Retour d'expérience PCI DSS

Frédéric Charpentier

xmco | Partners

XMCO PARTNERS : Who are we ?

- Xmco Partners is a **consulting** company specialized in **IT security** and **advisory**
- Xmco Partners is **independent** : the company is owned by its founders
- Our customers are Banks, Telecoms operators, Insurances and Governmental institutions
- The company is composed of 10 consultants working in a "**project mode**".

XMCO PARTNERS : Consulting and Advisory services

Penetration tests – Ethical hacking

In-depth penetration tests performed by true security experts
Network and Application level

Security audits ISO 27002 and PCI DSS

Technical and organizational assessment.
Remediation, follow-up and certification process

Vulnerability watch

Dedicated vulnerability alerts, support and solutions.

Intrusion response and Forensics

Specialists of Intrusion Detection, logs correlation and forensics analysis

AGENDA

- **PCI DSS in a nutshell**
- My experiences
- Vocabulary
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- Liability issues
- Conflict of interests

PCI DSS in a nutshell

- Being PCI compliant means that your **acquirer bank** agrees that your e-business platform handles customer **credit cards** with maximum care.

- To prove that to your bank, an organism named **PCI Council** have write 224 mandatory controls, organized into 12 main requirements.

- The e-business company must comply with theses requirements, perform a certification assessment and sent a **Report on Compliance** to the acquirer bank.

- If the bank accept the Report on Compliance, depending of the accuracy of the delivered documentation, the platform PCI compliant **for one year**, until the next assessment.

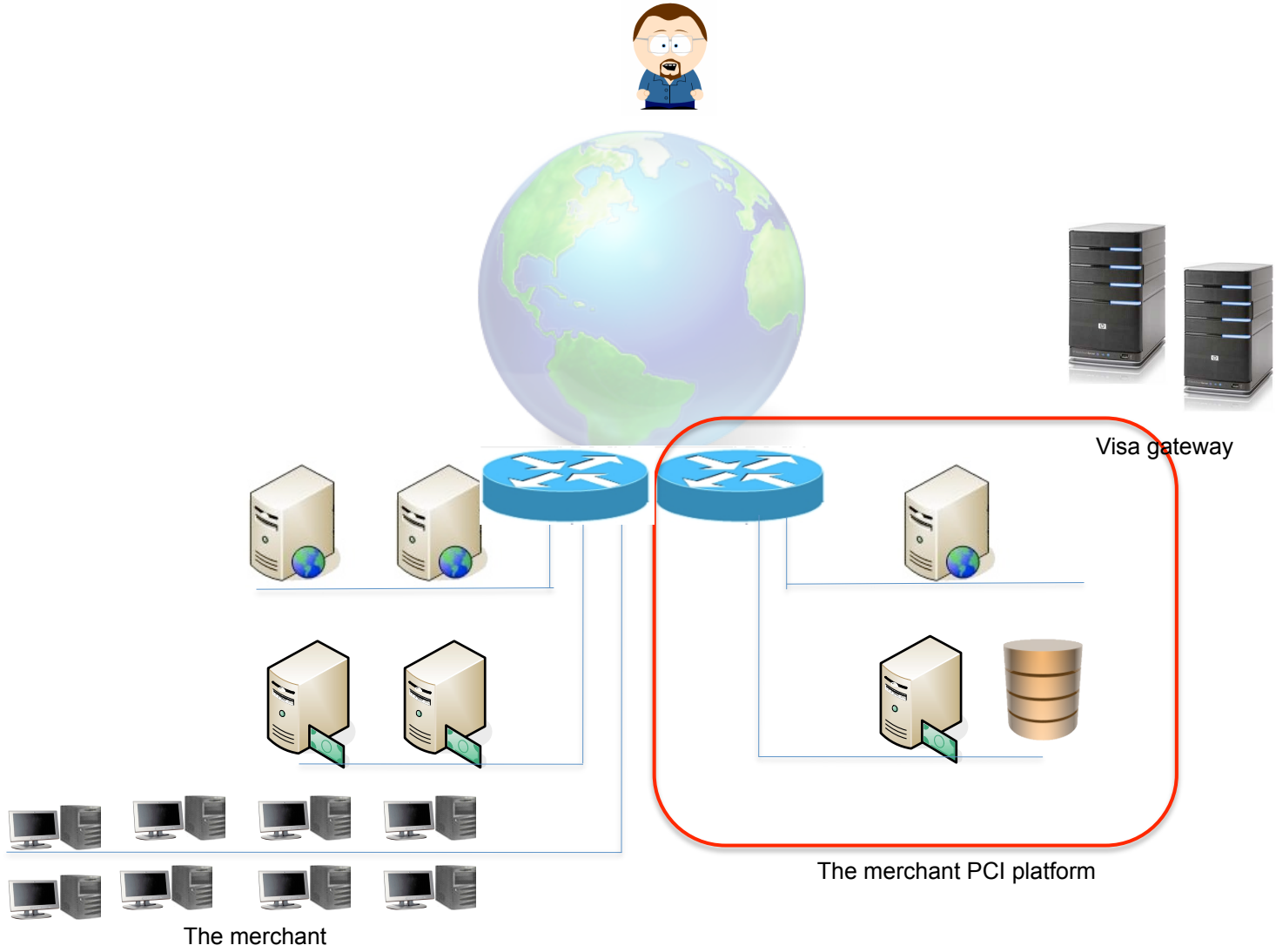
PCI DSS in a nutshell : the card path

The merchant

Visa gateway

xmco | Partners

PCI DSS in a nutshell : isolate the PCI devices



AGENDA

- PCI DSS in a nutshell
- **My experiences**
- Vocabulary
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- Liability issues
- Conflict of interests

My experiences

- An IT system with prepaid card for vehicle renting, refillable with a Visa from Internet.

  For a private company / a city services provider

- A B2C/B2B website selling "pay-n-go" insurance contracts over Internet

  For a insurance company

- A website is used to sell tickets while physical card reader devices are used to identify the customer regarding its visa's card number.

  For a train company

AGENDA

- PCI DSS in a nutshell
- My experiences
- **Vocabulary**
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- Liability issues
- Conflict of interests

PCI Vocabulary

- A **CDH device** is any system or network equipment which receive/transmit/process/store credit data of your customers, like the Primary Account Number (PAN)

- An **Acquirer** is bankcard association member – most often your credit card processing partner bank, that initiates and maintains relationships with merchants that accept payment cards

- A **Merchant** is defined as a location or store where purchases are made. The merchant is responsible for the security of the credit card information regardless of who they pass off the information to, such as a service provider.

  PCI Level 1 : Merchants processing over 6 million Visa transactions annually. Certification : Clean ASV scan, filled RoC by a QSA

  PCI Level 2 : Merchants processing between 1 to 6 Visa transactions annually. Certification : Clean ASV scan, filled SAQ

- A **Service Provider** is defined as an entity that handles credit card information on behalf of a merchant, acquirer, issuer, processor, or other service provider.

  PCI Level 1: "VisaNet processors or any service provider that stores, processes and / or transmits over 300,000 transactions per year"
  Certification : Attestation of Compliance Form, filled by a QSA

  PCI Level 2 : "Any service provider that stores, processes and / or transmits less than 300,000 transactions per year"
  Certification : Level 2 service providers will submit version D of the Self-Assessment Questionnaire (SAQ), , filled by a QSA

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- **Roadmap to the compliancy**
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- Liability issues
- Conflict of interests

ROADMAP TO THE COMPLIANCY

Step 1 : Read the PCI 1.2 document to understand the controls

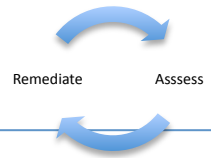
Step 2 : Scope of Assessment for Compliance

Step 3 : Get in touch with the PCI representative of your acquirer and define your auditor

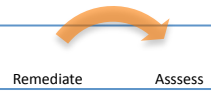
Step 4 : Inventory all CDH devices, softwares, accounts, IP, URLs of the PCI scope

Step 5 : Perform an in-depth penetration tests and remediate all flaws

Step 6 : Perform a Gap-Analysis PCI assessment with and remediate



Step 7 : Compliance audit : submit ROC or SAQ to your acquirer



Step 8 : Stay compliant with quaterly “clean” vulnerability scans and annual assessment

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- Roadmap to the compliancy
- **Key points**
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- Liability issues
- Conflict of interests

PCI DSS : Key points

- Do not store CDH or have a legitimate business reason to store CDH
- Apply firewall Best Practices
- Implement SSL everywhere credit card are transmitted over the public network
- Apply security fixes
- Apply OS security Best Practices no default password, nominative account (no root access), strong passwords and authentication, session timeout …
- Perform regular "human" penetration tests and follow OWASP Secure Coding
- Get a quarterly clean Automated Vulnerability Scans
- Get accurate logs, Intrusion Detection, WebApp firewall
- Write a security policy and a security awareness program signed by all impacted people

The 12 PCI requirements

12 main requirements, detailled into 224 controls

- ✓ Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- ✓ Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- ✓ Requirement 3: Protect stored cardholder data
- ✓ Requirement 4: Encrypt transmission of cardholder data across open, public networks
- ✓ Requirement 5: Use and regularly update anti-virus software or programs
- ✓ Requirement 6: Develop and maintain secure systems and applications
- ✓ Requirement 7: Restrict access to cardholder 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.
- ✓ Requirement 10: Track and monitor all access to network resources and cardholder data.
- ✓ Requirement 11: Regularly test security systems and processes.
- ✓ Requirement 12: Maintain a policy that addresses information security for employees and contractors.

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- Roadmap to the compliancy
- Key points
- **Common difficulties or mistakes**
- Credit card numbers retention
- Complex points
- Liability issues
- Conflict of interests

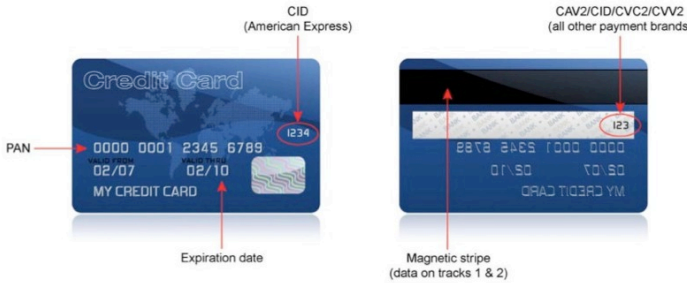
Common difficulties or mistakes

- A excessively large PCI scope
- The vendors pressure and their disinformation
- Misinterpretation of one or multiple requirements
- Starting a compliancy audit to soon without any self-assessment
- The PCI project is drive by the CSO instead of the board

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- **Credit card numbers retention**
- Complex points
- Liability issues
- Conflict of interests

CDH data protections rules



The following rules must be strictly applied on the PCI platform and its software:

- **The storage of the PIN code, CVV2, the Magnetic stripe data is prohibited.**
- **Never stored the PAN without a legitimate business reason**
  The CDH data must never appear clear text in temporary files, logs files, SQL databases…Use strong cryptography if storage is needed, prefers one-way hashing if possible
- **Erase CDH data from system memory as soon as possible**
  Programs must use free() functions and memory garbage collector as soon as the CDH are sent to the payment gateway.
- **Mask PAN when displayed**
  Except when the user fills the payment form. The PAN must never be redisplayed by the application to the user even when the payment is refused for errors or technical problems.
- **Never send unencrypted PAN by e-mail even for debugging**

CDH data protections rules

<u>If your business is bound to store</u> CDH data, PCI Requirement n°3 must be applied :

- Limit retention time
- Do not store the CVV2 or the PIN
- Mask the PAN when re-displayed through back-office application
- Render PAN, at minimum, unreadable anywhere it is stored (backup, logs...)
- Use encryption
  - column-level database encryption
  - disk encryption : the encryption key must not be linked to the native operating system access control mechanism
- Protect cryptographic keys

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- **Complex points**
- Liability issues
- Conflict of interests

PCI DSS : Complex points

PCI 11.2 : Quarterly ASV scans : stupid false-positives

For instance : "Web Server Predictable Session ID Vulnerability (QID:86310)"

Sample :

```
#1: Set-Cookie: F5-POOL=1208658112.20480.0000
#2: Set-Cookie: F5-POOL=1208658112.20480.0000
#3: Set-Cookie: F5-POOL=1208658112.20480.0000
```

PCI 11.4 : Network IDS : efficiency with HTTPS ?

PCI 6.6 : Web Application Firewall : is a new appliance mandatory ?

PCI 6.6 : For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by **either** of the following methods:

1 - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.

2 - Installing a web-application firewall in front of public-facing web applications

PCI 8.3 : Two-factor authentication : is SecurID are mandatory ?

PCI 8.3 Incorporate two-factor authentication for **remote access** (network-level access originating from outside the network) to the network by employees, administrators, and third parties.

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- **Liability issues**
- Conflict of interests

Liability issues

The mandatory Insurance covers :

CRIME/FIDELITY BOND including employee dishonesty, robbery, fraud, theft, forgery, alteration, mysterious disappearance and destruction. The minimum limit shall be $1,000,000 each loss and annual aggregate.

TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer or information technology Services, or from data damage/destruction/corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service and loss of income from network security failures in connection with the Services provided under this Agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate

Security Assessor shall maintain such insurance for **five** (5) years after the termination of this agreement

PCI SSC shall be named as an **additional insured** under the Commercial General Liability **for any claims** and losses arising out of, allegedly arising out of or in any way connected to the Security Assessor's performance of the Services under this agreement

Security Assessor agrees that it shall ensure that the Workers' Compensation/Employer's Liability insurers agree **to waive** subrogation rights, **in favor of PCI SSC**, for any claims arising out of or in any way connected to Security Assessor's performance of the Services under this Agreement

AGENDA

- PCI DSS in a nutshell
- My experiences
- Vocabulary
- Roadmap to the compliancy
- Key points
- Common difficulties or mistakes
- Credit card numbers retention
- Complex points
- Liability issues
- **Conflict of interests**

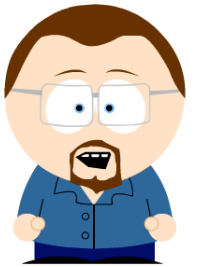
Conflict of interests

I want to be compliant and I pay for it

I want to be ethical

I want to win more project with this customer

I have a liability



Merchant

Auditor QSA

Conflict of interests

I am a customer

If you don't accept my RoC I can use another provider

I am responsible of the control

I want to keep my customer who made more than 6 millions transactions

Merchant

Acquirer (Bank)

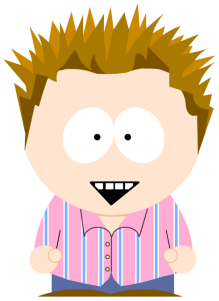
Conflict of interests

I want to be compliant

Merchant

I want to have customers for my hosting services

My company is also QSA



Hosting Provider also QSA

Documents

- The PCI DSS version 1.2

  https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

- PCI Data Storage Do’s and Don’ts

  https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

- Ten Common Myths of PCI DSS

  https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

fcharpentier@xmcopartners.com