Chương 8

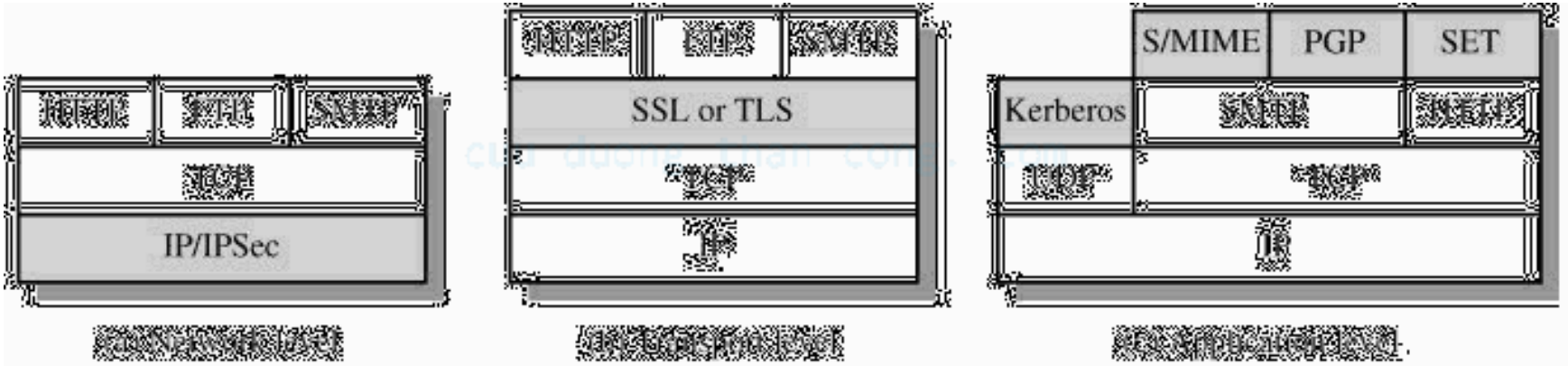
# AN TOÀN WEB

# Vấn đề an ninh Web (1)

- Web được sử dụng rộng rãi bởi các công ty, tổ chức, và các cá nhân
- Các vấn đề đặc trưng đối với an ninh Web
  - Web dễ bị tấn công theo cả hai chiều
  - Tấn công Web server sẽ gây tổn hại đến danh tiếng và tiền bạc của công ty
  - Các phần mềm Web thường chứa nhiều lỗi an ninh
  - Web server có thể bị khai thác làm căn cứ để tấn công vào hệ thống máy tính của một tổ chức
  - Người dùng thiếu công cụ và kiến thức để đối phó với các hiểm họa an ninh

# Vấn đề an ninh Web (2)

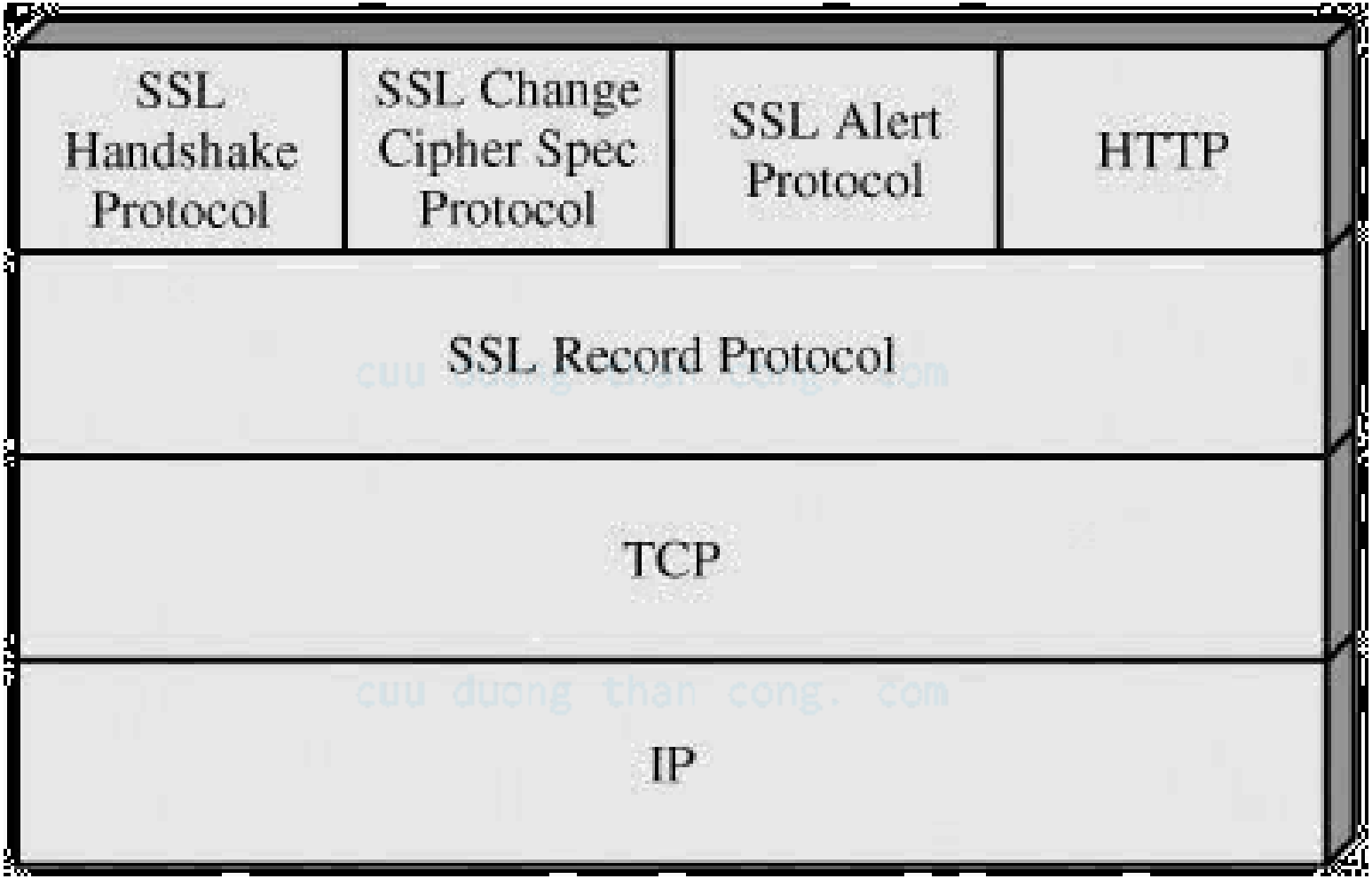
- Các hiểm họa đối với an ninh Web
  - Tính toàn vẹn
  - Tính bảo mật
  - Từ chối dịch vụ
  - Xác thực
- Các biện pháp an ninh Web



# SSL

- Là một dịch vụ an ninh ở tầng giao vận
- Do Netscape khởi xướng
- Phiên bản 3 được công bố dưới dạng bản thảo Internet
- Trở thành chuẩn TLS
  - Phiên bản đầu tiên của TLS ≈ SSLv3.1 tương thích ngược với SSLv3
- Sử dùng TCP để cung cấp dịch vụ an ninh từ đầu cuối tới đầu cuối
- Gồm 2 tầng giao thức

# Mô hình phân tầng SSL



# Kiến trúc SSL (1)

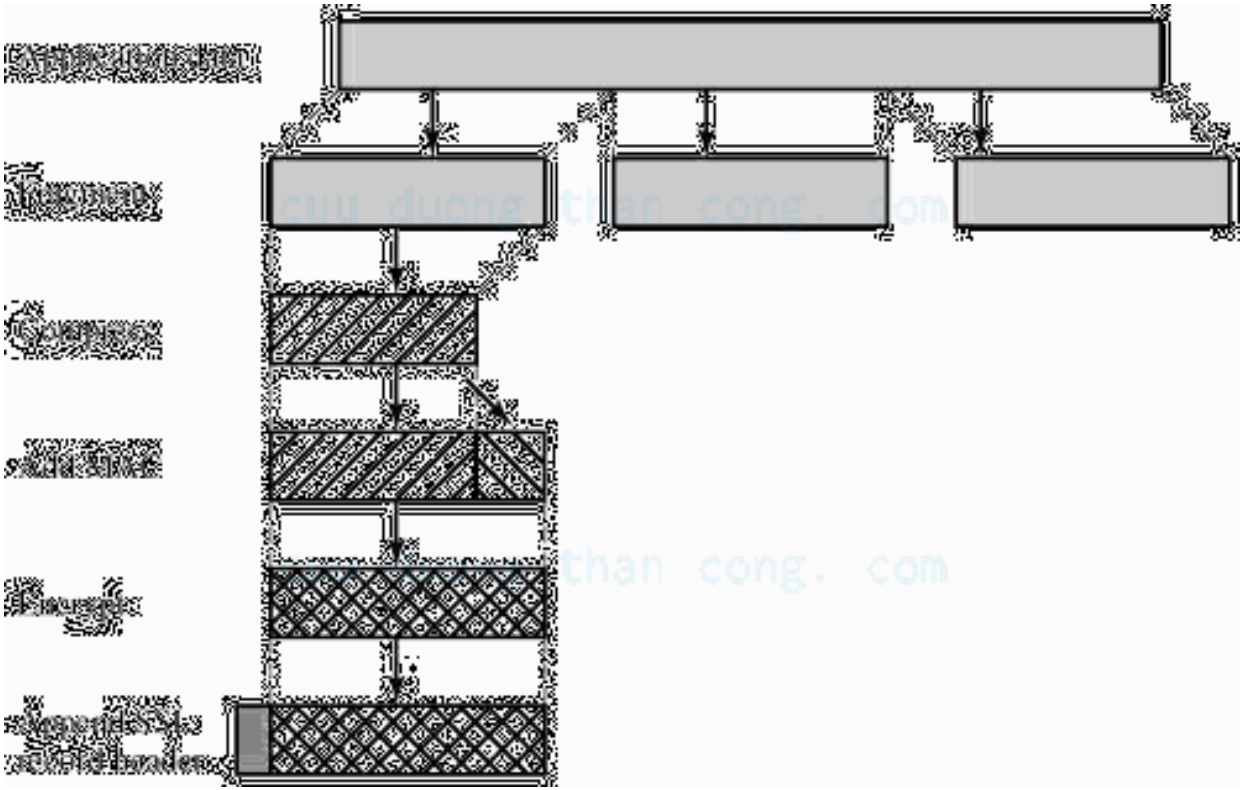
- Kết nối SSL
  - Liên kết giao tiếp từ điểm nút tới điểm nút
  - Mang tính nhất thời
  - Gắn với một phiên giao tác
  - Các tham số xác định trạng thái kết nối
    - Các số ngẫu nhiên chọn bởi server và client
    - Khóa MAC của server
    - Khóa MAC của client
    - Khóa mã hóa của server
    - Khóa mã hóa client
    - Các vector khởi tạo
    - Các số thứ tự

# Kiến trúc SSL (2)

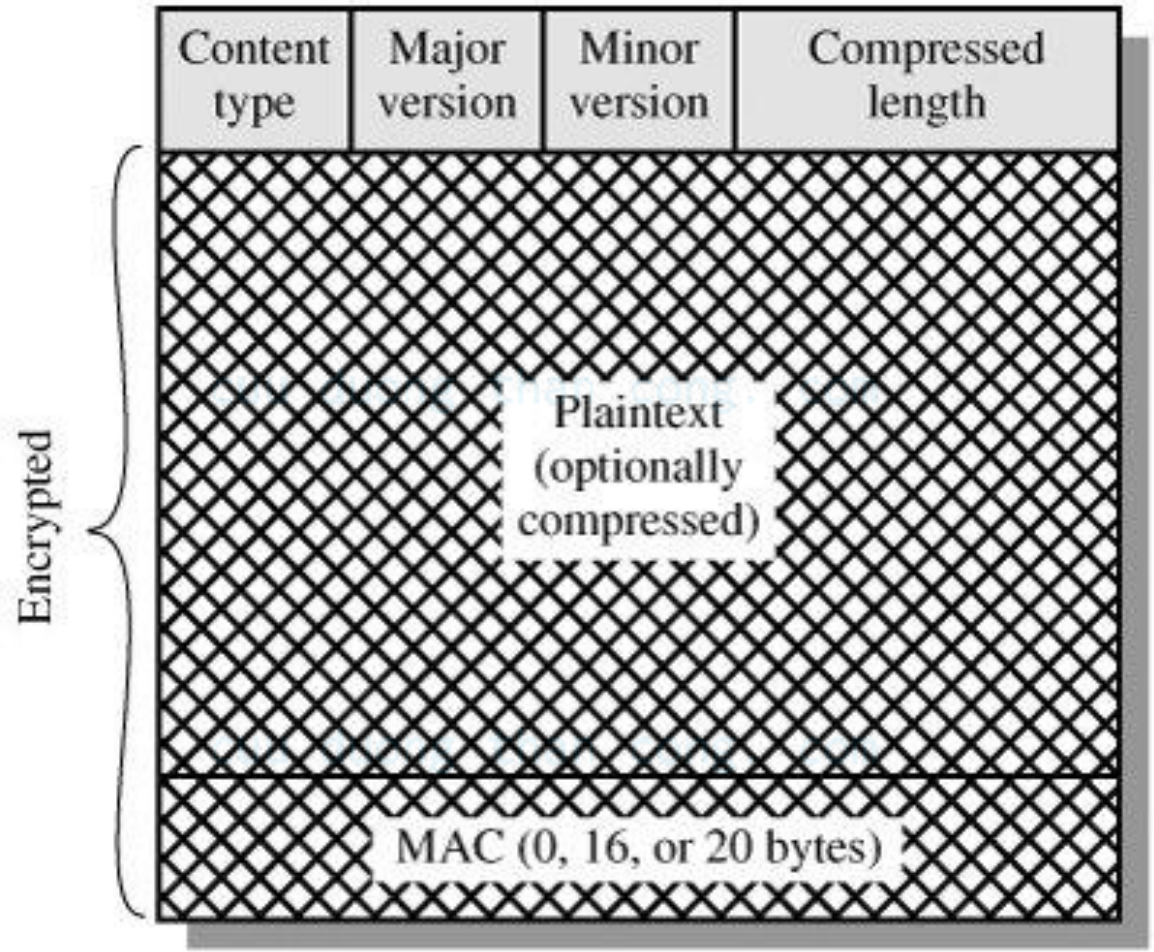
- Phiên SSL
  - Liên kết giữa client và server
  - Tạo lập nhờ giao thức bắt tay
  - Có thể bao gồm nhiều kết nối
  - Xác lập một tập các tham số an ninh sử dụng bởi tất cả các kết nối trong phiên giao tác
    - Định danh phiên
    - Chứng thực điểm nút
    - Phương pháp nén
    - Đặc tả mã hóa
    - Khóa bí mật chủ
    - Cờ có thể tiếp tục hay không

# Giao thức bản ghi SSL

- Cung cấp các dịch vụ bảo mật và xác thực
  - Khóa bí mật chung do giao thức bắt tay xác lập



# Khuôn dạng bản ghi SSL



# Giao thức đổi đặc tả mã hóa SSL

- Một trong ba giao thức chuyên dụng SSL sử dụng giao thức bản ghi SSL
- Chỉ gồm một thông báo chứa một byte dữ liệu có giá trị là 1
- Khiến cho trạng thái treo trở thành trạng thái hiện thời
  - Cập nhật đặc tả mã hóa cho kết nối

# Giao thức báo động SSL

- Dùng chuyển tải các báo động liên quan đến SSL tới các thực thể điểm nút
- Mỗi thông báo gồm 2 byte
  - Byte thứ nhất chỉ mức độ nghiêm trọng
    - Cảnh báo : có giá trị là 1
    - Tai họa : có giá trị là 2
  - Byte thứ hai chỉ nội dung báo động
    - Tai họa : unexpected_message, bad_record_mac, decompression_failure, handshake_failure, illegal_parameter
    - Cảnh báo : close_notify, no_certificate, bad_certificate, unsupported_certificate, certificate_revoked, certificate_expired, certificate_unknown

# Giao thức bắt tay SSL

- Cho phép server và client
  - Xác thực lẫn nhau
  - Thỏa thuận các giải thuật mã hóa và MAC
  - Thỏa thuận các khóa mật mã sẽ được sử dụng
- Gồm một chuỗi các thông báo trao đổi giữa client và server
- Mỗi thông báo gồm 3 trường
  - Kiểu (1 byte)
  - Độ dài (3 byte)
  - Nội dung ([redacted] byte)

# TLS

- Là phiên bản chuẩn Internet của SSL
  - Mô tả trong RFC 2246 rất giống với SSLv3
  - Một số khác biệt nhỏ so với SSLv3
    - Số phiên bản trong khuôn dạng bản ghi SSL
    - Sử dụng HMAC để tính MAC
    - Sử dụng hàm giả ngẫu nhiên để khai triển các giá trị bí mật
    - Có thêm một số mã báo động
    - Không hỗ trợ Fortezza
    - Thay đổi trong trao đổi chứng thực
    - Thay đổi trong việc sử dụng dữ liệu đệm