**Bài 6. Một số giao thức bảo mật mạng**

**1. Vị trí của mật mã trong mạng máy tính**

- Các giao thức bảo mật mạng:

+ Mã hóa khóa đối xứng

+ Mã hóa khóa công khai

+ Sinh khóa và trao đổi khóa

+ Hàm băm

+ Giải thuật chứng thực

+ Chữ ký số

+ Cơ sở hạ tầng khóa công khai

- Các giao thức bảo mật mạng ứng dụng trong thực tế:

+ Tầng mạng: Cơ sở hạ tầng khóa công khai (PKI) X.509, giao thức IP security (IPsec)

+ Tầng vận chuyển: Giao thức Secure Sockets Layer/Transport Layer Security (SSL/TLS)

+ Tầng ứng dụng: Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extension (S/MIME), Kerberos, Secure Shell (SSH)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Riêng tư/Mã hóa | Chứng thực | Ký/Toàn vẹn dữ liệu |
| Nhân viên nội bộ hoặc từ xa truy cập đến server | SSL 2.0 hoặc 3.0 (cung cấp bởi secure Server ID) | - Server chứng thực bởi Server ID  - Client chứng thực bởi mật khẩu hoặc bởi SSL 3.0 với Client ID | Ký vào văn bản, S/MIME sử dụng Client ID |
| Khách hàng truy cập đến server | SSL 2.0 hoặc 3.0 (cung cấp bởi secure Server ID) | Như trên | Không cần thiết |
| Nhân viên từ xa sử dụng e-mail | -SSL trên POP3 hoặc IMAP mail server  -S/MIME Client ID hoặc VPN sử dụng Ipsec | Server chứng thực bởi mật khẩu của Server ID | S/MIME sử dụng Client ID |
| Truyền thông với chi nhánh | -SSL  -VPN sử dụng IPsec | -Server chứng thực bởi Server ID  - Router/tường lửa chứng thực bởi Ipsec ID  - Client chứng thực bởi mật khẩu hoặc SLL 3.0 với Client ID | - Ký vào văn bản, S/MIME |

- Mã hóa tại tầng Transport:

+ Cung cấp an toàn cho gói TCP.

+ Có thể mã hóa hoặc chứng thực cho payload hoặc gói tin TCP (mã hóa header và payload).

+ Không ảnh hưởng đến dữ liệu nhận từ tầng ứng dụng.

+ => IP header không được mã hóa => attacker thu được sequence number và dùng chúng để tấn công.

- Mã hóa tại tầng Network:

+Bảo mật link-to-link.

+ Mã hóa hoặc chứng thực cho payload hoặc cả gói IP.

+ Không ảnh hưởng đến định tuyến.

+ Được xem như ứng dụng ở tunnel-mode.

- Mã hóa tại tầng Data-link:

+ Cung cấp bảo mật cho các frames.

+ Mã hóa hoặc chứng thực cho payload của frame.

+Phân tích traffic trên các frame đã mã hóa không thu được nhiều thông tin với các attacker.

+ Mã hóa tại tầng Datalink chi tiết hơn ở bài 7.

- Các giải thuật có thể thực hiện trên phần mềm hoặc phần cứng sử dụng công nghệ vi mạch tích hợp ứng dụng (Application Specific Integrated Circuit – ASIC).

+ Tại tầng Application: thực hiện bởi phần mềm.

+ Tại tầng Data-link: thực hiện bởi phần cứng.

+ Tại các tầng khác: thực hiện bởi phần mềm hoặc cứng hoặc cả 2.

+ Mã hóa thực hiện bởi phần cứng có hiệu suất cao nhất nhưng chi phí cao và kém linh hoạt khi cần thay đổi.

**2. Cơ sở hạ tầng khóa công khai**

- Để triển khai giải thuật mã hóa trong ứng dụng mạng, cần 1 cách phân phối các khóa bí mật dùng mạng mở. Mật mã khóa công khai là cách tốt nhất phân phối các khóa bí mật.

- Để dùng mã khóa công khai cần xây dừng 1 cơ sở hạ tầng khóa công khai (Public-key infrastructure – PKI) để hỗ trợ và quản lý các chứng chỉ khóa công khai.

- PKI cho phép người tham gia xác thực nhau và dùng thông tin từ chứng chỉ khóa công khai để mã hóa và giải mã thông tin trong lúc trao đổi.

- PKI thường bao gồm phần mềm Client và phần mềm Server, phần cứng (như thẻ thông minh) và các quy trình hoạt động liên quan.

- Người dùng có thể ký văn bản điện tử với khóa bí mật của mình và mọi người đều có thể kiểm tra bằng khóa công khai của người đó.

- PKI cho phép giao dịch điện tử diễn ra đảm bảo tính bảo mật, toàn vẹn và xóa thực lẫn nhau mà không cần trao đổi thông tin mật từ trước.

- Windows XP và Windows Server hỗ trợ cho PKI.

- Các PKI thực hiện chức năng khác nhau:

+ Xác định tính hợp pháp của người dùng trước khi cấp chứng chỉ khóa công khai cho họ

+ Phát hành chứng chỉ khóa công khai theo yêu cầu người dùng.

+ Gia hạn thời gian hợp lệ của chứng chỉ khi có yêu cầu.

+ Thuhooif chứng chỉ khóa công khai theo yêu cầu người dùng hoặc khi các khoáng riêng không còn an toàn.

+ Lưu trữ, quản lý các chứng chỉ khóa công khai.

+ Ngăn người ký chữ ký số phủ nhận chữ ký của họ.

+ Hỗ trợ việc cho phép các CA khác chứng thực chứng chỉ khóa công khai phát hành bởi các CA này.

- Danh sách một số hệ thống PKI:

+ Computer Associates eTrust PKI + Nexus

+ Entrust + OpenCA

+ Microsoft + RSA Security

+ VeriSign + …

- Verisign:

+ Thương hiệu uy tín nhất thế giới cung cấp chứng chỉ số.

+ Hiện đang bảo mật hơn 1 triệu máy chủ web trên toàn thế giới.

+ Hơn 40 ngân hàng lớn nhất thế giới và hơn 95% các công ty hàng đầu theo danh sách Fortune 500 lựa chọn chứng chỉ số SSL cung cấp bởi Verisign.

+ Hơn 90 ngàn tên miền tại 145 quốc gia hiển thị logo của Verisign, dấu hiệu được tin cậy nhất trên Internet.

+ Sử dụng giải thuật mã hóa SSL mạnh mẽ nhất:

1) Giải thuật mã hóa cao cấp từ 128 bits, an toàn gấp 288 lần so với giải thuật mã hóa 40 bits.

2) Chứng chỉ số cho phép dữ liệu trao đổi giữa người dùng và website được mã hóa từ 40-256 bits.

- X.509:

+ Được thành lập theo tiêu chuẩn ngành viễn thông của Liên minh Viễn thông Quốc tế (ITU) năm 1988.

+ Được gọi tắt là PKIX, gồm 4 phần cơ bản:

1. Endentity: người dùng chứng chỉ hoặc thiết bị (server, router) có hỗ trợ PKIX.
2. Certificate Authority (CA): tổ chức phát hành và thu hồi chứng chỉ.
3. Registration Authority (RA): xác minh danh tính của người chủ sở hữu chứng chỉ.
4. Repository: lưu trữ, quản lý chứng chỉ và danh sách các chứng chỉ bị thu hồi bởi CA.

+ Các giao dịch giữa người dùng, RA, CA và kho:

1. Đăng ký: đăng ký với CA hoặc RA (trực hoặc gián tiếp) trước khi chứng chỉ được cấp cho họ.
2. Khởi tạo: có thông tin ban đầu, gồm khóa công khai của CA và RA, các giải thuật chữ ký…
3. Chứng chỉ được phát hành: CA hoặc RA phát hành chứng chỉ trong kho lưu trữ.
4. Phục hồi khóa: CA hoặc RA cung cấp cơ chế khôi phục lại khóa riêng bị mất hoặc hỏng.
5. Tạo khóa: CA hoặc RA tạo ra cặp khóa mới cho người dùng.
6. Thu hồi chứng chỉ: Người dùng báo cho CA hoặc RA thu hồi chứng chỉ nếu họ bị mất khóa riêng, thay đổi tên/địa chỉ…
7. Chứng chỉ chéo: CA chứng thực cho các chứng chỉ được phát hành bởi CA khác.

+ Các định dạng của chứng chỉ X.509:

1. X.509 version 1 phát hành năm 1988.
2. X.509 version 2 không được dùng rộng rãi.
3. X.509 version 3 phát hành năm 1996, phổ biến nhất và dùng đến hiện nay.

+ X.509 gồm các thành phần:

1. Version: phiên bản sử dụng.
2. Serial number: số duy nhất được gán cho địa chỉ.
3. Algorithm: liệt kê tên hàm băm và giải thuật mã hóa công khai dùng để sinh ra chữ ký cho chứng chỉ. Vd: sha1RSA.
4. Issuer: tổ chức phát hành (CA ký và cấp chứng chỉ).
5. Validity period: thời hạn hiệu lực của chứng chỉ.
6. Subject: Tên chủ sở hữu chứng chỉ.
7. Public key: chứa khóa công khai và tham số liên quan, xác định thuật toán sử dụng cùng khóa.
8. Extension: cung cấp thêm 1 số thông tin.
9. Properties: cho giá trị của hàm băm của chứng chỉ.

**3. IPsec**

**-** Là giao thức bảo mật chính tại tầng Network (OSI) hoặc tầng Internet (TCP/IP).

**-** Là yếu tố quan trọng để xây mạng riêng ảo (VPN – Virtual Private Networks).

- Bao gồm giao thức chứng thưc, giao thức mã hóa, giao thức trao đổi khóa:

+ AH (Authentication Header): được sử dụng để xác định nguồn gốc gói tin IP và đảm bảo tính toàn vẹn của nó.

+ ESP (Encapsulating Security Payload): dùng để chứng thực và mã hóa gói tin IP (phần payload hoặc cả gói tin).

+IKE (Internet Key Exchange): dùng để thiết lập khóa bí mật cho người gửi và nhận.

- Ứng dụng:

+ Bảo mật kết nối giữa các chi nhánh văn phòng qua Internet.

+ Bảo mật truy cập từ xa qua Internet.

+ Thực hiện kết nối Internet và Extranet với các đối tác.

+ Nâng cao tính bảo mật trong thương mại điện tử.

- Cung cấp dịch vụ bảo mật:

+ Mã hóa quá trình truyền thông tin.

+ Đảm bảo tính nguyên vẹn của dữ liệu.

+ Phải được xác thực giữa các giao tiếp.

+ Chống quá trình replay trong các phiên bản bảo mật.

- Thuật toán được sử dụng trong IPsec bao gồm HMAC-SHA1 cho tính toàn vẹn dữ liệu (integrity protection), và thuật toán TripleDES-CBC và AES-CBC cho mã mã hóa và đảm bảo độ an toàn của gói tin. Toàn bộ thuật toán này được thể hiện trong RFC4305.

- Một SA cung cấp các thông tin:

+ Chỉ mục các thông số bảo mật: là một chuỗi nhị phân 32 bit được dùng để xác định 1 tập cụ thể của các giải thuật và thông số dùng trong truyền thông. SPI bao gồm AH và ESP để đảm bảo cả 2 đều dùng cùng giải thuật và thông số.

+ Địa chỉ IP đích.

+ Giao thức bảo mật: AH hay ESP. IPsec không cho phép AH hay ESP dùng đồng thời trong cùng 1 SA.

- IPsec gồm 2 phương thức:

1. Phương thức vận chuyển: được dùng khi có yêu cầu lọc gói tin và bảo mật point-to-point. Cả hai trạm cần 2 trạm đều cần hỗ trợ Ipsec sử dụng cùng giao thức xác thực và không đi qua 1 NAT nào. Nếu dữ liệu đi qua NAT sẽ bị đổi IP trong phần header và làm mất hiệu lực của ICV (giá trị kiểm soát tính toàn vẹn).
2. Phương thức đường hầm (Tunnel mode): dùng mode này khi cần kết nối Site-to-Site thông qua internet hoặc mạng công cộng khác. Tunnel Mode cung cập sự bảo về Gate-to-Gate.

-Authentication Header (AH bao gồm):

+ Next Header (8 bits): xác định header kết tiếp.

+ Payload Length (8 bits): chiều dài Authentication Header từ 32 bit, trừ 2.

+ Reserved (16 bits): sử dụng cho tương lai.

+ Security Parameters Index (32 bits): xác định 1 SA.

+ Sequence Number (32 bits): 1 giá trị tăng đơn điệu.

+ Authentication Data (variable): 1 vùng có chiều dài biến đổi (phải là 1 số nguyên từ 32 bits) chứa giá trị kiểm tra tính toàn ven với gói tin này.

-Các phương thức chứng thực:  
 + End-to-End Authentication.

+ End-to-Intermediate Authentication.

* Định dạng ESP:

+ Một gói ESP chứa các vùng:

1. Security Parameters Index (32 bits): xác định một SA.
2. Sequence Number (32 bits): một giá trị đếm tăng đơn điệu, cung cấp chức năng anti-replay (giống AH).
3. Payload Data (variable): 1 segment ở tầng Transport hoặc gói IP (tunnel mode) được bảo vệ bởi việc mã hóa.
4. Padding (255 bytes)
5. Pad Length (8 bits): chỉ ra số byte vùng đứng ngay trước vùng này.
6. Next Header (8 bits): chỉ ra kiểu dữ liệu chứa trong vùng payload data bằng cách chỉ ra header đầu tiên của vùng payload này.
7. Authentication Data (variable): một vùng có chiều dài biến đổi (phải là một số nguyên từ 32 bits) chứa ICV được tính bằng cách gói ESP trừ vùng Authentication Data.

-Các giải thuật sử dụng để mã hóa và chứng thực gồm:

+ Three-key triple DES

+ RC5

+ IDEA

+ Three-key triple IDEA

+ CAST

+ Blowfish

**4. SSL/TLS**

**-** Giao thức SSL (Secure Socket Layer Protocol) và giao thức TLS (Transport Layer Security Protocol) là giao thức bảo mật tại tầng Transport dùng chủ yếu trong thực tế.

- Được thiết kế và phát triển bởi Netscape, SSL dùng để bảo vệ ứng dụng WWW và các giao dịch điện tử.

- TLS là phiên bản sửa đổi của SSL v3.

- Giao thức SSL bao gồm 2 phần:

+ Phần 1 gọi là record protocol, đặt trên đỉnh của các giao thức tầng Transport.

+ Phần 2 đặt giữa các giao thức tầng Application (như HTTP) và record protocol, bao gồm các giao thức:

1. Handshake protocol
2. Change-cipher-spec protocol
3. Alert protocol

- Các giao thức của SSL:

+ Giao thức bắt tay lập các giải thuật mã hóa, giải thuật nén và các thông số sẽ được sử dụng bởi cả 2 bên trong việc trao đổi dữ liệu được mã hóa. Sau đó các giao thức bản ghi chịu trách nhiệm phân chia thông điệp vào các khối, nén, chứng thực chúng, mã hóa chúng, thêm header vào mỗi khối, sau đó truyền đi các khối kết quả.

+ Giao thức đổi mật mã cho phép các bên giao tiếp, có thể thay đổi các giải thuật hoặc các thông số trong 1 phiên truyền thông.

+ Giao thức cảnh báo là giao thức quản lý, thông báo cho các bên tham gia truyền thông khi có vấn đề xảy ra.

- Giao thức bắt tay của SSL

+ Phase 1: chọn giải thuật mã hóa như RSA, AES-128, 3DES, RC6, SHA-1… client sẽ khởi tạo với 1 thông điệp hello.

+ Phase 2: Server xác thực và trao đổi khóa. Server gửi cho Client:

1. Chứng chỉ khóa công khai của server.
2. Thông tin trao đổi khóa của server.
3. Yêu cầu chứng chỉ khóa công khai của client.

+ Phase 3: client xác thực và trao đổi khóa. Client trả lời Server các thông tin:

1. Chứng chỉ khóa công khai của Client.
2. Thông tin trao đổi khóa của Client.

+ Phase 4: hoàn thành bắt tay. Server và Client sẽ gửi nhau thông điệp finish.

**5) PGP và S/MIME**

- Có nhiều giao thức bảo mật cho tầng Application tập trung vào bảo mật Email và việc đăng nhập từ xa. Được dùng nhiều nhất:

+ PGP (Pretty Good Privacy).

+ S/MIME (Secure/Multipurpose Internet Mail Extension).

+ SSH (Secure Shell).

+ Kerberos (chứng thực cho mạng cục bộ).

- Cơ chế bảo mật E-mail

+ Bảo mật email là 1 ứng dụng cổ điển của các giải thuật mã hóa.

+ Cho E và D biểu thị 1 giải thuật mã hóa và giải mã khóa đối xứng. Cho E^ và D^ biểu thị một giải thuật mã hóa và giải mã khóa công khai.

+ Gỉa sử Alice muốn chứng minh với Bob là email M mà Bob nhận được là từ Alice gởi, Alice có thể gởi chuỗi sau cho Bob:

A black letter on a white background

Description automatically generated

+ Với  và  lần lượt là khóa công khai và khóa riêng.

+ Sau khi nhận được A black text on a white background

Description automatically generated từ Alice, với  là chữ ký vào M sử dụng khóa riêng của Alice. Trước tiên Bob so sánh chữ ký của CA trên chứng chỉ khóa công khai CA() và rút trích  từ đó. Sau đó Bob rút trích M và so sánh.

A close up of a letter

Description automatically generated

+ Nếu đúng M đến từ Alice.

+ Gỉa sử Alice muốn đảm bảo rằng M giữ được tính bí mật trong suốt quá trình truyền và cô biết khóa công khai của Bob ()< cô sẽ gửi chuỗi sau cho Bob:

A close-up of a number

Description automatically generated

Với  là khóa bí mật của cô.

+ Sau khi nhận được chuỗi từ Alice, Bob sử dụng khóa riêng của mình để giải mã:

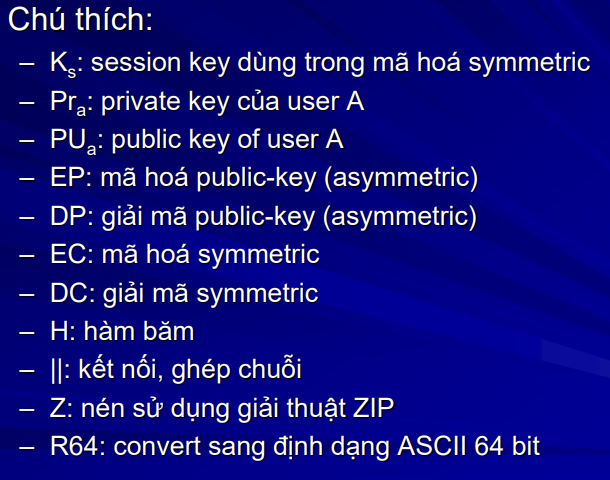
A close up of a number

Description automatically generated

+ Kế đó Bob dùng  giải mã để thu M:

A close-up of a number

Description automatically generated



- PGP:

+ Sử dụng để chứng thực thông điệp, mã hóa thông điệp, hoặc cả 2.

+ Cho phép định dạng tổng quát như chứng thực, nén ZIP, mã hóa…

+ Bản đầu được công bố vào năm 1991.

+ Kể từ 2002, PGP được đa dạng hóa thành tập hợp ứng dụng mã hóa, có thể dặt dưới sự quản trị của máy chủ bao gồm thư điện tử, chữ kí số, mật mã hóa ổ đĩa cứng, bảo mật tập tin, xóa tập tin an toàn…

+ Các phiên bản mới của PGP cho phép dùng cả OpenPGP và S/MIME.

- Chức năng của PGP:

+ Chỉ Authentication

+ Chỉ Confidentiality

+ Cả 2 cái trên

- Đặc tính của PGP:

A white table with red and blue text

Description automatically generated

- S/MIME:

+ Một chuẩn Internet về định dạng cho Email. Hầu như mọi Email trên Internet truyền qua giao thức SMTP theo dạng MIME.

+ S/MIME đưa 2 phương pháp an ninh cho email: mã hóa và chứng thực. Cả 2 đều dựa trên mã hóa bất đối xứng và PKI.

- Các tính năng của một Webmail client hộ trợ S/MIME:

+ Tạo chữ ký số cho 1 email gửi đi để đảm bảo người nhận email tin không có sự can thiệp và đến từ người gửi.

+ Mã hóa email gửi đi để ngăn bất cứ ai xem, thay đổi… Nội dung của email trước khi đến với người nhận.

+ Xác minh chữ ký số của email đã ký đến với quá trình liên quan đến một danh sách thu hồi chứng chỉ (CRL).

+ Tự động giải mã một email gửi đến để người nhận có thể đọc được nội dung của email.

+ Trao đổi chữ ký hoặc email mã hóa với những người dùng khác của S/MIME.

**6. Kerberos:**

**-** Một giao thức mã hóa để xác thực trong mạng máy tính hoạt động trên đường truyền không an toàn.

- Có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu.

- Mục tiêu thiết kế giao thức này nhằm vào client-server và đảm bảo chứng thực cho 2 chiều.

- Giao thức xây dựng dựa trên mã hóa khóa đối xứng và cần đến một bên thứ 3 mà cả 2 phía tham gia giao dịch tin tưởng.

- Mô tả phiên giao dịch:

+ Người dùng 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.

1. Người dùng nhập tên và mật khẩu tại máy tính mình (máy khách)
2. 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 dùng.
3. Phần mềm máy khách gửi gói tin (không mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung gói tin: “Người dùng XYZ muốn dùng dịch vụ” (cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS).
4. AS kiểm tra nhân dạng 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 dùng:

# Gói A: “Khóa phiên TGS/máy khách” được mã hóa với khóa công khai của người dùng.

# Gói B: “Vé chấp thuận” (bao gồm định danh người dùng (ID), địa chỉ mạng của người dùng, thời hạn của vé và “Khóa phiên TGS/máy khách”) được mật mã hóa với khóa bí mật của TGS.

1. Nhận được 2 gói tin trên, phần mềm máy khách giải mã gói A để có khóa phiên với TGS. (Người dùng không giải mã được gói 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.
2. Khi yêu cầu dịch vụ, người dùng gửi 2 gói tin sau tới TGS:

# Gói C: Bao gồm “Vé chấp thuận” từ gói B và chỉ danh (ID) của yêu cầu dịch vụ.

# Gói D: Phần nhận thực (bao gồm chỉ danh người dùng và thời điểm yêu cầu), mã hóa với “Khóa phiên TGS/Máy khách”.

1. Nhận được 2 gói C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người dùng:

# Gói E: “Vé” gồm chỉ danh người dùng, địa chỉ mạng người dùng, thời hạn dùng và “khóa phiên máy chủ/máy khách”) mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.

# Gói F: “Khóa phiên máy chủ/máy khách” mã hóa với “Khóa phiên TGS/máy khách”.

1. Nhận được 2 gói E và F, người dùng có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:

# Gói E thu được từ bước trc (trong đó có “Khóa phiên máy chủ/máy khách” mã hóa với khá bít mật của SS).

# Gói G: phần nhận thực mới, gồm chỉ danh người dùng, thời điểm yêu cầu và mã hóa với “Khóa phiên máy chủ/máy khách”.

1. SS giải mã “Vé” bằng khóa bí mật của mình và gửi gói tin sau tới người dùng để xác nhận định danh của mình và đồng ý cung cấp dịch vụ:

# Gói H: Thời điểm gói tin yêu cầu dịch vụ cộng 1, mã hóa với “Khóa phiên máy chủ/máy khách”.

1. Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người dùng có thể tin vào máy chủ SS và gửi yêu cầu sử dụng.
2. Máy chủ cung cấp dịch vụ cho người dùng.

**7. SSH:**

**-** Được tạo ra để bảo về việc đăng nhập từ xa đối với các cuộc tấn công bảo mật.

**-** Được định nghĩa trong RFC 4251.

**-** Sử dụng cổng TCP (22).

**-** Có thể hoạt động trên các flatform:

**+** Kết nối đến một máy chủ SSH trên 1 router của cisco từ 1 máy khách chạy windows

**+** Kết nối đến 1 máy chủ linux từ 1 router cisco hay kết nối một máy chủ windows 2008 từ một máy khách dùng hệ điều hành Linux.

**-** Tạo ra 1 kết nối bảo mật giữa 2 máy tính dùng các giải thuật mã hóa và chứng thực.

**-** Có khả năng nén dữ liệu, bảo mật dữ liệu truyền (SFTP) và sao chép file (SCP).

**-** Giao thức ứng dụng client-server. SSH chia thành 3 lớp trong tầng Application của mô hình mạng TCP/IP:

**+** Connection Layer.

**+** User Authentication Layer.

**+** Transport Layer.

- Được thực hiện qua 3 bước:

1) Định danh host: thực hiện qua việc trao đổi khóa. Khóa gồm 2 phần: khóa riêng và khóa công khai. Khóa công khai được dùng khi cần trao đổi giữa các máy chủ với nhau trong phiên làm việc SSH, dữ liệu sẽ được mã hóa bằng khóa công khai và chỉ giải mã bằng khóa riêng. Khi 2 hệ thống bắt đầu SSH, máy chủ gửi khóa công khia của nó cho máy khách, máy khsch sinh ra 1 khóa phiên ngẫu nhiên và mã hóa khóa này bằng khóa công cộng của máy chủ, sau đó gửi lại cho máy chủ. Máy chủ sẽ giải mã khóa phiên bằng khóa riêng của mình và nhận được khóa phiên. Khóa phiên là khóa dùng để trao đổi dữ liệu giữa 2 máy. Qúa trình đc xem là bước nhận diện máy chủ máy khách.

2) Mã hóa: # Sau khi hoàn thành bước 1, quá trình trao đổi dữ liệu diễn ra qua 1 bước trung gian là mã hóa/ giải mã. Dữ liệu gửi/nhận trên đường truyền được mã hóa và giải mã theo cơ chế đã thỏa thuận trước giữa máy chủ và máy khách.

# Chọn cơ chế mã hóa thường do máy khách quyết định. Các cơ chế mã hóa thường được chọn gồm: 3DES, IDEA và Blowfish. Chọn được cơ chế mã hóa, máy chủ và máy khách trao đổi khóa mã hóa cho nhau.

3) Chứng thực: # Mỗi định danh và truy nhập của người dùng có thể được cập theo nhiều cách.

# Việc chứng thực mật khẩu là 1 cách thông dụng để định danh người dùng, nhưng cũng có các cách khác: chứng thực RSA, dùng SSH-Keygen và SSH-Agent để chứng thực cặp khóa.