Merchant Secure E-Commerce (4D-Security)

[*1] Mahmut Özcan and [2] İ.Esen Yıldırım
[*1] Institute of Banking and Insurance, Banking, Marmara University, Istanbul, Turkey
[2]Faculty of Economics, Statistics, Marmara University, Istanbul, Turkey

Abstract

In this study, the precautions and developments to reduce e-commerce frauds in Payment Card Industry (PCI) are analyzed and introduced with their results. PCI has developed e-commerce security to a higher level by integrating 3D-Security mechanism. Although 3D-Security meets a big deficit by applying "Chip & PIN" virtually, the absolute security is not achieved in e-commerce by burnout of it. New model "Merchant Secure E-Commerce Model" is offered for preventing from malicious merchants. As the model controls the merchants' confidentiality, it provides 3D-Secure transactions with fourth security domain (4D-Security). In order to reach "Zero Risk E-Commerce", the study also offers cargo status integration and individual insurance of each order.

Key words: E-Commerce, E-Banking, 3D-Security, Payment Card Industry, Information Security.

1. Introduction

Electronic payments, which are performed over internet, become most popular with the development of technology and Payment Card Industry (PCI). As the increase in use of credit/debit cards in internet transactions and the number of merchants, the needs and security risks of e-commerce increase as well. For a secure e-commerce; customers, banks, merchants and the overall services framework should act in a secure manner. Otherwise, credit/debit cards can be used unintendedly in fraudulent transactions over internet. It results in the expense of monetary, operational and reputational cost for all parties.

In addition to detailed security controls of merchants, acquirer banks and issuer banks during the transaction, PCI has developed e-commerce security to a higher level by integrating virtual-card application, prepaid-card application and 3D-Security mechanism for cards. Development of 3D-Security system is one of the most sounding and widely-used application in e-commerce which is based on virtual application of "Chip & PIN" technology. 3D-Security provides card owner authentication and gives whole risk to the card owner. Banks and merchants have no risk as long as they support 3D-Security in e-commerce. Although 3D-Security covers some defects, there are some fraud relevant matters to solve. Basically, understanding or predicting the behavior of the merchants cannot be guaranteed in the situation of corporate disasters or bankruptcies. No mechanism can protect cardholders from merchants' malicious order collection and canvass. Any merchant immersed in debt (gone to bankruptcy) may cheat customers by collecting orders and do not deliver goods and services.

*Corresponding author: Mahmut Özcan Address: Institute of Banking and Insurance, Banking, Marmara University, Istanbul, Turkey. E-mail address: mozcan@gmail.com, Phone: +905456521500

For preventing card owners from malicious merchants, we need a new accredited mechanism which guarantees that the merchants are up-to-date confidential and trustable. In this study, we propose "*Merchant Secure (M-Secure) E-Commerce Model*" for worldwide usage. The new system is announced which comprises "*Merchant Control Servers (MCS)*" that keeps the merchants credibility score called as "*E-Commerce Score (ECS)*". MCS is designed for responding to online and batch ECS inquiries at attention. This model provides fourth security domain to 3D-Secure transactions by controlling the merchants' ECS values. Therefore, this mechanism is called as 4D-Security.

Providing that, cargo status integration and individual insurance of every order, 4D-Security system promises to guarantee "Zero Risk E-Commerce" in electronic payments.

2. 3D-Security

3D-Secure [1] is a protocol designed to be an additional security layer to acquirer security layer and issuer security layer for internet card transactions. 3D-Security scheme allows a cardholder to authenticate himself during an e-commerce transaction. By this way, authentication takes place before an authorization process. 3D-Security was developed by Visa [2] under the name Verified by Visa, is accepted as an application standard by Mastercard [3] under the name as MasterCard SecureCode, by JCB International [4] as J/Secure, by American Express [5] as American Express SafeKey.

3D-Security system targets to increase the security level of credit/debit card transactions performed over internet. It provides e-commerce merchants with cardholder authentication, ensuring the identity of cardholder is same as the identity of the buyer in internet environment. By this, the number of fraudulent transactions and chargeback costs will decrease noticeably. At the time transaction has been started, authentication of cardholder verified via associated *Access Control Server (ACS)* [6] of issuer bank. ACS is a certified trusted third party which can store some private information of cardholders on behalf of contracted issuer banks. As, an authorization process takes place after authentication process, cardholder may not assert or claim that transaction authorized without own will, this is non-repudiation.

To waive one's scruples, 3D-Security prevents use of cards from non-cardholders. With 3D-Security, the principle security routines (authentication, confidentiality, authorization and non-repudiation) [7] would be guaranteed. As, merchant is controlled by acquirer and issuer bank that it is confident via PCI [8] rules, and additionally ACS authenticates the cardholder, 3D-Secure transactions reach to the most secure level. Nowadays, in order to discuss secure internet payments, it should be performed by use of 3D-Security technology.

3. Weaknesses of 3D-Security

According to 2010 Internet Crime Report [9] of Internet Crime Complaint Center of USA, *the non-delivery of payment or merchandise* was the most reported offense during 2010. Correspondingly, with respect to the investigation of the one of Turkish top complaint website, paid but non-delivered products/services category takes first place with 39.7 percentage [10].

Above information reveals that merchant related complaints or crimes are the most modal fraud type of e-commerce transactions. What if any merchant makes insidious plan or changes good mind, banks and/or cardholders to be bought a pup unforeseeably. Although a transaction has been performed with 3D-Security facility, merchant may be fraudulent and may not deliver goods, products or services. Merchant frauds may reach to a higher-cost and can be more dangerous than the card data theft, and that risk must be considered [11].

Visa (MFP-Merchant Fraud Performance) [12], MasterCard (GMAP-Global Merchant Audit Programme and MOST-Merchant Online Status Tracking) [13], AMEX (HRSE-High Risk Service Establishment) [14] are the merchant fraud control mechanisms of international payment systems. Those mechanisms feed information to acquirer banks about potential dangerous activities of their merchants and necessary actions must be taken. All information gathered, processed and generated after transactions completed and transferred in an offline manner with periodic batch files. This non-proactive approach makes stopping and preventing the fraudulent merchants difficult and unsatisfactory for quick reactions. Most of the frauds can be realized and more destructive at the early periods after they were launched.

Even, all programs above have the capability of sending online warning/alert to issuers, during the period of sense and detection (fraud gap), the frauds would be continued and go on non-slowdown destruction. Above programs just would be able to stop frauds after a gap period and cannot promise real-time solution. Having inadequate mechanisms for detecting and preventing frauds at a time transaction is performed; merchant based frauds cannot be zeroed or even not limited effectively.

4. Merchant Secure E-Commerce and 4D-Security

3D-Security and international payments systems are not enough to stop malicious merchants who collect and not deliver orders. In order to distinguish whether e-commerce merchants are confident or not, we must have instant payment transaction investigation or periodic bulk data assessment on payment transaction set. The principle problem is not working out the authentication of merchant's identity but to understand when a merchant is changing behavior, breaking goodwill and attempting deceit because of various reasons, probable bankruptcy etc. Moreover, some merchants may be a forger and malevolent from primary stage indeed. Neither 3D-Security nor international payments systems are not capable of handling and revealing merchant fraud completely [15].

3D-Security weaknesses and inadequate international merchant fraud control mechanisms impel us to new motivation, developing a new system which prevents from merchant based frauds, minimizes financial and operational costs and encourages individuals to use e-commerce more in payment systems eventually. Our new model is called as *Merchant Secure (M-Secure) E-Commerce Model*, which provides payment transactions with merchant domain security. New domain, *Merchant Control Server (MCS)*, as ACS for card owner authentication in 3D-Security, would be responsible for keeping and maintaining the merchants' credibility score reflecting the confidentiality of merchants. With this additional security domain, all 3D-Secure transactions will be upgraded and reached to a higher security level, so this model can be named as 4D-Security.

4.1. Merchant Control Server (MCS) and E-Commerce Score (ECS)

MCS is the corporation that has a right of operating on merchant data on behalf of contracted banks. MCS must at least satisfy the rules that ACS has to obey, such as; PCI DSS, PCI key management routines, etc. On the other hand, every MCS has a data-center responsible for managing merchants' credibility indications and functions. MCS keeps, evaluates, manages and responses to inquiries of merchant ECS values. Any acquirer bank wants whose merchants to be involved in M-Security system, must register them to concerning MCS.

After establishment of MCS systems, merchants' ECS values may be learned easily by any issuer bank. To remind, there are 3 security domains in 3D-Security; first one is acquirer domain, second is issuer domain and third one is ACS domain. M-Security adds MCS domain security to e-commerce transactions. Any transaction performed with MCS security control and fulfilled the requirements of 3D-Security then it can be legitimately named as 4D-Secure transaction.

MCS hosts are designed to be able to respond ECS inquiries both in an online and offline manner. MCS is responsible also for keeping ECS values up-to-date. ECS values are updated with respect to transaction results, delivery results and customer complaints. ECS will be affected positively after transaction is approved, score grows up, and merchant confidentiality ascends. On the contrary, ECS will be decreased by the criticality level of concerning complaint at a time its reached, and merchant confidentiality descends. Reaching to specific quantities of complaints, signals to MCS to be able to pause the merchant's e-commerce activity temporarily or even permanently. By this way, awareness of issuer and customer would be facilitated and no more customers make financial loss.

4.2. Merchant Activity, Notification of Acquirer

For banks to be modeled in 4D-Security, it is necessary to share merchant activity with chosen MCS, by a *notification file*. Bank acquirer code, merchant code, merchant business name, proprietor full name, official address, sector code, taxation number and contact information (telephone, mobile number, email, fax etc) should initially be supplied to MCS servers. Any change in merchant activity must be informed instantly or daily at worst, such as; starting e-commerce (registration), stopping e-commerce (long-term passive mode), pausing (short-term passive mode) or activating (moving to active mode). Same file format can be used for all kind of

activities.

4.3. ECS Matrix

A matrix that is used for specifying which transaction effects ECS value at what extent and magnitude called as ECS matrix. Every MCS has unique intimate ECS matrix that is updated only by itself and not be propagated out. Merchant initialization (MI), merchant revocation (MR), merchant temporal revocation (TR), merchant activation (MA) and e-commerce transactions (TX) are the primary action types (one of the column types) in ECS matrix. As every combination of action types and other column types (amount, sector code, 3D-Secure flag, cargo status, etc) is included in the matrix, there must be at least one matching row and corresponding score value for every transaction processed.

4.4. ECS Decision Matrix and Evaluation

A matrix that is used for assessment of ECS value. Decision matrix is unique matrix that can be defined, updated and be propagated only by MCS. Each MCS has to have an inquiry service for issuer banks to get latest ECS decision matrix. Besides, MCS publishes up-to-date ECS decision matrix via web site. Decision matrix has three decisions; Accepted (A), Rejected (R), Issuer-Initiative (I). Making decision process over the ECS Decision matrix assessment is called as *evaluation*. Issuer banks have to reject a transaction which has evaluation result as Rejected. By and large, 'R' value means that transaction is not safe because merchant on which transaction is performed may have some risky conditions. 'A' value indicates there is no measured or known risk on the merchant. 4D-Security system uses 'I' result in uncertain situations, and defers to issuer bank decision mechanisms.

4.5. Shipping Information Affect

In the proposed model, shipment status information of products/services will be send to concerning MCS by cargo companies in batch files. Corresponding MCS record is marked as delivered up and ECS value of merchant is affected positively, as its described in ECS matrix. Most of the rows in the ECS matrices have been arranged as awaiting shipping result for the concrete or physical products whereas not for non-transportables (software, license, etc).

4.6. Customer Complaint Affect and ECS Recovery

Customers may have a chance to complain merchants about shopping, and report the situation to MCS. During reporting, some necessary security and consistency checks should be performed. To understand shopper and complainant are same, last 4 digits of card number, emboss name, merchant name, amount and other information on record may be validated. All of the complaints are logged in MCS records. Solid ones evaluated and necessary actions should be taken with respect to ECS matrix. Complaints decrease merchant ECS necessarily. Moreover, some serious complaints proven beyond doubt may pause merchant e-commerce activity temporarily or even stop permanently.

Merchant is able to make an objection to a complaint that reduces its ECS value. By citing product delivery voucher or document, it may justify the situation and get recover the score. It is

advised that customer satisfaction must be provided before score recovery. In case of give the customer complaint up with her own will, ECS can be corrected too. Score recovery conditions are announced by MCS.

4.7. Order Insurance

It is important for our model to supply every individual order with insurance. This must be an obligation for merchants to provide insurance mechanism on their payment framework. Customer can either introduce an insurance to an order or not. It must not be forgotten that insured products would be higher priced but more dependable.

4.8. Merchant Security without 3D-Security

New model has an advantage of providing both 3D-Secure and non-3D-Secure transactions with merchant security. Because, merchant security supported transactions have been checked by issuers via MCS even if the transaction is not 3D-Secure. Those transactions are not *4D-Secure* but *Merchant Secure*. Because 3D-Security is a well-known security standard as indicated in section 2 and used in most of the countries, attaining 4D-Security goal would not be that hard.

5. Applying Merchant Security

Applying *merchant security* to a transaction during its lifetime will be discussed deeply in this section, from merchant security perspective. At a time a shopping starts in a merchant, acquirer adds its MCS server description to a specific field of financial message and forwards message to issuer bank within PCI switching routine established before. Acquirer puts also a special value into Electronic Commerce Indicator (ECI) [16] subfield of payment message. By this way, acquirer indicates that transaction can be completed in issuer by applying the merchant security rules. At the issuer side, when the transaction reaches to issuer, issuer notices whether to make merchant security check or not from the ECI value. If necessary, issuer inquiries the ECS value of merchant from MCS that is introduced in MCS description field in the message. Afterwards, ECS value is evaluated in issuer as described in section 4.4 and issuer response generated for being transmitted to the acquirer. When the response reaches, acquirer informs customer about the payment result and saves merchant security information for future inner intelligence. Similarly, issuer also informs MCS about transaction response to update ECS in MCS. Transactions can be declined by issuer because of merchant security checks and assessment. The *rejection reason code* is inserted in appropriate fields of the response message.

5.1. 4D-Secure Not-Onus Transaction Flow

Transactions of which acquirer and issuer banks are the same called as *onus (OU)* transactions, otherwise they called as *not-onus (NO)* transactions. In this sub-section, it is tried to explain how the 4D-Security changes and affects the NO transaction flow in payment networks. Note that, as all 4D-Secure transactions are 3D-Secure too, they are recorded both in MCS and ACS systems. A sample 4D-Secure not-onus (acquirer and issuer are different) transaction flow is figured out in Figure 1 below. When an e-commerce transaction starts in acquirer side, card issuer bank is

identified by using card number and checked whether the issuer is registered to 3D-Security Directory (Visa, MasterCard directory etc). If so the related transaction fields are passed to related ACS server for 3D-Security controls. ACS makes 3D-Security checks over card owner private information and authenticates customer. Acquirer supplements also connection information of its contracted MCS into the financial message.

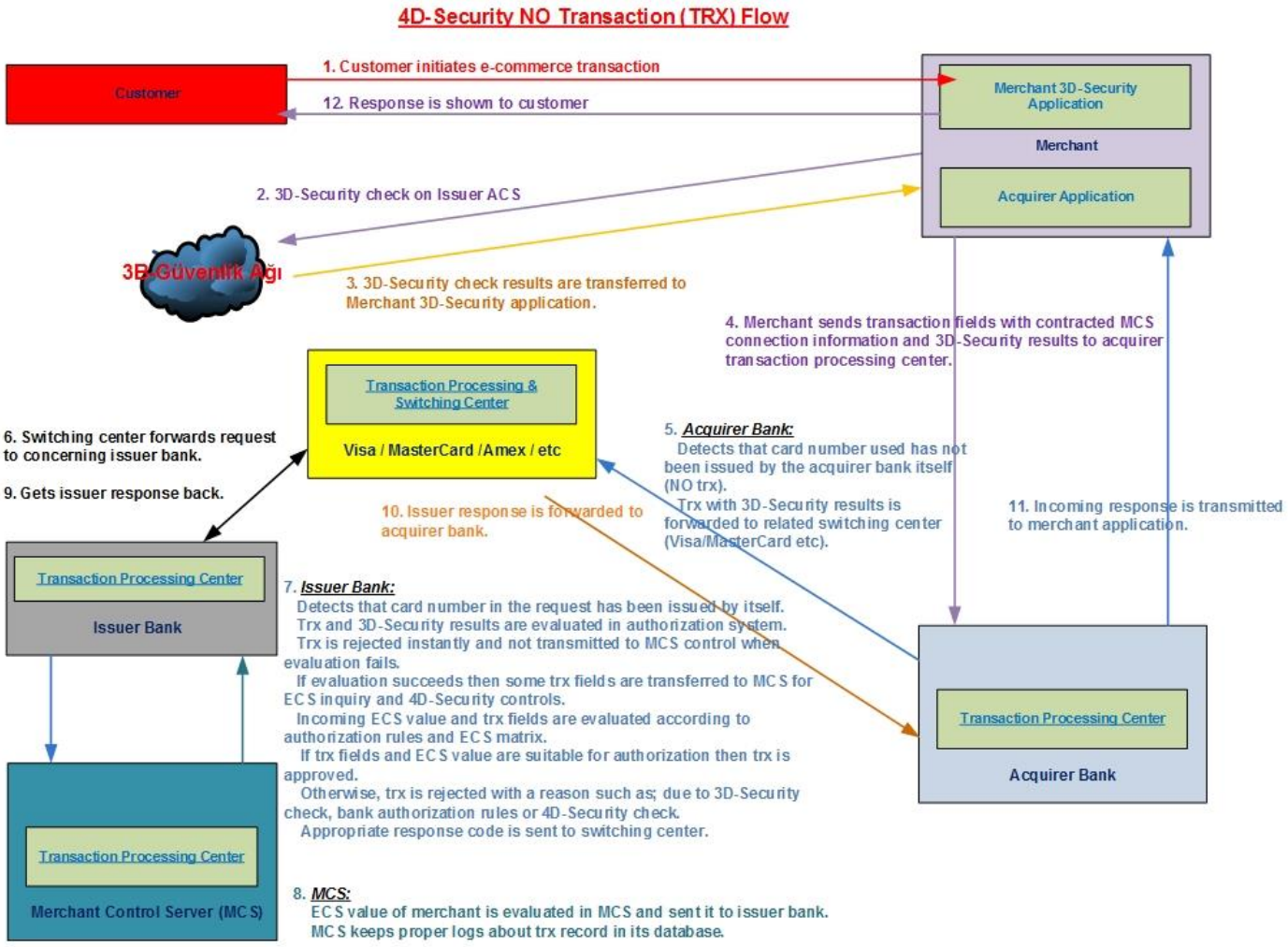

Figure 1. 4D-Secure Not-onus Transaction Flow Diagram

Afterwards, the transaction message is forwarded to issuer bank's authorization system over present payment network. Authorization uses MCS connection information and passes some of the transaction fields to the concerning MCS to make ECS value inquiry of acquiring merchant. MCS replies issuer inquiry with calculated ECS value of the merchant.

Issuer authorization system applies ECS to *decision matrix* and gets response of A, R or I. In case of A (Accepted) or R (Rejected) responses, authorization system complies to ECS decision

matrix and accepts/declines the transaction with proper logging. Response message is generated and sent to merchant (web, mobile, etc) site. When I (Issuer-Initiative) decision leaves from matrix, issuer should give authorization decision on its own independently. Whatever issuer decides must be posted to MCS about that judgment. Finally, transaction becomes accepted/rejected by notifying customer.

It is critical that issuer must inform MCS about final decision of transactions even in onus transactions. There are 2 goals for going to MCS even the transaction is onus. First, to register and track some transaction information (date, time, last digits of card number, amount, customer name-surname, etc) in the MCS database. Second, providing instant consistency to MCS in thinking the merchant's ECS may be affected by this transaction.

5.2. Contribution of Model

Through merchant security, additional security layer has been added to 3D-Security. E-commerce security has been upgraded to a higher level and it is reached to 4D-Security. With establishment of MCS, learning of merchant's confidentiality instantly and proactive protection of customers against merchant frauds in e-commerce shopping are the key advances. By this way, card owners are guarded against the malicious merchant who makes fraud on purpose. As risks related to merchants fine down to near zero with merchant security and risks in card owner resolved in 3D-Security, it is foreseen that no need to liability shifting mechanism [17] in 4D-Security.

Even in the countries that have very low fraud ratio, monetary lost can be reached to millions of dollars because of the merchant related frauds. Thanks to merchant security, it will avoid wasting most of money. Besides, waste of time, the quantity and the qualification of personnel who care about merchant related frauds, their reasons, their damages, precautions against them, chargeback[17] cost, liability shifting effort and other remaining operations will be fine down in the payment foundations (banks etc). Preserving more time, money and other resources will affect the quality of PCI related services and the reputation of bank positively.

Conclusion

Despite 3D-Security's expansive protection in the worldwide, e-commerce frauds have not been run out completely. Although it has equipped protection mechanisms for banks and merchants, it cannot be able to safeguard card owners against merchant related frauds significantly. 4D-Security, will prevent card owners from merchant malicious actions and feature comprehensive security for each party (acquirer, issuer and card owner). In addition to merchant security, advancing 4D-Security with cargo status integration and individual order insurance capability will reach e-commerce to risk-free. Reaching to near zero-risk e-commerce will raise card usage in shopping among individuals and boosts to struggle against shadow economy. Reduction in shadow economy and decreased fraud will make banks and countries more profitable with respect to monetary, operational and reputational aspects. Proposed 4D-Security model can be applicable e-commerce model for international use. After payment systems recognize merchant security model, 4D-Security will become widespread and be a common international system.

References

[1] Verified by VISA, http://www.visaeurope.com/making-payments/verified-by-visa/ (April 01, 2015).

[2] Visa Europe Official Website, http://www.visaeurope.com/ (April 09, 2015).

[3] MasterCard Official Website, http://www.mastercard.com/ (April 09, 2015).

[4] JCB, The Payment Solution Provider, http://www.jcbeurope.eu/ (April 09, 2015).

[5] American Express, https://www.americanexpress.com/ (April 09, 2015).

[6] Issuer Acces Control Server (ACS), Verified by Visa Acquirer and Merchant Implementation Guide, VISA, May 2011, p. 15.

[7] Ozcan M, Design and Development of Practical and Secure E-Mail Ssytem, Sabanci University, MSc Thesis, Istanbul, 2003. p.17-18.

[8] PCI Quick Reference Guide, PCI Security Standarts Council LLC, 2008.
[9] 2010 Internet Crime Report, Internet Crime Complaint Center, USA, 2010.

[10] Sikayetvar Complaints Categories, http://www.sikayetvar.com/kategori/internet/e-ticaret (June 12, 2014).

[11] Ozcan M, Mermod A, How Safe Is Electronic Banking? A Risk Analysis of Electronic Banking Systems in Turkey, International Conference on Banking and Finance Perspectives, Famagusta, North Cyprus Turkish Republic, April 2011, p.13.

[12] Merchant Operating Manual, Merchant Fraud Performance, http://www.moneris.com/~/media/Files/MerchantServices/merchant-manual-en.ashx (October 16, 2013).

[13] Global Merchant Audit Programme, Mastercard, p25.

[14] American Express Security Center, https://www.americanexpress.com/us/content/fraud-protection-center/home.html (April 09, 2015).

[15] Ozcan M, Secure E-Commerce Model for Turkish Electronics Banking, Marmara University, PhD Thesis, July 2014.

[16] Electronic Commerce Indicator (ECI), Verified by Visa Acquirer and Merchant Implementation Guide, VISA, May 2011, p. 30.

[17] Verified by Visa Overview, Verified by Visa Acquirer and Merchant Implementation Guide, VISA, May 2011, p. 8.