Mobile Computing and Storage Device Security

October 19, 2011

Today’s Plan
1. New policy and standard
2. Mobile phones
3. Portable storage devices
4. USB Trade-in events
5. Laptop encryption / PGP

New Policy
• Developed by Information Security and Compliance Committee (ISCAC) and the Governance for UF IT.
• Approved by Elias Eldayrie
• Effective August 17, 2011
• Supersedes existing policies

Why Bother?

Scope of the Policy
This policy applies to all mobile computing and storage devices used by the University of Florida constituency in the performance of their duties, and to all University of Florida Restricted Data when accessed through, or stored on, mobile computing and storage devices, regardless of the device’s ownership. University of Florida Restricted Data may not be released for storage on, or access through, devices that do not meet these requirements.

Restricted Data
Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records, research protocols and export controlled technical data.
### New Policy

1. **Restricted Data** stored on mobile computing and storage devices must be encrypted.
2. ...mobile computing devices must meet all applicable UF encryption standards. Mobile computing devices purchased with University of Florida funds... must also be recorded in the unit’s information assets inventory.
3. University of Florida information security policies applicable to desktop or workstation computers apply to mobile computing devices.

### New Standard

1. **Encryption**
   - Laptops must encrypt Restricted data. WDE required for laptops purchased after August 17, 2011; all laptops by August 2013.
     - i. Strong passphrase, not shared, not on a sticky note under the keyboard
     - ii. Key recovery and proof of encryption

2. **Authentication**
   - Strong passwords. Reduced complexity on small devices if lock or erase on 10 failures.
   - 30 min inactivity timeout

3. **Disposal**
   - Secure disposal

4. **Backup**
   - Copy of UF data on a secure server

5. **Physical Security**
   - Durable physical or electronic label
   - Used in a manner that deters theft
   - Tracking and recovery software

### Inventory

- Opportunity to evaluate all your laptops
- No specific method or technology
- Find laptops you never knew about
- Assess security controls:
  - Patch status
  - AV updates
  - Passwords
  - Install encryption
  - Have Dean/Chair send memo
Put a Label On

Electronic label

Custom order permanent label

UV pen in hidden location

Theft Deterrence

• Cable locks
• Locked cabinets
• Not visible in car!

To Catch a Thief

Bummer:
Software has to run + needs a wifi connection = probably won’t do anything when used with whole disk encryption

http://www.frontdoorsoftware.com/ufl/

Mobile Devices

ActiveSync Policies

• Disallow non-provisionable devices
• Require password
• Require encryption on the device
• Require encryption on the storage card
• Wipe after 10 passcode failures
• 15 minute timeout
• Will be enabled ‘soon’

BES Policies

• Passcode lock required
• Wipe after 10 passcode failures
• ‘Content Protection’ on
• 15 minute timeout
• Will be enabled ‘soon’
Compliant Devices

- Assembling a list at http://infosec.ufl.edu

Androids Dream of Encryption

- Encryption not in main codebase
- Support depends on manufacturer
- Workarounds (only until August 17, 2013):
  - Touchdown
  - Enterpid/Toggle?
  - WhisperCore?

Is iOS Really Encrypted?

- Upgrade from 3.x doesn’t enable Data Protection
- Settings > General > Passcode
- http://support.apple.com/kb/HT4175

Storage Devices

Portable Storage Encryption

Goal: Minimize possibility of errors
Tactic: Use hardware encrypted devices whenever possible

Software Encryption

- Should only use on external hard drives
- PGP
- Bitlocker To Go
- Truecrypt
- USB device restrictions
  - Deny write to unencrypted drives
  - Restrict based on device ID
USB Trade-In Program

- Faculty and staff only
- No charge
- Equivalent capacity
- One per person
- Old drives will be destroyed

Yes, Destroyed

Media Destruction

Drop off at Help Desk in the Hub
- Hard drives
- Tapes
- Floppies
- Flash drives
- Devices

USB Trade-In Dates

Hub:
- Oct 25 8-12
- Nov 10 1-4

Library West:
- Oct 27 1-4
- Nov 8 8-12

Buying Extra Drives

- UF Bookstores
- We can facilitate orders from CDW-G at discounted prices:
  - 2gb = ~$24
  - 4gb = ~$31
  - 8gb = ~$50
  - 16gb = ~$108
- Trying to get them added to MyUF Market

Encrypting With PGP
PGP @ UF

- Meets all policy requirements
- In use since 2007
  - Supported by security office
  - ~3,500 devices encrypted
  - Windows, Mac, and Linux
- CIO purchased additional licenses to cover all of UF

Recovery Tokens

Security-l@lists.ufl.edu

Proving Encryption

Installation Process

Step 1. Spinrite

Step 2. Install PGP Desktop

Step 3. Enroll with the Universal Server
Installation Process

Step 4. Configure Single-Sign On

Step 5. Wait…

Setting Up Your Policy Group

- Form on infosec.ufl.edu
- Unit name
- Contact
- Who is authorized for WDRT
- UFAD group
- Force Encrypt
- Help text
- Audio prompts
- Autoupdates

PGP Updates

What Could Go Wrong?

Password changes:
1. Use old password for Bootguard
2. Use new password at GINA
3. It will sync for next login
Don’t Be An Early Adopter

- Most problems caused by jumping too soon
- New hardware
- OS updates
- Version upgrades
- No support for SSDs!

When It Goes Wrong

Symantec Connect:
- http://www.symantec.com/connect/security
- Forums
- Blogs

Symantec support:
- We can help open tickets

Fixing Things

Links on infosec.ufl.edu:
- Rescue Disk
- WinPE

We’re Here to Help

Security-l@lists.ufl.edu
273-7478 273-1344