



# Windows Vista Security Posture

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

## A bit about myself...

- Network & Security Manager at Loughborough University
- Team of ten IT Professionals
- Worked at Loughborough for 9+ years
- JANET(UK) Trainer
- Security Researcher

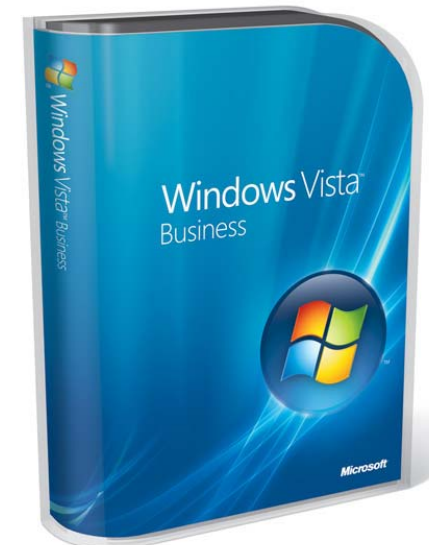


# Windows Vista Security Posture



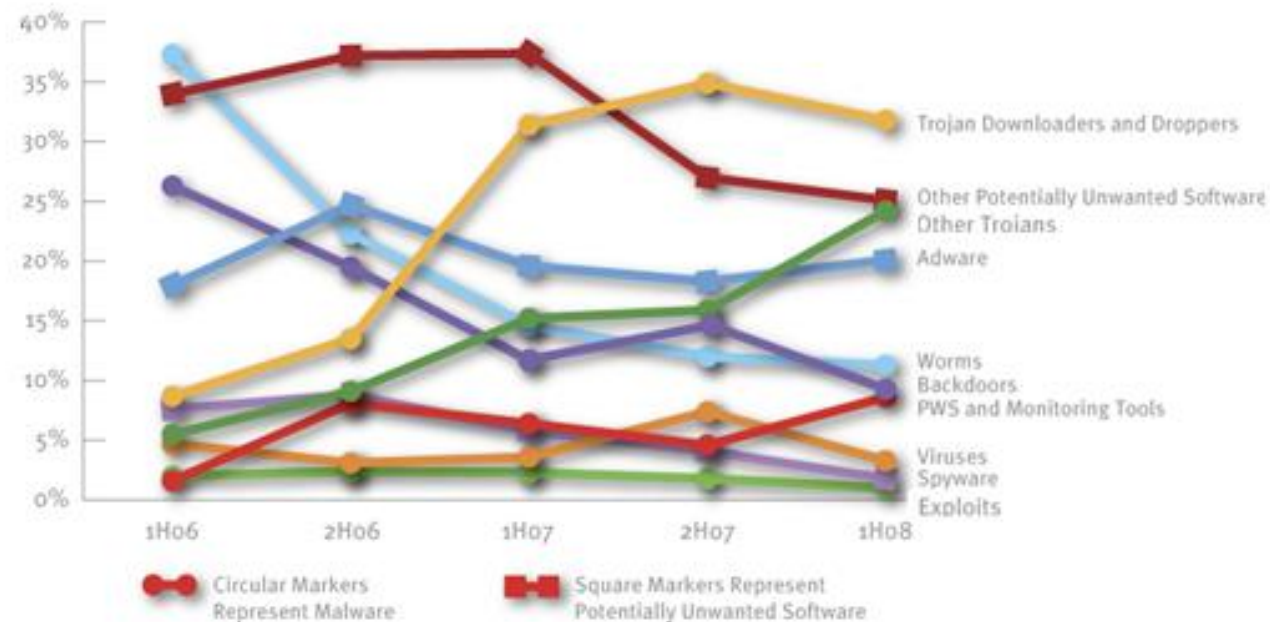
## Starting Points

- Five years worth of development, Windows Vista launches in 2007.
- Slow adoption of Vista in both home and business markets.
- Over to you...



# Latest News

- Microsoft Security Intelligence Report (Revision 5) released, November 3<sup>rd</sup> 2008 covers Q1 and Q2 2008.
- “The higher the level of service pack a machine runs, the lower the rate of infection!”



- <http://www.microsoft.com/security/portal/sir.aspx>

## Under the hood: Group Policy Objects

- Grown exponentially
- NT 4 tattoos
- Number frequently increase
  - AD Schema Extensions
- Vista has approx 2,500
- Allows for a very tailored configuration

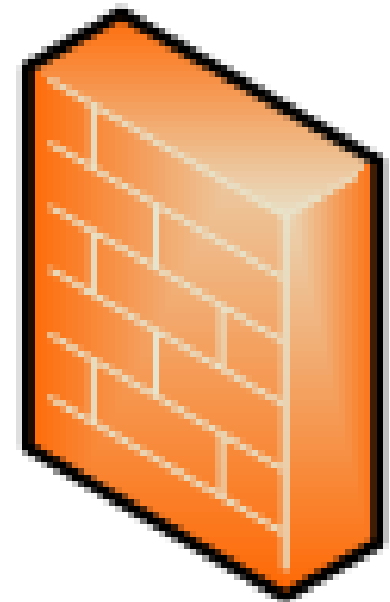
## Under the hood: Microsoft Security Centre

- Firewall
  - Monitors egress traffic
  - Location aware improvements
- Windows Defender
  - Software explorer
- Monitoring Improvements
  - Anti Virus
  - Anti Spyware
  - Firewall
  - Microsoft Update
  - Internet Explorer Settings
  - User Account Control



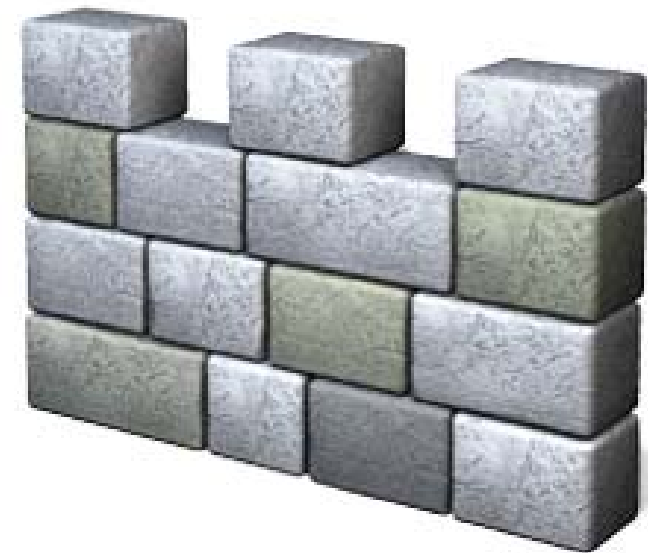
## Under the hood: Firewall

- Unchanged since W2K, until...
- Bi-direction firewall
  - Often features included in A/V Package
  - Most egress filtering disabled
- Configuration through wf.msc
- Group Policy creation
- Software vs Hardware firewall
  - Yoggie



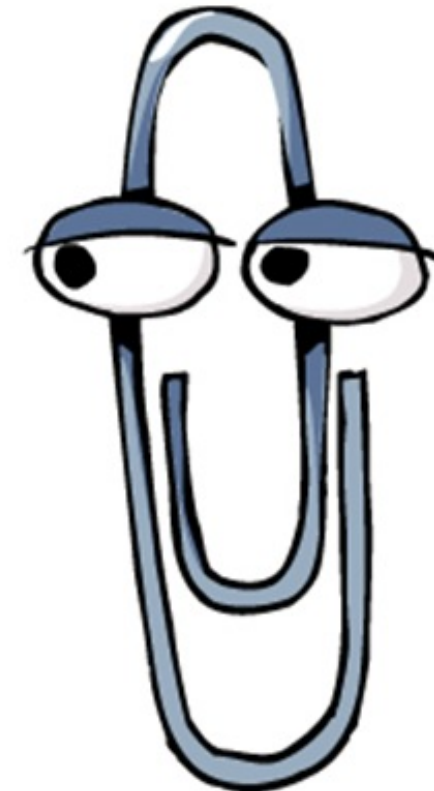
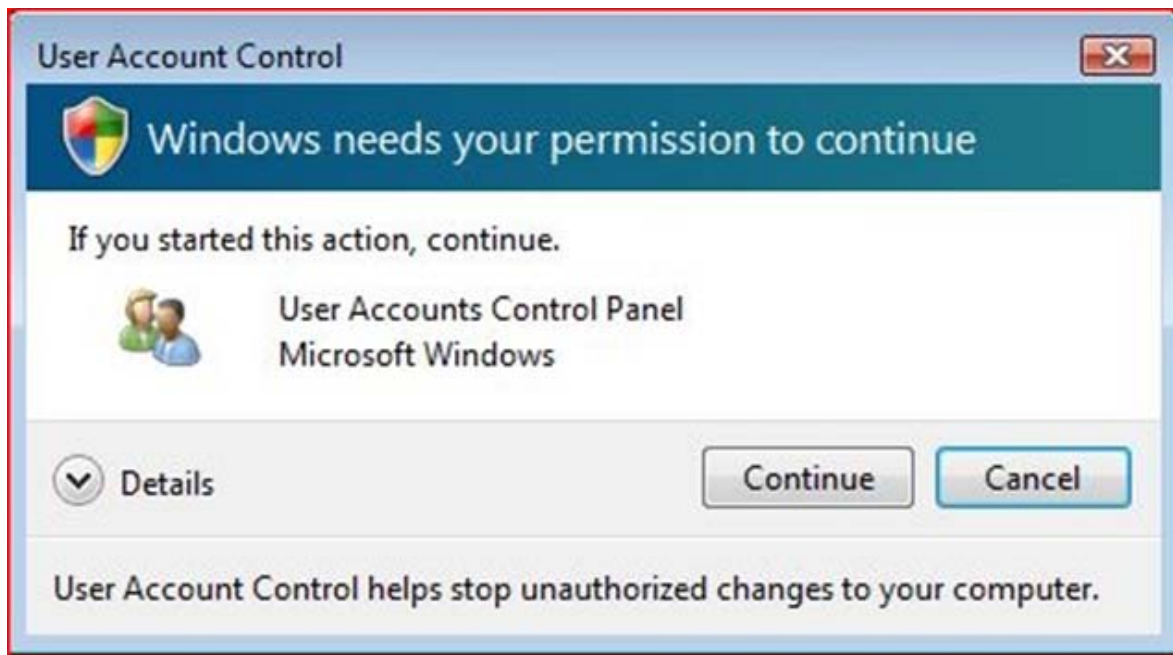
## Under the hood: Defender

- Spyware
- Schedule and removal
- Software Explorer aka msconfiq
- Updates, or not...
  - 2am every morning
  - Tools -> Options
  - MS KB918355



## Under the hood: User Account Control

- What do these features have in common?



## Under the hood: Filing System Protection

- BitLocker Drive Protection
  - Accidental data disposal
  - TPM
  - Encryption keys and RIPA Part 3
- Enhancements to traditional EFS
- Connection of USB devices
  - USB Sticks
  - USB hard discs
  - iPods etc

## Internet Explorer 7

- New architecture
- Phishing Filter
- SSL Certificate Warning
- Protected mode (in Vista)
  - Default, except in trusted zone
  - Uses new layering technology
    - User Account Control
    - Integrity of Applications
    - Process Privilege protections
  - Restrict Access
- Fix My Settings



## Networking Changes

- Network Access Protection (NAP)
  - Posture checking
  - Isolation
- Network Awareness
  - Connectivity
  - Connections
  - Location
- Network diagnostics framework
- Wireless improvements
- TCP Offloading support

# Network Posture

## Windows XP IPv4

```
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open taskscheduler
```

## Windows Vista IPv4/6

```
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wininit.exe
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open lsass.exe
49157/tcp open services.exe
```

## Network Services

49152/tcp open - wininit.exe Windows Startup Application

49153/tcp open - svchost.exe Audiosrv, Dhcp, Eventlog,  
lmhosts, wscsvc

49154/tcp open - svchost.exe EventSystem, FDResPub,  
LanmanWorkstation, netprofm, nsi, SSDPSRV, upnphost,  
W32Time, WebClient

49155/tcp open - svchost.exe AeLookupSvc, Appinfo,  
AppMgmt, BITS, Browser, CertPropSvc, EapHost, gpsvc,  
IKEEXT, iphlpsvc, LanmanServer, MMCSS, ProfSvc,  
RasMan, Schedule, seclogon, SENS, SessionEnv,  
ShellHWDetection, Themes, Winmgmt, wuauerv

49156/tcp open - lsass.exe KeyIso, Netlogon,  
ProtectedStorage, SamSs

## Network Attack Surface

- Network Attack Surface for Vista has changed:
- Many tools no longer work
  - Fport
  - Sys Internals TCP View
- PortQry 2.0
  - <http://support.microsoft.com/kb/832919>
- Reference Material

[http://www.symantec.com/avcenter/reference/Vista\\_Network\\_Attack\\_Surface\\_RTM.pdf](http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf)

<http://www.symantec.com/avcenter/reference/ATR-VistaAttackSurface.pdf>

<http://www.microsoft.com/technet/technetmag/issues/2007/02/VistaKernel/>

## Web Services for Devices

# What is web Services for Devices?

<http://msdn2.microsoft.com/en-us/library/aa386284.aspx>

<http://msdn2.microsoft.com/en-us/library/aa385800.aspx>

wsdapi	5357/tcp	Web Services for Devices
wsdapi	5357/udp	Web Services for Devices
wsdapi-s	5358/tcp	WS for Devices Secured
wsdapi-s	5358/udp	WS for Devices Secured

## 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

```

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...



## 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?

...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

## 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

## 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/>

## References

- Administering Windows Vista Security  
The Big Surprises
  - Mark Minasi
  - ISBN 0470108320
- Microsoft Vista for IT Security Professionals
  - Anthony Piltzecker
  - ISBN 159749139X
- Windows Vista Security
  - Roger Grimes, Jesper Johansson
  - ISBN 0470101555



**Questions?**

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