# Security Assessment of Payment Systems under PCI DSS Incompatibilities

Şerif Bahtiyar, Gürkan Gür, Levent Altay



# Security Assessment of Payment Systems Under PCI DSS Incompatibilities

Şerif Bahtiyar, Gürkan Gür, and Levent Altay

Provus - A MasterCard Company
Progress R&D Center, Ayazaga, 34396, Istanbul, TR
{serif.bahtiyar, gurkan.gur, levent.altay}@provus.com.tr

**Abstract.** With the ubiquitous proliferation of electronic payment systems, data and application security has become more critical for financial operations. The Payment Card Industry Data Security Standard (PCI DSS) has been developed by the payment industry to provide a widely-applicable and definitive security compliance among all components in electronic payment infrastructure. However, the security impact of PCI DSS incompatibilities and relevant security assessment approaches for such cases are yet to be investigated in a comprehensive manner. Therefore, in this paper we present a security assessment framework for payment systems under PCI DSS incompatibilities. Moreover, we analyze a case study to evaluate our proposal and to provide some guidelines to security experts for assessment of PCI DSS compliance.

**Keywords:** Payment system security, Security assessment, PCI DSS, Risk analysis, Data and applications security

## 1 Introduction

Electronic payments have been the driver of instant and ubiquitous economic transactions particularly for the last two decades. Moreover, sector statistics indicate that cash and check payments are declining while electronic payment methods are gradually taking over [1, 2]. Therefore, this profound trend of electronic payment proliferation has brought forth an inevitable consequence regarding security: the reliance of this infrastructure on information and computing systems with data and application security becoming more critical for financial operations. The payment related data such as the confidential data of payers and transactional records stored and transmitted in these systems are subject to various attacks and security threats. Taking these matters into consideration, the Payment Card Industry Data Security Standard (PCI DSS) has been developed by the payment industry to facilitate a widely-applicable and definitive security compliance for electronic payment infrastructure [3–5].

PCI DSS defines the essential *requirements* serving some determined *objectives* and mainly focusing on the most valuable asset in a payment system: cardholder data (CHD). It has been growing in volume and coverage since its inception with additional guidelines and best practices published by PCI Security

Standards Council (SSC). However, the security impact of PCI DSS incompatibilities and security assessment approaches considering the system context are yet to be investigated in a comprehensive manner. Although there are some assessment procedures, they are typically costly and require complicated and intense effort by the assessor and assessee. Therefore, in this paper we devise a security assessment framework for electronic payment systems focusing on PCI DSS incompatibilities. We evaluate our model using a case study representing payment industry context. The proposed model, *Hierarchical Context-based Security Assessment (HCOSA)*, is a simple yet effective method providing insights to institutions on their security level in addition to inherent security assessment functionality.

## 2 Payment Systems and PCI DSS

Payment can be described as the transaction of the financial value between the buyer and seller. Modern electronic payment systems are based on *Transaction Processing* (also known as *Transaction Switching*). This activity involves processing, transmission, and storage of cardholder related data at various constituents in the payment network. In addition to PCI DSS, well-known compliance standards in data security ISO 27001 and EI3PA have common goal controlling and protecting sensitive data. PCI DSS and EI3PA differ from ISO 27001 being more standardized and regulated specifically to CHD and consumer credit information, respectively. Additionally, ISO 27004, BIP 0074:2006, and NIST SP800-55 Revision 1 have been standardized, with the aim of measuring the effectiveness and verifying the implementations of mentioned standards.

The main goal of an attacker in payment systems regarding data security is to capture CHD and exploit it. In terms of information security aspects, most attackers endanger Integrity and Confidentiality attributes of the payment system [6]. Based on the resulting damage, relevant threats can be classified into two main categories, namely *exposure* or *disruption of CHD*. Disruption of CHD has been largely mitigated by EMV standard and thus rarely faced [7]. But the exposure of CHD is still an open issue for payment systems due to PCI DSS incompliant parties. Thus, PCI DSS focuses on decreasing the probability of the occurrence of CHD exposure in payment systems [8].

In Table 1, we list PCI DSS objectives and the related security dimensions and threats. For instance, Objective (1) (O1) states that a compliant institution should provide a robust network environment against unauthorized modification or destruction of the CHD and Cardholder Data Environment (CDE) which leads to better integrity [9]. Under O2, CHD should be transmitted securely across networks. In that regard, encryption provides the confidentiality and integrity of CHD. For computational environment, O3 implies deployment of antivirus software which again serves to the integrity and confidentiality objectives. O4 requires the configuration of access control and limited access based on designated roles. Moreover, it requires the system to uniquely identify, authenticate, log and control system access. However, O5 and O6 contain elements that are less

| Objectives | Directly Related to | Sample Threat types |
|---|---|---|
| Build and Maintain a Secure Network | Availability: prevention against data delays or removal | Merchant website and processor gateway outages |
| Protect CHD | Confidentiality: protection against unauthorized data disclosure | – Data theft<br>– Eavesdropping for accessing and decoding CHD |
| Maintain a Vulnerability Management Program | Integrity: prevention against unauthorized data modification | – Account tampering<br>– Payment fraud |
| Implement Strong Access Control Measures | Authenticity: authentication of data source and modifier | – Internal theft<br>– Physical acquisition of CHD |
| Regularly Monitor and Test Networks | Accountability | Any potential security threat |
| Maintain an Information Security Policy | Nonrepudiation: prevention against any one party from reneging on an agreement | Any potential security threat |

**Table 1.** PCI DSS requirements with key security objectives and threats.

intuitive. The former item contains a requirement for intrusion detection and/or prevention functions whilst the latter addresses a range of security management functions, including matters such as incident response and management of third party relationships.

With omnipresent threats to the payment networks and the necessity of cost-efficient and timely security assessment of related systems, simple and effective security assessment is crucial. However, PCI DSS requirements are generally difficult to define in measurable and quantitative terms, which makes the security assessment of an organization according to these objectives a challenging task. Therefore, we propose HCOSA for PCI DSS in this work, focusing on streamlined and effective security assessment functionality for PCI DSS actors. This approach allows for a continuous and repeatable compliance assessment for PCI DSS.

## 3 Proposed Methodology: Hierarchical Context-based Security Assessment (HCOSA) for PCI DSS

We devise a security assessment methodology regarding PCI DSS and factors on the security of a payment-related system, namely Hierarchical Context-based Security Assessment (HCOSA). We assess the security of card holder data within an organization according to incompatibilities to PCI DSS requirements based on this approach. Security information flow and participating parties for the assessment are shown in Fig. 1. Actually, PCI has defined 12 PCI DSS requirements (Ri) under 6 objectives, where the objectives have been used to group and explain the requirements more precisely. For example, PCI DSS O1 contains R1

and R2 that are related to availability of systems as shown in Table 1. PCI DSS R1 is *Install and maintain a firewall configuration to protect cardholder data.*

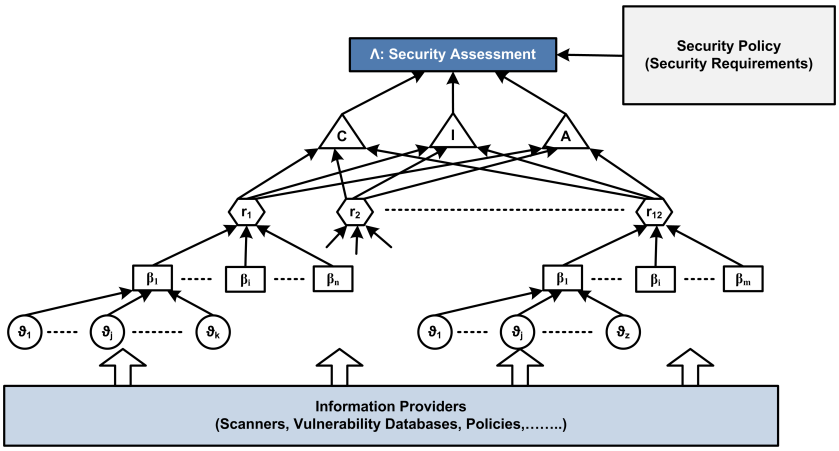



**Fig. 1.** Information flow for security assessment based on PCI-DSS.

In real life, systems have three main security objectives, namely confidentiality, integrity, and availability. Almost always, the objectives have different weights according to facts of organizations. For instance, availability is more significant than integrity for some services of financial institutions, which we have observed. Therefore, we compute the security assessment of an organization according to confidentiality, integrity, and availability requirements of CHD with Equation 1. Actually, a more granular security assessment formula may be constructed by considering many dependencies but this will increase the complexity of assessment with minor contribution to accuracy, which may be inapplicable in real life context.

$$\Lambda(t) = \kappa_c C(t) + \kappa_i I(t) + \kappa_a A(t). \tag{1}$$

Explanations of parameters used in all equations are provided in Table 2 and the values of parameters are within $[0, 1]$. In Equation 1, if $\Lambda(t) = 1$ or close to one, the security of CHD is high according to PCI DSS and the security policy of the organization, where $\sum \kappa_{x\in\{c,i,a\}} = 1$. Coefficients $\kappa_{x\in\{c,i,a\}}$ represents weights of confidentiality, integrity, and availability according to the security policy of an organization that contains CHD. On the other hand, we compute the three security objectives with $C(t) = \sum_{x=1}^{12} dc_x r_x(t)$, $I(t) = \sum_{x=1}^{12} di_x r_x(t)$, and $A(t) = \sum_{x=1}^{12} da_x r_x(t)$, where $\sum_{\forall x} dy_x \in \{dc_x, di_x, da_x\} = 1$. Specifically, we compute values of the three objectives according to satisfactions of each PCI DSS requirement and their dependencies related to the each security objective. For instance, assume that an organization partially satisfies PCI DSS Requirement 1 (R1), where the $r_1(t) = 0.53$. Assume also that $C(t)$ depends on that PCI DSS

| Parameter | Description |
|---|---|
| $\Lambda(t)$ | Security assessment |
| $C(t)$ | Assessed confidentiality |
| $I(t)$ | Assessed integrity |
| $A(t)$ | Assessed availability |
| $\kappa_c$ | Weight of confidentiality |
| $\kappa_i$ | Weight of integrity |
| $\kappa_a$ | Weight of availability |
| $r_x(t)$ | The effect of PCI-DSS requirement $x$ |
| $dc_x$ | Dependency coefficient of PCI-DSS requirement $x$ related to confidentiality |
| $di_x$ | Dependency coefficient of PCI-DSS requirement $x$ related to integrity |
| $da_x$ | Dependency coefficient of PCI-DSS requirement $x$ related to availability |
| $\beta_{x,y}(t)$ | Effect of sub requirement $y$ of PCI-DSS requirement $x$ |
| $\upsilon_j(x,y,t)$ | Effect of vulnerability $j$ to subrequirement $y$ of requirement $x$ |

**Table 2.** Model parameters and their descriptions.

requirement with $dc_1 = 0.34$. Thus, the total effect of the PCI DSS requirement for the computation of $\Lambda(t)$ is $dc_1 \cdot r_1(t) = 0.159$.

Organizations may partially or fully satisfy any subrequirement of a PCI DSS requirement. However, if a subrequirement of a PCI DSS requirement is not satisfied, which means $\beta_{x,y}(t) = 0$, the organization is then incompatible with that PCI DSS requirement, $r_x(t) = 0$. Moreover, each PCI DSS requirement consists of many subrequirements. Therefore, we compute the satisfaction of each PCI DSS requirement by considering effects of the subrequirements with $r_x(t) = \prod_{\forall y} \beta_{x,y}(t)$.

A subrequirement is compatible if it is resistant to potential vulnerabilities related to this subrequirement. Total effect of related vulnerabilities is the sum of effect of all vulnerabilities, which can be at most one. For this reason, we compute the compatibility of a subrequirement according to effects of potential vulnerabilities as following.

$$\beta_{x,y}(t) = 1 - \min\left(1, \sum_{\forall j} \upsilon_j(x,y,t)\right). \tag{2}$$

The impact of a vulnerability is determined according to information obtained from automated tools, such as scanners, vulnerability databases, security policies, and logs of security devices like firewalls and intrusion detection systems. For the sake of brevity, we do not present the impact of specific measurements about vulnerabilities and alternative measurements, such as the indicator of weakness in a firewall, in details. The impact of vulnerability and its measurement is challenging to determine since it is very context-dependent. Moreover, the gathered information needs to be pre-processed and evaluated for a consistent analysis. For instance, the impact factor of each requirement can be evaluated according to statistics on past breaches [10] and affected security objective due

to the inadequate related requirement [11]. Thus, we focus on the assessment framework itself in this work and determining values of the coefficients are out of scope of our paper.

## 4 Updating Firewalls in a Financial Institution

In this section, we present a case study for elaborating on HCOSA related to a financial institution managing its firewalls under PCI DSS compliance. The purpose of this case study is to show the effects of updating firewalls and routers and PCI DSS incompatibilities related to the updates. In this case study, we have simulated the network of this institution using MATLAB to evaluate HCOSA.

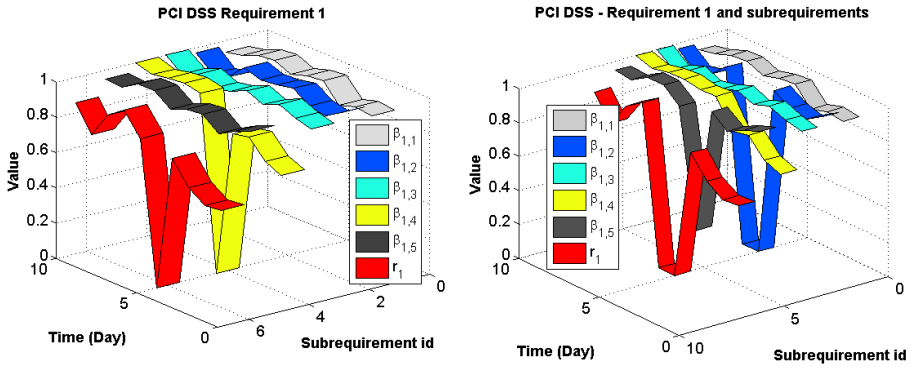
Let us consider a financial institution that has more than ten thousand employees at different physical locations over the world. The field of activity of the corporation is the processing of electronic payments that are carried out with various payment cards. Therefore, CHD is a very sensitive data for such corporation, which should be protected.

The internal (trusted) network of the corporation consists of all trusted networks in different physical locations and it contains CHD in addition to other information. A trusted network is connected to the internal network via the Internet (i.e., untrusted network). The perimeter security of a trusted network is established with firewalls, intrusion detection systems, intrusion prevention systems, and configurations of routers against attacks coming from the Internet.

The internal network of the institution is updated regularly according to various criteria, such as employees who leave or join, new security threats discovered, and technological improvements. The firewalls and routers are also maintained according to these updates. Additionally, the institution has PCI DSS certificate and it should preserve the certificate to carry out its business. On the other hand, changes related to firewalls and routers should comply with PCI DSS requirements. Specifically, PCI DSS requirement 1 (R1) is directly related to changes or configurations of firewalls and routers, stating the action *"Install and maintain a firewall configuration to protect cardholder data"* [3].

HCOSA is a multi-layered framework and considers subrequirements of a PCI DSS requirement for security assessment. R1 has five subrequirements and each subrequirement is related to different tasks of firewalls and router operation and maintenance. For instance, subrequirement 1.1 has seven tasks. Therefore, vulnerabilities related to each task affect the security of the corporation. In HCOSA, sources of vulnerability information are scanners, vulnerability databases, and other sources whose main tasks are to find security vulnerabilities. Actually, determining security vulnerabilities and their effects are complex tasks. In this case study, therefore, we assume that relevant vulnerabilities are known. Then we set their effects to subrequirements in an illustrative way to evaluate the proposed model.

In high-level evaluation, the security of an institution satisfies or not satisfies the PCI DSS requirements. In low-level evaluation, on the other hand, it is impossible to formally prove and verify the security of an ICT system. For this




(a) Single subrequirement case. (b) Multiple subrequirement case.

**Fig. 2.** The relationship among PCI DSS Requirement 1 and a major change in (a) a subrequirement (b) various subrequirements.

reason, if a subrequirement has a satisfaction ratio over a predefined threshold, the subrequirement is considered as *satisfactory*. In this case study, we assume that subrequirements are evaluated daily and a subrequirement is expected to have $\beta_{x,y} \geq 0.9$ for four consecutive days. If a subrequirement fails to satisfy this expectation, a maintenance process for firewalls and routers is initialized to improve security. However, some maintenance may have considerable negative effect for day five as shown in Fig. 2(a). There may be many reasons causing this negative effect. Simply, the lack of adequate qualified security experts, unexpected state of modifying network topology related to firewalls and routers in a complex network are some of them and they may result in unsatisfied subrequirement(s). Actually, the network in question is highly dynamic and compliance to PCI DSS may fluctuate over time. These fluctuations may be negligible if they satisfy the predefined threshold as shown for $\beta_{1,1}, \beta_{1,2}, \beta_{1,3}, \beta_{1,5}$ in Fig. 2(a).

Maintaining firewalls and routers regarding a subrequirement may affect only the subrequirement and its PCI DSS requirement as in Fig. 2(a) or it may affect many subrequirements and the PCI DSS requirement as in Fig. 2(b). For instance, the maintenance process to improve security level of subrequirement 4, $\beta_{1,4}$, is carried out in day five in this case study. The security level of $\beta_{1,4}$ is improved after the maintenance process but security levels of subrequirements $\beta_{1,2}$ and $\beta_{1,5}$ drop considerably as shown in Fig. 2(b). Therefore, the maintenance process related to firewalls and routers has been carried on until day seven to construct a system that satisfies all subrequirements of PCI DSS R1.

The case study shows that any change in the network of a financial corporation that contains CHD should be investigated carefully related to PCI DSS incompatibilities. Since such networks are very large, complex, and dynamic environments, the investigation has to be done in an automated way. HCOSA can be applied in network infrastructure to monitor and assess security of an organization related to PCI DSS in a continuous and repeatable process.

## 5 Conclusion

In this work, we investigate security assessment for PCI DSS requirements in payment systems. We devise a security assessment approach for PCI DSS in a context-based setting. We focus on PCI DSS incompatibilities and their effects on security. We provide some guidelines to security experts for assessment of PCI DSS compliance. In future work, we plan to extend our framework to include more advanced dependency models among PCI DSS requirements and improve the evaluation for our approach considering more heterogeneous contexts, such as evaluation of vulnerabilities and their effects in various contexts of payment systems.

## 6 Acknowledgments

This work is supported by EUREKA ITEA2 Project ADAX with project number 10030 and TEYDEB Project AKFiS with project number 1130018.

## References

1. Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., Singh, V.: A survey of payment card industry data security standard. IEEE Communications Surveys and Tutorials 12(3), 287–303 (Third 2010)
2. Choo, K.K.R.: New payment methods: A review of 2010-2012 FATF mutual evaluation reports. Computers & Security 36, 12–26 (2013)
3. Payment Card Industry (PCI) Data Security Standard: Requirements and security assessment procedures. `https://www.pcisecuritystandards.org/security_standards/documents.php/` (November 2013)
4. Peterson, G.: From auditor-centric to architecture-centric: SDLC for PCI DSS. Information Security Technical Report 15(4), 150–153 (2010)
5. Ataya, G.: PCI DSS audit and compliance. Information Security Technical Report 15(4), 138–144 (2010)
6. Verizon Risk Team: Verizon Enterprise Risk and Incident Sharing Metrics Framework. `http://www.verizonenterprise.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf` (2013)
7. Trustwave's SpiderLabs: Global security report. `https://www2.trustwave.com/2013GSR.html` (2013)
8. Ogundele, O., Zavarsky, P., Ruhl, R., Lindskog, D.: The implementation of a full EMV smartcard for a point-of-sale transaction and its impact on the PCI DSS. In: Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on Social Computing (SocialCom). pp. 797–806 (Sept 2012)
9. Rowlingson, R., Winsborrow, R.: A comparison of the payment card industry data security standard with ISO17799. Computer Fraud&Security 2006(3), 16–19 (2006)
10. Baker, W., Hutton, A., Hylender, C.D., Pamula, J., Porter, C., Spitler, M.: 2011 data breach investigations report. `http://www.verizonbusiness.com/resources/reports/rp_databreach-investigations-report-2011_en_xg.pdf` (2011)
11. Bradley, T., Chuvakin, A., Elberg, A., Koerner, B.J.: PCI Compliance: Understand and implement effective PCI data security standard compliance. Syngress Publishing (2007)