Enterprises and Encryption

Why Remote Management Matters

Amy Nelson
Dell, Security Architect
Data Security Solutions

IT Nightmare: Lost/Stolen Laptop

- Sales VP on a customer tour
  - Internal Sales Roadmap
  - Pre-release Demo
- HR Benefits coordinator
  - Employee PII
  - Benefits claims

Lost Laptop = Lost Data

Lost Data

- Intellectual Property -> =Loss of business advantage
  - Roadmaps
  - Pre-production demos
  - Design specifications
  - Supplier information
  - Organizational charts
- Personally Identifiable Information -> =Loss of reputation, fines
  - SSN's
  - Addresses
  - Payment information
  - Insurance information

What is the landscape?

87%

of organizations have experienced a security breach in 2013.

>650M

records have been compromised in 2014 in approximately 763 breaches.[2]

1/2

of all organizations admitted detecting an attack can take days, weeks or even months[4]

$201

the cost per lost or stolen record increased over the last year from $188 to $201.[3]

$5.9M

average amount paid following a security breach, up from $5.4M in 2013.[3]

73%

of companies concerned about lack of control and security in the Cloud.[5]

Endpoint Encryption, the Solution?

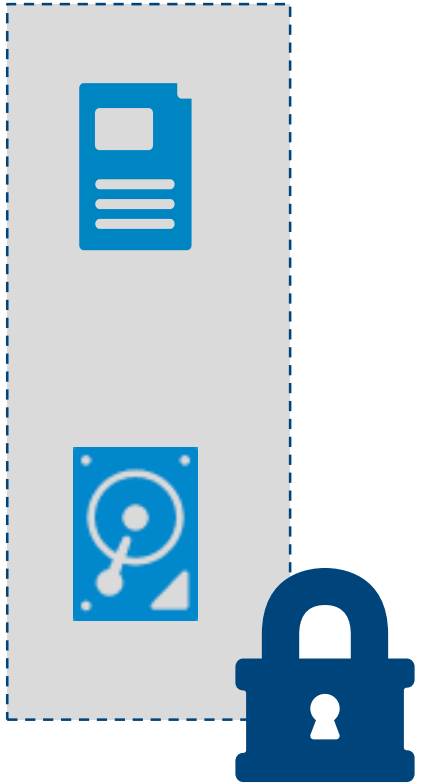
- PCI DSS 3.1
  - Requirement 3 – Protection methods ***such as encryption***, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls…. The data is unreadable and unusable to that person. [1]
- HIPPA
  - 45 CFR 164.312 - Encryption and decryption (Addressable). Implement a mechanism ***to encrypt and decrypt*** electronic protected health information. [2]
- Australian Privacy Policy 2013 and 2014 updates
  - "Agencies and organisations are required to take reasonable steps to protect the personal information they hold from misuse, interference, and loss, and from ***unathorised accesss, modification, or disclosure***." APP 11. [3]
- EU General Data Privacy Regulation
  - "Data controllers must implement appropriate security measures and provide, without undue delay, notification of personal data breaches to the supervisory authority as well as to those significantly affected by the breach….. Data controllers face fines of up to EU1M or 2% of their global annual turnover". [4]

Types of data at rest encryption

A short refresher

Data-at-rest (DAR) Encryption

- Local File Encryption
  - Operates on a file basis, at the file system level
  - Low overhead, low impact roll-out in after-market deployments
  - User aware
  - Media agnostic
- Full Disk Encryption
  - Operates at a sector basis, at the disk level
  - Requires a pre-boot authorization or authentication environment
  - Encrypts everything
  - Open to any User, unless locked
- Hardware-based Full Disk Encryption
  - TCG Opal and Enterprise SSC Self Encrypting Drives (SED)
  - Low overhead
  - Protection tied to power states of system



Protecting my data

Where do I start?

Protecting Your Data

- Why manage DAR encryption? Why report on DAR Encryption?
- What are the characteristics of a well-built solution? What am I managing? What am I reporting?
- Where is the management console? Where is the DAR?
- When do I deploy? When do I report?
- How do I evaluate a solution? How do I deploy, manage, and report?
- Know your needs

Evaluation: *Know Your Needs*

- Requirements Analysis:
  - Multi-User or Single-User Assets
  - Corporate or Bring-Your-Own-Device Assets
  - New, Existing or Mixed Asset Environment
  - Remote or on premise workers
  - Reporting and audit requirements
  - Data under corporate control or resident on 3rd-party cloud
- Data being protected
  - Personally Identifiable Information (PII)
  - Intellectual Property (IP)
  - Financial
- Threat model:
  - Insider Attacks
  - Network-based attacks
  - Physical attacks on travelling assets

Product checklist: *Requirements*

- ❑ Cryptographically isolates different users' data
- ❑ Deployable by IT staff through standard deployment models
- ❑ Deployable by End-Users with limited help-desk support
- ❑ Allows activation of product, deployment of policy inside and outside of firewall
- ❑ End-user authentication policy controls
- ❑ Tailored and customizable audit reports
- ❑ IT control of encryption keys inside of corporate firewall, independent of data location
- ❑ Policy applicability to fixed disks, removable media, cloud storage

Product Checklist: *Data to Protect*

- Each of type of data may be subject to different requirements
- PII and Financial data protection requirements vary by geo-political region, industry segment and/or public sector driven variances.
- Reporting requirements also vary by region, segment and sector
- Most regulatory/compliance schemes mandate additional processes and controls in addition to encryption
  - Access control
  - Destruction of data
  - Restrictions on sharing with 3rd parties
  - Length of storage
  - Notification and Consent

Product Checklist: *Threat Model*

- ❑ Integration with AD to enable seamless locking of accounts, group management
- ❑ Policy requiring periodic check-in of clients, or phone-home policy
- ❑ Interoperable with Anti-Malware/Virus/Spam products
- ❑ Interoperable with Trusted Computing Measured Boot, UEFI Secure Boot
- ❑ Encryption Keys stored encrypted
- ❑ Encryption Keys decrypted only with appropriate authorization, Derived Keys
- ❑ Dictionary attack mitigation
- ❑ Revocation or zeroization of keys on tamper

Product Checklist: *Threat Model*

- ❑ Integration with AD to enable seamless locking of accounts, group management
- ❑ Policy requiring periodic check-in of clients, or phone-home policy
- ❑ Interoperable with Anti-Malware/Virus/Spam products
- ❑ Interoperable with Trusted Computing Measured Boot, UEFI Secure Boot

Third Party Evaluated

Third Party Evaluation

Third Party Security Evaluations: FIPS v Common Criteria

- Penetration Testing
  - Generally vendor driven, non-standard
  - Evaluates a product against the latest, *known* attacks
- FIPS 140-2 is the US standard for evaluating cryptographic modules
  - Generally applies to devices, not systems, e.g. SED, TPM, cryptographic libraries
  - Evaluates correct implementation of cryptographic algorithms, handling of keys, and authorization of keys
- Common Criteria is the global agreement for evaluation of IT products
  - Can apply to devices and systems, e.g. Smartcard, TPM, Payment Systems, Servers, and Operating Systems
  - Evaluates, in addition to the integrity of the device or system, processes for design, manufacturing, deployment, support and remediation of the process.
  - For cryptographic products, may rely on country specific algorithm evaluations, such as FIPS 140
- Evaluation is performed over a vendor-defined boundary
- New to Common Criteria – Collaborative Protection Profiles

Why Collaborative Protection Profiles

"The purpose of the revision is to raise the general security of certified information and communications technology products without increasing costs or preventing timely availability of such products from commercial companies."

- Establishes international Technical Communities
- Establishes international, multi-stakeholder, multi-sector environments
- Participation from public and private sector entities
- Promotes fair competition
- Promotes consistency and alignment in testing activities across schemes

Full Disk Encryption (FDE) was addressed by the first collaborative Protection Profiles (cPP's) published (February 2015)

Full Disk Encryption cPP's

- FDE Encryption Engine and FDE Authorization Acquisition cPP's enable evaluation of
  - Software FDE
  - SED management Software
  - SED's
  - Hybrid or hardware accelerated software FDE
- Endorsed by US, Canada, Australia, New Zealand and the UK
- Published version evaluates
  - Locally managed, non-recoverable products
  - Authentication via Password, Token, or Smartcard
  - Verifies secure generation, storage, and destruction of keys
  - Verifies secure behavior of the system from provisioning to usage.
  - Provides assurance of predictable, repeatable evaluation results, regardless of scheme or lab

Upcoming changes to the FDE cPPs

- Version 2 in process in the Technical Community with the following features
  - Enterprise Management
    - Optional package allows evaluation of a remote management console in conjunction with an AA component
    - Evaluates specific key escrow and management processes
    - Requires secure communication between end-point and server
  - Power Management of SED's
    - Evaluates that drives entering a power saving state handle keys and authorization factors appropriately
    - Evaluates that authentication is supplied on exit from a power saving state
  - User Recovery
    - Optional features within the Enterprise Management package
    - Evaluates assisted and self-recovery mechanisms
  - Trusted FW Update

Version 2 gives customers assurance in the encryption solutions they need to protect their data.

The power to do more