ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NĂM HỌC 2014 - 2015
HỌC KỲ 1

ĐỀ THI CUỐI KỲ

Môn học: An toàn và an ninh mạng
Thời gian: 120 phút

Câu 1: Phân phối khoá 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 cập 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 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).

a) (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.

b) (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).

Câu 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 thoả thuận các tham số an ninh (các giải thuật và khoá mật mã). Giả sử phương pháp trao đổi khoá 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 khoá riêng và khoá công khai DSS trong đó khoá công khai DSS đã được chứng thực từ trước. Server cũng có sẵn một cặp khoá riêng và khoá công khai DSS trong đó khoá công khai DSS cũng đã được chứng thực từ trước.

a) (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.

b) (1,5 điểm)

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

Câu 3: An toàn thư điện tử (2,5 điểm)

Chương trình PGP của một người dùng A lưu trữ vòng khoá 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 khoá công khai (**Key Legitimacy**) được PGP tính theo quy tắc sau:

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

Vẽ mô hình tin cậy PGP tương ứng.

Câu 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 đích đến cuối cùng là máy tính H1 trong mạng cục bộ LAN2 qua các cổng an ninh GW1 của LAN1 và GW2 của LAN2. Các thiết bị H1, GW1, H2 và GW2 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 áp dụng được 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.