

AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình
Bộ môn Kỹ thuật máy tính & mạng
<http://dhthuyloi.blogspot.com>

Chương 4:

CÁC ỨNG DỤNG TRONG AN NINH MẠNG

- ◆ Các ứng dụng chứng thực
- ◆ An ninh Web
- ◆ An ninh giao dịch điện tử

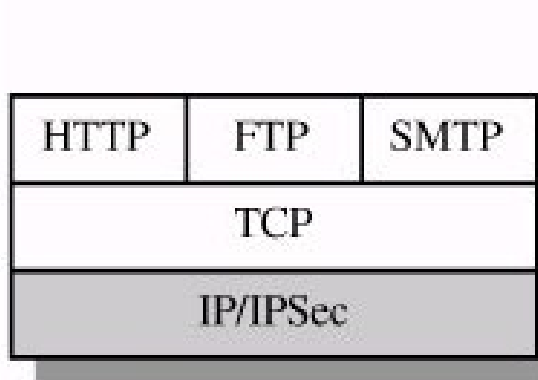
Bài 4.2 An ninh Web

- ◆ World Wide Web về cơ bản là một ứng dụng client/server qua TCP/IP Internet và TCP/IP nội mạng (intranet).
- ◆ Khi người dùng sử dụng dịch vụ Web, một kết nối giữa trình duyệt (client) và máy chủ Web (server) được thiết lập. Dữ liệu sẽ được truyền qua lại giữa client và server
- ◆ Kẻ tấn công có thể xem lén các giao vận mạng giữa trình duyệt và server, nhằm ăn cắp thông tin và thực hiện các hành vi bất hợp pháp

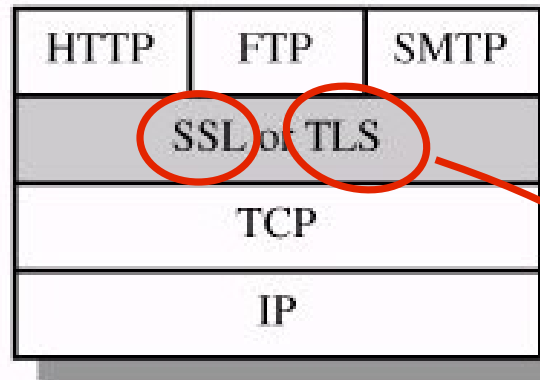
- ◆ Cần có cơ chế mã hoá để bảo mật cho dữ liệu truyền giữa client và server.
- ◆ Cần có giải pháp chứng thực để bảo vệ server trước nguy cơ tấn công của những kẻ giả mạo, và bảo vệ người dùng trước sự nguy hiểm của các trang web không an toàn

Có nhiều giải pháp an ninh cho Web ở nhiều cấp độ khác nhau:

màu xám: được mã hoá



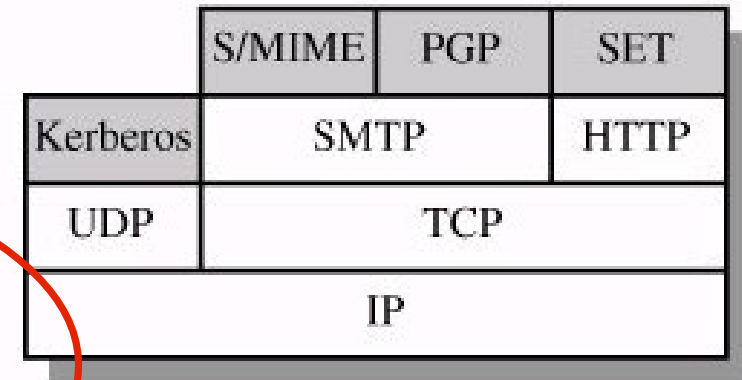
(a) Tầng mạng



(b) Tầng chuyển vận

phù hợp cho thiết lập an ninh web

Transport Layer Service



(c) Tầng ứng dụng

Giải pháp an ninh ở tầng Network (tầng Mạng)


- ◆ Sử dụng hệ thống giao thức bảo mật IPSec (IP Security - Bảo mật tầng IP)
- ◆ Đây là giải pháp bảo mật chung, hoàn toàn trong suốt đối với các ứng dụng và người dùng

Giải pháp an ninh ở tầng Transport (tầng Chuyển vận)

- ◆ Sử dụng SSL (Secure Sockets Layer) hoặc TLS (Transport Layer Service)
- ◆ Có thể triển khai SSL (hoặc TLS) thành một bộ phận của bộ giao thức nền, tách biệt hẳn với các ứng dụng.
- ◆ Hoặc nhúng SSL vào các gói phần mềm cụ thể. Ví dụ: Các trình duyệt Netscape và Microsoft Explorer được trang bị SSL, và hầu hết các server Web đều hỗ trợ SSL.

Giải pháp an ninh ở tầng Application (tầng Ứng dụng)

- ◆ Các dịch vụ an ninh được nhúng vào trong từng ứng dụng cụ thể.
- ◆ Ví dụ: Để đảm bảo an ninh cho ứng dụng giao dịch điện tử, người ta có thể sử dụng SET (Secure Electronic Transaction); để đảm bảo an ninh cho ứng dụng thư điện tử, người ta thường dùng PGP hoặc S/MIME.



◆ Phần tiếp theo sẽ tập trung chủ yếu vào
SSL (Secure Sockets Layer).

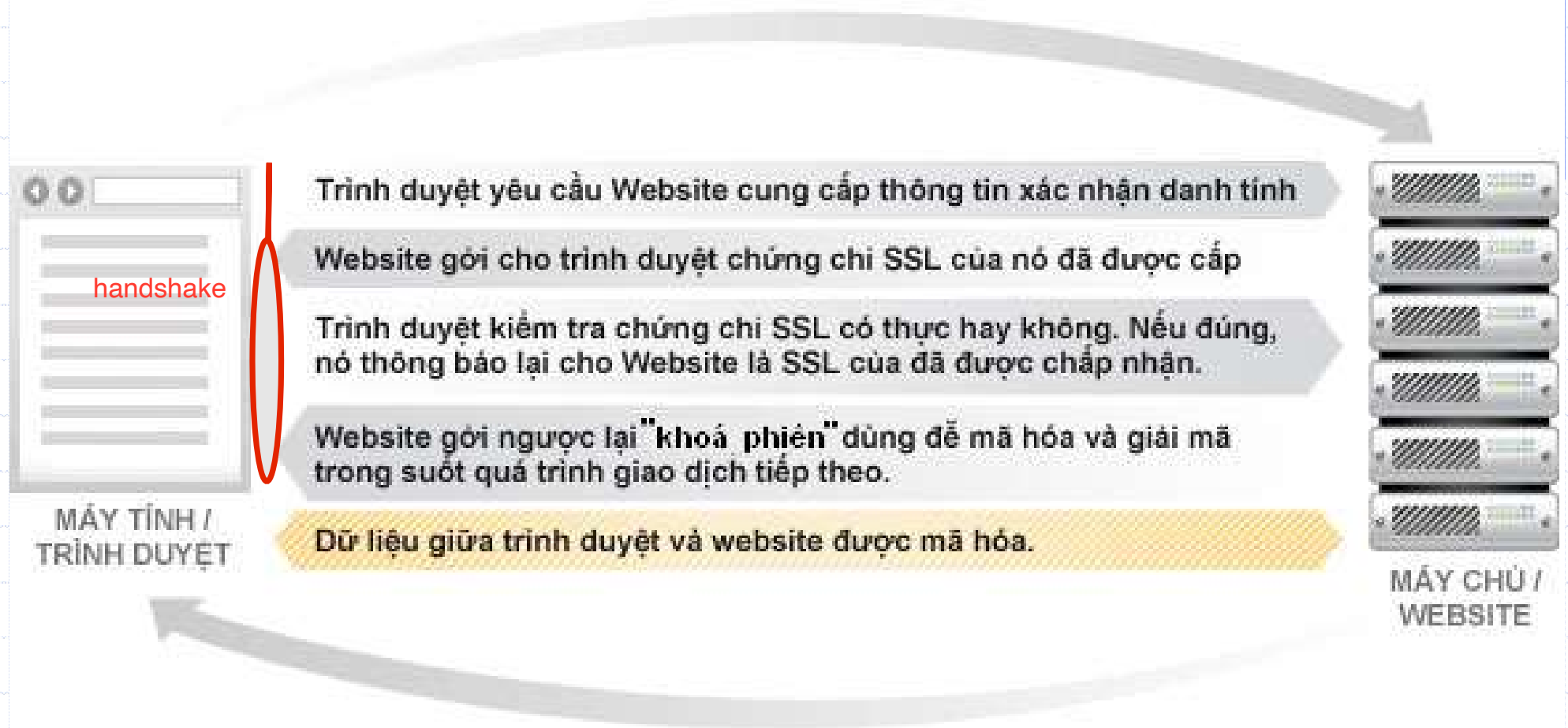
SSL (Secure Socket Layer)

- ◆ SSL một tiêu chuẩn của công nghệ bảo mật, tạo ra một liên kết được mã hóa giữa máy chủ web và trình duyệt.
- ◆ Liên kết này đảm bảo tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn.
- ◆ SSL được sử dụng rộng rãi trên hàng triệu Website ở khắp thế giới, giúp bảo vệ dữ liệu an toàn trên môi trường internet

SSL cung cấp những gì?

- ◆ Sự bảo mật: Các dữ liệu truyền tải giữa máy chủ và trình duyệt sẽ được mã hoá, đảm bảo tính riêng tư và toàn vẹn .
- ◆ Khả năng chứng thực: Mỗi chứng chỉ số SSL được tạo ra cho một Website duy nhất, khẳng định độ tin cậy của Website đó.
- ◆ Một cơ quan uy tín sẽ xác thực danh tính và độ tin cậy của Website trước khi cấp chứng chỉ SSL cho Website.

Kết nối an toàn bằng SSL



Cách nhận biết một Website tin cậy:

- ◆ Địa chỉ Website có dạng *https://...*
- ◆ Có biểu tượng ổ khoá an toàn trên thanh địa chỉ, gắn với tên của một tổ chức xác thực đáng tin cậy (ví dụ như Symantec Corporation, GeoTrust Inc...)

Tập tin Chính sách Hiện thị Nhật ký duyệt web Đồng đầu trang Dụng cụ Trợ giúp

Adayroi | Trung tâm thương mại

VINCOMMERCE GENERAL C (VN) https://www.adayroi.com

VINCOMMERCE GENERAL
COMMERCIAL SERVICES
JOINT STOCK COMPANY
Kết nối an toàn

You are securely connected to this site, owned by:

**VINCOMMERCE GENERAL
COMMERCIAL SERVICES JOINT
STOCK COMPANY**
Ho Chi Minh
Ho Chi Minh, VN

Xác minh bởi: GlobalSign nv-sa

Thùng tin thòm

Thực Phẩm - Tiêu Dùng

Mobile & Tablet

VINMEC

VINGROUP

VINSCHOOL

Thẻ VinID Bán hàng cùng

thương hiệu bạn r **Tìm kiếm**

LƯU THÔNG TIN TÍCH THÊM 10% V

Áp dụng đồng th mã giảm giá

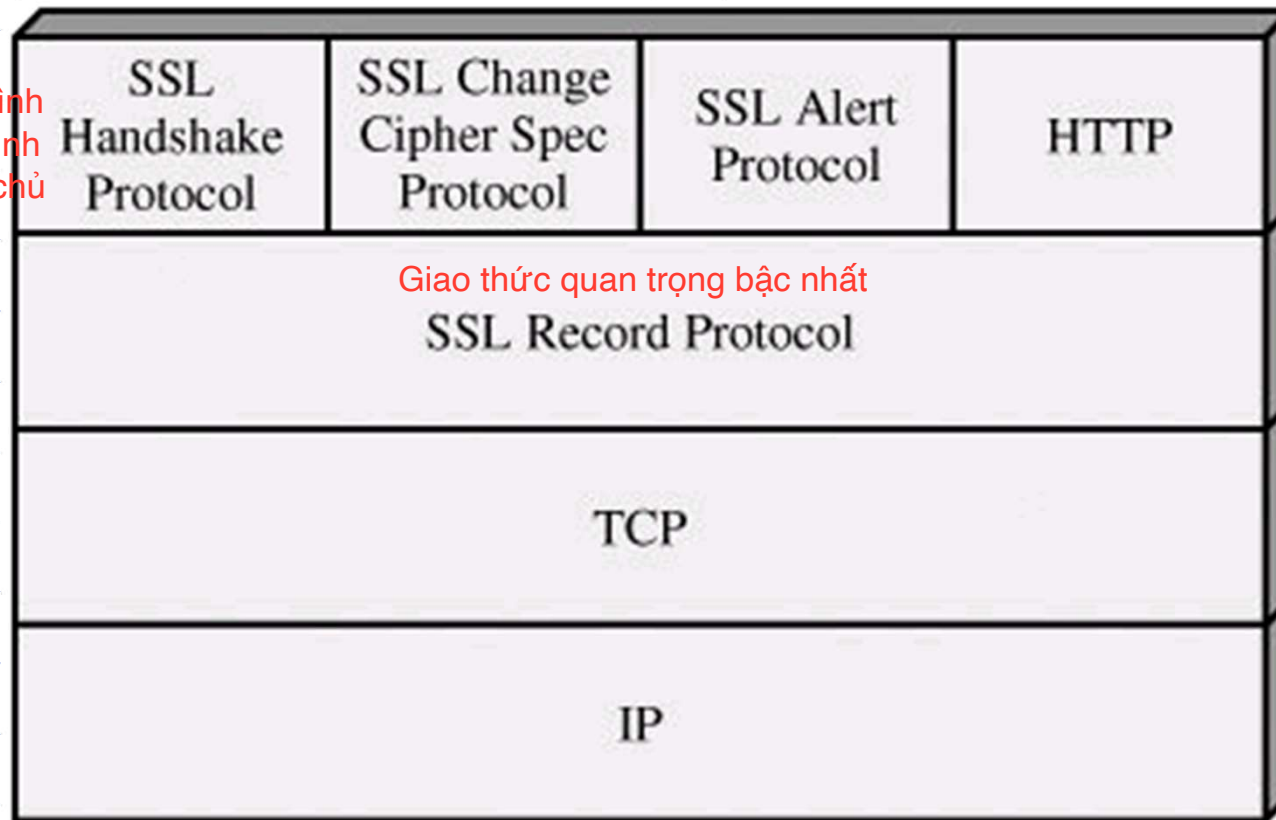
Tri ân
Thầy Cô 20-11

LOA BLUETOOTH LG PH1

Kiến trúc SSL

- ◆ SSL là một bộ giao thức, được triển khai trên hai tầng:

thiết lập quá trình
kết nối giữa trình
duyet và máy chủ



- ◆ Giao thức **SSL Record** cung cấp các dịch vụ an ninh cơ bản cho các giao thức khác nhau của tầng trên
- ◆ Ba giao thức SSL ở tầng trên gồm có: **SSL Handshake**, **Change Cipher Spec**, và **Alert**

Giao thức SSL Record (tạo ra các bản ghi SSL)



Dữ liệu ứng dụng

Dữ liệu tại tầng ứng dụng, chưa được mã hoá

1. Dữ liệu được đẩy xuống tầng transport

1. Phân đoạn

Dữ liệu được phân đoạn thành các khúc = nhau

2. Nén

2. Nén các đoạn đó lại => làm dữ liệu nhỏ lại, tăng tốc độ truyền

5 bước thiết lập kết nối

3. Nối với MAC

3. Lấy dữ liệu nén + ghép với mã MAC: đem toàn bộ dữ liệu đã nén đi qua hàm MAC
=> mục đích xác thực nội dung của thông tin xem có bị thay đổi trên đường truyền hay không

4. Mã hóa

4. Mã hoá (bảo mật): dùng khoá phiên (đã được trao đổi ở handshake)

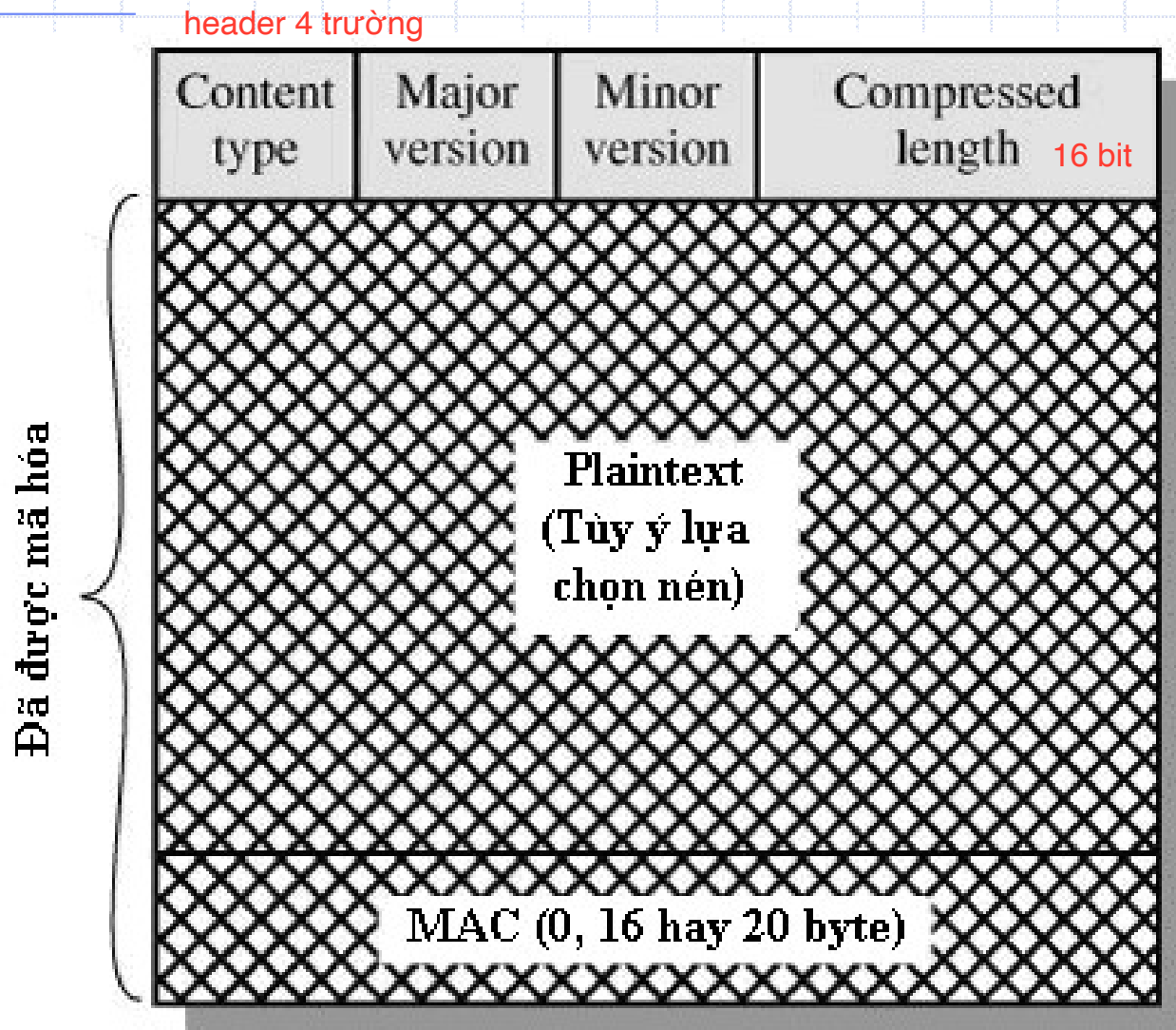
5. Chèn header bản ghi SSL

5. Ghép header: để nhận dạng được đây là gói tin SSL

Giải thích:

1. Dữ liệu từ tầng ứng dụng bên trên sẽ được chia thành các khối có kích thước không quá 2^{14} byte.
2. Mỗi khối có thể được nén để thu nhỏ kích thước (hoặc không nén).
3. Tính toán mã MAC của mỗi khối nói trên (tương tự mã Hash, nhưng có thêm mật khoá để bảo vệ). Sau đó giá trị MAC sẽ được ghép vào cuối khối.
4. Thực hiện mã hoá đối xứng với từng khối.
5. Chèn thêm phần Header vào đầu mỗi khối

Kết quả: Ta thu được các bản ghi SSL (ứng với mỗi khối) có dạng như sau:



- ◆ Các bản ghi SSL sẽ được chuyển xuống lớp TCP bên dưới để thực hiện truyền gửi ở lớp thấp hơn.
- ◆ Phần Header của mỗi bản ghi có 4 trường: **Content Type, Major Version, Minor Version, và Compressed Length.**

- ◆ **Content Type (8 bit):** Giao thức tầng trên sử dụng để xử lý phân đoạn bao ngoài.
- ◆ **Major Version (8 bit):** Biểu thị phiên bản chính của SSL đang dùng. Với SSLv3, giá trị là 3.
- ◆ **Minor Version (8 bit):** Biểu thị phiên bản phụ đang dùng. Với SSL, giá trị là 0.
- ◆ **Compressed Length (16 bit):** Chiều dài, tính bằng byte, của phân đoạn plaintext (hay phân đoạn nén nếu thi hành nén). Giá trị tối đa là $2^{14} + 2048$.

◆ Phương pháp nén, thuật toán mã hóa, thuật toán MAC và các khóa mật mã cần dùng để bảo vệ dữ liệu truyền gửi trong bản ghi SSL được quy định bởi giao thức **Handshake** ở tầng trên.

Giao thức SSL Handshake

(thiết lập kết nối giữa client và server)

- ◆ Giao thức Handshake (bắt tay) được sử dụng để thiết lập kết nối trước khi truyền dữ liệu đi
- ◆ Giao thức này cho phép server và client chứng thực lẫn nhau để cùng dàn xếp một kỹ thuật mã hóa, thuật toán MAC và các khóa mật mã cần dùng để bảo vệ dữ liệu truyền gửi trong bản ghi SSL

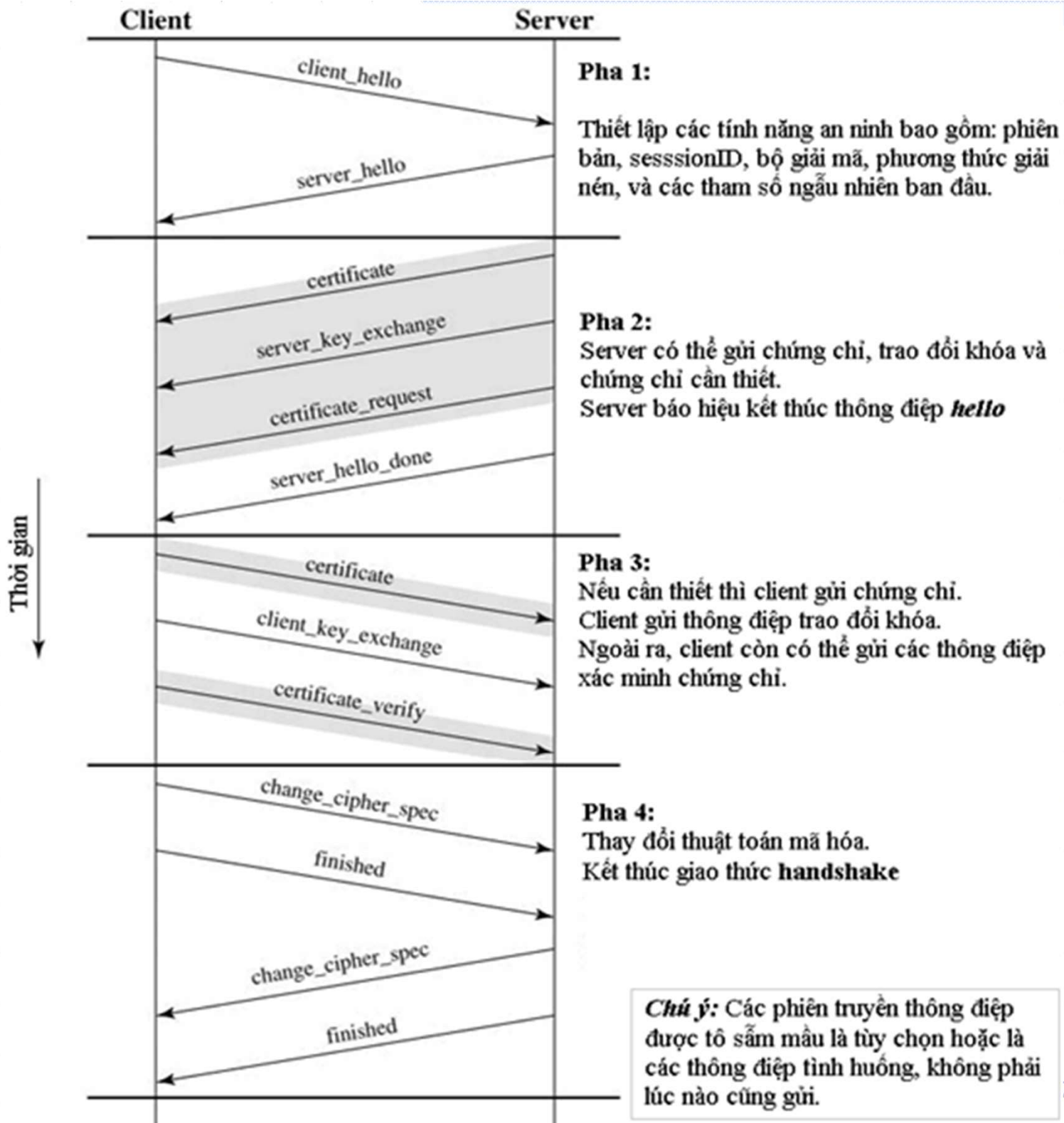
◆ Giao thức Handshake gồm một loạt thông điệp được trao đổi giữa client và server. Tất cả các thông điệp này đều có 3 trường như sau:



- ◆ **Type (1 byte):** Loại thông điệp, biểu thị một trong 10 loại thông điệp của giao thức Handshake.
- ◆ **Length (3 byte):** Chiều dài thông điệp tính bằng byte.
- ◆ **Content (≥ 0 byte):** Các tham số kết hợp với thông điệp này.

Hoạt động của giao thức Handshake

- ◆ Quá trình trao đổi thông điệp để thiết lập một kết nối logic giữa client và server được trình bày ở hình vẽ sau (quá trình này được chia thành bốn pha):



- ◆ Khi pha 4 hoàn thành, giao thức Handshake kết thúc, một kết nối an toàn được thiết lập, client và server có thể bắt đầu truyền dữ liệu tầng ứng dụng
- ◆ Công việc tiếp theo là của giao thức SSL Record, giao thức này sẽ thực hiện quá trình phân đoạn, nén, tính MAC, mã hoá... đối với dữ liệu ứng dụng như đã trình bày ở phần trước.

Giao thức SSL Alert (gửi các thông báo lỗi)

- ◆ Giao thức này dùng để gửi các thông điệp báo lỗi khi có lỗi xảy ra.
- ◆ Thông điệp của giao thức này có 2 trường như sau:



◆ Byte thứ nhất (**Level**): Chứa mức độ nghiêm trọng của lỗi.

+ Nếu Level = “*warning*”: Lỗi không nghiêm trọng

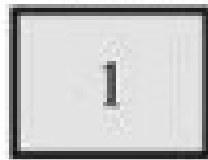
+ Nếu Level = “*fatal*”: Lỗi nghiêm trọng đã xảy ra

◆ Byte thứ hai (**Alert**): Chứa mã lỗi.

Giao thức SSL Change Cipher Spec (thay đổi phương pháp mã hoá)

- ◆ Giao thức này chỉ gửi một thông điệp duy nhất (thông điệp đó dài 1 byte và chứa giá trị bằng 1), có tác dụng cập nhật thuật toán mã hoá mới (cùng khoá mới và các tham số mới) cho kết nối hiện tại.
- ◆ Giao thức này thường được dùng kèm với pha 4 của giao thức Handshake.

1 byte



Hết Phần 4_2