Eject the Warp Core

A practical look at filesystem segregation and encryption.

What is filesystem segregation?

- Spreading out your system partitions across different storage devices / storage mediums.
- For instance: Some people store /home on a different partition or device so they can easily change distributions without losing their data.
- But this type of separation can also have security benefits.

/
(Everything Else)

SWAP
/home

Filesystem segregation across multiple storage devices.

What is filesystem encryption?

- Cryptographically locking a filesystem, unlockable by various authentication methods:
  - Passphrase
  - Keyfiles
  - Certificates
  - One-Time-Passwords

Common tools include:

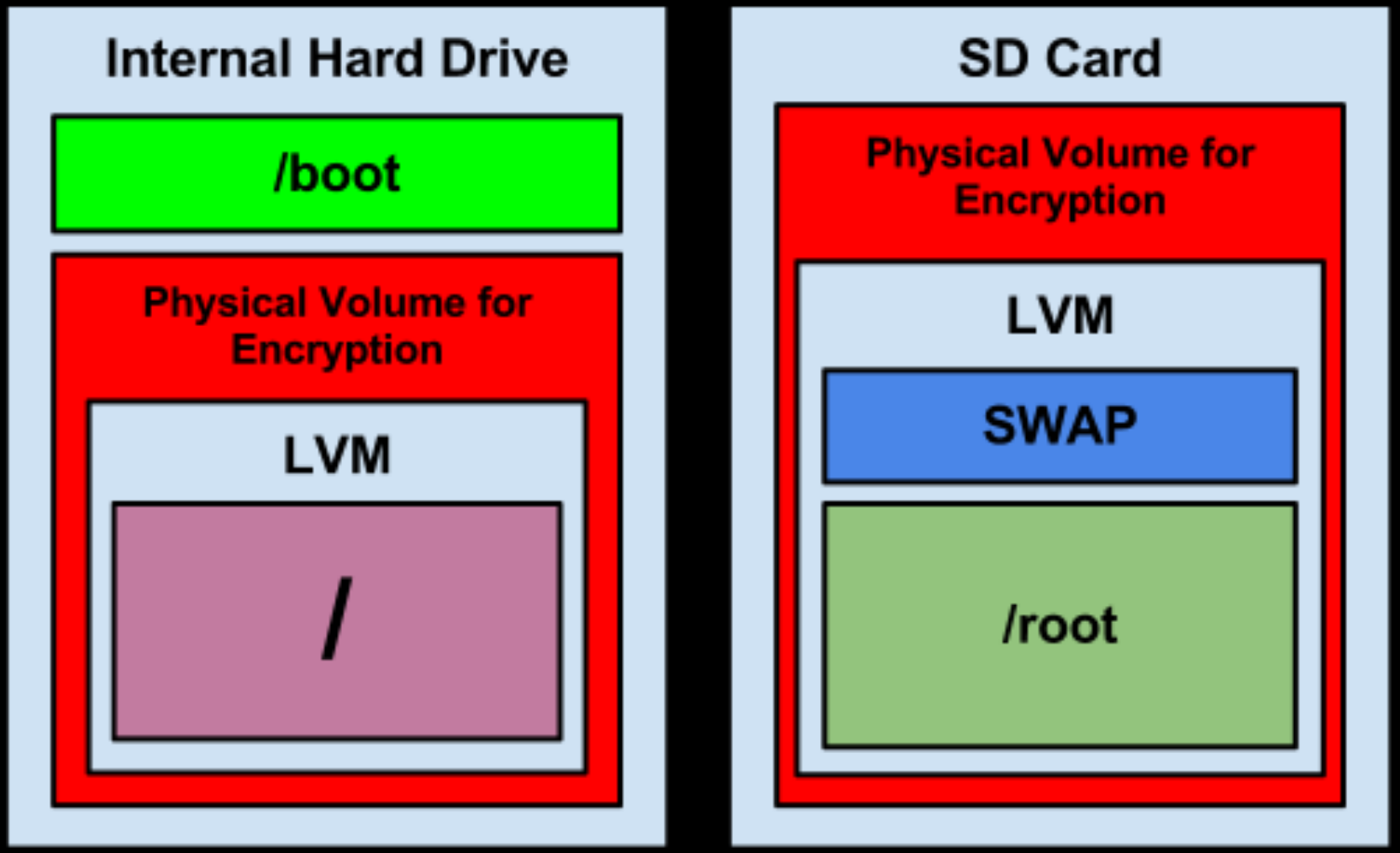
- TrueCrypt
- dm-crypt
- BitLocker
- FileVault

What happens when we combine these with removable storage?

By separating the most sensitive areas of our filesystem onto an encrypted, removable drive, we can better protect and secure our data from various interested parties.

The Ejectable Core Backtrack Machine

Partition Layout



Tools Used

- Backtrack 5
- Manual partition editing
- dm-crypt/OpenLUKS
- LVM2
- Some CryptTab Edits
  - To automate mounting of the "Core" on boot.
- chroot
- blkid

When booting this system with the core installed, it asks for two passwords: One for the local hard drive, and one for the core. If the system boots without the core, you have an option to skip mounting and continue the boot.

This allows us to boot a standard "Live CD" version of Backtrack without having to expose our sensitive data.

Keep in mind...

Like all forms of security - It relies on you to have a security-conscious mind.

- If you always keep your "Core" attached to your device, it defeats the purpose of filesystem segregation.
- If you use the same passphrase for your onboard and removable storage, it lessens the effectiveness of your encryption.

Practical Applications

- The obvious increase in security.
  - Even if the machine is taken, your data is guaranteed safe in your hands.
- Corporate deployment potential.
  - Each machine can have a base config while allowing each employee to maintain their own data and privacy.
  - Quick and easy deployments, employees don't have to worry about transferring data when upgrading or replacing their hardware.
- Increased data portability.
  - Using multiple machines becomes extremely easy to do.
- Better than backups.
  - Having the original data is always faster than restoring from backups.
  - Guaranteed that the data is always current.

Made possible by:

This work is based on work by Kevin Riggins on infosecramblings.com

Original Article: Backtrack 5 – Bootable USB Thumb Drive with “Full” Disk Encryption (bit.ly/BT5Enc)

Thanks to renderhead44 for the nice Truecrypt icon. [CC-BY-NC-SA-3.0] (bit.ly/IZIxmn)

Thanks to Everaldo Coelho for the Crystal Clear icons used in this presentation [LGPL] (bit.ly/JhxX4o)

Shameless Plug

My site: SamuraiLink3.com

Google+ Profile: bit.ly/tomwebster

Questions/Answers/Comments/Interpretive Dances