



Security Issues 2009

Matthew Cook
Network & Security Manager
Loughborough University

Why bother?

- Keep you computer running
- Keep your documents safe
- Identity theft
- Spreading infection
- Data Integrity (DPA: Data Protection Act)

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

The Easiest Security Improvement - Password

- Use a password with mixed-case characters
- Use a password with a 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 or film quotations
- <http://www.lboro.ac.uk/computing/doc/advice.html>
- Brute Force Password Cracking

Viruses

- Traditional viruses required human intervention.
 - Share it on floppy discs
 - Copy it
 - Email it
- Attached to programs, documents or emails.

Worms

- One stage on from viruses
- Auto replication
 - Open shares
 - Exploits in machines
 - Outlook Address book
- Eliminating the human interaction means whole computer networks can be compromised very swiftly.
- Recently Conficker

Trojans

- Appears to be an innocent program
- Actually contains malicious code
- A keylogger?
- Sometimes difficult to discover

- Insider code injection in this economic climate?

Anti Virus

- Becoming very top heavy
 - Antivirus
 - Anti Ad/Spy/Malware
 - SPAM Checker
 - Host based Intrusion Prevention
 - Posture Checking
 - Buffer Overflow Protection
 - Data Execution Prevention
- Running twice, three times, surely not?

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](#)
 > 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](#)
 > Level 112 General Acc with Excellent Skills, Level 99 Mage, level 92 Hit Points, level 67 Cooking, etc \$520

SUPERSTAR 

70     [View Gear](#)
 > Level 70 Draenei Priest With INCREDIBLE Gear, Mixed Epic T-4/T-5, Crafted Items, Flying Mount & Much More! MUST HAVE! **30% OFF**
\$4333
 > Includes A Level 70 Female Blood Elf Mage! \$933

SUPERSTAR 

70     [View Gear](#)
 > Level 70 Human Priest With Great Gear, Several Rare & Epic Items, Flying Mount & More! AWESOME BUY! 20,000g INCLUDED! \$3937
 > Includes A Level 70 Male Human Paladin!

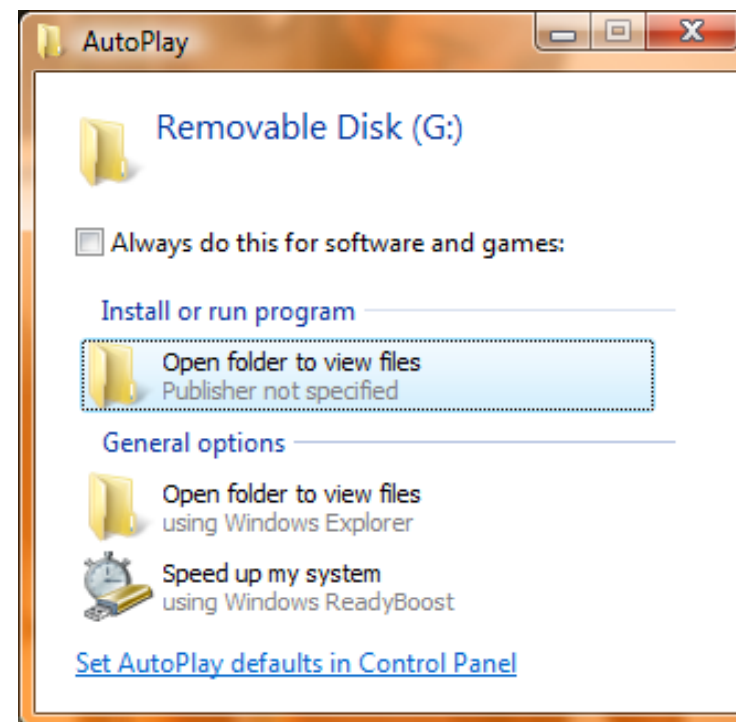
- Examples of virtual stolen goods, e-commerce for the bad guys
- David Philips, Malware in the Virtual World, 8th April 2008

Social Engineering

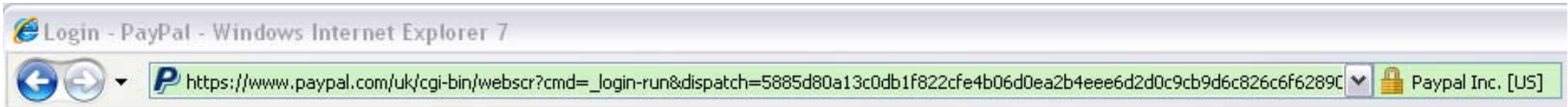
- Targeted Attacks
- General phishing attacks
- Mass Internet Attacks
- Drive by or Banner advert exploits
- Software download iWork 2009 (Warez Sites)

USB Sticks

- Theft or loss of data
- Worm propagation
 - Conficker
- Disable AutoRun?
- Not just USB Sticks
 - iPod
 - Generic MP3 Player
 - USB Hard Disc
 - Photo Frame



Extended Validation (EV) Certificates



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

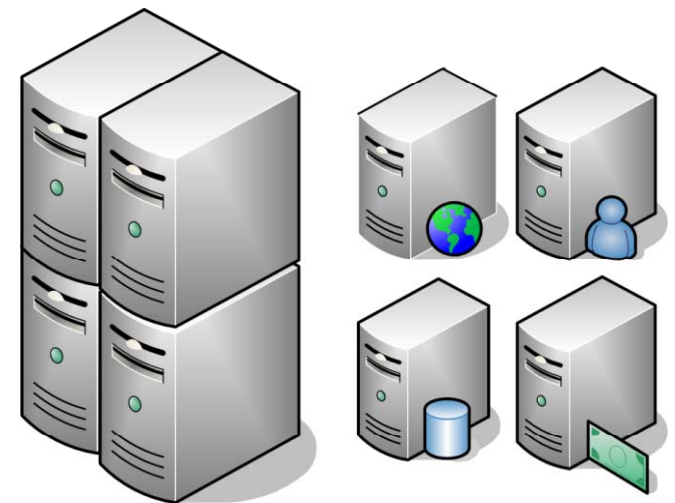
How Secure?

- Can secure Virtual Machines exist on the same host?
 - Do you want to run your Web and SQL server on the same physical computer, even if virtualised?
 - Breaking out of the VM is possible

- Is automatic provisioning a good idea?

- Where is the traditional DMZ?

- Shared VM Services
 - Anti Virus
 - HIDS/HIPS



Network Implications

- Is the virtual network secure?
 - Does your IDS/IPS have visibility of the virtual switch?
 - Network probe guest VM?
 - Increased frequency of SSL based attacks

- Expectation that the network can deliver:
 - Speed requirements, does it make sense to virtualise high bandwidth applications?
 - Same IP Everywhere (VMotion)
 - Automated VLAN changes



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?

IPv6

- Redesigned IPv6 network stack
- Enabled by default
- Conversations on local subnet
- AAAA DNS Lookups
 - Pre SP1 ICS Issues
- IPsec support
- Teredo NAT Tunnelling

Wireless Security

```

WirelessVM VMware Player Ethernet Sound Adapter Alps Bluetooth Adapter SanDisk Removable Disk
Applications Places System 1:47 PM
ja.net
delegate@wirelessvm:~
File Edit View Terminal Tabs Help
Aircrack-ng 1.0 beta1
[00:00:00] 104 keys tested (136.22 k/s)
KEY FOUND! [ training ]
Master Key      : D7 56 3A 71 69 70 51 47 D7 82 E0 2A 7B 82 94 AD
                  EE 5F 92 EE 75 A9 72 E8 16 F2 D1 CA 27 14 CF D0
Transcient Key  : 1E 85 CC F3 54 F1 34 C4 DB 75 04 61 20 48 2F 6E
                  FC 39 39 01 10 A5 13 CA 1E 01 E9 CA 06 BB FF D5
                  36 15 E8 40 40 55 AA 78 0A 7D D1 FD CF C6 84 A6
                  3F 45 F5 8D 07 8E E3 3F E9 9B F7 3E AC 04 16 2A
EAPOL HMAC      : 18 0F 3F 70 2A 91 EC 06 F0 1B 2E 66 3F BA 97 D1
    
```

To direct input to this virtual machine, press Ctrl+G.

Disc Security

- Already a hot topic
- Data Disposal (Dban)
- Data Encryption
 - Bitlocker
 - TrueCrypt
 - FIPS 140-2
- Not just discs...



Futures and Windows 7

- Windows 7 pre-beta 6801 post PDC2008
- Action Centre
 - Takes Security Centre, Defender, UAC
 - Sliding annoyance of alerts
- Firewall Filtering Platform
- Bitlocker Removable Storage Encryption
- Biometrics
- DNSSEC – Addressing RFC 3833
- AppLocker

Not just Computers

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

- Anything network connected...

...and at the end of the day.

- Passwords
- Virtualisation, you do have two Operating Systems!
- Secure your wireless access point
- Theft of physical hardware
- User interaction

Web Links

- Windows Vista Security Blog:
<http://blogs.msdn.com/windowsvistasecurity/>
- Microsoft Security Response Centre
<http://blogs.technet.com/msrc/>
- Microsoft Security Central
<http://www.microsoft.com/security/>
- SANS Internet Storm Centre
<http://isc.sans.org/diary.html>
- Security Focus
<http://www.securityfocus.com/>



Questions?

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