**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 1**





**TIỂU LUẬN MÔN AT&BM HTTT**

**Đề tài: Giao thức bảo mật SSL/TLS**

**Giảng viên: Thầy Vũ Minh Mạnh**

**Nhóm 11:**

|  |  |  |
| --- | --- | --- |
| Họ tên | MSV | Nhiệm vụ |
| Nguyễn Mạnh Dũng (NT) | B20DCCN138 | Viết báo cáo, Làm Slide. |
| Trần Quang Huy | B20DCCN328 | Ứng dụng của SSL, Thuyết trình. |
| Nguyễn Cảnh Huỳnh | B20DCCN338 | Hoạt động của SSL, Thuyết trình. |
| Nguyễn Hoàng Việt | B20DCCN728 | Kiến trúc của SSL, Thuyết trình. |

**Hà Nội, 2023**

**Mục lục**

[I. Giới thiệu 2](#_Toc1222936223)

[1. Sự ra đời của SSL 3](#_Toc1684196861)

[2. SSL và TLS 3](#_Toc1267765320)

[II. Kiến trúc 5](#_Toc2040891043)

[1. Vị trí hoạt động 5](#_Toc1423239079)

[2. Cấu trúc 6](#_Toc1979414237)

[3. Record Protocol 7](#_Toc1893867921)

[4. Handshake Protocol 8](#_Toc1745405339)

[5. Change Cipher Spec Protocol 9](#_Toc1654935020)

[6. Alert Protocol 9](#_Toc1126523902)

[III. Hoạt động của SSL/TLS 11](#_Toc1890157418)

[1. Mã hóa đối xứng 11](#_Toc986827339)

[2. Mã hóa bất đối xứng 11](#_Toc263144746)

[3. Truyền dữ liệu qua SSL/TLS trong thực tế 12](#_Toc1804796179)

[IV. Ứng dụng 14](#_Toc1244532474)

[V. Kết luận 17](#_Toc725857164)

# Giới thiệu

## Sự ra đời của SSL

Trong thời kỳ đầu của Internet, việc trao đổi dữ liệu được trao đổi dưới dạng bản rõ, điều này khiến cho các thông tin nhạy cảm có thể bị đánh cắp bởi những kẻ xấu trên đường truyền.

SSL (Secure Sockets Layer) được sinh ra để giải quyết vấn đề này bằng cách cung cấp một kênh truyền đảm bảo các thuộc tính sau:

**Tính xác thực**: Phía máy chủ luôn được xác thực; phía máy khách có thể tùy chọn xác thực.

**Tính bảo mật**: Dữ liệu được gửi sau khi thiết lập kênh chỉ hiển thị với các điểm cuối (endpoint).

**Tính toàn vẹn**: Dữ liệu được gửi sau khi thiết lập kênh nếu bị kẻ tấn công sửa đổi thì sẽ luôn phát hiện được.

Để sử dụng SSL, các website cần có chứng chỉ SSL (hay chứng chỉ TLS) được cấp bởi các cơ quan chứng nhận. Chứng chỉ này hoạt động như một dấu hiệu xác nhận rằng website đó đã được xác thực và được bảo vệ bởi SSL. Việc sử dụng SSL sẽ giúp tăng tính an toàn cho dữ liệu truyền qua mạng, tránh được các mối đe dọa an ninh và bảo vệ thông tin cá nhân của người dùng.

## SSL và TLS

SSL là tiền thân của một giao thức khác là TLS (Transport Layer Security). Việc thay đổi tên gọi chỉ do vấn đề pháp lý nên thuật ngữ "SSL/TLS" vẫn được sử dụng luân phiên để chỉ giao thức này.

Hiện nay đã có những phiên bản SSL/TLS sau đây được phát triển:

SSL 1.0: Không được phát hành.

SSL 2.0: Phát hành năm 1995, ngưng sử dụng.

SSL 3.0: Phát hành năm 1996, ngưng sử dụng.

TLS 1.0: Phát hành năm 1999, ngưng sử dụng.

TLS 1.1: Phát hành năm 2006, ngưng sử dụng.

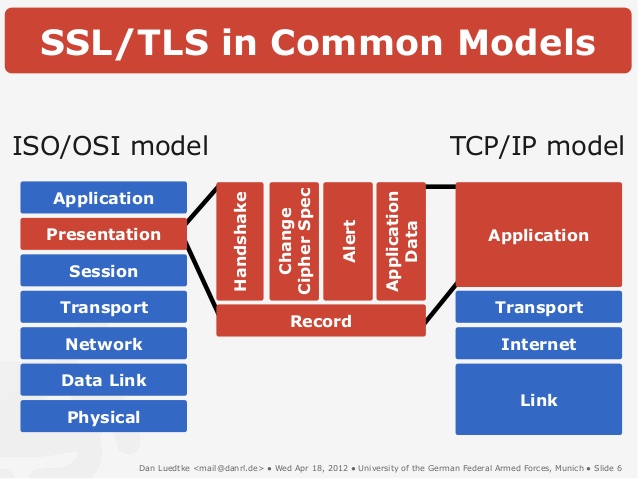
TLS 1.2: Phát hành năm 2008, đang được sử dụng.

TLS 1.3: Phát hành năm 2018, đang được sử dụng.

Các phiên bản của SSL/TLS liên tiếp được cho ra mắt để bắt kịp với sự phát triển của phần cứng, phần mềm cùng các phương thức tấn công. Phiên bản mới nhất TLS 1.3 được ra mắt năm 2018 và đang được sử dụng rộng rãi.

# Kiến trúc

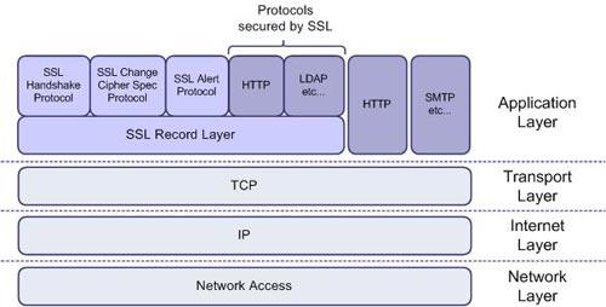
### Vị trí hoạt động



Vị trí hoạt động của SSL/TLS trong mô hình OSI hay TCP/IP không thể được xác định chính xác bởi vì SSL/TLS phải hoạt động trên nhiều tầng để đảm bảo tính bảo mật và tính toàn vẹn của dữ liệu.

Tuy nhiên, SSL/TLS hoạt động trên một giao thức ở tầng giao vận như TCP hay UDP và được sử dụng để bảo vệ các giao thức khác như HTTP hoặc FTP ở tầng ứng dụng. Vì vậy, ta có thể cho rằng SSL/TLS hoạt động ở giữa tầng Ứng dụng và tầng Giao vận trong cả hai mô hình OSI và TCP/IP.

### Cấu trúc



SSL/TLS gồm 4 thành phần chính: Record Protocol (Giao thức bản ghi), Handshake Protocol (Giao thức bắt tay), Change Cipher Spec Protocol (Giao thức thay đổi bộ mã hóa), Alert Protocol (Giao thức cảnh báo).

Record Protocol giúp đảm bảo tính toàn vẹn và bảo mật cho dữ liệu bằng cách sử dụng các thuật toán mã hóa đối xứng và bất đối xứng để mã hóa dữ liệu và các hàm băm để đảm bảo tính toán vẹn của dữ liệu.

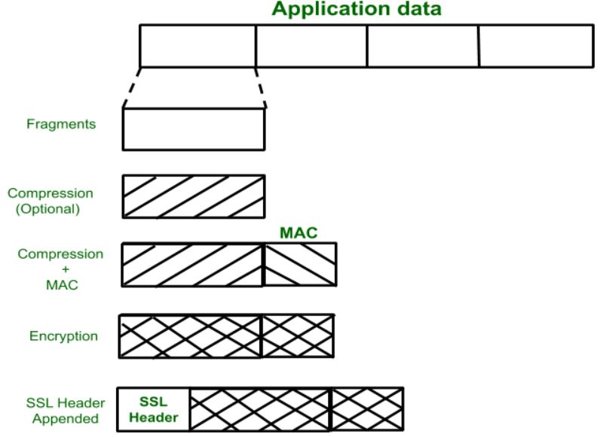
Handshake Protocol dùng để tạo một kênh truyền an toàn cho việc trao đổi thông tin qua các cơ chế xác thực và mã hóa.

Change Cipher Spec Protocol dùng để thông báo với các bên bộ mã hóa sẽ được sử dụng.

Alert Protocol dùng để cảnh báo các bên về các lỗi hoặc các sự cố bảo mật.

Sau đây là chi tiết về từng giao thức và cách chúng vận hành.

### Record Protocol



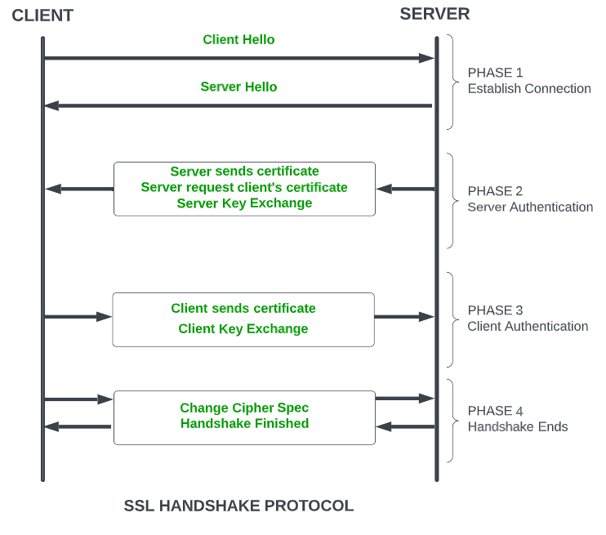
Record Protocol chịu trách nhiệm xác định các định dạng truyền dữ liệu, kiểm soát luồng dữ liệu

Dữ liệu từ tầng ứng dụng sau khi được đưa vào Record Protocol sẽ phải trải qua các bước sau:

* + Dữ liệu được chia thành các mảnh.
  + Các mảnh đó sau đó được nén (nếu cần) và đính kèm với MAC được sinh ra từ các hàm băm.
  + Các mảnh được mã hóa bằng khóa đã được thỏa thuận từ Handshake Protocol
  + Mỗi mảnh được đính thêm header chứa các thông tin tổng quan về mảnh đó.

Ngược lại khi nhận được dữ liệu từ tầng vận chuyển gửi tới Record Protocol sẽ làm ngược lại các bước giải mã, kiểm tra tính toàn vẹn, giải nén và kết hợp lại để tái tạo được dữ liệu ban đầu.

### Handshake Protocol



Handshake Protocol gồm 4 giai đoạn sau:

* Khởi tạo kết nối, trao đổi các gói tin “Hello”: Các gói tin này sẽ giúp client và server trao đổi được các thông tin như phiên bản SSL/TLS, các bộ mã hóa được hỗ trợ, số xác thực phiên của phiên trước (nếu có) và các thông tin phục vụ việc mã hóa.
* Server gửi chứng chỉ của mình cho client xác nhận cùng khóa công khai phục vụ việc mã hóa khóa phiên.
* Sau khi kiểm tra chứng chỉ của server, client tạo ra một khóa phiên và mã hóa nó bằng khóa công khai vừa nhận được. Cuối cùng client gửi khóa phiên đã được mã hóa cùng với chứng chỉ của mình nếu được yêu cầu cho server.
* Sau khi nhận được khóa phiên từ client, server sẽ sử dụng khóa bí mật để giải mã khóa phiên được gửi bởi client, sau đó server gửi thông điệp Change Cipher Spec cho client để thông báo rằng server sẽ bắt đầu sử dụng khóa phiên mới để mã hóa và giải mã các gói tin dữ liệu trong phiên tiếp theo. Sau khi client nhận được thông điệp này, nó cũng sẽ bắt đầu sử dụng khóa phiên mới để mã hóa và giải mã các gói tin dữ liệu.

### Change Cipher Spec Protocol

Dùng để thông báo với các bên bộ mã hóa sẽ được sử dụng. Giao thức này sẽ gửi một tin Change Cipher Spec khi một trong hai bên muốn thay đổi bộ mã hóa hay đồng thuận với một bộ mã hóa nào đó.

Tin Change Cipher Spec có độ dài 1 byte và có giá trị là 1. Nó sẽ thông báo cho bên còn lại rằng từ giờ , toàn bộ các gói tin dữ liệu được truyền qua kênh này sẽ được bảo vệ bởi bộ mã hóa này. Bên nhận sẽ phản hồi lại bằng một tin tương tự để xác nhận rằng nó đã nhận được thông báo về việc thay đổi bộ mã hóa. Và khi cả hai bên hoàn tất việc gửi tin Change Cipher Spec cho nhau, phiên kết nối này sẽ bắt đầu sử dụng bộ mã hóa mới cho các gói tin tiếp theo trong phiên.

### Alert Protocol

Alert Protocol được dùng cảnh báo client và server về các lỗi trong quá trình kết nối hoặc các vấn đề bảo mật khác.

Một cảnh báo gồm 2 byte thể hiện: Mức độ nghiêm trọng của cảnh báo và mô tả của cảnh báo.

Mức độ nghiêm trọng của cảnh báo gồm hai mức độ: cảnh báo mức độ cao và cảnh báo mức độ thấp. Cảnh báo mức độ bao gồm các cảnh báo như sự cố bảo mật, lỗi xác thực, có nguy cơ bị tấn công, còn các cảnh báo mức độ thấp bao gồm các cảnh báo khác như hết tài nguyên hay yêu cầu kết nối lại.

Khi một cảnh báo mức độ cao được gửi, kết nối sẽ bị ngắt ngay lập tức. Khi các cảnh báo mức độ thấp được gửi, kết nối vẫn sẽ được duy trì tuy có thể gặp gián đoạn hoặc các vấn đề khác.

# Hoạt động của SSL/TLS

Hoạt động của SSL/TLS dựa vào hai kỹ thuật mã hóa là: Mã hóa đối xứng và mã hóa đối xứng

### Mã hóa đối xứng

Mã hóa đối xứng (symmetric encryption) là kỹ thuật mã hóa sử dụng cùng một khóa bí mật để mã hóa và giải mã dữ liệu. Khóa bí mật này được sử dụng cho cả hai bước mã hóa và giải mã.

Trong quá trình mã hóa, dữ liệu đầu vào (plaintext) được mã hóa bằng cách sử dụng khóa bí mật để tạo ra dữ liệu đã mã hóa (ciphertext). Trong quá trình giải mã, khóa bí mật được sử dụng để giải mã dữ liệu đã mã hóa, trả về dữ liệu ban đầu.

### Mã hóa bất đối xứng

Mã hóa bất đối xứng (asymmetric encryption), là kỹ thuật mã hóa sử dụng một cặp khóa gồm hai khóa khác nhau để mã hóa và giải mã dữ liệu.

Khóa công khai được công khai, ai cũng có thể biết được khóa này, dùng để mã hóa dữ liệu và khóa bí mật được giữ bí mật, dùng để giải mã dữ liệu được mã hóa bằng khóa công khai.

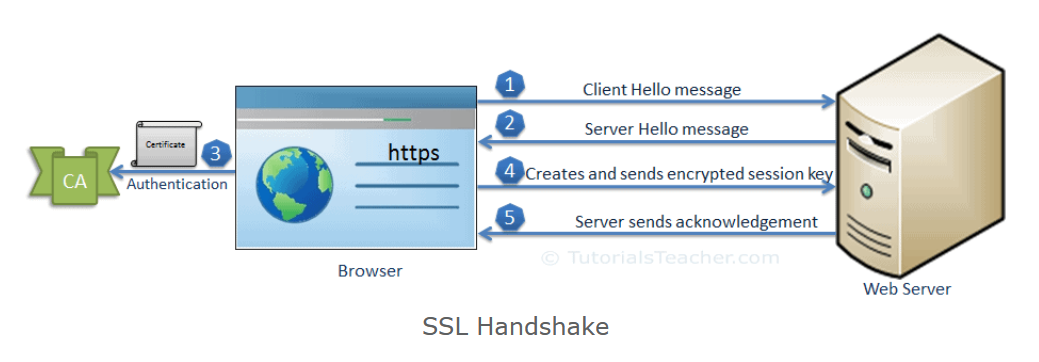
Quá trình mã hóa và giải mã dữ liệu trong mã hóa bất đối xứng được thực hiện theo cặp khóa công khai - khóa bí mật. Một đối tượng muốn gửi tin nhắn được mã hóa cho đối tượng khác sẽ sử dụng khóa công khai của đối tượng đó để mã hóa tin nhắn. Đối tượng nhận được tin nhắn sẽ sử dụng khóa bí mật của mình để giải mã tin nhắn đó.

### Truyền dữ liệu qua SSL/TLS trong thực tế

Ảnh có chứa văn bản

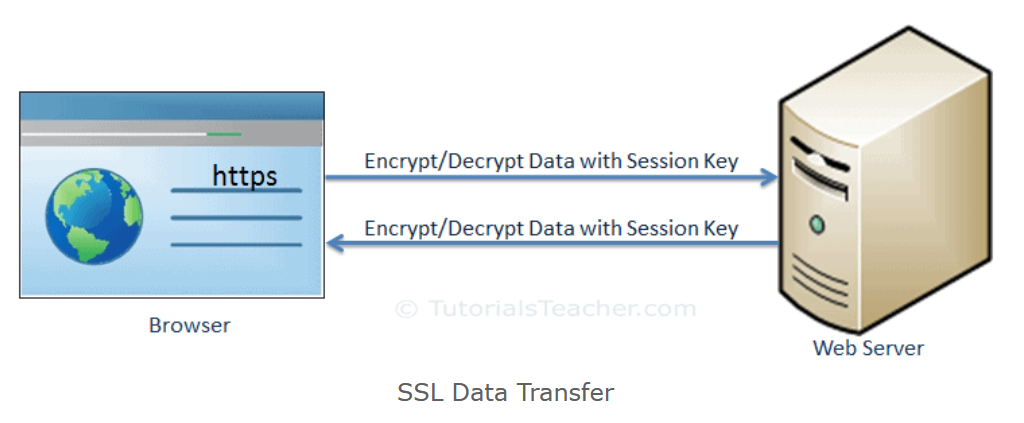
Mô tả được tạo tự động Giao tiếp SSL giữa trình duyệt và Server (hoặc bất kỳ hai hệ thống nào khác) được chia thành giai đoạn chính:

* Bắt tay SSL (SSL Handshake)
* Truyền dữ liệu thực tế (Data Transfer)



**SSL Handshake:**

* Ở giai đoạn này Handshake Protocol được thực thi, kỹ thuật mã hóa bất đối xứng sẽ được áp dụng cho việc trao đổi khóa phiên giữa Client và Server.
* Server sẽ tạo ra khóa công khai và khóa bí mật, khóa công khai sẽ được gửi đến client, client sẽ dùng khóa công khai đấy để mã hóa khóa phiên nó vừa tạo rồi gửi lại Server, Server dùng khóa bí mật để giải mã khóa phiên.



**Data Transfer:**

* Ở giai đoạn này kỹ thuật mã hóa đối xứng được sử dụng, Client và Server đều đang dùng chung khóa phiên có được từ giai đoạn trước phục vụ cho cả việc mã hóa và giải mã các dữ liệu được trao đổi.

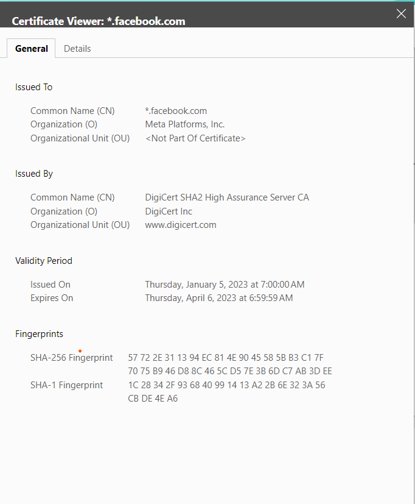
# Ứng dụng

SSL/TLS được sử dụng rộng rãi trong các ứng dụng truyền thông trên Internet như web, email, chat và file transfer. Cụ thể, SSL/TLS được sử dụng trong các ứng dụng sau:

* HTTPS (Hypertext Transfer Protocol Secure) cho truyền thông trên web
* SMTPS (Simple Mail Transfer Protocol Secure) và POP3S/IMAPS (Secure Post Office Protocol/Internet Mail Access Protocol) cho truyền thông trên email
* FTPS (File Transfer Protocol Secure) cho truyền thông trên file transfer.
* VPN (Virtual Private Network) cho truyền thông trên mạng riêng ảo.

Tuy nhiên ứng dụng nổi bật nhất của SSL/TLS chính là HTTPS. Khi chúng ta duyệt web, nếu để ý thì có thể thấy trong đường dẫn của nhiều website có biểu tượng khóa và trong URL của website đó bắt đầu bằng “https” (HTTP Secure). Đó là dấu hiệu cho việc Website đó đã được cấp một chứng chỉ SSL/TLS.

Chứng chỉ SSL/TLS là một chứng chỉ kỹ thuật số dùng để bảo mật và xác minh danh tính của trang web hoặc dịch vụ trực tuyến. Chứng chỉ được cấp bởi một bên thứ 3 đáng tin cậy có tên là “Tổ chức phát hành chứng chỉ”. Tổ chức này sẽ xác minh danh tính của trang web hoặc dịch vụ trước khi cấp chứng chỉ.

 Ở đây ta có thể thấy trang facebook.com được cấp chứng chỉ SSL/TLS từ tổ chức DigiCert.

Một trang Web có chứng chỉ SSL/TLS sẽ đảm bảo các đặc điểm sau:

* **Encryption**: Chứng chỉ SSL/TLS sử dụng thuật toán mã hóa để bảo mật thông tin liên lạc giữa trang web hoặc dịch vụ và người dùng. Điều này đảm bảo rằng thông tin nhạy cảm, chẳng hạn như thông tin đăng nhập và thông tin thẻ tín dụng, được bảo vệ khỏi bị chặn và đọc bởi các bên trái phép.
* **Authentication**: Chứng chỉ SSL/TLS xác minh danh tính của trang web hoặc dịch vụ, đảm bảo rằng người dùng đang giao tiếp với bên dự định chứ không phải với kẻ mạo danh. Điều này cung cấp sự đảm bảo cho người dùng rằng thông tin của họ đang được truyền đến một thực thể đáng tin cậy.
* **Integrity**: Chứng chỉ SSL/TLS sử dụng mã xác thực thông báo (MAC) để phát hiện bất kỳ hành vi giả mạo dữ liệu nào trong quá trình truyền. Điều này đảm bảo rằng dữ liệu được truyền đi không bị sửa đổi theo bất kỳ cách nào, bảo toàn tính toàn vẹn của nó.
* **Non-repudiation**: Chứng chỉ SSL/TLS cung cấp tính năng không từ chối dữ liệu, nghĩa là người nhận dữ liệu không thể phủ nhận việc đã nhận được dữ liệu đó. Điều này rất quan trọng trong các tình huống cần thiết lập tính xác thực của thông tin, chẳng hạn như trong các giao dịch thương mại điện tử.
* **Public-key Cryptography**: Chứng chỉ SSL/TLS sử dụng mật mã khóa công khai để trao đổi khóa an toàn giữa máy khách và máy chủ. Điều này cho phép máy khách và máy chủ trao đổi khóa mã hóa một cách an toàn, đảm bảo rằng thông tin được mã hóa chỉ có thể được giải mã bởi người nhận dự định.
* **Session Management**: Chứng chỉ SSL/TLS cho phép quản lý các phiên bảo mật, cho phép nối lại các phiên bảo mật sau khi bị gián đoạn. Điều này giúp giảm chi phí thiết lập kết nối an toàn mới mỗi khi người dùng truy cập trang web hoặc dịch vụ.
* **Chứng chỉ do các CA đáng tin cậy cấp**: Chứng chỉ SSL/TLS được cấp bởi các CA đáng tin cậy, những người chịu trách nhiệm xác minh danh tính của trang web hoặc dịch vụ trước khi cấp chứng chỉ. Điều này mang lại mức độ tin cậy và đảm bảo cao cho người dùng rằng trang web hoặc dịch vụ mà họ đang liên lạc là xác thực và đáng tin cậy.

Ngoài các đặc điểm chính này, chứng chỉ SSL/TLS còn có nhiều cấp độ xác thực khác nhau, bao gồm Xác thực tên miền (DV), Xác thực tổ chức (OV) và Xác thực mở rộng (EV). Mức độ xác thực xác định lượng thông tin được CA xác minh trước khi cấp chứng chỉ, với chứng chỉ EV cung cấp mức độ đảm bảo và tin cậy cao nhất cho người dùng.

# Kết luận

Nhìn chung, SSL/TLS là một thành phần quan trọng của bảo mật trực tuyến, cung cấp khả năng mã hóa, xác thực, tính toàn vẹn, chống thoái thác và các tính năng chính khác nhằm đảm bảo việc truyền thông tin nhạy cảm an toàn và đáng tin cậy qua internet.

Tuy nhiên, SSL/TLS vẫn không hoàn hảo và có thể bị tấn công bởi một số kỹ thuật như khai thác lỗ hổng của các phiên bản cũ, tấn công giả mạo chứng chỉ, và tấn công kết nối giữa máy khách và máy chủ. Do đó, việc ứng dụng SSL/TLS đòi hỏi sự cẩn trọng và các biện pháp bảo mật phù hợp.

Tóm lại, SSL/TLS là một công nghệ quan trọng để bảo vệ thông tin truyền tải trên internet. Tuy nhiên, để đảm bảo tính bảo mật, các tổ chức cần triển khai các biện pháp bảo mật đầy đủ và cập nhật SSL/TLS lên các phiên bản mới nhất và phù hợp.

**Tài liệu tham khảo**

1. [RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 (rfc-editor.org)](https://www.rfc-editor.org/rfc/rfc8446)
2. [Secure Socket Layer (SSL) - GeeksforGeeks](https://www.geeksforgeeks.org/secure-socket-layer-ssl/)
3. Giáo trình AT&BM – HTTT PTIT