Báo cáo SSL/TLS - Nguyễn Quốc Hùng

an ninh thông tin (Trường Đại học Kinh tế Thành phố Hồ Chí Minh)

ĐẠI HỌC KINH TẾ TP. HỒ CHÍ MINH (UEH)
TRƯỜNG CÔNG NGHỆ VÀ THIẾT KẾ
KHOA CÔNG NGHỆ THÔNG TIN KINH DOANH

BÁO CÁO ĐỒ ÁN HỌC PHẦN
BẢO MẬT THÔNG TIN TRONG THƯƠNG MẠI ĐIỆN TỬ
Đề tài: TÌM HIỂU VỀ BẢO MẬT SSL/TLS TRONG THƯƠNG MẠI ĐIỆN TỬ

GVHD: TS.GVC Nguyễn Quốc Hùng

Thực hiện: Nhóm 1

Tô Ngọc Nam (Trưởng nhóm)

Lê Đức Long

Phạm Xuân Duy

Nguyễn Thị Hoài Thu

Nguyễn Võ Thu Hương

TP. Hồ Chí Minh, Tháng 5/2023

MỤC LỤC

MỤC LỤC HÌNH ẢNH

BẢNG PHÂN CÔNG CÁC THÀNH VIÊN

Thành viên	Công việc phụ trách	Đánh giá (%)
Tô Ngọc Nam - 32101023906	Vai trò: Nhóm trưởng Công việc chính: (1) Phần định nghĩa (2) Phần công cụ tích hợp (3) Phần cách tích hợp (4) Phần Demo tích hợp SSL cho Web qua CPanel (5) Hoàn thiện hình thức báo cáo + tổng hợp file và nộp bài	100%
Phạm Xuân Duy – MSSV	Vai trò: Thành viên -Công việc chính: (1) Phần giới thiệu sơ lược (2) Phần Lợi ích – hạn chế điểm (3) Phần kết luận và đề xuất (4) Hoàn thiện hình thức báo cáo	100%
Lê Đức Long – MSSV	Vai trò: Thành viên Công việc chính: (1) Phần cách thức hoạt động (2) Phần đánh giá hiệu quả (3) Demo RSA	100%
Nguyễn Thị Hoài Thu – MSSV	Vai trò: Thành viên Công việc chính: (1) Phần những khái niệm liên quan (2) Phần phân loại (3) Phần những ứng dụng	100%
Nguyễn Võ Thu Hương – MSSV	Vai trò: Thành viên Công việc chính: (1) Phần mục đích của giao thức	100%

	(2) Phần HTTPS (3) Phần đề xuất phương pháp cải tiến	

Chữ ký (số) của nhóm trưởng

LỜI MỞ ĐẦU

Lời đầu tiên, nhóm em xin chân thành cảm ơn thầy TS.GVC Nguyễn Quốc Hùng là giảng viên của chúng em trong bộ môn Bảo mật thông tin trong TMĐT. Trong quá trình học tập, chúng em đã được thầy quan tâm hướng dẫn nhiệt tình từ thầy. Thầy đã

chia sẻ những kiến thức bổ ích, giúp chúng em có cái nhìn tổng thể hơn về chuyên ngành cũng như có cái nhìn hiểu biết hơn về bảo mật thời nay.

Trong thời đại của công nghệ thông tin và sự phát triển mạnh mẽ của thương mại điện tử, bảo mật thông tin trên mạng là một trong những vấn đề cấp bách và đặc biệt quan trọng. Nhất là khi thông tin cá nhân và tài sản trở thành mục tiêu của những kẻ xấu, các doanh nghiệp phải đảm bảo an toàn và bảo vệ thông tin của khách hàng. SSL/TLS là một trong những giải pháp bảo mật thông tin hiệu quả trên thương mại điện tử. Vì vậy, bài nghiên cứu này sẽ tập trung khám phá về các giao thức bảo mật SSL/TLS trong thương mại điện tử, đồng thời trình bày về ứng dụng và hướng phát triển của SSL/TLS trong tương lai. Bằng việc tìm hiểu sâu về SSL/TLS, chúng ta sẽ có cái nhìn toàn diện hơn về tầm quan trọng của bảo mật thông tin trong thương mại điện tử và giải pháp bảo mật hiệu quả để đảm bảo sự an toàn cho khách hàng và doanh nghiệp.

Dựa vào đó, nhóm đã lựa chọn chủ đề "Bảo mật SSL/ TLS trong Thương mại điện tử làm chủ đề nghiên cứu cho đồ án cuối kỳ môn học "Bảo mật thông tin trong Thương mại điện tử". Bố cục bài được chia làm 6 phần, nội dung chủ yếu đi sâu phân tích SSL/ TLS bao gồm cách thức hoạt động, ưu nhược điểm, tìm hiểu chứng chỉ SSL là gì, ứng dụng của nó trong Thương mại điện tử và cách tích hợp nó trên website. Hơn nữa, nhóm có đi sâu nghiên cứu các thuật toán của SSL/ TLS và demo triển khai chứng chỉ SSL cho website.

Trong quá trình nghiên cứu không thể tránh những sai sót mong thầy có thể góp để bài nghiên cứu này có thể hoàn thiện hơn và tích lũy được nhiều kinh nghiệm hơn trong tương lai. Lời cuối, lần nữa nhóm xin chân thành cảm ơn thầy, chúc thầy sẽ có nhiều sức khỏe, luôn thành công trên con đường giảng dạy và luôn đem lại những kiến thức bổ ích nhất đến thế hệ sau này.

Chương 1: Tổng quan về SSL/TLS

1.1 Giới thiệu sơ lược

1.1.1 Tổng quan về bảo mật website TMĐT ở Việt Nam

Doanh nghiệp và các trang thương mại điện tử đang trở thành mục tiêu tấn công an ninh mạng, bởi lượng dữ liệu lớn chứa thông tin cá nhân người dùng. 80% giá trị thị trường hiện tại từ các tài sản vô hình, do đó các doanh nghiệp cần phải bảo vệ cẩn thận các tài sản kỹ thuật trước những nguy cơ bị đe dọa và xâm nhập.

Mặc dù nhiều website đã bị tấn công mạng và gây thất thoát tài nguyên, nhiều doanh nghiệp vẫn chưa nhận thức rõ tính cần thiết của việc bảo mật website. Một cuộc khảo sát gần đây cho thấy 1/3 hệ thống website thương mại điện tử ở Việt Nam đều xuất hiện lỗi hoạt động nghiêm trọng, đây là một tỉ lệ khá lớn và ảnh hưởng đến hàng triệu người dùng đối mặt với nguy cơ bị rò rỉ thông tin cá nhân, khiến khách hàng mất niềm tin khi thực hiện giao dịch trên các sàn thương mại điện tử.

Nguyên nhân của tình trạng này đến từ việc bảo mật cho website chưa đủ mạnh, khiến các trang thương mại điện tử liên tục bị tấn công và đánh cắp thông tin. Với sự phát triển mạnh mẽ của người dùng internet và số người mua sắm online, các vụ tấn công mạng ngày càng gia tăng cả về số lượng và quy mô, đồng thời các hình thức tấn công cũng ngày càng tinh vi và phức tạp hơn.

Trong những năm gần đây, Việt Nam đã ghi nhận và xử lý gần 10.000 vụ tấn công website qua báo cáo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam. Gần 50% sự cố đến từ phát tán mã thông tin do những lỗ hổng bảo mật. Do đó, việc bảo mật website thương mại điện tử là rất quan trọng để đảm bảo sự an toàn của khách hàng và doanh nghiệp. Nếu thông tin và dữ liệu của khách hàng bị rò rỉ, nhiều doanh nghiệp phải chi một khoản lớn để đền bù cho khách hàng.

1.1.2 Giải pháp SSL/TLS giúp giải quyết vấn đề

Một trong mối đe dọa lớn nhất của vấn đề kinh doanh online đó chính là đe dọa an ninh mạng.

- Theo thống kê ước tính đến 2017, thiệt hại từ các cuộc tấn công mạng là 120,1 tỷ đồng.
- Hơn 2/3 khách hàng mua hàng trên online là nạn nhân của các cuộc tấn công trên mạng.
- Hơn 50.000 trang web lừa đảo mỗi tháng
- Gây ra nhiều thiệt hại

Việc mua bán online và thanh toán, chuyển khoản ngày càng nhiều kéo theo sự lừa đảo càng nhiều. SSL/ TLS sẽ là một trong những giải pháp ngày càng quan trọng

1.2 Mục đích của giao thức SSL/TLS

- Tính bảo mật: TLS/SSL cung cấp tính bảo mật bằng cách mã hóa dữ liệu được truyền đi. Điều này đảm bảo rằng thông tin nhạy cảm như thông tin đăng nhập, chi tiết thẻ tín dụng và thông tin cá nhân không thể bị chặn hoặc đọc bởi các bên trái phép.

- Tính toàn vẹn: TLS/SSL cũng đảm bảo tính toàn vẹn của dữ liệu, nghĩa là dữ liệu không thể bị thay đổi hoặc giả mạo trong quá trình truyền. Điều này đạt được bằng cách sử dụng chữ ký điện tử để xác minh rằng dữ liệu không bị sửa đổi trong quá trình truyền.

- Xác thực: TLS/SSL cung cấp xác thực bằng cách xác minh danh tính của máy chủ và trong một số trường hợp là máy khách. Điều này giúp ngăn chặn các cuộc tấn công trung gian và đảm bảo rằng người dùng đang giao tiếp với máy chủ dự định.

- Tin cậy: TLS/SSL được tin cậy trên một chuỗi tin cậy, trong đó cơ quan cấp chứng chỉ bên thứ ba (CA) cấp chứng chỉ kỹ thuật số cho các trang web. Điều này giúp người dùng tin tưởng rằng họ đang tương tác với một trang web hợp pháp chứ không phải một trang web giả mạo.

- Tuân thủ: TLS/SSL là tiêu chuẩn được chấp nhận rộng rãi và được yêu cầu bởi nhiều quy định tuân thủ, bao gồm Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) và Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA).

Tóm lại, TLS/SSL được sử dụng để bảo vệ thông tin truyền tải qua mạng và đảm bảo tính toàn vẹn, tính bảo mật và tính riêng tư của thông tin. Nó cũng giúp đảm bảo tính khả dụng của dịch vụ truyền tải thông tin qua mạng.

Chương 2: Cơ sở lý thuyết về SSL/TLS

2.1 Định nghĩa SSL/TLS

SSL là chữ viết tắt của thuật ngữ Secure Sockets Layer. Đây là giao thức bảo mật có vai trò quan trọng trong đảm bảo sự riêng tư và toàn vẹn dữ liệu khi chúng được gửi – nhận trên môi trường Internet.

SSL đóng vai trò quan trọng trong mã hóa thông tin, dữ liệu khi duyệt web, ứng dụng web, email, tin nhắn và thoại qua IP. Nhờ được mã hóa trong suốt quá trình gửi và nhận, bên thứ 3 không thể xem được nội dung gói tin đã gửi. Chỉ cho đến khi đến đúng bên nhận thì những thông tin, dữ liệu đó mới được giải mã.

Sau SSL, giao thức TLS (Transport Layer Security) là tên gọi sau này của SSL (từ năm 1999). Chuẩn SSL đã ngừng cập nhật từ năm 1996 và hiện nay gần như không được hỗ trợ nữa. Tuy nhiên, đến thời điểm hiện tại mọi người trên Thế Giới đều vẫn quen gọi SSL thay vì TLS.

Khi chúng ta nói chuyện, trao đổi thông tin với nhau hoặc giao dịch (mua bán) các dịch vụ liên quan đến SSL chính là đang nói về TLS. Có lẽ cộng đồng phải cần thêm thời gian nữa để làm quen với "tên gọi mới" TLS, mặc dù tên gọi này đã đổi hơn 20 năm qua.

❖ Đặc điểm của SSL/TLS:

- SSL sử dụng mã hoá khoá công khai để thực hiện trao đổi khóa phiên.
- Mỗi khoá phiên chỉ được dùng trong một phiên làm việc.
- Toàn bộ dữ liệu được mã hóa bởi khóa phiên và mã hóa khóa bí mật.
- Sử dụng hàm băm có khóa (MAC) để đảm bảo tính toàn vẹn và tính xác thực của thông điệp.
- Có ít nhất một thực thể (thông thường sẽ là server) có chứng chỉ số cho khóa công khai (Public key certificate).

❖ Cấu trúc của giao thức SSL

SSL được thiết kế để sử dụng TCP (Transmission Control Protocol) cung cấp một dịch vụ bảo mật đáng tin cậy từ "đầu cuối" đến "đầu cuối". SSL là hai giao thức được minh họa như dưới đây:

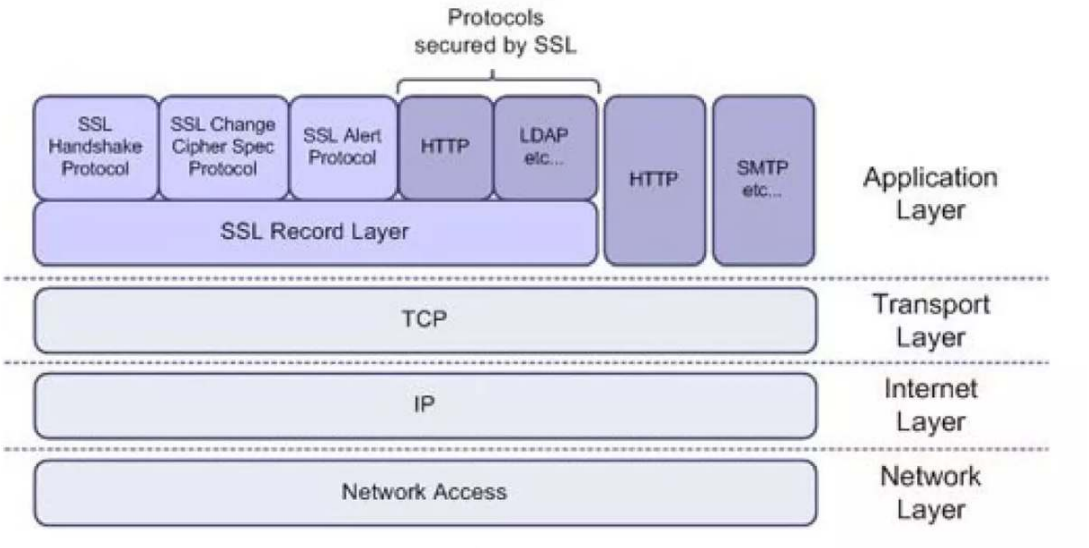


Figure 1: Chồng giao thức SSL

Có thể thấy SSL như một lớp trung gian bảo mật giữa Transport Layer và Application Layer. SSL sẽ có bốn thành phần (Handshake Protocol: Khởi tạo kết nối an toàn giữa client và server; Record Protocol: Mã hóa và giải mã thông tin truyền tải giữa client và server bằng cách sử dụng khóa phiên được tạo ra trong bước Handshake Protocol. Change Cipher Spec Protocol: Thông báo cho đối tác kết nối rằng khóa phiên sẽ được sử dụng để mã hóa và giải mã thông tin truyền tải và Alert Protocol: Thông báo lỗi hoặc cảnh báo cho client và server nếu có vấn đề xảy ra trong quá trình kết nối hoặc truyền tải dữ liệu.

SSL cung cấp dịch vụ kết nối an ninh có ba đặc tính cơ bản:

Kết nối bí mật: Mã hóa được sử dụng sau khi thiết lập kết nối để xác định một khóa bí mật. Mã hóa đối xứng được sử dụng để mã hóa dữ liệu (ví dụ các tiêu chuẩn mã hóa: Data Encryption Standard - DES, 3DES – Triple Data Encryption Standard, RC4).

Định danh của điểm kết nối có thể được xác thực bằng cách sử dụng mã hóa bất đối xứng hoặc khóa công khai (ví dụ như Rivest-Shamir-Adleman - RSA, Digital Signature Standard - DSS).

Kết nối đáng tin cậy. Thông điệp vận chuyển thông báo bao gồm kiểm tra tính toàn vẹn thông điệp sử dụng một MAC, hàm băm an toàn được sử dụng để tính toán MAC ví dụ SHA, MD5.

2.2 Những khái niệm liên quan

2.2.1 Mật mã học

Là một công cụ quan trọng để bảo vệ thông tin được truyền tải bằng máy tính. Mật mã học là quá trình biến đổi dữ liệu thành định dạng không thể đọc được, chỉ có người nhận đích thực mới có thể hiểu và sử dụng nó. Mật mã học là nghệ thuật và khoa học của việc che giấu thông tin quan trọng và bí mật khỏi việc vi phạm bởi những người không được ủy quyền. Do đó, nó nhằm bảo vệ và đảm bảo an toàn thông tin khỏi những kẻ tấn công mạng hoặc bất kỳ ai khác ngoài người nhận đích thực.

Mật mã học cho phép mọi người giao tiếp trên Internet và truyền tải thông tin quan trọng và bí mật một cách an toàn. Do đó, mật mã học cho phép người dùng sử dụng các phương tiện công khai hoặc riêng tư như internet để mua sắm trực tuyến và tránh trở thành nạn nhân của tội phạm và kẻ bắt đầu từ mật khẩu. Điều này được thực hiện bằng cách sử dụng những tiến bộ công nghệ mới nhất trong khoa học máy tính.Giúp người dùng và các tổ chức mã hóa và giải mã các thông điệp ẩn trong các mã, mật mã và số học để thông tin có thể được truyền tải một cách an toàn. Mật mã học bắt đầu từ các khóa mã hóa và khóa giải mã. Quá trình mã hóa và biến đổi văn bản rõ thành định dạng không thể đọc được được gọi là mã hóa; trong khi quá trình giải mã và chuyển đổi văn bản không thể đọc được thành thông tin có thể đọc được bằng cách sử dụng một khóa số đặc biệt được gọi là giải mã. Mục đích chính của mật mã học là bảo vệ thông tin, email, chi tiết thẻ tín dụng và các dữ liệu cá nhân khác được truyền qua một mạng công khai.

Dưới đây là một số nguyên tắc quan trọng của mật mã học:

- Mã hóa: Mã hóa là một trong những nguyên tắc quan trọng của mật mã học. Nguyên tắc này cho biết rằng một tin nhắn hoặc thông tin phải được mã hóa để trở thành không thể đọc được, nhằm bảo vệ sự riêng tư của cá nhân. Nguyên tắc này cũng cho thấy rằng người nhận thông tin phải giải mã thông tin đã nhận được bằng cách sử dụng một khóa số đặc biệt.
- Xác thực: Một trong những nguyên tắc quan trọng của mật mã học là xác định nguồn gốc của thông tin. Khi nguồn thông tin được xác định, việc giao tiếp một cách an toàn trở nên dễ dàng hơn. Xác thực chỉ có thể thực hiện được bằng cách

cung cấp một sự trao đổi khóa đặc biệt để được sử dụng phù hợp bởi người gửi để chứng minh danh tính của mình.

- Tính toàn vẹn: Tính toàn vẹn của thông tin gửi cho người nhận rất quan trọng. Nguyên tắc này cho biết rằng mật mã học đảm bảo tính toàn vẹn của dữ liệu bằng cách cung cấp các mã và khóa số để đảm bảo rằng những gì chúng ta nhận được là chính xác và từ người được định. Người nhận được đảm bảo rằng thông tin nhận được không bị thay đổi hoặc bị đe dọa trong quá trình truyền tải. Ví dụ, một hàm băm mật mã học được sử dụng để đảm bảo tính toàn vẹn của thông tin.
- Không thể chối bỏ: Nguyên tắc này đảm bảo rằng người gửi thông tin không thể từ chối việc gửi thông tin đó. Nguyên tắc này sử dụng chữ ký số để ngăn người gửi từ việc phủ nhận nguồn gốc của dữ liệu.

Phân loại mật mã học

Mật mã học được chia thành 3 loại chính:

❖ **Mã hóa khóa bí mật**

Mã hóa khóa bí mật (Secret Key Cryptography) hay còn gọi là mã hóa đối xứng (symmetric encryption): chỉ sử dụng một khóa duy nhất cho việc mã hóa và giải mã dữ liệu. Khi người gửi dữ liệu gửi thông tin, họ mã hóa dữ liệu bằng cùng một khóa mà người nhận sẽ sử dụng để giải mã thông tin. Hạn chế của kỹ thuật này là việc phân phối một khóa duy nhất có thể rơi vào tay một kẻ tấn công, người có thể dễ dàng giải mã thông tin.

Có rất nhiều thuật toán cho mã hóa khóa bí mật như AES, DES, 3DES, RC4, Blowfish and Twofish

❖ **Mã hóa khóa công khai:**

Mã hóa khóa công khai (Public Key Cryptography) hay còn gọi là mã hóa bất đối xứng (asymmetric encryption) sử dụng một cặp chìa khóa số. Hệ thống hai khóa cho phép các bên giao tiếp một cách an toàn hơn trên mạng công cộng. Trong mật mã khóa công khai, mỗi bên giao tiếp có một cặp khóa, một khóa là "khóa bí mật" (private key), khóa thứ hai là "khóa công khai" (public key), khóa công khai có thể được chia

sẻ giữa các bên. Khi gửi thông tin, người gửi mã hóa thông tin bằng cách sử dụng khóa công khai, và người nhận giải mã thông tin bằng cách sử dụng khóa riêng của mình thành định dạng đọc được.

Có nhiều thuật toán khác nhau cho mã hóa khóa công khai như: Diffie-Hellman, RSA, ECC, DSA.

❖ **Hàm băm:**

Hàm băm (hash function) là một phương pháp không yêu cầu sử dụng bất kỳ khóa số nào, mà thay vào đó nó sử dụng một giá trị băm có độ dài cố định để mã hóa văn bản thông thường. Hàm băm là một phép biến đổi đơn giản, được thực hiện bằng cách áp dụng một thuật toán băm lên dữ liệu đầu vào. Nếu dữ liệu không bị thay đổi, giá trị băm sẽ không thay đổi. Đây là một phương pháp mã hóa một chiều, được sử dụng để đảm bảo tính toàn vẹn của thông điệp.

Một số thuật toán băm phổ biến: MD5, SHA-1, SHA-2

2.2.2 Cơ sở hạ tầng khóa công khai

Cơ sở hạ tầng khóa công khai (PKI) là một tập hợp giao thức, quy trình và hạ tầng để tạo ra và xác thực chứng chỉ kỹ thuật số, được sử dụng để trao đổi thông tin an toàn và xác thực. Nó được phát triển để hỗ trợ mật mã khóa công khai. PKI đã được thiết kế để đảm bảo sự chấp nhận kỹ thuật và tính hợp pháp cho việc truyền thông an toàn của các tin nhắn bí mật dưới dạng điện tử thông qua cấu trúc của nó. Các thành phần cơ bản của PKI:

Cơ quan cấp chứng chỉ (CA): Còn được gọi là Cơ quan cấp phát chứng chỉ, được sử dụng để cấp chứng chỉ và danh sách thu hồi (revocation lists). Một chứng chỉ là một cấu trúc dữ liệu gồm giá trị của khóa công khai và thông tin xác định thuộc về chủ sở hữu của khóa bí mật tương ứng. Mỗi chứng chỉ khóa công khai được cấp cho một cá nhân và mỗi chứng chỉ có chữ ký số của CA phát hành. Chứng chỉ có tuổi thọ từ một đến hai năm. Chứng chỉ có thể bị thu hồi vì một số lý do như mất khóa bí mật, khóa bí mật bị lộ hoặc tuổi thọ của chứng chỉ đã kết thúc, v.v. Nếu xảy ra bất kỳ một trong những tình huống này, thực thể đã cấp chứng chỉ phải yêu cầu vô hiệu hóa (thu hồi) chứng chỉ khóa công khai. Có nhiều cơ chế thu hồi để thu hồi chứng chỉ và cho phép người dùng kiểm tra tính hợp lệ của chứng chỉ (chứng chỉ vẫn còn hiệu lực hay

đã bị thu hồi). Tất cả các cơ chế thu hồi cần được thực hiện đúng thời gian và hiệu quả. Một trong các cơ chế thu hồi là CRL (Danh sách thu hồi chứng chỉ) là một danh sách chứa các chứng chỉ đã bị thu hồi và được ký số bởi thực thể đã cấp chứng chỉ đó trước đây.

Cơ quan đăng ký (RA): được sử dụng để gửi tất cả các yêu cầu đến CA và xác thực danh tính của tất cả người dùng và đăng ký thông tin của người dùng cuối trước khi cấp chứng chỉ. Dịch vụ được cung cấp bởi RA có thể truy cập thông qua hai cách:

1) Đăng nhập quản trị viên qua trình duyệt vào hệ thống.

2) Gọi giao diện dịch vụ web thông qua hệ thống ứng dụng.

RA chỉ có một quản trị viên siêu cấp có thể truy cập vào tất cả các chức năng do RA cung cấp, trong đó quản trị viên siêu cấp này có thể thêm nhiều quản trị viên hơn nếu cần. Mỗi quản trị viên muốn quản lý hệ thống phải sử dụng thẻ thông minh riêng của mình để ngăn người chưa xác thực thực hiện bất kỳ hoạt động nào trên cơ quan đăng ký (RA).

Hệ thống phân phối và kho lưu trữ chứng chỉ: được sử dụng để cung cấp cơ chế lưu trữ, chúng lưu trữ thông tin về chứng chỉ và CRL. Sự phức tạp của PKI có thể được ẩn đi đối với hệ thống khách hàng bằng cách thêm một thành phần nữa là Cơ quan Xác thực (VA), mà phản hồi các yêu cầu từ phía khách hàng về trạng thái thu hồi chứng chỉ và đánh giá tính khả dụng của chứng chỉ thay mặt cho hệ thống khách hàng.

2.2.3 Khóa phiên

Khóa phiên (session key) là bất kỳ khóa đối xứng nào được sử dụng để mã hóa chỉ một phiên liên lạc. Nói cách khác, đó là một khóa tạm thời chỉ được sử dụng một lần, trong một khoảng thời gian nhất định, để mã hóa và giải mã dữ liệu gửi giữa hai bên; các cuộc hội thoại trong tương lai giữa hai người sẽ được mã hóa bằng các khóa phiên khác nhau. Khóa phiên giống như mật khẩu mà ai đó đặt lại mỗi khi họ đăng nhập.

2.3 Lịch sử của SSL/TLS

2.3.1 Lịch sử phiên bản

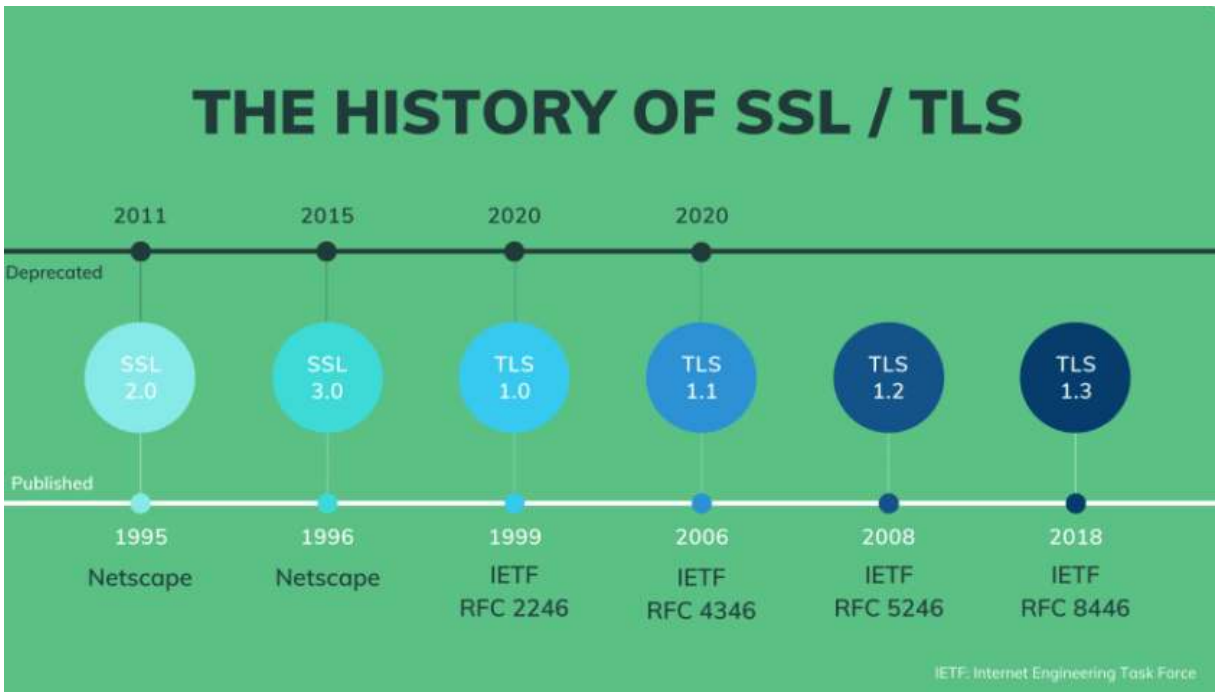


Figure 2: Lịch sử của SSL/ TLS

SSL 1.0

Năm 1994, Netscape đã hoàn thiện phiên bản SSL 1.0, nhưng phiên bản này không được công bố công khai vì có một số lỗ hổng bảo mật đáng kể. Nhược điểm bao gồm sự dễ bị tấn công bằng cách phục hồi tấn công (replay attacks) và một lỗ hổng dễ dàng để kẻ tấn công thay đổi các tin nhắn văn bản thô của người dùng.

SSL 2.0

Sau khi SSL 1.0 thất bại, Netscape tiếp tục phát hành phiên bản 2.0 và vào tháng 2 năm 1995. SSl 2.0 chứa các lỗ hổng cấu trúc không nên được chấp nhận và đã bị loại bỏ vào năm 2011:

- Các tin nhắn Handshake không được bảo vệ, điều này có thể cho phép một kẻ tấn công MITM gian lận khách hàng sử dụng một thuật mã yếu hơn so với thông thường.
- Phiên có thể dễ dàng bị chấm dứt. Một kẻ tấn công MITM có thể dễ dàng chèn một TCP FIN để đóng phiên, và các bên không thể xác định liệu việc kết thúc phiên có hợp pháp hay không.

- Cùng một khóa được sử dụng cho tính toàn vẹn tin nhắn và mã hóa, điều này là một vấn đề nếu khách hàng và máy chủ thỏa thuận về một thuật toán mã hóa yếu.

SSL 3.0

SSL 3.0 được công bố công khai vào tháng 11 năm 1996, với mục tiêu khắc phục những khuyết điểm của SSL 2.0.

- SSL 3.0 có thể chống lại cuộc tấn công MITM9 bằng cách lưu trữ các thông điệp xác thực đã được hoàn thành bao gồm băm từ tất cả các bước trao đổi trước đó.
- SSL 3.0 sử dụng HMAC10 sử dụng mã hóa 128-bit. Kẻ tấn công không thể thay đổi thông tin ngay cả trên một kết nối mở. Nó cung cấp xác thực tin nhắn chính.
- SSL 3.0 cho phép người dùng can thiệp vào quá trình bắt tay và thay đổi thuật toán và khóa theo yêu cầu.
- SSL 3.0 có một giao thức trao đổi khóa chung. Nó cho phép trao đổi khóa Diffie - Hellman và Fortezza và chứng chỉ non - RSA.
- SSL 3.0 sử dụng thuật toán băm SHA2 - 1, an toàn hơn rất nhiều so với thuật toán MD51. Nó cũng cung cấp thêm các bộ mã hóa khác.

Tuy nhiên, SSL 3.0 đã trở thành đối tượng của một loạt các cuộc tấn công như cuộc tấn công SSL Renegotiation, cuộc tấn công POODLE, cuộc tấn công LUCKY13, cả về cơ chế trao đổi khóa và hệ thống mã hóa mà nó hỗ trợ. Phiên bản SSL này không còn an toàn nữa do:

- Tráo đổi khóa - Tráo đổi khóa của SSL 3.0 dễ bị tấn công MITM9 khi sử dụng việc khôi phục phiên hoặc thương lượng.
- Lớp ghi - Padding không xác định trong Cipher Block Chaining (CBC) cho phép phục hồi dữ liệu văn bản rõ, đó là cuộc tấn công POODLE. Những khuyết điểm trong chế độ CBC phản ánh bởi những khuyết điểm trong bộ mã hóa dòng nó sử dụng

- Nguyên tắc mã hóa tùy chỉnh - SSL 3.0 xác định cấu trúc cho HMAC, chữ ký số, nhưng những cấu trúc này thiếu kiểm tra mật mã. Hơn nữa, SSL 3.0 và các phiên bản trước của nó dựa vào SHA2 - 1 và MD51 là các thuật toán băm của chúng, mà có độ yếu tương đối.
- Khả năng giới hạn - SSL 3.0 không thể sử dụng nhiều tính năng đã được thêm vào các phiên bản TLS mới hơn, cũng như các tính năng được bao gồm trong ClientHello, mà SSL 3.0 không hỗ trợ.

TLS 1.0

TLS 1.0 được dựa trên phiên bản cuối cùng của SSL, tức là SSL 3.0. TLS 1.0 được định nghĩa lần đầu trong RFC 2246 vào tháng 1 năm 1999 như là một phiên bản nâng cấp của SSL 3.0, được viết bởi Christopher Allen và Tim Dierks của Consensus Development.

TLS 1.0 là một giao thức đã tồn tại trong hai thập kỷ và đã có những lỗ hổng bảo mật như cuộc tấn công BEAST12, cuộc tấn công CRIME13; ngoài ra, nó còn hỗ trợ mã hóa yếu không đảm bảo tính bảo mật cho các kết nối hiện đại.

TLS 1.1

TLS 1.1 được phát hành vào năm 2006 là một giao thức đã tồn tại trong một thập kỷ, được thiết kế để khắc phục một số lỗi trong TLS 1.0, nhưng không có sự thay đổi đáng kể trong phiên bản mới hơn. Do những lỗ hổng và thuật toán băm của nó, TLS 1.0 và TLS 1.1 đã bị loại bỏ vào năm 2020 và không còn được sử dụng. Sử dụng TLS 1.1 là một ý kiến không tốt, mặc dù nó đã giải quyết một phần vấn đề của TLS 1.0, nhưng vì giao thức này không cung cấp bất kỳ chế độ mã hóa cipher nào, giao thức này không hoạt động trong thế giới hiện đại.

TLS 1.2

Giao thức bảo mật TLS 1.2 mới nhất đã được phát hành lần đầu vào tháng 8 năm 2008.

Khi kích hoạt TLS 1.2 trên trình duyệt web, người dùng sẽ an toàn khỏi các cuộc tấn công như BEAST12 và sử dụng các bộ mã hóa an toàn hơn, từ đó giảm sự phụ thuộc vào RC4 stream cipher. Phiên bản mới chuẩn bị trình duyệt web cho các lỗ hổng đã được phát hiện trong các giao thức bảo mật cũ.

Hầu hết các trình duyệt web hiện nay mặc định hỗ trợ TLS 1.2, tuy nhiên, một số người dùng có thể gặp khó khăn khi kết nối với các trang web không hỗ trợ TLS 1.2 vì không thể thực hiện thỏa thuận đúng. Theo Tiêu chuẩn Tuân thủ PCI16, các trang web chịu trách nhiệm về thanh toán bằng thẻ tín dụng, như Apple, Microsoft, Google và Mozilla (chịu trách nhiệm với trình duyệt Safari, Microsoft Edge, Internet Explorer, Google Chrome và Firefox) phải sử dụng TLS 1.2.

Cho đến nay, TLS 1.2 được coi là giao thức bảo mật an toàn và là giao thức bảo mật mặc định, nhưng việc phát hiện ra các lỗ hổng mới đặt tính đáng tin cậy của TLS 1.2 vào thách thức. Nghiên cứu đã tiết lộ hai lỗ hổng mới trong giao thức TLS 1.2, tạo điều kiện cho các cuộc tấn công tương tự như POODLE để xâm nhập vào hệ thống. Phương pháp mã hóa Cipher Block Chaining (CBC) cho phép tấn công MITM9 trên các phiên VPN và web được mã hóa. Hỗ trợ của TLS 1.2 cho phương pháp mã hóa cũ này và những điều chỉnh nhỏ trong các cuộc tấn công POODLE làm cho việc tấn công hệ thống trở nên khả thi.

ZOMBIE POODLE, tương tự như cuộc tấn công POODLE nhưng mạnh mẽ hơn nhiều, tấn công vào phương pháp mã hóa cũ trong TLS 1.2. Ngay cả khi một hệ thống đã hoàn toàn khắc phục lỗ hổng POODLE, ZOMBIE POODLE vẫn có thể tấn công thành công hệ thống.

TLS 1.3

Cách đây vài năm, SSL/TLS chỉ được sử dụng bởi các cơ quan chính phủ và các công ty công nghệ khổng lồ. Ngày nay, TLS 1.3 đang được các tổ chức sử dụng để bảo vệ dữ liệu và cung cấp an ninh.

Theo các thông tin thì lượng người dùng TLS 1.2 vẫn còn chiếm ưu thế vượt trội hơn so với phiên bản TLS 1.3, điều này cho thấy một điều rằng mặc dù mức độ bảo mật, xử lý của TLS 1.3 vượt trội hơn nhưng vẫn còn gặp nhiều trở ngại có thể do hệ thống đã cũ không thể nâng cấp. Tuy nhiên trong tương lai gần thì TLS 1.3 sẽ chiếm ưu thế.

Ưu điểm so với 1.2

- Lợi ích về tốc độ - thời gian thực hiện bắt tay của TLS 1.3 đã được rút ngắn, chỉ cần một vòng chuyến để hoàn thành bắt tay, số lượng đàm phán đã giảm từ 4 xuống còn 2.

- Bộ mã đơn giản hơn - TLS 1.3 hỗ trợ bộ mã không bao gồm thuật toán chữ ký và trao đổi khóa; tuy nhiên, nó sử dụng ECDHE để đảm bảo bí mật tiến lên hoàn hảo. TLS 1.3 có 5 bộ mã khác nhau:

  TLS_AES_256_GCM_SHA384

  TLS_CHACHA20_POLY1305_SHA256

  TLS_AES_128_GCM_SHA256

  TLS_AES_128_CCM_8_SHA256

  TLS_AES_128_CCM_SHA256

- Cải thiện bảo mật - TLS 1.3 đã loại bỏ tất cả các tính năng không an toàn như SHA-1, RC4, DES, 3DES, AES-CBC, MD5, tạo điều kiện thuận lợi cho hacker. TLS 1.3 đáng tin cậy hơn so với TLS 1.2.

Tóm lại, TLS 1.3 nhanh hơn và an toàn hơn TLS 1.2. Hầu hết các lỗ hổng lớn trong TLS 1.2 xuất phát từ các thuật toán mã hóa cũ vẫn được hỗ trợ. TLS 1.3 không còn hỗ trợ các thuật toán mã hóa dễ bị tấn công, và do đó ít dễ bị tấn công từ mạng.

2.3.2 Thống kê số lượng sử dụng SSL/ TLS

Theo số liệu từ Netcraft: "Đến tháng 1 năm 2022 có tổng cộng 1.205.428.664 trang web trên thế giới và 96,5% trong số đó được bảo vệ bằng mã hóa SSL/TLS".

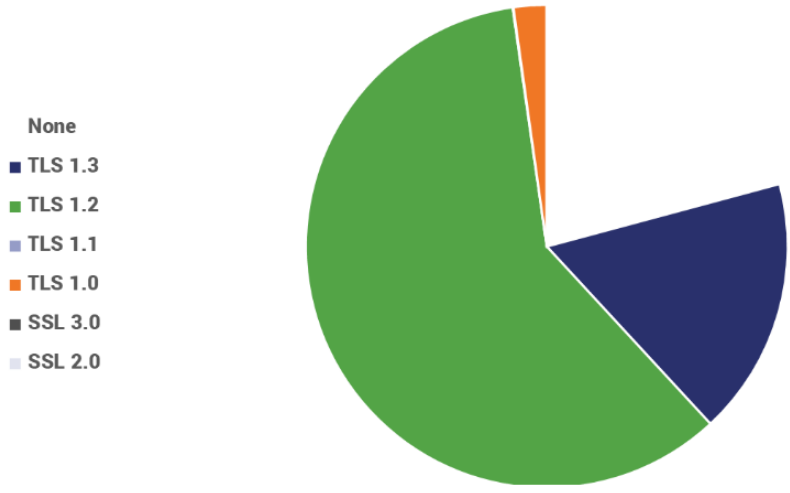


Figure 3: Các phiên bản SSL/ TLS

Nhận xét: Theo các thông tin thì lượng người dùng TLS 1.2 vẫn còn chiếm ưu thế vượt trội hơn so với phiên bản TLS 1.3, điều này cho thấy một điều rằng mặc dù mức

độ bảo mật, xử lý của TLS 1.3 vượt trội hơn nhưng vẫn còn gặp nhiều trở ngại có thể do hệ thống đã cũ không thể nâng cấp. Tuy nhiên trong tương lai gần thì TLS 1.3 sẽ chiếm ưu thế.

Theo khảo sát của SSL Pulse:

"Tỷ lệ áp dụng TLS 1.3 theo thời gian: Tỷ lệ áp dụng của TLS 1.3 liên tục tăng lên, từ 11,78% vào ngày 17 tháng 9 năm 2018 lên đến 48,09% vào ngày 31 tháng 12 năm 2020. Lưu ý rằng tỷ lệ áp dụng TLS 1.3 tăng với tốc độ cao hơn đáng kể so với các phiên bản TLS cũ. Đặc biệt, chỉ sau 264 ngày (30 tháng 4 năm 2019) kể từ khi TLS 1.3 (RFC 8446) được chính thức thông qua (10 tháng 8 năm 2018), tỷ lệ áp dụng đã vượt qua 15%. Ngược lại, việc chuyển từ TLS 1.1 sang TLS 1.2 mất khoảng năm năm để đạt tỷ lệ 15% sau ngày thông qua của TLS 1.2".

"Xét về giao thức mã hóa SSL/TLS, TLS 1.2 được sử dụng rộng rãi nhất, chiếm 84,6% tổng số kết nối được mã hóa tính đến tháng 1 năm 2022. TLS 1.3, phiên bản mới nhất của giao thức, chiếm 15,4% kết nối được mã hóa."

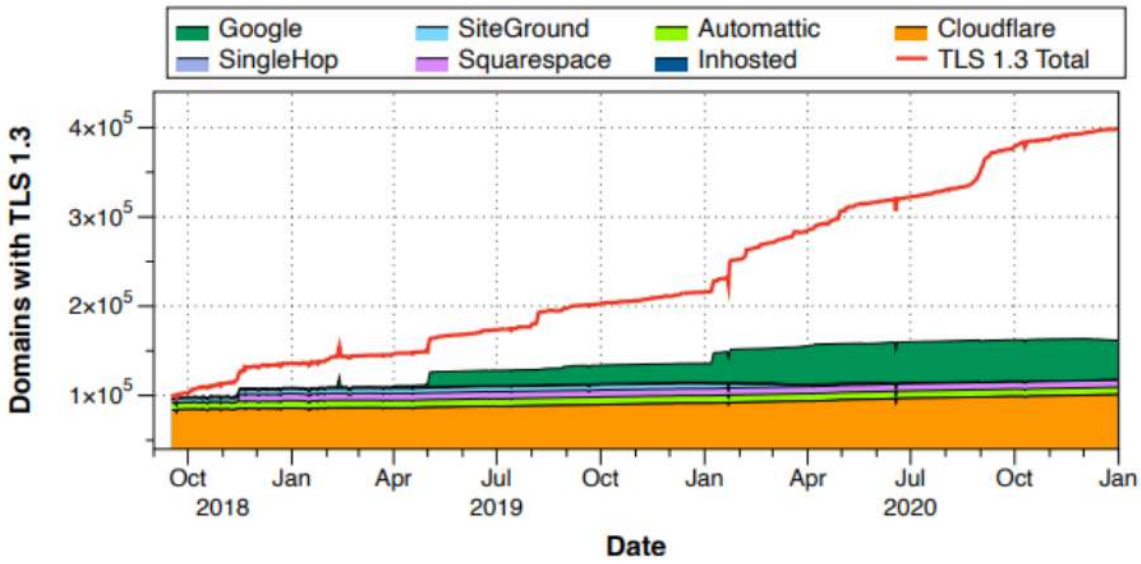


Figure 4: Tỉ lệ chấp nhận TLS 1.3 theo nền tảng

Nhận xét: TLS 1.2 chiếm 84,6% điều này không ngạc nhiên vì TLS 1.2 đã được sử dụng trong một thời gian dài và đã được chứng minh là an toàn và đáng tin cậy trong các ứng dụng web.

Tuy nhiên, điều đáng chú ý là tỷ lệ sử dụng TLS 1.3, phiên bản mới nhất của giao thức, cũng đã đạt được 15,4% kết nối được mã hóa. Đây là một tín hiệu tích cực và cho thấy sự chuyển đổi từ TLS 1.2 sang TLS 1.3 đang diễn ra dần dần trên Internet.

TLS 1.3 mang lại nhiều cải tiến về hiệu suất và bảo mật, bao gồm việc loại bỏ các thuật toán cũ không an toàn và tăng cường tính bảo mật trong quá trình xác thực và mã hóa.

Sự gia tăng trong việc sử dụng TLS 1.3 là một dấu hiệu tích cực, đồng thời cũng đòi hỏi sự cập nhật và nâng cấp từ phía các máy chủ và trình duyệt web để hỗ trợ phiên bản này. Việc khuyến khích và thúc đẩy việc sử dụng TLS 1.3 sẽ giúp tăng cường tính bảo mật và hiệu suất của các kết nối mã hóa trên Internet.

2.4 Cách thức hoạt động của SSL/TLS

SSL/TLS mã hóa bằng cách sử dụng kết hợp Symmetric và Asymmetric Encryption như sau:

- Sử dụng **Asymmetric Encryption** để trao đổi **Session Key** (khóa cho phiên làm việc này thuộc nhóm **Symmetric Encryption Key**)

- Sử dụng **Symmetric Encryption Key** đã trao đổi để mã hóa dữ liệu hiển thị trên trang web cũng như trong quá trình vận chuyển dữ liệu thuộc 1 phiên làm việc…

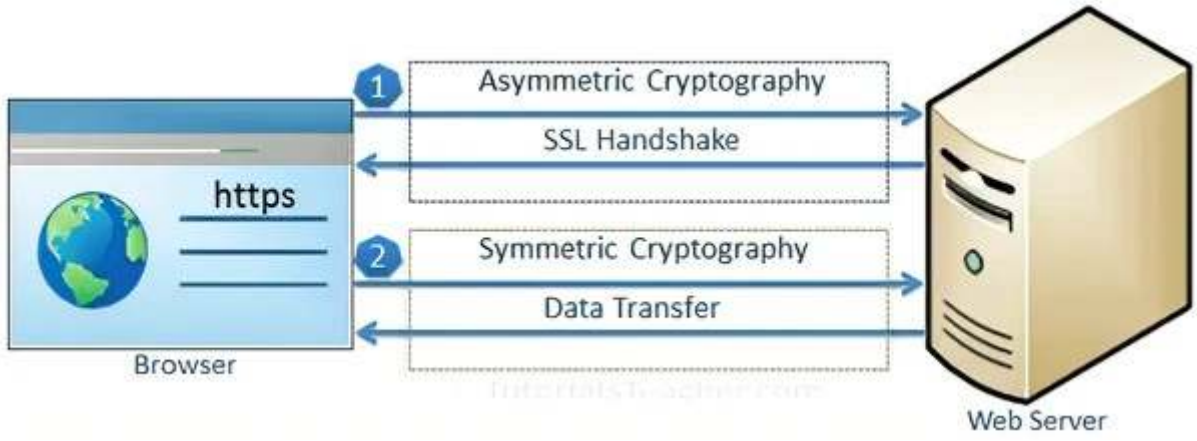


Figure 5: Cách thức hoạt động của SSL/ TLS

Giao thức SSL truyền dữ liệu một cách an toàn

Về cơ bản 2 giai đoạn

Giai đoạn 1: Handshake Protocol

Figure 6: Giai đoạn Handshake

1. Client gửi yêu cầu tới Web server (bao gồm thông tin cần thiết để server có thể giao tiếp:

Supported versions	TLS 1.3 TLS 1.2
Supported cipher suites	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
Supported key exchange groups	Finite Field Groups (DHE) Elliptic Curve Groups (ECDHE)
Key share	Client's DHE public key Client's ECDHE public key
Supported signature algorithms	RSA-PSS ECDSA

Figure 7: Gói tin yêu cầu tới server

- **SSL/TLS Version**: Phiên bản SSL/TLS được hỗ trợ.
- **Cipher Suites**: Danh sách các ciphersuite (kết hợp giữa thuật toán mã hóa đối xứng và bất đối xứng) mà máy chủ hỗ trợ. Ví dụ, đây là một ví dụ về một bộ mã hóa: ***TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256***
    - Key Exchange Algorithms (RSA, DH, **ECDH**, PSK)
    - Authentication/Digital Signature Algorithm (**RSA**, DSA)
    - Bulk Encryption Algorithms (**GCM**, AES)
    - Message Authentication Code Algorithms (SHA384, **SHA256)**

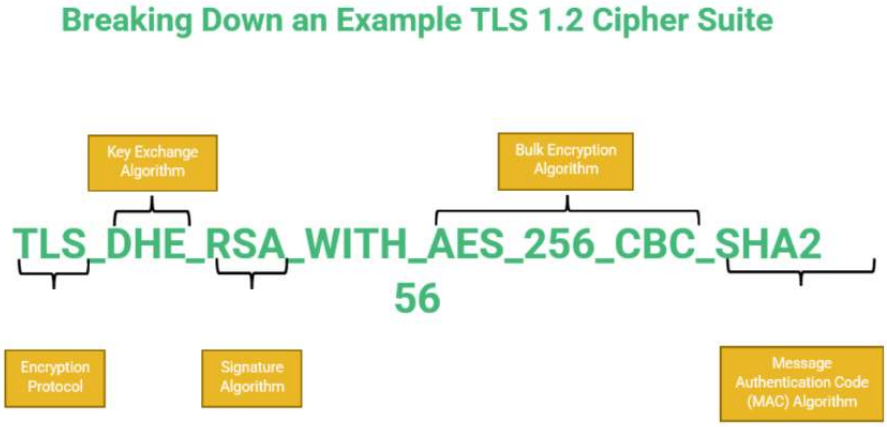


Figure 8: Cipher Suite TLS 1.2

Do RSA Key Exchange có vấn đề với Oracle Padding Attack và vì Perfect Forward Secrecy là bắt buộc với TLS 1.3, Cipher Suites mặc định sẽ sử dụng Ephemeral Diffie-Hellman làm Key Exchange và Signature Algorithm nên được ghi rút gọn lại còn 2 thành phần

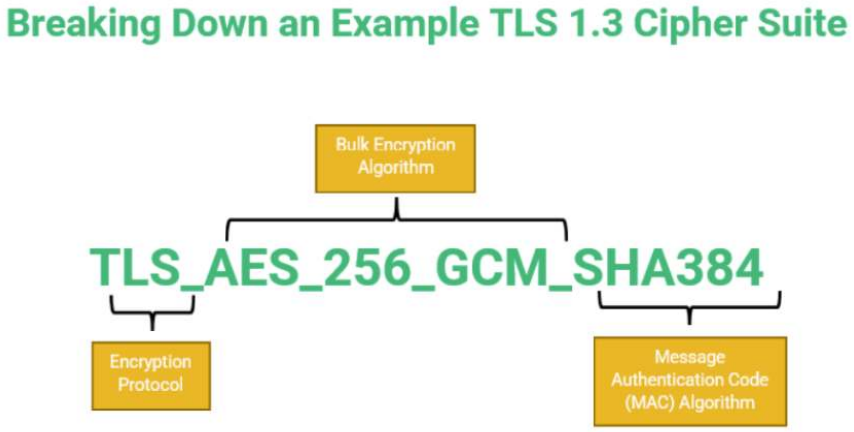


Figure 9: Cipher Suite TLS 1.3

- **Key Exchange Algorithm**: Thuật toán trao đổi khóa như RSA
- **Certificate**: Chứng chỉ số của máy chủ chứa thông tin về công khai của máy chủ và được ký bởi một tổ chức phát hành chứng chỉ (Certificate Authority - CA).
- Server Hello Done: Thông báo cho máy khách biết rằng máy chủ đã hoàn thành quá trình gửi yêu cầu.

2. Phản hồi lại Client qua gói tin gồm (SSL version, cipher suites, session-specific data, SSL cert, **public key**,..)

Selected versions	TLS 1.3
Selected cipher suites	TLS_AES_256_GCM_SHA384
Selected key exchange groups	Finite Field Groups (DHE)
Key share	Server's DHE public key
Certificate request *	Request for client's certificate
Server Certificate	Server's certificate
Certificate verify	Signature of entire handshake
Server Finish	MAC of entire handshake

Figure 10: Gói tin Server phản hồi

3. Client xác thực SSL Cert có hợp lệ hay không thông qua CA (Certificate Authority)
4. Nếu không hợp lệ thì từ chối kết nối
    a. Nếu hợp lệ thì Client tạo ra session key được mã hóa bởi **publickey** rồi gửi tới webserver
    b. Server dùng **private key** để giải mã lấy session key
5. Gửi gói tin **xác nhận** tới Client được mã hóa bằng session key, Client giải mã gói tin bằng session key để cho biết server đã sẵn sàng và chuyển sang giai đoạn truyền dữ liệu sử dụng mã hóa đối xứng

TÓM LẠI:

Với TLS, cụ thể Handshake là quá trình client và server thống nhất về Cipher Suite sẽ được sử dụng để tạo kết nối bảo mật. Ví dụ với TLS 1.2, quá trình Handshake được tóm lược như sau:

- Client và server xác định Cipher Suite được hỗ trợ bởi cả 2 phía;
- Server gửi Certificate và Public Key cho client;
- Client xác thực Certificate và Digital Signature;
- 2 bên triển Key Exchange Protocol để tạo Symmetric Session Keys;
- Quá trình mã hóa bắt đầu và HMAC được dùng để bảo đảm quá trình Handshake không bị can thiệp.

RESUMPTION & PRE-SHARED KEY

Không phải lúc nào Web Server và Client cũng trải qua quá trình handshake đầy đủ này, đôi khi sẽ xảy ra quá trình handshake rút gọn bằng cách nối lại khóa chia sẻ trước đó (Pre Shared Key - PKD).

Figure 11: Quá trình handshake rút gọn

Sau lần bắt đầu đầu tiên thì Client và Server đã biết nhau nên không cần phải xác thực lại. Vì vậy Server có thể gửi một hay nhiều "ticket" cho Client, chức năng của nó là xác thực danh tính cho lần handshake tiếp theo. Nó bao gồm thời gian khả dụng của ticket và một số thông tin khác

Trong lần handshake tiếp theo thì Client chỉ cần gửi một yêu cầu đơn giản chứa danh sách PSK hay ticket được nhận từ lần handshake trước đó

Giai đoạn 2: Record Protocol (Data Transfer)

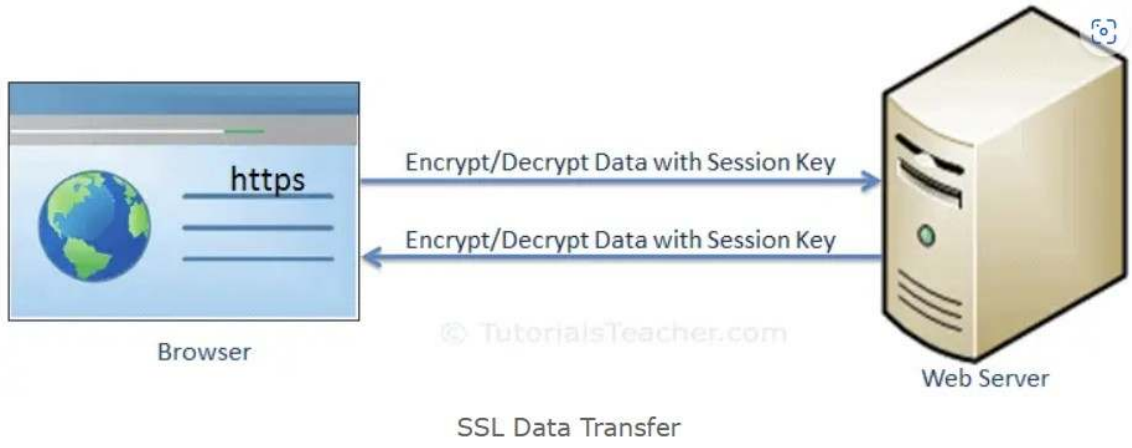


Figure 12: Giai đoạn Record

Trong giai đoạn này, **tất cả các tin nhắn gửi đi** sẽ được mã hóa bằng **session key** dùng chung được thiết lập trong quá trình **handshake**. Sau đó, các tin nhắn được phân mảnh và nén lại, sau đó chèn thêm MAC (Giá trị MAC được tính dựa trên một thuật toán băm như HMAC) để duy trì tính toàn vẹn của dữ liệu

Cuối cùng gói tin được mã hóa bằng mã hóa khóa đối xứng và thêm SSL Header rồi gửi sang phía bên kia.

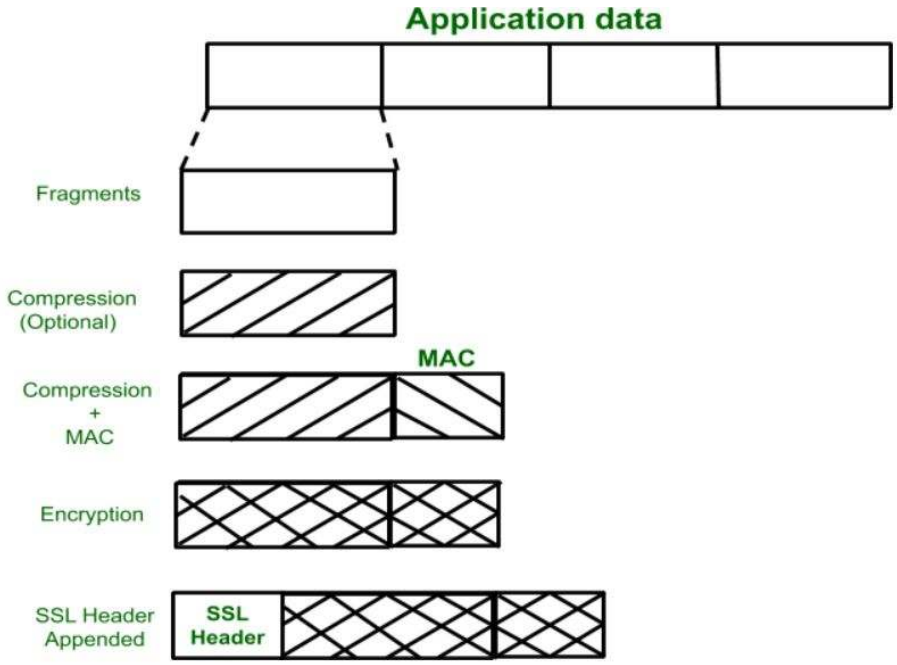


Figure 13: Dữ liệu ứng dụng

Chúng sẽ được xác minh để xem liệu có bất kỳ sửa đổi nào trong quá trình truyền tải hay không. Nếu không, các tin nhắn sẽ được giải mã bằng cùng một **session key** đối xứng hay gọi là mã hóa đối xứng, các thuật toán phổ biến bao gồm AES (Advanced Encryption Standard) và 3DES (Triple Data Encryption Standard). Vì vậy, chúng sẽ đạt được cả **tính bảo mật và tính toàn vẹn** trong giao thức này. Và vì lượng dữ liệu được mã hóa trong giai đoạn này lớn nên thường được gọi là mã hóa hàng loạt.

Ngoài ra, SSL/TLS còn có giao thức:

Alert

Được sử dụng để chuyển các cảnh báo liên quan đến SSL tới thực thể ngang hàng. Cũng như các ứng dụng khác sử dụng SSL. Cảnh báo có thể được mã hóa hoặc không được mã hóa và có thể xảy ra trong khi handshake hoặc trong giai đoạn record

Có hai loại cảnh báo:

- **Cảnh báo đóng cửa:** Kết nối giữa máy khách và máy chủ phải được đóng đúng cách để tránh bất kỳ loại tấn công cắt ngang nào. Một tin nhắn **close_notify**

được gửi cho người nhận biết rằng người gửi sẽ không gửi tin nhắn nữa trên kết nối đó.

- **Cảnh báo lỗi:** Khi phát hiện lỗi, bên phát hiện sẽ gửi tin nhắn cho bên kia. Khi truyền hoặc nhận được tin nhắn cảnh báo, cả hai bên ngay lập tức đóng kết nối. Một số ví dụ về cảnh báo lỗi là:
    - unexpected_message: message không thích hợp
    - decompression_failure: không thể giải nén
    - handshake_failure: không thể bắt tay do không phù hợp với danh sách cipher suit

Change Cipher Spec

Đây là giao thức đơn giản nhất, nó bao gồm một message đơn 1 byte giá trị là 1. Mục đích chính là để thực hiện **chuyển đổi** từ quá trình trao đổi khóa và thỏa thuận ciphersuite sang việc sử dụng các khóa và thuật toán mã hóa đã được thống nhất.

Sau khi nhận được message, phía đối tác cũng thực hiện việc chuyển đổi và từ đó, cả hai bên sử dụng các khóa và thuật toán đã thỏa thuận để mã hóa và giải mã dữ liệu.

2.5 Những thuật toán sử dụng trong SSL/TLS

2.5.1 Thuật toán trao đổi khóa

Ở phiên bản TLS 1.2 việc sử dụng mã hóa bất đối xứng diễn ra ở quá trình Trao đổi khóa. Tiêu biểu là RSA, sử dụng tính chất toán học của số nguyên tố để tạo một cặp public và private key. RSA dựa trên cơ sở của việc khó phân tích thừa số đối với tích của 2 số nguyên tố lớn. Đối với RSA, key size hiệu quả được đề xuất là 2048 bit (đến năm 2030), sau năm 2030 là 3072 bit.

Quy trình sinh Public key và Private Key

Step	A				B		
	Private	Public	Calculated	Sent	Calculated	Public	Private
1	p, q	e, N	N=p*q	e,N→			

2	p, q	e, N, o		←o	$o=i^e \bmod N$	e, N, o	i
3	p, q, i	e, N, o	$=(p-1)*(q-1)$ $d=e^{-1} \bmod$ $i=o^d \bmod N$			e, N, o	i

Bước 1: A chọn 2 số nguyên tố private **p, q** , 1 số public **e** và tính số public **N = p * q.** Sau đó A gửi e và N sang cho B;

Bước 2: B xác định con số input **i** (văn bản gốc) cần mã hóa, tính và gửi o sang cho A. Như vậy lúc này sẽ có e, N và o được public;

Bước 3: Khi nhận được thông tin mã hóa o từ B, A tính sau đó tìm thông tin đầu vào **(**=(q-1)*(p-1))

Như vậy bằng phương án sử dụng public key của A (e và N), B có thể **mã hóa thông tin đầu vào i** thành **thông tin mã hóa o** và gửi sang cho A qua các kênh không bảo mật. Về phía mình, A có thể giải mã o để đọc được i bằng cách sử dụng private key. Sau đó chuyển các con số thành văn bản.

Ví dụ minh họa:

Tham số	Giá trị	Ghi chú
p	11	Số nguyên tố ngẫu nhiên đầu tiên
q	17	Số nguyên tố ngẫu nhiên thứ hai
N	187	p*q
	160	(p-1)*(q-1)
e	7	public key, chọn ngẫu nhiên sao cho BCNN (e,)=1
i (plain text)	99	Văn bản gốc, chuyển hóa từ văn bản thành con số
o (cipher text)	176	Bản mã,
d	23	private key,
check i	99	Kiểm tra văn bản

2.5.2 Thuật toán chữ ký số

Thuật toán chữ ký, còn được gọi là thuật toán xác thực, xác thực danh tính của người gửi tin nhắn cho người nhận. Điều này rất quan trọng đối với giao tiếp an toàn vì nó đảm bảo rằng giao tiếp đang diễn ra với một máy chủ hợp pháp. (Nói cách khác, kẻ xấu không mạo danh chủ sở hữu chứng chỉ và giao tiếp thay cho họ.)

Quá trình ký

- Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm)
- Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)
- Thông điệp ban đầu (message) được ghép với chữ ký số(Digital signature) tạo thành thông điệp đã được ký (Signed message)
- Thông điệp đã được ký (Signed message) được gửi cho người nhận

Quá trình xác thực

- Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
- Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)
- Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số tạo ra chuỗi đại diện thông điệp MD2
- So sánh MD1 và MD2: Nếu trùng nhau thì thông điệp còn nguyên vẹn và ngược lại

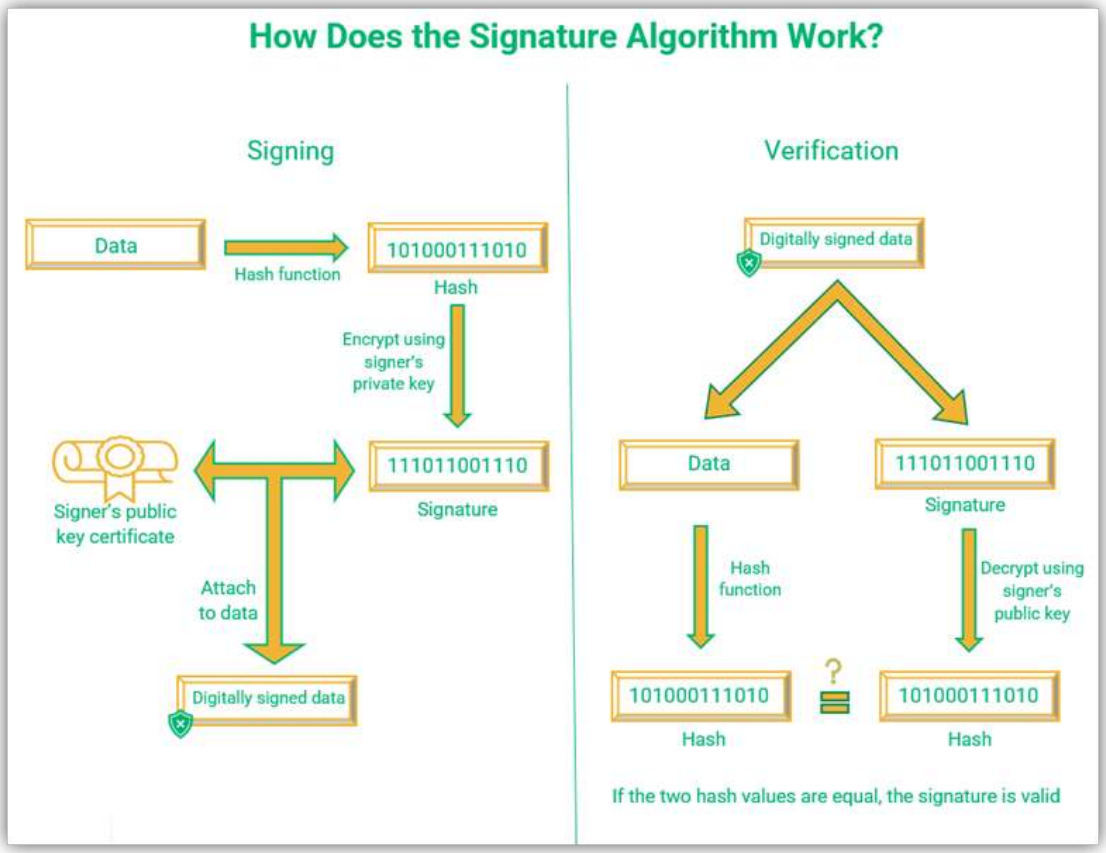


Figure 14: Thuật toán ký số và xác thực

Chương 3: Ứng dụng của SSL/ TLS

3.1 Những ứng dụng của SSL/TLS

Bảo mật trang web: SSL/TLS được sử dụng để bảo vệ giao tiếp giữa trình duyệt web và máy chủ web thông qua HTTPS. Điều này đảm bảo rằng thông tin nhạy cảm như thông tin đăng nhập, thông tin cá nhân và giao dịch tài chính được mã hóa và bảo vệ khỏi nguy cơ đánh cắp hoặc xâm nhập.

Bảo mật Email: SSL/TLS được sử dụng trong các giao thức email như SMTP, POP3 và IMAP để mã hóa dữ liệu và bảo vệ quá trình truyền tải email. Điều này đảm bảo rằng email được gửi và nhận qua kết nối SSL/TLS không thể bị đánh cắp hoặc đọc trái phép.

VPN (Virtual Private Network): SSL/TLS được sử dụng trong các ứng dụng VPN để tạo kênh kết nối bảo mật giữa người dùng và máy chủ VPN. Điều này đảm bảo rằng dữ liệu được mã hóa và bảo mật khi truyền qua mạng công cộng và bảo vệ khỏi các cuộc tấn công MITM.

Cổng thanh toán trực tuyến: SSL/TLS được sử dụng trong cổng thanh toán trực tuyến để bảo vệ quá trình thanh toán và giao dịch tài chính trực tuyến. Khi giao dịch được thực hiện qua HTTPS, thông tin thanh toán và tài khoản ngân hàng được mã hóa và bảo vệ an toàn.

Truyền tải dữ liệu qua mạng nội bộ: SSL/TLS được sử dụng để bảo vệ dữ liệu truyền tải trong mạng nội bộ của một tổ chức. Điều này đảm bảo rằng dữ liệu nội bộ không thể bị đánh cắp hoặc truy cập trái phép khi truyền qua mạng.

Ứng dụng di động: SSL/TLS được sử dụng trong các ứng dụng di động để bảo mật giao tiếp và truyền tải dữ liệu giữa ứng dụng và máy chủ. Điều này đảm bảo tính bảo mật và riêng tư của thông tin người dùng và dữ liệu trong môi trường di động.

Ứng dụng trong thanh toán: SSL/TLS cũng được áp dụng để bảo vệ các giao dịch thanh toán qua điện thoại di động, ví điện tử và các ứng dụng thanh toán khác. Điều này giúp tăng cường độ tin cậy và an toàn trong các giao dịch thanh toán trực tuyến và góp phần thúc đẩy sự phát triển của thương mại điện tử.

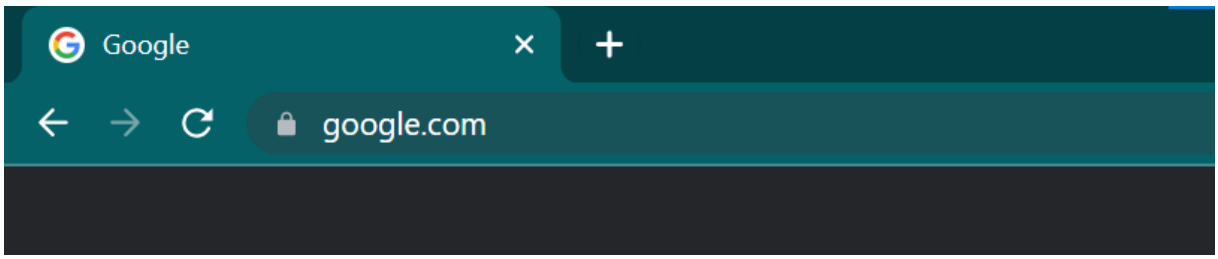
3.2 Tích hợp SSL cho Website

3.2.1 Chứng chỉ SSL là gì?

Chứng chỉ SSL (còn được gọi là chứng chỉ kỹ thuật số) đóng một vai trò quan trọng trong việc bảo mật giao tiếp giữa hai hệ thống.

Chứng chỉ SSL là một tệp dữ liệu được phát hành bởi Certificate Authority (CA) được cấp phép.

Chứng chỉ SSL xuất hiện ở bất kỳ trang Web https nào. Bất kỳ trang web https nào đều có một biểu tượng khóa an toàn trong thanh địa chỉ như hình dưới đây.



Chúng ta có thể kiểm tra chứng chỉ SSL của trang google.com bằng cách thực hiện các bước sau:

Bước 1: Nhấn vào biểu tượng ổ khóa.

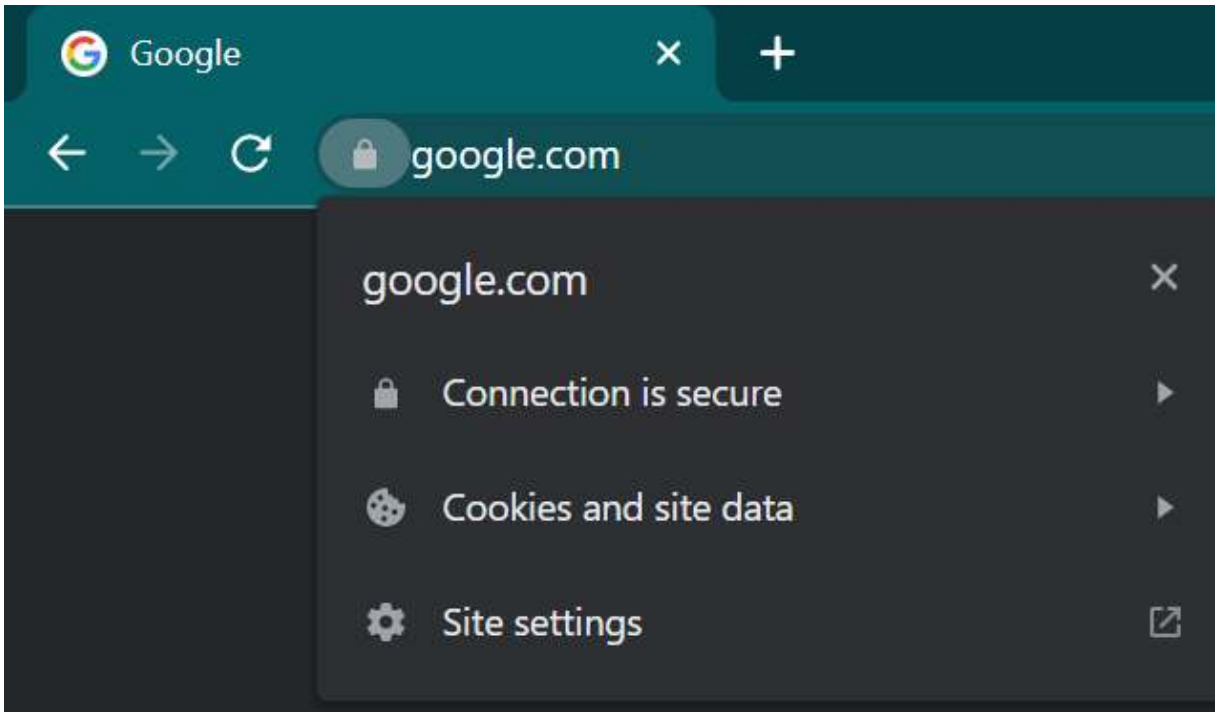
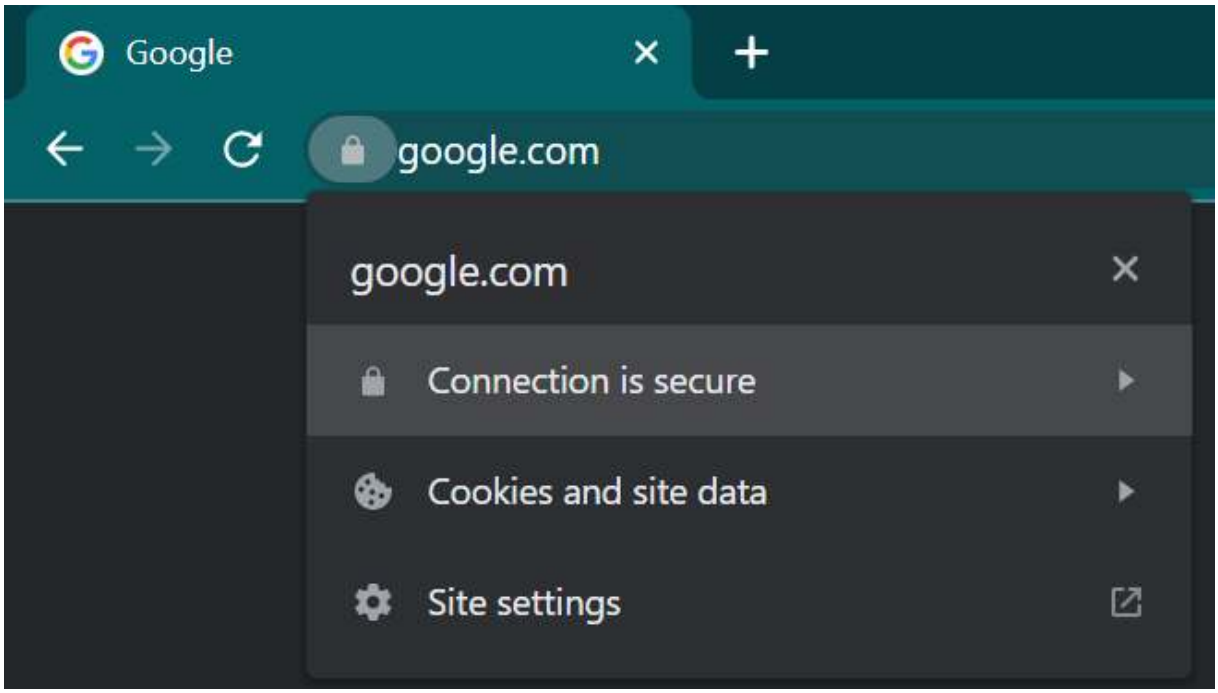
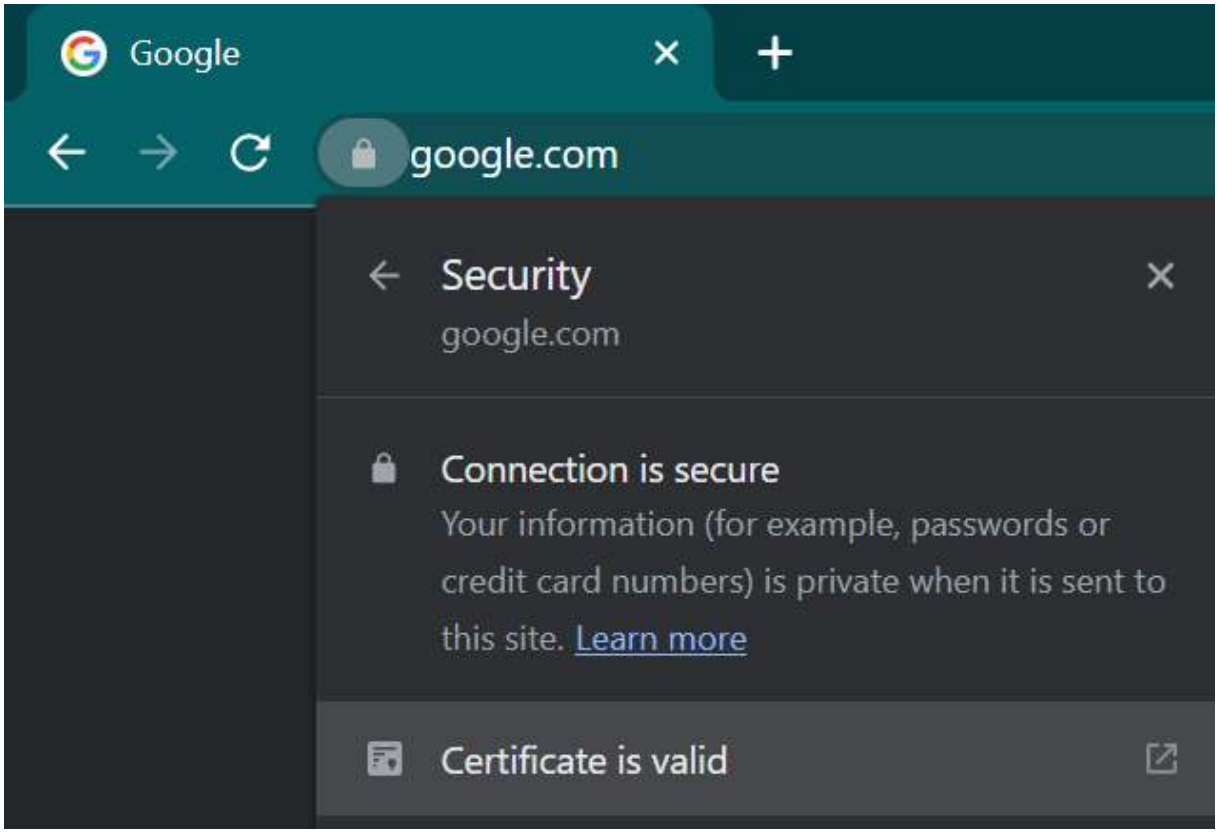


Figure 15: Kiểm tra chứng chỉ SSL

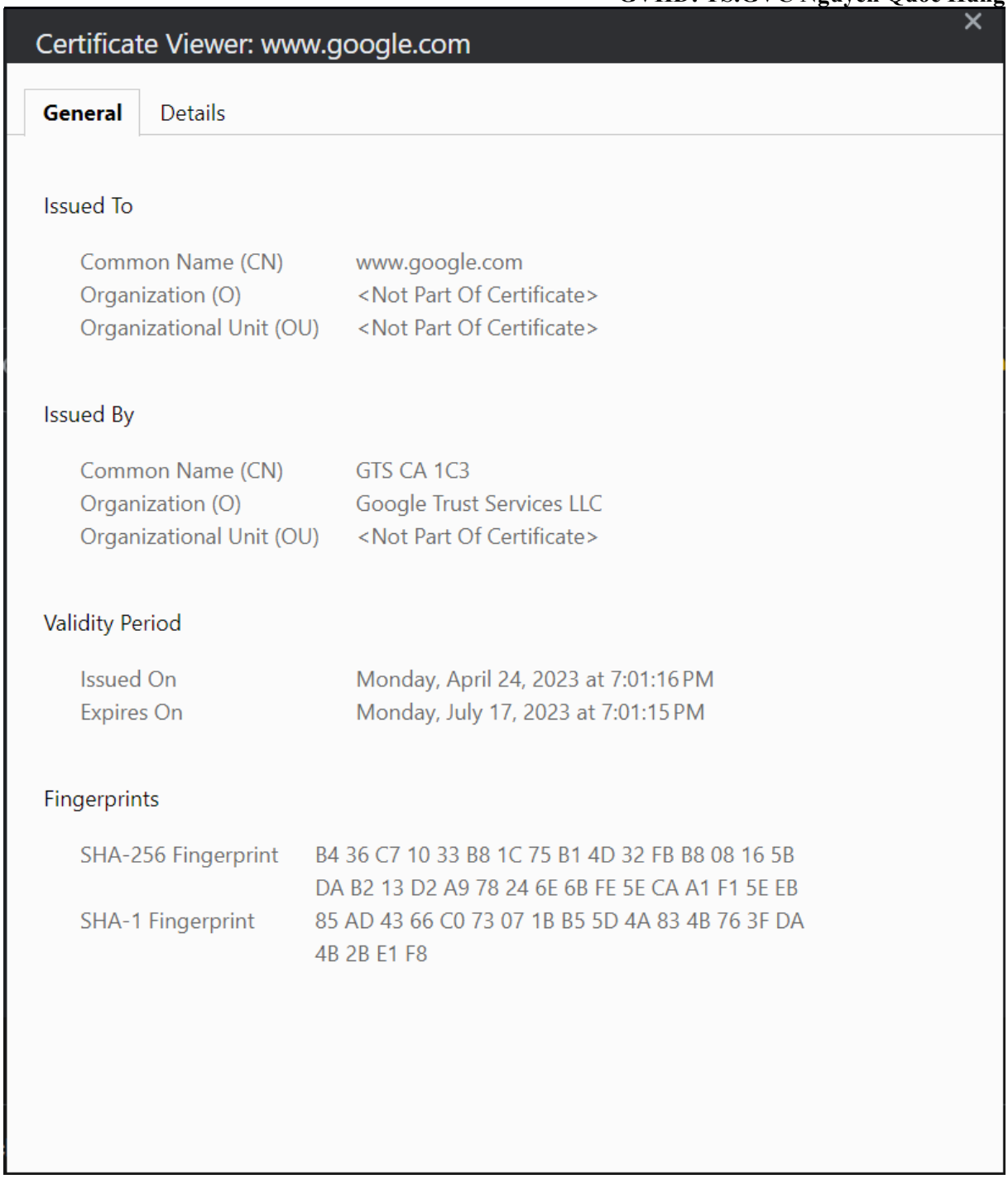
Bước 2: Chọn Connection is secure.



Bước 3: Chọn Certificate is valid.



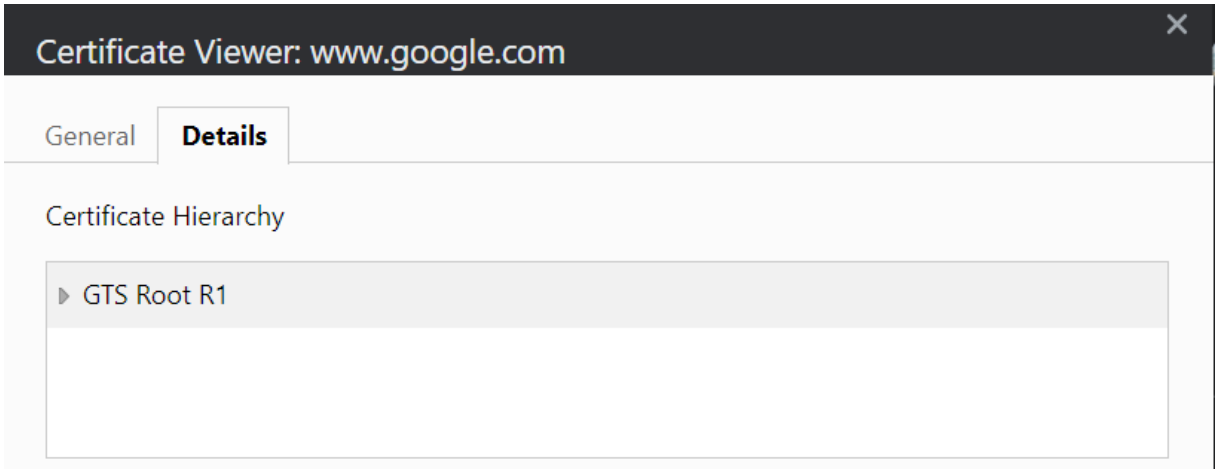
Tại đây chúng ta sẽ xem được những thông tin về chứng chỉ SLL tại web google.com.



Có thể nói chứng chỉ SSL thức chất là các chứng chỉ X.509. Bởi lẽ SSL sử dụng định dạng X.509 (X.509 là một tiêu chuẩn định nghĩa định dạng của chứng chỉ kỹ thuật số. X.509 sử dụng một ngôn ngữ chính thức được gọi là Abstract Syntax Notation One (ASN.1) để biểu diễn cấu trúc dữ liệu của chứng chỉ). Chứng chỉ SSL theo định dạng X.509 bao gồm các thông tin sau:

- Version: Số phiên bản của định dạng dữ liệu chứng chỉ theo X.509.
- Serial number: Định danh duy nhất của chứng chỉ được gán bởi CA
- Public Key: Khóa công khai của chủ sở hữu
- Subject: Tên chủ sở hữu, địa chỉ, quốc gia và tên miền
- Issuer: Tên của CA đã cấp chứng chỉ
- Valid-From: Ngày bắt đầu có hiệu lực của chứng chỉ
- Valid-To: Ngày hết hạn
- Signature Algorithm: Thuật toán được sử dụng để tạo chữ ký
- Thumbprint: Băm của chứng chỉ
- Thumbprint Algorithm: Thuật toán được sử dụng để tạo băm của chứng chỉ

Những thông số này chúng ta có thể xem ở mục Detail sau khi thực hiện bước 3 đã nhắc tới ở trên:



3.2.2 Làm thế nào để có được chứng chỉ SSL

Chúng ta có thể nhận chứng chỉ SSL từ bất kỳ Cơ quan cấp chứng chỉ (CA) được ủy quyền nào để bảo mật giao tiếp giữa hai hệ thống. Có hai cách để nhận chứng chỉ SSL:

- Mua chứng chỉ từ CA
- Nhận chứng chỉ miễn phí từ CA
- Tự tạo và tự ký chứng chỉ SSL

3.2.2.1 Một số nhà cung cấp SSL miễn phí

Dưới đây là một số nhà cung cấp SSL miễn phí phổ biến:

- Let's Encrypt: Một nhà cung cấp SSL miễn phí được phát triển bởi Internet Security Research Group (ISRG). Chứng chỉ SSL được phát hành bởi Let's Encrypt được hỗ trợ bởi hầu hết các trình duyệt hiện đại và có thời hạn 90 ngày.
- Cloudflare: Một cung cấp chứng chỉ SSL miễn phí thông qua Cloudflare Free SSL. Nhà cung cấp này cũng cung cấp các tính năng bảo mật khác như bảo vệ DDOS và tường lửa ứng dụng web.
- Comodo (tên mới là Sectigo): Một là một trong những nhà cung cấp SSL lâu đời nhất. Điểm nổi bật của Comodo là tính ổn định và độ tin cậy cao của các chứng chỉ SSL.
- SSL.com: Một nhà cung cấp chứng chỉ SSL miễn phí cho mục đích thử nghiệm và kiểm tra, bên cạnh các gói trả phí. Chứng chỉ này cũng được hỗ trợ bởi hầu hết các trình duyệt hiện đại.
- ZeroSSL: Tổ chức cung cấp chứng chỉ SSL miễn phí với tính năng tự động hóa, cho phép người dùng dễ dàng tạo và quản lý chứng chỉ SSL cho các trang web của mình.
- SSL For Free: Cho phép người dùng tạo chứng chỉ SSL miễn phí cho các tên miền của họ thông qua một quy trình đơn giản và có thể được tích hợp vào các máy chủ web của họ.
- GoGetSSL: Cung cấp các gói chứng chỉ SSL miễn phí và trả phí, với tính năng hỗ trợ đa ngôn ngữ và nhiều loại chứng chỉ khác nhau.
- FreeSSL: Một là một nhà cung cấp SSL miễn phí đơn giản và dễ sử dụng, cho phép người dùng tạo chứng chỉ SSL với một số tính năng cơ bản.
- Buypass: Cung cấp các gói chứng chỉ SSL miễn phí và trả phí, với tính năng hỗ trợ đa ngôn ngữ và tích hợp nhiều tính năng bảo mật khác nhau.
- GlobalSign FreeSSL: Cung cấp các chứng chỉ SSL miễn phí với tính năng bảo mật cao, bao gồm mã hóa 256-bit và hỗ trợ đa loại trình duyệt.

3.2.2.2 Mua chứng chỉ từ CA

Chúng ta có thể mua chứng chỉ SSL từ CA. Giá khác nhau tùy thuộc vào CA và loại chứng chỉ SSL. Sau đây là các bước tổng thể để mua chứng chỉ SSL từ CA:

- Bước 1: Chọn nhà phát hành Certificate Authority (CA): Hiện nay có nhiều CA uy tín như Comodo, DigiCert, RapidSSL, GeoTrust, thawte, Certum, v.v. Chúng

ta sẽ dựa trên ngân sách của và các tính năng cần thiết để lựa chọn sao cho phù hợp.

- Bước 2: Mua chứng chỉ: Sau khi chọn được chứng chỉ phù hợp thì tiến hành thanh toán để mua chứng chỉ. Đối với một số CA thì bước này sẽ xuất hiện sau khi gửi CSR.
- Bước 3: Tạo và gửi CSR (Certificate Signing Request) cho CA: Cần thực hiện tạo CSR từ máy chủ web và gửi nó đến CA.
- Bước 4: Tải xuống chứng chỉ SSL (sau khi xác thực thành công).

3.2.2.3 Tự tạo và tự ký chứng chỉ SSL

Tự tạo và tự ký chứng chỉ SSL: Chúng ta cũng có thể tạo và tự ký chứng chỉ SSL bằng các công cụ như OpenSSL. Tuy nhiên, chứng chỉ SSL tự ký này sẽ không được các trình duyệt hiện đại chấp nhận mặc dù nó có thể được sử dụng để mã hóa dữ liệu.

3.2.3 Các định dạng chứng chỉ SSL

Có nhiều định dạng khác nhau của chứng chỉ X.509 như PEM, DER, PKCS # 7 và PKCS # 12. Các định dạng PEM và PKCS # 7 sử dụng mã hóa Base64 ASCII trong khi DER và PKCS # 12 sử dụng mã hóa nhị phân. Các tệp chứng chỉ có các phần mở rộng khác nhau dựa trên định dạng và mã hóa mà chúng sử dụng.

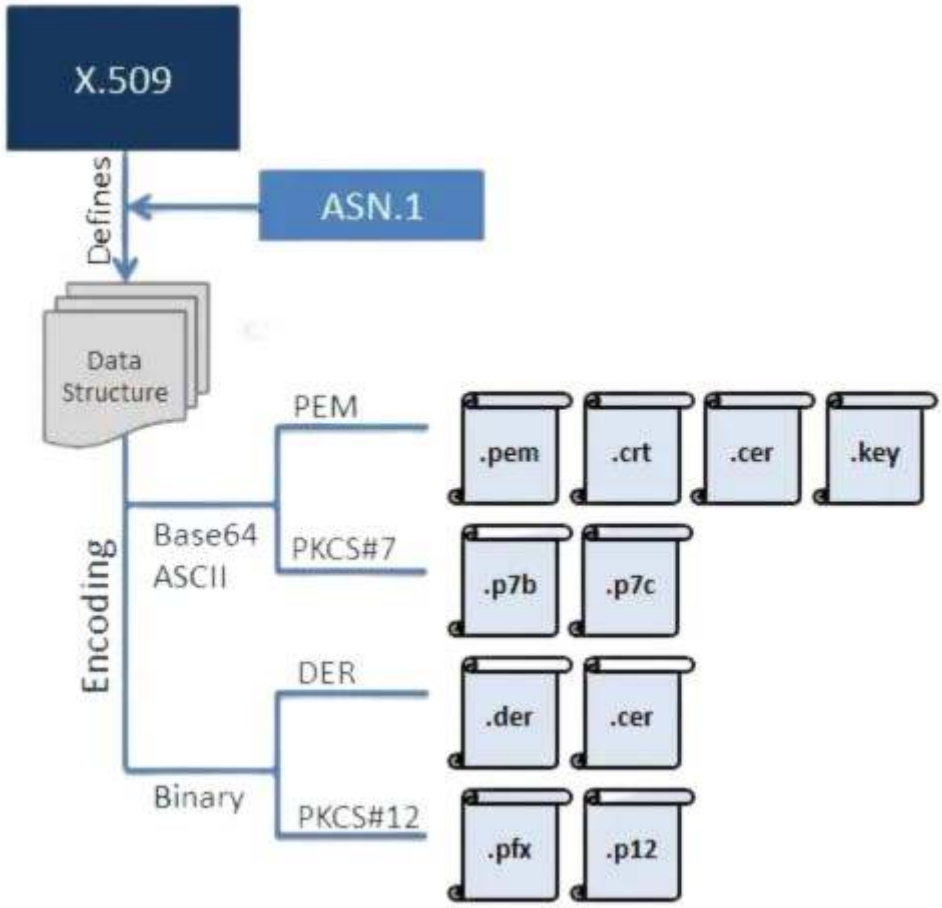


Figure 16: Phần mở rộng tệp của Chứng chỉ X.509

3.2.3.1 Định dạng PEM

Hầu hết các CA (Cơ quan cấp chứng chỉ) cung cấp chứng chỉ ở định dạng PEM trong các tệp được mã hóa Base64 ASCII. Các loại tệp chứng chỉ có thể là .pem, .crt, .cer hoặc .key. Tệp .pem có thể bao gồm chứng chỉ máy chủ, chứng chỉ trung gian và khóa riêng trong một tệp duy nhất. Chứng chỉ máy chủ và chứng chỉ trung gian cũng có thể nằm trong một tệp .crt hoặc .cer riêng biệt. Khóa riêng có thể nằm trong một tệp .key.

Các tệp PEM sử dụng mã hóa ASCII, vì vậy bạn có thể mở chúng trong bất kỳ trình soạn thảo văn bản nào như notepad, MS word, v.v. Mỗi chứng chỉ trong tệp PEM được chứa giữa các câu lệnh ---- BEGIN CERTIFICATE---- và ----END CERTIFICATE----. Khóa riêng được chứa giữa các câu lệnh ---- BEGIN RSA PRIVATE KEY----- và -----END RSA PRIVATE KEY-----. CSR được chứa giữa các câu lệnh -----BEGIN CERTIFICATE REQUEST----- và -----END CERTIFICATE REQUEST-----

3.2.3.2 Định dạng PKCS#7

Định dạng PKCS#7 là một tiêu chuẩn cú pháp tin nhắn mật mã. Chứng chỉ PKCS # 7 sử dụng mã hóa Base64 ASCII với phần mở rộng tệp .p7b hoặc .p7c. Chỉ chứng chỉ mới có thể được lưu trữ ở định dạng này, không phải khóa riêng. Chứng chỉ P7B được chứa giữa các câu lệnh "-----BEGIN PKCS7-----" và "-----END PKCS7-----".

3.2.3.3 Định dạng DER

Chứng chỉ DER ở dạng nhị phân, chứa trong các tệp .der hoặc .cer. Các chứng chỉ này chủ yếu được sử dụng trong các máy chủ web dựa trên Java.

3.2.3.4 Định dạng PKCS#12

Chứng chỉ PKCS # 12 ở dạng nhị phân, chứa trong các tệp .pfx hoặc .p12. PKCS # 12 có thể lưu trữ chứng chỉ máy chủ, chứng chỉ trung gian và khóa riêng trong một tệp .pfx duy nhất với mật khẩu bảo vệ. Các chứng chỉ này chủ yếu được sử dụng trên nền tảng Windows.

3.3 Cài đặt SSL cho Website

Để tích hợp SSL/TLS cho website, chúng ta có thể làm theo các bước sau:

- Mua/xin/tạo chứng chỉ SSL/TLS từ một nhà cung cấp dịch vụ uy tín (xem thêm 3.3.2)
- Cài đặt chứng chỉ SSL/TLS trên máy chủ web. Quá trình này tùy thuộc vào loại máy chủ đang sử dụng. Nếu như sử dụng một dịch vụ lưu trữ web, chúng ta có thể cần liên hệ với nhà cung cấp dịch vụ của bạn để biết cách cài đặt chứng chỉ SSL/TLS.
- Cập nhật mã nguồn của website để sử dụng HTTPS thay vì HTTP. Cần thay đổi tất cả các liên kết và URL trên website của bạn để sử dụng HTTPS. Nếu như sử dụng một CMS (Content Management System) như WordPress hoặc Drupal, thì có thể cài đặt một plugin để tự động chuyển đổi liên kết và URL sang HTTPS.
- Kiểm tra lại website của để đảm bảo rằng SSL/TLS được tích hợp đúng cách.

Sau khi tích hợp thành công, Website của bạn sẽ được bảo vệ bởi một kết nối an toàn và thông tin được truyền tải giữa máy khách và máy chủ sẽ được mã hóa.

Chương 4: Đánh giá hiệu quả của SSL/TLS

4.1 Lợi ích của việc tích hợp SSL/TLS

1. Đáp ứng được yêu cầu bảo mật

SSL/TLS đáp ứng các yêu cầu bảo mật được quy định bởi các tổ chức và luật pháp. Việc sử dụng SSL/TLS giúp các doanh nghiệp tránh các rủi ro pháp lý liên quan đến bảo mật và bảo vệ các thông tin nhạy cảm của khách hàng.

Mã hóa dữ liệu: SSL/TLS sử dụng mã hóa dữ liệu để bảo vệ các thông tin nhạy cảm như ID người dùng, mật khẩu và số thẻ tín dụng được truyền qua Internet. Việc sử dụng mã hóa giúp ngăn chặn các kẻ xâm nhập đánh cắp thông tin và sử dụng nó cho mục đích gian lận.

Cung cấp các chứng chỉ SSL được phát hành bởi các tổ chức có uy tín để xác nhận tính xác thực của các trang web. Nhờ đó, người dùng có thể chắc chắn rằng họ đang truy cập vào một trang web chính hãng và không bị lừa đảo.

Tăng cường độ tin cậy: SSL/TLS giúp tăng độ tin cậy của các trang web thương mại điện tử. Với sự đảm bảo về bảo mật thông tin, người dùng cảm thấy an tâm hơn khi thực hiện các giao dịch trực tuyến và đưa ra quyết định mua hàng.

2. Ngăn chặn Lừa đảo

Đôi khi, người dùng có thể nhận được email lừa đảo (Thường dưới dạng quảng cáo và xác nhận gửi hàng) đưa các liên kết đến một trang web khác. Mục đích duy nhất của các trang web này là thu thập thông tin nhạy cảm như chi tiết thẻ tín dụng. Tuy nhiên, các trang web này gần như không thể có được chứng chỉ SSL xác thực. Khi khách truy cập không nhận thấy chứng chỉ SSL, họ có thể sẽ không nhập bất kỳ thông tin bí mật nào.

3. Tăng lưu lượng truy cập và bán hàng

Chứng chỉ SSL cho phép khách truy cập trang web của bạn cảm thấy an toàn trên trang web của bạn. Nó làm cho trang web của bạn đáng tin cậy hơn và nếu bạn đang sử dụng

nó cho thương mại điện tử, khách hàng của bạn có thể nhập thông tin cá nhân của họ một cách an toàn, thực hiện thanh toán

Người dùng có thể chỉ cần cho biết trang web có SSL hay không bằng cách kiểm tra URL của trang web. Nếu nó bắt đầu bằng http:// - trang web không được bảo mật và không có SSL, tuy nhiên, nếu nó bắt đầu bằng https://, điều này cho biết rằng trang web được bảo mật và có SSL làm cho khách hàng cảm thấy an tâm hơn khi truy cập dẫn đến lưu lượng truy cập và bán hàng tăng

4. Yêu cầu phần mềm thấp

SSL không yêu cầu cài đặt phần mềm máy khách. Điều duy nhất cần thiết là kết nối Internet thông qua trình duyệt web tiêu chuẩn. Do đó, chi phí mua, bảo trì và quản lý phần mềm có thể được tiết kiệm đáng kể. Điều này có thể có lợi cho cả các tổ chức quy mô nhỏ và lớn.

5. Cải thiện SEO

Google và các công cụ tìm kiếm khác ưu tiên xếp hạng các trang web được bảo vệ bằng SSL/TLS cao hơn trong các kết quả tìm kiếm, giúp các trang web đó có được sự chú ý và tăng khả năng tiếp cận của khách hàng.

4.2 Hạn chế của bảo mật SSL/ TLS

1. Giảm hiệu suất

Khi chứng chỉ SSL được sử dụng trên một trang web, tốc độ giao dịch sẽ giảm đáng kể. Điều này xảy ra do nó yêu cầu cả hai bên tham gia giao tiếp phải cố gắng và thực hiện thêm các thao tác trao đổi handshakes cũng như mã hóa và giải mã tin nhắn, khiến loại giao tiếp này chậm hơn so với giao tiếp không có SSL.. Tuy nhiên, sự chậm lại hiệu suất này sẽ chỉ đáng chú ý đối với các trang web có số lượng người truy cập lớn.

2. Gia hạn và nâng cấp thường xuyên

Chứng chỉ SSL cần được gia hạn và nâng cấp. Nếu không được gia hạn và nâng cấp theo thời gian, sẽ có thông báo bật lên cho biết chứng chỉ SSL đã hết hạn, có nghĩa là trang web không còn an toàn nữa. Do đó, khách hàng có thể mất lòng tin khi thực hiện các giao dịch.

3. Giảm tốc độ truy cập và lưu lượng truy cập

SSL/TLS kéo dài thời gian tải trang web trên trình duyệt. Khi trình duyệt lần đầu tiên kết nối với máy chủ web được bảo mật SSL/TLS, một phiên bảo mật sẽ được bắt đầu bởi máy khách và máy chủ web. Quá trình sơ bộ này bao gồm một thủ tục bắt tay qua lại phức tạp mà cuối cùng sẽ dẫn đến một kết nối an toàn. Khi kết nối được thiết lập, cả máy khách và máy chủ web đều phải mã hóa và giải mã thông tin trước khi có thể đọc được ở một trong hai đầu của giao tiếp.

4. Vấn đề đối với Plugins

Nếu trang web của bạn phụ thuộc vào nhiều plugin, bạn có thể gặp sự cố nếu áp dụng SSL/TLS trên toàn bộ trang web của mình. Nhiều phiên bản plugin cũ hơn không được xây dựng với tính năng chuyển đổi HTTPS.

5. Các biến chứng của giao thức

Nếu chứng chỉ SSL không được triển khai đúng cách, các tệp sẽ được phân phát qua HTTPS sẽ được phân phát qua HTTP. Do đó, sẽ không có một thông báo cảnh báo hiển thị cho khách truy cập nói rằng dữ liệu của họ được bảo vệ.

6. Lỗ hổng trong bảo mật

Về cơ bản, SSL/TLS được kế thừa từ thuật toán ký và mã hóa. Nếu các thuật toán này có điểm yếu, thì SSL/TLS cũng sẽ bị tấn công. Hơn nữa, còn do phiên làm việc quá lâu trong quá trình bắt tay, khóa phiên được tạo giữa client và server trong suốt quá trình kết nối. Khi khóa này còn tồn tại, mỗi khi thông điệp được gửi, tồn tại một lỗ hổng bảo mật trong khi kết nối dễ bị xâm nhập. Vì vậy, trang web sẽ bị tấn công một cách dễ dàng nếu không cập nhật các phiên bản SSL/TLS một cách thường xuyên.

Chương 5: Đề xuất phương pháp cải tiến

TLS 1.3 được thiết kế để cải thiện tính bảo mật và hiệu suất so với các phiên bản trước đó, bao gồm TLS 1.2. Có một số lý do chính để TLS 1.3 hạn chế được các cuộc tấn công hơn so với TLS 1.2:

- Loại bỏ các thuật toán khóa yếu: TLS 1.3 loại bỏ các thuật toán bảo mật khóa cũ và yếu như RC4, MD5 và SHA-1. Các thuật toán này đã bị khai thác thành công trong quá khứ và không còn được coi là an toàn.
- Sử dụng các thuật toán bảo mật mới: TLS 1.3 sử dụng các thuật toán bảo mật mới hơn, bao gồm các thuật toán băm SHA-256 và SHA-384, thuật toán mã hóa AES-GCM và các thuật toán khóa công khai mới như Curve25519 và Ed25519.
- Loại bỏ các giao thức bảo mật yếu: TLS 1.3 loại bỏ các giao thức bảo mật cũ và yếu như RSA key exchange và static Diffie-Hellman key exchange. Thay vào đó, nó sử dụng các giao thức mới và cải tiến như Elliptic Curve Diffie-Hellman (ECDHE) key exchange, kết hợp với các thuật toán khóa công khai mới để đảm bảo tính riêng tư và bảo mật.
- Cải thiện cơ chế xác thực: TLS 1.3 cung cấp một cơ chế xác thực tốt hơn so với phiên bản trước đó, bao gồm một cơ chế xác thực riêng tư và khóa công khai mới. Các chứng chỉ số được mã hóa bằng thuật toán Elliptic Curve Digital Signature Algorithm (ECDSA) hoặc RSA-PSS để đảm bảo tính toàn vẹn của chúng.
- Tăng tốc độ kết nối: TLS 1.3 sử dụng các cơ chế mới để tăng tốc độ kết nối, bao gồm sử dụng các giao thức mới như 0-RTT, cho phép các kết nối được thiết lập nhanh hơn. Điều này giúp giảm thiểu thời gian đợi và tăng tốc độ tải trang web.

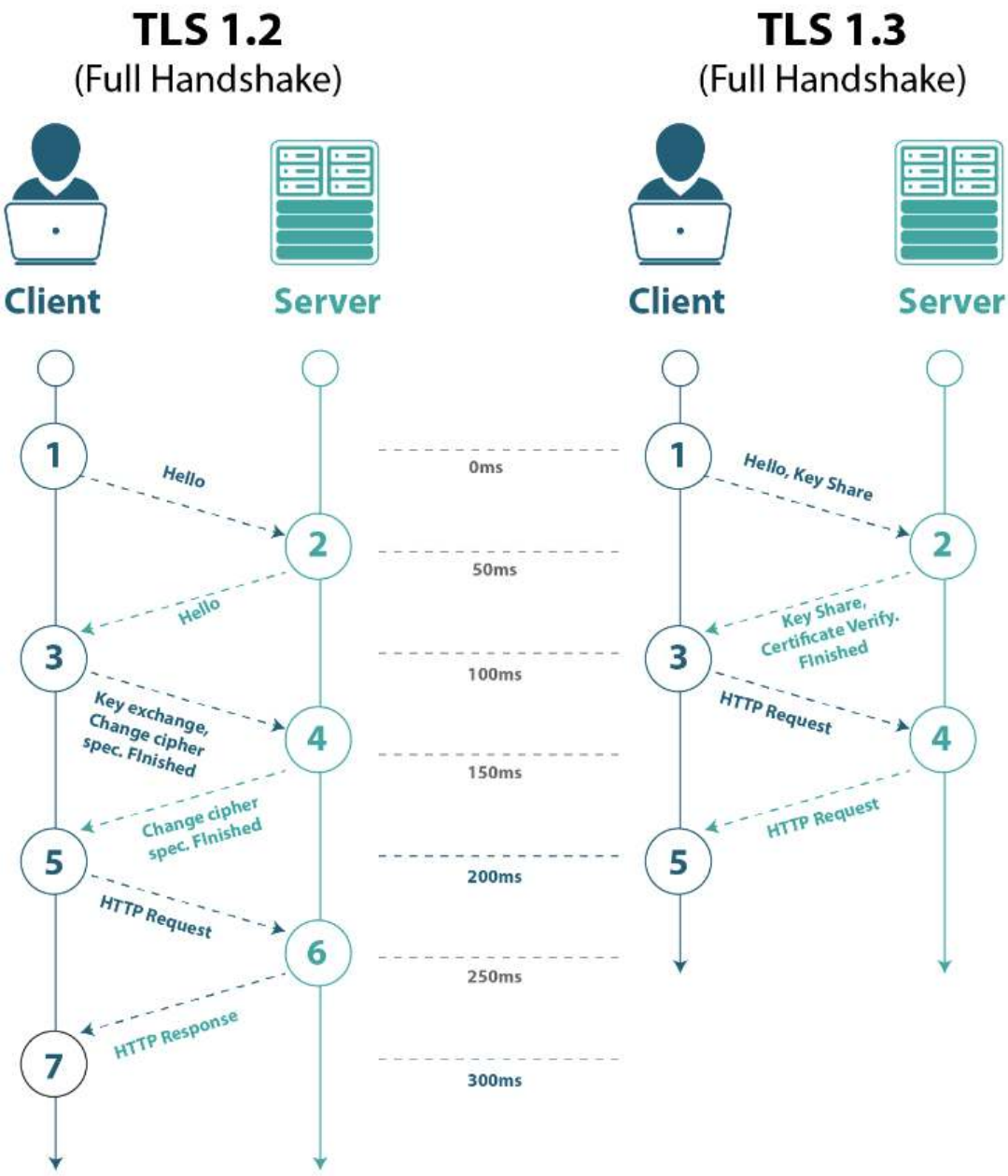


Figure 17: So sánh tốc độ làm việc giữa hai phiên bản TLS 1.2 và 1.3

Về mặt bảo mật, TLS 1.3 loại bỏ hoàn toàn khả năng tương thích ngược và có một thiết kế bảo mật chức năng hoàn toàn mới.

Mặc dù TLS 1.3 được thiết kế để cải thiện tính bảo mật và giảm thiểu các cuộc tấn công so với các phiên bản trước đó, nhưng nó vẫn có thể bị tấn công. Dưới đây là một số cuộc tấn công có thể xảy ra trên TLS 1.3:

- Tấn công bắt gói tin (Packet Capture Attack): Kẻ tấn công có thể bắt và giải mã các gói tin để truy cập thông tin nhạy cảm được truyền tải qua kết nối TLS 1.3. Tuy nhiên, TLS 1.3 sử dụng mã hóa cường độ để giảm thiểu nguy cơ này.

- Tấn công giả mạo máy chủ (Server Impersonation Attack): Kẻ tấn công có thể giả mạo máy chủ và yêu cầu người dùng kết nối đến máy chủ giả mạo thay vì máy chủ đích thực. Tuy nhiên, TLS 1.3 sử dụng một số kỹ thuật để đối phó với tấn công này, như "Server Certificate Verificaton" và "Encrypted Server Name Indication" (ESNI).

- Tấn công đầu cuối (Man-in-the-Middle Attack): Một kẻ tấn công có thể giả mạo máy chủ và yêu cầu người dùng kết nối đến máy chủ giả mạo thay vì máy chủ đích thực. TLS 1.3 cũng sử dụng một số kỹ thuật để đối phó với tấn công này, như "Zero round-trip time resumption" (0-RTT) và "ephemeral key exchange".

- Tấn công giả mạo chứng chỉ (Certificate Forgery Attack): Kẻ tấn công có thể tạo ra các chứng chỉ SSL/TLS giả mạo để giả mạo máy chủ. TLS 1.3 sử dụng "Certificate Transparency" và "Encrypted Server Name Indication" (ESNI) để giảm thiểu nguy cơ này.

Tuy nhiên, các cuộc tấn công này đều rất khó để thực hiện và yêu cầu các kỹ năng và công cụ tấn công chuyên nghiệp.

Dưới đây chúng tôi đề xuất một số cách cụ thể để cải tiến TLS 1.3 và ngăn chặn các cuộc tấn công gồm:

- Sử dụng các thuật toán mã hóa mạnh hơn:

TLS 1.3 sử dụng các thuật toán mã hóa mạnh hơn như AES-GCM và ChaCha20-Poly1305 để đảm bảo tính bảo mật cao hơn cho dữ liệu được truyền qua mạng. Ngoài ra, bạn cũng nên sử dụng các thuật toán mã hóa khác như RSA hoặc ECDSA để xác thực chữ ký số và tránh các cuộc tấn công như MITM.

- Sử dụng chứng chỉ SSL/TLS có độ dài an toàn:

Chứng chỉ SSL/TLS được sử dụng để xác thực máy chủ và tạo khóa phiên. Bạn nên sử dụng chứng chỉ có độ dài an toàn tối thiểu là 2048 bit để ngăn chặn các cuộc tấn công brute force.

- Sử dụng cơ chế kiểm soát truy cập:

Các cơ chế kiểm soát truy cập như phân quyền và giới hạn truy cập có thể giúp ngăn chặn các cuộc tấn công từ các tài khoản không được phép truy cập vào thông tin nhạy cảm. Bạn nên sử dụng các cơ chế này để tăng tính bảo mật cho hệ thống.

- Sử dụng HSTS:

HSTS là một cơ chế bảo mật HTTP được sử dụng để đảm bảo rằng trang web chỉ được truy cập qua HTTPS và không được truy cập qua HTTP. Bạn nên sử dụng HSTS để giảm thiểu nguy cơ bị tấn công man-in-the-middle.

- Sử dụng mã hóa end-to-end:

Mã hóa end-to-end giúp bảo vệ dữ liệu trên toàn bộ đường truyền từ nguồn đến đích. Bạn nên sử dụng các giải pháp mã hóa end-to-end để đảm bảo tính bảo mật cao hơn cho dữ liệu được truyền qua mạng.

- Sử dụng các cơ chế bảo vệ bổ sung:

Ngoài những giải pháp bảo mật trên, bạn nên sử dụng các cơ chế bảo vệ bổ sung như tường lửa, phát hiện xâm nhập và quản lý sự kiện để giảm thiểu nguy cơ bị tấn công từ bên ngoài.

Tuy nhiên, để đảm bảo tính bảo mật cao nhất cho hệ thống, nên theo dõi các thông tin bảo mật mới nhất và cập nhật hệ thống của mình để đảm bảo tính bảo mật liên tục.

Chương 6: Kết luận và đề xuất hướng phát triển

6.1 Kết luận

Tình hình thương mại điện tử ngày nay đang phát triển mạnh mẽ trên toàn cầu. Sự phổ biến của internet và công nghệ di động đã tạo điều kiện thuận lợi cho sự phát triển của thương mại điện tử. Người tiêu dùng ngày càng quen thuộc với việc mua sắm trực tuyến và các nền tảng thương mại điện tử như Shopee, Lazada, Tiki,Amazon, Alibaba, eBay, v.v. đã trở thành các công ty dẫn đầu trong bảo mật Thương mại điện tử. Các doanh nghiệp nhỏ và vừa cũng đang chuyển dịch sang thương mại điện tử để tận dụng cơ hội bán hàng trực tuyến và tiếp cận khách hàng mới.
Tuy nhiên, sự phát triển của thương mại điện tử cũng đặt ra nhiều thách thức về bảo mật thông tin và bảo vệ quyền riêng tư của người dùng. Các vụ vi phạm dữ liệu và tấn công mạng liên tục xảy ra, gây thiệt hại về kinh tế và uy tín cho các doanh nghiệp và cả người dùng. Do đó, bảo mật thông tin và bảo vệ quyền riêng tư là những vấn đề cấp bách đối với thương mại điện tử, và việc áp dụng các giải pháp bảo mật như SSL/TLS đóng vai trò quan trọng trong việc giảm thiểu các rủi ro liên quan đến bảo mật.

SSL/TLS là một công nghệ bảo mật quan trọng trong thương mại điện tử, giúp bảo vệ thông tin nhạy cảm của khách hàng và tăng cường sự tin cậy của doanh nghiệp trong các giao dịch trực tuyến. Tích hợp SSL/TLS cho website chính là bức tường bảo vệ hoàn hảo mọi thế lực xấu tấn công. Đồng thời giúp cho uy tín của website được nâng lên cao hơn, tạo sự tin tưởng đến khách hàng. Giúp doanh nghiệp cạnh tranh công bằng với mọi đối thủ trên thị trường kinh doanh. Tuy nhiên, SSL/TLS cũng gặp một số thách thức như việc cải tiến mã hóa, bị tấn công, giảm hiệu suất thời gian tải mạng. Để giải quyết những thách thức này, các nhà cung cấp SSL/TLS và các tổ chức bảo mật đang nghiên cứu và phát triển các giải pháp bảo mật mới nhằm cải thiện tính bảo mật và hiệu suất của SSL/TLS.

Bài nghiên cứu đã chỉ ra được các vấn đề cần phân tích của bảo mật SSL/ TLS trong bảo mật Thương mại điện tử. Chủ đề đã cung cấp một lượng kiến thức cho người đọc hiểu biết thêm về bảo mật SSL/ TLS. Tuy có rất nhiều nguồn để tham khảo nhưng trong quá trình nghiên cứu, kiến thức còn hạn hẹp dẫn đến bài nghiên cứu vẫn còn những thiếu sót đáng kể.

6.2 Hướng phát triển đề tài

Dựa vào những nhược điểm của SSL/ TLS và phần kết luận, nhóm đề xuất hướng nghiên cứu trong tương lai, mở rộng phạm vi nghiên cứu bằng một chủ đề mới chẳng hạn "Phát triển một giải pháp bảo mật mới cho SSL/TLS dựa trên công nghệ blockchain". Nghiên cứu sẽ tập trung vào việc phát triển một hệ thống phân tán để lưu trữ và quản lý các chứng chỉ SSL/TLS, sử dụng công nghệ blockchain để đảm bảo tính bảo mật và độ tin cậy. Nghiên cứu cũng sẽ xây dựng một ứng dụng mẫu để minh họa tính khả thi và hiệu quả của giải pháp. Ngoài ra, có thể tìm hiểu và phân tích sâu hơn về ứng dụng của SSL/ TLS trong một số lĩnh vực khác như ngân hàng. Ngân hàng thường xuyên giao tiếp với khách hàng thông qua các kênh trực tuyến, bao gồm các trang web, ứng dụng di động, và email. Các thông tin nhạy cảm như thông tin tài khoản, mật khẩu, và số thẻ tín dụng của khách hàng được gửi qua các kết nối mạng này, do đó đòi hỏi một mức độ bảo mật cao. Cho nên đây cũng là một chủ đề có thể phân tích và đi sâu vào nghiên cứu.

Hơn nữa, nhóm cũng đề xuất cải tiến, phát triển SSL/ TLS sử dụng các giải mã tiên tiến hơn để đảm bảo tính bảo mật của các kết nối. Ngoài ra, các nhà kinh doanh Thương mại điện tử nên tìm hiểu kiến thức về SSL/ TLS để bảo vệ trang web cũng như tạo điều kiện cho việc kinh doanh trên nền tảng Thương mại điện tử cách tốt hơn.

Cuối cùng, chính phủ và các tổ chức nên thúc đẩy mạnh mẽ nâng cao nhận thức về bảo mật, cung cấp thông tin chi tiết về các rủi ro bảo mật và các biện pháp bảo mật như SSL/TLS đến người dùng, giúp họ hiểu rõ hơn về tính bảo mật của các hoạt động trực tuyến và họ có thể tự bảo vệ mình. Bên cạnh đó, có thể đầu tư vào nghiên cứu và phát triển các công nghệ bảo mật mới và nâng cấp SSL/TLS để đáp ứng nhu cầu ngày càng cao về tính bảo mật.

TÀI LIỆU THAM KHẢO

AWS. (không ngày tháng). Được truy lục từ Chứng chỉ SSL/TLS là gì?: https://aws.amazon.com/vi/what-is/ssl-certificate/

Digicert. (không ngày tháng). Được truy lục từ What is SSL, TLS and HTTPS?: https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https

G., H. (2022, 8 17). *HOSTINGER*. Được truy lục từ HTTPS và TLS/SSL là gì? Giải thích về tầm quan trọng của một website an toàn: https://www.hostinger.vn/huong-dan/https-tls-ssl-la-gi

ORALE. (không ngày tháng). *Siebel Security Guide*. Được truy lục từ Siebel CRM Siebel Security Guide, Siebel Innovation Pack 2017, Rev. A: https://docplayer.net/85585179-Siebel-crm-siebel-security-guide-siebel-innovation-pack-2017-rev-a-e.html

SECURITY, W. (2022, 05 24). *InfoSec Insights*. Được truy lục từ What Is an SSL/TLS Cipher Suite?: https://sectigostore.com/blog/what-is-an-ssl-tls-cipher-suite/

SSL Support Team. (2014, 9 5). *SSL.com*. Được truy lục từ Pros And Cons Of SSL / HTTPS / TLS: https://www.ssl.com/article/pros-and-cons-of-ssl-https-tls/

Thọ, C. t. (2018, 4 23). Được truy lục từ Sự phát triển của giao thức bảo mật TLS/SSL: https://phutho.gov.vn/vi/su-phat-trien-cua-giao-thuc-bao-mat-tlsssl

tin, A. t. (2022, 7 19). Được truy lục từ Giải pháp an toàn thông tin cho nhà cung cấp dịch vụ ví điện tử: https://m.antoanthongtin.vn/giai-phap-khac/giai-phap-an-toan-thong-tin-cho-nha-cung-cap-dich-vu-vi-dien-tu-108165

Wikipedia. (không ngày tháng). *Wikipedia*. Được truy lục từ Transport Layer Security: https://en.wikipedia.org/wiki/Transport_Layer_Security

Hết