

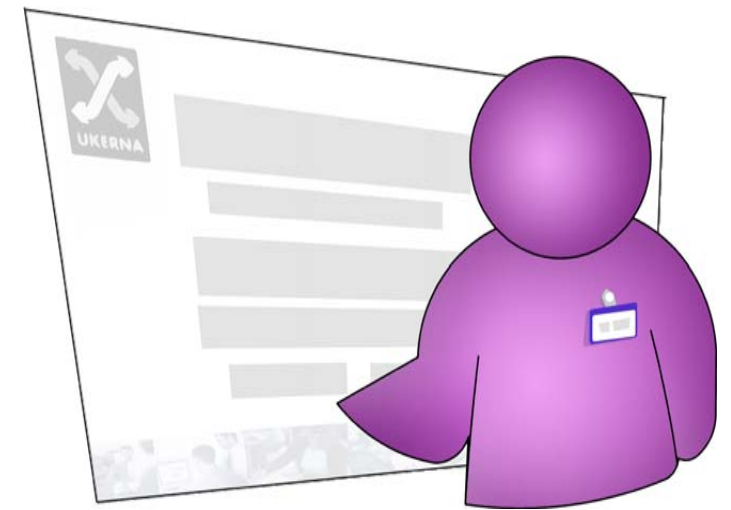
Windows Vista Security and Networking





Introduction

- Matthew Cook
- Senior IT Security Specialist
(Loughborough University)
- UKERNA Contracted Trainer
- Further details available at:
<http://escarpment.net/>





Background

- Times are changing
- Security is a key concern
- A large problem is delivering rich content in a secure manner

- Dedicate less time to security
- More time to new technology



Under the hood

- Enhanced Buffer Overflow Protection
 - NX bit in hardware
 - Address Space Layout Randomisation
- Services
 - More services by default
 - Restricted Services
 - Per service ACLs
- Signed drivers
- Kernel Patch Protection (x64)



Logon

- GINA
- User Account Control
 - Standard User or Administrator
 - Administrator Approval Mode
 - File system and registry virtualisation



Group Policy

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



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



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

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

Networking Changes

- Network Access Protection (NAP)
 - Posture checking
 - Isolation
- Network Awareness
 - Connectivity
 - Connections
 - Location
- Network diagnostics framework
- Wireless improvements
- TCP Offloading support
- SMB 2.0



IPv6

- Redesigned IPv6 network stack
- Enabled by default
- IPSec support
- Teredo NAT Tunnelling

Recommendations

- Don't forget basic security principals:
- Passwords
- Anti Virus
- Patching
- Securing the Install
- Protecting the LAN
- Educating Users



UKERNA Training

- Portfolio of network based training
- Over 10 different courses
- Training venues in many locations
- Comprehensive course workbook + CD

- Using Logfiles for Security
- Basic Networking
- Wireless LAN Fundamentals
- Firewalls: Planning and Implementation

Questions?

<http://escarpment.net/>