CHƯƠNG 7: MỘT SỐ ỨNG DỤNG AN NINH MẠNG

7.1 An toàn IP

Có khá nhiều ứng dụng an ninh chuyên biệt như: S/MIME, PGP, Kerberos, SSL/HTTPS. Tuy nhiên có những cơ chế an ninh mà xuyên suốt nhiều tầng ứng dụng như là cơ chế an ninh IP được cài đặt trên mạng cho mọi ứng dụng. Chẳng hạn doanh nghiệp có thể sử dụng mạng TCP/IP riêng không cho phép liên kết với các trang không tin cậy, mã hóa các gói tin gửi đi và xác thực các gói tin đến. An toàn mức IP thực hiện ba chức năng chính: xác thực, bảo mật và quản trị khóa.

7.1.1. IPSec

IPSec là cơ chế an ninh IP tổng quan. Nó cung cấp: xác thực, bảo mật và quản trị khoá. IPSec được dùng trên mạng LAN, mạng WAN riêng và chung và trên cả mạng Internet.

Lợi ích của IPSec:

- Khi IPSec được cài đặt trên bức tường lửa/router, nó cung cấp an toàn mạnh cho mọi việc truyền tin qua vành đai. IPSec trong bức tường lửa chống mọi luồng tin từ bên ngoài đi vào qua nó.
- IPSec nằm dưới tầng vận chuyển nên trong suốt với mọi ứng dụng. Không cần thiết phải thay đổi phần mềm trên hệ thống máy chủ hoặc của người sử dụng.
- IPSec có thể trong suốt với người sử dụng đầu cuối. Nó cũng có thể cung cấp an toàn cho người sử dụng riêng biệt, khi họ truy cập từ xa đến mạng của công ty hay cần thiết lập mạng ảo an toàn trong công ty cho một số ứng dụng quan trọng.

7.1.2. Kiến trúc an ninh IP

Đặc tả an ninh IP rất phức tạp, được định nghĩa qua một số chuẩn (RFC): bao gồm RFC 2401/2402/2406/2408 và có nhiều chuẩn khác được nhóm theo loại. Hỗ trợ các đặc tính này là bắt buộc đối với IP6 và tuỳ chọn với IP4. Trong cả hai trường hợp các đặc tính bảo mật được cài đặt như phần mở rộng của tiêu đề nối tiếp tiêu đề IP chính:

- Tiêu đề xác thực (AH – Authentication Header) là tiêu đề mở rộng dùng cho xác thực.
- Bao bọc tải trọng bảo mật (ESP – Encapsulating Security Payload) là tiêu đề mở rộng dùng cho mã hóa.

7.1.2.1. Dịch vụ IPSec

IPSec nhằm đạt các mục đích sau: kiểm soát truy cập, toàn vẹn không kết nối, xác thực nguồn gốc dữ liệu, từ chối tải lại gói (đây là một dạng của toàn vẹn liên kết từng phần), bảo mật (mã hoá), bảo mật dòng lưu lượng giới hạn.

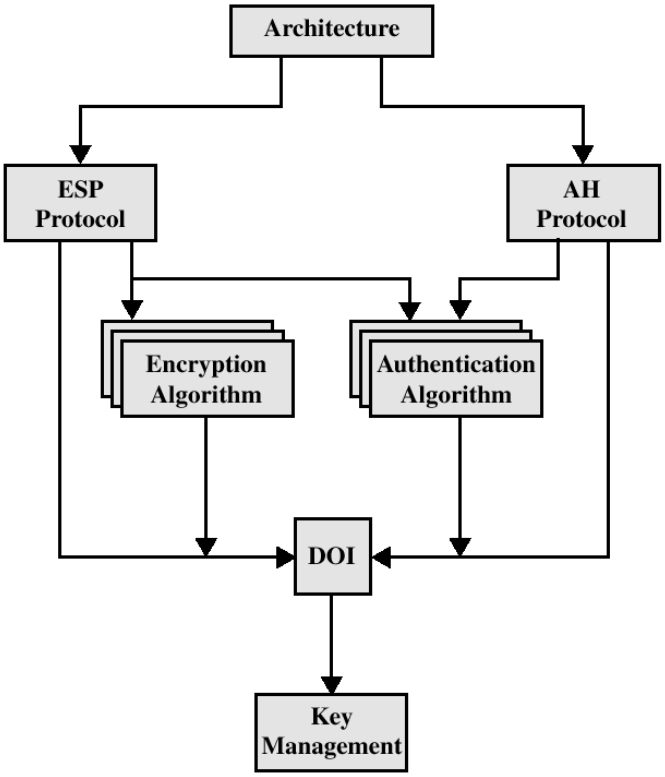
7.1.2.2. Liên kết an toàn

Khái niệm khóa xuất hiện trong cả hai cơ chế xác thực và bảo mật cho IP là liên kết an toàn. Đây là quan hệ một chiều giữa người gửi và người nhận mà cung cấp dịch vụ an ninh cho luồng vận chuyển và được xác định bởi 3 tham số:

- Chỉ số các tham số bảo mật (SPI): là xâu bit gắn với liên kết, nó cho phép hệ thống nhận tin lựa chọn liên kết để xử lý.

- Địa chỉ IP đích.
- Định danh giao thức bảo mật: chỉ rõ liên kết là AH hay ESP.

Ngoài ra có một số các tham số khác như: chỉ số dãy (sequence number), thông tin về tiêu đề xác thực và tiêu đề mở rộng AH & EH, thời gian sống. Có lưu trữ cơ sở dữ liệu của các liên kết an toàn.



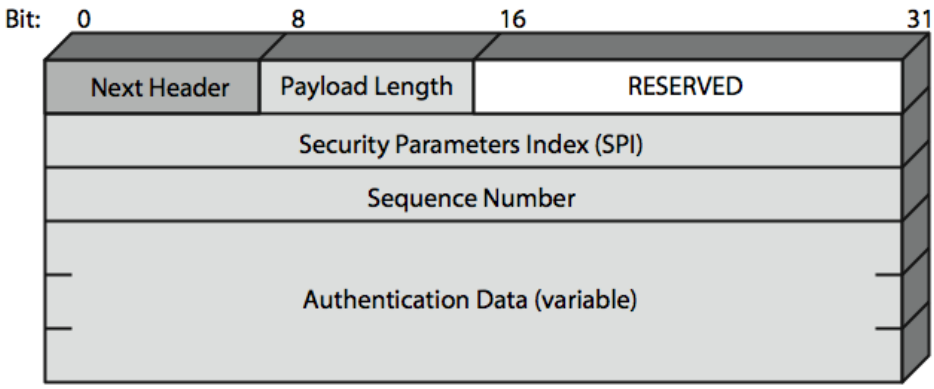
Kiến trúc IPSec

7.1.2.3. Tiêu đề xác thực (Authentication Header - AH)

AH cung cấp sự hỗ trợ cho toàn vẹn dữ liệu và xác thực của các gói IP:

- Hệ thống đầu cuối/chuyển mạch có thể xác thực người sử dụng/ứng dụng.
- Ngăn tấn công theo dõi địa chỉ bằng việc theo dõi các chỉ số dãy và chống tấn công tải lại.

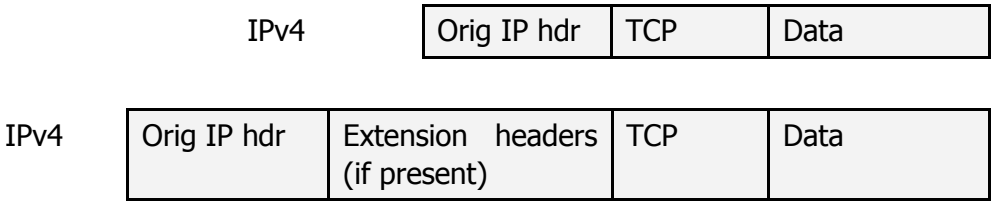
AH dựa trên sử dụng MAC: HMAC–MD5–96 hoặc HMAC – SHA -1-96



Tiêu đề xác thực

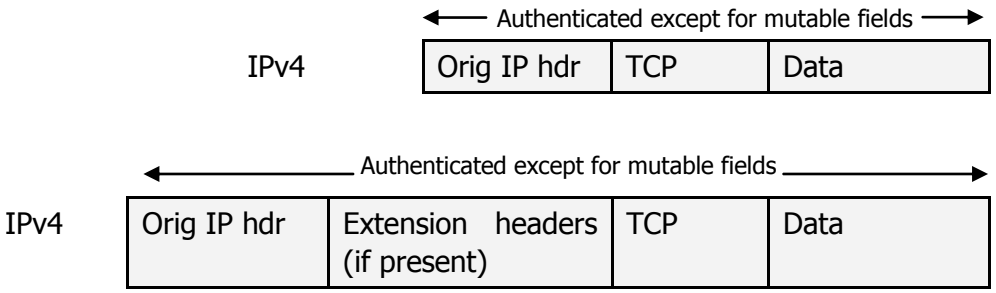
- Next Header - Tiêu đề tiếp theo (8 bit): xác định kiểu tiêu đề tiếp theo tiêu đề này.
- Payload Length - Độ dài tải trọng (8 bit): chiều dài của tiêu đề xác thực ở dạng từ 32 bit, trừ 2. Ví dụ chiều dài mặc định của trường dữ liệu xác thực là 96 bit tức là 3 từ 32 bit. Cộng với phần cố định 3 từ của tiêu đề, ở đây có tổng cộng 6 từ trong tiêu đề và trường độ dài tải trọng sau khi trừ 2 có giá trị là 4.
- Reserved - để dành (16 bit) sử dụng sau này.
- SPI - chỉ số các tham số bảo mật xác định liên kết bảo mật
- Sequence Number - dãy số (32 bit): giá trị dãy đếm đơn điệu tăng, dùng để phát hiện việc gửi lại bản sao của một gói tin nào đó.
- Authentication Data – giá trị dùng để kiểm tra tính toàn vẹn của gói dữ liệu nhận được.

Trong các hình vẽ sau chỉ ra hai cách mà dịch vụ IPSec xác thực được dùng.



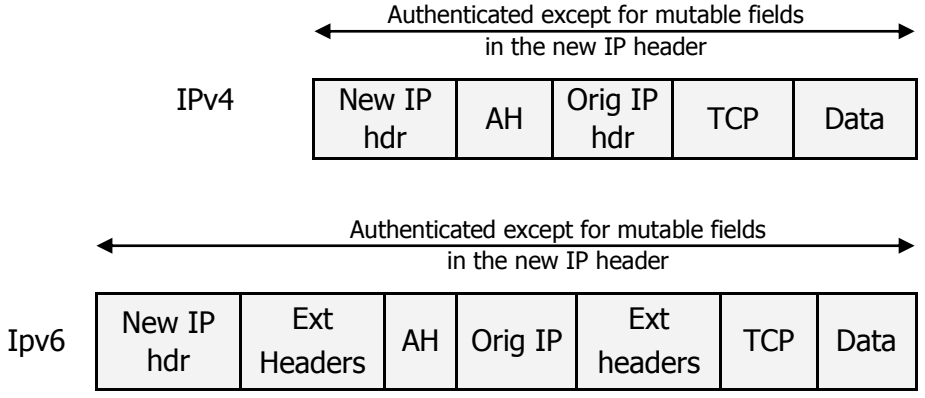
Trước khi áp dụng IPSec

Trường hợp đầu, xác thực được cung cấp trực tiếp giữa hai trạm của server và client. Hai bên chia sẻ khóa mật, ở đây sử dụng SA dạng vận chuyển.



Chế độ vận chuyển cho xác thực tiêu đề

Đối với AH trong chế độ vận chuyển sử dụng IP4, AH được chèn sau tiêu đề IP gốc. Còn với IP6, AH được xem như tải trọng đầu cuối, tức là không bị kiểm tra hoặc xử lý bởi các chuyển mạch trung gian. Xác thực bao trùm toàn bộ gói, trừ các trường thay đổi được đặt bằng 0 để tính MAC.



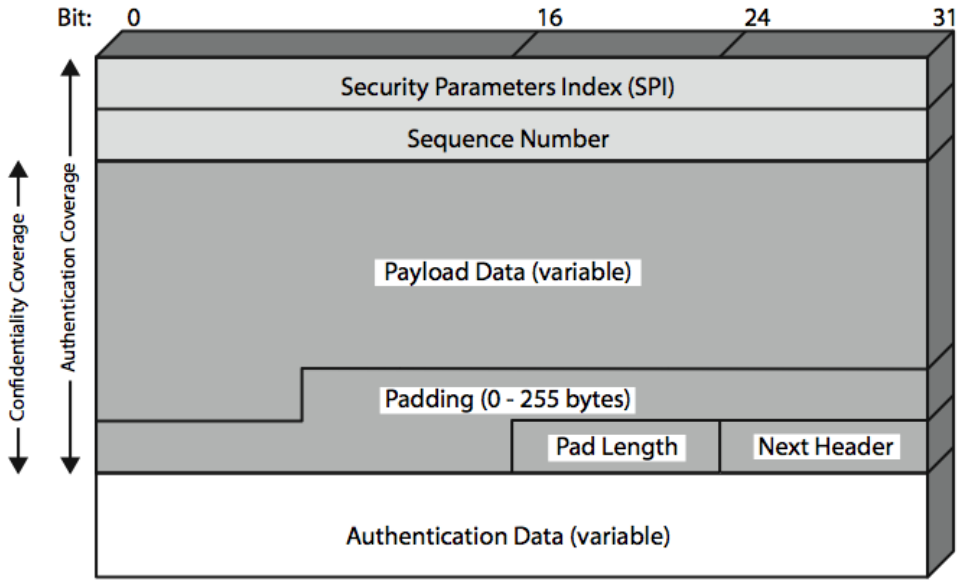
Chế độ đường hầm cho xác thực tiêu đề

Đối với AH trong chế độ đường hầm, toàn bộ gói tin IP gốc được xác thực và AH được chèn giữa tiêu đề IP gốc và tiêu đề IP mới (là địa chỉ của bức tường lửa hoặc một cổng an toàn nào đó).

7.1.2.4. Bao bọc tải trọng bảo mật (ESP)

ESP đảm bảo bảo mật nội dung mẩu tin và luồng vận chuyển giới hạn, có lựa chọn cung cấp dịch vụ xác thực như AH và hỗ trợ phạm vi rộng các mã, các chế độ mã và bộ đệm, bao gồm:

- DES, Triple DES, RC5, IDEA, CAST,…
- CBC và các chế độ khác.
- Bộ đệm cần thiết để lấp đầy các kích thước khối, các trường cho luồng vận chuyển.



- Chỉ số các tham số bảo mật (SPI): xác định liên kết an toàn.
- Sequence Number - dãy số (32 bit): giá trị đếm đơn điệu tăng, dùng để phát hiện việc gửi lại bản sao của một gói tin nào đó.
- Payload Data – dữ liệu tải trọng là gói tin (trong chế độ vận chuyển) hoặc gói IP (trong chế độ đường hầm) được mã hóa.
- Padding – bộ đệm dùng để bổ sung vào bản rõ trước khi mã hóa.
- Độ dài bộ đệm.
- Tiêu đề tiếp theo.
- Dữ liệu xác thực là trường có độ dài thay đổi chứa giá trị kiểm tra tính toàn vẹn được tính dựa vào toàn bộ ESP trừ trường dữ liệu xác thực.

7.1.2.5. Chế độ vận chuyển và chế độ ống (đường hầm) cho ESP

ESP được sử dụng với 2 chế độ: vận chuyển và ống. Trong chế độ ống không cần giữ tường minh địa chỉ đích.

Chế độ vận tải được sử dụng để mã và tuỳ chọn xác thực dữ liệu IP:

- Dữ liệu được bảo vệ nhưng phần đầu vẫn để rõ để biết địa chỉ đích. Nếu lựa chọn xác thực sẽ có thêm ESP Authentication Data.
- Kẻ phá hoại vẫn có thể phân tích vận chuyển một cách hiệu quả.
- Là lựa chọn tốt đối với ESP máy chủ vận chuyển tới máy chủ.

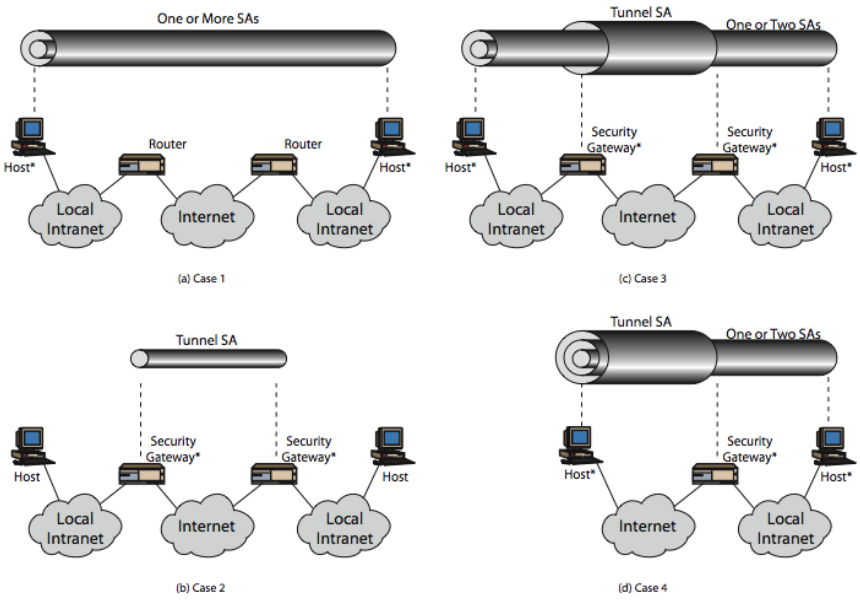
Chế độ ống mã toàn bộ gói IP:

- Bổ sung tiêu đề mới, có thể thêm phần xác thực nếu lựa chọn.
- Tại mỗi cổng chuyển tiếp trung gian sẽ kiểm tra và xử lý tiêu đề IP và các phần rõ, còn giữ nguyên phần mã hóa.
- Tốt cho mạng riêng ảo VPN (Virtual Private Network), cổng đến cổng an toàn.

7.1.2.6. Kết hợp các liên kết an toàn (SA – Secure Association)

Các liên kết an toàn có thể cài đặt qua AH hoặc ESP. Để cài đặt cả hai cần kết hợp các liên kết an toàn.

- Tạo nên bó các liên kết an toàn.
- Có thể kết thúc tại các điểm cuối cùng nhau hoặc khác nhau.
- Kết hợp bởi các chế độ vận chuyển kề và ống lặp.



Tài liệu về kiến trúc IPSec đưa ra bốn ví dụ kết hợp SA:

Trường hợp 1: bảo mật cho các hệ thống đầu cuối cài đặt IPSec và chia sẻ khóa mật thích hợp. Các liên kết có thể có như sau:

- AH ở chế độ vận chuyển.
- ESP ở chế độ vận chuyển.
- AH tiếp theo ESP ở chế độ vận chuyển.
- Bất kỳ a, b hoặc c ở trong AH hoặc ESP ở chế độ đường hầm.

Trường hợp 2: bảo mật giữa các cổng (chuyển mạch, các bức tường lửa,…) và các máy chủ không cài đặt IPSec. Trường hợp này mô tả một mạng riêng ảo đơn giản. Ở đây chỉ cần SA đường hầm duy nhất với AH, ESP hoặc ESP với lựa chọn xác thực. Không cần các đường hầm lồng nhau.

Trường hợp 3: dựa trên trường hợp 2 bổ sung bảo mật giữa các đầu cuối. Liên kết bảo mật trong trường hợp 1, 2 có thể dùng ở đây. Đường hầm từ cổng đến cổng cung cấp xác thực hoặc bảo mật hoặc cả hai cho mọi luồng dữ liệu giữa hai đầu cuối. Các máy chủ có thể cài đặt IPSec với SA đầu cuối đến đầu cuối.

Trường hợp 4 hỗ trợ máy chủ ở xa sử dụng Internet tiếp cận bức tường lửa của công ty để truy cập máy chủ tại đó. Chỉ cần có đường hầm giữa máy chủ từ xa và bức tường lửa. Có thể kết hợp một số SA.

7.1.2.7. Quản trị khoá

Quản lý sinh khóa và phân phối khóa giữa các bên trao đổi thông tin, thông thường cần hai cặp khoá, 2 khóa trên một hướng cho AH và ESP.

Trong cơ chế Quản trị khóa thủ công, người quản trị hệ thống thiết lập cấu hình cho từng hệ thống.

Trong cơ chế Quản trị khóa tự động:

- Hệ thống tự động dựa vào yêu cầu về khóa cho các liên kết an toàn trong hệ thống lớn.
- Có các thành phần như thủ tục trao đổi khóa Oakley và liên kết an toàn trên mạng ISAKMP.

7.1.2.8. Oakley

Oakley là thủ tục trao đổi khoá, dựa trên trao đổi khóa Diffie-Hellman. Ở đây bổ sung các đặc trưng để khắc phục các điểm yếu như Cookies, nhóm (tham số tổng thể), các chỉ số đặc trưng (nonces), kết hợp trao đổi khóa Diffie Hellman với việc xác thực. Có thể sử dụng số học trên trường số nguyên tố hoặc đường cong elip.

7.1.2.9. ISAKMP

ISAKMP liên kết an toàn trên Internet và thủ tục quản trị khoá. Nó cung cấp khung để quản lý khoá, xác định các thủ tục và định dạng gói để thiết lập, thỏa thuận, điều chỉnh và xoá các liên kết an toàn (SA – Secure Associations). ISAKMP độc lập với thủ tục trao đổi khoá, thuật toán mã hóa và phương pháp xác thực.

Trao đổi và tải trọng ISAKMP.

Có một số kiểu tải trọng ISAKMP: an toàn, đề xuất, dạng vận chuyển, khoá, định danh, chứng nhận, hash, chữ ký, nonce và xoá.

ISAKMP có bộ khung cho 5 kiểu trao đổi mẩu tin: cơ sở, bảo vệ định danh, xác thực, tích cực và thông tin.

7.2. An toàn Web

7.2.1. Khái niệm

Web ngày càng được sử dụng rộng rãi bởi các công ty, chính phủ và cá nhân, nhưng Internet và Web có những lỗ hổng lớn và có nhiều mối đe dọa an toàn như:

- Tính toàn vẹn: sửa đổi dữ liệu, ngựa thành Toroa, thay đổi bộ nhớ.
- Bảo mật: theo dõi trên mạng, do thám từ máy chủ hay trạm, theo dõi luồng thông tin xem máy trạm nào liên hệ với máy chủ.

- Từ chối dịch vụ: xóa luồng của người sử dụng, làm tràn máy với các đe dọa, làm tràn bộ nhớ, cô lập máy để từ chối dịch vụ.
- Xác thực: giả mạo người dùng hợp pháp, giả mạo dữ liệu.

Như vậy cần bổ sung cơ chế bảo mật cho Web.

7.2.2. SSL (Secure Socket Layer)

SSL là dịch vụ an toàn tầng vận chuyển, ban đầu được phát triển bởi Netscape. Sau đó phiên bản 3 của nó được thiết kế cho đầu vào công cộng và trở thành chuẩn Internet, được biết đến như an toàn tầng vận chuyển TLS (Transport Layer Security).

SSL sử dụng giao thức TCP để cung cấp dịch vụ đầu cuối đến đầu cuối tin cậy và có 2 tầng thủ tục.

Được phát triển bởi Netscape, giao thức SSL đã được sử dụng rộng rãi trên mạng Internet trong việc xác thực và mã hóa thông tin giữa máy trạm và máy chủ. SSL có thể sử dụng để hỗ trợ các giao dịch an toàn cho rất nhiều ứng dụng khác nhau trên Internet. SSL không phải là một giao thức đơn lẻ mà là một tập các thủ tục đã được chuẩn hóa để thực hiện các nhiệm vụ bảo mật sau:

- Xác thực máy chủ: Cho phép người sử dụng xác thực được máy chủ muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hóa công khai để chắc chắn rằng chứng chỉ và khóa công cộng của máy chủ là có giá trị và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy của máy trạm.
- Xác thực máy trạm: Cho phép phía máy chủ xác thực được người sử dụng muốn kết nối. Phía máy chủ cũng sử dụng các kỹ thuật mã hóa công khai để kiểm tra xem chứng chỉ và khóa công cộng của máy trạm có giá trị hay không và được cấp phát bởi một CA trong danh sách các CA đáng tin cậy không.
- Mã hóa kết nối: Tất cả các thông tin trao đổi giữa máy trạm và máy chủ được mã hóa trên đường truyền nhằm nâng cao khả năng bảo mật.

Hoạt động của SSL

Giao thức SSL hoạt động dựa trên hai nhóm con giao thức là giao thức "bắt tay" và giao thức "bản ghi". Giao thức "bắt tay" xác định các tham số giao dịch giữa hai đối tượng có nhu cầu trao đổi thông tin hoặc dữ liệu, còn giao thức "bản ghi" xác định khuôn dạng cho tiến hành mã hóa và truyền tin hai chiều giữa hai đối tượng đó. Giao thức SSL "bắt tay" sẽ sử dụng SSL "bản ghi" để trao đổi một số thông tin giữa máy chủ và máy trạm vào lần đầu tiên thiết lập kết nối SSL.

Một giao dịch SSL thường bắt đầu bởi quá trình "bắt tay" giữa hai bên. Các bước trong quá trình "bắt tay" có thể như sau:

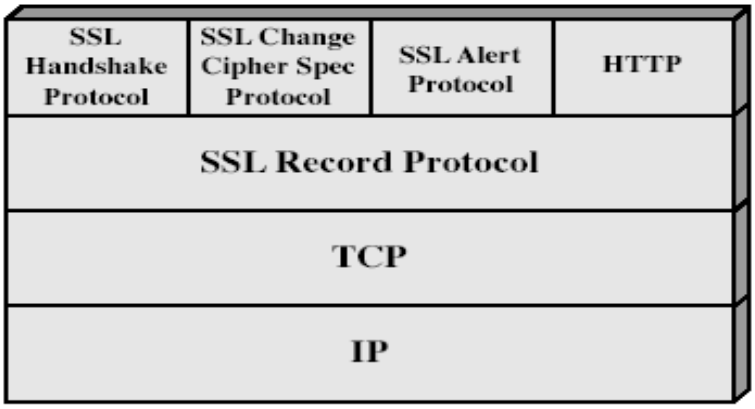
- Máy trạm sẽ gửi cho máy chủ số phiên bản SSL đang dùng, các tham số của thuật toán mã hoá, dữ liệu được tạo ra ngẫu nhiên và một số thông tin khác mà máy chủ cần để thiết lập kết nối với máy trạm.
- Máy chủ gửi cho máy trạm số phiên bản SSL đang dùng, các tham số của thuật toán mã hoá, dữ liệu được tạo ra ngẫu nhiên và một số thông tin khác mà máy trạm cần để thiết lập kết nối với máy chủ. Ngoài ra máy chủ cũng gửi chứng chỉ của nó đến máy trạm và yêu cầu chứng chỉ của máy trạm nếu cần.
- Máy trạm sử dụng một số thông tin mà máy chủ gửi đến để xác thực máy chủ. Nếu như máy chủ không được xác thực thì người sử dụng sẽ được cảnh báo và kết nối

không được thiết lập. Còn nếu như xác thực được máy chủ thì phía máy trạm sẽ thực hiện tiếp bước 4.

- Sử dụng tất cả các thông tin được tạo ra trong giai đoạn bắt tay ở trên, máy trạm (cùng với sự cộng tác của máy chủ và phụ thuộc vào thuật toán được sử dụng) sẽ tạo ra premaster secret cho phiên làm việc, mã hóa bằng khóa công khai mà máy chủ gửi đến trong chứng chỉ ở bước 2 và gửi đến máy chủ.
- Nếu máy chủ có yêu cầu xác thực máy trạm, thì phía máy trạm sẽ đánh dấu vào phần thông tin riêng chỉ liên quan đến quá trình "bắt tay" này mà hai bên đều biết. Trong trường hợp này, máy trạm sẽ gửi cả thông tin được đánh dấu và chứng chỉ của mình cùng với premaster secret đã được mã hóa tới máy chủ.
- Máy chủ sẽ xác thực máy trạm. Trường hợp máy trạm không được xác thực, phiên làm việc sẽ bị ngắt. Còn nếu máy trạm được xác thực thành công, máy chủ sẽ sử dụng khóa bí mật để giải mã premaster secret, sau đó thực hiện một số bước để tạo ra master secret.
- Máy trạm và máy chủ sẽ sử dụng master secret để tạo ra các khóa phiên , đó chính là các khóa đối xứng được sử dụng để mã hóa và giải mã các thông tin trong phiên làm việc và kiểm tra tính toàn vẹn dữ liệu.
- Máy trạm sẽ gửi một lời nhắn đến máy chủ thông báo rằng các thông điệp tiếp theo sẽ được mã hóa bằng khóa phiên. Sau đó nó gửi một lời nhắn đã được mã hóa để thông báo rằng phía máy trạm đã kết thúc giai đoạn "bắt tay".
- Máy chủ cũng gửi một lời nhắn đến máy trạm thông báo rằng các thông điệp tiếp theo sẽ được mã hóa bằng khóa phiên. Sau đó nó gửi một lời nhắn đã được mã hóa để thông báo rằng máy chủ đã kết thúc giai đoạn "bắt tay".
- Lúc này giai đoạn "bắt tay" đã hoàn thành và phiên làm việc SSL bắt đầu. Cả hai phía máy trạm và máy chủ sẽ sử dụng các khóa phiên để mã hóa và giải mã thông tin trao đổi giữa hai bên, và kiểm tra tính toàn vẹn dữ liệu

7.2.3. Kiến trúc SSL

SSL được thiết kế để dùng TCP cung cấp dịch vụ an toàn đầu cuối. Nó không phải là thủ tục duy nhất, mà có hai lớp thủ tục.



Ở đây kết nối SSL là:

- Tạm thời, đầu cuối đến đầu cuối, liên kết trao đổi.
- Gắn chặt với một phiên SSL.

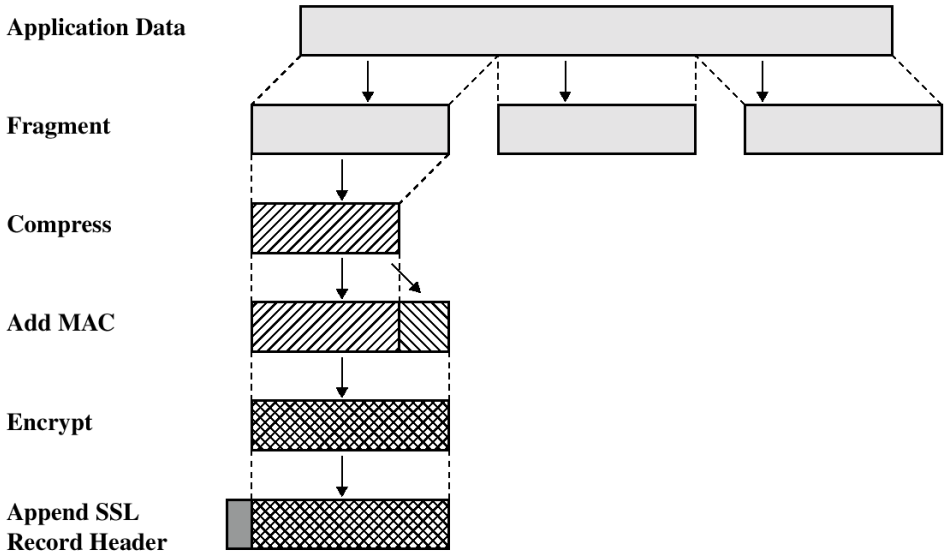
Và phiên SSL:

- Liên kết giữa người sử dụng và máy chủ.
- Được tạo bởi thủ tục HandShake Protocol.
- Xác định một tập các tham số mã hoá: định danh phiên, giấy chứng nhận X509, phương pháp nén, thuật toán mã hóa, khóa mật,…
- Có thể chia sẻ bởi kết nối SSL lặp.

7.2.3.1. Dịch vụ thủ tục bản ghi SSL

Dịch vụ thủ tục bản ghi SSL đảm bảo tính toàn vẹn của bản tin:

- Sử dụng MAC với khóa mật chia sẻ.
- Giống như HMAC nhưng với bộ đệm khác và cung cấp bảo mật.
- Sử dụng mã đối xứng với khóa chung xác định bởi thủ tục HandShake.
- IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128.
- Bản tin được nén trước khi mã.



Bước đầu tiên là chia gói, sau đó nén lại. Tiếp theo tính MAC của bản nén và đính kèm, ở đây khóa mật chung được sử dụng. Rồi mã hóa và bổ sung tiêu đề SSL.

7.2.3.2. Thủ tục thay đổi đặc tả mã SSL (SSL Change Cipher Spec Protocol)

Đây là một trong 3 giao thức chuyên biệt của SSL. Đây là mẩu tin đơn gồm 1 bit với giá trị 1, buộc trạng thái treo trở thành hiện thời và cập nhật bộ mã đang dùng.

7.2.3.3. Thủ tục nhắc nhở SSL (SSL Alert Protocol)

Truyền đi lời nhắc của SSL liên quan cho thành viên gồm 2 byte. Byte đầu chỉ rõ giá trị nhắc nhở hoặc cảnh báo. Byte thứ hai nêu các cảnh báo hoặc nhắc nhở cụ thể.

Nhắc nhở đặc biệt:

- Cảnh báo: mẩu tin không chờ đợi, bản ghi MAC tồi, lỗi giải nén, lỗi Handshake, tham số không hợp lệ.
- Nhắc nhở: đóng ghi chú, không chứng nhận, chứng nhận tồi, chứng nhận không được hỗ trợ, chứng nhận bị thu hồi, chứng nhận quá hạn, chứng nhận không được biết đến.

Mẩu tin nhắc nhở cũng được nén và mã như mọi dữ liệu SSL.

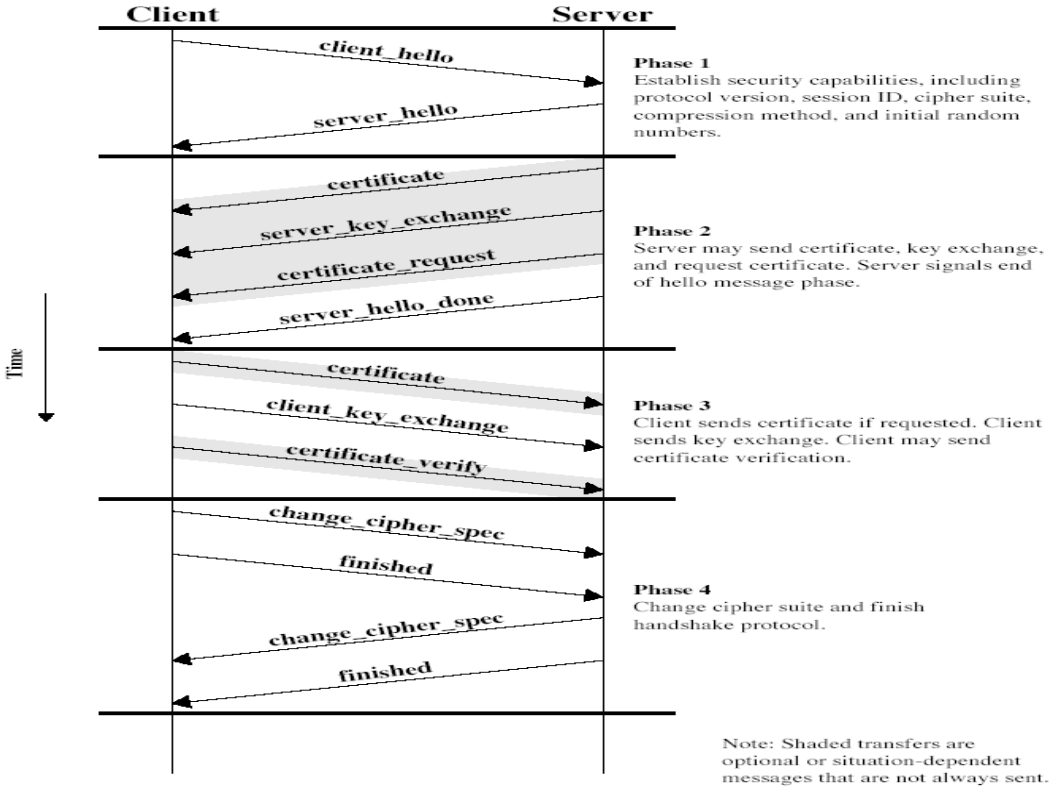
7.2.3.4. Thủ tục bắt tay SSL (SSL HandShake Protocol)

Phần phức tạp nhất của SSL là thủ tục bắt tay. Thủ tục này cho phép máy chủ và máy trạm:

- Xác thực nhau.
- Thỏa thuận thuật toán mã hóa và MAC.
- Thỏa thuận khóa mã sẽ dùng.

Nó bao gồm bốn giai đoạn trao đổi một loạt thông tin:

- Thiết lập các khả năng bảo mật.
- Xác thực máy chủ và trao đổi khoá
- Xác thực máy trạm và trao đổi khoá.
- Kết thúc việc trao đổi.



7.2.3.5. An toàn tầng vận chuyển (TLS)

TLS là sáng kiến từ IETF chuẩn với mục đích tạo ra SSL chuẩn. TLS được định nghĩa trong tài liệu RFC 2246 giống như SSLv3.

Với một số khác biệt nhỏ:

- Số ký hiệu kích thước bản ghi.
- Sử dụng HMAC thay cho MAC.
- Hàm giả ngẫu nhiên tăng độ mật.
- Có mã ghi chú bổ sung.
- Có một số thay đổi hỗ trợ mã.
- Thay đổi kiểu chứng nhận và thỏa thuận.

- Thay đổi bộ đệm và tính toán mã.

7.3. Thanh toán điện tử an toàn

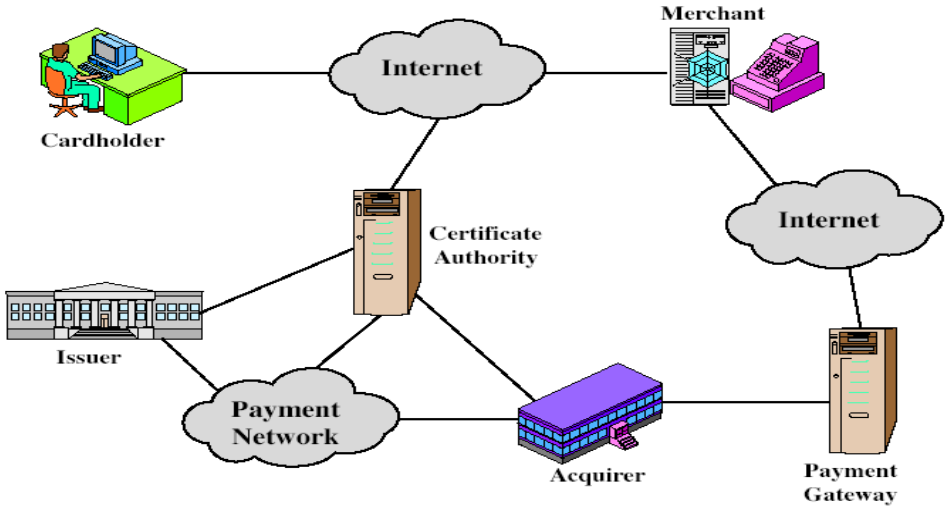
7.3.1. Yêu cầu

Đây là mã mở và đặc tả an toàn nhằm bảo vệ thanh toán thẻ tín dụng trên Internet. Nó được phát triển năm 1996 bởi Master, Visa Card và không phải hệ thống trả tiền. Thanh toán điện tử an toàn là tập các giao thức và định dạng an toàn dùng để

- Trao đổi an toàn giữa các đối tác.
- Tin tưởng vì sử dụng giấy chứng nhận X509v3.
- Riêng biệt vì hạn chế thông tin vừa đủ cho những người tham gia giao dịch.

Các thành phần tham gia Thanh toán điện tử:

- Người giữ thẻ: người mua là chủ sở hữu thẻ thanh toán hợp pháp do Ngân hàng cấp.
- Người bán: tổ chức cung cấp dịch vụ bán hàng trên mạng.
- Nơi cấp thẻ là tổ chức tài chính như ngân hàng cung cấp thẻ thanh toán.
- Tổ chức thanh toán: tổ chức tài chính thực hiện việc chuyển tiền từ thẻ thanh toán của người mua sang tài khoản của người bán. Thông thường người bán chấp nhận nhiều loại thẻ của nhiều ngân hàng khác nhau. Tổ chức thanh toán là trung gian được các ngân hàng và người bán ủy quyền.
- Cổng thanh toán: là chức năng của Tổ chức thanh toán dùng để xử lý hóa đơn trả tiền.
- Nơi cấp giấy chứng nhận: là tổ chức tin cậy có trách nhiệm cấp giấy chứng nhận X509 cho khóa công khai của chủ thẻ, người bán và cổng thanh toán.



7.3.2. Thanh toán điện tử an toàn

Ta mô tả trình tự các bước của một giao dịch thanh toán điện tử:

- Người mua mở tài khoản.
- Người mua nhận được chứng nhận.
- Người bán có chứng nhận của họ.
- Người mua đặt hàng.
- Người bán được kiểm chứng.
- Đơn đặt hàng và trả tiền được gửi.

- Người bán yêu cầu giấy phép trả tiền.
- Người bán duyệt đơn đặt hàng.
- Người bán cung cấp hàng và dịch vụ.
- Người bán yêu cầu trả tiền.

7.3.3. Chữ ký kép

Chúng ta có hai thông tin liên quan chặt chẽ với nhau là đơn mua hàng và hóa đơn thanh toán nhưng lại gửi cho hai đối tác khác nhau là người bán và Tổ chức thanh toán mà lại không cho các bên biết các thông tin không cần thiết, người bán không biết thông tin về thẻ thanh toán, Tổ chức thanh toán không biết thông tin về hàng hóa đã mua. Để giải quyết vấn đề đó người ta tạo ra chữ ký kép.

Người mua tạo chữ ký kép trên

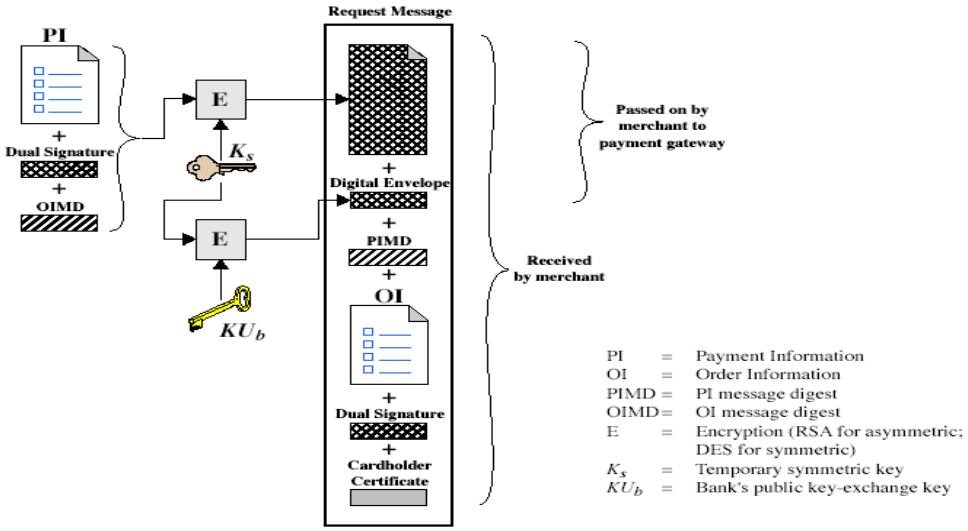
- Thông tin đơn đặt OI cho người bán.
- Thông tin trả tiền PI cho ngân hàng.
- Không bên nào biết chi tiết của người khác. Nhưng cần phải biết là họ được kết nối với nhau. Sử dụng chữ ký kép cho mục đích này.
- Ký trên bản ghép của OI và PI, ở đây H là hàm băm, KR_C là khóa riêng của chủ thẻ:

$$DS = E_{KR}[H(H(PI) \,||\, H(OI))]$$

7.3.4. Yêu cầu trả tiền

Trao đổi yêu cầu trả tiền gồm 4 mẩu tin sau:

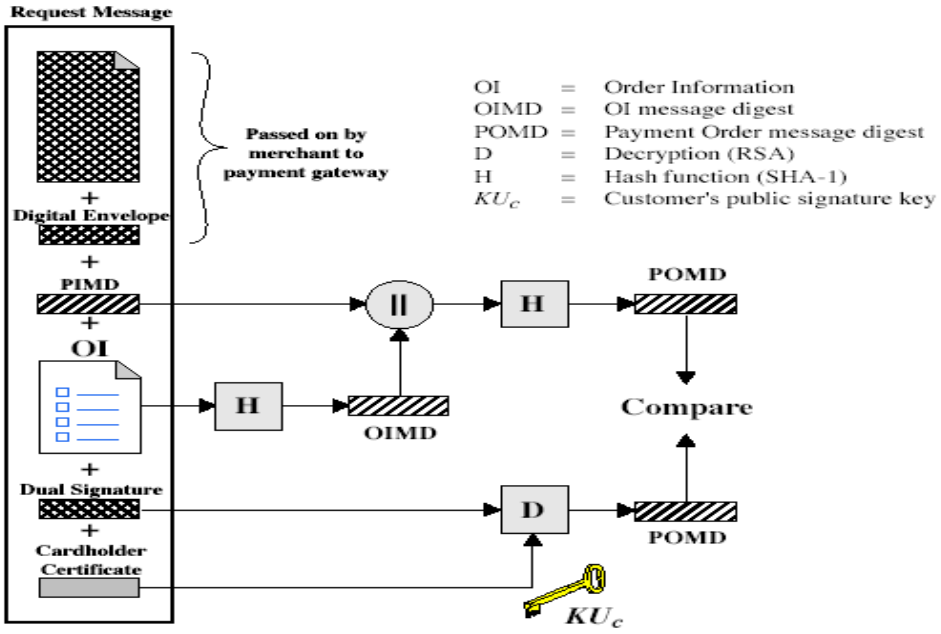
- Khởi tạo yêu cầu – nhận chứng nhận.
- Khởi tạo trả lời – ký trả lời.
- Yêu cầu trả tiền – của OI và PI.
- Trả lời trả tiền – đơn phúc đáp.
- Yêu cầu trả tiền – người mua.



Trong thông tin yêu cầu của người mua bao gồm phần gửi cho người bán và phần thông qua người bán chuyển tiếp cho cổng trả tiền. Phần gửi cho người bán có đơn mua hàng, chữ ký kép, giấy chứng nhận của chủ thẻ và bản băm của hóa đơn trả tiền.

Phần gửi chuyển cho cổng trả tiền gồm bản mã của khóa phiên được mã bằng khóa công khai của ngân hàng và bản mã của hóa đơn trả tiền được mã bằng khóa phiên.

Yêu cầu trả tiền – người bán



- Kiểm tra chứng nhận người giữ thẻ bằng chữ ký của CA.
- Kiểm tra chữ ký kép bằng cách sử dụng khóa chữ ký công khai của người mua để tin tưởng rằng đơn không bị giả mạo khi truyền và được ký sử dụng chữ ký khóa riêng của người giữ thẻ.
- Xử lý đơn đặt và gửi tiếp thông tin trả tiền cho cổng trả tiền để xác thực (mô tả sau).
- Gửi phản hồi trả tiền cho người giữ thẻ.

Giấy phép cổng trả tiền

- Kiểm chứng mọi chứng nhận .
- Giải mã phong bì điện tử của khối giấy phép và nhận được khóa đối xứng, sau đó giải mã khối giấy phép.
- Kiểm tra chữ ký của người bán trên khối giấy phép.
- Giải mã phong bì điện tử khối trả tiền, nhận được khóa đối xứng, sau đó giải mã khối trả tiền.
- Kiểm tra chữ ký kép trên khối trả tiền.
- Kiểm tra rằng, thanh toán ID nhận được từ người bán phù hợp với danh tính trong PI nhận được (không trực tiếp) từ người bán.
- Yêu cầu và nhận được giấy phép từ nơi phát hành.
- Gửi trả lời giấy phép cho người bán.

Nhận trả tiền

Người bán gửi cho cổng trả tiền yêu cầu nhận trả tiền. Cổng kiểm tra yêu cầu đó. Sau đó yêu cầu chuyển tiền đến tài khoản người bán. Thông báo cho người bán và chờ trả lời việc nhận.

7.4. Quản trị an ninh mạng

7.4.1. Khái niệm cơ bản về SNMP

Hệ thống quản trị mạng là tập hợp các công cụ để theo dõi và kiểm soát được tích hợp theo nghĩa sau:

- Giao diện thao tác duy nhất với tập các lệnh đủ mạnh và thân thiện để thực hiện hầu hết các nhiệm vụ quản trị mạng.
- Với số tối thiểu các các thiết bị riêng rẽ mà hầu hết phần cứng và phần mềm đòi hỏi cho quản trị mạng đều được tích hợp thành thiết bị đã có của người dùng.

Mô hình quản trị mạng được sử dụng cho Giao thức quản trị mạng đơn giản SNMP bao gồm những thành phần chính sau:

- Trạm quản trị;
- Tác tử quản trị;
- Cơ sở thông tin quản trị (MIB);
- Giao thức quản trị mạng.

Trong đó Trạm quản trị thường là thiết bị đứng tách rời nhưng có khả năng cài đặt trên hệ thống chia sẻ. Mặt khác Trạm quản trị phục vụ như giao diện cho người quản trị mạng kết nối vào hệ thống quản trị mạng. Trạm có tối thiểu:

- Tập các ứng dụng quản trị để phân tích dữ liệu, khắc phục lỗi, …
- Giao diện để người quản trị theo dõi và kiểm soát mạng;
- Có khả năng chuyển các yêu cầu của mạng thành việc theo dõi và kiểm soát thực tế các thành phần ở xa trong mạng;
- Cơ sở dữ liệu thông tin được lấy từ MIB của mọi thực thể được quản trị trên mạng.

Thành phần khác là quản trị tác tử. Các thiết bị chính như: máy chủ, bridges, routers và hubs có thể được trang bị SNMP, sao cho chúng có thể được điều khiển từ trạm quản trị. Các tác tử quản trị đáp ứng các yêu cầu về lấy thông tin và truyền hành động từ trạm.

Để quản trị các nguồn lực trong mạng, mỗi nguồn lực được thể hiện như một đối tượng. Mỗi đối tượng như một biến dữ liệu biểu diễn một khía cạnh của tác tử quản trị. Tập hợp các đối tượng được tham chiếu như cơ sở thông tin quản trị (MIB).

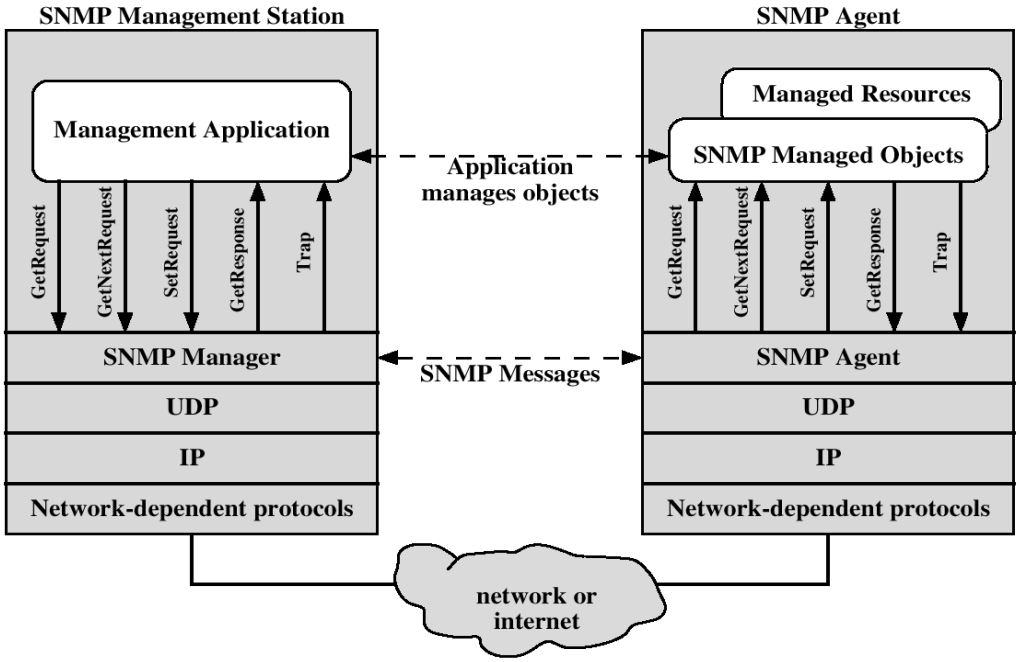
Các trạm và tác tử quản trị được kết nối thông qua giao thức quản trị mạng. Giao thức được sử dụng để quản trị mạng TCP/IP là giao thức quản trị mạng cơ bản SNMP. Nó bao gồm các khả năng chính sau:

- Get: cho phép trạm quản trị nhận giá trị của đối tượng tại tác tử.
- Set: cho phép trạm quản trị đặt giá trị của đối tượng tại tác tử.
- Notify: cho phép tác tử nhắc nhở trạm quản trị về một sự kiện quan trọng.

Kiến trúc quản trị mạng

Trên hình vẽ sau: từ trạm quản trị ba kiểu thông báo được gửi: GetRequest, GetNextRequest và SetRequest. Ba thông báo sẽ được trả lời bởi tác tử dạng thông báo GetResponse.

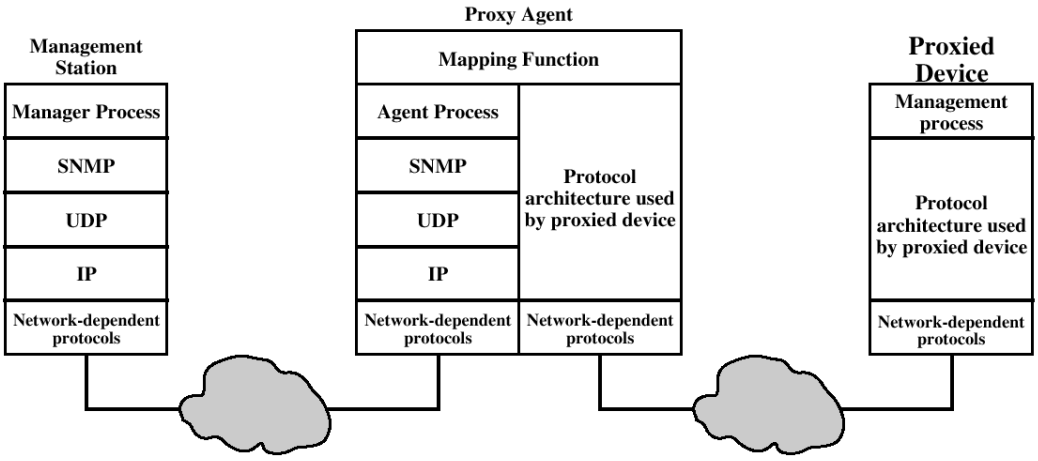
Vì SNMP dựa trên UDP là giao thức không kết nối nên SNMP cũng là không kết nối. Mỗi trao đổi là một giao dịch riêng rẽ giữa trạm và tác tử quản trị.



Proxies

Trong SNMP mọi tác tử và trạm quản trị đều cần hỗ trợ UDP và IP. Điều đó hạn chế quản trị trực tiếp đến các thiết bị và loại trừ một số bridges và modems mà không hỗ trợ một phần nào giao thức TCP/IP. Và còn một số hệ thống nhỏ chỉ cài đặt TCP/IP để hỗ trợ ứng dụng của chúng.

Để hỗ trợ các thiết bị không cài đặt được SNMP, khái niệm proxy đã được phát triển. Trong sơ đồ sau tác tử SNMP hoạt động như proxy đại diện cho một hoặc nhiều thiết bị. Kiểu kiến trúc giao thức như vậy thường gặp. Trạm quản trị gửi yêu cầu liên quan đến thiết bị cho tác tử proxy của nó. Tác tử proxy này chuyển yêu cầu thành giao thức quản trị được dùng trong thiết bị. Tương tự, nếu cảnh báo sự kiện từ thiết bị được truyền về proxy, proxy sẽ gửi nó đến trạm quản trị dưới dạng thông báo chuẩn của quản trị mạng.



Quản trị mạng phân tán

Trong sơ đồ quản trị mạng tập trung truyền thống, một máy chủ đóng vai trò trạm quản trị mạng và có thể có một hoặc hai trạm khác đóng vai trò dự phòng. Phần còn lại của các thiết bị trên mạng chứa phần mềm tác tử và MIB để theo dõi và kiểm soát từ trạm quản trị. Khi mạng lớn dần lên, sơ đồ tập trung như vậy không còn phù hợp, thông tin trao đổi qua lại quá nhiều. Trong sơ đồ phân tán có các trạm quản trị ở nhiều mức khác nhau, thường được nói đến như các máy chủ quản trị. Mỗi máy như vậy sẽ quản trị trực tiếp một số tác tử. Máy chủ trung gian đóng vai trò quản trị việc theo dõi và kiểm soát các tác tử trong trách nhiệm của nó. Nó cũng đóng vai trò tác tử cung cấp thông tin và tiếp nhận điều khiển từ máy chủ quản trị ở mức cao hơn.

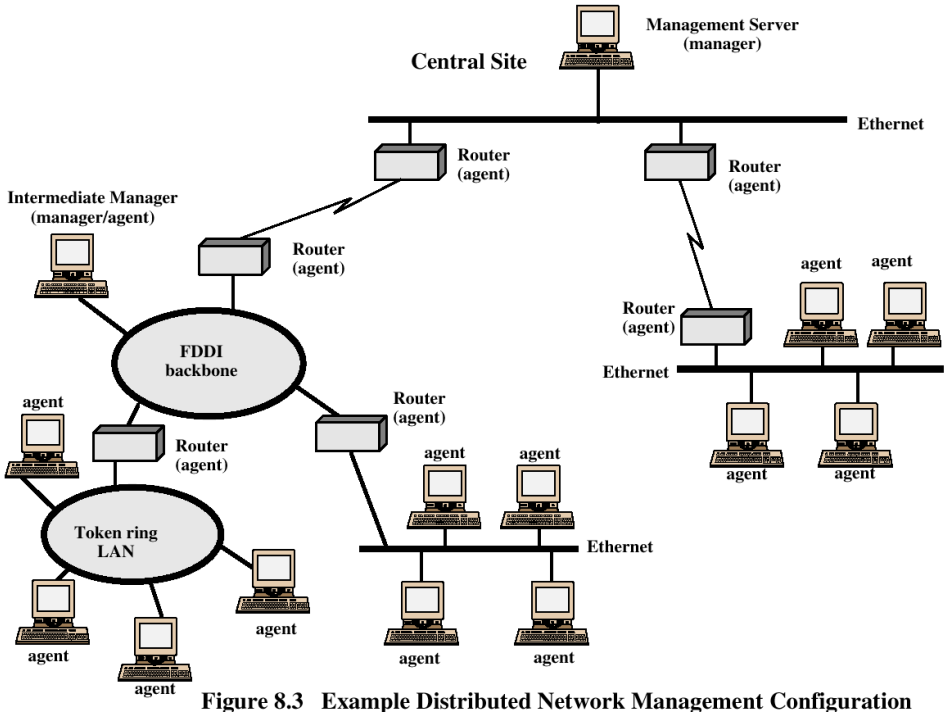


Figure 8.3 Example Distributed Network Management Configuration

7.4.2. Tiện ích cộng đồng (khu vực) SNMPv1

Mỗi tác tử kiểm soát MIB địa phương của nó và có thể kiểm soát việc sử dụng MIB của một số quản trị khác. Có ba khía cạnh khác nhau của việc kiểm soát đó:

- Dịch vụ xác thực: Tác tử mong muốn hạn chế truy cập đến MIB cho một số quản trị có chủ quyền.
- Chính sách truy cập: Tác tử muốn cung cấp một số quyền khác nhau cho một số quản trị khác nhau.
- Dịch vụ Proxy: Tác tử muốn hoạt động như proxy cho một số tác tử khác. Điều này kéo theo việc cài đặt dịch vụ xác thực hoặc/và chính sách truy cập cho các tác tử khác trên hệ thống proxy.

Có hai yếu tố hỗ trợ kiểm soát truy cập:

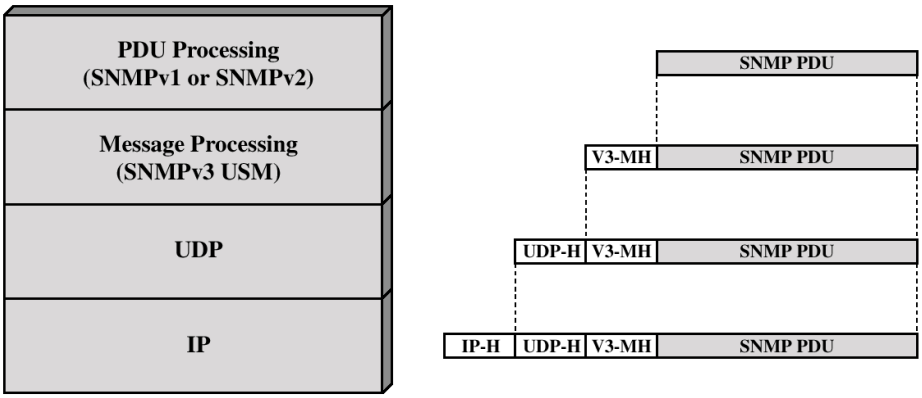
- SNMP MIB view: một tập các đối tượng trong MIB, chúng khác nhau cho mỗi cộng đồng khác nhau.
- SNMP access mode: có hai lựa chọn READ-ONLY hoặc READ-WRITE. Kiểu truy cập này được xác định cho mỗi cộng đồng.

Chính sách truy cập bao gồm tên cộng đồng SNMP và hồ sơ cộng đồng SNMP. Cộng đồng SNMP có hai thành phần là tác tử SNMP và tập các quản trị SNMP. Còn hồ sơ cộng đồng SNMP bao gồm các tập con của MIB xác định tầm nhìn tại tác tử đó cộng thêm với kiểu truy cập đến các đối tượng đó.

7.4.3. SNMPv3

SNMPv3 định nghĩa khả năng an ninh kết hợp với SNMPv2 hoặc SNMPv1. Sơ đồ sau mô tả định dạng của một đơn vị dữ liệu giao thức. Xuống mỗi tầng xử lý đơn vị dữ liệu được thêm phần đầu tương ứng. Thông tin trao đổi giữa trạm quản trị và tác tử được thể hiện dạng thông báo SNMP. SNMPv3 đặc tả mô hình an ninh của người sử dụng USM (User security model) trong phần đầu V3MH. Như vậy việc sử dụng SNMPv3 cho phép đặc tả yêu cầu an ninh của người sử dụng trong USM vào phần tiêu đề bổ sung của mỗi đơn vị dữ liệu giao thức. Phần thực thi xử lý các đơn vị dữ liệu sẽ kiểm soát quyền truy cập dựa trên mô hình an ninh của người sử dụng USM.

Kiến trúc SNMP



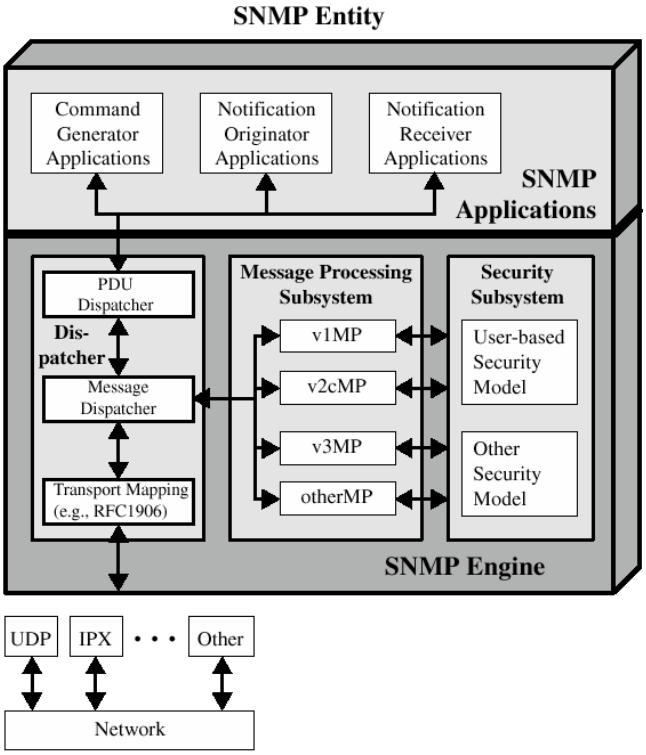
IP-H = IP header
UDP-H = UDP header
V3-MH = SNMPv3 message header
PDU = Protocol data unit

Kiến trúc SNMP bao gồm họ các thực thể SNMP đang tương tác và phân tán. Mỗi thực thể cài đặt một phần khả năng của SNMP và tác động như một nút tác tử, một nút quản trị hoặc kết hợp cả hai. Mỗi thực thể bao gồm tập các modules mà tương tác với nhau tạo nên dịch vụ.

Thực thể SNMP

Mỗi thực thể SNMP chứa một cơ chế SNMP duy nhất. Một cơ chế SNMP cài đặt các chức năng gửi, nhận, xác thực, mã/giải mã thông điệp và kiểm soát truy cập đến các đối tượng quản trị. Các chức năng này được cung cấp như dịch vụ cho một hay nhiều ứng dụng mà được cấu hình với cơ chế SNMP tạo thành thực thể SNMP.

Một tập các modules đòi hỏi cho tác tử SNMP, trong khi đó một tập khác yêu cầu cho quản trị SNMP. Sau đây ta xét thực thể SNMP cho quản trị SNMP. Hình vẽ sau là sơ đồ khối của quản trị SNMP truyền thống. Nó tương tác với tác tử SNMP bằng cách xuất các lệnh get, set và bằng việc nhận các thông điệp và cũng tương tác với các quản trị khác bằng cách xuất InformRequest PDU.



Command Generator Applications theo dõi và thao tác dữ liệu quản trị tại các tác tử ở xa, chúng xử dụng các đơn vị dữ liệu PDU bao gồm các lệnh Get, GetNext, GetBulk và Set. Notification Originator Applications khởi tạo các thông điệp không đồng bộ; Đơn vị dữ liệu giao thức PDU InformRequest được sử dụng cho ứng dụng này; Notification Receiver Applications xử lý thông điệp không đồng bộ được gửi đến.

Cơ chế SNMP thực hiện hai chức năng chính:

- Nó nhận đơn vị dữ liệu giao thức PDU từ các ứng dụng SNMP, thực hiện xử lý thông tin cần thiết, bao gồm chèn mã xác thực và mã hóa, sau đó đóng gói PDU thành thông điệp để truyền.
- Nó nhận thông điệp SNMP gửi đến từ tầng vận chuyển, thực hiện các xử lý cần thiết, bao gồm xác thực và giải mã, sau đó mở gói PDU từ thông điệp và truyền nó cho ứng dụng SNMP tương ứng.

Cơ chế SNMP cho tác tử cũng có các thành phần như đối với quản trị cộng thêm phân hệ kiểm soát truy cập. Cơ chế SNMP cho tác tử chứa ba kiểu ứng dụng. Command Responder Application cung cấp truy cập đến dữ liệu quản trị. Notification Originator Applications cũng khởi tạo các thông điệp không đồng bộ. Proxy Forwarder Application chuyển tiếp các thông điệp giữa các thực thể. Phân hệ quản lý quyền truy cập cung cấp dịch vụ xác thực quyền truy cập cho MIB để đọc và đặt giá trị mới cho các đối tượng quản trị.

Ứng dụng SNMPv3

Cụ thể các bước của ứng dụng SNMPv3 được xảy ra như mô tả trong sơ đồ sau:

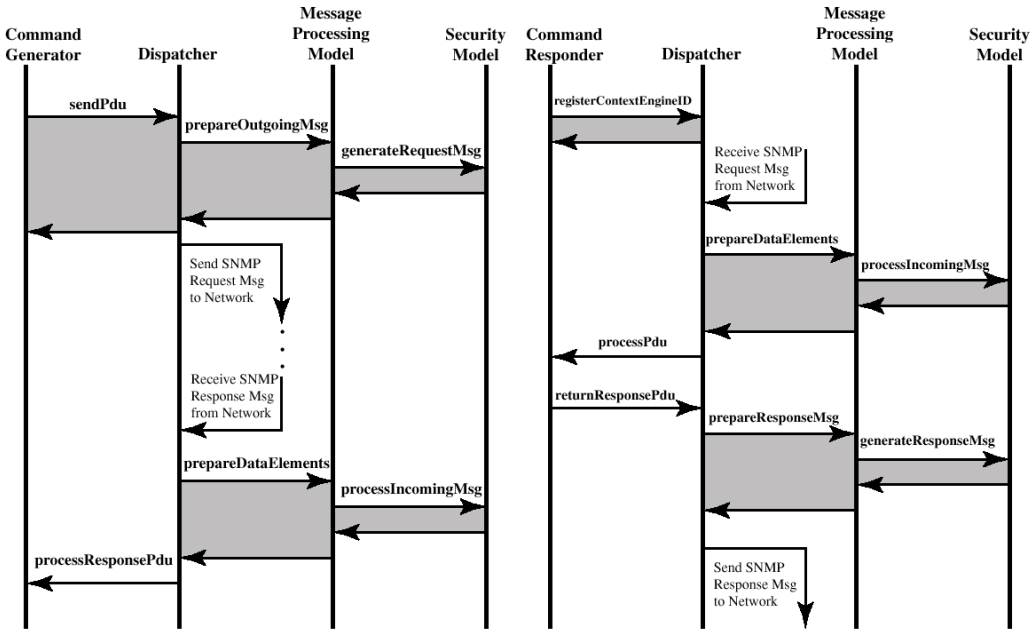
Command Generator application sử dụng hai module của Dispatcher là SendPdu và ResponsePdu. SendPdu cung cấp cho Dispatcher thông tin về đích đến, các tham số an ninh và bản thân PDU được gửi. Dispatcher sẽ sử dụng mô hình xử lý thông điệp và

mô hình an ninh để chuẩn bị gói tin. Dispatcher truyền gói tin đó cho lớp vận chuyển (UDP).

Command responder application sử dụng bốn module của Dispatcher là registerContextEngineID, unregisterContextEngineID, processPdu, returnResponsePdu và một module của phân hệ kiểm soát truy cập là isAccessAllowed. Command responder application kích hoạt command responder gắn nó với cơ chế SNMP để xử lý kiểu PDU tương ứng. Một khi command responder đã đăng ký thì mọi gói tin không đồng bộ nhận được sẽ chứa liên kết đăng ký đó. Sau đó command responder cởi gắn kết khỏi cơ chế SNMP bằng unregisterContextEngineID.

Dispatcher sử dụng processPdu phân phối các PDU yêu cầu cho các ứng dụng trả lời tương ứng. Lệnh command responder thực hiện các bước sau:

- Kiểm tra nội dung yêu cầu của PDU;
- Xác định quyền truy cập có được phép không cho thao tác quản trị trong PDU;
- Tham số mô hình an ninh chỉ rõ phân hệ quyền truy cập nào được sử dụng;
- Nếu quyền truy cập được phép, lệnh command responder sẽ thực hiện thao tác quản trị và chuẩn bị PDU trả lời.
- Gọi Dispatcher với returnResponsePdu để gửi PDU trả lời.



(a) Command Generator or Notification Originator (b) Command Responder

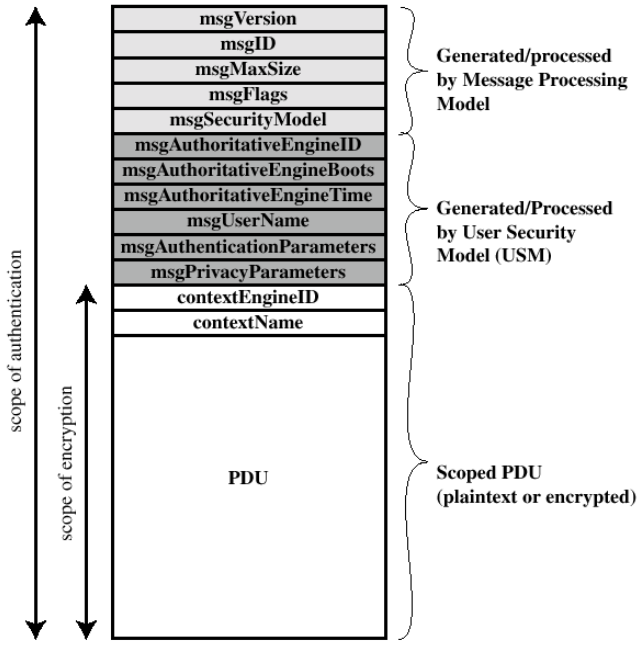
7.4.4. Mô hình xử lý thông điệp và mô hình an ninh người sử dụng

Mô hình xử lý thông điệp

Mô hình này nhận PDU từ Dipatcher, đóng gói nó thành thông điệp, sử dụng mô hình an ninh của người sử dụng USM bằng cách chèn thêm tham số và tiêu đề thông điệp.

Phần sau mô tả định dạng thông điệp SNMPv3 với mô hình an ninh người sử dụng USM (User Security Model).

Năm trường đầu tiên được sinh ra bởi mô hình xử lý thông điệp cho thông điệp gửi đi và chúng được xử lý cho thông điệp gửi đến. Sáu trường tiếp theo cho biết các tham số được sử dụng bởi USM. Cuối cùng, đơn vị dữ liệu giao thức PDU cùng với contextEngineID và contextName tạo thành gói PDU được dùng để xử lý.



Mô hình an ninh người sử dụng USM

USM cung cấp dịch vụ xác thực và bảo mật cho SNMP. Nó được thiết kế để chống các mối đe dọa sau:

- Sửa đổi thông tin: thực thể không được phép thực hiện các thao tác quản trị để sửa thông tin của các đối tượng.
- Mạo danh: thao tác quản trị không được phép đối với thực thể nào đó có thể tìm cách thực hiện.
- Sửa dòng truyền: thay đổi thứ tự, làm trì hoãn gói tin.
- Bảo mật: theo dõi thay đổi giữa quản trị và tác tử.

USM không được thiết kế để chống các đe dọa sau:

- Từ chối dịch vụ: kẻ tấn công có thể ngăn việc trao đổi giữa quản trị và tác tử.
- Phân tích đường truyền: kẻ tấn công có thể quan sát các mẫu tin truyền giữa quản trị và tác tử.

Các hàm mã hóa đòi hỏi có hai khóa: khóa riêng (privKey) và khóa xác thực (authKey). Các cặp khóa riêng biệt này được bảo trì cho mỗi người sử dụng sau:

- Người sử dụng địa phương: mọi người ở cơ chế SNMP đó có quyền thực hiện thao tác quản trị.

- Người sử dụng ở xa: mọi người ở cơ chế SNMP ở xa có trao đổi thông tin.

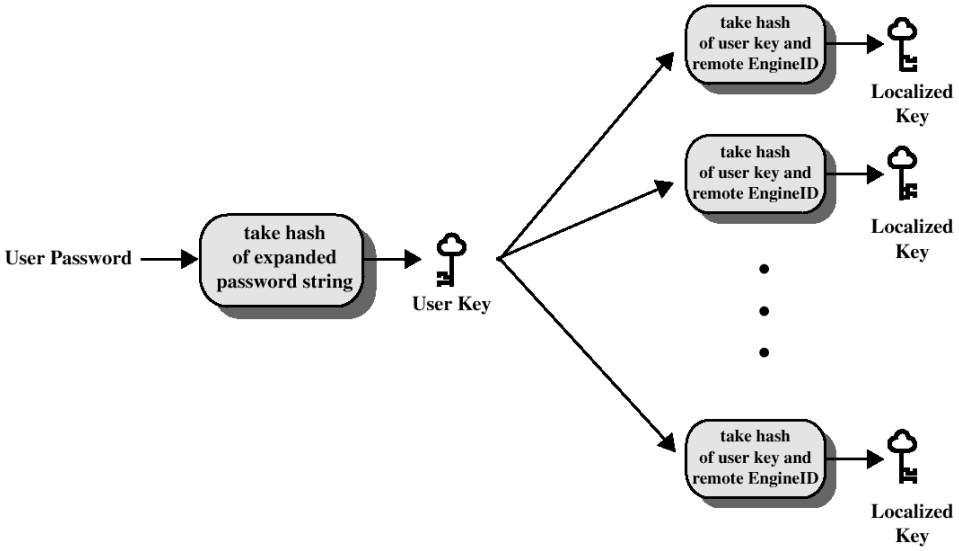
USM sử dụng các giao thức xác thực sau: HMAC-MD5-96, HMAC-SHA-96, đồng thời sử dụng chế độ mã khối dây chuyền CBC của chuẩn mã dữ liệu DES.

Trong mọi gói tin truyền, một trong hai thực thể là người truyền hoặc người nhận được chỉ định bởi cơ chế SNMP có chủ quyền tuân thủ các quy tắc sau:

- Khi thông điệp SNMP chờ đợi trả lời, thì người nhận thông điệp này phải có chủ quyền.
- Khi thông điệp SNMP không chờ đợi trả lời, thì người gửi thông điệp này phải có chủ quyền.

Quá trình địa phương hóa khóa

Bản băm mật khẩu người sử dụng kết hợp với bản băm định danh của máy ở xa để tạo ra khóa địa phương. Như vậy các khóa này phụ thuộc vào cả mật khẩu người sử dụng nhập và định danh của máy ở xa.



Mô hình kiểm soát quyền truy cập dựa trên tầm nhìn VACM (View-based access control model)

VACM có hai đặc tính quan trọng:

- VACM xác định việc truy cập đến các đối tượng được quản trị ở MIB địa phương bởi người sử dụng từ xa có được phép không;
- VACM sử dụng MIB để:
  - Xác định chính sách truy cập cho tác tử đó;
  - Làm cho nó có thể sử dụng để cấu hình từ xa.

VACM làm cho cơ chế SNMP được cấu hình để ép buộc một tập nào đó các quyền truy cập, được gọi là chính sách truy cập. Việc xác định quyền truy cập phụ thuộc vào các yếu tố sau:

- Người sử dụng đưa ra yêu cầu truy cập. Sử dụng VACM tác tử cho phép các người sử dụng có các quyền khác nhau. Chẳng hạn người quản trị mạng diện rộng có chủ

quyền lớn có thể thay đổi các đề mục tại MIB địa phương, trong khi đó người quản trị ở mức trung gian chỉ có thể theo dõi, có thể có quyền chỉ đọc và hạn chế truy cập đến MIB địa phương. Quyền truy cập được phân theo nhóm.

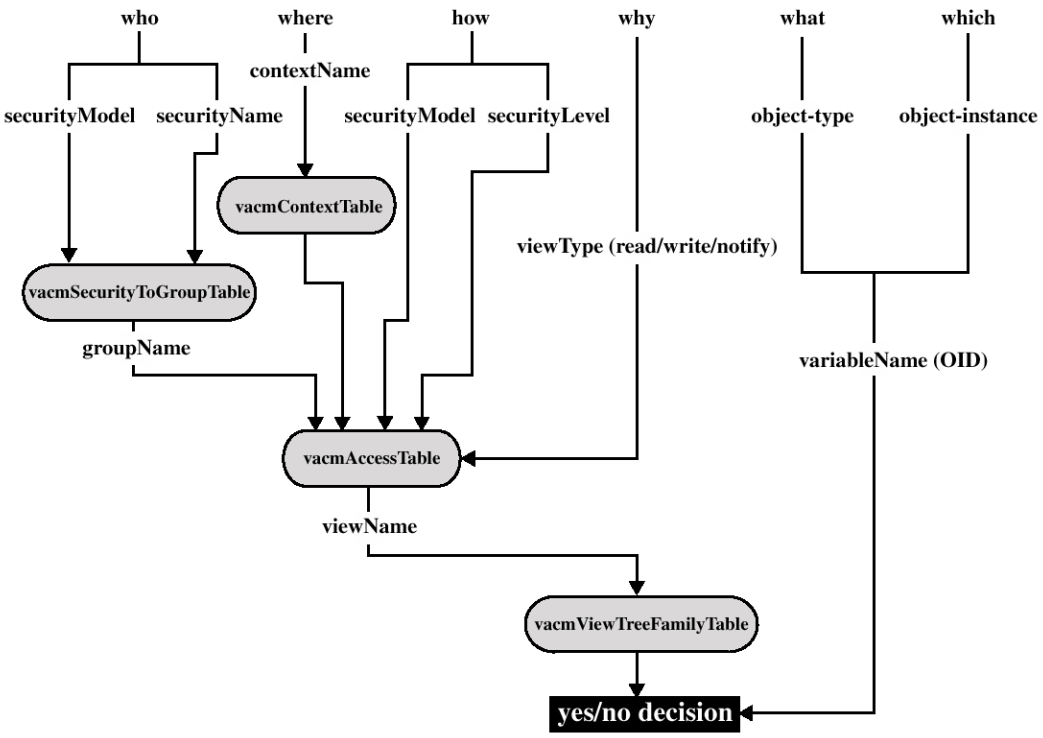
- Mức độ an ninh, theo đó yêu cầu được gửi trong thông điệp SNMP. Thông thường, tác tử yêu cầu xác thực quyền được viết.
- Mô hình an ninh được sử dụng để xử lý thông điệp yêu cầu. Tác tử được cấu hình để cung cấp các quyền truy cập khác nhau tùy thuộc vào mô hình an ninh.
- Kiểu truy cập được xử lý: đọc, viết và nhắc nhở.

Xử lý kiểm soát truy cập

Sơ đồ sau chỉ rõ cách dựa vào yêu cầu đầu vào và sử dụng các bảng khác nhau trong VACM MIB để ra quyết định kiểm soát quyền truy cập.

Ứng dụng SNMP sử dụng VACM thông qua module isAccessAllowed với các tham số đầu vào: securityModel, securityName, securityLevel, viewType, contextName và variableName. Mọi tham số này đều cần thiết để ra quyết định cho phép truy cập.

- Bảng vacmSecurityToGroupTable dựa vào securityModel và securityName để xác định groupName;
- Bảng vacmContextTable chứa danh sách các contextName đã được thừa nhận;
- Bảng vacmAccessTable dựa vào các tham số xác định viewName;
- Bảng vacmViewTreeFamilyTable sẽ lấy tầm nhìn phù hợp với viewName và hỗ trợ quyết định cấp quyền truy cập



TÓM LƯỢC CUỐI BÀI

Chúng ta đã xem xét

- An ninh IP và giao thức bảo mật Interrnet IPsec.
- An ninh Web và giao thức bảo mật tầng vận chuyển SSL.
- Chuẩn thanh toán điện tử an toàn SET.

CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

1. IPSec là cơ chế an ninh không cung cấp dịch vụ nào:
   A. Bảo mật
   B. Xác thực
   C. Chống từ chối
   D. Quản trị khóa
2. Đâu không phải là lợi ích của IPSec
   A. Kiểm soát đi qua Router cài IPSec
   B. Trong suốt với mọi ứng dụng
   C. Cung cấp dịch vụ an ninh cho người sử dụng riêng biệt
   D. Là dịch vụ an ninh hướng ứng dụng
3. Đâu không phải là thành phần của kiến trúc IPSec
   A. Tiêu đề xác thực AH
   B. Giao thức bắt tay
   C. Bao bọc tải trọng bao mật ESP
   D. Quản trị khóa
4. IPSec không cung cấp khả năng:
   A. Kiểm soát truy cập, toàn vẹn không kết nối
   B. Bảo mật dữ liệu
   C. Xác thực dữ liệu gốc, từ chối tải lại
   D. Đảm bảo tính sẵn sàng
5. Giao thức Tiêu đề xác thực không cung cấp khả năng:
   A. Xác thực gói IP
   B. Bảo mật dữ liệu
   C. Chống mạo danh địa chỉ IP
   D. Chống trì hoãn gói IP
6. Điều gì AH không thực hiện được trong chế độ vận tải
   A. Xác thực tải trọng IP
   B. Xác thực một phần được chọn của tiêu đề IP
   C. Xác thực toàn bộ gói IP
   D. Xác thực phần mở rộng tiêu đề IP6
7. Điều gì AH không thực hiện được trong chế độ đường ống
   A. Xác thực toàn bộ gói IP bên trong
   B. Xác thực một phần được chọn của tiêu đề IP ngoài
   C. Xác thực toàn bộ gói IP bên ngoài
   D. Xác thực phần mở rộng tiêu đề IP6
8. Trường nào không có trong định dạng AH:
   A. NextHeader và Payload length
   B. Security Parameter Index
   C. Padding

D. Sequence Number

9. Bao bọc tải trọng bảo mật ESP không cung cấp khả năng nào
   A. Trao đổi khóa
   B. Bảo mật nội dung tin và luồng truyền có giới hạn
   C. Có lựa chọn xác thực
   D. Hỗ trợ rộng việc lựa chọn mã, xác thực, bô đệm
10. Điều gì ESP có xác thực không thực hiện được trong chế độ vận chuyển
   A. Xác thực tiêu đề IP
   B. Mã tải trọng IP
   C. Mã phần mở rộng tiêu đề IP6
   D. Xác thực tải trọng IP
11. Điều gì ESP có xác thực không thực hiện được trong chế độ đường ống
   A. Mã toàn bộ gói IP trong
   B. Xác thực toàn bộ gói IP trong
   C. Xác thực tiêu đề IP ngoài
   D. Mã tiêu đề IP ngoài
12. Trường nào không có trong định dạng ESP:
   A. Security Parameter Index
   B. Payload Length
   C. Sequence Number
   D. NextHeader và Pad length
13. Đâu không phải là thành phần trong kiến trúc của SSL
   A. Giao thức bản ghi SSL
   B. Giao thức bắt tay SSL
   C. Giao thức cảnh báo và thay đổi đặc tả mã SSL
   D. Giao thức xác thực
14. Mục nào không phải là mục đích của một phiên SSL
   A. Liên kết người sử dụng với máy chủ
   B. Được tạo bởi giao thức bắt tay SSL
   C. Chỉ dùng cho một kết nối
   D. Xác định một tập các tham số mã
15. Bước nào không nằm trong thao tác bản ghi SSL:
   A. Chia đoạn và nén
   B. Bổ sung mã xác thực MAC
   C. Mã hóa và bổ sung tiêu đề bản ghi SSL
   D. Cảnh báo các chứng nhận không hợp lệ
16. Mục nào không phải là trường trong định dạng của bản ghi SSL
   A. Kiểu nội dung và phiên bản chính
   B. Phiên bản phụ và độ dài nén
   C. HMAC
   D. Mã văn bản rõ và MAC
17. Đâu không phải là cải tiến của TLS so với SSL
   A. Dùng HMAC thay cho MAC, dùng hàm giả ngẫu nhiên tăng độ mật
   B. Có ghi chú mã bổ sung, thay đổi đệm và tính toán mã
   C. Thay đổi kiểu chứng nhận và thỏa thuận
   D. Hỗ trợ mọi mã giống SSLv3 kể cả Fortezza
18. Điều nào không cần thiết trong giao dịch điện tử:
   A. Gửi Thông tin mua hàng cho người bán
   B. Gửi Thông tin trả tiền cho cổng thanh toán
   C. Gửi thông tin mua và thông tin trả tiền cho người bán
   D. Chữ ký kép của người mua gắn thông tin mua và thông tin trả tiền

19. Chữ ký kép chứa các thông tin nào
    A. Bản băm thông tin mua hàng
    B. Bản băm thông tin trả tiền
    C. Băm hai bản trên và mã bằng khóa riêng người mua
    D. Ghép hai bản băm trên và mã bằng khóa riêng người mua
20. Mục nào không nằm trong qui trình chủ thẻ gửi yêu cầu trả tiền
    A. Dùng khóa công khai ngân hàng mã khóa phiên
    B. Dùng khóa riêng người mua mã khóa phiên
    C. Dùng khóa phiên mã thông tin tra tiền đính kèm chữ ký điện tử kép và bản băm thông tin mua hàng
    D. Gửi thông tin mua, bản băm trả tiền và bản mã mục C cho người bán
21. Mục nào không nằm trong qui trình người bán kiểm tra yêu cầu trả tiền
    A. Băm thông tin mua hàng
    B. Ghép với bản băm thông tin trả tiền và băm tiếp
    C. Giải mã chữ ký kép bằng khóa phiên rồi sánh với B
    D. Giải mã chữ ký kép bằng khóa công khai người mua rồi sánh với B

ĐÁP ÁN CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

Câu 1: C, Vì ở đây không có chữ ký điện tử
Câu 2: D, Đây là dịch vụ an ninh tầng mạng trong suốt với các ứng dụng
Câu 3: B, Giao thức bắt tay là thuộc về SSL không phải của IPSec
Câu 4: D, Đảm bảo tính sãn sàng không thuộc phạm vi của IPSec, cần đến công nghệ Cluster
Câu 5: B, Ở đây không thực hiện mã hóa dữ liệu
Câu 6: C, Cần để rõ địa chỉ IP để gói tin đến đúng đích
Câu 7: C, Chỉ xác thực toàn bộ gói IP bên trong
Câu 8: C, Chỉ xác thực nên không cần thêm bộ đệm
Câu 9: A, Đây là nhiệm vụ của quản trị khóa
Câu 10: A, Muốn dùng lựa chọn này sử dụng AH
Câu 11: C, D, Tiêu đề IP ngoài không thuộc thẩm quyền bảo vệ của ESP
Câu 12: B, Trường này không có trong mô tả định dạng của ESP
Câu 13: D, Không có giao thức xác thực riêng trong thành phần SSL
Câu 14: C, Được thiết kế để dùng cho phiên làm việc có thể có nhiều kết nối
Câu 15: D, Cảnh báo thuộc chức năng giao thức cảnh báo
Câu 16: C, Không dùng HMAC
Câu 17: D, TLS cải tiến hỗ trợ nhiều loại mã
Câu 18: C, Thông tin trả tiền tường minh không được gửicho người bán
Câu 19: D, Ghép hai bản băm và ký khóa riêng gọi là chữ ký kép
Câu 20: B, Khóa phiên dành cho Ngân hàng, nên dùng khóa công khai của ngân hàng mã khóa phiên
Câu 21: C, Người bán không dùng khóa phiên mà dùng khóa công khai người mua để kiểm tra chữ ký kép

THUẬT NGỮ TRONG BÀI

- IPSec: là cơ chế an ninh IP tổng quan. Nó cung cấp: xác thực, bảo mật và quản trị khoá. IPSec được dùng trên mạng LAN, mạng WAN riêng và chung và trên cả mạng Internet.

- Tiêu đề xác thực AH: cung cấp sự hỗ trợ cho toàn vẹn dữ liệu và xác thực của các gói IP; hệ thống đầu cuối/chuyển mạch có thể xác thực người sử dụng/ứng dụng; ngăn tấn công theo dõi địa chỉ bằng việc theo dõi các chỉ số dãy và chống tấn công tải lại.
- Bao bọc tải trọng bảo mật ESP: đảm bảo bảo mật nội dung mẩu tin và luồng vận chuyển giới hạn, có lựa chọn cung cấp dịch vụ xác thực như AH và hỗ trợ phạm vi rộng các mã, các chế độ mã và bộ đệm.
- Liên kết an toàn SA: đây là quan hệ một chiều giữa người gửi và người nhận mà cung cấp dịch vụ an ninh cho luồng vận chuyển và được xác định bởi 3 tham số
    - Chỉ số các tham số bảo mật (SPI): là xâu bit gắn với liên kết, nó cho phép hệ thống nhận tin lựa chọn liên kết để xử lý.
    - Địa chỉ IP đích
    - Định danh giao thức bảo mật: chỉ rõ liên kết là AH hay ESP.

- SSL là dịch vụ an toàn tầng vận chuyển, ban đầu được phát triển bởi Netscape. Sau đó phiên bản 3 của nó được thiết kế cho đầu vào công cộng và trở thành chuẩn Internet, được biết đến như an toàn tầng vận chuyển TLS (Transport Layer Security). Giao thức SSL hoạt động dựa trên hai nhóm con giao thức là giao thức "bắt tay" và giao thức "bản ghi".
- Giao thức "bắt tay" xác thực các bên tham gia và xác định các tham số giao dịch giữa hai đối tượng có nhu cầu trao đổi thông tin hoặc dữ liệu.
- Giao thức "bản ghi" xác định khuôn dạng cho tiến hành mã hóa và truyền tin hai chiều giữa hai đối tượng đó. Giao thức SSL "bắt tay" sẽ sử dụng SSL "bản ghi" để trao đổi một số thông tin giữa máy chủ và máy trạm vào lần đầu tiên thiết lập kết nối SSL.
- Thanh toán điện tử an toàn: là tập các giao thức và định dạng an toàn dùng để trao đổi an toàn giữa các đối tác, tin tưởng vì sử dụng giấy chứng nhận X509v3, riêng biệt vì hạn chế thông tin vừa đủ cho những người tham gia giao dịch.
- Chữ ký kép: Chúng ta có hai thông tin liên quan chặt chẽ với nhau là đơn mua hàng và hóa đơn thanh toán nhưng lại gửi cho hai đối tác khác nhau là người bán và Tổ chức thanh toán. Mà lại không cho các bên biết các thông tin không cần thiết, người bán không biết thông tin về thẻ thanh toán, Tổ chức thanh toán không biết thông tin về hàng hóa đã mua. Để giải quyết vấn đề đó người ta tạo ra chữ ký kép.
- Tổ chức thanh toán: tổ chức tài chính thực hiện việc chuyển tiền từ thẻ thanh toán của người mua sang tài khoản của người bán. Thông thường người bán chấp nhận nhiều loại thẻ của nhiều ngân hàng khác nhau. Tổ chức thanh toán là trung gian được các ngân hàng và người bán ủy quyền.

CÂU HỎI THƯỜNG GẶP

Câu 1. Cho một số ví dụ ứng dụng của Ipsec?
Câu 2. Các dịch vụ được cung cấp bởi Ipsec là gì?
Câu 3. Mô tả giao thức tiêu đề xác thực AH? Định dạng và các chế độ làm việc của nó?
Câu 4. Mô tả giao thức bao bọc tải trọng bảo mật ESP? Định dạng và các chế độ làm việc của nó?
Câu 5. Các tham số nào xác định liên kết an ninh SA? Và các tham số nào đặc trưng cho bản chất của một SA cụ thể?
Câu 6. Nêu sự khác biệt giữa chế vận chuyển và chế độ đường ống?
Câu 7. Tấn công trì hoãn là gì?
Câu 8. Nêu các cách tiếp cận cơ bản của các liên kết an toàn?
Câu 9. SSL bao gồm những giao thức gì?

Câu 10. Sự khác biệt giữa SSL kết nối và SSL phiên là gì?
Câu 11. Các dịch vụ nào được cung cấp bởi giao thức bản ghi SSL?
Câu 12. Nêu các bước được thực hiện trong giao thức bản ghi SSL?
Câu 13. Nêu các bước trong giao thức bắt tay SSL?
Câu 14. Mô tả các bước của Thanh toán điện tử an toàn SET?
Câu 15. Nêu cách tạo ra chữ ký kép?
Câu 16. Mô tả quá trình xử lý trả tiền của người mua?
Câu 17. Mô tả quá trình xử lý trả tiền của người bán?
Câu 18. Mô tả quá trình xử lý trả tiền của cổng trả tiền?

TRẢ LỜI CÂU HỎI THƯỜNG GẶP

1. Một số ví dụ IPSec:
   - Chi nhánh Công ty kết nối qua Internet
   - Truy cập từ xa qua Internet đến mạng cục bộ
   - An ninh thương mại điện tử tăng cường.
2. Dịch vụ cung cấp bởi IPSec là:
   - Kiểm soát truy cập
   - Toàn vẹn không kết nối
   - Xác thực dữ liệu gốc
   - Chống tấn công lặp
3. Xem bài giảng
4. Xem bài giảng
5. Ba tham số xác định liên kết an ninh là
   - Chỉ số các tham số an ninh SPI
   - Địa chỉ IP đích
   - Định danh thủ tục an ninh
6. Sự khác biệt giữa chế độ vận chuyển và đường ống là
   - Chế độ vận chuyển xác thực 1 phần tiêu đề IP (AH), mã hóa tải trọng IP (ESP)
   - Chế độ đường ống xác thực (AH) và mã hóa (ESP) toàn bộ gói IP trong
7. Tấn công trì hoãn: ở đó kẻ tấn công nhận bản sao của gói xác thực và gửi lại sau đến cùng đích đó
8. Các cách tiếp cận liên kết an ninh cơ bản:
   - Hai máy chủ cài IPSec
   - Hai cổng cài đặt IPSec, không máy chủ nào cài IPSec
   - Hai cổng cài đặt IPSec, các máy chủ đầu cuối cài IPSec
   - Truy cập từ xa: máy chủ từ xa, tường lửa và máy chủ mạng con cài IPSec
9. SSL gồm 2 tầng thủ tục trên TCP: Giao thức bản ghi và trên đó là Giao thức bắt tay, Thay đổi đặc tả mã, Cảnh báo và http

10. Sự khác biệt giữa SSL kết nối và phiên:
    - Kết nối SSL: tạm thời, đầu cuối đến đầu cuối, liên kết trao đổi, gắn chặt với một phiên
    - Phiên SSL: Liên kết giữa người sử dụng và máy chủ, tạo bởi thủ tục HandShake Protocol, Xác định một tập các tham số mã hoá, chia sẻ bởi kết nối SSL lặp.
11. Giao thức bản ghi cung cấp dịch vụ: bảo mật và toàn vẹn thông điệp
12. Các bước trong Giao thức bản ghi: phân đoạn, nén, MAC, mã, thêm tiêu đề SSL
13. Giao thức bắt tay có 4 pha: thiết lập tham số an ninh, xác thực máy chủ, xác thực máy trạm, trao đổi đặc tả mã và kết thúc

14. Xem bài giảng
15. Tạo chữ ký kép: Băm đơn mua hàng và thông tin trả tiền, băm tiếp bản ghép chúng và mã bằng khóa riêng người mua

CÂU HỎI TỰ LUẬN

Câu 1. Nêu một số ứng dụng của IPsec? Lợi ích khi dùng IPsec?

Câu 2. Nêu kiến trúc của IPsec?

Câu 3. Các dịch vụ mà IPsec có thể cung cấp trên tầng IP là gì?

Câu 4. Liên kết SA được định danh duy nhất bởi bộ ba thuộc tính nào? Liệt kê các tham số SA?

Câu 5. Nêu các trường của Tiêu đề xác thực AH?

Câu 6. Nêu định dạng gói tin IP4 và IP6 trước và sau khi áp dụng AH trong chế độ vận chuyển?

Câu 7. Nêu định dạng gói tin IP4 và IP6 trước và sau khi áp dụng AH trong chế độ đường hầm?

Câu 8. Nêu định dạng của giao thức Bao bọc tải trọng bảo mật ESP?

Câu 9. Mô tả chế độ vận chuyển và đường hầm của ESP?

Câu 10. Mô tả 4 trường hợp kết hợp an ninh cơ bản?

Câu 11. Nêu các mối đe dọa an ninh Web?

Câu 12. Nhiệm vụ an ninh của SSL là gì?

Câu 13. Nêu kiến trúc SSL?

Câu 14. Mô tả thủ tục Bản ghi SSL?

Câu 15. Mô tả thủ tục Bắt tay SSL?

Câu 16. Nêu các yêu cầu an ninh của Thanh toán điện tử an toàn SET?

Câu 17. Nêu trình tự các sự kiện trong Thanh toán điện tử?

Câu 18. Mô tả chữ ký kép trong SET?

Câu 19. Nêu sơ đồ người mua gửi yêu cầu trả tiền?

Câu 20. Nêu sơ đồ chứng nhận trả tiền?

Câu 21. Mô tả các thành phần cơ bản của mô hình quản trị mạng?

Câu 22. Nêu vai trò của Trạm quản trị mạng?

Câu 23. Giải thích nhiệm vụ của Tác tử quản trị mạng?

Câu 24. Giải thích sơ đồ kiến trúc quản trị mạng? Nêu vai trò tác tử proxy trong mô hình quản trị mạng?

Câu 25. Mô tả cấu hình của mô hình quản trị mạng phân tán?

Câu 26. Nêu tiện ích khu vực của giao thức quản trị mạng SNMP?

Câu 27. Mô tả các thành phần của thực thể SNMP? Các chức năng chính của cơ chế SNMP là gì?

Câu 28. Mô tả các bước của ứng dụng SNMPv3? Nêu mô hình xử lý thông điệp SNMPv3?

Câu 29. Mô tả mô hình VACM? Việc kiểm soát quyền truy cập phụ thuộc vào các yếu tố nào?

BÀI TẬP TRẮC NGHIỆM

1. **Ví dụ nào không đúng về việc IPsec có thể cung cấp truyền thông an toàn trên các mạng?**

A. Kết nối an toàn với chi nhánh công ty trên Internet;
B. Truy cập từ xa an toàn trên Internet;
C. Thiết lập kết nối các mạng nội bộ với nhau;
D. Hỗ trợ bảo mật và xác thực trên mạng hàng ngang.

2. An ninh tầng IP không đảm bảo chức năng nào?

A. Xác thực;
B. Chống từ chối dịch vụ;
C. Bảo mật;
D. Quản trị khóa.

3. Đâu không phải là lợi ích khi dùng Ipsec?

A. Khi cài trên bức tường lửa hoặc router nó cung cấp an ninh cho mọi đường truyền qua lại mà sử dụng IP.
B. IPsec xử lí các vấn đề an ninh về đường truyền trong nội bộ công ty hoặc giữa một nhóm người trong công ty.
C. IPsec nằm dưới tầng vận chuyển, nên nó trong suốt với các ứng dụng - không cần thay đổi các phần mềm của người sử dụng;
D. IPsec có thể cung cấp an ninh cho người sử dụng đơn lẻ, truy cập từ xa vào mạng của công ty.

4. IPsec không thể cung cấp dịch vụ nào?

A. Kiểm soát truy cập;
B. Toàn vẹn không kết nối;
C. Xác thực dữ liệu gốc;
D. Chống từ chối người gửi.

5. AH không cung cấp dịch vụ nào?

A. Bảo mật luồng truyền;
B. Xác thực dữ liệu gốc;
C. Kiểm soát truy cập;
D. Từ chối gói tin bị làm trễ.

6. ESP chỉ bảo mật không cung cấp dịch vụ nào?

A. Bảo mật;
B. Xác thực dữ liệu gốc;
C. Kiểm soát truy cập;
D. Bảo mật luồng truyền.

7. ESP bảo mật và xác thực không cung cấp dịch vụ nào?

A. Bảo mật;
B. Xác thực dữ liệu gốc;
C. Kiểm soát truy cập;
D. Tính sẵn sàng.

8. Trường nào không tham gia bộ thuộc tính duy nhất của liên kết an ninh SA?

A. Chỉ số tham số an ninh SPI;
B. Số đếm dãy số;
C. Địa chỉ IP đích;
D. Định danh giao thức an ninh AH hoặc ESP.

9. Tiêu đề xác thực AH không chứa các trường nào?
A. Next header và Payload length;
B. Reserved;
C. Pad length;
D. SPI và Sequence number.

10. Chế độ vận chuyển của AH không có trường nào trong IP4?
A. Tiêu đề IP gốc;
B. AH được bổ sung;
C. TCP;
D. IP mới được thêm vào.

11. Chế độ đường hầm của AH không có trường nào trong IP4?
A. Tiêu đề IP gốc;
B. Tiêu đề mở rộng;
C. TCP;
D. IP mới được thêm vào.

12. Bao bọc tải trọng bảo mật ESP không chứa các trường nào?
A. Next header và Payload length;
B. SPI;
C. Sequence number;
D. Dữ liệu tải trọng và dữ liệu xác thực.

13. Quản trị khóa là một phần của IPsec bao gồm xác định và phân phối khóa mật giành cho trao đổi nhận và gửi AH và ESP. Thông thường có số khóa là:
A. 2;
B. 3 ;
C. 4 ;
D. 6.

14. Kiến trúc SSL không bao gồm thành phần nào
A. Giao thức TCP và IP;
B. Giao thức bản ghi SSL;
C. Giao thức Bắt tay, HTTP;
D. Giao thức xác thực.

15. Giao thức bản ghi SSL không bao gồm bước nào sau đây?
A. Phân đoạn dữ liệu, nén và bổ sung Mac;
B. Bổ sung bản băm hash;

C. Mã hóa;
D. Bổ sung tiêu đề bản ghi SSL.

16. Mục tiêu của giao thức Bắt tay không gồm phần nào?

A. Xác thực nhau;
B. Thỏa thuận thuật toán mã hóa và MAC;
C. Thỏa thuận khóa mã sẽ dùng;
D. Thỏa thuận hàm băm sẽ dùng.

17. Giao thức bắt tay SSL không bao gồm bước nào?

A. Thiết lập các khả năng bảo mật;
B. Mã hóa thông tin trao đổi;
C. Xác thực máy chủ và trao đổi khoá;
D. Xác thực máy trạm và trao đổi khoá.

18. Mục nào không thuộc yêu cầu của Thanh toán điện tử an toàn?

A. Cung cấp bảo mật thông tin đặt hàng và trả tiền;
B. Tin tưởng sự toàn vẹn của mọi dữ liệu truyền;
C. Cung cấp xác thực người giữ thẻ là người sử dụng tài khoản thẻ hợp pháp;
D. Đảm bảo cho bên bán biết thông tin tài khoản của người mua.

19. Mục nào không thuộc trình tự sự kiện trong Thanh toán điện tử an toàn?

A. Người mua mở tài khoản và nhận Giấy chứng nhận. Người bán cũng có Giấy chứng nhận;
B. Người mua đặt hàng và người bán được kiểm chứng;
C. Lệnh mua hàng và trả tiền được gửi. Người bán yêu cầu chứng thực trả tiền và duyệt đơn;
D. Người bán duyệt lệnh trả tiền và đơn mua hàng.

20. Chữ ký điện tử kép không bao gồm giai đoạn nào

a) Bản băm của thông tin đặt hàng OIMD
b) Bản băm của thông tin trả tiền PIMD.
c) Mã hai bản băm OIMD và PIMD bằng khóa riêng của người mua
d) Ghép hai bản băm OIMD và PIMD và băm tiếp thành POMD và mã bằng khóa riêng của người mua.