Volume : 1, Issue : 1
January - June 2011

ISSN : 2229 - 3515

Authors personal coppy

international journal of ADVANCES IN SOFT COMPUTING TECHNOLOGY

Editor-in-Chief
Dr.Vaka Murali Mohan

Published by
BHAVANA RESEARCH CENTER

© 2011 BRC

Tokenization for improving Payment Card Industry Data Security Standard

Surekha.T [1]* and Siva Ram Prasad.R [2]

1.Krishnaveni Engineering College for Women, Narsaraopet, Guntur(Dt), A.P INDIA

2.Acharya Nagarjuna University, Namburu, Guntur(Dt), A.P INDIA

Key Words:
Tokenization, PCI DSS, PCI Compliance, Data Security

Abstract: *Tokenization for improving Payment Card Industry Data Security Standard (PCIDSS) is presented in this paper. The main objective of this study is to evaluate how the adoption of a security Standard can impact the network design and the security infrastructure. The entire Dominican Market is facing the experience of getting PCI DSS Compliance. Tokenization issues i.e: security standards adoption, object replacement, character replacement, masking and randomizers are explained in detailed. Requirements for PCI DSS establishment, materials, procedure, analysis and recommendations are also explained in detailed.*

1. Introduction:

Now a days outsourcing of payment processing has become a popular option. PCI compliance- the security measures mandated by the Payment Card Industry of any transmits sensitive credit card information. The PCI DSS (Data Security Standard) is a set of 12 requirements that merchants must adhere to, or risk some hefty fines and penalties. PCI compliance is not a quick and easy standard to reach. The reason for this should be obvious: the data that you are responsible for protecting is sensitive in the extreme and anything less than the strongest possible protection will result in breaches, loss of data, and loss of reputation. Several experts did several experiments in this lines some of them are Robert Kidd [1] presented the penalties ranging from fines to the ultimate sanction of issuers removing the right to accept cards, organizations across every vertical market are now aware of the business risk linked to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS). Vanesa Gil Laredo [2] reported the number of people using credit or debit cards for payments, with organizations. Paul Meadow croft [3] presented the data security breaches when the subject made the headlines regularly throughout the year.

* ***Prof. T. Surekha***
Vice Principal and Head, Dept. of CSE
Krishnaveni Engineering College for Women,
Kesanupalli (V), Narasaraopet (M),
Guntur (Dt, AP, INDIA
Ph. No.: 91-9290823257
E-mail: tsurekha1234@yahoo.co.in

Anton A. Chuvakin and Branden R. Williams [4] presented the PCI DSS compliance. Hsinchun Chen and Andrea L. Houston [5] focused on digital libraries, starting with a discussion of the historical visionaries, definitions, driving forces and enabling technologies and some key research issues and describe some of the emerging techniques for building large-scale digital libraries, including a discussion of semantic interoperability, the "Grand Challenge" of digital library research. Michael Owen et al [6] discussed the applicability of the standard's requirements to more generic corporate security practices. Luther Martin [7] discussed the ongoing battle between security vendors over encryption versus tokenization often focuses on issues that are largely irrelevant. A closer look at the two technologies shows that the strengths and weaknesses of both are actually very similar. The problem with outsourcing payment processing lies in the fact that you have now greatly increased the number of electronic transmissions that must be made. And a hacker could attempt to interrupt, intercept, divert, or otherwise manipulate those transmissions.

To overcome this problem a new technology was adopted that is called tokenization. With this method everyone can safely transfer their data without falling into the wrong hands. Tokenization is an affordable option to reach PCI compliance because it can generally be integrated with minimum interruptions or changes to the company's. Tokenization works as, if a person accepts a payment card or the associated sensitive information from a customer. This process can be applied to retail outlets or in card-not-present transactions. The customer's information is sent to the service providers - the company providing the tokenization or payment processing - who, in turn, provide a randomly generated, totally unique ID number and return it to the person. Now, with this number - or token - in place, it

is the only information that a person needs to store on-site. This number is all they need to access customer records; conduct multiple transactions, or even institute recurring billing procedures. The most obvious benefit from this is that, with nothing but a list of randomized 16-digit numbers on your own system, there is nothing of value for a thief to take. Even if they managed to intercept a token in transmission, decrypted the signals and everything, there is, in truth, nothing for them to do with the numbers. Methods like tokenization become a great way to reach PCI compliance because of the responsibility shift to a company that is prepared to spend the time and resources to protect card holder data. Guarding this information is a constant battle, and the only way to ensure its safety is through perpetual vigilance. Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information without compromising its security. Tokenization has become popular as a means of bolstering the security of credit card and e-commerce transactions while minimizing the cost and complexity of compliance with industry standards and government regulations. Tokenization allows information to be reformatted in a fashion that renders it useless to outsiders -- thus reducing the risk of unauthorized access to, or breaches of, the information -- while still allowing organizations, their business partners and their underlying applications to use this sensitive information to process transactions in a format they expect, with little modification to business workflows.

When an application receives tokenized data it needs to process, there are two choices: It can either have the tokenization algorithms added to its code to reverse the process or, more commonly, contact a secured corporate token server that tokenizes information on a large scale and maintains the original information values; no key management required. In this case the application sends predetermined tokenized data elements through secure communications channels to the token server and receives the original information in return. While encryption may seem like it takes a similar level of effort, when comparing the workflow of a number of systems that pass sensitive data to the number of systems that must process this data, one finds that tokenization is much more efficient.

2. Tokenization also provides a number of ways to protect information. These include:

* Object replacement: This is a direct replacement of some or all of the data in the data set with similar data types (usually from tables), i.e. given name, surname, street name, city, state, etc. so the name 'Joe' might become 'John' and 'Smith' becomes 'Jones.'

* Character replacement: This is a replacement of some or all of the data in the data set using known reversible algorithms, i.e. primary account number (PAN), CCV, etc.

*** Masking:** This is the replacement of some or all of the data in the data set with a single character. For example: 5009 9087 8793 5642 (original credit card number); xxxx xxxx xxxx 5642 (masked credit card number). The details of the card are shown in figure1.

*** Randomizers:** This is the replacement of some or all of the data in the data set with ranges of similar data types, i.e. "increase exp. date month between 2-6 months" or "modify birth date year by decreasing between 10-15 years."

Instead of using production data in development or testing environments, tokenization protections can be used to rapidly create unique production data that simulates production data sets but has been modified to protect the sensitive information. This not only reduces the level of security required to protect non-production environments, but it also eliminates the risk of insider loss of sensitive information from these systems. But, as mentioned in the last paragraph, the rules used shouldn't invalidate testing the processing of information. For example, tokenizing a "state" value may invalidate your test workflow if the maximum credit interest charged varies by state. An example of tokenized production data to similar test data is shown below.

	Production Data	Test Data
Given Name	James	Bob
Surname	Smith	Jones
Acnt #	5009 9087 8793 5642	4567 8903 2890 4598
Exp Date	3/11	12/12
CCV2	567	342
Birth date	3/12/78	3/12/67

3.Tokenization issues:

Security standards adoption So why isn't tokenization more widespread? The main issue with tokenization is security standards adoption. For example, the current version of the Payment Card Industry Data Security Standard (PCI DSS) only formally recognizes encryption technologies for protecting credit card transactions. While the Security Standards Council (SSC) for PCI DSS has recognized the value of tokenization -- and is studying its

capabilities -- it has yet to put it in the PCI DSS as an acceptable substitution for encryption. This means that organizations that must comply with PCI DSS, and similar standards requiring the protection of information in storage or transit, must look at the value of tokenization and whether it increases the security of their processing and storage architectures.

The objective of this case study is to evaluate how the adoption of a security Standard can impact the network design and the security infrastructure. The entire Dominican Market is facing the experience of getting PCI DSS Compliance. If decide not to be compliant with the standard they can be fined and eventually lose the right to do business with card brands. The Security Standard Council and the brands themselves are pushing hard to get everybody to be in compliant status. The current Case study is related to PCI DSS and this standard covers different areas such as policies design, security approach, network architecture, software Design, application security, transmission encryption requirements and so on. This work will be focused only in the network designing activities and changes and the security schema for applications. Of course, if this activities are related to cards or cardholder environment, because PCI DSS it's only applicable to those cases.

PCI DSS is a Security Standard details in a card are shown in figure1. Its objective is to protect cardholder data. Its requirements should be applied on any system, server and/or network containing this type of data. Cardholder data includes: PAN: Principal Account Number or Card Number, Cardholder Name, Card Expiration Date, Service Code, Sensitive Authentication Data: Full magnetic stripe data, CAV2/CVC2/CVV2/CID1 and PINs/PIN blocks. "The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS2. If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply (PCI Security Standards Council LLC, ". The vast majority of financial institutions (or any institution affected by the standard) do not possess a whole infrastructure or resources exclusively dedicated to handle card transactions and cardholders' data thus in most cases

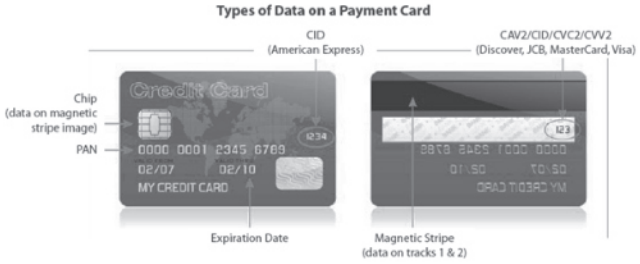

Figure 1. Payment card industry data security standards

not to say in all of them, PCI DSS requirements will affect the entire technological infrastructure and organization; that is the reason why this standard supposes such a big impact on the institutions willing to comply with it.

4. PCI DSS establishes the following twelve requirements:

Build and Maintain a Secure Network

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.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

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

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

But, how such common sense directives can be so difficult to achieve? Some of the problems come with the sizes of the companies and the comprehension of the standard as well. Sometimes, misconception of the requirements leads to major difficulties on implementations. The PCI network is shown in figure 2.

PCI Limitations:

* The fastest way to reduce the scope of a PCI gap assessment is to eliminate the storage, processing and transmission of cardholder data on as many systems as possible.
* The following methods can be used to reduce PCI scope with some limitations:
  *Remove the PAN.
  *Truncate the PAN, leaving only the first 6 and last 4 digits.
  * One-Way Hash the PAN.

*Tokenize the PAN.

* The following limitations apply to the methods above:
  *Although a system may not store the PAN, it may still process or transmit it and is therefore still in-scope.
  *Systems that receive PAN before it's truncated, hashed/ tokenized/ that do the actual truncation, hashing or tokenization are still in-scope.
  *Systems that don't store transmit or process cardholder data, but are directly connected to the cardholder environment are still in-scope.

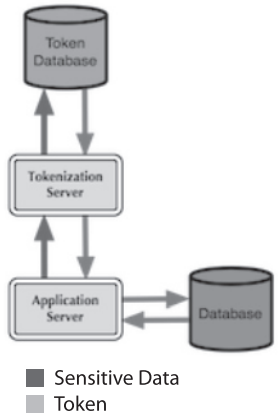

Fig.2. Tokenization Architecture

5. Materials, Procedure and Analysis:

The information presented on the following report was gathered by performing interviews with people working in the technology and security areas. Names of the participants of the interviews had been hidden for confidentiality purposes. During those interviews questions regarding to the design of the network and the original infrastructure diagrams from a couple of years ago were made. There was a recompilation of existent documentation to know which things were already implemented and established regarding documentation requirements. Tests3 on the field were also performed to validate the truthfulness of the information provided by the interviewed personnel.

Materials:

Networking Administrators Level 1
and Level 24
Security Administrators Level 1 and
Level 2
Application Developers
System Users
Policies
Network diagrams
Configuration procedures
Application development documentation
PCI DSS project complete documentation
Configuration Files

Procedure:

Review Network Designs and configuration files.
Discuss information with personnel of the networking and security areas.
Execute activities to prove the affirmations of participants.
Policies revision and discussion with affected users. PCI DSS requirements and Security Assessment is shown in figure 3.

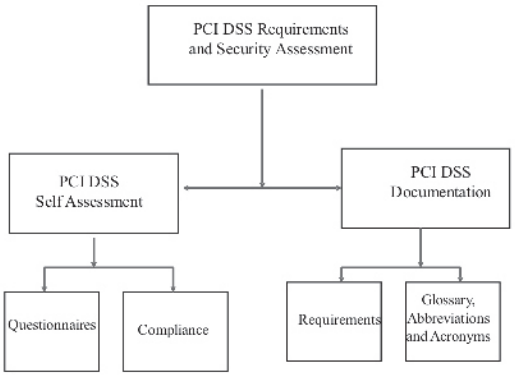

Figure 3. PCI DSS Procedure

Analysis:

A process took place in which all retrieved network diagrams were evaluated against the real configurations of the network in order to determine the veracity if evolution of the network presented in the set of diagrams. This analysis was made considering selected PCI DSS Requirements that are directly related to network designing and security.

In the following Section there is a discussion of what was found. This is an attempt to examine and in some cases question those changes thinking of PCI DSS requirements. The current status of the network will be presented in the last diagram to evaluate the network status towards achieving PCI DSS compliance. Starting from upper left corner the server farm can be seen connected to a core switch where all users were also connected. Different network segments separate users and servers. The access control between them was implemented at the application and databases level. There was neither a firewall implementation to protect servers from user access or an Intrusion Prevention System (IPS) to analyze traffic flowing between them. Implementation of Intrusion Prevention Systems is not only a good security practice but also part of PCI DSS requirements.

In front of the core switch there was an IPS to monitor traffic going in and out the most internal part of the network containing servers and users inside. This IPS seems to be strategically located to inspect every packet going to and coming from those internal segments, but the truth is that the proxy server they had to control

Internet navigation was connected straight to the Internet. The traffic going to Internet from any of the segments behind the IPS went directly to the content switch H3 not passing through the IPS before leaving or entering the internal segments in that part of the network thus not being monitored. So traffic entering the network was being analyzed in that point anyhow IPSs analyze traffic based on policies, signatures and traffic patterns learned and configured through a period of tuning and customization for the intended traffic they will be monitoring. Thus the policies you have on one IPS might not be effective monitoring certain type of traffic. In this case, the internal traffic was being analyzed by Internet IPSs and this could be highly ineffective monitoring.

Web and VPN Servers were behind the firewall it looks like any traffic from the Internet had to go through the firewall to access them and databases serving web applications were separated on a DMZ. Even though H3 and H4 had an interface connected directly to the segment of web servers. If any of them was compromised there was an open entry to that segment that was supposedly protected by the firewall.

6. Results and Recommendations:

Generally security has three important stages: Policy creation: to regulate the correct use of resources Infrastructure implementation: to ensure the policies are being followed Alertness: to evaluate how effective the implementation. Also, consider whether the new changes are necessary to improve security. It can be affirmed that PCI DSS also considers those stages. The standard is not only about implementing solutions for security, data loss prevention antivirus or encryption, just to name a few. It is also about documenting those implementations as well as creating policies and making users aware. They should create a configuration norm for routers and communication equipments configuration norm. Methods of enforcing the application of the norm should be created. There should be a correction on the updates and patches policy:

To make it extensive to the whole system components

To establish the minimum timeframe in which the updates must be applied.

To include a structured procedure to audit the updates activities.

Production, Test and Development environments should be isolated. In case the correction involves long-term activities this should be planned, projected and start to be executed in the minor time possible.

7. Conclusions:

Tokenization for improving Payment Card Industry Data Security Standard is presented in this paper. The main objective of this study is to evaluate how the adoption of a security Standard can impact the network design and the security infrastructure. The entire Dominican Market is facing the experience of getting PCI DSS Compliance. Tokenization issues i.e: security standards adoption, object replacement, character replacement, masking and randomizers are explained in detailed. Requirements for PCI DSS establishment, materials, procedure, analysis and recommendations are also explained in detailed.

8. References:

1. Robert Kidd "Counting the cost of non-compliance with PCI DSS" Computer Fraud & Security, Vol. 2008, Issue 11, Nov 2008, pp 13-14.
2. Vanesa Gil Laredo "PCI DSS compliance: a matter of strategy" Card Technology Today, Vol. 20, Issue 4, April 2008, Page 9.
3. Paul Meadowcroft "Card fraud will PCI-DSS have the desired impact" Card Technology Today, Vol. 20, Issue 3, March 2008, pp 10-11.
4. Anton A. Chuvakin and Branden R. Williams "About PCI" Book, Chapter1, PCI Compliance (Second Edition), Understand and Implement Effective PCI Data Security Standard Compliance, 2010, Pages 1-7.
5. Hsinchun Chen and Andrea L. Houston "Digital Libraries: Social Issues and Technological Advances" Advances in Computers, Vol. 48, 1999, pp 257-314.
6. Michael Owen., senior consultant and Colin Dixon "A new baseline for cardholder security" Network Security, Vol. 2007, Issue 6, June 2007, pp 8-12.
7. Luther Martin "Protecting credit card information: encryption vs tokenization" Network Security, Vol. 2010, Issue 6, June 2010, pp 17-19.