Thời gian : 120 phút
Lớp INT3307

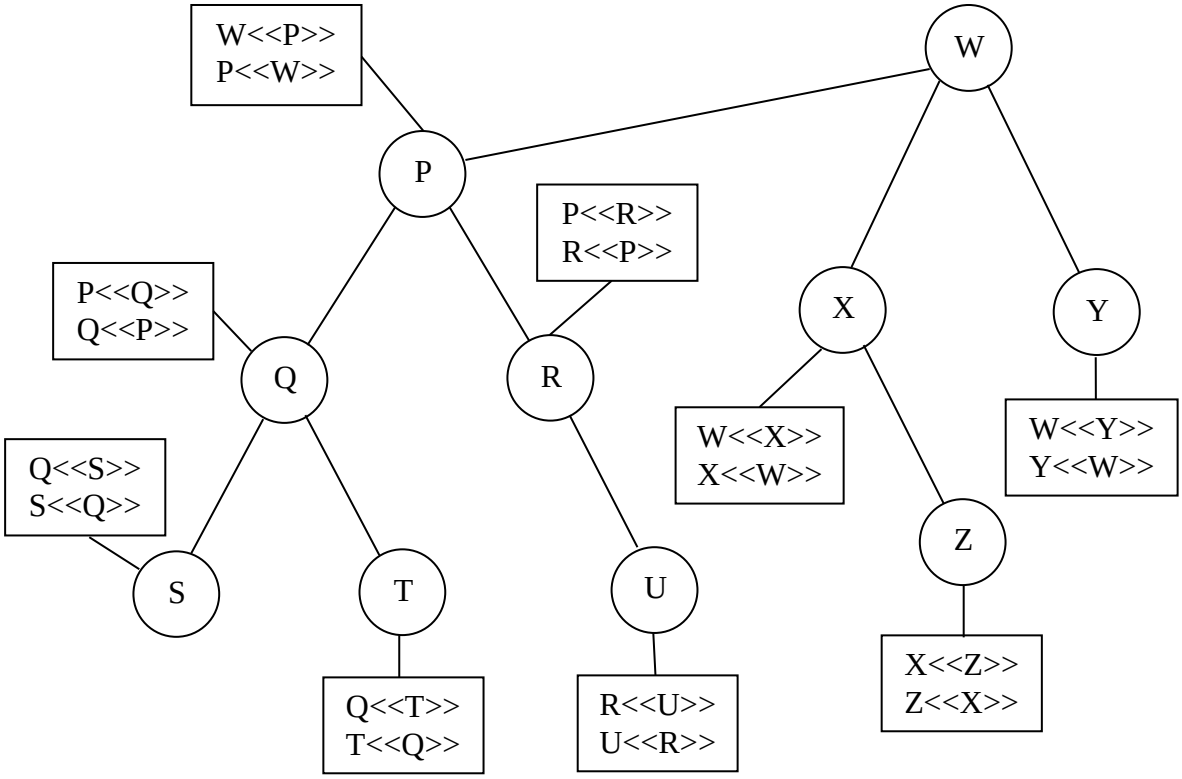
Được phép tra cứu tất cả các loại tài liệu
Không được cho người khác mượn tài liệu dưới bất kỳ hình thức nào

Đáp án đề thi số 1
An toàn và an ninh mạng

(4 câu, 3 trang, thang điểm 10)

1. Chứng thực X.509 (2 điểm)

Xét dịch vụ xác thực X.509. Cho một mô hình phân cấp các cơ quan chứng thực với các chứng thực lẫn nhau được mô tả như hình vẽ dưới đây.



Một người dùng A có chứng thực do Y cấp. Một người dùng B có chứng thực do Q cấp. Hãy cho biết chuỗi các chứng thực lẫn nhau và cách thức cho phép A xác minh và tin cậy được vào chứng thực của B.

Nếu chứng thực của A và chứng thực của B có cùng khóa công khai thì có vấn đề gì về an ninh không? Giải thích.

Đáp án

Chuỗi các chứng thực lẫn nhau: Y<<W>>W<<P>>P<<Q>>Q<<B>>

Cách thức cho phép A xác minh và tin cậy được vào chứng thực của B do Q cấp: A có chứng thực do Y cấp nên có khóa công khai hợp lệ của Y và tin cậy vào Y; A sử dụng khoá công khai hợp lệ của Y để kiểm tra Y<<W>>. Nếu Y<<W>> hợp lệ thì A có khoá công khai hợp lệ của W. A sử dụng khoá… Cứ như vậy thì A sẽ có khoá công khai hợp lệ

của Q và sử dụng nó để xác minh Y<<B>>. Nếu hợp lệ thì A sẽ có khoá công khai hợp lệ của B.

do đó A có thể xác minh được chứng thực của W do Y cấp đúng là chứa khóa công khai hợp lệ của W, đồng thời tin cậy vào W; tương tự như vậy từ chứng thực của P do W cấp A có khóa công khai hợp lệ của P và tin cậy vào P; từ chứng thực của Q do P cấp A có khóa công khai hợp lệ của Q và tin cậy vào Q; cuối cùng A xác minh và tin cậy được vào chứng thực của B do Q cấp.

2. An toàn mức giao vận (3 điểm)

Trong một ứng dụng Web, hai bên client và server sử dụng giao thức Handshake trong chuỗi giao thức SSL để xác thực lẫn nhau và thỏa thuận các tham số an ninh (các giải thuật và khóa mật mã). Giả sử phương pháp trao đổi khóa được client và server thống nhất sử dụng sau khi trao đổi các thông báo *client_hello* và *server_hello* ở giai đoạn 1 là RSA. Tuy nhiên, khóa công khai RSA mà server có sẵn và được chứng thực chỉ có tính năng ký (không thể sử dụng để mã hóa).

a. *(1,5 điểm)*

Vẽ sơ đồ trao đổi thông báo 4 giai đoạn giữa client và server trong giao thức Handshake SSL nêu trên theo cách an toàn nhất có thể.

b. *(1,5 điểm)*

Với mỗi thông báo tùy chọn (tức những thông báo không phải đối với bất kỳ phương pháp trao đổi khóa nào cũng được gửi) và thông báo *client_key_exchange*, hãy chỉ ra nó có những tham số cụ thể gì.

Đáp án

a) *Sơ đồ như hình 5.6 trong sách giáo trình (trang 168 slides bài giảng) với tất cả các thông báo tùy chọn có thể.*

b) *Thông báo certificate do server gửi cho client chứa khóa công khai RSA có sẵn chỉ có tính năng ký của server.*

Thông báo server_key_exchange chứa khóa công khai RSA tức thời do server tạo ra có tính năng mã hóa, khóa này được ký với khóa riêng tương ứng với khóa công khai RSA có sẵn đã gửi trong thông báo certificate.

Thông báo certificate_request chứa các tham số như giải thích ở trang 180 của slides bài giảng.

Thông báo certificate do client gửi cho server chứa một khóa công khai có tính năng ký của client.

Thông báo client_key_exchange chứa khóa phiên do client tạo ra (pre_master_secret) được mã hóa với khóa công khai tức thời có tính năng mã hóa của server.

Thông báo certificate_verify chứa giá trị băm dựa trên các thông báo trước đó (handshake_messages) và master_secret được ký với khóa riêng tương ứng với khóa công khai client đã gửi cho server trong thông báo certificate ở bước 3.

3. An toàn thư điện tử (3 điểm)

Chương trình PGP của một người dùng A lưu giữ vòng khóa công khai có các trường **Public Key**, **User ID**, **Owner Trust**, và **Signatures** như sau:

Public Key	PU_A	PU_B	PU_C	PU_D	PU_E	PU_F	PU_G	PU_H	PU_I
User ID	A	B	C	D	E	F	G	H	I
Owner Trust	*Tột bậc*	*Hoàn toàn*	*Hoàn toàn*	*Một phần*	*Một phần*	*Không tin cậy*	*Hoàn toàn*	*Hoàn toàn*	*Không biết*
Signatures	-	A	B	C	C, D	D, E	E, F	G	H, K

Tính hợp lệ của khóa công khai (**Key Legitimacy)** được PGP tính theo các quy tắc sau:

- Khóa công khai của bản thân người dùng A là *hợp lệ*.
- Nếu một khóa công khai có ít nhất một chữ ký có độ tin cậy (**Signature Trust**) là *tột bậc* thì nó *hợp lệ*.
- Nếu không, tính hợp lệ của khóa công khai được tính bằng tổng trọng số độ tin cậy của các chữ ký. Trọng số 1 được gán cho các chữ ký có độ tin cậy *hoàn toàn*. Trọng số 1/2 được gán cho các chữ ký có độ tin cậy *một phần*. Nếu tổng trọng số đạt tới hoặc vượt ngưỡng là 1 thì khóa công khai được xác định là *hợp lệ*.
- Trong tất cả những trường hợp còn lại, khóa công khai được coi là *không hợp lệ*.

Vẽ mô hình tin cậy PGP tương ứng.

Đáp án

Sơ đồ với 9 vòng tròn tương ứng với các ký hiệu từ A đến I, trong đó các vòng tròn A, B, C, G, và H được tô xám hoàn toàn, các vòng tròn D và E được tô xám một nửa, còn các vòng tròn còn lại không tô (0,75), vòng tròn A có viền kép, các vòng tròn còn lại đều có viền đơn (0,25), vẽ các mũi tên đi từ B đến A, C đến B, D đến C, E đến C và D, F đến D và E, G đến E và F, H đến G, I đến H, và I đến một dấu hỏi chấm (K) (1,00). Các vòng tròn A, B, C, D, E và F có một dấu chấm ở giữa, các vòng tròn còn lại không có dấu chấm (1,00).

4. An toàn IP (2 điểm)

Trong giao thức ESP, để chống tấn công lặp lại, với mỗi liên kết an ninh, bên gửi A duy trì một bộ đếm để đánh số thứ tự cho các gói tin gửi đi, bên nhận B phát hiện các gói tin lặp hoặc đến quá trễ thông qua một cơ chế cửa sổ. Giả sử cửa sổ có kích thước $W = 128$,

số thứ tự lớn nhất B nhận được trong một gói tin hợp lệ cho đến thời điểm hiện tại là N = 199, B mới nhận được các gói tin hợp lệ có số thứ tự lẻ trong khoảng từ 72 đến 199, còn các gói tin có số thứ tự chẵn trong khoảng này thì chưa nhận được. Hãy mô tả kết quả xử lý tại B khi nhận được lần lượt các gói tin sau:

a. *(0,5 điểm)*

Một gói tin hợp lệ có số thứ tự là 72

b. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 73.

c. *(0,5 điểm)*

Một gói tin hợp lệ có số thứ tự là 200.

d. *(0,5 điểm)*

Một gói tin hợp lệ có số thứ tự là 72.

Đáp án

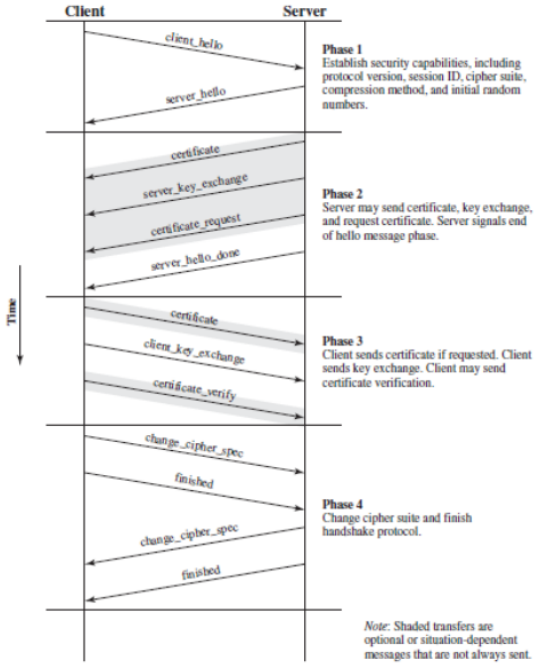
a) *B kiểm tra thấy gói tin nằm trong cửa sổ, chưa được đánh dấu nên kiểm tra MAC của gói tin, thấy hợp lệ nên đánh dấu ô tương ứng với gói tin thứ 72 trong cửa sổ và nhận gói tin*

b) *B kiểm tra thấy gói tin nằm trong cửa sổ và đã được đánh dấu nên loại bỏ gói tin (không cần kiểm tra MAC)*

c) *B kiểm tra thấy gói tin nằm bên phải cửa sổ nên kiểm tra MAC của gói tin, thấy gói tin hợp lệ nên dịch chuyển cửa số một vị trí làm cho ô tận cùng bên trái là 73, ô tận cùng bên phải là 200, ô 200 được đánh dấu, gói tin được nhận.*

d) *B kiểm tra thấy gói tin nằm bên trái cửa sổ nên loại bỏ gói tin.*

Lược đồ giao thức Handshake



Nguyễn Đại Thọ An toàn và an ninh mạng 168