Secure Storage

Secure Storage

- Secure file formats:
- MS office, Acrobat allow password protection by encryption.
- MS Office creates an encryption key by hashing a password 50000 times
  - Makes brute force cracking impractical
  - Acrobat brute forcing can try 75million guesses per second.
  - Office brute forcing can only try 5000 guesses per second.

Windows EFS

- Encrypted file system
- Uses public/private keys
- Documents can store multiple copies of decryption key, encrypted by different public keys (allows many users to share a document).
- Data recovery Applets (DRAs) allow admin to decrypt documents.

Windows EFS

- But:
- Encrypts file contents, not names, metadata
- Only works with EFS file system
- Cached, temp files unencrypted
- Uses Windows password as part of private key.

Truecrypt

- 3rd party solution
- Encrypt complete hard drive or TC containers.
- Mount as a drive in windows; device in Linux
- Provision for plausible denial. Hide TC inside another TC.
- Requires root rights to create an NTFS container, but anyone can mount a TC container and use it.
- Shut down (not supported) since May 2014

Bit Locker

- Windows technology
- Creates a plain text partition for pre-booting, and an encrypted partition for Windows, data.
- Uses TPM to manage keys.

Free Compusec

- Open source solution
- Intercepts drive R/W commands and encrypts/decrypts the stream
- Full drive encryption only
- Modifies MBR to load Compusec drivers to mount drive.

Limitations

- These disk encryption schemes keep a symmetric key loaded into memory during operation.
- A RAM sniffing attack (e.g. cold boot attacks, *Inception*, *WinLockPwn* (Adam Bolieu)) can extract the key, making the entire drive visible to an attacker.
- Such attacks require physical access.