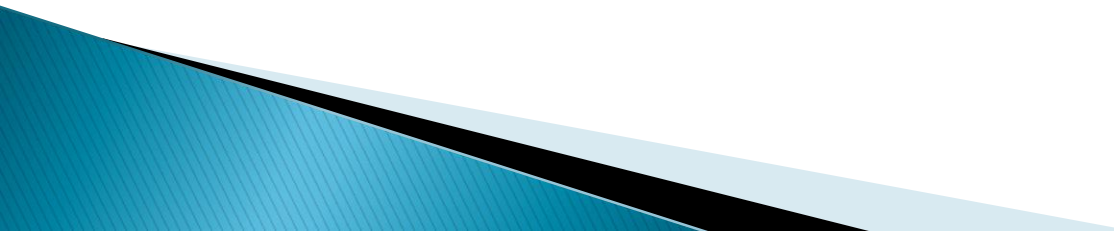


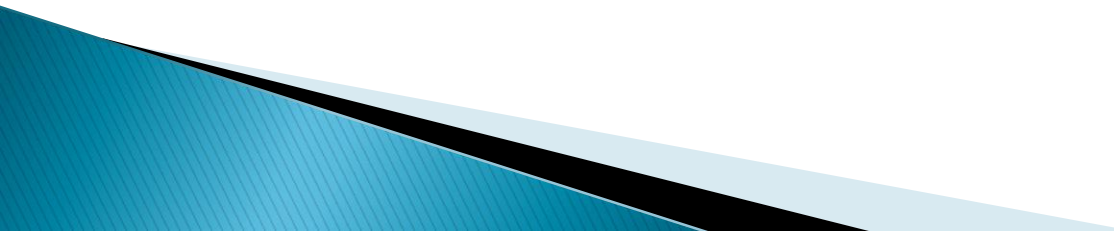
The Secure Sockets Layer (SSL) Protocol



Overview

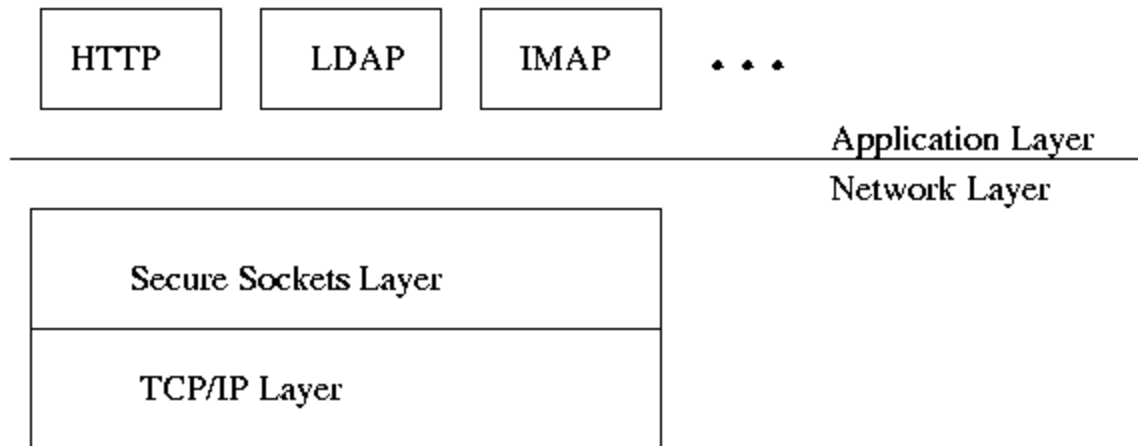
- ▶ What is SSL?
 - ▶ How does SSL work?
 - ▶ How to implement SSL?
 - ▶ Summary and Comments.
- 

What is SSL?

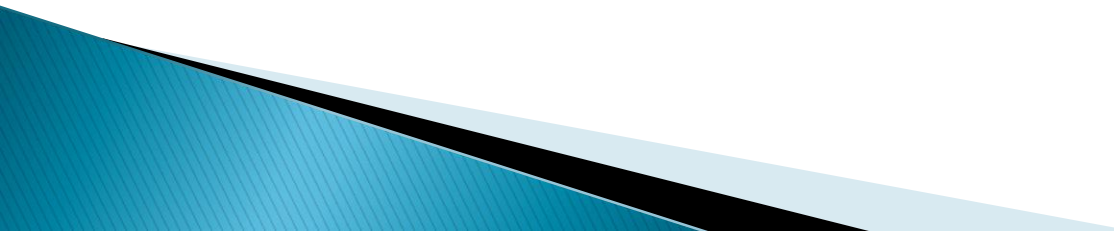
- ▶ A protocol developed by Netscape.
 - ▶ It is a whole new layer of protocol which operates above the Internet TCP protocol and below high-level application protocols.
- 

What is SSL?

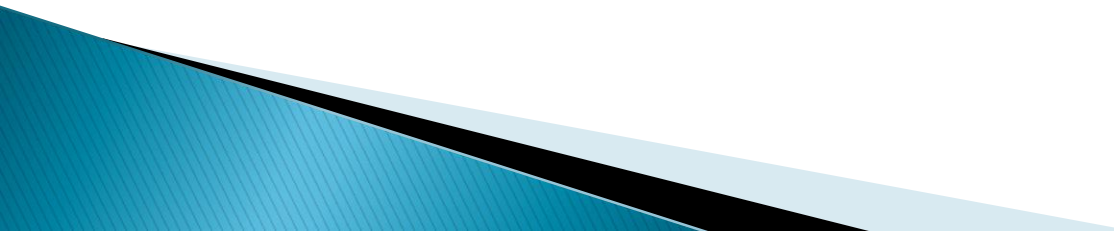
Figure 1 SSL runs above TCP/IP and below high-level application protocols

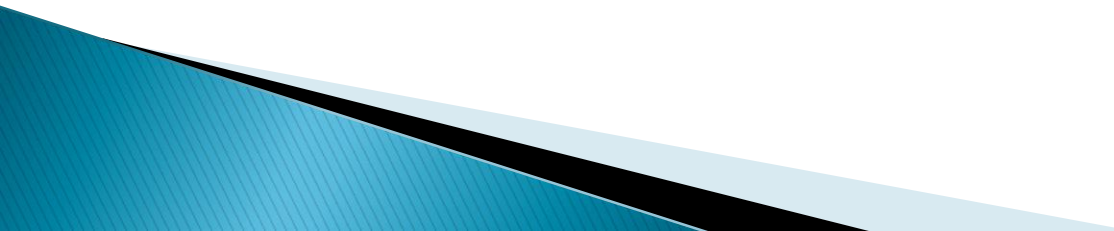


What Can SSL Do?

- ▶ SSL uses TCP/IP on behalf of the higher-level protocols.
 - ▶ Allows an SSL-enabled server to authenticate itself to an SSL-enabled client;
 - ▶ Allows the client to authenticate itself to the server;
 - ▶ Allows both machines to establish an encrypted connection.
- 

What Does SSL Concern?

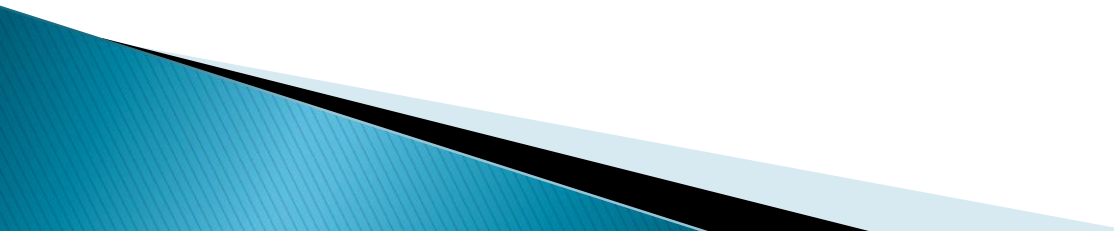
- ▶ SSL server authentication.
 - ▶ SSL client authentication. (optional)
 - ▶ An encrypted SSL connection or Confidentiality. This protects against electronic eavesdropper.
 - ▶ Integrity. This protects against hackers.
- 

- ▶ SSL includes two sub-protocols: the SSL Record Protocol and the SSL Handshake Protocol.
 - ▶ Record Protocol -- defines the format used to transmit data.
 - ▶ Handshake Protocol -- using the Record protocol to exchange messages b/t an SSL-enabled server and an SSL-enabled client.
- 

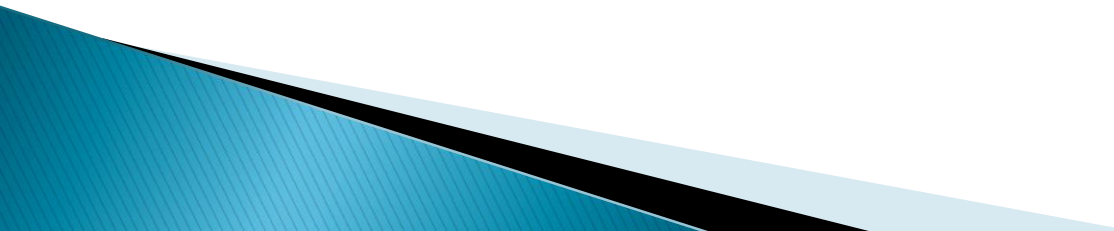
- ▶ The exchange of messages facilitates the following actions:

Authenticate the server to the client; Allows the client and server to select a cipher that they both support; Optionally authenticate the client to the server; Use public-key encryption techniques to generate share secrets; Establish an encrypted SSL conn.

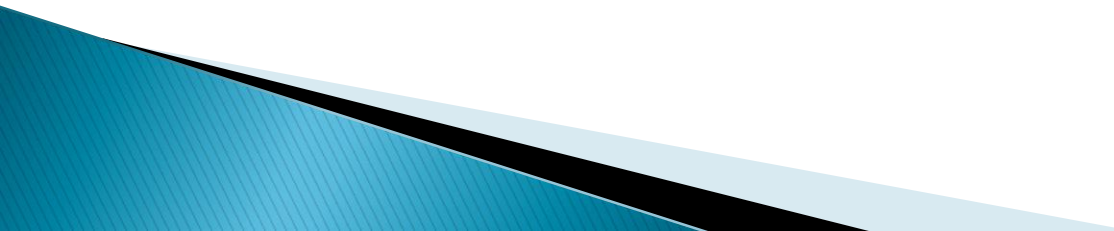
Two Useful Terms

- ▶ A certificate.
 - ▶ A certificate has the following content:
 1. The certificate issuer's name
 - ▶ 2. The entity for whom the certificate is being issued (aka the subject)
 - ▶ 3. The public key of the subject
 - ▶ 4. Some time stamps
- 

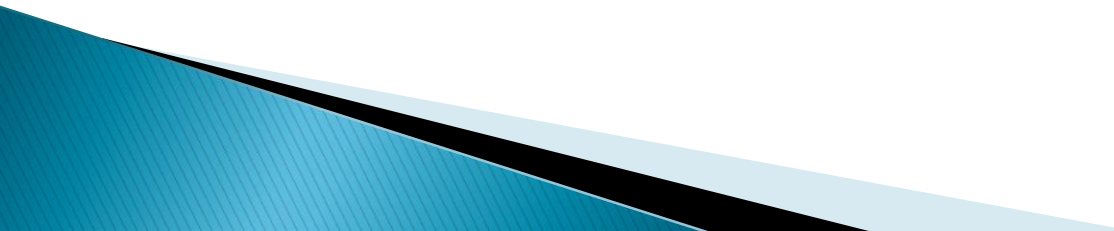
Two useful Terms

- ▶ A digit signature -- A message digest derived from the original one, has following important properties:
 - ▶ 1. The digest is difficult to reverse
 - ▶ 2. It is hard to find a different message that computed to the same digest value.
- 

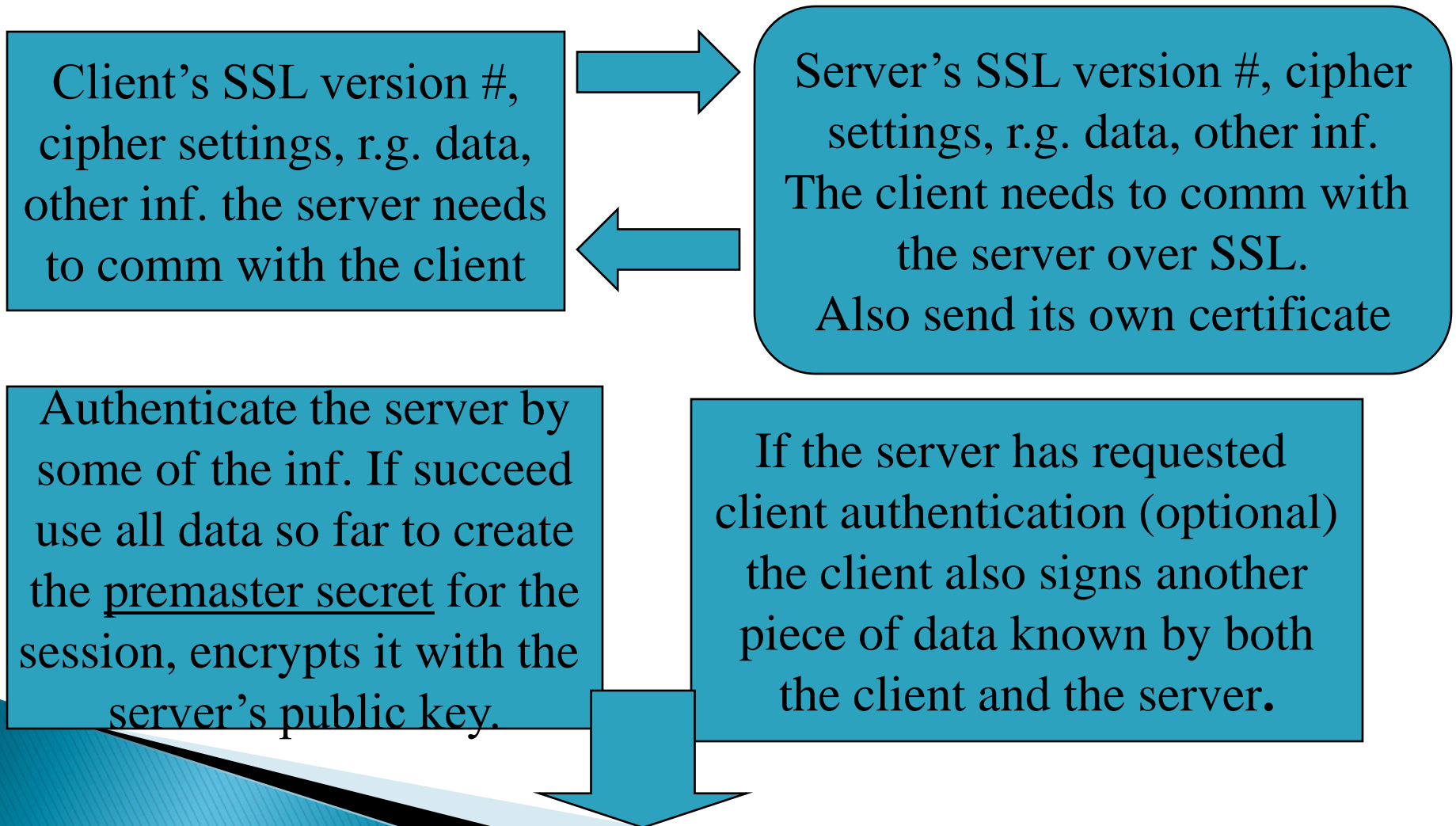
How does SSL Work?

- ▶ How a client and a server create a secure connection?
 - ▶ The SSL protocol uses RSA public key cryptography for Internet Security.
 - ▶ Public key encryption uses a pair of asymmetric keys for encryption and decryption.
- 

How does SSL Work?

- ▶ Each pair of keys consists of a public key and a private key. The public key is made public by distributing it widely; the private key is always kept secret.
 - ▶ Data encrypted with the public key can be decrypted only with the private key, and vice versa.
- 

How Does SSL Work?



If the server has requested client authen., the server attempts to authen the client. If succeed, uses its private key decrypt the premaster secret, then perform a series of steps to generate the master secret
Use the master secret to generate the session keys.

Also performs a series of steps, starting from the same premaster secret to generate the master secret.

Use the master secret to generate the session keys

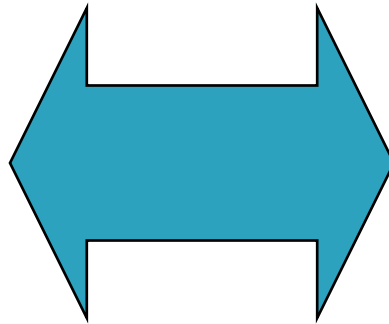


Session keys are used to encrypt and decrypt information exchange during the SSL session and to verify its integrity.

Master secrets protect session keys in transit.

Informing the server
that the future
message from here
will be encrypted with
the session key.

Then sends a separate
(encrypted) message
indicating that the
client portion of
handshake is finished.



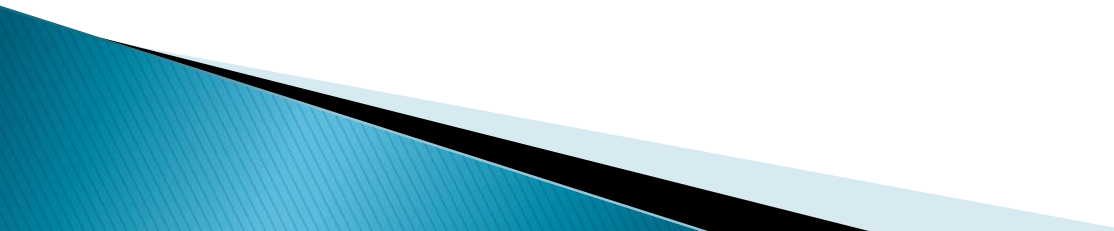
Informing the client
that the future message
from here will be
encrypted with the
session key.

Then sends a separate
(encrypted) message
indicating that the server
portion of handshake
is finished.

The SSL handshake is now complete. The server and the client use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

Note that both client and server authentication involve encrypting some pieces of data with one key of a public-private key pair and decrypting it with the other key.

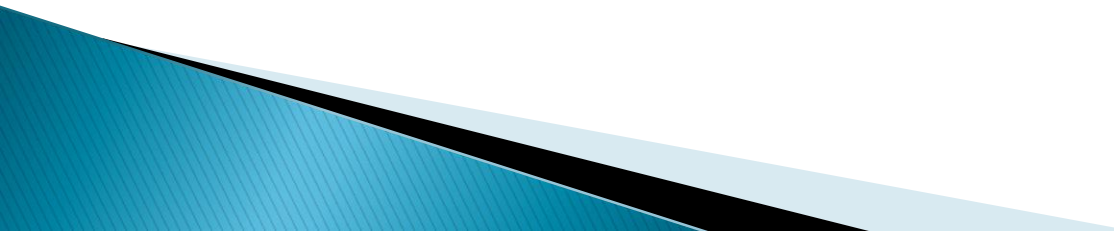
Some Implementations of SSL

- ▶ **OpenSSL** (<http://www.openssl.org/>)-- Provides Information about a free, open-source implementation of SSL.
 - ▶ **Apache-SSL** (<http://www.apache-ssl.org/>)-- Describes Apache-SSL, a secure Webserver, based on Apache and SSLesy/OpenSSL.
- 

Some Implementations of SSL

- ▶ SSLeay (<ftp://ftp.uni-mainz.de/pub/internet/security/ssl/SSL/>) -- a free implementation of Netscape's Secure Socket Layer
- ▶ Planet SSL (<http://www.rsasecurity.com/standards/ssl/developers.html>)-- provides C-programs and Java-programs of SSL.

Summary

- ▶ SSL -- the Record Protocol and the Handshake Protocol.
 - ▶ How to create a secure connection b/t a client and a server.
 - ▶ Some implementations.
- 

What Is a Proxy Server?

- ▶ Intermediary server between clients and the actual server
- ▶ Proxy processes request
- ▶ Proxy processes response
- ▶ Intranet proxy may restrict **all** outbound/inbound requests the intranet server

What Does a Proxy Server Do?

- Between client and server
- Receives the client request
- Decides if request will go on to the server
- May have cache & may respond from cache
- Acts as the client with respect to the server
- Uses one of it's own IP addresses to get page from server

Usual Uses for Proxies

- ▶ Firewalls
- ▶ Employee web use control (email etc.)
- ▶ Web content filtering (kids)
 - Black lists (sites not allowed)
 - White lists (sites allowed)
 - Keyword filtering of page content

User Perspective

- Proxy is invisible to the client
- IP address of proxy is the one used or the browser is configured to go there
- Speed up retrieval if using caching
- Can implement profiles or personalization

Main Proxy Functions

- Caching
- Firewall
- Filtering
- Logging

Web Cache Proxy

- Our concern is not with browser cache!
- Store frequently used pages at proxy rather than request the server to find or create again
- Why?
 - **Reduce latency:** faster to get from proxy & so makes the server seem more responsive
 - **Reduce traffic:** reduces traffic to actual server

Proxy Caches

- Proxy cache serves hundreds/thousands of users
- Corporate and intranets often use
- Most popular requests are generated only once
- Good news:
Proxy cache hit rates often hit 50%
- Bad news:
Stale content (stock quotes)

How Does a Web Cache Work?

- Set of rules in either or both
 - Proxy admin
 - HTTP header

Don't Cache Rules

- HTTP header
 - *Cache-control: max-age=xxx, must-revalidate*
 - *Expires: date...*
 - *Last-modified: date...*
 - *Pragma: no-cache* (doesn't always work!)
- Object is *authenticated* or *secure*
- Fails proxy filter rules
 - URL
 - Meta data
 - MIME type
 - Contents

Getting From Cache

- Use cache copy if it is *fresh*
 - Within date constraint
 - Used recently and modified date is not recent

Getting From Cache

- Use cache copy if it is *fresh*
 - Within date constraint
 - Used recently and modified date is not recent

Getting From Cache

- Use cache copy if it is *fresh*
 - Within date constraint
 - Used recently and modified date is not recent

2. Firewalls

- Proxies for security protection
- More on this later