Presenter Background

**Education**
- B.S. of Information Technology (2007)
  - Concentration in Network Administration
- B.S. of Information Networking and Telecommunications (2009)
  - Concentration in Internetworking
- B.S. of Justice Studies (2009)
- Paralegal Certificate (2008)
- Internetworking Certificate (2009)

**Industry Affiliations**
- Kansas State University Security Incident Response Team (SIRT) Member
- Information Systems Security Association (ISSA) Member
- Information Systems Audit and Control Association (ISACA) Member
- Institute of Electrical and Electronics Engineers (IEEE) Member
- Federal Information Systems Security Educators’ Association (FISSEA) Member
- Association of Information Technology Professionals (AITP) Member
Why Security?

• Many reasons
  – Financial
  – Political
  – Legal
  – Moral
  – Public Image and Reputation
  – Why not?
Sample Legal Requirements

- Electronic Communication Policy (ECP)
- Health Insurance Portability and Accountability Act (HIPPA)
- Public Records Act (PRA)
- Information Practices Act (IPA)
- Family Educational Rights and Privacy Act (FERPA)
- Children’s Online Privacy Protection Act (COPPA)
- Fair Credit Reporting Act (FCRA)
- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act of 2002
Predicted Security Trends for 2009

- Attackers will keep innovating with more creative methods of/for attack
- Phishing attacks will decline
- As mobility grows, so will mobile security challenges
- Network access controls will continue to mature and be more widely adopted
- Laws and regulations will continue to expand in scope and size
- Virtualization technology will face new challenges
- Security in/through the “cloud” ???
- Continued increases in secure software development
- Encryption, Encryption, Encryption
- The line between understanding what is legitimate and what is not will continue to be blurred even further
Security Administration

• There are three primary categories of controls and we will focus primarily on administrative controls

• **Physical Controls**
  – Facility protection, security guards, locks, monitoring, environmental controls, intrusion detection

• **Technical Controls**
  – Logical access controls, encryption, security devices, identification, and authentication

• **Administrative Controls**
  – Policies, standards, procedures, guidelines, screening personnel, security-awareness training
CIA Triad

• Three fundamental principles of security, collectively known as the CIA triad.

• **Confidentiality**
  – The ability to hide information from those people unauthorized to view it.

• **Integrity**
  – The ability to ensure that data is an accurate and unchanged representation of the original secure information.

• **Availability**
  – The ability to ensure that the information concerned is readily accessible to the authorized viewer at all times.
Beginnings of Windows Security

- It starts at step one, with the configuration of your computer to install Windows on.
- There are many steps that you can perform when you first install Windows to provide a better security posture for yourself and for your organization – we will review some of them next.
Windows Setup Steps

• Password protect computer BIOS

• Use NTFS on all your partitions

• Customize the installation of Windows setup and remove unneeded software
  – Windows Messenger
  – MSN Explorer
  – UPnP
  – Games
  – Indexing Service
  – Outlook Express
Windows Setup Steps Cont.

• Password protect every user account on the machine

• Remove, disable, and/or rename unused or useless accounts
  – Guest
  – ASPNET
  – Administrator

• Disable Simple File Sharing

• Disable boot from CD-ROM and USB devices
Windows Setup Steps Cont.

• Disable hidden admin shares (i.e. C$ or ADMIN$)

• Enable Data Execution Prevention (DEP)

• Launch folder windows in separate process

• Prompt for password when coming out of standby or from screensaver

• Disable file and print sharing

• Disable autorun and autoplay

• Disable unused and unneeded services
Windows Setup Steps Cont.

- Please refer to handouts for further examples, sample registry edits, Windows service matrix, etc.
## Hardening Windows Services

### Windows XP Service Guide

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Service Name</th>
<th>Automatic</th>
<th>Manual</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerter</td>
<td>Alerter</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Application Layer Gateway Service</td>
<td>ALG</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Management</td>
<td>AppMgmt</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic Updates</td>
<td>wuauserv</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background Intelligent Transfer Service</td>
<td>BITS</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClipBook</td>
<td>ClpSrv</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM Event System</td>
<td>EventSystem</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM+ System Application</td>
<td>COMSysApp</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Browser</td>
<td>Browser</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptographic Services</td>
<td>CryptSvc</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCOM Server Process Launcher</td>
<td>DcomLaunch</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Dhcp</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Link Tracking Client</td>
<td>TrkWks</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Transaction Coordinator</td>
<td>MSDTC</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Client</td>
<td>DnsCache</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error Reporting Service</td>
<td>ERSvc</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Log</td>
<td>Eventlog</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible Authentication Protocol Service</td>
<td>EapHost</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fast User Switching Compatibility</td>
<td>FastUserSwitchingCompatibility</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health Key and Certificate Management Service</td>
<td>hkmsvc</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Help and Support</td>
<td>helpsvc</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP SSL</td>
<td>HTTPFilter</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Interface Device Access</td>
<td>HidServ</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP/CD-Burning COM Service</td>
<td>ImapiService</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indexing Service</td>
<td>ciscv</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSEC Services</td>
<td>PolicyAgent</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Disk Manager</td>
<td>dmserver</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For More Information Visit These Sites:

- [http://www.theeldergeek.com/services_guide.htm](http://www.theeldergeek.com/services_guide.htm)
- [http://www.blackviper.com/WinXP/servicecfg.htm](http://www.blackviper.com/WinXP/servicecfg.htm)
Additional Windows Config Steps

• Ensure Automatic Updates is turned on or set the machine up to use the campus WSUS server

• Make sure the Windows firewall is enabled and active

• Ensure that antivirus software is installed, working, and up-to-date

• Allow users to use something other than IE for internet browsing such as Firefox
Useful Windows Utilities

• Microsoft Baseline Security Analyzer
  – “A easy-to-use tool that helps small and medium businesses determine their security state in accordance with Microsoft security recommendations.“

• Process Explorer
  – "Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.“
More Useful Widows Utilities

• Process Monitor
  – "An advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity."

• Windows XP Security Console
  – "Windows XP Security Console allows you to assign various restrictions to specific users, whether you're running XP Pro or XP Home. XP Home leaves you completely without the Group Policy Editor, while XP Pro lacks the ability to use the Group Policy Editor to selectively apply policies to specific users."
Macintosh Setup Steps

• Set EFI/Firmware Password

• Set passwords for all local user accounts

• Disable automatic login

• Customize the firewall to only allow essential applications and to stealth all other ports

• Use secure virtual memory

• Disable automatic login
Macintosh Setup Steps Cont.

- Require a password to wake the computer from sleep
- Have antivirus software installed, working, and up to date
- Make sure to obtain all of the Apple software updates
- Disable or turn off Airport if not needed
- Disable remote control infrared receiver if not needed
- Disable Bluetooth if not needed
Macintosh Security Link

• Please refer to the following links for more information


Ubuntu Firewall Example

- Please refer to the handout for an example IPTables script that can be used to secure a Linux machine.

Example IPTables Firewall Script

```bash
#!/bin/sh

## This flushes/clears any and all previously cached tables
echo "[*] Flushing existing iptables rules and tables..."
iptables -F
iptables -X
iptables -F -t nat

## This sets the default policy for the iptables chains
echo "[*] Changing default chain policy..."
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```
Printer Security
Printer Security Basics

• Disable unused services
  – FTP
  – IPP
  – LPD
  – Telnet

• Change the password for the embedded web server and for command line access

• Set IP Filtering or ACLs on the printers to only allow access to them from campus IP address space
Printer Security Basics Cont.

• Apply firmware updates as released

• Use up-to-date drivers as applicable

• Monitor printers through a management console such as one of the following:
  – HP Web JetAdmin
  – Dell Open Manage
  – Nagios
Demonstration

• We will work through a couple demonstrations of techniques mentioned or basic configuration examples.
Questions?

- Does anyone have any questions?
- There will be more time at the group luncheon for questions as well.
The End

Thank you for your time and attention

John Godfrey
Residential Networking Help Desk Coordinator
Department of Housing & Dining Services
Derby Dining Center 133 A
Phone: 785-532-0307
E-Mail: jgodfrey@ksu.edu