

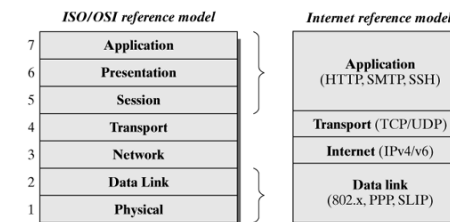
Protezione e Sicurezza nei Sistemi Operativi: Secure Sockets Layer

Ozalp Babaoglu

ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA

Internet layered architecture

- Internet protocols are layered
- Each layer provides services to the layer above hiding details of layers below
 - Logical separation
 - Easier to develop and maintain
 - Interoperability
- Two reference models: ISO/OSI and TCP/IP



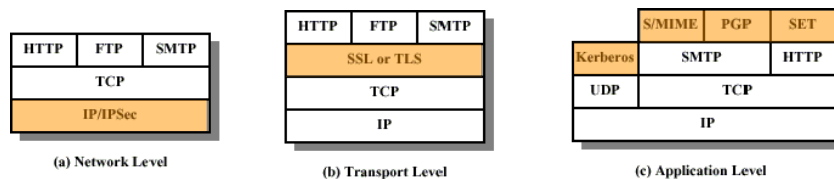
© Babaoglu

Sicurezza

2

Introduction

- Security in the Internet:
 - at which level?



© Babaoglu

Sicurezza

3

Introduction

- Security at the application level
 - Pros: designed for specific application requirements
 - Cons: requires multiple security mechanisms
- Security at the transport level
 - Pros: provides common interface to security services
 - Cons: requires (minor) modification to applications
- Security at the network level
 - Pros: works with security-ignorant applications
 - Cons: may require modifications at the OS level

© Babaoglu

Sicurezza

4

Introduction

- Security at the application level
 - S/MIME
 - PGP
 - Kerberos
 - SET — Secure Electronic Transfer
- Security at the transport level
 - SSL (Secure Sockets Layer)
- Security at the network level
 - IPSec

SSL: Secure Sockets Layer

- Probably the most widely-used security service on the Internet
- A general purpose service implemented as a set of protocols that rely on TCP
- Proposed by *Netscape Communications Corporation* in 1994 as part of their *Navigator* browser
- Adopted as a standard by the IETF under the name *Transport Layer Security* (TLS)
- Guarantees *confidentiality*, *integrity* and *authentication* for Internet communications

Internet Archaeology

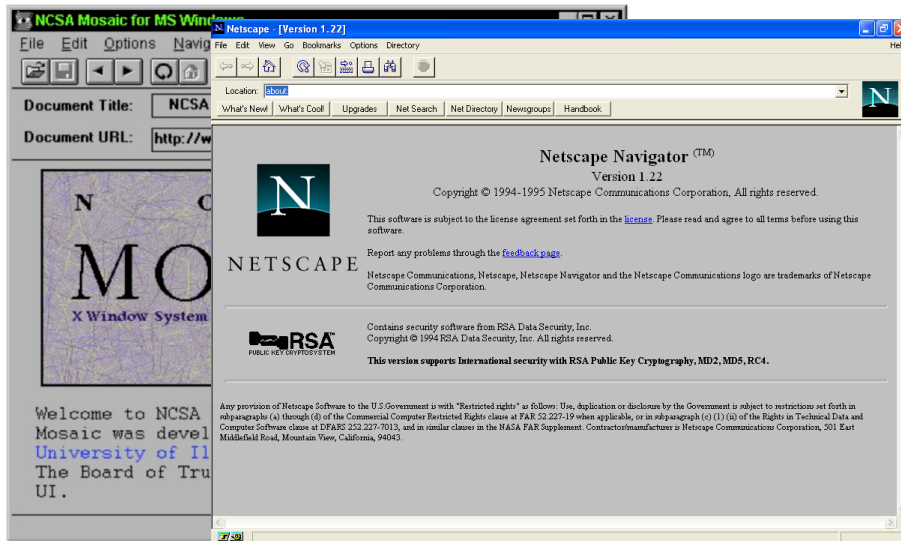
- Pre 1993 Internet was essentially text only: Archie, Gopher, WAIS
- 1993 — *National Center for Supercomputing Applications* at the *University of Illinois at Urbana-Champaign* releases **Mosaic**, the first graphic web browser
- 1994 — *Mosaic Communications Corporation* founded by Jim Clark and Marc Andreessen



Internet Archaeology

- October 1994 — **Mosaic Netscape 0.9** released
- November 1994 — Company renamed *Netscape Communications Corporation* and its product renamed **Netscape Navigator**
- Netscape dominated the browser market until around 2000 when **Microsoft Internet Explorer** came along and took over the browser market

Internet Archaeology



© Babaoglu

Siurezza

9

SSL: Secure Sockets Layer

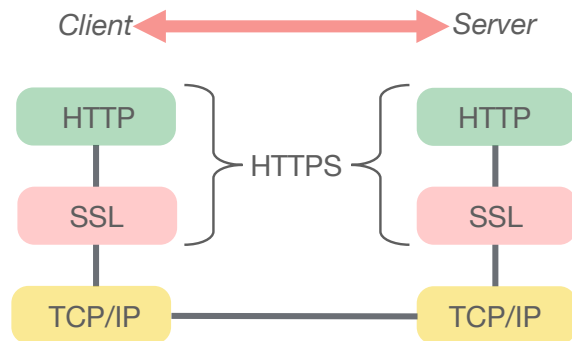
- E-commerce
- On-line trading
- Internet banking
- Any time confidential data (password, credit card number) needs to be sent to a remote host

© Babaoglu

Siurezza

10

SSL: Secure Sockets Layer



Other protocols on top of SSL: ftps, ssh, smtps

© Babaoglu

Siurezza

11

SSL: Secure Sockets Layer

- Based on
 - **Symmetric** ciphers
 - **Asymmetric** ciphers
 - Certificates
 - Message Authentication Code (MAC)

© Babaoglu

Siurezza

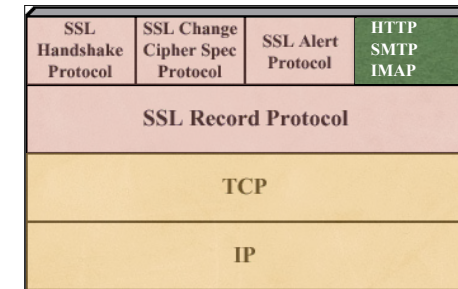
12

Hybrid solution for secret key management

1. A generates $(K_A[pub], K_A[priv])$
2. A announces its public key to B : $\{K_A[pub], A\}$
3. B generates session key K_S
4. B sends session key to A : $C(K_A[pub], K_S)$
5. A decrypts to obtain $K_S = D(K_A[priv], C(K_A[pub], K_S))$
6. A can delete $(K_A[pub], K_A[priv])$
7. A and B switch to symmetric cryptography using the session key K_S

SSL: Implementation

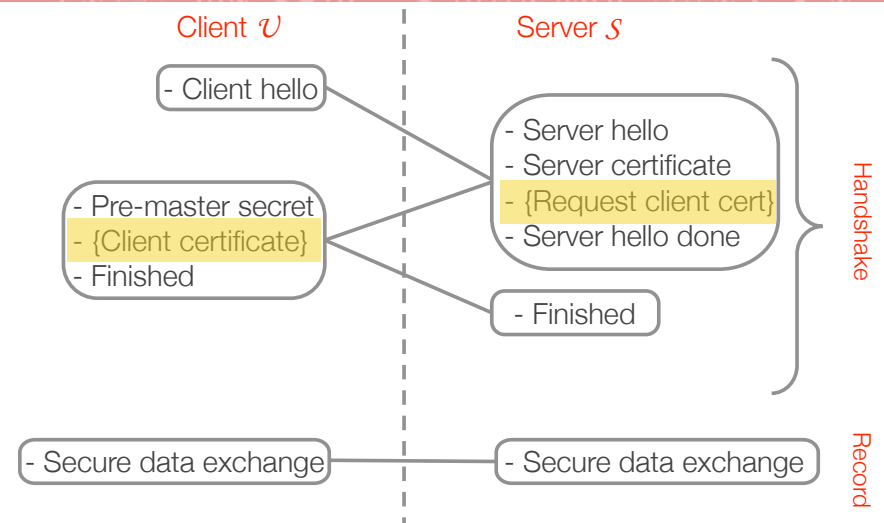
- SSL **Handshake protocol** creates a channel that is secure, reliable and authenticated between client and server
- SSL **Record protocol** transports messages in encapsulated blocks that are encrypted and authenticated



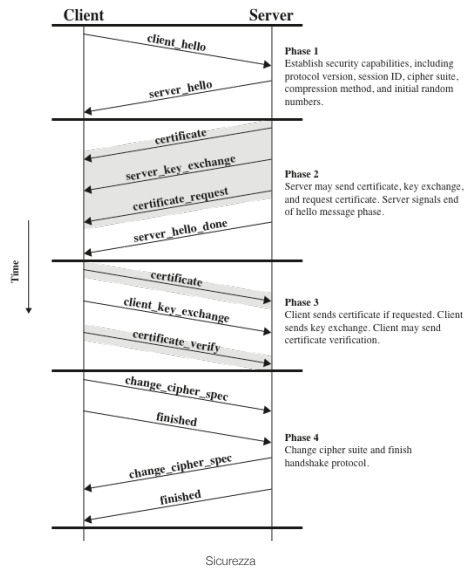
SSL: Handshake and Record

- **Handshake**: uses *public-key cryptography* to establish a secure channel between client and server such that
 - there is mutual *authentication*
 - client and server agree on *encryption/decryption algorithms*
 - client and server agree on a *secret key*
- **Record**: uses *private-key cryptography* with the agreed upon algorithms and secret key to confidentially exchange data

SSL: Handshake e Record



SSL: Handshake Protocol



SSL – Sessions and Connections

- **SSL Session**
 - A long-lasting association between a client and a server
 - Created by the *Handshake Protocol*
 - Associated to a set of security parameters
 - Used to avoid the expensive negotiation of new security parameters
- **SSL Connection**
 - A transport connection between a client and a server
 - Connections are transient
 - Every connection is associated with one session
- **Between any pair of parties**
 - There may be multiple connections
 - Normally there is a single session

SSL – Sessions and Connections

- **Session state**
 - **Session identifier:** arbitrary byte sequence to identify an active session
 - **Peer certificate:** an X509.v3 certificate of the peer; may be null
 - **Compression method:** used to compress data prior to encryption
 - **Cipher spec:** specifies the data encryption algorithm
 - **Master secret:** 48 byte secret shared between client and server

SSL – Sessions and Connections

- **Connection State**
 - **Client/Server random:** Random byte sequences used as identifier chosen by the client and the server at each connection
 - **Client/Server write MAC secret key:** Secret key used in *Message Authentication Code (MAC)* operations on data sent by the client/server
 - **Client/Server write secret key:** Encryption key for data encrypted by the client/server and decrypted by the server/client
 - **Sequence Numbers**

SSL Authentication

- Authentication of the server to the client through a certificate is mandatory
- Authentication of the client to the server is optional
- If requested by the server, the client usually authenticates itself through a mechanism that does *not* require certificates such as login/password
- Because certificates for SSL are usually expensive and clients should not be expected to incur their cost for accessing a secure server

SSL Authentication

- TLS/SSL Certificate prices from Thawte

	SSL Web Server with EV	SSL Web Server	SSL123
Issuance Time	Most certificates issued in 1-3 days	Most certificates issued in one day	Most certificates issued in minutes
Price: <input checked="" type="radio"/> 1 Year <input type="radio"/> 2 Years	Best for: Credit Card Transacting Websites Banks and Financial Institutions \$344 <input type="button" value="BUY NOW"/> <input type="button" value="RENEW"/>	Best for: Enterprise Applications Business Websites \$218 <input type="checkbox"/> add wildcard + \$470 <input type="button" value="BUY NOW"/> <input type="button" value="RENEW"/>	Best for: Securing Internal Servers Private Websites \$149 <input type="checkbox"/> add wildcard + \$596 <input type="button" value="BUY NOW"/> <input type="button" value="RENEW"/>
Identity validation and customer assurance	Prominent visible assurance to increase trust and boost customer confidence	Visible assurance to customers that your website and domain are tied to your organization.	SSL encryption with padlock icon

SSL – Record Protocol

- SSL Record Protocol provides
 - **Confidentiality**: The *Handshake Protocol* defines a shared secret key that is used to encrypt SSL payloads
 - **Integrity**: The *Handshake Protocol* defines a shared secret key that is used to generate *Message Authentication Codes* attached to payloads

SSL and browsers

- The overall security of the SSL channel used by a browser cannot be any greater than the security of the weakest protocol in the browser's cipher suite
- In your browser, it is advisable to disable all protocols based on short keys (64 bits or less for symmetric ciphers, 512 bits or less for asymmetric ciphers)

SSL and browsers

■ <https://browserleaks.com/ssl>

SSL/TLS Client Test

The page shows the SSL/TLS capabilities of your web browser, determines supported TLS protocols and cipher suites and marks if any of them are weak or insecure, displays a list of supported TLS extensions and key exchange groups. Using this data, it calculates the TLS-fingerprint in JA3 format. It also tests how your web browser handles requests for insecure mixed content.

Your Web Browser :

User-Agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.83 Safari/537.36

Protocol Support :

TLS 1.3	✓ Enabled
TLS 1.2	✓ Enabled
TLS 1.1	✗ Disabled (Good)
TLS 1.0	✗ Disabled (Good)

Mixed Content Test :

Images	✓ Upgraded to HTTPS
Audio	✓ Upgraded to HTTPS
Video	✓ Upgraded to HTTPS
CSS	✓ Blocked
Scripts	✓ Blocked
Frames	✓ Blocked

TLS Fingerprint :

JA3 Hash 53f640df993ca882b70e1c82af5da49
JA3 Fingerprint 772,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,

Handshake :

TLS Protocol TLS 1.3 [HSTS/2.0]
Cipher Suite 0x1302 TLS_AES_256_GCM_SHA384 Recommended TLS 1.3

SSL and browsers

■ <https://www.ssllabs.com/ssltest/viewMyClient.html>



Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

[Other User Agents »](#)

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1 Safari/605.1.15

Protocol Support

Your user agent has good protocol support.
Your user agent supports TLS 1.2 and TLS 1.3, which are recommended protocol version at the moment.

CVE-2020-0601 (CurveBall) Vulnerability

Your user agent is not vulnerable.
For more information about the CVE-2020-0601 (CurveBall) Vulnerability, please go to [CVE-2020-0601](#).
To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.

Logjam Vulnerability

Your user agent is not vulnerable.
For more information about the Logjam attack, please go to [weakdh.org](#).
To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.

SSL Certificate Errors

■ <https://badssl.com>

This Connection Is Not Private

This website may be impersonating "untrusted-root.badssl.com" to steal your personal or financial information. You should go back to the previous page.

[Go Back](#)

Safari warns you when a website has a certificate that is not valid. This may happen if the website is misconfigured or an attacker has compromised your connection.

To learn more, you can [view the certificate](#). If you understand the risks involved, you can visit [this website](#).

