



Ohio Information Security Conference '08

Kevin Kampman

Senior Analyst

kkampman@burtongroup.com

...But the Information was Encrypted!

www.burtongroup.com

Tuesday – 18 March 2008

...But the Information was Encrypted!

2



Thesis

- Encryption is not a panacea for compliance or for confidentiality
 - It is a control that can be used to protect the confidentiality of information in certain instances
 - Just because something is encrypted does not mean that it is protected
- There are tradeoffs that must be considered when using encryption
 - Availability and usability may suffer
- Encryption by itself is generally insufficient to provide any protection
 - There is a supporting cast that must also be in place

...But the Information was Encrypted!

3



Agenda

- So you want to encrypt...
- Regulations
- The supporting cast
- Recommendations

...But the Information was Encrypted!

4







Agenda

- *So you want to encrypt...*
- Regulations
- The supporting cast
- Recommendations

So You Want to Encrypt...

5

Speaking about data at rest – there are options!

Layer	Description	Vendors
 Users	<p>Users could be taught to encrypt sensitive files</p> <ul style="list-style-type: none">-Protects against anyone else accessing the information-But users might forget	<p>ISC, PGP</p> <p>Policy-based encryption from CREDANT</p>
 Applications	<p>Applications can be designed (or redesigned) to encrypt sensitive information</p> <ul style="list-style-type: none">-Access is controlled through the application-Application architects determine what is sensitive-Limits access to those who have legitimate access to the application	<p>Certicom, Cryptomathic, Entrust, NTRU, Oracle, EMC/RSA, Secude, Verisign</p>
 Repositories	<p>Information could be encrypted in the repository (DBMS, etc.)</p> <ul style="list-style-type: none">-Particular columns can be encrypted in the DBMS-Files by policy in the repository-Access is limited to those who have legitimate access to the repository	<p>Oracle, Sybase, IBM, Microsoft, AppSecInc, Ingrian, NetLib, Protegrity, Valyd</p>
 Media	<p>The media could be encrypted either through an appliance or directly on the media itself</p> <ul style="list-style-type: none">-Protects against lost or stolen media-Access via the application or operating system is not protected	<p>Appliances: Decru, NeoScale, Vormetric</p> <p>Products: Pointsec, Safeboot, Utimaco, GuardianEdge, PGP, etc.</p> <p>Backup applications</p> <p>Hardware: Seagate</p>



So You Want to Encrypt...

6

We can also encrypt data in motion

- Link encryption
- Virtual private networks (IPSec or SSL/TLS)
- Secure web sessions

Different alternatives protect against different threats

- There is a significant difference between someone stealing a laptop and someone hacking into a server
- There is a significant difference between someone eavesdropping on network traffic and an administrator looking at data

The type of encryption has to be matched to the risk!

- Encryption is a control that can be used to manage risk but only if it is appropriate to the threat and consequences

So You Want to Encrypt...

7



Not all types of encryption can counter all threats

Threat	Where to use encryption	Other considerations
A thief stealing a device or media or loss of a device by an employee	On the media – hard disk, tape, USB memory stick, etc. Application and repository encryption can also be used	Usability of the media Recovery of the information Forensics may be more difficult
An eavesdropper sniffing the network	Data in motion – IPsec or SSL/TLS VPN	Network monitoring Network performance
Someone accessing data in an unauthorized manner	Within the application or possibly the repository	Cost of application updates Availability of primary information Search may be more difficult
An individual gaining unauthorized application access	Encryption is not helpful	One-way hashing may prevent the disclosure of sensitive information but also limits uses of the information
Insiders	Encryption may not be helpful depending on the insider access	Use other mechanisms to detect inappropriate use
Regulators	Depends on the regulation	There are alternatives to encryption

...But the Information was Encrypted!

8



Agenda

- So you want to encrypt...
- **Regulations**
- The supporting cast
- Recommendations

Regulations

9



The bottom line requirement is to protect sensitive information in the first place

- Encryption is not required but can be used as a control

There are other alternatives

- Do not store sensitive information if you do not have to
- Use zoning, access control, authentication, vulnerability management, network devices, and other compensating controls

Encryption is seen as a get out of jail free card under the disclosure laws (i.e. you don't have to disclose the event)

- There is a tradeoff between the risk of a breach (and the necessary notification) and the technology implementation
- Breach notification laws have certainly gotten the encryption vendor's attention!
- But, if encryption is not used properly or if there are other weaknesses, it may not matter
- What does it mean to encrypt?





Regulations

10

Highlights of the California Security Breach Notice Law (SB1386)

- When
 - *"...disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."*
- What is a breach?
 - *"breach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information..."*
- What is personal information?
 - *"personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account"*



Regulations

11

Highlights of PCI Requirement 3: Protect Stored Cardholder Data

- While PCI does start out talking about how encryption can help you...
 - *"Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person."*
- ...PCI also says that there are other options!
 - *"Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities"*
 - Don't store the data
 - Mask or render the information unreadable
 - Truncate the cardholder data



Regulations

12

More highlights of PCI Requirement 3: Protect Stored Cardholder Data – If encryption is used:

- *"If disk encryption is used ..., logical access must be managed independently of native operating system access control mechanisms ... Decryption keys must not be tied to user accounts"*
- *"Protect encryption keys used for encryption of cardholder data against both disclosure and misuse"*
 - *"Restrict access to keys to the fewest number of custodians necessary"*
 - *"Store keys securely in the fewest possible locations and forms"*
- *"Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:"*
 - *"Generation of strong keys"*
 - *"Secure key distribution"*
 - *"Secure key storage"*
 - *"Periodic changing of keys ... preferably automatically At least annually"*
 - *"Destruction of old keys"*
 - *"Split knowledge and establishment of dual control of keys..."*
 - *"Prevention of unauthorized substitution of keys"*
 - *"Replacement of known or suspected compromised keys"*
 - *"Revocation of old or invalid keys"*
 - *"Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities"*

...But the Information was Encrypted!

13



Agenda

- So you want to encrypt...
- Regulations
- ***The supporting cast***
- Recommendations



The Supporting Cast

14

Encryption algorithms are strong and hard to break

- Encryption algorithms are tested for obvious weaknesses
 - AES went through a four year selection process
- Long keys (256 bit for example) are sufficient to limit today's brute force attacks

An attack will go after the weakest link in the encryption system

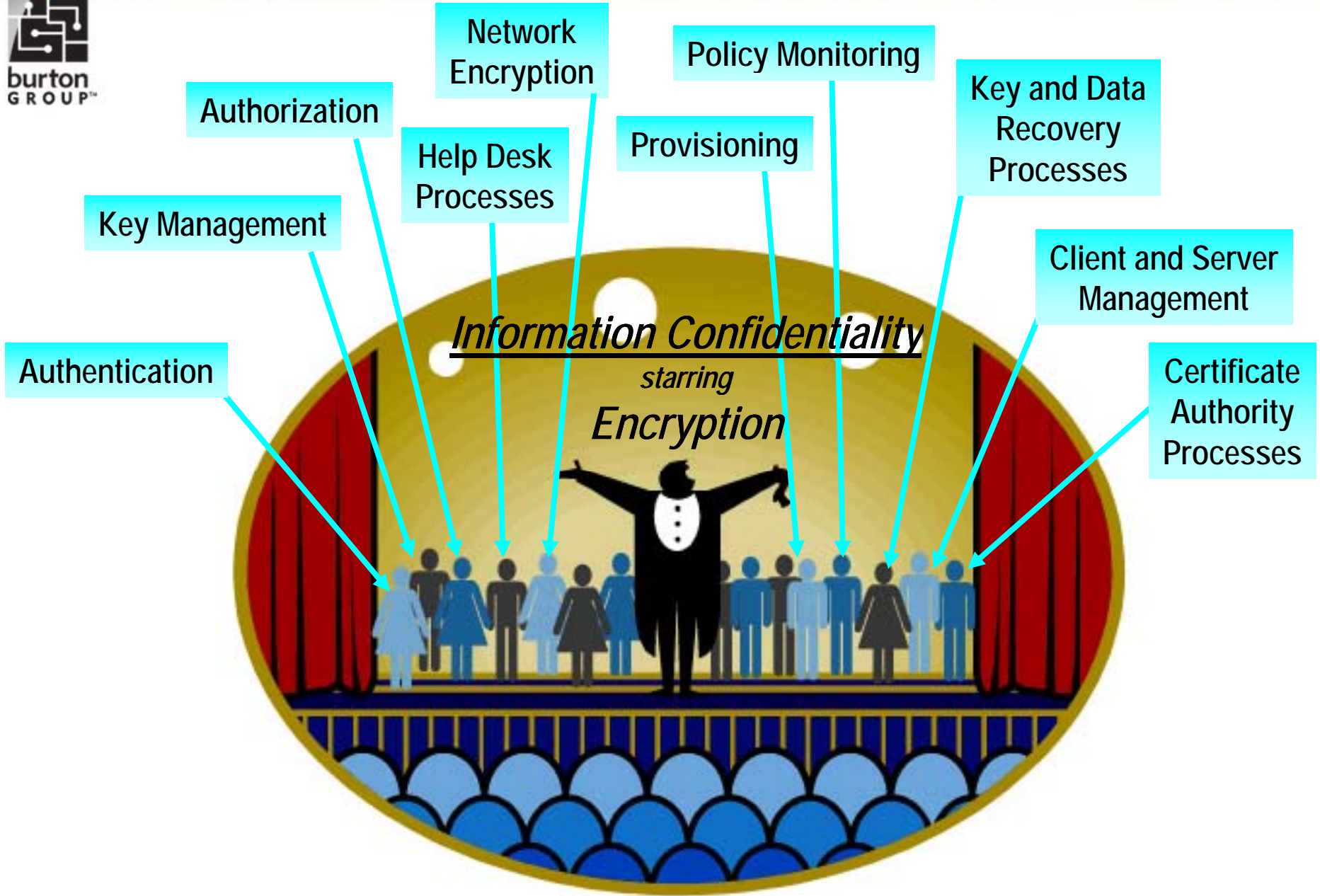
- No one is going to try to brute force all of the possible keys
 - At the very least, an attacker will find a way to reduce the key space
- Attackers are unlikely to find weaknesses in the algorithms
- Attackers will look for weaknesses in the supporting cast of mechanisms and processes

So even if the information was encrypted...

- Without proper support, the information may still be disclosed



The Supporting Cast



...But the Information was Encrypted!

16



Agenda

- So you want to encrypt...
- Regulations
- The supporting cast
- **Recommendations**

Choose your point of encryption based on the risk

- Encryption is a control and must be balanced against the risk
- In some cases encryption is not the best control to use

There are tradeoffs!

- Availability of information
- Usability of media and devices

Use the supporting cast properly

- The supporting cast is necessary to the security of the system
- Processes are very important
 - It is not just the key management processes
 - Helpdesk, recovery, provisioning, and authorization processes are just as important

...But the Information was Encrypted!

18



Conclusion

- Just because something is encrypted does not mean that it is protected
 - The supporting cast must be in place in order to provide the necessary protection
- There are other controls that can be superior to encryption for a given situation
- Many times we are under the misapprehension that encryption is what is required



...But the Information was Encrypted!

19



References

- *Security and Risk Management Strategies* Research
 - What and Why PCI?: Inside the Payment Card Industry Data Security Standard
 - Encryption for Mobile Hosts: Protection on the Fly
 - Security in the Palm of Your Hand
 - Database Encryption: The Hot Topic in Structured Information Protection
 - E-Discovery: No More Losing Needles in the Electronic Haystack
 - Cryptographic Systems Provide Foundations for Information Security
- *Security and Risk Management Strategies* Reference Architecture
 - Encryption Technical Position
 - Information Confidentiality Technical Position
 - Information Integrity Technical Position