ENFORCING SET AND SSL PROTOCOLS IN E-PAYMENT

Nancy Awadallah

Department of Computer and Information Systems, Sadat Academy for Management Sciences, Egypt

ABSTRACT

The main incentive for the use of electronic commerce (E-commerce) and spread on a large scale is that most of business activities need payment system. As E-commerce requires an efficient payment system which is stable and secure for supporting electronically commerce. This paper proposed to enforce SET, SSL protocols for encrypting e-payment information. It also presented several methods to take under consideration to avoid fraud and keep our site safe.

KEYWORDS

E-commerce, E-payment, Security risks, SET, SSL.

1. INTRODUCTION

E-payment process is essential issue to electronic transactions. The e-commerce picture is not complete without successful e-payment steps.

Fraud amount in e-payment has increased and become major concern for web clients [16].

The security requirements for e-payment or e-commerce in general, such as message privacy, message integrity, authentication, authorization, non - repudiation, and secure payment [17].

Authentication and Security in E-commerce should not be inflicting harm of users' privacy [18].

Personal information should be protected which involved in all steps of a payment on the Internet. The banking industry strategy is centered on identity spoofing and user authentication.

In E-commerce, the information travels via the most popular E-commerce transactions secure protocols SSL and SET [19] as discuss in section 4.

2. LITERATURE REVIEW

Authentication and a secure connection between the client and the service provider website are considered the beginning point for any service online via using a protocol such as SSL (Secure Socket layer).

A. Kr. Luhach ,S. K. Dwivedi et C. K. Jha , discussed the using E-commerce with SOA and it's importance and defines the problems in the existing security of E-commerce platforms. They also suggested a design of SOA security framework for supported E-commerce system [2].

DOI:10.5121/ijcsit.2017.9210

Y. Jing , proposed a 3D model framework for e-commerce security system structure and presented variety of countermeasures to solve e-commerce security problems such as : security strategy , legal protection , social moral norms , perfect management strategy[3] .

Eric W.K et al, used six design attributes defined by a group of specialists and E-payment service users using the Delphi method, an online conjoint experiment is conducted [4].

A.Takyi, P. O. Gyaase, developed a model of a protocol which ensures convenience ,security, verification of merchant ,cardholder authentication, and requires authentication from the cardholder. Cardholder, issuer, merchant, and acquirer are considered into account [5].

M. Z. Ashrafi and S. K. Ng ,proposed a preserving e-payment scheme that ensure authenticity while keeping the customer's sensitive details secret from the respective parties involved in the online transaction [14].

A. Plateaux et al ,proposed a detailed description and an analysis of the 3D-Secure protocol, through a new privacy-orienting model for e-payment architectures.

Z. Chen , said that it's important to understand the e-commerce platform, integrate network technology which is applied in the application of electronic commerce, the technology, knowledge, management and human resources in one [24].

3. ONLINE PAYMENT SYSTEMS AND PROCESS

E-payment process including security issues such as verification, identification, and authentication with different and competing interests.

- **Account-Based**

Credit Cards: once using the cardholder's name, credit card number and expiry dates are done the Authentication is done.
Fraudsters could use this information [9][10].

Debit Card: value of online transaction is discounted immediately to the cardholder's bank account [9].

Mediating Systems: PayPal payment is a mediating service for online transactions.

Mobile Payment Systems: are represented by wireless devices. [11].

Online Banking: Electronic bill will enter customer payment details are automatically and the payer only authorizes.

- **Electronic Currency Systems**

It includes smart cards and online cash systems [10][12][20].

3.1 E-Payment Process

No business can be found without a payment system. The famous form of B2C payment is accepting credit cards over the Internet. Physical world paying for goods and services is moving to mobile devices.

3.1.1 The process for accepting credit card payments

Users' credit- and debit-card information are stored in PayPal servers [1].

3.1.2 Receiving Payments Using PayPal

The payment process is a transformation process as it converts the "commerce" concept into "e-commerce." A payment processor and gateway are two kinds of payment systems that customer should consider for website:

Payment processors, such as PayPal will send a customer to a checkout page that is hosted by the processing company. But, payment gateways, such as Authorize.net integrate directly with site shopping cart and the transaction is invisible to the customer.

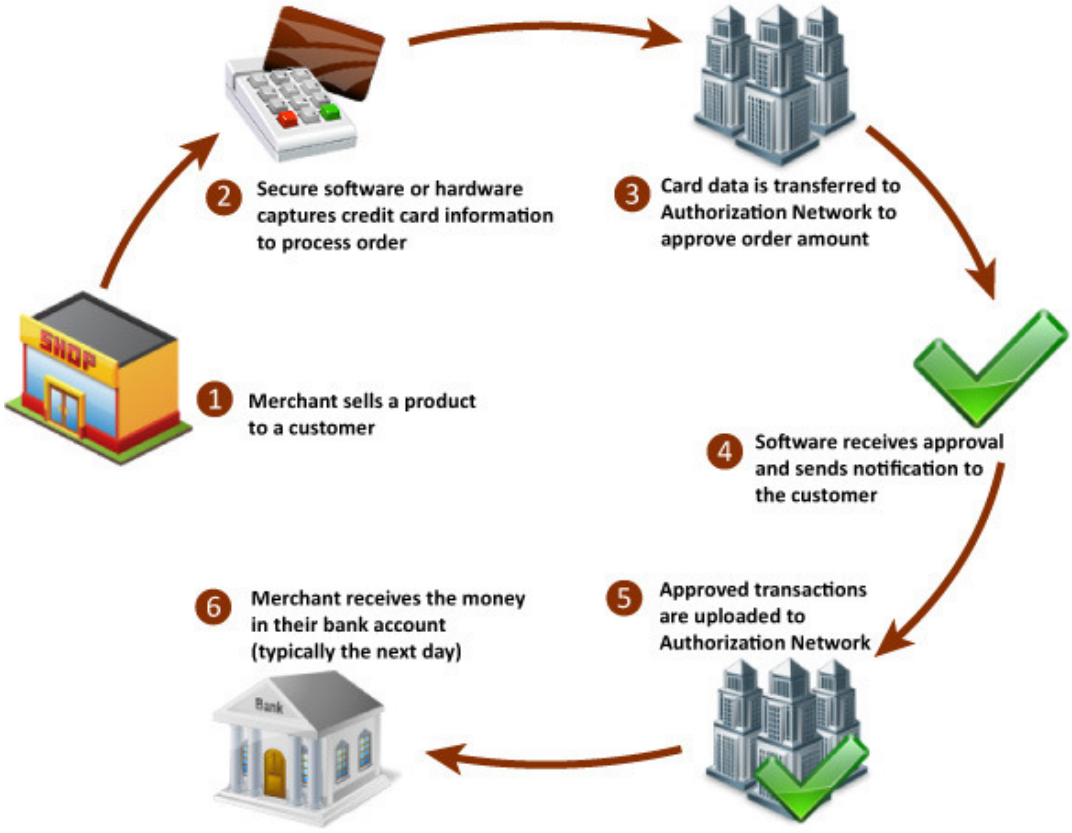

Figure 1. Online credit card transaction

4. E-PAYMENT SYSTEM REQUIREMENTS

Personal data involved in online payment must be protected against threats.
The personal information is divided in three parts, the first one is the identity information which includes the information about the client's identity, the second one is the information includes the detailed data linked to the expected service, the third part is banking information which includes client's the personal account number and bank name [15].

There are requirements should be taken into account in the e-payment system:

- The confidentiality of transactions
- The integrity of transmitted information
- The confidentiality of client's identity towards the Service Provider
- The client's authentication
- The banks authentication
- The non-reusability
- The confidentiality of order information
- The confidentiality of banking information [15]

In table 1., we introduce definitions of dimensions risks of using the E-payment service .

Table 1. E-payment service dimensions risks [4]

Dimension of perceived risk	Definition
Privacy	E-payment usage may exposes to customer identity theft.
Time	Losses to time, and effort caused by wasting time setting up purchasing and researching.
Performance	Performance problems, that cause the E-payment service to not perform as expected.
Financial	potential Internet fraud due to financial losses because of

4.1 Security Risks in Mobile Devices

Computers are considered tool to attack information systems, it's growing rapidly and becoming dangerous.

Mobile devices security concerns are:

- Identity theft is represented by (30%)
- Downloading malicious applications are represented by (33%);
- Data theft from the device are represented by (44%);
- Mobile devices infected by malware (60%)
- Loss of devices that include sensitive information (66%) [23].

Cyberwarefare refers to The attack usually is done through viruses, DoS, or botnets.

• Cyberwarfare, includes threats: Online acts of spy and security breaches .

• Sabotage, which means using the Internet to prevent online communications to cause damage.

5. E-COMMERCE SECURITY PROTOCOLS

SMS is vulnerable to snooping, spoofing, message interception, and social-engineering based bypasses of security measures these technologies used have weak security.

5.1 SET: Secure Electronic Transactions

SET is a protocol used to secure payment transactions and authenticate the parties involved in the transaction. It provides confidentiality of the information as using cryptography and digital certificates for ensuring of payment integrity, and authenticates cardholders, banks and merchants, so it achieves the trust needed for consumers.

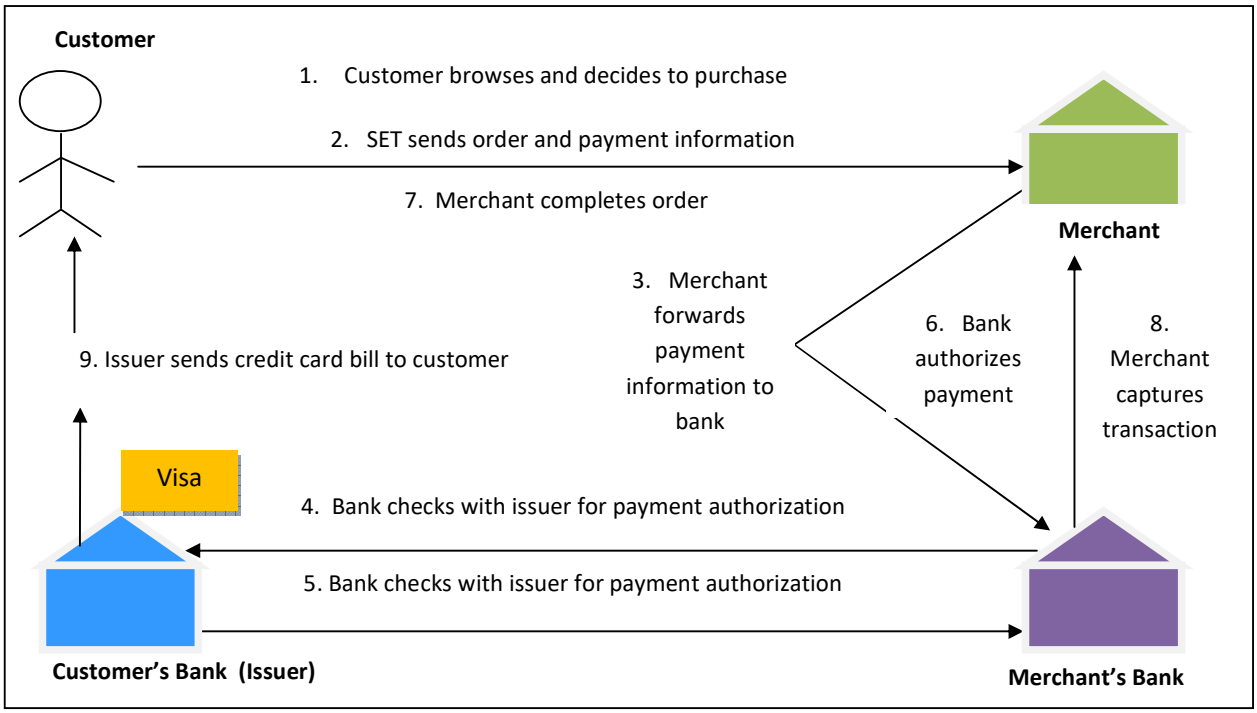

Figure 2. Secure Electronic Transactions

5.1.1 SET Protocol for Encrypting Payment Information

According to step 2: "Encrypted payment info ", in this section we will process this step in programming way using PHP tool.

The Mcrypt module is one of the easiest solutions that allows high-grade encryption, add-in for PHP. The Mcrypt library ensures that only users can decrypt data.

The following Mcrypt functions that use to encrypt and decrypt data:

```
<?php
$desc = "Stuff you want encrypted";
$k = "Secret passphrase used to encrypt your data";
$cp = "MCRYPT_SERPENT_256";
$md = "MCRYPT_MODE_CBC";
function encrypt($desc, $k, $cp, $md) {
// Data Encryption
return (string)
          base64_encode
             (
             mcrypt_encrypt
                (
                $cp,
                substr(md5($k),0,mcrypt_get_key_size($cp, $md)),
                $desc,
                $md,
                substr(md5($k),0,mcrypt_get_block_size($cp, $md))
                )
             );
}
function decrypt($desc, $k, $cp, $md) {
// Data Decryption
   return (string)
          mcrypt_decrypt
             (
             $-cp,
             substr(md5($k),0,mcrypt_get_key_size($cp, $md)),
             base64_decode($desc),
             $mode-md,
             substr(md5($k),0,mcrypt_get_block_size($cp, $md))
             );
}
?>
```

Information which be required by mcrypt() function :

- Encrypted data (desc).
- The key (k) used to unlock and encrypt customer data.
- The cipher (cp) used for data encryption.
- The mode (md) used to encrypt the data.

In the case of user data and user passphrase are stolen, they can search the ciphers until finding the correct one. using the md5() function on the key before we use it is considered the additional , as in case of having both passphrase and data ,the intruder won't get what they want.

5.2 SSL : Secure Socket Layer

This protocol using a combination of public - private key cryptography and digital certificate [13] so it provides communications privacy over the Internet. SSL provides a private between the server and the client.

A handshake between the cardholder's browser and the merchant server has a role in the encryption process of the information transmitted by the cardholder [7] [8].

Figure 3 shows transferring sensitive data over the internet via SSL connection in order to,only the server is authenticated using a digital certificate.

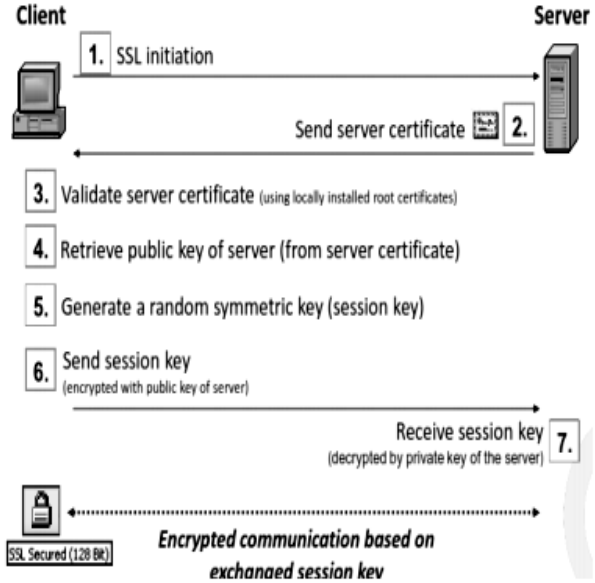

Figure 3. SSL Secured Connection Steps [25]

5.2.1 SSL Protocol for Securing Data

We need to force the web pages with sensitive data to be accessed through SSL as it's important to use it for securing the data that passes between the server and the client's browser. In case for example, if customer tried to access the next link http://localhost/mobileshop/credit-card-details/ , the customer should be redirected to **https**://localhost/mobileshop/credit-card-details/
At the same time, enforcing SSL protocol will not needed in all places of the site, and because that makes web pages invisible to search engines and reduces performance.
We want to make sure that the, customer logout, customer registration, and modification pages detail of customer are accessible only via SSL.
To redirect the page to https page to be secured, the next example processes this issue. (the code is written by php language).

In the customer page which be filled with (his/ her) data, we will add the next method to code:

```
// Page with Sensitive Data

private function _IsSensitivePage()
{
if (isset($_GET['Cust_Register'])
isset($_GET['Cust_Account'])
isset($_GET['Cust_CreditCard'])
isset($_GET['Cust_Address'])
isset($_GET['Cust_Checkout'])
isset($_POST['Cust _Login']))
return true;
```

```
return false;}
```

In the __constructor() method , we add the next code :

```
 // Class constructor
                        public function __construct()
{
$is_https = false;
// Is the page being accessed through an HTTPS connection?
if (getenv('HTTPS') == 'on')
$is_https = true;
```

```
// Use HTTPS when accessing sensitive pages
if ($this->_IsSensitivePage() && $is_https == false && USE_SSL != 'no')
{
$redirect_to =
Link::Build(str_replace(VIRTUAL_LOCATION, '', getenv('REQUEST_URI')),
'https');
header ('Location: '. $redirect_to);
exit();
}
// Don't use HTTPS for non-sensitive pages
if (!$this->_IsSensitivePage() && $is_https == true)
{
$redirect_to =
Link::Build(str_replace(VIRTUAL_LOCATION, '', getenv('REQUEST_URI')));
header ('Location: '. $redirect_to);
exit();
}
$this->mSiteUrl = Link::Build('');
}
```

After this addition, load http://localhost/mobileshop/credit-card-details/
will redirect us to **https**://localhost/mobileshop/credit-card-details/ .

6. METHODS TO PROTECT E-COMMERCE SITE FROM FRAUD AND HACKING

The potential risk which be executed by hackers are Stealing credit card and other sensitive information from E-commerce sites. To reassure and protect the e-commerce site's users, it's necessary to know how to protect sensitive customer data. The next table (table 2) describes different methods to how we can prevent fraud and keep our site safe.

7. CONCLUSION

SET and SSL are the major common Ecommerce security protocols. Each protocol has its use, its own encryption mechanism, its strategy and its products. In this paper, author discussed the two protocol and how we can use PHP programming to encrypt e-payment information and secure sensitive data.

At the same time it is not an easy to take a rule for using sensitive data via internet, (sensitive data is represented in any private information such as credit card number, passwords. So in this paper, author also introduced several methods to take under consideration to avoid fraud and keep our site safe.

Table 2. Methods to protect E-commerce site

Method	Description
For online checkout ,use a secure connection (as explained in section 5.2)	Use SSL authentication for data protection. We use a payment gateway to validate credit cards that uses live address verification services right on our checkout.
Sensitive data shouldn't store	Don't store a huge amount of records on your customers.
Require strong passwords	Requiring the use of symbols or numbers and a minimum number of characters from customers.
Using system alerts for suspicious activity	Using an alert notification for any up normal transactions coming through from the same IP address.
Make a Layer for security	To keep your business safe from any criminals is layering the security. It is possible to add website layers of security and applications such as search queries, contact forms.
Patch your systems	Patch everything immediately.
Having a DDoS protection	With Distributed Denial of Service (DDoS) attacks increasing sophistication .E-commerce sites should deal with cloud-based DDoS protection .
A fraud management service should be considered	Companies of credit card offer fraud management and chargeback management services.

REFERENCES

[1] N. Leavitt,"Payment Applications Make E-Commerce Mobile ",IEEE Computer Society, 2010 .

[2] A. Kr. Luhach ,S. K. Dwivedi , C. K. Jha ," Designing a logical security framework for E-commerce system based on SOA" , International Journal on Soft Computing (IJSC) , Vol. 5, No. 2, 2014 .

[3] Y. Jing , "On-line Payment and Security of E-commerce " , Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09),China , pp. 046-050,2009 .

[4] E.W.K. See-To, K.K.W. Ho, "A study on the impact of design attributes on E-payment service utility ",Information & Management 53 pp. 668–681, 2016 .

[5] A.Takyi,P. O. Gyaase ,"Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce " , Springer-Verlag Berlin Heidelberg , pp. 232–239,2012 .

[6] Hall, J., Kilbank, S., Barbeau, M., Kranakis, E.: WPP," A Secure Payment Protocol for Supporting Credit Card Transaction Over Wireless Network", IEEE International Conference on Telecommunications (ICT), Bucharest ,Romania, 2001.

[7] 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.

[8] Li, Y.," The Design of the Secure Payments Systems Based on SET Protocol", International Conference on Computer Science and Information Technology, 2008.

[9] 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 .

[10] Turban, E., Lee, J.K., King, D., Liang, T.P., Turban, D.," Electronic Commerce: Managerial Perspective" 2010.Prentice Hall ,2010.

[11] Xiao, H., Christianson, B., Zhang, Y.," A Purchase Protocol with Live Cardholder Authentication for Online Payment.",The Fourth International Conference on Information Assurance and Security ,2008.

[12] 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) , 2000.

[13] J. Guitart ,D. Carrera, V.Beltran, J. Torres, E.Ayguade´," Designing an overload control strategy for secure e-commerce applications" , Computer Networks 51 , pp. 4492–4510, 2007.

[14] M. Z. Ashrafi , S. K. Ng , "Enabling Privacy-preserving e-payments using one-time payment details", Computer Standards & Interfaces 31 ,pp. 321–328, 2009.

[15] A. Plateaux ,P. Lacharme, V. Coquet, S. Vernois ,K. Murty ,C. Rosenberger , "An e-payment Architecture Ensuring a High Level of Privacy Protection" , Institute for Computer Sciences, Social Informatics and Telecommunications Engineering , pp. 305–322, 2013 .

[16] Espelid, Y., Netland, L.–H., Klingsheim, A.N., Hole, K.J.," A proof of concept attack against norwegian internet banking systems ", Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 197–201. Springer, Heidelberg ,2008 .

[17] W. Kou, "Payment Technologies for E-Commerce ", Springer, Verlag Berlin, Heidelberg, 2003.

[18] Katsikas, S.K., L´opez, J., Pernul, G.," Trust, privacy and security in E-business: Requirements and solutions ", In: Bozanis, P., Houstis, E.N. (eds.) PCI 2005. LNCS, vol. 3746, pp. 548–558. Springer, Heidelberg , 2005.

[19] S.E.T. Secure electronic transaction specification. Book 1: Business Description. Version, 1 (2002).

[20] W. Kou , "Introduction to E-Payment: An Essential Piece of the E-Commerce Puzzle" , Payment Technologies for E-Commerce, Springer-Verlag Berlin Heidelberg ,2003 .

[21] S. E. Fienberg ,"Privacy and Confidentiality in an e-Commerce World: Data Mining, Data Warehousing, Matching and Disclosure Limitation", Statistical Science, Vol. 21, No. 2, A Special Issue on Statistical Challenges and Opportunities in Electronic Commerce Research (May, 2006), pp. 143-154.

[22] W.Wop ,"Fraud Risks in E-commerce Transactions",The Geneva Papers on Risk and Insurance ,Vol. 27 No. 3, pp. 383-394, July 2002.

[23] Davis, M. A. ,"2012 Strategic Security Survey." Information Week , May 14, 2012.

[24] Z. Chen, "Research on Network Architecture of the E-commerce Platform and Optimization of the System Performance", The Open Cybernetics & Systemics Journal, pp. 2266-2271, 2015.

[25] N. Kawatra, V. Kumar , "Analysis of E-Commerce Security Protocols SSL and SET " , National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC), 2011.