Proc. of the Intl. Conf. on Advances in Computer and Electronics Technology -- ACET 2013

ISBN: 978-981-07-7227-7

Enhancing the Security of Visa 3-D Secure against Spoofing Attacks

Pita Jarupunphol and Wipawan Buathong

***Abstract*— Visa 3-D Secure is an e-payment system based on the integration of SSL/TLS with the three-domain architecture. It employs cryptographic techniques to secure communication links among participants in e-commerce transactions and also provides credit card verification via Visa Secure Server. Although several security vulnerabilities can be addressed, spoofing attacks are still effective and can be considered as potential threats to Visa 3-D Secure. Threats of spoofing and impersonation have become more effective due to advances in computing and communications technologies. However, security mechanisms incompatible with the past e-payment infrastructure are also enabled by these technological advances. PKI-based authentications used in the SET scheme can be considerable in the current era for enhancing the security of Visa 3-D Secure against spoofing attacks.**

***Keywords*— Certification Authorities (CAs), Public Key Infrastructure (PKI), Secure Electronic Transactions (SET), Spoofing Attacks, Visa 3-D Secure**

I. Introduction

The Secure Socket Layer (SSL) protocol, together with the Internet Engineering Task Force (IETF)'s SSL based Transport Layer Security (TLS) protocol [1], is one of the main industry standard means for securing communications over the Internet. Although SSL/TLS uses well established handshake and cryptographic techniques to guarantee the secrecy and integrity of transmitted data, SSL/TLS was considered insufficient for addressing essential e-commerce security requirements. For example, the default handshake phase of SSL/TLS identifies the server, but not the client [2]. Moreover, there is no financial institution involved in payment verification in SSL/TLS. E-commerce transactions using SSL/TLS are categorised as 'card-not-present', in which the merchant must be responsible if the customers uses a stolen credit card to initiate e-commerce transactions [3]. Furthermore, SSL/TLS is not designed to protect against repudiation of a transaction. No cryptographic evidence is generated that can be used later to help establish whether both consumer and merchant really participated in the transaction.

Accordingly, several secure protocols were proposed to address the limitations in the security provisions for e-commerce that were not being fulfilled by SSL/TLS (e.g., SET (Secure Electronic Transactions), MasterCard SPA (Secure Payment Application), and Visa 3-D (3-Domain) Secure).

Pita Jarupunphol, Wipawan Buathong
Department of Informatics, Phuket Rajabhat University
Thailand

Although some of them, such as SET, could technically provide e-commerce transactions with a high level of security protection, they were considered as too 'complicated' and rejected by e-commerce participants [4]. Eventually, Visa 3-D Secure (Verified by Visa or VbV) [5] has been widely used by a number of e-commerce websites. It is an e-payment system based on one of SET extensions, namely the three domain architecture. Visa 3-D Secure was proposed to address SSL/TLS problems where absence of verification of the card-holder can result in credit card fraud at the consumer side. Visa 3-D Secure provides e-commerce merchants with cardholder verification, whilst still retaining the 'ease-of-use' associated with use of SSL/TLS. In other words, it is a 3-D version of SSL/TLS equipped with an entity verification mechanism among e-commerce participants.

Although Visa 3-D Secure can address several potential e-commerce security risks, dealing with web spoofing attacks conditioned by the intent to deceive is difficult to achieve. Web spoofing [2], [6], [7] was pointed out as a potential threat to e-commerce security. It is an active attack on web client/server communications that allows malicious parties to eavesdrop on and modify the data transmitted from a victim to a real server. This type of attack can be performed either when the connection is not secure or during the establishment of a secure connection. Besides, the rapid increases in computing and communications speed also mean that malicious parties can exploit them to facilitate web spoofing attacks. Due to these technological advances, this paper argues that PKI-based authentication methods utilised by SET can be considered for enhancing the security of Visa 3-D Secure against attacks. This paper discusses potential vulnerabilities associated with the use of Visa 3-D Secure, focusing in particular on web spoofing and suggests ways in which the identified security vulnerabilities can be addressed.

II. SET – Overview

SET was a prominent security protocol for an electronic payment system invented by Visa and MasterCard in 1996 [8], [9]. SET architecture utilises PKI to address limitations found in SSL/TLS. A number of reputable IT organisations participated in SET developments (e.g., GTE, IBM, Microsoft, Netscape and Verisign). SET employs both symmetric and asymmetric cryptography to protect purchasing information sent between SET participants, including customer, merchant, the acquirer, and the issuer. Key management for SET is based

Proc. of the Intl. Conf. on Advances in Computer and Electronics Technology -- ACET 2013

ISBN: 978-981-07-7227-7

on the use of a PKI to reliably distribute public keys between SET participants. SET supports long key lengths for both symmetric and asymmetric encryption, such as triple DES and 1,024-bit RSA [10].

SET enforces the use of digital signatures to authenticate identity of customer and merchant in order to mitigate the risk of information being manipulated by a malicious third party. In the SET scheme, Certificate Authority (CA) issues digital certificates to the issuing bank or 'the issuer' *($CERT_{ISS}$ = $Sign_{(SKCA)}[PK_{ISS}]$)* and the acquiring bank or 'the acquirer' *($CERT_{ACC}$ = $Sign(SK_{CA})[PK_{ACC}]$)*. The issuer and the acquirer also play important roles in issuing digital certificates that are mandatory in the SET scheme. Customers must apply for digital certificates from their issuing bank *($CERT_{CUS}$ = $Sign(SK_{ISS})[PK_{CUS}]$)*, whilst the acquiring bank will be responsible for issuing digital certificates for merchants *($CERT_{MER}$ = $Sign(SK_{ACC})[PK_{MER}]$)* [10], [11]. In addition, customer purchasing information is classified into order and payment information (OI and PI) [8], [9]. Both OI and PI are encrypted with separate public keys. Merchant public keys are used to encrypt OI ($E(PK_{MER})$ *[OI]*), and acquiring bank public keys are used to encrypt PI ($E(PK_{ACC})$ *[PI]*). This is to make sure that the encrypted OI can only be decrypted by the merchant and the encrypted PI can only be decrypted by the acquiring bank.

SET is designed to ensure the merchant obtain cardholder authentication as part of an e-commerce transaction. SET enforces customer self-authentication. They perform this on their local PC by entering a password that activates their digital wallet prior to initiating a transaction. The customer's PC then transmits OI and PI, encrypted with separate public keys, to the merchant *$Sign(SK_{CUS})\{E(PK_{MER})[OI] | E(PK_{ACC})[PI]\}$* [8], [9], [10]. In addition, SET is designed to protect against repudiation of a transaction by having the issuing bank and the acquiring bank both play a crucial role in verifying the transaction. The issuing bank will provide a payment authorisation (PA) to the acquiring bank once the cardholder has been authenticated and agreed the payment. Similarly, the acquiring bank will inform the merchant once the PA has been provided by the issuing bank. Due to having both issuer and the acquirer involved in verifying each transaction, SET transactions are approved by major financial institutions such as Visa and MasterCard as 'card present' transactions. An overview of the interaction among the participants in SET transaction can be briefly described below.

1) $C \rightarrow M : SET_{request}$ (The cardholder requests SET initialisation from the merchant).
2) $M \rightarrow C : SET_{response}$ (The merchant responds SET initialisation to the customer).
3) $C \rightarrow M$: $Sign(SK_{CUS})\{E(PK_{MER})[OI]|E(PK_{ACC})[PI]\}$ (The cardholder submits and signs OI and PI encrypted by the merchant's public key and the acquirer's public key respectively).
4) $M \rightarrow A$: $E(PK_{ACC})[PI]$ (The merchant forwards PI encrypted by the acquirer's public key to the acquirer).
5) $A \rightarrow SET_{gateway} \rightarrow I : PA_{request}$ (The acquirer requests payment authorisation from the issuer via SET payment gateway).
6) $I \rightarrow SET_{gateway} \rightarrow A : PA_{response}$ (The issuer responds payment authorisation to the issuer via SET payment gateway).
7) $A \rightarrow M : PA$ (The acquirer sends a payment authorisation to the merchant).
8) $M \rightarrow C : PA_{confirmation}$ (The merchants confirms and captures the transaction).

Although the security architecture of SET was superior to SSL/TLS in preventing potential e-commerce fraud [12], SET was not implemented. The elegant security architecture of SET caused a number of significant problems. PKI solutions expected to be a 'magic pill' for e-commerce security issues instead became 'toxic'. A number of criticisms were leveled at SET. Interoperability among SET products was the major criticism of SET, since SET enforced the use of digital certificates for end entity verification. SET architecture relied on applications from different software vendors. All major SET products, such as digital wallets, EFTPOS applications, payment gateway applications, and digital certificates, must work together. This included certificate translations among PKI vendors acting as trusted third parties (TTPs) that had different certificate policies. Interpreting a certificate issued as part of a different TTPs was problematic due to the differences.

In addition to interoperability issues, several criticisms were also related to the computing and communications speed insufficient to support SET operations [13], [14]. According to Bellis [15], "the amount of overhead involved in the massive Public Key Infrastructure (PKI) and registration process required by SET, [means] it will never be widely adopted". That author further points out that adding the extra overhead of a PKI infrastructure was not appropriate for the payment process at that time. This view was also supported by Treese and Stewart [3], who argued that PKI in SET was incompatible with the existing e-payment infrastructure (of the 1990s). In addition, the low speed and high complexity of transactions was a common criticism of SET, and these properties reduced its attractiveness to both merchants and consumers. In order to improve the speed performance of SET, additional approaches were required (e.g., cryptographic hardware acceleration and elliptic curve cryptography), according to a comparative performance analysis conducted by Gartner Group in 1998 [16]. The speed of Internet also made SET inflexible, since digital wallets needed to be downloaded and installed in the consumer's PC in order to

Proc. of the Intl. Conf. on Advances in Computer and Electronics Technology -- ACET 2013

ISBN: 978-981-07-7227-7

address potential misuse of credit card numbers [1]. Although many software vendors were developing and standardising digital wallets in order to make it easier for consumers to use them (e.g., the MasterCard wallet based on IBM wallet v2.1 [17] supported both the SET and SSL protocols), consumers were still required to obtain digital wallets and set up their digital certificates and credit card details into the wallets.

III. Visa 3-D Secure – Overview

In Visa 3-D Secure, the payment gateway is implemented in the acquirer domain [18]. This gateway provides an interface between the merchant/acquirer's payment system and the Visa proprietary payment network VisaNet. Merchants are just responsible for installing an SSL/TLS Merchant Plug-In (MPI) at their servers, in the same way they would implement SSL/TLS. The MPI has additional functions to handle communication between the various entities; Visa 3-D Secure simply uses a URL redirection technique to enable communication that is protected using SSL/TLS among entities within the three domains: cardholder-merchant, cardholder-ACS, merchant-Visa Directory, and Visa Directory-ACS [18], [19].

The issuer needs to maintain a special server known as the Access Control Server (ACS). The ACS is used to support cardholder authentication. This enables the merchant to authenticate the cardholder, and obtain a signed guarantee from the Issuer ACS that the cardholder was present during the transaction. Merchants are provided with evidence, in the form of a message signed by the Issuer ACS, that the cardholder was present and the Issuer has authorised the transaction. This gives the merchant protection against the possibility of a 'card-not-present' chargeback. The Visa directory, a server in the Interoperability domain, enables communication between merchant servers and card issuers.

The following numbered sequence of steps summarises the operation of Visa 3-D Secure [20].

1) $C \rightarrow M : CR, \{PI\}_{SSl|TLS}$ (The cardholder submits a checkout request (CR) to the merchant. All purchasing information (PI) transmitted to the merchant server will be protected by SSL/TLS).
2) $MPI \mid M \rightarrow VDir : URR, PI$ (After the purchase information has been transmitted to the merchant server (M), The MPI at the merchant server sends a URL request (URR) to the Visa directory for the URL of the ACS of the issue of the card).
3) $VDir \rightarrow I : URR$ (The Visa directory checks the validity of the card and queries its participation in the 3-D Secure scheme with the ACS at the issuer server (I)).
4) $I \rightarrow VDir : CM, URL$ (The issuer sends a confirmation message (CM) and the URL to the Visa directory confirming the validity of the card details).
5) $VDir \rightarrow [MPI \mid M] : UR$ L (The URL of the issuer's ACS is sent to the MPI from the Visa directory).
6) $[MPI \mid M] \rightarrow C \rightarrow [ACS \mid I] : PVR$ (The MPI redirects the cardholder browser to the issuer's ACS for payment verification request (PVR)).
7) $[ACS \mid I] \rightarrow C : SAR$ (The ACS requests secret authentication (SA) information, such as username and password, from the cardholder).
8) $C \rightarrow [ACS \mid I] : \{SA\}_{SSl|TLS}$ (The cardholder enters his/her SA into the browser on his/her PC, from where it is sent to the issuer's ACS).
9) $[ACS \mid I] \rightarrow C : SAR \rightarrow [MPI \mid M] : Sign(SK_{ISS})[PV]$ (If the cardholder validation process is successful, the issuer's ACS redirects the cardholder browser back to the MPI and sends a payment verification (PV) sign by the issuer).
10) $M \rightarrow A : TD, PAR$ (The merchant transmits transaction details (TD) to the acquirer to request payment authorisation (PA) as in a 'normal' Internet transaction).
11) $A \rightarrow I : PAR$ (The acquirer sends a payment authorisation request (PAR) to the issuer via Visanet).
12) $I \rightarrow A : PA$ (The issuer responds by sending a PA to the acquirer).
13) $A \rightarrow M : PA$ (The acquirer sends the PA details back to the merchant).
14) $M \rightarrow C : TC$ (The merchant confirms the transaction (TC) and issues a receipt to the cardholder).

IV. Advantage of Visa 3-D Secure

Visa 3-D Secure imposes minimal overheads on end-users, since it is based on SSL/TLS and the only step required of the user is to register for the service with their card issuer (e.g., using a web registration procedure). Visa 3-D Secure benefits the merchant because it preserves the payment model used for existing SSL/TLS-protected e-commerce transactions. The initialisation is simple for both merchant and customer, especially for those already experienced in SSL/TLS. The merchant simply needs to install a special plug-in on his/her server, and the cardholder needs no special software. They must simply follow an on-line enrollment process with the card issuer, using a 'standard' web browser.

As part of Visa 3-D Secure's cardholder authentication mechanism, Visa 3-D Secure enables the merchant to authenticate the cardholder, and to obtain a signed guarantee from the Issuer ACS that the cardholder is present during the transaction. In this light, merchants are provided with evidence, in the form of a message signed by the Issuer ACS, that the cardholder was present and that the Issuer has authorised the transaction. This gives the merchant protection against the possibility of a 'card not present chargeback', where the merchant loses the value of the transaction if the cardholder denies that it took place. Therefore, Visa 3-D

Proc. of the Intl. Conf. on Advances in Computer and Electronics Technology -- ACET 2013

ISBN: 978-981-07-7227-7

Secure payments are regarded as 'card-present-transaction' where merchants no longer need to be responsible for disputed transactions.

v. Potential Vulnerabilities of Visa 3-D Secure

According to Barron's Dictionary of Computer and Internet Terms [21, p.450], spoofing is defined as "the act of impersonating a user or a machine". In the context of e-commerce, web spoofing has long been discussed in the literature as a potential threat that may lead to undesirable outcomes, i.e., loss of confidential or financial information. According to Felten [6], "Web spoofing allows an attacker to create a 'shadow copy' of the entire World Wide Web. Accesses to the shadow Web are funneled through the attacker's machine, allowing the attacker to monitor all of the victim's activities including any passwords or account numbers the victim enters".

In web spoofing, the attacker can monitor and modify any information transmitted by the victim to the server if SSL/TLS is not in use. Although SSL/TLS is used, a malicious third party ('man in the middle') can interpose itself between the user PC and the genuine server prior to SSL session establishment. The man in the middle can impersonate the user PC to the genuine server during SSL session establishment, since the SSL client is (typically) not authenticated. Similarly, the malicious server can impersonate the genuine server to the user PC — the malicious server can even establish an SSL connection with the user PC to remove any suspicions from the mind of the user. In this case, the URL displayed by the client web browser will be that of the attacker rather than the genuine server. Even if the end user checks this URL, however, an incorrect URL may go unnoticed for two possible reasons. Firstly, the attacker may register a URL which closely the genuine server may in any case be unknown to the end user. Many Internet merchants sub-contract the processing of credit card payments to third-party payment providers — hence, during a transaction the end user will find that they are connected to a server with a name bearing no relationship to the name of the merchant from whom they are making a purchase. In such a case the end user, no matter how diligent they may be in checking displayed URLs and that the SSL 'padlock' logo is displayed, will have no way of verifying whether they are connected to a genuine or false third party payment server.

Furthermore, Felten et al. [6] described how, using JavaScript (or other active content), a malicious server can rewrite the URL displayed to a user to make it appear that the user PC is connected to a server other than the one to which it is actually connected. Ye, Yuan and Smith [22] argued that it was possible to conduct such URL rewriting attacks (against both the address bar and status line) even when an SSL connection has been established. If such an attack is possible, then even the most careful URL checking will be ineffective. The authors [22] proposed a method to improve the effectiveness of spoofing attacks. In this method the man in the middle attacker does not even have to obtain an SSL server certificate. Instead of creating a genuine SSL session with the user PC, the attacker simply uses JavaScript to make it appear to the user as if an SSL connection has been established— this is achieved by faking the padlock symbol. In order to complete the deception, the attacker also needs to emulate the SSL/TLS warning window, which a user may expect. Ye et al. [22] demonstrated that this can be achieved using JavaScript for both Netscape Navigator and Internet Explorer.

Therefore, the spoofing technique is not only effective against SSL/TLS protected e-commerce transactions, but also potentially works even if the transaction is protected by Visa 3-D Secure. For example, an attacker establishes a bogus merchant site, which may be entirely fictional, or may be a 'copy' of a genuine web site. In the latter case, creating a convincing copy of a web site is simple using the spoofing techniques described by Felten et al. [6]. In this case, an e-commerce user lured into visiting the bogus merchant may expect to see an SSL connection without knowing that it was created by the bogus server. The bogus merchant then redirects the user PC to a web site which impersonates the Issuer ACS server, with potentially serious consequences to the user. The following notations represent spoofing attack scenario on Visa 3-D Secure. Please note that S{...} means the transaction entity is spoofed.

1) $C \rightarrow S\{M\}$: $\{CR\}_{SSl|TLS}$ (The cardholder submits a checkout request (CR) to the spoofed merchant. The connection is either protected by SSL/TLS or the spoofed merchant creates the false impression that an SSL/TLS connection has been established).
2) $[MPI \mid S\{M\}] \rightarrow C \rightarrow [ACS \mid S\{I\}]: PVR$ (The spoofed merchant does not attempt to connect to the Visa Directory. Instead, the cardholder is immediately redirected to another web site (also operated by the attacker) which impersonates the Issuer ACS. Again, the spoof ACS can either set up a genuine SSL session, or can simply fake one).
3) $[ACS \mid S\{I\}] \rightarrow C: SAR$ (The spoofed Issuer ACS requests secret authentication(SA) information, such as username and password, from the cardholder).
4) $C \rightarrow [ACS \mid S\{I\}] : \{SA\}_{SSl|TLS}$ (The cardholder enters his/her SA into the browser on his/her PC, from where it is sent to the spoofed Issuer ACS. At this point the attacker has learnt not only the card details but also the cardholder authenticating information. The attacker now has all the information necessary to make fraudulent transactions using 3-D Secure at the cardholder's expense).
5) $[ACS \mid S\{I\}] \rightarrow C \rightarrow [MPI \mid S\{M\}]$ (The spoofed Issuer ACS can then redirect the cardholder PC back to the spoofed merchant).

ISBN: 978-981-07-7227-7

6) $S\{M\} \rightarrow C: ERROR$ (the spoofed merchant simply displays an error message of some kind, terminating the (fake) transaction).

Please note that variants of the above attack exist where the spoofed merchant sits between the genuine merchant and the cardholder. When the spoofing technique is applied, the transaction can proceed normally, with the correct Visa 3-D Secure exchanges between MPI, Visa Directory and Acquirer. The spoofed merchant then redirects the cardholder PC to the spoofed Issuer ACS which actually transfers all the data to and from the genuine ACS. This means that the request for card-holder SA shown to the cardholder can be the screen generated by the genuine ACS, incorporating any special messages that the cardholder expects to see. Such a process, although more complicated to mount, means that countermeasures involving cardholder specific screens provided by the Issuer ACS can be vulnerable. A fraudulent e-commerce merchant can obtain his/her public key certified by a TTP in order to fool consumers that the e-commerce web site is free from eavesdropping and tampering. In this case, it is difficult for consumers to differentiate if the web site is real or unreal, since the secure connection indicator and other SSL related features are still regularly performed [6]. It is plausible that such an attack will not be noticed by consumers. To make matters worse, there will be no simple way of identifying the entity which was responsible for stealing the user authentication information.

VI. Effects on Computing and Communications Speed on E-Commerce Security

The continuing rapid growth in computing and Internet communications speed can have either a positive or negative effect on e-commerce security. The speed and availability of both computer processing and data communications continues to increase, enabling the provision of ever more complex applications. In terms of communications speed, the availability of low cost network bandwidth has grown rapidly. For general Internet users, broadband Internet access, as provided by ADSL, has become ubiquitous. The bandwidth of a ADSL broadband connection is much greater than that of a modem connection, which only offers up to 56 kb/s, but was mostly used in 2003. In the 2002-2012 decade, "the strong growth of broadband connections all over the world driven by hybrid fiber cable (HFC) and asynchronous digital subscriber line (ADSL) technologies, according to IEEE [23, p.47]. In [24] the Moore's Law was applied to analyse the growth of Internet traffic by the authors. Although there is no precise conclusion that whether the internet traffic growth rate is 3 times or 4 times every year, it is sufficient for any businesses or individuals to know that its growth is at least more than double. These increasingly complex applications are typically designed to facilitate their operation by the majority of unsophisticated end-users, who require something both effective and easy to use. For example, Internet users are much less likely to encounter situations where their browsers do not respond quickly enough when searching for Internet products or services, or do not respond quickly after the payment button has been clicked. Merchants can enhance their web sites with more complex features in order to make them look more attractive. On the other hand, the rapid increases in computing and communications speed also mean that malicious parties can exploit them to penetrate information security systems, including those based on cryptographic techniques. The continuing growth in computing and data communications speeds will facilitate distributed attacks of various types (e.g., Denial of Service attacks, distributed cryptanalysis, etc.). This includes spoofing attacks already discussed in this article. For example, slow Internet speed was pointed out by Ye Yuan and Smith [7] in 2002 as one of limitations to what web spoofing can achieve. The authors argued that spoofing the appearance of web browsers typically required a number of images to be downloaded while most home users connected to the Internet using a modem, and were restricted to at most 56 kbits/sec. The spoofing could result in an obvious major reduction in performance leading to suspicion that something was amiss. However, all these limitations may no longer be effective at the current state due to the rapid increase in computing and communications speed. As a result, there is always a risk that a consumer can be persuaded to divulge their authentication information to an attacker. If user authentication is based on a user name/password technique, this can be a major risk, since the attacker who learns the password can now impersonate the user at will. In addition, the Visa 3-D Secure HTTP redirection may be vulnerable to spoofing techniques, since no effective end entity authentication mechanisms are in use.

Although other limitations of web spoofing were pointed out in [22], [25] — i.e., it was impossible to confine the fake location line to the correct position in the spoofed location bar, preventing spoofing attacks requires certain level of user security awareness. Human factors are a major source of vulnerabilities in secure e-commerce applications, including Visa 3-D Secure. Users cannot reliably determine who they are communicating with, even when SSL/TLS security is in use. They may also fail to take simple security precautions, such as checking URLs in the location and status line [20]. According to Herzberg [2, p.65], "The security of the security and identification indicators depends on users noticing, and correctly interpreting, them". The author supports that it is not realistic to expect users to inspect the HTML code and the location bar (URL). A number of user spoofing awareness experiments discussed in the same article [2] imply that it is almost impracticable to completely address different types of spoofing attacks. Recently, Murdoch and Anderson [26] provided some evidence to confirm that Visa 3-D Secure has become a target of phishing attack (some evidences can be obtained from [27], [28]). The authors state that Visa 3-D

Proc. of the Intl. Conf. on Advances in Computer and Electronics Technology -- ACET 2013

ISBN: 978-981-07-7227-7

Secure ignores good design principles for online card transaction authentication and has significant vulnerabilities, which has become a target of online fraud. Nevertheless, it has lousy technology, but got the economics right boasting hundreds of millions of accounts. It is difficult for consumers to verify the legitimacy of a merchant, because the Visa 3-D Secure transaction process appears to work normally. Even the website protected by Visa 3-D Secure is legitimate like securesuite.co.uk [29], more than eighty responses were suspicious its legitimacy. It appears that the use of Visa 3-D Secure has not made the situation any worse than would be the case if SSL/TLS was used in the 'standard' way. In Jarupunphol [20], there is a possibility of risk being transferred to e-commerce users, since the Visa 3-D Secure scheme provides the merchant with evidence that the cardholder has been authenticated. In this case, merchants may no longer be responsible for card-not-present chargebacks for Visa 3-D Secure payments. Instead, consumers may have to bear the risk of fraudulent transactions (Please note that this reliability shifting was evidenced in Murdoch and Anderson [26]).

VII. Enhancing the Security of Visa 3-D Secure

Because of the possibility of spoofing attacks, there is a risk that a consumer can be persuaded to divulge their authentication information to an attacker. If user authentication is based on a user name/password technique this is clearly a major risk, since the attacker who learns the password can impersonate the user at will. In this case, a more sophisticated method of user authentication, where knowledge of one authentication exchange does not help to impersonate the user subsequently, can be used to improve the security of Visa 3-D Secure. In response to spoofing attacks, Activation During Shopping (ADS) [30] was proposed by Visa in which unregistered cardholders are offered the opportunity of signing up during the purchase process. They are required to confirm their identity by answering security questions to their card issuer. Although the ADS scheme can be used to verify the cardholder identity at some level, it is difficult to verify if the site is legitimate based on these security questions. The possibility of a man in the middle attack still exists and can be a potential threat to Visa 3-D Secure.

In this case, well-established 'one-time password' or challenge-response techniques — see, for example, [31, pp. 395–397], was suggested in [20] as a more sophisticated method of user authentication, where knowledge of one authentication exchange does not help to impersonate the user subsequently. For instance, one-time password is an authentication system based on a transformed password scheme that generates a different online password each time by passing the entered password through a one-way hash function n times, where n decreases by 1 on each new login [32]. As a consequence, this technique can be used to protect against replay attacks as well as eavesdropping, since it is infeasible to invert the one-way function (for further details, see [33].

In addition to the one-time password authentication system, challenge-response is a common authentication technique whereby an individual is prompted to provide some private information, is another potential solution for HTTP redirection vulnerability. The server in this case sends the client a random value (a challenge), which is different when requesting each authentication. In addition, the value must be incorporated into the client's response as an additional input to the one-way function generating a transformed password [34]. The status of challenge will be confirmed by the server when processing the response. Therefore, this technique can protect against replay attacks where the communication message can be recorded and later used for re-authentication.

Among well-established authentication methods discussed above, PKI-based authentication methods used in the SET scheme introduced in 1996 can be effective against spoofing attacks due to advances in computing and communications. Several SET criticisms may no longer be effective at the current state, since the computing and communications performance are much more advanced than when SET was terminated in 2002. These technological advances also facilitate other SET projects — e.g., SET/EMV proposed to address SET problems related to the secrecy of private keys [35]. SET/EMV is a project of SET integrating with the EMV (Europay, MasterCard, and Visa) specifications, which is a global standard for inter-operation of integrated circuit cards defining how compliant IC cards or "chip cards" and payment terminals should interact.

VIII. Concluding Remarks

This paper describes potential vulnerabilities associated with the use of Visa 3-D Secure. Although the Visa 3-D Secure offers advantages over SSL/TLS to the parties involved in a transaction, it still contains significant security vulnerabilities arising from spoofing techniques. Moreover, these potential threats to Visa 3-D Secure are also facilitated by the rapid growth of computing and communications technologies in the 2002-2012 period.

While it is not realistic to expect all users to be aware of spoofed elements due to human factors, secure means of authentication are necessary for protecting e-commerce transactions against spoofing attacks. Security questions used by the ADS scheme may be helpful in verifying the cardholder identity. However, they are insufficient to prevent a man in the middle. A more secure means of user authentication, e.g. based on tokens, one-time passwords and/or challenge response, can be used to reduce HTTP redirection vulnerabilities of Visa 3-D Secure. In this case, theft of

ISBN: 978-981-07-7227-7

authenticating information via false redirection is no longer effective. Due to advances in computer and communication technologies, PKI-based authentication used in the SET scheme can also be considerable for enhancing the security of Visa 3-D Secure against spoofing attacks. However, this also means that significant barriers restricting SET implementation such as interoperability issues must also be addressed.

References

[1] E. Rescorla, SSL and TLS: Designing and Building Secure Systems. Addison-Wesley, 2001.

[2] A. Herzberg, "Why Johnny can't surf (safely)? attacks and defenses for web users," Computers & Security, vol. 28, no. 12, pp. 63 – 71, 2009.

[3] G. W. Treese and L. C. Stewart, Designing Systems for Internet Commerce. Massachusetts: Addison-Wesley, 1998.

[4] P. Jarupunphol and W. Buathong, "Secure Electronic Transactions (SET): A case of secure system project failures," International Journal of Engineering and Technology, vol. 5, no.2, pp. 278-282, 2013.

[5] ——, "PKI in B2C E-Commerce," in Proceedings of the International Conference on E-Technologies and Business on the Web (EBW2013). University of the Thai Chamber of Commerce (UTCC), May 2008, pp.228–235.

[6] E. W. Felten, D. Balfanz, D. Dean, and D. S. Wallach, "Web spoofing: An internet con game," in Proceedings of the Twentieth National Information Systems Security Conference. Gaithersburg, MD: National Institute of Standards and Technology, October 1997, pp. 476–487.

[7] Z. Ye and S. Smith, "Trusted paths for browsers," in 11th USENIX Security Symposium. USENIX Association, August 2002, pp. 263–279.

[8] L. Loeb, Secure Electronic Transactions: Introduction and Technical Reference. Boston: Artech House, 1998.

[9] M. S. Merkow, J. Breithaupt, and K. L. Wheeler, Building SET Applications for Secure Transactions. John Wiley and Sons, New York, 1998.

[10] SET Secure Electronic Transaction Specification, Version 1.0 ed., Secure Electronic Transaction LLC (SETCo), May 1997.

[11] SET Secure Electronic Transaction Specification, Version 1.0 ed., Secure Electronic Transaction LLC (SETCo), May 1997.

[12] J. D. Tygar, "Atomicity in electronic commerce," netWorker, vol. 2, pp. 32–43, May 1998.

[13] P. Jarupunphol and C. J. Mitchell, "Measuring SSL and SET against e-commerce consumer requirements," in Proceedings of the International Network Conference (INC 2002). Plymouth University Press, July 2002, pp. 323–330.

[14] ——, "The future of SET," in Proceedings of UKAIS 2002. Leeds Metropolitan University, April 2002, pp. 9–17.

[15] E. Bellis, Beautiful Security. Sebastopol: O'Reilly, 2009, ch. Beautiful Trade: Rethinking E-Commerce Security.

[16] SET Comparative Performance Analysis, Gartner Group, November 1998.

[17] Internet Wallet Choices and Answers for Business and Technical Managers, IBM e-business, 1999.

[18] 3-D Secure: System Overview — Version 1.0.2, Visa International, September 2002.

[19] P. Jarupunphol and C. J. Mitchell, "Measuring 3-D Secure and 3D SET against e-commerce end-user requirements," in Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference. National University of Ireland, Galway, June 2003, pp.51–64.

[20] P. Jarupunphol, "A critical analysis of 3-D Secure," in Proceedings of the 3rd Electronic Commerce Research and Development (E-COM-03). Gdansk, Poland, October 2003, pp. 87–94.

[21] D. A. Downing, M. A. Covington, M. M. Covington, and C. A. Covington, Dictionary of Computer and Internet Terms, 10th ed. New York: Barron's, 2009.

[22] Z. Ye, Y. Yuan, and S. Smith, "Web spoofing revisited: SSL and beyond," Technical Report TR2002–417, February 2002.

[23] I. C. Society, A Brief History of Communications, 2nd ed. IEEE, 2012.

[24] K. G. Coffman and A. M. Odlyzko, Handbook of Massive Data Sets. Kluwer, 2002, ch. Internet growth: Is there a 'Moore's Law' for data traffic?, pp. 47 – 93.

[25] F. De Paoli, A. L. DosSantos, and R. A. Kemmerer, "Vulnerability of 'secure' web browsers," in Proceedings of the Twentieth National Information Systems Security Conference. Gaithersburg, MD: National Institute of Standards and Technology, October 1997, pp. 476–487.

[26] S. J. Murdoch and R. Anderson, "Verified by visa and mastercard securecode: or, how not to design authentication," in 14th International Conference on Financial Cryptography and Data Security '10, Tenerife, Canary Islands, Spain, January 2010.

[27] "Scam report – verified by visa activation," Millersmiles.co.uk.

[28] K. Peters, "Verified by visa security program used as bait in phishing scams," Internetretailer.com.

[29] "Is securesuite.co.uk a phishing scam?" Ambrand.com.

[30] "Verified by visa – activation during shooping fact sheet," Visa Europe, 2005, http://www.visaeurope.com, last accessed on 13 May 2013.

[31] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.

[32] W. Ford and M. S. Baum, Secure Electronic Commerce. Prentice Hall, 2001.

[33] N. Haller, C. Metz, P. Nesser, and M. Straw, A One- Time Password System – RFC2289, February1998, http://www.faqs.org/ftp/rfc/pdf/rfc2289.txt.pdf.

[34] D. W. Davies and W. L. Price, Security for Computer Networks, 2nd ed. New York: John Wiley and Sons, 1989.

[35] P. Jarupunphol and C. J. Mitchell, "Implementation aspects of SET/EMV," in Towards the Knowledge Society: e-Commerce, eBusiness and eGovernment, The 2nd IFIP Conference on e-commerce, e-business and e-government, IFIP I3E 2002 (J. L. Monteiro, P. M. Swatman, and L. V. Tavares, eds.), pp. 305–315, Kluwer Academic Publishers (IFIP Conference Proceedings 233), Boston (2002), October 2002.

Pita Jarupunphol is a lecturer in informatics at Phuket Rajabhat University. He completed his B.B.A. (business computing) from Dhurakitpundit University (Thailand) in 1996. He received his Master's Degree in information systems from the University of Wollongong (Australia) in 1999. His research interests include different aspects of e-commerce security. In addition to e-commerce security, he is also interested in mind-machine and cognitive informatics.

Wipawan Buathong is an assistant professor and a Head of Informatics Department at Phuket Rajabhat University. She received Bachelor's Degree in computer education from Surin Teacher College (Thailand) in 1994. She receives her Master's Degree in Information Technology from King Mongkut's University of Technology Thonburi (Thailand) in 2001. Her research interests include data mining and e-commerce security.