Enhancing Security of Online Payments

A Conceptual Model for a Robust E-Payment Protocol for E-Commerce

Takyi, Augustine; Gyaase, Patrick Ohemeng Kwadwo

Published in:
Contemporary Research on E-business Technology and Strategy

DOI (link to publication from Publisher):
10.1007/978-3-642-34447-3_21

Publication date:
2012

Document Version
Early version, also known as pre-print

Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce

Augustine Takyi[1] and Patrick Ohemeng Gyaase[2]

[1] Computer Science Department
Sunyani Polytechnic, Sunyani
P.O. Box 206, Sunyani
augustinektakyi@yahoo.com
[2] Faculty of Information, Communication Sciences and Technology
Catholic University College of Ghana, Fiapre Sunyani
P.O. Box 363, Sunyani
kgyaase@gmail.com

Abstract. The rapid growth of the Internet and its adoption for commercial transactions is indisputable. However, the core security protocols of the Internet today are susceptible to security lapses, especially when it comes to online payment systems which are indispensable to the growth of e-commerce across the globe. This has led to the development of various online payment protocols to ensure the security of online transactions such as Secure Electronic Transaction and The Secure Socket Layer. In designing online payment protocols, there is often a trade-off between security and convenience. More and more participants of online transactions suffer in one way or another from fraudsters. Ghana is gaining notoriety in online fraud, and there is therefore a need to protect the interest of the participants in the areas of authentication, confidentiality, replay attacks as well as flexibility if e-commerce is to thrive in developing countries. This paper looks at some online payment protocols and develops a conceptual model of a protocol which requires live authentication from the cardholder. This ensures security, convenience, cardholder authentication, and verification of merchant; it is easy to implement without complications and to compare with other existing online payment protocols. Participants that are considered in this work are the Cardholder, Issuer, Merchant, and Acquirer.

Keywords: cardholder, issuer, merchant, authentication, non-repudiation, integrity.

1 Introduction

There is widespread usage of the Internet for commercial activities, but the core designs of Internet protocols make online transactions susceptible to risks. Extra measures are needed to minimize these risks. To effectively support e-commerce, e-payment systems must be secure, reliable and convenient with good authentication, privacy, integrity and non-repudiation. Online payment frauds cause millions of dollars in loss yearly, exposing the weakness in security of online payment systems[1].

V. Khachidze et al. (Eds.): iCETS 2012, CCIS 332, pp. 232–239, 2012.

In 2009, the United Kingdom reported $696 million losses due to card fraud while Australia recorded $US 144 million[2]. The statistics suggest that card-not present fraud, such as online payment fraud, is the most prevalent. Most proposed protocols to combat this are theoretically secure but their implementation has been unfeasible. [3] The confidence of online transaction participants therefore needs to be improved if the developing world is to benefit from the global adoption of e-commerce [4].

2 Online Payment Systems

Online payment transaction involves a complex set of practical and analytical challenges, including technological capabilities of service providers, commercial relationships, regulations and laws, security issues such as identification, authentication and verification with co-ordination among parties with different and competing interests[5].

2.1 Account-Based Online Payments

Credit Cards enable the holder to make credit purchases with a fixed limit.Credit cards were not specifically designed for online payment, hence the inherent risks associated with their use as such. [6] Authentication is done using the cardholder's name, credit card number and expiry dates. This information, if intercepted when provided for online transaction, could be used by fraudsters[7].

Debit Card: The value for online transaction is directly debited to the cardholder's bank account[6].

Mediating Systems: This System employs traditional payment means, with further layers. Using the service requires registration by providing credit card or bank account details as the source of payments. A very successful mediating service for online transactions is the PayPal payment system[5].

Mobile Payment Systems: Mobile payments are conducted through wireless devices. They may be used to conduct payments through a bank account or telephone bill[8].

Online Banking: A merchant redirects to the customer bank's web site to effect payment where customer payment details are automatically entered from the electronic bill and the payer only authorises.

2.2 Electronic Currency Systems

Smart Card Systems: Smart Cards are plastic cards with memory chips and embedded microprocessors which store more information than credit cards with inbuilt transaction processing capability[9] [7].

Online Cash Systems. Online cash systems such as Virtual BBVA (Spain) and similar systems in Italy, Austria and Australia [5] work via prepaid cards with different arrangements, but most require merchant subscriptions. Electronic tokens representing a certain value are exchanged in a similar way to cash.

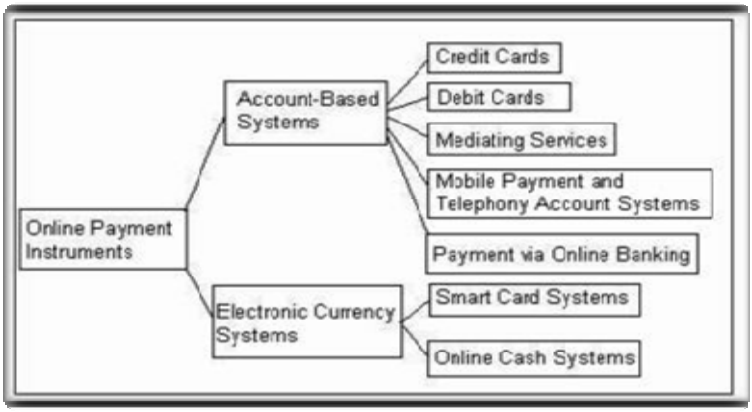

Fig. 1. Classification of on-line payment Systems for E-Commerce [10]

2.3 Online Card Processing

The five parties in e-payment environment are the Cardholder, Issuer Bank, Merchant, Acquirer Bank and Payment Gateway. The transactions between the banks are proven secured and reliable. The participants at risk are Cardholders and Merchants[7] [6].

Increasing globalization and the need to promote e-commerce in developing countries require a more secured, reliable and convenient e-payment protocol that is easy to deploy and convenient in application to all participants.

This paper presents a conceptual model for securing online transaction between parties with a balanced trade-off between Security and convenience.

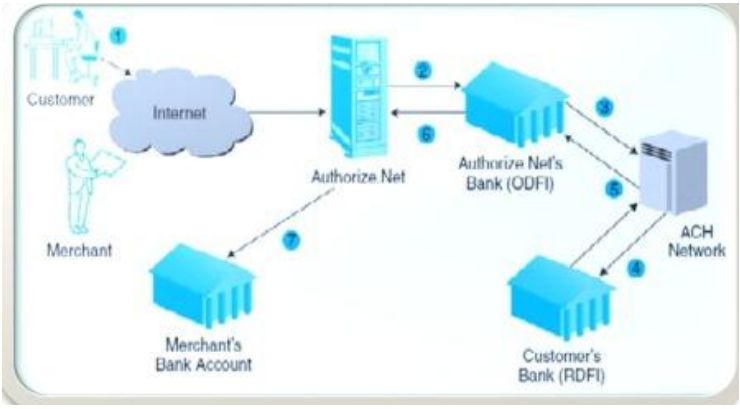

Fig. 2. Online Payment Process cycle [10] [6]

3 Electronic Payment Protocols

The success of e-commerce is based on standards, such as TCP/IP and HTTP, low-cost Internet access and protocols supporting online payments. E-payment protocols define e-commerce, distinguishing viable e-commerce sites from their information-only sites. An e-payment protocol does not move just data; it moves money.

i. iKP Family Protocols

The design; implementation and deployment iKP Secure Electronic Payment Protocol involves three parties: the buyer, the merchant and the acquirer gateway. The (i) is a variable representing the number of parties with public keys-pairs. [11] With 3KP all the parties possess public key-pairs.

ii. Secure Electronic Transaction (SET)

SET is an open encryption and security specification, designed to protect credit card transactions online and supported by companies such as VISA and MasterCard. [12] Designed for e-commerce, it provides confidentiality through encryption and data integrity with digital signature and authenticates both the cardholder and the Merchant. [12] SET also facilitates interoperability among software and network providers [13] [14]. SET requires a Public Key Infrastructure (PKI) which is a complete system for certificates. The certificates are issued by independent certificate authorities [14]. Replay attacks are a security concern to participants of SET protocol.

iii. One-Time Payment Scheme (CCT)

One-time credit card transaction number is designed to generate unique transaction numbers for single use in each transaction[12] [15], preventing replay attacks and eavesdropping. However, there Merchant verification concerns that could lead to fraud.

iv. Live Cardholder Authentication

This protocol authenticates the cardholder live, during the process of payment, combining both telephone banking and online banking together. The payment information are encrypted and forwarded through the Internet. The cardholder authentication is accomplished through a phone by the issuing bank requesting the customer for a PIN and the amount involved. Authentication is done using a combination of correct credit card details, i.e. phone number, PIN, and the transaction value. [16] The cardholder cannot authenticate the Merchant.

v. Secure Socket Layer (SSL)

The Secure Socket Layer protocol provides a private, encrypted session between the client and the server. The protocol and its related certificates are widely used in web browsers. The server authenticates itself to the client using the server certificate, but the authentication of the client to the server is optional[4] [17]. The information transmitted by the cardholder is encrypted with a sessional key generated through a handshake between the cardholder's browser and the merchant server. The absence of cardholder authentication and verification and cardholder authentication leaves room for fraud in the event of lost cards.

4 The Proposed Robust E-Payment Protocol (REPP)

Online payments have yet to gain wide usage in Ghana, due to security and high frequency of fraud in the online payment system[18]. To enable a roll-out of online payments, the indispensability of a more robust secure payment protocol that will withstand most common security threats cannot be over-emphasized. Such a protocol must be usable and convenient, giving the cardholder the options to make changes to or stop a transaction.

Cardholder authentication should be a key factor in deploying online payment protocol, as most of the existing protocol is silent with regards to the former. The merchant should also be verifiable, to enable the cardholder to feel secure and confident to do business with the merchant online. Furthermore, the ease of implementation for such protocol should be paramount.

The proposed Robust E-Payment Protocol (REPP) incorporates a solution to the above weaknesses identified in existing protocols, and if implemented can reduce fraud associated with e-payments in developing countries such as Ghana.

Robust Electronic Payment Protocol requires a merchant to register and obtain a certificate from a trusted Certificate Authority as indicated in **Step E** in the illustration below before operating online services. Hence, all merchants under the transaction of this protocol are trustworthy. Also, all data flow in the protocol is encrypted using SSL.

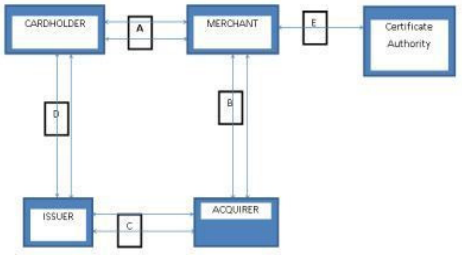

Fig. 3. A conceptual Model for Robust E-payment Protocol (REPP)

4.1 How the Protocol Works

- Purchase request: Cardholder makes an order at the merchant site **(Step A)**
- Authorization and Authentication Request: Merchant, through the Acquirer, validates whether the cardholder has enough funds **(Step B**)
- Authorization and Authentication: Acquirer forwards validation to Issuer **(Step C)**
- Authorization and Authentication: Issuer then confirms the purchase from the cardholder by prompting the cardholder to input his password
- Authorization and Authentication Response: Issuer then forwards the result to the Merchant through the Acquirer **(Steps, D, C, B, A)**
- Purchase response: Merchant Response **(Step A)**

Purchase Request

A cardholder initiates transaction by providing credit card details, which translates to a dual signature of the order and the payment details as shown below:

$OI = k_m(OI)$…..i and $PI = k_I(PI)$……ii, Where OI = Order information, k_m = Merchant encryption key, PI = Payment Information, K_I = Issuer encryption key.

Equation (i) shows how order information is encrypted and forwarded to the merchant and (ii) shows how payment information is encrypted and forwarded to the issuer.

Both signatures are then forwarded to the merchant through Cipher text (SSL) which the merchant decrypts; the merchant then forwards the payment details to the Acquirer for onward transmission to the issuer.

Authorization and Authentication Request

The card issuer receives the payment request and decrypts it, identifies the cardholder and automatically rings the cardholder to authenticate the purchase. The cardholder then confirms by inputting a secret PIN through the phone. The issuer then forwards the authorization information to the merchant through SSL.

Purchase Response

The merchant, upon receiving the authorization through the payment gateway, then confirms the purchase to the cardholder or declines.

4.2 Comparative Analysis

SET improved upon the 3KP protocol by introducing dual signature, which prevented merchants from accessing the payment details hence making SET a bit more secure than 3KP. Nevertheless, the implementation of SET was still more complex than with the 3KP protocol, due to overhead costs in acquiring PKI.

The SSL protocol was easy to implement and more convenient to use, but absence of cardholder authentication and merchant verification made fraud rampant in the SSL protocol.

The live authentication payment protocol makes the merchant anonymous but provides live cardholder authentication.

One time transaction Number prevents replay attacks on the online payment system environment, but with no merchant verification and cardholder authentication.

The proposed REPP combines security, convenience and ease of use. The advantage of REPP over the protocols discussed is the option for the cardholder to terminate the transaction. Therefore, errors or fraud can easily be identified by the cardholder and the transaction can be terminated.

Table 1. Comparison of The proposed REPP with existing Protocol

Protocol	Security	Usability	Cardholder Authentication	Verification of Merchant	CardHolder Termination	Implementation
3KP	secured	Complex	good	yes	No	Complex
SET	secured	Complex	good	yes	No	Complex
SSL	secured	Convenient	seldom	No	No	Easy
CCT	secured	Convenient	seldom	No	No	Easy
LCA	secured	Convenient	good	No	No	Easy
REPP	secured	Convenient	good	yes	Yes	Easy

5 Conclusion

Though yet to be practically implemented, the proposed Robust Electronic Payment Protocol (REPP) theoretically compares very well with live cardholder authentication in terms of security, usability, cardholder authentication and implementation. However, the REPP verifies the merchant as much as SET does. The result therefore indicates that REPP is much more capable of minimizing fraud, convenient to use, and easy to implement in the real world. This proposed protocol could be an antidote to the recent fraudulent activities within the e-commerce environment. The proposed protocol would be implemented to test its robustness in a future work.

References

[1] http://travel.state.gov, http://travel.state.gov/travel/cis_pa_tw/cis/cis_1124.html (2010), http://travel.state.gov (accessed September 10, 2011)
[2] http://www.apca.com.au, http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Payment_Fraud_St (2009), http://www.apca.com.au (accessed November 5, 2010)
[3] Levi, A., Kroc, C.K.: CONSEPP:Conevient and Secure Electronic Payment Protocol Based on X9.59. In: 17th Annual Computer Security Applications Conference, New Orleans, Louisiana (2001)
[4] Hwang, J.-J., Yeh, T.-C., Li, J.-B.: Securing On-line Credit Card Payments Without Disclosing Information. Computer Standards and Interfaces, 119–129 (2003)
[5] Paunov, C., Vickery, G. http://www.oecd.org/dataoecd/37/19/36736056.pdf (April 18, 2006), http://www.oecd.org/dataoecd/37/19/36736056.pdf (accessed September 20, 2011)
[6] Sumanjeet, S.: Emergence of Payment Systems in the Age of Electronic Commerce: the State of Art. Global Journal of International Business Research, 17–36 (2009)
[7] Turban, E., Lee, J.K., King, D., Liang, T.P., Turban, D.: Electronic Commerce: Managerial Perspective 2010. Prentice Hall (2010)

[8] Xiao, H., Christianson, B., Zhang, Y.: A Purchase Protocol with Live Cardholder Authentication for Online Payment. In: The Fourth International Conference on Information Assurance and Security (2008)
[9] Bellare, M., Garay, J.A., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G., Herreweghen, E.V., Waidner: Design, Implementation and Deployment of the iKP Secure Electronic Payment System. IEEE Jurnal of Selected Areas in Communication 18(4) (April 2000)
[10] Hall, J., Kilbank, S., Barbeau, M., Kranakis, E.: WPP: A Secure Payment Protocol for Supporting Credit Card Transaction Over Wireless Network. In: IEEE International Conference on Telecommunications (ICT), Bucharest, Romania (2001)
[11] Fourati, A., Ayed, H.K.B., Kamoun, F., Benzekri, A.: A SET Base Approach to Secure the Payment in Mobile Commerce. In: 27th Annual IEEE Conference on Local Computer Networks, Tampa, Florida (2002)
[12] Ford, W.: Secure Electronic Commerce; Building the Infrastructure for Digital Signatures and Encryption, 2nd edn. Prentice Hall (2001)
[13] Paulson, L.C.: Verifying the SET Protocol: Overview. In: Abdallah, A.E., Ryan, P.Y.A., Schneider, S. (eds.) FASec 2002. LNCS, vol. 2629, pp. 4–14. Springer, Heidelberg (2003)
[14] Knospe, H., Schwiderski-Grosche, S.: Online Payment for Access to Heterogeneous Mobile Networks. In: IST Mobile and Wireless Telecommunication Summit, Thesaloniki, Greece (2002)
[15] Li, Y., Zhang, X.: Securing Credit Card Transaction with One-Time Payment Scheme. Electronic Commerce Research and Application, 413–426 (2005)
[16] Kaol, W.-C., Fang, C.-Y., Chen, Y.-Y., Shen, M.-H., Wong, J.: Integrating Flexible Electrophoretic and One-Time Password Generator in Smart Cards. IEEE (2008)
[17] Li, Y.: The Design of the Secure Payments Systems Based on SET Protocol. In: International Conference on Computer Science and Information Technology (2008)
[18] http://www.ibonus.net, http://www.ibonus.net/web/home/ (2011), http://www.ibonus.net (accessed September 11, 2011)
[19] MTN, http://www.mtn.com.gh/NewsArtDetails.aspx?AID=112&ID&CID=38&MID=11&FirstParentID=1 (2009), http://www.mtn.com.gh (accessed September 11, 2011)
[20] http://www.authorize.net, http://www.authorize.net/resources/howitworksdiagram/ (2011), http://www.authorize.net (accessed September 23, 2011)
[21] http://www.bog.gov.gh, http://www.bog.gov.gh/index1.php?linkid=183&adate=28/01/2008&archiveid=1102&page=1 (Febuary 2008), http://www.bog.gov.gh (accessed September 23, 2011)