Mục lục

[**Chương 1: Tổng quan về an toàn mạng** 2](#_Toc46259318)

[**1.** **Trình bày về tấn công bị động và tấn công chủ động, cho ví dụ. So sánh sự khác nhau giữa hai kiểu tấn công này.** 2](#_Toc46259319)

[**2.** **Tìm hiểu về các dịch vụ an toàn và các kỹ thuật an toàn mạng, các khái niệm về giao thức an toàn.** 3](#_Toc46259320)

[**Chương 2: Giao thức xác thực** 4](#_Toc46259324)

[**1.** **Trình bày được các nguyên thủy xác thực.** 4](#_Toc46259325)

[**2.** **Giải thích được kết quả xác thực (tại sao có thể coi là tính xác thực của thực thể đã được thiết lập). (Câu 1 trong các đề): (Thêm timestamp)** 5](#_Toc46259326)

[**3.** **Trình bày hoạt động của các giao thức xác thực (trùng với câu 4)** 6](#_Toc46259327)

[**4.** **Với các giao thức xác thực (PAP, CHAP, KERBEROS, EAP, RADIUS, và chuẩn 802.1x) cần nắm được:** 6](#_Toc46259328)

[**Chương 3:** **Các giao thức an toàn cho dữ liệu tầng ứng dụng** 16](#_Toc46259335)

[**1.** **Trình bày về mô hình truyền/nhận thư điện tử. Các thành phần chính trong hệ thống, mối quan hệ giữa các thành phần đó ?** 16](#_Toc46259336)

[**2.** **Trình bày đặc điểm cơ bản một số giao thức truyền/nhận thư cơ bản: SMTP, MINE, IMAP, POP3;** 17](#_Toc46259337)

[**3.** **Tìm hiểu cơ bản về S/MINE và PGP.** 19](#_Toc46259338)

[**4.** **Hiểu được các hiểm họa an toàn thông tin đối với các dịch vụ web và email, từ đó trình bày các giải pháp an toàn (ở tầng ứng dụng và tầng giao vận) để chống lại các hiểm họa đó.** 20](#_Toc46259339)

[**5.** **Trình bày các đặc điểm cơ bản của các giao thức con của SSH (SSH Trans, SSH Auth, SSH Conn), SSH Port forwarding.** 21](#_Toc46259340)

[**6.** **Trình bày đặc điểm cơ bản của bộ giao thức SSL/TLS, đặc biệt là hai giao thức con Handshake hay Record .** 25](#_Toc46259341)

[**Chương 4: Giao thức an toàn mạng riêng ảo** 29](#_Toc46259342)

[**1.** **VPN:** 29](#_Toc46259343)

[**2.** **Trình bày về SA:** 30](#_Toc46259344)

[**3.** **IPSec:** 31](#_Toc46259345)

[**4.** **AH và ESP:** 33](#_Toc46259346)

[**5.** **IKE:** 36](#_Toc46259347)

[**Chương 5. Các giao thức an toàn mạng không dây** 38](#_Toc46259348)

[**1.** **Mạng không dây (Wireless network):** 38](#_Toc46259349)

[**2.** **Trình bày đặc điểm cơ bản về các cơ chế an toàn cơ bản như: xác thực, kiểm soát truy cập, mã hóa trong mạng WLAN.** 40](#_Toc46259350)

[**3.** **Trình bày giao thức xác thực bắt tay 4-bước dùng khóa chia sẻ trước (Pre-shared key) trong WLAN, mô tả được các bước hoạt động. Phân tích tấn công vào khóa dòng RC4 lên giao thức này.** 42](#_Toc46259351)

[**4.** **Tìm hiểu kỹ giao thức TKIP trong WPA và những cải tiến về mặt an toàn của giao thức này so với giao thức WEP.** 43](#_Toc46259352)

[**5.** **Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WEP.** 44](#_Toc46259353)

[**6.** **Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WPA .** 45](#_Toc46259354)

[**7.** **Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WPA2.** 45](#_Toc46259355)

[**8.** **Phân tích độ an toàn, ưu, nhược điểm của các giao thức WEP, WPA, WPA2.** 46](#_Toc46259356)

[**9.** **Trình bày các tấn công phổ biến vào mạng WLAN ( Các vấn đề an toàn thông tin khi chuyển hữu tuyến -> vô tuyến)** 46](#_Toc46259357)

[**10.** **So sánh sự khác nhau giữa 3 giao thức WEP, WPA, WPA 2** 47](#_Toc46259358)

[**CHƯƠNG CUỐI: GIẢI ĐỀ** 49](#_Toc46259359)

[**AT13 01** 49](#_Toc46259360)

[**AT13 02** 52](#_Toc46259361)

[**AT13 03** 55](#_Toc46259362)

[**AT13 04** 58](#_Toc46259363)

[**AT12 01** 61](#_Toc46259364)

[**AT12 02** 64](#_Toc46259365)

[**AT12 03** 66](#_Toc46259366)

[**AT11 01** 69](#_Toc46259367)

[**AT11 02** 73](#_Toc46259368)

[**5.** **Các khái niệm khác:** 76](#_Toc46259369)

# **Chương 1: Tổng quan về an toàn mạng**

1. **Trình bày về tấn công bị động và tấn công chủ động, cho ví dụ. So sánh sự khác nhau giữa hai kiểu tấn công này.** **(\*)**

* **Tấn công bị động**: Là kiểu tấn công chặn bắt thông tin như nghe trộm và quan sát truyền tin.
* Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.
* Tấn công bị động rất khó bị phát hiện bởi vì chúng không thay đổi bất kỳ dữ liệu nào.
* Ví dụ: Bob gửi thông tin username và password đến Alice để Alice đóng tiền học giúp, trong lúc đó, hacker lắng nghe trên đường truyền và bắt được gói tin chứa nội dung username và password của Bob (kiểu tấn công man-in-the-middle)
* **Tấn công chủ động:** Là các tấn công sửa đổi luồng dữ liệu hay tạo ra luồng dữ liệu giả, có thể được chia làm 4 loại nhỏ sau:
* Giả mạo (Masquerade): Một thực thể (người dùng, máy tính, chương trình, ...) giả mạo một thực thể khác.
  + Ví dụ: Mallic (Hacker) giả làm Alice gửi thông điệp cho Bob. Khi đó Bob không biết điều này và nghĩ rằng thông điệp là của Alice.
* Phát lại (Replay): bắt giữ dữ liệu thụ động và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
  + Ví dụ: Mallic (hacker) sao chép lại thông điệp mà Alice gửi cho Bob, sau đó một thời gian Mallic gửi bản sao chép này cho Bob.
* Sửa đổi thông báo (Modification of messages): Một bộ phận của thông báo hợp lệ được sửa đổi hoặc các thông báo bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.
  + Ví dụ: Bob gửi gói tin A với nội dung “Gửi em 5 triệu qua tài khoản xx” đến Alice. Mallic (Hacker) ở giữa chặn bắt thông tin và bắt được gói tin A, sau đó Mallic thay đổi nội dung gói tin A thành “Gửi em 5 triệu đô qua tài khoản yy” và gửi đến Alice.
* Từ chối dịch vụ: Ngăn hoặc cấm việc sử dụng bình thường hoặc quản lý các tiện ích truyền thông.
  + Ví dụ: Hacker thực hiện tấn công DoS bằng cách gửi hàng loạt gói tin request đến máy chủ Web gây nên nghẽn băng thông đến máy chủ, khiến cho các máy client không thể truy cập đến máy chủ này.
* Tấn công chủ động dễ phát hiện nhưng lại rất khó ngăn chặn tuyệt đối, đòi hỏi việc bảo vệ vật lý tất cả các phương tiện truyền thông ở mọi lúc, mọi nơi.
* **So sánh:**
  + Giống: đều là hình thức tấn công có chủ ý nhằm phá vỡ tính an toàn của thông tin, hệ thống thông tin được bảo vệ.
  + Khác

|  |  |
| --- | --- |
| Chủ động | Bị động |
| Dễ phát hiện | Khó phát hiện |
| Thay đổi nội dung | Không thay đổi nội dung |
| Giả mạo, gửi lại, thay đổi thông báo và từ chối dịch vụ | Chặn bắt thông tin và phân tích lưu lượng |

1. **Tìm hiểu về các dịch vụ an toàn và các kỹ thuật an toàn mạng, các khái niệm về giao thức an toàn.** **(\*)**

* **Các dịch vụ an toàn mạng**: là dịch vụ nâng cao an toàn của các hệ thống. Mỗi dịch vụ an toàn sử dụng một hay nhiều kỹ thuật đảm bảo an toàn. Có thể được phân loại như sau:
* **Dịch vụ bảo mật**: Nhằm chống lại các tấn công thụ động vào dữ liệu trên kênh truyền. Đối với loại đánh cắp nội dung thông tin, thì một vài mức bả vệ có thể được chỉ ra. Đây là loại dịch vụ nhằm bảo vệ dữ liệu trên kênh giữa hai người dùng trong một khoảng thời gian.
* **Dịch vụ xác thực:** Dịch vụ xác thực liên quan đến việc xác thực trong truyền thông. Trong trường hợp nhận một thông báo, dịch vụ xác thực đảm bảo người nhận xác thực được nguồn gốc thông báo. Trong trường hợp tương tác diễn ra trong một khoảng thời gian thì dịch vụ xác thực đảm bảo:
* Tại thời điểm thiết lập kết nối, dịch vụ xác thực đảm bảo hai thực thể tham gia kết nối xác thực được lẫn nhau
* Trong thời gian kết nối, dịch vụ đảm bảo không thể có một bên thứ ba đóng giả một trong hai thực thể truyền thông hợp pháp
* **Dịch vụ đảm bảo tính toàn vẹn:**
* Đảm bảo tính toàn vẹn hướng kết nối đảm bảo dòng dữ liệu nhận được cũng như gửi không thể bị lặp lại, chèn thêm vào, thay đổi, thay đổi trật tự cũng như gửi lại. Dịch vụ này nhắm vào cả những thay đổi đối với dòng dữ liệu cũng như vấn đề từ chối dịch vu.
* Đảm bảo tính toàn vẹn không kết nối thì chỉ liên quan với từng thông báo riêng rẽ và nói chung chỉ nhằm chống lại việc thay đổi nội dung thông báo.
* **Dịch vụ chống chối bỏ:** nhằm ngăn chặn người gửi hoặc người nhận chối bỏ việc đã gửi thông báo hoặc đã nhận thông báo. Như vậy khi thông báo đã được gửi, người nhận có thể chúng minh được rằng ai là người đã gửi thông báo. Tương tự, khi thông báo đã được nhận, người gửi có thể chứng minh được ai là người đã nhận thông báo.
* **Dịch vụ kiểm soát truy cập:** nhằm hạn chế và kiểm soát truy cập tới các hệ thống máy chủ hoặc các ứng dụng qua các kênh truyền thông.
* **Dịch vụ đảm bảo tính sẵn sàng:** Đảm bảo ngăn ngừa hoặc phục hồi lại sự sẵn sang của tài nguyên trong hệ thống.
* **Các kỹ thuật an toàn mạng:** Kỹ thuật an toàn là kỹ thuật được thiết kế để phát hiện, ngăn ngừa hoặc loại bỏ tấn công.
* **Định danh:** là việc gắn định danh cho người dùng và kiểm tra sự tồn tại của định danh đó
* **Cấp quyền:** là việc xác định một chủ thể đã được xác thực được phép thực hiện những thao tác nào lên những đối tượng nào trong hệ thống
* **Xác thực:** là quá trình kiểm tra tính chân thực của danh tính được xác lập trong quá trình định danh
* **Mã hóa:** là phương pháp để biến thông tin từ định dạng bình thường sang dạng thông tin không thể hiểu được nếu không có phương tiện giải mã.
* **Ký:** Chữ ký điện tử là thông tin đi kèm theo dữ liệu nhằm mục đích xác định người chủ của dữ liệu đó
* **Công chứng**
* **Ngăn cản vật lý**
* **Các khái niệm về giao thức an toàn mạng:**
* Giao thức mạng là tập hợp các quy tắc và quy ước điều khiển việc trao đổi thông tin giữa các hệ thống máy tính.
* Một giao thức an toàn (giao thức mật mã) là một kiểu giao thức mật mã được sử dụng để bảo vệ dữ liệu trên máy tính và dữ liệu truyền thông. Công cụ chính là dùng mật mã. Nó thường được kết hợp với một trong các khía cạnh sau:
* Trao đổi, thỏa thuận khóa
* Xác thực thực thể
* Mã hóa đối xứng và xác thực thông báo
* An toàn truyền thông dữ liệu ở mức ứng dụng
* Các phương pháp chống chối bỏ.
* Một số tác vụ chính của các giao thức an toàn mạng thường là bảo mật việc truyền file, giao dịch Web và mạng riêng ảo:
* Giao thức xác thực: PAP, CHAP, Kerberos, Radius, EAP,…
* Giao thức VPN: SSL-VPN, IPSEC-VPN,…
* Giao thức bảo mật dịch vụ: S/MINE, PGP, SFTP, FTPS, SCP, HTTPS
* Giao thức an toàn mạng không dây: 802.11i, WTLS,…

# **Chương 2: Giao thức xác thực**

1. **Trình bày được các nguyên thủy xác thực.(\*)**

* Có 3 nguyên thủy xác thực:
  + Truyển trực tiếp yếu tố bí mật:
    - Nhược điểm: mật khẩu có thể bị chặn thu tuy nhiên thực tế vẫn được sử dụng rộng rãi
* Để đảm bảo an toàn thì quá trình xác thực nên được thực hiện qua một kênh mã hóa.
  + - Phương án lưu trữ mật khẩu: lưu dưới dạng rõ, dạng băm và dạng băm có phụ gia
  + Thách đố bằng nonce:
    - Nonce là một đại lượng được sinh ngẫu nhiên, sao cho không bao giờ lặp lại.
      * Để không lặp lại, nonce thường có kích thước lớn (~128 bít)
      * Việc nonce không lặp lại giúp đảm bảo tính tươi của thông điệp (thông điệp chỉ được sử dụng 1 lần) trong xác thực
      * Nonce luôn được sinh bởi bên xác thực (authentication server).
    - Gồm có các sự kết hợp thách đố: mật mã đối xứng + nonce, băm + nonce, chữ ký số + nonce và mã hóa khóa công khai + nonce
  + Thách đố bằng timestamp:
    - Timestamp đại lượng chỉ thời gian trên đồng hồ của mỗi bên tham gia xác thực.
      * Luôn có sự sai lệch giữa đồng hồ của các bên nên phải xác định một sai số chấp nhận được:



* + - * Mỗi timestamp sẽ hợp lệ trong một khoảng thời gian nhất định -> để chống tấn công phát lại (replay attack) bên xác thực cần có cơ chế đảm bảo mỗi timestamp chỉ được sử dụng một lần (ví dụ: ghi nhớ timestamp gần nhất được sử dụng bởi mỗi thực thể)
    - Gồm có các sự kết hợp thách đố: mật mã đối xứng + timestamp, băm + timestamp, chữ ký số + timestamp và mã hóa khóa công khai + timestamp.

1. **Giải thích được kết quả xác thực (tại sao có thể coi là tính xác thực của thực thể đã được thiết lập). (Câu 1 trong các đề): (Thêm timestamp) (\*)**
2. **Mật mã đối xứng + timestamp:**
3. Điều kiện và mục đích:

* Điều kiện:
  + Bob và Alice thống nhất cơ chế nhãn thời gian
  + Alice và Bob chia sẻ khóa bí mật KAB
* Mục đích: Bob xác thực được Alice

1. Trình bày các bước:

* B1: Alice gửi yêu cầu xác thực với Bob đồng thời Alice sẽ thực hiện mã hóa thời gian TA của Alice bằng khóa KAB đã chia sẻ trước.
* B2: Bob sau khi nhận được bản mã sẽ sử dụng KAB để giải mã => thu được TA mà Alice đã gửi. Chấp nhận xác thực của Alice nếu TA hợp lệ.

1. Giải thích: TA nằm trong khoảng thời gian cho phép và chỉ có Alice mới có khóa KAB để má hóa thông điệp
2. **Hàm băm + timestamp:**
3. Điều kiện và mục đích:

* Điều kiện:
  + Bob và Alice thống nhất cơ chế nhãn thời gian
  + Alice và Bob chia sẻ khóa bí mật KAB
* Mục đích: Bob xác thực được Alice

1. Trình bày các bước:

* B1: Alice gửi yêu cầu xác thực với Bob đồng thời Alice gửi timestamp của mình là TA. Sau đó Alice băm TA với KAB đã được chia sẻ từ trước (H(KAB || TA) và gửi cho Bob
* B2: Bob sau khi nhận được. Trước hết sẽ kiểm tra tính hợp lệ của TA(có nằm trong ngưỡng thời gian được cho phép không?=> Nếu còn hợp lệ thì ok). Sau đó Bob sẽ thực hiện lấy TA kết hợp với KAB đã chia sẻ từ trước băm lại một lần nữa. Sau đó lấy bản băm vừa băm được so sánh với bản băm mà nhận được từ Alice. Nếu trùng nhau thì xác nhận đó là Alice

1. Giải thích:

* TA nằm trong ngưỡng thời gian cho phép.
* Và chỉ có Alice mới có khóa KAB để băm thông điệp

1. **Chữ ký số + timestamp**
2. Điều kiện và mục đích:

* Điều kiện:
  + Bob và Alice thống nhất cơ chế nhãn thời gian
  + Alice có cặp khóa bí mật, công khai
* Mục đích: Bob xác thực được Alice

1. Trình bày các bước:

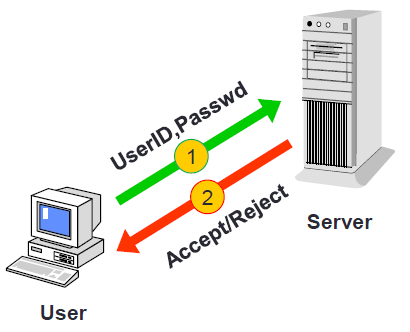
* B1: Alice gửi yêu cầu xác thực với Bob đồng thời Alice gửi timestamp của mình là TA. Sau đó sẽ gửi chữ ký của Alice trên TA (sử dụng khóa bí mật của mình để mã hóa TA)
* B2: Sau khi nhận được. Đầu tiên Bob kiểm tra tính hợp lệ của TA xem có còn trong ngưỡng thời gian cho phép hay không. Sau đó lấy khóa công khai của Alice để kiểm tra chữ ký (hành động giải mã chữ ký). Sau đó lấy TA vừa giải mã được so sánh với TA nhận được từ Alice. Nếu trùng thì xác nhận đó là Alice và ngược lại.

1. Giải thích:

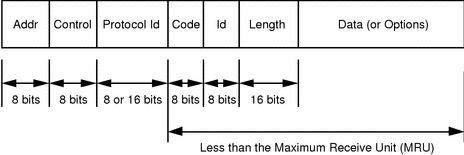
* TA nằm trong ngưỡng thời gian cho phép.
* Và chỉ có Alice mới có khóa bí mật để tạo chữ ký

1. **Trình bày hoạt động của các giao thức xác thực (trùng với câu 4)**
2. **Với các giao thức xác thực (PAP, CHAP, KERBEROS, EAP, RADIUS, và chuẩn 802.1x) cần nắm được: (\*)**

* **Đặc điểm cơ bản.**
* **Các thành phần**
* **Cơ chế hoạt động và vẽ được hình mô tả**
* **PAP (Password Authentication Protocol):**
* Các đặc điểm cơ bản:
  + PAP (Password Authentication Protocol, RFC1334): là một giao thức bắt tay hai chiều có sử dụng mật khẩu.
  + Xác thực dựa trên mật khẩu là giao thức mà hai thực thể chia sẻ một mật khẩu trước và sử dụng mật khẩu như là cơ sở xác thực.
  + PAP được sử dụng bởi giao thức PPP để xác nhận người dùng trước khi cho phép họ truy cập vào tài nguyên hệ thống.
* Các thành phần : Client (Remote User) và Server (Authenticator)
* Cơ chế hoạt động



* **Client** (Remote User) gửi yêu cầu xác thực (Authentication-Request) cho Server (Authenticator): User\_ID, Passwd
* **Server** gửi trả “Xác thực-OK” (Authentication-Ack) nếu thông tin về User\_ID và Passwd là chính xác, còn không thì gửi trả “Không xác thực” (authentication-nak).
* Khuôn dạng gói tin:



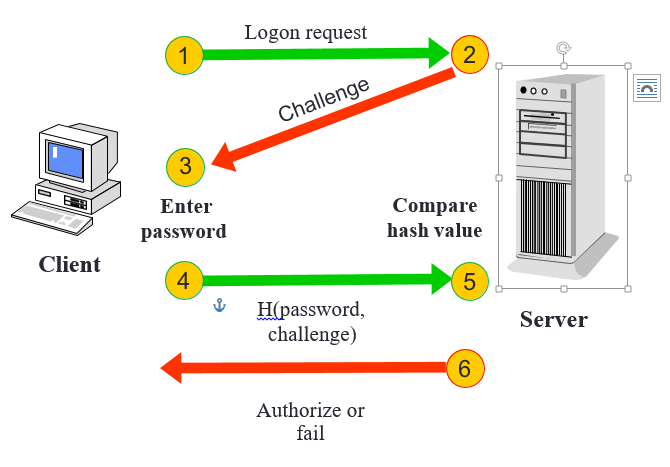
* Addr: trường địa chỉ là 1 byte, và là phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được đặt thành 0xff
* Control: trường điều khiển là 1 byte, và là một phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được được đặt thành 0x03
* Protocol Id: xác định loại thông tin chứa trong trường thông tin của khung và luôn luôn là 0xc023 cho các khung PAP
* Code: trường code là 1 byte và xác định loại khung PAP. Các mã PAP được chỉ định như sau:

0x01 Authenticate- Request

0x02 Authenticate- Ack

0x03 Authenticate- Nak

* Identifier: trường identifier là 1 byte và trợ giúp cho việc kết hợp các yêu cầu và trả lời.
* Length: trường length là 2 byte, và cho biết độ dài của khung PAP bao gồm trường code, identifier, length và data. Chiều dài không được vượt quá đơn vị nhận được tối đa (MRU)
* Data: trường data là 0 hoặc nhiều byte. Nó chứa thông tin liên quan đến đàm phán xác thực, theo định đạng được xác định bởi trường mã.
* Độ an toàn của giao thức xác thực :
* Không đảm bảo độ an toàn do mật khẩu không được mã hóa trên đường truyền nên dễ bị đánh cắp mật khẩu
* **CHAP**
* Các đặc điểm cơ bản
* CHAP (Challenge-Handshake Protocol, RFC 1994): Là mô hình xác thực dựa trên Username/Pasword.
* CHAP thực hiện xác thực dựa trên một bí mật được chia sẻ (vd mật khẩu người dùng).
* Thường được sử dụng khi Client logon vào các remote servers của công ty.
* Các thành phần: Client và Server
* Cơ chế hoạt động



Bước 1: client gửi yêu cầu kết nối tới Server

Bước 2: Server sẽ gửi lại Client một bản tin có các trường chính sau đây:

* 01 - Xác định loại bản tin là: challenge
* ID - Xác định phiên đó - trường này có tác dụng chống hình thức tấn công gửi lại khi bên thứ 3 bắt được gói tin
* random - số ngẫu nhiên sinh bởi Server (số nonce)
* Server - Tên xác thực của nó - Tên của Server .Tên này sẽ có trong cơ sở dữ liệu của Client và tương ứng sẽ là password kèm theo user này.

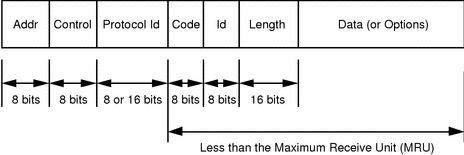
Bước 3:Client nhận được bản tin challenge (code=01) sẽ xử lý như sau:

* Lấy ID, random ở bản tin challenge gửi sang, rồi căn cứ vào tên xác thực là Server để tìm ra password xác thực. Lúc này Client đã có các thông tin như : ID, số ngẫu nhiên và password tương ứng với username Server.3 thông số đó được lấy làm đầu vào hàm băm MD5 Hash. Đầu ra là một giá trị gọi là số hassh.
* Sau khi xử lý xong, Client sẽ gửi lại Server một bản tin có code =02, gọi là bản tin response.
* Trong bản tin này có 2 trường vẫn giữ nguyên giá trị như bản tin challenge là: ID và random. Ngoài ra còn có thêm kết quả của hàm hash, tên xác thực của Client cũng được gửi đi.

Bước 4: Server nhận được kết bản tin response từ Client. Nó tìm kiếm password tương ứng với username mà nó nhận được.  Sau đó nó cũng tính toán giá trị MD5 Hash với 3 thông số đầu vào: ID, random và password vừa tim. Cuối cùng nó so sánh giá trị 2 hàm Hash: giá trị nó tự tính toán và giá trị nó nhận được.

Bước 5: Nếu giá trị nó tính và giá trị nó nhận được giống nhau thì gửi bản tin có code=03, success. Nếu không giống nhau thì gửi bản tin có code=04, fail.Nếu Client nhận được bản tin code=03 thì quá trình xác thực kết thúc. Còn không thì xác thực ko thành công và kết nối bị Fail.

* Khuôn dạng gói tin:



* Addr: trường địa chỉ là 1 byte, và là phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được đặt thành 0xff
* Control: trường điều khiển là 1 byte, và là một phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được được đặt thành 0x03
* Protocol Id: xác định loại thông tin chứa trong trường thông tin của khung và luôn luôn là 0xc223 cho các khung CHAP
* Code: trường code là 1 byte và xác định loại gói CHAP. Các mã CHAP được chỉ định như sau:

0x01 Challenge

0x02 Respone

0x03 Success

0x04 Failure

* Identifier: trường identifier là 1 byte và trợ giúp cho việc kết hợp các thách thức, phản hồi và trả lời.
* Length: trường length là 2 byte, và cho biết độ dài cảu gói CHAP bao gồm trường code, identifier, length và data.
* Data: trường data là 0 hoặc nhiều byte. Nó chứa thông tin liên quan đến đàm phán xác thực, theo định dạng được xác định bởi trường mã.
* Độ an toàn của giao thức xác thực: An toàn hơn so với giao thức PAP vì mật khẩu đã được mã hóa trên đường truyền
* **KERBEROS**
* Các đặc điểm cơ bản
* Là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn.
* Có khả năng chống lại việc nghe lén vào đảm bảo tính toàn vẹn của dữ liệu.
* Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình client – server và đảm bảo xác thực cho cả hai chiều.
* Giao thức được xây dựng dựa trên mật mã khóa đối xứng và cần đến một bên thứ ba gọi là “Trung tâm phân phối khóa” (Key Distribution Center).
* Các thành phần
* Client, Server
* Máy chủ xác thực (Authentication Server – AS): sử dụng các thông tin có trong database để xác thực người dùng.
* Máy chủ cấp vé ((Ticket Granting Server – TGS): cung cấp vé dịch vụ cho phép người dùng truy nhập vào các máy chủ trên mạng.
* Cơ sở dữ liệu (Database): chứa dữ liệu của KDC và của người dùng (Client).
* Trung tâm phân phối khóa KDC (Key Distribution Center)
* Cơ chế hoạt động: Sau đây là mô tả một phiên giao dịch (giản lược) của Kerberos. Trong đó: AS = Máy chủ chứng thực (authentication server), TGS = Máy chủ cấp vé (ticket granting server), SS = Máy chủ dịch vụ (service server). Một cách vắn tắt: người sử dụng chứng thực mình với máy chủ chứng thực AS, sau đó chứng minh với máy chủ cấp vé TGS rằng mình đã được chứng thực để nhận vé, cuối cùng chứng minh với máy chủ dịch vụ SS rằng mình đã được chấp thuận để sử dụng dịch vụ.

B1: Người sử dụng nhập tên và mật khẩu tại máy tính của mình (máy khách). Phần mềm máy khách thực hiện hàm băm một chiều trên mật khẩu nhận được. Kết quả sẽ được dùng làm khóa bí mật của người sử dụng.

B2: Phần mềm máy khách gửi một gói tin (không mật mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung của gói tin đại ý: "người dùng XYZ muốn sử dụng dịch vụ". Cần chú ý là cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS.

B3: AS kiểm tra nhân dạnh của người yêu cầu có nằm trong cơ sở dữ liệu của mình không. Nếu có thì AS gửi 2 gói tin sau tới người sử dụng:

* Gói tin A: "Khóa phiên TGS/máy khách" được mật mã hóa với khóa bí mật của người sử dụng.
* Gói tin B: "Vé chấp thuận" (bao gồm chỉ danh người sử dụng (ID), địa chỉ mạng của người sử dụng, thời hạn của vé và "Khóa phiên TGS/máy khách") được mật mã hóa với khóa bí mật của TGS.

B4: Khi nhận được 2 gói tin trên, phần mềm máy khách giải mã gói tin A để có khóa phiên với TGS. (Người sử dụng không thể giải mã được gói tin B vì nó được mã hóa với khóa bí mật của TGS). Tại thời điểm này, người dùng có thể nhận thực mình với TGS.

B5: Khi yêu cầu dịch vụ, người sử dụng gửi 2 gói tin sau tới TGS:

* Gói tin C: Bao gồm "Vé chấp thuận" từ gói tin B và chỉ danh (ID) của yêu cầu dịch vụ.
* Gói tin D: Phần nhận thực (bao gồm chỉ danh người sử dụng và thời điểm yêu cầu), mật mã hóa với "Khóa phiên TGS/máy khách".

B6: Khi nhận được 2 gói tin C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người sử dụng:

* Gói tin E: "Vé" (bao gồm chỉ danh người sử dụng, địa chỉ mạng người sử dụng, thời hạn sử dụng và "Khóa phiên máy chủ/máy khách") mật mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.
* Gói tin F: "Khóa phiên máy chủ/máy khách" mật mã hóa với "Khóa phiên TGS/máy khách".

B7: Khi nhận được 2 gói tin E và F, người sử dụng đã có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:

* Gói tin E thu được từ bước trước (trong đó có "Khóa phiên máy chủ/máy khách" mật mã hóa với khóa bí mật của SS).
* Gói tin G: phần nhận thực mới, bao gồm chỉ danh người sử dụng, thời điểm yêu cầu và được mật mã hóa với "Khóa phiên máy chủ/máy khách".

B8: SS giải mã "Vé" bằng khóa bí mật của mình và gửi gói tin sau tới người sử dụng để xác nhận định danh của mình và khẳng định sự đồng ý cung cấp dịch vụ:

* Gói tin H: Thời điểm trong gói tin yêu cầu dịch vụ cộng thêm 1, mật mã hóa với "Khóa phiên máy chủ/máy khách".

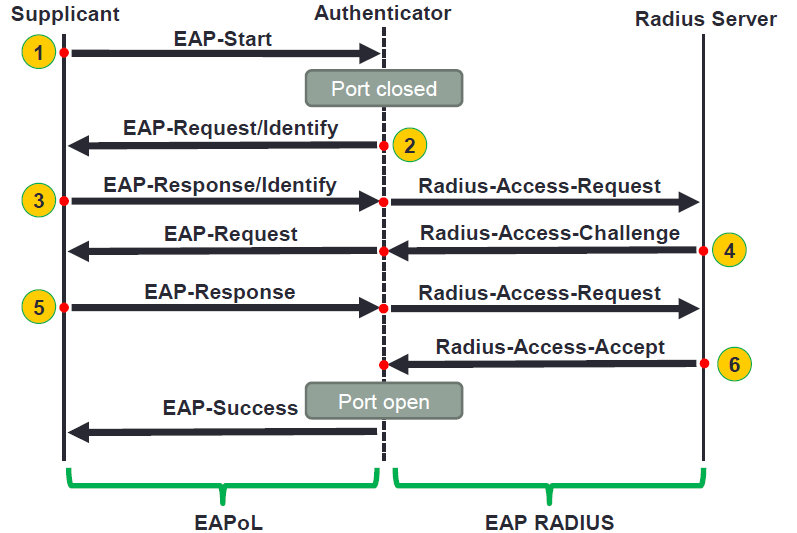
B9: Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người sử dụng có thể tin tưởng vào máy chủ SS và bắt đầu gửi yêu cầu sử dụng dịch vụ.

B10: Máy chủ cung cấp dịch vụ cho người sử dụng.

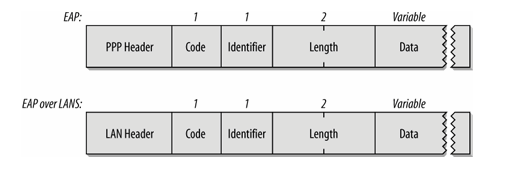
* Độ an toàn của giao thức xác thực : theo lý thuyết Kerberos là khá an toàn, tuy nhiên Kerberos chỉ cung cấp dịch vụ chứng thực, do đó nó không ngăn được dạng thỏa hiệp gây ra do lỗi phần mềm máy chỉ, quản trị viên cấp giấy phép cho người sử dụng trái phép, hoặc việc lựa chọn mật khẩu yếu.

Nếu máy chủ trung tâm ngừng hoạt động thì mọi hoạt động sẽ ngừng lại. Điểm yếu này co thể được hạn chế bằng cách sử dụng nhiều máy chủ Kerberos.

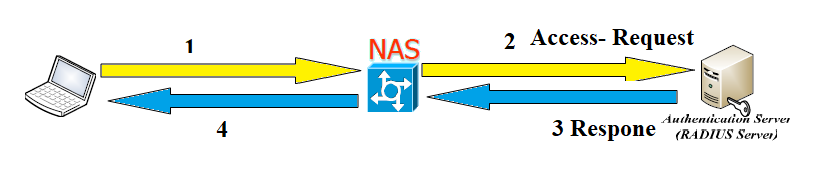
* **EAP**
* Các đặc điểm cơ bản
* EAP(Extensible Authentication Protocol, RFC 3748) hay còn gọi là giao thức xác thực mở rộng, là một framework xác thực thường được sử dụng trong các mạng không dây và trong các kết nối điểm-điểm (PPP).
* Do hoạt động ở lớp 2 (Data link) nên EAP có thể truyền tin giữa các thiết bị mà không cần địa chỉ IP.
* EAP là phương thức xác thực bao gồm yêu cầu định danh người dung (password,cetificate,…),giao thức được sử dụng (MD5,TLS\_Transport Layer Security, OTP\_ One Time Password,…) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.
* Bản thân EAP không phải là một phương thức xác thực. Khi sử dụng EAP ta cần chọn một phương thức xác thực cụ thể như CHAP, TLS, TTLS…
* Ưu điểm của EAP là linh hoạt trong triển khai.
* Có 4 loại EAP message:
  + EAP request
  + EAP response
  + EAP success
  + EAP failure
* Các thành phần của EAP
* Peer (client): còn được gọi là supplicant (máy tính, điện thoại…).
* Authenticator: thường là các AP, NAS, đóng vai trò phân phối các thông báo EAP được gửi từ Client tới Server xác thực và ngược lại.
* Authentication Server: cung cấp các dịch vụ xác thực cho authenticator (Radius server…). AS tiếp nhận các thông báo EAP được chuyển từ authenticator đến và thực hiện xác thực client (peer).
* Cơ chế hoạt động: quá trình trao đổi EAP với Radius server



* Khuôn dạng gói tin:

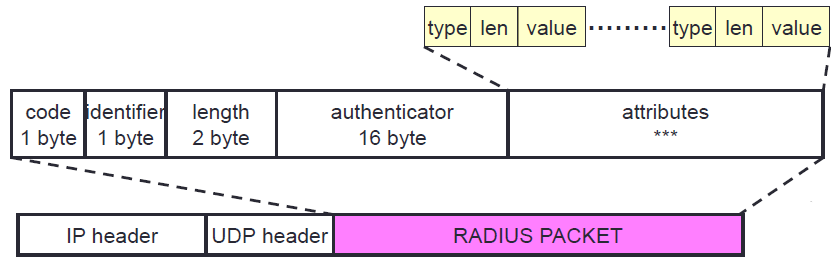


* Code: trường code là 1 byte và xác định loại gói EAP. Các mã EAP được chỉ định như sau:
  1. Request
  2. Respone
  3. Success
  4. Failure
* Identifier: trường identifier là 1 byte và trợ giúp cho việc kết hợp các yêu cầu và phản hồi
* Length: trường length là 2 byte, và cho biết độ dài cảu gói EAP bao gồm trường code, identifier, length và data.
* Data: trường data là 0 hoặc nhiều byte. Định dạng của trường data được xác định bởi trường code.
* **RADIUS**
* Các đặc điểm cơ bản
* RADIUS (Remote Authentication Dial-In User Service): giao thức hoạt động theo mô hình Client- Server, trong đó RADIUS client hay NAS (Network Access Server) tương tác với RADIUS server thông qua một hoặc nhiều RADIUS proxies.
* RADIUS được thiết kế dựa trên nền tảng kiến trúc AAA (Authentication-Authorization-Accouting) đó là Xác Thực - Ủy Quyền – Kế toán và hoạt động ở tầng 7 (Application Layer).
* RADIUS hỗ trợ nhiều phương thức xác thực khác nhau như PPP, PAP, CHAP…
* Các thành phần: Radius server, Radius client, Suplicant
* Cơ chế hoạt động



­ Hoạt động chung

* + - 1. User gửi thông tin dùng để xác thực tới NAS.
      2. NAS sẽ đóng gói chúng vào AccesRequest và gửi tới RADIUS server.
      3. Server phản hồi: Yes/No/Challenge.
      4. NAS gửi phản hồi cho người dùng.
* Client sẽ tạo ra một “Access-Request” chứa các thuộc tính như trên: mật khẩu của user, ID của client và ID port mà user này sẽ truy cập vào. Mật khẩu khi nhập vào sẽ được ẩn (Mã hóa RSA hoặc MD5).
* “Access- Request” sẽ được gửi cho RADIUS server thông qua mạng. Nếu không trả lời trong một khoảng thời gian qui ước thì yêu cầu sẽ được gửi lại.
* RADIUS server xác nhận client gửi. Những yêu cầu từ các client nào không chia sẽ thông tin bảo mật với RADIUS sẽ không được xác nhận và trả lời. RADIUS server sẽ tìm kiếm trong cơ sở dữ liệu (CSDL) user có cùng tên trong yêu cầu. Chỉ mục của user trong CSDL sẽ chứa danh sách các đòi hỏi cần thiết cho phép user truy cập vào mạng.
* Nếu bất cứ điều kiện nào không thỏa mãn, RADIUS server sẽ gửi một trả lời “Access- Reject”
* Nếu tất cả các điều kiện đều thỏa mãn và RADIUS server muốn đưa ra một yêu cầu đòi hỏi user phải trả lời, thì RADIUS sẽ gửi một trả lời “Access-Challenge”
* Client sẽ gửi lại (re-submit) “Access-Request” với một số hiệu yêu cầu (request ID) mới, nhưng thuộc tính usename-password được lấy từ thông tin vừa mới nhập vào, và kèm luôn cả thuộc tính trạng thái từ Access-Challenge
* RADIUS server có thể trả lời một access-request bằng một Access-Accept, Access-Reject hoặc một Access-Challenge khác.
* Nếu tất cả các điều kiện đáp ứng, danh sách các giá trị cấu hình của user sẽ được RADIUS server đưa vào thông báo trả lời “Access- Accept”.
* Khuôn dạng gói tin”



* Code : Trường Code là một octet, và xác định kiểu gói của RADIUS. Khi một gói có mã không hợp lệ sẽ không được xác nhận.

Các mã RADIUS (RADIUS Code) được gán như sau:

1 Yêu cầu truy câp

2 Chấp nhận truy cập

3 Từ chối truy cập

4 Yêu cầu kiểm toán

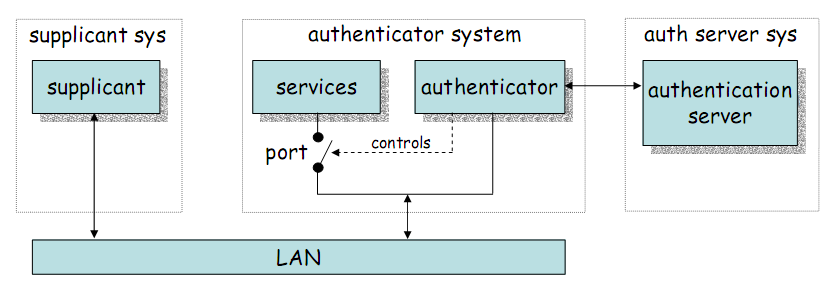
5 Đáp ứng kiểm toán

11 Đòi hỏi truy cập

12 Trạng thái máy chủ

13 Trạng thái máy khách

255 Dự phòng

* Identifier: Trường Identifier là một octet, tương ứng giữa các Request- Respone.
* Length: Trường Length là hai octet, nó bao gồm chiều dài của các trường Code, Identifier, Length, Authenticator, Attribute. Những octet nằm ngoài khoảng quy định của trường Length bị xem như là octet dư thừa và sẽ bị bỏ qua khi nhận. Những gói ngắn hơn giá trị trường Length chỉ ra nó sẽ bị loại bỏ. Giá trị nhỏ nhất của trường Length là 20 và lớn nhất là 4096.
* Authenticator: Trường Authenticatior là 16 octet, chứa cá thông tin được dùng để xác thực giữa client và server, và được sử dụng trong thuật toán ẩn mật khẩu.
* Attributes: vùng chứa các thông tin xác thực, ủy quyền cũng như cấu hình chi tiết của gói tin RADIUS
* Độ an toàn của giao thức xác thực: Authenticator giúp cho quá trình giao tiếp giữa NAS và máy chủ AAA được bảo mật nhưng nếu kẻ tấn công tóm được cả hai gói tin RADIUS Access-Request và Access-Response thì có thể thực hiện "tấn công từ điển" để phân tích việc đóng gói này. Trong điều kiện thực tế để việc giải mã khó khăn cần phải sử dụng những thông số dài hơn.
* **CHUẨN 802.1X**
* Các đặc điểm cơ bản
* Là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE.
* Hoạt động trên cả môi trường có dây truyền thống và không dây.
* Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.
* Các thành phần
* Supplicant
* Authenticator
* Authenticator Server (AS)
* Cơ chế hoạt động
* Supplicant yêu cầu truy nhập tới các dịch vụ (muốn kết nối vào mạng).
* Authenticator kiểm soát truy cập vào các dịch vụ (kiểm soá  
  của một cổng)
* Authenticator Server (AS) cấp quyền truy cập tới các dịch vụ:
* Supplicant xác thực nó với AS.
* Nếu xác thực thành công, AS sẽ chỉ thị cho Authenticator mở công dịch vụ
* AS thông báo cho Supplicant là truy cập được phép
* Các giao thức:
* EAP (Extensible Authentication Protocol) [RFC 3748]
* Là giao thức vận tải để mang các các thông điệp của các giao thức xác thực“thật sự” (VD: TLS)
* Rất đơn giản, gồm 4 thông điệp: EAP Request, EAP Response, EAP Success,EAP failure.
* Hoạt động ở tầng Datalink – OSI
* EAPOL (EAP over LAN) [802.1X]
* Được dùng để đóng gói các thông điệp EAP vào trong các giao thức LAN(VD: Ethernet).
* EAPOL được dùng để mang các thông điệp EAP giữa STA và AP
* RADIUS (Remote Access Dial-In User Service) [RFC 2865- 2869, RFC 2548]
* Được dùng để mang các thông điệp EAP giữa AP và AS
* Thuộc tính MS-MPPE-Recv-Key được dùng để truyền khóa phiên từ AS đến AP
* RADIUS được dùng trong WPA và là tùy chọn cho RSN
* Hoạt động ở tầng ứng dụng – OSI

# **Chương 3:** **Các giao thức an toàn cho dữ liệu tầng ứng dụng**

1. **Trình bày về mô hình truyền/nhận thư điện tử. Các thành phần chính trong hệ thống, mối quan hệ giữa các thành phần đó ? (\*)**

* Mô hình truyền/nhận thư điện tử:



* WebMail(Phần mềm thư điện tử qua Web): loại phần mềm thư điện tử không cần phải cài đặt mà nó được cung ứng bởi các máy chủ (web server)

Ví dụ: mail.Yahoo.com, hay hotmail.com, gmail.com

* MUA (Mail User Agent) –Email Client: Là loại phần mềm thư điện tử được cài đặt trên từng máy tính của người dùng.

Ví dụ: Microsoft Outlook, Microsoft Outlook Express, Netscape Comunicator, hay Eudora.

* MTA (Mail Transfer Agent): là máy chủ thư điện tử, nhằm cung ứng các dịch vụ thư điện tử
* Cách thức truyền tin:
* Soạn thảo: nhập các trường chính như: chủ đề, nội dung, đối tượng nhận gửi, thông tin phần định dạng,…
* Thư sẽ được chuyển đổi sang một định dạng chuẩn xác định bởi RFC 822 (Standard for the Format of ARP Internet Text Messages)
* Thư sau khi chuyển đổi sẽ gồm hai phần: phần tiêu đề (header) và phần thân (body)
* Quá trình gửi thư
* MUA kết nối tới MTA trên Mail Server
* MUA cung cấp thông tin cho MTA: định danh đối tượng gửi, nhân thư, DNS,…
* Máy chủ thư sẽ thực hiện các thao tác: Định danh đối tượng nhận, thiết lập kết nối truyền thư

1. **Trình bày đặc điểm cơ bản một số giao thức truyền/nhận thư cơ bản: SMTP, MINE, IMAP, POP3;**

* SMTP
* SMTP là giao thức tầng ứng dụng, SMTP được đánh giá là một giao thức truyền thông điệp thư đáng tin cậy và có hiệu quả cao
* SMTP chạy trên tầng TCP/IP, sử dụng port 25.
* **Định dạng bản tin:** SMTP: giao thức để trao đổi các bản tin thư điện tử. RFC 822: chuẩn định dạng bản tin dạng văn bản
* **Thủ tục làm việc SMTP:** Mỗi phiên làm việc SMTP gồm các phần sau:

– Khởi tạo phiên (Session Initiation)

– Khởi tạo Client (Client Initiation)

– Truyền thư (Mail Transactions)

– Kết thúc phiên và kết nối (Terminating Session and Connections)

* **Các trạng thái của SMTP:**
  + Khi Client gửi 1 lệnh SMTP tới Server, client nhận trả về 1 mã trạng thái cho máy gửi biết điều gì đã xảy ra.
  + Với thông điệp đáp trả có gắn 3 con số ở đầu dòng để thể hiện từng trạng thái riêng.
* **Hạn chế của SMTP:**

– Chỉ sử dụng với dữ liệu dạng ASCII 7 bit.

– Không có cơ chế xác thực

– Thông điệp gửi đi không được mã hóa

– Dễ bị tổn thương (bởi spam, mất định danh người gửi)

* **Giải pháp:**

– SMTP mở rộng

– MIME (Mở rộng thư tín Internet đa mục tiêu)

* **Giao thức MINE:** MIME (Multipurpose Internet Mail Extension): RFC 2045, 2046.
  + Là một chuẩn Internet về định dạng cho thư điện tử. Hầu như mọi thư điện tử Internet được truyền qua giao thức SMTP theo định dạng MIME. Vì gắn liền với chuẩn SMTP và MIME nên đôi khi thư điện tử Internet còn được gọi là thư điện tử **SMTP/MIME**.
  + MIME cho phép gửi các thông điệp trên internet mà không chỉ thuần là văn bản, có thể gửi mail kèm ảnh, link, ….
  + MIME không chỉ dùng cho mail mà có thể dùng cho các message nói chung, ví dụ như trong http
  + Thêm các dòng trong Header của bản tin khái báo kiểu nội dung MIME : MIME version, method sử dụng để mã hóa dữ lieeuk, kiểu dữ liệu đa phương tiện, kiểu con, khai báo tham số, dữ liệu đã mã hóa
  + Biến đổi dữ liệu non-ASCII sang dạng ASCII
* **Phương pháp mã hóa base64**
* Gồm các bước chính sau:
* Chia file nhị phân thành nhiều nhóm nhỏ dài 3byte
* Mã hóa từng nhóm 3byte thành 4 ký tự ASCII 7bit in ấn như sau:
* Gộp 3 byte thành 24bit liên tiếp, chia thành 4 nhóm 6bit có giá trị từ 0-63.
* Mỗi nhóm 6bit tương ứng với 1 ký tự in ấn như sau:

0-25 -> A-Z

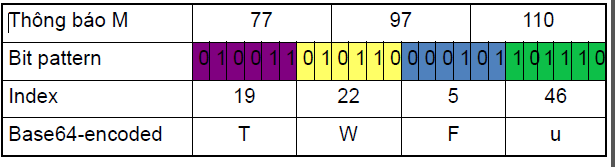
26-51-> a-z

52-61-> 0-9

62-> +

63-> /

* Ví dụ:



* **Giao thức POP3**
* **Tổng quan giao thức:**
* POP3 ( Post Office Protocol ver 3) là giao thức tầng ứng dụng, dùng để truy nhập và lấy thư điện tử từ mailbox trên máy chủ thư tín thông qua kết nối TCP/IP, port 110.
* Trước POP3 có 2 phiên bản ra đời trước là: Năm 1984 sử dụng POP, 1988 sử dụng POP2. Đến nay, POP3 được sử dụng thông dụng nhất và được xác định trong RFC 1939.
* **Hoạt động của POP3**
* POP3 client xác thực thành công với server, server có khóa và mở được maildrop thích hợp. Client có thể truy nhập tới mailbox của mình trên server để kiểm tra, nhận thư…
* Nếu Maildrop không mở (-ERR), server đóng kết nối or client gửi lệnh xác nhận và bắt đầu lại từ đầu
* Thiết lập kết nối TCP ở công 110
* Client gửi lệnh QUIT tới server thì trạng thái Trasaction chuyển sang Update.
* Server gửi goodbye tới client và đóng kết nối TCP, kết thúc phiên làm việc.
* **Giao thức IMAP**
* **Tổng quan giao thức:**
* IMAP (Internet Messages Access Protocol) được phát minh bởi Mark Crispin năm 1986 tại trường ĐH Stanford.
* IMAP là giao thức hoạt động ở tầng ứng dụng, cho phép Client truy nhập email trên một Server từ xa.
* IMAPv2 được phát minh năm 1987, IMAPv4 được phát minh năm 1994, được miêu tả trong RFC 2060 sử dụng port 143/tcp.
* IMAPv4 email được lưu trữ trên mail server và có thể truy cập từ bất kì máy email client IMAP4 nào trên mạng.
* IMAP4 có thể thực hiện các thao tác như: tạo, xóa, sửa đổi tên mailbox, kiểm tra mail mới, update mail cũ (trong RFC 2822), thiết lập và xóa cờ trạng thái
* **Mục đích sử dụng IMAP:**
* Tương thích đầy đủ với các chuẩn thông điệp Internet (MIME)
* Cho phép truy nhập & quản lý thông điệp từ nhiều máy tính khác nhau
* Hỗ trợ truy nhập đồng thời tới các mailbox dùng chung
* Phần mềm bên Client không cần biết kiểu lưu trữ file của Server

1. **Tìm hiểu cơ bản về S/MINE và PGP.**

* **Giao thức SMINE**
* S/MIME (Security/Multipurpose Internet Mail Extensions (MIME): Là một phiên bản cho giao thức MIME hỗ trợ mã hóa.
* SMIME đưa vào hai phương pháp an toàn cho email dựa trên mã hóa bất đối xứng và PKI.

- Mã hóa email: Động tác mã hóa = mã hóa message bằng public key của người nhận. Giải mã bằng private key của người nhận.

- Xác thực email: Động tác ký = mã hóa message bằng private key của người gửi. Xác thực = dùng public key của người gửi giải mã bản tin.

* Các phiên bản S/MIME
* Phiên bản S/MIME v1: năm 1995, nhưng không được công bố chính thức.
* Phiên bản S/MIME v2 được IETF chính thức công bố vào tháng 3/1998 là một tiêu chuẩn Internet tại RFC 2311 và RFC 2312 . S/MIME đã trở thành một trong những tiêu chuẩn hàng đầu về bảo mật thông điệp.
* Phiên bản S/MIME v3 được IETF đề xuất vào tháng 6/1999 nhằm tăng cường khả năng của S/MIME, bao gồm RFC 2632 , RFC 2633 và RFC 2634, được cập nhật mới đây nhất tại RFC 5751 tháng 1/2010.
* Trong Thông tư số 01/2011/TT-BTTTT ngày 04/01/2011 của Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định Bắt buộc áp dụng tiêu chuẩn S/MIME v3.2 và được xếp vào nhóm Tiêu chuẩn về an toàn thông tin.
* **Giao thức PGP**
* PGP (Pretty Good Privacy):

- Là một chương trình cung cấp tính năng mã hóa và xác thực cho dữ liệu. PGP thường được sử dụng để ký, mã hóa, và giải mã văn bản, e-mail, các tập tin, thư mục và phân vùng đĩa toàn bộ để tăng tính bảo mật của thông tin liên lạc e-mail.

- Được tạo ra bởi Phil Zimmermann vào năm 1991.

- PGP còn được sử dụng khá phổ biến cho nhiều đối tượng cũng như các ứng dụng khác ngoài e-mail.

* PGP sử dụng các thuật toán:   
  • Mã hóa đối xứng: DES, 3DES, AES, v.v.

• Mã khóa KCK: RSA, ElGamal.

• Hàm băm: SHA-1, MD-5, v.v.

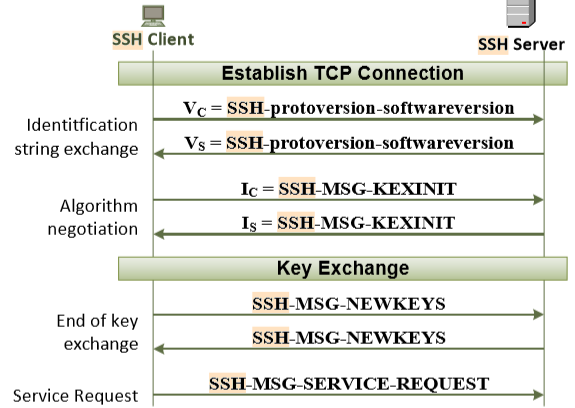
* + - Chữ ký: RSA, DSS, ECDSA, v.v.

1. **Hiểu được các hiểm họa an toàn thông tin đối với các dịch vụ web và email, từ đó trình bày các giải pháp an toàn (ở tầng ứng dụng và tầng giao vận) để chống lại các hiểm họa đó. (\*)**

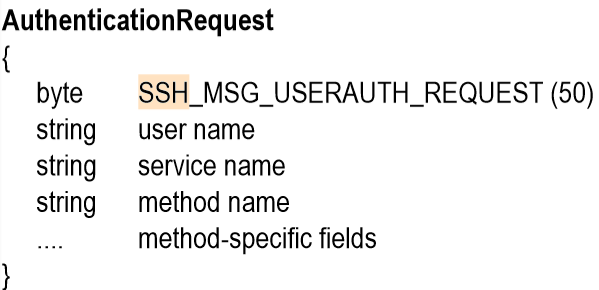
* Các hiểm họa an toàn thông tin đối với dịch vụ Web:
  + Người dùng không thể xác thực được server: người dùng cứ mặc định gửi request đến server chứ không có bất kỳ phương pháp nào để xác thực đó chính là server.
  + Dữ liệu được truyền dưới dạng rõ => dễ bị tấn công (như tấn công chặn bắt thông tin, thay đổi thông tin)
  + Dễ bị tấn công Social Engineering để lộ thông tin tài khoản, mật khẩu,…=> Người dùng có thể bị kiểm soát máy tính, đánh cắp dữ liệu,…
* Các hiểm họa an toàn thông tin đối với dịch vụ Email:
  + Thư có thể bị đọc/sửa trên đường truyền
  + Thư có thể bị đọc/sửa trên máy chủ
* Không thể yên tâm khi gửi thư. Nếu như chỉ sử dụng SMTP và MINE thì người khác vẫn có thể đọc được thư. => Dễ bị tấn công chặn bắt thư và xem nội dung cũng như sửa đổi các nội dung và định danh người gửi.
  + Người dùng dễ nhận được các email giả mạo chứa mã độc, hay các phần mềm độc hại khác.
* Các giải pháp an toàn ở tầng ứng dụng:
  + Đối với dịch vụ Email:
    - Hai giao thức chủ yếu là S/MINE và PGP
    - Nguyên tắc thực hiện: mã hóa, ký số, kết hợp ký và mã
* Các giải pháp an toàn ở tầng giao vận:
  + Đối với dịch vụ Web:
    - Sử dụng giao thức an toàn lớp dưới: SSL/TLS, HTTP + TLS = HTTPS
    - Để sử dụng TLS:
      * Kích hoạt TLS trước khi bắt đầu HTTP
      * Gọi TLS như là một dịch vụ tùy chọn của HTTP:
        + Trong chuẩn RFC 7838: HTTP Alternative services
        + RFC 8164: Opportunistic Security for HTTP/2
    - HTTPS được thiết kế để chống lại tấn công ở giữa và tấn công nghe trộm. Mọi thông tin trong thông báo HTTPS đều được mã hóa và xác thực bao gồm cả phần header và nội dung.

1. **Trình bày các đặc điểm cơ bản của các giao thức con của SSH (SSH Trans, SSH Auth, SSH Conn), SSH Port forwarding. (\*)**

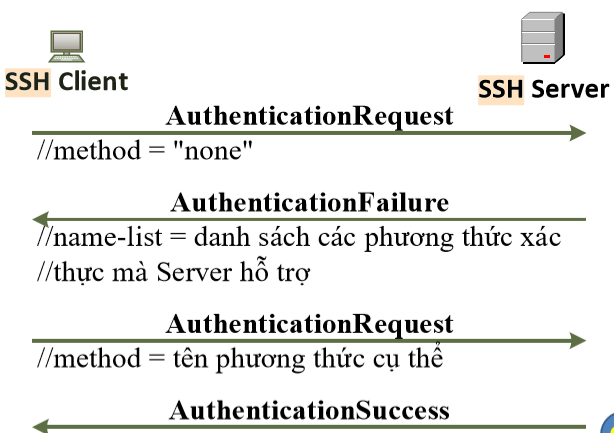
* Chức năng chủ yếu là SSH là remote login. Ngoài ra còn có chức năng khác: truyền file an toàn với SCP, SFTP. Nó còn có thể được sử dụng để bảo vệ bất kỳ ứng dụng nào nhờ cơ chế port forwading
* Các giao thức con của SSH:
  + SSH trans: là giao thức làm nhiệm vụ quan trọng nhất: xác thực server, bảo vệ dữ liệu khi truyền, trao đổi khóa bí mật giữa hai bên (sử dụng thuật toán mã khối).
    - SSH packet exchange:



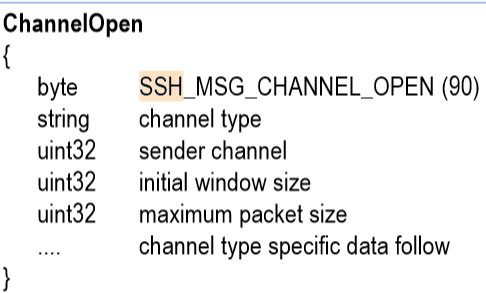
* + - B1: Client mở kết nối TCP tới server (đây không phải là một phần của SSH trans)
    - B2: Client gửi đến Server -> Vc là chuỗi định danh client, Server gửi lại cho Client -> Vs là chuỗi định danh server. (2 chuỗi này được sử dụng trong xác thực server)
    - B3: Client và Server thỏa thuận bộ thuật toán và tham số: client đề xuất nhiều (Ic), server lựa chọn một bộ (Is). Bộ thuật toán gồm: trao đổi khóa, mã hóa, xác thực và nén.
    - B4: Key exchange -> trao đổi khóa sử dụng Diffie Hellman. Server được xác thực bằng mật mã khóa công khai trong quá trình trao đổi khóa.
      * Gọi là SSH Server host key (Ks).
      * Một server có thể có nhiều host key
      * Nhiều server có thể có chung một host key.
      * Mô hình tin cậy: client quản lý danh sách các khóa công khai của các server tin cậy, sử dụng PKI.
    - B5: Client gửi đến Server thông tin về Newkeys và Server cũng gửi ngược lại. Báo hiệu việc kết thúc trao đổi khóa. Cả hai bên có khóa chung để mã hóa mọi thông điệp.
    - B6: Client gửi yêu cầu dịch vụ (có thể là SSH-AUTH hoặc SSH-CONN).
  + SSH auth:



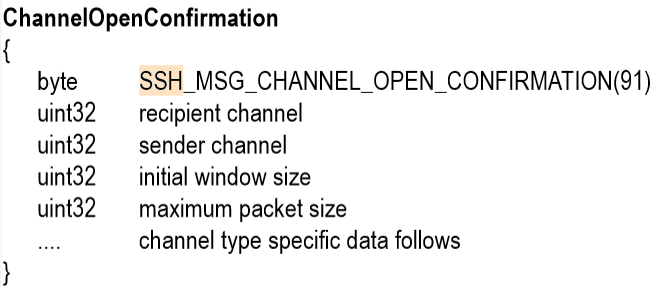
* + - SSH\_MSG\_USERAUTH\_REQUEST: Các kiểu dữ liệu: byte, uint32, string,… được định nghĩa tại mục 5 của RFC 4251: SSH protocol architecture
    - Method name: phương thức xác thực: được chọn trong số các phương thức là Server hỗ trợ. “Public key”, “password”, “hostbased”. “none” để yêu cầu danh sách.
    - Username để định danh người dùng
    - Service name: dịch vụ muốn được thực thi sau khi xác thực thành công
    - Method-specific fields: tùy thuộc vào phương thức xác thực cụ thể được sử dụng.
    - Kịch bản điển hình:



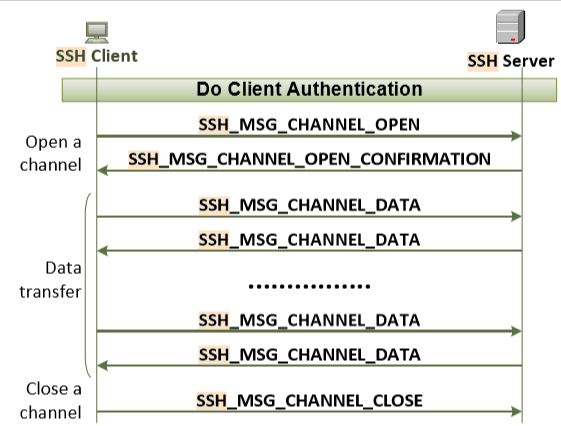
* + SSH conn:



* + - Channel type: “session” :thực thi ứng dụng từ xa, “x11”: X Window System, “forwarded-tcpop”: Remote port forwarding, “direct-tcpip”: local port forwarding.
    - Sender channel: số hiệu kênh đối với sender của thông điệp này. Hai bên có thể sử dụng hai số hiệu khác nhau để tham chiếu đến cùng một kênh
    - Initial window size: số byte tối đa được phép gửi cho sender của thông điệp này trước khi phải chờ đợi nó gửi thông điệp điều chỉnh kích thước cửa số. Mỗi bên tự quyết định giá trị này.



* + - Recipient channel: số hiệu kênh đối với receiver của thông điệp này (tức là sender của thông điệp ChannelOpen)
    - Sender channel: Số hiệu kênh đối với sender của thông điệp này
    - Kịch bản điển hình

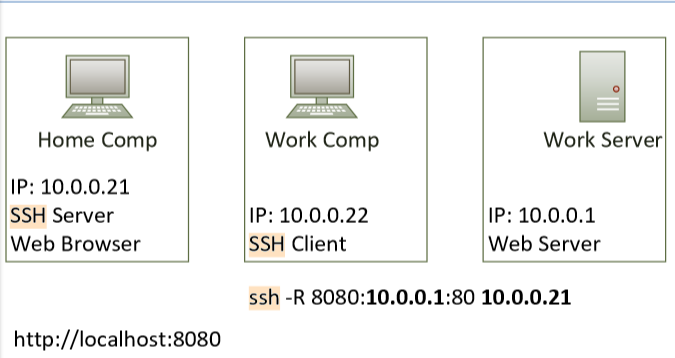


* SSH port forwarding:
  + SSH local port forwarding:

A screenshot of a cell phone

Description automatically generated

* + - SSH server và app server nằm gần nhau, SSH client và app client nằm cùng nhau
    - Cho phép app client kết nối app server thông qua cổng <Iport> trên máy cục bộ ssh client
    - Webserver địa chỉ: <http://localhost:8080>
    - Mục đích: app client muốn kết nối đến app server => sử dụng ssh client để tạo đường hầm trực tiếp từ port 8080 đến port 80 thông qua ssh server qua port 20
    - SSH client sử dụng câu lệnh: ssh -L 8080:10.0.0.1:80 10.0.0.1, trong đó:
      * L 8080: local port 8080 :cổng của ssh client
      * 10.0.0.1:80 : địa chỉ IP của máy đích và port của web server
      * 10.0.0.1: địa chỉ IP của ssh server
* Tạo trực tiếp đường hầm socket an toàn từ port 8080 của ssh client đến app server port 80 thông qua đường hầm ssh sử dụng chuyển tiếp qua cổng 22 của ssh server
  + SSH remote port forwarding

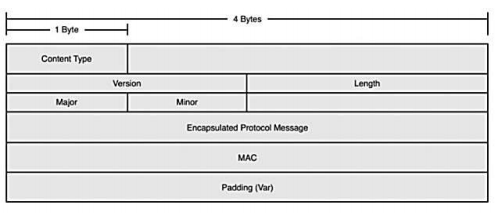


Cách thức một nhân viên của KMAComp sử dụng dịch vụ Remote Port Forwading của SSH để thiết lập kết nối an toàn:

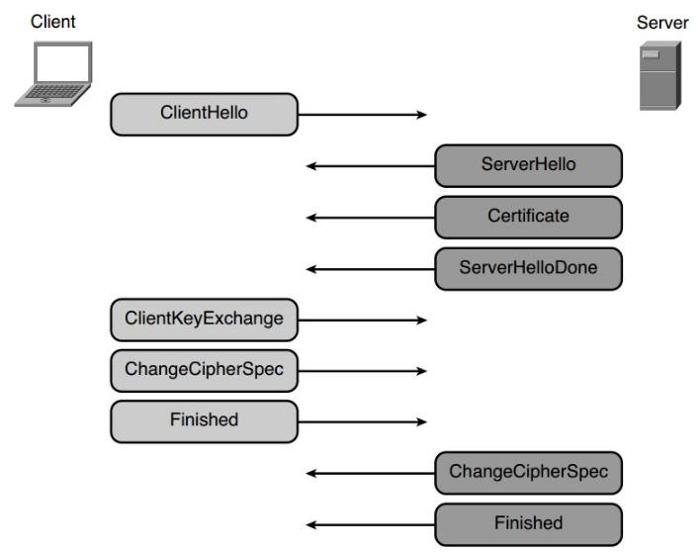
* + - Gỉa sử webserver có tên miền: <http://localhost:8080>
    - Mục đích: thiết lập kết nối an toàn từ Home Comp đến Webserver thông qua Work comp của nhân viên
    - Sử dụng SSH, Home Comp đang muốn kết nối an toàn từ cổng 8080 của mình đến cổng 80 của Webserver => sử dụng Remote Port Forwarding vì Webserver và Home Comp đang ở xa nhau => sử dụng thành phần trung gian Work comp
    - Bên phía Work comp sẽ thực hiện: ssh -R 8080:10.0.01:80 10.0.0.21, trong đó:
      * 8080 là R port, là cổng từ xa của Home Comp
      * 10.0.0.1 là localhost : localhost chính là địa chỉ ip của Webserver mà Home Comp muốn truy cập đến
      * 80 là port của Webserver
      * 10.0.0.21: là địa chỉ IP của Home Comp
* Để Home Comp muốn truy cập tạo 1 đường hầm trực tiếp từ port 8080 đến port 80 của Webserver thì cần phải sử dụng Work comp bằng cách Work comp sẽ thực hiện câu lệnh trên => Mở một cổng trực tiếp một socket an toàn trực tiếp từ port 8080 đến port 80

1. **Trình bày đặc điểm cơ bản của bộ giao thức SSL/TLS, đặc biệt là hai giao thức con Handshake hay Record .**

* **Đặc điểm cơ bản của giao thức SSL**
* SSL (Secure Sockets Layer) là một giao thức cung cấp dịch vụ truyền thông có bảo mật giữa client và server, cho phép client và server xác thực lẫn nhau sử dụng chữ ký số và bảo mật thông tin trao đổi qua lại bằng cách mã hóa các thông tin đó
* Được phát triển bởi hãng Netscape.
* SSL nằm giữa tầng application và tầng transport trong mô hình OSI, và sử dụng TCP làm giao thức vận chuyển nhằm truyền các gói tin một cách tin cậy.
* Bên trong mỗi gói tin SSL là phần Record header chịu trách nhiệm đóng gói các message sẽ truyền đi. Hình dưới đây là định dạng Record trong gói tin SSL



* Content type: 1byte, cho biết loại message được đóng gói bên trong record này. Có 4 loại message:
* Handshake: 22
* Change Cipher Spec:20
* Application: 23
* Alert: 21
* Length: 2 byte, chiều dài của recode này
* Encapsulated protocol message: Phần message hoặc application data được trao đổi giữa client và server trong phiên làm việc. Sau khi các tham số liên quan đến encryption và hash được thương lượng xong thì trường này sẽ được mã hóa
* MAC: giá trị MAC (message authentication code) được tính toán cho phần application data chứa trong encapsulated protocol message để đảm bảo tính toàn vẹn
* Padding: chèn thêm vào phàn encapsulated protocol message cho đủ kích thước của một block. Trường này không cần khi dùng kiểu mã hóa dòng (stream cipher)
* **Những dịch vụ an toàn mà SSL cung cấp**
* Xác thực server: Cho phép người sử dụng xác thực được server muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hoá công khai để chắc chắn rằng certificate và public ID của server là có giá trị và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của client. Điều này rất quan trọng đối với người dùng. Ví dụ như khi gửi mã số credit card qua mạng thì người dùng thực sự muốn kiểm tra liệu server sẽ nhận thông tin này có đúng là server mà họ định gửi đến không.
* Xác thực Client: Cho phép phía server xác thực được người sử dụng muốn kết nối. Phía server cũng sử dụng các kỹ thuật mã hoá công khai để kiểm tra xem certificate và public ID của server có giá trị hay không và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của server không. Điều này rất quan trọng đối với các nhà cung cấp. Ví dụ như khi một ngân hàng định gửi các thông tin tài chính mang tính bảo mật tới khách hàng thì họ rất muốn kiểm tra định danh của người nhận.
* Mã hoá kết nối: Tất cả các thông tin trao đổi giữa client và server được mã hoá trên đường truyền nhằm nâng cao khả năng bảo mật. Điều này rất quan trọng đối với cả hai bên khi có các giao dịch mang tính riêng tư. Ngoài ra, tất cả các dữ liệu được gửi đi trên một kết nối SSL đã được mã hoá còn được bảo vệ nhờ cơ chế tự động phát hiện các xáo trộn, thay đổi trong dữ liệu. ( đó là các thuật toán băm – hash algorithm).
* **Các giao thức con của SSL**
* Giao thức SSL record: phân mảnh, nén, tính MAC, mã hóa dữ liệu
* Giao thức SSL handshake (gọi là giao thức bắt tay) : thực hiện chức năng thỏa thuận các thuật toán, tham số, trao đổi khóa, xác thực server và client (nếu có lựa chọn)
* Giao thức SSL Alert: thông báo lỗi
* Giao thức SSL Change cipher spec protocol: thông báo xác nhận kết thúc giai đoạn Hanshake protocol
* **Quá trình bắt tay của client và server sử dụng SSL**



* Giai đoạn 1: Thiết lập protocol version, ID phiên, thuật toán mã hóa, phương pháp nén, trao đổi giá trị random
* B1: Client gửi một thông điệp ClientHello tới server. Các thành phần quan trọng của một thông điệp ClientHello:
  + Version: phiên bản SSL cao nhất mà client hỗ trợ.
  + Random: Một cấu trúc ngẫu nhiên được sinh ra, bao gồm một nhãn thời gian 32 bit và 28 byte được sinh bởi bộ sinh số ngẫu nhiên bảo mật.
  + Session ID: định danh phiên
  + CipherSuite: danh sách thuật toán mã hóa và băm mà client hỗ trợ (TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA)
  + Compression method: danh sách thuật toán nén dữ liệu mà client hỗ trợ.
* B2: Server gửi SeverHello tới client để trả lời cho gói ClientHello, nội dung tương tự như ClientHello, tuy nhiên có một số điểm khác biệt
  + Version : Server chọn ra phiên bản SSL cao nhất mà cả client và server cùng hỗ trợ.
  + Random : giá trị ngẫu nhiên được sinh ra bởi server, bốn byte đầu là nhãn thời gian (để tránh các giá trị ngẫu nhiên lặp lại), các byte còn lại sẽ được tạo bởi bộ sinh số ngẫu nhiên bảo mật lập mã.
  + CipherSuiter : lựa chọn ciphersuite tốt nhất trong danh sách các ciphersuite mà nó và client hỗ trợ.
  + CompressionMethod : lựa chọn một phương pháp nén trong các phương pháp nén mà nó nhận được từ client.

Sau hai bước này, client và server đã thương lượng xong các thuật toán mã, nén dữ liệu và thuật toán băm.

* Giai đoạn 2 : server gửi certificate, dữ liệu trao đổi khóa và ueeu cầu client gửi lại certificate nếu được thiết lập xác thực client.
* Bước 3 : server gửi chứng thư (SSL certificate) của nó cho client, và trong certificate này có chứa public key của server.

Client nhận được certificate của server sẽ sử dụng public key cảu CA để kiểm tra chữ kỹ số đó. Nếu certificate của server hợp lệ thì client chấp nhận public key của server trong certificate đó.

* Bước 4 : server gửi ServerHelloDone tới client để cho biết server đã gửi hết tất cả các thông tin mà nó có cho client.
* Giai đoạn 3 : client gửi certificate nếu được yêu cầu, kết quả kiểm tra chứng chỉ server và dữ liệu trao đổi khóa)
* Bước 5 : ClientKeyExchange do client gửi đến server và chứa thông tin để tạo ra masterkey
* client sinh một Pre\_master secret
* mã hóa nó bằng public key lấy từ certificate của server
* thuật toán mã hóa đã thương lượng (ví dụ RSA)

Server :

* giải mã private key của mình.
* Bây giờ cả client và server sẽ sử dụng pre\_master secret cùng với hai số ngẫu nhiên đã sinh trước đó để tạo ra master key
* Từ master key sẽ tạo ra session key dùng để mã hóa dữ liệu
* Giai đoạn 4 : Change CipherSuit và kết thúc giai đoạn HandShake
* Bước 6 : ChangCipherSpec : client gửi thông báo đến server để cho biết tất cả các gói tin trao đổi giữa client và server đều sẽ được mã hóa bằng các thuật toán và session key đã thương lượng trước đó.
* Bước 7 : Finished : do client gửi đến server để cho biết client đã hoàn tất việc thiết lập tunnel
* Bước 8 : ChangeCipheSpec : server gửi thông báo này đến client để cho biết tất cả các gói tin trao đổi giữa server và client đều sẽ được mã hóa bằng các thuật toán và sessio key đã thương lượng trước đó
* Bước 9 : Finished : do server gửi đén client để cho biết server đã hoàn tất việc thiết lập tunnel
* **So sánh SSL và TLS**

|  |  |  |
| --- | --- | --- |
|  | **SSL** | **TLS** |
| Version | 1.2, 2.0, 3.0 | 1.0 (SSL 3.1), 1.1, 1.2, 1.3 |
| Nhà sản xuất | Netscape | IETF |
| Chuẩn | Chưa chuẩn hóa | được chuẩn hóa |
| Xác thực | MAC | HMAC (hàm băm+khóa) |
| Thông điệp cảnh báo | It thông điệp cảnh báo | Nhiều thông điệp cảnh báo và thêm nhiều giải thuật |

# **Chương 4: Giao thức an toàn mạng riêng ảo**

1. **VPN:**

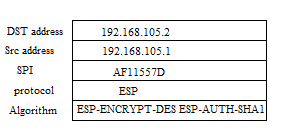
* **Định nghĩa**
* **Lợi ích của VPN**
* **Các mô hình VPN thông dụng**
* Mạng riêng ảo (Virtual Private Network - VPN): là mạng sử dụng mạng công cộng (như Internet, ATM/Frame Relay của các nhà cung cấp dịch vụ) làm cơ sở hạ tầng để truyền thông tin nhưng vẫn đảm bảo là một mạng riêng và kiểm soát được truy nhập. Đặc điểm của mạng riêng:
  + Toàn quyền quản trị
  + Cô lập lưu lượng: lưu lượng không thể đi qua mạng chung, nếu có thì phải có sự chuyển đổi địa chỉ
  + Sử dụng dải địa chỉ IP dành riêng: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
  + VPN là một khái niệm, không phải là một giao thức. Nó có thể được hiện thực hóa bằng các giao thức khác nhau
* Trong thực tế người ta thường nói tới hai khái niệm VPN đó là: mạng riêng ảo kiểu tin cậy (Trusted VPN) và mạng riêng ảo an toàn (Secure VPN).
  + Trusted VPN: Được xem như 1 số mạch thuê của 1 ISP viễn thông, duy trì tính toàn vẹn và khả năng sử dụng cho mạng liên lạc của khác hàng. Không đảm bảo an ninh an toàn và bảo mật cho khách hàng.
  + Secure VPN: Là các mạng riêng ảo có sử dụng mật mã để bảo mật (mã hóa và xác thực) dữ liệu. Dữ liệu ở đầu ra của 1 mạng được mã hóa rồi chuyển vào mạng công cộng (ví dụ: mạng Internet) như các dữ liệu khác để truyền tới đích và sau đó được giải mã dữ liệu tại phía thu
* Ảo (Virtual): Nghĩa là cơ sở hạ tầng vật lý của mạng hoàn toàn trong suốt với kết nối VPN.
* Riêng (Private): Chỉ tính riêng biệt của lưu lượng dữ liệu khi qua VPN. Dữ liệu truyền luôn luôn được giữ bí mật và chỉ có thể được truy cập bởi những nguời sử dụng được trao quyền.
* Mạng (Network): là thực thể hạ tầng mạng giữa những người sử dụng đầu cuối, những trạm hay những node để mang dữ liệu.
* Ví dụ: Mạng VLAN, mạng sử dụng đường leased line, mạng MPLS VPN, mạng IPsec VPN, SSL VPN...
* Phân loại theo cấu trúc: VPN gồm có 2 loại (Remote Access VPN và Site-to-Site VPN)
  + Remote access VPN : VPN truy cập từ xa) : cung cấp truy cập tin cậy cho các nhân viên di động, nhân viên ở xa, nhân viên làm việc tại nhà,…truy cập đến các tài nguyên mạng của đơn vị mình.
  + Site to Site VPN: gồm có 2 loại:
    - Intranet VPN (VPN cục bộ) : mở rộng các dịch vụ của mạng nội bộ tới các trụ sở ở xa, cho phép các văn phòng chi nhánh liên kết một cách bảo mật tới trụ sở chính của doanh nghiệp. Còn được gọi là mạng riêng ảo chi nhánh.
    - Extranet VPN (VPN mở rộng): mở rộng cho phép khách hàng và đối tác có thể truy cập một cách bảo mật đến Intranet của doanh nghiệp.
* Lợi ích: Tính bí mật, tính toàn vẹn, xác thực, chống tấn công phát lại

1. **Trình bày về SA:**

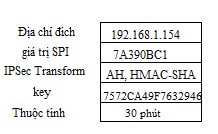
* **Khái niệm:**
  + SA (Security Associations) là một khái niệm cơ bản của bộ giao thức IPSec. SA là một kết nối logic theo một hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSec.
  + Có hai kiểu SA
* ISAKMP SA (hay IKE A)
* IPSec SA
* **Trình bày các thành phần cơ bản của SA (SPI, Đ/c IP đích, giao thức con của IPSec).**
* Một SA gồm 3 phần: <Chỉ số tham số an toàn, Địa chỉ IP đích, Giao thức an toàn>



* SPI:
* Là một trường 32 bit, dùng để xác định một SA để gắn với một gói dữ liệu
* Là một chỉ số duy nhất cho mỗi bản ghi của cơ sở dữ liệu SADB (giống khóa chính).
* Được định nghĩa bởi người tạo SA, được lựa chọn bởi hệ thống đích khi thương lượng SA.
* SPI nhận các giá trị trong khoảng từ 1…255
* Địa chỉ IP đích: Là địa chỉ IP của Node đích
* Giao thức an toàn:
* Mô tả giao thức an toàn IPSec được dùng, có thể là AH hoặc ESP
* Với hai điểm liên lạc: cần một SA cho mỗi hướng.
* SA có thể cung cấp các dịch vụ an toàn cho một phiên VPN (được bảo vệ bởi AH hay ESP).
* Nếu một phiên VPN được bảo vệ kép bởi cả AH và ESP thì mỗi hướng kết nối cần định nghĩa 2 SA.
* **Trình bày cơ bản được hai cơ sở dữ liệu về SA là SAD và SPD.**
  + Cơ sở dữ liệu tổ hợp an toàn (SAD - Security Association Database): Duy trì thông tin liên quan tới mỗi SA, bao gồm: các khoá, thuật toán, thời gian có hiệu lực của SA, chuỗi số tuần tự.
  + Cơ sở dữ liệu chính sách an toàn (SPD - Security Policy Database)
* Lưu các chính sách để thiết lập các SA
* Duy trì thông tin về các dịch vụ an toàn kèm theo với một danh sách chính sách các điểm vào và ra.
* Định nghĩa luồng lưu lượng được xử lý/bỏ qua
* **Các ví dụ về SA (IPSec SA và IKE SA), phân biệt IKE SA và IPSec SA.**
* Ví dụ IPSec SA



* Ví dụ IKE SA



* Phân biệt IKE SA và IPSec SA:
  + IKE SA chứa các thông số để tạo nên kênh truyền bảo mật, còn IPSec SA chứa các thông số để đóng gói dữ liệu theo ESP hay AH, hoạt động theo tunnel mode hay transport mode
  + IKE SAs (được thiết lập trong IKE session)
  + IPSec SAs (các SA này được IKE thương lượng

1. **IPSec:**

- **Trình bày đặc điểm cơ bản về giao thức IPSec:**

* IPSec = Internet Protocol Security là một bộ giao thức để đảm bảo an toàn thông tin liên lạc sử dụng bộ giao thức Internet bằng cách xác thực và mã hóa mỗi gói tin IP của một phiên.
* Được phát triển bởi IETF
* Thực hiện việc an toàn các gói IP
* Cung cấp các khả năng:
* Xác thực nguồn gốc thông tin
* Kiểm tra tính toàn vẹn thông tin
* Đảm bảo bí mật nội dung thông tin
* Cung cấp khả năng tạo và tự động làm tươi khoá mật mã một cách an toàn
* IPSec cung cấp một khung an toàn tại tầng 3 của mô hình OSI
* Thực hiện đảm bảo an toàn tại tầng IP
* Các giao thức tầng trên và các ứng dụng có thể dùng IPSec để đảm bảo an toàn mà không cần phải thay đổi gì => Các gói IP sẽ được bảo vệ mà không phụ thuộc vào các ứng dụng đã tạo ra nó
* IPSec hoàn toàn trong suốt với người dùng
* IPSec hoạt động ở hai chế độ:
* Chế độ Transport (end-to- end)
* Chế độ Tunnel (cho VPN)

**- Kể tên các thành phần và giao thức con của IPSec:**

* IPSec bao gồm 2 giao thức:
* Tiêu đề xác thực (AH – Authentication Header)
* Đảm bảo tính toàn vẹn,
* Cung cấp khả năng bảo vệ chống lại sự giả mạo,
* Cung cấp chế độ xác thực đối với máy chủ

ICV = hash (IP header + payload + key )

* Đóng gói tải an toàn (ESP – Enscapsulating Security Payload): Thực hiện các chức năng như AH, nhưng có thêm tính năng đảm bảo bí mật dữ liệu.
  + ICV = hash (New IP header + IP header + payload )
  + Payload = encrypt (IP header + payload + IV)

- **Các dịch vụ an toàn mà IPSec đem lại**

* Host – to – host
* Host – to – gateway
* Gateway – to – gateway

- **Ưu, nhược điểm của IPSec.**

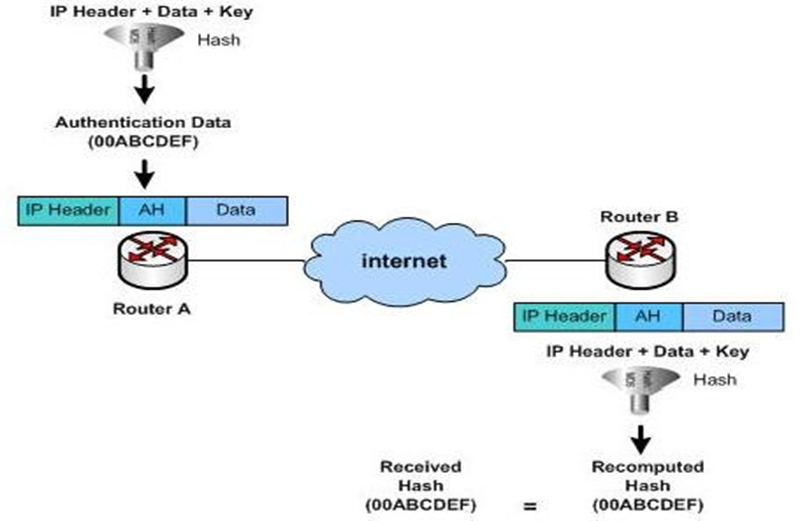
* **Ưu điểm:**
* Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan tới bảo mật.
* IPSec được thực hiện bên dưới lớp TCP và UDP ,đồng thời nó hoạt động trong suốt đối với các lớp này.Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
* IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối,điều này giúp che dấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua Internet.
* **Nhược điểm:**
* Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
* IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
* Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
* Việc phân phối các phần cứng và phầm mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia

1. **AH và ESP: (\*)**

* **Các dịch vụ an toàn mà chúng cung cấp:**
  + AH: xác thực, toàn vẹn.
  + ESP: xác thực, toàn vẹn, mã hóa, chống replay gói tin cũ
* **Vẽ được khuông dạng gói tin, xác định các đoạn được xác thực và/hoặc đoạn được mã hóa) (Câu 2 – bài tập)**
* **Phân tích được các trường trong AH Header (Next header, payload length (chiều dài thông điệp AH), reserverd (0), SPI (chỉ ra SPI được sử dụng + SPD), Sequence number (số thứ tự gói tin AH) , ICV=Hash(IP header + payload+key), và các trường của ESP (ESP Header (Sequence number, SPI), ESP Trailer(Padding, Pad length, Next header), ESP Authentication(ICV = HMAC(ESP header + Payload + ESP trailer + Key) (Câu 2 -bài tập)**
* **So sánh sự khác nhau giữa AH và ESP. Nêu được các ưu, nhược điểm của AH và ESP.**

|  |  |
| --- | --- |
| AH | ESP |
| Được đóng gói bởi giao thức IP (trường protocol trong IP là 51) | ESP được đóng gói bởi giao thức IP (trường protocol trong IP là 50) |
| Đảm bảo tính xác thực, toàn vẹn | Đảm bảo tính xác thực, toàn vẹn, mã hóa |
| Đảm bảo tính xác thực mạnh | Đảm bảo tính xác thực yếu |
| Không Nat ra internet | Nat ra internet |

* **Giải thích được khả năng đảm bảo toàn vẹn và xác thực dữ liệu cho gói tin IP nhờ giao thức AH, khả năng vượt NAT của AH.**



Bước 1: toàn bộ gói IP ( bao gồm IP Header và Data) được chạy qua một giải thuật băm một chiều cùng với 1 key (hai bên đã thỏa thuận trước)

Bước 2: giá trị băm thu được dùng xây dựng một AH Header, đưa header này chèn vào dữa IP Header và Data của gói tin ban đầu.

Bước 3: Gói dữ liệu sau khi thêm AH header được truyền tới đối tác.

Bước 4: Bên thu thực hiền hàm băm với IP Header và data với key mà hai bên đã thỏa thuận trước, kết quả thu được một giá trị băm

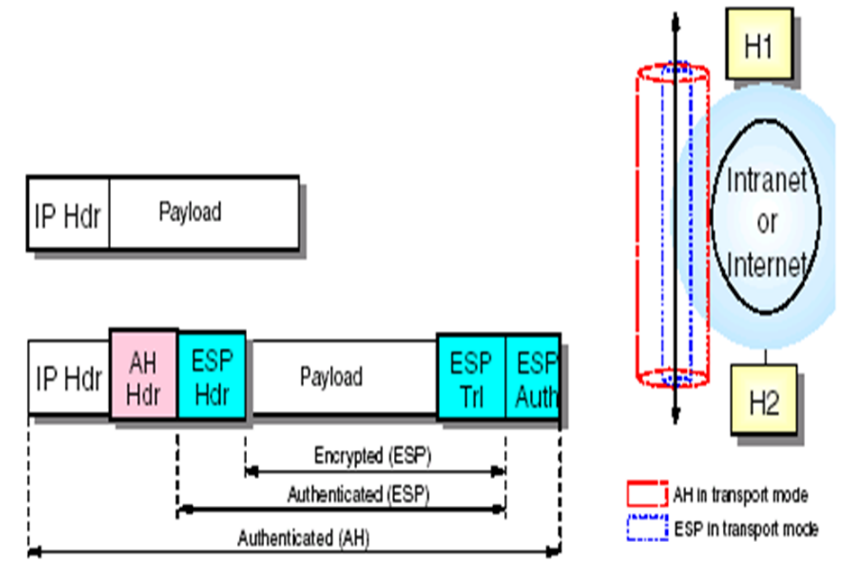
Bước 5: bên thu tách giá trị băm trong AH Header và so sánh với giá trị băm mà nó vừa tính. Nếu hai mã này giống nhau thì gói tin này đã được đảm bảo toàn vẹn và xác thưc, nếu khác nhau thì bên thu sẽ phát hiện ra ngay gói tin này không còn toàn vẹn (dựa vào tính chất kháng va chạm của hàm băm)

* **Giải thích được khả năng đảm bảo toàn vẹn, xác thực dữ liệu và mã hóa cho gói tin IP nhờ giao thức ESP.**

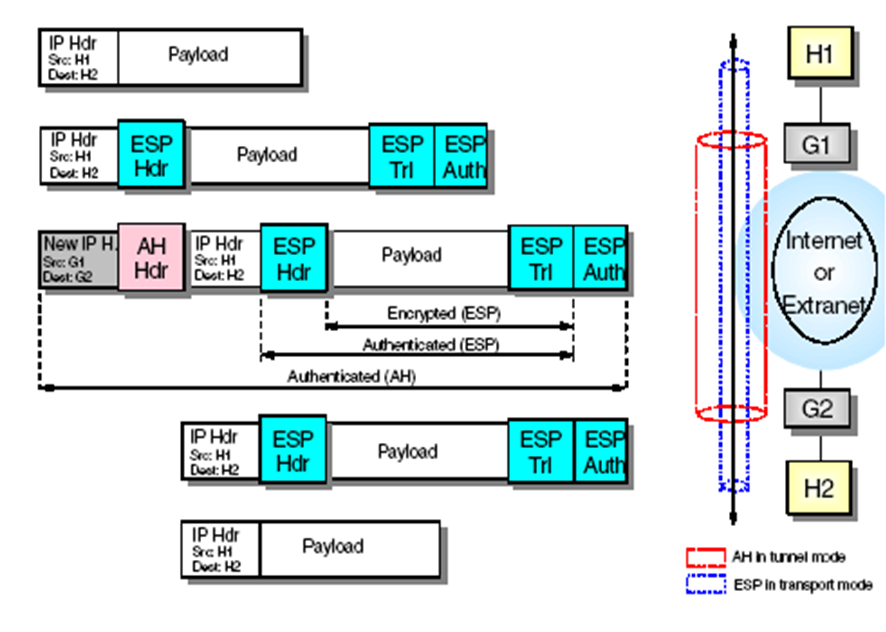
A screenshot of a cell phone

Description automatically generated

* **Vẽ và phân tích được định dạng gói tin khi được bảo vệ kép bởi AH và ESP. (Câu 2 – Bài tập)**
  + Chế độ transport



* + Chế độ tunnel



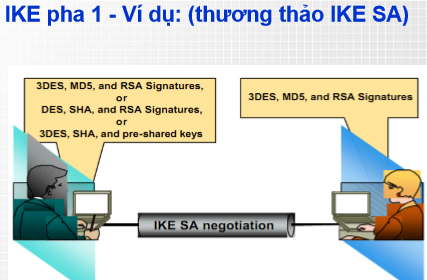
1. **IKE:**

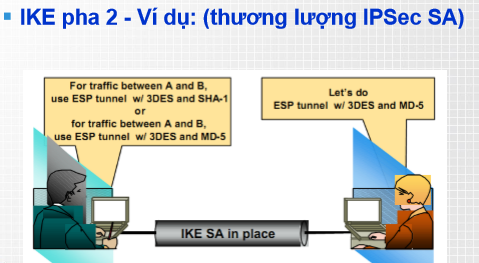
* **Đặc điểm cơ bản:**
  + Là giao thức để quản lý, trao đổi khóa trong IPSec
  + Cho phép thương lượng và tạo tự động các IPSec SA giữa các bên liên lạc IPSec.
  + IKE cũng chịu trách nhiệm xoá các khoá, SA sau khi một phiên truyền tin kết thúc
  + IKE không nhanh nhưng hiệu quả vì một số lượng lớn SA được thương lượng chỉ với một số thông điệp vừa phải.
  + IKE được xây dựng dựa trên nền tảng của hai giao thức
* Giao thức phân phối khóa Oakley
* Giao thức quản lý khóa ISAKMP
  + IKE Có thể được sử dụng bên ngoài IPSec
  + IKE hiện đã được phát triển với 2 phiên bản, phiên bản IKEv1 và IKEv2.
* **Vai trò trong bộ giao thức IPSec**
* IPSec cần các SA để bảo vệ lưu lượng
* Nếu chưa có các SA, IPSec sẽ yêu cầu IKE cung cấp các IPSec SA.
* IKE mở một phiên quản lý với các bên tham gia, và thương lượng tất cả các SA và các khóa cho IPSec.
* IPSec bắt đầu thực hiện bảo vệ lưu lượng.
* **Mô tả các bước cơ bản của hai pha hoạt động của IKE và vai trò của từng pha trong giao thức IKE, cho ví dụ.**
* IKE gồm 2 pha: 2 pha trao đổi khoá sẽ tạo ra IKE SA và một đường hầm an toàn giữa 2 hệ thống:
  + Một bên sẽ đưa ra một trong các thuật toán, phía kia sẽ chấp nhận hoặc loại bỏ kết nối.
  + Khi 2 bên đã thống nhất được thuật toán sử dụng thì sẽ tạo khoá cho IPSec
  + Khoá này có được nhờ sử dụng thuật toán DiffieHellman.
* Pha 1:
  + Xác thực các bên tham gia và cung cấp bảo vệ cho việc thương lượng ở pha 2: Để thiết lập IKE SA, các bên tham gia phải xác thực lẫn nhau (2-chiều). Các phương pháp xác thực: »Dùng khóa bí mật chia sẻ trước »Dùng các số Nonce được mã hóa RSA »Chữ ký số RSA »Chứng chỉ số -certificate
  + Mã hóa phiên IKE: –Phiên IKE được mã hóa bởi DES hoặc 3DES –Khóa dùng cho mã hóa được đưa ra bởi trao đổi khóa DH. –Trong Main mode, định danh các bên cũng được mã hóa –Trong Aggressive mode, định danh các bên không được mã hóa
  + Toàn vẹn phiên IKE

Pha 2: Mục đích chính là thỏa thuận được các khóa mật mã sử dụng để bảo vệ đường truyền cho các thực thể, và các SA cho trao đổi dữ liệu

* + Bước 1 : Thương thảo chính sách : một bên sẽ đưa ra một danh sách các giao thức IPSec và các thuật toán, bên nhận sẽ lựa chọn hoặc có yêu cầu khác. Sau khi thương lượng xong, 2 SA được thiết lập cho mỗi bên : Một SA cho lưu lượng INBOUND và một SA cho lưu lượng OUTBOUND
  + Bước 2 : Khóa phiên được làm tươi hoặc trao đổi qua DH : Khóa này làm nhiệm vụ cho: xác thực, toàn vẹn, mã hóa (nếu cần) trong phiên IPSec.
    - Có 2 lựa chọn:
      * Làm tươi khóa KM thu được bằng DH trong pha 1
      * Thực hiện trao đổi khóa DH lần 2, để thu được Ks (rekey)
  + Bước 3 : các SA, Keys cùng với SPI được truyền tới IPSec driver : Kết quả pha 2:
    - Là một cặp SA mới (inbound & outbound) được dùng để bảo vệ lưu lượng IP
    - Mỗi SA có SPI và key riêng của nó
    - Các khóa mới được tạo cho: xác thực, toàn vẹn hay mã hóa.
    - Sau khi cặp SA mới được tạo ra, cặp SA cũ bị xóa, và lưu lượng được bảo vệ với cặp SA mới

**Cho ví dụ**





# **Chương 5. Các giao thức an toàn mạng không dây**

1. **Mạng không dây (Wireless network):**

* **Phân loại (5 loại mạng không dây)** 
  + Mạng không dây (Wireless Network): Là phƣơng thức truyền dữ liệu từ điểm này đến điểm khác không sử dụng đƣờng dây vật lý mà sử dụng sóng vô tuyến, sóng hồng ngoại và vệ tinh.
  + Các kết nối được thiết lập theo chuẩn định sẵn: 802.11, 802.15, 802.16…
  + Ưu điểm: – Tính di động – Tính đơn giản – Tính linh hoạt – Tiết kiệm chi phí – Khả năng mở rộng
  + Nhược điểm: – Nhiễu – Độ an toàn – Phạm vi – Tốc độ
  + Phân loại:
  + WPAN (Wireless Personal Area Network):
* Mạng không dây cá nhân: Bao gồm các công nghệ vô tuyến có vùng phủ sóng trong phạm vi vài chục mét.
* Mục đích phục vụ các thiết bị ngoại vi: máy in, bàn phím, chuột, đồng hồ, ĐTDĐ.
* Các công nghệ sử dụng: Bluetooth, Wibree, ZigBee, Wireless USB,
* Chuẩn của công nghệ: IEEE 802.15
* Sóng Bluetooth:
* Là công nghệ không dây tầm gần giữa các thiết bị điện tử.
* Hỗ trợ truyền dữ liệu ở khoảng cách ngắn giữa các thiết bị di động và cố định.
* Tốc độ tối đa: 1Mbps
* Sóng vô hướng và dải băng tần 2,4 GHz
  + WLAN (Wireless Local Area Network):
* Mạng không dây cục bộ (Wifi): Bao gồm các công nghệ vô tuyến có vùng phủ sóng trong phạm vi vài trăm mét.
* Nổi bật là công nghệ Wifi với nhiều chuẩn mở rộng khác nhau thuộc họ 802.11 a/b/g/h/i/n...
* Mục đích phục vụ các thiết bị: Laptop, thiết bị cầm tay, máy in…
* Các công nghệ sử dụng: Wifi, HiperLAN và HiperLAN2
* Chuẩn của công nghệ: IEEE 802.11
  + WMAN (Wireless Metropolitan Area Network):
* Mạng không dây đô thị (WiMax): Phạm vi phủ sóng trong vòng vài Km, thường bao phủ cả một quận, huyện, khu dân cư, hay thành phố.
* Công nghệ sử dụng: WiMax
* Tốc độ truyền dữ liệu: 128 Mbps – 300 Mbps
* Mục đích phục vụ: Cung cấp mạng không dây trong đô thị.
* Chuẩn của công nghệ: IEEE 802.16
  + WWAN (Wireless Wide Area Network):
* Mạng không dây diện rộng: Công nghệ UMTS/GSM/CDMA2000.
* Phạm vi phủ sóng là một khu vực rộng, một quốc gia, thậm chí toàn cầu.
* Mạng 2,5G. 3G
  + WRAN (Wireless Regional Area Network):
* Mạng vô tuyến khu vực: Công nghệ IEEE 802.22
* Phạm vi phủ sóng 40-100 Km.
* Tốc độ 22 Mbps
* Sử dụng các khoảng trắng trong phổ tần số TV, băng tần UHF, VHF 6/7/8Mhz
* Mục đích truyền thông tới các vùng xa xôi hẻo lánh.
* **Các mô hình WLAN thông dụng (mô hình Ad-hoc, BSS, ESS), phân biệt các mô hình này.**
  + Ad-hoc:
  + Các máy trạm liên lạc trực tiếp với nhau mà không phải thông qua AP nhƣng phải trong phạm vi cho phép.
  + Các máy trạm có vai trò ngang hàng với nhau. (Peer-to-peer)
  + Khoảng cách liên lạc trong phạm vi 100m.
  + Sử dụng thuật toán Spokesman Election Algorithm.
  + Máy trạm có trang bị card mạng không dây.

A close up of a computer

Description automatically generated

* + BSS:
  + Bao gồm các điểm truy nhập AP (Access Point) gắn với một đường mạng hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell.
  + AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng.
  + Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP.
  + Thiết bị AP có thể sẽ yêu cầu một trong những điều kiện sau, trước khi cho phép một máy trạm tham gia vào:
    - SSID phải giống nhau.
    - Một tốc độ truyền dữ liệu tương thích.
    - Hoàn tất vấn đề xác thực.

A picture containing person, skiing, air, jumping

Description automatically generated

* + ESS:
  + Mạng ESS thiết lập hai hay nhiều AP với nhau nhằm mục đích mở rộng phạm vi phủ sóng.
  + Một ESS là một phân vùng mạng logic.
  + Tên mạng của một ESS được gọi là ESSID
  + Các Cell phải chồng lên nhau 10-15% để đạt đƣợc thành công trong quá trình chuyển vùng

A picture containing person, photo, table, street

Description automatically generated

1. **Trình bày đặc điểm cơ bản về các cơ chế an toàn cơ bản như: xác thực, kiểm soát truy cập, mã hóa trong mạng WLAN.**

* **Phương thức xác thực**
* Xác thực hệ thống mở:
* Các STA không cần cung cấp chứng thực của mình cho AP trong quá trình xác thực. Vì vậy bất kỳ một STA nào cũng có thể xác thực chính nó với AP và sau đó sẽ thực hiện phiên gắn kết với AP.
* Xác thực bất cứ ai yêu cầu xác thực
* Thường được dùng ở những nơi truy cập công cộng như Internet café, nhà ga, sân bay.
* Được cài đặt mặc định trong các thiết bị WLAN.
* Xác thực khóa chung (Shared-key):
* Khóa chia sẻ sẽ được sử dụng để xác thực thông qua một giai đoạn bắt tay bốn bước như sau:
* STA gửi một yêu cầu xác thực tới AP.
* AP gửi trả một thông báo “challenge” ở dạng rõ.
* STA phải mã hóa “challenge” sử dụng khóa WEP đã được chia sẻ và gửi bản mã cho AP.
* AP sẻ giải mã và so sánh với “challenge” ban đầu, phụ thuộc vào kết quả so sánh này, AP sẽ chấp nhận xác thực STA hay không.
* Xác thực địa chỉ MAC:
* AP sẽ gửi địa chỉ MAC của Client cho RADIUS Server, Server này sẽ kiểm tra địa chỉ MAC này với danh sách địa chỉ MAC được cho phép.
* Nếu không có RADIUS Server, có thể tạo ra một danh sách địa chỉ MAC trên AP.
* Vì các địa chỉ MAC được truyền dưới dạng văn bản, do đó có thể bằng cách dò sóng, những kẻ xâm nhập có thể tạo ra địa chỉ MAC hợp lệ truy cập vào mạng.
* Xác thực mở rộng EAP:
* EAP (Extensible Authentication Protocol) được định nghĩa trong RFC 2284.
* Cung cấp xác thực hai chiều, có nghĩa là mạng (RADIUS Server) sẽ xác thực người sử dụng và người sử dụng cũng xác thực mạng (RADIUS Server).
* Sau khi quá trình xác thực hoàn tất, RADIUS Server và Client sẽ xác định khóa WEP, Client sẽ sử dụng khóa này để bắt đầu phiên kết nối (KS).
* Trong khi đó, RADIUS Server sẽ mã hóa và gửi khóa WEP đó được gọi là khóa phiên (KS) đến AP. AP sẽ sử dụng KS để mã hóa khóa quảng bá (broadcast key) và gửi đến Client. Client và AP sử dụng khóa này trong suốt một phiên làm việc.
* EAP là một cơ sở tốt cho xác thực và có thể được sử dụng cho một vài giao thức xác thực khác.
* EAP-TLS – Extensible Authentication Protocol Transport Layer Security.
* EAP-FAST – EAP Flexible Authentication via Secured Secured
* EAP-SIM – EAP Subcriber Identity Module
* Cisco LEAP – Lightweight Extensible Authentication Protocol
* EAP-PEAP– EAP Protected Extensible Authentication Protocol
* EAP-MD5 – EAP Message Digest Algorithm 5
* EAP-OTP – EAP On Time Password
* EAP-TTLS – EAP Tunneled Transport Layer Security
* **Phương thức mã hoá:**
* B1: Trước khi gửi thông điệp lên mạng, hệ thống sẽ tính giá trị ICV (Integrity message digest) và chèn vào cuối thông điệp.
* B2: Tiếp đến dùng các thuật toán mã hóa để mã hoá thông điệp (gồm thông điệp gốc và ICV).
* B3: Cuối cùng là thêm phần Header vào thông điệp và truyền đến người nhận.

Thông điệp ICV

IV Bản mã( Cipher Text)

IV Bản mã( Cipher Text)

Thông điệp ICV

Mã hóa Giải mã

Đóng gói và gửi thông điệp Nhận và giải mã thông điệp

* Một số phương thức mã hoá trong WLAN được dùng trong các giao thức: WEP, WPA, WPA2.

|  |  |  |  |
| --- | --- | --- | --- |
|  | WEP | WPA | WPA2 |
| Mã hóa | RC4 | RC4 | AES |
| Luân phiên khóa | không | Khóa phiên động | Khóa phiên động |
| Phân phối khóa | Gán bằng tay trên mỗi thiết bị | Khả năng phân phối tự động | Khả năng phân phối tự động |
| Xác thực | Sử dụng khóa WEP để xác thực | Có thể dùng 802.1x & EAP | Có thể dùng 802.1x & EAP |

* Phương thức kiểm soát truy cập
* Kiểm soát dựa vào SSID:
* SSID là thuật ngữ tên mạng, vì SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ phát hiện.
  + Trong hệ thống xác thực đóng, người dùng phải khai báo đúng giá trị SSID để có thể xác thực và kết nối với mạng.
  + Sử dụng chế độ tắt quảng bá SSID để kiểm soát giá trị SSID.
* Kiểm soát dựa vào địa chỉ MAC:
* Danh sách các địa chỉ MAC truy nhập ứng với thiết bị cho phép được thiết lập trên AP.
* Khi thiết bị có địa chỉ MAC không nằm trong danh sách kết nối vào mạng sẽ bị ngăn chặn kết nối mạng.
* Kiểm soát dựa vào giao thức:
* WLAN có thể lọc các gói tin truyền trên mạng dựa trên các  
  giao thức lớp 2 đến lớp 7.
* Các giao thức ứng với dịch vụ mạng sẽ bị cấm hoặc cho phép  
  tùy thuộc vào địa chỉ MAC hoặc địa chỉ IP được cấp phát đến  
  thiết bị người dùng

1. **Trình bày giao thức xác thực bắt tay 4-bước dùng khóa chia sẻ trước (Pre-shared key) trong WLAN, mô tả được các bước hoạt động. Phân tích tấn công vào khóa dòng RC4 lên giao thức này.**

* Mô tả các bước thực hiện: Qúa trình xác thực bắt tay 4 bước dùng khóa chia sẻ:

Step1: STA -> AP: Authentication request

Step2: AP -> STA: NAP

Step3: STA -> AP: EK(NAP) (According to RC4 stream cipher, K is the stream key)

Step4: AP -> STA: Authentication response

* + B1: STA -> AP: STA gửi yêu cầu xác thực đến Access point (AP)
  + B2: AP -> STA: Ap gửi thách thức xác thực NAP – NAP là một chuỗi 128 bít (số nonce) dưới dạng rõ
  + B3: STA -> AP: STA phản hồi lại thách thức – xác thực bằng cách sử dụng khóa K (khóa dòng – sinh ra từ khóa đã chia sẻ từ trước), mã hóa thách thức NAP bằng khóa K (K = RC4(IV,psk)) dựa trên RC4 và gửi bản mã cho AP
  + B4: AP -> STA: Sau khi AP nhận được bản mã thì sẽ sử dụng khóa K của mình để giải mã bản mã vừa nhận được thu được NAP, sau đó sẽ so sánh với NAP ở bước 2. Nếu trùng nhau thì xác thực thành công.
* Phân tích tấn công vào giao thức này để thu được khóa dòng RC4:
  + Việc sử dụng giao thức xác thực dùng khóa chia sẻ trước xảy ra vấn đề: sử dụng khóa chia sẻ trước => không có trao đổi khóa tự động, không có cách quản lý cơ sở khóa an toàn, không làm mới khóa một cách an toàn
  + Đồng thời, giao thức xác thực dùng khóa chia sẻ trước bắt buộc phải dùng WEP, khóa WEP được dùng để xác thực và mã hóa dữ liệu => Hacker lợi dụng điều này để thâm nhập mạng.
  + Hacker sẽ thực hiện thu cả hai tín hiệu (client đứng giữa lắng nghe), văn bản chưa mã hóa do AP gửi và văn bản đã mã hóa do Client gửi để giải mã khóa WEP. => Dễ dàng sniff khóa chung (stream key)
  + Sau đó, Hacker sẽ lấy bản rõ và bản mã XOR với nhau và tìm được stream key RC4.

1. **Tìm hiểu kỹ giao thức TKIP trong WPA và những cải tiến về mặt an toàn của giao thức này so với giao thức WEP.**

A screenshot of a cell phone

Description automatically generated

* + 1. Hoạt động TKIP
* TKIP dùng hàm băm IV để chống lại việc giả mạo gói tin, cung cấp phương thức kiểm tra tính toàn vẹn của thông điệp MIC để đảm bảo tính chính xác của gói tin, sử dụng khóa động bằng cách đặt cho mỗi frame một chuối số riêng để chống lại dạng tấn công giả mạo.
* Tạo khóa packet key: Băm (địa chỉ nguồn – địa chỉ MAC (48 bit) + TSC – giá trị của bộ đếm TKIP (48 bit) + base key (104 bit)). => mỗi gói tin có 1 packet ley khác nhau
* IV = TSC -> mỗi một gói tin sẽ có 1 IV khác nhau
* Sau đó lấy 2 giá trị IV và Packet ket đi qua thuật toán RC4 sinh ra Stream Cipher => khóa dòng
* Tạo ra khóa để mã hóa: lấy khóa dòng XOR với bản rõ => thu được bản mã (dòng bit khóa XOR dòng bit rõ => dòng bit mã
  + 1. Những điểm cải tiến (về tính an toàn) của TKIP so với WEP
* WEP sử dụng khóa cơ sở là giống nhau cho tất cả các gói tin trong khi TKIP sẻ dung một khóa mới (packet key) sẽ được đưa ra cho mỗi gói tin từ địa chỉ nguồn, 48 bit TKIP seq counter (TSC) và 104 bit khóa cơ sở

|  |  |
| --- | --- |
| **Điểm yếu** | **Nâng cấp** |
| Sự tương quan của các IV với các khóa yếu | Hàm trộn khóa cho môi gói tin |
| Tấn công phát lại | Đánh số thứ tự IV |
| Dễ bị giả mạo | MIC |

* + 1. Hoạt động của WEP (thêm)
* Base key – khóa mà client đã chia sẻ trước với Access point và sử dụng cho tất cả các gói tin
* IV của mỗi gói tin là khác nhau
* Để mã hóa: sử dụng giá trị IV (24 bit) và base key => kết hợp 2 giá trị này qua thuật toán RC4 => tạo ra stream cipher (mã dòng) => tạo ra khóa dòng. Sau đó thực hiện phép XOR giữa khóa dòng và bản rõ (bit rõ) => bản mã (bit khóa)

1. **Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WEP.**

* Xác thực:
* Gồm hai loại xác thực: Xác thực mở và xác thực khóa chia sẻ
* Các STA cần xác thực với AP (nhưng AP không xác thực lại với STA
* Hai bên chia sẻ chung một khóa bí mật
* Khóa này phải được thực hiện bằng tay
* Khóa này là khóa tĩnh (rất hiếm khi được thay đổi)
* Việc xác thực dựa trên giao thức thách thức-phản hồi đơn giản, gồm 4 bước:
* B1: STA => AP: Yêu cầu xác thực
* B2: AP => STA: Thách thức xác thực (r) // r là chuỗi 128 bits
* B3: STA => AP: Phản hồi xác thực (eK(r)).
* B4: AP => STA: xác thực thành công/thất bại
* K = RC4(IV + KShared), KShared là khóa chia sẻ trước giữa AP và STA.
* Toàn vẹn dữ liệu
* Sử dụng mã kiểm tra CRC-32
* Tính toàn vẹn trong WEP được bảo vệ bằng giá trị CRC (Cyclic Redundancy Check) được mã hóa
* Giá trị ICV được tính toán và được gắn vào thông điệp
* Cả thông điệp và ICV được mã hóa cùng nhau
* ICV là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị (không bắt buộc) phải thay đổi theo từng gói dũ liệu
* Vì máy gửi tạo ra ICV không theo định luật hay tiêu chuản, IV bắt buộc phải được gửi đến máy nhận ở dạng không mã hóa
* Mã hóa
* Sử dụng RC4, Khóa dài 40 bit, hoặc 104 bit
* Sử dụng IV dài 24 bit:
  + Hoạt động: Đối với mỗi thông điệp được gửi đi:
    - RC4 được khởi tạo với khóa chia sẻ (giữa STA và AP)
    - RC4 tạo ra một chuỗi byte giả ngẫu nhiên (key stream).
    - Chuỗi key stream này được XOR với thông điệp
    - RC4 được khởi tạo với khóa chia sẻ và một giá trị IV (giá trị khởi đầu).
    - Khóa chia sẻ là giống nhau đối với mỗi thông điệp.
    - 24-bit IV thay đỗi cho mỗi thông điệp
* Quản lý khóa: Sử dụng khóa chia sẻ trước, không có trao đổi khóa tự động, không có cách quản lý cơ sở khóa an toàn, không làm mới khóa một cách an toàn.
* Vấn đề chống tấn công phát lại: Không chống được

1. **Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WPA .**

* Mã hóa: Sử dụng TKIP (bắt buộc) để mã hóa:
* Thuật toán mã: RC4 => Đã vá những lỗ hổng của WEP
* IV dài hơn (48 bit) + Hàm trộn khóa (Lấy ra một khóa cho mỗi gói tin) + MIC (8 byte => Michael)
* Xác thực và quản lý khóa: 802.1x kết hợp với EAP
* Toàn vẹn: Thuật toán Michael (64 bit) => MIC
* Chống tấn công phát lại: 48bit bộ đếm chuỗi TKIP (TSC) được dùng để sinh IV và tránh tấn công phát lại. IV được đặt lại bằng 0 khi thiết lập khóa mới.

1. **Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WPA2.**

* Mã hóa:
  + Sử dụng thuật toán AES

• Chế độ CCMP (Counter mode (CRT) và CBC-MAC) (bắt buộc)

• Cần phần cứng mới hỗ trợ AES

* Giao thức TKIP (RC4 => chạy trên phần cứng cũ, Michael, đã vá các lỗ hổng của WEP) (tùy chọn)
* Xác thực: 802.1X/EAP (TKIP, EAP-TLS)
* Toàn vẹn: CCMP (Counter Mode CBC-MAC Protocol) = CRT + CBC-MAC
* Chống tấn công phát lại: Dùng số thứ tự gói tin (48 bit) – PN để ngăn chặn tấn công phát lại

1. **Phân tích độ an toàn, ưu, nhược điểm của các giao thức WEP, WPA, WPA2.**

|  |  |  |
| --- | --- | --- |
|  | WEP | WPA |
| Độ an toàn | **Giao thức mã hoá yếu**  WEP có thể được coi như một cơ chế bảo mật ở mức độ thấp nhất. vì vậy WEP không cung cấp độ bảo mật cần thiết cho đa số các ứng dụng không dây cần độ an toàn cao. WEP có thể bị bẻ khóa dễ dàng bằng các công cụ sẵn có. | Phân phối khóa hiệu quả.  Giới thiệu giao thức  TKIP (Temporal Key Integrity Protocol)  Cải tiến so với WEP:   * Xác thực mạnh với 802.1x và EAP * Tăng độ dài IV và độ dài khóa mã là 104bit * Sử dụng thuật toán toàn vẹn Michael |
| Ưu điểm | Sinh khóa trên mỗi gói tin bằng cách ghép nối IV trực tiếp với khóa chia sẻ trước | Giải quyết được vấn đề của WEP bằng cách giới thiệu khái nhiệm PTK trong kiến trúc khóa và sử dụng hàm dẫn xuất khoa thay vì ghép nối khóa trực tiếp để tạo khóa cho mỗi gói tin |
| Nhược điểm | +Ở xác thực:  • STA có thể bị giả mạo  + Ở toàn vẹn và chống tấn công phát lại:  • Không có bảo vệ chống tấn công phát lại  • Kẻ tấn công có thể thao tác trên các thông điệp mặc dù đã có cơ chế ICV và mã hóa.  + Ở tính bí mật:  • Sử dụng lại IV:  – Không gian IV quá nhỏ  – Nhiều IV được khởi tạo bằng 0 ở giai đoạn khởi đầu  • Các khóa RC4 yếu: Mã hóa WEP có thể bị phá bằng cách bắt lấy vài triệu thông điệp. | + Chia sẻ khóa trước:  WAP vẫn sử dụng chế độ chia sẻ khóa trước, dễ bị tấn công  + Toàn vẹn dữ liệu:  Sử dụng thuật toán Michael – 64 bit để xác thực yếu chỉ tốt hơn mã kiểm tra CRC32  + Mã hóa:  Sử dụng mã hóa yêu RC4 |

1. **Trình bày các tấn công phổ biến vào mạng WLAN ( Các vấn đề an toàn thông tin khi chuyển hữu tuyến -> vô tuyến)**

* Tấn công bị động : Kẻ tấn công chỉ lắng nghe trên mạng mà không làm ảnh hưởng tới bất kỳ tài nguyên nào trên mạng.

– Không tác động trực tiếp vào thiết bị nào trên mạng

– Không làm cho các thiết bị mạng biết được hoạt động của nó

* Phát hiện mạng: Phát hiện Access Point, phát hiện máy trạm kết nối, phát hiện địa chỉ MAC của các thiết bị tham gia, kênh…
* Nghe trộm: Chặn bắt lưu lượng, phân tích giao thức, nguồn và đích kết nối.
* Tấn công chủ động : Kẻ tấn công sử dụng các kỹ thuật làm ảnh hưởng tới mạng.

– Là hình thức tấn công tác động trực tiếp lên thông tin, dữ liệu của mạng.

* Dò tìm mật khẩu AP :

+ Vét cạn (WPS - Wifi Protected Setup)

+ Tấn công từ điển

* Giả mạo AP:kẻ tấn công có thể sao chép tất cả các thông tin về AP hợp pháp như địa chỉ MAC, SSID,… để giả mạo AP hợp pháp. Gửi các gói beacon với địa chỉ vật lý (MAC) giả mạo và SSID giả để tạo ra vo số AP giả mạo.
* Tấn công người đứng giữa
* Từ chối dịch vụ

+ Làm ngắt kết nối: kẻ tấn công gửi liên tục các frame hủy kết nối bằng cách giả mạo địa chỉ MAC nguồn và đích của AP đến Client. Client nhận được frame này sẽ ngắt kết nói

+ Chèn ép tín hiệu: sử dụng bộ phát tín hiệu RF (radio frequency) công suất cao làm nghẽn hoặc nhiếu tín hiệu RF của các AP hợp pháp

1. **So sánh sự khác nhau giữa 3 giao thức WEP, WPA, WPA 2**

|  |  |  |
| --- | --- | --- |
| **WEP** | **WPA** | **WPA2** |
| Là thành phần tùy chọn  trong tiêu chuẩn IEEE 802.11 | Tiêu chuẩn an ninh của wifi alliance đặt ra | Tương tự WPA |
| Khóa WEP đc cấu hình thủ công trên AP và các STA | Khuyến nghị nên sd xác thực 802.1X/EAP để nhận khóa tự động, có hỗ trợ  cài đặt thủ công như WEP | Tương tự WPA |
| Sử dụng mã hóa dòng | Tương tự WEP | Sử dụng mã hóa khối, có  hỗ trợ mã hóa dòng |
| Mã hóa trên từng gói tin dựa vào sự thay đổi giá trị IV, giá trị đc kết hợp trực  tiếp với PMK để hình thành khóa | Sd phương pháp mã hóa liên tiếp và phức tạp hơn, qt tạo khóa có thông qua khóa trung gian PTK | Tương tự WPA |
| Độ dài khóa nhỏ, 64 bít hoặc 128 bit | Độ dài khóa lớn, kết hợp nhiều thành phần thông  tin để sinh khóa | Tương tự WPA |
| Sd thuật toán CRC để ktra  tính toàn vẹn dl, độ tin cậy thấp | Sd thuật toán Michael để  tính toán ra mã MIC. Độ tin cậy cao hơn RCR | Sd CCMP/AES để tính  mã MIC, độ tin cậy cao nhất |
| K có khả năng xác thực 2 chiều | Hỗ trợ khả năng xác thực 2 chiều, sd IEEE  802.1X/EAP | Tương tự WPA |
| Phương pháp đơn giản, k yc cao về năng lực phần  cứng | Phức tạp hơn WEP nhưng cũng k yc cao về phần  cứng | Phức tạp, yc cao về năng lực xử lý của phần cứng |
| Thích hợp vs mạng quy mô nhỏ | Phù hợp mạng quy mô nhỏ và trung bình | Thiwchs hợp với mạng quy mô lớn và các doanh  nghiệp |

# **CHƯƠNG CUỐI: GIẢI ĐỀ**

## **AT13 01**

1. Cho sơ đồ xác thực bằng hàm băm và nonce như sau:
2. Alice -> Bob: “Alice”
3. Bob -> Alice: NB;
4. Alice -> Bob: H(KAB || NB);

Anh/chị hãy:

1. Trình bày điều kiện ban đầu, mục đích của giao thức

* Điều kiện ban đầu: Alice và Bob chia sẻ khóa bí mật KAB
* Mục đích của giao thức: Bob xác thực được Alice

1. Trình bày hoạt động của giao thức, bao gồm hành động của Bob sau bước thứ 3

* B1: Khởi tạo: gửi yêu cầu xác thực
* B2: (Gửi thử thách - Challenge) Khi có yêu cầu xác thực từ Alice thì Bob gửi lại 1 Chagllenge là một số nonce NB (số ngẫu nhiên) mà Bob sinh ra (số này chỉ sử dụng được 1 lần)
* B3: Alice gửi Bob một hàm băm gồm số NB và khóa KAB đã được chia sẻ từ trước
* B4: Bob lấy KAB đã chia sẻ trước đó và NB đã sinh ra ở bước 2 thực hiện băm lại H(KAB || NB) và so sánh với bản băm mà Alice đã gửi. Nếu trùng nhau thì khẳng định đó là Alice và ngược lại.

1. Giải thích quyết định cuối cùng của Bob:

Bob khẳng định Alice vì: chỉ có Alice mới có khóa KAB để sinh ra bản băm. Đồng thời, phải thỏa mãn 2 điều kiện:

* + 1 thông điệp response chỉ có thể được tạo ra bằng giá trị bí mật : giá trị H(KAB||NB) được thực hiện nhờ Alice có khóa bí mật (thỏa mãn)
  + 2 thông điệp response phải có tính tươi : Gía trị NB không lặp lại sẽ đảm bảo cho H(KAB||NB) có tính tươi, chống tấn công phát lại (thỏa mãn)
* Xét ở trường hợp lý tưởng: không có ai chặn bắt trên đường truyền

1. **Cho mô hình mạng dưới đây**

**H1(10.0.1.2/24)--------(10.0.1.1/24)G1(172.16.0.1/24)--------IPSEC(AH TUNNEL)---------(172.16.0.2/24)G2(10.0.2.1/24)------------(10.0.2.2/24)H2**

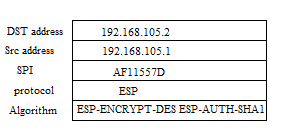
**Giả sử 2 gateway G1 và G2 người ta thiết lập giao thức IPSEC sử dụng giao thức AH ở chế độ tunnel. Hai gateway này kết nối mạng LAN 10.0.1.0/24 và 10.0.2.0/24 với nhau. Xét một gói tin UDP được gửi đi từ H1 đên H2. Hãy trình bày quá trình biến đổi gói tin qua kết nối IPSEC.**

**Yêu cầu: có vẽ hình để thể hiện cấu trúc gói tin qua các phép biến đổi; chỉ rõ giá trị của các trường:source IP, destination IP, protocol, next header (nếu có thể xác định qua dữ liệu đã cho) trong từng header.**

1. Bạn hãy trình bày khái niệm, các thành phần của tổ hợp an toàn (SA) trong bộ giao thức IPSEC và cho ví dụ về một IPSEC SA.

* **Khái niệm**
  + SA (Security Associations) là một khái niệm cơ bản của bộ giao thức IPSec. SA là một kết nối logic theo một hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSec.
  + Có hai kiểu SA
* ISAKMP SA (hay IKE A)
* IPSec SA
* **Các thành phần của SA:** Một IPSec SA bao gồm các thông tin sau:
  + Dùng giao thức an toàn nào: AH hay ESP
  + Thuật toán mã hóa/giải mã & khóa nào: DES | 3 DES
  + Phương pháp và khóa xác thực nào được dùng cho AH | ESP: Hàm băm (HMAC, MD5, SHA1), chữ ký số (RSA), chứng chỉ số, Diffie-Hellman để quản lý khóa…
  + Thông tin liên quan đến khoá như: khoảng thời gian thay đổi và khoảng thời gian làm tươi của khoá.
  + Thông tin liên quan đến chính SA, bao gồm: địa chỉ nguồn SA, khoảng thời gian làm tươi
* Một SA gồm 3 phần: <Chỉ số tham số an toàn, Địa chỉ IP đích, Giao thức an toàn>



* SPI:
* Là một trường 32 bit, dùng để xác định một SA để gắn với một gói dữ liệu
* Là một chỉ số duy nhất cho mỗi bản ghi của cơ sở dữ liệu SADB (giống khóa chính).
* Được định nghĩa bởi người tạo SA, được lựa chọn bởi hệ thống đích khi thương lượng SA.
* SPI nhận các giá trị trong khoảng từ 1…255
* Địa chỉ IP đích: Là địa chỉ IP của Node đích
* Giao thức an toàn:
* Mô tả giao thức an toàn IPSec được dùng, có thể là AH hoặc ESP
* Với hai điểm liên lạc: cần một SA cho mỗi hướng.
* SA có thể cung cấp các dịch vụ an toàn cho một phiên VPN (được bảo vệ bởi AH hay ESP).
* Nếu một phiên VPN được bảo vệ kép bởi cả AH và ESP thì mỗi hướng kết nối cần định nghĩa 2 SA.
* **Các cơ sở dữ liệu dành cho SA:** Một SA sử dụng 2 cơ sở dữ liệu
  + Cơ sở dữ liệu tổ hợp an toàn (SAD - Security Association Database)
    - Duy trì thông tin liên quan tới mỗi SA, bao gồm: các khoá, thuật toán, thời gian có hiệu lực của SA, chuỗi số tuần tự.
  + Cơ sở dữ liệu chính sách an toàn (SPD - Security Policy Database)
    - Lưu các chính sách để thiết lập các SA
    - Duy trì thông tin về các dịch vụ an toàn kèm theo với một danh sách chính sách các điểm vào và ra.
    - Định nghĩa luồng lưu lượng được xử lý/bỏ qua
* **Ví dụ về SA**: 

1. Cho sơ đồ hoạt động của giao thức WEP VÀ WPA TKIP như sau:

A screenshot of a cell phone

Description automatically generated

* + 1. Mô tả hoạt động TKIP
* TKIP dùng hàm băm IV để chống lại việc giả mạo gói tin, cung cấp phương thức kiểm tra tính toàn vẹn của thông điệp MIC để đảm bảo tính chính xác của gói tin, sử dụng khóa động bằng cách đặt cho mỗi frame một chuối số riêng để chống lại dạng tấn công giả mạo.
* Tạo khóa packet key: Băm (địa chỉ nguồn – địa chỉ MAC (48 bit) + TSC – giá trị của bộ đếm TKIP (48 bit) + base key (104 bit)). => mỗi gói tin có 1 packet ley khác nhau
* IV = TSC -> mỗi một gói tin sẽ có 1 IV khác nhau
* Sau đó lấy 2 giá trị IV và Packet ket đi qua thuật toán RC4 sinh ra Stream Cipher => khóa dòng
* Tạo ra khóa để mã hóa: lấy khóa dòng XOR với bản rõ => thu được bản mã (dòng bit khóa XOR dòng bit rõ => dòng bit mã
  + 1. Những điểm cải tiến (về tính an toàn) của TKIP so với WEP
* WEP sử dụng khóa cơ sở là giống nhau cho tất cả các gói tin trong khi TKIP sẻ dung một khóa mới (packet key) sẽ được đưa ra cho mỗi gói tin từ địa chỉ nguồn, 48 bit TKIP seq counter (TSC) và 104 bit khóa cơ sở

|  |  |
| --- | --- |
| **Điểm yếu** | **Nâng cấp** |
| Sự tương quan của các IV với các khóa yếu | Hàm trộn khóa cho môi gói tin |
| Tấn công phát lại | Đánh số thứ tự IV |
| Dễ bị giả mạo | MIC |

## **AT13 02**

1. Cho sơ đồ xác thực bằng mật mã đối xứng và nonce như sau:
   1. Alice -> Bob: “Alice”
   2. Bob -> Alice: NB;
   3. Alice -> Bob: {NB}KAB

Anh/chị hãy:

* + 1. Trình bày điều kiện ban đầu, mục đích của giao thức
* Điều kiện ban đầu: Alice và Bob chia sẻ khóa bí mật KAB. Dựa trên kênh truyền bí mật an toàn.
* Mục đích: Bob xác thực được Alice
  + 1. Trình bày hoạt động của giao thức, bao gồm hành động của Bob sau bước thứ 3
* B1: Khởi tạo: gửi yêu cầu xác thực
* B2: (Gửi thử thách - Challenge) Khi có yêu cầu xác thực từ Alice thì Bob gửi lại 1 Chagllenge là một số nonce NB (số ngẫu nhiên) mà Bob sinh ra (số này chỉ sử dụng được 1 lần)
* B3: (Response) Alice nhận đc NB => Alice giải đố cái thách thức đó bằng cách mã hóa NB bằng khóa bí mật chia sẻ trước là KAB => Sử dụng các thuật toán đối xứng: DES, AES, IDEA,…
* B4: (Decision) Khi Bob nhận được response từ Alice, Bob sẽ thực hiện: giải mã bằng KAB để thu được NB, lấy NB vừa giải mã so sánh với NB ở bước số 2. Chấp nhận nếu thấy NB trùng với NB đã gửi.
  + 1. Giải thích quyết định cuối cùng của Bob
* Bob chấp nhận đó là Alice (hay NB trùng với NB đã gửi) bởi vì cả 2 cùng chia sẻ khóa bí mật KAB, khi so sánh bằng nhau thì xác nhận đó là Alice vì chỉ có Alice mới có khóa KAB để mã hóa thông điệp.
* Xét ở trường hợp lý tưởng: không có ai chặn bắt trên đường truyền

1. **Cho mô hình mạng dưới đây:**

**H1(10.0.1.2/24)--------------IPSEC(AH+ESP)-----------(10.0.2.2/24)H2**

**Hai máy trạm H1 và H2 kết nối với nhau bằng giao thức IPSEC sử dụng kết hợp hai giao thức AH và ESP ở chế độ transport. Xét một gói tin TCP được gửi từ H1 đến H2.. Hãy trình bày quá trình biến đổi gói tin qua kết nối IPSEC.**

**Yêu cầu: có vẽ hình để thể hiện cấu trúc gói tin qua các phép biến đổi; chỉ rõ giá trị của các trường:source IP, destination IP, protocol, next header (nếu có thể xác định qua dữ liệu đã cho) trong từng header.**

1. Bạn hãy nêu định nghĩa về một mạng VPN đồng thời giải thích rõ ràng tính “riêng” và “ảo” của VPN. Có mấy mô hình VPN thông dụng (phân loại theo kiến trúc), nêu tên và mục đích của từng mô hình?

* Mạng riêng ảo (Virtual Private Network - VPN): là mạng sử dụng mạng công cộng (như Internet, ATM/Frame Relay của các nhà cung cấp dịch vụ) làm cơ sở hạ tầng để truyền thông tin nhưng vẫn đảm bảo là một mạng riêng và kiểm soát được truy nhập. Đặc điểm của mạng riêng:
  + Toàn quyền quản trị
  + Cô lập lưu lượng: lưu lượng không thể đi qua mạng chung, nếu có thì phải có sự chuyển đổi địa chỉ
  + Sử dụng dải địa chỉ IP dành riêng: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
  + VPN là một khái niệm, không phải là một giao thức. Nó có thể được hiện thực hóa bằng các giao thức khác nhau
* Trong thực tế người ta thường nói tới hai khái niệm VPN đó là: mạng riêng ảo kiểu tin cậy (Trusted VPN) và mạng riêng ảo an toàn (Secure VPN).
  + Trusted VPN: Được xem như 1 số mạch thuê của 1 ISP viễn thông, duy trì tính toàn vẹn và khả năng sử dụng cho mạng liên lạc của khác hàng. Không đảm bảo an ninh an toàn và bảo mật cho khách hàng.
  + Secure VPN: Là các mạng riêng ảo có sử dụng mật mã để bảo mật (mã hóa và xác thực) dữ liệu. Dữ liệu ở đầu ra của 1 mạng được mã hóa rồi chuyển vào mạng công cộng (ví dụ: mạng Internet) như các dữ liệu khác để truyền tới đích và sau đó được giải mã dữ liệu tại phía thu
* Ảo (Virtual): Nghĩa là cơ sở hạ tầng vật lý của mạng hoàn toàn trong suốt với kết nối VPN.
* Riêng (Private):
  + Chỉ tính riêng biệt của lưu lượng dữ liệu khi qua VPN.
  + Dữ liệu truyền luôn luôn được giữ bí mật và chỉ có thể được truy cập bởi những nguời sử dụng được trao quyền.
* Ví dụ: Mạng VLAN, mạng sử dụng đường leased line, mạng MPLS VPN, mạng IPsec VPN, SSL VPN...
* Phân loại theo cấu trúc: VPN gồm có 2 loại (Remote Access VPN và Site-to-Site VPN)
  + Remote access VPN : VPN truy cập từ xa) : cung cấp truy cập tin cậy cho các nhân viên di động, nhân viên ở xa, nhân viên làm việc tại nhà,…truy cập đến các tài nguyên mạng của đơn vị mình.
  + Site to Site VPN: gồm có 2 loại:
    - Intranet VPN (VPN cục bộ) : mở rộng các dịch vụ của mạng nội bộ tới các trụ sở ở xa, cho phép các văn phòng chi nhánh liên kết một cách bảo mật tới trụ sở chính của doanh nghiệp. Còn được gọi là mạng riêng ảo chi nhánh.
    - Extranet VPN (VPN mở rộng): mở rộng cho phép khách hàng và đối tác có thể truy cập một cách bảo mật đến Intranet của doanh nghiệp.

1. Cho biết trong giao thức WEP thiết bị AP xác thực các máy trạm như sau:
2. STA -> AP: Authentication request
3. AP -> STA: r
4. STA -> AP: iv, RC4(iv,psk)⮾r

Anh/chị hãy:

* Trình bày quá trình xác thực, bao gồm cả hành động của AP sau bước 2
* Trình bày tấn công mạo danh lên giao thức

1. Qúa trình xác thực: Việc xác thực dựa trên giao thức thách thức-phản hồi đơn giản gồm 4 bước:

B1: STA -> AP: STA gửi yêu cầu xác thực đến Access point (AP)

B2: AP -> STA: Ap gửi thách thức xác thực r – r là một chuỗi 128 bít (số nonce)

B3: STA -> AP: STA phản hồi lại thách thức – xác thực bằng cách sử dụng khóa K (khóa dòng – sinh ra từ khóa đã chia sẻ từ trước), mã hóa thách thức r bằng khóa K (K = RC4(IV,psk)) và giá trị IV

B4: AP -> STA: Sau khi AP nhận được bản mã thì sẽ sử dụng khóa K của mình để giải mã bản mã vừa nhận được thu được r, sau đó sẽ so sánh với r ở bước 2. Nếu trùng nhau thì xác thực thành công.

* Sau khi xác thực STA thành công, trạng thái gắn kết sẽ được thiết lập và hai bên sử dụng lại khóa dùng để xác thực cho việc mã hóa dữ liệu.

1. Tấn công mạo danh lên giao thức:

* Tấn công mạo danh địa chỉ MAC:
  + Các AP hiện nay đều có chức năng hạn chế truy cập bằng việc lọc địa chỉ MAC của người dùng. Kẻ tấn công có thể giả mạo địa chỉ MAC của một máy tính trong hệ thống để thâm nhập vào AP và điều khiển các chính sách an ninh an toàn của AP theo hướng có lợi cho kẻ tấn công.
  + Để chống tấn công này, trên AP phải có chính sách truy cập an toàn bằng việc thiết lập mật khẩu mạnh kết hợp với dùng giao thức điều khiển truy nhập có bảo mật như https hoặc ssh. Không dùng telnet
* Tấn công mạo danh AP
  + Đối với mạng không dây, việc truy cập đến đường truyền của người sử dụng là rất đơn giản. Kẻ tấn công có thể sao chép tất cả các thông tin về AP hợp pháp như SSID, MAC,… để giả mạo AP hợp pháp. Bước tiếp theo là kẻ tấn công đợi người dùng kết nối đến hoặc tấn công DoS lên AP hợp pháp để bắt buộc người dùng kết nối lại với AP giả mạo. Mọi dữ liệu khi đó đều đi qua AP giả mạo của kẻ tấn công
  + Đây là dạng tấn công Man-in-the-middle, tấn công này sẽ không thể thực hiện được nếu như có sự xuất hiện xác thực 2 chiều.

## **AT13 03**

1. Cho sơ đồ xác thực bằng mật mã khóa công khai và nonce như sau:
2. Alice -> Bob: “Alice”
3. Bob -> Alice: {NB}KPA;
4. Alice -> Bob: NB

Anh/chị hãy:

* Trình bày điều kiện ban đầu, mục đích của giao thức
  + Điều kiện ban đầu: Alice có cặp khóa bí mật, công khai
  + Mục đích: Bob xác thực được Alice
* Trình bày hoạt động của giao thức, bao gồm hành động của Bob sau bước thứ 3
  + B1: Khởi tạo: gửi yêu cầu xác thực
  + B2: Bob gửi cho Alice: mã hóa NB bằng khóa công khai của Alice
  + B3: Alice nhận được bản mã, Alice sử dụng khóa bí mật của mình để giải mã bản mã và thu được NB. Sau đó gửi cho NB cho Bob
  + B4: Bob sau khi nhận được NB từ Alice sẽ so sánh với NB đã sinh ra ở bước 2 mà Bob đã gửi cho Alice. Nếu trùng nhau thì chính là Alice và ngược lại
* Giải thích quyết định cuối cùng của Bob
  + Khi Bob mã hóa NB bằng khóa công khai của Alice, một người C xen vào k thể giải mã được vì k có khóa bí mật của Alice. Chỉ có duy nhất Alice có khóa riêng của mình mới có thể thực hiện giải mã thông điệp mà Bob gửi để thu được NB => Xác nhận đó là Alice.
  + Xét ở trường hợp lý tưởng: không có ai chặn bắt trên đường truyền

1. **Cho mô hình mạng dưới đây**

**H1(10.0.1.2/24)--------(10.0.1.1/24)G1(172.16.0.1/24)--------IPSEC(ESP TUNNEL)---------(172.16.0.2/24)G2(10.0.2.1/24)------------(10.0.2.2/24)H2**

**Giả sử 2 gateway G1 và G2 người ta thiết lập giao thức IPSEC sử dụng giao thức ESP ở chế độ tunnel. Hai gateway này kết nối mạng LAN 10.0.1.0/24 và 10.0.2.0/24 với nhau. Xét một gói tin TCP được gửi đi từ H1 đên H2. Hãy trình bày quá trình biến đổi gói tin qua kết nối IPSEC.**

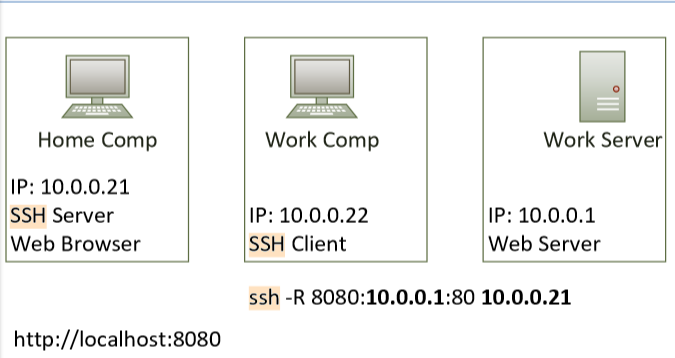
**Yêu cầu: có vẽ hình để thể hiện cấu trúc gói tin qua các phép biến đổi; chỉ rõ giá trị của các trường:source IP, destination IP, protocol, next header (nếu có thể xác định qua dữ liệu đã cho) trong từng header.**

1. **Trên quan điểm của người sử dụng dịch vụ**, bạn hãy trình bày các hiểm họa an toàn thông tin đối với dịch vụ Web và email, từ đó trình bày các giải pháp an toàn (ở tầng ứng dụng và tầng giao vận) để chống lại các hiểm họa đó.

* Các hiểm họa an toàn thông tin đối với dịch vụ Web:
  + Người dùng không thể xác thực được server: người dùng cứ mặc định gửi request đến server chứ không có bất kỳ phương pháp nào để xác thực đó chính là server.
  + Dữ liệu được truyền dưới dạng rõ => dễ bị tấn công (như tấn công chặn bắt thông tin, thay đổi thông tin)
  + Dễ bị tấn công Social Engineering để lộ thông tin tài khoản, mật khẩu,…=> Người dùng có thể bị kiểm soát máy tính, đánh cắp dữ liệu,…
* Các hiểm họa an toàn thông tin đối với dịch vụ Email:
  + Thư có thể bị đọc/sửa trên đường truyền
  + Thư có thể bị đọc/sửa trên máy chủ
* Không thể yên tâm khi gửi thư. Nếu như chỉ sử dụng SMTP và MINE thì người khác vẫn có thể đọc được thư. => Dễ bị tấn công chặn bắt thư và xem nội dun cũng như sửa đổi các nội dung và định danh người gửi.
  + Người dùng dễ nhận được các email giả mạo chứa mã độc, hay các phần mềm độc hại khác.
* Các giải pháp an toàn ở tầng ứng dụng:
  + Đối với dịch vụ Email:
    - Hai giao thức chủ yếu là S/MINE và PGP
    - Nguyên tắc thực hiện: mã hóa, ký số, kết hợp ký và mã
* Các giải pháp an toàn ở tầng giao vận:
  + Đối với dịch vụ Web:
    - Sử dụng giao thức an toàn lớp dưới: SSL/TLS, HTTP + TLS = HTTPS
    - Để sử dụng TLS:
      * Kích hoạt TLS trước khi bắt đầu HTTP
      * Gọi TLS như là một dịch vụ tùy chọn của HTTP:
        + Trong chuẩn RFC 7838: HTTP Alternative services
        + RFC 8164: Opportunistic Security for HTTP/2
    - HTTPS được thiết kế để chống lại tấn công ở giữa và tấn công nghe trộm. Mọi thông tin trong thông báo HTTPS đều được mã hóa và xác thực bao gồm cả phần header và nội dung.

1. Chính sách an toàn thông tin của công ty KMACOMP quy định không cho phép truy cập vào Web Server từ mạng bên ngoài. Bạn hãy trình bày cách thức mà một nhân viên của KMAComp sử dụng dịch vụ Remote Port Forwarding của SSH để thiết lập một kết nối an toàn từ Home Comp tới Web server thông qua Work Comp của mình. Địa chỉ IP của các máy cho trên hình dưới đây:

Home Comp (10.0.0.21) (ssh server) -----------[--Work comp(10.0.0.22) – ssh client----------Webserver(10.0.0.1) – application server]



Cách thức một nhân viên của KMAComp sử dụng dịch vụ Remote Port Forwading của SSH để thiết lập kết nối an toàn:

* Gỉa sử webserver có tên miền: <http://localhost:8080>
* Mục đích: thiết lập kết nối an toàn từ Home Comp đến Webserver thông qua Work comp của nhân viên
* Sử dụng SSH, Home Comp đang muốn kết nối an toàn từ cổng 8080 của mình đến cổng 80 của Webserver => sử dụng Remote Port Forwarding vì Webserver và Home Comp đang ở xa nhau => sử dụng thành phần trung gian Work comp
* Bên phía Work comp sẽ thực hiện: ssh -R 8080:10.0.01:80 10.0.0.21, trong đó:
  + 8080 là R port, là cổng từ xa của Home Comp
  + 10.0.0.1 là localhost : localhost chính là địa chỉ ip của Webserver mà Home Comp muốn truy cập đến
  + 80 là port của Webserver
  + 10.0.0.21: là địa chỉ IP của Home Comp
* Để Home Comp muốn truy cập tạo 1 đường hầm trực tiếp từ port 8080 đến port 80 của Webserver thì cần phải sử dụng Work comp bằng cách Work comp sẽ thực hiện câu lệnh trên => Mở một cổng trực tiếp một socket an toàn trực tiếp từ port 8080 đến port 80

## **AT13 04**

1. Cho sơ đồ xác thực bằng chữ ký số và nonce như sau:
   1. Alice -> Bob: “Alice”
   2. Bob -> Alice: NB;
   3. Alice -> Bob: sigA(NB)
   4. Bob: sử dụng KPA để kiểm tra chữ ký; chấp nhận nếu chữ ký hợp lệ

Anh/chị hãy:

* + 1. Trình bày điều kiện ban đầu, mục đích của giao thức
* Điều kiện ban đầu: Alice có cặp khóa bí mật, khóa công khai
* Mục đích: Bob xác thực được Alice
  + 1. Trình bày hoạt động của giao thức, bao gồm hành động của Bob sau bước thứ 4
* B1: Khởi tạo: gửi yêu cầu xác thực
* B2: Gửi thử thách - Challenge) Khi có yêu cầu xác thực từ Alice thì Bob gửi lại 1 Chagllenge là một số nonce NB (số ngẫu nhiên) mà Bob sinh ra (số này chỉ sử dụng được 1 lần)
* B3: Alice ký lên NB bằng cách sử dụng khóa bí mật của Alice để mã hóa NB
* B4: Bob sau khi nhận được bản mã thì thực hiện giải mã chữ ký (sử dụng khóa công khai của Alice) => thu được NB. So sánh với NB mà Bob đã gửi cho Alice ở bước số 2. Nếu trùng nhau thì khẳng định đó là Alice và ngược lại
  + 1. Giải thích quyết định cuối cùng của Bob
* Vì chỉ có Alice mới có khóa bí mật của Alice để tạo được chữ ký cho NB. Người khác cũng tạo được chữ ký với NB tuy nhiên khi Bob sử dụng KPA để giải mã chữ ký thì không thu được NB nữa vì Bob sử dụng khóa công khai của Alice.
* Xét ở trường hợp lý tưởng: không có ai chặn bắt trên đường truyền

1. **Cho mô hình mạng dưới đây:**

**H1(10.0.0.1/24)--------------IPSEC(AH+ESP)-----------(10.0.0.2/24)H2**

**Hai máy trạm H1 và H2 kết nối với nhau bằng giao thức IPSEC sử dụng kết hợp hai giao thức AH và ESP ở chế độ transport. Xét một gói tin TCP được gửi từ H1 đến H2.. Hãy trình bày quá trình biến đổi gói tin qua kết nối IPSEC.**

**Yêu cầu: có vẽ hình để thể hiện cấu trúc gói tin qua các phép biến đổi; chỉ rõ giá trị của các trường:source IP, destination IP, protocol, next header (nếu có thể xác định qua dữ liệu đã cho) trong từng header.**

1. Anh/chị hãy trình bày những vấn đề an toàn thông tin phát sinh trong mạng máy tính khi thay kết nối hữu tuyến bằng kết nối vô tuyến.

* Mạng không dây là phương thức truyền dữ liệu từ điểm này điểm khác không sử dụng đường dây vật lý mà sử dụng sóng vô tuyến, sóng hồng ngoại và vệ tinh. Mạng không dây sử dụng sóng raido hay sóng cực ngắn để duy trì các kênh truyền thông giữa các thiết bị với nhau.
* Đối với mạng WLAN, trong quá trình truyền thông có thể gặp các tấn công như:
  + Tấn công nghe trộm thông tin: thu thập các thông tin nhạy cảm như username, password, e-mail,… khi mạng WLAN không sử dụng các phương pháp mã hóa. Đây là dạng tấn công Man-in-the-middle.
  + Tấn công giả mạo địa chỉ MAC: các hacker giả mạo địa chỉ MAC của người dùng để thâm nhập vào AP và điều khiển các chính sách an ninh an toàn của AP theo hướng có lợi cho kẻ tấn công.
  + Tấn công giả mạo AP: giả mạo AP để đánh lừa người dùng xác thực với AP giả mạo sau đó thu thập thông tin của người dùng. Đây là một dạng tấn công Man-in-the middle
  + Tấn công hủy xác thực: hacker chèn các frame yêu cầu xác thực lại vào mạng bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng. Thông thường người dùng sẽ kết nối lại để phục hồi dịch vụ, nhưng kẻ tấn công vẫn tiếp tục gửi các gói yêu cầu xác thực lại cho người dùng và làm cho người dùng không thể xác thực được.
  + Tấn công làm ngắt kết nối: hacker gửi hủy gắn kết bằng cách giả mạo địa chỉ MAC nguồn và đích đến AP và các client tương ứng. Client sẽ nhận được frame này và nghĩ rằng frame hủy kết nối gửi từ AP hợp pháp đến. Đồng thời hacker cũng gửi frame đến AP. Khi các client bị ngắt kết nối sẽ thực hiện kết nối lại với AP ngay lập tức nưng kẻ tấn công tiếp tục gửi các frame hủy kết nối đến AP và client làm cho các client mất kết nối.
  + Tấn công chẻn ép tín hiệu: các hacker sử dụng AP phát hiện tín hiệu mạnh làm cho người dùng không thể truy nhập được tới các AP hợp pháp hoặc làm nhiễu tín hiệu của các AP hợp pháp

1. Anh/chị hãy trình bày các bước mà một người dùng cần thực hiện để truy cập tới máy chủ dịch vụ nếu cơ chế xác thực là Kerberos, hãy giải thích tạo sao nói Kerberos là một giao thức Single Sign-On. Lưu ý: chỉ cần trình bày về nguyên tắc, không cần công thức cụ thể)
2. Cơ chế hoạt động

B1: Người sử dụng nhập tên và mật khẩu tại máy tính của mình (máy khách). Phần mềm máy khách thực hiện hàm băm một chiều trên mật khẩu nhận được. Kết quả sẽ được dùng làm khóa bí mật của người sử dụng.

B2: Phần mềm máy khách gửi một gói tin (không mật mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung của gói tin đại ý: "người dùng XYZ muốn sử dụng dịch vụ". Cần chú ý là cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS.

B3: AS kiểm tra nhân dạnh của người yêu cầu có nằm trong cơ sở dữ liệu của mình không. Nếu có thì AS gửi 2 gói tin sau tới người sử dụng:

* Gói tin A: "Khóa phiên TGS/máy khách" được mật mã hóa với khóa bí mật của người sử dụng.
* Gói tin B: "Vé chấp thuận" (bao gồm chỉ danh người sử dụng (ID), địa chỉ mạng của người sử dụng, thời hạn của vé và "Khóa phiên TGS/máy khách") được mật mã hóa với khóa bí mật của TGS.

B4: Khi nhận được 2 gói tin trên, phần mềm máy khách giải mã gói tin A để có khóa phiên với TGS. (Người sử dụng không thể giải mã được gói tin B vì nó được mã hóa với khóa bí mật của TGS). Tại thời điểm này, người dùng có thể nhận thực mình với TGS.

B5: Khi yêu cầu dịch vụ, người sử dụng gửi 2 gói tin sau tới TGS:

* Gói tin C: Bao gồm "Vé chấp thuận" từ gói tin B và chỉ danh (ID) của yêu cầu dịch vụ.
* Gói tin D: Phần nhận thực (bao gồm chỉ danh người sử dụng và thời điểm yêu cầu), mật mã hóa với "Khóa phiên TGS/máy khách".

B6: Khi nhận được 2 gói tin C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người sử dụng:

* Gói tin E: "Vé" (bao gồm chỉ danh người sử dụng, địa chỉ mạng người sử dụng, thời hạn sử dụng và "Khóa phiên máy chủ/máy khách") mật mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.
* Gói tin F: "Khóa phiên máy chủ/máy khách" mật mã hóa với "Khóa phiên TGS/máy khách".
* Gói tin E thu được từ bước trước (trong đó có "Khóa phiên máy chủ/máy khách" mật mã hóa với khóa bí mật của SS).
* Gói tin G: phần nhận thực mới, bao gồm chỉ danh người sử dụng, thời điểm yêu cầu và được mật mã hóa với "Khóa phiên máy chủ/máy khách".

B7: Khi nhận được 2 gói tin E và F, người sử dụng đã có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:

B8: SS giải mã "Vé" bằng khóa bí mật của mình và gửi gói tin sau tới người sử dụng để xác nhận định danh của mình và khẳng định sự đồng ý cung cấp dịch vụ:

* Gói tin H: Thời điểm trong gói tin yêu cầu dịch vụ cộng thêm 1, mật mã hóa với "Khóa phiên máy chủ/máy khách".

B9: Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người sử dụng có thể tin tưởng vào máy chủ SS và bắt đầu gửi yêu cầu sử dụng dịch vụ.

B10: Máy chủ cung cấp dịch vụ cho người sử dụng.

1. Kerberos là một giao thức Single Sign-On vì: Chỉ cần người dùng xác thực 1 lần là người dùng có thể sử dụng mọi dịch vụ trong máy chủ dịch vụ mà không cần phải xác thực nhiều lần.

## **AT12 01**

1. Bạn hãy trình bày khái niệm giao thức xác thực và giải thích các thuật ngữ: Authenticator, Supplicant, Network access server, authentication server. Vẽ hình và mô tả các bước hoạt động của giao thức xác thực CHAP.

* Giao thức xác thực:
  + Xác thực là hành vi xác nhận sự thật một thuộc tính của một dữ kiện hoặc tổ tức. Liên quan đến xác nhận danh tính của một người hoặc một chương trình phần mềm, dữ liệu máy tính, truy tìm nguồn gốc của một vật và đảm bảo các sản phẩm đã được công bố công khai là của mình. Xác thực bao gồm việc xác minh tính hợp lệ của ít nhất một dạng định danh.
  + Một giao thức xác thực là một kiểu của giao thức mật mã với mục đích xác thực các thực thể có nhu cầu truyền thông an toàn. Có rất nhiều kiểu giao thức xác thực khác nhau như:
    - AKA
    - CHAP
    - RADIUS
    - PAP
    - LAN Manager
    - EAP
    - HIP
    - KEBEROS
    - NTLM
    - …
* Giải thích các thuật ngữ:
  + Authenticator: bên xác thực (là bên trung gian đứng giữa Supplicant với AS) đóng vai trò trung chuyển thông báo từ Supplicant đến AS. Là điểm cuối của liên kết yêu cầu xác thực. Authenticator cũng được coi như là Network Access Server hoặc RADIUS Client.
  + Supplicant (hoặc Peer): bên xác thực. Thực chất là client. Là một thực thể được xác thực bởi Authenticator. Supplicant có thể được kết nối với Authenticator tại một điểm cuối của một phân đoạn LAN kiểu điểm-điểm hoặc của một liên kết không dây 802.11
  + Network access server: máy chủ cung cấp dịch vụ truy cập vào mạng cho Supplicant. NAS cũng được xem là Authenticator hoặc RADIUS Client
  + Authentication server: Máy chủ xác thực đóng vai trò giúp Authenticator xác thực Supplicant. Tức là cung cấp dịch vụ xác thực cho Authenticator.
* Giao thức xác thực CHAP
  + CHAP là giao thức bắt tay 3 bước, xác thực sử dụng mật khẩu và không truyền mật khẩu dạng rõ (nhưng vẫn lưu mật khẩu trong csdl ở dạng rõ)
  + Mô hình:

A screenshot of a cell phone

Description automatically generated

* Mô tả các bước:
  + Bước 1: Client gửi yêu cầu xác thực (Đăng nhập) đên server (giai đoạn khởi tạo kết nối) => Gửi username
  + Bước 2: Server sau khi nhận được gửi một thông điệp “thách thức” đến client. (Thách thức chính là số nonce)
  + Bước 3: Client nhập mật khẩu
  + Bước 4: Client đáp ứng lại với một giá trị tính toán bằng cách sử dụng hàm băm trên thách thức kết hợp với password vừa nhập (Password chính là khóa bí mật được chia sẻ từ trước giữa client và server).
  + Bước 5: Server sẽ tính toán lại giá trị băm (lấy mật khẩu trong csdl của mình + nonce gửi đi ở bước 2) so với giá trị băm nhận được từ client
  + Bước 6: Nếu phù hợp sẽ chấp nhận việc chứng thực, còn không thì sẽ hủy kết nối.

? Lưu mật khẩu trong csdl dưới dạng rõ mà kf dạng băm: trong tính chất của hàm băm, vì hàm băm chỉ là hàm 1 chiều => nếu lưu mật khẩu dưới dạng băm thì k thể giải mã hàm băm để lấy mật khẩu rồi lại băm lại với challenge. => Bắt buộc lưu mật khẩu ở dạng rõ.

1. Bạn hãy trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WPA. Nêu những cải tiến của WPA so với WEP, đồng thời nêu những hạn chế của WPA.
2. WPA

* Mã hóa:
  + Sử dụng TKIP (bắt buộc) để mã hóa:
    - Thuật toán mã: RC4 => Đã vá những lỗ hổng của WEP
    - IV dài hơn (48 bit) + Hàm trộn khóa (Lấy ra một khóa cho mỗi gói tin) + MIC (8 byte => Michael)
* Xác thực và quản lý khóa:
  + 802.1x kết hợp với EAP
* Toàn vẹn:
  + Thuật toán Michael (64 bit) => MIC
* Chống tấn công phát lại:
  + 48bit bộ đếm chuỗi TKIP (TSC) được dùng để sinh IV và tránh tấn công phát lại. IV được đặt lại bằng 0 khi thiết lập khóa mới.

1. Những cải tiến của WPA so với WEP

* WPA: Sử dụng 802.1x và EAP cho xác thực và thỏa thuận khóa tự động. Nhưng vẫn hỗ trợ manual key sharing giống như WEP.
* Giải quyết vấn đề của WEP bằng cách giới thiệu khái niệm PTK trong kiến trúc khóa và sử dụng hàm dẫn xuất khóa thay vì ghép nối trực tiếp để tạo ra khóa mã cho mỗi gói tin
* Tăng kích cỡ IV lên 48 bít, sử dụng PTK để làm tươi khóa cho mỗi phiên liên lạc, làm tăng không gian khóa. IV đưuọc đặt về 0 mỗi khi thiết lập một PTK mới. Trong khi WEP hạn chế về không gian khóa ( khóa tĩnh, IV ngắn, phương pháp sinh và sử dụng khóa trực tiếp), việc thay đổi IV là tùy chọn.
* Sử dụng thuật toán toàn vẹn dữ liệu Michael, xác thực địa chỉ nguồn và đích thay vì CRC32 của WEP không xác thực header.
* Sử dụng IV như là 1 số thứ tự để chống tấn công replay, còn WEP không có giải pháp cho chống tấn công replay.

1. Hạn chế của WPA

* Chia sẻ khóa trước: WAP vẫn sử dụng chế độ chia sẻ khóa trước, dễ bị tấn công
* Toàn vẹn dữ liệu: Sử dụng thuật toán Michael – 64 bit để xác thực yếu chỉ tốt hơn mã kiểm tra CRC32
* Mã hóa: Sử dụng mã hóa yếu RC4

## **AT12 02**

1. Bạn hãy trình bày lịch sử phát triển, các dịch vụ an toàn mà SSL đem lại. Hãy cho biết giao thức SSL có mấy giao thức con, nêu tên và trình bày vai trò của từng giao thức này.

* Lịch sử phát triển SSL:
  + SSL 1.0: Do Netscape thiết kế đầu năm 1994. Hiện không còn sử dụng.
  + SSL 2.0: Do Netscape công bố vào 11/1994. Không khuyến khích sử dụng trong môi trường thực tế. Version này chưa có sự trợ giúp chuỗi chứng chỉ.
  + SSL 3.0: Được thiết kế bởi Netscape và Paul Kocher vào 11/1996. Đã có sự trợ giúp cho chuỗi chứng chỉ và đã được sử dụng cho hầu hết các trình duyệt phổ thông.
  + TLS 1.0 (SSL 3.1) Transport Layer Security. Là chuẩn Internet dựa trên SSL 3.0 vào 1/999 được quy định trong RFC 2246.Tuy nhiên, giao thức này không được hỗ trợ đối với nhiều trình duyệt thông dụng (ví dụ Netscape). Hiện nay đã có các phiên bản mới của TLS đó là TLS v1.1, TLS v1.3 và TLS v1.3 (2016)
  + SSL/TLS đem lại các yếu tố sau cho truyền thông trên Internet: Bí mật (sử dụng mật mã). Toàn vẹn (Sử dụng MAC). Xác thực (Sử dụng chứng chỉ số X.509). SSL/TLS ngày nay được sử dụng ở các web server và các trình duyệt internet.
* Các dịch vụ an toàn của SSL:
  + Xác thực thực thể (1 chiều hoặc 2 chiều):
    - Xác thực client: Cho phép phía server xác thực được người sử dụng muốn kết nối.
    - Xác thực server: Cho phép người sử dụng xác thực được server muốn kết nối..
  + Thỏa thuận bộ tham số mật mã: Cả hai bên Server và Client thỏa thuận các kỹ thuật mật mã.
  + Trao đổi khóa phiên
  + Nén dữ liệu
  + Bí mật dữ liệu: Tất cả các thông tin trao đổi giữa client và server được mã hóa trên đường truyền nhằm nâng cao khả năng bảo mật.
  + Xác thực (và toàn vẹn) dữ liệu
* SSL có 4 giao thức con: giao thức Record, giao thức Handshake, giao thức Alert, giao thức Change cipher spec.
  + Giao thức Record: phân mảnh, nén, tính MAC và mã hóa dữ liệu
  + Giao thức Handshake: thực hiện chức năng thỏa thuận các thuật toán, tham số, trao đổi khóa, xác thực server và client (nếu có lựa chọn)
  + Giao thức Alert: thông báo lỗi
  + Giao thức Change cipher sec: thông báo xác nhận kết thúc giai đoạn Handshake protocol.

1. Cho giao thức xác thực bắt tay 4 bước dùng khóa chia sẻ trước trong WLAN được thực hiện như sau:

Step1: STA -> AP: Authentication request

Step2: AP -> STA: NAP

Step3: STA -> AP: EK(NAP) (According to RC4 stream cipher, K is the stream key)

Step4: AP -> STA: Authentication response

Bạn hãy mô tả các bước thực hiện trên và phân tích khả năng tấn công vào giao thức này để có thể thu được khóa dòng RC4:

* Mô tả các bước thực hiện:
  + B1: STA -> AP: STA gửi yêu cầu xác thực đến Access point (AP)
  + B2: AP -> STA: Ap gửi thách thức xác thực NAP – NAP là một chuỗi 128 bít (số nonce) dưới dạng rõ
  + B3: STA -> AP: STA phản hồi lại thách thức – xác thực bằng cách sử dụng khóa K (khóa dòng – sinh ra từ khóa đã chia sẻ từ trước), mã hóa thách thức NAP bằng khóa K (K = RC4(IV,psk)) dựa trên RC4 và gửi bản mã cho AP
  + B4: AP -> STA: Sau khi AP nhận được bản mã thì sẽ sử dụng khóa K của mình để giải mã bản mã vừa nhận được thu được NAP, sau đó sẽ so sánh với NAP ở bước 2. Nếu trùng nhau thì xác thực thành công.
* Phân tích tấn công vào giao thức này để thu được khóa dòng RC4:
  + Việc sử dụng giao thức xác thực dùng khóa chia sẻ trước xảy ra vấn đề: sử dụng khóa chia sẻ trước => không có trao đổi khóa tự động, không có cách quản lý cơ sở khóa an toàn, không làm mới khóa một cách an toàn
  + Đồng thời, giao thức xác thực dùng khóa chia sẻ trước bắt buộc phải dùng WEP, khóa WEP được dùng để xác thực và mã hóa dữ liệu => Hacker lợi dụng điều này để thâm nhập mạng.
  + Hacker sẽ thực hiện thu cả hai tín hiệu (client đứng giữa lắng nghe), văn bản chưa mã hóa do AP gửi và văn bản đã mã hóa do Client gửi để giải mã khóa WEP. => Dễ dàng sniff khóa chung (stream key)
  + Sau đó, Hacker sẽ lấy bản rõ và bản mã XOR với nhau và tìm được stream key RC4.

## **AT12 03**

1. Trình bày các đặc điểm cơ bản của các mô hình WLAN thông dụng (mô hình Ad-hoc, BSS, ESS) và vẽ hình minh họa.

* Ad-hoc:
  + Các máy trạm liên lạc trực tiếp với nhau mà không phải thông qua AP nhƣng phải trong phạm vi cho phép.
  + Các máy trạm có vai trò ngang hàng với nhau. (Peer-to-peer)
  + Khoảng cách liên lạc trong phạm vi 100m.
  + Sử dụng thuật toán Spokesman Election Algorithm.
  + Máy trạm có trang bị card mạng không dây.

A close up of a computer

Description automatically generated

* BSS:
  + Bao gồm các điểm truy nhập AP (Access Point) gắn với một đường mạng hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell.
  + AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng.
  + Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP.

A picture containing person, skiing, air, jumping

Description automatically generated

* ESS:
  + Mạng ESS thiết lập hai hay nhiều AP với nhau nhằm mục đích mở rộng phạm vi phủ sóng.
  + Một ESS là một phân vùng mạng logic.
  + Tên mạng của một ESS được gọi là ESSID
  + Các Cell phải chồng lên nhau 10-15% để đạt đƣợc thành công trong quá trình chuyển vùng

A picture containing person, photo, table, street

Description automatically generated

1. Bạn hãy trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WEP. Nêu ưu, nhược điểm của giao thức WEP.

* **Xác thực:**
* Gồm hai loại xác thực: Xác thực mở và xác thực khóa chia sẻ
* Các STA cần xác thực với AP (nhưng AP không xác thực lại với STA
* Hai bên chia sẻ chung một khóa bí mật
* Khóa này phải được thực hiện bằng tay
* Khóa này là khóa tĩnh (rất hiếm khi được thay đổi)
* Việc xác thực dựa trên giao thức thách thức-phản hồi đơn giản, gồm 4 bước:
* B1: STA => AP: Yêu cầu xác thực
* B2: AP => STA: Thách thức xác thực (r) // r là chuỗi 128 bits
* B3: STA => AP: Phản hồi xác thực (eK(r)).
* B4: AP => STA: xác thực thành công/thất bại
* K = RC4(IV + KShared), KShared là khóa chia sẻ trước giữa AP và STA.
* **Toàn vẹn dữ liệu**
* Sử dụng mã kiểm tra CRC-32
* Tính toàn vẹn trong WEP được bảo vệ bằng giá trị CRC (Cyclic Redundancy Check) được mã hóa
* Giá trị ICV được tính toán và được gắn vào thông điệp
* Cả thông điệp và ICV được mã hóa cùng nhau
* ICV là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị (không bắt buộc) phải thay đổi theo từng gói dũ liệu
* Vì máy gửi tạo ra ICV không theo định luật hay tiêu chuản, IV bắt buộc phải được gửi đến máy nhận ở dạng không mã hóa
* **Mã hóa**
* Sử dụng RC4, Khóa dài 40 bit, hoặc 104 bit
* Sử dụng IV dài 24 bit

Hoạt động: Đối với mỗi thông điệp được gửi đi:

* + - RC4 được khởi tạo với khóa chia sẻ (giữa STA và AP)
    - RC4 tạo ra một chuỗi byte giả ngẫu nhiên (key stream).
    - Chuỗi key stream này được XOR với thông điệp

– RC4 được khởi tạo với khóa chia sẻ và một giá trị IV (giá trị khởi đầu).

* + - Khóa chia sẻ là giống nhau đối với mỗi thông điệp.
    - 24-bit IV thay đỗi cho mỗi thông điệp
* **Quản lý khóa:** Sử dụng khóa chia sẻ trước, không có trao đổi khóa tự động, không có cách quản lý cơ sở khóa an toàn, không làm mới khóa một cách an toàn.
* **Vấn đề chống tấn công phát lại:** Không chống được
* **Ưu, nhược điểm:**
  + **Ưu điểm****:** Sinh khóa trên mỗi gói tin bằng cách ghép nối IV trực tiếp với khóa chia sẻ trước
  + **Nhược điểm**
  + **Về vấn đề xác thực**: Xác thực chỉ là một chiều, AP không được xác thực bởi STA, STA có thể gắn kết với một AP giả mạo: cùng 1 khóa chia sẻ giống nhau được dung cho cả mã hóa và xác thực
* Điểm yếu này có thể được dung để bẻ khóa
  + Không có khóa phiên nào được thiết lập trong suốt quá trình xác thực
    - Kiểm soát truy cập không được tiếp tục
    - Khi một STA đã được xác thực và gắn kết với AP thì attacker có thể gửi thông điệp sử dụng địa chỉ MAC của STA đó
    - Việc phát lại các thông điệp của STA vẫn có thể xảy ra.
  + **Về vấn để toàn vẹn dữ liệu:** Sử dụng mã kiểm tra CRC-32
  + **Về vấn đề mã hóa:** Sử dụng mã hóa yếu RC4, độ dài khóa 40bit hoặc 104 bít. Sử dụng IV có độ dài 24 bít( cỡ 17tr giá trị có thể của IV, nếu một STA có thể tr trung bình 500 frame(có độ dài tối đa trong một giây thì số lượng IV này sẽ sư dụng được trong khoảng 7h, IV sẽ bị lặp lại sau mỗi 7h).
* **Vấn đề về khóa:** Sử dụng khóa chia sẻ trước, không có trao đổi khó tự động, không có cách quản lý cơ sở khóa an toàn, không làm mới khóa một cách an toàn.
* **Vấn đề chống tấn công phát lại:**  WEP không được thiết kế để chống tấn công phát lại

## **AT11 01**

1. Hãy trình bày kỹ thuật tấn công thăm dò và kỹ thuật tấn công từ chối dịch vụ? Cho ví dụ và cách phòng chống?

* Kỹ thuật tấn công thăm dò: là hình thức tấn công nhằm thu thập các thông tin về hệ thống định tấn công (nạn nhân), các dịch vụ đang chạy, các lỗ hổng,… Từ đó tìm ra các điểm yếu.
  + Qúa trình: đầu tiên hacker sử dụng ping sweap để tìm ra các địa chỉ IP đang hoạt động. Sau đó, hacker sẽ xác định những port cũng như dịch vụ mạng đang “sống” => Hacker thu thập được dạng và phiên bản của hệ điều hành. Sau đó hacker sẽ tiến hành đánh cắp dữ liệu hoặc phá hủy hệ điều hành của mạng.
  + Một số công cụ được sử dụng: Packet sniffer, Port scanner,…
  + Ví dụ:Hacker thực hiện ping sweap đến dải địa chỉ từ 192.167.1.0 đến 192.167.255.255 dể tìm ra các địa chỉ IP đang hoạt động. Sau đó sử dụng công cụ Port Scanner để thực hiện quét cổng và kiểm tra trạng thái. Từ đó xác định được các điểm yếu của máy nạn nhân => Sau khi thu thập được thông tin thì sẽ lấy những thông tin đó thực hiện những mục đích khác.
  + Cách phỏng chống: sử dụng hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS). Hệ thống này nếu thấy số lượng các gói tin ICMP echo request/s nhiều bất thường sẽ thông báo đến admin. Khi đó admin sẽ thực hiện rà soát lại hệ thống
* Kỹ thuật tấn công từ chối dịch vụ: là kiểu tấn công nhằm ngăn chặn việc sử dụng bình thường các trang thiết bị truyền thông, Tấn công này có đích xác định. Một dạng khác của tấn công từ chối dịch vụ là phá vỡ toàn bộ mạng bằng việc làm mất khả năng hoạt động hoặc quá tải bởi các thông báo.
  + Ví dụ: Kẻ tấn công gửi đến máy chủ Web một lượng lớn dữ liệu => làm nghẽ băng thông đến máy chủ, khiến cho các máy client khác không thể truy cập đến máy chủ này
  + Tấn công từ chối dịch vụ làm mất tính sẵn sàng của mạng, máy và ứng dụng.
  + Cách phòng chống: sử dụng phần mềm giám sát băng thông mạng như Nagios, Zabbix, Pandora, SolarWinds,…

1. Bạn hãy vẽ khuôn dạng gói tin IP được bảo vệ bởi giao thức ESP ở chế độ tunnel. Phân tích các trường của ESP Header và ESP Trailer (trong đó ESP header gồm: SPI, Sequence number; ESP Trailer gồm: Padding, Pad length, next header). Viết công thức tính trường ICV trong ESP Authentication.

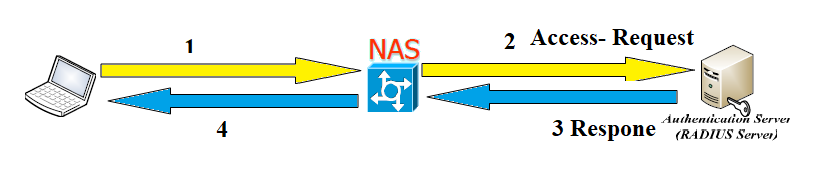
A screenshot of a cell phone

Description automatically generated

* Ở chế độ tunnel: gói Ip mới được xây dựng cùng với một tiêu đề IP mới. ESP bảo vệ cả gói tin ban đầu, bao gồm cả tiêu đề IP và Payload = TCP|UDP header + Data
* ESP header gồm có:
  + SPI (32 bit) : mỗi bên liên lạc tùy chọn giá trị SPI, bên nhận dựa vào SPI, địa chỉ IP đích, giao thức IPSec (ESP) => xác định một SA duy nhất để áp cho gói tin nhận được.
  + Sequence number (32 bit): khởi tạo bằng 0, tăng lên 1 nếu mỗi gói tin được gửi => để chống trùng lặp gói tin
* ESP traler gồm có:
  + Padding (0-255 bytes): là phần dẽ liệu được thêm vào gói tin (trước khi mã hóa) để đoạn dữ liệu được mã hóa là một số nguyên lần của một khối các byte. Nó cũng được dùng để che dấu độ dài thực của Payload
  + Pad length: xác định số byte padding đã thêm vào
  + Next header: chế độ tunnel, gói tin IP => next header = 4. Còn trong chế độ transport: TCP => 6, UDP => 17
* ESP Authentication: chứa giá trị ICV
  + ICV = HMAC (ESP header + Payload + ESP trailer + Key) : bội của 32 bit

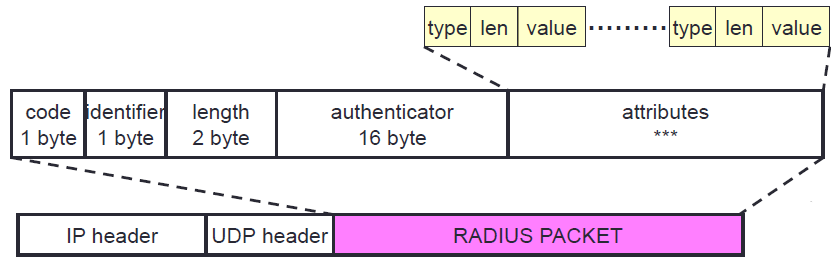
1. Hãy cho biết khái niệm, cơ chế hoạt động của giao thức RADIUS? Vẽ và phân tích khuôn dạng gói tin RADIUS?

* RADIUS (Remote Authentication Dial-In User Service): giao thức hoạt động theo mô hình Client- Server, trong đó RADIUS client hay NAS (Network Access Server) tương tác với RADIUS server thông qua một hoặc nhiều RADIUS proxies.
* RADIUS được thiết kế dựa trên nền tảng kiến trúc AAA (Authentication-Authorization-Accouting) đó là Xác Thực - Ủy Quyền – Kế toán và hoạt động ở tầng 7 (Application Layer).
* RADIUS hỗ trợ nhiều phương thức xác thực khác  
  nhau như PPP, PAP, CHAP,…
* Các thành phần: Radius server, Radius client, Suplicant
* Cơ chế hoạt động



Hoạt động chung

* + - 1. User gửi thông tin dùng để xác thực tới NAS.
      2. NAS sẽ đóng gói chúng vào AccesRequest và gửi tới RADIUS server.
      3. 3. Server phản hồi: Yes/No/Challenge. 4
      4. . NAS gửi phản hồi cho người dùng.
* Client sẽ tạo ra một “Access-Request” chứa các thuộc tính như trên: mật khẩu của user, ID của client và ID port mà user này sẽ truy cập vào. Mật khẩu khi nhập vào sẽ được ẩn (Mã hóa RSA hoặc MD5).
* “Access- Request” sẽ được gửi cho RADIUS server thông qua mạng. Nếu không trả lời trong một khoảng thời gian qui ước thì yêu cầu sẽ được gửi lại.
* RADIUS server xác nhận client gửi. Những yêu cầu từ các client nào không chia sẽ thông tin bảo mật với RADIUS sẽ không được xác nhận và trả lời. RADIUS server sẽ tìm kiếm trong cơ sở dữ liệu (CSDL) user có cùng tên trong yêu cầu. Chỉ mục của user trong CSDL sẽ chứa danh sách các đòi hỏi cần thiết cho phép user truy cập vào mạng.
* Nếu bất cứ điều kiện nào không thỏa mãn, RADIUS server sẽ gửi một trả lời “Access- Reject”
* Nếu tất cả các điều kiện đều thỏa mãn và RADIUS server muốn đưa ra một yêu cầu đòi hỏi user phải trả lời, thì RADIUS sẽ gửi một trả lời “Access-Challenge”
* Client sẽ gửi lại (re-submit) “Access-Request” với một số hiệu yêu cầu (request ID) mới, nhưng thuộc tính usename-password được lấy từ thông tin vừa mới nhập vào, và kèm luôn cả thuộc tính trạng thái từ Access-Challenge
* RADIUS server có thể trả lời một access-request bằng một Access-Accept, Access-Reject hoặc một Access-Challenge khác.
* Nếu tất cả các điều kiện đáp ứng, danh sách các giá trị cấu hình của user sẽ được RADIUS server đưa vào thông báo trả lời “Access- Accept”.
* Khuôn dạng gói tin”



* Code : Trường Code là một octet, và xác định kiểu gói của RADIUS. Khi một gói có mã không hợp lệ sẽ không được xác nhận.

Các mã RADIUS (RADIUS Code) được gán như sau:

1 Yêu cầu truy câp (Access-Request)

2 Chấp nhận truy cập (Access- Accept)

3 Từ chối truy cập (Access- Reject)

4 Yêu cầu kiểm toán (Accouting- Request)

5 Đáp ứng kiểm toán (Accouting- Response)

11 Đòi hỏi truy cập (Access- Challenge)

12 Trạng thái máy chủ (Status- Server)

13 Trạng thái máy khách (Status- Client)

255 Dự phòng (Reserved)

* Identifier: Trường Identifier là một octet, tương ứng giữa các Request- Respone.
* Length: Trường Length là hai octet, nó bao gồm chiều dài của các trường Code, Identifier, Length, Authenticator, Attribute. Những octet nằm ngoài khoảng quy định của trường Length bị xem như là octet dư thừa và sẽ bị bỏ qua khi nhận. Những gói ngắn hơn giá trị trường Length chỉ ra nó sẽ bị loại bỏ. Giá trị nhỏ nhất của trường Length là 20 và lớn nhất là 4096.
* Authenticator: Trường Authenticatior là 16 octet, chứa cá thông tin được dùng để xác thực giữa client và server, và được sử dụng trong thuật toán ẩn mật khẩu.
* Attributes: vùng chứa các thông tin xác thực, ủy quyền cũng như cấu hình chi tiết của gói tin RADIUS

## **AT11 02**

1. Hãy trình bày kiến trúc hệ thống thư điện tử, phân tích các điểm yếu về bảo mật và cách khắc phục? Trình bày giao thức khắc phục SMINE trong ứng dụng này?

* **Kiến trúc hệ thống thư điện tử:**

A screenshot of a cell phone

Description automatically generated

* + UA: User agent : chương trình hỗ trợ để soạn thảo thư
  + MTA: message transfer agent
    - MTA Client (trong mail server): trung chuyển bức thư từ mail server này đến mail server khác
    - MTA Server: nhận bức thư từ MTA Client đưa về MTA Server
  + MAA: message access agent
    - Người chuyển thư từ mail server đến người nhận thư
  + MTA Client gửi thư đến mail server của mình sử dụng giao thức SMTP (25). Mail server của A đến mail server của B cũng sử dụng SMTP. Từ mail server B gửi đến B bằng giao thức POP3 (110) hoặc IMAP (143)
* **Phân tích điểm yếu về bảo mật và cách khắc phục:**
  + Điểm yếu:
    - Từ quan điểm server:
      * Khả năng mạo danh người gửi: ví dụ: SMTP k có cơ chế xác thực
      * Máy chủ thư bị lạm dụng để phát tán thư rác, mã độc: k có cơ chế bảo vệ cho server
    - Từ quan điểm người dùng:
      * Thư có thể bị đọc/sửa trên đường truyền
      * Thư có thể bị đọc/sửa trên máy chủ
  + Cách khắc phục:
    - Giải pháp chống lạm dụng máy chủ:
      * SMTP không yêu cầu xác thực, mọi server đều mở
      * POP3 luôn yêu cầu xác thực
* Giải pháp xác thực cho SMTP: kỹ thuật POP Before SMTP (để giúp quá trình xác thực giống giao thức POP), mở rộng SMTP thành ESMTP, thêm module xác thực “Authentication”.
  + - Giải pháp chống mạo danh người gửi:
      * SMTP cho phép điền bất kỳ địa chỉ nào vào trường “FROM”
      * Sử dụng SPF được định nghĩa trong chuẩn RFC 7208 (2014), vận dụng cho SMTP giữa các mail server. Chủ sở hữu domain quy định những máy (IP) nào được phép gửi thư với domain của mình (qua SPF record trong cấu hình DNS): định nghĩa những địa chỉ IP nào thì mới được gửi mail => được add vào SPF record, những người nào ngoài những IP đó thì không gửi được. Chỉ chống giả mạo domain, không chống được giả mạo định danh (nhưng giúp truy vết nhanh chóng)
    - Chống can thiệp nội dung:
      * Chống can thiệp trên đường truyền:
        + Mã hóa, kỹ số nội dung thư: S/MINE, PGP
        + Mã hóa, xác thực kênh truyền: SSL/TLS

Như là 1 phần giao thức thư

Như là giao thức tầng giao vận

* + - * Chống can thiệp bởi server: mã hóa, ký số nội dung thư
* **Giao thức S/MINE: bảo vệ thư ngay tại tầng ứng dụng**
  + Nguyên tắc: mã hóa, ký số và kết hợp ký và mã
  + Mã hóa thư điện tử: sử dụng mật mã khóa công khai

A close up of a sign

Description automatically generated

* + - Alice gửi thư sử dụng khóa công khai của Bob để mã hóa thư cần gửi rồi gửi đến mail server của Yahoo.com.
    - Thông qua quá trình định tuyến thì thư đã được mã hóa gửi đến mail server của Google.com. Sau đó mail server sẽ gửi đến Bob, Bob sử dụng khóa bí mật của mình để thực hiện giải mã thư.
  + Ký số:

A picture containing drawing

Description automatically generated

* + - Alice gửi bức thư m, Alice ký số bằng cách băm bức thư, rồi sau đó sử dụng khóa bí mật của mình để ký lên bảng băm => kết quả thu được là chữ ký. Sau đó Alice sẽ gửi bản rõ của thư + chữ ký đến mail server yahoo.
    - Thông qua quá trình định tuyến, thư được gửi đến mail server Google. Sau đó mail server sẽ gửi đến Bob. Khi đó Bob thực hiện kiểm tra thư đó có phải của Alice hay không bằng cách: giải mã chữ ký bằng cách lấy khóa công khai của Alice => thu được bảng băm H(m). Sau đấy Bob thực hiện băm lại 1 lần nữa thông tin m để thực hiện so sánh với H(m) vừa giải mã được. Nếu trùng nhau thì đảm bảo:
      * Trên đường truyền bức thư k bị sửa
      * Chắc chắn bức thư là Alice gửi
  + Mã hóa kết hợp ký số:

A close up of a map

Description automatically generated

* + - Alice gửi bức thư m, Alice ký số bằng cách băm bức thư, rồi sau đó sử dụng khóa bí mật của mình để ký lên bảng băm => kết quả thu được là chữ ký. Alice sẽ bó thư m với chữ ký (thư truyền dưới dạng rõ)
    - Sau đó Alice sử dụng khóa công khai của Bob để mã hóa toàn bộ thư m + chữ ký => thu được bản mã c. Sau đấy Alice gửi bản mã C đến mail server Yahoo.
    - Thông qua quá trình định tuyến, thư được gửi đến mail server Google. Sau đó mail server Google sẽ gửi thư đến Bob. Bob sau khi nhận được thư sẽ thực hiện giải mã thư bằng cách sử dụng khóa bí mật của mình => thu được thư dưới dạng rõ + chữ ký. Khi đó Bob thực hiện kiểm tra thư đó có phải của Alice hay không bằng cách: giải mã chữ ký bằng cách lấy khóa công khai của Alice => thu được bảng băm H(m). Sau đấy Bob thực hiện băm lại 1 lần nữa thông tin m để thực hiện so sánh với H(m) vừa giải mã được. Nếu trùng nhau thì đảm bảo:
      * Trên đường truyền bức thư k bị sửa
      * Chắc chắn bức thư là Alice gửi
  + Cách thức làm việc của S/MINE:
    - Sử dụng PKI -> khóa công khai (dù là của người nhận hay người gửi) được lưu ở dạng chứng thư số
    - Nội dung thư được mã (base64) lại bằng MINE
    - Thông điệp MINE sẽ được ký hoặc mã, hoặc kết hợp ký và mã
    - Kết quả được mã lại bằng MINE

1. **Các khái niệm khác:**

* Peer: Điểm cuối khác của 1 kết nối PPP, hoặc của 1 phân đoạn LAN kiểu điểm-điểm, hoặc của 1 liên kết không dây. Peer sẽ được xác thực bởi Authenticator.
* AAA: Cung cấp mô hình, hạ tầng cho cơ chế điều khiển truy nhập mạng. Các dịch vụ điều khiển truy nhập mạng được cung cấp bởi AAA gồm:
  + Authentication: Dịch vụ kiểm tra định danh của người dùng hoặc thiết bị
  + Authorization: Dịch vụ gán quyền cho một yêu cầu truy nhập mạng.
  + Accouting: Kiểm toán, phân tích hoặc tính cước….