ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0079 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

Privacy and Protection in Electronic Transaction: A Review of The E-Commerce Security Protocols

Taroub Ahmed Mustafa Sa'ed
Faculty of Technology and Applied Science
Al –Quds Open University
Palestine
tessa@qou.edu

***Abstract*—E-commerce applications are becoming popular day by day as they are working like a virtual shop. Writing good E-commerce application is tedious task and complex also. The applications if made complex are very difficult to maintain. Usability is a very basic concept in the E-commerce application. User has to get the information at one click and with proper feedback. As these are web based applications, efficiency matters a lot for this application. As transaction in e-commerce faces the problems such as database exploits, log data mining and sniffing attacks which can be resolved by using different security measure. Hence, security is important in e-commerce application. In today's electronic world of business, trust is the center component between the consumer and the internet Merchant. Researchers found trust very important, especially, in the relationships between consumers and e-vendors. Based on the analysis of the basic concepts, the security infrastructure and payment system of electronic commerce and the thorough and comprehensive research on the security technology, authentication and transaction process, this paper points out some aspects of excellence and deficiencies in security protocols beginning with iKP, SSL, SET, 3d-Secure and finally other modified models of 3d-secure protocols.**

Keywords: Electronic Commerce, SET, Sniffing Attack, Log Data Mining, DBMS exploit, DES, RSA, 3d-Secure, SSL.

I. Introduction

The internet is a network of networks. Connecting a business to the internet implies a global reach. In other words, a company can reach anyone who has an access to the internet such as customers, suppliers, on-line banks, mediators, etc. At the same time, the company can be reached by anyone. So, the internet creates vast opportunities for businesses with some threats. For example, anybody from anywhere on the internet (an intruder or a hacker) can illegally enter a company computer resource and messes the computer resource from a remote site. In addition, it is not difficult task to tap a message in the middle of the net and steal or change its content, which is definitely a crime. While the internet is dramatically changing the way business is conducted, security issues are of deeper concern than ever before. The internet is basically an insecure communication medium. Hawker [6] states that the only assumption which can safely be made when considering the internet as a communication medium is that it offers no security whatsoever. Most people are skeptical about the security of the internet. People are happy using the World Wide Web for browsing, finding, reading or downloading information from the internet. However, when considering sending a credit card number over the internet, they are reluctant to do it, even if they are told that the transfer is secured. This is because many media expose bad news about the internet security, although security technology for the internet exists and good enough for protecting transactions via the internet.
The core activities of e-commerce are business transactions between two parties or possibly mediated by a third party. In fact, the practice conducted by company before the term e-commerce appears is Electronic Data Interchange (EDI), which is basically electronic transaction via computer networks. The major concern of electronic transactions is how to protect transactions from eavesdroppers (which can steal and modify the information in the transactions) and how to make sure those transactions are authenticated.
This paper begins by outlining basic concepts in section 2, while section 3 deals with protocols in Electronic Transaction like SSL , SET and 3d-sercure protocols. Also other modified models of 3d-Secure will be discussed. Finally, the conclusion, discussion and references.

II. Basic Concepts

A. Security Issues in E-Commerce Application

E-commerce was established in 1991; it is selling and buying of products and services by business and consumers via computer network such as internet. From the year 1991 till today, life has faced drastic changes due to technological advancements, but simultaneously they have made our lives more complex. Moreover, E-Commerce became a need for development and modifying to protect the data and information from any attack, from here the definition of security in EC has emerged[4].

Electronic commerce lets companies integrate internal and external business processes through information and communication technologies. Companies conduct these business processes over intranets, extranets, and the internet. E-commerce lets businesses reduce costs, attain greater market reach, and develop closer partner relationships. However, using the internet as the underlying backbone network has led to new risks and concerns. Often, industry analysts considered trust and security as the main hurdles in growing e-commerce. A number of factors have hampered the growth of e-commerce in developing countries. Yet, the main perceived obstacle to increased internet usage is very similar in companies from both developed and developing countries. Firms already using the internet consider the lack of network security to be the primary problem, followed by slow and unstable connections. This litany of evolutionary phases masks a number of growing technical challenges, which could be addressed as the following[17][16]:

- security and authentication.
- content management and publication.
- reliable systems, messaging, and data.
- complex interactions and transactions.
- business model implementation and business process enactment.
- distributed processing and distributed data.

Clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce.[12].

There are different types of security issues in any e-commerce application which needs to be addressed as the following[1][11]:

1) Malicious Code such as Viruses.

2) Unwanted Programs: These are installed without the user's informed consent. It has three types:

- Browser parasites: It can monitor and change settings of a user's browser.
- Adware: It calls for unwanted pop-up ads.
- Spyware: It can be used to obtain information, such as a user's keystrokes, e-mail, IMs, etc.

3) Phishing and Identity Theft: which means that any deceptive, online attempt by a third party to obtain confidential information for financial gain – Most popular type: e-mail scam letter – It is one of fastest growing forms of e-commerce crime

4) Hacking and Cyber vandalism.

5) Credit Card Fraud.

6) Spoofing (Pharming) and Spam (Junk) Web Sites.

7) Denial of service (DoS) attack and Distributed denial of service (DDoS) attack.

8) Other Security Threats: like:

- Sniffing: Type of eavesdropping program that monitors information travelling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs: Single largest financial threat.
- Poorly designed server and client software: Increase in complexity of software programs has contributed to increase is vulnerabilities that hackers can exploit.

B. Mechanisms and Technologies to Build Trust

Trust is especially an important factor under conditions of uncertainty and risk. The importance of trust is elevated in e-commerce because of the high degree of uncertainty and risk present in most on line transactions. In today's electronic world of business, trust is the center component between the consumer and the internet Merchant. Researchers found trust very important, especially, in the relationships between consumers and e-vendors[17].

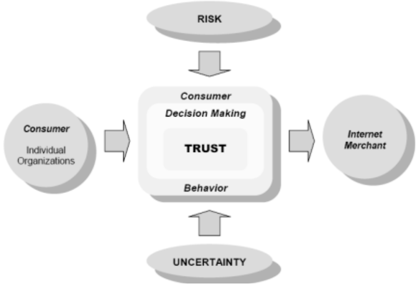

Fig 1: A Relationship between Consumer and internet Merchant[17].

There is a strong relation between consumer trust and security aspects that govern the whole transaction processes in an e-commerce website.

As a new form of commercial activity, e-commerce involves more uncertainty and risks than traditional commerce because they are less well known to consumers. Factors that affecting trust in e-commerce for consumers include security risks, privacy issue and lack of reliability e-commerce processes in general. A consumer cannot monitor the safety and security of sending sensitive personal and financial information. Online business organizations should search for high-tech security mechanism to protect itself from intrusion and also protect it's customer from being indirectly invaded. There are two lines of defense for e-commerce which are technology solutions and policy solutions, here we state some of adapted solutions: [1][11][3].

1) Encryption Approach: Encryption is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. It's purpose is:

(a) to secure stored information.

(b) to secure information transmission..

There are several types of encryption that differs in the context of it's functionalities. In Symmetric Key Encryption, both the sender and the receiver use the same key to encrypt and decrypt messages while Public Key Encryption used two mathematically related digital keys which are public key and private key[11][3].

2) Secure Socket Layer: The most common form of securing channels is through the Secure Sockets Layer (SSL) of TCP/IP. The SSL protocol provides data encryption, server

authentication, optional client authentication, and message integrity for TCP/IP connections. Secure Socket Layer (SSL) is a security protocol, first developed by Netscape Communications Corporation and now taken over by the transport layer security working groups. The design goal of the protocol is to prevent eavesdropping, tampering or message forgery when a data is transported over the internet between two communicating applications[3].

3) Secure Hypertext Transfer Protocol (S-HTTP): S-HTTP is a secure message-oriented communications protocol designed for use in conjunction with HTTP. It is designed to coexist with HTTP and to be easily integrated with HTTP applications. Whereas SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely. Using S-HTTP, any message may be signed, authenticated, encrypted or any combination of these. Generally, S-HTTP attempts to make HTTP more secure[3].

4) Trust Seals Programs: A number of Trustmark seals have been developed to provide assurance about Web business practices and policies through the Web interface. One example is TRUSTe, which audit a site’s stated privacy policies and allows sites to display the TRUSTe seal if privacy policies and disclosure meet specific standards. Cheskin and Sapient [5], found that where trust mark seals were recognized, they increase consumer perceptions of a site’s trustworthiness.

Seal programs such as TRUSTe, BBBOnLine, MultiCheck and WebTrust allow licensees who abide by posted privacy policies and/or allow compliance monitoring to display means for addressing consumer privacy concerns.

5) Digital Signature: Digital signature means a digital method executed by a party with the intent to authenticate a record, which is a unique to the person using it and is capable of verification. It is linked to the data in such a manner that if the data is changed, the electronic signature is invalidated. A digital signature is normally a hash of the message which is encrypted with the owner’s private key[11][3].

6) Secure Electronic Transaction (SET):

A SET specification for credit/payment card transactions is required for the safety of all involved in e-commerce. It is designed to meet three main objectives. First, it will enable payment security for all involved, authenticate card holders and merchants, provide confidentiality for payment data and define protocols and potential electronic security service providers. It will also enable interoperability among applications developed by various vendors and among different operating systems and platform[11][3].

7) Privacy Policy Statements: A privacy policy statement is a contractual commitment to consumers outlining how their personal information will be treated. The evidence suggests that posting a self-reported guarantee of compliance with e-commerce standards is an effective means of increasing consumer trust. Privacy policy statements appear to be most beneficial to the web merchants that have the greatest need to increase consumer trust . Privacy is the willingness of consumers to share information over the internet that allows purchases to be conducted.

8) Digital Certificate: A digital certificate is a digital document issued by a trusted third party institution known as a certification authority that contains the name of the subject or company, the subject’s public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority and other identifying information. The Certification Authority (CA) is a trusted third party that hands out certificates and publishes identities and public keys in a directory. The certificate is signed with the private key of the Certification Authority; therefore, its authenticity can be confirmed by using the known public key of the CA[11][3].

C. Encryption Technology

Encryption is the key security schemes adopted for electronic payment systems, which is used in protocols like SSL and SET. It is a very old technology for keeping messages secret from unauthorized access. One of the oldest methods of encryption was developed by Spartan generals around the fifth century of BC [6]. The basic idea of encryption is only an authorized person can reveal information from an encrypted message by using a key.

Encryption algorithms can be sited to two types, namely symmetric cryptography (single key cryptography) and asymmetric cryptography or public key (two keys) cryptography. A well-known symmetric cryptography is DES (Data Encryption Standard) developed by IBM for the US government. A well-known public key cryptography is RSA cryptosystem.

Data Encryption Standard (DES) is the most widely used symmetric cryptography. DES was adopted by NIST (National Institute of Standards and Technology) in 1977 to provide an encryption algorithm to be used in protecting federal unclassified information from unauthorized disclosure or undetected modification during transmission or while in storage [10].

The DES algorithm uses a 56-bit key to encrypt plaintext to ciphertext or to decrypt ciphertext to plaintext. The DES consists of 16 "rounds" of operations that mix the data and key together in a prescribed manner using the fundamental operations of permutation and substitution. The goal is to completely scramble the data and key so that every bit of the ciphertext depends on every bit of the data plus every bit of the key.

The RSA Cryptosystem is an asymmetric cryptosystem developed by the trio: Ronald Rivest, Adi Shamir and Leonard Adleman [13]. The RSA cryptosystem is based on the principle that if two large prime numbers are multiplied, the resulting number is hard to factor back to its original numbers. In the RSA cryptosystem the two numbers are keys, namely private and public keys. A private key must be kept secret, while a public key can be revealed to anyone.

Obviously, the RSA cryptosystem is more complex and harder to manage than DES since it involves two keys. However, an inherent benefit will be revealed shortly.

In the RSA cryptosystem, a sender may encrypt a message using his/her private or public key. Let A and B be two parties that use the RSA cryptosystem and KPA, KTA, be the public key and the private key for A, KPB, KTB be the public key, the private key for B respectively. Assume that B knows KPA and A knows KPB. There are two possible scenarios:

1. A sends a message to B. Before sending the message, A encrypts the message using KPB. Since A uses KPB to encrypt the message then only B can decrypt the message using KTB. This is called the encryption path of the RSA cryptosystem.
2. A sends a message to B. Before sending the message, A encrypts the message using, KTA. Next, B decrypts the message using KPA. If B can decrypt the message using KPA, then the message must come from A. This is called the authentication path, which can be used as a digital signature (the message is digitally signed by A). Note that A cannot deny (non-repudiation principle) that he/she has signed the message since the message can only be decrypted using A's public key (KPA) [13].

III. SSL, SET AND 3D-SERCURE: PROTOCOLS OF ELECTRONIC COMMERCE

Electronic commerce, as exemplified by the popularity of the internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce. Most people are skeptical about the security of the internet. People are happy using the World Wide Web for browsing, finding, reading or downloading information from the internet. However, when considering sending a credit card number over the internet, they are reluctant to do it, even if they are told that the transfer is secured. This is because many media expose bad news about the internet security, although security technology for the internet exists and good enough for protecting transactions via the internet, it requires the customer and merchant to trust each other: an undesirable requirement even in face-to-face transactions, and across the internet it admits unacceptable risks[19].

Secure payment systems are critical to the success of E-commerce. There are four essential security requirements for safe electronic payments (Authentication, ,Validity, Encryption, Integrity and Non-repudiation).

We will discuss later on here after a brief history of the security protocols, three famous protocols: SSL, SET and 3d-sercure and other modified models of 3d-Secure protocol.

A. History of Security Protocols

iKP which was in usage beginning with mid-1996, is actually the ancestor of SET. iKP is known for the longevity, security and the simplicity of the connection mechanism which made its experience to be unique. SET appeared at the initiative of VISA and MasterCard, in order to satisfy other needs that iKP did, such as: information confidentiality (both the card owner and the seller had to be authenticated in order to protect all parties were involved), independency from other protocols, platforms and operating systems, etc. [2].

However after 2000 new ideas for other protocols much better than SET, started to appear. Moreover since SET proved to be somehow a failure, especially because the actions of the seller were relatively complex. In fact there should have been established more communications with the customer, with the bank and with the payment gateway. Seeing this lack of interest, a new payment scheme was created at the initiatives of Visa.

Compared to SET, 3D-Sercure answers a simpler scheme and allows the integration of a much easier usage for the seller and the buyer. Most responsibilities are now transferred to banks. The main innovation in terms of security is the introduction of SSL/ TLS. TLS (Transport Layer Security) is the IETF version of SSL. At the beginning 3D-Secure was called 3D-SSL.

Nowadays it is in general use (starting with 1st of March 2003) and it is supported by Visa, MasterCard, American Express, etc. [2].

B. SSL protocol:

The SSL protocol, widely deployed today on the internet, has helped create a basic level of security sufficient for some hearty souls to begin conducting business over the Web. SSL is implemented in most major Web browsers used by consumers, as well as in merchant server software, which supports the seller's virtual storefront in cyberspace. Hundreds of millions of dollars are already changing hands when cybershoppers enter their credit card numbers on Web pages secured with SSL technology.

SSL is implemented in all popular browsers and web servers. Furthermore, it is the basis of the Transport Layer Security (TLS) protocol. In this sense, SSL provides a secure channel between the consumer and the merchant for exchanging payment information. This means any data sent through this channel is encrypted, so that no one other than these two parties will be able to read it. In other words, SSL can give us confidential communications, it also introduces huge risks:

- The cardholder is protected from eavesdroppers but not from the merchant. Some merchants are dishonest: pornographers have charged more than advertised price, expecting their customers to be too embarrassed to complain. Some others are just hackers who put up a snazzy illegal Web site and profess to be the XYZ Corp., or impersonate the XYZ Corp. and collecting credit card numbers for personal use.
- The merchant has not protected from dishonest customers who supply an invalid credit card number or who claim a refund from their bank without cause. Contrary to

popular belief, it is not the cardholder but the merchant who has the most to lose from fraud. Legislation in most countries protects the consumer [20].

C. SET Protocol

Visa and MasterCard and a consortium of 11 technology companies made a promise to banks, merchants, and consumers: they would make the internet safe for credit card transactions and send electronic commerce revenues skyward. With great fanfare, they introduced the Secure Electronic Transaction protocol for processing online credit card purchases [9]. SET is an open standard for encryption and security specification for credit card transactions on the internet [18]. The SET is a set of security protocols and formats that main section are application protocol and payment protocol. The electronic commerce parties based on SET protocols can be illustrated as Fig. 2. [14]

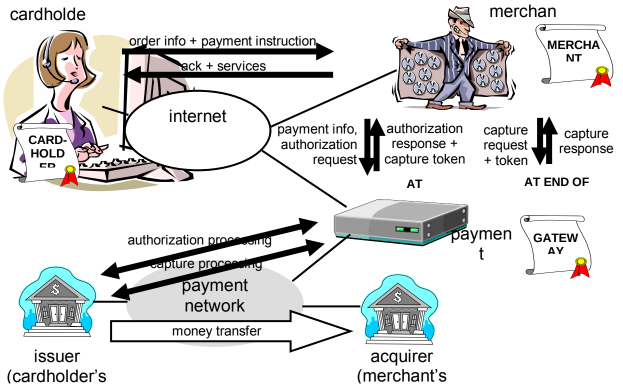

Fig 2: Parties in Set protocol

Key Technologies of SET:

- Confidentiality of information: DES.
- Integrity of data: RSA digital signatures with SHA-1 hash codes.
- Cardholder account authentication: X.509v3 digital certificates with RSA signatures.
- Merchant authentication: X.509v3 digital certificates with RSA signatures.
- Privacy: separation of order and payment information using dual signatures.

Dual Signatures:

An important innovation introduced in SET; the dual Signature. The purpose of the dual signature is the same as the standard electronic signature: to guarantee the authentication and integrity of data. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card's number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods and service [15]. So, Dual Signature links two messages securely but allows only one party to read each as shown in Fig. 3 .

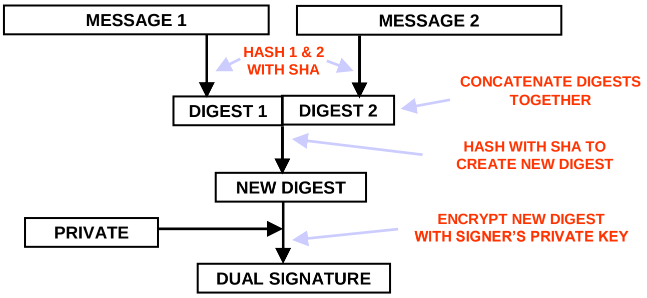
MESSAGE 1
MESSAGE 2
HASH 1 & 2 WITH SHA
CONCATENATE DIGESTS TOGETHER
DIGEST 1
DIGEST 2
HASH WITH SHA TO CREATE NEW DIGEST
NEW DIGEST
ENCRYPT NEW DIGEST WITH SIGNER'S PRIVATE KEY
PRIVATE
DUAL SIGNATURE

Fig. 3 Dual Signature: Links two messages securely but allows only one party to read each.

Fig.4 shows the model of dual signature. When the dual signature is constructed, it gets the hash of the concatenated hashes of OI (Order Information) and PI (Payment Information) as inputs. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual signature is sent to both the merchant and the bank. The protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not reveal the content of the OI or PI, and thus privacy is preserved. We can summarize these steps as follows:

1. Take the hash (SHA-1) of the payment and order information.
2. These two hash values are concatenated [H(PI) || H(OI)] and then the result is hashed.
3. Customer encrypts the final hash with a private key creating the dual signature.

DS = E_{KRC} [H(H(PI) || H(OI))].

$$DS = E_{KR_c}[H(H(PI) \,||\, \mathrm{H(OI)})]$$

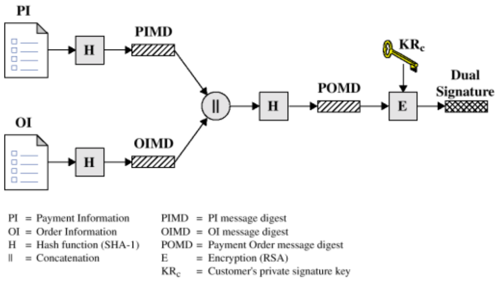

Fig. 4 Dual Signature Model [15]

4. The merchant request payment authorization.
5. The merchant confirm the order.
6. The merchant provides the goods or service.
7. The merchant requests payments.

SET has many merits:

• SET has provided merchant protective method, cost-cutting and enough security for the electronic payment. It makes the business exempted from the online fraud.

• As for the consumer, SET has guaranteed validity of online merchant as credit card number of cardholder will not be stolen. SET keeps more secrets for the consumer to improve the satisfaction of their on-line shopping experience.

• SET helps the bank and the credit card company to expand the service to more broad space – internet. And it lowers the probability of credit card on-line fraud.

• Therefore SET seems more competitive than other online payment method.

• SET has defined interface for all quarters of online transaction so that a system can be built on the products made by the different manufacturers.

Although SET has been widely used in the electronic payment area and has gained more attention from the electronic commerce promoter, the SET transaction mode can not be used on the B2B business model but B2C model only. Even for B2C model, its application is also limited. For example, it can only be applied in some types of card payment service. Its deficiencies mainly display on following aspects [7]:

1. DES algorithm and the RSA algorithm are used in SET protocol to carry on the encryption and the decryption process. SET protocol use DES as symmetrical encryption algorithm. However, DES was no longer a safe algorithm right now. Therefore, DES should be replaced by more intensive and safer algorithm. Moreover, along with the development of processing speed and storage efficiency enhancement of the computer, the algorithm will be cracked successively. It is necessary to improve the extendibility of encryption service.
2. SET protocol is huge and complex in the application process. In a typical SET transaction process, the digital certificates need to be confirmed 9 times, transmitted 7 times; the digital signature need be confirmed 6 times, and 5 times signature, 4 symmetrical encryptions and 4 asymmetrical encryptions are carried out. SET protocol involves many entities such as customers, merchants and banks. All of them need to modify their systems to embed interoperability. As the SET requests installment software in the network of bank, on the business server and PC of the customer and it also need to provide certificates to all quarters, so running cost of the SET is rather high.
3. The protocol cannot prove transactions which are done by the user who signs the certificate. The protocol is unable to protect cardholder and business since the signature received finally in the protocol is not to confirm the content of the transaction but an authentication code. If cardholders and trade companies have the dispute cannot provide alone the evidence to prove its transaction between themselves and the banks.
4. SET protocol specification has not mentioned how to store or destroy this kind of data safely after business processes complete and whether the data should be stored in the computer of the consumers, or the online store, or in the receipt bank. This kind of Vulnerability possibly will cause these data later under the latent attack.
5. SET protocol has not considered the fairness of transaction individual. Credit card information of cardholder retransmitted through online merchant, although has been undergone the encryption, still could be known by the merchants what the cardholder has bought. This process has not provided anonymous to consumers, consequently it is a serious potential danger.
6. In the document of transaction, time is the especially important information. In the written contract, the date when the document signs and signature are equally crucial content and should be prevented from forge and the distortion. On the other hand, it is easy to changes the timer of some document on the computer. For that reason, the corresponding security measure in the electronic transaction process should be taken to protect the safety of the date and time information of the document.

Meanwhile it could prevent lawsuit from transaction denial thereafter. Although there are some drawbacks in the SET protocol, it is still the most standard and the safest in the present electronic commerce security protocol and the international standard of the security electron payment [20].

D. 3-D Secure Protocol.

The three-Domain Secure (3-D Secure) model of VISA provides the issuers with the ability to authenticate cardholders during an online purchase. This reduces the fraudulent use of credit cards and increases traceability of the transaction. The model divides the payment system into:

Issuer Domain, Acquirer Domain and Interoperability Domain [8], as shown in fig. 5.

- The issuer domain is integrated by the Cardholder, a Visa member financial institution (Issuer) and a VISA component Access Control Server (ACS). This domain is responsible for managing the enrolment of their cardholders in the service and for authenticating cardholders during online purchases by means of ACS.
- The Acquirer domain is integrated by Merchant, a VISA financial institution (acquirer) and a VISA component Merchant Server Plug-in (MPI). This domain is responsible for defining the procedures to ensure that merchants participating in the internet transactions are operating under a merchant agreement with the Acquirer, and providing the transaction processing for authenticated transactions by means of MPI.
- The Interoperability Domain is integrated by Visa Directory Server (DS) and Authentication History Server (AHS). The Visa directory Server handles all the communication between Merchant and the appropriate ACS in the process of request if the payment authentication is available. AHS stores the messages from the ACS for each attempted payment authentication and could be used by acquirers and issuers in case of disputes.

The following figure represents the Domain model of VISA and the principal flows in the payment protocol.

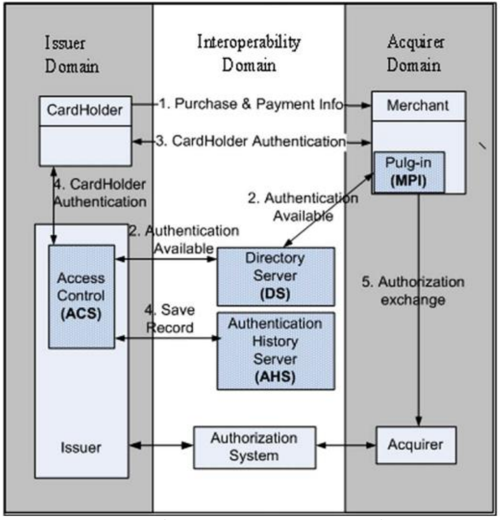
Issuer Domain
Interoperability Domain
Acquirer Domain
CardHolder
1. Purchase & Payment Info
Merchant
3. CardHolder Authentication
Pulg-in (MPI)
4. CardHolder Authentication
2. Authentication Available
2. Authentication Available
Access Control (ACS)
Directory Server (DS)
5. Authorization exchange
4. Save Record
Authentication History Server (AHS)
Issuer
Authorization System
Acquirer

Fig. 5: Domain model of VISA and the principal flows in the payment protocol [8].

The payment protocol in 3-D Secure

Principal Messages

1. VEReq – Message from MPI to the DS or from DS to the ACS, asking whether authentication is available for a particular card number.
2. VERes – Message from the ACS or the DS, telling the MPI whether authentication is available.
3. PAReq – Message request sent from the MPI to the ACS (via the cardholder browser), to issuer to authenticate its cardholder.
4. PARes – Message formatted, digitally signed, and sent from the ACS to the MPI (via the cardholder browser) providing the results of the issuer's 3-D Secure cardholder authentication.

Flows of messages

1. First, the cardholder indicates the decision to buy, sending the purchases and payment info at this moment, MPI software is activated.

2. The MPI sends a message (VEReq) to the DS to determine whether authentication services are available for the cardholder.

- If the cardholder is enrolled and authentication is available, the response message (VERes) instructs the MPI on how to contact the ACS (protocol continues with step 3).
- If the account number of the cardholder falls outside of participating card ranges, the merchant proceeds with a standard authorization request.

3. The MPI sends an authentication request (PAReq) to the ACS. This is usually sent via the cardholder browser.

4. The ACS authenticates the cardholder by causing an authentication dialog to be displayed to the cardholder asking for a password, or by some other authentication method, such as a Visa chip card. The ACS formats and digitally signs the authentication response (PARes), then returns it to the MPI.

5. If the authentication response indicates successful authentication, the merchant forwards an authorization request with the requisite data to its acquirer for submission into an authorization system.[8]

E. Intermediary-3D Secure

Mildrey Carbonell & elt. [8] proposed a multiparty electronic commerce protocol in which the intermediary plays the role of a payment mediator. This intermediary helps the customer to make purchases and payments with many providers simultaneously as a single payment transaction. They proposed model decreases the number of customer operations in the traditional multiparty payment process. This optimization in the payment process for this kind of multiparty scenarios is particularly interesting when we consider the devices which have some resources constraint (computational or connectivity), this is the case of portable devices. Also, in the secure infrastructure proposed, is not assumed to have strong trusting restrictions in the intermediary entity (i.e. not need to be a TTP) which implies a more flexible scenario. In addition, they adapted the 3D Secure_ payment protocol, using their intermediary, to offer the possibility of making secure payment with multiple providers that not need to be enrolled in VISA 3D Secure.

In this multiparty electronic commerce model, the intermediary plays the role of payment mediator between one customer and many providers. Here, the customer delegates the multipayment transactions to the intermediary and creates a single secure transaction between customer and his providers. This model is a secure solution in which the customer creates a short-term certificate for the intermediary as authorization credential to forward and distribute the payment info. This will be used in the distribution process to create evidence of the intermediary's participation. Also by this means, the provider can obtain the customer's authentication and assurance of purchase integrity. Unlike to other secure solutions in e-commerce models with intermediary, in this secure solution the intermediary is not represented as a trusted entity (is not a TTP) [8].

IV. DISCUSSION

Since 1990s a lot of Security protocols appeared but only a few of them succeeded and became widely implemented. Among the most successful are SSL and SET.

Secure Socket Layer protocol (SSL) is used by the vast majority of internet secure transactions. SSL is implemented in all popular browsers and web servers. It was originally designed by Netscape. It was developed to provide encryption and authentication between a web client and a web server. Furthermore, it is the basis of the Transport Layer Security (TLS) protocol.

Secure Electronic Transactions protocol (SET) is another protocol competing with SSL. In E-Commerce whether with SSL or SET, usually uses payment credit and debit card infrastructure. Here we try to answer the big question: which to use SSL OR SET protocol?.

The three major players in this issue is: customers, merchants and financial institutions(usually banks).

We have seen that SSL provides security for communication between the first two players (the customer and the merchant), while SET provides security for communication among all three players. Here we must state some facts about SSL, which are: SSL is the basis of the TLS. Also SSL and TLS are not limited to web applications. In fact, they can be used for authentication and data encryption in IMAP mail access. Furthermore, SSL can be seen as a layer between the application layer and the transport layer. On the sender side, it receives data (for example http messages) from the application layer and encrypts it before directing the encrypted data to a TCP socket. The opposite happens at the receiver side.

SSL is popular today. It enabled servers and browsers provide a popular platform for card transactions. In spite of that, SSL was not developed specifically for card payment, but instead for generic secure communication between a client and a server.

The generic design of SSL may cause problems. For example, by using SSL we can authenticate the customer and the merchant, but we can't be sure whether the merchant is authorized to accept payment, nor whether the customer is authorized to pay money. SSL also doesn't tie a client to a specific card. For these reasons we need a protocol that handles authentication and authorization for card payments transactions. The protocol that could do that was the SET protocol.

SET was developed in 1996 by Visa, MasterCard, Microsoft, Netscape, IBM among others. This protocol was designed specifically to secure card payment transactions over the internet. It encrypts payment related messages. SET can't be used for general purposes like encrypting arbitrary text of images. SET involves all three players in E-payment. In SET all three players must have certificates.

The customer's and merchant's certificates are issued by their banks in order to assure that they are permitted to make/receive payments by cards. In a SET transaction, the customers card number is passed to the merchant's bank. This number is never seen by the merchant as plaintext.

SET beats SSL in secure issues since it has the following properties:

- All players must hold trusted certificates.
- All parties are authenticated.
- SET provides privacy, merchant will never see the customer's card number.
- SET provides data integrity.
- SET provides customer non-repudiation guarantee.
- SET provides customer and merchant authorization.

But in the other side, SET is not easy to implement and SET requires the customer to install an e-wallet. It is expensive to integrate with legacy applications.

SET is safe since it addresses all the parties involved in typical credit card transactions: consumers, merchants, and the banks. Besides the interoperability problem, it has difficulties to spread since it needs all the participants to have

some part of the software, even very expensive hardware. It may be clearly in the interests of the credit card companies and banks, but it looks quite different from the perspective of merchants and consumers. In order to process SET transactions, the merchants have to spend several million dollars in equipment and services when they already have what are arguably sufficient security provisions in SSL. To consumers, they have to install software also.

SET can work in Real Time or be a store and forward transfer, and is industry backed by the major credit card companies and banks. Its transaction can be accomplished over the WEB or via email. It provides confidentiality, integrity, authentication, and, or non-repudiation.

SET is a very comprehensive and very complicated security protocol. It has to be simplified to be adopted by every parties involved in E-commerce transaction.

In my opinion, for merchants to build trust, they should adapt the SET protocol, in spite of its heavy cost.

V. Conclusion

Electronic commerce is now one of the widest applications in internet since it helps businesses to expand their marketing strategy and to reduce their costs. This growth has motivated the development of research to improve electronic services. Security, as one of these research topics, constitutes a critical point in the implementation of new business models because the process of traditional business such as paper-based contracts, personal purchases, etc. must be adapted to flows of information inside an unreliable network like the internet. So, payment should be the process with the highest security level in e-commerce operations because it is the step where the customer legally ends the business by making the money transference.

Many secure electronic payment solutions have been proposed. Some of them describe online payment with a cash payment model, like e-Cash, DigiCash, NetCash, and Cybercash. Others, such as NetBill, NetCheque and BankNet, present a cheque payment model. And, in a card payment schema, open solutions such as iKP and SET have been developed as a standard of secure payment. iKP and SET were not widely used in the internet but they constitute a starting point in the development of secure payment solutions. Today, the most popular solution in the card payment schema is the 3-D Secure protocol (3-D Secure) developed by VISA and MasterCard, which is based on the ideas of iKP and SET. This protocol provides the card issuer with the ability of authenticating its cardholders during an

doi:10.15849/icit.2015.0079 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

online purchase. Given that VISA has licensed this protocol and that many vendor communities use it, 3D Secure is considered a standard for authenticated payment [8]. This paper focused on SET and, 3D Secure protocols.

Electronic payment solutions are mostly focused on traditional two party business models. However, many business models involve some intermediary entities to help negotiation. Mildrey Carbonell & elt. [8] proposed a multiparty electronic commerce protocol in which the intermediary plays the role of a payment mediator. This intermediary helps the customer to make purchases and payments with many providers simultaneously as a single payment transaction. Even though, these proposed models solved many problems of previous one, they still suffer many gaps in the payment process.

We expect to see other advanced models in the near future that overcome all the disadvantages of the previous protocols and models.

REFERENCES

[1] Adam Jolly, “The Secure Online Business”, Great Britain and the United States- Kogan Page Limited 2003, pp: 93-118.

[2] Bellare, M., Garay, J., Hauser, R. ,Journal of Selected Areas in Communications,Vol. 18, No.4, 2000.

[3] Donal O.Mahony, Michael Peirce Hitesh Tewari, “Electronic Payment Systems for E-Commerce“, Artech House computer security series-Boston 2001, Second Edition, pp: 19-69

[4] E. Harrison McKnight and Norman L. Chervany., "What Trust Means in E-Commerce customer Relationships: An Interdisciplinary Conceptual Typology", International Journal of Electronic Commerce , 2001–2002, p. 35–59.

[5] "eCommerce Trust Study", research report, Cheskin and Studio Archetype/Sapient. Materials of Dagstuhl Seminar,1999.

[6] Hawker, A., "Security and Controls in Information Systems", London, Routledge, 2000.

[7] M Franklin, M Yang, “Towards Provably Secure Efficient Electronic Cash,” ReportCUCS-018-92. Columbia University Department of Computer Science, 2005.

[8] Mildrey Carbonella, Jose´ Marı´a Sierraa, Javier Lopezb, "Secure Multiparty Payment with an Intermediary Entity", computers & security 28 (2009) 289–30.

[9] Nikki Goth Itoi., "PROMISES, PROMISES What ever happened to SET", available at: http://www.herring.com/mag/issue51/promises.html.

[10] NIST (1995), "The Data Encryption Standard": An Update, http://csrc.nist.gov/publications/nistbul/csl95-02.txt.

[11] PETER C. CHAPIN, CH. SKALKA, and X. SEAN WANG, “Authorization in Trust Management: Features and Foundations”, ACM Computing Surveys, Vol. 40, No. 3, Article 9,August 2008,pp: 9.1-9.48.

[12] Pradnya B. Rane , Dr. B.B.Meshram, "Transaction Security for E-commerce Application", International Journal of Electronics and Computer Science Engineering. Available Online at: www.ijecse.org ISSN- 2277-1956. pp: 1720-1726.

[13] Rivest, R., A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and a Public Key Cryptosystem", Communication of the ACM, vol 21, pp.120-128, 1978.

[14] S Lu, S Smolka, “Model checking the secure electronic transaction (SET) protocol,” Proceedings of the 7th International Symposium on Modeling Analysis and simulation of Computer and Telecommunication Systems, 1999:358-364.

[15] S. William, "Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc., 1999 pp553- 554.

[16] Stuart Feldman, “The Changing Face of E-Commerce: Extending the Boundaries of the Possible”, IEEE INTERNET COMPUTING, MAY • JUNE 2000, p.:82-83.

[17] Vijay Ahuja, “Building Trust in Electronic Commerce”, IEEE/2000, pp:61-63.

[18] Visa and MasterCard, "SET Secure Electronic Transaction", Book2, Programmer's Guide,1997.5.

[19] YangLi, YunWang ,"Secure Electronic Transaction", http://islab.oregonstate.edu.

[20] Z. Boping, Sh. Shiyu, "An Improved SET Protocol", Proceedings of the 2009 International Symposium on Information Processing (ISIP’09), Huangshan, P. R. China, August 21-23, 2009, pp. 267-272, ISBN 978-952-5726-02-2 (Print), 978-952-5726-03-9 (CD-ROM).