Lớp INT3307

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

(4 câu, 3 trang, thang điểm 10)

1. Phân phối khóa (2,5 điểm)

a. (0,75 điểm)

KDC là bên sinh ra khóa phiên K_s (0,25 điểm).

K_s được KDC gửi cho A ở bước 2, nó được mã hóa với khóa chủ chung của KDC và A là K_a để đảm bảo tính bảo mật (0,25 điểm).

K_s được KDC gửi cho B bằng cách gửi cho A ở bước 2 rồi thông qua A gửi cho B ở bước 3, nó được mã hóa với khóa chủ chung của KDC và B là K_b để đảm bảo tính bảo mật (0,25 điểm).

b. (0,75 điểm)

N_1 dùng để chống tấn lại hình thức tấn công lặp lại (0,25 điểm).

Nếu không có N_1 thì mỗi khi A gửi thông báo ở bước thứ nhất để thiết lập một kết nối logic mới với một khóa phiên mới với B, địch thủ có thể gửi lại cho A thông báo nó bắt được ở bước 2 trong một kết nối logic trước đó khiến cho khóa phiên dùng cho kết nối logic mới sẽ trùng với khóa phiên của kết nối logic cũ (0,25 điểm).

Khi có N_1 thì mỗi lần nhận được thông báo ở bước 2, A sẽ kiểm tra xem N_1 có trùng với N_1 ở bước 1 ngay trước đó hay không, nếu trùng thì là thông báo hợp lệ, còn nếu không trùng thì là tấn công lặp lại (không phải do KDC mới tạo ra sau khi nhận được thông báo ở bước 1 mà là một thông báo ở một kết nối logic trước đây được gửi lại) (0,25 điểm).

c. (1 điểm)

Giải thích tác dụng của N_2 (dùng để chống lại hình thức tấn công gì, nếu không có N_2 thì hình thức tấn công đó diễn ra như thế nào, còn khi có N_2 thì tấn công bị chống lại như thế nào, tại sao trong thông báo ở bước 5 lại dùng $f(N_2)$ thay vì N_2)?

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 server chỉ có một khóa công khai RSA được chứng thực từ trước. Khóa công khai này vừa có thể sử dụng để mã hóa, vừa có thể dùng để xác minh chữ ký. Client cũng chỉ có một khóa công khai được chứng thực từ trước, nhưng khóa công khai này được tạo ra bằng giải thuật Diffie-Hellman.

d. (1 điểm)

Vẽ sơ đồ trao đổi thông báo 4 giai đoạn giữa client và server trong giao thức Handshake SSL theo cách an toàn nhất có thể. Lưu ý là client và server có thể tạo ra các cặp khóa riêng và khóa công khai tức thời (không được chứng thực) theo bất kỳ giải thuật mật mã khóa công khai nào.

e. (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	PU_I
User ID	A	B	C	D	E	F	G	H	I
Owner Trust	*Tột bậc*	*Không tin cậy*	*Không biết*	*Một phần*	*Một phần*	*Một phần*	*Hoàn toàn*	*Hoàn toàn*	*Hoàn toàn*
Signatures	-	D, F	B, D	A	B, C	A, G	A	B, D, E	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.

4. An toàn IP (2,5 điểm)

Trong giao thức ESP có sử dụng tùy chọn xác thức, 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 $W = 64$, số thứ tự lớn nhất B nhận được trong một gói tin hợp lệ cho đến thời điểm hiện tại là $N = 250$, B đã nhận được tất cả các gói tin hợp lệ từ 1 đến 250 ngoại trừ các gói tin có số thứ tự từ 180 đến 190. Hãy mô tả kết quả xử lý theo đúng trình tự tại B khi nhận được lần lượt các gói tin sau:

1. (0,5 điểm)

Một gói tin hợp lệ có số thứ tự là 187.

2. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 253.

3. *(0,5 điểm)*

Một gói tin hợp lệ có số thứ tự là 253.

4. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 187.

5. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 190.

ĐẠI HỌC QUỐC GIA HÀ NỘI — Khoa Công nghệ Thông tin
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ — Học kỳ I, Năm học 2016 - 2017
Thời gian : 120 phút — *Được phép tra cứu tất cả các loại tài liệu*
Lớp INT3307 — *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, 3 trang, thang điểm 10)

1. Phân phối khóa (2,5 điểm)

Xét một giao thức phân phối khóa và xác thực lẫn nhau giữa hai chủ thể A và B thông qua một trung tâm phân phối khóa KDC (Key Distribution Center). Mỗi khi A muốn thiết lập một kết nối logic với B và cần một khóa phiên sử dụng một lần K_s (cho đúng kết nối logic đó chứ không được sử dụng lại cho các kết nối logic khác giữa hai bên), các bước sau đây sẽ được thực hiện.

6. A → KDC: $ID_A \| ID_B \| N_1$
7. KDC → A: $E(K_a, [K_s \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])])$
8. A → B: $E(K_b, [K_s \| ID_A])$
9. B → A: $E(K_s, N_2)$
10. A → B: $E(K_s, f(N_2))$

A có một khóa chủ K_a chỉ A và KDC biết được. Tương tự, B dùng chung một khóa chủ K_b với KDC. Truy vấn A gửi cho KDC bao gồm định danh của A, định danh của B, và một số ngẫu nhiên N_1 chỉ sử dụng một lần (mỗi thông báo ở bước 1 sẽ có một giá trị N_1 khác nhau). N_2 cũng là một giá trị ngẫu nhiên chỉ sử dụng một lần, nhưng do B sinh ra, f là một hàm thực hiện một biến đổi nào đó trên N_2 (chẳng hạn cộng N_2 với 1).

(5 (0,75 điểm)

Bên nào (A, B, hay KDC) sinh ra khóa phiên K_s? Nó được phân phối tới A và B một cách an toàn (đảm bảo tính bảo mật của khóa) như thế nào?

(6 (0,75 điểm)

Giải thích tác dụng của N_1 (dùng để chống lại hình thức tấn công gì, nếu không có N_1 thì hình thức tấn công đó diễn ra như thế nào, còn khi có N_1 thì tấn công bị chống lại như thế nào)?

(7 (1 điểm)

Giải thích tác dụng của N_2 (dùng để chống lại hình thức tấn công gì, nếu không có N_2 thì hình thức tấn công đó diễn ra như thế nào, còn khi có N_2 thì tấn công bị chống lại như thế nào, tại sao trong thông báo ở bước 5 lại dùng $f(N_2)$ thay vì N_2)?

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 server chỉ có một khóa công khai RSA được chứng thực từ trước. Khóa công khai này vừa có thể sử dụng để mã hóa, vừa có thể dùng để xác minh

chữ ký. Client cũng chỉ có một khóa công khai được chứng thực từ trước, nhưng khóa công khai này được tạo ra bằng giải thuật Diffie-Hellman.

(8 (1 điểm)

Vẽ sơ đồ trao đổi thông báo 4 giai đoạn giữa client và server trong giao thức Handshake SSL theo cách an toàn nhất có thể. Lưu ý là client và server có thể tạo ra các cặp khóa riêng và khóa công khai tức thời (không được chứng thực) theo bất kỳ giải thuật mật mã khóa công khai nào.

(9 (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	PU_I
User ID	A	B	C	D	E	F	G	H	I
Owner Trust	*Tột bậc*	*Không tin cậy*	*Không biết*	*Một phần*	*Một phần*	*Một phần*	*Hoàn toàn*	*Hoàn toàn*	*Hoàn toàn*
Signatures	-	D, F	B, D	A	B, C	A, G	A	B, D, E	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.

4. An toàn IP (2,5 điểm)

Trong giao thức ESP có sử dụng tùy chọn xác thức, 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 $W = 64$, số thứ tự lớn nhất B nhận được trong một gói tin hợp lệ cho đến thời điểm hiện tại là $N = 250$, B đã nhận được tất cả các gói tin hợp lệ từ 1 đến

250 ngoại trừ các gói tin có số thứ tự từ 180 đến 190. Hãy mô tả kết quả xử lý theo đúng trình tự 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 187.

b. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 253.

c. *(0,5 điểm)*

Một gói tin hợp lệ có số thứ tự là 253.

d. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 187.

e. *(0,5 điểm)*

Một gói tin không hợp lệ có số thứ tự là 190.