HTTP Secure

Hypertext Transfer Protocol Secure (**HTTPS**) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

- The **Hypertext Transfer Protocol** (**HTTP**) is an Application Layer protocol for distributed, collaborative, hypermedia information systems. HTTP is a request/response standard typical of client-server computing. In HTTP, web browsers typically act as clients, while an application running on the computer hosting the web site acts as a server. The client, which submits HTTP requests, is also referred to as the *user agent*. The responding server, which stores or creates *resources* such as HTML files and images, may be called the *origin server*.

- SSL (***S**ecure **S**ockets **L**ayer)* a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http*:.

Web Security

- Basic Authentication
- Secure Socket Layer (SSL)

Basic Authentication

A simple user ID and password-based authentication scheme, and provides the following:

- To identify which user is accessing the server
- To limit users to accessing specific pages (identified as Universal Resource Locators, URLs

Secure Socket Layer (SSL)

- Netscape Inc. originally created the SSL protocol, but now it is implemented in World Wide Web browsers and servers from many vendors. SSL provides the following
  - Confidentiality through an encrypted connection based on symmetric keys
  - Authentication using public key identification and verification
  - Connection reliability through integrity checking
- There are two parts to SSL standard, as follows:
  - The SSL Handshake is a protocol for initial authentication and transfer of encryption keys.
  - The SSL Record protocol is a protocol for transferring encrypted data

Secure Socket Layer Cont..

- The client sends a "hello" message to the Web server, and the server responds with a copy of its digital certificate.
- The client decrypts the server's public key using the well-known public key of the Certificate Authority such as VeriSign.
- The client generates two random numbers that will be used for symmetric key encryption, one number for the receiving channel and one for the sending channel. These keys are encrypted using the server's public key and then transmitted to the server.
- The client issues a challenge (some text encrypted with the send key) to the server using the send symmetric key and waits for a response from the server that is using the receive symmetric key.
- Optional, server authenticates client
- Data is exchanged across the secure channel.

- **Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
- TLS is an IETF standards track protocol

- The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. TLS provides RSA security with 1024 and 2048 bit strengths.

protocol

- An agreed-upon format for transmitting data between two devices. The protocol determines the following:
- the type of error checking to be used
- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message
- There are a variety of standard protocols from which programmers can choose. Each has particular advantages and disadvantages; for example, some are simpler than others, some are more reliable, and some are faster.

Cryptographic protocol

- A **security protocol** (**cryptographic protocol** or **encryption protocol**) is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods.
- A protocol describes how the algorithms should be used. A sufficiently detailed protocol includes details about data structures and representations, at which point it can be used to implement the security check.
- Cryptographic protocols are widely used for secure application-level data transport. A cryptographic protocol usually incorporates at least some of these aspects:
- Key agreement or establishment
- Entity authentication
- Symmetric encryption and message authentication material construction
- Secured application-level data transport
- Non-repudiation methods

Blind signature

- A **blind signature**, is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

digital cash

- A system that allows a person to pay for goods or services by transmitting a number from one computer to another. Like the serial numbers on real dollar bills, the digital cash numbers are unique. Each one is issued by a bank and represents a specified sum of real money. One of the key features of digital cash is that, like real cash, it is anonymous and reusable. That is, when a digital cash amount is sent from a buyer to a vendor, there is no way to obtain information about the buyer. This is one of the key differences between digital cash and credit card systems. Another key difference is that a digital cash certificate can be reused.

Electronic money

- **Electronic money** (also known as **e-currency**, **e-money**, **electronic cash**, **electronic currency**, **digital money**, **digital cash** or **digital currency**) refers to money or scrip which is exchanged only electronically. Typically, this involves the use of computer networks, the internet and digital stored value systems. Electronic Funds Transfer (EFT) and direct deposit are all examples of electronic money. Also, it is a collective term for financial cryptography and technologies enabling it.

Passes/Farecards
See map or kiosk for fare
Each passenger 5 and older needs a farecard to enter and exit all stations
SELECT PURCHASE
1
MAXIMUM CHANGE: $5.00
CANCEL
COINS
AUDIO
PRESS + TO ADD VALUE
PRESS – TO DEDUCT VALUE
PUSH TO RETURN
INSERT PAYMENT
2
TARGET
BILL RETURN
TRADE IN FARECARD
3
TAKE PASS/FARECARDS
COIN RETURN

Electronic funds transfer

- **Electronic funds transfer** or **EFT** refers to the computer-based systems used to perform financial transactions electronically.
- The term is used for a number of different concepts:
- Cardholder-initiated transactions, where a cardholder makes use of a payment card
- Direct deposit payroll payments for a business to its employees.
- Direct debit payments from customer to business, where the transaction is initiated by the business with customer permission
- Electronic bill payment in online banking.
- Transactions involving of electronic money, possibly in a private currency
- Wire transfer via an international banking network (generally carries a higher fee)
- Electronic Benefit Transfer

Financial transaction

- A **financial transaction** is an event or condition under the contract between a buyer and a seller to exchange an asset for payment. In accounting, it is recognized by an entry in the books of account. It involves a change in the status of the finances of two or more businesses or individuals.

- Peer-to-peer payment systems are extremely popular. The best and most widely known example is PayPal. PayPal allows you to pay for just about anything online as long as the seller also has a PayPal account. Many online sellers use PayPal such as 75% of eBay sellers, overstock.com, ritzcamera.com, and Walgreens.com. PayPal is also sometimes used to pay for personal debts in situations where both parties have an account