

01000101

## 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 Points2




## 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 Points3



## Attack Points

What are the attack points?

Vulnerable HUMANS!	Vulnerable SERVERS!	Vulnerable CLIENTS!
-----------------------	------------------------	------------------------

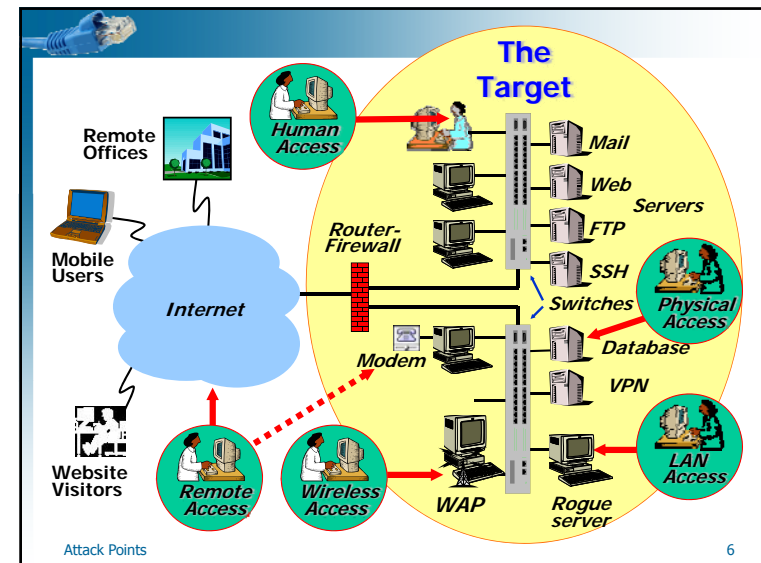
- Being vulnerable means always having to say you're sorry
- Humans are creatures of habit. They will base passwords, PINs, combinations on birthdays, children's names or nicknames, etc.
- When security gets in the way, humans will find a way around it

Attack Points4

## 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 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:

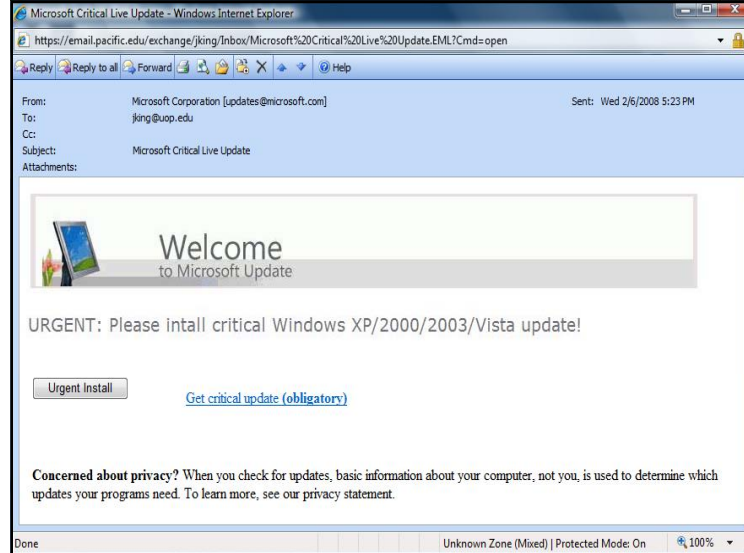
<http://www.trustedbank.com/general/custverifyinfo.asp>

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

Thank you,  
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Attack Points 11



Microsoft Critical Live Update - Windows Internet Explorer

https://email.pacific.edu/exchange/jking/Inbox/Microsoft%20Critical%20Live%20Update.EML?Cmd=open

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

Sent: Wed 2/6/2008 5:23 PM


Welcome to Microsoft Update

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

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

Mail.com is a webmail service

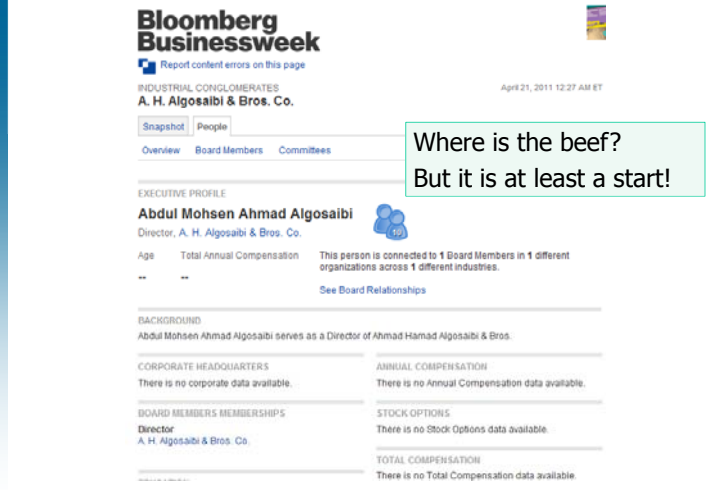
# dig -x 70.37.89.77  
;; QUERY: 1, ANSWER: 0, AUTHORITY: 1  
;; AUTHORITY SECTION: msnhst.microsoft.com.

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

### Security Advisory – March 14, 2011 Adobe Flash Player, Reader, and Acrobat

A critical vulnerability exists in Adobe Flash Player 10.2.152.33 and earlier versions (Adobe Flash Player 10.2.154.18 and earlier for Chrome users) for Windows, Macintosh, Linux and Solaris operating systems, Adobe Flash Player 10.1.106.16 and earlier versions for Android, and the Authplay.dll component that ships with Adobe Reader and Acrobat X (10.0.1) and earlier 10.x and 9.x versions of Reader and Acrobat for Windows and Macintosh operating systems.

## 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







## Click We Must

### Malware For All

May 17, 2007, [www.eweek.com](http://www.eweek.com)

- As a social experiment, someone bought an ad on Google that offered to infect people's machines with malware. The ad read, "Drive-By Download. Is your PC virus-free? Get it infected here!" Over a period of six months, the ad was clicked on 409 times; it was displayed 259,723 times.
- That works out to a rate of 0.16 percent. Clicking on the link supplied took users to a "malicious" web site; however, the site did not contain any malicious code.

Attack Points

22

## News! – Human Access

### Social Engineering, the USB Way


June 7, 2006, [darkreading.com](http://darkreading.com)

- Credit union hires firm to assess security of its network. Firm takes collection of worthless vendor giveaway thumb drives and imprints them with custom Trojan that collects passwords, logins and machine-specific information from the user's computer and email the findings back.
- "I made my way to the credit union at about 6 a.m. to make sure no employees saw us. I then proceeded to scatter the drives in the parking lot, smoking areas, and other areas employees frequented."
- Of the 20 USB drives planted, 15 were plugged into company computers. Data obtained helped compromise additional systems.

Attack Points

24


## Attack Points



We are told as children, *"Don't pick something up off the street and put it in your mouth! You don't know where that gum/penny has been!"*

So why do we pick up a strange USB drive and stick it into our computers?

*"You don't know where that USB drive has been!"*



Attack Points 25

## Gullible CEOs on Facebook

### Social Engineering via Facebook

Jan. 04, 2008 Computerworld

- A Hong Kong-based security company duped gullible CEOs and finance directors into revealing personal details that could be used for so-called spear-phishing attacks.
- "We used a fake Web mail account to create a fake Facebook account. With this, we approached individuals who we knew to be in quite senior positions and simply asked to be their friends, explaining that we knew them while at school."
- "We found personal details, including dates of birth, mobile phone numbers, home addresses, company name and job titles, and even [a] mother's date of birth."
- C-level management can be easy high-value targets. Why?

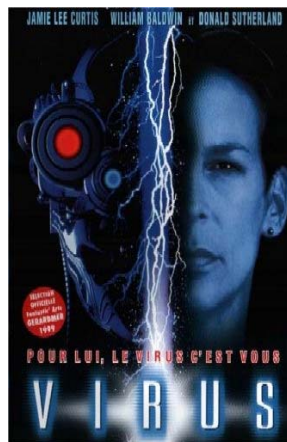
Use social networking (self marketing), not technology savvy, often 'exempt' from 'annoying' computer policies....

Attack Points 26

## Attack Points

### Human Access

- Via social engineering
- Via email & attachments
- phishing
- Spear phishing (targeted)
- Whaling (high-value)
- Via malicious websites
- Spyware implants
- Trojan implants



Attack Points 27

## 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 28




## 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 29




## 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 30



## 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 31




## 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](#)
- [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/](http://www.attrition.org/errata/cpo/)



Attack Points 32




## 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*
- Multiple Whitebox desk/laptops – *Nitol botnet*

**2012**

[www.attrition.org/errata/cpo/](http://www.attrition.org/errata/cpo/)

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



Attack Points

33

## Computer Supply Chain Sources

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

34

## 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](http://en.wikipedia.org/wiki/Farewell_Dossier)



Attack Points

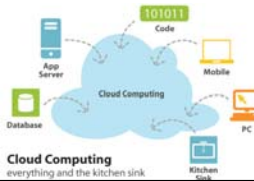
35

## 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

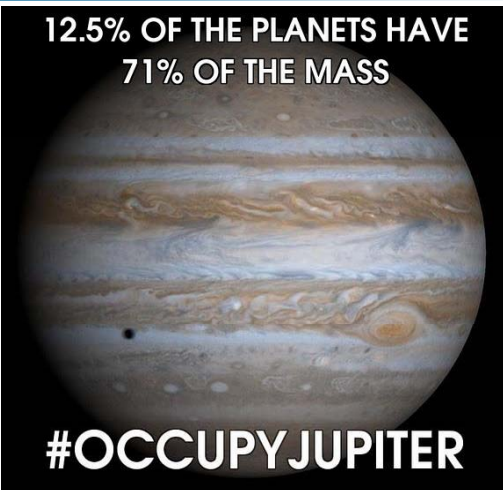
*Reboot the Cloud!*



Attack Points

**-MOTD-**

**12.5% OF THE PLANETS HAVE  
71% OF THE MASS**



**#OCCUPYJUPITER**

Attack Points 37

**Hackers Strut Their Stuff in Las Vegas**

8/6/07 [www.taipeitimes.com](http://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 38

**Hackers Strut Their Stuff in Las Vegas**

8/6/07 [www.taipeitimes.com](http://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 39

**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

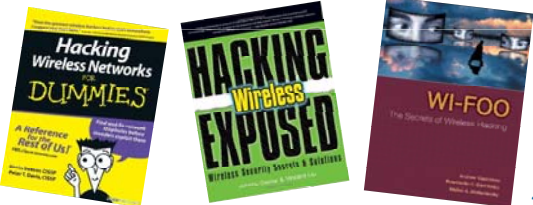
**This LAN is your LAN.....and now  
...This LAN is my LAN**

Attack Points 40

## Attack Points

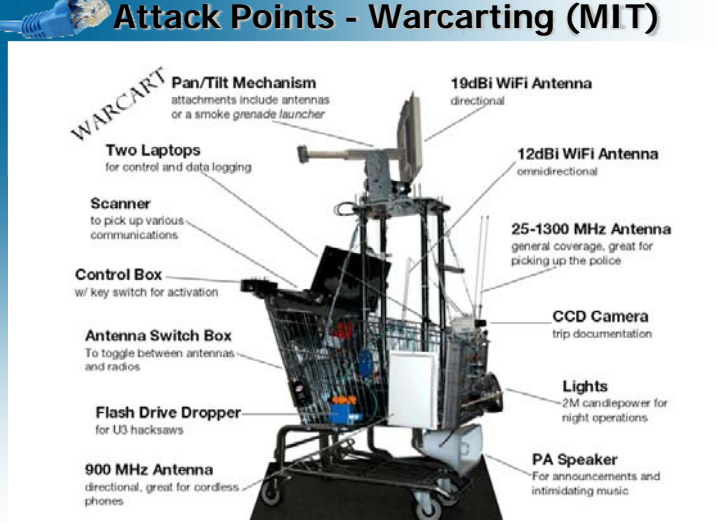
### Wireless Access

- 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](http://www.wardrive.net)



Attack Points 41

## Attack Points - Warcarting (MIT)



Labels for Warcart components:

- WARCART**
- Pan/Tilt Mechanism**: attachments include antennas or a smoke grenade launcher
- Two Laptops**: for control and data logging
- Scanner**: to pick up various communications
- Control Box**: w/ key switch for activation
- Antenna Switch Box**: To toggle between antennas and radios
- Flash Drive Dropper**: for US hacksaws
- 900 MHz Antenna**: directional, great for cordless phones
- 19dBi WiFi Antenna**: directional
- 12dBi WiFi Antenna**: omnidirectional
- 25-1300 MHz Antenna**: general coverage, great for picking up the police
- CCD Camera**: trip documentation
- Lights**: 2M candlepower for night operations
- PA Speaker**: For announcements and intimidating music

Attack Points 42

## News!

### Fine & Community Service for Wireless Piggybacking

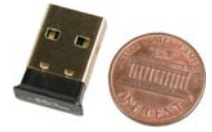
May 24, 2007, [www.woodtv.com](http://www.woodtv.com)

- 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 43

## 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 44

## 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 45

## Attack Surfaces





Attack Points 46

## 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 ...

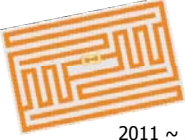



Attacks - Update 47


## Misc. Wireless Attack Points

### Radio-frequency identification (RFID)

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



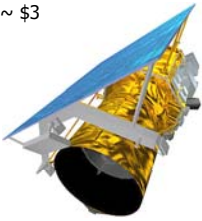
2011 ~ \$.05



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 48



### 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 49

### 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 50

### Attack Points

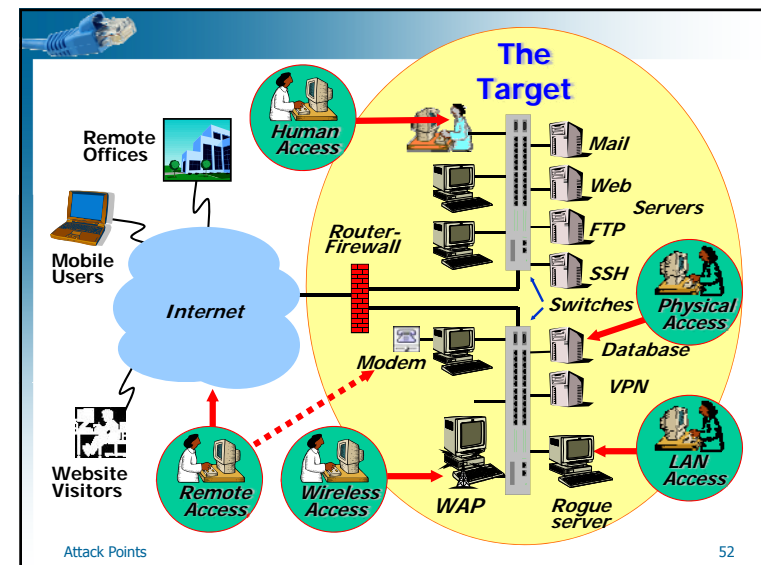
#### Remote Access (MODEM, VPN, Teleworkers)

- 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

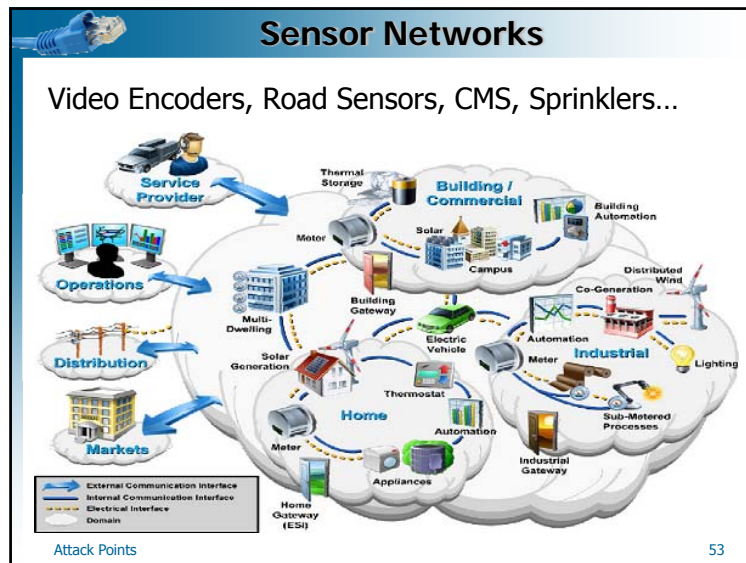
The 'outside' is now 'inside'...



Attack Points 51







53

### 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*

Attack Points

54

### Tools

Where do tools come from?

The image shows four books related to hacking tools. The first book is 'Hacker Toolbox' with a red cover. The second is 'Power Hacker' with a green cover. The third is 'Hacker's Tool Chest' with a yellow cover. The fourth is 'Hacker's Tool Chest 2nd Edition' with a black cover. A legend at the bottom left defines the connection types: External Communication Interface (blue arrow), Internal Communication Interface (red arrow), Electrical Interface (yellow arrow), and Domain (grey box).

Attack Points

55

### 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

56



01000101

## 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....

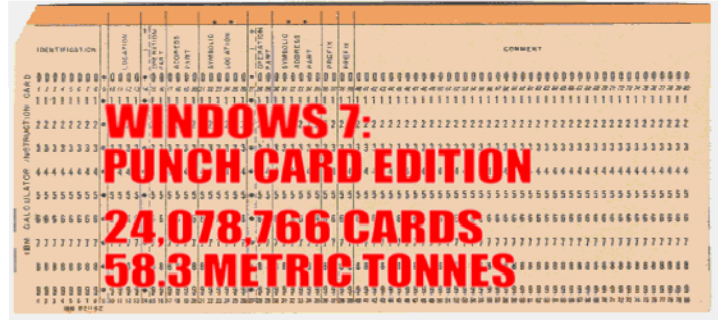
Now its 'How'



Attack Points

57





**WINDOWS 7.**  
**PUNCH CARD EDITION**  
**24,078,766 CARDS**  
**58.3 METRIC TONNES**

Attack Points

58