
Personal Mobile
Disk Encryption


Disk Encryption:
The not so tasty
vegetables of IT

Encryption: It's good for you

- Can we trust encryption?
- "My computer is secure. I don't need encryption"
- Can encryption be supported?

Laptop Theft

- We bring more data with us
  - Laptops, Phones, USB drives & PDAs
- Theft is #2 most common attack on data
- We depend on physical security
- We're responsible to protect data


Disk Encryption
Protects Data on Stolen
Laptops

Disk Encryption Basics

- Symmetric Keys
- Typically longer keys are stronger
- Block Ciphers
  - AES Advanced Encryption Standard
  - DES Data Encryption Standard

Tough Questions

- Where should confidential data be stored?
- Should this data be encrypted?
- How will we manage keys?

Buyer Beware

- “Encryption Consumers”
- Ask **tough** questions of vendors
- Teach the basics

Questions for Vendors

- Get the details before purchase
- What encryption do you support?
  - Don’t buy proprietary encryption
- How are keys managed?
  - Don’t use vendor supplied keys

Key Encapsulation

- Passwords aren't good encryption keys
  - Keys are typically 256 random bits
- Key storage is like a matryoshka doll
- Password unlocks encryption key
- Encryption key unlocks data

Key Management

- Protect the keys
- Create recovery keys
- Use Key escrow

Truecrypt
It's FREE

- Open source and publicly reviewed
- Cross platform
  - Windows, Linux & OSX (Coming Soon)
- Encrypted files are accessed as drives
- Never stores decrypted data to

Truecrypt Key Storage

- Password decrypts volume header
- Volume header contains the Master Key
- Master Key can decrypt data
- Make copies of header
  - Backup & Restore Master Key
  - Create Recovery Keys

Keyfiles

- Use a random file and a password
- 2 factor authentication
  - USB key with keyfile (Something you have)
  - Password (Something you know)
- Protects against key stroke loggers

Create Recovery Keys

- Truecrypt lets you backup your master key
- Changing passwords won't generate a new master key
- You must create a new encrypted volume to protect your master key

Best Practices

- Truecrypt is great for individual use
- Find confidential data
  - Cornell's Spider (Windows & Linux)
  - CC, SSN, or custom
- Update on mobile device policy

Truecrypt Demo

- Create encrypted volume
- Create / Restore recovery key
- Use USB device as password
- Create escrow key

Resources

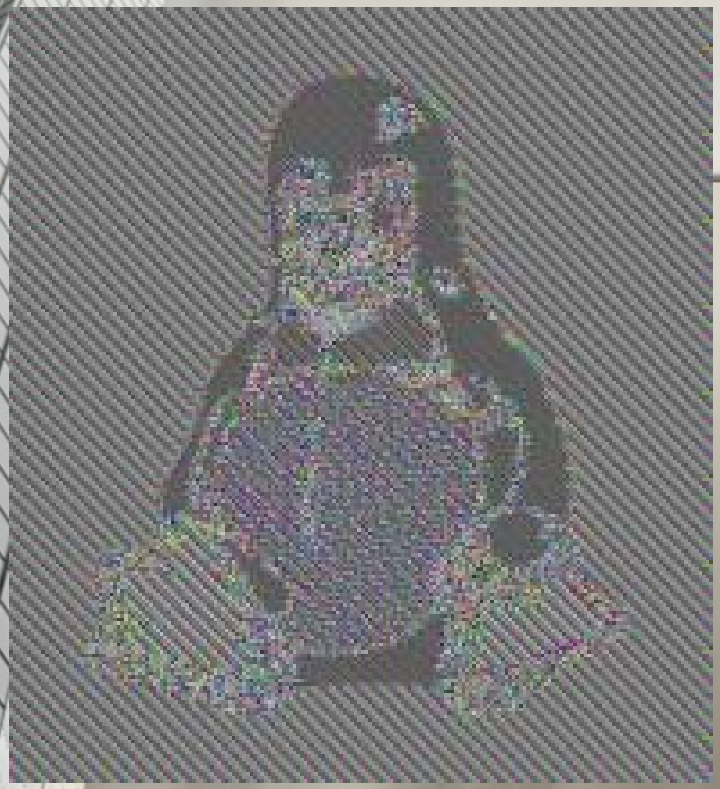
- Wikipedia.org
  - Cryptography, Ciphers, MOO
- MS Info on AES
  - http://tinyurl.com/euc9c
- U. Minnesota Encryption Tools List
  - http://tinyurl.com/j6kdj
- Cornell Spider – Find Confidential Data
  - http://itso.iu.edu/Cornell_Spider

Other Encryption Software

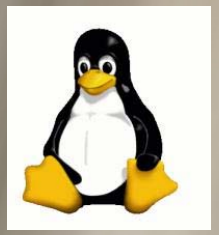
- GPG – Open source public key
- Built in Encryption Windows, Linux, OSX
- PGP – Pretty Good Protection RSA
- Pointsec, Safeguard, secure zip
- **http://tinyurl.com/j6kdj**

Mode of Operation

- AES-CBC
  - CBC Cipher Block Chaining
- Ensure integrity and resist cryptanalysis
- AES can only encrypt 128 bits
- Use CBC to encrypt large files



Encrypted Blocks



Block Chaining