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. Phân phối khóa và xác thực người dùng (2,5 điểm)

a. (1 điểm)

(a) Trao đổi với dịch vụ xác thực : để có thẻ cấp thẻ

(1) $C \rightarrow AS : ID_C \parallel Hệ_C \parallel ID_{tgs} \parallel TS_1$

(2) $AS \rightarrow C : E_{KC}[K_{C,tgs} \parallel Hệ_{tgs} \parallel ID_{tgs} \parallel TS_2 \parallel Hạn_2 \parallel Thẻ_{tgs}]$

$Thẻ_{tgs} = E_{Ktgs}[K_{C,tgs} \parallel Hệ_C \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Hạn_2]$

(b) Trao đổi với dịch vụ cấp thẻ : để có thẻ dịch vụ

(3) $C \rightarrow TGS : ID_V \parallel Thẻ_{tgs} \parallel Dấu_C$

(4) $TGS \rightarrow C : E_{KC,tgs}[K_{C,V} \parallel Hệ_V \parallel ID_V \parallel TS_4 \parallel Thẻ_V]$

$Thẻ_V = E_{KV}[K_{C,V} \parallel Hệ_C \parallel ID_C \parallel AD_C \parallel ID_V \parallel TS_4 \parallel Hạn_4]$

$Dấu_C = E_{KC,tgs}[Hệ_C \parallel ID_C \parallel AD_C \parallel TS_3]$

(c) Trao đổi xác thực client/server : để có dịch vụ

(5) $C \rightarrow V : Thẻ_V \parallel Dấu_C$

(6) $V \rightarrow C : E_{KC,V}[TS_5 + 1]$

$Dấu_C = E_{KC,V}[Hệ_C \parallel ID_C \parallel AD_C \parallel TS_5]$

b. (1,5 điểm)

(1) $C \rightarrow AS : ID_C \parallel Hệ_C \parallel ID_{tgsrem} \parallel TS_1$

(2) $AS \rightarrow C : E_{KC}[K_{C,tgsrem} \parallel Hệ_{tgsrem} \parallel ID_{tgsrem} \parallel TS_2 \parallel Hạn_2 \parallel Thẻ_{tgsrem}]$

$Thẻ_{tgsrem} = E_{Ktgsrem}[K_{C,tgsrem} \parallel Hệ_C \parallel ID_C \parallel AD_C \parallel ID_{tgsrem} \parallel TS_2 \parallel Hạn_2]$

(3) $C \rightarrow TGS_{rem} : ID_{Vrem} \parallel Thẻ_{tgsrem} \parallel Dấu_C$

(4) $TGS_{rem} \rightarrow C : E_{KC,tgsrem}[K_{C,Vrem} \parallel Hệ_{Vrem} \parallel ID_{Vrem} \parallel TS_4 \parallel Thẻ_{Vrem}]$

$Thẻ_{Vrem} = E_{KVrem}[K_{C,Vrem} \parallel Hệ_C \parallel ID_C \parallel AD_C \parallel ID_{Vrem} \parallel TS_4 \parallel Hạn_4]$

$Dấu_C = E_{KC,tgsrem}[Hệ_C \parallel ID_C \parallel AD_C \parallel TS_3]$

(5) $C \rightarrow V_{rem} : Thẻ_{Vrem} \parallel Dấu_C$

(6) $V_{rem} \rightarrow C : E_{KC,Vrem}[TS_5 + 1]$

$Dấu_C = E_{KC,Vrem}[Hệ_C \parallel ID_C \parallel AD_C \parallel TS_5]$

2. An toàn mức giao vận (2,5 điểm)

a. (1 điểm)

Sơ đồ như hình 5.6 trong sách giáo trình (trang 168 của slides bài giảng) với tất cả các thông báo tùy chọn có thể (0,5 điểm).

Thông báo server_key_exchange cho phép client xác thực server (0,25 điểm).

Thông báo certificate_verify cho phép server xác thực client (0,25 điểm).

b. (1,5 điểm)

Thông báo certificate do server gửi cho client chứa khóa công khai DSS có sẵn của server (0,25 điểm).

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 DSS có sẵn của server (0,25 điểm).

Thông báo certificate_request chứa các tham số như giải thích ở trang 180 của slides bài giảng (0,25 điểm).

Thông báo certificate do client gửi cho server chứa một khóa công khai DSS có sẵn của client (0,25 điểm).

Thông báo client_key_exchange chứa khóa phiên do client tạo ra (pre_master_secret) được mã hóa với khóa công khai RSA tức thời của server (0,25 điểm).

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 DSS có sẵn của client (0,25 điểm).

3. An toàn thư điện tử (2,5 điểm)

Sơ đồ với 8 vòng tròn tương ứng với các ký hiệu từ A đến H, trong đó các vòng tròn A, C, E, và F được tô xám hoàn toàn, các vòng tròn D và G được tô xám một nửa, còn các vòng tròn còn lại (B và H) không tô (0,5 điểm), vòng tròn A có viền kép, các vòng tròn còn lại đều có viền đơn (0,25 điểm), vẽ các mũi tên đi từ B đến D, G và I, từ C đến B và D, từ D đến A, từ E đến A và D, từ F đến C, từ G đến E, và từ H đến F và G, lưu ý I là một dấu hỏi chấm chứ không phải một vòng tròn (0,75 điểm). Các vòng tròn A, B, D, E, và G có một dấu chấm ở giữa, các vòng tròn còn lại không có dấu chấm (1,00 điểm).

4. An toàn IP (2,5 điểm)

a. (1 điểm)

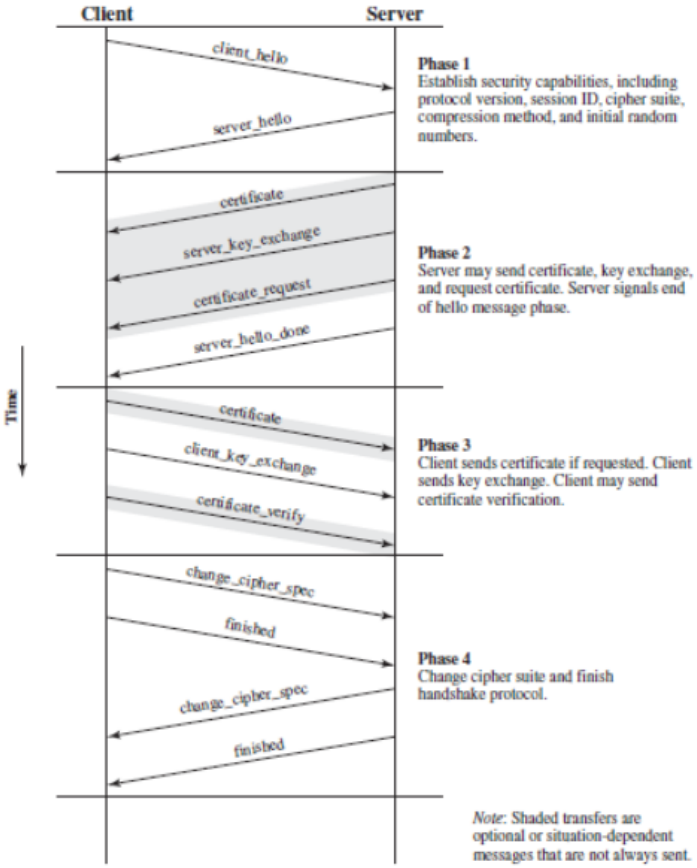
Khuôn dạng như hình 8.8.c IPv4 trang 286 trong sách giáo trình (0,75 điểm). Liên kết an ninh được sử dụng ở chế độ đường hầm (0,25 điểm).

b. (1,5 điểm)

Chống được tất cả các hình thức tấn công (0,75 điểm). Với tấn công sửa đổi dữ liệu do phần dữ liệu nằm trong phạm vi xác thực (0,25 điểm), với tấn công lặp lại cho cơ chế chống tấn công lặp lại sử dụng số thứ tự của tùy chọn xác thực của giao

thức ESP (0,25 điểm), với tấn công đọc trộm dữ liệu do phần dữ liệu nằm trong phạm vi mã hóa (0,25 điểm).

Lược đồ giao thức Handshake



Nguyễn Đại Thọ An toàn và an ninh mạng 168

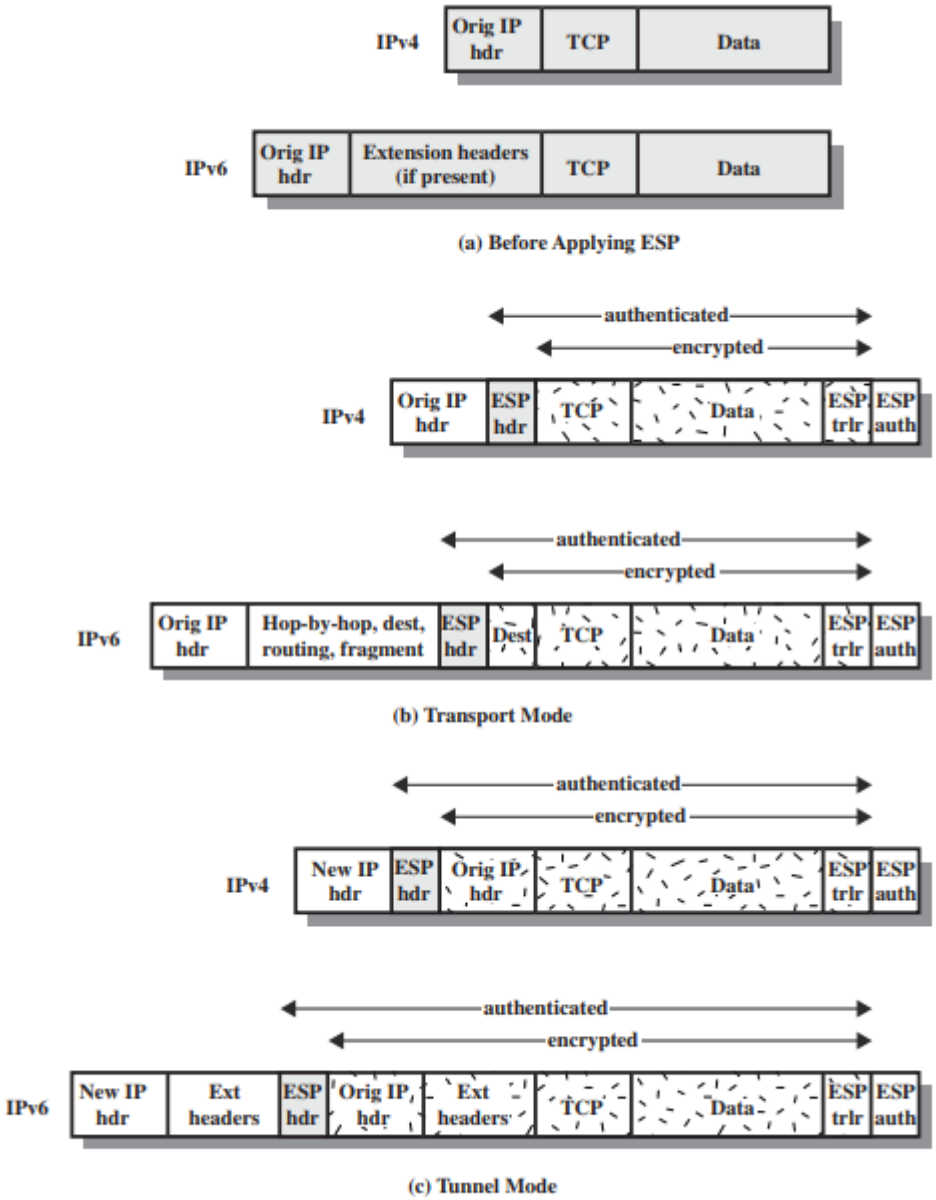


Figure 8.8 Scope of ESP Encryption and Authentication

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

Đề thi số 1
An toàn và an ninh mạng

(4 câu, 2 trang, thang điểm 10)

1. Phân phối khóa và xác thực người dùng (2,5 điểm)

Xét hội thoại xác thực Kerberos 4. Như đã biết, trong trường hợp người dùng thuộc về một phân hệ A muốn truy nhập vào server dịch vụ thuộc về một phân hệ B khác với A thì các bên liên quan bao gồm client C, server xác thực AS của phân hệ A, server cấp thẻ TGS của phân hệ A, server cấp thẻ TGS của phân hệ B và server dịch vụ V của phân hệ B phải trao đổi với nhau tổng cộng 8 thông báo (kể cả thông báo V gửi cho C để C xác thực V).

c. (1 điểm)

Hãy thêm các thông tin $Hệ_C$, $Hệ_{tgs}$ và $Hệ_V$ chỉ phân hệ của người dùng, phân hệ của server cấp thẻ TGS và phân hệ của server dịch vụ V một cách tương ứng vào những chỗ thích hợp trong hội thoại xác thực Kerberos 4 để tổng số thông báo trao đổi trong trường hợp truy nhập liên phân hệ giảm xuống còn 6. Yêu cầu đặt ra là giữ nguyên các thông tin khác của hội thoại Kerberos 4 và cũng không được thêm bất kỳ thông tin nào khác vào hội thoại ngoài các thông tin chỉ phân hệ đã nêu.

d. (1,5 điểm)

Viết hội thoại trao đổi liên phân hệ cho phép người dùng thuộc một phân hệ này truy nhập vào server dịch vụ thuộc một phân hệ khác (ở xa)?

2. An toàn mức giao vận (2,5 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. Client có sẵn một cặp khóa riêng và khóa công khai DSS trong đó khóa công khai DSS đã được chứng thực từ trước. Server cũng có sẵn một cặp khóa riêng và khóa công khai DSS trong đó khóa công khai DSS cũng đã được chứng thực từ trước.

c. (1 điểm)

Vẽ sơ đồ trao đổi thông báo 4 giai đoạn giữa client và server trong giao thức Handshake SSL nêu trên theo cách thức cho phép hai bên xác thực lẫn nhau. Chỉ rõ thông báo nào cho phép client xác thực server và ngược lại thông báo nào cho phép server xác thực client.

d. (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.

3. An toàn thư điện tử (2,5 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
User ID	A	B	C	D	E	F	G	H
Owner Trust	*Tột bậc*	*Không tin cậy*	*Hoàn toàn*	*Một phần*	*Hoàn toàn*	*Hoàn toàn*	*Một phần*	*Không tin cậy*
Signatures	-	D, G, I	B, D	A	A, D	C	E	F, G

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.

4. An toàn IP (2,5 điểm)

Xét các gói tin IPv4 được truyền từ nguồn ban đầu là máy tính H1 trong mạng cục bộ LAN1 đến đích cuối cùng là máy tính H2 trong mạng cục bộ LAN2 qua các cổng an ninh GW1 của LAN1 và GW2 của LAN2. Các thiết bị H1, GW1, GW2 và H2 đều có khả năng cung cấp dịch vụ IPSec. Các gói tin IPSec được truyền trên mạng Internet từ GW1 đến GW2 chống được các hình thức tấn công phân tích lưu lượng hữu hạn và giả mạo nguồn gốc dữ liệu.

a. (1 điểm)

Vẽ khuôn dạng các gói tin IPSec sao cho chúng được áp dụng ít liên kết an ninh nhất có thể nhưng vẫn đáp ứng được các yêu cầu đã nêu. Chế độ sử dụng liên kết an ninh này có tên gọi là gì (giao vận, đường hầm, kề với giao vận hay đường hầm nhiều bước)?

b. (1,5 điểm)

Các gói tin IPSec đã vẽ chống được tấn công nào trong các tấn công sau đây: sửa đổi dữ liệu, lặp lại, đọc trộm dữ liệu? Giải thích lý do với từng hình thức tấn công.