Chapter 08: IP Security

IP security là khả năng năng được thêm vào các version hiện nay của Internet Protocol (IPv4 ỏ IPv6) bằng cách thêm headers.

Chức năng: xác thực(authentication); Confidentiality(bảo mật); key management (quản lý khóa).

Chức năng xác thực sử dụng HMAC message authentication code.

Xác thực có thể được áp dụng cho toàn bộ các gói IP ban đầu (chế độ đường hầm) hoặc đến tất cả các gói tin ngoại trừ các **tiêu đề IP** (transport mode).

Tính bí mật được cung cấp bởi một đị nh dạng mã hóa được gọi là đóng gói tải trọng an ninh**(encapsulating security payload**). Cả hai tunnel và transport mode có thể được cung cấp. IKE đị nh nghĩa một số kỹ thuật để quản lý khoá.

IP Security Tổng quan

- Năm 1994, Hội đồng Kiến trúc Internet (IAB) đã đưa ra một báo cáo có tựa đề "An ninh trong kiến trúc Internet" (RFC 1636).
- Báo cáo xác định các khu vực quan trọng cho cơ chế bảo mật.
- Trong số đó là sự cần thiết để bảo đảm cơ sở hạ tầng mạng từ giám sát trái phép và kiểm soát lưu lượng truy cập mạng và sự cần thiết để đảm bảo người dùng cuối của người sử dụng lưu lượng truy cập bằng cách sử dụng xác thực và kỹ thuật mã hóa.
- Để đảm bảo an ninh, IAB bao gồm xác thực và mã hóa như các tính năng bảo mật cần thiết trong các thế hệ tiếp theo IP, mà đã được ban hành như IPv6
- May mắn thay, những khả năng bảo mật được thiết kế để sử dụng được cả với IPv4 hiện tại và IPv6 trong tương lai.
- Điều này có nghĩa rằng các nhà cung cấp có thể bắt đầu cung cấp các tính năng bây giờ, và nhiều nhà cung cấp hiện nay có một số khả năng IPsec trong các sản phẩm của họ.

 Các đặc điểm kỹ thuật IPsec hiện hữu như là một tập hợp các tiêu chuẩn Internet.

Các ứng dụng của IPsec

 IPsec cung cấp khả năng để **bảo đảm liên lạc** trên một mạng LAN, trên mạng private và công cộng WANs, và trên Internet. Ví dụ về việc sử dụng bao gồm:

- Bảo vệ kết nối văn phòng chi nhánh qua Internet.
- Bảo vệ truy cập từ xa qua Internet
- Thiết lập mạng diện rộng và mạng nội bộ kết nối với các đối tác
- Tăng cường an ninh thương mại điện tử

Lợi ích của IPsec

 Trong một tường lửa hoặc router, nó cung cấp bảo mật mạnh mẽ mà có **thể được áp dụng cho tất cả các lưu lượng truy cập** qua các vành đai.

 IPsec trong một tường lửa có khả năng chống bỏ qua nếu tất cả lưu lượng truy cập từ bên ngoài phải sử dụng IP và tường lửa là phương tiện duy nhất của lối vào từ Internet vào tổ chức.

 IPsec là dưới lớp truyền tải (TCP, UDP) và như vậy là trong suốt đối với các ứng dụng.

 IPsec có thể được minh bạch cho người dùng cuối.

 IPsec có thể cung cấp bảo mật cho người dùng cá nhân

ứng dụng đị nh tuyến

IPsec có thể đảm bảo rằng

- Một quảng cáo bộ định tuyến (router mới quảng cáo hiện diện của nó) xuất phát **từ một bộ định tuyến được xác thực.**

- Một quảng cáo hàng xóm (một router nhằm thiết lập hoặc duy trì một mối quan hệ hàng xóm với một bộ định tuyến trong một miền định tuyến) xuất phát **từ một bộ định tuyến được xác thực.**

- Một tin nhắn chuyển hướng xuất phát từ router mà gói IP ban đầu đã được gửi.

- Một bản cập nhật định tuyến được **không giả mạo**.(not forged).

Tài liệu IPsec

- IPsec bao gồm ba khu chức năng:

  - chứng thực,
  - bí mật, và
  - quản lý khoá

- Toàn bộ các đặc điểm kỹ thuật IPsec được rải rác trên hàng chục RFC và dự thảo văn bản IETF, làm cho này sự phức tạp và khó khăn nhất để nắm bắt tất cả các thông số kỹ thuật của IETF

- The documents can be categorized into the following groups

  - Architecture

  o RFC4301 Security Architecture for Internet Protocol

  - Authentication Header (AH)

  o RFC4302 IP Authentication Header

  - Encapsulating Security Payload (ESP)

  o RFC4303 IP Encapsulating Security Payload (ESP)

  - Internet Key Exchange (IKE)

o RFC4306 Internet Key Exchange (IKEv2) Protocol

• Cryptographic algorithms

Dịch vụ IPsec

- IPsec cung cấp dịch vụ an ninh tại các lớp IP bằng **cách cho phép một hệ thống để lựa chọn giao thức bảo mật cần thiết, xác định các thuật toán (s) để sử dụng cho các dịch vụ (s), và đặt ở vị trí bất kỳ khóa mật mã cần thiết** để cung cấp các yêu cầu dịch vụ.

- RFC 4301 liệt kê các dịch vụ sau đây:

• Kiểm soát truy cập

• toàn vẹn hướng kết nối

• xác thực nguồn gốc dữ liệu

• Loại bỏ các gói tái hiện lại(replays) (một hình thức toàn vẹn xếp từng phần)

• Tính bảo mật (mã hóa)

• lưu lượng giao thông bảo mật giới hạn

• Other

Chế độ Transport

- chế độ Transport cung cấp **bảo vệ chủ yếu cho các giao thức lớp trên.**

- Đó là, bảo vệ chế độ vận chuyển kéo dài đến tải trọng(payload) của một gói tin IP.

- Thông thường, phương tiện giao thông được sử dụng cho giao tiếp **end-to-end giữa hai máy chủ** (ví dụ, một khách hàng và một máy chủ, hoặc hai máy trạm)

- để mã **hóa và xác thực dữ liệu tùy chọn IP**

• có thể làm phân tích giao thông nhưng hiệu quả

- tốt cho ESP lưu lượng host-to-host

Chế độ đường hầm(Tunnel mode)

- Tunnel mode cung **cấp bảo vệ cho toàn bộ gói tin IP.**
- để đạt được điều này, sau khi **các lĩnh vực AH hoặc ESP được thêm vào** gói tin IP, toàn bộ các lĩnh vực gói cộng với an ninh được coi là **payload** của gói IP mới bên ngoài với **một tiêu đề IP mới bên ngoài**
- Toàn bộ ban đầu, nội, gói tin **đi qua một đường hầm** từ một điểm của một mạng IP khác; không có các router trên đường đi có thể kiểm tra các tiêu đề IP bên trong

- mã hóa toàn bộ gói IP
- thêm tiêu đề mới cho hop tiếp theo
- không có router trên đường có thể kiểm tra tiêu đề IP bên trong
- tốt cho các VPN, cửa ngõ vào cổng an ninh

Điểm khác nhau giữa transport mode và tunnel mode:

Transport : bảo vệ upper-layer protocol.

Tunnel: entire IP packet.

Ở transport: chia làm 4 tầng và ở tầng thứ 4: orig IP hdr -> ESP hdr

Ở tunnel có 5 tầng: tầng 4 ESP hdr -> orig IP hdr và tầng thứ 5 có: new IP hdr.

IP Security Policy

- ơ bản để các hoạt động của IPsec là khái niệm về một chính sách an ninh áp dụng cho mỗi gói IP đi qua từ một nguồn đến đích.
- chính sách IPsec được xác đị nh chủ yếu bởi sự tương tác của hai cơ sở dữ liệu,

- cơ sở dữ liệu liên kết an ninh (SAD) và
- cơ sở dữ liệu chính sách an ninh (SPD)

 Security Associations

 Cơ sở dữ liệu Hiệp hội An toàn

 Database Security Policy

 IP Traffic Processing

Hiệp hội bảo mật (SA)

 Một khái niệm quan trọng xuất hiện trong cả các cơ chế xác thực và bảo mật cho IP là hiệp hội bảo mật (SA)

 một **kết nối hợp lý một chiều** giữa người gửi và người nhận mà dành dị ch vụ an ninh cho giao thông vận chuyển trên nó

 xác định bởi 3 thông số:

- **Security Parameters Index** (SPI): Một chuỗi bit được gán cho SA này và có ý nghĩa nội bộ
- **IP Destination Address**: đị a chỉ của thiết bị đầu cuối đích
- **Security Protocol Identifier**: chỉ ra cho dù hiệp hội là một hiệp hội an ninh AH hoặc ESP

Cơ sở dữ liệu Hiệp hội An toàn (SAD)

Trong từng thực hiện IPsec, có một cơ sở dữ liệu Hiệp hội An toàn danh nghĩa xác đị nh các thông số liên quan với mỗi SA.

- Security Parameter Index
- Sequence Number Counter
- Sequence Counter Overflow

- Anti-Replay Window
- AH Information
- ESP Information
- Lifetime of this Security Association
- IPsec Protocol Mode
- Path MTU

Cơ sở dữ liệu Chính sách An ninh (SPD):

Các phương tiện mà lưu lượng IP có liên quan đến SAs cụ thể (hoặc không có SA trong trường hợp lưu lượng truy cập được phép bỏ qua IPsec) là Database Security Policy danh nghĩa.

Đóng gói An Ninh Payload (ESP)

- ESP có thể được sử dụng **để cung cấp bảo mật, xác thực nguồn gốc dữ liệu, toàn vẹn phi kết nối, và dịch vụ chống phát lại** (một hình thức toàn vẹn xếp từng phần), và (giới hạn) lưu lượng dòng chảy bảo mật.
- Tập hợp các dịch vụ cung cấp **phụ thuộc vào tùy chọn** đã chọn tại thời điểm Hiệp hội An toàn (SA) thành lập và vào vị trí của việc thực hiện trong một topo mạng.
- ESP **có thể làm việc với một loạt các thuật toán mã hóa và xác thực.**

Mã hóa và xác thực Algs

- Các **Payload Data, Padding, Pad Length, và Next Header** lĩnh vực được **mã hóa** bằng các dịch vụ ESP.
- Nếu thuật toán được sử dụng để mã hóa dữ liệu đồng bộ tải trọng yêu cầu mật mã, chẳng hạn như là một vector khởi tạo (IV), sau đó các dữ liệu có thể được thực hiện một cách rõ ràng vào đầu của trường Payload Data.

- Nếu được đưa vào, một IV thường không được mã hóa, mặc dù nó thường được gọi như là một phần của bản mã.

Padding

- Các trường Padding phục vụ nhiều mục đích:
  - mở rộng plaintext đến chiều dài yêu cầu
  - để sắp xếp thời gian pad và các lĩnh vực tiêu đề tiếp theo
  - Cung cấp một phần bảo mật lưu lượng giao thông

Dịch vụ chống Replay

- replay là khi kẻ tấn công gửi một bản sao của một gói tin xác thực
- số thứ tự sử dụng để ngăn chặn các cuộc tấn công này
- sender khởi tạo chuỗi số 0 khi một SA mới được thiết lập
  - tăng cho mỗi gói
  - không được vượt quá giới hạn của (2mũ 32)-1
- nhận sau đó chấp nhận các gói tin với số seq trong cửa sổ của (N -W + 1)

Kết hợp Hiệp hội An Ninh

- SA có thể thực hiện một trong hai AH hoặc ESP
- thực hiện cả hai cần phải kết hợp SAs
  - tạo thành một bó hiệp hội an ninh
  - có thể chấm dứt ở thiết bị đầu cuối khác nhau hoặc cùng
  - kết hợp bởi
    - giao kề
    - hầm lặp

- ết hợp xác thực và mã hóa
    - ESP với xác thực, đi kèm bên trong ESP & AH ngoài, gói vận chuyển bên trong & ngoài ESP

IPSec Key Management

- ử lý thế hệ & phân phối chính
- thường cần 2 cặp phím
    - 2 mỗi hướng cho AH & ESP
- ẫn quản lý khoá
    - quản trị Sys tay cấu hình mỗi hệ thống
- quản lý khoá tự động
    - hệ thống tự động cho vào việc tạo ra nhu cầu của các phím cho SA trong các hệ thống lớn
    - có Oakley & ISAKMP yếu tố