End-To-End Architecture for E-commerce Security

Houssam El Ismaili [1], Hanane Houmani [2], Adil Lebbat [3]

Architecture of SystemsTeam - ENSEM, Hassan II University, Casablanca - Morocco

(1) houssamelismaili@gmail.com

(2) h.houmani@ensem.ac.ma

(3) adil.lebbat@gmail.com

ABSTRACT

Business-to-consumer electronic commerce (e-commerce), one form of which is Web-based shopping, is defined as electronic-based economic transactions conducted between individual consumers and organizations. While this form of ecommerce is forecasted to grow rapidly for the foreseeable future, it still represents only a small fraction of total consumer spending. To better take advantage and be prepared for this economic phenomenon, organizations need to identify and understand factors that may impact consumers' decisions to engage in Web-based e-commerce.

Recently, the importance of E-commerce security has been discussed in both the academic and practitioner press. The impact of security on the use of e-commerce has been established empirically. The research reported here builds on the electronic payment security, we will study the security of e-commerce protocols in order to correct their faults and propose new protocols. In addition, we will propose a new architecture to ensure security of end-to-end electronic payment transactions regardless of the protocol used.

KEYWORDS

Electronic commerce, Cryptographic protocols, Secure Socket Layer (SSL), Secure Electronic Transaction (SET), 3D-Secure, Payment Card Industry Data Security Standard (PCI-DSS)

1 INTRODUCTION

Broadly defined, electronic commerce can be viewed as "any form of economic activity conducted via electronic connections" [1]. There are several forms of electronic commerce, such as business-to-business, business-to-consumer, or government-to-constituent. The focus of this research is electronic payment security of retail goods and services over the Web, an area of business-to-consumer electronic commerce [2].

Many people see the model showing how the business will be orchestrated in the future on the Internet. But before this becomes possible, the user should be reassured about the safety of financial information's and credit cards sent through the Internet. It is now possible to insert and steal confidential information for illegal or improper use without the awareness of the owner of the card.

Regional statistics reinforce the growth story. EMarketer—which publishes analysis and insight on digital marketing and commerce—projects those U.S. online shoppers spends $224.2 billion in 2012 which is higher by 15.4% than that of $194.3 billion in 2011. Latin America has recorded a 24% increase in online sales in 2010. Africa and the Middle East are also recording rapid growth in Internet users which is projected to rise from 150 million in 2009 to 297 million in 2015. Annual e-commerce revenues in Australia are on track to nearly double from $16.9 billion in 2009 to $33.9 billion in 2015. In Asia-Pacific, online retail markets are growing faster than U.S. and Europe that is driven in part by consumers' adoption of mobile shopping [3].

"Where there is smoke, there is fire". And where there is money being made, you can be sure that online predators will swarm. Therefore, it is not surprising that revenue losses from fraudulent e-commerce transactions have risen in parallel with e-commerce sales by more than double in the last decade. In its 2012 Online Fraud Report, CyberSource noted that fraud losses in North America raised from $1.7 billion in 2001 to a peak of $4 billion in 2009 then experienced a two-year decline, and then resumed an upward trend. In 2011, e-commerce fraud losses totaled approximately $3.4 billion, a $700 million increase over 2010[3].

These direct financial losses are largely borne by the merchant or card issuer and take two forms:

- Credits or reversals issued by the e-commerce merchant to consumers who claim fraudulent use of their accounts.

ISBN: 978-0-9853483-6-6 ©2013 SDIWC

- Chargebacks by card issuers who (depending on the circumstances) return fraudulent transactions to the merchant bank or the ecommerce merchant as a financial liability.

These losses are typically caused by security problems.

2 RELATED WORK

There have been many studies of E-commerce security. Security in E-commerce was described in the paper written by Dhilon [4] who introduce the stages to be provided for online purchase, the approach is based on encryption and compression for making information unreadable. However, E-commerce security has become a consistent and growing problem as new internet technologies and application are developed; it needs new architecture to adapt to many changes. Al-SLamy [5] described the role of Pretty Good Privacy (PGP) to provide confidentiality, authentication, compression and segmentation services for E-commerce security.

Currently, e-commerce security measures are summarized in the use of cryptographic protocols [6,7,8,9,10,11,12,13,14,15]. These protocols allow using cryptography to send confidential information on the Internet without being readable to malicious individuals. However, it turned out that these protocols are not as secure as we thought they would be. Indeed, several errors were discovered in cryptographic protocols after some years of use. The consequences that can generate vulnerability in a cryptographic protocol can be costly and irreversible for companies and individuals. Thus, the need to study the security of these protocols and correct errors is unquestionable.

Secure Sockets Layer (SSL) is a commonly used protocol used to encrypt messages between web browsers and web servers [16]. It encrypts the datagrams of the Transport Layer protocols. SSL is also widely used by merchants to protect the consumer's information during transmission, such as credit card numbers and other sensitive information. SSL is used to provide security and data integrity over the Internet and thus plays an important role. SSL has now become part of Transport Layer Security (TLS), which is an overall security protocol. One of the major problems of SSL is that the merchant can store the sensitive information of the cardholder, and the protocol does not prevent the non repudiation because the client authentication is optional.

SET (Secure Electronic Transaction) come to resolve the weakness of SSL in authentication and protection of sensitive information, SET ensures payment integrity, confidentiality and authentication of merchants and cardholders [17]. But SET is characterized by the complexity and the cost supported by the merchant (compared to the alternative proposed by SSL) because of the logistics of certificates distributing and client software installation, also it's difficult to manage non-repudiation. To deal with it, VISA introduce 3D-secure [18], this protocol is based on the introduction of additional control when buying online in addition to the classic sensitive cardholder data. The customer will validate the payment in new window by entering a secret data agreed with its own bank (password, date of birth, code received by SMS or generated by a personal drive).

There is no model in the literature or architecture that can enable a secure end-to-end transaction. If hackers get the access for a client's computer and install malicious software like Key logger, they can capture confidential information of a cardholder. Similarly there are E-merchants who continue to use revoked and invalid certificates. In this case, the client browser cannot detect such problems when the automatic update of security certificate is disabled, which may lead to a situation of fraud. Bearing this in mind, we propose a new architecture which we believe will be a possible solution to detect e-commerce fraud. Therefore, before starting to explain the proposed solution, we will define the terminology and basic concepts of e-commerce and security.

3 E-COMMERCE ACTORS

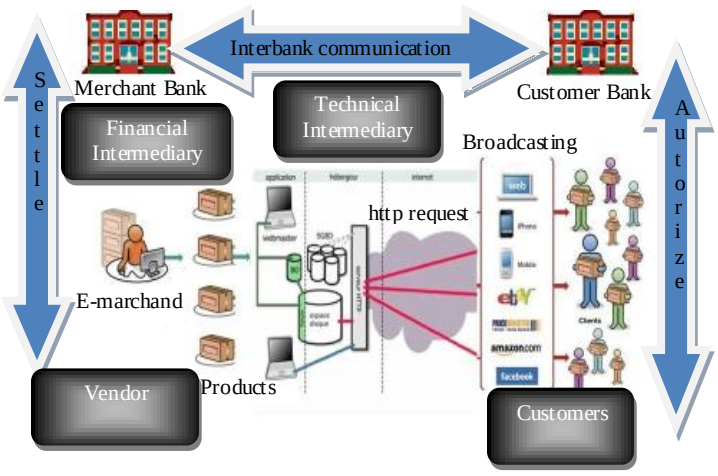

Fig. 1 Schema of E-commerce actors

ISBN: 978-0-9853483-6-6 ©2013 SDIWC

• The customer: can be a person or a company wishing to order a product or service. As a component of e-commerce, it is the target of threats. He/she must be careful to be on the right server and select what he/she wants with the right price. That is why it is important that the vendor must reassure the security of the transaction to the customer.
• The vendor: is usually a company that manages the website "Catalogue" and its security, setup a system of client identification, handle requests and send items bought to customers and find a way to get the cash. Vendors for catalogue management may involve a technical intermediary. They will also deal with potential malicious customers who don't pay or refuse the transaction while keeping the goods delivered (repudiation). To avoid such problems, the vendor may also choose to use the services of a financial intermediary to collect the money generated by the sale.

E-commerce actors are subject to various threats. The effect of these threats is evident: compromising the availability, integrity or confidentiality of e-commerce transaction.

4 SECURITY RISK MANAGEMENT

Risk management consists of four phases [19] assessments, planning, implementation and monitoring. In the assessment phase of risk management, organizations evaluate their security risks by determining their assets, threats, and vulnerabilities. The second phase, planning, focuses on security policies by defining which threats are tolerable and which are not. A threat is tolerable if the cost to safeguard the threat is too high or the risk is too low. In the implementation phase, technology is chosen to prevent high priority threats. The monitoring phase is ongoing and usually determines if the chosen tactics were successful or not.

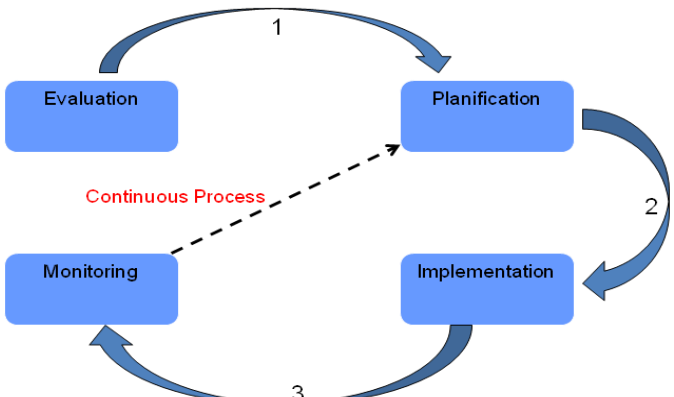

Fig. 2 Risk management flowchart

4.1 Physical protection

It is essential to think about security at the physical level. In this area we should consider several points:

- Monitoring of computers containing confidential information (use a surveillance company).
- Risk of fire or catastrophe (have a backup system).

4.2 Server protection

- The operating system of the server must be properly installed and configured.
- Good management of server users, management of process and file systems.
- Install the Web server on a machine different from other servers (mail ...) to avoid vulnerabilities associated with these services.
- Have a daily backup of all actions on the server.

4.3 Network protection

- The use of a firewall is very essential.
- Think about a network architecture that will protect the areas which have sensitive information. If a hacker enters to the network make he /she lose time, so that you can to identify and prevent this attack.
- Data writing will only take place from the inside to the outside and never vice versa.

4.4 Application protection

- Checking data integrity (using file signatures).
- The separation of the various users working on the server (server administrator, designer of pages, etc.).
- Logging client's connections. (In case of fraud we can go back to the hacker).Be careful to programs and scripts run on the server side (CGI).
- Use of client authentication system.

ISBN: 978-0-9853483-6-6 ©2013 SDIWC

5 END-TO-END ARCHITECTURE

All E-commerce security solutions don't treat the problem from beginning to end. There are protocols for secure transfer other than authenticating communicating entities. We also discuss about actions to secure the network or the client computer and precautions to protect sensitive data of cardholders. Security in E-commerce is not treated in its entirety. A purchase transaction is secure if it can allocate all the mechanisms of protection against threats throughout its life cycle. A transaction is born at the client or the client browser when a cardholder wishes to make a payment on a website, so the operation must be protected from the origin, and then protect the transfer of sensitive data (Pan, expiration date, CVV2) between the client and the merchant, and between the merchant and the customer's bank. Another important aspect of security is the protection of sensitive data among card issuers to avoid internal fraud (banks for example). An example of a security is encryption of database that contains card numbers.

The proposed architecture is designed with the intention to implement the necessary measures to secure a transaction from beginning to end. The model uses other protocols such as SET and 3D-Secure with some improvements that will be explained in the following paragraphs.

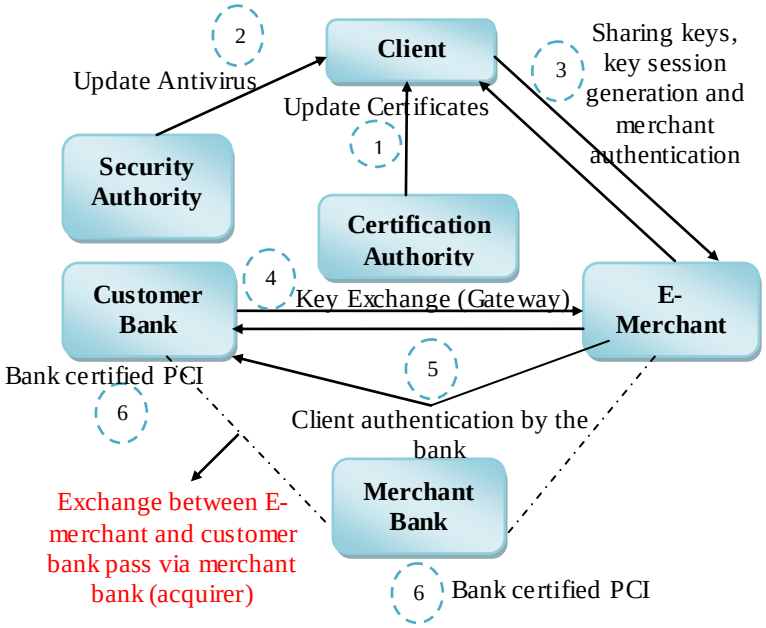

Fig. 3 End to End Architecture

5.1 Client side security

If hackers access the client computer and install malicious software like Keylogger for example, they can capture cardholder confidential information. Similarly there are E-merchants who continue to use revoked and invalid certificates. In this case, the client browser cannot detect such problems when the automatic update of security certificate is disabled, which may lead to a situation of fraud. The update program communicates with certification authorities to update the status of certificates and add new ones. To encrypt sensitive data, client browsers use protocols such as 3DES, RSA, SHA-1 ... The type and size of the keys may change, and browsers must be aware that this feature can be disabled. The establishment of a system of protection against threats on client side, forcing the update of certificates and encryption protocols, minimize fraud and improve trust between the E-merchant and the customer.

5.2 Transfer security

To ensure the confidentiality, integrity and authentication, the model uses the same approach as SET but client authentication without security certificates. Authentication is similar to the 3D-Secure authentication (password, token...). The model avoids the complexity of deploying SET because it is not easy to give each client a certificate rather it will be easier to assign a password or a temporary token that the client can present to authenticate with its issuing bank. And in order to authenticate the client, the merchant must be able to redirect the client request to the url of the issuer bank. Unlike 3D-Secure which redirect the request to VISA that supports this feature, it is the merchant who will undertake this task by extracting the first six digits of the card (bin), and then the merchant retrieves the url of the customer bank from the table bin/url. This table can be powered by VISA, MasterCard or other organizations. In order that the merchant can retrieve the first six digits of the card number, we will not encrypt all the digits in the secure exchange between the customer and the merchant, just the masked part 678912******6482 which will be encrypted according to the standard PCI. One of the major problems of the 3D-Secure authentication is phishing. To remedy this issue the model uses mutual authentication between the client and the bank. On the authentication page of the bank, the bank must be authenticated by displaying such a

ISBN: 978-0-9853483-6-6 ©2013 SDIWC

secret code known only by the customer and the bank, and then the client can enter his personal secret code.

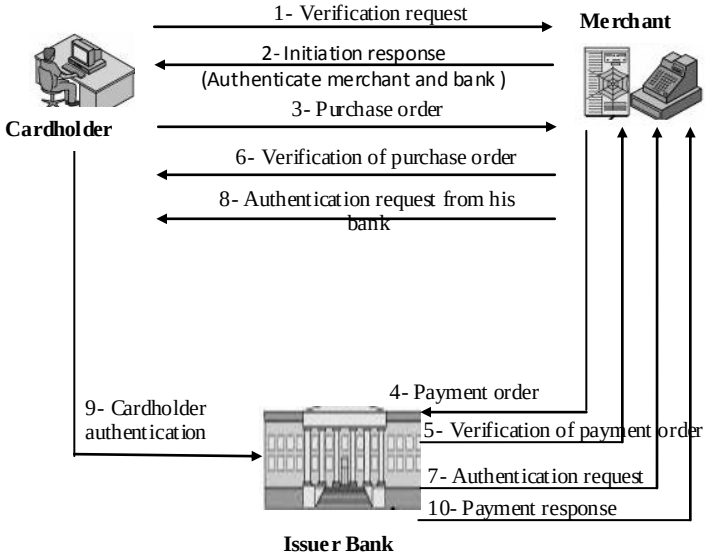

Fig. 4 Transfer diagram

- Initialization request: Before starting purchase the cardholder and the merchant agree upon the order description amount. Then the cardholder sends to the merchant his local ID and a fresh random challenge (Step 1). The purpose of step 2 is to give the cardholder with the merchant's signature certificate and the issuer bank encryption certificate.

=> Authenticate the merchant and the bank

⇨ Purchase request: After validating both certificates, the cardholder sends the purchase request which contains the payment order, order information and the dual signature (Step 3). The payment order is encrypted under the issuer bank key, then payment order and information order are encrypted under the merchant key, The merchant validates the order information .If the validation is successful, then the merchant sends the payment order encrypted to the issuer bank (Step 4), then the issuer bank sends the response (Step 5) to the merchant, the merchant sends the response to the cardholder (Step 6). If the verification if ok then the cardholder is requested to be authenticated (Step 7, 8).

⇨ Confidentiality by using double encryption(merchant and issuer bank certificates)

⇨ Integrity by using dual signature

⇨ Authenticate the card by the issuer

⇨ The merchant is not in the possession of the credit card number

⇨ In order to authenticate the cardholder, the request is sent directly to the issuer bank basing on his first six digits of credit card number.

- Cardholder authentication: The cardholder will be redirected to the issuer bank site to enter his confidential code (Step 9). The issuer validates the code and sends the final payment response to the merchant (Step 10).

⇨ Authenticate the cardholder, Possibility of mutual authentication (phishing)

5.3 Card issuers security

To protect cardholder's sensitive data against malicious users of the issuer company, it is imperative that these companies have security mechanisms for these data. PCI-DSS (Payment Card Industry Data Security Standard) have been developed in order to enhance the security of cardholder data and facilitate the adoption of uniform safety rules. The trace files and logs may contain cardholder confidential information's, the database bank contains key authentication, so encryption, rights management and access monitoring are mandatory to prevent fraud.

5.4 End-To-End architecture advantages

Here is a summary of the advantages of End-To-End Architecture:

Client side security	Transfer security	Card issuers security
- Protection of cardholder sensitive information at client side - Forcing the update of certificates and encryption protocols	- Authentication of cardholder, merchant and issuer bank - Integrity by using dual signature - Confidentiality - Simplicity of the payment process - Reduction of the logistics and the cost of implementation (compared to SET and 3D-Secure)	- Encryption of trace files and logs - Encryption of bank database - Management of server access - Respecting the PCI Standard

Tab. 1 EE Architecture advantages

ISBN: 978-0-9853483-6-6 ©2013 SDIWC

5.5 End-to-End architecture Vs SSL, SET and 3D-Secure

Find bellow the comparison between the proposed solution and the other protocols of E-commerce security:

	SSL	SET	3D-Secure	E-E-Architecture
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Authentication	Optional for client	Yes	Yes	Yes
Merchant doesn't store sensitive data	No	Yes	Yes	Yes
Non-Repudiation	No	Yes but Complicated	Yes	Yes
Non-Revocation	No	No	No	Yes
Protection of sensitive data on departure	No	No	No	Yes
Protection of sensitive data on arrival	No	No	No	Yes
Payment responsibility	Merchant or bank	Cardholder or bank	Cardholder	Cardholder
Complexity	Low	High	High	Low
Cost	Low	High	High	Low

Tab. 2 EE Architecture Vs SSL, SET and 3D-Secure

6 CONCULUSION

To create a trustworthy environment between buyers and sellers on the Internet is one of the major problems to be solved. Implementation of security mechanisms distributed on different nodes of the E-Commerce chain, i.e., authentication of participants, data encryption and hash provide high security for the online purchase. If the problem of security is solved from beginning to end, more people will buy online and E-commerce will be pushed a huge step forward. It is in this sense that we propose a new architecture for secure end to end e-commerce transaction. In the future works, we will show how we can benefit from multi-agent systems to improve the architecture and consolidate the security of e-commerce. In addition, we will give formal specification improvements of SET protocol. With this specification we can analyze the new protocol to provide formal proofs for the security of the new protocol.

7 REFERENCES

[1] R.T. Wigand, (1997). "Electronic commerce: Definition, theory, and context," The Information Society: An International Journal, Vol. 13, No. 1, pp. 1-16.

[2] C.Van Slyke, F. Belnger and C. Comunale Factors Influencing the Adoption of Web-Based Shopping: The Impact of Trust .

[3] RSA http://www.rsa.com/products/EDS/whitepapers/

[4] G. Dhillon and J. Ohri , Optimizing Security in E-commerce through Implementation of Hybrid Technologies

[5] A. Al-Slamy, E-Commerce security.

[6] J. Clark and J. Jacob. A survey of authentication protocol literature.

[7] V. Cortier, S. Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. J. Comput. Secur., 14(1):1–43, January 2006.

[8] V. Cortier, Steve Kremer, and Bogdan Warinschi. A survey of symbolic methods in computational analysis of cryptographic systems. J. Autom. Reason., 46(3-4):225–259, April 2011.

[9] S. Escobar, C. Meadows, and Jos´e Meseguer. A rewriting- based inference system for the nrl protocol analyzer: grammar generation. In Proceedings of the 2005 ACM workshop on Formal methods in security engineering, FMSE '05, pages 1–12, New York, NY, USA, 2005. ACM.

[10] R. Kemmerer, C. Meadows, and J. Millen. Three Systems for Crypto- graphic Protocol Analysis. Journal of Cryptology, 7(2):79–130, 1994.

[11] P. Lafourcade, V. Terrade, and S. Vigier. Comparison of cryptographic verification tools dealing with algebraic properties. In Pro- ceedings of the 6th international conference on Formal Aspects in Security and Trust, FAST'09, pages 173–185, Berlin, Heidelberg, 2010. Springer- Verlag.

[12] A. Liebl. Authentication in distributed systems: A bibliography. Operating Systems Review, 27(4):122–136, October 1993.

[13] G. Lowe. Towards a completeness result for model checking of security protocols. In Proceedings of 11th IEEE Computer Security Foundations Workshop, pages 96–108, 1998.

[14] C. Meadows. The NRL Protocol Analyzer: An Overview. Journal of Logic Programming, 1994.

[15] C. Meadows. What makes a cryptographic protocol secure? In Proceedings of ESOP 03. Springer-Verlag, April

2003.
[16] A.Craft, R. Kakar, E-Commer Security
[17] H.Houmani, M.Mejri, Formal Analysis of SET and NSL Protocols Using the Interpretation Functions-based Method
[18] GPayments, VISA 3-D Secure vs. MasterCard SPA, www.gpayments.com
[19] B. Gehling and D. Stankard, eCommerce security