Introduction

This web page is an informational page containing information about the secure electronic transaction protocol (SET). The following information is intended for an audience with some background in the area of computer networks. However, if the reader is unfamiliar with or possesses no prior knowledge of computer networks, a glossary of frequently used terms is provided to help the reader become more acquinted with the subject.

OverView: What is SET?

The Secure Electronic Transaction protocol also know as SET is a method for providing secure credit card transactions on the Internet. The SET protocol is designed to operate both in real time, as on the World Wide Web, and in a store-and-forward environment, such as e-mail. Furthermore, as an open standard, SET is designed to allow consumers, merchants, and banking software companies to independently develop software for their respective clienteles and to have them interoperate successfully.

However, inorder for secure transactions to work, SET must possess the following qualities:

- Confidentiality: others cannot eavesdrop on an exchange.
- Integrity: the messages received are identical to the messages sent.
- Authenticity: you are assured of the persons with whom you are making an exchange.
- Non-Repudiability: none of the involved parties can deny that the exchange took place.

In addition to these four requirements, SET also assumes that that a hierarchy of certificate authorities that can vouch for the bindings between a user and a public key already exists. Therefore, consumers, merchants, and acquirers must exchange certificates before a party can know what public key to employ to encrypt a message for a particular correspondent.

Finally, the following is a diagram of how the the Secure Electronic Transaction protocol works, and a description of each step of the transaction.

The SET protocol like any other protocol operates via a sequence of message exhanges. There is a total of ten steps (message exhanges) taken for a transaction, and the parties involved include the consumer, vendor, and a network of banks. The following are the ten steps taken during an electronic transaction:

- In the first two message exchanges between the consumer and merchant, the consumer and merchant signal their intention to do business.

They then exchange certificates and establish a transaction ID number. From this both the consumer and merchant will be able to extract each others public key and verify that they are indeed talking to who the other side claims to be.
- In the third step following the initial handshake, the consumer sends a purchase request to the merchant containing the signed hash of the goods and services order, which is negotiated outside the protocol. This request is accompanied by the consumer's credit card information, encrypted so that only the merchant's acquiring bank can read it.
- At this point, the merchant has to choice of either acknowledging the order request of the customer first and seek authorization later, or it can perform authorization first and then confirm the customer's order request.
- Steps five and six of the protocol involves the authorization of the customers order request. The authorization process work as follows. The vendor will send the consumers request to its acquiring bank. The acquiring bank will reformat the request and send it over a bankcard network to bank that issued the consumers credit card. The issuer bank will then respond to the acquiring bank with its response and the acquiring bank will forward the outcome to the vendor.
- Steps seven and eight gives the consumer a query capability allowing them to check on the status information of the purchase.
- Finally, steps nine and ten allows the merchant to submit authorizations for capture and settlement. The process works as follows: At the time of the delivery of goods or services, merchant will submit a capture request to its own acquiring bank to obtain payment. This request is then forwarded by the acquiring bank over the bankcard network to issuing bank for settlement of payment.

Related Information

- Glossary - This page contains a glossary of frequently used terms.
- NetBill Paper - This page contains a technical report regarding a particular electronic transaction protocol know as NetBill.

Annotated Links

The following is a summary of the sources that I have used in the creation of this site. Unless otherwise stated the intended audience for each of the following sites is someone with a background and understanding of computer networks:

- Secure Transaction and the Internet - This is a page from the Purdue University Computer Science department. It is a brief tutorial describing the characteristics that are needed inorder for secure transaction to exist on the Internet. It also briefly describes the security issues involved and how to address them. This is not a very recent page being last modified on 8/12/1996.

- Secure Electronic Transaction - This is another page from the Purdue University Computer Science department. This is a very short page providing a skeleton overview of the workings of SET. This is not a very recent page being last modified on 8/12/1996.

- Network Definitions - This page althought not specifically related to SET is a good reference page providing an extensive list of network definitions. This is a great page to take a look at for those who do not have a strong background in computer networks. It is unkown how recent this document is and when it was last modified.

- SET-VISA - This a commercial page from Visa providing a description of how Secure Electronic Transaction works. This is a medium length page explaining how SET works and the processes and mechanisms involved. However, this is not a very technical page, rather the contents are intended for a general audience. How recent this page is and when it was last modified is also unkown.

- Set Standard Specification - This page provides three downloads in either Microsoft Word for Windows format, Adobe Acrobat, Microsoft Word for Mac in SIT format, and Microsoft Word for Windows in ZIP format. All three documents are intended for an advanced reader who possesses advanced knowledge in this area. The three downloads are:
  - BOOK1: Business Description - This download contains a very detailed description of the SET protocol. It covers in detail all aspects of the protocol from its basic concept to the purchasing process. This document is very detailed and technical at times. Also this document is very lengthy, the Microsoft Word for Windows in ZIP format when unzipped contains eight Microsoft word documents averaging 30 pages each.
  - BOOK2: Programmer's Guide - This is another download, and like BOOK1, this document is also extremely detailed and lengthy serving as a programmer's guide to SET. The contents are very technical and specific.
  - BOOK3: Formal Protocol Definitions - This download provides a technical specification of the SET protocol. This document is very detailed and specific, and the entire document is in psuedo code outlining how the protocol works. This is a very long document. The Microsoft Words for Windows version contains 259 pages.

  How recent this page is and when it was last modified is unkown.

- SET CMU - This is a page form Carniege Mellon University giving a very brief overview of the SET protocol and some of the problems that it poses. This page was last modified on 4/18/1997.

- SET Transaction - This is another page from Carneige Mellon providing a description of the steps involved in a SET transcation. This page was last modified on 4/18/1997.

- NetBill - This is the official NetBill protocol homepage. This page offers a complete description of the NetBill protocol. It also provides many visual descriptions and examples as well. The information available at this site is quite extensive. This page was last updated on 10/28/1997.

- NetBill USENIX - This paper appears in Proceedings of the First USENIX Workshop on Electronic Commerce. This page is similar to a RFC in format and provides a very detailed outline of how the protocol works. The contents of this document are pretty advanced and is intended for someone with a strong understanding of computer networks. This page was last modified on 5/7/1998.

- NetBill Overview - This document was prepared for the March 1995 IEEE CompCon Conference. This paper discusses the design of the NetBill protocol and the implementation of the protocol for the World Wide Web (WWW). This page was last updated on 5/7/1998.

If you have any questions or comments please send me an e-mail.
Last updated 11/9/1998.