Best Practices for Protecting Mobile Data in the Enterprise

Rich Mogull
Securosis, L.L.C.

The Triple Threat

Why All The Attention On Encryption?

Bad Guys Value Data

Breach Notifications

Direct Regulations

The Top 4 Causes Of Data Breaches

- Lost/Stolen Laptops
- Lost/Stolen Backup Tapes
- Inadvertent Disclosure
- Hacking/Compromise

Lost Laptops and Portable Media

- May 23, 2005: MCI: laptop stole with 16,500 employee records from unlocked car
- August 30, 2005: JPMorgan Chase laptop stolen with information of premier private banking clients
- June, 2006: IRS loses nearly 500 laptops over 3.5 years
- March, 2006: Ernst & Young loses laptop with personal information of thousands of corporate customers
  - June, 2006: 243,000 Hotels.com customers exposed in second incident, laptop stolen from car in February
- February, 2006: a Deloitte & Touche employee leaves a CD with personal records of 9,290 McAfee employees in airline seatback

The law of data breaches

Businesses suffer from breaches even if customers don’t suffer from fraud.

The Three Laws of Data Encryption

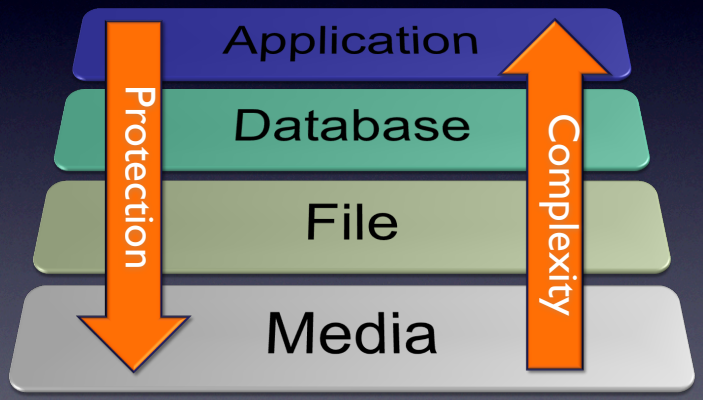
If Data Moves Physically or Virtually

For Separation of Duties

Mandated Encryption

Securosis.com

Encryption Layers



Securosis.com

Encryption Options

File/Folder

Application/
Database

Media

Mobile Encryption Options

Portable Media

Whole Drive

Partial-System

Securosis.com

Where to Encrypt

Separation of Duties

- Database Fields
- Workstation File/Folder
- Server
- NAS
- Applications

Movement/Media Protection

- Tape
- SAN
- Laptops/FDE
- Email
- Portable Media

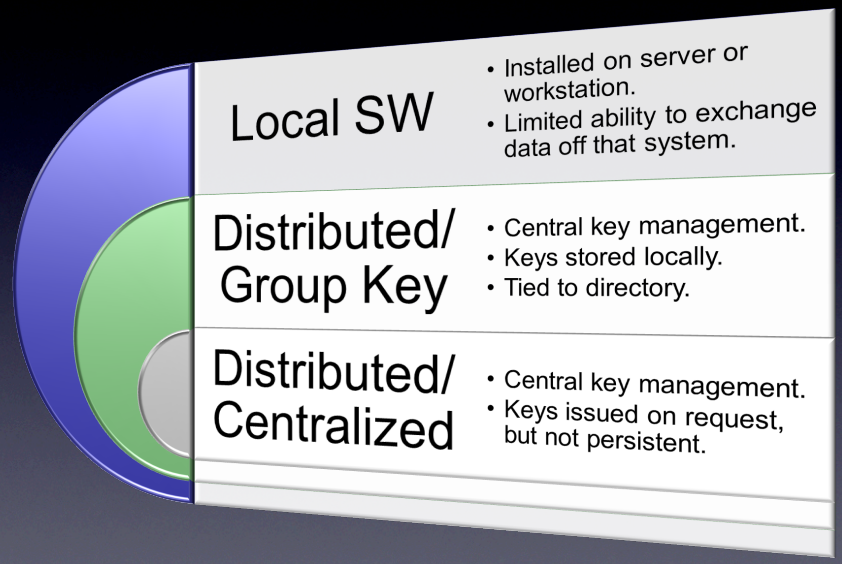
Securosis.com

Layered Encryption

Protect from administrators or other system users

Securosis.com

File/Folder



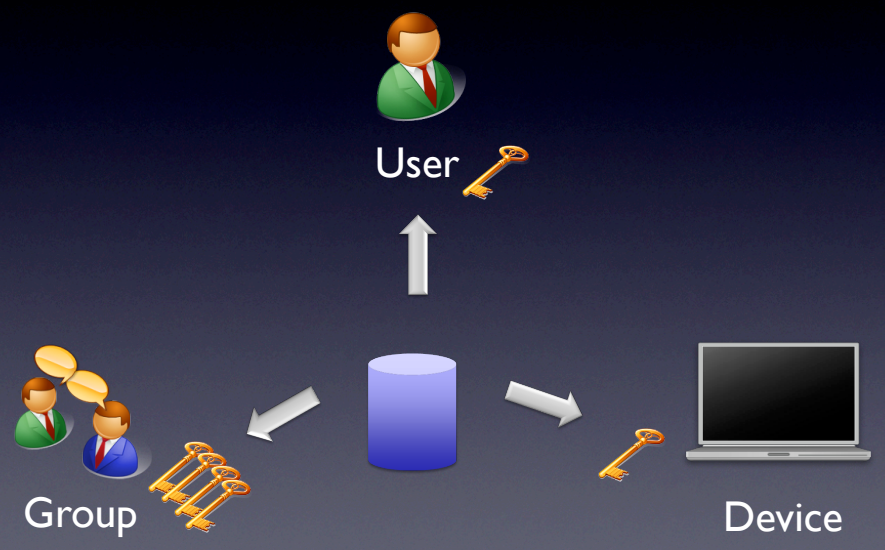
Local SW
- Installed on server or workstation.
- Limited ability to exchange data off that system.

Distributed/ Group Key
- Central key management.
- Keys stored locally.
- Tied to directory.

Distributed/ Centralized
- Central key management.
- Keys issued on request, but not persistent.

Securosis.com

Key Management

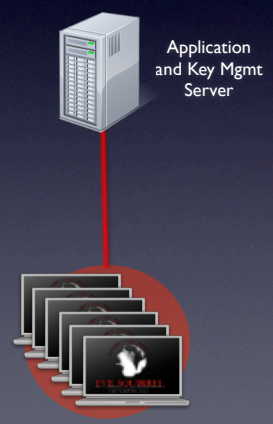


Securosis.com

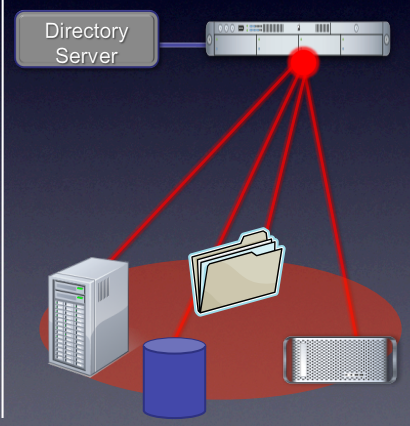
Key Management Options

Local

Managed/ Application



Centralized



Securosis.com

Centralized Key Management

- Cross platform
- Cross Application
- Separation of Duties
- Directory Integration
- Hardened
- Key Backup/Restore/Rotation

Securosis.com

Creating Your Key Management Strategy

- Determine protection and compliance requirements.
- Decide who will manage the encryption, and if SoD is required.
- Analyze capabilities
- Group like-managed encryption with centralized management.
- Don't try to force all encryption to centralized.
- You can still leverage centralized for backup/restore/rotation even if primary management is at the application layer.
- Plan for the future- encryption is rapidly changing, be careful about lock-in.

Data Security

Authentication

- Pre-boot must integrate with your identity and access management infrastructure.

Deployment

- Encrypt images and existing systems. Background encryption. Software deployment.

Infrastructure Integration

- Support backup infrastructure, system updates, and configuration management.

Manageability

- Integrate with identity management, key management, and systems management.

Key Management

- Backup, rotation, migration.

When and How to Encrypt

Laptops	Always	Full Drive or Equivalent
Desktops	Highly Sensitive	File/Folder
Portable Media	Sensitive or Always	Media or Folder
Servers	Risk Based	Varies

Encryption Everywhere

Securosis.com

What It Means

- Laptop encryption is a mandatory risk control for sensitive data.
- Encryption is the commodity, manageability and integration are the differentiators.
- Encryption will self-consolidate and integrate more efficiently with information-centric security tools than traditional endpoint protection.
- Eventually you will purchase encryption management, the encryption engine will be built-in.

Rich Mogull

Securosis, L.L.C.

rmogull@securosis.com
http://securosis.com
AIM: securosis
Skype: rmogull