

Laptop Encryption

Tom Throwe

RHIC and ATLAS Computing Facility

1 August 2007

Outline

- 1 Introduction
 - Requirements
 - Realities

- 2 Software
 - Products

- 3 Conclusions
 - Conclusions

Outline

- 1 Introduction
 - Requirements
 - Realities

- 2 Software
 - Products

- 3 Conclusions
 - Conclusions

Requirements

Due to high profile coverage of the theft or loss of laptops, encryption of the contents of laptop disks is becoming mandatory.

- TMR-22 (as presently written).
 - “Note: All portable/mobile devices are assumed to contain PII unless a designated authorizing Federal management official determines there is no PII on the device.”
 - “Install encryption software for all portable/mobile devices that contain SUI or may contain SUI in the future.”
 - “Encryption is required for protecting SUI hosted on all portable/mobile devices, desktop computer systems, and any removable media. Encryption of the entire contents of the hard drive(s) of each desktop computer system/workstation (including laptops) is preferred for protection against data theft or loss and additional defense against cyber attacks.”

Outline

1 Introduction

- Requirements
- Realities

2 Software

- Products

3 Conclusions

- Conclusions

Realities

- While “Federal Information Processing Standard (FIPS) 140-2 Level 1 or higher encryption” is required by TMR-22, products certified at this level are only available under Windows.
- Full disk encryption is not required
 - Takes over MBR so dual boot option is eliminated.
 - Sleep or Hibernation modes can be adversely affected.
 - Backup issues.
 - Performance issues.
- Container based systems are allowed (and encouraged).
- All laptops must have auditable encryption software on them.
 - Most people will not have any SUI or PII on their machines.
 - Just have to demonstrate that the machine is capable of encrypting files.
- Other Labs are ahead of us on laptop encryption.

Outline

- 1 Introduction
 - Requirements
 - Realities

- 2 Software
 - Products

- 3 Conclusions
 - Conclusions

FileVault

- Built in to Mac OS X 10.3 or above.
- Encrypts your home directory using AES-128.
- On-the-fly encryption of everything in your home directory.
- Files are encrypted using your account password. There is also a master password that can be set.

Pointsec

- Full disk encryption for a Windows and Linux, but have only heard the Windows version discussed by ITD.
- On-the-fly encryption of everything on the disk.
- Software is proprietary and licensed (product was recently bought by Check Point Software Technologies LTD) and will be provided by ITD.
- Only product FIPS 140-2 certified.
- Prompted for token and/or password at boot time.
- A key is held in escrow.

Windows EFS

- Windows Encrypted File System (EFS).
- Built in to Windows 2000/XP(/Vista?).
- Container (Folder) based encryption.
- On-the-fly encryption of everything in the folder.
- FIPS compliant algorithms, but do not know if certified.
- Uses locally generated certificates.

Gnu Privacy Guard (GPG)

- Available under Windows, Mac OS and Linux.
- File based encryption.
- Mainly used for secure file sharing with PKI (email).
- Can be used to encrypt files with a symmetric key.

Linux EncFS

- Linux Encrypted File System (EncFS).
- Container based encryption.
- On-the-fly encryption of everything in the container.
- FIPS compliant algorithms, but not certified.
- Runs in user space using the FUSE kernel module (Filesystem in USErspace), so do not need root privileges to use (after it is installed).
- If not mounted, can backup the container.

TrueCrypt

- Runs under Windows and Linux.
- Container based encryption where the container is a virtual disk, physical disk partition or entire device (USB flash drive).
- Encrypted portable media can be mounted from both Windows and Unix
- On-the-fly encryption of everything in the container using AES-256.
- FIPS compliant algorithms, but not certified.
- Plausible deniability.

TrueCrypt (cont.)

- Windows installation just requires downloading and running a Windows installer binary.
- Very good user guide explaining installation and configuration.
- Administrative privileges to install, but all mounting and encryption/decryption can be done without administrative privileges.
- Wizard for creating and mounting containers.
- Containers mount on a drive letter.
- If not mounted, a container can be backed up.

TrueCrypt (cont.)

- Linux documentation is limited (man page and generic information from the user guide).
- Linux installation requires a kernel module.
 - On RHEL and SL, need to build kernel module and utilities from source.
 - Distribution is missing the `dm.h` header file, but it does not seem to have changed since 2002.
 - Once the header file is installed in `/usr/src/kernels/<your kernel>/drivers/md/dm.h`, the code builds (`./build.sh`) and installs (`./install.sh`) without a problem.
- Requires `sudo` setup for non-root user to mount a container.
- `truecrypt -c` interactively creates a container.
- `truecrypt <volume> <mount point>` mounts the container.
- Can mount container anywhere you have permission to write.
- If not mounted, can backup the container.

Outline

- 1 Introduction
 - Requirements
 - Realities

- 2 Software
 - Products

- 3 Conclusions
 - Conclusions

Conclusions

- Auditable encryption software required on all laptops.
 - Need to demonstrate that the machine is capable of encrypting files.
- Recommend TrueCrypt since it works on Windows and Linux and encrypted media can be mounted under both systems.
- Recommend that you install the software or something will be installed for you.
- Links are available at http://www.phy.bnl.gov/computing/index.php/Disk_Encryption