

SSL

Eleni Stroulia

http and https

- http
 - Stateless protocol
 - Non secure connection
 - Non Secure Sockets
 - port 80
- https
 - Session based protocol
 - Secure connection
 - Secure Sockets
 - port 443

Historical background

- SSL Version 1.0 was introduced in the Mosaic browser in 1994
- SSL Version 2.0 was commercially offered later in the same year
 - HTTPs is the web protocol that utilizes SSL to encrypt , and is used worldwide today for secure web communications.
 - S-HTTP was an alternative method for encrypting web communications; was inferior because it did not encrypt some session information; was designed to send individual messages securely where SSL is designed to establish a secure connection between two computers.
- Microsoft's Private Communications Technology (PCT) was released in 1995 with some advantages over SSL Version 2.0.
- Shortly afterward, Netscape released SSL Version 3.0
- In 1996, SSL was unchallenged as the de facto standard and the Internet Engineering Task Force (IETF) began its formal standardization
- In 1999, IETF completed its work and established SSL as the official standard for secure Web communications under the name Transport Layer Security (TLS).

11-07

3

Cryptography

- Algorithm-based (depends on a complex algorithm)
- Key-based (depends on a “secret” key)
 - Symmetric
 - Uses a single key, which both parties have, for encryption and decryption
 - Key distribution is the inherent weakness in symmetric cryptography.
 - Minimal CPU cycles are required to verify keys.
 - Symmetric ciphers are fortified by algorithmic strength and key lengths.
 - SSL symmetric key lengths range from 40 to 168 bits.
 - Asymmetric (PKI)
 - Information encrypted with one key can be decrypted only with the other key of the pair.
 - Public key infrastructure (PKI) cryptography is up to 1000 times more CPU intensive than symmetric cryptography.
 - The Rivest, Shamir, Adelman (RSA) algorithm uses modular arithmetic to enable the concept of public and private keys.
 - All SSL transactions begin with an asymmetric key exchange.

11-07

4

Message Digests

(one-way function, hash function)

- To guarantee the integrity of a message
- Desiderata
 - Digest algorithms produce unique digests for different messages.
 - It is too difficult to
 - determine the message from the digest
 - find two different messages which create the same digest

11-07

5

Digital Signatures

- To ensure the identity of the sender
- Using private-public key pairs
- Data about the sender is encrypted using the private key; the public key can be used to decrypt it, verifying that the signature was really generated using the corresponding private key.

11-07

6

Message Security

- Confidentiality.
- Authentication.
- Message Integrity.
- Non-Repudiation.
- Time-Date Stamping.

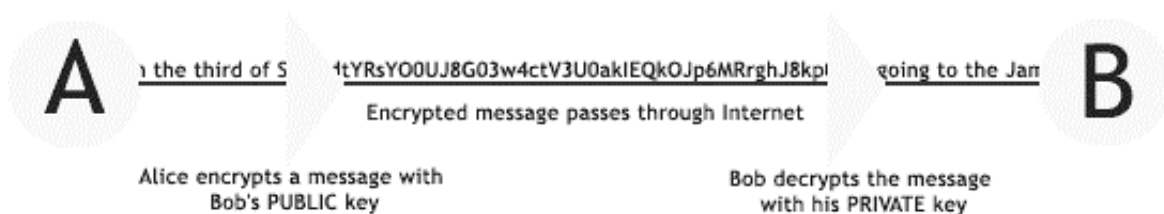
11-07

7

Confidentiality

How does Alice know that only Bob will see the message?

1. Alice encrypts the message with Bob's public key
2. Only Bob can decrypt it with his private key



11-07

8

Authentication, message integrity, non repudiation

How does Bob know that it was really Alice who sent the message?

1. Alice creates a digest of the message.
2. Alice encrypts the digest with her private key. The encrypted digest is the digital signature.
3. The encrypted digest is sent to Bob along with the message (encrypted with Bob's public key)
4. When Bob receives the message, he decrypts the whole message with his private key; he sees the message and the digital signature; he decrypts the signature with Alice's public key and gets the message digest, as sent by Alice
5. Bob then re-creates a digest of the message using the same function that Alice used.
6. Bob compares the digest that he created with the one that Alice encrypted. If the digests match, then Bob can be confident that the signed message is indeed from Alice. If they don't match, then the message has been tampered with — or isn't from Alice at all.

11-07

9

Certificates

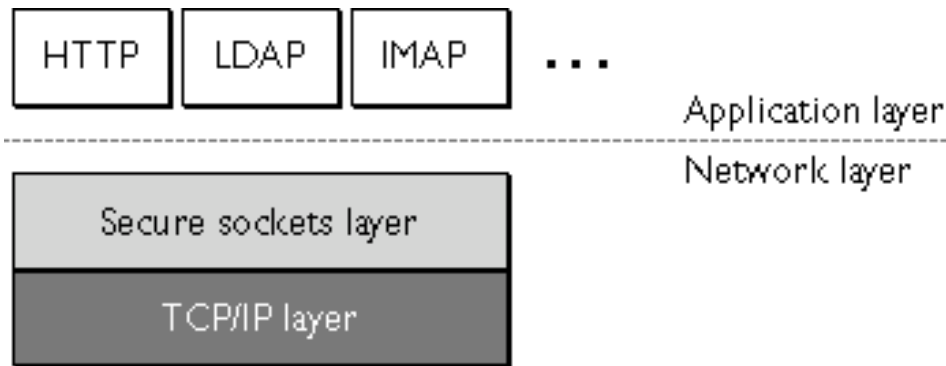
- How does Bob know that Eve did not simply produce a pair of keys and advertised them as Alice's?
- A trusted authority issues a certificate to Alice, after verifying that she is who she says she is
- The certificate associates a public key with the real identity of a subject
 - Subject: Distinguished Name, Public Key
 - Common Name =Joe Average
 - Organization or CompanyOName =Snake Oil, Ltd.
 - Organizational Unit=Research Institute
 - City/LocalityLName=Snake City
 - State/Province=Desert
 - Country=XZ
 - Issuer: Distinguished Name, Signature
 - Period of Validity: Not Before Date, Not After Date
 - Administrative Information: Version, Serial Number
 - Extended Information: Basic Constraints, Netscape Flags, etc.

11-07

10

Introduction to SSL

- Originally developed by Netscape Communication, now accepted universally on the World Wide Web for AUTHENTICATED and ENCRYPTED communication between clients and servers
- IETF standard called Transport Layer Security is based on SSL
- SSL protocol runs above TCP/IP and below higher level protocols such as HTTP
- Uses TCP/IP to authenticate itself to an SSL enabled client



11-07

11

What does SSL actually do?

- SSL server authentication allows a user to confirm a server's identity.
 - if the user is sending a credit card number over the network and wants to check the receiving server's identity.
- SSL client authentication allows a server to confirm a user's identity.
 - if the server is a bank sending confidential financial information to a customer and wants to check the recipient's identity.
- An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software
 - Confidentiality
 - Tampering detection

11-07

12

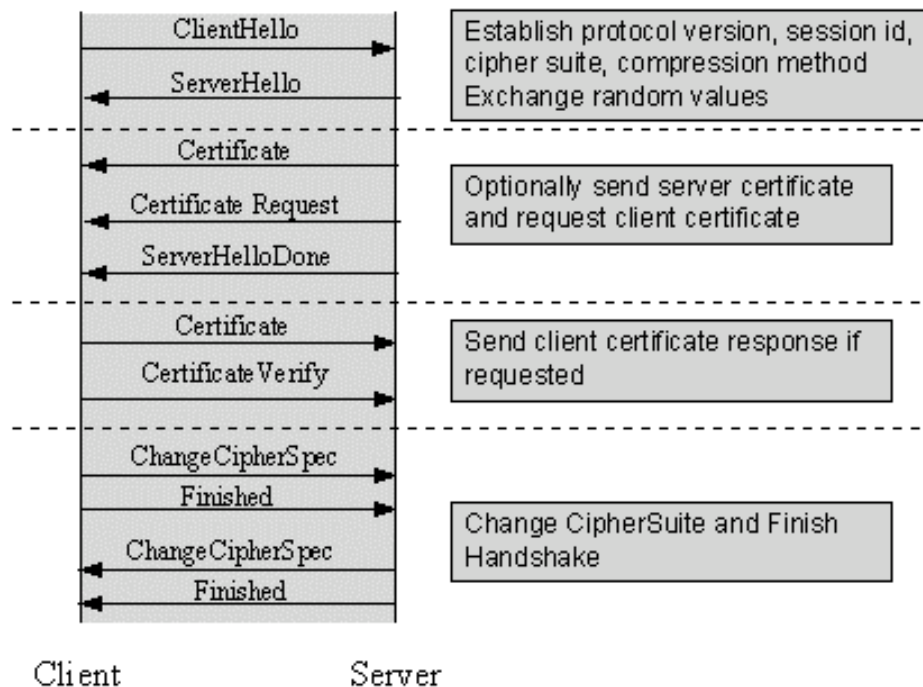
The SSL protocol

- The SSL handshake protocol.
 - involves using the SSL record protocol to exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection.
- The SSL record protocol
 - defines the format used to transmit data.

11-07

13

The SSL Handshake Protocol



11-07

14

The SSL Handshake Protocol

- Negotiate the Cipher Suite, supportable by both of them, to be used during data transfer (SSL3.0 defines 31 Cipher Suites)
 - A Cipher Suite is defined by the following components:
 - Key Exchange Method: how the shared secret symmetric cryptography key used for application data transfer will be agreed upon by client and server
 - Cipher for Data Transfer (stream vs. block ciphers)
 - Message Digest for creating the Message Authentication Code (MAC)
- Establish and share a session key between client and server
- Optionally authenticate the server to the client
- Optionally authenticate the client to the server

11-07

15

The SSL Handshake Protocol-1

1. The client sends its SSL version number, cipher settings, randomly generated data
2. The server sends its SSL version number, cipher settings, randomly generated data
 1. sends its own certificate
 2. requests the client's certificate.
3. The client authenticates the server
4. The client creates the premaster secret for the session, encrypts it with the server's public key and sends it to the server.
 1. signs another piece of data that is unique to this handshake and known by both the client and server.
5. The server authenticates the client.

11-07

16

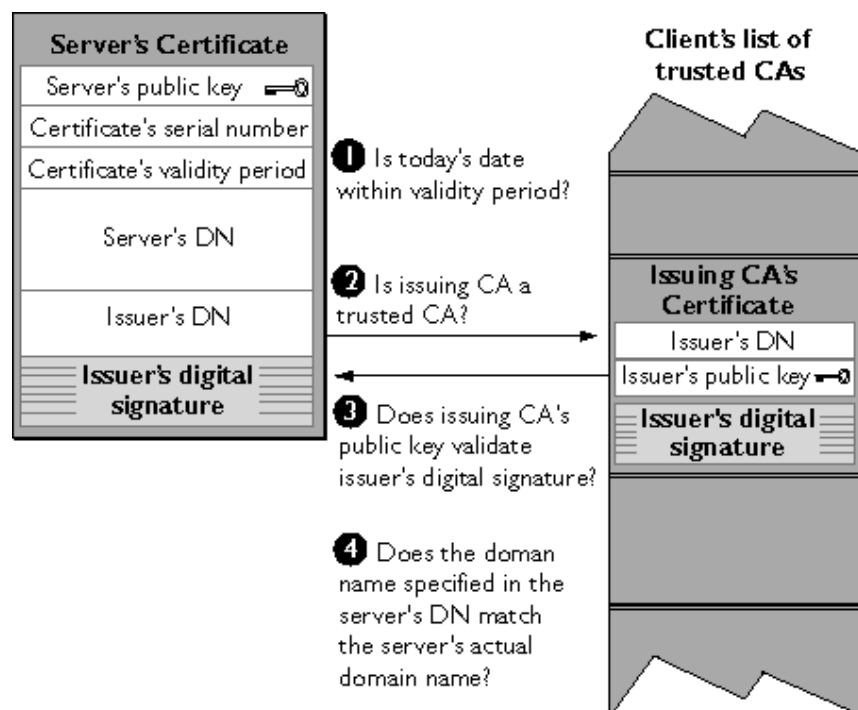
The SSL Handshake Protocol-2

6. The server uses its private key to decrypt the premaster secret; then client and server perform a series of steps (starting from the same premaster secret) to generate the master secret.
7. Both the client and the server use the master secret to generate the (symmetric) session keys.
8. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key and a separate (encrypted) message indicating that the client portion of the handshake is finished.
9. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key and a separate (encrypted) message indicating that the server portion of the handshake is finished.

11-07

17

Server authentication



11-07

18

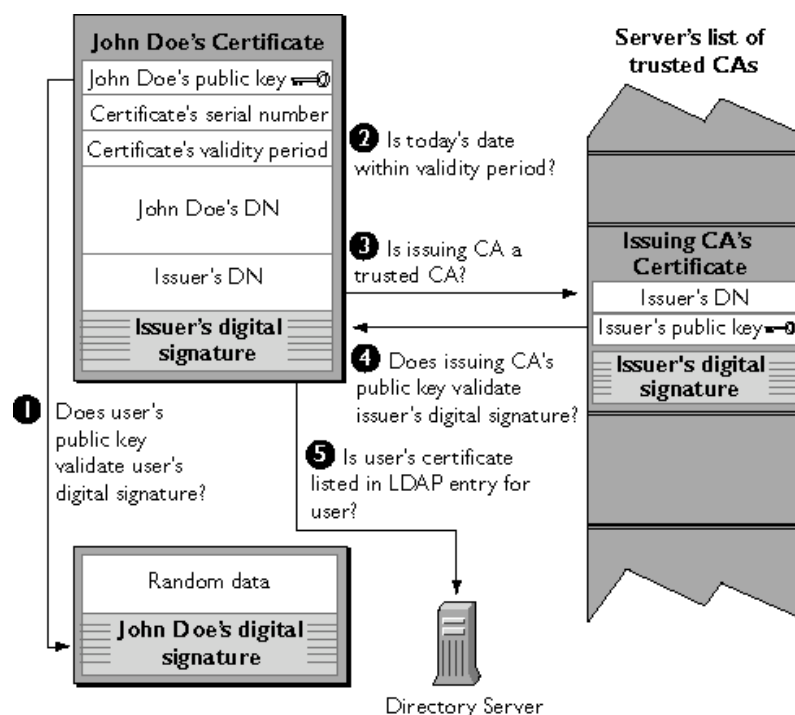
Server authentication

- Is today's date within the validity period?
- Is the issuing CA a trusted CA?
- Does the issuing CA's public key validate the issuer's digital signature?
- Does the domain name in the server's certificate match the domain name of the server itself?
 - Man-in-the-middle
- The server is authenticated.

11-07

19

Client authentication



11-07

20

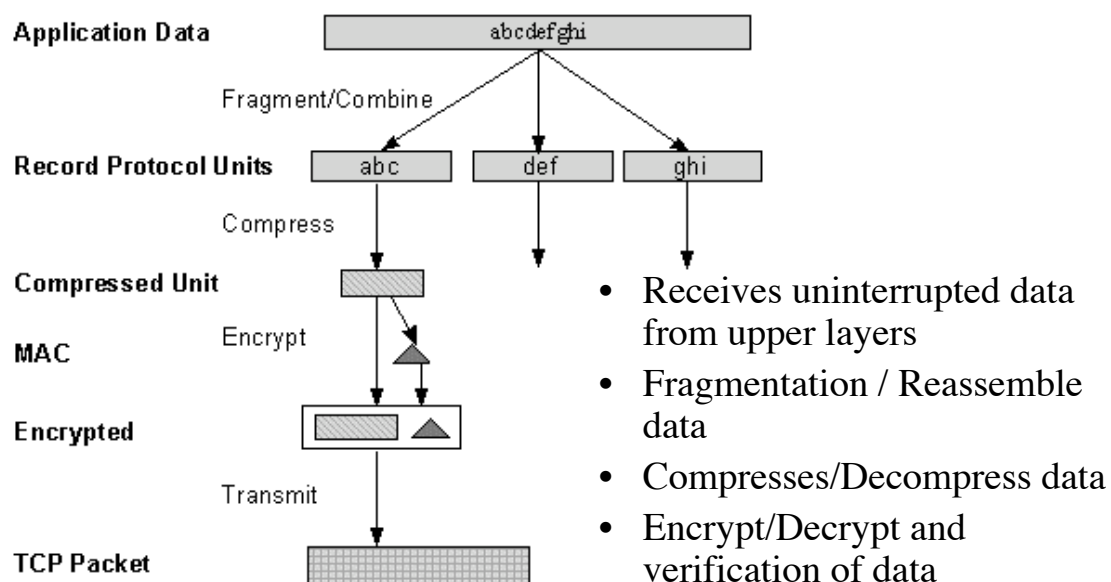
Client authentication

- Does the user's public key validate the user's digital signature?
- Is today's date within the validity period?
- Is the issuing CA a trusted CA?
- Does the issuing CA's public key validate the issuer's digital signature?
- Is the user's certificate listed in the LDAP entry for the user?
- Is the authenticated client authorized to access the requested resources?

11-07

21

The SSL Record Protocol

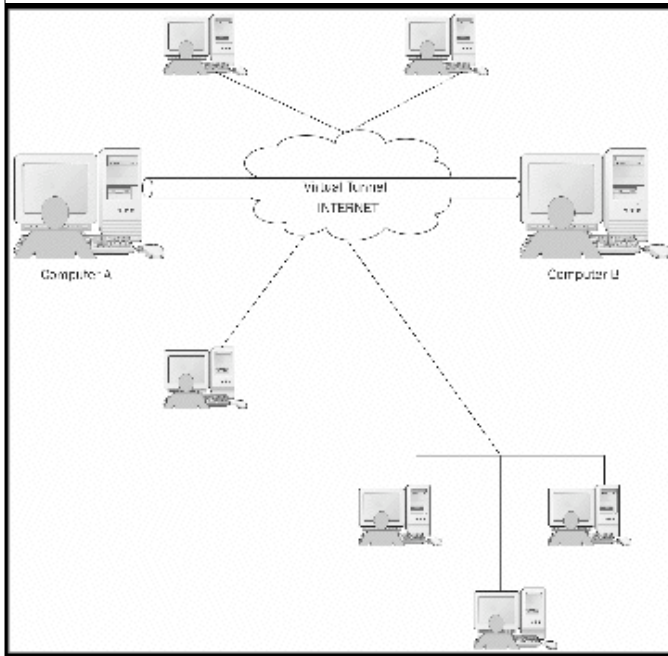


11-07

22

Virtual Private Networks

- The VPN nodes can communicate without any other machine being able to intercept their communications.
- Communications can be sniffed — intermediate routers can be set into 'promiscuous mode' to listen to all traffic on the network wire and reads in all data being transmitted.



References

- <http://afongen.com/writing/pke/>
- <http://www.youdzone.com/signature.html>
- <http://docs.sun.com/source/816-6156-10/contents.htm>
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns50/ns140/networking_solutions_white_paper09186a0080136858.shtml
- http://httpd.apache.org/docs/2.0/ssl/ssl_intro.html
- <http://search.cpan.org/dist/Crypt-SSLeay/SSLeay.pm>