

ECPE/COMP-178 Computer Network Security

Attack Points

DAY 1

Course Outline

- A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
- B. Ping sweeps, port scans, traceroute, & OS fingerprinting
- C. Attacker Profiles
- D. Attack Points**
 - Human access
 - Physical access
 - LAN (insider) access
 - Remote (Internet) access
 - Wireless access
- E. Anatomy of an Attack
 - Step 1: Target survey
 - Step 2: Vulnerability assessment
 - Step 3: Vulnerability exploitation
 - Step 4: Maintaining access/persistence
 - Step 5: Covering tracks
- F. Physical access attacks
- G. The future: emerging technologies

Attack Points



2

Attack Points

What are the attack points?
What is being exploited?

The exploited vulnerabilities are the same as those exploited by the hackers, criminal organizations, cyberwarriors

It's all the same game!

Attack Points

3

Attack Points

What are the attack points?

Vulnerable	Vulnerable	Vulnerable
HUMANS!	SERVERS!	CLIENTS!

- Being vulnerable means always having to say you're sorry
- Humans are creatures of habit. They will base passwords, PINs, combinations on birthdays, children's names or nicknames, etc.
- When security gets in the way, humans will find a way around it

Attack Points

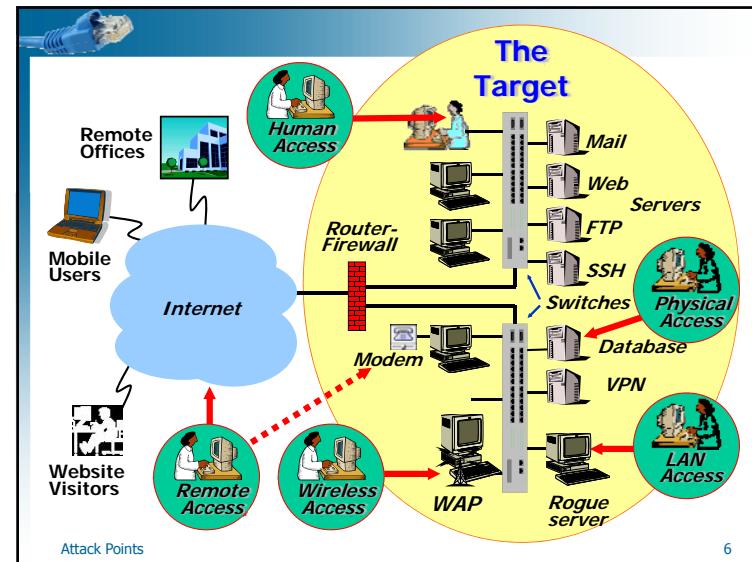
4

Attack Points

- Human access
 - ◆ Social engineering
- Physical access
 - ◆ Supply chain access
 - ◆ Insider access
- LAN access
 - ◆ Behind the firewall, but no physical access
- Wireless access
- Remote access
 - ◆ Attack via the Internet
 - ◆ VPN (or modem) (teleworkers)

Attack Points

5



Attack Points

The attacker must either:

- Have physical access
- Send message/attachment exploiting a human vulnerability
- Know/guess a username and password (i.e. exploit a configuration vulnerability)
- Send message (e.g. a specially constructed packet) exploiting a server vulnerability
- Send message (e.g. from your malicious server) exploiting a client vulnerability

The attacker can now:

- Exploit the victim (e.g. download files from the target, upload executables to the target)
- Maintain access (e.g. upload a back door, modify the registry, install a rootkit)
- Cover tracks (e.g. delete logs)

You will do most of these!

Attack Points

7

Attack Points

- **Exploiting a Human vulnerability** requires sending the target an executable that they must execute, or enticing the target to visit a malicious website, or simply guessing a password
- **Exploiting a Configuration vulnerability** requires knowing or guessing the vulnerability – for example, a default username and password
Password = username, blank, username-reversed Dictionary attack
- **Exploiting a Server Program vulnerability** requires sending the server a malicious message that, for example, overflows a buffer and then pushes a shell to the attacker
- **Exploiting a Client Program vulnerability** (e.g. IE) requires sending the target an executable that they must execute, or enticing the target to visit a website with a malicious webpage that exploits the target's browser

Attack Points

8

Low-tech Fraud

Man Pleads Guilty to Breaking Into eBay Accounts

March 21, 2007, www.theregister.co.uk

- An Australian man plead guilty to breaking into 90 eBay accounts and using them to steal US \$34,000. He also broke into email accounts and a bank.
- He advertised non-existent iPods via the hacked eBay accounts pocketing the money from the fraudulent sales.
- Faces up to 11 years in jail and fines of US \$8,007.
- Apparently guessed most of the eBay account passwords.

Attack Points 9

Lame Passwords

Lax passwords expose quarter of PC users to theft

- McAfee survey findings indicate 25% of computer users in Europe are at risk from online fraud owing to poor password habits (3,500 respondents)
- 43% never change their passwords
- 24% use same password for all online accounts
- 59% always or mostly use same password for everything
- 30% use passwords of only 1 to 6 characters in length
- 61% do not have pin codes to protect their mobile devices
- Of those having pin codes, 29% only use default settings.

Countermeasure: Enforce a password policy & policy setting!

At least make it a challenge...

Attack Points 10

Any phish will byte good bait



Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

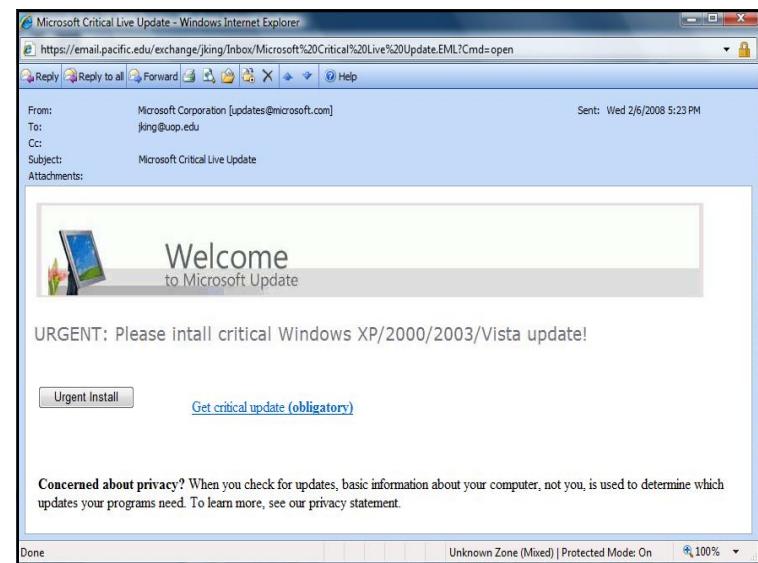
<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Attack Points 11



The screenshot shows a Microsoft Critical Live Update window in Internet Explorer. The email subject is "Microsoft Critical %20Live%20Update.EML?Cmd=open". The body of the email reads:

From: Microsoft Corporation [updates@microsoft.com]
To: jking@uop.edu
Cc:
Subject: Microsoft Critical Live Update
Attachments:

The message content is:

Welcome to Microsoft Update

URGENT: Please install critical Windows XP/2000/2003/Vista update!

[Get critical update \(obligatory\)](#)

Concerned about privacy? When you check for updates, basic information about your computer, not you, is used to determine which updates your programs need. To learn more, see our privacy statement.

Done Unknown Zone (Mixed) | Protected Mode: On 100%

Phishing

A closer look...

Attack Points

13

Email – April 2011

Salam,

Regards to adverts of possible investments, I wish to bring to your notice our interest to partner with you/your company for great business prospects.

Kindly furnish me with a business plan and proposal for a Joint venture/partnership with you/your company.

We look forward to going into a good business relationship with you or your company. May the peace of Almighty Allah be with you all and my regards to your families.

Abdul Mohsen Ahmad Algosaibi
General Director.
Ahmad Hamad Algosaibi & Bros.

Address Info

Partial SMTP header

```
Return-Path: <mailto:mohsenalgosaibi.com>
Received: from RD00155D313FE0.mail.com ([70.37.89.77])
```

Mail.com is a webmail service

```
# dig -x 70.37.89.77
;; QUERY: 1, ANSWER: 0, AUTHORITY: 1
;; AUTHORITY SECTION: msnhst.microsoft.com.
```

SMTP Return address

```
mohsenalgosaibi.com. A 85.233.160.70
Netblock: Namesco – UK Registrar/Hosting provider
```

Name and Company Lookup

Where is the beef?
But it is at least a start!

Bloomberg
Businessweek

INDUSTRIAL CONGLOMERATES
A. H. Algosaibi & Bros. Co.

Snapshot People

Overview Board Members Committees

EXECUTIVE PROFILE

Abdul Mohsen Ahmad Algosaibi
Director, A. H. Algosaibi & Bros. Co.

Age Total Annual Compensation This person is connected to 1 Board Members in 1 different organizations across 1 different industries.

See Board Relationships

BACKGROUND

Abdul Mohsen Ahmad Algosaibi serves as a Director of Ahmad Hamad Algosaibi & Bros.

CORPORATE HEADQUARTERS There is no corporate data available.

ANNUAL COMPENSATION There is no Annual Compensation data available.

BOARD MEMBERS MEMBERSHIPS Director A. H. Algosaibi & Bros. Co.

STOCK OPTIONS There is no Stock Options data available.

TOTAL COMPENSATION There is no Total Compensation data available.



Wikipedia Entry

A blue network cable with a RJ45 connector is shown against a white background.

Adobe Hit With Zero-Day

Again....and again....and again...

Security Advisory – [insert date]

A critical vulnerability exists in Adobe Flash Player..

A critical vulnerability exists in Adobe Reader..

A critical vulnerability exists in Adobe Acrobat..



Aug 2010 - Malware Widget

- "Small Business Success Index" widget offered by Network Solutions and Widgetbox
- Part of the standard NSI domain parking page
- Infected with r57shell – and found on
 - ◆ 500,000 Websites
 - ◆ 5 million Network Solutions parked domains

A screenshot of a web browser displaying the homepage of "grow smart business". The page features a large banner with the site's name and a subtext "Benchmarks, articles, and tools to help grow your small business". Below the banner are several navigation tabs: HOME, RESEARCH, BLOG, RESOURCES, SURVEY, and ABOUT. On the left side, there are three main call-to-action boxes: "Small Business Success Index", "Small Business Success Index", and "Badges". Each box contains a "Take Survey Now" button. The "Badges" box also includes a "Get Widget" button. To the right of these boxes is a sidebar titled "Small Business Success Index" which lists various metrics with their current status (e.g., SISI INDEX: 75 C, Capital Access: 87 C). At the bottom of the sidebar is a "Read More" link. The browser's address bar shows the URL "http://growsmartbusiness.com/badges/" and the search term "ipad".

Shell Behind The Widget

The screenshot shows a web browser window with three tabs open. The main tab displays a MySQL database interface with several dropdown menus and input fields. Below this is a search results page for 'Microsoft' on a website called 'grow smart business'. At the bottom of the browser window, there's a navigation bar for 'network solutions'.

Attack Points

PHYSICAL ACCESS

If the machine is on...

- View documents
- Copy files
- Retrieve hashed passwords
- Install tools and rootkits
- Modify the Registry

If the machine is off....boot from a CD and ...

- View documents
- Copy files
- Retrieve stored password hashes from the hard drive
- Install tools and rootkits
- Modify the Registry

You will do the above

Attack Points

Physical Access

"10 Immutable Laws of Security" @ Microsoft TechNet

#3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore

- Can open the case and replace BIOS chips [Osbroke](#)
- Can remove your hard drive, clone it, take that to read, conduct brute-force attacks.
- Can replace keyboard with one that contains a radio transmitter. They could then monitor everything you type, including your password.

Attack Points

Physical Access

Supply Chain Access

- In October 2008 The Office of the National Counterintelligence Executive (ONCIX) warned that credit card readers used at point of sale in Europe had been tampered with, either where manufactured (China) or in transit to financial institutions. Credit card information intercepted by the rogue devices was being relayed back to criminals in Pakistan and China via the mobile phone network.

YASA - Yet Another Security Agency

Attack Points

Supply Chain Attacks

Age of Globalization

- Can the supply chain be secured?
- Why send malicious code via Internet if you can pre-infect parts or consumer devices?
- Malicious or from 'improper digital hygiene'?

Vectors

- Designers & Developers (hardware & software)
- Testers, Sysadmins
- Shippers, Janitors
- Business partners w/ 'inside' network connections

Diversion to Counterfeit/Grey Market

Attack Points 25

Certified Pre-Own3d

- Digital Picture Frames – *win32Mocmex.AM*
- USB thumb drives – *w32Fakerecy, w32.SillyFDC*
- **TomTom** GPS devices – *win32Perlovga.A Trojan, backdoor*
- **Seagate** Hard drives – *win32.AutoRun.ah*
- MP3 players – *worm.win32.Fujack.aa*
- **Apple** Video iPod – *RavMonE.exe virus*
- **Razer** device drivers - *Worm*
- **Cisco** VPN Client CD – *Mexican Narco Corridos MP3s*
- **Energizer** USB Charger - *Trojan* 2010
- **Vodafone** HTC phone – *mariposa bot*
- Dell Rack Server – *malware*
- **Olympus** camera – *autorun worm*
- IBM USB drive distributed at AusCERT - *malware*
*Creative * HP * ASUS * Toshiba*
www.attrition.org/errata/cpo/

Attack Points 26



Certified Pre-Own3d - more

- **Amazon** EC2 Cloud Image – *SSH key pre-authorized*
- **Cisco** Info/Warranty CD – *Links to malware repositories*
- **HP Procurve Switch** - *Virus*
- **Cisco** Cisco & Linksys Routers – *Forced update with Cloud Connect service that tracked complete Internet history* 2012
- **Multiple** Whitebox desk/laptops – *Nitol botnet*

www.attrition.org/errata/cpo/

If it happens to top tier manufacturers –
what is happening at others?



Attack Points 27

Computer Supply Chain Sources

	Dell	HP	Lenovo
System Design	China, US, Singapore, Taiwan, India	US, India	China, US, Taiwan, Japan
Motherboard Assembly	China	China	China
System Assembly	China, US, Brazil, Ireland, Malaysia	China, Canada, US, Czech Republic, India, Australia	China, Mexico, Hungary, India, Japan, Czech Republic, Brazil
BIOS Design	China, US, India	China, US, India	China, US, Japan

Most use the same BIOS suppliers

BIOS Suppliers	Phoenix, Award, Internal	Phoenix, Award, Softex, AMI, Award, Internal	Phoenix, Award, Insyde, AMI, Internal
----------------	--------------------------	--	---------------------------------------

Supply Chain Risk Management Software Assurance Forum October 2008

Attack Points 28

Supply Chain Attack - 1982

- Soviets obtained Western technology for Siberian Natural Gas pipeline
- CIA had added extra features to pipeline software
- Pumps & valves would exceed design limits
- Resulted in an enormous explosion
- NORAD thinks it's the bomb
- National Security Council then briefed by CIA

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

Attack Points



29

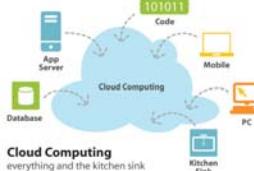
Physical Access

Outsourcing can provide the physical access

- Less physical control of computers and networks
- Less oversight of staff (hiring, practices)
- Less control over Intellectual Property (IP)
- Less control over Confidential Information (SSNs)
- Harder to detect a leak or breach
- May increase risk from local employees (revenge)
- Cloud Services – Outsource w/abstracted location
- Cloud email & email sanitation
- Cloud data storage

Reboot the Cloud!

Attack Points



Cloud Computing
everything and the kitchen sink

-MOTD-

12.5% OF THE PLANETS HAVE
71% OF THE MASS



#OCCUPYJUPITER

Attack Points

31

Hackers Strut Their Stuff in Las Vegas

8/6/07 www.taipeitimes.com

Hackers gathered in Las Vegas showed ways to crack electronic key-card systems used at security-sensitive places including the White House and the Pentagon. Zac Franken uses simple electronics in a device that can be spliced into wires connecting key card readers to computer systems that control door locks on many businesses.

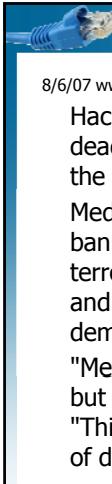
7/25/12 Computerworld

Black Hat presenter demonstrates that 5 million Onity keycard-protected hotel rooms can be hacked w/ \$20 worth of hardware. Access takes only 200 ms.

Attack Points



32



Hackers Strut Their Stuff in Las Vegas

8/6/07 www.taipeitimes.com

Hackers gathered in Las Vegas showed ways to crack deadbolt locks used at security-sensitive places including the White House and the Pentagon.

Medeco deadbolt locks, relied on worldwide at embassies, banks and other tempting targets for thieves, spies or terrorists can be opened in seconds with a strip of metal and a thin screw driver, Marc Tobias of Security.org demonstrated.

"Medeco has one of the best designed locks in the world, but with this kind of attack it's all irrelevant," he said.

"This is not the only company. There are lots of them; lots of deadbolts with similar weakness."



Attack Points

LAN Access

News!

Fine & Community Service for Wireless Piggybacking

May 24, 2007, www.woodtv.com

- Sam Peterson will perform 40 hours of community service and pay a US \$400 fine for using a wireless network without permission. Peterson parked outside a Wi-Fi cafe in Sparta, Michigan and checked his email on a daily basis. *If he had gone inside for a cup of coffee and used the Internet while there, there would have been no grounds for prosecution.*
- The cafe's owner was unaware that Peterson's activity was illegal in Michigan. Peterson was caught because the local police chief became suspicious of him sitting in his car using his computer outside the cafe.

Attack Points 37

Bluetooth Devices

- Over 1B Bluetooth devices – Ubiquitous Networks
- Printers, laptops, keyboards, cars, cellphones
- 48-bit device identifier
- first 3 bytes = manufacturer, last 3 unique (in theory)
- Discoverable and non-discoverable modes
- Bluesnarfing - data, calendar, phonebook, image theft
- Bluebugging - unauthorized connection to serial profile
- Bluesniffing - commands, events, packets
- Bluesniping - long-distance attacking
- Bluesmacking - buffer overflow, DOS

Attack Points 38



Bluetooth Devices

Basic Bluetooth security tips

- Enable Bluetooth only when you need it
- Keep the device in non-discoverable (hidden) mode
- Use long and difficult to guess PIN key when pairing the device (key such as 1234 is unacceptable)
- Reject all unexpected pairing requests
- Check list of paired devices from time to time to ensure there are no unknown devices on the list
- Update your mobile phone firmware to a latest version
- Enable encryption when establishing BT connection to your computer

Attack Points 39



Attack Surfaces



Attack Points 40

 **Steal Cars With A Laptop**

NEW YORK - Security technology created to protect luxury vehicles may now make it easier for tech-savvy thieves to drive away with them.

In April '07, high-tech criminals made international headlines when they used a laptop and transmitter to open the locks and start the ignition of an armor-plated BMW X5 belonging to soccer player David Beckham, the second X5 stolen from him using this technology within six months.

Beckham's BMW X5s were stolen by thieves who hacked into the codes for the vehicles' RFID chips ...

[Attacks - Update](#) 41




 **Misc. Wireless Attack Points**

Radio-frequency identification (RFID)

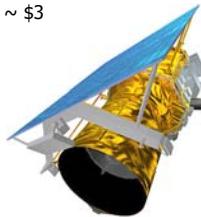
- Passports, credit cards, toll collection, inventory
- Readers can be made for under \$10



2011 ~ \$.05



2011 ~ \$3



Satellites

- Satellite Internet
- Hijacking U.S. military satellite transponders ~ CB's
- Jamming ~ Captain Midnight, HBO, & Galaxy 1
- Bouncing video off of transponders ~ pirate TV

[Attack Points](#) 42

 **Satellite Attacked**

- In 2007 and 2008 two NASA/USGS satellites were attacked multiple times via a ground station connected to the Internet. Landsat 7 and Terra AM-1 earth mapping satellites were accessed, the latter one was under the control of the attackers but not tampered with.

Hackers are not rocket scientists

[Attack Points](#) 43



 **Attack Points**

Remote (Internet) Access

Research (recon)

- ARIN (American Registry for Internet Numbers)
- Target website
- Google hacking
- IP sweeps & port scans
- Vulnerability (Pen) tests

Exploit

- User vulnerabilities
- Configuration vulnerabilities
- Client vulnerabilities
- Server vulnerabilities
- User cluelessness – (Go2MyPc)

[Attack Points](#) 44



Attack Points

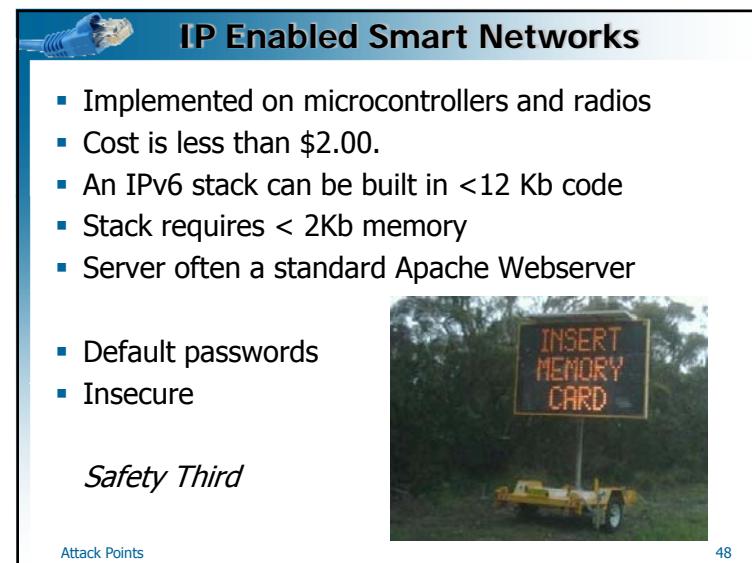
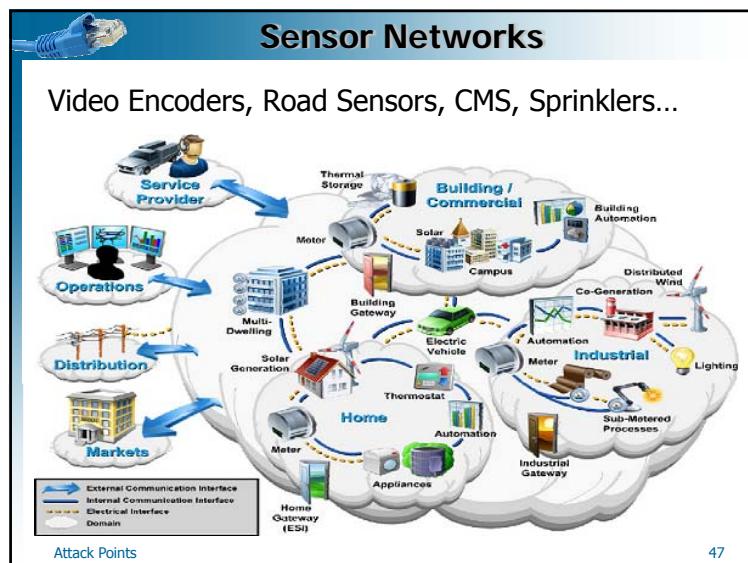
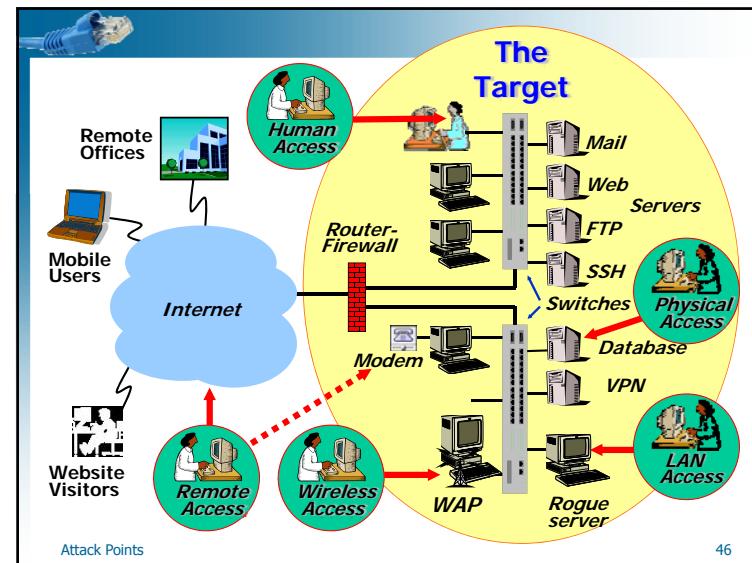
Remote Access (MODEM, VPN, Teleworkers)

- MODEM (Faxmodem) + NIC = Backdoor
- Built into many desktops – even today - invisible
- User wants access to desktop – turns on RAS
- Legacy modems in closets attached to servers/routers
- War dialing (often part of pen test)
- Indirect access via Teleworkers
- Home networks easier to breach (DSL, cable)
- Home computers lacking corporate AV, policies
- Home computers may be running P2P clients
- Ride along on their VPN link

The 'outside' is now 'inside'...



Attack Points 45



Tools

Where do tools come from?



Attack Points

49

Tools

Where do tools come from?

- Someone else writes them
 - ◆ (ECPE/COMP-178's tools)
- Attacker writes
 - ◆ The vulnerability is a zero day gift
 - ◆ The vulnerability is attacker's zero day
 - ◆ The vulnerability is in the public domain
- Attacker adapts from an existing public exploit
 - ◆ Reverse engineer the hacker tool or the patch

Given away Traded Sold (PayPal) Stolen

Attack Points

50

Malware Trend

Malware and hacking - bigger problem than ever

- Even though we do recommended stuff
 - ◆ Patch, Passwords, AV client, etc.

The current Malware model

- Largely trojans, worms, downloaders
- Professionally written
- Criminally motivated and funded
- 90+% of compromised records – criminal sector
 - ◆ Records, not mere credentials



Attack Points

51

Malware Cycle

- Email contains initial downloader
or
- Induced (SEO, email) to visit website with payload
 - ◆ Website may be "innocent" or clueless
 - ◆ Most (77%) are legitimate
 - ◆ Malicious ads from legitimate ad services
 - ◆ Malicious sponsored ads on search engines
 - ◆ Poisoned search engine results
- Downloader starts larger download (may delay)
- Checks in to bot command and control
- Waits for instructions

▪ Mobile – a new opportunity



Attack Points

52

SEO Black Hat

Link farm: a group of sites and web pages hyperlinked to each other to increase their *PageRank* in the search engines

Keyword stuffing: hackers add many extra pages to compromised websites (Link farms) that contain:

- ◆ topic-related keywords and
- ◆ content taken from legitimate sites & feeds

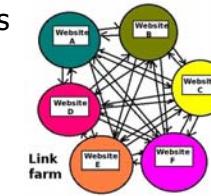
Search engine spiders find what appears to be valid content relevant to the keywords used, and no malware (pages appear safe – but they are not, depending on user agent string, etc.)

Attack Points

53

Link Farming

- Millions of deceptive (small malicious) web sites exist
- Use 'Bulletproof' hosting firms (spam R us)
- Look real – but are bogus content
- Teams dedicated to promoting/reviewing on blogs
- Used for SEO to cook rankings



- Double-Click (Google) served malvertisements
- King Features (Comics!) had malicious PDF's

Attack Points

54

SEO Poisoning

Cloaking: webserver hosting SEO Poisoned misleading pages looks at two HTTP fields it gets from each browser visiting a page:

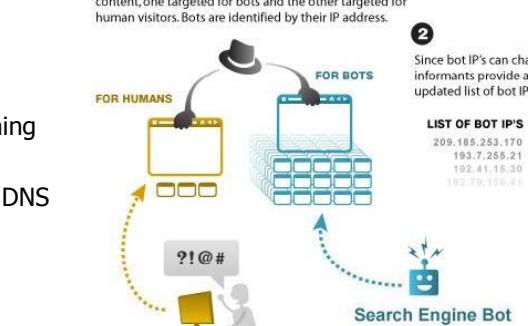
- *HTTP referrer:* the link the browser followed
- *User Agent String:* identifies the browser type
- ◆ Browsers from an SEO poisoned link are redirected to a server hosting malicious page (e.g. fake AV)
- ◆ A search-engine bot crawling the page is given the misleading content...which appears ok
- ◆ Text-based browsers (security researchers?)
- Are avoided, redirected to CNN

Attack Points

55

SEO Cloaking

- 1 Sites engaged in black hat SEO prepare two sets of content, one targeted for bots and the other for human visitors. Bots are identified by their IP address.
- 2 Since bot IP's can change, black hat informants provide a regularly updated list of bot IP addresses.
- 3 Bots are served abundant fabricated content packed with targeted keywords. This false information boosts rankings.
- 4 Human visitors often won't find the best information despite the site's high rankings.



Attack Points

56

SEO Poisoning

- SEO poisoned news event link
- Which redirects to a malicious page that injects malware or a fake alert message
- Obfuscated code on malicious page

Be careful of links when searching...

Attack Points 57

The screenshot shows a search result from 'All Salon . Salon.com' dated 27 Feb 2010. The URL is 'http://www.salon.com/video/live_hawaii_tsunami_in_asia_south_east_asia_1.1000000000000001'. The page content includes a video player and satellite images of Thailand before and after the tsunami.

Browser Vulnerabilities

Period	Chrome	Safari	Firefox	Internet Explorer	Opera
2010	191	119	100	59	31
2009	41	94	169	45	25

Attack Points 58

Acrobat – huge problem
Java – just say no

Adobe Default

- No!

Attack Points 59

The screenshot shows the 'Trust Manager' settings in Adobe Reader preferences. The 'PDF File Attachments' section has a checkbox 'Allow opening of non-PDF file attachments with external applications' checked. Other sections like 'Automatic Updates' and 'Internet Access from PDF Files outside the web browser' are also visible.

Trojan Payload

- Fakeware/Scareware
 - ◆ Fake Security Scanner
 - ◆ Fake Anti-Virus Scanner
- Ransomware
- Fake Password Vault
- Google search: fake antivirus popup 469,000 results
- Now click on images tab

Attack Points 60

The screenshot shows a 'Critical Systems Warning!' dialog box with the text: 'Your system is probably infected with latest version of Trojan-Adw-X.a. Full system optimization will greatly increase your computer's performance and prevent data loss. Click OK to download anti-virus software! (Recommended)'. There are 'OK' and 'Cancel' buttons at the bottom.

SHIELD YOUR EYES

Fakeware

- Kit based
- Free to \$2,000 USD

Attack Points

61

Fake Piracy Scam

- Claims to detect pirated files - sets wallpaper to:

Warning! Piracy detected!

Pirated content was detected on your PC!
You are seriously violating copyright by:
 - Media files downloaded from torrents
 - Pirated movies from peer-to-peer networks
 - Cracked software from file-sharing services

 Copyright fund has received report and has started an investigation. You'll receive subpoena in a week

RIAA MPAAP copyright alliance

Attack Points

62

Fake Piracy Scam

- Tax on clueless
- Traffic fee?
- Fraud warning?
 - Irony Meter Pegs

Thank you for your decision. The program of Internet piracy disengagement is based on the consent of every citizen having the right to an amnesty if the unlawful exchange of intellectual property (music, films, software etc.) does not take place repeatedly.

You can pay the damages, as well as a fine and proceed to express to the copyright holder in exchange for a waiver of liability. After payment, you will receive a certificate that will give the bill issued by our organization. Once the bill is settled, you get the right to use the items of intellectual property obtained via the Internet, while all the issues with the copyright holder will be settled.

STATEMENT

Description	Price
Legal license purchase	\$15
Copyright holder fee	\$249
Damage compensation for the use of intellectual property obtained via the Internet	\$126
Traffic fee	\$1
Total:	\$99.85

Payment Information

Cardholder Name: FirstLast
 Card Number: 1111222233444444
 Expiration date: 01 / 2011
 CVV2/CVC2: 123 [What is CVV?]

Your IP address, billing information and connection information will be recorded, traced and checked for fraud. All fraudulent transactions will be investigated and prosecuted in accordance with applicable law.

Proceed

After pressing "Proceed", your information will be verified. This will take approximately 30 seconds. Please, do not reload or refresh the page.

Attack Points

63

Infection Injection Detection

- July 28, 2011 90,000+ pages compromised in mass iFrame injection attack

Google

"http://willysy.com/images/banners/"

About 21,000 results

TRISPORT-iframe src="http://willysy.com/images/banners/"/ style...
 Register Now. GET BY GET. 1. Add event to your cart. 2. Click Checkout. 3. Register your details or login using your existing account ...
 carlinspeaks.com/links/2.html

pornify-iframe src="http://willysy.com/images/banners/"/ style...
 porn messages. If there are any error warning messages shown above, please correct them first before proceeding. Error messages are displayed at the very ...
 www.pornify.com/links/2.html

gamerhost-iframe src="http://willysy.com/images/banners/"/ style...
 1 day ago ... (Degenero, Apple, Bladegix, Game Center, Megalomix, NHCX, Playstation1.P, TNN, V-P, Imprenta1, reginawill1, ...
 gamefocus.co.uk/ ... Cached Google

10minutelinkstrack.org="http://willysy.com/images/banners/"/ style...
 1 day ago ... Pumeroku.us/line src="http://willysy.com/.Base.Wax-HighFlur-Finish-Brige-Trails-Power-Trails-Henrich-X-Aztecseries...
 www.10minutelinkstrack.org/ ... Cached Google

Attack Points

64

Zeus

- ZeuS trojan – steals banking information
- Malware-in-the-middle form grabbing
- Targets Windows New: BlackBerry, Android
- Source and binaries found on GitHub in 2011
- Common in social media sites
- The most established toolkit, very configurable
- Data exfiltration/C&C via RC4 encrypted HTTP post, e.g. designed to go through firewalls
- Product activation key (similar to Windows)
- Polymorphic – each install has unique signature
- Dashboards track bots, product payment
- Granular management, metrics w/ drill-down info

Attack Points 65

Zeus Banking Toolkit

- ZeuS trojan is 'Man in the Browser' MITB
- Waits for banking transaction to occur
- Can modify/inject data to either side
- Bank sees transactions from authenticated user
- User sees real bank website (and more)
- ZeuS makes extra transaction(s) - sent to mules



Attack Points 66

Zeus Banking Toolkit

- *Injecting some harvesting code into the legitimate website is exponentially more effective at harvesting credentials than redirecting to a fake banking site*
- *...and almost impossible to detect*
- *ZeuS is the browser in the middle!*

Attack Points 67

Command & Control Servers



ZeuS
461 online 22:34 Feb 02, 2013
Source: zeustracker.abuse.ch

Attack Points 68

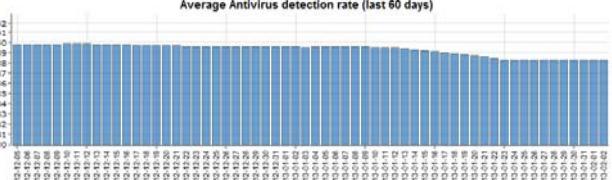
Zeus Meets – Kicks AS

Top ten Zeus hosting ISPs (by number of Zeus C&Cs)

ZeuS C&C count	AS number	AS name
193	8075	MICROSOFT-CORP---MSN-AS-BLOCK - Microsoft
12	33182	DIMENOC---HOSTDIME - HostDime.com, Inc.
12	36351	SOFTLAYER - SoftLayer Technologies
11	35818	WEBFACTOR-4S Webfactor SRL
10	8426	CLARANET-AS ClaraNET
6	21844	THEPLANET-AS - ThePlanet.com Intern
5	16265	LEASEWEB LEASEWEB AS
5	24940	HETZNER-AS Hetzner Online AG RZ
5	32475	SINGLEHOP-INC - SingleHop
5	34282	UKNOC-AS UKNOC AS



Average Antivirus detection rate (last 60 days)



Attack Points

69

Phishing

- Targeted SpearPhishing
- May spoof to look internal
- Sender has internal details (research)
- Targets senior executives
- Targets accounting to access payroll
- Payload targets
 - ◆ Adobe
 - ◆ MS Office

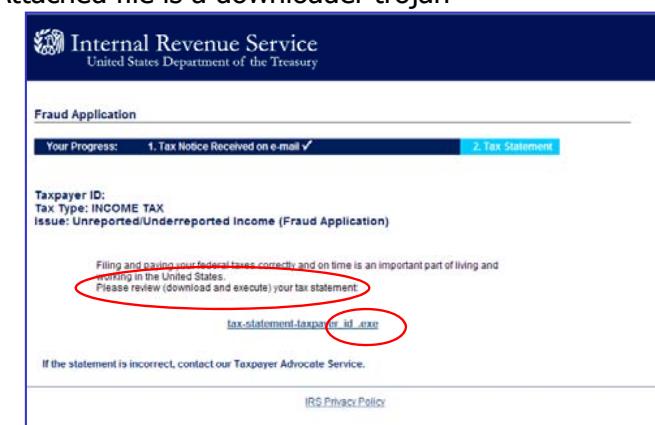


Attack Points

70

Fake IRS Notice

- Attached file is a downloader trojan



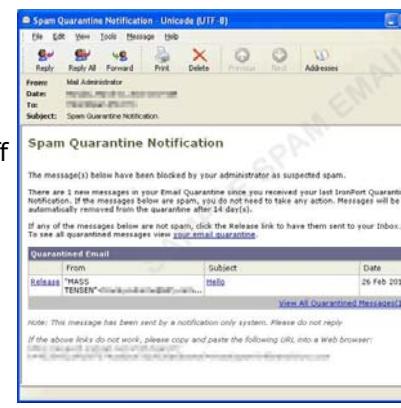
Attack Points

71

Fake Email Quarantine

Fake SPAM quarantine

- Fake bounce notice
- All links lead to a downloader trojan
- Who from?
- SMTP headers a tipoff
 - ◆ Not easy to find



Attack Points

72

Fake Sirius Notice

Important Information About Your SIRIUS Service
Call 1-866-935-9116.

YOUR ACCOUNT REQUIRES ATTENTION

Account Number: 3009663047
Dear RICHARD,

Our records indicate that the card on your account was reported lost or stolen by the existing company. As a result, the payment for your SIRIUS service was not processed.

To ensure you continue listening to your favorite SIRIUS programming, update your billing information with a new credit card. Simply go online to make a payment. It's safe, secure, and fast!

If you have questions about your bill or account, you can speak with a SIRIUS Customer Care Representative at 1-866-935-9143.

Thanks,
The SIRIUS Team

PAY ONLINE - QUICK AND EASY >

Attack Points

73

Fake Sirius Notice

EVERYTHING WORTH LISTENING TO IS ON SIRIUS XM SATELLITE RADIO

Please note: this is not a promotional e-mail. As a SIRIUS subscriber, you will periodically receive service notices via e-mail. These service notices are intended to provide you with helpful information that will facilitate and enhance your SIRIUS listening experience.

Have you moved or changed your billing information? Please take a minute now to update your account information.

You can read our entire [Privacy Policy](#).

SIRIUS® Radio
1221 Avenue of the Americas
New York, NY 10020
www.sirius.com
Customer Care: 1-868-539-SIRIUS
Schedule and channel assignments are subject to change. Check sirius.com for the latest updates.

© 2010 SIRIUS XM Radio Inc. SIRIUS, XM and all related marks and logos are trademarks of SIRIUS XM Radio Inc. and its subsidiaries. All other marks, channel names and logos are the property of their respective owners.

Attack Points

74

Crime Does Pay

- Oct. 2012 FTC - Federal Court Judgements
- U.S. Participants (a tiny spec)
- Kristy Ross – must return \$163M
- Marc D'Souza – must return \$8.2M
- Officers/Directors of two businesses used "to conduct a massive 'scareware' scheme that marketed a variety of computer security software via deceptive advertising."
- Belize - Innovative Marketing, Inc. (IMI)
- Cincinnati - ByteHosting Internet Services

Attack Points

75

Course Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
 B. Ping sweeps, port scans, traceroute, & OS fingerprinting
 C. Attacker Profiles
 D. Attack Points

- Human access
- Physical access
- LAN (insider) access
- Remote (Internet) access
- Wireless access

 E. Anatomy of an Attack

- Step 1: Target survey
- Step 2: Vulnerability assessment
- Step 3: Vulnerability exploitation
- Step 4: Maintaining access/persistence
- Step 5: Covering tracks

 F. Physical access attacks
 G. The future: emerging technologies

Overview of who they are and where they get in....

Now its 'How'

Attack Points

76

