear-text protocols whenever possible
 - IM, webmail, social networking sites, Telnet, FTP, SNMP
 - Careful when surfing HTTP sites (most of the Internet)
 - Remember your cable network may be very public
- Ensure SSL has established correctly
 - Verify URL
 - Don't accept SSL/TLS certificate warnings!
 - Don't be fooled by the lock favicon (e.g. sslstrip)
- Heed SSH warnings too
 - SSHv1 mitm attack yields clear-text data
 - Downgrade attack SSHv2 -> SSHv1 (decrypt)
- Social networking - use caution and discretion
 - Remember Pipl? Think twice...



Defense

- Phishing
 - Don't be fooled – it's a hook.
 - Never, ever, ever, ever, ever click on a link in e-mail or chat, unless you are 100% sure (digitally signed preferably)
 - Don't set your e-mail client to download images automatically
 - Verify URL and SSL before doing anything
 - Don't trust e-mail addresses and phone numbers from e-mails
 - Avoid filling in forms that ask for personal info until you are certain you are at the right place
 - Be especially careful with attachments (more on this in a bit)
 - <http://www.antiphishing.org/>

Defense

- Email Security
 - Use SMIME, PGP or something with:
 - PKI or even a simpler Web of Trust
 - Digital Signatures
 - Can thwart numerous attacks
 - Spoofing, interception, mitm manipulation/injection, etc.
 - Get your organizations and friends to do the same
 - Set mail client to *not* download images automatically
 - Secure configuration of mail client
 - Check vendor documentation (i.e. RTFM :)

Defense

- Attachments
 - This can be one of the hardest things to defend against
 - *If you open it, you could be in trouble.*
 - Chances are if it made it to you, AV won't catch it either.
 - If it is questionable, open it in a safe environment
 - Sacrificial system, VM, lab network, etc.
 - I keep a VM just for such situations – revert to snapshot
 - Process Monitor – <http://www.sysinternals.com/>
 - Monitors all Registry, file, network, tokens, etc.
 - InCtrl5 - <http://www.pcmag.com/>
 - Similar functionality and creates a report for you of changes
 - Digital signatures help so much here

Defense

- Wireless Networks
 - Avoid automatically connecting to wireless networks
 - KarmSploit and other tools could ruin your day
 - Even if deliberate, *use at your own risk!*
 - Very hard to defend yourself on open wireless networks
 - On your own network(s)
 - Avoid WEP and even WPA as of very recently
 - Use WPA2 with AES encryption if at all possible
 - If in PSK mode, un-guessable passphrase
 - Uncommon SSID (helps avoid rainbow tables)
 - Avoid attributable SSID names (e.g. Joe's Network)
 - MAC-filtering really doesn't help very much
 - Consider alternatives (\$\$)
 - Cellular modem (e.g. 3G, EV-DO, WiMAX, etc.)

Or you could
do this instead...



Defense

- Man-in-the-middle Defenses
 - Infrastructure teams have more options
 - IDS, port-security, Dynamic ARP Inspection (DAI), port authentication (802.1X), Network Access Control (NAC), etc.
 - Can be difficult for mobile users – especially on wireless
 - Awareness is key here
 - Do everything else we've discussed first
 - Use a firewall that has some sort of "ARP Protection" feature
 - Prevents the gratuitous ARP replies from being cached
 - ZoneAlarm Pro has this feature (no enabled by default!)
 - Use a cellular modem instead ☺

Defense

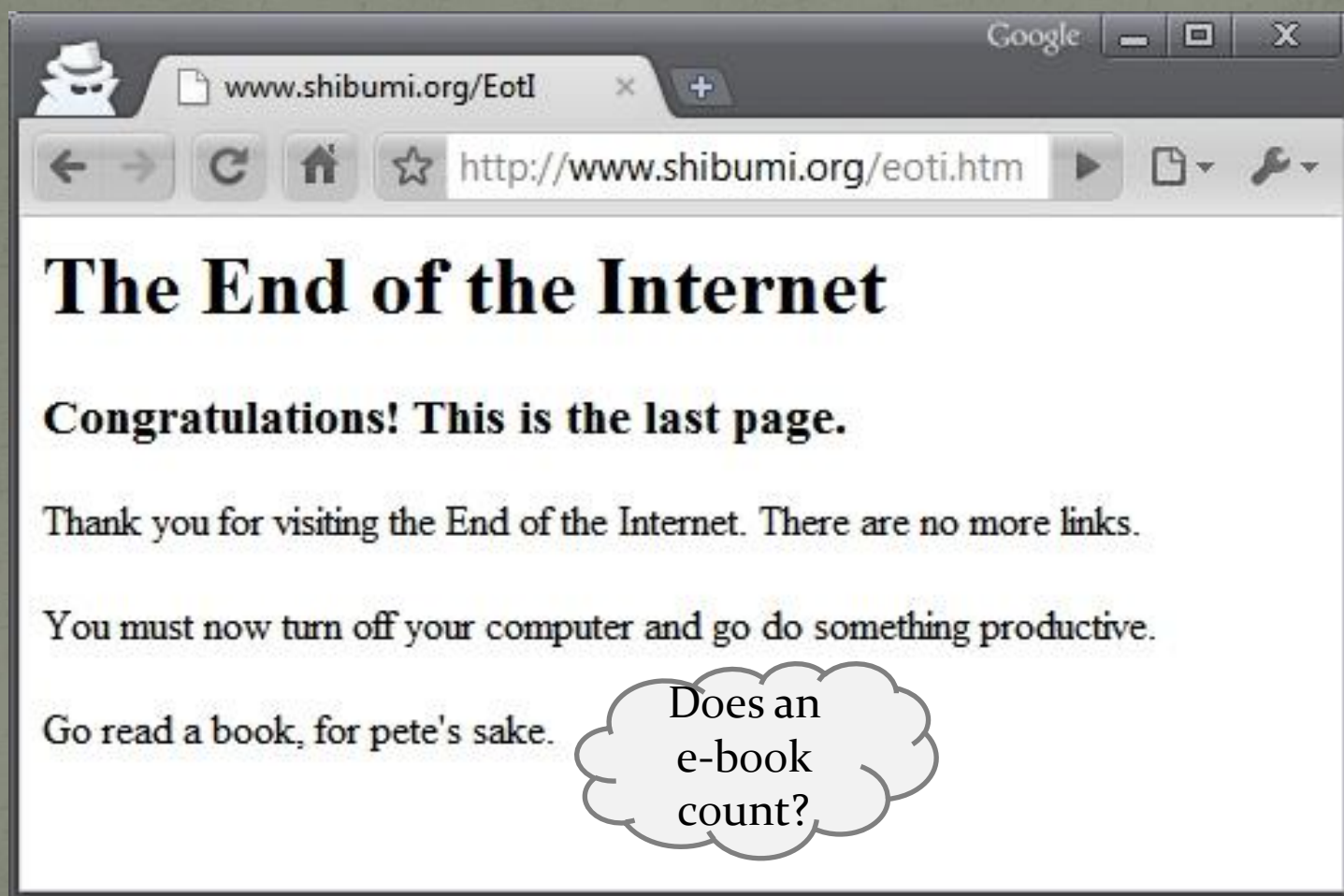
- RFID protection
 - Use an RFID-blocking wallet – no kidding
 - Tell vendors, “I’ll pass, thank you.”
 - Vote for legislation that requires disclosure when used.
 - Support efforts to actually verify their security level.
 - Scan for their presence in your IDs and clothing.
 - Uh, don’t let a chip be injected into your body.
 - Then prepare for it all to happen anyway...



In Summary

- The Net is a very dangerous place.
- It really is the Wild, Wild, Web (WWW) right now.
- We could unplug but...that's not going to happen!
- Remember that our ignorance, arrogance and apathy are the adversary's best friend...
- There is no “silver bullet” for effective defense.
- It takes a combination of people, process and technology working together to make the difference.
 - *You are the people that make it happen... ☺*

And with that, you've reached the...



Thank you for attending!

- Bryce Galbraith
CISSP, GCIH, GSEC, CEH, CHFI, Security+, and CCNA
bryce@layeredsec.com
<http://blog.layeredsec.com/>

...happy surfing! ☺