TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
VÀ TRUYỀN THÔNG  
BỘ MÔN AN TOÀN HỆ THỐNG THÔNG TIN

-----🙞🙜🕮🙞🙜-----

****

**Báo cáo**

**Giao thức bảo mật SSL, TLS và HTTPS trong ứng dụng thực tế, xu thế và đánh giá**

**Giảng viên:** Nguyễn Anh Chuyên

**Sinh Viên:** Vũ Thanh Bình

Nguyễn Bá Đạt

Hoàng Văn Giới

**Lớp:** An toàn thông tin K13A

Thái nguyên, 9/2016

Mục Lục

[**I. Giao thức bảo mật SSL** 3](#_Toc462325110)

[**1. SSL là gì?** 3](#_Toc462325111)

[**2. Ứng dụng của SSL với một số dịch vụ:** 6](#_Toc462325112)

[**3. Đánh giá** 9](#_Toc462325113)

[**II. Giao thức bảo mật TLS** 11](#_Toc462325114)

[**1. TLS là gì?** 11](#_Toc462325115)

[**2. Lịch sử TLS** 11](#_Toc462325116)

[**3. Vùng hoạt động của TLS** 13](#_Toc462325117)

[**4. Các thành phần của TLS** 15](#_Toc462325118)

[**5. Đánh giá TLS** 15](#_Toc462325119)

[**6. Ứng dụng của TLS** 17](#_Toc462325120)

[**III.** **Giao thức bảo mật** 18](#_Toc462325121)

[**1.** **HTTPS là gì, vì sao lại dùng HTTPS?** 18](#_Toc462325122)

[**2.** **Vấn đề với HTTP** 19](#_Toc462325123)

[**3.** **HTTPS giải quyết vấn đề như thế nào** 19](#_Toc462325124)

[**4.** **Khi nào thì bạn đang kết nối qua HTTPS?** 20](#_Toc462325125)

[**5.** **Vì sao người dùng Internet cần phải hiểu rõ HTTPS?** 22](#_Toc462325126)

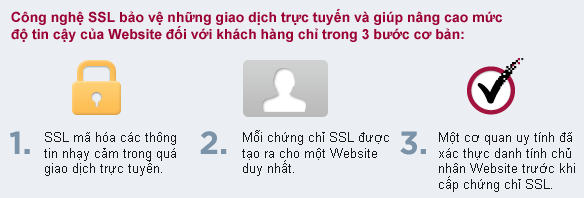
[PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC HTTPS 24](#_Toc462325127)

**I. Giao thức bảo mật SSL**

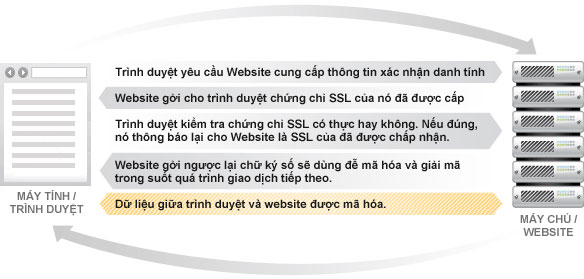
**1. SSL là gì?**

SSL là viết tắt của từ Secure Sockets Layer. Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết giữa máy chủ web và trình duyệt. Liên kết này đảm bảo tất cả dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn.

SSL đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời. SSL là một chuẩn công nghệ được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến với khách hàng của họ.  
***a. SSL làm việc như thế nào?***



***b. Những gì xảy ra khi một máy tính kết nối với một Website đã được chứng thực ?***



***c. Trình duyệt làm thế nào để kiểm tra một SSL là có thực hay không ?***

Khi Website gửi cho trình duyệt một chứng chỉ SSL, trình duyệt sẽ gửi chứng chỉ này đến một máy chủ lưu trữ các chứng chỉ số đã được phê duyệt.

Về mặt kỹ thuật, SSL sử dụng mã hóa công khai. Kỹ thuật này giúp cho Website và trình duyệt tự thỏa thuận (bước 4 ở hình trên) một bộ khóa sẽ dùng trong suốt quá trình trao đổi thông tin sau đó. Bộ khóa sẽ thay đổi theo mỗi trong lần giao dịch kế tiếp, một người khác sẽ không thể giải mã ngay cả khi có được dữ liệu của máy chủ lưu trữ chứng chỉ số nói trên.

**Giao thức SSL là gì?**

SSL được phát triển bởi Netscape, ngày nay giao thức SSL đã được sử dụng rộng rãi trên World Wide Web trong việc xác thực và mã hoá thông tin giữa client và server. Tổ chức IETF (Internet Engineering Task Force ) đã chuẩn hoá SSL và đặt lại tên là TLS (Transport Layer Security). Mặc dù là có sự thay đổi về tên nhưng TSL chỉ là một phiên bản mới của SSL. Phiên bản TSL 1.0 tương đương với phiên bản SSL 3.1. Tuy nhiên SSL là thuật ngữ được sử dụng rộng rãi hơn.

SSL được thiết kế như là một giao thức riêng cho vấn đề bảo mật có thể hỗ trợ cho 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, IMAP và FTP.

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).

Giao thức SSL bao gồm 2 giao thức con:

– Giao thức SSL record: xác định các định dạng dùng để truyền dữ liệu

– Giao thức SSL handshake (gọi là giao thức bắt tay) : sử dụng SSL record protocol để trao đổi một số thông tin giữa server và client vào lấn đầu tiên thiết lập kết nối SSL

**Các thuật toán dùng trong SSL**

Các thuật toán mã hoá và xác thực của SSL được sử dụng bao gồm:

– DES (Data Encryption Standard) là một thuật toán mã hoá có chiều dài khoá là 56 bit.  
– 3-DES (Triple-DES): là thuật toán mã hoá có độ dài khoá gấp 3 lần độ dài khoá trong mã hoá DES

– DSA (Digital Signature Algorithm): là một phần trong chuẩn về xác thực số đang được được chính phủ Mỹ sử dụng.

– KEA (Key Exchange Algorithm) là một thuật toán trao đổi khoá đang được chính phủ Mỹ sử dụng.

– MD5 (Message Digest algorithm) được phát thiển bởi Rivest.

– RSA: là thuật toán mã hoá công khai dùng cho cả quá trình xác thực và mã hoá dữ liệu được Rivest, Shamir, and Adleman phát triển.

– RSA key exchange: là thuật toán trao đổi khoá dùng trong SSL dựa trên thuật toán RSA.  
– RC2 and RC4: là các thuật toán mã hoá 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.

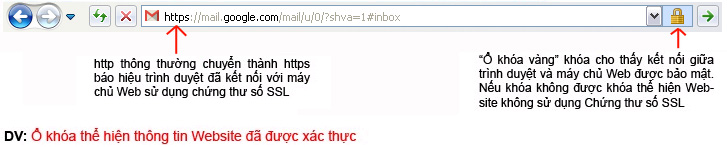
Khi một client và server trao đổi thông tin trong giai đoạn bắt tay (handshake), họ sẽ xác định bộ mã hoá mạnh nhất có thể và sử dụng chúng trong phiên giao dịch SSL.

**2. Ứng dụng của SSL với một số dịch vụ:**

|  |  |  |
| --- | --- | --- |
| Dịch vụ | Port | Mô tả dịch vụ |
| Nsiiop | 261 | IIOP trên SSL/TLS |
| https | 443 | HTTP trên SSL/TLS |
| Smtps | 465 | SMTP trên SSL/TLS |
| Nntps | 563 | NNTP trên SSL/TLS |
| Ldaps | 636 | LDAP trên SSL/TLS |
| Ftps-data | 989 | FTP-data trên SSL/TLS |
| Ftps | 990 | FTP trên SSL/TLS |
| Telnets | 992 | Telnet trên SSL/TLS |
| Imaps | 994 | Imap trên SSL/TLS |
| Pop3s | 995 | Pop3 trên SSL/TLS |

**a. DV-SSL:**

Domain Validation (DV): chứng thư số SSL chứng thực cho Domain Name - Website . Khi 1 Website sử dụng DV SSL thì sẽ được xác thực tên domain , website đã được mã hoá an toàn khi trao đổi dữ liệu



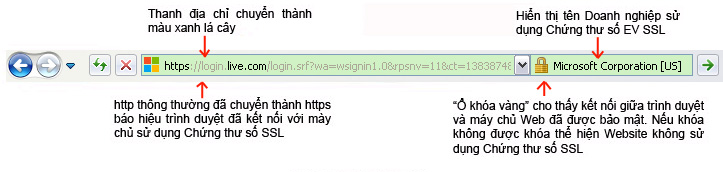
**b. OV-SSL:**

Organization Validation (OV): chứng thư số SSL chứng thực cho Website và xác thực doanh nghiệp đang sở hữu website đó.

**c. EV-SSL:**

Extended Validation (EV): cho khách hàng của bạn thấy Website đang sử dụng chứng thư SSL có độ bảo mật cao nhất và được rà soát pháp lý kỹ càng.

Với thanh đại chỉ sang màu xanh với hiển thị đầy đủ thông tin của công ty, cung cấp một cấp độ cao hơn tin tưởng vào website của bạn.



**d. Wildcard SSL:**

(Wildcard SSL Certificate): sản phẩm lý tưởng dành cho các cổng thương mại điện tử. Các website dạng này thường có thể tạo ra các trang e-store dành cho các chủ cửa hàng trực tuyến, mỗi e-store là một sub domains và được chia sẻ trên một địa chỉ IP duy nhất. Khi đó, để triển khai giải pháp bảo bảo mật giao dịch trực tuyến (khi đặt hàng, thanh toán, đăng ký & đăng nhập tài khoản,...) bằng SSL, chúng ta có thể dùng duy nhất một chứng chỉ số Wildcard cho tên miền chính của website và dùng chung một địa chỉ IP duy nhất để chia sẻ cho tất cả mọi sub domains.

SSL được phát triển cho phép trao đổi riêng tư trên mạng Internet, cho phép các ứng dụng khách/chủ giao tiếp an toàn, ngăn ngừa tấn công, bóc tách dữ liệu hay phá hủy thông điệp trái phép như an toàn truyền siêu văn bản, an toàn trao đổi thư điện tử… Trong [*Thông tư số 01/2011/TT-BTTTT*](http://mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/DispForm.aspx?ID=7734) ngày 04/01/2011 của Bộ trưởng Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định **Bắt buộc áp dụng** tiêu chuẩn SSL phiên bản 3.0 và được xếp vào nhóm **Tiêu chuẩn về an toàn thông tin**.

**3. Đánh giá**

**a. Tại sao nên sử dụng SSL?**

Bạn đăng ký domain để sử dụng các dịch vụ website, email v.v... -> luôn có những lỗ hổng bảo mật -> hacker tấn công -> SSL bảo vệ website và khách hàng của bạn.

Bảo mật dữ liệu: dữ liệu được mã hóa và chỉ người nhận đích thực mới có thể giải mã.

Toàn vẹn dữ liệu: dữ liệu không bị thay đổi bởi tin tặc.

Chống chối bỏ: đối tượng thực hiện gửi dữ liệu không thể phủ nhận dữ liệu của mình.

**b. Lợi ích khi sử dụng SSL?**

Bạn đăng ký domain để sử dụng các dịch vụ website, email v.v… -> luôn có những lỗ hổng bảo mật -> hacker tấn công -> SSL bảo vệ website và khách hàng của bạn.

Bảo mật và mã hóa các thông điệp trao đổi giữa trình duyệt và server.

Bảo mật các giao dịch giữa khách hàng và doanh nghiệp, các dịch vụ truy nhập hệ thống.

Bảo mật webmail và các ứng dụng như Outlook Web Acess, Exchange, và Office Communication Server.

Bảo mật các ứng dụng ảo hóa như Citrix Delivery Platform hoặc các ứng dụng điện toán mây.

Bảo mật dịch vụ FTP.

Bảo mật truy cập Control panel.

Bảo mật các dịch vụ truyền dữ liệu trong mạng nội bộ, file sharing, extranet.

Bảo mật VPN Access Servers, Citrix Access Gateway.

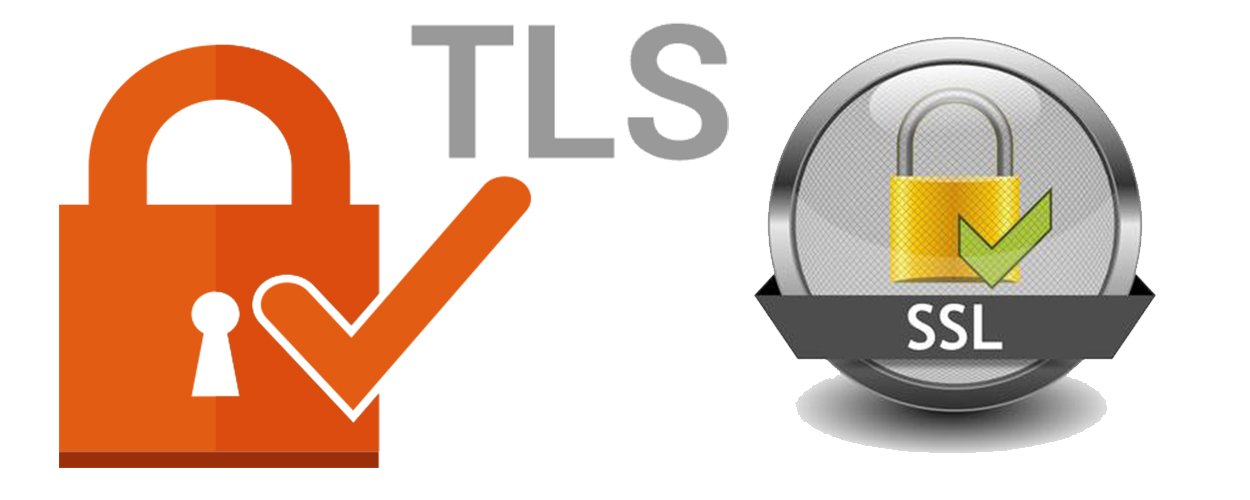
Nâng cao hình ảnh, thương hiệu và uy tín doanh nghiệp.

Tạo lợi thế cạnh tranh, tăng niềm tin của khách hàng đối với website, tăng số lượng giao dịch, giá trị giao dịch trực tuyến của khách hàng. Website không được xác thực và bảo mật sẽ luôn ẩn chứa nguy cơ bị xâm nhập dữ liệu, dẫn đến hậu quả khách hàng không tin tưởng sử dụng dịch vụ.

**II. Giao thức bảo mật TLS**

**1. TLS là gì?**

- TLS (Transport Layer Security: "Bảo mật tầng truyền tải") là giao thức mật mã nhằm mục đích bảo mật sự vận chuyển trên Internet.



- Giao thức này mật mã hóa khóa bất đối xứng bằng các chứng thực X.509 để xác thực bên kia và để trao đổi một khóa đối xứng. Sau đó, khóa phiên được dùng để mã hóa các dữ liệu được truyền qua lại hai bên. Phương pháp này cho phép bảo mật dữ liệu hoặc thông điệp và xác thực tính toàn vẹn của các thông điệp qua các mã xác thực thông điệp (message authentication code). Một chính sách quan trọng, bí mật chuyển tiếp (forward secrecy),làm cho không thể tính ra khóa phiên ngắn hạn từ khóa bí mật bất đối xứng dài hạn.

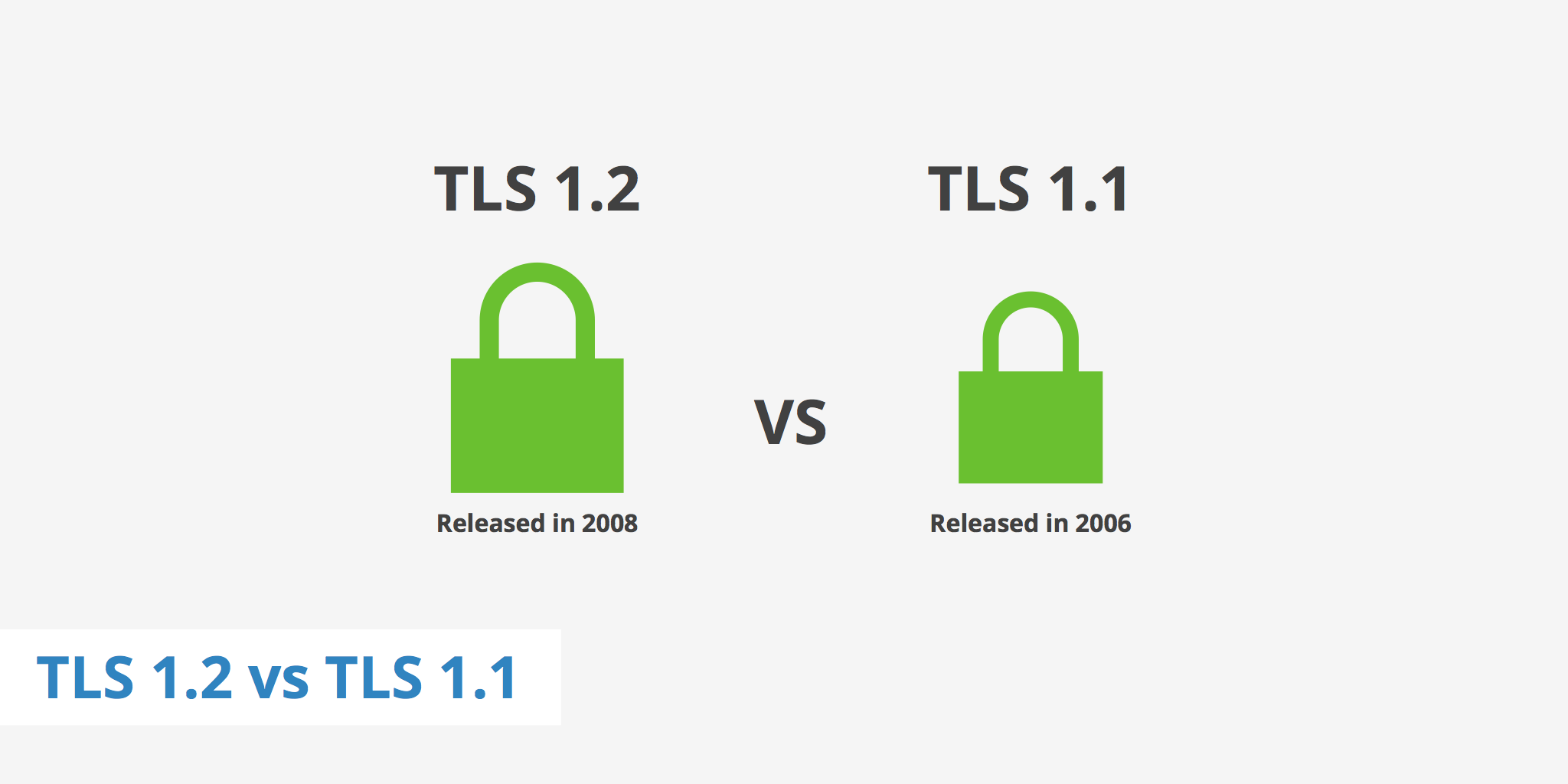
- Do sử dụng các chứng thực X.509, giao thức này cần các nhà cung cấp chứng thực số và hạ tầng khóa công khai để xác nhận mối quan hệ giữa một chứng thực và chủ của nó, cũng như để tạo, ký, và quản lý sự hiện lực của các chứng thực.

2. Lịch sử TLS

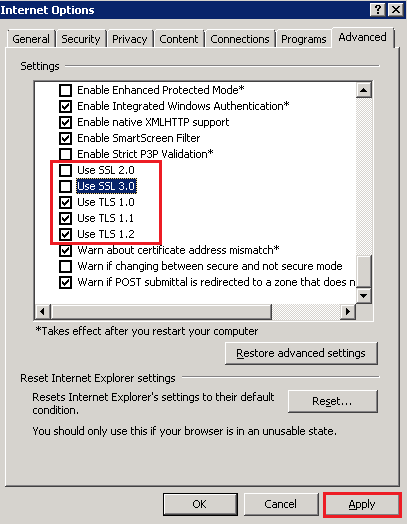
- Giao thức TLS trực thuộc chương trình tiêu chuẩn của lực lượng đặc nhiệm kỹ thuật Internet (**IETF**-The Internet Engineering Task Force), là sự kế thừa cho SSL.



- TLS 1.0 được định nghĩa trong RFC 2246 vào tháng Giêng năm 1999. Sự khác biệt giữa TLS 1.0 và SSL 3.0 có ý nghĩa rằng chúng đã không tương thích. TLS 1.0 đã cho phép khả năng hạ cấp kết nối đến SSL 3.0. TLS 1.1 (RFC 4346, tháng 4 năm 2006) và TLS 1.2 (RFC 5246, tháng 8 năm 2008) là những phiên bản sau này. Các trình duyệt hiện tại hỗ trợ TLS 1.0 theo mặc định và có thể tùy chọn hỗ trợ TLS 1.1 và 1.2.

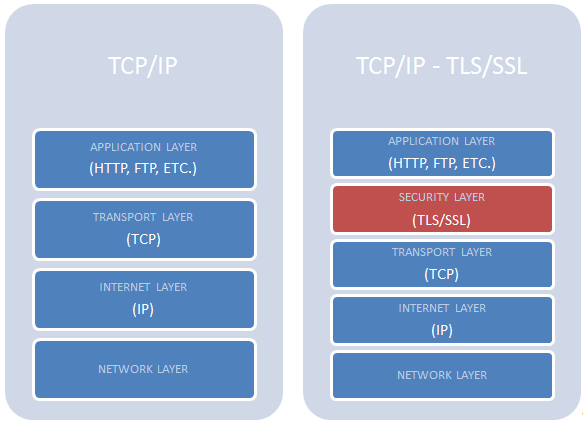


- TLS phát triển từ giao thức Secure Sockets Layer (SSL) và phần lớn đã thay thế nó, mặc dù các điều khoản SSL hoặc SSL / TLS vẫn đôi khi được sử dụng. sự khác biệt chính giữa SSL và TLS là TLS tạo ra một giao thức an toàn và hiệu quả hơn là xác thực thông điệp, thế hệ tài liệu quan trọng và các bộ mã hoá được hỗ trợ, TLS hỗ trợ các thuật toán mới hơn và an toàn hơn. TLS và SSL không tương thích, mặc dù TLS hiện đang cung cấp một số tính tương thích ngược để làm việc với các hệ thống kế thừa.

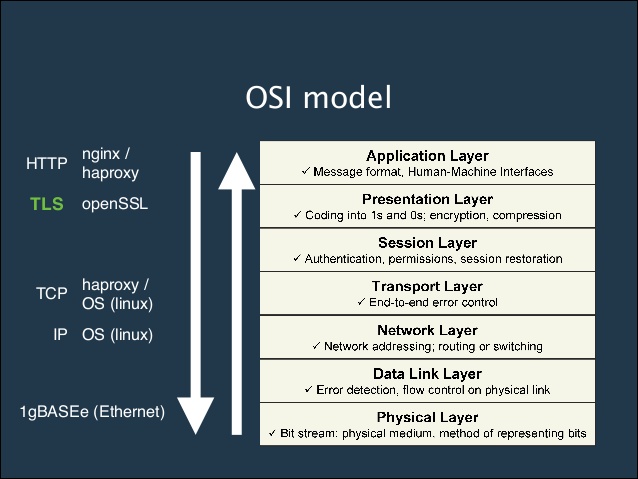


3. Vùng hoạt động của TLS

- Trong khung nhìn mô hình TCP/IP, TLS mã hóa dữ liệu của các kết nối mạng trên một tầng phụ thấp của tầng ứng dụng.



- Theo hệ thống tầng cấp của mô hình OSI, TLS/SSL được khởi chạy ở tầng 5 (tầng phiên) rồi hoạt động trên tầng 6 (tầng trình diễn): trước tiên tầng phiên bắt tay dùng mật mã bất đối xứng để đặt cấu hình mật mã và chìa khóa chia sẻ dành cho phiên đó; sau đó, tầng trình diễn mã hóa phần còn lại của thông điệp dùng mật mã đối xứng và khóa của phiên đó. TLS phục vụ tầng giao vận bên dưới, các đoạn trong tầng này chứa dữ liệu mật mã hóa.



**4. Các thành phần của TLS**

- Theo thông số kỹ thuật giao thức, TLS bao gồm hai lớp: giao thức bản ghi (TLS Record Protocol) và giao thức bắt tay (TLS Handshake Protocol).

+) Giao thức bản ghi cung cấp bảo mật kết nối.

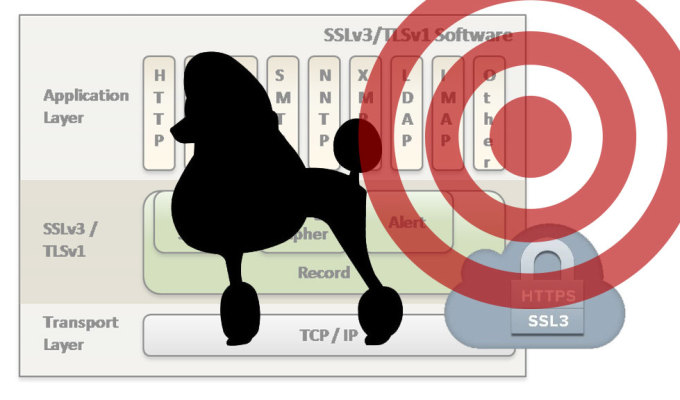
+) Giao thức bắt tay cho phép máy chủ và máy khách xác nhận lẫn nhau và đàm phán các thuật toán mã hóa và khóa mật mã trước khi dữ liệu được trao đổi.

**5. Đánh giá TLS**

- Với bất kỳ công nghệ mã hóa thì các sai sót thực hiện không thể tránh khỏi, và TLS cũng vậy. Lỗ hổng Heartbleed trên Open SSL, một lỗ hổng cực kỳ nghiêm trọng trên bộ thư viện mã nguồn mở OpenSSL của hai giao thức SSL/TLS cho phép những kẻ tấn công có thể đọc được một phần bộ nhớ của máy chủ bị nhiễm mã độc, nó có thể tiết lộ dữ liệu của người dùng máy chủ đã cố che dấu.



- TLS là không dễ bị tấn công POODLE, bởi vì nó xác định rằng tất cả các byte đệm phải có giá trị như nhau và được xác nhận, một biến thể của cuộc tấn công đã khai thác triển khai một số giao thức TLS mà không xác nhận một cách chính xác đệm mã hóa. Điều này làm cho một số hệ thống dễ bị tổn thương đến POODLE, cho dù họ vô hiệu hóa SSL - một trong những kỹ thuật được khuyến cáo cho việc chống lại một cuộc tấn POODLE.



6. Ứng dụng của TLS

- TLS được phát triển để đóng gói các giao thức ứng dụng cụ thể như HTTP, FTP, SMTP, NNTP và XMPP;



- Cho phép trao đổi riêng tư trên mạng Internet, cho phép các ứng dụng khách/chủ giao tiếp an toàn, ngăn ngừa tấn công, bóc tách dữ liệu hay phá hủy thông điệp trái phép như an toàn truyền siêu văn bản, an toàn trao đổi thư điện tử….

- Ban đầu, TLS được sử dụng chủ yếu với những giao thức truyền vận tin cậy như TCP, tuy nhiên, nó cũng được thực hiện với những giao thức truyền vận định hướng gói tin như UDP và giao thức điều khiển tắc nghẽn (Datagram Congestion Control Protocol - DCCP), sau đó đã được chuẩn hóa độc lập và gọi là Giao thức an toàn gói tin tầng giao vận (Datagram Transport Layer Security - DTLS).

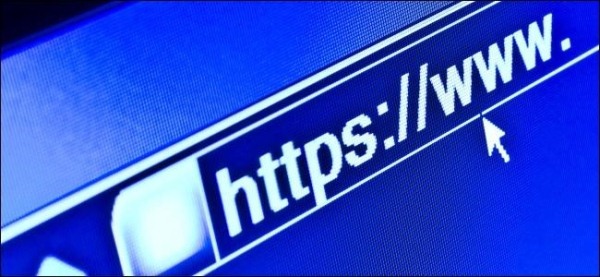
- Sử dụng rộng rãi trong các ứng dụng như duyệt Web, thư điện tử, fax qu Internet, nhắn tin nhanh, và VoIP



1. **Giao thức bảo mật**
2. **HTTPS là gì, vì sao lại dùng HTTPS?**

**Việc hiểu được cơ chế hoạt động và ý nghĩa của giao thức HTTPS là tối quan trọng, bởi giao thức này sẽ giúp giữ an toàn cho bạn khi đang sử dụng các dịch vụ ngân hàng trực tuyến, thương mại điện tử và chống lừa đảo giả dạng (phishing).**

**Mỗi khi bạn sử dụng giao thức HTTPS, thanh địa chỉ của trình duyệt sẽ xuất hiện biểu tượng hình khóa. Nói ngắn gọn, HTTPS (viết tắt của HTTP Secure – HTTP An toàn) là phiên bản bảo mật của giao thức HTTP (HyperText Transfer Protocol - Giao thức truyền tải siêu văn bản) vốn là cốt lõi của Internet. Hãy cùng tìm hiểu về giao thức này qua bài viết của trang How To Geek:**



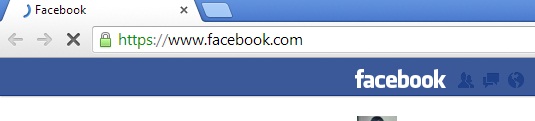
1. **Vấn đề với HTTP**

**Khi bạn kết nối với một trang web thông qua giao thức HTTP, trình duyệt sẽ tìm địa chỉ IP tương ứng với trang web đó và kết nối với địa chỉ IP này. Trình duyệt sẽ mặc nhiên coi rằng bạn đang kết nối với đúng máy chủ cần kết nối. Dữ liệu gửi qua HTTP cũng không hề được mã hóa, thay vào đó chỉ sử dụng dạng ký tự văn bản bình thường, do đó những kẻ nghe/xem lén trên mạng Wi-Fi của bạn, nhà mạng mà bạn đang sử dụng và cả những cơ quan tình báo như NSA đều có thể dò tìm ra các trang web mà bạn đã ghé thăm cũng như các thông tin bạn đã gửi/nhận. Như vậy, những kẻ nghe lén sẽ dễ dàng lấy cắp được mật khẩu, số thẻ tín dụng và các thông tin khác mà bạn gửi qua HTTP.**

**Không chỉ có vậy, nếu chỉ sử dụng HTTP, bạn sẽ không có cách nào để xác thực rằng mình đang kết nối vào đúng trang web cần tới cả. Ví dụ, qua hình thức lừa đảo phishing, bạn có thể đang truy cập vào một trang web giả dạng làm một ngân hàng hoặc một trang bán hàng qua mạng. Ngay cả khi bạn truy cập vào các trang web thông thường qua HTTP, khả năng bạn bị người khác theo dõi và lấy cắp thông tin cá nhân vẫn có thể xảy ra.**

**Nói tóm lại, vấn đề lớn nhất của HTTP là giao thức này không được mã hóa. HTTPS sử dụng mã hóa để khắc phục các vấn đề này.**

1. **HTTPS giải quyết vấn đề như thế nào**



**Facebook cũng đã chuyển sang sử dụng HTTPS để tăng tính bảo mật và riêng tư**

**Dù chưa đảm bảo được tính bảo mật 100% nhưng HTTPS vẫn an toàn hơn rất nhiều so với HTTP. Khi bạn kết nối vào một máy chủ sử dụng HTTPS, trình duyệt sẽ kiểm tra chứng thực bảo mật (security certificate) của trang web này để xem xem chứng thực nói trên có được cung cấp bởi một đơn vị đáng tin cậy hay không. Nhờ đó, khi bạn truy cập vào những địa chỉ như https://nganhangA.com, trình duyệt của bạn sẽ xác thực được rằng bạn đang truy cập vào địa chỉ thực của Ngân Hàng A.**

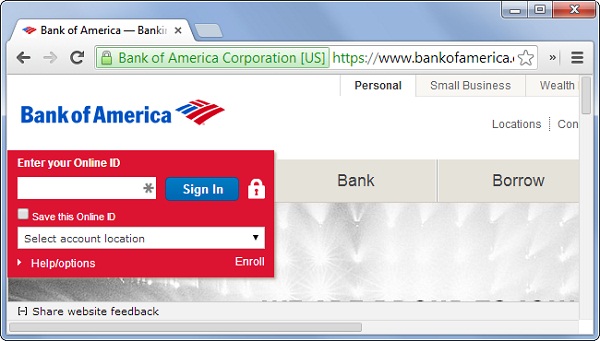
**Dĩ nhiên, HTTPS không phải là không có lỗ hổng: các đơn vị cấp phát chứng thực bảo mật sẽ xác nhận rằng https://nganhangA.com là địa chỉ xác thực của Ngân hàng A. Do đó, nếu các đơn vị cấp phát chứng thực để lọt một trang web xấu nào đó, bạn vẫn có thể bị lừa đảo khi truy cập vào các địa chỉ giả sử dụng HTTPS.**

**Dù có lỗ hổng nhưng HTTPS vẫn tỏ ra hữu ích trong hầu hết các trường hợp sử dụng. Khi bạn cần cung cấp các thông tin như số thẻ tín dụng hoặc địa chỉ email, các trang web uy tín thường chuyển sang sử dụng các kênh HTTPS được mã hóa. Nhờ đó, các nhà mạng hoặc hacker gần như không thể dò tìm thông tin của bạn.**

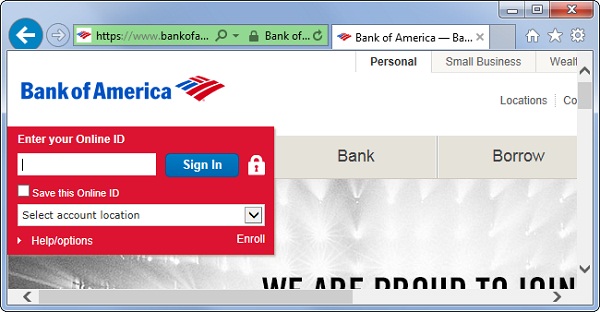
**HTTPS cũng hỗ trợ tăng cường tính riêng tư. Ví dụ, hiện nay Google đang sử dụng giao thức HTTPS cho cả trang tìm kiếm của mình.  Trước đây, do chỉ sử dụng HTTP nên bất kì ai cùng mạng Wi-Fi đều có thể theo dõi các tìm kiếm Google của bạn. Nếu như bạn truy cập vào các trang web khác, ví dụ như Wikipedia thông qua HTTPS, những người cùng mạng cũng không thể biết được bạn đang xem thông tin về chủ đề nào.**

1. **Khi nào thì bạn đang kết nối qua HTTPS?**

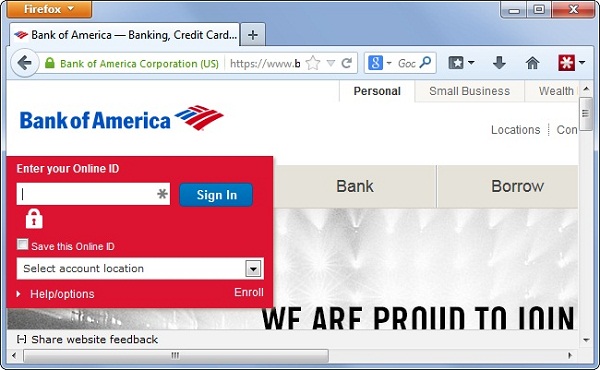
**Khi kết nối với máy chủ xác thực qua HTTPS, trình duyệt của bạn sẽ hiện biểu tượng khóa ngay bên cạnh ô địa chỉ. Bạn có thể click vào biểu tượng này để đọc thêm các thông tin về bảo mật. Tất cả các trình duyệt đều sẽ hiện biểu tượng khóa và hiển thị dòng chữ https:// trong ô địa chỉ, thay vì lược bớt phần http:// như khi sử dụng HTTP thông thường.**



**HTTPS trên Chrome**



**HTTPS trên Internet Explorer**



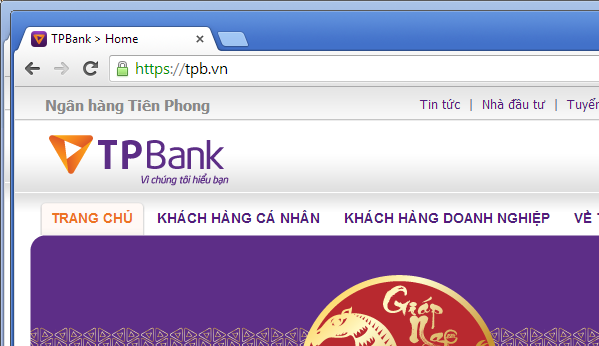
**HTTPS trên Firefox**

1. **Vì sao người dùng Internet cần phải hiểu rõ HTTPS?**

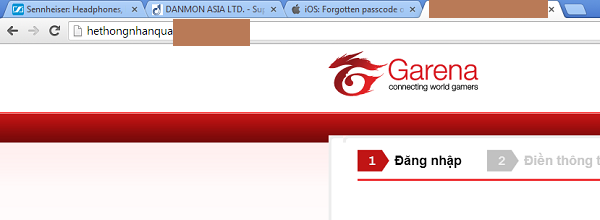
**Bạn phải để ý xem trang web đang sử dụng có dùng HTTPS hay không mỗi khi đăng nhập hoặc cung cấp thông tin thanh toán. Nếu trình duyệt không hiện biểu tượng hình khóa và giao thức HTTPS trong lúc bạn nhập tên tài khoản, mật khẩu, số thẻ tín dụng, mã an toàn…, bạn không nên cung cấp các thông tin này. Nếu cần thiết, hãy liên hệ trực tiếp với đơn vị đang yêu cầu thông tin của bạn để làm rõ.**

**Hiện nay, hầu hết các trang web uy tín tại Việt Nam và trên thế giới đã chuyển sang sử dụng HTTPS, ví dụ như trang web của các ngân hàng hoặc các trang web bán hàng qua mạng có sử dụng thẻ tín dụng. Tuy vậy, một số trang web lớn vẫn chưa chuyển sang sử dụng HTTPS, và do đó thông tin bạn gửi lên trang web này gần như bị mở (không được mã hóa) với hacker và các đối tượng xấu khác.**

**Dù không phải là hoàn hảo nhưng HTTPS cũng là một biện pháp chống hình thức lừa đảo giả dạng (phishing). Nếu bạn đang sử dụng một mạng Wi-Fi công cộng (tại quán café, sân bay…) để truy cập vào tài khoản ngân hàng của mình, hãy để ý tìm biểu tượng hình khóa, dòng chữ HTTPS trên ô địa chỉ và địa chỉchính xác của trang ngân hàng trực tuyến này. Đây là cách hiệu quả nhất để xác thực rằng bạn đang truy cập vào đúng địa chỉ, thay vì vào một trang web lừa đảo, giả dạng khác. Nếu bạn không thấy HTTPS, chắc chắn mạng truy cập của bạn không an toàn.**



**Các ngân hàng tại Việt Nam đã chuyển sang sử dụng HTTPS**



**Ví dụ về một trang web lừa đảo. Trang web này sẽ yêu cầu cung cấp nhiều thông tin nhạy cảm nhưng chỉ sử dụng HTTP thông thường**

**Tránh bị lừa đảo giả dạng (phishing)**

**Những kẻ lừa đảo hiện tại đã phát hiện ra rằng chúng không thể giả dạng làm các ngân hàng uy tín thông qua HTTPS được nữa, do đó chúng sẽ tìm cách biện pháp ranh ma hơn.**

**Ví dụ, kẻ lừa đảo có thể gửi mail có chứa đường dẫn tới địa chỉ web https://nganhanga.com.324924.com. Trên trình duyệt web, biểu tượng hình khóa vẫn sẽ được hiển thị bên cạnh giao thức HTTPS, song thực tế bạn đang truy cập vào một phần (subdomain) có tên "nganhangA.com" của trang web 324924.com chứ không phải là trang web của Ngân Hàng A.**

**Trong mọi trường hợp, hãy kiểm tra xem địa chỉ bạn đang truy cập có phải là địa chỉ chính xác (nganhangA.com) hay không? Ngân Hàng A có thể được chia làm các tên miền nhỏ như tenmien1.nganhanga.com hoặc tenmien2.tenmien3.nganhanga.com, và do đó bạn cần xác nhận phần cuối cùng của tên miền đang truy cập. Nếu như địa chỉ đang truy cập có phần cuối cùng trước dấu / (dấu xược) đầu tiên chính xác là nganhangA.com và đang hiện biểu tượng khóa HTTPS, bạn có thể an tâm cung cấp các thông tin cần thiết.**

**Nếu cẩn thận, bạn hãy tránh click vào các đường link được cung cấp qua email, trừ khi địa chỉ gửi đã được xác thực. Bạn cũng có thể truy cập thẳng vào địa chỉ của ngân hàng và tìm đến tính năng cần sử dụng, thay vì click vào các đường link được gửi qua email.**

# **PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC HTTPS**

**Để hiểu rõ hơn hoạt động của giao thức HTTPS được mô tả trong bài viết này, bạn nên có sẵn kiến thức cơ bản về một số khái niệm liên quan sau:**

* **Symmetric Encryption (hay Secret Key Encryption) và Asymmetric Encryption (hay Public-key Cryptography).**
* **Các chức năng của SSL Certificate (một loại digital certificate) cũng như là các thông tin được chứa trong nó.**
* **Vai trò của Central Authority (CA).**

**I. Giới thiệu**

**Giao thức HTTPS sử dụng port 443, giúp đảm bảo các tính chất sau của thông tin:**

* **Confidentiality: sử dụng phương thức encryption để đảm bảo rằng các thông điệp được trao đổi giữa client và server không bị kẻ thứ ba đọc được.**
* **Integrity: sử dụng phương thức hashing để cả client và server đều có thể tin tưởng rằng thông điệp mà chúng nhận được có không bị mất mát hay chỉnh sửa.**
* **Authenticity: sử dụng digital certificate để giúp client có thể tin tưởng rằng server/website mà họ đang truy cập thực sự là server/website mà họ mong muốn vào, chứ không phải bị giả mạo.**

**Liên quan tới vấn đề này tôi có từng viết một bài về**[**Desktop Phishing**](https://manthang.wordpress.com/2010/10/30/desktop-phishing-nghe-thuat-phishing-moi/)**. Việc nhờ đến bên thứ 3 (thường là CA) để xác thực danh tính của website cộng thêm sự chú ý của người dùng rằng website đó có sử dụng HTTPS và SSL certificate của nó còn hiệu lực sẽ giúp loại bỏ hoàn toàn nguy cơ bị desktop phishing.**

**II. Sử dụng HTTPS như thế nào?**

**Trước hết, muốn áp dụng HTTPS thì trong quá trình cấu hình Webserver, bạn có thể dễ dàng tự tạo ra một SSL certificate dành riêng cho website của mình và nó được gọi là self-signed SSL certificate.**

**SSL certificate tự cấp này vẫn mang lại tính Confidentiality và Integrity cho quá trình truyền thông giữa server và client. Nhưng rõ ràng là không đạt được tính Authenticity bởi vì không có bên thứ 3 đáng tin cậy nào đứng ra kiểm chứng sự tính xác thực của certificate tự gán này. Điều này cũng giống như việc một người tự làm chứng minh nhân dân (CMND) cho mình rồi tự họ ký tên, đóng dấu luôn vậy!**

**Vì vậy, đối với các website quan trọng như E-Commerce, Online Payment, Web Mail,… thì họ sẽ mua một SSL certificate từ một Trusted Root CA nào đó như VeriSign, Comodo, GoDaddy,… Ở đây, các CA có  nhiệm vụ chính là cấp phát và quản lý các certificate.**

**Thực chất thì SSL certificate cũng là một loại digitial certificate (một loại file trên máy tính). Vì HTTPS có dính tới giao thức SSL nên người ta mới đặt tên cho nó là SSL certificate để phân biệt với các loại digital certificate khác như Personal Certificate, Server Certificate, Software Publisher Certificate, Certificate Authority Certificate.**

**Dưới đây là một số thông tin quan trọng được chứa trong SSL certificate:**

* **Thông tin về chủ sở hữu của certificate (có thể là tổ chức, tên cá nhân hoặc tên miền của website).**
* **Thông tin và digital signature của CA mà cấp certificate này.**
* **Khoảng thời gian mà certificate còn hiệu lực.**
* **Public key của website. Còn private key không có trong certificate mà được lưu trữ trên chính server và tuyệt đối không được để lộ cho bất cứ client nào.**
* **Một số thông tin phụ khác như: loại SSL certificate, các thuật toán dùng để encryption và hashing, chiều dài (tính bằng bit) của key, cơ chế trao đổi key (như RSA, DSA).**
* **v.v…**

**III. Quá trình giao tiếp giữa client và server thông qua HTTPS**

**1. Client gửi request cho một secure page (có URL bắt đầu với https://)**

**2. Server gửi lại cho client certificate của nó.**

**3. Client (web browser) tiến hành xác thực certificate này bằng cách kiểm tra (verify) tính hợp lệ của chữ ký số của CA được kèm theo certificate.**

**Giả sử certificate đã được xác thực và còn hạn sử dụng hoặc client vẫn cố tình truy cập mặc dù Web browser đã cảnh báo rằng không thể tin cậy được certificate này (do là dạng self-signed SSL certificate hoặc certificate hết hiệu lực, thông tin trong certificate không đúng) thì mới xảy ra bước 4 sau.**

**4. Client tự tạo ra ngẫu nhiên một symmetric encryption key (hay session key), rồi sử dụng public key (lấy trong certificate) để mã hóa session key này và gửi về cho server.**

**5. Server sử dụng private key (tương ứng với public key trong certificate ở trên) để giải mã ra session key ở trên.**

**6. Sau đó, cả server và client đều sử dụng session key đó để mã hóa/giải mã các thông điệp trong suốt phiên truyền thông.**

**Và tất nhiên, các session key sẽ được tạo ra ngẫu nhiên và khác nhau trong mỗi phiên làm việc với server. Ngoài encryption thì cơ chế hashing sẽ được sử dụng để đảm bảo tính Integrity cho các thông điệp được trao đổi.**

**IV. Tổng kết**

**HTTPS là một giao thức phổ biến trên Internet và rất cần thiết để đảm bảo an toàn, tin cậy cho môi trường Web. Tuy nhiên, vẫn có những cách thức mà attacker có thể sử dụng để “qua mặt” cơ chế bảo vệ của HTTPS (như**[**SSLStrip**](http://www.thoughtcrime.org/software/sslstrip/)**).**

**Để kết thúc bài viết và cũng để các khái niệm liên quan tới HTTPS trở nên gần gũi và dễ hiểu hơn với mọi người, dưới đây là một tình huống thực tế:**

**CMND của người A do Công an ở địa phương B cấp. Người A này muốn thực hiện một giao dịch gì đó rất quan trọng với tổ chức C chẳng hạn. Và giả sử CMND của A là thứ duy nhất mà C có thể dựa vào để tin tưởng được các thông tin về A như khuôn mặt, tên, tuổi, nơi ở… Vì C thấy CMND cũng có thể bị làm giả và để chắc rằng các thông tin về A được ghi trong CMND là chính xác thì cách tốt nhất là C đem CMND của A đến nhờ bên B xác thực giùm.**

**Như vậy, có thể coi:**

* **Bên A là website**
* **Bên B là CA**
* **CMND của A chính là SSL Certificate do B cấp**
* **Bên C là Web client**