Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

"SET" to Pull Down the Insecurity Barrier in Front of E-commerce

Thousands of people use their credit cards everyday, to make payments over the Internet, although many feel insecure and others even reluctant to use the Internet. This paper addresses the topic of Secure Electronic Transaction (SET).

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

"SET" TO PULL DOWN THE INSECURITY BARRIER IN FRONT OF E-COMMERCE

July 25, 2001
Onur Arikan

Introduction:

Thousands of people use their credit cards everyday, to make payments over the Internet. But still giving out their credit card numbers make many of them feel insecure and others even reluctant to use the net although all technical possibilities are there.

For this reason to encourage even more customers for electronic commerce, they should be assured that the credit card numbers are totally safe and not seen by anybody all through the process. And this is exactly what "Secure Electronic Transaction" (SET) is for.

Brief History of SET:

SET is a technical specification for securing the financial transactions on the Internet. On February 1, 1996, Visa International and MasterCard announced together with others (including Microsoft, IBM, Netscape, SAIC, GTE, RSA, Terisa Systems, and VeriSign), the development of a single technical standard for safeguarding credit card purchases made over open networks. This standard was to be called the SET Secure Electronic Transaction ™ specification. Prior to this effort, Visa and MasterCard were pursuing separate specifications, and the new SET specification represented a convergence of those individual efforts. In mid December 1997, a new corporate entity called SET Secure Electronic Transaction LLC SETCo was formed by Visa and MasterCard to provide a structure that would govern and direct the future development of the SET Secure Electronic Transaction protocol, as well as other key functions that are required to support the implementation of this standard. In conjunction to this, agreements with American Express and JCB Co., Ltd. to become full partners in SETCo have been negotiated.

The Role of SETCo Today:

SETCo is an organisation to manage the Specification, oversee Software Compliance Testing and coordinate efforts related to the adoption of SET as the global payment standard. SETCo participants are several companies committed to the advancement of the SET protocol who are working together to encourage payment brands, financial institutions, merchants, cardholders, and software vendors to adopt SET as the most comprehensive payment solution for global Internet commerce. A list of vendors to provide SET certificates, interoperability

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

results, technical standard specs and extensions, participation agreements, enrollment for compliance tests and much more are all accessible at SETCo website.

What is SET?

SET basically is a system for ensuring the security of financial transactions on the Internet. The highlight that SET brings to on-line security systems is the use of Digital Certificates. With SET a digital wallet is given to each customer. Digital wallet is a file or set of records for a user that contains all account information, such as credit-card numbers and digital certificate. When the customer has the electronic wallet the payment transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank. Therefore, privacy and confidentiality is secured among all parties.

Security Levels of SET:

SET protocol provides enhancements mainly at three security areas. Therefore much more complete and better safety is achieved over other payment methods. These are:

Privacy, via cryptography that renders intercepted messages unreadable.

Integrity, via hashing and signing assures that messages sent are received without alteration.

Authentication, via digital certificates which assures that the parties involved in the transaction are who they claim to be, and prevents them from denying that they sent a message.

The *privacy* or confidentiality of transactions is achieved by cryptography. There are two forms of cryptography used in SET protocol. RSA and DES.

RSA is an asymmetric algorithm used for signatures and public-key encryption of symmetric encryption keys and bank card numbers. DES on the other hand is symmetric and it takes care of the encryption of the data that is to be transmitted during the transaction.

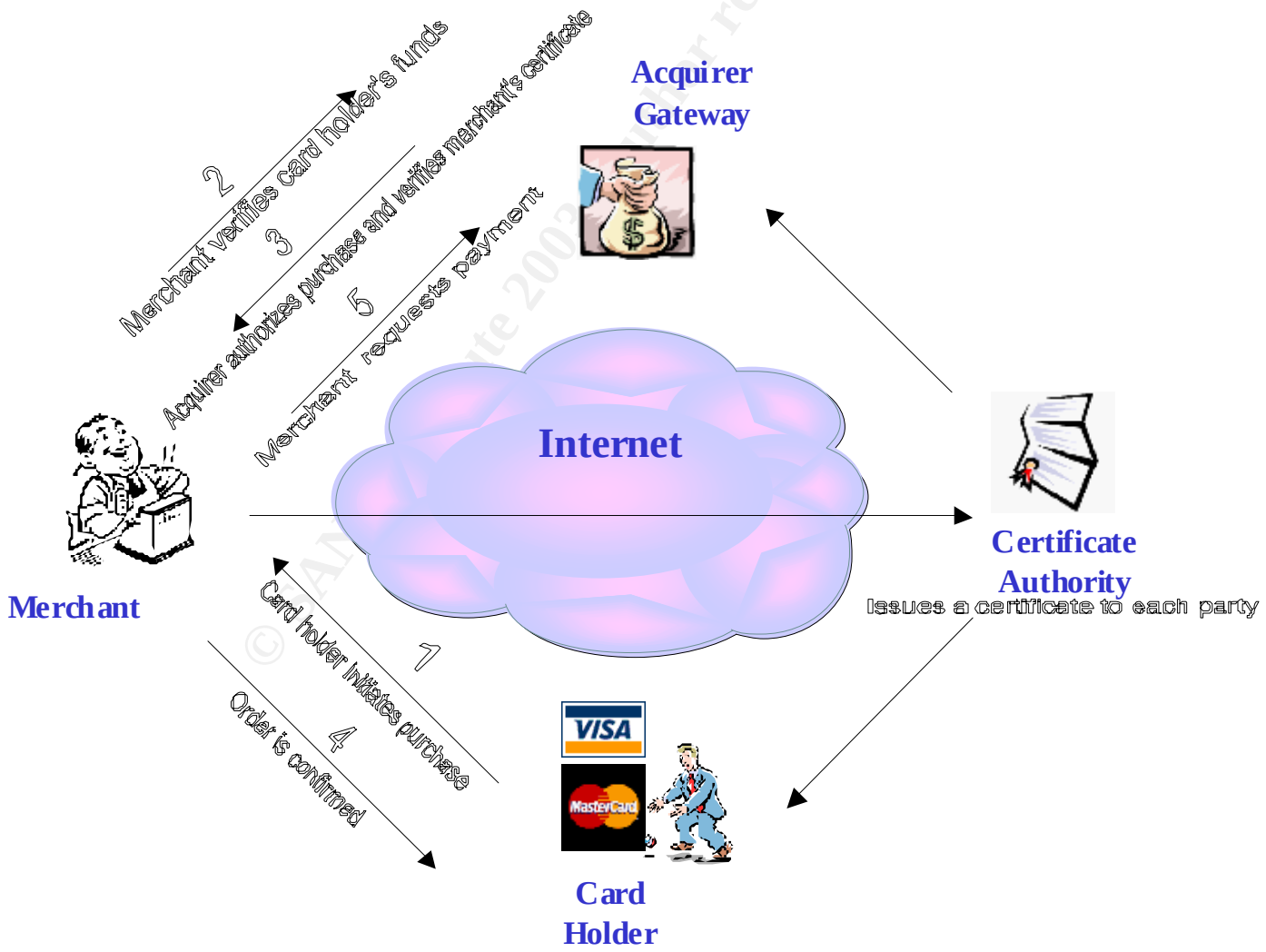
So the SET protocol combines two best two encryption methods to achieve SET cryptography level. It does so by encrypting the message data using a randomly generated symmetric DES encryption key. This key is, in turn, encrypted using the message recipient's RSA public key. The second one is the "digital envelope" of the message and is sent to the recipient along with the encrypted message itself. After receiving the digital envelope, the recipient decrypts it using his own private key and obtains the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

The *integrity* is assured by using one-way cryptographic hashing algorithms and digital signatures. A hashing algorithm is a function used to calculate a unique integrity value, called the hash value or message digest, from the original data ie. the message. But the hash function by it self does not guarantee absolute data integrity. For this it needs to be combined with a secret encryption key. Here is where digital signing comes into the picture.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Authentication deals with assuring that the message was in fact sent by the party who claims to have sent it. Each party in a SET transaction is authenticated by the use of digi tal certificates. These certificates are issued by a trusted third party known as a Certification Authority (CA), which vouches for the identity of the certificate holder. Each digital certificate contains both owner identification information, and a copy of one of the owner's public keys. Furthermore each certificate is digitally signed by the Certificate Authority to ensure it's validity. To administrate the validity of all certificates an hierarchy of trust has been constructed.

SET in Action :



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Above figure depicts the components and phases of SET processes. There are several parties involved each having a role for an end to end secured transaction. First, there is the customer/cardholder and the mercha nt this cardholder wishes to purchase something from. Then there is the Acquirer, which is a financial institution that supports the card brand/s that the merchant accepts as payment. The acquirer is responsible for all the necessary financial transactions between the cardholder's and merchant's banks, and makes sure the merchant gets paid. Finally there is the Certificate Authority, who issues digital certificates to all the parties involved so that they can identify each other properly.

The cardholder, after browsing the electronic store and made the purchasing decision, selects SET as the form of payment and starts the transaction. Then the SET protocol initiates the following steps:

1. The merchant's software sends the cardholder the digital certificate of the merchant for the card's brand.
2. Then the cardholder's software the **"wallet"** identifies correspondant parties, encrypts cardholder's digital certificate and the payment agreement and sends this information to the merchant.
3. The merchant issues an authoriz ation request to the acquirer after decrypting only the payment agreement fields and meanwhile the users account information still encrypted. This is important because SET protocol keeps the cardholder's card information hidden from the merchant, which mak es SET shopping safer than face-to-face shopping, and no doubt much safer than mail or telephone ordering (MOTO). The customer information with SET is only available to the Bank.
4. Upon receipt of the authorization request from the merchant, the acquirer dec rypts it and requests authorization from the cardholder's bank for the amount of the purchase. Getting the confirmation, the acquirer encrypts the message and forwards it to the merchant.
5. The merchant's software then, checks for the authorization, encrypts and sends the response to the cardholder's wallet application.
6. The merchant requests payment from the cardholder's bank via the acquirer.

SET seems to work out many problems both for the merchant selling goods over the Internet, and for the customers purc hasing goods from online storefronts. The fraud possibility is significantly minimized and cardholders gained confidence to shop on the net. Besides it is excellent for the merchant, as he will know not only that he can release the goods, but also that he will receive payments for those goods. SET brings the biggest advantage probably to the card issuer who have otherwise the most to lose from fraud.

Digital Certificate and Digital Signature:

Digital certificate is an electronic identification that prove s the user is really the one, who he or she claims to be. It's issued by a bank, clearinghouse or a recognized Certificate Authority and contains information about the user.

Digital Certificates allows the customer's transaction to be individually authent icated by matching unique card numbers to customer -unique information like date of birth, mother's maiden name, and so on, held within the PC. When there is no match the transaction is not

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

authorized. Digital Certificate also contains basic financial information, the issuer's financial information, and some encryption data.

For SET to work, not only cardholders but also merchants receive unique Digital Certificates. In this case, with the certificate the transactions between the merchant and the financial institution that issued the card are authenticated. Certificates will be transmitted to merchants along with purchase requests and encrypted payment instructions. The merchant can, on receiving a certificate, be assured at a minimum that the account number has been validated by the card sponsor or its agent.

It should be noted that, a certificate does not stand by itself. In fact, related with every certificate granted by a Certification Authority (CA) there is the CAs own digital signature - and behind that signature may be an association signature, and so on, back to a root signature known and acknowledged by all implementors of SET software. This makes spoofing of certificates extremely unlikely.

The digital signature on the other hand is a code, that guarantees a sender's identity. Within the SET description it is noted that the Digital Signature that applies to a particular cardholder will not change and it is permanent information that is directly coupled with the physical card itself. Therefore if an unauthorized person decrypts it, the digital signature will be altered and the recipient will know of the intrusion. SET method for Digital Signatures first encrypts only a digest (hash value) of a message with the *senders private key*, and appends it to the original message. Then the whole message, including the signature, is encrypted with the *recipients public key*.

SET brings a new concept of Digital Signatures; that is the "Dual Signatures". When there are more than one message within a transaction which are to be handled as seperate steps, two signatures are generated at once to cover each step. For example an order message linked with a payment instruction is a very specific application area for this technique.

How safe is SET?

The encryption algorithm SET uses 1,024-bits. This is really a very strong encryption technique especially in public use. The time it would take to break this encryption especially with all the various level of encryption that are occurring, is upwards to 2,800,000,000,000 years using 100 computers each able to process 10,000,000 instructions per second. Even then, only a single message could be broken and with the next message, the entire process would need to start over.

SET has been approved for export from the US, provided that it's only used in financial transactions, and not as a mechanism to pass secret or sensitive information to those outside the US.

With SET, parties involved in a transaction only get information that is necessary for them to complete their side of the transaction. The online merchant does not get the credit card number. This goes directly to the credit institution who just informs the merchant whether the transaction has been approved or not. SET reduces the risk of the merchant misusing a credit

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

card or accidentally giving access to a hacker. This makes SET payment, much safer than face-to-face shopping.

The credit institutions are usually very reputable institutions operating at the highest levels of security. SET has been endorsed by most of the major banking institutions.

Conclusion:

All through the years since it was first announced by Visa International and MasterCard in beginning of 1996, SET today has mature technical specifications and has a very wide market acceptance. Today all components of SET, have the ability to process SET secured transactions. There are already products for each component; Certificate Authorities, Payment Gateways, merchants and cardholders, which make the system succesfully run.

SET is safer than other payment methods and the insecurity barrier in front of e-commerce is getting pulled down.

References:

1) SET Secure Electronic Transaction LLC web site
www.setco.org/setmark.html

2) Eric Wolrath's web site

www.wolrath.com/set.html

3) Mastercard International web site

www.mastercardintl.com/newtechnology/set

4) National Electronic Commerce Resource Center Technology Update web site

www.tda.ecrc.ctc.com/kbase/doc/update/setspecs.htm

5) Trintech web site

www.trintech.com/whatsnew/what_is_set.html

6) VISA web site

www.visa.com/nt/ecomm/set/main.html#set

www.visa.com/nt/ecomm/set/setsafe.html

7) eStartupHelp web site (A community for e-commerce startups)

www.esartuphelp.com/privacy1.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**