TailieuVNU.com

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Khoa Công nghệ Thông tin
Năm học 2019 - 2020

Thời gian : 90 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, 3 trang, thang điểm 10)

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

Cho một môi trường phân tán mở trong đó các người dùng sử dụng các trạm làm việc để truy nhập dịch vụ trên các server phân tán khắp nơi trên mạng. Yêu cầu đặt ra là các server chỉ cho các người dùng được phép truy nhập dịch vụ và các truy vấn truy nhập dịch vụ cần được xác thực. Thay vì cài đặt một dịch vụ xác thực trên mỗi server, người ta sử dụng một server xác thực (AS) và một server cấp thẻ (TGS). AS biết mật khẩu của tất cả các người dùng (dưới dạng giá trị băm) và lưu trữ những thông tin này trong một cơ sở dữ liệu tập trung. Chức năng của nó là xác thực những người dùng muốn truy nhập các server dịch vụ. TGS biết một người dùng nhất định có được phép truy nhập một dịch vụ nhất định hay không. Xét hội thoại xác thực giả tưởng sau.

(i) Một lần mỗi phiên người dùng đăng nhập

(1) C → AS: $ID_c \parallel ID_{tgs}$

(2) AS → C: $E(K_c, Thẻ_{tgs})$

(ii) Một lần với mỗi kiểu dịch vụ

(3) C → TGS: $ID_c \parallel ID_v \parallel Thẻ_{tgs}$

(4) TGS → C: $Thẻ_v$

(iii) Một lần với mỗi phiên dịch vụ

(5) C → V: $ID_c \parallel Thẻ_v$

$Thẻ_{tgs} = E(K_{tgs}, [ID_c \parallel AD_c \parallel ID_{tgs} \parallel TS_1 \parallel Hạn_1])$

$Thẻ_v = E(K_v, [ID_c \parallel AD_c \parallel ID_v \parallel TS_2 \parallel Hạn_2])$

Trong đó, C là một trạm làm việc, ID_C là định danh của người dùng trên C, ID_{tgs} là định danh của TGS, V là server dịch vụ, ID_V là định danh của V, $Thẻ_{tgs}$ là thẻ được trạm làm việc sử dụng để truy nhập TGS, $Thẻ_V$ là thẻ được trạm làm việc sử dụng để truy cập server dịch vụ V, AD_C là địa chỉ mạng của C, K_C là khóa sinh ra từ mật khẩu người dùng, K_{tgs} là khóa bí mật chia sẻ chung giữa AS và TGS, K_V là khóa bí mật chia sẻ chung giữa TGS và V, TS_1 là nhãn thời gian tại thời điểm phát hành $Thẻ_{tgs}$, TS_2 là nhãn thời gian tại thời điểm phát hành $Thẻ_V$, $Hạn_1$ và $Hạn_2$ cho biết khoảng thời gian có giá trị của các thẻ tương ứng.

Giả sử địch thủ không thể tấn công lặp lại.

TailieuVNU.com

a. (1 điểm)

Dễ thấy trong thông báo (2), thẻ cấp cho trạm làm việc được mã hóa hai lần, lần đầu với khóa bí mật K_{tgs} và lần sau với khóa bí mật Kc. Lần mã hóa sau có cần thiết hay không? Giải thích vì sao.

b. (1,5 điểm)

Các người dùng và các server dịch vụ thuộc về các tổ chức hành chính khác nhau được phân vào các phân hệ khác nhau. Mỗi người dùng và mỗi server dịch vụ chỉ được phân vào một phân hệ. Tuy nhiên, các người dùng được phân vào một phân hệ nhất định có thể truy nhập vào các server dịch vụ thuộc các phân hệ khác, ngược lại các server được phân vào một phân hệ nhất định cũng sẵn sàng cung cấp dịch vụ cho các người dùng thuộc các phân hệ khác đĩ nhiên với điều kiện các người dùng đó đã được xác thực.

Không được nâng cấp hội thảo giả tưởng trong đề bài lên phiên bản Kerberos 4 hay phiên bản Kerberos 5, viết chi tiết các thông báo trao đổi cho hội thoại xác thực liên phân hệ cho phép người dùng trong một phân hệ nhất định truy nhập server dịch vụ trong một phân hệ khác. Các server cấp thẻ trong hai phân hệ này chia sẻ một khóa bí mật chung với nhau. Người dùng muốn truy nhập server dịch vụ trong một phân hệ khác cần xin cấp thẻ để truy nhập server đó. Trạm làm việc của người sử dụng tiến hành các bước để xin server cấp thẻ cục bộ (trong cùng phân hệ với người sử dụng) cấp thẻ cấp thẻ để truy nhập vào server cấp thẻ ở xa (trong phân hệ kia), sau đó dùng thẻ này xin server cấp thẻ ở xa cấp thẻ truy nhập server dịch vụ trong cùng phân hệ với server cấp thẻ 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 bắt tay trong chuỗi giao thức SSL để xác thực lẫn nhau và thỏa thuận các tham số an ninh (giải thuật và khóa). Giả sử phương pháp trao đổi khóa được client và server thống nhất sử dụng là Diffie-Hellman trong đó server có cặp khóa riêng và khóa công khai Diffie-Hellman cố định (khóa công khai được chứng thực), còn client sinh ra cặp khóa riêng và khóa công khai Diffie-Hellman một cách tức thời (khóa công khai không được chứng thực).

a. (1 điểm)

Vẽ sơ đồ trao đổi thông báo 4 giai đoạn giữa client và server trong giao thức bắt tay SSL nêu trên.

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.

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

TailieuVNU.com

User ID	A	B	C	D	E	F	G	H	I
Owner Trust	*Tốt 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, F	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 chống tấn công lặp lại. Giả sử cửa sổ có kích thước $W = 256$, số thứ tự lớn nhất B nhận được trong một gói tin hợp lệ cho đến thời điểm hiện tại là $N = 365$, B đã nhận được tất cả các gói tin hợp lệ có số thứ tự lẻ nhưng chưa nhận được một gói tin có số thứ tự chẵn nào trong cửa sổ chống tấn công lặp lại. Hãy mô tả kết quả xử lý theo đúng trình tự tại B khi nhận được lần lượt các gói tin sau:

365
256
109

a. (0,5 điểm)

Một gói tin không hợp lệ có số thứ tự là 365.

b. (0,5 điểm)

Một gói tin hợp lệ có số thứ tự là 367.

112

c. (0,5 điểm)

Một gói tin hợp lệ có số thứ tự là 112.

d. (0,5 điểm)

Một gói tin hợp lệ có số thứ tự là 111.

e. (0,5 điểm)

Một gói tin không hợp lệ có số thứ tự là 112.