Global Information Assurance Certification Paper

Secure Electronic Transactions (SET)™

Christopher Cross

November 2, 2000

In the world of e-commerce, there is a continuing need to create a safe and trusted purchasing environment for consumers, merchants, and financial institutions alike. One possible solution being presented and tested is Secure Electronic Transaction (SET)™. SET is a messaging protocol designed to provide a mechanism to secure electronic credit card payments over open, unsecured networks such as the Internet. Visa and MasterCard developed SET, with participation from several technology companies, including Microsoft, IBM, NetScape, SAIC, GTE, Terisa Systems and VeriSign. SET utilizes encryption technology using RSA key algorithms to secure the information.

To utilize SET in a transaction, the cardholders are required to install an e-wallet on their machines. The e-wallet is basically an online version a physical wallet that is used to store and encrypt credit-card numbers and other information. The e-wallet is used by the cardholders Web browser to make an SET purchase by interacting with a merchants storefront and point of sale application. On the merchant side, they need to install point of sale software to support their Web servers and storefront applications. Additionally, the cardholders and merchants must receive digital certificates from their respective card-issuing financial institutions. Once the cardholders have received the electronic credit card and digital certificate, purchases can be made from the SET compliant merchants. A typical SET transaction would proceed in a manner similar to the one outlined below.

- Consumer has made a purchase and initiates a payment transaction.
- A private session key is negotiated between the consumer's browser and the merchant's server using public key cryptography.
- The consumer places his order information, electronic credit card data, and his digital certificate into an electronic "envelope".
- The envelope is encrypted using the negotiated session key and is sent to the merchant.
- The merchant opens (decrypts) the envelope and extracts the order information.
- The merchant places the consumer's electronic bankcard and digital certificate, along with the merchant's own digital certificate, into an electronic envelope and is sent to an "Acquirer".
- Once the consumer's and the merchant's identities have been verified, the acquirer validates the electronic credit card with the issuing bank.
- Upon validation, the acquirer issues an authorization to the merchant.
- The merchant completes the transaction with the consumer (by shipping goods or authorizing services, etc.).
- The merchant will request settlement from the acquirer who will then authorize the electronic credit card institution to release funds to the merchant's bank.

SET provides several advantages over other methods. SET uses X.590 digital certificates that provides for an internationally recognized hierarchy of trust. The root certificate, that is known to all SET software and ensures the identities of all parties involved, tops this hierarchy. By ensuring all identities, a trusted purchasing environment can be provided. Another advantage is ability of SET to handle multi-party transactions. Most transactions will involve five parties - the cardholder, the merchant, the cardholder's bank, the merchant's bank, and the credit card provider. Other protocols such as SSL can only handle one-to-one transactions. Limiting the merchant's access to the cardholder's credit card details is another advantage. The merchant can read information that pertains to the cardholder's electronic order only and receive approval codes from their banks without ever seeing the consumer's credit card details. This means that SET transactions are more secure and private than when the consumer provides their credit card in-person or during a phone transaction.

SET has some disadvantages versus other methods too. Rollout of SET has been slow and transaction speed continues to be a question. The inclusion of the various elements (Certificate of Authority, Acquirers, and e-wallets) creates a more complex transaction environment, increased costs, as well as the increased processing time for the transaction approval process. In addition, despite more public awareness, consumers are still slow to implement the use of e-wallets.

SET addresses security holes that exists in other payment methods. Rather than just providing a secure channel for transmitting data, SET utilizes digital certificates, e-wallets, Certificate Authorities, and acquirers to provide security and privacy for the cardholder's information. SET fills holes in authentication caused by United States limits on encryption key lengths and appears to negate the threat of web spoofing since the acquirer authenticates all parties involved. Data integrity problems are mitigated by the use of message digests as well as the use of public key cryptography appears to provide another method to negate the threat of web spoofing.

Despite the limited acceptance in the United States, SET has enjoyed some success in Europe and Asia. In response to marketplace concerns, extensions to the original SET specification have been developed. These enhancements attempt to make SET useful and viable to a broader base of users. Business functions not addressed in the original specification may be included by the use of approved SET extensions that do not compromise the security, integrity, or performance of the protocol. Some of the extensions recently approved allow:

- Processing of transactions that use the SSL protocol for transport, to allow merchants and payment processors a single payment-processing platform.
- Transactions stored on smart cards
- Debit card functionality

In addition to the use of SET extensions, there are other methods for the SET standard to gain wider acceptance. For example, instead of replacing existing payment methods, SET can be used on the backend. Merchants can continue to use their existing point of sale and storefront applications without having to deploy e-wallet software to consumers. Hosted payment gateways to reduce some of the hardware costs associated with implementation are another.

Despite the increased security and reduction in the possibility for online fraud, the increased costs associated with implementing SET will make it cost prohibitive for most merchants, particularly the smaller ones. The goal to create a safe and trusted purchasing environment for consumers, merchants, and financial institutions alike will not be met until the battle over electronic transaction standards is won.

"SET Basics." E-Commerce 101. URL: http://www.ipier.com/ecom101/SET-basic.html (11/02/2000).

"Frequently Asked Questions About SET."
URL: http://www-s2.visa.com.au/nt/abt_set/faq.html (11/02/2000).

Pei, Gan Sze. "Cryptography with SET and SSL." CP3070 : Report E-Commerce Security. URL: http://www.cs.jcu.edu.au/~pei/cryptography.htm (11/02/2000).

"Secure Socket Layer (SSL) vs. Secure Electronic Transaction (SET™)."
URL: http://www.paradata.com/onpay_setvsssl.html (11/02/2000).

"Encryption Protocols." Assignment 3B.
URL: http://magrathea.citywest.unisa.edu.au/ec1998s3/8726837U//ass3/index.html (11/02/2000).

"Security Issues of Internet Commerce."
URL: http://students.depaul.edu/~cbarron/secwind2.html (11/02/2000).

URL: http://www.visa.com (11/10/2000).

URL: http://www.setco.org (11/06/2000).

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event