Thời gian : 90 phút
Lớp INT3307

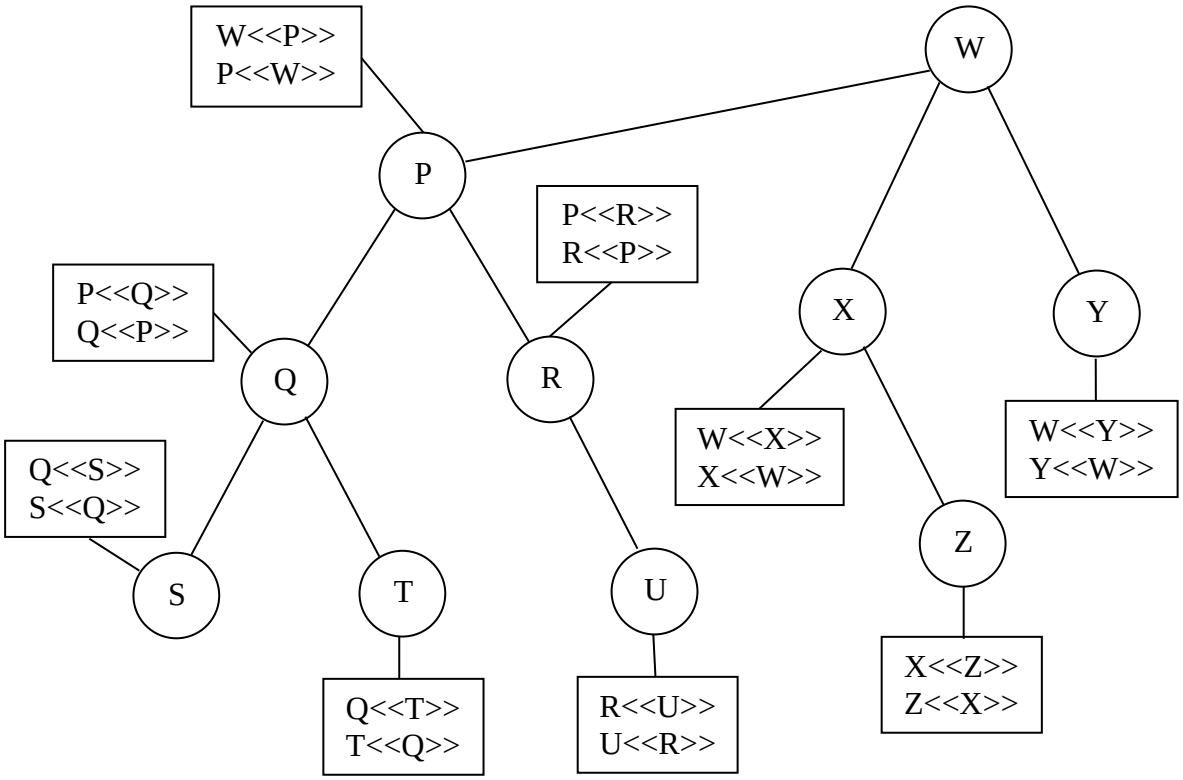
Được phép tra cứu tất cả các loại tài liệu
Không được cho người khác mượn tài liệu dưới bất kỳ hình thức nào

Lời giải Đề thi số 1
An toàn và an ninh mạng

(4 câu, 2 trang, thang điểm 10)

1. Phân phối khóa (3 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 S cấp. Một người dùng B có chứng thực do Z cấp. Hãy cho biết chuỗi các chứng thực lẫn nhau và cách thức cho phép A xác minh tính hợp lệ của khóa công khai của B trong chứng thực do Z cấp.

Xét hai chứng thực khóa công khai của hai người dùng khác nhau được cấp bởi hai cơ quan chứng thực khác nhau. Nếu hai chứng thực này chứa các khóa công khai giống nhau thì có thể nảy sinh những vấn đề gì liên quan đến an ninh. Giải thích.

Lời giải

Chuỗi các chứng thức lẫn nhau A cần có là:

S<<Q>>Q<<P>>P<<W>>W<<X>>X<<Z>>Z<<B>> 0,75 điểm

Lưu ý: Mỗi một trong các sai sót sau bị trừ 0,25 điểm: Viết không đúng định dạng chuỗi các chứng thực lẫn nhau (chẳng hạn có dấu phẩy giữa hai chứng thực liên tiếp, mỗi chứng thực cố ý viết trên một dòng riêng,...); Thiếu Z<<B>>; Cơ quan chứng thực đứng đầu chuỗi không phải là S; Thiếu một chứng thực khóa công khai trong chuỗi,...

Cách thức A xác minh tính hợp lệ của khóa công khai của B trong chứng thực Z<<B>>:

Vì A có chứng thực khóa công khai do S cấp nên A có khóa công khai hợp lệ của S.

A sử dụng khóa công khai hợp lệ của S để xác minh S<<Q>>, nếu hợp lệ thì A có khóa công khai hợp lệ của Q.

A sử dụng khóa công khai hợp lệ của Q để xác minh Q<<P>>, nếu hợp lệ thì A có khóa công khai hợp lệ của P.

Cứ như vậy,…

A sử dụng khóa công khai hợp lệ của Z để xác minh Z<<B>>, nếu hợp lệ thì A có khóa công khai hợp lệ của B. 1,25 điểm

Lưu ý: Mỗi một trong các sai sót sau bị trừ 0,25 điểm: Nói "sử dụng khóa công khai" mà không nói chính xác là "sử dụng khóa công khai hợp lệ"; Viết thiếu điều kiện "nếu hợp lệ"; Viết thiếu câu mở đầu "Vì A có chứng thực…" (câu mở đầu cũng được coi là đúng không bị trừ điểm nếu viết là "A lấy khóa công khai hợp lệ trực tiếp từ S khi xin S cấp S<<A>>"); Chỉ viết câu "A sử dụng khóa công khai hợp lệ của S…" rồi đến luôn "Cứ như vậy" (vì không thể hiện được tính lặp lại trong giải thích),…

Hai người dùng có khóa công khai giống nhau thì cũng có khóa riêng giống nhau, từ đó sẽ dẫn tới các tấn công nghe lén và giả mạo làm mất tính bảo mật và tính xác thực của các thông báo. Cụ thể

- Tấn công nghe lén vi phạm tính bảo mật: Khi một người thứ ba sử dụng khóa công khai để mã hóa các thông báo gửi cho một trong hai người có khóa công khai giống nhau thì người kia có thể sử dụng khóa riêng của mình để giải mã tất cả các thông báo đó, vi phạm tính bảo mật của các thông báo này (lẽ ra các thông báo này chỉ người thứ nhất và người thứ ba mới được phép biết nội dung) 0,5 điểm
- Tấn công giả mạo vi phạm tính xác thực: Một trong hai người có thể sử dụng khóa riêng của mình để ký các thông báo gửi cho một người thứ ba nói là do người kia gửi, người thứ ba lấy khóa công khai hợp lệ của người thứ hai để kiểm tra thấy chữ ký là hợp lệ thì coi các thông báo là do người thứ hai tạo ra và gửi đi, nhưng thực tế các thông báo này đều là của người thứ nhất. 0,5 điểm

Lưu ý: Nếu sinh viên nào nêu được tình huống như tấn công người ở giữa vào giải thuật trao đổi khóa Diffie-Hellman thì cũng được tính 0,5 điểm

2. Xác thực người dùng (2 điểm)

Xét hội thoại xác thực một chiều sử dụng mật mã khóa công khai sau đây.

A → B : ID_A

B → A : N_1

A → B : E(PR_a, N_1)

Trong đó, ID_A là định danh của A, N_1 là một giá trị ngẫu nhiên do B sinh ra không bao giờ trùng với những giá trị đã được sinh ra trước đó, PR_a là khóa riêng của A, B đã có khóa công khai hợp lệ tương ứng của A từ trước khi hội thoại diễn ra.

a. (1 điểm)

Giải thích hoạt động của giao thức đã cho (Phục vụ mục đích gì ? Vì sao có thể đạt được mục đích đó ?)

Lời giải

Giao thức cho phép B xác thực A. 0,25 điểm

Giải thích : Vì chỉ A có khóa riêng tương ứng với khóa công khai B đã có sẵn và được B nhìn nhận là thực sự của A (0,25 điểm) nên chỉ A mới có thể tạo ra bản mã của N_1 để gửi cho B trong thông báo số 3 (0,25 điểm) mà khi B sử dụng khóa công khai tương ứng để giải mã thì nguyên bản thu được chính là N_1 mà B đã sinh ra và gửi cho A ở thông báo số 2 (0,25 điểm).

b. (1 điểm)

Giao thức đã cho không an toàn. Có thể thực hiện hình thức tấn công gì khiến nó thực hiện sai mục đích kỳ vọng ?

Lời giải

Địch thủ C có thể sử dụng giao thức để khiến A ký vào một thông báo (N_1) nào đó do địch thủ chọn (0,25 điểm). Sau đó, địch thủ gửi chữ ký (E(PR_a, N_1)) đến một người dùng D khai báo đấy là do A gửi (0,25 điểm) và D tin vào điều đó (0,25 điểm) trong khi thực tế là thông báo do C tạo ra, người trao đổi với D là C chứ không phải là A (0,25 điểm).

Lưu ý : Sinh viên có thể viết các hội thoại giữa A và C cũng như giữa C và D thay cho 2 ý đầu tiên trong lời giải mẫu vẫn được tính 0,25 điểm cho mỗi ý nhưng phải nói rõ ràng D tin vào điều đó trong khi thực tế không phải vậy mới được 0,25 điểm cho mỗi một trong hai ý cuối.

3. 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. 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.

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.

Lời giải

Vẽ đầy đủ tất cả các thông báo (không thiếu bất kỳ thông báo tùy chọn nào) 0,75 điểm

Thông báo server_key_exchange cho phép client xác thực server còn thông báo certificate_verify cho phép server xác thực client (0,25 điểm) (phải trả lời đúng cả hai ý mới được 0,25 điểm, chỉ cần sai một ý là bị 0 điểm cho câu hỏi này)

Lưu ý : Mỗi thông báo bị thừa hay thiếu bị trừ 0,25 điểm, nhưng cho sinh viên 0,25 điểm thay vì 0 điểm nếu vẽ được cơ bản bộ khung của giao thức SSL Handshake. Tên gọi của các thông báo nếu sai về chính tả thì không bị trừ điểm, nhưng nếu sai về ngữ nghĩa thì cũng bị trừ 0,25 điểm.

b. (2 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.

Lời giải

Thông báo certificate ở giai đoạn 2 chứa chứng thực khóa công khai DSS của server (Có thể viết tắt là $CA\langle\langle S\rangle\rangle^{DSS}$ hay $CA\langle\langle S\rangle\rangle_{DSS}$) 0,25 điểm

Thông báo server_key_exchange chứa khóa công khai RSA có chức năng mã hóa của server (0,25 điểm) được ký với khóa riêng DSS của server (0,25 điểm) (Có thể viết tắt là $S\{PU_s^{RSA}\}^{DSS}$)

Thông báo certificate_request bao gồm certificate_type và certificate_authorities trong đó certificate_type chỉ ra kiểu giải thuật mật mã khóa công khai là DSS và chế độ sử dụng là chữ ký số (cũng có thể viết là xác thực), không cần nói rõ về certificate_authorities (0,25 điểm)

Thông báo certificate ở giai đoạn 3 chứa chứng thực khóa công khai DSS của client (Có thể viết tắt là $CA\langle\langle C\rangle\rangle^{DSS}$ hay $CA\langle\langle C\rangle\rangle_{DSS}$) 0,25 điểm

Thông báo client_key_exchange chứa khóa bí mật pre_master_secret được sinh ra bởi client (0,25 điểm) và được mã hóa với khóa công khai RSA của server (0,25 điểm) (Có thể viết tắt là $E(PU_s^{RSA}, \text{pre\_master\_secret})$)

Thông báo certificate_verify chứa chữ ký của client trên các thông báo client và server trước đó trao đổi với nhau và master_secret sử dụng khóa riêng DSS của client (0,25 điểm)

4. An toàn IP (2 điểm)

a. (1 điểm)

Tài liệu chuẩn về kiến trúc IPSec đặc tả 4 trường hợp kết hợp các liên kết an ninh với nhau. Vẽ khuôn dạng các gói tin IPSec cho trường hợp cung cấp nhiều dịch vụ an ninh nhất nhưng lại qua xử lý IPSec tại ít thiết bị nhất có thể. Khuôn dạng này tương ứng với chế độ nào trong các chế độ giao vận, đường hầm, kề với giao vận và đường hầm nhiều bước.

Lời giải

Định dạng bao gồm trường đầu tiên là New IP Header, sau đó là ESP Header, rồi Original IP Header, IP Payload, ESP Trailer và cuối cùng là Authentication. Phạm vi Mã

hóa (Encrypted) là từ Original IP Header đến ESP Trailer, còn phạm vi Xác thực (Authenticated) là từ ESP Header đến ESP Trailer. 0,75 điểm

Chế độ đường hầm được sử dụng 0,25 điểm

Lưu ý : Mỗi một trường hợp sau đây bị trừ 0,25 điểm : Sai, thiếu, hoặc thừa trường thông tin ; Sai trật tự trường ; Sai hoặc thiếu phạm vi mã hóa ; Sai hoặc thiếu phạm vi xác thực,…

b. (1 điểm)

Nêu hai lý do khiến cho cách thức kết hợp kề với giao vận các liên kết an ninh AH và ESP (không kèm theo tùy chọn xác thực) theo thứ tự ESP trước, AH sau được lựa chọn thay vì AH trước, ESP sau.

Lời giải

Lý do thứ nhất : Với thứ tự ESP trước, AH sau bên nhận có thể thực hiện đồng thời (song song) hai thao tác giải mã (thực hiện giao thức ESP) và kiểm tra tính xác thực (thực hiện giao thức AH) của thông báo trong khi với thứ tự AH trước, ESP sau thì chỉ có thể kiểm tra tính xác thực của thông báo sau khi đã hoàn thành thao tác giải mã. 0,5 điểm

Lý do thứ hai : Với thứ tự AH trước, ESP sau nếu địch thủ cố tính gửi quá nhiều thông báo không hợp lệ (kèm với mã xác thực thông báo sai) thì bên nhận sẽ mất quá nhiều thời gian để giải mã rồi mới phát hiện ra và loại bỏ các thông báo này có thể dẫn tới quá tải, từ chối dịch vụ trong khi với thứ tự ESP trước, AH sau bên nhận có thể kịp thời phát hiện các thông báo là không hợp lệ thông qua kiểm tra MAC (mã xác thực thông báo) không phải thực hiện thao tác giải mã vẫn có thể phát hiện và loại bỏ các thông báo này, không dẫn tới quá tải, từ chối dịch vụ. 0,5 điểm