

B211 Internet Computing

SSL, SET and Electronic Payment Systems

B211 Week 12 Lecture 2: SSL, SET and EPS

1

Lecture Outline

- Secure E-Commerce Transactions
- S-HTTP
- Secure Socket Layer (SSL)
- Secure Electronic Transaction (SET)
- Digital Cash

B211 Week 12 Lecture 2: SSL, SET and EPS

2

Support for Electronic Commerce Services

- Most e-commerce services involve financial transactions and system of payment, and a lot of it takes place through the web.
- Security is major consideration, since most transactions are confidential.

B211 Week 12 Lecture 2: SSL, SET and EPS

3

Early Web Merchant Services

- Early web services for commerce involved:
 - HTML versions of order forms, viewed through the browser, then printed, filled and returned by ordinary mail.
 - Catalogs in HTML for on-line viewing.
- The next step
 - Submit orders on-line – front-end HTML forms, back-end CGI.
- Then came
 - *Shopping cart applications*
 - user browse multiple on-line catalogues, put items in a shopping cart, and purchase all the items at the end .

B211 Week 12 Lecture 2: SSL, SET and EPS

4

Secure HTTP (S-HTTP)

- Using normal HTTP is very insecure as HTTP transfers data unencrypted
 - not appropriate for billing information and credit card transactions.
- S-HTTP produced by Enterprise Integration Technology (EIT) extends HTTP by
 - Allowing clients and servers to sign, authenticate, and encrypt HTTP packets.
 - Uses extra HTTP headers to indicate required processing for signing, authentication and encryption/decryption.
 - Adds additional data to the HTTP packet to store certificate and encryption key information.

B211 Week 12 Lecture 2: SSL, SET and EPS

5

Secure Socket Layer (SSL)

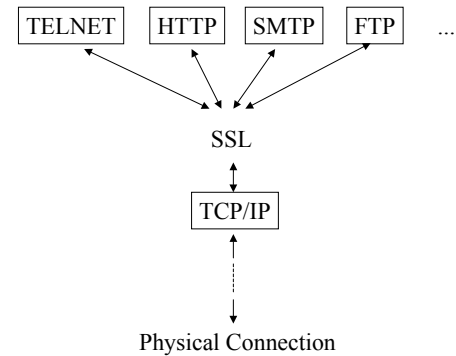
- SSL is the most dominant web cryptographic protocol for general browser/server communication today.
- Originally introduced by Netscape in Navigator 1.0, and later adopted by Microsoft for Internet Explorer.
 - All major browsers supports SSL.
- Overtook S-HTTP as the cryptographic system of choice.

B211 Week 12 Lecture 2: SSL, SET and EPS

6

SSL Characteristics

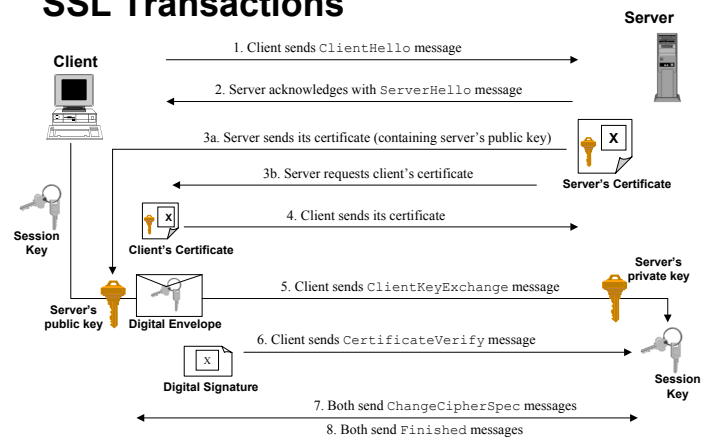
- Operates on the transport layer of TCP/IP
 - as oppose to S-HTTP which operates only on HTTP at the application layer
 - This means it will be able to secure messages from all possible protocols beside HTTP
 - see next diagram



SSL Characteristics (cont'd)

- An SSL connection offers a choice of cipher suite
 - When an SSL client first contacts a server, they negotiate which *cipher suite* (encryption algorithms, digest functions and authentication methods) to use
 - they pick the strongest set both client and server can support.
- During an SSL session, all communication are encrypted.

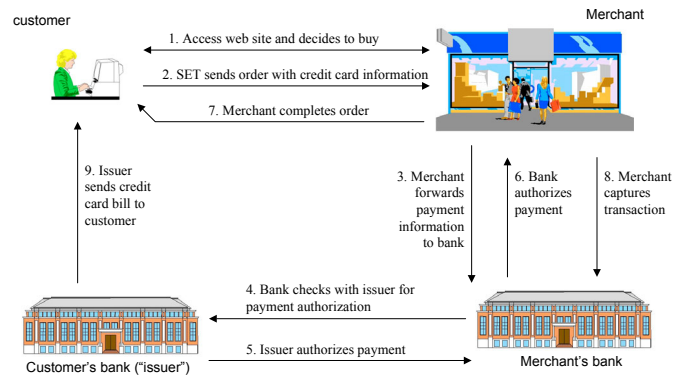
SSL Transactions



Secure Electronic Transaction (SET)

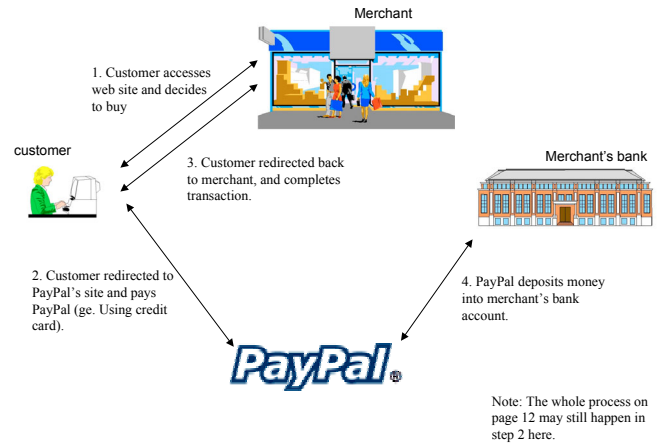
- SET is a protocol for electronic credit card payment.
 - It only works within the credit card system.
- Developed by a consortium of companies led by MasterCard, Visa, Netscape and Microsoft.
- Provides a lot of high-level services specific to card transactions, eg.
 - Cardholder registration
 - Merchant registration
 - Purchase request
 - Payment Authorisation
 - Funds Transfer
 - Refunds to customers
 - Credits

SET in a Credit Card Transaction



Payment Intermediaries

- Instead of a merchant implementing their own payment systems, there are also intermediary companies today that does it for the merchant.
 - Eg. PayPal (<http://www.paypal.com>)
 - Only works because both customer and merchant are willing to sign-up to PayPal. Like all network systems, no matter how good it is technically, it will only be successful if there are enough people on the system. PayPal has about 33,000 web sites using it.



Digital Cash

- There are also other possible forms of payment systems which are electronically based, but not tied to off-line systems.
- *Digital Cash* involves using encrypted packets (eg containing digital certificates) to represent money, which can be transferred to cover payments
 - Unfortunately in the end, institutions such as banks still need to provide the monetary value for these electronic payments.
 - They also suffered from the lack of uniform standards, resulting in users having to store their electronic money in multiple systems to use them.

Digital Cash (cont'd)

- Not many digital cash systems are in use today.
- Some previously much publicized systems:
 - CyberCash (<http://www.cybercash.com>)
 - eCash (<http://www.ecash.net/>)

On-line Frauds

- Mechanisms such as SSL and SET have made on-line financial transactions as safe (and in certain cases more safe) than off-line ones.
 - Eg. read <http://www.noie.gov.au/projects/consumer/index.htm#fraud>
- Like conventional payments, how secure the on-line transaction is usually depends more on human procedures, rather than the technology.
 - Eg. how carefully the operators handles print-outs of credit card information.