23c3 Security in the cardholder data processing?!

Manuel Atug and Thilo W. Pannen
SRC Security Research & Consulting GmbH, Bonn, Germany, sdpais@src-gmbh.de

Experiences and lessons learned with the Payment Card Industry Data Security Standard (PCI DSS)

MasterCard and Visa have jointly released the PCI Data Security Standard defining security requirements for the processing of card data. The aim of the programmes is the protection of sensitive cardholder data to foster the trust of customers, merchants and their service providers in the payment systems and to limit probability of cardholder data compromises.

SRC is an auditor approved by MasterCard and Visa to carry out PCI Security Scans and PCI Security Audits. Currently, SRC serves about 3000 merchants and 40 payment service providers around Germany, Austria, France, Russia, Ukraine, Slovakia, Greece, Israel and others.

The structure of this paper is as follows: first, this paper will introduce the PCI security requirements. Then, the company's experiences of several hundred security scans and dozens of security audits will be highlighted. Finally, an outlook of the developments will be given.

1 Introduction

In view of the rising fraud in card payments, the payment schemes MasterCard International and Visa International have initiated the programmes **MasterCard Site Data Protection (SDP)** and **Visa Account Information Security (AIS)** in order to improve the security of card data processing and storage in card processing payment systems.

The programmes are targeting members, merchants and service providers that store, process or transmit cardholder data. They have to comply without exception to the Payment Card Industry Data Security Standard (PCI DSS) which defines the technical and organisational requirements of the payment schemes. This standard is also endorsed by the card associations American Express, Diners Club, JCB and Discover.

Entities that are not able to demonstrate compliance with the PCI DSS (which can be regarded as the state-of-the-art) at the time of a compromise will face indemnity for losses.

The average losses incurred per card misused fraudulently range between 2.000 EUR and 3.000 EUR. Also, a fee between 5 EUR and 15 EUR may be charged for each card that has to be reissued. There could also be additional fees by the payment systems for investigation, litigation and incident handling for the compromise.

Another significant and probably greater risk of a compromise is the loss of reputation and confidence of consumers.

As we have seen from various compromises, businesses also go bust. The probably “best” known example is Card Systems Solutions, a company that died after a compromise.

The PCI DSS consists of the following documents:

- PCI Data Security Standard,
- PCI DSS Self-Assessment Questionnaire,
- PCI DSS Security Scanning Procedures,
- PCI DSS Security Audit Procedures,

according to MasterCard and Visa. The latest version 1.1 was introduced in September 2006 and is available at https://www.pcisecuritystandards.org/.

Depending on the number of transactions per year, a merchant or service provider will have to validate his compliance by means of a Self-Assessment, Security Scan(s) and/or a Security Audit performed by approved auditors (Qualified Security Assessors resp. Approved Scanning Vendors).

MasterCard and Visa coercively enforced the implementation of the program SDP resp. AIS according to the PCI Standards until **June 30th 2005**.

2 The PCI Data Security Standard

The PCI Data Security Standard comprises a set of tools to ensure the safe handling of sensitive cardholder information. First, the sensitive data in payments is described, then the PCI Data Security Standard and its components are presented in the following.

2.1 Definition of sensitive cardholder data

The standard ISO/IEC 7813 "*Information technology - Identification cards - Financial transaction cards*" issued by the ISO (International Organization for Standardization, see http://www.iso.org), defines the structure and data content of financial transaction cards, among which there are the sensitive data items which have to be protected according to the PCI DSS.

The next figure shows the example of the Track 2 magnetic stripe contents according to the ISO standard. Character codes are based on a 5 bit modified ASCII format, the length of track 2 can be up to 40 numeric digits.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
S T X	PAN																				S E P	EXP			SVC			PVV					DD (incl. CVV)						E T X

Figure 1: Track 2 data according to ISO 7813

STX:	Start Sentinel (";")	PVV:	PIN Verification Value
PAN:	Primary Account Number	DD:	Discretionary Data including Card Verification Value (CVV)
SEP:	Separator ("=")	ETX:	End Sentinel ("?")
EXP:	Expiration Date		
SVC:	Service Code		

2.1.1 Format of Track 2

Primary Account Number (PAN)

The Primary Account Number (PAN) comprises a six-digit Issuer Identification Number (IIN), a variable length (maximum 12 digits) individual account number and a check digit which is computed by means of the the Luhn formula (Mod-10). The PAN comprises at the utmost 19 digits.

Cardholder Name

The cardholder's name can be 2 to 26 characters including surname, surname separator, first name or initial space when required, middle name or initial period (when followed by title), title (when used).

Service Code

The service code is a numeric field with three sub-fields represented by individual digits. It is used to indicate the issuer's acceptance criteria for magnetic stripe transactions and whether a related integrated circuit supporting the equivalent application as identified by the magnetic stripe or embossing is present on the card.

Expiration Date

The expiration date comes in the YYMM format, where YY represents the last two digits of the year and MM is the numeric representation of the month.

PVV

The PIN Verification Value (PVV) is a data item that the cardholder possesses for verification of identity. It does NOT contain the PIN in clear text, but is computed using cryptography and verified by the card issuer during authorisation of a transaction. According to the ISO standard, the PVV is regarded as a part of the discretionary data.

2.1.2 CVC2/CVV2

The three digit Card Validation Code 2 (CVC2, MasterCard) or Card Verification Value 2 (CVV2, Visa) is printed on the card's signature panel and shall be used for card-not-present transactions like Mail-Order/Phone-Order (MOTO) or e-commerce transactions. Presentation of the CVC2 and CVV2 should help the merchant to verify that the customer has the actual card at hands during a card-not-present transaction. This data is not stored anywhere else on the card.

For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic.

2.2 PCI DSS requirements and components

The PCI DSS requires any entity to protect cardholder data by a set of organisational and technical measures.

The standard applies to all systems and applications that store, process or transmit cardholder data like servers, firewalls, routers, wireless access points, network appliances and other security appliances.

While it is not allowed to store CVC2/CVV2, PVV or full magnetic stripe data after authorisation of a transaction under any circumstances, a merchant or service provider may store the PAN, the cardholder name, the service code and the expiration date.

Whenever such data is stored, it has to be rendered unreadable by one of the following measures:

- one way hashing of cardholder data (e.g. SHA, MD5, RIPEMD),
- substitution of cardholder data by pseudo-number computed by index tokens and PADs,
- truncation or masking of the cardholder data like 1234 56xx xxxx 7890
- encryption of cardholder data with strong and public methods (3DES, RSA1024, AES-256).

(A masked PAN which contains only the first six and last four digits in clear text at the utmost is **not** regarded as sensitive data.)

The PCI DSS contains twelve requirements grouped under six headlines, which are:

1. Build and Maintain a Secure Network
    - Requirement 1: Install and maintain a firewall configuration to protect data
    - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data
    - Requirement 3: Protect stored data
    - Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks
3. Maintain a Vulnerability Management Programme
    - Requirement 5: Use and regularly update anti-virus software
    - Requirement 6: Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
    - Requirement 7: Restrict access to data by business need-to-know
    - Requirement 8: Assign a unique ID to each person with computer access

- Requirement 9: Restrict physical access to cardholder data

5. Regularly Monitor and Test Networks
   - Requirement 10: Track and monitor all access to network resources and cardholder data
   - Requirement 11: Regularly test security systems and processes
6. Maintain an Information Security Policy
   - Requirement 12: Maintain a policy that addresses information security

This standard details technical requirements for the secure storage, processing and transmission of cardholder data.

2.2.1 PCI Self-Assessment Questionnaire

The PCI Self-Assessment Questionnaire comprises 74 yes/no questions and has to be filled in by merchants or service providers depending on their classification.

The purpose of the PCI Self-Assessment Questionnaire is to validate the compliance of the entity with the PCI DSS.

2.2.2 PCI Security Scan

To demonstrate compliance with the PCI DSS, merchants and service providers are required to have quarterly PCI Security Scans conducted as defined by each payment scheme’s security programme. PCI Security Scans are scans conducted over the Internet and have to be performed by an Approved Scanning Vendor in compliance with the requirements of „PCI DSS Security Scanning Procedures 1.1“.

The purpose of the PCI Security Scan (off-site vulnerability scan) is to uncover well-known security flaws in the architecture and the configuration of the system analysed which can be exploited to access components of the firewall system, server systems or the internal network.

These scans have to be conducted “non-intrusive” and “non-destructive” so that the production systems are not affected. Therefore, finger-printing techniques are most commonly employed.

The result of a scan is a detailed report which describes the type of vulnerability or risk, a diagnosis of the associated issues, and a guidance on how to fix the vulnerabilities identified.

The report also categorises the vulnerabilities identified in the scan process into five level ranging from “low” to “urgent”.

The PCI DSS does not accept vulnerabilities of level three to five, which would allow an attacker to gain full access to cardholder data or compromise the system.

2.2.3 PCI Security Audit

PCI Security Audits are conducted by a Qualified Security Assessor in accordance with the requirements of „PCI DSS Security Audit Procedures 1.1“.

Service providers or large merchants that are required to undergo an annual onsite review, must validate compliance on all applications and systems where cardholder data is stored, processed, or transmitted.

The audit consists of a review of documents (policies and procedures) and a site inspection during which samples are taken. Also the auditor interviews selected personnel to scrutinise the implementation of the technical and organisational measures required by PCI DSS.

3 Top Ten security issues within the PCI Security Scan

The top ten list of security issues provided in this chapter is based on the performance of security scans of several thousand IP addresses.

It has to be noted that these vulnerabilities are classified as critical, i.e. a merchant or service provider will fail to pass the security scan and to prove compliance with the requirements.

Please note that this top ten list is a subset of all vulnerabilities deemed as critical.

3.1 SSL server has SSLv2 enabled

There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular web-servers, mail-servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.

3.2 SSL server supports weak encryption

SSL encryption ciphers are classified based on encryption key length as follows:

- HIGH - key length larger than 128 bits
- MEDIUM - key length equal to 128 bits
- LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security.

3.3 OpenSSH local SCP shell command execution

SCP is a secure copy application that is a part of OpenSSH. It is used to copy files from one computer to another over an encrypted SSH connection. If SCP is given all-local paths to copy, it acts like the system "cp" command.

OpenSSH is susceptible to a local SCP shell command execution vulnerability. This issue is due to a failure of the application to properly sanitise user-supplied input prior to utilising it in a "`system()`" function call.

If SCP is used in an all-local fashion, without any hostnames, it utilises the "`system()`" function to execute a local copy operation. By utilising the "`system()`" function, a shell is spawned to process the arguments. If filenames are created that contain shell metacharacters, they will be processed by the shell during the "`system()`" function call. Attackers can create files with names that contain shell metacharacters along with commands to be executed. If a local user then utilises SCP to copy these files (likely during bulk copy operations involving wildcards), then the attacker-supplied commands will be executed with the privileges of the user running SCP.

3.4 Windows TCP/IP remote code execution and Denial of Service (MS05-019)

Microsoft Security Update MS05-019 was not installed. This update resolves different security issues, e.g. IP Validation Vulnerability, ICMP Connection Reset Vulnerability, ICMP Path MTU Vulnerability, TCP Connection Reset Vulnerability and Spoofed Connection Request Vulnerability.

3.5 Web server vulnerable to cross-site scripting attacks

The Web server does not filter script embedding from links displayed on a server's Web site.

A malicious user can exploit this vulnerability to cause JavaScript commands or embedded scripts to be executed by any user who clicks on the hyperlink. Upon clicking the hyperlink, the Web server will generate an error message including the specified or embedded script. The specified or embedded script is executed in the client's browser and treated as content originating from the target server returning the error message (even though the scripting may have originated from another site entirely).

3.6 Management Interfaces accessible on Cisco device

This vulnerability applies to Cisco devices which use protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be publicly accessed, and are an invitation for malicious users to break in.

3.7 Cisco IOS HTTP configuration arbitrary administrative access

Cisco IOS contains a vulnerability that makes it possible for remote users to gain level 15 privileges (the enable level, the most privileged level) on an affected Cisco device.

By sending a crafted URL, it's possible to bypass authentication and execute any command on the device. This will only happen if the user is using a local database for authentication (usernames and passwords are defined on the device itself). The same URL will not be effective against every Cisco IOS software release and hardware combination. However, there are only a few different combinations to try, so it would be easy for an attacker to test them all in a short period of time.

3.8 Session-Fixation social engineered session hijacking

This vulnerability affects a Web application that uses cookies (e.g. session IDs) in an insecure way. Specifically, the security scanner created a web session with the target using a session ID specified by the scanner itself. The target application simply started a new session with this specified session ID. This issue is generally called "session-fixation" and is vulnerable to session-hijacking attacks.

3.9 Web server uses plain-text form based authentication

The Web server uses plain-text form based authentication. An attacker could easily gain access to the unprotected authentication data (login and password) by usage of sniffing techniques.

3.10 Mail server accepts plaintext credentials

The Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to authenticate and identify the user. Optionally, it also negotiates a security layer for subsequent protocol interactions.

The server accepts PLAIN or LOGIN as one of the AUTH parameters. The authentication credentials are transmitted in plaintext over the network and no encryption is performed.

4 Top ten security issues within the PCI Security Audit

The following top ten list is compiled by SRC auditors using their experiences during the preparation and execution of PCI security audits at customers.

4.1 Key Management

The key management processes of the PCI DSS require to protect the complete lifecycle of a cryptographic key, beginning at the generation, through distribution, storage, periodic change until key destruction.

Also, the four-eyes principle has to be put in place to prevent a „single point of failure“, i.e. no single person could gain access to a key.

The experience of SRC shows that none or only parts of the PCI key management processes and policies are in place when starting the audit. Also, entities do either not fully understand the requirements, e.g. how to check for newly generated, weak keys, or do not know how to put organisational and technical measures in place (like four-eyes principle).

4.2 Design of network and access control

PCI requires to limit the potential access to critical applications to a minimum. Therefore servers have to be separated by firewalls, VLANs or routers from the company network to reduce the risk of a compromise.

It is common to have only a single, company-wide network which allows to connect to every server from the LAN e.g. from (public) meeting room to central host. This issue can be addressed by a re-segmentation of the LAN and restriction of access rules.

4.3 Security maintenance

PCI requires that all systems, system components and software have the latest vendor-supplied security patches installed. The relevant patches have to be installed within 30 days.

SRC found that maintenance very often follows the “never change a running system” approach, which exposes the systems to very high risks. Sometimes the process of patching a system is not convenient for a merchant or service provider, and requires to re-boot systems or switch into a single-user mode.

This hesitation to update is very often accompanied by the lack of proper testing facilities (also required by PCI).

4.4 Firewall misconfiguration

PCI requires to use firewalls between Internet and DMZ and internal network zones. Also the firewall rules have to employ a “deny-all” policy. The firewall may grant access only to those protocols, ports and IP ranges that are required by business needs.
SRC found many exceptions from these principles like:

- rule set is not up to date, old rules were not eliminated;
- no “deny all” rule included;
- unnecessary protocols were able to pass into the DMZ (P2P, IRC, IDENT);

Very often, there is not a current network diagram available.

4.5 Misuse of cardholder data

PCI does not allow to use live card data for development or testing purposes. This is, unfortunately, very often the case, though the payment systems provide test cards on request.

4.6 Access to cardholder data not limited

PCI requires to limit access to cardholder data only to those whose job requires such access. This principle is not fully enforced and many exceptions were found during the audits. The reasons are manifold, sometimes the “I’m the boss and therefore need access to everything” syndrome can be observed, in other cases the access rules have grown historically and were not shrunk-to-fit.

4.7 Physical access

PCI requires to physically protect access to cardholder data or to systems which store, process or transmit cardholder data. Therefore system components have to be physically protected by data centre like measures (e.g. CCTV, visitor’s badges and logbook). Also physical access to these components has to be restricted. This is not limited to electronic media (e.g. hard disks, backup tapes, CD) but also includes access to cardholder data printed on paper.

The disposal of any media has to be secured by purging (military wiping), degaussing, incineration, pulping or cross-cut shredding.

Very often, these processes are not or only partly implemented according to PCI requirements. Examples are: racks in data centres were not locked, no secured paper disposal, network jacks in the sensitive areas were accessible. Also cardholder data is only deleted from hard disk, though they have to be securely wiped.

4.8 Internal security scan and penetration tests

PCI requires to carry out internal security scans and penetration tests of sensitive applications and systems, in addition to (external) security scans conducted by approved scanning vendors.

SRC found that either the tests are not carried out at all or, if they are carried out, they often do not comply with PCI requirements.

4.9 Intrusion detection and file integrity

PCI requires to use intrusion detection systems (IDS) and file integrity monitoring applications. The experience of SRC shows that most merchants and service providers were not familiar with those systems and therefore did not use them at all.

4.10 Organisational policies and procedures

PCI requires not only to implement organisational and technical measures, but also to develop and maintain written policies and procedures.

Examples are: information security policy, password policy, daily operational security procedures, hiring/leaving policies, incident response plan.

SRC found that in large companies these policies are mainly common and put alive, but are not subject to a regular review once implemented. On the other side, small companies employ policies required which are not documented.

5 Summary and Outlook

The PCI Data Security requirements are based on common sense and industry best practice. It is derived from the ISO 17799 (ISO 2700x) information security management standard and customised to the needs of the payment industry.

Though one could have expected that most of the PCI DSS requirements are already put in place for vested interests, the experience and reality reveals a different picture.

The payment industry is pushing all entities that store, process or transmit cardholder data to validate compliance with the PCI DSS. It seems to be a matter of time until the first entity is stopped from accepting or processing card data because of non-compliance.

The consolidation in the payment market happening today is driven by the need for investments in security measures and the increase in security requirements as the payment systems are constantly monitoring and tracking the attacks that take place day by day. They reserve the right to quickly react to security incidents by raising the security bar.

For all these reasons it becomes less attractive for merchants to store, process or transmit cardholder data on own systems, unless there is a strong business need. SRC observes that many merchants, especially small ones with, let’s say, less than 100.000 transactions per year and brand, are increasingly outsourcing transaction processing to service providers.

This development is beneficial to the payment market as the risks of a compromise are reduced. Cards will only be used by customers if they are fully confident in the payment systems.

Merchants will accept payment cards only if the costs of acceptance are low.

PCI DSS seems to be an effective tool to maintain the confidence of consumers and merchants in card payments which is also underpinned by the experiences of SRC.

It is likely that the PCI DSS will be amended in near future by a so-called “payment application best practices” programme which will require a certification for payment applications. By that, software vendors will be included into the programmes and will be mandated to develop software with regard to PCI DSS.