Crypto Filesystems for OpenSolaris

Darren Moffat

Today

- Per file only
  - encrypt(1)/decrypt(1) & digest(1)/mac(1)
  - Legacy: crypt(1), des(1) – not recommended for use

Options

- Linux cryptoloop / MacOS X File Vault Style
  - Encrypted block device
  - For Solaris this means extend lofi(7d)
- Windows XP Style
  - Encryption in the file system
- VFS Shim
  - Make a stackable VFS module that interposes on all reads/writes/mmap etc.

Choosen Path (1): lofi

- Extend lofi(7d) and lofiadm(1m)
  - Prototype developed by myself and Casper Dik
  - Working just now with AES_CBC
  - Includes support for encrypted swap space
    - Ephemeral key on boot
  - PAM module for mounting encrypted “disks” at login

Lofi Solution: Where & When

- Plan to put up as an OpenSolaris project real soon.
- lofiadm(1m) changes need to be cleaner.
  - Needs crypto framework extensions for userland admin commands seeing kernel provider info.

Choosen Path (2): ZFS

- Encryption in ZFS
- Set encryption policy at the file system level
- Will support encrypted zvol as well
- Will support keys in hardware
- Phased delivery
  - Mainly different key management systems
    - Eg for escrow, backup/restore
- Hope to support secure delete via this
- NOT taking on encrypted root filesystem

ZFS Solution: Where & When

- First Draft of design doc due mid January to zfs-discuss@opensolaris.org & security-discuss@opensolaris.org
- First Prototype due end January
- Hope to have phase 1 support integrated for Solaris Nevada shipping – not yet commited.
- Has same pre-requisites as lofi(7d) solution