PCI DSS Compliance

Ulf Mattsson, CTO
Bio

20 years with IBM Development & Services
- IBM Software Development & IBM Research consulting resource
- IBM Certified IT Architect in IT Architecture & IT Security

Created Protegrity's Data Security Technology
- Protegrity Policy driven Data Encryption (1994)

Inventor of 20+ Patents
- In the areas of Encryption Key Management, Separation of Duties, Policy Driven Data Encryption, Tokenization, Internal Threat Protection, Data Usage Control, Dynamic Access Control, Intrusion Prevention and Cross System Layer Security.

Master's degree in Physics and degrees in Finance and Electrical engineering
- Research member of the International Federation for Information Processing (IFIP) WG 11.3 Data and Application Security.
Agenda

- Data Protection Options for PCI and Beyond
- PCI Case Studies
- Advanced Attacks on Data Flow
- Determining Risks
- Cost Effective Approach
March 18, 2009: The Reality of PCI-DSS Compliance

ISSA New York Metro Chapter - Educational Program

Summary

The 2007 Computer Security Institute (CSI) Report indicates that more than one fifth of those surveyed have been victimized by a targeted attack. The study also concluded that financial fraud overtook virus attacks for the first time in seven years as the number one cause of financial losses from an IT security breach. Finally, customer and proprietary information was the second worst cause of financial loss. These trends show that the payment card industry faces more data security threats than ever before. The Payment Card Industry Data Security Standard (PCI-DSS) was created to mitigate these threats.

This session examines the challenges faced by organizations as they address their PCI DSS compliance requirements.

Presenter Bios

Ulf Mattsson, Protegrity Corporation

Ulf T. Mattsson, Chief Technology Officer, Protegrity Corporation, created the initial architecture of Protegrity’s database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM’s Research and Development organization. He specializes in the areas of IT Architecture and IT Security. Ulf is the inventor of a number of European patents and US Patents in the areas of Encryption Key Management, Separation of Duties, Policy Driven Data Encryption, Internal Threat Protection, Data Usage Control, Dynamic Access Control, Intrusion Prevention and Cross System Layer Security. He holds a master’s degree in physics, a degree in finance and a degree in electrical engineering.
How to Evaluate Encryption Technologies

Ulf Mattsson, CTO
Protegrity
Ulf Mattsson
Company Name: Protegrity
Expertise: Enterprise Key Management and Data Encryption

Job Title: CTO
Expert Bio: Ulf T. Mattsson is the CTO at Protegrity. Ulf created the initial architecture of Protegrity’s database security technology. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM’s Research and Development organization, in the areas of IT Architecture and IT Security.

Company Description: Protegrity provides data security management products, specifically enterprise key management and application firewalls.

http://www.knowpci.com
## Discussion of Data Protection for PCI DSS

| Build and maintain a secure network. | 1. *Install and maintain a firewall configuration to protect data*  
| | 2. *Do not use vendor-supplied defaults for system passwords and other security parameters*  
| Protect cardholder data. | 3. *Protect stored data*  
| | 4. *Encrypt transmission of cardholder data and sensitive information across public networks*  
| Maintain a vulnerability management program. | 5. *Use and regularly update anti-virus software*  
| | 6. *Develop and maintain secure systems and applications*  
| Implement strong access control measures. | 7. *Restrict access to data by business need-to-know*  
| | 8. *Assign a unique ID to each person with computer access*  
| | 9. *Restrict physical access to cardholder data*  
| Regularly monitor and test networks. | 10. *Track and monitor all access to network resources and cardholder data*  
| | 11. *Regularly test security systems and processes*  
| Maintain an information security policy. | 12. *Maintain a policy that addresses information security*  

---

[protegrity](#)
<table>
<thead>
<tr>
<th>Cardholder Data</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
<th>PCI DSS Req. 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name ¹</td>
<td>Yes</td>
<td>Yes ¹</td>
<td>No</td>
</tr>
<tr>
<td>Service Code ¹</td>
<td>Yes</td>
<td>Yes ¹</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date ¹</td>
<td>Yes</td>
<td>Yes ¹</td>
<td>No</td>
</tr>
<tr>
<td>Sensitive Authentication Data ²</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe Data ³</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2/CID</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

¹ These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company’s practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

² Sensitive authentication data must not be stored after authorization (even if encrypted).

³ Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.
Requirement 3: Protect stored cardholder data

Section 3.4

- Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:
  - One-way hashes based on strong cryptography
  - Truncation
  - Index tokens and pads (pads must be securely stored)
  - Strong cryptography with associated key-management processes and procedures

- The MINIMUM account information that must be rendered unreadable is the PAN.

Notes:
- If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.
- “Strong cryptography” is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms
Requirement 3: Protect stored cardholder data

Section 3.5

“Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.

• 3.5.1 Restrict access to keys to the fewest number of custodians necessary
• 3.5.2 Store keys securely in the fewest possible locations and forms.”

Section 3.6

“Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

• 3.6.1 Generation of strong keys
• 3.6.2 Secure key distribution
• 3.6.3 Secure key storage
• 3.6.4 Periodic changing of keys
• As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically. At least annually.
• 3.6.5 Destruction of old keys
• 3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)
• 3.6.7 Prevention of unauthorized substitution of keys
• 3.6.8 Replacement of known or suspected compromised keys
• 3.6.9 Revocation of old or invalid keys
Requirement 3.6.6: Split knowledge and dual control

Split knowledge and dual control of keys requires two or three people, each knowing only their part of the key, to reconstruct the whole key.

The principle behind dual control and split knowledge is required to access the clear text key.

- Only a single master key will be needed under this control.
- The determination of any part of the key must require the collusion between at least two trusted individuals.

Any feasible method to violate this axiom means that the principles of dual control and split knowledge are not being upheld.

- At least two people are required to ‘reconstruct’ the key, and they each must have a physical thing and they each must have some information that is required.

The use of a key in memory to encipher or decipher data, or access to a key that is enciphered under another key does not require such control by PCI DSS.

- Keys appearing in the clear in memory, the principles of dual control and split knowledge are difficult but not impossible to enforce.

PCI – Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be “above and beyond” other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

When evaluating “above and beyond” for compensating controls, consider the following:

*Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

- **a)** Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).
The PCI Security Standards Council (https://www.pcisecuritystandards.org/) manages the PCI DSS standards

- End-to-end encryption is likely to be a central focus as the council seeks input on how this might best be achieved in the payment-card environment through different technologies.


- "Today we say if you're going outside the network, you need to be encrypted, but it doesn't need to be encrypted internally," PCI Security Standards Council says.

"But as an example, if you add end-to-end encryption, it might negate some requirements we have today, such as protecting data with monitoring and logging.

- Maybe you wouldn't have to do that. So we'll be looking at that in 2009."
Data Protection Approaches

Data Access Control

• How the data is presented to the end user and/or application

Data Protection

• How sensitive data is rendered unreadable
Data Protection Options

Data Stored As

- Clear – actual value is readable
- Hash – unreadable, not reversible
- Encrypted – unreadable, reversible
- Replacement value (tokens) – unreadable, reversible
- Partial encryption/replacement – unreadable, reversible
Data Protection Options

- Data in the Clear
  - Audit only
  - Masking
  - Access Control Limits

- Advantages
  - Low impact on existing applications
  - Performance
  - Time to deploy

- Considerations
  - Underlying data exposed
  - Discover breach after the fact
  - PCI aspects
Data Protection Options

Hash

- Non – reversible
- Strong protection
  - Keyed hash (HMAC)
  - Unique value if salt is used

Advantages

- None really

Considerations

- Key rotation for keyed hash
- Size and type
- Transparency
Data Protection Options

Strong Encryption

- Industry standard (NIST modes - AES CBC …)
- Highest security level

Advantages

- Widely deployed
- Compatibility
- Performance

Considerations

- Storage and type
- Transparency to applications
- Key rotation
Data Protection Options

Format Controlling Encryption

- Maintains data type, length

Advantages

- Reduces changes to downstream systems
- Storage
- Partial encryption

Considerations

- Performance
- Security and compliance
- Key rotation
- Transparency to applications
Data Protection Options

Replacement Value (i.e. tokens, alias)

- Proxy value created to replace original data
- Centrally managed, protected

Advantages

- No changes to most downstream systems
- Out of scope for compliance
- No local key rotation
- Partial replacement

Considerations

- Transparency for applications needing original data
- Availability and performance for applications needing original data
Different ‘Tokenizing’ Approaches & Topologies

123456 123456 1234

ABCDEF GHIJKL 1234

Branch Office / Stores

Home Office / HQ

Outsourced / ASP

ASP Central Tokenizer

Token & Encrypted CCN

On-site Central Tokenizer

Token & Encrypted CCN

On-site Local Tokenizer

Token & Encrypted CCN

Algorithmic Tokenizer

‘Encryption’ Algorithm

Application

Token

Network

Network
Limit Exposure across the Data Flow - Partial Encryption/Tokenizing

A policy driven approach

- Decide what sensitive bytes to protect
- A high level of transparency to applications

Some applications
  - Partial clear data

  123456 777777 1234

Few applications
  - Full clear data

Many applications/tools
  - Moving data around
How to Protect the Data Flow Against Advanced Attacks

Point Of Data Acquisition

Encrypt

Continuously protected data flow

Decrypt

Payment Authorization

Settlement & Charge-back

Unprotected sensitive information:

Protected sensitive information
Applications are Sensitive to the Data Format

- Binary (Hash) - No Applications
- Binary (Encryption) - Few Applications
- Alphanumeric (Token) - Many Applications
- Numeric (Token) - Most Applications
- Numeric (Clear Text) - All Applications

Increased intrusiveness:
- Application changes
- Limitations in functionality
- Limitations in data search
- Performance issues

This is a generalized example
Preserving the Data Format

This is a generalized example
Field Level Data Protection Methods vs. Time

- **Protection Level**
  - High
  - Medium

- **Time**

- **Strong Encryption** (AES CBC)
- **Keyed Hash** (HMAC)
- **Format Controlling Encryption** (AES FCE)
- **Plain Hash** (SHA-1 on CCN)
- **Tokenized Data**
- **Key Rotation**
Format Controlling Encryption vs. Time

- **Tokenized Data**
  - High Protection Level

- **AES FCE**
  - (numeric & IV)
  - Medium Protection Level

- **AES FCE**
  - (alphanumeric & fix IV)
  - Low Protection Level

Time
Field Level Data Protection Methods vs. Time

Protection Level

High

Tokenized Data

AES CBC (rotating IV)

AES CBC (fix IV, long data)

AES CBC (fix IV, short data)

AES ECB

Medium

Time

[Graph showing different levels of protection methods over time, including AES ECB, AES CBC with different IV rotation and fixed IV options for short and long data lengths.]
Payment card data: know your defense options
By Ulf Mattsson

http://ssrn.com/abstract=1126002
# Data Protection Options & Cost Factors

<table>
<thead>
<tr>
<th>Storage</th>
<th>Performance</th>
<th>Storage</th>
<th>Security</th>
<th>Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Format Control Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Token (reversible)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Highest 🟥 🟥 🟥 🟥 🟥 Lowest
## Data Protection Capabilities

<table>
<thead>
<tr>
<th>Storage</th>
<th>Performance</th>
<th>Storage</th>
<th>Security</th>
<th>Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>☺</td>
<td>☻</td>
<td>☺</td>
<td>☺</td>
</tr>
<tr>
<td>Strong Encryption</td>
<td>☻</td>
<td>☻</td>
<td>☺</td>
<td>☻</td>
</tr>
<tr>
<td>Format Controlling Encryption</td>
<td>☻</td>
<td>☻</td>
<td>☻</td>
<td>☻</td>
</tr>
<tr>
<td>Token</td>
<td>☺</td>
<td>☺</td>
<td>☻</td>
<td>☻</td>
</tr>
<tr>
<td>Hash</td>
<td>☻</td>
<td>☺</td>
<td>☻</td>
<td>☻</td>
</tr>
</tbody>
</table>

Highest ☺ ☻ ☻ ☻ ☻ Lowest ☻ ☻ ☻ ☻ ☻
Data Protection Implementation Choices

- Data Protection Options are not mutually exclusive

Data Protection Layers
- Application
- Database
- File System

Data Protection Topologies
- Remote services
- Local service

Data Security Management
- Central management of keys, policy and reporting
How to lock down enterprise data with infrastructure services
By Ulf Mattsson

# Data Protection Implementation Choices

## System Layer

<table>
<thead>
<tr>
<th>System Layer</th>
<th>Performance</th>
<th>Transparency</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>●</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Database</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>File System</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
</tbody>
</table>

## Topology

<table>
<thead>
<tr>
<th>Topology</th>
<th>Performance</th>
<th>Scalability</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Service</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Remote Service</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Highest ● ● ○ ○ ○ ○ Lowest ○
Column Encryption Performance - Different Topologies

Data Loading (Batch)

10,000,000 – 1,000,000 – 100,000 – 10,000 – 1,000 – 0

Encryption Topology

Rows Per Second

Data Warehouse Platforms

Mainframe Platforms

Unix Platforms

Windows Platforms

Queries (Data Warehouse & OLTP)

Network Attached Encryption (SW/HW)

Local Encryption (SW/HW)
Generalization: Encryption at Different System Layers

- **Ease of Deployment (Transparency)**
- **Separation of Duties (Security Level)**

<table>
<thead>
<tr>
<th>Layer</th>
<th>High</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File System Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Layer SAN/NAS…</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Application Transparency – Encryption, Tokens & Hashing

Transparency level

High

Database Encryption

Low

Hashing

Database Operation

Look-up

Range Search

Process Clear-values

Smart Tokens
Application Transparency

Transparency level

High

Database
File Encryption

3rd Party Database
Column Encryption

Native Database
Column Encryption

Low

Plain Hash
(SHA-2)

Key based Hash
(HMAC)

Smart Tokens

Tokens

Security Level
Business Value vs. Ease of Compliance

- Deleting Data
- Masking One-way
- Masking-Two-Way
- Clear Data

Lost Data
Re usable Data

Ease of Compliance

High

Low

Encryption
Tokenizing
Hashing
Simple Masking

Business Value

Lost Data

Reusable Data
Protecting the Data Flow: Case Studies
Data Level Attacks

MALWARE / TROJAN

DBA ATTACK

DMZ

Serve

Load Balancing

Network Devices

Enterprise Apps

DB Server

SAN, NAS, Tape

Internal Users

TRANSACTIONS

Network

Server

SQL INJECTION

SNIFFER ATTACK

MEDIA ATTACK

OS ADMIN FILE ATTACK
Securing the enterprise data flow against advanced attacks

By Ulf Mattsson

Case Studies

- **One of the most widely recognized credit and debit card brands in the world**
  - Their volume of data is in the multiple billions of rows and needed a solution that would not degrade performance.

- **Major financial institution**
  - Protecting high-worth clients financial information.
  - Central key management and separation of duties were of the utmost importance.

- **One of the world largest retailers**
  - Protecting the flow of sensitive credit card information from the store, through to back office systems and into the data warehouse and storage.
  - The central key management and ability to support thousands of stores was critical for this success.
  - Transparent to exiting applications.
  - Protect sensitive information in their Teradata data warehouse. iSeries (AS/400), zSeries (mainframe), Oracle and MS SQL Server, and to protect files that reside across platforms including Unix and z/Series.
Security for the Sensitive Data Flow

Points of collection:
- Web Apps
- Retail Locales
- Store Back Office
- Store Back Office Applications

Collection:
- Store DB

Aggregation:
- Polling Server
- Multiplexing Platform
- ERP

Operations:
- Policy

Analytics:
- Detailed Analytical
- Focused / Summary Analytical
- Tactical
- Active Access / Alerting

Archive:

Partners (Financial Institutions)
Case 1: Goal – PCI Compliance & Application Transparency

Credit Card Entry → Application → File Encryption Windows → FTP → Local Store Location (Branch) → Application → File Encryption

 FTP Encryption

Database Encryption: DB2 (zOS, iSeries), Oracle, SQL Server

Central HQ Location

File Encryption: Windows, UNIX, Linux, zOS

Financial Institution

Settlement Batch
Case 1: File Encryption & FTP

Credit Card Entry

POS Application

FTP Application

Network

File System (Memory)

Storage (Disk)

Backup (Tape)

Unprotected sensitive information: @$%^D&^YTOIuo*^ 123456 123456 1234

Protected sensitive information: @$%^D&^YTOIuo*^ 123456 123456 1234

Attacker

Attacker

Attacker

Attacker
Case 1: From Encrypted File to Encrypted Database

FTP Application

Network

File

Application

Database

File

Unprotected sensitive information:

Protected sensitive information:

123456 123456 1234

123456 123456 1234

ATTACKER

ATTACKER

@$%^D%^YTOIUO%^
Case 2a: Goal – Addressing Advanced Attacks & PCI

Credit Card Entry

Application Encryption

Application

File Encryption

Windows

Local Store Location (Branch)

Continuously encrypted computing: protection of sensitive data fields

Application

FTP

Central HQ Location

Database Encryption:
DB2
Oracle
SQL Server

File Encryption:
Windows,
UNIX,
Linux,
zOS

Decryption

Settlement FTP

Financial Institution
Case 2a: Application Encryption to Encrypted Database

Unprotected sensitive information: 123456 123456 1234

Protected sensitive information: 123456 777777 1234
Case 2b: Goal – Addressing Advanced Attacks & PCI

Continuous encrypted computing: protection of sensitive data fields

Local Store Location

Central HQ Location

Application

Database Encryption: SQL Server

Database Encryption: DB2 zOS

Credit Card Entry

FTP
Case 2b: From Encrypted Database to File & FTP

Unprotected sensitive information: ____________________________________________
Protected sensitive information: ____________________________________________

Point Of Data Acquisition

Order Application

123456 123456 1234

Database

Extraction Application

FTP Application

File

Storage (Disk)

Backup (Tape)

aVdSaH 1F4hJ5 1D3a

aVdSaH 1F4hJ5 1D3a

aVdSaH 1F4hJ5 1D3a
Case 2b: From Selectively Encrypted File to Encrypted Database

Unprotected sensitive information: 123456 123456 1234

Protected sensitive information: aVdSaH 1F4hJ5 1D3a

FTP Application

Network

File

Storage (Disk)

Backup (Tape)

Application

Database
Case 3: Goal – Addressing Advanced Attacks & PCI

Continuously encrypted computing: protection of sensitive data fields

Application

Databases

Files

Central HQ Location

Online

Financial Institution

Local Store Location (Branch)

Authorizing Transaction

Credit Card Entry

Encrypting Gateway

Decrypting Gateway
Case 3: Gateway Encryption

Unprotected sensitive information: 123456 123456 1234
Protected sensitive information: 123456 777777 1234
Continuous protection of enterprise data: a comprehensive approach
By Ulf Mattsson

How to keep sensitive data locked down across applications, databases, and files, including ETL data loading tools, FTP processes and EDI data transfers.

## Determine Risk

Data Security Risk = Data Value * Exposure

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Value</th>
<th>Exposure</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Number</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>5</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>CVV</td>
<td>5</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>Customer Name</td>
<td>3</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>Secret Formula</td>
<td>5</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Employee Name</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Employee Health Record</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Zip Code</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Enables prioritization
Groups data for potential solutions
Matching Data Protection Solutions with Risk Level

- **Low Risk (1-5)**: Monitor
- **At Risk (6-15)**: Monitor, mask, access control limits, format control, encryption
- **High Risk (16-25)**: Replacement, strong encryption
Matching Data Protection Solutions with Risk Level

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Number</td>
<td>25</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>20</td>
</tr>
<tr>
<td>CVV</td>
<td>20</td>
</tr>
<tr>
<td>Customer Name</td>
<td>12</td>
</tr>
<tr>
<td>Secret Formula</td>
<td>10</td>
</tr>
<tr>
<td>Employee Name</td>
<td>9</td>
</tr>
<tr>
<td>Employee Health Record</td>
<td>6</td>
</tr>
<tr>
<td>Zip Code</td>
<td>3</td>
</tr>
</tbody>
</table>

Select risk-adjusted solutions for costing

- Low Risk (1-5): Monitor
- At Risk (6-15): Monitor, mask, access control limits, format control encryption
- High Risk (16-25): Replacement, strong encryption
Estimate Costs

Cost = Solution Cost + Operations Cost

- Solution Cost = cost to license or develop, install and maintain
- Operations Cost = cost to change applications, impact on downstream systems, meeting SLAs, user experience
Operation Cost Factors

Performance
- Impact on operations - end users, data processing windows

Storage
- Impact on data storage requirements

Security
- How secure is the data at rest
- Impact on data access – separation of duties

Transparency
- Changes to application(s)
- Impact on supporting utilities and processes
Solution should be able to change with the environment

- Progress from less to more secure solution, or the reverse
- Add new defenses for future threats
- Plug into existing infrastructure, integrate with other systems
The Protegrity Defiance© Suite

Data Protection System (DPS)
- Encryption, monitoring, masking
- Database, file and application level

Threat Management System (TMS)
- Web application firewall

Enterprise Security Administrator
- Security policy
- Key management
- Alerting, reporting, and auditing
Protegrity Solutions

Protecting data
Protecting web applications
Managing data security
## Protegrity and PCI

| Build and maintain a secure network.                      | 1.   Install and maintain a firewall configuration to protect data   |
|                                                      | 2.   Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data.                                | 3.   Protect stored data                                             |
|                                                      | 4.   Encrypt transmission of cardholder data and sensitive information across public networks |
| Maintain a vulnerability management program.            | 5.   Use and regularly update anti-virus software                   |
|                                                      | 6.   Develop and maintain secure systems and applications            |
| Implement strong access control measures.              | 7.   Restrict access to data by business need-to-know                |
|                                                      | 8.   Assign a unique ID to each person with computer access         |
|                                                      | 9.   Restrict physical access to cardholder data                     |
| Regularly monitor and test networks.                   | 10.  Track and monitor all access to network resources and cardholder data |
|                                                      | 11.  Regularly test security systems and processes                  |
| Maintain an information security policy.                | 12.  Maintain a policy that addresses information security           |
Data Security Management

- An integral part of technical and business process

Security Policy

- Centralized control of security policy
- Consistent enforcement of protection
- Separation of duties

Reporting and Auditing

- Compliance reports
- Organization wide security event reporting
- Alerting
- Integration with SIM/SEM

Key Management
Cost Effective Data Protection

- Uses Risk as an adjusting factor for determining a Data Protection strategy
- Risk = Data Value * Exposure
- Determines solutions that fit the risk level, then determines cost
- Cost = Solution Cost + Operational Cost
- Prepare for the future
How to Protect the Data Flow Against Advanced Attacks

Point Of Data Acquisition

123456 123456 1234

Encrypt

123456 777777 1234

↓

Continuously protected data flow

Unprotected sensitive information:

Protected sensitive information

123456 777777 1234

Payment Authorization

Settlement & Charge-back

123456 123456 1234

123456 123456 1234

123456 123456 1234
How to Protect the Weak Links in your Data Flow

Review Risk & Determine Protection Approach

- Analyze the Data Flow
- Identify Assets and Assign Business Value to each
- Identify Vulnerabilities for each Asset
- Identify potential Attack Vectors & Attackers
- Assess the Risk
- Compliance Aspects
- Select Data Protection Points & Protection Methods

Assess Total Impact

- Functionality Limitations
- Performance & Scalability
- Application Transparency
- Platform Support & Development Life Cycle Support
- Key Management, Administration & Reporting
- Deployment Cost, Time & Risk
PCI and Beyond - How to Secure Data in the Most Cost Effective Manner

Ulf T. Mattsson
Protegrity Corp.

January 20, 2009

Abstract:
The Payment Card Security Industry Data Security Standard (PCI DSS), US State and federal laws encourage and require businesses to encrypt consumers' computerized personal information and payment data. Most state data breach notice laws do not require businesses to notify their customers when customers' digital personal information has been stolen or lost if the information was encrypted.

Organizations are now required to protect sensitive data, or face the wrath of public consequences - be that public disclosure to your customers or regulatory non-compliance. With growing incidents of intrusions across industries and strong regulatory requirements to secure private data, enterprises need to make DBMS security a top priority.
Data Masking – One-way vs. Two-way

- **Data Quality & Exposed Details**
  - High
  - Low

- **Development**
  - Fire Fighting
  - Two-Way Masking
  - One-Way Masking

- **Testing**
  - 3rd Party Interface Testing

- **Staging**
  - One-Way Masking

- **Production**
  - Partner Interface
  - Two-Way Masking

- **Operational**
  - Analytics

- **Information Life Cycle**

**Unprotected sensitive information:**

**Protected sensitive information:**
Meet the Experts

Ulf Mattsson

I created the initial architecture of Protegrity's database security technology, for which the company owns several patents.

Chief Technology Officer
Protegrity Corp.

I created the initial architecture of Protegrity's database security technology, for which the company owns several patents. My IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organisation, in the areas of IT architecture and IT security.
Separation of Duties (DBA)

Separation of Duties (DBA)

Yes - No

No

No

No

Yes

Index Protection

Database Column Encryption

Database Table Encryption

Database File Encryption

protegrity
The Goal: Good, Cost Effective Security

The goal is to deliver a solution that is a balance between security, cost, and impact on the current business processes and user community.

- Security plan - short term, long term, ongoing
- How much is ‘good enough’
- Security versus compliance
  - Good Security = Compliance
  - Compliance ≠ Good Security
Risk Adjusted Data Protection

- Assign value to your data
- Assess exposure
- Determine risk
- Understand which Data Protection solutions are available to you
- Estimate costs
- Choose most cost effective method
Assign Value to Your Data

Identify sensitive data
- If available, utilize data classification project
- Rank what is sensitive on its own (think PCI)
- Consider what is sensitive in combination (think Privacy)

How valuable is the data to (1) your company and (2) to a thief
- Corporate IP, Credit Card numbers, Personally Identifiable Information

Assign a numeric value: high=5, low=1
Assess Exposure

- Locate the sensitive data
  - Applications, databases, files, data transfers across internal and external networks

- Location on network
  - Segmented
  - External or partner facing application

- Access
  - How many users have access to the sensitive data?
  - Who is accessing sensitive data?
  - How much and how frequently data is being accessed?

- Assign a numeric value: high=5, low=1
Determine Risk

Data Security Risk = Data Value * Exposure

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Value</th>
<th>Exposure</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Number</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>5</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>CVV</td>
<td>5</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>Customer Name</td>
<td>3</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>Secret Formula</td>
<td>5</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Employee Name</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Employee Health Record</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Zip Code</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Enables prioritization
Groups data for potential solutions
### Example – Software Application

<table>
<thead>
<tr>
<th>Priority</th>
<th>Threat ID</th>
<th>Attack Vector</th>
<th>Requirements ID</th>
<th>Attacker</th>
<th>Time</th>
<th>Skill</th>
<th>Professional</th>
<th>HW Investment</th>
<th>No</th>
<th>Money</th>
<th>Human Resources</th>
<th>Customer Exposure</th>
<th>Vendor Exposure</th>
<th>Vendor Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>1.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>1.0, 42.0, 43.0, 44.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>2.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>2.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>3.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>2.0, 3.0, 19.0, 32.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>8</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>4.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>4.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>5.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>4.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>6.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>4.0, 1.0, 41.0, 42.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>7.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>5.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>8.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>5.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>9.0</td>
<td>Using xxx an attacker can yyy the data knowing aaa and bbb</td>
<td>6.0</td>
<td>xxx Administrator, User with yyy rights</td>
<td>8</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example - Attack by DBA

Skill & Effort Level

Programming

OS level

SQL

Data Leakage

Data Dump

Key Dump

Damage Level

Data Dump

Key Dump

Attack Vector 1

Attack Vector 2

Attack Vector 3
Data Classification by Level of Protection

- Confidential
  - Email Msgs.: A
  - Struct. Files: A
  - Access DBs: A
  - Data in Transit: E, R
  - Appl. Data: B, A
  - Central Database: E, R

- Proprietary
  - Email Msgs.: A
  - Struct. Files: A
  - Access DBs: A
  - Data in Transit: E, A
  - Appl. Data: B, A
  - Central Database: E, A

- Internal Use
  - Email Msgs.: A
  - Struct. Files: A
  - Access DBs: A
  - Data in Transit: A
  - Appl. Data: R
  - Central Database: B, A

- Customer
  - Email Msgs.: A
  - Struct. Files: A
  - Access DBs: A
  - Data in Transit: E, R
  - Appl. Data: R
  - Central Database: B, A

- Public
  - Email Msgs.: A
  - Struct. Files: A
  - Access DBs: A
  - Data in Transit: R
  - Appl. Data: B, A
  - Central Database: R

Biz Risk
- High (Red)
- Med (Yellow)
- Low (Green)

E = Encryption
R = Redundancy
B = Auto Backup
A = Access Control
<table>
<thead>
<tr>
<th>Endpoint Security</th>
<th>Network Security</th>
<th>Access Controls</th>
<th>Data Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policies</strong></td>
<td><strong>Policies</strong></td>
<td><strong>Policies</strong></td>
<td><strong>Policies</strong></td>
</tr>
<tr>
<td>70&lt;sup&gt;th&lt;/sup&gt; Percentile</td>
<td>99&lt;sup&gt;th&lt;/sup&gt;</td>
<td>80&lt;sup&gt;th&lt;/sup&gt;</td>
<td>40&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>Percentile</td>
<td>Percentile</td>
<td>Percentile</td>
</tr>
<tr>
<td><strong>Enforcement</strong></td>
<td><strong>Enforcement</strong></td>
<td><strong>Enforcement</strong></td>
<td><strong>Enforcement</strong></td>
</tr>
<tr>
<td>80&lt;sup&gt;th&lt;/sup&gt; Percentile</td>
<td>90&lt;sup&gt;th&lt;/sup&gt;</td>
<td>50&lt;sup&gt;th&lt;/sup&gt;</td>
<td>30&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>Percentile</td>
<td>Percentile</td>
<td>Percentile</td>
</tr>
<tr>
<td><strong>Practices</strong></td>
<td><strong>Practices</strong></td>
<td><strong>Practices</strong></td>
<td><strong>Practices</strong></td>
</tr>
<tr>
<td>40&lt;sup&gt;th&lt;/sup&gt; Percentile</td>
<td>95&lt;sup&gt;th&lt;/sup&gt;</td>
<td>50&lt;sup&gt;th&lt;/sup&gt;</td>
<td>10&lt;sup&gt;th&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>Percentile</td>
<td>Percentile</td>
<td>Percentile</td>
</tr>
</tbody>
</table>

Gap Analysis: Regulations - Policies - Enforcement - Practice

Regulations

- Gap #1

Written Policies

- Gap #2

Enforcement

- Gap #3

Security Practices
Security Documentation Review / Analysis

Security Documentation Overall

- Policy Completeness: Below Avg.
- Policy Enforceability: Average
- Policy Awareness: Above Avg.
- Organization issues
- Punishment specs
- Very good in IT
- Security architect?
- Excellent
- Not in most docs
- Reviewed few apps
- Being upgraded

Security Architecture
Network Security
Storage Security
Application Security
Database Security
## Control Effectiveness Rating

<table>
<thead>
<tr>
<th>Effectiveness</th>
<th>Strong</th>
<th>Mixed</th>
<th>Weak</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Control</th>
<th>DB access control</th>
<th>Externally facing</th>
<th>Internally facing</th>
<th>Awareness of control</th>
<th>Compliance with control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate data center</td>
<td>![Green]</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td>![Red]</td>
<td></td>
</tr>
<tr>
<td>Division data centers</td>
<td>![Green]</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td>![Red]</td>
<td></td>
</tr>
<tr>
<td>Regional offices</td>
<td>![Green]</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td>![Red]</td>
<td></td>
</tr>
<tr>
<td>Home offices</td>
<td>![Yellow]</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td>![Yellow]</td>
<td></td>
</tr>
<tr>
<td>Remote users</td>
<td>![Yellow]</td>
<td>![Green]</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td></td>
</tr>
<tr>
<td>Service providers</td>
<td>![Yellow]</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td>![Yellow]</td>
<td></td>
</tr>
<tr>
<td>Resellers</td>
<td>![Yellow]</td>
<td>![Red]</td>
<td>![Red]</td>
<td>![Red]</td>
<td></td>
</tr>
</tbody>
</table>

*Effectiveness ratings cover the use of the control across multiple organizations and applications in the enterprise*

*Effectiveness ratings are also applied to service providers who handle sensitive data on behalf of the enterprise*
DATA SECURITY BEST PRACTICES STUDY -- RESTRICTED ACCESS -- DO NOT DISTRIBUTE

This interview is being conducted as part of a study of data security best practices. The study is being conducted for the organization Information Security organization by Protegity. EVERYTHING YOU SAY IS COVERED BY A VERY STRICT NON-DISCLOSURE AGREEMENT. We want your detailed feedback about the handling of sensitive data within your organization at organization. This feedback will be used to help organization improve its data protection policies and procedures. Please feel free to share your experiences and feelings. YOU WILL NEVER BE IDENTIFIED TO ANYONE ELSE WITHIN organization AT ANY TIME.

<table>
<thead>
<tr>
<th>OVERVIEW</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  What types of confidential business data do you handle as part of your job?</td>
<td></td>
</tr>
<tr>
<td>2  What are the procedures you have to follow when you handle confidential information?</td>
<td></td>
</tr>
<tr>
<td>3  What security policies affect how you handle this information?</td>
<td></td>
</tr>
<tr>
<td>4  How do you keep track of changes to the security policies and procedures?</td>
<td></td>
</tr>
<tr>
<td>5  Who is responsible for monitoring and enforcing these policies and procedures?</td>
<td></td>
</tr>
</tbody>
</table>

FILL IN THE FOLLOWING BEFORE THE INTERVIEW

| a   | Date of the interview: |          |
| b   | Name of the enterprise: | organization International |
| c   | Name of the interviewee: | First Name | Last Name |
| d   | Phone # of the Interviewee: |          |
| e   | Email address of the Interviewee: |          |
| f   | Name of Interviewer |          |
Organization data security vulnerability points under study:
1. Endpoint security / desktop security / wireless security
2. Customer access to Organization via Web Applications
3. Web application development and access controls
4. Global bulk file transfer to/from member institutions
5. Corporate network infrastructure, including firewalls, IDS/IPS
6. XxxNet/YyyNet global infrastructure
7. Application-to-database access controls
8. Database management controls, including separation of duties
9. Key management systems
10. Customer premises HW/SW data protection (the XXX)
11. Protection of stored data in SAN, NAS and backup tapes
Questions?

If you would like a copy of the slides, please email ulf.mattsson@protegrity.com
Organizations are now required to protect sensitive data, or face the wrath of public consequences - be that public disclosure to your customers or regulatory non-compliance. With growing incidents of intrusions across industries and strong regulatory requirements to secure private data, enterprises need to make DBMS security a top priority.
A practical implementation of transparent encryption and separation of duties in enterprise databases: protection against external and internal attacks on databases
Mattsson, U.T.
Volume , Issue , 19-22 July 2005 Page(s): 559 - 565
Digital Object Identifier 10.1109/CECT.2005.9

Summary: Security is becoming one of the most urgent challenges in database research and industry, and there has also been increasing interest in the problem of building accurate data mining models over aggregate data, while protecting privacy at the level of individual records. Instead of building walls around servers or hard drives, a protective layer of encryption is provided around specific sensitive data items or objects. This prevents outside attacks as well as infiltration from within the server itself. This also allows the security administrator to define which data stored in databases are sensitive and thereby focusing the protection only on the sensitive data, which in turn minimizes the delays or burdens on the system that may occur from other bulk encryption methods. Encryption can provide strong security for data at rest, but developing a database encryption strategy must take many factors into consideration. We present column-level database encryption as the only solution that is capable of protecting against external and internal threats, and at the same time meeting all regulatory requirements. We use the key concepts of security dictionary, type transparent cryptography and propose solutions on how to transparently store and search encrypted database fields. Different stored data encryption strategies are outlined, so you can decide the best practice for each situation, and each individual field in your database, to handle different security and operating requirements. Application code and database schemas are sensitive to changes in the data type and data length, the paper presents a policy driven solution that allows transparent data level encryption that does not change the data field type or length.
### PCI 3.1 Keep cardholder data storage to a minimum.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.</td>
<td>Obtain and examine the company policies and procedures for data retention and disposal, and perform the following:</td>
</tr>
<tr>
<td></td>
<td>• Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons)</td>
</tr>
<tr>
<td></td>
<td>• Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data</td>
</tr>
<tr>
<td></td>
<td>• Verify that policies and procedures include coverage for all storage of cardholder data</td>
</tr>
<tr>
<td></td>
<td>• Verify that policies and procedures include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for a review, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements</td>
</tr>
</tbody>
</table>
PCI 3.2 Do not store sensitive authentication data

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.2</strong> Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:</td>
<td><strong>3.2</strong> If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps:</td>
</tr>
<tr>
<td><strong>3.2.1</strong> Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. <em>Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</em> - The cardholder’s name, - Primary account number (PAN), - Expiration date, and - Service code <em>To minimize risk, store only these data elements as needed for business.</em> <em>Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</em></td>
<td><strong>3.2.1</strong> For a sample of system components, examine the following and verify that the full contents of any track from the magnetic stripe on the back of a card are not stored under any circumstance: - Incoming transaction data - All logs (for example, transaction, history, debugging, error) - History files - Trace files - Several database schemas - Database contents</td>
</tr>
</tbody>
</table>
## PCI 3.3 Mask PAN when displayed

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
</tr>
</thead>
</table>
| **3.2.2** Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.  
   *Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.* | **3.2.2** For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:  
   - Incoming transaction data  
   - All logs (for example, transaction, history, debugging, error)  
   - History files  
   - Trace files  
   - Several database schemas  
   - Database contents |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block. | **3.2.3** For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:  
   - Incoming transaction data  
   - All logs (for example, transaction, history, debugging, error)  
   - History files  
   - Trace files  
   - Several database schemas  
   - Database contents |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).  
   *Notes:*  
   - This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.  
   - This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts. | **3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN. |
### PCI DSS Requirements

**3.4** Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:
- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

The MINIMUM account information that must be rendered unreadable is the PAN.

**Notes:**
- If for some reason, a company is unable to render the PAN unreadable, refer to Appendix B: Compensating Controls.
- “Strong cryptography” is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.

### Testing Procedures

**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods:
- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads, with the pads being securely stored
- Strong cryptography, with associated key-management processes and procedures

**3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).

**3.4.c** Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.

**3.4.d** Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.

**3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must

**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).

**3.4.1.b** Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).
## PCI 3.5 Protect cryptographic keys

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
</tr>
</thead>
</table>
| not be tied to user accounts. | 3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. 
  Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately. |

### 3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:

<table>
<thead>
<tr>
<th></th>
<th>Testing Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.</td>
<td>3.5.1 Examine user access lists to verify that access to keys is restricted to very few custodians.</td>
</tr>
<tr>
<td>3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.</td>
<td>3.5.2 Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Testing Procedures</th>
</tr>
</thead>
</table>
| 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: | 3.6.a Verify the existence of key-management procedures for keys used for encryption of cardholder data. 
  Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at [http://csrc.nist.gov](http://csrc.nist.gov). |
|                  | 3.6.b For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer’s keys (used to transmit data between customer and service provider). |
|                  | 3.6.c Examine the key-management procedures and perform the following: |

#### 3.6.1 Generation of strong cryptographic keys

| 3.6.1 Verify that key-management procedures are implemented to require the generation of strong keys. |

#### 3.6.2 Secure cryptographic key distribution

| 3.6.2 Verify that key-management procedures are implemented to require secure key distribution. |

#### 3.6.3 Secure cryptographic key storage

| 3.6.3 Verify that key-management procedures are implemented to require secure key storage. |
PCI 3.6 Fully document and implement all key-management processes and procedures

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
</tr>
</thead>
</table>
| 3.6.4 Periodic cryptographic key changes  
  ▪ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically  
  ▪ At least annually | 3.6.4 Verify that key-management procedures are implemented to require periodic key changes at least annually. |
| 3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys | 3.6.5.a Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).  
  3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys. |
| 3.6.6 Split knowledge and establishment of dual control of cryptographic keys | 3.6.6 Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key). |
| 3.6.7 Prevention of unauthorized substitution of cryptographic keys | 3.6.7 Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys. |
| 3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities | 3.6.8 Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities. |
Online Exposure²

- Insider incidences were much larger in terms of the amount of data compromised.
- Hacking and malware proved to be the attack method of choice among cybercriminals, targeting the application layer and data more than the operating system.
- The type of asset compromised most frequently (82%) is without doubt online data.
  - Compromises to online data repositories were seen in more cases than all other asset classes combined by a ratio of nearly five to one.
  - Offline data, networks, and end-user devices were all closely grouped.

Cloud Services

Why aren't enterprises falling all over themselves to buy and use cloud services? Is it risk aversion? Is it a lack of confidence in the service providers? Is it just another version of the insource/outsource debate? Or is it something else more fundamental as discussed at http://www.internetevolution.com/document.asp?doc_id=170782&image_number=1

Cloud-Related Issues That Have IT Pros Concerned

- Security: 53%
- Performance: 33%
- Control: 31%
- Vendor lock-in: 30%
- Support: 25%
- Configurability: 18%
- Speed to activate new services or expand capacity: 17%

% indicating they're very concerned about these issues

Data: InformationWeek Analytics Cloud Computing Survey of 172 business technology professionals considering or using cloud services
What is The PCI Knowledge Base?

Industry-specific Best Practice Partners (e.g., NRF, NACS)

Over 300 Hours of 100% Anonymous Interviews with PCI Experts

Panel of PCI Experts who Answer Questions in our Discussion Forums

Content Sponsors (IT and payment vendors) fund our research

Weekly Webinar series on PCI, PA-DSS, security & compliance

PCI Solutions: Catalog of options, linked to our research findings

Reports and Subscription Services on Compliance Trends and Opportunities

Education products and services “powered by the PCI KB,” with Partners

Source: PCI Knowledge Base, March 2009
Based on Over 300 Hours of 100% Anonymous Interviews – Not a Survey

Interviews with merchants focus on best practices, experiences, QSA and vendor feedback, budgets and priorities.

- F1000 Retailers
- SME Retailers
- QSAs
- Payment Processors
- Banks
- Retail Consultants
- IT Providers
- E-Comm Retailers
- Hospitality
- Other Merchants

Interviews with QSAs, consultants and providers focused on vulnerabilities, risk and technology adoption trends.

Source: PCI Knowledge Base, January 2023
Over 90% of Retail Security Breaches Due to SW POS or Shopping Cart

- **Software POS**: 71%
- **Shopping Cart**: 21%
- **Backend SW**: 6%
- **Hardware**: 2%

Check to be sure all your service providers are currently PCI compliant, because it will reduce the risk of a security breach.

Source: Verifone, 2008
Show Common Brick & Mortar and E-Commerce Security Vulnerabilities

- CR Tampering
- Installed Skimmers
- Cameras
- Shared Passwords

- Outdated Wireless Encryption (WEP)

- Network Access
- SQL Injection

- Eavesdropping on restaurant or corporate networks

- Unencrypted Network Access
- Chargeback Risk

- POS Terminals

- Restaurant Servers

- Restaurant Web Site

- Franchisee Web Site

- Corporate Network

- Host Servers

- Merchant Acquirers

- Card Issuers

- Payment Terminals

- PIN Pad Tampering
- Handheld Skimmers
- Social Engineering
- Unsecure Apps

- Credit Card Data
- MSR Track Data
- TLog Files
- Reports Data
- Password Guessing

- Weak Access Control
- Firewalls “Open”
- AV Not Up-to-Date
- Log files Disabled
- Poor Key Management

- Not Updated Network IDS / IPS
- Unsecured Ports

- Unencrypted Network Access
- Chargeback Risk

Source: Adapted from Verifone, 2008
PCI is Not Just About POS – It’s Affected the Entire Company, and More

Business policies and procedures for handling CC data

IT Infrastructure of the “Cardholder Environment”

Configuration of these Apps

PIN Entry Devices must be PCI PED compliant

Payment Apps must be PA-DSS compliant (if packaged) or PCI-DSS compliant (if customized)

must be PCI-DSS compliant

must be PCI-DSS compliant

must be PCI-DSS compliant

Running fully compliant apps does not make the whole company compliant.

The “new standards” are PA-DSS and PCI PED. Most firms do not yet comply with them.

The “multi-level” process makes “outsourcing PCI” a complex proposition.

Source: PCI Knowledge Base, March 2023
Implement Enterprise Key Management for Needed Confidential Data

Current vs Potential Use of Enterprise Key Mgmt

Larger retailers have already made major efforts to reduce the number of confidential data repositories, in DBs, in Apps, and in the ability to download confidential data to PCs.

Best Practice Description

- **Implement a centralized, automated management process for encryption keys, particularly if the encryption keys are native to each application, OS, or DB. This is the best way to effectively meet the split knowledge and key rotation requirements of PCI without major outages.**

  **Level of Investment**
  $25,000 – 125,000, or more, for enterprise key management.

  **Potential Savings**
  $50,000 – 200,000 if implemented after a QSA finds a problem and recommends a different tool.

  **Best for**
  F1000 retailers who have data to encrypt across multiple systems where the data is handed off.

  **Primary Dept Owner**
  IT Infrastructure

  **PCI Reqmts Met**
  3.6

Source: PCI Knowledge Base, January 2009

---

![Image](image)
Upgrade Access Controls To Secure Virtualized Servers

Current vs Potential Use of Secure, Virtualized Servers

Server virtualization is saving money in the data center, but deployment in the cardholder environment has been limited, as tracking access to confidential data requires IDS/IPS, and access control upgrades.

<table>
<thead>
<tr>
<th>Best Practice Description</th>
<th>F1000</th>
<th>SME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that as you implement server and desktop virtualization in the cardholder environment and for other servers with confidential data that intrusion and access controls have been upgraded to enable tracking of individual access to confidential data.</td>
<td>99%</td>
<td>99%</td>
</tr>
<tr>
<td>Level of Investment</td>
<td>$10K – $40K, for security controls upgrades, but this increases as more servers protected increases.</td>
<td>45%</td>
</tr>
<tr>
<td>Potential Savings</td>
<td>$10K – $50K, primarily on manual tracking, monitoring, but some savings on PCI audit, through better reporting tools.</td>
<td>5%</td>
</tr>
<tr>
<td>Best for</td>
<td>Larger companies.</td>
<td>20%</td>
</tr>
<tr>
<td>Primary Dept Owner</td>
<td>IT Infrastructure and application</td>
<td>5%</td>
</tr>
<tr>
<td>PCI Reqmts Met</td>
<td>2.2.1</td>
<td>22.1</td>
</tr>
</tbody>
</table>

Source: PCI Knowledge Base, March 2022
Tokenization: Reduce Scope via Data Centralization & Outsourcing

BUYER 1
(Virtual) POS

BUYER 2
Shopping Cart

BUYER 3
Call Center

GL / AR / AP
Sales Audit
Loss Prevention

FRONT OFFICE APPLICATIONS

BACK OFFICE APPLICATIONS

“Real” Data

Secure Data Storage, Mgmt & Retrieval

“Fake” Data

PAYMENT PROCESSING

ISO / Processor
Payment Gateway
Acquiring Bank

Source: PCI Knowledge Base, March
Since June 2008, our interview data has shown a major shift in how merchants, payment processors and PCI assessors view tokenization. Beyond just understanding and embracing the technology for card data, companies are viewing it as a strategy for reducing risk to all types of confidential data.

Source: PCI Knowledge Base, March 2009
Most ERP vendors use 3rd party payment SW to avoid having their apps in scope for PA-DSS.

**Modularized ERP Application**

<table>
<thead>
<tr>
<th>Financial &amp; Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materials Management</td>
</tr>
<tr>
<td>Production Planning</td>
</tr>
<tr>
<td>Order Entry</td>
</tr>
<tr>
<td>Purchasing</td>
</tr>
<tr>
<td>Financial Control</td>
</tr>
<tr>
<td>Distribution/Logistics</td>
</tr>
<tr>
<td>Asset Management</td>
</tr>
</tbody>
</table>

**E-Commerce Module**

<table>
<thead>
<tr>
<th>Change Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Management</td>
</tr>
<tr>
<td>Modularized Application</td>
</tr>
<tr>
<td>E-Comm Module</td>
</tr>
<tr>
<td>Payment Module</td>
</tr>
<tr>
<td>Key Management</td>
</tr>
</tbody>
</table>

**E-Comm and payment vendors usually have no problems with change control and security testing, but key management and log management are issues.**

Vendors affected: Payment providers to SAP, Oracle Apps, Infor Global, Sage, Microsoft Dynamics, Lawson, Epicor, QAD

Source: PCI Knowledge Base, November 2021
Best Practice: Segment Network Against Downloaded Malware

Key controls to improve security and reduce PCI compliance costs: Internal firewalls to segment your in-store and home office network.

POS Devices

POS Controller Under Counter

Back Office POS Controller

Internal Firewall

Office PC (Web Browsing)

External Firewall

File Sharing w/ Malware

Internet

BotNet Attackers

Any systems that collect, process or store card data, or any systems that are connected to those systems must meet all 12 PCI controls.

Source: PCI Knowledge Base, November 2008
Automate Log Management and Integrate with SIM Analytics

Current vs Potential Use of automated log mgmt

For those restaurateurs that are not outsourcing the review of their logs (which is most larger restaurateurs), the need to automate the log review and add analytics is critical. This remains one of the weakest PCI security controls in terms of actually using the data.

Best Practice Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Investment</th>
<th>Potential Savings</th>
<th>Best for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a centralized log management and analysis process. Replace manual log reviews with automated tools. SIM tools can be justified based on improved visibility and responsiveness to potential security breaches. Include logs from both the wired and the wireless environments.</td>
<td>$10,000 – 25,000 for projects, depending on size &amp; complexity</td>
<td>$20,000 – 200,000 in reduced assessment costs and security control cost avoidance costs.</td>
<td>F1000 restaurateurs who cannot segment networks and have call data throughout the enterprise.</td>
</tr>
<tr>
<td>Primary Dept Owner</td>
<td>Network management, with support from IT Infrastructure.</td>
<td>1, 10, 11</td>
<td>Source: PCI Knowledge Base, March 2009</td>
</tr>
</tbody>
</table>
Where is the PCI Knowledge Base (www.KnowPCI.com)?

We're a PCI Research Community. The website launched in April 2008.

We've conducted 320+ hours of anonymous interviews and have 2000+ members.

Search our database of over 3000 comments by merchants, PCI assessors, banks, card processors and many more.

Ask questions of peers and assessors in our free PCI Discussion Forums.

Latest PCI News Feeds.

We host a weekly PCI Research Webinar Series.

The "Knowledge Base" is our proprietary research database.

Purchase our latest research reports & trend analysis.

Panel of 95 PCI experts.

Supporting Adverts like Google.