Tạp chí Tin học và Điều khiển học, T. 19, S. 2 (2003), 159–166

GIAO THỨC SECURE SOCKETS LAYER

NGUYỄN BỘI HỒNG MINH

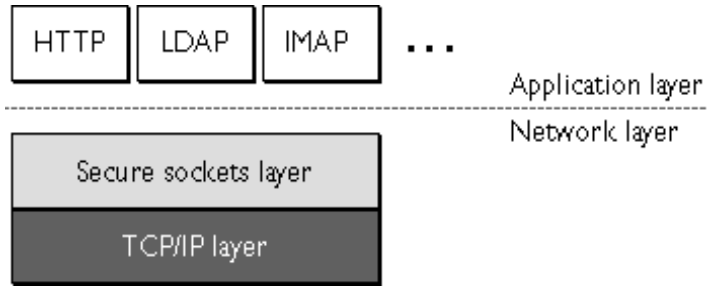
Ban Khoa học & Công nghệ - Tổng công ty Hàng không Việt Nam.

Abstract. E-Commerce is new way to do business. In this way, buyers can meet sellers easier. It has given the buyer a lot of value on business such as: decrease in marketting-fee, distribution-fee, ... But it makes a lot of technical problems. Among those problems, the security of information is very important. In this paper, we present the Secure Socket Layer (SSL) protocol. This protocol is using widely to secure the information that transmited between computers on Internet. And we advice how to implement this protocol in different size of applications.

Tóm tắt. Thương mại điện tử - một phương thức kinh doanh mới cho phép người mua hàng tiếp xúc dễ dàng hơn với người bán hàng. Đi đôi với lợi ích về kinh doanh như giảm chi phí tiếp thị, giảm chi phí phân phối, ... là các vấn đề về kỹ thuật. Trong đó, bảo mật thông tin là vấn đề được đặt lên hàng đầu. Trong bài báo này trình bày giao thức Secure Socket Layer (SSL) là giao thức hiện nay được sử dụng rộng rãi để đảm bảo an ninh thông tin được truyền giữa các máy tính trên Internet. Bài báo cũng đưa ra các hướng áp dụng giao thức này đối với các ứng dụng có quy mô khác nhau.

1. GIỚI THIỆU VỀ GIAO THỨC

Trong các ứng dụng trên Internet hiện nay, giao thức SSL được sử dụng rộng rãi như là một giao thức bảo mật dữ liệu được truyền giữa máy chủ (Server) và máy Trạm (Client) hiệu quả. Bản phác thảo của SSL được đưa ra đầu tiên bởi tổ chức IETF. Sau đó được Hãng NETSCAPE phát triển thành một chuẩn của IETF. Phiên bản này của SSL được sửa đổi các lần vào tháng 11-12/1994 , tháng 1-2/1995. Trong mô hình DoD (U.S Department Of Defense), SSL đặt ở giữa TCP/IP và lớp trên như HTTP, IMAP, LDAP ...



Hình 1. SSL ở giữa TCP/IP và các giao thức ở lớp trên

Những ứng dụng của SSL trên Internet hoặc trong các mạng TCP/IP là:

- Quá trình xác thực máy chủ cho phép máy trạm xác thực nhận dạng máy chủ. Chương trình hỗ trợ SSL (SSL-enable) trên máy trạm có thể dùng các kỹ thuật cơ bản về khóa công khai (public-key) để kiểm tra rằng bản xác thực của máy chủ (server's certificate) và định danh công cộng (public-ID) là hợp lệ và đã được xuất ra bởi người có thẩm quyền cấp chứng

nhận (CA) được liệt kê trong danh sách CA tin cậy (trusted CAs) trên máy trạm. Sự xác nhận này vô cùng quan trọng nếu người dùng gửi đi các thông tin quý giá như số của thẻ tín dụng (Credit card number) qua mạng và muốn kiểm tra nhận dạng máy chủ - là máy sẽ nhận thông tin này.

- Quá trình xác thực trên máy trạm cho phép máy chủ xác thực nhận dạng người dùng. Sử dụng kỹ thuật giống như trên, chương trình hỗ trợ SSL trên máy chủ có thể kiểm tra bản xác thực của máy trạm (client's certificate) và định danh công cộng có hợp lệ hay không, có được xuất ra bởi người có thẩm quyền cấp chứng nhận được liệt kê trong danh sách CA tin cậy trên máy chủ hay không. Sự xác nhận này vô cùng quan trọng nếu máy chủ gửi thông tin quan trọng tới máy trạm và cần kiểm tra nhận dạng máy trạm.

- Kết nối đã được mã hóa bởi SSL yêu cầu tất cả các thông tin được gửi giữa máy chủ và máy trạm đều được mã hóa bởi chương trình gửi và được giải mã bằng chương trình nhận với độ tin cậy ở mức cao. Độ tin cậy là rất quan trọng ở bất kỳ hoạt động riêng nào. Thêm vào đó, tất cả số liệu được truyền qua kết nối đã được mã hóa bởi SSL sẽ được bảo vệ với một cơ chế phát hiện sự thâm nhập và nó sẽ tự động quyết định xem số liệu có bị thay đổi trên đường truyền hay không.

2. GIAO THỨC SSL

Giao thức SSL bao gồm 2 giao thức phụ: giao thức Bản ghi SSL (SSL record) và giao thức Bắt tay SSL (SSL handshake). Giao thức bản ghi SSL định nghĩa khuôn dạng được dùng để truyền số liệu. Giao thức Bắt tay SSL sử dụng giao thức bản ghi SSL để chuyển các chuỗi thông báo (message) giữa máy chủ và máy trạm khi chúng thiết lập kết nối SSL. Sự trao đổi các thông báo này được thiết kế thuận tiện cho các hoạt động sau:

- Xác thực máy chủ với máy trạm.
- Cho phép máy chủ và máy trạm chọn thuật toán mã hóa mà cả hai bên đều có khả năng sử dụng.
- Xác thực máy trạm với máy chủ.
- Sử dụng kỹ thuật mã hóa khóa công khai để tạo Bí mật dùng chung (shared-secrets).
- Thiết lập kết nối được mã hóa bởi SSL.

2.1. Giao thức bản ghi SSL

2.1.1. Khuôn dạng phần đầu của bản ghi SSL

Trong SSL, số liệu gửi đi được gói trong các bản ghi, nó gồm phần đầu (header) và phần số liệu (data). Mỗi phần đầu của bản ghi bao gồm 2 hoặc 3 bytes. Nếu bit cao nhất trong byte đầu tiên là 1 thì phần đầu có độ dài 2 bytes và bản ghi không có phần bổ sung (padding), ngược lại thì phần đầu có độ dài 3 bytes và bản ghi có phần bổ sung. Trong trường hợp phần đầu có độ dài 3 bytes, bit tiếp theo trong byte đầu có một ý nghĩa đặc biệt. Nếu là 0 thì bản ghi là bản ghi số liệu. Nếu là 1 thì loại bản ghi này được dự phòng sẽ sử dụng trong tương lai. Chiều dài bản ghi (Record-length) không bao gồm phần đầu.

Với phần đầu có độ dài 2 bytes, chiều dài bản ghi được tính như sau:

RECORD-LENGTH = ((byte[0] & 0x7f) <<8)) | byte[1];

trong đó , byte[0] biểu diễn byte đầu tiên nhận được.

Với phần đầu có độ dài 3 bytes, chiều dài bản ghi được tính như sau:

RECORD-LENGTH = ((byte[0] & 0x3f) << 8)) | byte[1];
IS-ESCAPE = (byte[0] & 0x40) != 0;
PADDING = byte[2];

Giá trị PADDING chỉ rõ số byte số liệu được máy thu bổ sung thêm vào bản ghi ban đầu. Số liệu bổ sung được dùng để đảm bảo chiều dài bản ghi là bội số của kích thước khối mật mã (ciphers block size) khi mật mã khối được dùng để mã hoá. Máy phát khi phát bản ghi có phần bổ sung (padded record) sẽ bổ sung thêm dữ liệu vào cuối của dữ liệu thông thường và sau đó mã hóa toàn bộ. Giá trị của dữ liệu bổ sung là không quan trọng nhưng dạng đã mã hóa của nó phải được gửi cho máy thu biết để đảm bảo giải mã bản ghi được đúng. Máy thu khi thu được bản ghi có phần bổ sung sẽ giải mã toàn bộ số liệu sau đó sẽ trừ giá trị RECORD-LENGTH đi giá trị PADDING để quyết định chiều dài thực của bản ghi. Phần dữ liệu bổ sung phải được huỷ bỏ đi.

2.1.2. Khuôn dạng số liệu của bản ghi SSL

Phần số liệu của bản ghi SSL bao gồm 3 thành phần được phát và thu theo thứ tự như sau:

MAC-DATA[MAC-SIZE]

ACTUAL-DATA[N]

PADDING-DATA[PADDING]

Trong đó: ACTUAL-DATA là phần dữ liệu thực sự được phát.

PADDING-DATA là phần dữ liệu bổ sung được gửi khi mật mã khối được sử dụng và cần phải có phần bổ sung.

MAC-DATA là mã xác thực của thông báo (Message Authentication Code).

Khi bản ghi SSL được gửi theo dạng rõ ràng, không sử dụng mật mã, thì tổng số PADDING-DATA sẽ là 0 và tổng số MAC-DATA sẽ là 0. Khi có sự mã hoá, PADDING-DATA sẽ phụ thuộc vào kích thước khối mật mã. MAC-DATA phụ thuộc vào CIPHER-CHOICE. MAC-DATA được tính toán như sau:

MAC-DATA = HASH[SECRET, ACTUAL-DATA, PADDING-DATA, SEQUENCE-NUMBER]

trong đó SEQUENCE-NUMBER là giá trị 32 bit.

MAC-SIZE phụ thuộc vào thuật toán phân loại được sử dụng. Với MD2 và MD5 thì MAC-SIZE là 16 bytes (128 bits).

Nếu máy trạm đang gửi thông báo thì SECRET là CLIENT-WRITE-KEY (máy chủ sẽ dùng SERVER-READ-KEY để kiểm tra MAC). Nếu máy trạm đang nhận thông báo thì SECRET là CLIENT-READ-KEY (máy chủ dùng SERVER-WRITE-KEY để tạo MAC).

SEQUENCE-NUMBER là bộ đếm được tăng bởi cả máy thu và máy phát. Với mỗi hướng phát xạ, có 1 cặp bộ đếm được giữ (1 bởi máy phát và 1 bởi máy thu). Mỗi lần thông báo được gửi bởi máy phát thì bộ đếm tăng lên 1. Số này sẽ trở về 0 nếu nó vượt quá giá trị 0XFFFFFFFF (hệ 16). Trước khi bản ghi đầu tiên được gửi, số hiệu dãy được đưa về 0.

Máy thu dùng giá trị của số hiệu dãy (sequence number) như là giá trị đầu vào của hàm tính MAC (Hàm HASH). Việc tính MAC-DATA phải phù hợp từng bit với MAC-DATA được phát. Nếu việc so sánh không thấy giống nhau thì bản ghi được coi là hỏng và nó coi như có lỗi "I/O Error" .

Trong trường hợp sử dụng mật mã khối, chiều dài dữ liệu (được diễn tả trong RECORD-LENGTH) phải là bội số của kích thước khối mật mã. Nếu không đúng thì bản ghi được coi là hỏng và nó coi như có lỗi "I/O Error".

Khuôn dạng bản ghi SSL được dùng cho mọi liên lạc SSL và việc chuyển dữ liệu của ứng dụng lớp trên. Khuôn dạng bản ghi SSL được dùng bởi cả máy chủ và máy trạm.

Với phần đầu có độ dài 2 byte, độ dài tối đa của bản ghi là 32767 bytes. Với phần đầu có độ dài 3 byte, độ dài tối đa của bản ghi là 16383 bytes.

2.2. Giao thức bắt tay SSL

2.2.1. Hoạt động của giao thức bắt tay SSL

Giao thức bắt tay SSL có 2 giai đoạn chính. Giai đoạn đầu được dùng để thiết lập kênh thông tin riêng. Giai đoạn sau được dùng để xác thực máy trạm.

Giai đoạn 1

Máy trạm bắt đầu cuộc gọi bằng cách gửi thông báo CLIENT-HELLO. Máy chủ khi nhận được thông báo này sẽ xử lý nó và trả lời bằng thông báo SERVER-HELLO. Trong giai đoạn này cả máy trạm và máy chủ đều có đủ thông tin để biết rằng có cần Mã khóa chủ (master-key) mới hay không. Nếu không cần, thì chúng chuyển sang giai đoạn 2. Nếu cần, trong thông báo SERVER-HELLO sẽ bao gồm đầy đủ thông tin để máy trạm tạo mã khóa chủ mới. Các thông tin đó là: xác thực đã được ký bởi máy chủ (server's signed certificate), danh sách đặc tả khối mã hóa (bulk cipher specifications) và định danh liên kết (connection-id) (định danh liên kết là một giá trị ngẫu nhiên được tạo bởi máy chủ). Máy trạm tạo mã khóa chủ và trả lời với thông báo CLIENT-MASTER-KEY.

Chú ý rằng mỗi đầu cuối của SSL sử dụng một cặp mật mã (một cho thông tin đến và một cho thông tin đi). Khi máy trạm hoặc máy chủ tạo khóa của phiên làm việc (session-key), thực chất chúng tạo 2 khóa SERVER-READ-KEY (được biết như là CLIENT-WRITE-KEY) và SERVER-WRITE-KEY (được biết như là CLIENT-READ-KEY). Mã khóa chủ được dùng bởi máy trạm và máy chủ để tạo các khóa của phiên làm việc khác nhau.

Cuối cùng, máy chủ gửi thông báo SERVER-VERIFY cho máy trạm sau khi mã khóa chủ được quyết định. Đây là bước cuối cùng để xác thực máy chủ vì chỉ có máy chủ khi có khóa công khai thích hợp mới có thể biết mã khóa chủ.

Giai đoạn 2

Là giai đoạn xác thực. Máy chủ đã được xác thực với máy trạm trong giai đoạn 1, vì vậy giai đoạn 2 chủ yếu để dùng xác thực máy trạm. Máy chủ sẽ gửi yêu cầu tới máy trạm. Máy trạm sẽ trả lời nếu nó có đủ thông tin, ngược lại nó sẽ trả lời với thông báo ERROR. Khi thực hiện xong việc xác thực, nó gửi thông báo hoàn thành (finished-message). Với máy trạm đó là thông báo CLIENT-FINISH bao gồm dạng đã được mã hóa của CONNECTION-ID để máy chủ kiểm tra. Nếu việc kiểm tra xác định là sai thì máy chủ sẽ trả về thông báo ERROR. Khi một thành phần gửi đi thông báo hoàn thành, nó phải tiếp tục lắng nghe cho tới khi nó cũng nhận được thông báo hoàn thành từ thành phần kia. Khi cả hai đều nhận được thông báo hoàn thành thì giao thức bắt tay SSL được hoàn thành. Lúc này các giao thức lớp trên có thể bắt đầu hoạt động.

2.2.2. Sơ đồ các thông báo (Protocol Message)

Sau đây là sơ đồ thông báo của một số tình huống trong giao thức bắt tay SSL. Trong 3 ví dụ sau, ta có 2 thành phần chính là máy trạm (C) và máy chủ (S). Ký hiệu "{something}key" diễn tả số liệu "something" đã được mã hóa sử dụng khóa "key".

Khi không có định danh phiên làm việc:

client-hello	C $\longrightarrow$ S: challenge, cipher_specs
server-hello	S $\longrightarrow$ C: connection-id, server_certificate, cipher_specs
client-master-key	C $\longrightarrow$ S: {master_key}server_public_key
client-finish	C$\longrightarrow$ S: {connection-id}client_write_key
server-verify	S $\longrightarrow$ C: {challenge}server_write_key
server-finish	S $\longrightarrow$ C: {new_session_id}server_write_key

Khi định danh phiên làm việc được tìm thấy bởi cả máy trạm và máy chủ

client-hello	C ⟶ S: challenge, session_id, cipher_specs
server-hello	S ⟶ C: connection-id, session_id_hit
client-finish	C ⟶ S: {connection-id}client_write_key
server-verify	S ⟶ C: {challenge}server_write_key
server-finish	S ⟶ C: {session_id}server_write_key

Khi sử dụng định danh phiên làm việc và có xác thực máy trạm

client-hello	C ⟶ S: challenge, session_id, cipher_specs
server-hello	S ⟶ C: connection-id, session_id_hit
client-finish	C ⟶ S: {connection-id}client_write_key
server-verify	S ⟶ C: {challenge}server_write_key
request-certificate	S ⟶ C:{auth_type, challenge}server_write_key
client-certificate	C ⟶ S: {cert_type, client_cert, response_data}client_write_key
server-finish	S ⟶ C: {session_id}server_write_key

2.2.3. Xử lý lỗi

Khi một trong hai thiết bị phát hiện được lỗi nó sẽ gửi thông báo tới thiết bị kia. Với những lỗi không khắc phục được thì máy trạm và máy chủ sẽ kết thúc kết nối một cách an toàn. Chúng sẽ xoá hết giá trị định danh phiên làm việc tương ứng. Giao thức bắt tay SSL định nghĩa các lỗi sau:

NO-CIPHER-ERROR

Lỗi này do máy trạm gửi trả lại máy chủ khi nó không tìm thấy phương pháp mã hóa hoặc kích thước khóa mà nó và máy chủ cùng hỗ trợ. Lỗi này là lỗi không khắc phục được.

NO-CERTIFICATE-ERROR

Khi thông báo REQUEST-CERTIFICATE được gửi tới máy trạm, lỗi này có thể được gửi nếu máy trạm không có xác thực để trả lời thông báo trên. Lỗi này là lỗi có thể khắc phục được.

BAD-CERTIFICATE-ERROR

Lỗi này được gửi khi xác thực được xác định là sai bởi thiết bị thu. Được xác định là "sai" khi chữ ký trong xác thực là sai hoặc khi giá trị trong xác thực là không thích hợp. Lỗi này là lỗi có thể khắc phục được.

UNSUPPORTED-CERTIFICATE-TYPE-ERROR

Lỗi này được gửi khi máy trạm hoặc máy chủ nhận được kiểu xác thực mà nó không hỗ trợ. Lỗi này là lỗi có thể khắc phục được.

2.2.4. Các thông báo của giao thức bắt tay SSL

Chúng được đóng gói trong khuôn dạng được chỉ ra bởi giao thức bản ghi SSL và gồm 2 phần:

- Một byte diễn tả kiểu của thông báo
- Phần số liệu của thông báo.

Máy trạm và máy chủ chuyển các thông báo này cho tới khi cả hai đều gửi thông báo kết thúc.

Sau khi cặp khóa của phiên làm việc đã được quyết định bởi từng trạm, phần nội dung của thông báo được mã hóa sử dụng các khóa đó. Phía máy trạm, điều này xảy ra sau khi nó kiểm tra định danh của phiên làm việc hoặc tạo khóa của phiên làm việc mới và gửi tới máy chủ. Phía máy chủ, điều này xảy ra sau khi định danh của phiên làm việc được xác nhận là đúng hoặc máy chủ nhận được thông báo khóa của phiên làm việc từ phía máy trạm.

2.2.5. Các thông báo từ phía máy trạm

1) CLIENT-HELLO (Trong giai đoạn 1; được gửi dưới dạng không mã hóa). Khi lần đầu tiên máy trạm nối với máy chủ nó được yêu cầu gửi thông báo CLIENT-HELLO. Thông báo đầu tiên đến từ phía máy trạm nếu không phải là thông báo này thì sẽ bị coi là lỗi. Trong thông báo này, máy trạm gửi tới máy chủ:

- Phiên bản giao thức SSL trên máy trạm.

- Đặc tả phương pháp mã hóa trên máy trạm.

- Một số dữ liệu đặc biệt (challenge data) được dùng để xác thực với máy chủ. Sau khi cả hai đồng ý khóa của phiên làm việc, máy chủ trả lại thông báo SERVER-VERIFY và CHALLENGE-DATA đã được mã hóa.

- Số liệu định danh phiên làm việc. Nó chỉ được gửi nếu máy trạm tìm thấy định danh phiên làm việc trong bộ nhớ của nó với máy chủ đó.

Sau khi gửi xong, máy trạm đợi thông báo SERVER-HELLO. Bất kỳ thông báo nào gửi lại từ phía máy chủ sẽ bị bỏ qua (trừ thông báo lỗi).

2) CLIENT-MASTER-KEY (Trong giai đoạn 1; hầu hết được gửi dưới dạng không mã hóa). Máy trạm gửi thông báo này khi nó đã quyết định mã khóa chủ cho máy chủ sử dụng. Chú ý rằng khi định danh phiên làm việc đã được đồng ý thì thông báo này không được gửi.

Chú ý rằng MASTER-KEY được đưa cho máy chủ trong thông báo CLIENT-MASTER-KEY. CHALLENGE-DATA được đưa cho máy chủ trong thông báo CLIENT-HELLO. CONNECTION-ID được đưa cho máy trạm trong thông báo SERVER-HELLO.

Chú ý rằng mã khóa chủ không bao giờ được dùng trực tiếp để mã hóa số liệu.

CLIENT-MASTER-KEY phải được gửi sau CLIENT-HELLO và trước CLIENT-FINISH. CLIENT-MASTER-KEY phải được gửi nếu SERVER-HELLO bao gồm giá trị SESSION-ID-HIT giá trị 0.

3) CLIENT-CERTIFICATE (Trong giai đoạn 2;được gửi dưới dạng đã mã hóa).

Nó được gửi bởi máy trạm trả lời lại thông báo REQUEST-CERTIFICATE của máy chủ. Nó sẽ cung cấp dữ liệu xác thực của mình cho máy chủ trong thông báo này.

4) CLIENT-FINISH (Trong giai đoạn 2;được gửi dưới dạng đã mã hóa).

Máy trạm gửi thông báo này khi nó đồng ý với máy chủ. Máy trạm phải tiếp tục lắng nghe máy chủ cho tới khi nó nhận được thông báo SERVER-FINISH. Số liệu CONNECTION-ID là định danh kết nối ban đầu mà máy chủ gửi trong thông báo SERVER-HELLO và được mã hóa sử dụng khóa của phiên làm việc đã đồng ý.

Client phải gửi thông báo lại sau khi nó đã nhận được thông báo SERVER-HELLO. Nếu thông báo SERVER-HELLO có cờ SESSION-ID-HIT là khác 0 thì máy trạm gửi thông báo CLIENT-FINISH. Ngược lại, thông báo CLIENT-FINISH sẽ được gửi sau thông báo CLIENT-MASTER-KEY.

2.2.6. Các thông báo từ phía máy chủ

1) SERVER-HELLO (Trong giai đoạn 1; được gửi dưới dạng không mã hóa).

Máy chủ gửi lại thông báo này cho máy trạm sau khi nhận được thông báo CLIENT-

HELLO. Trong thông báo này có thông tin sau:

Cờ SESSION-ID-HIT: có giá trị khác 0 khi định danh phiên làm việc được gửi từ phía máy trạm được máy chủ tìm thấy trong bộ nhớ của nó. Ngược lại, nó bằng 0. Khi cờ này khác 0, máy chủ và máy trạm tính toán cặp khóa của phiên làm việc mới dựa trên giá trị khóa mã chủ. Chú ý rằng:

SERVER-READ-KEY = CLIENT-WRITE-KEY

SERVER-WRITE-KEY = CLIENT-READ-KEY

Trong thông báo này có giá trị CONNECTION-ID là giá trị ngẫu nhiên được dùng bởi máy chủ và máy trạm trong nhiều mục đích.

2) SERVER-VERIFY (Trong giai đoạn 1;được gửi dưới dạng đã mã hóa).

Máy chủ gửi thông báo này sau khi cặp khóa của phiên làm việc (SERVER-READ-KEY và SERVER-WRITE-KEY) đã được tạo. Thông báo nay bao gồm bản sao đã được mã hóa của dữ liệu CHALLENGE-DATA được gửi từ máy trạm trong thông báo CLIENT-HELLO. Máy trạm sẽ giải mã CHALLENGE-DATA và kiểm tra với giá trị ban đầu của số liệu này. Nếu không đúng, liên kết sẽ được kết thúc từ phía máy trạm. Thông báo này được gửi sau khi máy chủ nhận được thông báo CLIENT-MASTER-KEY.

3) SERVER-FINISH (Trong giai đoạn 2;được gửi dưới dạng đã mã hóa)

Máy chủ gửi thông báo này sau khi nó và máy trạm đã thoả thuận xong quá trình bắt tay và sẵn sàng phục vụ các ứng dụng ở lớp trên. Trong thông báo này có giá trị SESSION-ID-DATA nó sẽ được lưu vào bộ nhớ của cả máy chủ và máy trạm như là giá trị định danh của phiên làm việc. Đồng thời khóa mã chủ (được lấy từ thông báo CLIENT-MASTER-KEY cũng được lưu vào bộ nhớ của cả hai máy. Thông báo này phải được gửi sau thông báo SERVER-VERIFY.

4) REQUEST-CERTIFICATE (Trong giai đoạn 2;được gửi dưới dạng đã mã hóa).

Máy chủ có thể gửi thông báo này trong giai đoạn 2 khi nó yêu cầu bản xác thực của máy trạm. Máy trạm trả lời bằng thông báo CLIENT-CERTIFICATE nếu nó có thể cung cấp được xác thực của mình, ngược lại máy trạm sẽ trả lời bằng thông báo lỗi NO-CERTIFICATE-ERROR.

Thông báo này có thể gửi sau thông báo SERVER-VERIFY và trước thông báo SERVER-FINISH.

3. KẾT LUẬN

Giao thức SSL cho phép xác thực máy chủ, máy trạm và mã hóa thông tin trong các phiên liên lạc giữa máy chủ và máy trạm trên Internet. Nó được sử dụng rộng rãi trong các ứng dụng thương mại điện tử (E-Commerce). Tuy nhiên với mô hình sử dụng SSL cài đặt trên máy chủ và máy trạm có nhược điểm lớn là nó làm giảm khả năng đáp ứng của máy chủ. Ví dụ với dịch vụ sử dụng HTTP, thí nghiệm đã đo được:

Với máy chủ SunE450 - CPU tốc độ 250 MHz:

- Số yêu cầu máy chủ phục vụ được trước khi cài SSL là 350 yêu cầu/giây.
- Số yêu cầu máy chủ phục vụ được sau khi cài SSL là 04 yêu cầu/giây.

Với máy chủ sử dụng Chip Intel PII - CPU tốc độ 333 MHz:

- Số yêu cầu máy chủ phục vụ được trước khi cài SSL là 550 yêu cầu/giây.
- Số yêu cầu máy chủ phục vụ được sau khi cài SSL là 41 yêu cầu/giây.

Để khắc phục nhược điểm trên, các hãng sản xuất thiết bị truyền thông tích hợp SSL vào trong thiết bị, nó sẽ không làm giảm khả năng đáp ứng của máy chủ. Một số sản phẩm phải được kể đến là:

- *Content Service Switch CSS 11000 của Hãng CISCO*
- *Intel NetStructure 7110, 7180 của Hãng Intel*
- *SonicWall SSl-R3 , SonicWall SSl-R6 của Hãng SonicWall*

Hiện nay ở Việt Nam, thương mại điện tử đang bắt đầu được quan tâm phát triển. Đối với các ứng dụng trên Internet dùng cho thương mại điện tử nói riêng hoặc có yêu cầu bảo mật dữ liệu cao nói chung, việc sử dụng SSL là một giải pháp hữu hiệu. Giải pháp này có ưu điểm lớn là đơn giản và thuận tiện. Tại đầu cuối, các trình duyệt WEB thông dụng hiện nay (của hãng Microsoft, Netscape...) đều đã hỗ trợ SSL. Các nhà cung cấp dịch vụ chỉ cần cài đặt SSL ở phía máy chủ. Với các ứng dụng có quy mô nhỏ (mức truy cập trong khoảng 20-30 truy cập/giây) có thể sử dụng giải pháp dùng SSL cài trực tiếp lên máy chủ. Với các ứng dụng có quy mô lớn hơn có thể sử dụng các thiết bị SSL chuyên dụng.

TÀI LIỆU THAM KHẢO

[1] CCITT. Recommendation X.208: *"Specification of Abstract Syntax Notation One"* (ASN.1) 1988.

[2] CCITT. Recommendation X.209: *"Specification of Basic Encoding Rules for Abstract Syntax Notation One"* (ASN.1) 1988.

[3] CCITT. Recommendation X.509: *"The Directory - Authentication Framework"*, 1988.

[4] CCITT. Recommendation X.520: *"The Directory - Selected Attribute Types"*, 1988.

[5] Kipp E.B. Hickman, Netscape Communications Corp., Secure Sockets Layer Protocol.

[6] R. Rivest. RFC 1321: The MD5 Message Digest Algorithm. April 1992.

[7] R. Rivest. RFC 1319: The MD2 Message Digest Algorithm. April 1992.

[8] B. Schneier., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Published by John Wiley & Sons, Inc. 1994.

[9] Tim Parker,*Teach yourself TCP/IP*, Published by Sams Publishing, 1996.

Nhận bài ngày 15 - 3 - 2003