HZVAULT

majinboo - NDH 2k10

EXISTING

- Introduction
- Existing solutions
- HZVault design
- Conclusion
- Questions

INTRODUCTION

- Data need to be accessed everywhere
- Everyone have sensitive data to protect
- Only a few solutions on the market with major drawbacks

MAJOR RISKS

- Laptop and external HDDs are often filled with sensitive data
- Only one physical access is enough for dumping data or installing backdoors

DATA PROTECTION DIFFICULTIES

- Full disk encryption is not easy to install
- Each technology work on only one OS :
  - o TrueCrypt on Windows
  - o Luks on Linux
  - o GELI on FreeBSD

WHAT DO WE NEED TO PROTECT ?

- Avoid backdoors on the system :
  - o write access should be controlled
  - o read access is less dangerous
- Avoid data leak :
  - o read access should be controlled

IDEAS

- Full disk Encryption
- Data separated from system
- Virtualization in order to avoid incompatibilities

GLOBULL : ADVANTAGES

- Hardware AES
- Virtualization Support (Optional)

GLOBULL : DRAWBACKS

- Expensive
- Limited Host compatibility
- Capacity limited to 160 GB

DATALOCKER : ADVANTAGES

- Hardware AES
- Capacity up to 320 GB
- Less expensive than Globull

DATALOCKER : DRAWBACKS

- Still expensive
- No virtualization solution

HZVAULT

- Full AES encryption for any HDD or USB Key
- Enhanced compatibility
- Possibility to use multiple OSes (Linux, *BSD, Windows, ...)

CONCEPTION

- Luks provide AES Encryption
- Minimal Debian Linux for Level 0
- VirtualBox for Virtualization
- User-friendly interfaces for installation, configuration and utilization

ENCRYPTION

- /boot unencrypted
- Two encrypted partitions :
    - o Level 0 + OSes
    - o Data
- /tools partition : FreeOTFE for accessing the drive from Windows

EVIL MAID ATTACK

- Modification of boot-loader
- Boot-loader will log password
- Only need a couple of seconds

PROTECTION

- Two different passwords
- Boot-loader integrity check performed before unlocking data partition
- Still vulnerable to complex attacks
- Best solution (maybe in a future release) : booting from RO media like CD-R

LEVEL 0

- Debian Linux
- Performs only a few tasks :
  - o Integrity checks
  - o Virtualization
  - o User interfaces

VIRTUALIZATION

- Access from the VM to physical devices on the host : DVD-ROM and USB devices.
- Auto-detection of host hardware (e.g. optimizing RAM utilization)
- Compatibility with host without VT instructions

FLAVORS

- without virtualization :
    - o small USB Keys
    - o netbooks
- without software AES :
    - o Datalocker
    - o GloBull

RELEASE

- Exclusive pre-release for challenge winners
- First version available in a few days
- OpenSource (beerware license)
- IRC : #hzvault on FreeNode

CONCLUSION

- Easy to use and affordable solution
- Complementarity with existing hardware encryption solutions

GREETZ & QUESTIONS

- Greetz : Free_Man & T0ka7a
- Questions ?