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

What are the attack points?
What is being exploited?

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

It's all the same game!

Attack Points

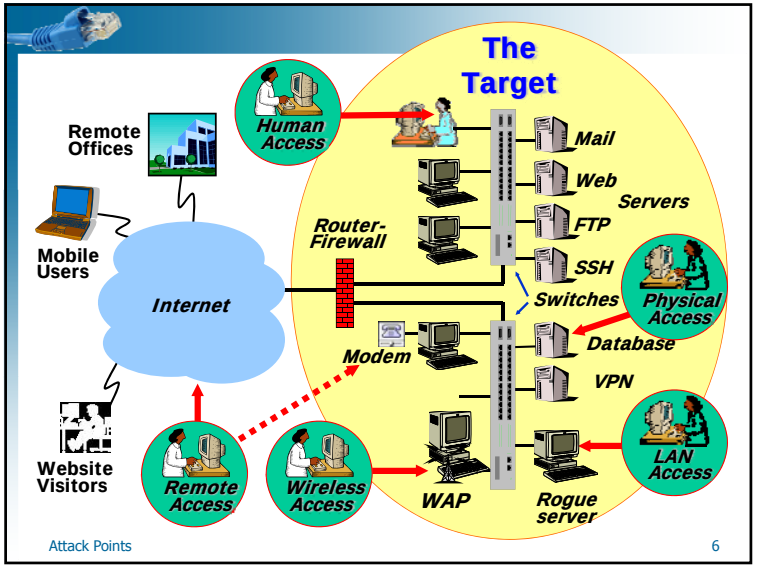
What are the attack points?

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

- **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

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

- 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

Low-tech Fraud

Man Pleads Guilty to Breaking Into eBay Accounts

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

- 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.

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...

Any phish will byte good bait

TrustedBank™

Dear valued customer of TrustedBank,

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

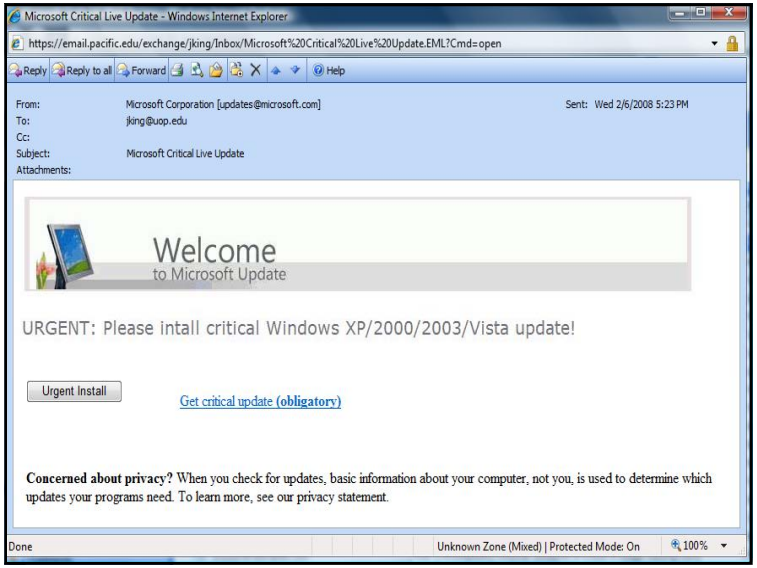
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

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

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

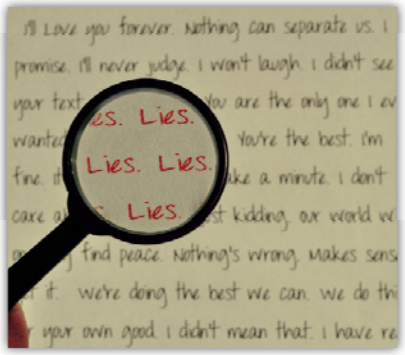
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.



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: <mailbox@**mohsenalgosaibi.com**>
Received: from RD00155D313FE0.mail.com ([70.37.89.77])

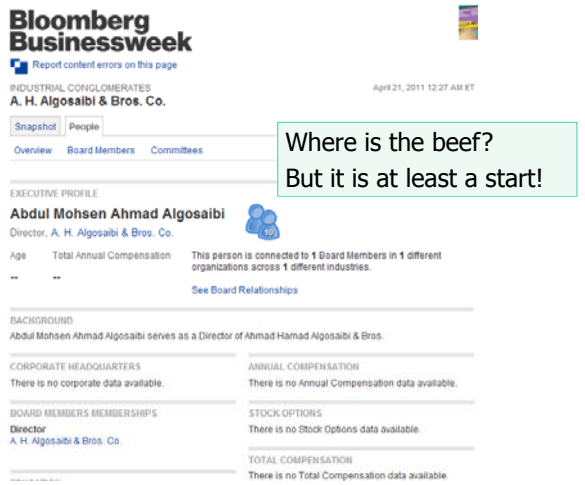
Mail.com is a webmail service

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!

Wikipedia Entry

The Al Gosaibi family (Arabic: القصيبي, classical Arabic al-Qusaibi) is a prominent Arab family in Bahrain and the Eastern Province of Saudi Arabia. It is a trading family, involved in many successful businesses.

Phishing attempts are getting better….

No english spelling errors, grammar errors

Domain name matches family name

Some reseach, domain registration, involved

Adobe Hit With Zero-Day

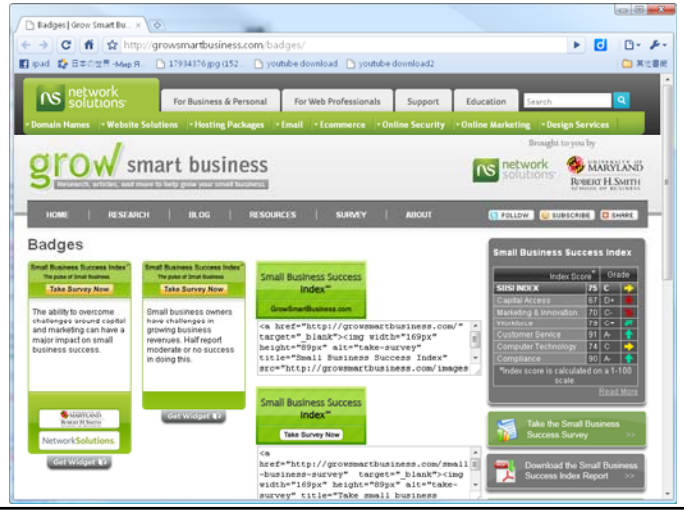
Again….and again….and again…

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..

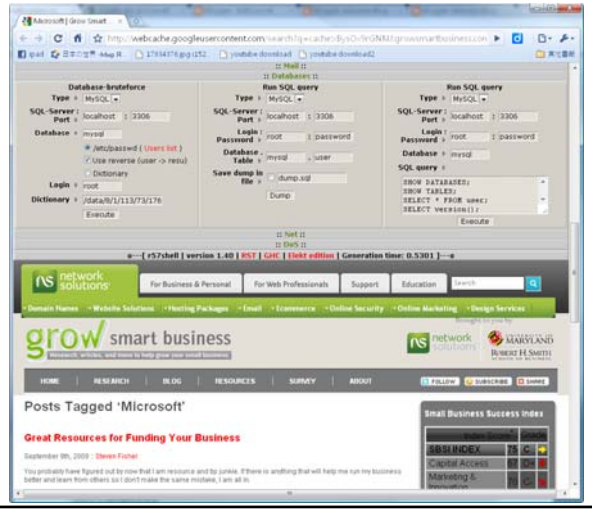
Aug 2010 - Malware Widget

- "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

Widgets For The Masses



Shell Behind The Widget



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***

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.

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*

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

Certified Pre-0wn3d

- 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**
- Vodaphone 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/

Certified Pre-0wn3d - 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?

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

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

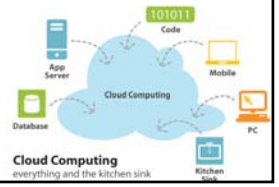
- http://en.wikipedia.org/wiki/Farewell_Dossier

Physical Access

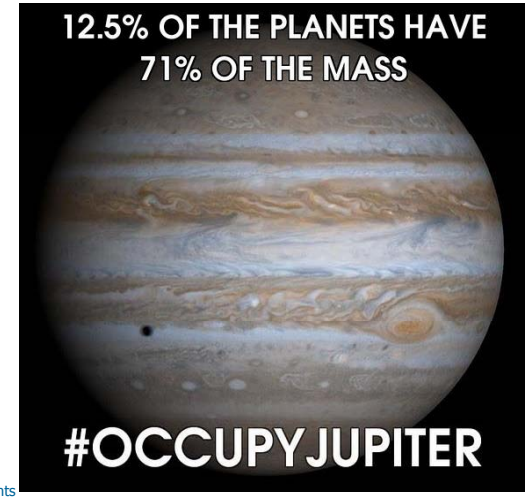
Outsourcing can provide the physical access

- 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!



-MOTD-



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.

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 lot of them; lots of deadbolts with similar weakness."

Attack Points

LAN Access

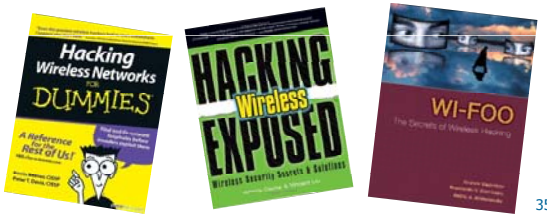
- View shares on Windows computers
- Grab usernames/privileges on Windows computers
- Grab password hashes on Windows computers
- Hack the ARP cache for man-in-the-middle attack
  - Ettercap lab does this
- Default 'workgroup' – browse for booty
- Null session exploit – enumerate users, shares
- Shared storage – files, software, license keys

This LAN is your LAN.....and now
...This LAN is my LAN

Attack Points

Wireless Access

- From a laptop "View wireless networks"
- Connect to unprotected networks – Wardriving
- Launch Wireshark and observe traffic
- Crack WEP keys, WPA keys, maybe WPA2 keys
  - www.wardrive.net



Attack Points - Warcarting (MIT)

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.

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

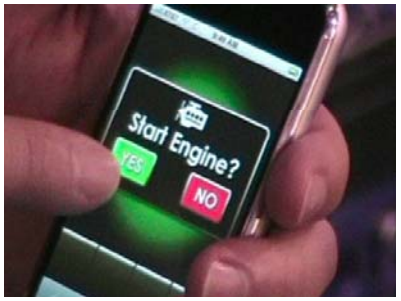
- Bluesnarfing - data, calendar, phonebook, image theft
- Bluebugging - unauthorized connection to serial profile
- Bluesniffing - commands, events, packets
- Bluesniping - long-distance attacking
- Bluesmacking - buffer overflow, DOS

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 Surfaces



Steal Cars With A Laptop

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

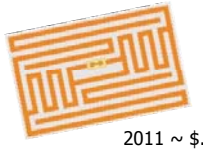
In April '07, high-tech criminals made international headlines when they used a laptop and transmitter to open the locks and start the ignition of an armor-plated BMW X5 belonging to soccer player David Beckham, the second X5 stolen from him using this technology within six months.

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

Misc. Wireless Attack Points

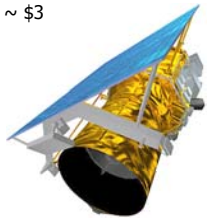
Radio-frequency identification (RFID)

- 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*

Satellite Attacked

- In 2007 and 2008 two NASA/USGA 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

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)

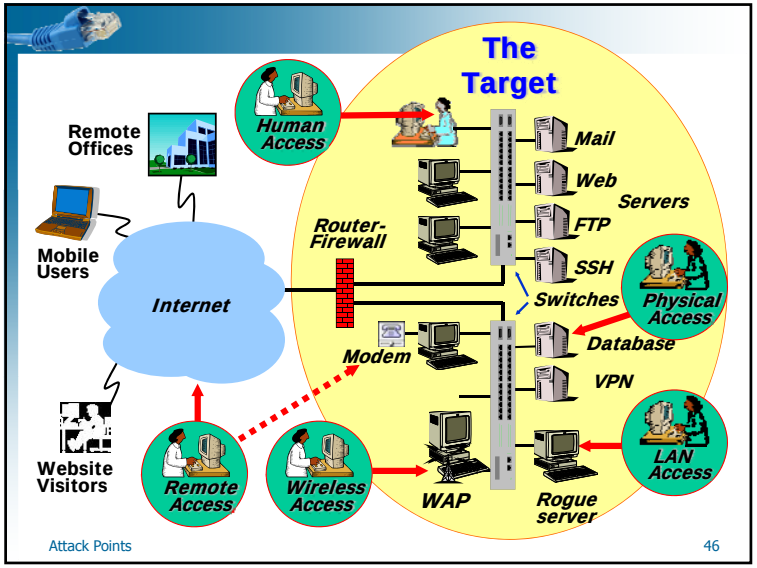
Attack Points

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)

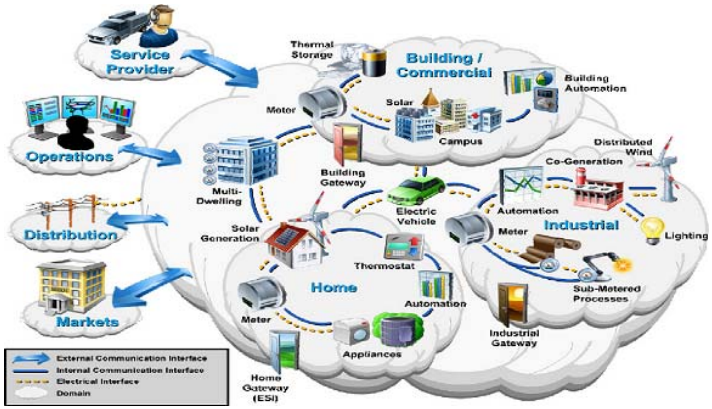
- Indirect access via Teleworkers
- Home networks easier to breach (DSL, cable)
- Home computers lacking corporate AV, policies
- Home computers may be running P2P clients
- Ride along on their VPN link

The 'outside' is now 'inside'…



Sensor Networks

Video Encoders, Road Sensors, CMS, Sprinklers…



IP Enabled Smart Networks

- Implemented on microcontrollers and radios
- Cost is less than $2.00.
- An IPv6 stack can be built in <12 Kb code
- Stack requires < 2Kb memory
- Server often a standard Apache Webserver

- Default passwords
- Insecure

Safety Third

Tools

Where do tools come from?

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

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

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

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.)

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

SEO Poisoning

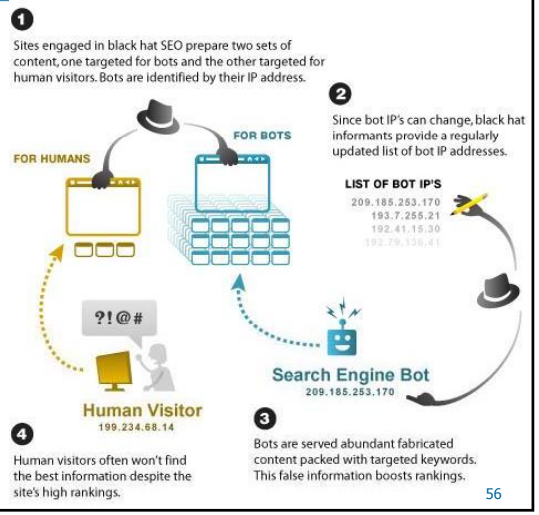
Cloaking: webserver hosting SEO Poisoned misleading pages looks at two HTTP fields it gets from each browser visiting a page:

- *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

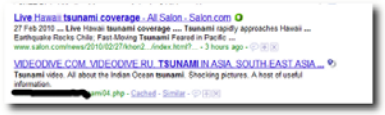
SEO Cloaking

Additive
Link Farming
Cloaking
Fast-Flux DNS



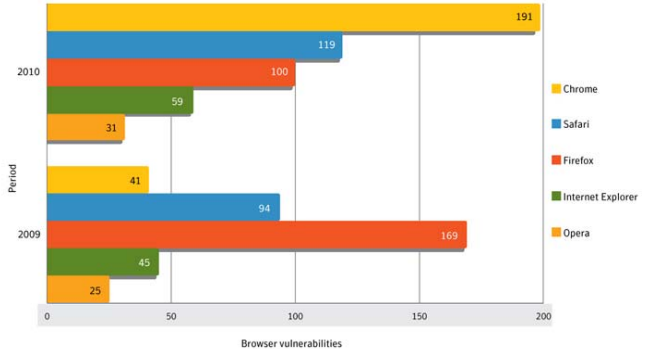
SEO Poisoning

- 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...

Browser Vulnerabilities

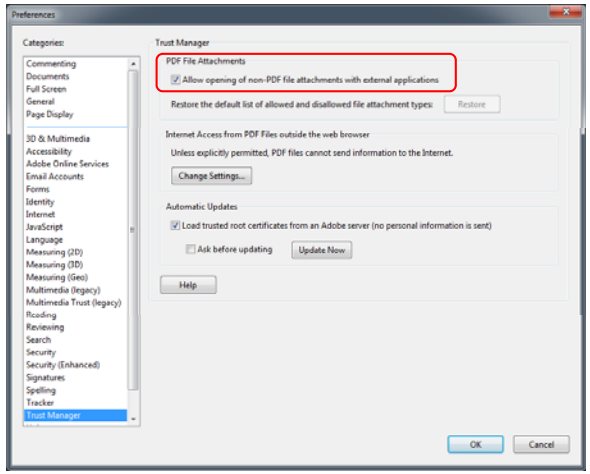


Acrobat – huge problem

Java – just say no

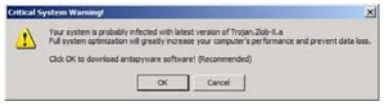
Adobe Default

- No!



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

Fakeware

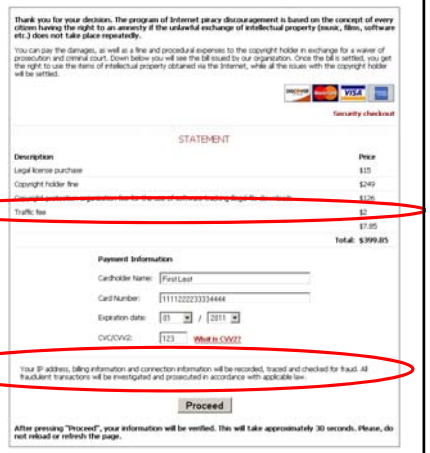
- Kit based
- Free to $2,000 USD

Fake Piracy Scam

- Claims to detect pirated files - sets wallpaper to:

Fake Piracy Scam

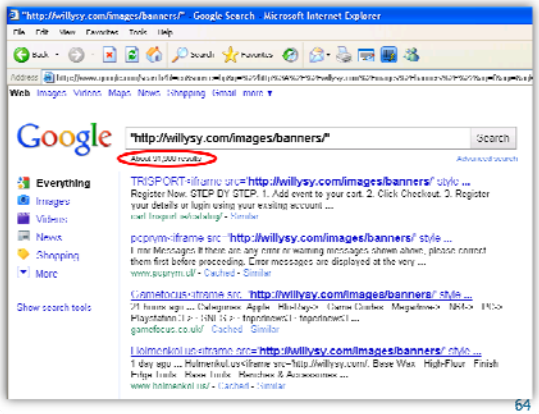
- Tax on clueless
- Traffic fee?
- Fraud warning?
  - Irony Meter Pegs



Infection Injection Detection

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

A good example of Google as a security tool



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

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

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 impossibe to detect*
- *ZeuS is the browser in the middle!*

Command & Control Servers

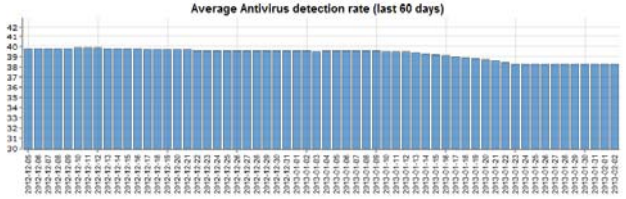
ZeuS
461 online 22:34 Feb 02, 2013
Source: zeustracker.abuse.ch

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 - Mic	US
12	33182	DIMENOC---HOSTDIME - HostDime.com,	Florida
12	36351	SOFTLAYER - SoftLayer Technologies	Texas
11	35818	WEBFACTOR-AS Webfactor SRL	Romania
10	8426	CLARANET-AS ClaraNET	Europe
6	21844	THEPLANET-AS - ThePlanet.com Intern	US
5	16265	LEASEWEB LEASEWEB AS	Netherlands
5	24940	HETZNER-AS Hetzner Online AG RZ	Germany
5	32475	SINGLEHOP-INC - SingleHop	US
5	31282	UKNOC-AS UKNOC AS	UK

Average Antivirus detection rate (last 60 days)

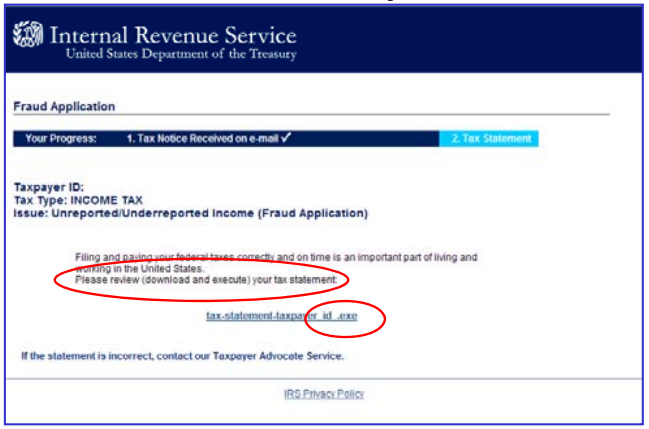


Phishing

- 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

Fake IRS Notice

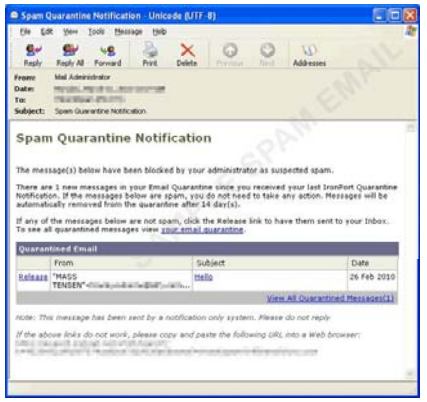
- Attached file is a downloader trojan



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



Fake Sirius Notice

Fake Sirius Notice

EVERYTHING WORTH LISTENING TO IS ON SIRIUS SATELLITE RADIO | XM 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: 1-888-539-SIRIUS

Look B4 U Click

Schedule and channel assignments are subject to change. Check sirius.com for the latest updates.

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

Course Outline

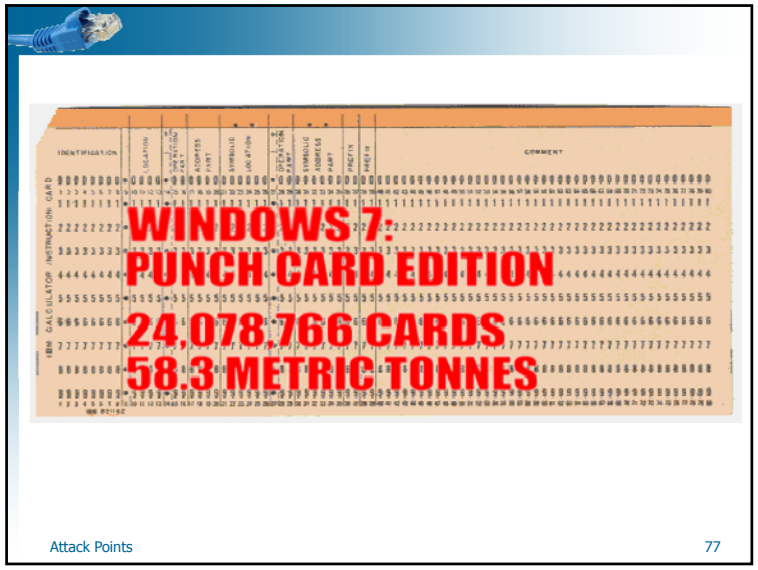
A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   - Human access
   - Physical access
   - LAN (insider) access
   - Remote (Internet) access
   - Wireless access

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

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

Now its 'How'


WINDOWS 7:
PUNCH CARD EDITION
24,078,766 CARDS
58.3 METRIC TONNES
Attack Points
77