Whole Disk Encryption

Encrypting drives under Windows, Linux, and MacOSX

By: The Doctor [412/724/301/703] [ZS|Media]
drwho@virtadpt.net
https://drwho.virtadpt.net/
PGP key ID: 0x807B17C1
PGP fingerprint: 7960 1CDC 85C9 0B63 8D9F DD89 3BD8 FF2B 807B 17C1

By: Punkbob (MacOSX stuff)
By: Other folks at the DC #cryptoparty

V1.0

What is it?

- Encrypting all the data on the drive
  - Hard drive
  - Removable media
- Data never hits the drive unencrypted
- Protects data at rest, i.e., when it's offline
- Protects some data in motion, i.e., if you don't specifically unlock it
  - If you encrypt the OS, you have to unlock it

What do people do with it?

- Encrypt the system drive to protect everything
  - Requires a passphrase to boot
- Encrypt a partition to protect some data
  - Requires a passphrase to access but not boot
- Encrypt removable drives in case they get lost or are stolen
  - No passphrase == no access

Options for Windows, I

- TrueCrypt (https://truecrypt.org/)
  - Open source, cross-platform (kind of)
  - Can create encrypted volumes that look like big files full of noise
  - Can encrypt hard drives without having to reinstall the OS or data
    - Takes time to complete
    - Will require a passphrase on boot
  - Can create hidden volumes inside of encrypted volumes
    - Deniable
    - If second passphrase not given, volume can potentially be destroyed

Options for Windows, I.5

- Truecrypt (cont'd)
  - Can create a hidden volume with a copy of your existing OS
  - Work with less secure stuff in the primary
  - Work with more secure stuff in the secondary
  - Helps mitigate data leakage through temp and swap files
  - Not protecting hidden volume with both passphrase can result in corruption of the hidden volume

Options for Windows, II

- Symantec PGP Desktop
  - Includes a disk encryption component
  - Requires a passphrase to boot
  - Commercial software
  - Can be centrally managed
  - Multiple keys can access drives
  - Have to trust that there are no backdoors

Options for Linux, I

- LUKS (Linux Unified Key Setup)
  - Built into the kernel
  - Any file system can be created inside of a LUKS volume (FAT-16... ReiserFS4)
  - Multiple passphrases on the same volume
  - Keyfiles can also be used to unlock volumes
  - Many distros support installing to LUKS volumes
    - Passphrase or keyfile on boot
  - Volumes can be created on any storage media
  - Retrofitting requires backing up and restoring everything or setting up on first install

Distributions that support installing to LUKS volumes

- Debian/Ubuntu (alternate install disks)
- Redhat/derivatives
- Slackware (takes a little work)
  - ftp://ftp.slackware.com/pub/slackware/slackware-current/README_CRYPT.TXT
- Arch Linux (takes a little work)
  - https://wiki.archlinux.org/index.php/Installing_Arch_Linux_on_LUKS
- Gentoo (takes work)
  - https://wiki.gentoo.org/wiki/DM-Crypt_LUKS

Options for Linux, II

- EncFS – Encrypted file system in userspace
  - Sits on top of existing file system
  - Files (and filenames) are encrypted
  - Attempting to manipulate them without accessing will corrupt them
  - Requires no elevated privileges
  - Supported by many distros
    - Ubuntu will ask you to set it up when an account created
  - Can be retrofitted without much trouble
  - Does not protect the rest of your system

Options for MacOSX, I

- Filevault
  - Built into OSX
  - Introduced with Panther (10.3)
  - Up to 10.6 (Snow Leopard), will encrypt home directory (works like Linux's EncFS)
  - From 10.7 (Lion), can encrypt entire drive (Filevault 2) (works like TrueCrypt)
  - Security history is dodgy
    - VileFault is capable of cracking v1 and v2
    - Early versions store passphrase in system keychain, where it can be extracted
    - Filevault 1 is vulnerable to keyloggers

FileVault, cont'd

- If your local account can be reset from your Apple ID, Apple can theoretically be coerced or tricked into doing so, which also exposes your encrypted drive (Mountain Lion)
- You can store your decryption key with Apple, which puts it into someone else's hands.
- Also, answers to authentication questions can be Googled, social engineered, or inferred
- Howto: https://support.apple.com/kb/HT4790

Options for MacOSX, II

- Symantec PGP Desktop for OSX
  - Haven't used it, don't know how well it works
  - Good luck.

FileVault Warnings

- If you use it to encrypt your hard drive and you then upgrade OSX to the next release, your system is wrecked
- You'll have to reinstall everything
- Decrypt your hard drive before upgrading to the next major release

Setting up Truecrypt

- Download
- Check the cryptographic signature!
- Run the installer
- Start TrueCrypt
- System → Encrypt System Partition/Drive
- Follow the instructions in the wizard
- It'll ask you to create a rescue disk
  - Burn the .iso image to CD and put it away
- You can also decrypt a drive this way

TrueCrypt Warnings

- If you upgrade major system components (mainboard, CPU) generate a new rescue disk
- Rescue disks are unique to that system's hardware configuration
- Pre-upgrade rescue disks won't work and you'll have to rebuild your system

Risks

- Putting laptops in sleep mode means the data is still accessible – don't do this!
  - Shut your machine down when not in use!
- Presence of encrypted media is inherently suspicious
  - “What do you have to hide…?”
- Some agencies train their personnel to assume that hidden volumes are present if they see a copy of TrueCrypt
- Swap space is often not encrypted
  - If you can encrypt swap space, do so

Risks, cont'd

- Evil Maid attack
  - Attacker accesses your shut down machine
  - Attacker installs a hacked boot loader
  - Hacked boot loader captures your passphrase or decrypted volume key
  - TPM doesn't help – Evil Maid attack has already been implemented for this
  - Physically lock your machine up somehow
  - Boot from removable media that you trust more
    - USB key that you carry on your person

Special Thanks

- Punkbob for helping me with the MacOSX stuff
- Everybody at the DC #cryptoparty who filled in stuff I forgot

I know I forgot some stuff...

Here I throw the floor open for discussion...

Comments?

Questions?

Anything we missed?