



Mobile Device Security

Dr. Charles J. Antonelli

Information Technology Security Services
School of Information

The University of Michigan

April 7, 2009

Why we're here

- Discuss best practices in safe use of mobile devices
- Help users self-manage devices



HAVE YOU THOUGHT ABOUT YOUR
**RESEARCH
MAKING
HEADLINES?**

Agenda

- Motivation
- Threats to data
- Scanning data
- Securing data

Not covered here

PDA's

Cell phones

Digital cameras

- Protecting the confidentiality, integrity, and availability of an organization's information assets is not only good business ...
 - ... it is required by federal and state laws and by contractual requirements

Threats to data

- Type of data
 - Research
 - Patient
 - Human subject (IRB)
 - Administrative
 - Proprietary
 - Contractual
 - Confidential
- Threats
 - Compromise
 - Corruption
 - Loss of device
 - Theft of device
 - Theft of data (by malware)
 - Loss of encryption key
 - Import/export/use restrictions on encryption

Fundamental threats
Loss of confidentiality
Loss of integrity
Loss of availability

Recent news items

Date Made Public	Name	Type	# Records
Aug 4, 2008	Arapahoe College, CO	Flash drive	15,000
Aug 5, 2008	TSA	Laptop	33,000
Aug 7, 2008	Harris County Hospital, TX	Flash drive	1,200
Aug 28, 2008	Reynoldsburg, SD	Laptop	4,259
Aug 30, 2008	RIT	Laptop	13,800
Sep 12, 2008	Tennessee State University	Flash drive	9,000
Oct 7, 2008	University of North Dakota	Laptop	84,000
Nov 9, 2008	Charlottesville, NC	2 laptops	25,000
Nov 24, 2008	Starbucks, Seattle	Laptop	97,000
Dec 12, 2008	OHSU (Chicago)	Laptop	890
Jan 26, 2009	City of Madison, WI	Laptop	500
Feb 9, 2009	Parkland Memorial Hospital, TX	Laptop	9,300
Feb 18, 2009	Rio Grande Food Project, NM	Laptop	36,000

Scanning data

- Scan data at rest (in permanent storage)
- Freely available tools
- Pattern matching ASCII data
 - Credit card numbers, social security numbers, license numbers, ...
- Significant limitations
 - False positives
 - ◆ Unrelated data
 - False negatives
 - ◆ Binary, obfuscated, encrypted data

Securing data

- Secure data at rest (in permanent storage)
 - Encryption
- Secure data in transit (moving through a network)
 - Encryption
- Secure the mobile device
 - Physical security

<http://safecomputing.umich.edu/MDS/>

Securing data at rest

- Data in permanent storage
 - Disk, tape, flash, CD/DVD
- Standards-based solutions:
 - Strong encryption
 - ◆ Accept no substitutes
 - Renders data inaccessible without a digital *key*
 - Issue: *key escrow*

Securing data at rest

- Free & built-in encryption:
 - Windows Vista (Enterprise and Ultimate)
 - ◆ BitLocker
 - Windows XP
 - ◆ Encrypting File System (EFS)
 - Mac OS X
 - ◆ Encrypted disk image (Disk Utility)
 - ◆ FileVault
 - Linux
 - ◆ TrueCrypt (some assembly required)

BitLocker *Windows Vista*

- Encrypts all data on drive
- System-selected recovery password
 - Store it in a safe place
- Use conditions
 - Requires special hardware in the laptop
 - Requires two disk partitions
 - ◆ Otherwise use Encrypting File System (EFS)
 - While enabling or disabling, can access disk
 - Encrypts everything on the disk
 - ◆ Files, directories, registry, ...

Encrypting File System (EFS)

Windows Vista or XP

- Encrypts specified folder contents
- System-selected encryption key
 - ◆ Store it in a safe place
- Use conditions
 - When enabling/disabling, can't access volume
 - Encrypted files and directories shown in green
 - Does not encrypt anything else on disk

- Encrypts user home volume contents
- User-selected master password
 - Unlocks all home volumes
 - Store it in a safe place
- Use conditions
 - When enabling/disabling, can't access volume
 - Requires free space equal in size to volume
 - Does not play well with Sophos AV & TimeMachine
 - Does not encrypt anything else on disk

Encrypted disk image

Mac OS X

- Create an encrypted volume
- User-selected password
 - Store it in a safe place
- Use conditions
 - Does not encrypt anything else on disk

Securing data in transit

- Data moving through a network
- Standards-based solutions:
 - Strong encryption
 - ◆ Accept no substitutes
 - Renders network data inaccessible to compromise or corruption without possession of a digital key

Securing data in transit

- Free encryption
 - VPN
 - ◆ Cisco VPN client (ITCom)
<http://www.itcom.itd.umich.edu/vpn/>
 - ◆ Built-in Mac OS X VPN client configuration files
<http://www.engin.umich.edu/caen/network/wireless/docs/macospvn/>
 - SSH, SFTP, SCP
 - ◆ SSH Secure Shell (U-M Blue Disc)
<https://www.itd.umich.edu/bluedisc/>
 - ◆ PuTTY
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Securing the mobile device

- Secure the device
 - Lock it up, lock it down, out of sight
- Secure the data on the device
 - Password protect the laptop
 - Data encryption
 - ◆ See “protecting data at rest”
- Be aware of travel-related restrictions
 - Importing/exporting/use of crypto
http://www.research.umich.edu/policies/federal/export_proc10-23-2008.html



Final Note

- Thanks for attending!



Appendix A
Demonstrations



Flash encryption demo

Lexar Secure II Jump Drive

- Encrypted container on the flash drive
- Software on flash drive encrypts and decrypts data in the container on the fly
- User-supplied password
 - Store it in a safe place
- Excellent documentation:
http://www.safecomputing.umich.edu/tools/download/securityshorts_encrypt_thumbdrive.pdf

- Control Panel | BitLocker Drive Encryption
- Select Turn on BitLocker
 - Initialize TPM (if necessary)
 - Save recovery password
 - ◆ Make multiple copies
 - Turn on disk encryption & reboot
- Excellent documentation:
http://www.safecomputing.umich.edu/tools/download/securityshorts_encrypt_docs_with_Bitlocker.pdf

- Select folder or group of folders to be encrypted
- Properties | Advanced
 - Check 'Encrypt contents to secure data'
 - Click OK in both dialogs
 - Check 'Apply changes to this folder, subfolders, and files'
- Back up file encryption key
 - Store it in a safe place

- System preferences | Security | FileVault
- Set master password if none exists
 - Store it in a safe place
- Select Turn On FileVault...
- Documentation:
<http://safecomputing.umich.edu/tools/SS-EncryptDocsMac.pdf>

Encrypted disk image demo

Mac OS X

- Applications | Utilities | Disk Utility
- File | New | Blank Disk Image
- Specify 128 or 256-bit AES encryption
- Specify other options as usual
 - E.g. sparse image
- Specify a password when prompted
 - Store it in a safe place
 - Also to your keychain

- Free encryption

- VPN

- ◆ Cisco VPN client (ITCom)

- <http://www.itcom.itd.umich.edu/vpn/>

- ◆ Built-in Mac OS X VPN client configuration files

- <http://www.engin.umich.edu/caen/network/wireless/docs/macospvn/>

- SSH, SFTP, SCP

- ◆ SSH Secure Shell (U-M Blue Disc)

- <https://www.itd.umich.edu/bluedisc/>

- ◆ PuTTY

- <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Scanning demo

Mac OS X

- Cornell Spider
<http://www2.cit.cornell.edu/security/tools>
- Download and install Spider_OSX.dmg
- Set preferences
 - Starting directory
 - Scan depth
 - Regular expressions
 - Log file
- Start Spider