HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

----□□□----

BÁO CÁO

MÔN HỌC: CƠ SỞ AN TOÀN THÔNG TIN

ĐỀ TÀI: TÌM HIỂU VỀ GIAO THỨC BÁO MẬT SSL/TLS

Giáo viên hướng dẫn: Hoàng Xuân Dậu
Lớp môn học: D19AT03
Nhóm thực hiện: G08
Thành viên thực hiện:

1. Châu Phan Hoài Linh – B19DCAT110
2. Lê Thị Linh – B19DCAT111
3. Lê Đức Long – B19DCAT114
4. Phạm Xuân Long – B19DCAT117
5. Nguyễn Thị Quỳnh Mai – B19DCAT121

Hà Nội, Tháng 9/2021

PHÂN CÔNG CÔNG VIỆC

Nhóm G08

STT	Mã SV	Họ và tên	Công việc
1	B19DCAT117	Phạm Xuân Long	Nhóm trưởng, phân công công việc. Thuyết trình
2	B19DCAT111	Lê Thị Linh	Tìm hiểu và viết báo cáo phần Kiến trúc
3	B19DCAT121	Nguyễn Thị Quỳnh Mai	Tìm hiểu và viết báo cáo phần Hoạt động. Tổng hợp báo cáo.
4	B19DCAT114	Lê Đức Long	Tìm hiểu và viết báo cáo phần Ứng dụng
5	B19DCAT110	Châu Phan Hoài Linh	Thiết kế Slide

MỤC LỤC

Lời nói đầu

Ngày nay việc bảo mật thông tin là yếu tố vô cùng quan trọng để quyết định sự sống còn của một tổ chức, công ty hay doanh nghiệp. Với sự phát triển nhanh chóng của công nghệ đã mang lại nhiều tiện ích cho người dùng nhưng đồng thời cũng đặt ra một nhu cầu tất yếu về sự an toàn và bảo mật thông tin. Việc truyền tải các thông tin nhạy cảm trên mạng rất không an toàn vì chúng ta có thể không biết được đối tượng cần trao đổi chính xác là ai hay dữ liệu mạng bị chặn, dữ liệu bị kẻ khác tấn công để đọc trộm, nghe lén và thậm chí là bị chèn, sửa, xóa dữ liệu.

SSL/TLS giải quyết các vấn đề trên, đây là giao thức an ninh thông tin mạng được sử dụng rộng rãi nhằm mã hóa và cung cấp một kênh an toàn giữa các máy tính trên mạng. SSL/TLS cung cấp tính xác thực, tính bảo mật và tính toàn vẹn thông qua các thuật toán mã hóa mà nó sử dụng, cho phép các thông tin nhạy cảm được truyền đi an toàn.

I. Kiến trúc của giao thức bảo mật SSL/TLS

1. Giới thiệu và lịch sử của giao thức bảo mật SSL/TLS

a. Giới thiệu

SSL (Secure Socket Layer) – Tầng Socket bảo mật: là giao thức đa mục đích được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (socket 443) nhằm mã hóa toàn bộ thông tin đi/ đến, mà ngày nay được sử dụng rộng rãi trong giao dịch điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân PIN (Personal Information Number) trên Internet, trên các thẻ tín dụng...

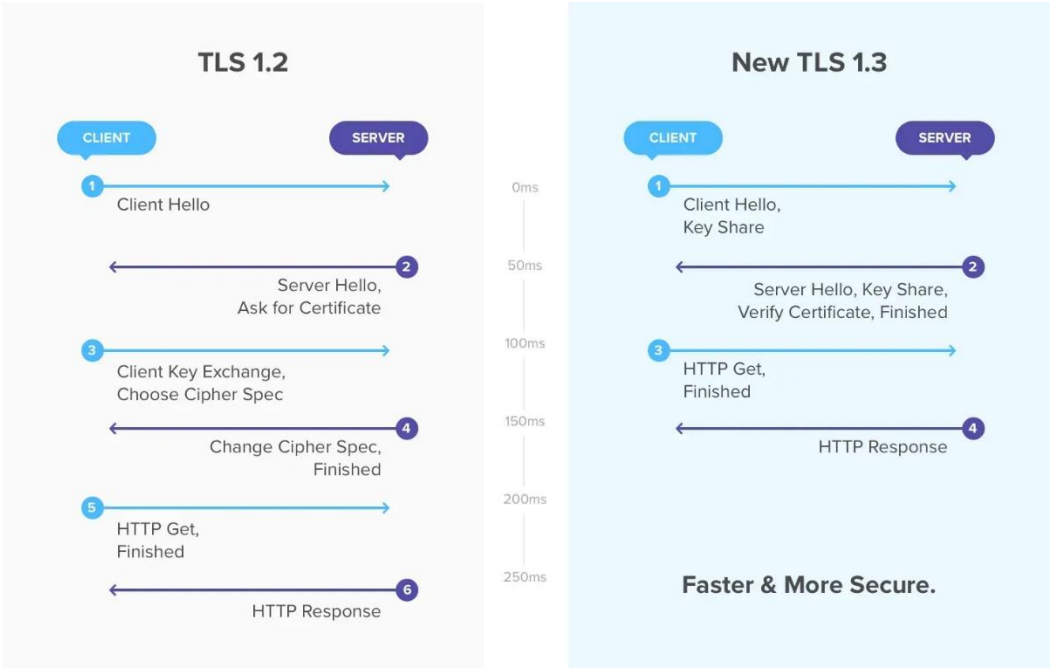
SSL/TLS là một giao thức cho phép truyền đạt thông tin một cách bảo mật, an toàn và tính toàn vẹn dữ liệu khi vận chuyển qua mạng.

b. Lịch sử

SSL là giao thức bảo mật do công ty Netscape phát minh năm 1993. Các phiên bản SSL được phát triển bao gồm: phiên bản 1.0 phát hành năm 1993, phiên bản 2.0 phát hành năm 1995 và phiên bản 3.0 phát hành năm 1996. Sau phiên bản 3.0, SSL chính thức dừng phát triển. SSL hiện ít được sử dụng do có nhiều lỗi và không được cập nhật.

Giao thức SSL được sử dụng rộng rãi trên World Wide Web trong việc xác thực và mã hóa thông tin giữa phía khách (client) và phía máy chủ (server). Tổ chức IETF (Internet Engineering Task Force: Lực lượng công tác kỹ thuật về Internet) đã chuẩn hóa SSL và đặt lại tên là TLS (Transport Layer Security: Bảo mật tầng giao vận).

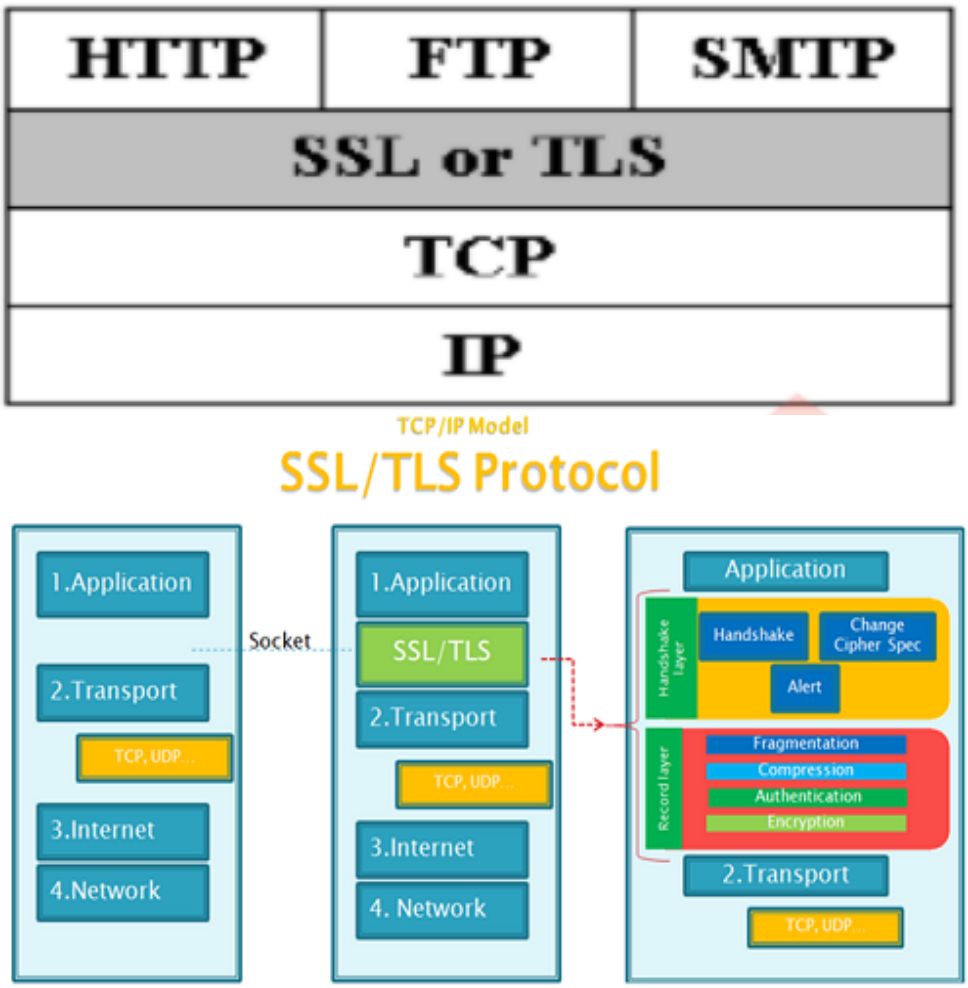
TLS được phát triển vào năm 1999 dựa trên SSL 3.0. Các phiên bản của TLS gồm: phiên bản 1.0 phát hành năm 1999, phiên bản 1.1 phát hành năm 2005, phiên bản 1.2 phát hành năm 2008, phiên bản 1.3 vẫn là bản thảo và chưa được phát hành chính thức cho đến tháng 10 năm 2017. Hiện nay phiên bản TLS 1.2 được sử dụng rộng rãi nhất, còn SSL chỉ được giữ lại tên với lý do lịch sử.



Hình 1: Sự khác nhau giữa TLS 1.2 và TLS 1.3

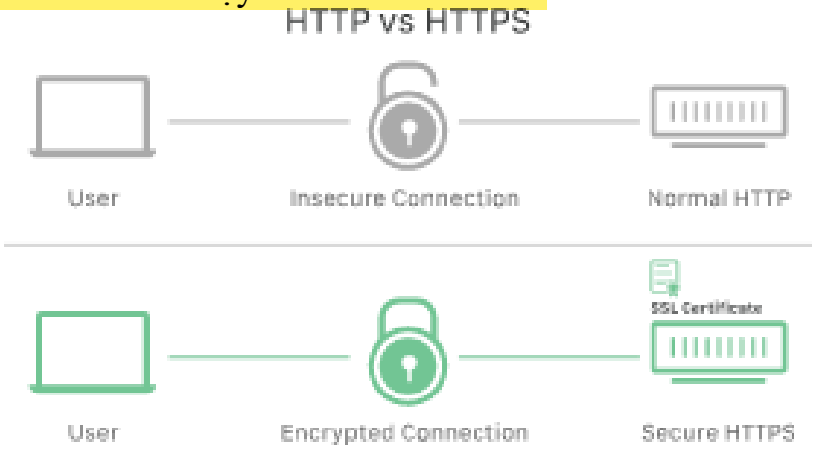
2. Kiến trúc của giao thức bảo mật SSL/TLS

SSL được thiết kế như là một giao thức riêng cho vấn đề bảo mật có thể hỗ trợ rất nhiều ứng dụng. Giao thức SSL hoạt động bên trên TCP/IP và bên dưới các giao thức ứng dụng tầng cao hơn như là HTTP (Hyper Text Transpot Protocol: Giao thức truyền tải siêu văn bản), IMAP (Internet Messaging Access Protocol: Giao thức truy nhập bản tin Internet) và FTP (File Transport Protocol: Giao thức truyền file). SSL có thể sử dụng để hỗ trợ các giao dịch an toàn cho rất nhiều ứng dụng khác nhau trên Internet.



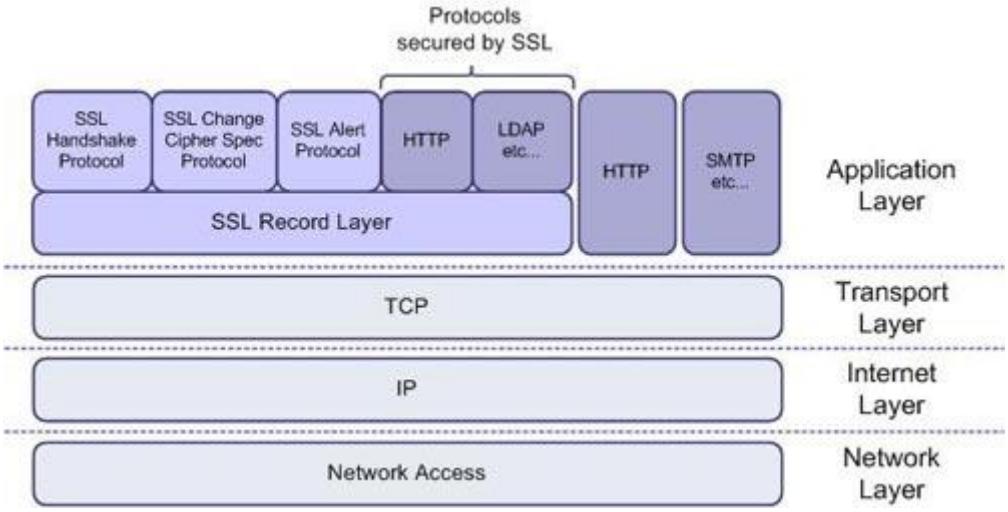
Hình 2: Vị trí của SSL/TLS trong bộ giao thức TCP/IP

SSL/TLS hoàn toàn độc lập với các giao thức tầng ứng dụng khác nhau, như HTTP, SMTP và FTP.
Chẳng hạn, giao thức bảo mật web HTTPS = HTTP + SSL/TLS – có nghĩa là HTTPS tạo ra bởi HTTP chạy trên nền SSL/TLS.



Hình 3: HTTP và HTTPS

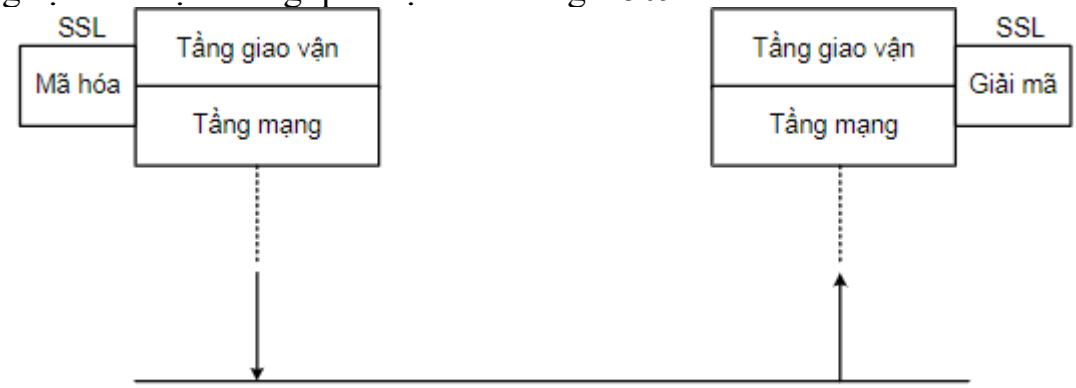
Một trong các điều kiện để SSL/TLS có thể hoạt động là ít nhất một thực thể (thường là máy chủ) tham gia phiên truyền thông phải có chứng chỉ số cho khóa công khai (Public key certificate).



Hình 4: Các giao thức con của SSL/TLS

⇨ Cấu trúc và giao thức SSL/TLS được đặt giữa tầng vận chuyển (Transport Layer) và tầng ứng dụng (Application Layer).

SSL/TLS có thể xem như một tầng giao thức trung gian giữa tầng mạng và tầng giao vận trong mô hình DoD (5 tầng) hoặc OSI (7 tầng) của mạng máy tính. Trong SSL/TLS mỗi thông điệp được chuyển đi cho một đối tác được cung cấp chứng nhận giao dịch hoặc nhận từ đối tác đó đều được mã hóa bởi một khóa đối xứng khi chuyển đi và được giải mã khi nhận đến, thông điệp đó còn được gắn một mật mã nhận dạng được hệ thống cấp cho mỗi đối tác, SSL sử dụng sự xác nhận thông qua mật mã chung X509.



Hình 5: SSL trong giao thức mạng

Một website sử dụng giao thức http được tích hợp SSL có tính năng bảo mật thông tin gửi từ phía máy khách (client side)vào trang web đến phía máy chủ (server side)vì thông tin ở tầng giao vận bên máy khách phải qua tầng phụ SSL để được mã hóa (theo luật mã hóa công khai đã được SSL cung cấp cho máy chủ trang web) rồi mới quay về tầng mạng để tiếp tục chuyển đi: dữ liệu truyền đi trên môi trường Internet đã được mã hóa (ciphertext). Phía máy chủ khi dữ liệu về đến tầng mạng thì lại được đưa sang tầng phụ SSL để được giải mã (bằng khóa riêng của phía máy chủ tương ứng với khóa công khai trên trang web) rồi quay về tầng giao vận để chuyển xuống tầng áp dụng: thông tin tầng ứng dụng nhận được lại là thông tin tường minh (plaintext).

SSL/TLS là một bộ gồm có 4 giao thức con. Các giao thức của SSL/TLS gồm:

- **SSL Handshake Protocol:** Giao thức bắt tay của SSL có nhiệm vụ trao đổi các thông điệp xác thực thực thể và thiết lập các thông số cho phiên làm việc.
    - Thương lượng thuật toán và cơ chế mã hóa để bảo vệ dữ liệu được gửi trong SSL Record
    - Trao đổi khóa
    - Xác thực server và client
- **SSL Change Cipher Spec Protocol:** (giao thức đơn giản nhất) Giao thức thiết lập việc sử dụng các bộ mã hóa được hỗ trợ bởi cả 2 bên tham gia phiên truyền thông.
    - Thông báo kết quả của quá trình Handshake
- **SSL Alert Protocol:** Giao thức cảnh báo của SSL.
    - Thông báo lỗi
- **SSL Record Protocol:** Giao thức bản ghi của SSL có nhiệm vụ tạo đường hầm an toàn để chuyển thông tin đảm bảo tính bí mật, toàn vẹn và xác thực.
    - Phân đoạn gói dữ liệu
    - Nén
    - Xác thực message và đảm bảo tính toàn vẹn
    - Mã hóa

Việc kết nối giữa một trình duyệt web tới bất kỳ điểm nào trên mạng Internet đi qua rất nhiều các hệ thống độc lập. Và không có bất kỳ sự bảo vệ nào với các thông tin trên đường truyền. Không một ai kể cả người sử dụng lẫn Web server có bất kỳ sự kiểm soát nào đối với đường đi của dữ liệu hay có thể kiểm soát được liệu có ai đó xâm nhập vào thông tin trên đường truyền**.**

Để bảo vệ những thông tin trên mạng Internet hay bất kỳ mạng TCP/IP nào. SSL/TLS đã kết hợp những yếu tố sau để thiết lập được một giao dịch an toàn:

- **Xác thực:** Các bên giao tiếp (client và server) có thể xác thực nhau bằng cách sử dụng mật mã khóa chung. Đảm bảo tính xác thực của trang mà bạn sẽ làm việc ở đầu kia của kết nối. Cũng như vậy, các trang Web cũng cần phải kiểm tra tính xác thực của người dùng.
- **Mã hóa:** Sự bí mật của lưu lượng dữ liệu được bảo vệ vì kết nối được mã hóa trong suốt sau khi một sự thiết lập quan hệ ban đầu và sự thương lượng khóa session đã xảy ra. Đảm bảo thông tin không thể bị truy cập bởi đối tượng thứ ba. Để loại trừ việc nghe trộm những thông tin "nhạy cảm" khi nó được truyền qua Internet, dữ liệu phải được mã hóa để không thể bị đọc được bởi những người khác ngoài người gửi và người nhận.
- **Toàn vẹn dữ liệu:** Đảm bảo thông tin không bị sai lệch. Thể hiện chính xác thông tin gốc gửi đến. Tính xác thực và tính toàn vẹn của lưu lượng

dữ liệu cũng được bảo vệ vì các thông báo được xác thực và được kiểm tra tính toàn vẹn một cách trong suốt bằng cách sử dụng MAC.

SSL không phải là một giao thức đơn lẻ, mà là một tập các thủ tục đã được chuẩn hoá để thực hiện các nhiệm vụ bảo mật sau:

- ***Xác thực server:*** Cho phép người sử dụng xác thực được server muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hoá công khai để chắc chắn rằng certificate và public ID của server là có giá trị và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của client. Điều này rất quan trọng đối với người dùng. Ví dụ như khi gửi mã số credit card qua mạng thì người dùng thực sự muốn kiểm tra liệu server sẽ nhận thông tin này có đúng là server mà họ định gửi đến không.
- ***Xác thực Client:*** Cho phép phía server xác thực được người sử dụng muốn kết nối. Phía server cũng sử dụng các kỹ thuật mã hoá công khai để kiểm tra xem certificate và public ID của server có giá trị hay không và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của server không. Điều này rất quan trọng đối với các nhà cung cấp. Ví dụ như khi một ngân hàng định gửi các thông tin tài chính mang tính bảo mật tới khách hàng thì họ rất muốn kiểm tra định danh của người nhận.
- ***Mã hoá kết nối:*** Tất cả các thông tin trao đổi giữa client và server được mã hoá trên đường truyền nhằm nâng cao khả năng bảo mật. Điều này rất quan trọng đối với cả hai bên khi có các giao dịch mang tính riêng tư. Ngoài ra, tất cả các dữ liệu được gửi đi trên một kết nối SSL đã được mã hoá còn được bảo vệ nhờ cơ chế tự động phát hiện các xáo trộn, thay đổi trong dữ liệu. (đó là các thuật toán băm – hash algorithm).

II. Hoạt động của giao thức bảo mật SSL/TLS

1. Thuật toán của giao thức bảo mật SSL/TLS

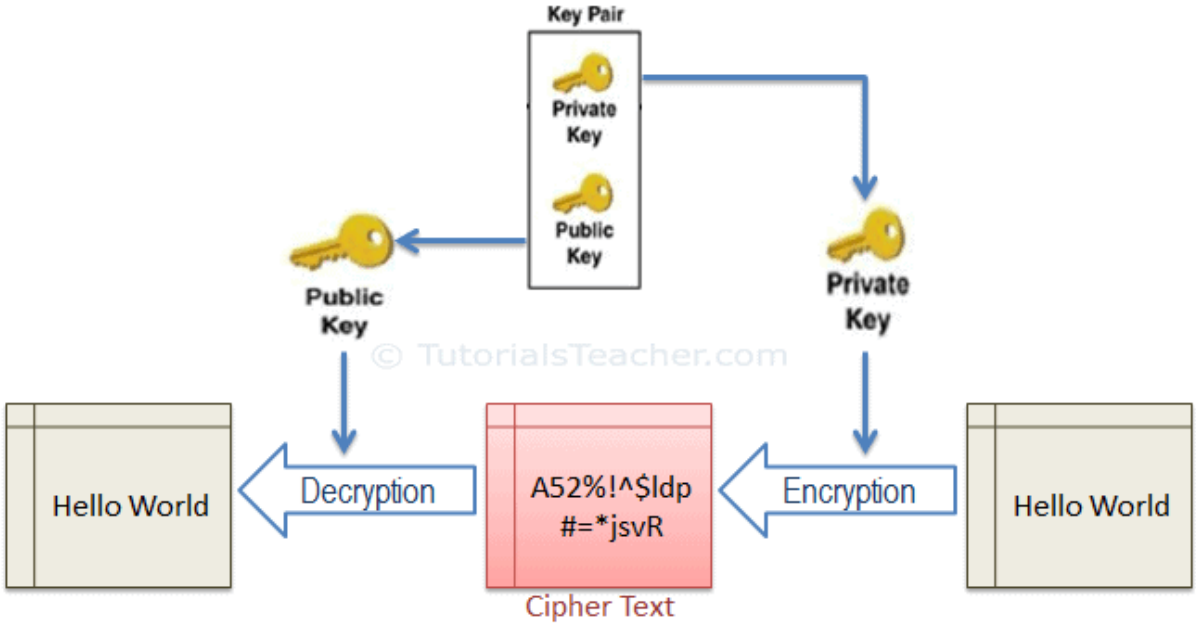
SSL/TLS sử dụng hai dữ liệu mã hóa:

- Mã hóa Bất đối xứng – Asymmetric Cryptography:

  Mã hóa Bất đối xứng (Mã hóa khóa công khai) sử dụng cặp key toán học để mã hóa và giải mã data, cặp key này gồm:

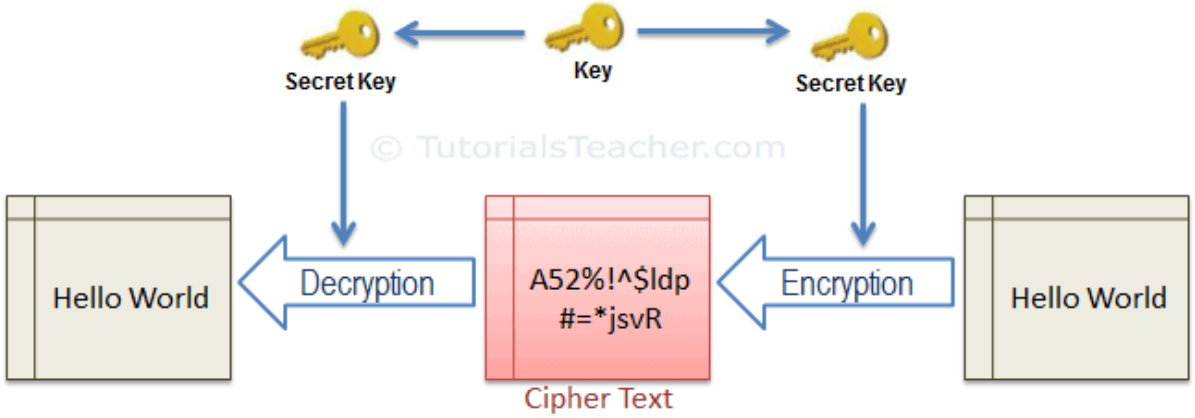
  - Khóa công khai – Public key: được share với bất kỳ ai/ client/ browser nào có nhu cầu giao tiếp với server.
  - Khóa bí mật – Private key: được server lưu giữ cẩn thật, không được phép tiết lộ ra bên ngoài.

  Cặp khóa này được sinh ra bởi thuật toán dùng để mã hóa và giải mã data. Data được mã hóa bởi Public key chỉ có thể được giải mã bởi Private key của cặp khóa đó.



Hình 6: SSL sử dụng Mã hóa bất đối xứng để khởi tạo giao tiếp (SSL Handshake)

- Mã hóa đối xứng – Symmetric Cryptography
  Thuật toán mã hóa đối xứng chỉ có một khóa được dùng chung cho cả hai việc mã hóa và giải mã dữ liệu.
  Cả 2 phía client và server cần phải giữ bí mật khóa này.

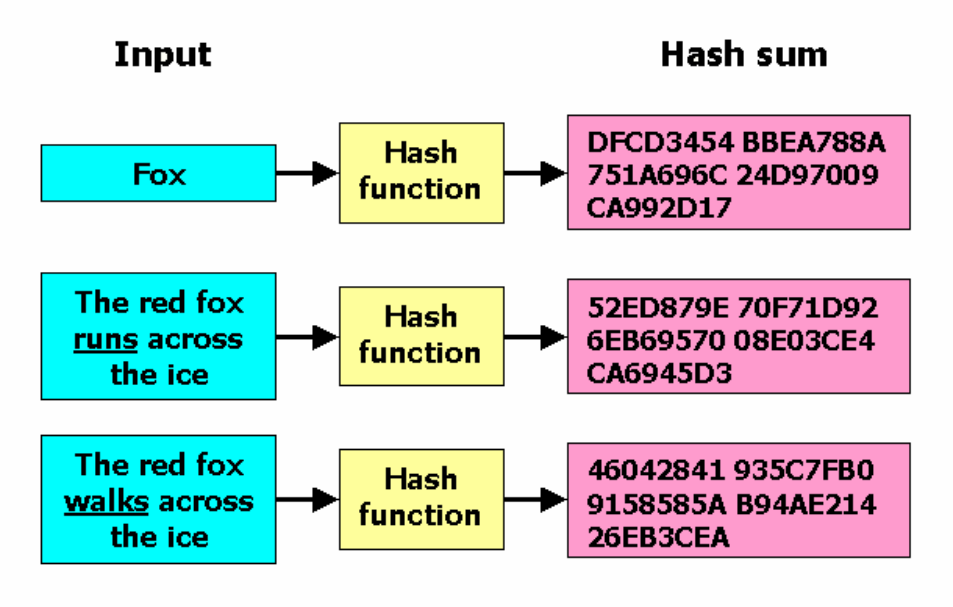


Hình 7: SSL sử dụng Thuật toán mã hóa đối xứng (với session key – khóa theo phiên) sau khi hoàn thành SSL Handshake.

Giao thức SSL/TLS hỗ trợ rất nhiều các thuật toán mã hóa, sử dụng trong quá trình xác thực server và client như hàm băm:

- Hàm băm là giải thuật nhằm sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu (có thể là một chuỗi ký tự, một đối tượng trong lập trình hướng đối tượng, v.v...).

Một hàm băm nhận đầu vào là một xâu ký tự dài (hay *thông điệp*) có độ dài tùy ý và tạo ra kết quả là một xâu ký tự có độ dài cố định.

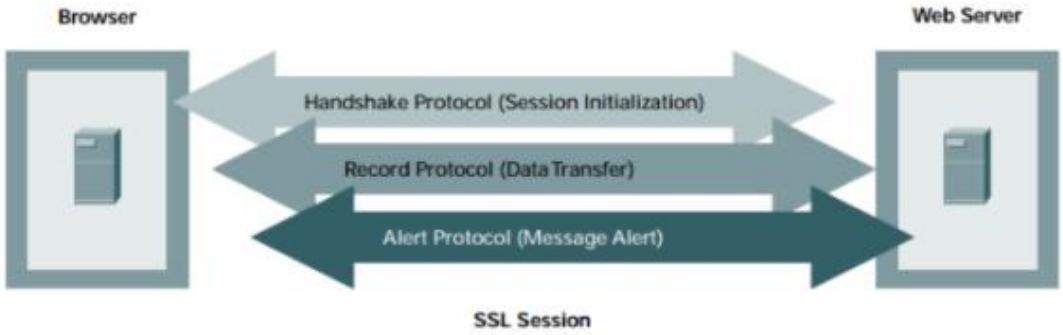


Hình 7: Hàm băm

Một số thuật toán được sử dụng:

- DES (Data Encryption Standard): là một thuật toán mã hóa có chiều dài khóa là 56 bit.
- 3-DES (Triple-DES): là thuật toán mã hóa có độ dài khóa gấp 3 lần độ dài khóa trong mã hóa DES.
- DSA (Digital Signature Algorithm): là một phần trong chuẩn về xác thực số đang được chính phủ Mỹ sử dụng
- KEA (Key Exchange Algorithm): là một thuật toán trao đổi khóa đang được chính phủ Mỹ sử dụng
- -MD5 (Message Digest Algorithm): được phát triển bởi Rivest
- RSA: là thuật toán mã hóa công khai dùng cho cả quá trình xác thực và mã hóa dữ liệu được Rivest, Shamir và Adleman phát triển
- RSA key exchange: là thuật toán trao đổi khóa dùng trong SSL dựa trên thuật toán RSA
- RC2 and RC4: là các thuật toán mã hóa được phát triển bởi Rivest dùng cho RSA Data Security
- SHA-1 (Secure Hash Algorithm): là một thuật toán băm đang được chính phủ Mỹ sử dụng

2. Hoạt động của giao thức bảo mật SSL/TLS



Hình 8: Mô hình truyền thông giữa Web Server và Browser dựa trên SSL/TLS

Mô hình một phiên truyền thông giữa máy chủ Web (Web Server) và máy khách web (Browser) dựa trên SSL/TLS. Theo đó, giao thức Bắt tay (Handshake) khởi tạo phiên làm việc (có sự hỗ trợ của giao thức Change Cipher Spec), giao thức Bản ghi (Record) vận chuyển dữ liệu an toàn và giao thức Cảnh báo (Alert) gửi các cảnh báo khi xảy ra lỗi hoặc một sự kiện đặc biệt.

Toàn bộ cơ chế hoạt động và hệ thống thuật toán mã hóa sử dụng trong SSL/TLS được phổ biến công khai, trừ khóa phiên chia sẻ tạm thời (session key) được sinh ra tại thời điểm trao đổi giữa hai ứng dụng là tạo ngẫu nhiên và bí mật đối với người quan sát trên mạng máy tính.

- Khởi tạo phiên làm việc.

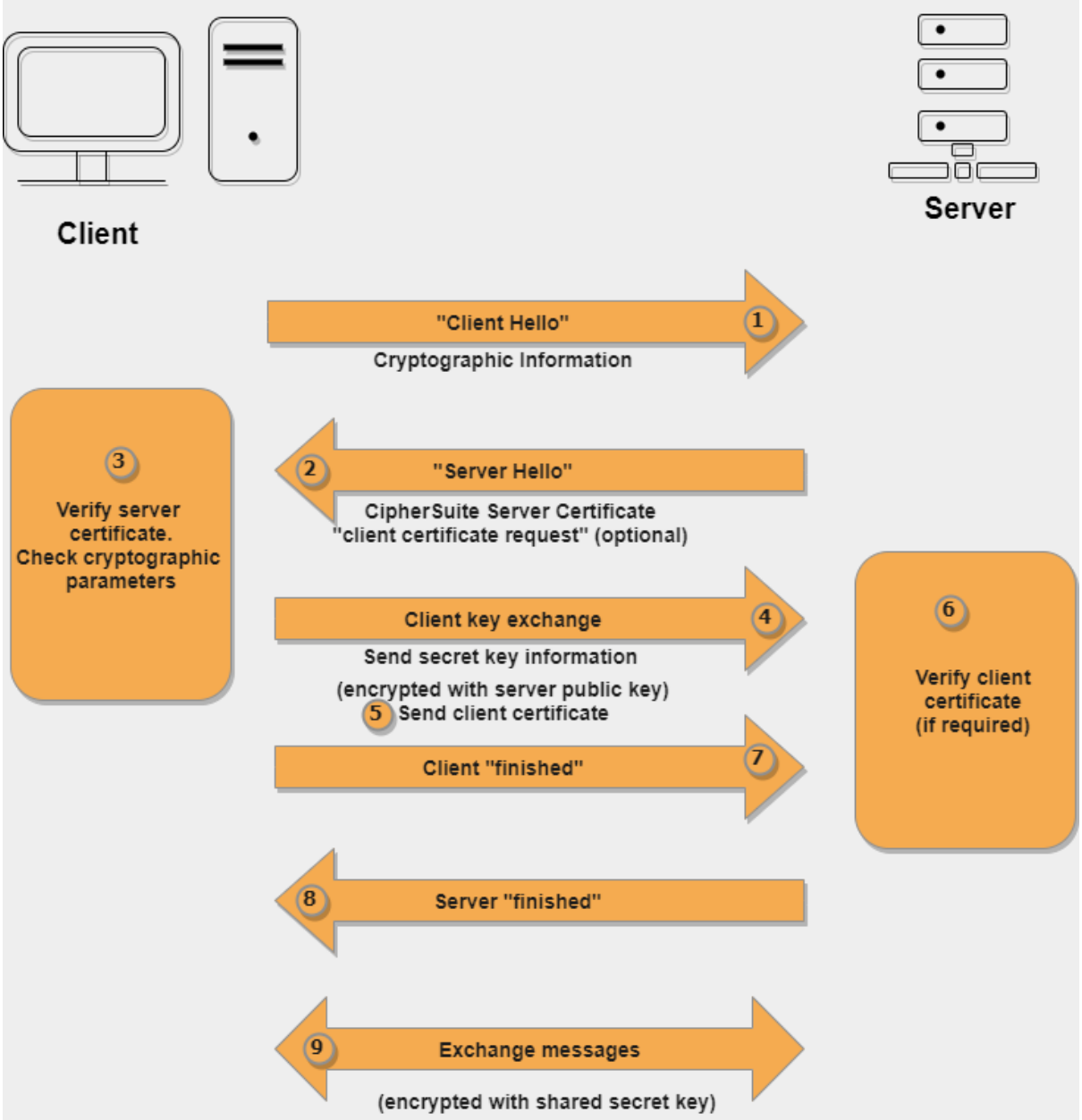
Việc giao tiếp thông qua SSL luôn bắt đầu từ quá trình SSL Handshake.

Quá trình khởi tạo phiên làm việc trong SSL/TLS được thực hiện bởi giao thức SSL Handshake với sự hỗ trợ của giao thức SSL Change Cipher Spec. Các nhiệm vụ được các bên tham gia truyền thông thực hiện trong quá trình này bao gồm:

(1) Xác thực thông tin nhận dạng.

(2) Đàm phán thống nhất các bộ mã hóa sử dụng.

(3) Trao đổi khóa và các thông số khác cho phiên truyền thông.



Hình 9: Khởi tạo phiên làm việc trong SSL/TLS

Quá trình này sử dụng thuật mã hóa "bất đối xứng" cho phép browser/client xác thực (web) server, tiếp đó là lấy public key từ server và thiết lập giao tiếp bảo mật trước khi thật sử gửi và nhận data.

Quá trình khởi tạo phiên làm việc biểu diễn giữa SSL Client (máy khách) và SSL Server (máy chủ) gồm các bước sau:

1. SSL Client gửi thông điệp “client hello” và thông tin mã hóa (Cryptographic information) đến SSL Server.
2. SSL Server gửi thông điệp “server hello”, các bộ mã hóa hỗ trợ (CipherSuite) và chứng chỉ máy chủ (Server certificate) đến SSL Client.

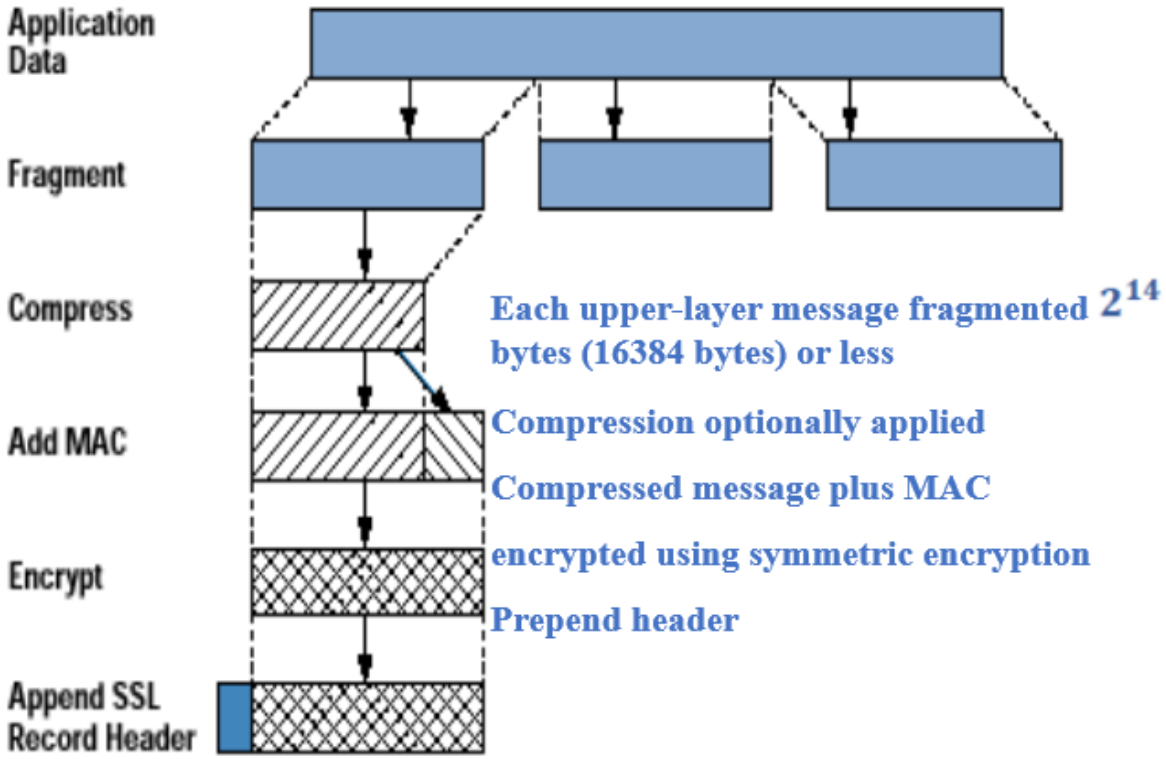
SSL Server cũng có thể gửi yêu cầu máy khách cung cấp chứng chỉ máy khách (Client certificate) nếu cần thiết.

3. Nhận được yêu cầu, SSL Client kiểm tra chứng chỉ máy chủ và kiểm tra các tham số mã hóa. Hai bên thống nhất sử dụng các bộ mã hóa tốt nhất cùng hỗ trợ cho phiên làm việc. Nếu chứng chỉ máy chủ không hợp lệ quá trình, quá trình khởi tạo phiên kết thúc không thành công. Nếu chứng chỉ máy chủ hợp lệ tiếp tục bước tiếp theo.
4. Trao đổi khóa máy khách (Client key exchange). SSL Client sinh khóa phiên – session key (hoặc các tham số mã hóa cho phiên), mã hóa khóa phiên sử dụng khóa công khai (public key) của SSL Server lấy từ chứng chỉ máy chủ và gửi cho SSL Server.
5. SSL Client cũng có thể gửi chứng chỉ máy khách cho máy chủ nếu được yêu cầu.
6. SSL Server sử dụng khóa riêng (private key) của mình để giải mã khôi phục khóa phiên (session key) gửi từ SSL Client. SSL Server cũng có thể kiểm tra chứng chỉ máy khách nếu cần thiết.
7. Client gửi thông điệp kết thúc khởi tạo phiên “finished”.
8. Server gửi thông điệp kết thúc khởi tạo phiên “finished”.

Sau khi quá trình khởi tạo thành công, hai bên SSL Client và SSL Server xác thực được các thông tin nhận dạng của nhau sử dụng chứng chỉ số, thống nhất các bộ mã hóa tốt nhất sử dụng và trao đổi được các khóa phiên, hoặc các tham số mã hóa phiên, hai bên thiết lập thành công kênh bảo mật cho truyền dữ liệu trong phiên.

- Vận chuyển dữ liệu an toàn

Quá trình vận chuyển dữ liệu an toàn thực hiện bởi giao thức SSL Record sau khi khởi tạo phiên làm việc thành công. Giao thức SSL Record sử dụng các tham số mã hóa và các bộ mã hóa thiết lập trong quá trình khởi tạo để tạo đường hầm vận chuyển dữ liệu an toàn. SSL Record đảm bảo tính bí mật cho khối dữ liệu sử dụng mã hóa đối xứng với khóa phiên và đảm bảo tính toàn vẹn và xác thực cho khối dữ liệu sử dụng hàm băm có khóa (MAC)



Hình 10: Quá trình xử lý dữ liệu bởi SSL Record tại bên gửi

Quá trình xử lý dữ liệu bởi SSL Record tại bên gửi gồm các bước:

- Phân mảnh dữ liệu (Fragment): Dữ liệu từ ứng dụng (Application Data) được phân mảnh thành các khối cho phù hợp với việc đóng gói và truyền của các lớp giao thức tầng thấp hơn.
- Nén dữ liệu (Compress): Từng khối dữ liệu được nén để giảm kích thước. Bước nén dữ liệu là không bắt buộc.
- Thêm MAC (Add MAC – Add Message Authentication Code): Tính toán giá trị MAC (sử dụng hàm băm có khóa) cho khối dữ liệu nén và ghép giá trị MAC vào khối dữ liệu. Việc thêm MAC và kiểm tra MAC ở bên nhận để đảm bảo tính toàn vẹn và xác thực khối dữ liệu.
- Mã hóa (Encrypt): Mã hóa khối dữ liệu (gồm khối dữ liệu nén và MAC) để đảm bảo tính bí mật sử dụng mã hóa khóa đối xứng với khóa phiên.
- Thêm đề mục của SSL Record (Append SSL Record Header): thêm đề mục của SSL Record vào khối dữ liệu đã mã hóa và chuyển xuống tầng giao vận để chuyển sang bên nhận.

Quá trình xử lý dữ liệu khối dữ liệu nhận được tại bên nhận được thực hiện bởi SSL Record theo trình tự ngược lại, gồm các bước: Tách đề mục của SSL

Record, Giải mã, Tách và kiểm tra MAC, Giải nén và Ghép các mảnh dữ liệu thành chuỗi dữ liệu để chuyển cho lớp ứng dụng.

III. Ứng dụng của giao thức bảo mật SSL/TLS

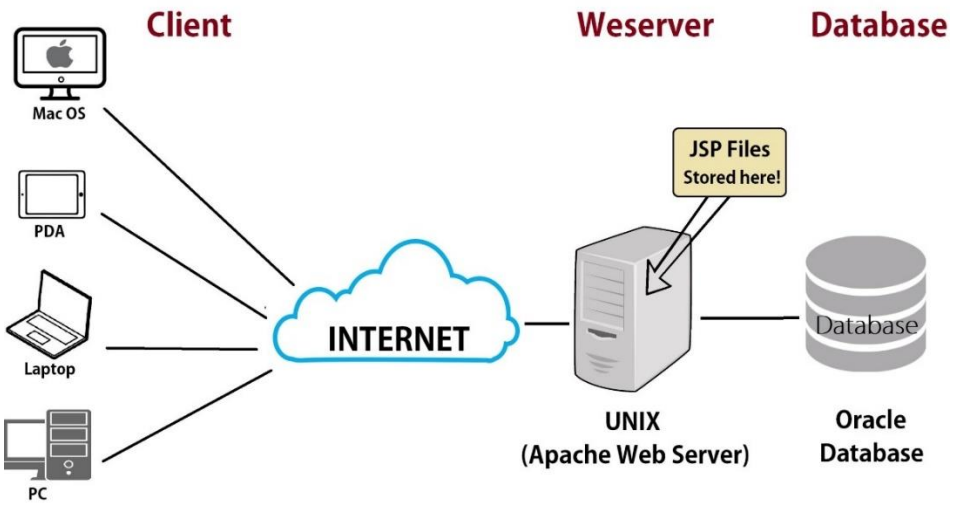
SSL/TLS vẫn là giao thức bảo mật cao nhất mà chưa một giao thức bảo mật nào có thể thay thế vai trò của nó.

- Ứng dụng đi kèm SSL/TLS được IANA (Internet Assigned Numbers Authority) công nhận:

Dịchvụ	Cổng	Mô tả
Nsiiop	261	Dịch vụ tên IIOP trên TLS/SSL
https	443	HTTP trên TLS/SSl
Smtps	465	SMTP trên TLS/SSL
Nntps	563	NNTP trên TLS/SSL
Ldaps	636	LDAP trên TLS/SSL
Ftps-data	989	FTP (dữ liệu) trên TLS/SSL
Ftps	990	FTP (Điều khiển) trên TLS/SSL
Imap	994	IRC trên TLS/SSL
Pop3s	995	POP3 trên TLS/SSL

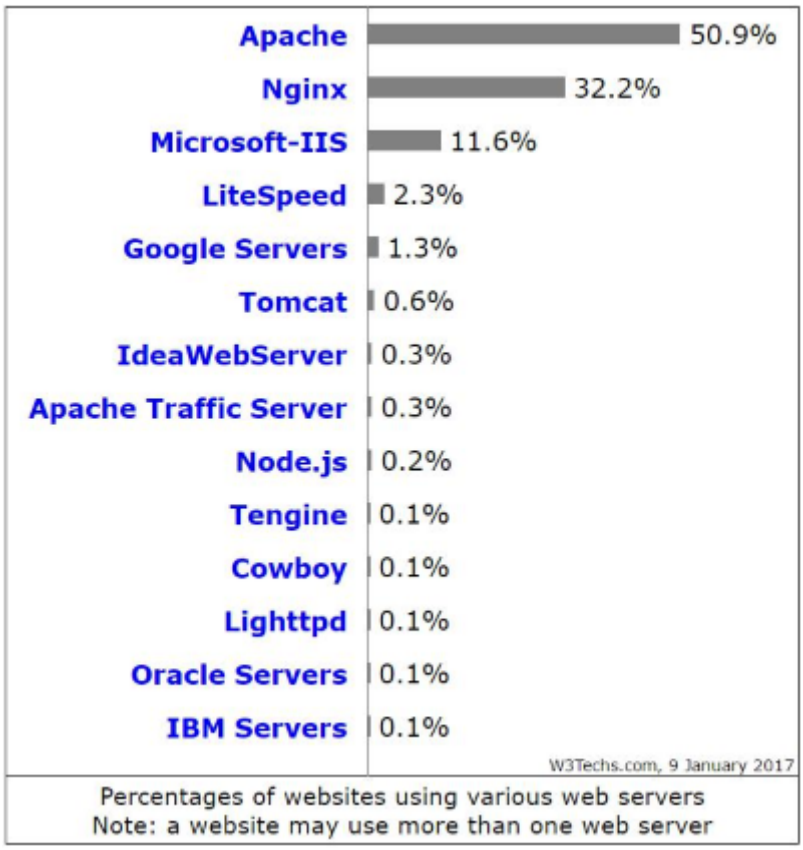
Hình 11: Các ứng dụng đi kèm SSL

- Ứng dụng SSL/TLS trên Web Server để bảo vệ Web Server an toàn hơn

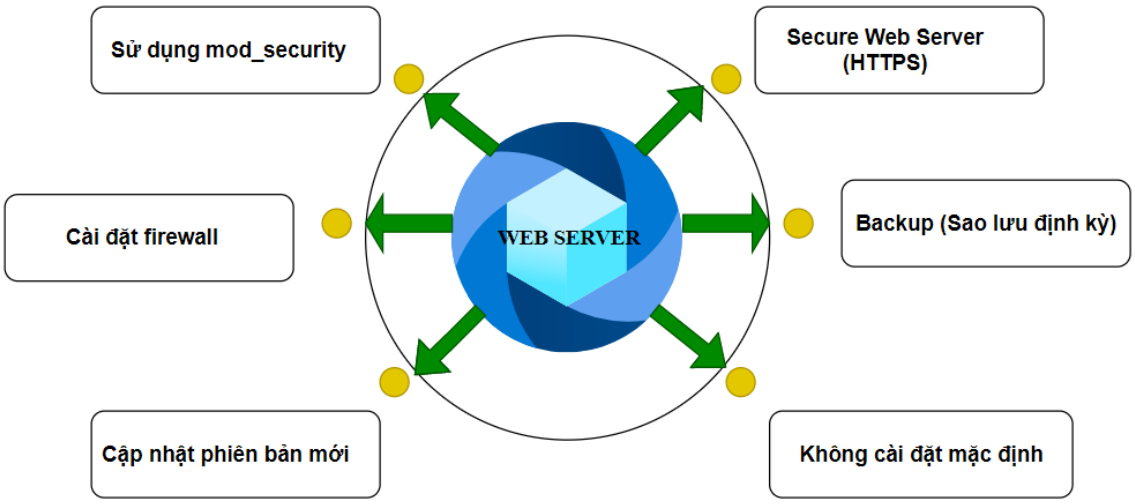


Hình 12: Truyền dữ liệu từ client đến Web server

Web server là máy chủ cài đặt các chương trình phục vụ các ứng dụng web. Webserver có khả năng tiếp nhận request từ các trình duyệt web và gửi phản hồi đến client thông qua giao thức HTTP hoặc các giao thức khác

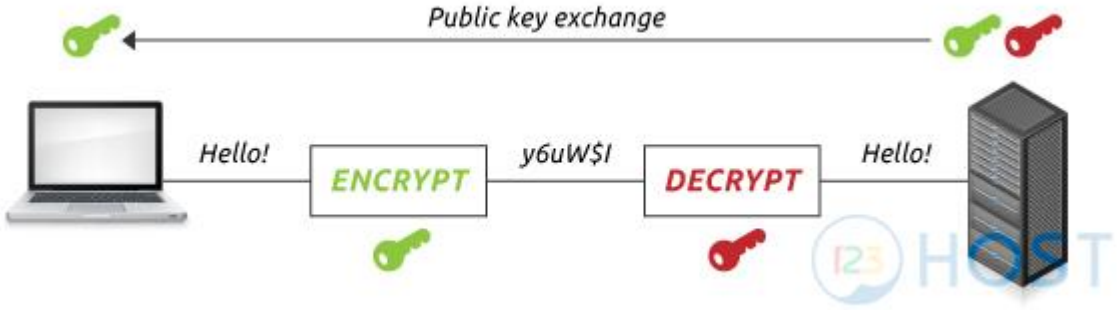


Hình 13: Các loại Web Server trên thị trường



Hình 14: Một số phương pháp cho Web server an toàn

- Ứng dụng SSL/TLS trong mã hóa thông tin nhạy cảm



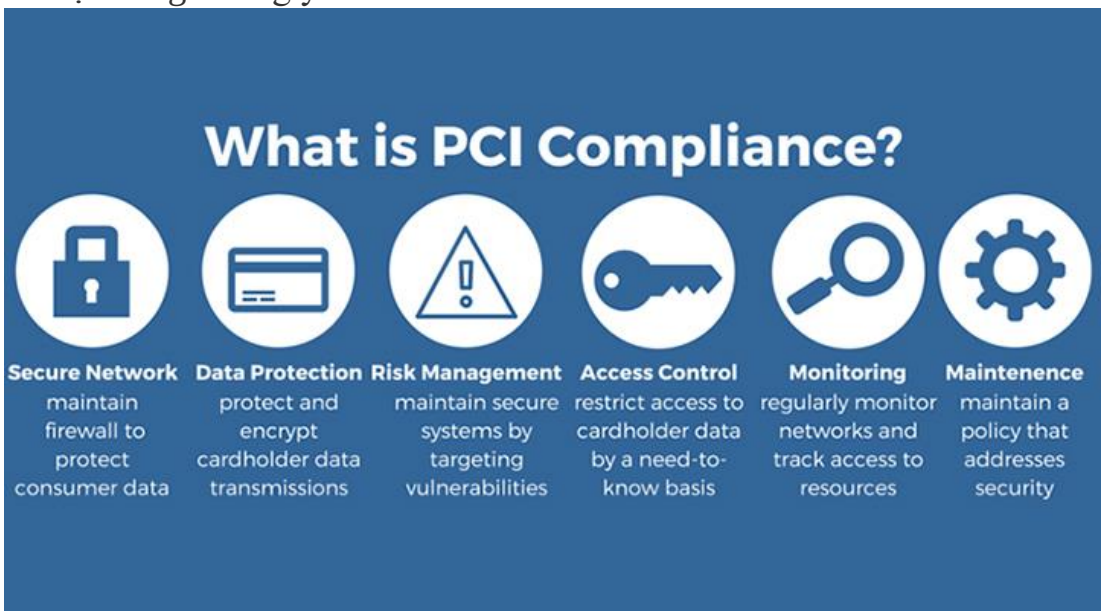
Hình 15: Dữ liệu được mã hóa trong quá trình truyền.

- Ứng dụng SSL/TLS cung cấp danh tính xác thực

Hình 16: SSL/TLS bảo vệ các giao dịch trực tuyến.

- SSL/TLS được yêu cầu cho PCI Compliance

  Các trang web yêu cầu thông tin thẻ tín dụng phải vượt qua bài kiểm tra để đảm bảo các tiêu chuẩn thanh toán bằng thẻ của PCI. Sử dụng SSL là một trong những yêu cầu đó.



Hình 17: PCI Compliance

- SSL/TLS cần thiết cho SEO

Bộ máy tìm kiếm Google đã quy định rằng các trang web có chứng chỉ SSL sẽ được ưu tiên hơn trên bảng kết quả tìm kiếm. Vì vậy, có SSL là tiêu chuẩn SEO để trang web của bạn được lên top tìm kiếm.

SEO (Search Engine Optimization - tối ưu hóa công cụ tìm kiếm), là một quy trình nâng cao thứ hạng của website trên các công cụ tìm kiếm giúp người dùng có thể tìm thấy trang web dễ dàng hơn trên bảng kết quả tìm kiếm.

Hình 18: SEO

- Ứng dụng SSL/TLS trong email

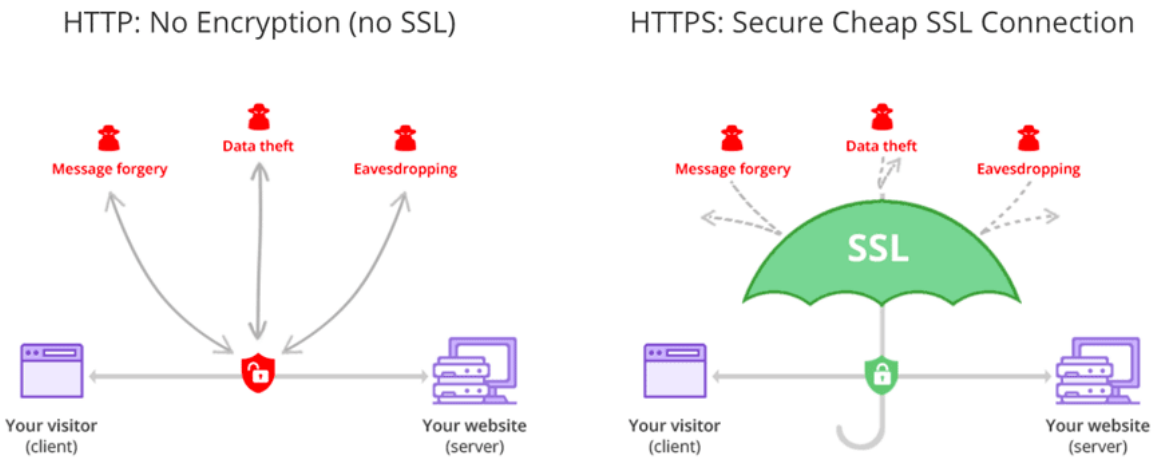
SSL/TLS là các giao thức bảo mật email phổ biến nhất để bảo vệ email khi nó di chuyển trên Internet.

Khi ứng dụng email của người dùng gửi và nhận thư, nó sẽ sử dụng Transmission Control Protocol (TCP – một phần của lớp vận chuyển và ứng dụng email khách sử dụng nó để kết nối với máy chủ email) để khởi tạo "handshake" với máy chủ email.

TLS rất quan trọng vì phần lớn các máy chủ email và ứng dụng email khách sử dụng nó để cung cấp mức mã hóa cơ bản cho email của người dùng.

- Với việc sử dụng SSL, các Website có thể cung cấp khả năng bảo mật thông tin, xác thực và toàn vẹn dữ liệu đến người dùng. SSL được tích hợp sẵn vào các browser và Web server, cho phép người sử dụng làm việc với các trang Web ở chế độ an toàn. Khi Web browser sử dụng kết

nối SSL tới server, biểu tượng ổ khóa sẽ xuất hiện trên thanh trạng thái của cửa sổ browser và dòng "http" trong hộp nhập địa chỉ URL sẽ đổi thành "https". Một phiên giao dịch HTTPS sử dụng cổng 443 thay vì sử dụng cổng 80 như dùng cho HTTP



Hình 19: HTTP và HTTPS

Ngoài ra SSL/TLS còn ứng dụng vào:

- Đóng gói các giao thức ví dụ như HTTP, FTP, SMTP, NNTP và XMPP
- Cho phép trao đổi riêng tư trên mạng
- Cho phép các ứng dụng client-server giao tiếp với nhau an toàn

- Các tác dụng của các giao thức con của SSL/TLS
  - SSL Record: Dùng để xác định các định dạng được sử dụng khi truyền dữ liệu như trong trường protocol version sẽ cho biết sử dụng SSL 3.0, TLS 1.1, TLS 1.2 hay TLS 1.3, có trường hashing để đảm bảo tính toàn vẹn và xác thực.
  - SSL Handshake: Đây là giao thức giúp client và server trao đổi các thông tin để thiết lập kết nối SSL.
  - SSL Change Cipher Spec: Sinh ra trạng thái tiếp theo để gắn vào trạng thái hiện tại, và ở trạng thái hiện tại cập nhật lại bộ mã hóa để sử dụng trên kết nối này
  - SSL Alert: Được dùng để truyền cảnh báo với liên kết bên kia như không thể thiết lập các thông số bảo mật được đưa ra từ lựa chọn có sẵn, certificate nhận được không hợp lệ, hoặc certificate đã hết hạn đăng ký…
- Nhược điểm của SSL/TLS:
  - Nhược điểm lớn nhất là chi phí, khi mà bạn phải gia hạn chứng chỉ SSL hàng năm với giá còn cao hơn cả chi phí tên miền và hosting. Tuy nhiên, nếu website của bạn không yêu cầu bảo mật quá cao, vẫn có những gói SSL giá rẻ hoặc thậm chí miễn phí cho bạn sử dụng.

- Hiệu suất là một bất lợi khác cho SSL. Bởi vì thông tin mà bạn gửi phải được mã hóa bởi máy chủ, nó sẽ chiếm nhiều tài nguyên máy chủ hơn so với thông tin không được mã hóa. Tuy nhiên, sự khác biệt về hiệu suất chỉ rõ ràng đối với các trang web có số lượng khách truy cập rất lớn.

Tài liệu tham khảo

1. Bài giảng An toàn bảo mật hệ thống thông tin PTIT TS.Hoàng Xuân Dậu
2. Giáo trình Mật mã học và an toàn thông tin TS.Thái Thanh Tùng
3. https://en.wikipedia.org/wiki/Transport_Layer_Security
4. https://www.ssl.com

LỜI CẢM ƠN

Lời đầu tiên, chúng em xin gửi lời cảm ơn chân thành tới thầy Hoàng Xuân Dậu đã đồng hành cùng chúng em và truyền đạt cho sinh viên những kiến thức giá trị và cho bọn em cơ hội được tìm hiểu và nghiên cứu đề tài Giao thức bảo mật SSL/TLS. Đây là một đề tài giúp chúng em có cái nhìn rõ hơn về An toàn thông tin. Mặc dù đã cố gắng nhưng chắc chắn những hiểu biết và kỹ năng của chúng em còn nhiều thiếu sót và hạn chế. Vậy nên, bài Báo cáo khó có thể tránh khỏi những thiếu sót và những chỗ chưa chuẩn xác, kính mong thầy xem xét và góp ý giúp bài Báo cáo của chúng em được hoàn thiện hơn để em rút kinh nghiệm và chỉnh chu hơn trong những bài tập khác.