Ôn tập An toàn mạng máy tính - Cấp cứu 2 tờ A4

I. Tổng quan

A. Một số khái niệm

Dữ liệu

Dữ liệu là một tập hợp các dữ kiện, chẳng hạn như số, từ, hình ảnh, nhằm đo lường, quan sát hoặc chỉ là mô tả về sự vật. Dữ liệu gồm có 2 trạng thái:

- Transmission state (Dữ liệu đang được trao đổi, truyền tải)
- Storage state (Dữ liệu đang được lưu trữ)

Khi trao đổi dữ liệu, có 4 yêu cầu như sau:

1. **Tính bí mật** (Confidentiality) - Khả năng chỉ cho phép những người có quyền truy cập vào thông tin đó
2. **Tính toàn vẹn** (Integrity) - Khả năng đảm bảo rằng thông tin không bị thay đổi hoặc sửa đổi mà không được phép.
3. **Tính không thể từ chối** (Non-repudiation) - Khả năng xác định người gửi hoặc người nhận một thông điệp.
4. **Tính sẵn sàng** (Availability) - Khả năng đảm bảo rằng thông tin hoặc hệ thống có sẵn khi cần thiết.

Một số khái niệm khác

- Tam giác bảo mật bao gồm 3 thành phần là **Security** (Restrictions), **Functionality**(Features) và **Usability**(GUI). Khi ta thiên về một thành phần nào thì 2 thành phần còn lại trong tam giác sẽ bị yếu đi. VD: Tăng tính bảo mật thì sẽ hạn chế hơn về tính năng và giao diện ít thân thiện người dùng hơn, ngược lại, nếu thêm nhiều tính năng mới thì dễ có lỗ hỏng bảo mật và người dùng sẽ gặp khó khăn hơn khi mới sử dụng lần đầu.

B. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

1. Eavesdropping (Nghe trộm)

- Cách thức tấn công: Sử dụng một thiết bị mạng (router, card mạng…) và một ứng dụng (Tcpdump, Ethereal, Wireshark…) để giám sát lưu lượng mạng, bắt các gói tin đi qua thiết bị này. Từ đó, “nghe trộm” được thông tin từ các phiên trao đổi dữ liệu.

- Nhận xét: Thực hiện dễ dàng hơn với mạng không dây. **Không** có cách nào ngăn chặn việc nghe trộm trong một mạng công cộng.
- Cách phòng chống: Mã hoá dữ liệu trước khi truyền chúng trên mạng.

2. Cryptanalysis

- Cách thức tấn công: Sử dụng một hoặc nhiều phương pháp khác nhau để tìm kiếm thông tin hữu ích từ dữ liệu đã mã hoá mà không cần biết khoá giải mã. Điển hình là phương pháp giải mã thông qua thống kê **tần suất xuất hiện** của các ký tự.
- Nhận xét: Khi sử dụng phương pháp phân tích thông kê tần suất, cần phải sử dụng các công cụ toán học và máy tính có hiệu suất cao khi cipher text có kích thước lớn dần.
- Cách phòng chống: Sử dụng những giải thuật mã hoá không thể hiện cấu trúc thống kê trong chuỗi mật mã; Sử dụng khoá có độ dài lớn để chống Brute-force attacks.

3. Password Pilfering

Cơ chế chứng thực được sử dụng rộng rãi nhất là dùng username - tên người dùng và password - mật khẩu.

Password Pilfering là một hình thức tấn công nhằm đánh cắp mật khẩu của người dùng, có nhiều phương pháp khác nhau để thực hiện điều này.

3.1. Guessing

- Đúng như tên của nó, đây là đoán mật khẩu, hiệu quả khi đối phương có mật khẩu ngắn hoặc đang sử dụng mật khẩu mặc định.

3.2. Social engineering

- Là phương pháp sử dụng các kỹ năng xã hội để ăn cắp thông tin mật của người khác thông qua các thủ thuật như Mạo danh, Lừa đảo qua email, Thu thập thông tin từ giấy tờ bị loại bỏ, Tạo trang web đăng nhập giả hoặc chỉ đơn giản là Kết bạn làm quen rồi lấy cắp thông tin cá nhân của mục tiêu.
- Ý kiến cá nhân: Đây có thể được xem là phương pháp nguy hiểm nhất khi nó tấn công vào yếu tố con người nhiều hơn là hệ thống.

3.3. Dictionary Attacks

- Tên tiếng Việt là tấn công từ điển, thực hiện bằng cách duyệt tìm từ một từ điển các username và password đã được mã hoá (thu được từ các file SAM của Window hoặc từ trong thư mục /etc/passwd trong Linux).

3.4. Password Sniffing

- Là một phần mềm dùng để bắt các thông tin đăng nhập từ xa như username và password đối với các ứng dụng mạng phổ biến như Telnet, FTP, SMTP, POP3.
- Cách phòng chống Password Sniffing là sử dụng các giao thức như HTTPS, SSH để mã hóa toàn bộ thông điệp truyền đi.

3.5. Một số quy tắc bảo vệ mật khẩu

1. Sử dụng mật khẩu dài kết hợp giữa chữ thường, chữ hoa, số và các ký tự đặc biệt. Không dùng các từ có trong từ điển, các tên và mật khẩu thông dụng => gây khó khăn cho việc đoán mật khẩu và tấn công sử dụng từ điển.
2. Không tiết lộ mật khẩu với những người không có thẩm quyền hoặc qua điện thoại, thư điện tử hoặc bất kỳ phương tiện truyền thông nào => chống lại social engineering.
3. Thay đổi mật khẩu định kỳ và không sử dụng trở lại những mật khẩu cũ => Chống tấn công sử dụng từ điển.
4. Không sử dụng cùng một mật khẩu cho các tài khoản khác nhau.
5. Không sử dụng những phần mềm đăng nhập từ xa mà không có cơ chế mã hoá như là Telnet.
6. Huỷ hoàn toàn các tài liệu có lưu các thông tin quan trọng sau khi sử dụng xong mục đích ban đầu.
7. Tránh nhập các thông tin trong các cửa sổ popup và Không click vào các đường liên kết lạ, không rõ nguồn gốc.

4. Identity Spoofing

- Là phương pháp tấn công cho phép kẻ tấn công mạo nhận nạn nhân mà không cần sử dụng mật khẩu của nạn nhân.
- Các phương pháp phổ biến bao gồm:
    - Man-in-the-middle attacks
    - Message replays attacks
    - Network spoofing attacks
    - Software exploitation attacks

4.1. Man-in-the-middle

- Kẻ tấn công cố gắng dàn xếp với thiết bị mạng (hoặc cài đặt một thiết bị của riêng mình) giữa hai hoặc nhiều người sử dụng, sau đó chặn và sửa đổi hay làm giả dữ liệu truyền giữa những người sử dụng rồi tiếp tục truyền chúng tới địa chỉ đích như chưa từng bị tác động bởi kẻ tấn công.

- Mã hoá và chứng thực các gói IP là biện pháp chính để ngăn chặn các cuộc tấn công Man-in-the-midle.

4.2. Messeage Replays

- Trong một số giao thức xác thực, sau khi người dùng A chứng thực mình với hệ thống là một người dùng hợp pháp, A sẽ được cấp một chứng thực (giấy phép) thông qua. Với giấy phép này, A sẽ nhận được những dịch vụ cung cấp bởi hệ thống.
- Những kẻ tấn công có thể ngăn chặn gói tin chứa chứng thực đó, giữ một bản sao, và sử dụng nó sau này để mạo nhận (đóng vai) người dùng A.

4.3. Network spoofing

- **SYN flooding** là khi kẻ tấn công lấp đầy bộ đệm TCP của máy tính mục tiêu với một khối lượng lớn các gói SYN, làm cho máy tính mục tiêu không thể thiết lập các thông tin liên lạc với các máy tính khác.
- **TCP hijacking** là một kỹ thuật sử dụng các gói tin giả mạo để chiếm đoạt một kết nối giữa máy tính nạn nhân và máy đích. Để ngăn chặn kỹ thuật tấn công này, có thể sử dụng phần mềm như TCP Wrappers để kiểm tra địa chỉ IP tại tầng Transport.
- **ARP spoofing** hoặc ARP Poisoning diễn ra khi kẻ tấn công thay đổi địa chỉ MAC đích hợp pháp của một địa chỉ IP đến một địa chỉ MAC khác được lựa chọn bởi những kẻ tấn công. Nói ngắn gọn, là thay đổi địa chỉ MAC đích thành địa chỉ mong muốn của kẻ tấn công. Để ngăn chặn các cuộc tấn công ARP spoofing, cần phải tăng cường kiểm tra các tên miền, và chắc chắn rằng địa chỉ nguồn và địa chỉ đích trong một gói tin không được thay đổi trong khi truyền.

5. Buffer-Overflow Exploitations

- Buffer-Overflow là lỗi xảy ra khi quá trình ghi dữ liệu vào bộ đệm nhiều hơn kích thước khả dụng của nó.
- Các hàm strcat(), strcpy(), sprintf(), vsprintf(), bcopy(), get(), scanf()… trong ngôn ngữ C có thể bị khai thác bằng lỗi này vì không kiểm tra xem liệu bộ đệm có đủ lớn để dữ liệu được sao chép vào mà không gây ra tràn bộ đệm hay không.

6. Repudiation

- Trong một số trường hợp chủ sở hữu của dữ liệu có thể không thừa nhận quyền sở hữu của dữ liệu để tránh hậu quả pháp lý. Người này có thể cho rằng chưa bao giờ gửi hoặc nhận các dữ liệu đó. Ngay cả khi dữ liệu đã được chứng thực, chủ sở hữu của dữ liệu xác thực có thể thuyết phục quan tòa rằng vì những sơ hở, bất cứ ai cũng có thể dễ dàng chế tạo tin nhắn và làm cho nó trông giống như thật.
- Sử dụng các thuật toán mã hóa và xác thực có thể giúp ngăn ngừa các cuộc tấn công bác bỏ.

7. Intrusion

- Tấn công xâm nhập bất hợp pháp vào một mạng với mục đích truy cập vào hệ thống máy tính của người khác, đánh cắp thông tin và tài nguyên máy tính hoặc băng thông của nạn nhân.
- Phòng chống bằng cách đóng các cổng UDP hoặc TCP không cần thiết, sử dụng IP scan và Port scan để kiểm tra các lỗ hỏng trong hệ thống.

8. Denial of Service Attacks

- Tấn công từ chối dịch vụ nhằm ngăn chặn người dùng hợp pháp sử dụng những dịch vụ mà họ thường nhận được từ các máy chủ. Thường buộc máy tính mục tiêu phải xử lý một số lượng lớn những thứ vô dụng nhằm tiêu hao tài nguyên máy, dẫn đến không hoạt động được nữa. Nếu cuộc tấn công được phát sinh từ một nhóm các máy tính phân bố khắp nơi thì sẽ trở thành **DDoS - Distributed Denial of Serivce Attack**.
- Công cụ để thực hiện tấn công DoS có thể là Jolt2, Bubonic.c, Land and LaTierra, Targa, Blast20, Nemesy, Panther2,Crazy Pinger, Some Trouble, UDP Flood, FSMax.
- DoS có các hình thức cơ bản sau: Smurf, Buffer Overflow Attack, Ping of death, Teardrop và SYN Attack
- Trong Smurf, máy của attacker sẽ gởi rất nhiều lệnh ping đến một số lượng lớn máy tính trong một thời gian ngắn trong đó địa chỉ IP nguồn của gói ICMP echo sẽ được thay thế bởi địa chỉ IP của nạn nhân. Các máy tính này sẽ trả lại các gói ICMP reply đến máy nạn nhân, buộc máy nạn nhân phải xử lý một lượng lớn các gói tin trong thời gian ngắn đó.
- Trong DDoS, Attackers thường sử dụng Trojan để kiểm soát cùng lúc nhiều máy tính nối mạng. Attacker cài đặt một phần mềm đặc biệt (phần mềm zombie) lên các máy tính này (máy tính zombie) để tạo ra một đội quân zombie (botnet) nhằm tấn công DoS sau này trên máy nạn nhân

9. Malicious Software

Các phần mềm độc hại bao gồm:

- **Virus** - Một phần mềm có thể sao chép chính nó để lây nhiễm sang máy khác trong hệ thống, không đứng một mình mà phải được gắn vào một tập tin khác.
- **Worms** - Cũng là một chương trình có thể tự sao chép chính nó nhưng có thể tự đứng một mình. Một Worm có thể tự thực thi tại bất kỳ thời điểm nào.
- **Trojan horses** - Thường nguỵ trang mình kèm theo những chương trình ứng dụng thông thường và vô hại. Không tự sao chép bản thân và chỉ thực hiện khi người dùng chạy chương trình có đính kèm Trojan. Chức năng chính của Trojan là điểu khiển máy tính từ xa, ăn cắp thông tin của nạn nhân hoặc làm nhiệm vụ backdoor.
- **Logic bombs** - Chương trình con hoặc lệnh được nhúng trong một chương trình khác. Nó được kích hoạt bởi điều kiện được thiết lập bởi kẻ tấn công.

- **Backdoors** - Những đoạn chương trình bí mật thường được đính kèm vào những chương trình khác, Backdoors sẽ mở một hoặc nhiều port trên máy nạn nhân giúp kẻ tấn công xâm nhập thông qua các port đó.
- **Spyware** - Phần mềm tự cài đặt chính nó trên máy tính của người dùng. Spyware thường được sử dụng để theo dõi xem người dùng làm gì và quấy rối họ. Các loại phổ biến là Browser hijacking - Thay đổi trình duyệt của user và Zombieware - Biến máy của user thành zombie dùng trong DDoS.

C. Lý lịch của những kẻ tấn công

Các attacker được chia thành các loại bao gồm:

- **Black-hat hackers** - Là những người có tri thức đặc biệt về hệ thống máy tính. Họ quan tâm đến những chi tiết tinh tế của phần mềm, giải thuật, mạng máy tính và cấu hình hệ thống. Ngoài ra còn các loại hacker khác như **White-hat** và **Grey-hat**.
- **Script kiddies** - Là những chú bé sử dụng các script hoặc các chương trình được phát triển bởi các hacker mũ đen để tấn công các máy tính và gây thiệt hại cho người khác. Mấy anh trai này chỉ biết dùng công cụ có sẵn chứ không hiểu cách hoạt động của chúng cũng như tự phát triển ra công cụ tương tự.
- **Cyber spies** - Thường hoạt động trong lĩnh vực quân sự, kinh tế với mục đích đánh chặn truyền thông trên mạng và phá mã các thông điệp.
- **Vicious employees** - Những người cố tình vi phạm an ninh để làm hại công ty của chính họ vì các lý do cá nhân.
- **Cyber terrorists** - Những kẻ khủng bố cực đoan sử dụng máy tính và công nghệ mạng làm công cụ.

D. Mô hình bảo mật cơ bản

Một mô hình bảo mật cơ bản gồm 4 thành phần:

- Hệ thống mã hoá (Cryptosystem)
- Tường lửa (Firewalls)
- Hệ thống phần mềm chống độc hại(Anti-Malicious System software – AMS software)
- Hệ thống tìm kiếm xâm nhập (Intrusion Detection System – IDS)

Đối với phương thức phòng thủ, ta có phương thức phòng thủ theo lớp (layer):

- Application
- Host
- Internal Network

- Perimeter
- Physical
- Policies, Procedures and Awareness

II. Malware

A. Trojan

1. Khái niệm

Phần mềm Trojan đầu tiên trên máy tính là **Back Orifice** với port xâm nhập là 31337.

Trojan là chương trình gây hại, thường hoạt động bí mật và có công dụng phổ biến là **thiết lập quyền điều khiển từ xa** cho hacker trên máy bị nhiễm Trojan.

Trojan có thể xâm nhập vào hệ thống qua rất nhiều con đường nhau như qua ứng dụng nhắn tin, file đính kèm trong email, phần mềm miễn phí trên mạng…

2. Phân loại Trojan

Ta có các loại Trojan thường thấy như sau:

- **RAT** - Remote Access Trojan: Biến máy tính bị nhiễm thành server để máy của hacker có thể truy cập vào và nắm quyền điều khiển. RAT tự động kích hoạt mỗi khi máy tính hoạt động và thường vô hiệu hóa việc chỉnh sửa registry nên khóa xóa Trojan này. Phổ biến có Back Orifice, Girlfriend, Netbus…
- **Keyloggers**: Bao gồm 2 loại phần cứng và phần mềm, kích thước nhỏ gọn và sử dụng ít bộ nhớ nên khó phát hiện. Chúng có nhiệm vụ chủ yếu là ghi lại diễn biến của bàn phím rồi lưu lại trên máy hoặc gửi về cho hacker. Một keylogger thường gồm **3 thành phần** chính là **Chương trình điều khiển** để điều phối hoạt động và thiết lập, **Tập tin hook** để ghi nhận các thao tác bàn phím và **Tập tin nhật ký (log)** - Nơi chứa đựng toàn bộ những gì hook ghi nhận được.
- **Trojan lấy cắp password**: Đúng như tên gọi, chúng ăn cắp các mật khẩu lưu trên hệ thống rồi gửi về cho hacker. Các loại phổ biến là Barri, Kuang, Barok.
- **FTP Trojan**: Loại này mở cổng **21** trên máy bị nhiễm nên mọi người đều có thể truy cập máy này để tải dữ liệu.
- **Trojan phá hoại**: Có khả năng phá hủy đĩa cứng, mã hoá các file. Rất nguy hiểm và khó kiểm soát.
- **Trojan chiếm quyền kiểu leo thang**: Thường được gắn vào một ứng dụng hệ thống nào đó và sẽ cho hacker quyền cao hơn quyền đã có trong hệ thống khi ứng dụng này chạy.

3. Một số Trojan phổ biến

- Loại Keyloggers
    - KGB Spy.
    - Blazing Tool Perfect Keylogger
    - Stealth Keylogger
- Loại RAT
    - DJI RAT
    - HackerzRAT
    - NET BUS
- Công cụ tạo Trojan
    - Trojan Horse Construction Kit
    - Dark Horse Trojan Virus Maker

B. Phòng chống Trojan

Dưới đây là một số bước cần thực hiện nhằm phòng chống Trojan:

- Quét các port đang mở với các công cụ như Netstat, Fport, TCPView.
- Quét các tiến trình đang chạy với Process Viewer, What's on my computer, Insider.
- Quét những thay đổi trong Registry với MsConfig, What's running on my computer.
- Quét những hoạt động mạng với Ethereal, WireShark.
- Chạy các phần mềm diệt Trojan như Trojan Hunter, Trojan Guard.

Một số cổng đi cùng các Trojan thông dụng:

Trojan	**Protocol**	**Port**
Back Orifice	UDP	31337 hoặc 31338
Deep Throat	UDP	2140 và 3150
NetBus	TCP	12345 và 12346
Whack-a-mole	TCP	20034
NetBus 2 Pro	TCP	21544
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423 và 40426

C. Virus

2. Tính chất của Virus

1. Tính lây lan.
2. Tính phá hoại.
3. Tính nhỏ gọn.
4. Tính tương thích.
5. Tính phát triển và kế thừa.

3. Phân loại virus

3.1. Phân loại theo phương pháp tìm đối tượng lây nhiễm

1. Virus thường trú
2. Virus không thường trú

3.2. Phân loại theo đối tượng nhiễm và môi trường hoạt động

1. Boot Virus
2. File-System Virus
3. File-Format Virus
4. Macro Virus
5. Script Virus
6. Registry Virus

3.3. Phân loại theo phương pháp lây nhiễm

1. Ghi đè
2. Ghi đè bảo toàn
3. Dịch chuyển
4. Song hành
5. Nối thêm
6. Chèn giữa
7. Định hướng lại lệnh nhảy

8. Điền khoảng trống

3.4. Cách phân loại khác theo tính năng và bản chất

1. System Sector or Boot Virus: lây nhiễm trên cung boot của đĩa.
2. File Virus: lây nhiễm trên các file thực thi.
3. Macro Virus: lây nhiễm trên các tập tin word, excel, access…
4. Source Code Virus: ghi đoạn code của Trojan đè hoặc nối tiếp vào đoạn code của tập tin chủ.
5. Network Virus: tự phát tán theo email bằng cách sử dụng lệnh và các giao thức của mạng máy tính.
6. Stealth Virus: có thể ẩn với các chương trình chống virus.
7. Polymorphic Virus: có thể thay đổi đặc điểm của nó với mỗi lần lây nhiễm.
8. Cavity Virus: duy trì kích thước file không thay đổi trong khi lây nhiễm.
9. Tunneling Virus: tự che giấu dưới những dạng anti-virus khi lây nhiễm.
10. Camouflage Virus: ngụy trang dưới dạng những ứng dụng chính hãng của người dùng.
11. Shell Virus: đoạn mã của virus sẽ tạo thành một shell xung quanh đoạn mã của chương trình bị lây nhiễm, tương tự như một chương trình con trên chương trình gốc nguyên thủy.
12. Add-on Virus: ghi đoạn mã của nó nối tiếp vào điểm bắt đầu của chương trình bị lây nhiễm và không tạo ra thêm bất kỳ thay đổi nào khác.
13. Intrusive Virus: viết đè đoạn code của nó lên một phần hoặc hoàn toàn đoạn code của file bị lây nhiễm.

D. Các kỹ thuật của Virus

1. Kỹ thuật cơ bản

Các kỹ thuật cơ bản của Virus bao gồm 9 kỹ thuật như sau:

1. Kỹ thuật lây nhiễm
2. Kỹ thuật định vị trên vùng nhớ
3. Kỹ thuật kiểm tra sự tồn tại
4. Kỹ thuật thường trú
5. Kỹ thuật mã hoá
6. Kỹ thuật nguỵ trang
7. Kỹ thuật phá hoại

8. Kỹ thuật chống bẫy
9. Kỹ thuật tối ưu

1.1. Kỹ thuật lây nhiễm

Là kỹ thuật cơ bản cần phải có của mỗi virus. Có thể đơn giản hoặc phức tạp tuỳ loại virus.

- Kỹ thuật lây nhiễm Boot Record / Master Boot của đĩa: thay thế BR hoặc MB trên phân vùng hoạt động với chương trình virus.
- Kỹ thuật lây nhiễm file thực thi: chương trình virus sẽ được ghép vào file chủ bằng cách nối thêm, chèn giữa, điền vào khoảng trống, ghi đè

Thuật toán thường dùng để lây nhiễm một file .COM: Mở file, Ghi lại thời gian/ngày tháng/thuộc tính, Lưu trữ các byte đầu tiên (thường là 3 byte), Tính toán lệnh nhảy mới, Đặt lệnh nhảy, Chèn thân virus chính vào, Khôi phục thời gian/ngày tháng/thuộc tính, Đóng file

1.2. Kỹ thuật định vị trên vùng nhớ

Phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment:offset mới.

Virus macro và virus script thực chất là các lệnh của chương trình ứng dụng nên không cần tiến hành kỹ thuật này. Với virus boot và virus file thì đây là một kỹ thuật quan trọng, cần phải có.

1.3. Kỹ thuật kiểm tra sự tồn tại

Mỗi virus chỉ nên lây nhiễm/kiểm soát một lần để đảm bảo không làm ảnh hưởng đến tốc độ làm việc của máy tính => Cần có kỹ thuật kiểm tra sự tồn tại của mình trước khi lây nhiễm hoặc thường trú.

Kỹ thuật kiểm tra thường là:

- Dò tìm đoạn mã nhận diện trên file hoặc bộ nhớ.
- Kiểm tra theo kích thước hoặc nhãn thời gian của file

1.4. Kỹ thuật thường trú

Cũng có thể gọi đây là kỹ thuật phân phối vùng nhớ, được thực hiện trước khi triển khai định vị tới vùng nhớ đã xác định đó.

- Các virus boot phải phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, biến, vùng đệm.
- Các virus file cần phải kiểm tra xem chương trình đã thường trú chưa, nếu chưa sẽ định rõ vùng nhớ muốn sử dụng, copy phần virus vào bộ nhớ, sau đó khôi phục file chủ và trả quyền điều khiển về cho file chủ.

1.5. Kỹ thuật mã hoá

Che giấu mã lệnh thực sự của chương trình virus. Thủ tục mã hoá cũng chính là thủ tục giải mã.

1.6. Kỹ thuật nguỵ trang

Giấu giếm, nguỵ trang sự tồn tại của virus trên đối tượng chủ. Những virus sử dụng kỹ thuật này thường chậm bị phát hiện nên có khả năng lây lan mạnh.

Quy trình nén file để ngụy trang sự tồn tại của virus:

- Kiểm tra kích thước file chủ định lây nhiễm
- Nén file chủ
- Gắn đoạn mã cần lây nhiễm vào file chủ
- Có thể chèn thêm những đoạn ký tự vô nghĩa khi kích thước file chủ + virus vẫn nhỏ hơn kích thước file chủ ban đầu.
- Giải nén file chủ trước khi file này thực thi.

1.7. Kỹ thuật phá hoại

Rất đa dạng trong phương thức phá hoại, có thể liên quan tới việ phá hoái dữ liệu trên máy tính hoặc phá hoại trực tiếp các chương trình hệ thống.

1.8. Kỹ thuật chống bẫy

Chọn lọc file trước khi lây nhiễm theo một số tiêu chí nào đó nhằm tránh những file bẫy của chương trình Antivirus.

1.9. Kỹ thuật tối ưu

Gồm các kỹ thuật viết mã và thiết kế nhằm tối ưu chương trình về tốc độ và kích thước

2. Các kỹ thuật đặc biệt

2.1. Kỹ thuật tạo vỏ bọc

Là kỹ thuật chống gỡ rối / dịch ngược mã lệnh virus nhằm chống lại phần mềm antivirus. Thường mã hoá hoặc sử dụng các lệnh JMP và CALL để chương trình lộn xộn, phức tạp. Ngoài ra còn sử dụng các thủ tục giả để phân tích viên gặp khó khăn khi phân biệt các tác vụ.

2.2. Kỹ thuật đa hình

Là kỹ thuật chống lại phương pháp dò tìm đoạn mã mà các chương trình antivirus thường sử dụng để nhận dạng một virus đã biết bằng cách tạo ra các bộ giải mã khác biệt.

2.3. Kỹ thuật biến hình

Cũng là một kỹ thuật chống lại các kỹ thuật nhận dạng của chương trình antivirus bằng cách sinh ra cả đoạn mã mới hoàn toàn. Đây là một kỹ thuật khó và phức tạp.

2.4. Kỹ thuật chống mô phỏng và theo dõi

Một số chương trình antivirus hiện đại sử dụng phương pháp heuristic để phát hiện virus dựa trên hành vi của chương trình. Kỹ thuật này nhằm chống lại sự phát hiện của chương trình antivirus như vậy. Thông thường là chèn thêm những đoạn mã lệnh "rác" không ảnh hưởng đến logic của chương trình xen kẻ giữa những mã lệnh thực sự.

3. Các kỹ thuật trên mạng

3.1. Kỹ thuật lây nhiễm trên mạng

- Sử dụng hàm GetLogicalDriveStrings để lây lan qua các ổ đĩa chia sẻ từ xa được ánh xạ thành ổ đĩa cục bộ.
- Sử dụng các hàm API để liệt kê các ổ đĩa mà người sử dụng đã kết nối.

3.2. Kỹ thuật phát tán virus trên mạng

- Sử dụng sự phổ biến của email, chặn các API hỗ trợ mạng.

3.3. Kỹ thuật phá hoại trên mạng

- Tạo các cổng nghe đợi sẵn để virus có thể tiến hành các hoạt động phá hoại hay do thám như lấy trộm mật khẩu, khởi động máy, phá hoại hệ thống…
- Tấn công từ chối dịch vụ (DoS)

E. Phòng chống Virus

- Hạn chế sử dụng đĩa mềm hoặc USB không rõ nguồn gốc mà chưa có sự kiểm tra bằng các phần mềm diệt virus.
- Không cài đặt các phần mềm không cần thiết hoặc download từ trên mạng về.
- Không sử dụng các phần mềm không có bản quyền.
- Không nên mở xem các thư điện tử lạ.
- Phải cài các phần mềm chống virus tốt nhất.
- Phải sao lưu dữ liệu thường xuyên

3. Chương trình quét và diệt Virus

Các chương trình tìm diệt Virus sẽ quét các tập tin thực thi, tập tin office, tập tin đính kèm E-mail, các tập tin được download và những dạng tập tin khác có thể trở thành host của Virus (Hostable files).

Các phương pháp quét chuẩn bao gồm:

- **Basic scanning**
    - Tìm chữ ký của virus đã được biết đến trong các tập tin hostable, bao gồm cả cấu trúc, định dạng, các mẫu, và những đặc trưng khác.
    - Kiểm tra kích thước của các file hệ thống đã bị thay đổi để phát hiện nhiễm virus.
- **Heuristic scanning**: quét các đoạn mã đáng ngờ trong các tập tin thực thi dựa trên công nghệ heuristics.
- **ICV scanning**
    - Sử dụng giải thuật HMAC để tính toán giá trị kiểm tra tính toàn vẹn của tập tin thực thi chưa bị nhiễm virus và một khoá mã hoá cố định.
    - Một giá trị ICV được nối vào cuối của tập tin thực thi không bị nhiễm virus
    - Các virus không biết mật mã sẽ không thể thay đổi ICV
    - Khi một tập tin bị nhiễm virus, giá trị ICV của nó sẽ thay đổi so với giái trị ICV ban đầu.

F. Các phần mềm độc hại phổ biến

- Malware (Phần mềm độc hại): Là một thuật ngữ tổng quát dùng để mô tả bất kỳ phần mềm có hành vi gây hại hoặc xâm phạm đối với máy tính hay hệ thống. Malware có thể bao gồm virus, worm, trojan, ransomware, spyware, adware và nhiều loại khác.
- Virus: Là một chương trình máy tính có khả năng tự sao chép và gắn kết vào các tệp tin khác mà không cần sự sự chấp nhận hoặc sự hiểu biết của người sử dụng.
- Worm (Sâu máy tính):Giống như virus, nhưng có khả năng tự lây lan qua mạng và các thiết bị khác mà không cần sự tương tác của người sử dụng.
- Trojan (Trojan Horse):Là một loại malware được giấu giếm trong các tệp hoặc chương trình có vẻ hữu ích hoặc không nguy hiểm để lừa dối người sử dụng và tạo điều kiện cho việc tấn công từ bên trong.
- Ransomware : Mã hóa dữ liệu trên máy tính của nạn nhân và đòi tiền chuộc để cung cấp khóa giải mã. Nếu người dùng không thanh toán, dữ liệu của họ có thể bị mất hoặc không thể truy cập.
- Spyware:Thu thập thông tin về hành vi người sử dụng mà không sự chấp thuận của họ, thường được sử dụng để định hình quảng cáo hoặc thu thập thông tin cá nhân.
- Adware:Hiển thị quảng cáo không mong muốn trên máy tính của người sử dụng, thường đi kèm với các ứng dụng miễn phí.
- Keylogger (Ghi chú phím):Thu thập thông tin từ bàn phím của người sử dụng mà không họ biết, thường được sử dụng để đánh cắp thông tin đăng nhập và mật khẩu.

- Rootkit:Là một loại phần mềm độc hại mà mục tiêu chính là ẩn đi sự tồn tại của nó hoặc sự tồn tại của các hoạt động độc hại khác trên hệ thống.
- Botnet:Một mạng các máy tính bị nhiễm malware và được điều khiển từ xa để thực hiện các hành động xấu, như tấn công mạng hoặc gửi thư rác.

III. Các giải thuật mã hóa

A. Giới thiệu về mã hóa

Một số khái niệm

- Thông điệp, văn bản: là một chuỗi hữu hạn các ký hiệu lấy từ bảng chữ cái, các con số và được ký hiệu là m.
- Phép mã hóa: là việc biến đổi một văn bản sao cho nó không thể hiểu nổi đối trừ người nhận được mong muốn. Phép mã hoá được ký hiệu là e(m).
- Khóa: là thông số đầu vào của phép mã hoá hoặc giải mã. Khoá mã hoá ký hiệu là k_e, khoá giải mã ký hiệu là k_d.
- Chuỗi mật mã: là chuỗi kết quả qua phép mật mã hoá và thường được ký hiệu là c, với: c = $e(m,k_e)$.
- Phép giải mã: là việc xác định văn bản gốc m từ chuỗi mật mã c và khoá giải mã k_d, và được ký hiệu là $d(c,k_d)$.
- Như vậy: $d(c,k_d) = m$.

Phân loại các giải thuật mã hóa

- Giải thuật mã hóa cổ điển: Vigenère, Caesar, Playfair, Hill,…
- Giải thuật mã hóa hiện đại:
    - Mã hóa đối xứng (symmetric):
        - Mã hóa theo các khối bit: DES, AES, RC2, RC6, MARS,…
        - Mã hóa theo từng bit: RC4
    - Mã hóa bất đối xứng (asymmetric): RSA

B. Giải thuật mã hóa cổ điển

1. Mã thay thế đơn giản (Substitution Cipher)

- Khóa là 1 hoán vị của bảng chữ cái. Do đó sẽ có 26! ~ 4.1026 kiểu khóa khác nhau.

- Mỗi kí tự của thông điệp m được thay bằng ký hiệu tương ứng qua khóa, từ đó cho ra chuỗi mật mã c.

A	B	C	D	E	F	G	H	I	J	K	L	M
k	m	j	z	p	b	o	d	t	s	g	v	i
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
y	w	l	x	n	c	q	a	r	f	e	u	h

Vì đây là hoán vị nên các bạn không cần chuẩn bị sẵn hình như trên đâu chỉ cần hiểu phương thức mã hóa là được. Nhưng khuyến khích nên soạn sẵn 1 bảng chữ cái để không lẫn lộn.

Giả sử ta có thông điệp m là HELLO. Khi này ta sẽ lần lượt mã hóa thông điệp m dựa trên khóa trên:

- e(H) = d
- e(E) = p
- e(L) = v
- e(O) = w

Cuối cùng ta có được chuỗi mật mã sau: c = DPVVW.

2. Mã thay thế n-gram

- Cũng tương tự như mã thay thế đơn giản nhưng ở đây chúng ta thay thế cho từng cụm ký tự.
- Khóa vẫn sẽ là hoán vị của bảng chữ cái nên khi này có 26^n kiểu khác nhau, với n là số ký tự trong 1 cụm.
- Khóa sẽ được biểu diễn dưới dạng bảng với các hàng biểu diễn ký hiệu đầu tiên, các cột biểu diễn ký hiệu thứ hai.

3. Mã hoán vị bậc d (Permutation Cypher)

- Chia thông điệp **m** ra thành từng khối có chiều dài là **d**. Sau đó hoán vị lần lượt từng khối để tạo ra chuỗi mật mã **c**.
- Ví dụ:

Ta có m: Cryptool1 và d = 3. Mỗi block ta sẽ hoán vị theo cách thức 1,2,3 -> 3,1,2 Qua phép mã hóa hoán vị bậc d, ta được chuỗi mật mã c: yCropt1ol.

4. Mã dịch chuyển (Shift Cypher)

Giải thuật Vigenère

- Khóa là 1 chuỗi gồm d ký tự và sẽ được lặp lại cho đến khi độ dài khóa bằng độ dài văn bản m.
- Khi mã hóa, từng ký tự sẽ được thay ký tự tương ứng trên bảng mã Vigenère với cột là ký tự cần thay ở m, hàng là ký tự cùng thứ tự trên chuỗi khóa
- Ví dụ

Ta có: Thông điệp: HAITC Khóa: MANU Khi này do khóa có độ dài ít hơn thông điệp nên lặp lại từng kí tự của khóa cho đến khi bằng, ta được: MANUM.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Sử dụng bảng mã Vigenère ở trên, ta mã hóa m như sau:

e(H, M) = T

e(A, A) = A

e(I, N) = V

e(T, U) = N

e(C, M) = O

Khi đó ta được: c = TAVNO.

Giải thuật Caesar

Giải thuật Caesar tương tự như giải thuật Vigenère nhưng nó đơn giản hơn. Ở Vigenère, chúng ta mã hóa từng ký tự theo cách khác nhau. Nhưng ở Caesar, chúng ta mã hóa các ký tự theo 1 cách duy nhất là dịch các kí tự sang phải **k** lần cho trước.

Nói cách khác, khóa của giải thuật Caesar chỉ là chuỗi có 1 ký tự (d = 1) được lặp lại sao cho độ dài của nó bằng thông điệp m.

5. One - time Pad (OTP)

Quy trình mã hóa OTP:

- Đầu tiên các ký tự của thông điệp m được đưa về dạng nhị phân (cụ thể ký tự đó tương ứng mã nhị phân ra sao thì tùy đề sẽ có cung cấp).
- Sau đó mỗi mã nhị phân đó sẽ cộng XOR (khác = 1, giống = 0) với mã nhị phân tương ứng từ khóa.
- Cuối cùng chuyển các mã nhị phân nhận được về dạng ký tự thì sẽ được chuỗi mã hóa c.

6. Mã tuyến tính (Affine Cipher)

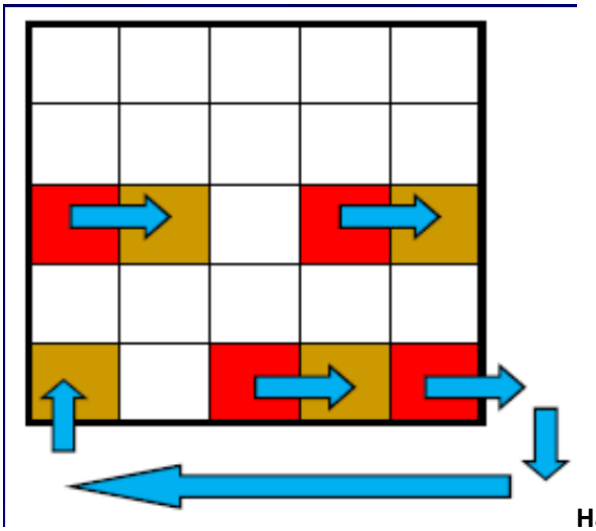
Affine Cipher là một loại mật mã thay thế dùng một bảng chữ cái, trong đó mỗi chữ cái được ánh xạ tới một số sau đó mã hóa qua một hàm số toán học đơn giản.

Việc mã hóa được thực hiện dưới dạng sau:

e(x) = ax + b (mod 26) với a là số nguyên tố từ 1-26, b là số bước nhảy cũng có giá trị từ 1-26.

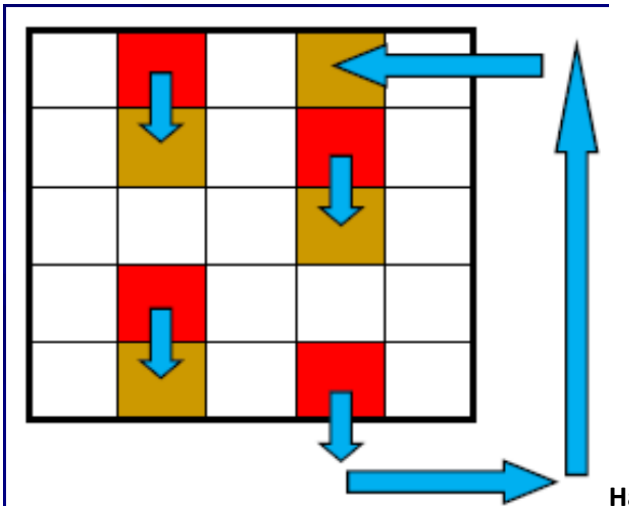
7. Mã Playfair

- Giải thuật sẽ sử dụng 1 ma trận khóa dạng 5x5 hoặc 6x6.
- Ma trận đầu tiên sẽ được thêm vào các ký tự của khóa.
- Nếu ma trận chưa đầy thì sẽ được bổ sung bằng các ký tự từ A->Z. Trong đó I và J được coi là 1 ký tự.
- Khi bổ sung các ký tự cho ma trận thì không được thêm các ký tự đã có trước đấy.
- Giải thuật mã hóa:
    - Mã hóa từng cặp 2 ký tự liên tiếp nhau.
    - Nếu dư 1 ký tự, thêm ký tự “x” vào cuối.
    - Nếu 2 ký tự nằm cùng dòng, thay thế bằng 2 ký tự tương ứng bên phải. Ký tự ở cột cuối cùng được thay bằng ký tự ở cột đầu tiên.



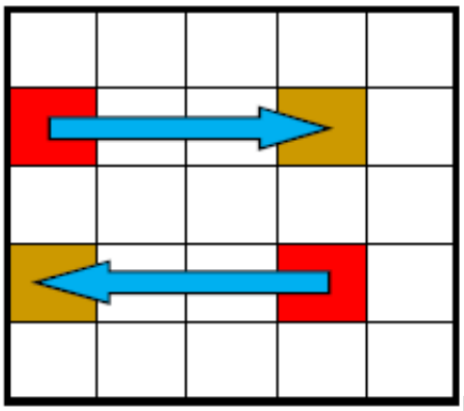
Hai kí tự cùng dòng

- Nếu 2 ký tự nằm cùng cột được thay thế bằng 2 ký tự bên • dưới. Ký tự ở hàng cuối cùng được thay thế bằng ký tự ở hàng trên cùng



Hai kí tự cùng cột

- Nếu 2 ký tự lập thành hình chữ nhật được thay thế bằng 2 ký tự tương ứng trên cùng dòng ở hai góc còn lại.



Hai kí tự tạo thành hình chữ nhật

8. Mã Hill

- Các ký tự được gán giá trị lần lượt là A = 01, B = 02, …, Z = 26.
- Chọn ma trận vuông Hill (ma trận H) làm khoá. Kích cỡ của ma trận tùy vào số lượng ký tự trong plaintext được mã hóa cùng lúc.
- Mã hoá từng chuỗi n ký tự trên plaintext (vector P) với n là kích thước ma trận vuông Hill: C = HP mod 26.
- Tương tự với việc giải mã: P = H−1C mod 26.

9. Phương pháp phá mã cổ điển

- Dựa vào đặc điểm ngôn ngữ.
- Dựa vào tần suất xuất hiện của các chữ cái trong bảng chữ cái thông qua thống kê chính thức.
- Dựa vào số lượng các ký tự trong bảng mã để xác định thông điệp gốc.

C. Giải thuật mã hóa hiện đại

- Mã hóa khóa đối xứng (vd như DES, AES): Sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã.
- Mã hóa bất đối xứng (vd như RSA, ECC): Sử dụng cặp khóa, gồm khóa công khai (public key) và khóa riêng tư (private key). Khóa công khai được chia sẻ với mọi người, trong khi khóa riêng tư được giữ bí mật.

1. Giải thuật mã hóa DES

- Dùng khoá có độ dài 56 bit để mã hoá các khối dữ liệu đầu vào 64 bit.
- Cả bên mã hóa lẫn bên giãi mã đều dung chung một khóa và DES thuộc vào hệ mã khóa bí mật
- Giải thuật DES được hiểu nhanh là như sau:
    - Sử dụng một khoá K tạo ra n khoá con K1, K2, …, Kn bằng giải thuật sinh khóa.
    - Hoán vị dữ liệu đầu tiên (Initial permutation).
    - Thực hiện mã hóa DES qua n vòng lặp. Tại mỗi vòng lặp:
        - Dữ liệu được tách thành hai phần.
        - Áp dụng các phép toán thay thế lên một phần, phần còn lại giữ nguyên.
        - Hoán vị hai phần cho nhau.
    - Hoán vị dữ liệu lần cuối (Final Permutation).

2. Giải thuật mã hóa AES

- Kích thước khối dữ liệu đầu vào là 128 bit tương ứng với 16 bytes.
- Kích thước khoá lần lượt là 128, 192, 256 bit (AES-128, AES-192, AES-256).
- Mỗi khoá con là một cột gồm 4 bytes.
- Mỗi khối dữ liệu đầu vào tạo thành một ma trận 4x4, gọi là ma trận trạng thái. Ma trận trạng thái này sẽ biến đổi trong quá trình thực hiện mã hoá.
- Các hàm thực hiện trong các vòng lặp của giải thuật:
    - Hàm SubBytes: mỗi byte trong state được thay thế với các byte khác, sử dụng một bảng look-up được gọi là S-box. S-box được dùng bắt nguồn từ hàm ngược trên trường GF(28).
- Hàm ShiftRows: các phần tử của hàng đầu tiên sẽ không thay đổi vị trí, hàng thứ hai dịch sang trái một cột, hàng thứ ba dịch sang trái hai cột, hàng cuối cùng sẽ dịch sang trái ba cột.
- Hàm MixColumns: mỗi cột được xem như một đa thức và được nhân modulo x4 + 1 với một biểu thức cố định c(x) = 3x3 + x2 + x + 2.
- Hàm AddRoundKey: mỗi byte trong bảng trạng thái được thực hiện phép XOR với một byte trong khoá con, từ đó sinh ra 1 khóa con mới.

3. Giải thuật mã hóa công khai RSA

- Thuật toán RSA có hai khóa:
    - khóa công khai (hay khóa công cộng).
    - khóa bí mật (hay khóa cá nhân).
- Cặp khóa RSA được sinh ra từ 2 số nguyên tố lớn ngẫu nhiên.
- Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa thông điệp, và thông điệp đó chỉ có thể được giải mã bằng khóa bí mật tương ứng.
- RSA hay được ứng dụng vào chữ ký điện tử bằng cách dùng khóa bí mật để ký chữ ký và dùng khóa công khai để xác minh chữ ký.
- Giải thuật RSA rất an toàn nhưng tốc độ mã hoá và giải mã chậm hơn giải thuật DES hàng ngàn lần.

- Do đó người ta kết hợp RSA với các giải thuật mã hóa khác bằng cách dùng RSA để mã hoá khoá mà các giải thuật khác đã dùng để mã hoá khối văn bản.

D. Bẻ gãy một hệ thống mật mã

Các khả năng tấn công trên hệ thống:

- Tấn công chỉ dựa trên chuỗi mật mã (ciphertext-only attack): đối phương chỉ biết một vài mẫu chuỗi mật mã c.
- Tấn công dựa trên văn bản đã biết (known-plaintext attack): đối phương đã biết độ dài đáng kể của văn bản gốc m và chuỗi mật mã c.
- Tấn công dựa trên văn bản được chọn (chosen-plaintext attack): đối phương đã có được một số lượng nhất định các cặp thông điệp và chuỗi mật mã tương ứng (m, c).
- Tấn công dựa trên chuỗi mật mã được chọn (chosen-ciphertext attack).
- Tấn công dựa trên khóa được chọn (chosen-key attack).
- Tấn công lựa chọn thích nghi bản mã (Adaptive chosen-ciphertext attack).
- Timing attack.
- Rubber hose attack.

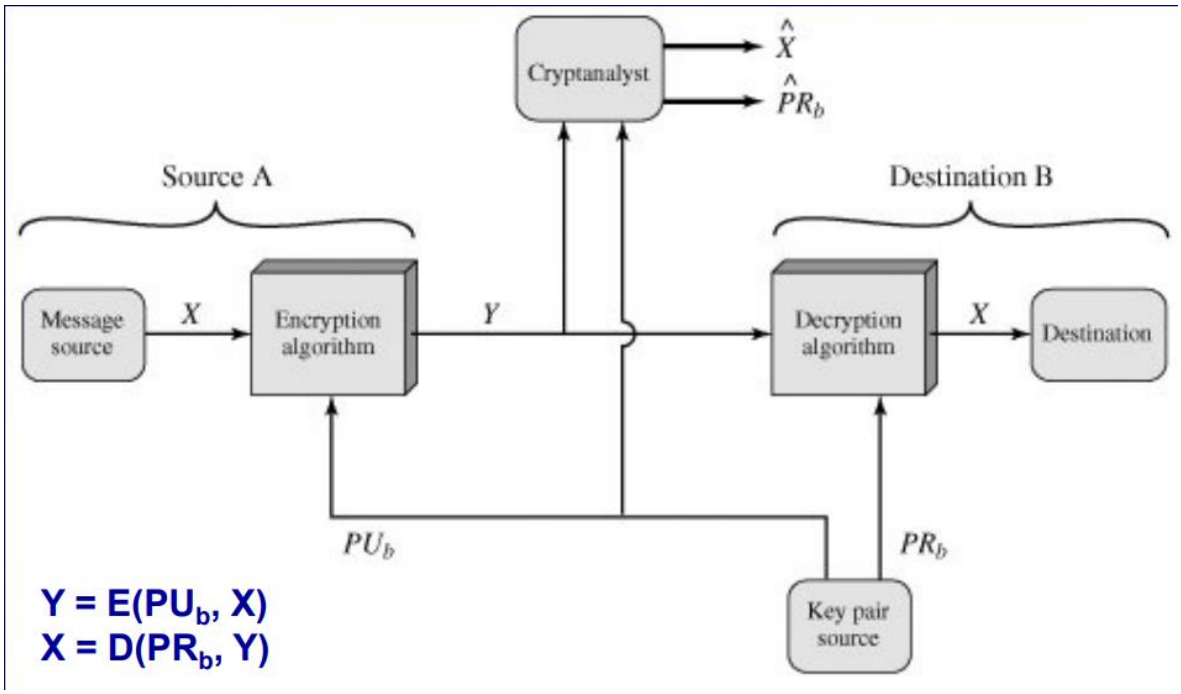
IV. Mã hóa công khai và quản lý khóa

A. Hệ mã hoá khoá công khai

- Các bước chủ yếu khi thực hiện mã hoá khoá công khai:
    1. Mỗi user tạo ra một cặp khoá được sử dụng cho việc mã hoá và giải mã thông điệp.
    2. Mỗi user sẽ công bố khoá công khai của mình lên cho mọi người biết. Khoá riêng sẽ được giữ kín.

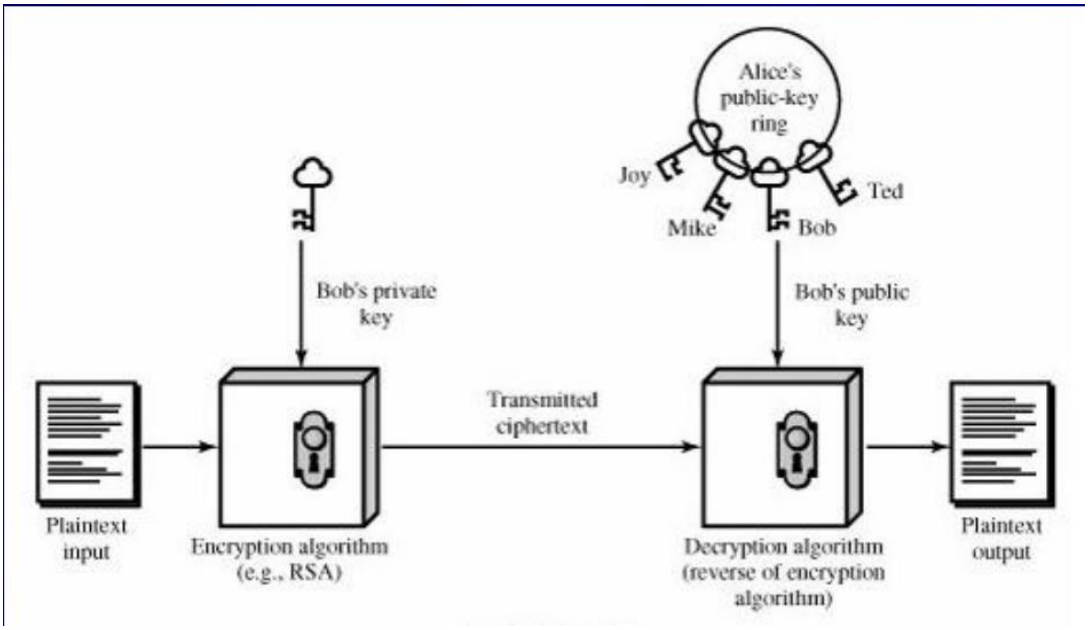
3. Nếu B muốn gửi một tin nhắn bí mật cho A, B mã hoá tin nhắn này bằng cách sử dụng khoá công khai của A.
4. Khi A nhận được tin nhắn, A giải mã nó bằng cách sử dụng khoá riêng của A. Không có ai khác có thể giải mã thông điệp bởi vì chỉ có A có khoá riêng của A.

- Ứng dụng:
    - Bảo mật (mã hoá/giải mã): một văn bản được mã hoá bằng khoá công khai của một người sử dụng thì chỉ có thể giải mã với khoá bí mật của người đó.



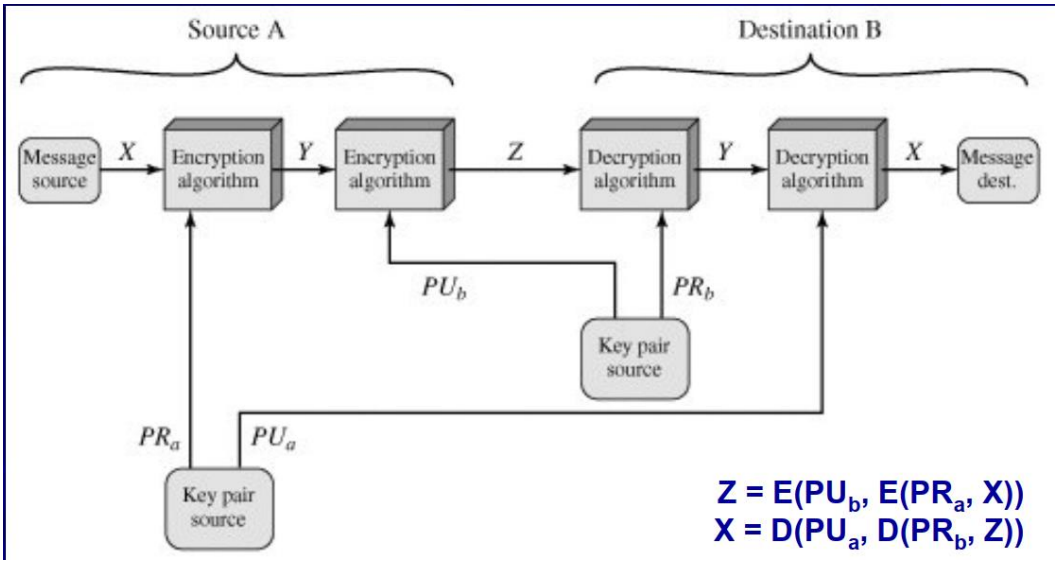
Secrecy

    - Chứng thực: Một người sử dụng có thể mã hoá văn bản với khoá bí mật của mình. Nếu một người khác có thể giải mã với khoá công khai của người gửi thì có thể tin rằng văn bản thực sự xuất phát từ người gắn với khoá công khai đó.



Authentication

- Trao đổi khoá: Hai bên hợp tác để trao đổi session key. Trước tiên, mã hoá thông điệp X sử dụng khoá bí mật của người gửi (cung cấp chữ ký số) để được Y. Kế đó, mã hoá tiếp Y với khoá công khai của người nhận. Chỉ có người nhận đã xác định trước mới có khoá bí mật của người nhận và khoá công khai của người gửi để giải mã hai lần để được X.



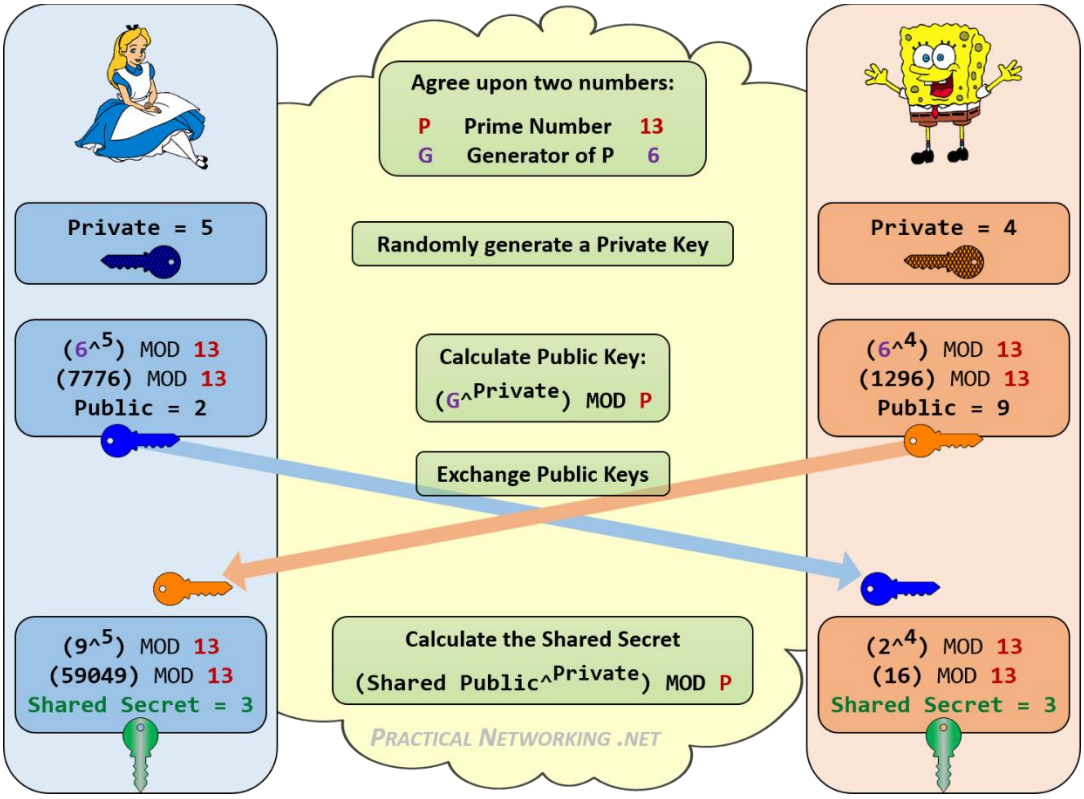
Authentication và Secrecy

- Một số giải thuật hệ mã hoá khoá công khai:
  - RSA: có cả 3 ứng dụng.
  - Elliptic Curve: có cả 3 ứng dụng.
  - Diffie-Hellman: chỉ có trao đổi khóa.

- DSS: chỉ có chứng thực.

B. Giao thức trao đổi khoá Diffie-Hellman

- Cho phép hai người dùng trao đổi khóa bí mật dùng chung trên mạng công cộng, sau đó có thể sử dụng để mã hóa các thông điệp.
- Thuật toán tập trung vào giới hạn việc trao đổi các giá trị bí mật, xây dựng dựa trên bài toán khó logarit rời rạc.
- Ví dụ:
  - A và B chọn số nguyên tố chung là p = 13 và phần tử sinh g là 6.
  - A tạo khóa bí mật $\mathbf{a}_{PK}$ = 5, và tính khóa công khai $\mathbf{a}_{PU}$ = 65 mod 13 = 2. rồi gửi cho B khóa công khai $\mathbf{a}_{PU}$.
  - B tạo khóa bí mật $\mathbf{b}_{PK}$ = 4, và tính khóa công khai $\mathbf{b}_{PU}$ = 64 mod 13 = 9. và rồi gửi cho A khóa công khai $\mathbf{b}_{PU}$.
  - Cả A và B đều tính được khóa chung K = 95 mod 13 = 24 mod 13 = 3



C. Hệ RSA

- Văn bản rõ được mã hóa ở dạng khối, kích cỡ của khối phải nhỏ hơn hoặc bằng log2(n).

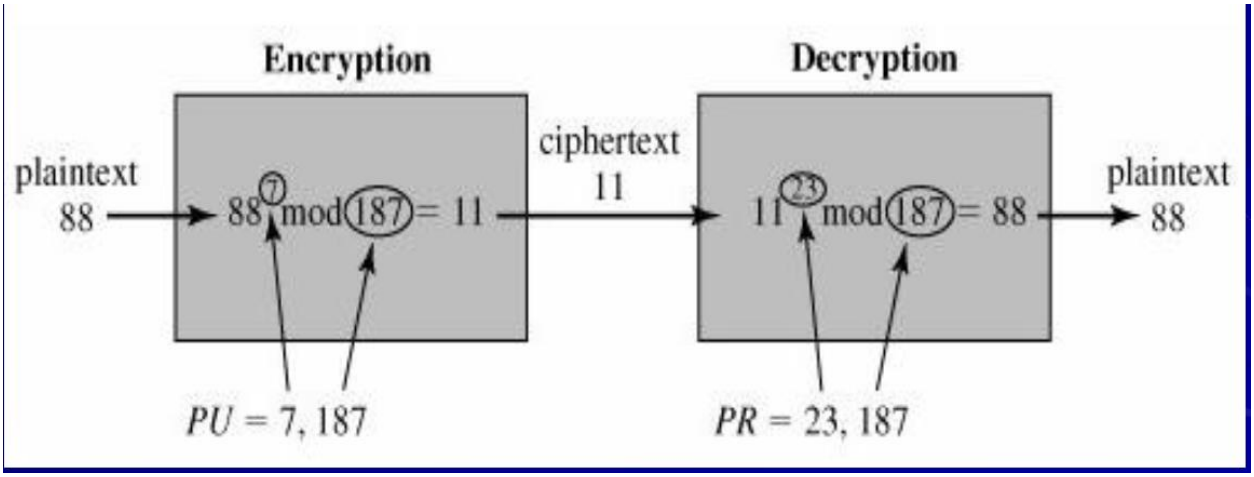
- Trong thực tế, kích thước khối là i bit, với $2^i < n <= 2^{i+1}$.
- Giải thuật:
    - Sinh cặp khóa:
        - Tạo ngẫu nhiên 2 số nguyên tố p và q
        - Tính n = p * q (công bố công khai)
        - Tính phi(n) = (p - 1) * (q - 1)
        - Chọn số nguyên e sao cho Ước số chung lớn nhất của e và phi n là 1 (người gửi biết) (**gcd (phi(n), e) = 1; 1 < e < phi(n**))
        - Tính $d = e^{-1}$ (mod phi (n)) = 1 (chỉ người nhận biết) ($ed \equiv 1 \pmod{(p-1)(q-1)}$)
        - Công thức để tính: d = (1 + x.phi(n))/ e với d và x là số nguyên
        - Khoá công khai là (e, n)
        - Khoá bí mật là (d, n)
    - Mã hóa: Thực hiện hàm mã hóa $c = m^e \bmod n$
    - Giải mã: Thực hiện hàm giải mã $m = c^d \bmod n = (m^e)^d \text{ mode } n = m^{ed} \bmod n$
- Các yêu cầu sau đây phải được đáp ứng:
    - Các giá trị của e, d, n phải thỏa mãn sao cho $m^{ed} \bmod n = m$, với m < n.
    - Phải dễ dàng tính toán được $m^e \bmod n$ và c^d cho tất cả các giá trị của m < n.
    - Không khả thi để xác định d khi cho e và n.
    - p và q phải là các số nguyên tố rất lớn để không thể phân tích được n = p * q.

Mã hóa:

- Phaintext: m < n
- Ciphertext: $C = m^e \bmod n$

Giải mã:

- Ciphertext: C
- Plaintext: $m = C^d \bmod n$



D. Quản lý khoá

1. Thẩm quyền thu hồi khoá

- Thu hồi khoá khi khoá bị sai sót hoặc có tính phá hoại.
- Thường được tham gia bởi từ hai thực thể trở lên.
- Cần đảm bảo:
    - Càng nhiều bên tham gia càng tốt (chống phá hoại).
    - Càng ít bên tham gia càng tốt (thu hồi nhanh).

2. Phân phối khoá mới

- Phải phân phối khoá mới sau khi khoá cũ bị thu hồi nhằm đảm bảo hệ thống tiếp tục hoạt động một cách an toàn.
- Giảm thời gian giữa thời điểm thu hồi khoá và thời điểm phân phối khoá mới tới mức tối thiểu.
- Phải đảm bảo yêu cầu về an ninh và yêu cầu về tính sẵn sàng của hệ thống.

3. Thông báo thông tin về thu hồi khoá

- Thông báo về một khóa nào đó bị thu hồi cần đến được tất cả những người đang sử dụng nó trong thời gian ngắn nhất có thể.
- Có 2 cách thông báo:
    - Thông tin được chuyển từ trung tâm tới người dùng.
    - Người dùng lấy thông tin từ trung tâm.
- Cung cấp các chứng thực có thời hạn.

4. Các biện pháp thực hiện khi lộ khoá

- Hầu hết các trường hợp thu hồi khoá xảy ra khi khoá bí mật đã bị lộ. Hai khả năng xảy ra:
    - Các văn bản mã hóa với khóa công khai sau thời điểm T không còn được xem là bí mật.
    - Các chữ ký số thực hiện với khóa bí mật sau thời điểm T không còn được xem là thật.
- Cần xác định người có quyền thu hồi khóa, cách thức truyền thông tin tới người dùng, cách thức xử lý các văn bản mã hóa với khóa bị lộ.

V. Chứng thực dữ liệu

A. Tổng quan

1. Vai trò:

- **Chứng thực** (authentication) nhằm:
    - Xác nhận nguồn gốc dữ liệu
    - Thuyết phục người dùng là dữ liệu này chưa bị sửa đổi hay giả mạo
- Chứng thực là cơ chế quan trọng để duy trì tính toàn vẹn và không thể từ chối của dữ liệu.

2. Các phương pháp:

- **Mã hóa thông điệp:** sử dụng khóa bí mật và khóa công khai để mã hóa thông điệp
- **Mã chứng thực thông điệp** (MAC – Message Authen Code): một hàm và một khóa bí mật tạo ra 1 giá trị có chiều dài cố định sử dụng để chứng thực
- **Hàm băm** (Hash function): Ánh xạ một thông điệp vào một giá trị băm có chiều dài cố định để chứng thực.

4. Ví dụ về chứng thực:

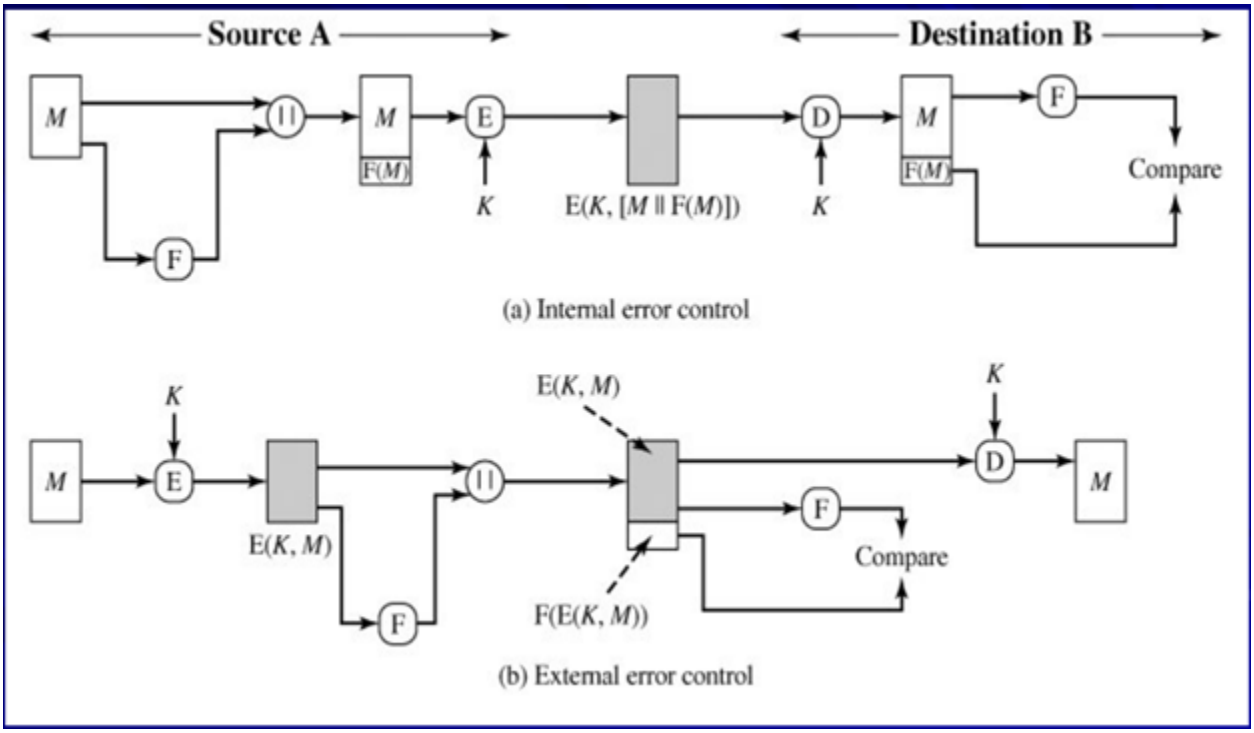
- Giả sử Alice và Bob chia sẻ một khoá bí mật chung **K**. Alice muốn gởi một chuỗi dữ liệu **M** cho Bob và thuyết phục Bob rằng **M** thực sự đến từ Alice và không bị sửa trong quá trình truyền. Điều này có thể thực hiện như sau:
- Alice gởi **M** cùng với **C** cho Bob, với **C=EK(M) và E** là một giải thuật mã hoá thông thường đã quy ước trước giữa Alice và Bob.
- Do chỉ có Alice và Bob biết **K**, Bob có thể sử dụng **K** để giải mã **C** thu được **M'**.
- Bob sẽ được thuyết phục rằng **M** thực sự đến từ Alice và **M** không bị thay đổi trong quá trình truyền nếu và chỉ nếu **M'=M**.

- Tuy nhiên, phương pháp này cho phép Alice có thể từ chối Charlie rằng **M** xuất phát từ Alice vì **M** có khả năng xuất phát từ Bob do cùng chia sẻ khoá bí mật **K**. → Nhược điểm này được giải quyết bằng mật mã hoá khoá công khai.
- Nếu chuỗi **M** ngắn, có thể mã hóa **M** trực tiếp để xác nhận nó.
- Nếu chuỗi **M** dài, chỉ cần tính toán một h ngắn đại diện cho **M** và mã hóa **h**.

Vậy h được tạo ra như thế nào?

- **h** được tạo ra mà không sử dụng khoá bí mật được gọi là digital digest hoặc digital fingerprint (dấu vân tay kỹ thuật số), có thể thu được từ một hàm băm (Hash Function).
- **h** được tạo ra bằng cách sử dụng một khoá bí mật được gọi là một mã xác thực thông điệp (MAC – Message Authentication Code).
- **h** cũng có thể thu được bằng cách sử dụng giải thuật checksum kết hợp một hàm băm để tạo ra một mã xác thực tin nhắn keyed-hash (HMAC - Keyed-Hash Message Authentication Code)

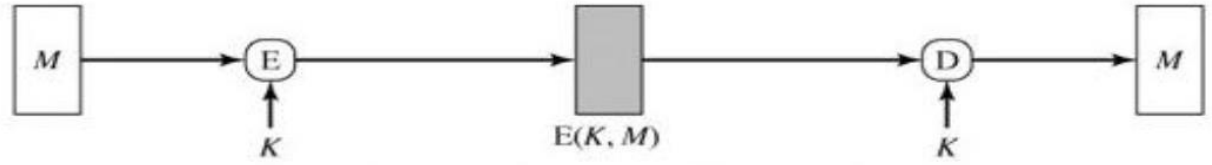
5. Điều khiển lỗi khi gởi thông điệp



- **a) Kiểm soát lỗi nội bộ**
- **b) Kiểm soát lỗi bên ngoài**
- **Giải thích kí hiệu:**
    - M : Message, là thông điệp

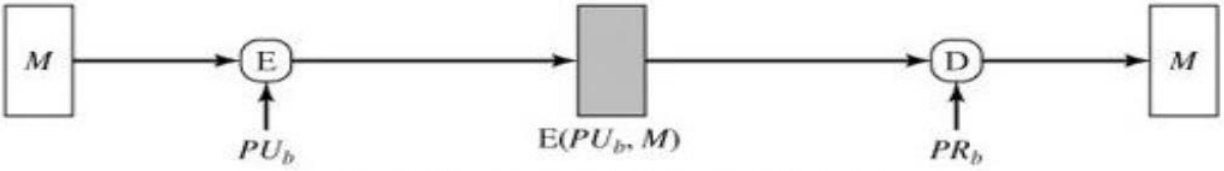
- E : Encrypt, là hàm mã hóa
- D : Decrypt, là hàm giải mã
- K : Khóa
- F(M) : là hàm băm của dữ liệu M đầu vào
- II: Phép nối, dùng để nối 2 chuỗi kí tự, chuỗi bên dưới dùng để kiểm tra sau khi bên kia giải mã M

6. Các công dụng cơ bản của mã hóa



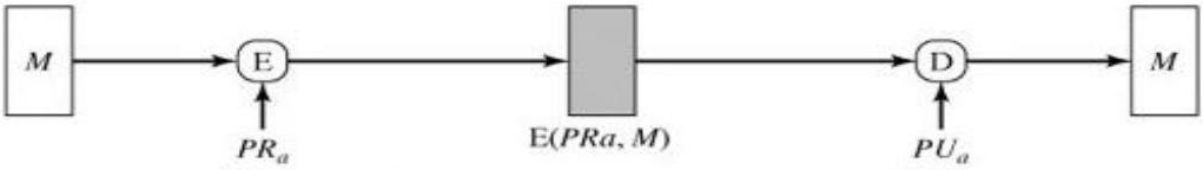
(a) Symmetric encryption: confidentiality and authentication

Bảo mật và xác thực



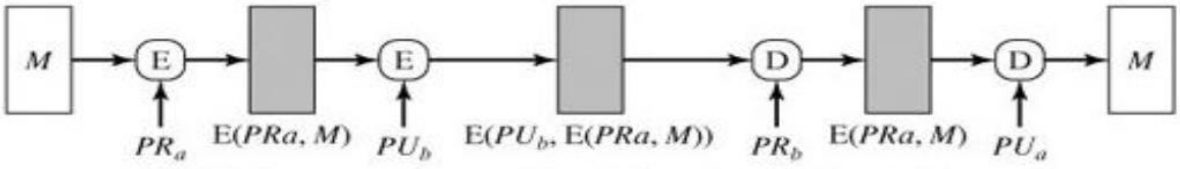
(b) Public-key encryption: confidentiality

Bảo mật



(c) Public-key encryption: authentication and signature

Xác thực và chữ kí số



(d) Public-key encryption: confidentiality, authentication, and signature

Bảo mật, xác thực và chữ kí số

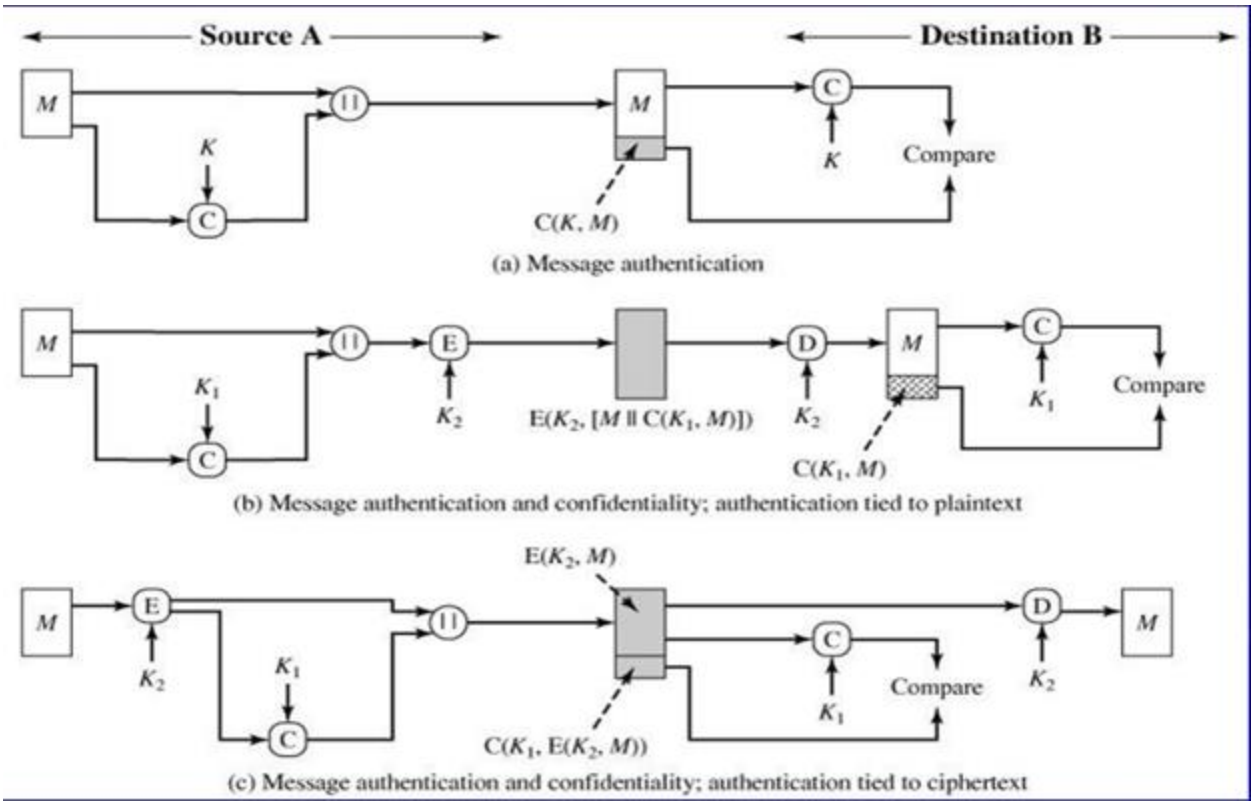
- **Giải thích kí hiệu**
    - PU : public key , khóa công khai
    - PR : Private key, khóa bí mật
    - A : bên gửi
    - B : bên nhận
    - Các kí hiệu còn lại(xem lại ở trên)
- **a) Mã hoá khoá đối xứng (khoá bí mật):**
    - Bảo mật: chỉ A và B chia sẻ K
    - Chứng Thực:
        - Có thể đến chỉ từ A
        - Không thay đổi trong quá trình truyền
        - Yêu cầu một số định dạng và dự phòng
    - Không cung cấp chữ ký:
        - Người nhận có thể giả mạo thông điệp
        - Người gửi có thể phủ nhận thông điệp
- **b) Mã hoá khoá bất đối xứng (khoá công khai)**
    - A → B: $E(PU_b, M)$
    - Bảo mật:
        - Chỉ B có PR_b giải mã
    - Không cung cấp chứng thực
        - Bất cứ ai cũng có thể sử dụng PU_b để mã hoá thông điệp và tự xưng là A.
- **c) Mã hóa khóa công khai: chứng thực và chữ ký số:**
    - A → B: $E(PR_a, M)$
    - Cung cấp chứng thực và chữ ký số
        - Chỉ A có PRa để mã hoá
        - Không bị thay đổi trong quá trình truyền
        - Yêu cầu một số định dạng và dự phòng
        - Bất kỳ ai cũng có thể sử dụng PUa để xác minh chữ ký số
- **d. Mã hoá khoá công khai: bảo mật, chứng thực, và chữ ký số**

- A → B: E(PUb, E(PRa, M))
- Cung cấp bảo mật nhờ PUb.
- Cung cấp chứng thực và chữ ký số nhờ PRa.

B. Mã chứng thực thông điệp

1. Khái niệm:

- Là một **kỹ thuật chứng thực** liên quan đến việc sử dụng một khoá bí mật để tạo ra một khối dữ liệu có kích thước nhỏ cố định (checksum hoặc MAC) và được thêm vào thông điệp.
- Kỹ thuật này giả sử rằng 2 phía tham gia truyền thông là A và B chia sẻ một khoá bí mật K. Khi A có một thông điệp gởi đến B, A sẽ tính toán MAC như là một hàm của thông điệp và khoá: MAC=C(K, M), với:
  - M: thông điệp đầu vào có kích thước biến đổi
  - C: hàm MAC
  - K: khoá bí mật chia sẻ giữa người gởi và người nhận
- Thông điệp cộng với MAC được truyền tới người nhận. Người nhận thực hiện các tính toán tương tự trên các thông điệp đã nhận sử dụng cùng một khóa bí mật, để tạo ra một MAC mới.
- MAC vừa tạo sẽ được so với MAC nhận. Giả sử chỉ người nhận và người gửi biết khóa bí mật:
  - Nếu MAC nhận phù hợp với MAC vừa tính thì thông điệp không bị thay đổi trong quá trình truyền và chắc chắn được gởi tới từ người gởi đã biết.
  - Nếu MAC nhận khác với MAC vừa tính thì thông điệp đã bị thay đổi hoặc bị giả mạo và được gởi từ attacker
- MAC: mã chứng thực thông điệp có chiều dài cố định Chiều dài thông thường của MAC: 32..96 bit. Để tấn công cần thực hiện 2n lần thử với n là chiều dài của MAC (bit)
- Chiều dài thông thường của khoá K: 56..160 bit Để tấn công cần thực hiện 2k lần thử với k là chiều dài của khoá K (bit).
- **Ứng dụng trong:**
  - Banking: sử dụng MAC kết hợp triple-DES
  - Internet: sử dụng HMAC và MAC kết hợp AES



- **a. Chứng thực**
  - A → B: M II C(K, M)
  - Chứng thực: chỉ A và B chia sẻ K
- **b. Chứng thực và bảo mật: chứng thực gắn liền với plaintext**
  - A → B: E(K2, [M II C(K, M)])
  - Chứng thực: chỉ A và B chia sẻ K1
  - Bảo mật: chỉ A và B chia sẻ K2
- **c. Chứng thực và bảo mật: chứng thực gắn liền với ciphertext**
  - A → B: E(K2, M) II C(K1, E(K2, M))
  - Chứng thực: sử dụng K1
  - Bảo mật: sử dụng K2

2. Khả năng bị bruteforce:

- Sử dụng khóa bí mật (hoặc khóa công khai) -> mất 2^(k-1) lần thử cho một khóa k bit. Nếu biết cyphertext C (P_i=D(K_i,C)) -> cần thử với tất cả K_i đến khi nào P_i có plaintext chấp nhận được.

- Sử dụng MAC -> Giả sử k>n (kích thước khoá lớn hơn kích thước MAC) và MAC1 = C(K, M1), việc thám mã phải thực hiện $MAC_i = C(K_i, M_1)$ với tất cả các giá trị có thể của K_i. Ít nhất có một khoá đảm bảo $MAC_i = MAC_1$
- Lưu ý rằng sẽ có 2k MACs được tạo ra nhưng chỉ có 2n < 2k giá trị MAC khác nhau. Do đó, một số khoá sẽ tạo ra các MAC chính xác và attacker không có cách nào để biết được đó là khoá nào. Trung bình, có 2k/2n = 2(k-n) khoá được tạo ra và attacker phải lặp đi lặp lại các cuộc tấn công.

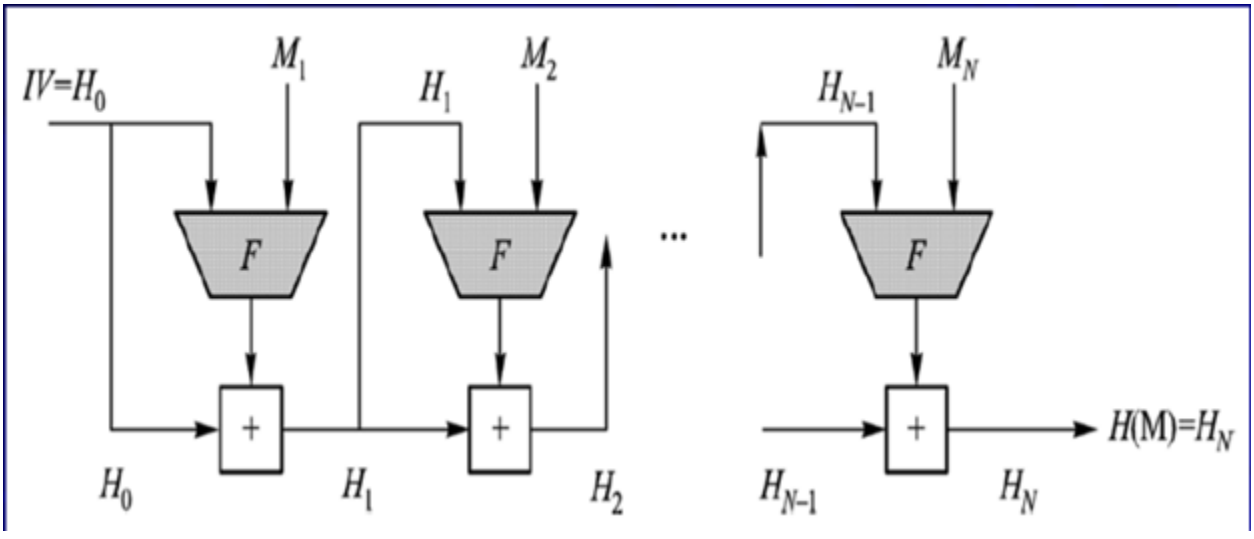
C. Hàm băm

1. Khái niệm

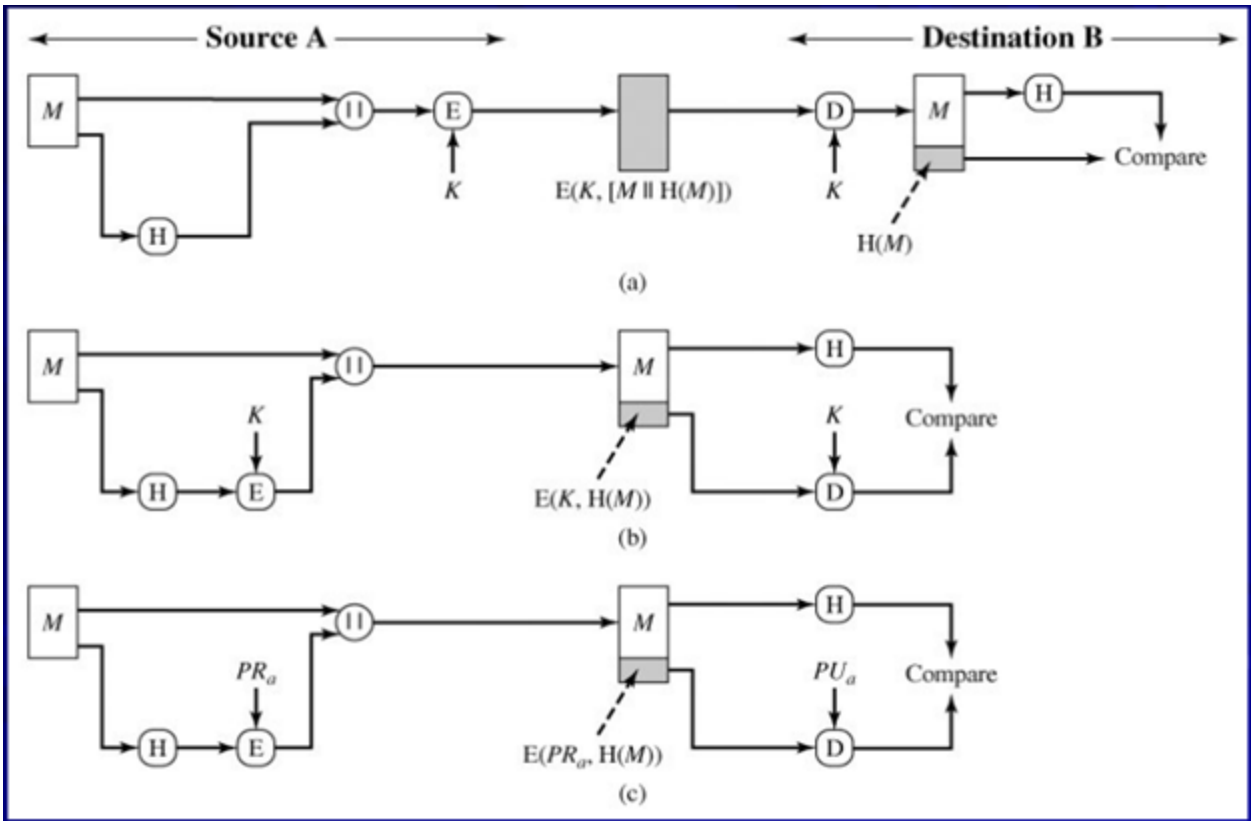
- Một hàm băm nhận một chuỗi dài ở đầu vào, ngắt nó thành nhiều mảnh, trộn lẫn chúng và tạo ra một chuỗi mới với chiều dài ngắn.
- Lưu ý: Không phải mọi hàm băm đều thích hợp cho việc tạo ra một dấu vân tay kỹ thuật số.
- Để sinh ra một dấu vân tay kỹ thuật số tốt, H cần phải có:
    - Thuộc tính một chiều (one-way property)
    - Thuộc tính duy nhất.

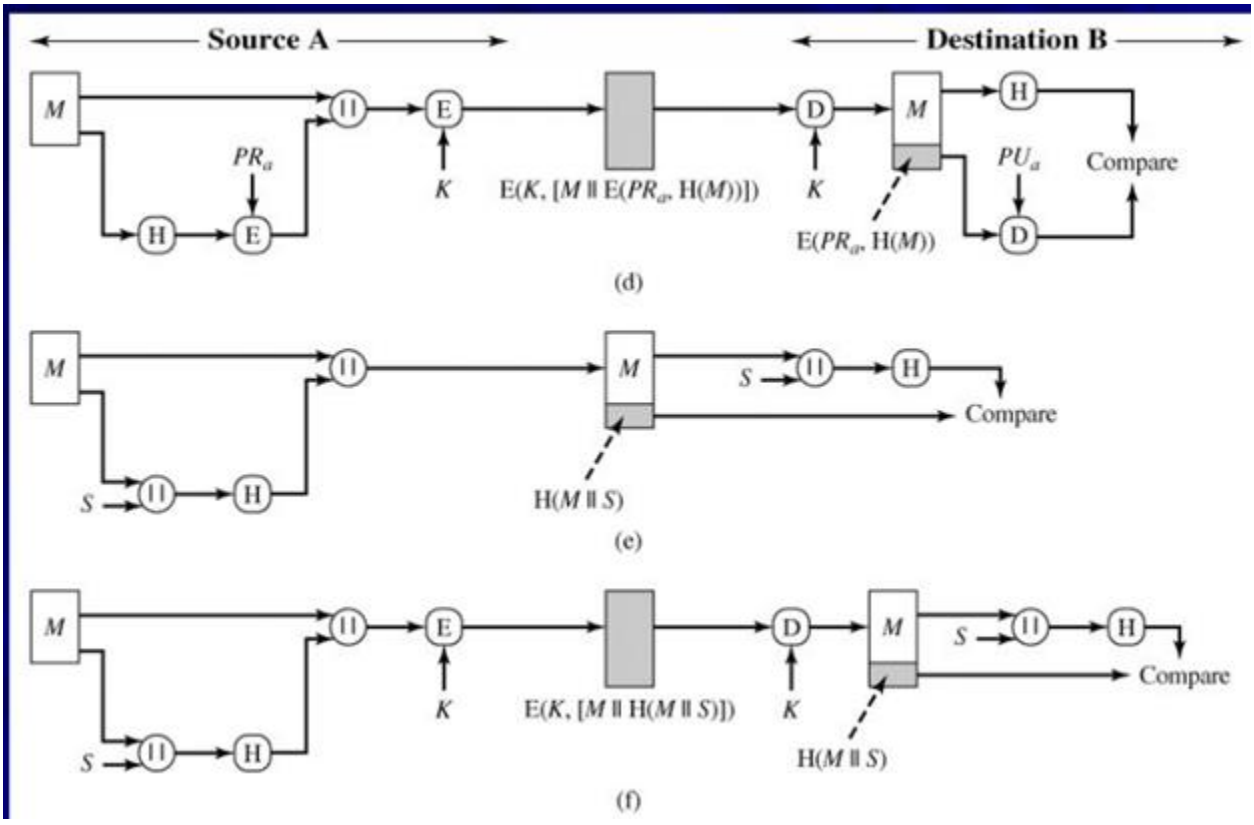
2. Cấu trúc cơ bản Hàm băm

- Trung tâm của cấu trúc cơ bản này là một hàm nén. Các giải thuật băm khác nhau sử dụng những hàm nén khác nhau.
- Trong cấu trúc cơ bản này, M là khối rõ, IV là một vector khởi tạo, F là một hàm nén, + là một số dạng của toán tử cộng modular.



3. Các công dụng của hàm băm


Source A
Destination B
M
H
E
K
E(K, [M || H(M)])
D
M
H
Compare
H(M)
(a)
M
K
H
E
M
H
K
Compare
D
E(K, H(M))
(b)
M
PRa
H
E
M
H
PUa
Compare
D
E(PRa, H(M))
(c)


Source A
Destination B
M
PRa
H
E
K
E(K, [M || E(PRa, H(M))])
D
M
H
PUa
Compare
E(PRa, H(M))
(d)
M
S
H
M
S
Compare
H(M || S)
(e)
M
S
H
K
E(K, [M || H(M || S)])
D
M
S
H
Compare
H(M || S)
(f)

- **Sơ đồ (a) - Mã hoá thông điệp cộng với mã băm**
    - A → B: E(K, [M II H(M)])
    - Bảo mật: chỉ A và B chia sẻ K
    - Chứng thực: H(M) được bảo vệ bằng mật mã
- **Sơ đồ (b) - Mã hoá mã băm chia sẻ với khoá bí mật**
    - A → B: M II E(K, H(M))
    - Chứng thực: H(M) được bảo vệ bằng mật mã
- **Sơ đồ (c) - Mã hoá khoá bí mật với mã băm của người gởi**
    - A → B: M II E(PRA, H(M))
    - Chứng thực và chữ ký số:
        - H(M) được bảo vệ bằng mật mã
        - Chỉ A có thể tạo E(PRA, H(M))
- **Sơ đồ (d) - Mã hoá kết quả của (c) với khoá bí mật chia sẻ**
    - A → B: E(K, [M II E(PRA, H(M))])
    - Bảo mật: chỉ A và B chia sẻ K
    - Chứng thực và chữ ký số
- **Sơ đồ (e) - Tính mã băm của thông điệp cộng với trị bí mật**
    - A → B: M II H(M II S)
    - Chứng thực: chỉ A và B chia sẻ S
- **Sơ đồ (f) - Mã hoá kết quả của (e)**
    - A → B: E(K, [M II H(M II S)])
    - Chứng thực: chỉ A và B chia sẻ S
    - Bảo mật: chỉ A và B chia sẻ K

4. Giới thiệu về các hàm băm

- **MD5:** (Message-Digest algorithm 5) là một hàm băm mật mã với giá trị băm dài 128 bit diễn tả bởi một số thập lục phân 32 ký tự (RFC 1321).Được dùng chủ yếu để kiểm tra tính toàn vẹn của tập tin trên nguyên tắc hai dữ liệu vào X và Y hoàn toàn khác nhau thì xác suất để có cùng một md5 hash giống nhau là rất nhỏ.
- **SHA** (Secure Hash Algorithm – Giải thuật băm an toàn) .Giải thuật an toàn:Cho một giá trị băm nhất định được tạo nên bởi một trong những giải thuật SHA, việc tìm lại được đoạn dữ liệu gốc

là không khả thi. Bất cứ thay đổi nào trên đoạn dữ liệu gốc, dù nhỏ, cũng sẽ tạo nên một giá trị băm hoàn toàn khác với xác xuất rất cao.

- **SHA có 2 phiên bản:**
    - **SHA-1:** : trả lại kết quả dài 160 bit. Được sử dụng rộng rãi để thay thế MD5 trong nhiều ứng dụng và giao thức bảo mật khác nhau, bao gồm TLS, SSL, PGP, SSH, S/MIME, IPSec
    - **SHA-2:** có 4 giải thuật: trả lại kết quả dài 224, 256, 384, và 512 (y = 512 và R= 2^128 -1)

D. Chữ ký số

1. Sử dụng khoá công khai để tạo chữ ký số:

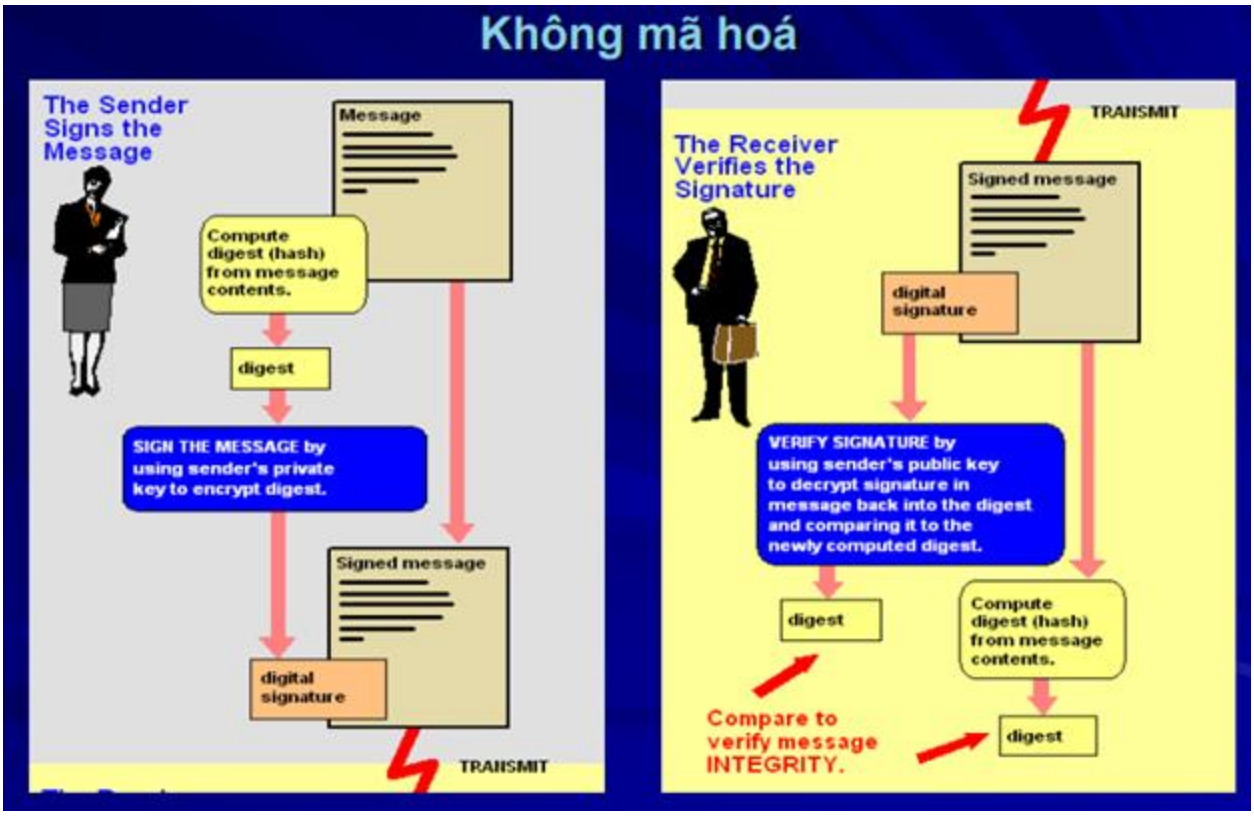
- Giả sử A cần gởi cho B một thông điệp mật kèm chữ ký điện tử, A sẽ sử dụng khoá công khai của B để mã hoá thông điệp rồi dùng khoá cá nhân của mình để mã hoá chữ ký, sau đó gởi cả thông điệp lẫn chữ ký cho B. B sẽ dùng khoá công khai của A để giải mã chữ ký, rồi dùng khoá cá nhân của mình để giải mã thông điệp của A.
- Việc tạo chữ ký và kiểm chứng chữ ký thường được thực hiện nhờ hàm băm.

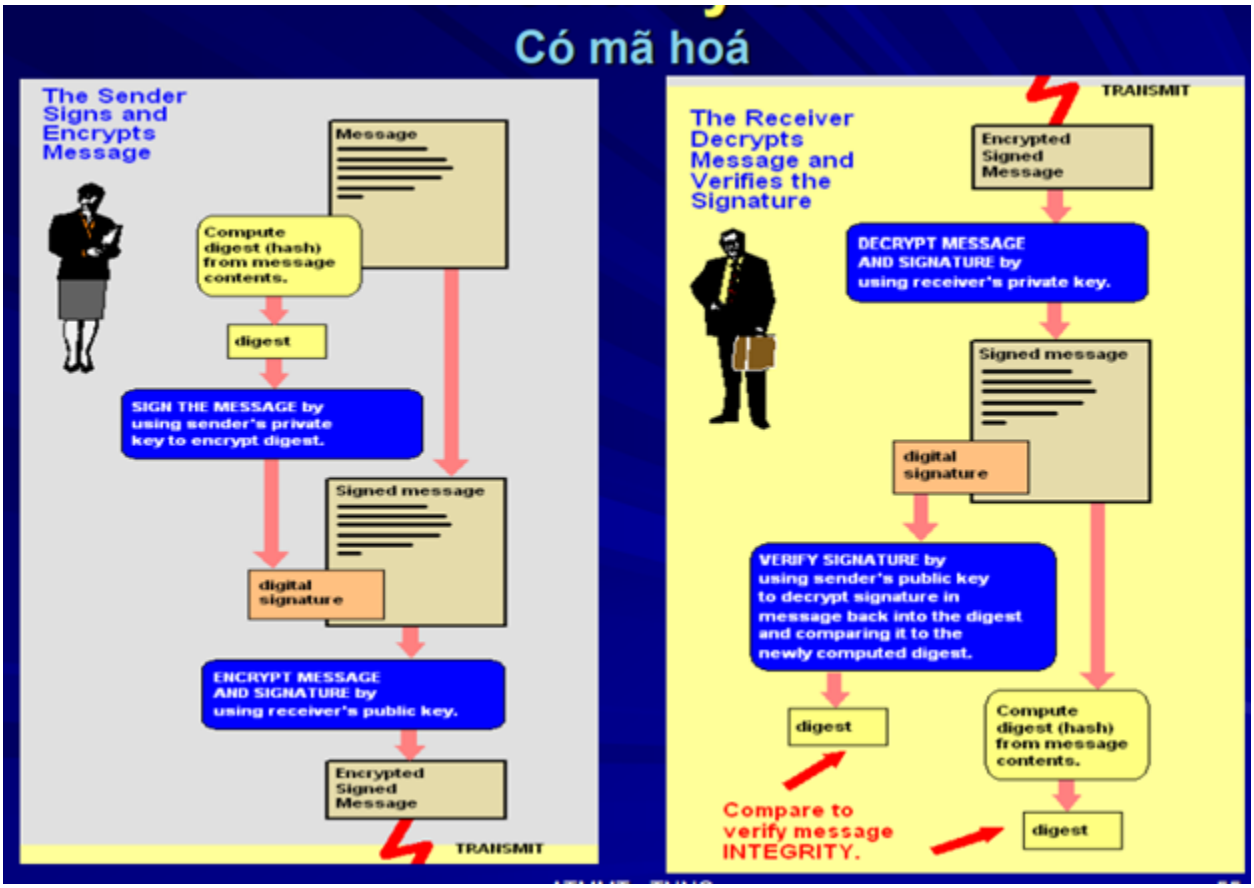
2. Ký vào thông điệp:

- Dùng giải thuật băm để thay đổi thông điệp cần truyền đi để được một **message digest** (MD5 thu được digest có chiều dài 128-bit hoặc SHA thu được digest 160-bit).
- Sử dụng khóa private key của người gửi để mã hóa **message digest** thu được ở bước trên. Bước này thường dùng giải thuật RSA. Kết quả thu được gọi là **digital signature** của thông điệp ban đầu. Gộp **digital signature** vào thông điệp ban đầu ("ký nhận" vào thông điệp). Sau đó, mọi sự thay đổi trên message sẽ bị phát hiện. Việc ký nhận này đảm bảo người nhận tin tưởng thông điệp này xuất phát từ người gửi chứ không phải là ai khác.
- **Các bước kiểm tra:**
    - Dùng **public key** của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của thông điệp
    - Dùng **giải thuật (MD5 hoặc SHA) băm** thông điệp nhận được. So sánh kết quả thu được ở bước 1 và 2. Nếu trùng nhau, ta kết luận thông điệp này không bị thay đổi trong quá trình truyền và thông điệp này là của người gửi.

Lưu ý:

- Có mã hóa sẽ có Dòng Encrypt và Decrypt
- Không mã hóa ta sẽ không thấy có dòng Encrypt và Decrypt


Không mã hoá
The Sender Signs the Message
Message
Compute digest (hash) from message contents.
digest
SIGN THE MESSAGE by using sender's private key to encrypt digest.
Signed message
digital signature
TRANSMIT
The Receiver Verifies the Signature
TRANSMIT
Signed message
digital signature
VERIFY SIGNATURE by using sender's public key to decrypt signature in message back into the digest and comparing it to the newly computed digest.
digest
Compute digest (hash) from message contents.
Compare to verify message INTEGRITY.
digest


Có mã hoá
The Sender Signs and Encrypts Message
Message
Compute digest (hash) from message contents.
digest
SIGN THE MESSAGE by using sender's private key to encrypt digest.
Signed message
digital signature
ENCRYPT MESSAGE AND SIGNATURE by using receiver's public key.
Encrypted Signed Message
TRANSMIT
The Receiver Decrypts Message and Verifies the Signature
TRANSMIT
Encrypted Signed Message
DECRYPT MESSAGE AND SIGNATURE by using receiver's private key.
Signed message
digital signature
VERIFY SIGNATURE by using sender's public key to decrypt signature in message back into the digest and comparing it to the newly computed digest.
digest
Compute digest (hash) from message contents.
Compare to verify message INTEGRITY.
digest

VI. Giao thức bảo mật mạng

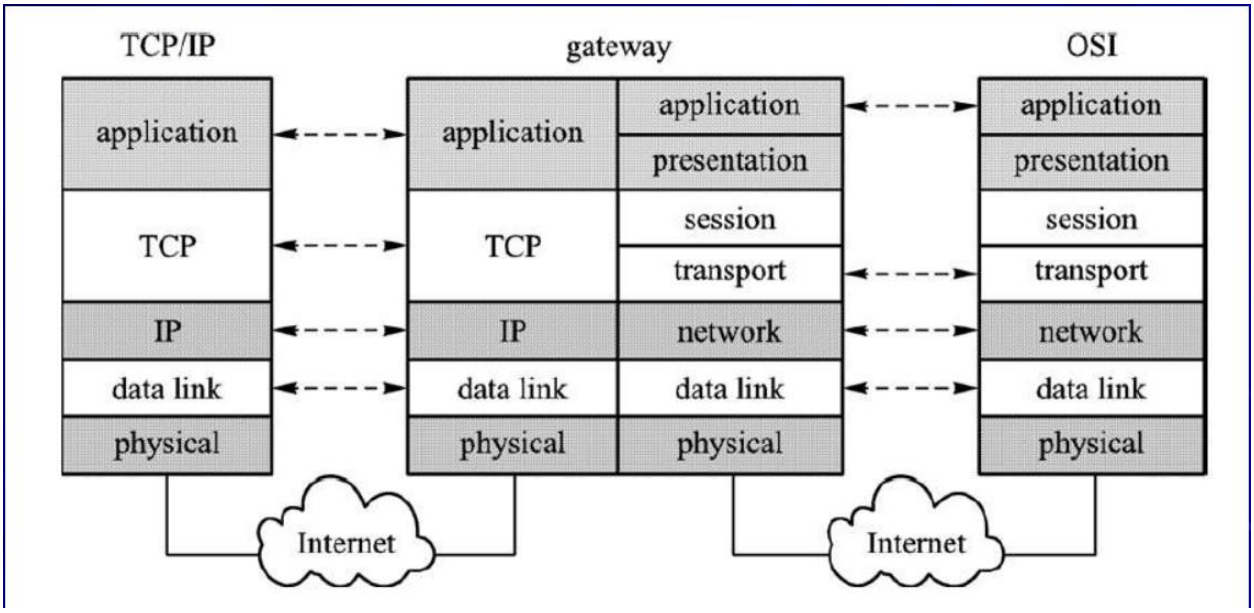
A. Vị trí của mật mã trong mạng máy tính

- **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
- Sử dụng các giải thuật mã hóa ở các lớp khác nhau sẽ cung cấp các mức độ bảo vệ khác nhau
- **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)

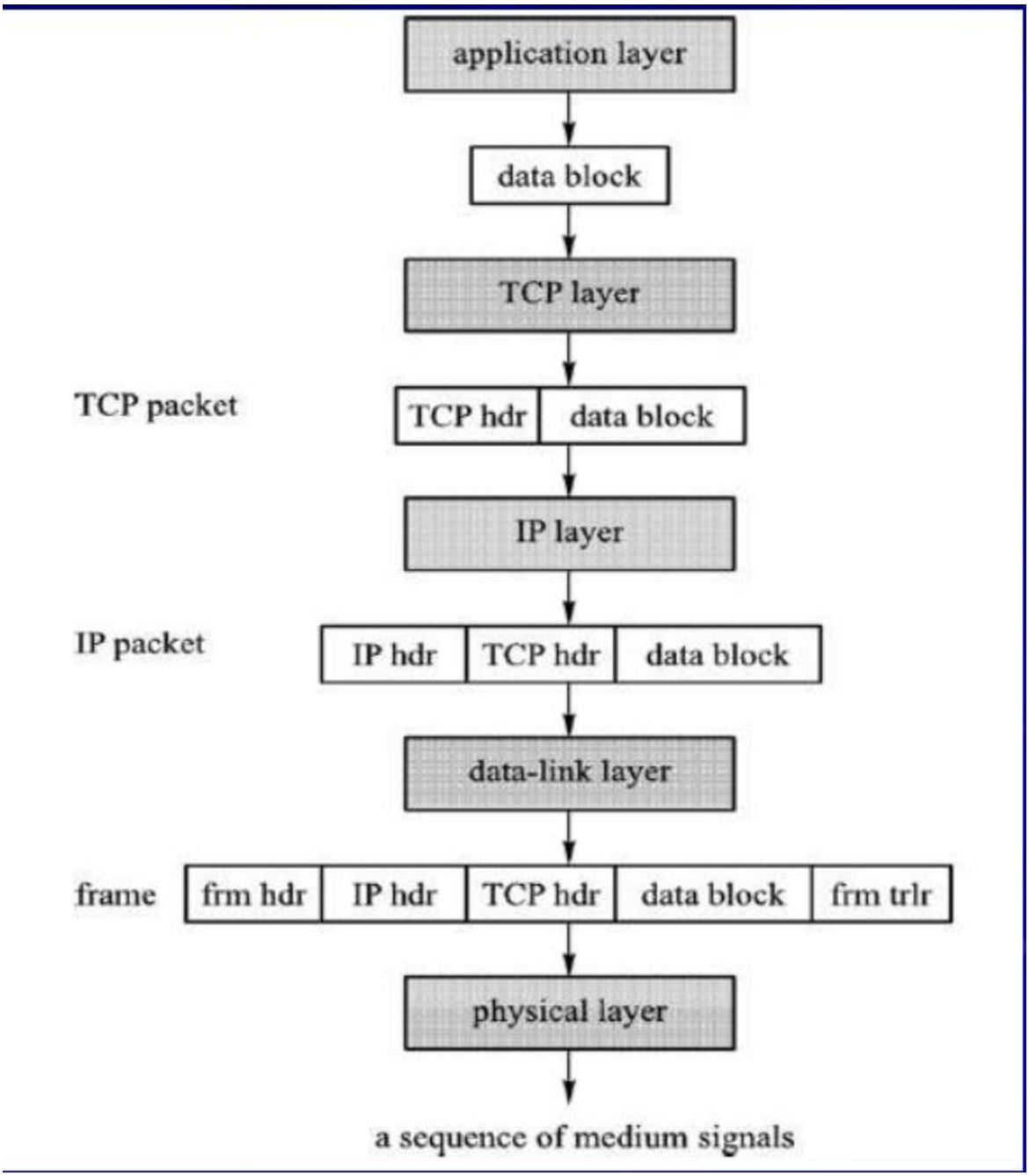
Các loại kết nối	**Riêng Tư/Mã hóa**	**Chứng thực**	**Ký/Toàn vẹn dữ liệu**
Nhân viên nội bộ hoặc từ xa truy cập đến server	SSL 2.0 hoặc 3.0 (cung cấp bởi secure Server ID)	- Server chứng thực bởi Server ID - Ký vào văn bản, S/MIME sử dụng Client ID	Client chứng thực bởi mật khẩu hoặc bởi SSL 3.0 với 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

Các loại kết nối	Riêng Tư/Mã hóa	Chứng thực	Ký/Toàn vẹn dữ liệu
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

1. Sự Tương Ứng giữa kiến trúc TCP/IP và mô hình OSI:



2. Mô hình đóng gói và mã hóa dữ liệu tại các lớp mạng:



- **Mã hóa tại lớp ứng dụng:**
    - Bảo mật end-to-end
    - Dữ liệu được mã hóa sẽ tiếp tục đi qua các lớp khác như bình thường.
    - Khi đến TCP Header và IP Header sẽ không mã hóa (do việc mã hóa nằm ở các lớp dưới) -> vì thế attacker có thể phân tích và sửa chữa nội dung.
    - Ví dụ: có thể thay đổi IP đích trong IP header để phân phối gói tin đến nơi khác.
- **Mã hoá tại lớp vận chuyển(Transport Layer):**

    - Cung cấp sự an toàn cho gói TCP
    - Có thể mã hóa phần payload hoặc cả gói tin (header và payload)
    - không ảnh hưởng đến dữ liệu trước đó
    - Tuy nhiên IP header không được mã hóa -> attacker có thể thu được sequence number để tấn công.
- **Mã hoá tại lớp mạng (Network Layer):**
    - Bảo mật link-to-link
    - Mã hóa cả gói tin(payload + header)
    - Không ảnh hưởng định tuyến
    - Được xem như ứng dụng của tunnel - mode
- **Mã hoá tại lớp liên kết dữ liệu (Data-Link Layer):**
    - Cung cấp bảo mật cho các frames
    - Mã hóa payload của frame
    - Việc mã hoá tại lớp liên kết dữ liệu(xem thêm bài 7)
- **Công nghệ vi mạch tích hợp ứng dụng(ASIC):**
    - Áp dụng các giải thuật lên ASIC:
    - Tầng ứng dụng: Thực hiện bởi phần mềm
    - Tầng Data-link: Thực hiện bởi phần cứng
    - Tại các tầng khác: một trong 2 hoặc cả 2
    - Mã hóa sử dụng phần cứng sẽ tiêu hao tài nguyên nhiều hơn nhưng hiệu suất sẽ tốt hơn so với phần mềm
- Các giải thuật mã hoá có thể được thực hiện trên phần mềm hoặc trên phần cứng sử dụng công nghệ vi mạch tích hợp ứng dụng (Application Specific Integrated Circuit – ASIC).
    - Tại lớp ứng dụng: được thực hiện bởi phần mềm.
    - Tại lớp liên kết dữ liệu: được thực hiện bởi phần cứng.
    - Tại các lớp khác: được thực hiện bởi phần mềm hoặc phần cứng hoặc cả hai.
    - Việc triển khai mã hoá được thực hiện bởi phần cứng có hiệu suất cao nhất nhưng chi phí cao và kém linh hoạt khi cần thay đổi

B. Cơ sở hạ tầng khoá công khai

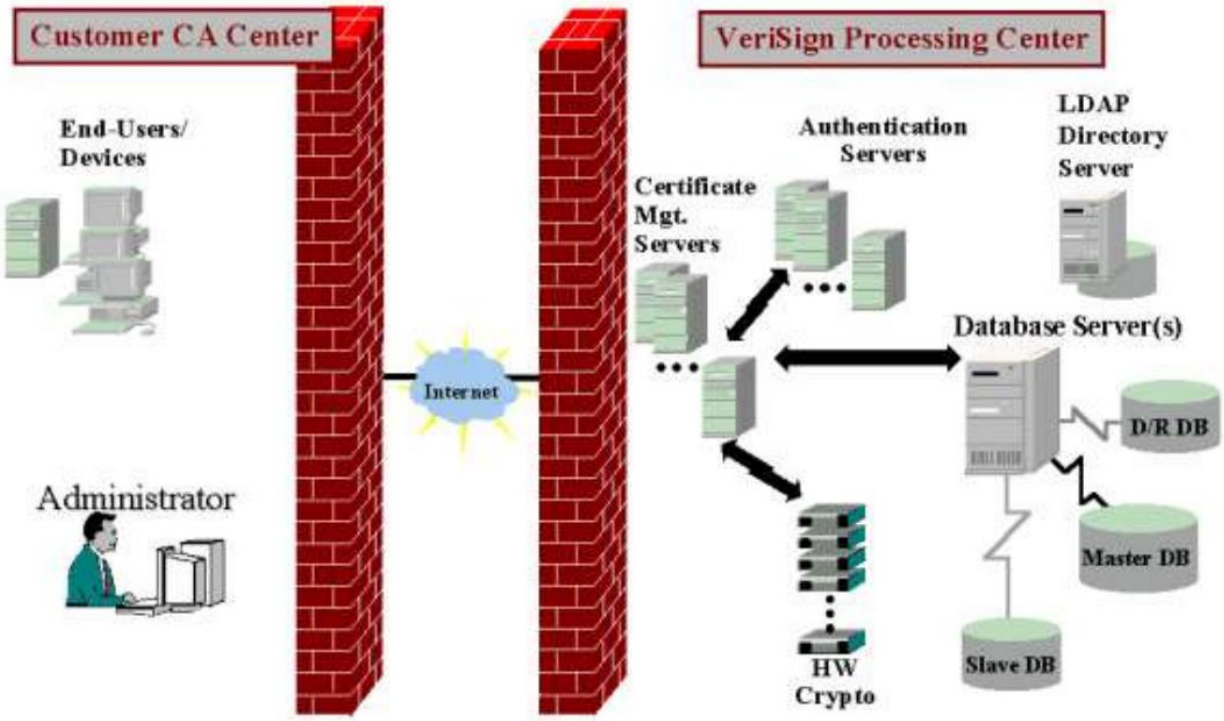
- **Tổng quan:**

    - Sử dụng Mật mã khóa công khai là cách tốt nhất để triển khai các giải thuật mã hóa trong các ứng dụng mạng.
    - cần xây dựng hạ Tầng khoá công khai (Public-key infrastructure - PKI)
    - PKI cho phép người tham gia xác thực lẫn nhau và sử dụng khóa công khai để mã hóa và giải mã trong quá trình trao đổi
- **Các tính chất của PKI:**
    - Riêng tư
    - Toàn vẹn
    - Không thể phủ nhận
    - Dễ dàng sử dụng
    - Xác thực
- **Khái quát về PKI:**
    - PKI gồm phần mềm (client và server) và phần cứng(thẻ thông minh) và các quy trình hoạt động khác
    - Người dùng có thể sử dụng khóa bí mật để ký các văn bản điện tử và người khác có thể sử dụng khóa công khai để xác thực
    - PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn và xác thực lẫn nhau mà không cần phải trao đổi các thông tin mật từ trước.
- **PKI thực hiện các chức năng sau:**
    - Xác định tính hợp pháp của người dùng
    - Phát hành chứng chỉ khóa công khai
    - Gia hạn thời gian chứng chỉ
    - Thu hồi khóa công khai
    - Lưu trữ và quản lí khóa công khai
    - Ngăn chặn người kí phủ nhận
    - Hỗ trợ các CA khác chứng thực chứng chỉ của khóa công khai được phát hành bởi CA này.
- **Danh sách một số hệ thống PKI:**
    - Computer Associates eTrust PKI
    - VeriSign
    - Entrust

- OpenCA
- Nexus
- Microsoft

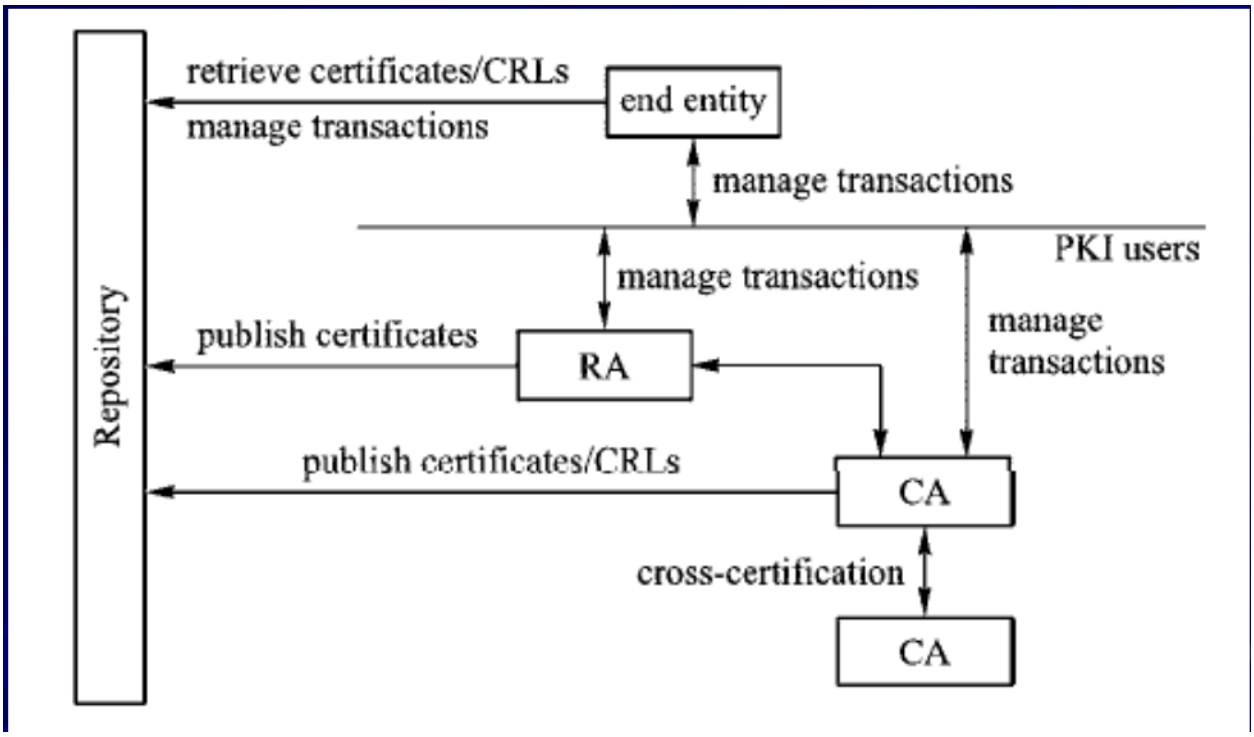
1. VeriSign

- **Tổng quan:**
  - Là thương hiệu uy tín nhất thế giới trong lĩnh vực cung cấp chữ ký số
  - Bảo mật hơn 1 triệu máy chủ web trên toàn world
  - Hơn 40 ngân hàng lớn , 90000 tên miền tại 145 Quốc gia sử dụng.
  - Hơn 90 000 tên miền tại 145 quốc gia hiển thị logo VeriSign
- **Giải thuật:**
  - Sử dụng giải thuật mã hóa SSL mạnh mẽ nhất:
    - Giải thuật mã hóa cao cấp từ 128bits trở lên
    - Có thể trao đổi dữ liệu giữa người dùng và website được mã hóa từ 40-256bits
- **Topology:**



2. X.509

- **Tổng quan:**
    - được gọi tắt là PKIK, gồm 4 phần cơ bản:
        - End entity: là người dùng chứng chỉ hoặc thiết bị (server, router) có hỗ trợ PKIX
        - Certificate Authority (CA): tổ chức có trách nhiệm phát hành và thu hồi chứng chỉ.
        - Registration Authority (RA): có trách nhiệm xác minh danh tính của người chủ sở hữu chứng chỉ.
        - Repository: có trách nhiệm lưu trữ, quản lý chứng chỉ và danh sách các chứng chỉ bị thu hồi bởi CA
- **Kiến trúc**



- **Các giao dịch giữa người dùng, RA, CA và kho:**
    - Đăng kí (với CA hoặc RA)
    - Khởi tạo chứng chỉ (khóa công khai,chữ kí,…)
    - Chứng chỉ được phát hành
    - phục hồi khóa
    - Tạo khóa
    - Thu hồi chứng chỉ

- Chứng chỉ chéo

- **Các thành phần chứng chỉ X.509**
  - Version(phiên bản) (hiện tại là version 3)
  - Serial number (số serial)
  - Algorithm (tên hàm băm + giải thuật mã hóa)
  - Issuer (tổ chức phát hành)
  - Validity period: thời gian hiệu lực
  - Subject (tên chủ sở hữu)
  - Public key (khóa công khai)
  - Extension (cung cấp thêm các thông tin khác)
  - Properties: Giá trị hàm băm của chứng chỉ

C. IPsec

1. Tổng quan:

- 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 thực, 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 của IPSec:**
  - 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.

2. Các thông tin một SA cung cấp:

- 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.

3. Các phương thức của IPSec:

- gồm 2 phương thức:
    - **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).
    - **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.

4. Định dạng AH:

- Authentication Header bao gồm các vùng :
    - **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.

5. Định dạng ESP

- Một gói ESP chứa các vùng:
    - **Security Parameters Index (32 bits):** xác định một SA
    - **Sequence Number (32 bits):** một giá trị đếm tăng đơn điệu, cung cấp chức năng anti-replay (giống AH).
    - **Payload Data (variable):** 1 segment ở tầng Transport hoặc gói IP (tunnel mode) được bảo vệ bởi việc mã hóa.
    - **Padding (255 bytes)**
    - **Pad Length (8 bits):** chỉ ra số byte vùng đứng ngay trước vùng này.
    - **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.
    - **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.

6. Các giải thuật mã hoá và chứng thực

- Three-key triple DES
- RC5
- IDEA
- Three-key triple IDEA
- CAST
- Blowfish

D. SSL/TLS

1. Tổng quan

- 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.
- SSL dùng để bảo vệ ứng dụng WWW và các giao dịch điện tử.

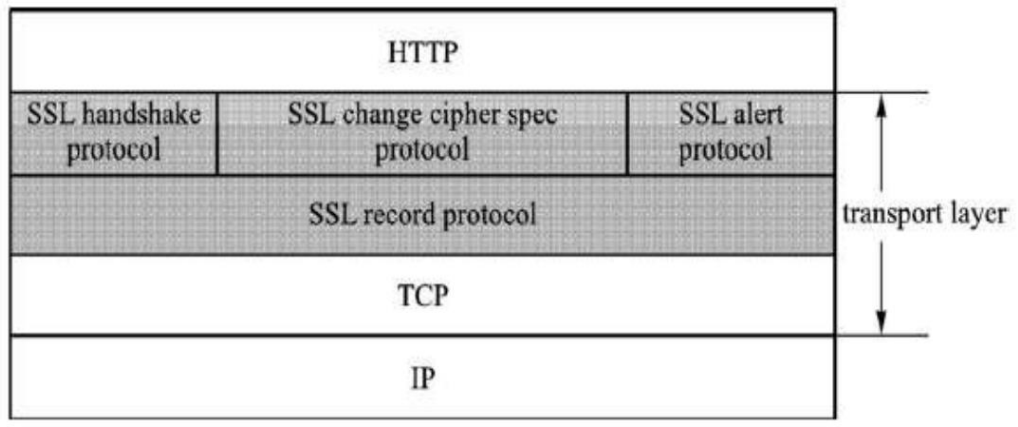
- TLS là phiên bản sửa đổi của SSL v3
- Giao thức SSL bao gồm 2 phần:
    - Phần 1 gọi là record protocol, đặt trên đỉnh của các giao thức tầng Transport.
    - Phần 2 đặt giữa các giao thức tầng Application (như HTTP) và record protocol, bao gồm các giao thức:
        - Handshake protocol
        - Change-cipher-spec protocol
        - Alert protocol

2. Các giao thức của SSL:

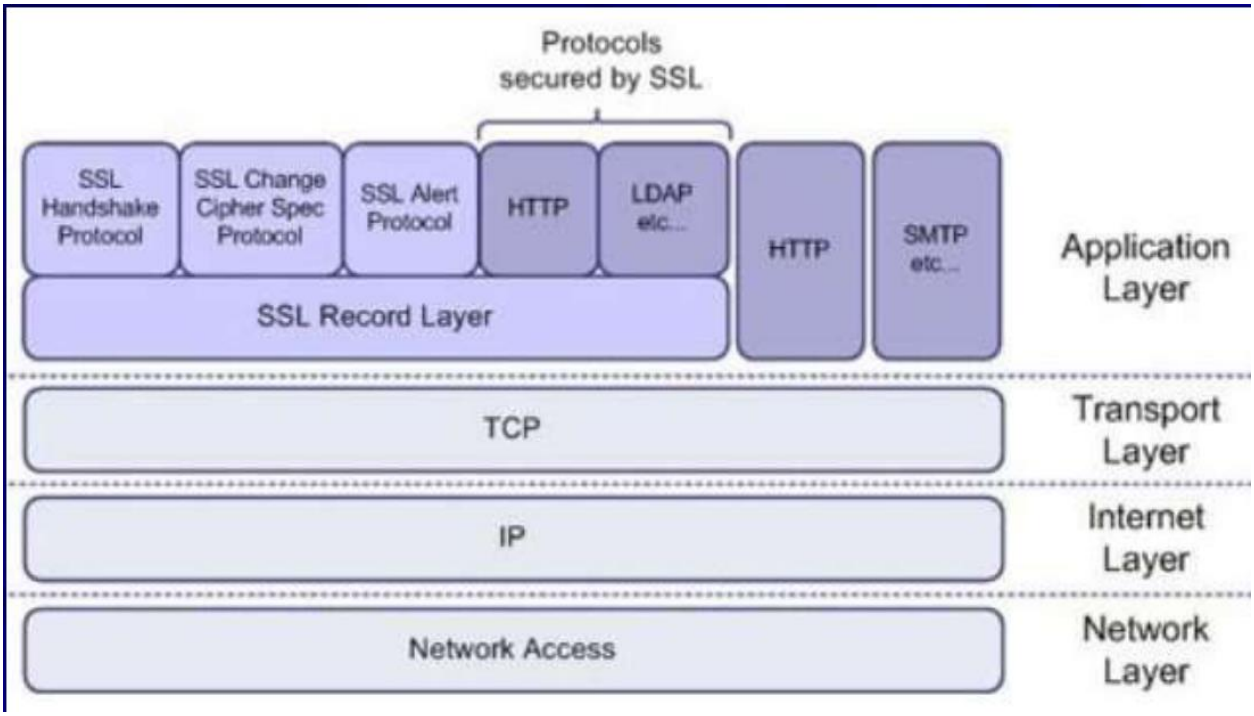
- Bao gồm 2 thành phần: record protocol (đặt trên đỉnh giao thức vận chuyển) và cách giao thức handsake protocol, change-cipher-spec protocol, alert protocol (nằm giữa tầng ứng dụng và record protocol

- **Giao thức bắt tay** (handshake protocol) thành lập các giải thuật mã hóa, giải thuật nén, và các thông số sẽ được sử dụng bởi cả hai bên trong việc trao đổi dữ liệu được mã hóa. Sau đó, các giao thức bản ghi (record protocol) chịu trách nhiệm phân chia thông điệp vào các khối, nén mỗi khối, chứng thực chúng, mã hóa chúng, thêm header vào mỗi khối, và sau đó truyền đi các khối kết quả.
- **Các giao thức đổi mật mã** (change-cipher-spec protocol) cho phép các bên giao tiếp có thể thay đổi các giải thuật hoặc các thông số trong một phiên truyền thông.
- **Các giao thức cảnh báo** (alert protocol) là một giao thức quản lý, nó thông báo cho các bên tham gia truyền thông khi có vấn đề xảy ra.

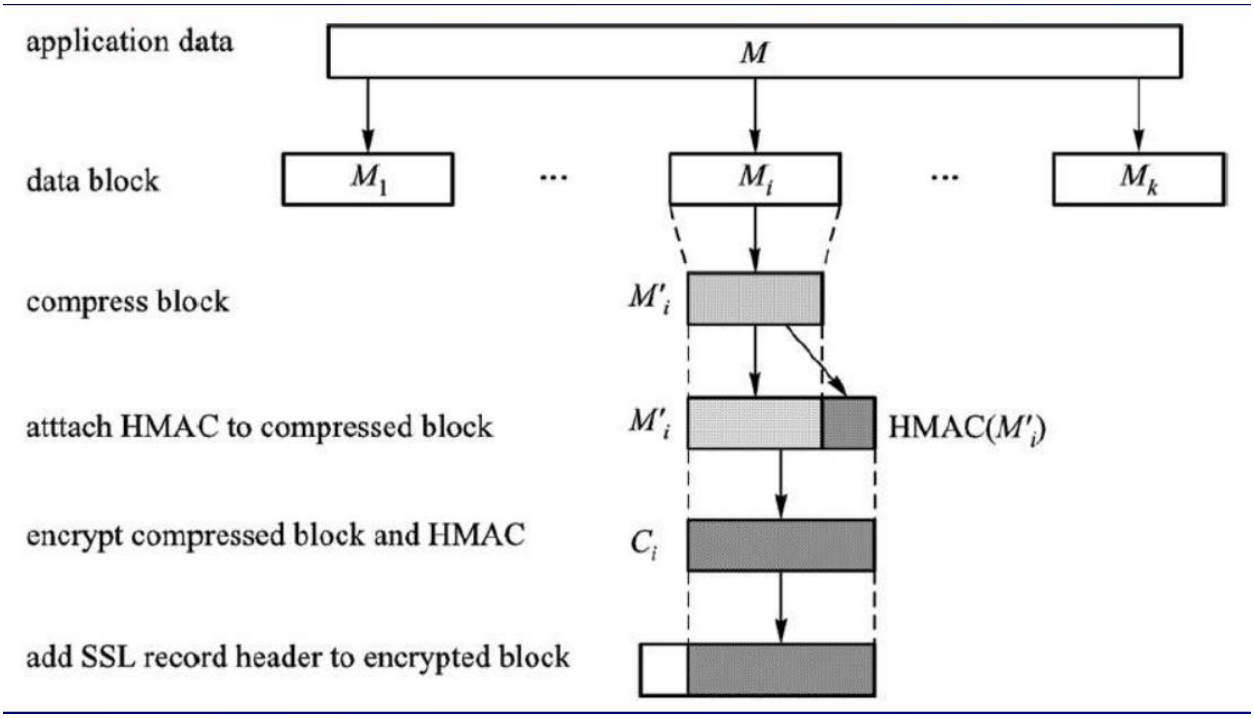
3. Cấu trúc SSL



SSL structure



Giao thức bản ghi (record protocol) của SSL

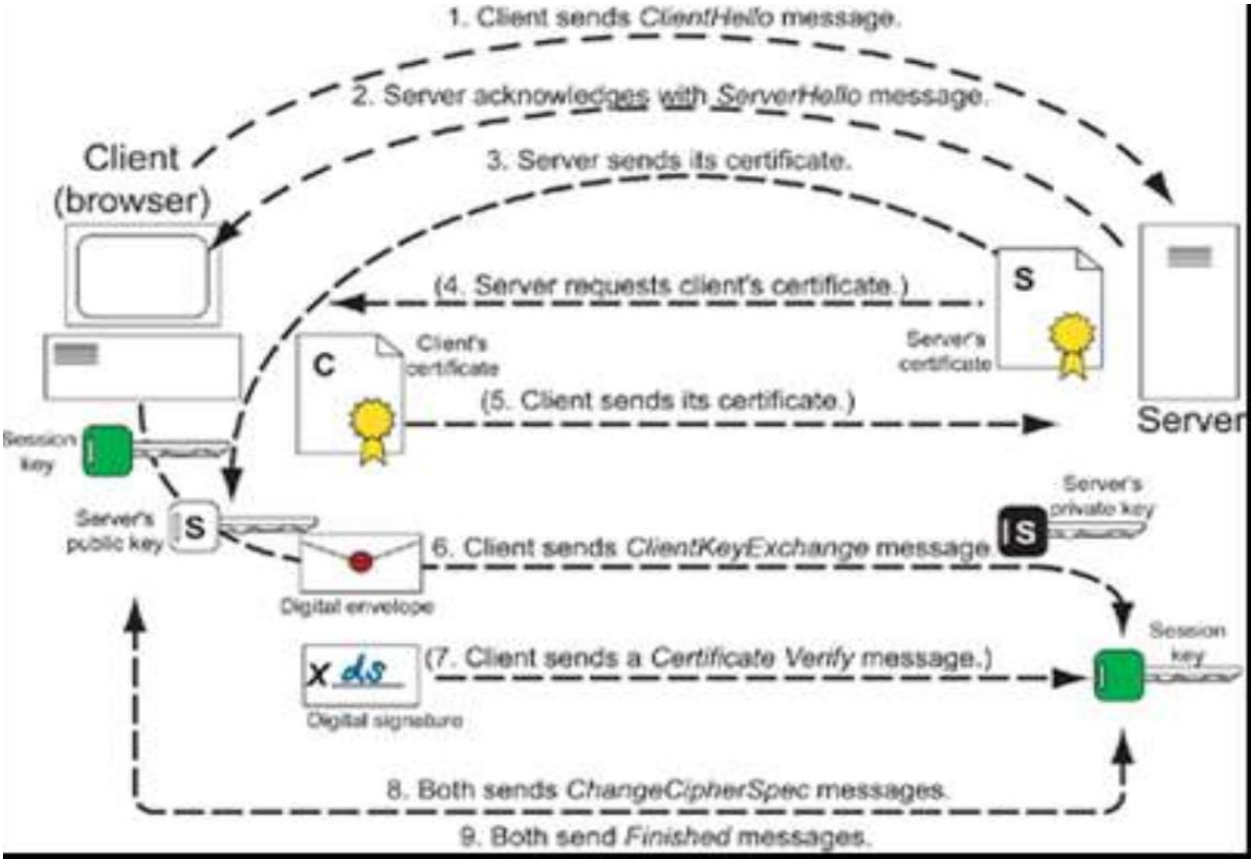


4. Tìm hiểu sâu về giao thức bắt tay

- **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:
    - Chứng chỉ khóa công khai của server.
    - Thông tin trao đổi khóa của server.
    - 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:
    - Chứng chỉ khóa công khai của Client
    - Thông tin trao đổi khóa của Client.
- **Phase 4:** hoàn thành bắt tay. Server và Client sẽ gửi nhau thông điệp finish.

5. Quá trình thiết lập kết nối SSL



Phân tích quá trình thiết lập kết nối SSL:

- Trong mô hình giả định, ta có một Client (browser) cố gắng giao tiếp với Server.
- Đầu tiên, Client gửi lời chào đến Server.
- Thứ 2, Server tiếp nhận lời chào từ Client.
- Thứ 3, Server gửi chứng chỉ kèm khóa công khai của Server cho Client.
- Thứ 4, Server yêu cầu ngược lại chứng chỉ của Client.

- Thứ 5, Client gửi chứng chỉ của bản thân kèm public key của nó cho Server.
- Thứ 6, Client mã hóa Section key được tạo ra bởi Client bằng khóa công khai của Server và gửi tin nhắn muốn trao đổi khóa. Sau khi nhận tin thì Server dùng khóa bí mật của bản thân để giải mã và lấy được Section key chung của cả Client và Server.
- Thứ 7, Client gửi 1 tin nhắn chứng thực chứng chỉ của bản thân cho Server. Nhằm đảm bảo Section key được gửi từ phía Client chứ không phải bên nào khác, đồng thời đảm bảo tính toàn vẹn của thông điệp trao đổi khóa.
- Thứ 8 và thứ 9, cả 2 bên trao đổi xác nhận đã thiết lập kết nối với nhau và từ bây giờ khi trao đổi với nhau thì thông điệp sẽ được mã hóa bằng section key.

E. PGP và S/MIME

1. Tổng quan

- 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 Email**
    - 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
    - Giả 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:

$$M \| \hat{E}_{K_A^r}(H(M)) \| \mathrm{CA}\langle K_A^u \rangle,$$

    - Với K^u_A và K^r_A lần lượt là khóa công khai và khóa riêng tư.
    - Sau khi nhận được M II S_M II CA < K^u_A > từ Alice, với S_M là chữ Ký vào M sử dụng khóa riêng tư của Alice. Trước tiên Bob so sánh chữ ký của CA trên chứng chỉ khóa công khai CA (K^u_A) và rút trích K_A từ đó. Sau đó Bob rút trích M và so sánh

$$S_M = \hat{E}_{K_A^r}(H(M))$$

    - Nếu đúng, Bob tin là M đến từ Alice

- Giả sử Alice muốn đảm bảo rằng M giữ được tính bí mật trong suốt quá trình truyền và cô ấy biết khoá công khai của Bob (K^u_B), cô ấy sẽ gửi cho Bob chuỗi sau:

$$E_{K_A}(M) \| \hat{E}_{K_B^u}(K_A)$$

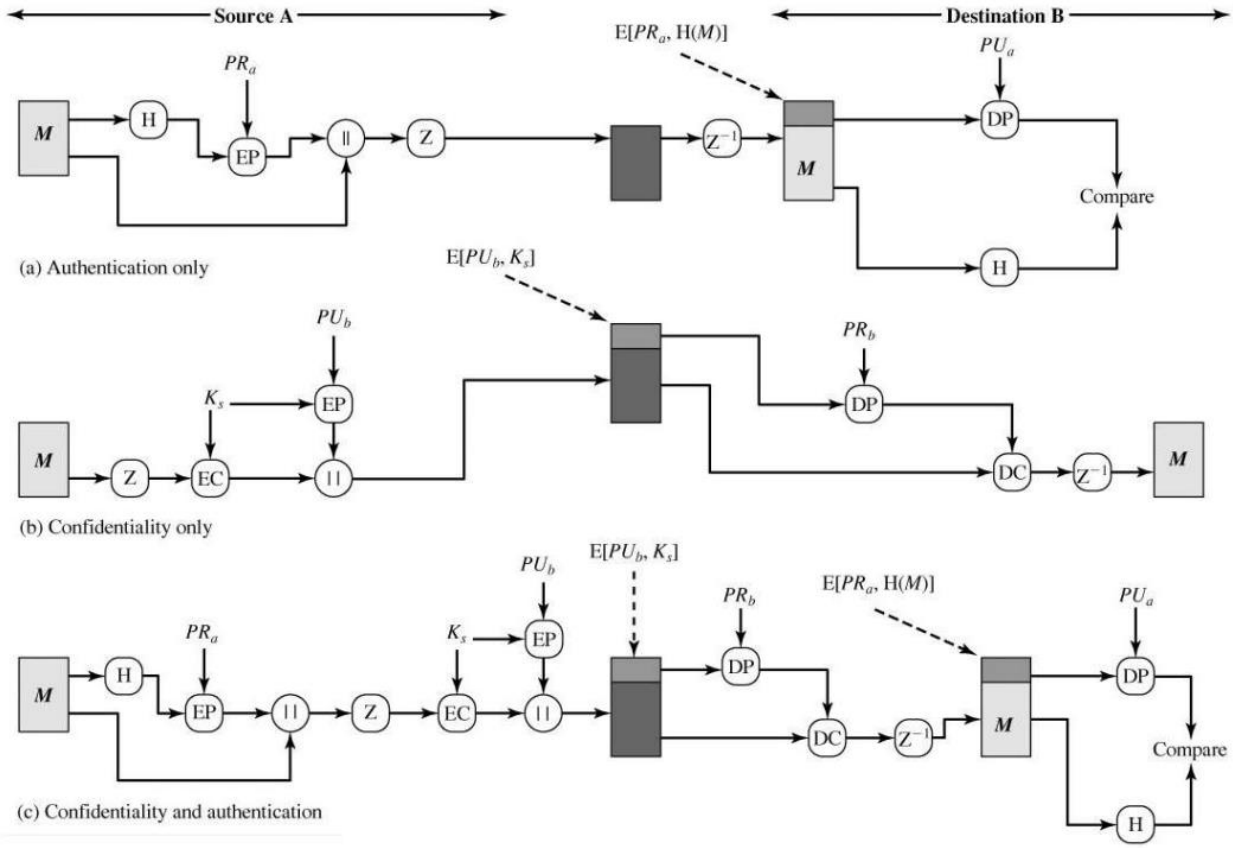
- Với K_A là khóa bí mật của Alice
- Sau khi nhận được chuỗi từ Alice ,Bob sử dụng khóa riêng tư của mình để giải mã:

$$\hat{D}_{K_B^r}(\hat{E}_{K_B^u}(K_A)) = K_A$$

- Kế đó Bob dùng (K_A) để giải mã thu được M: $D_{K_A}(E_{K_A}(M)) = M.$

2. PGP

- PGP có thể được sử dụng để chứng thực một thông điệp, mã hoá thông điệp, hoặc cả chứng thực lẫn mã hoá.
- PGP cho phép những định dạng tổng quát như chứng thực, nén ZIP, mã hoá...
- **Các chức năng của PGP:**



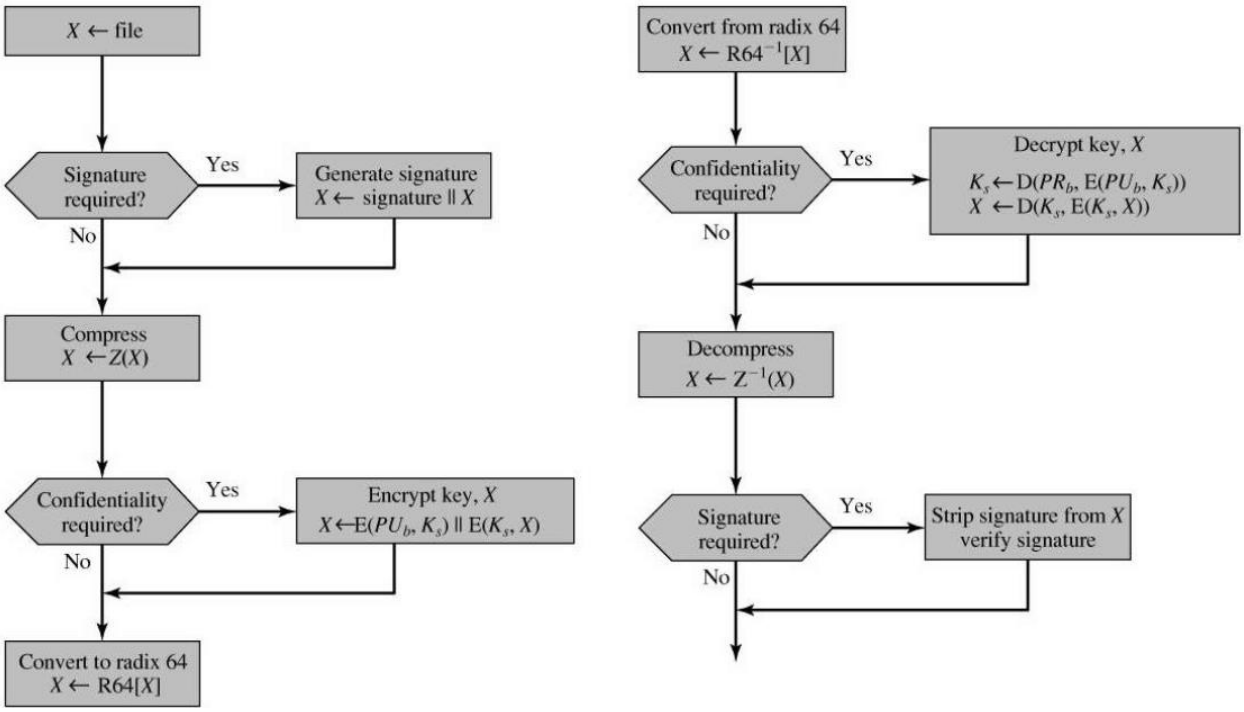
- **(sơ đồ a)** chỉ chứng thực

- **(sơ đồ b)** chỉ Bảo mật
- **(sơ đồ c)** Chứng thực và bảo mật

Chú thích:

- K_s: session key dùng trong mã hoá symmetric
- Pr_a: private key của user A
- PU_a: public key of user A
- EP: mã hoá public-key (asymmetric)
- DP: giải mã public-key (asymmetric)
- EC: mã hoá symmetric
- DC: giải mã symmetric
- H: hàm băm
- ||: kết nối, ghép chuỗi
- Z: nén sử dụng giải thuật ZIP
- R64: convert sang định dạng ASCII 64 bit

- **Truyền và nhận thông điệp**

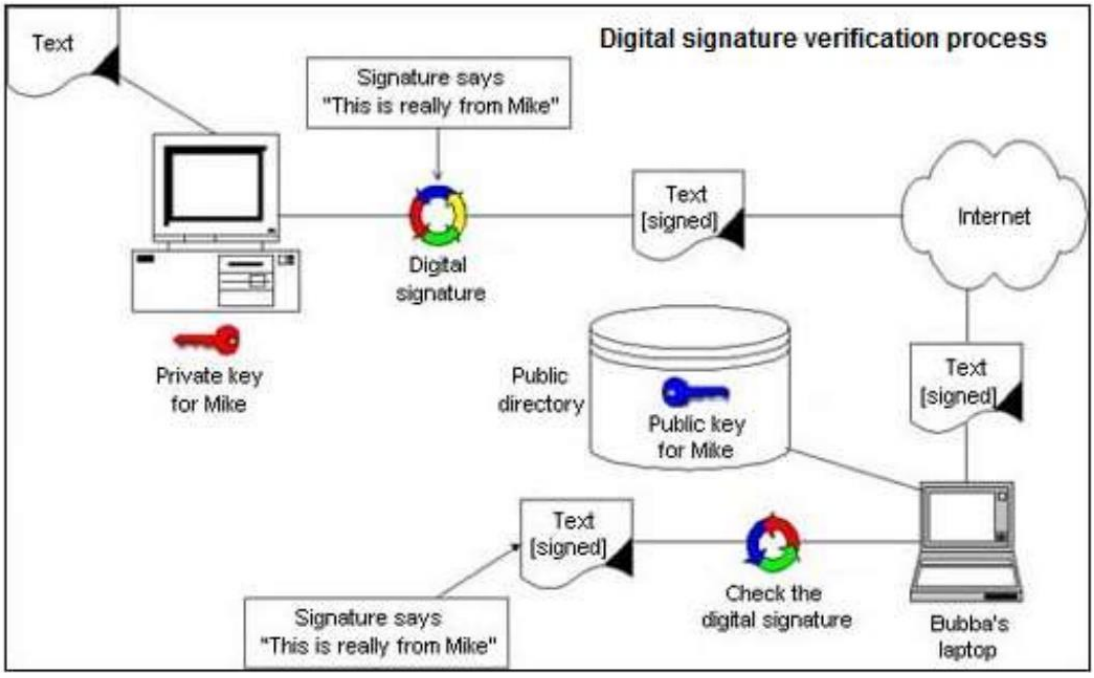


- **Một số Đặc tính của PGP**

Đặc tính	PGP 2.x (RFC 1991)	OpenPGP (RFC 2440)
Định dạng khóa	Khóa V3	Khóa V4
Thuật toán khóa bất đối xứng	*RSA (mã hóa & chữ ký)	RSA (mã hóa & chữ ký) *DSA (chữ ký) *Elgamal (mã hóa)
Thuật toán khóa đối xứng	*IDEA	IDEA *Triple-DES CAST5 Blowfish AES 128, 192, 256 Twofish
Hàm băm mật mã	*MD5	MD5 *SHA-1 RIPEMD-160 SHA-256 SHA-384 SHA-512
Thuật toán nén	ZIP	ZIP gzip bzip2

3. 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
- **Sơ đồ Chứng thực chữ kí số:**



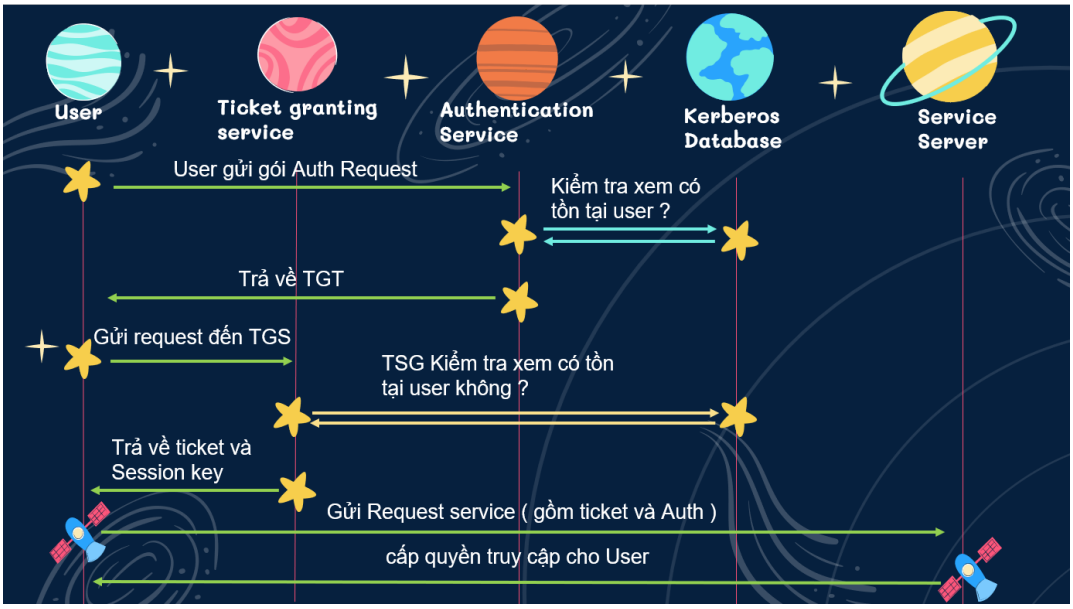
- **Các tính năng của một Webmail client hộ trợ S/MIME:**
    - Tạo chữ ký số cho 1 email gửi đi để đảm bảo người nhận email tin không có sự can thiệp và đến từ người gửi.
    - Mã hóa email gửi đi để ngăn bất cứ ai xem, thay đổi… Nội dung của email trước khi đến với người nhận.
    - Xác minh chữ ký 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

F. Kerberos

1. Tổng quan:

- Là một giao thức mã hoá dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn.
- Có thể chống lại việc nghe lén hay gửi lại các thông tin cũ,đảm bảo tín toàn vẹn dữ liệu
- Mục tiêu nằm vào client-server và đảm bảo chứng thực 2 chiều.
- Xây dựng trên mã hóa đối xứng , cần 1 bên thứ 3 uy tín để làm chung gian.

2. Mô tả cách hoạt động:



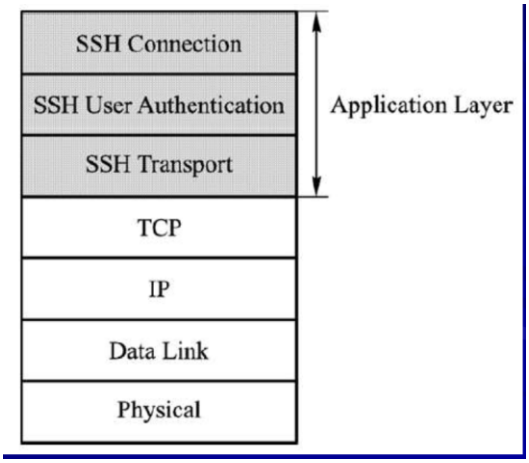
- **Giải thích thuật ngữ:**

- User: người dùng
- Ticket granting service: phiên chứng chỉ
- Authenticaion service: bên thứ 3 trung gian
- Database : nơi lưu trữ user
- Service server: Bên cung cấp chứng chỉ

G. SSH

1. Tổng quan:

- Được định nghĩa trong RFC 4251
- Sử dụng cổng TCP 22
- Hoạt động trên các flatform khác nhau:
  - Kết nối đến một máy chủ SSH trên một router của Cisco từ một máy khách chạy Windows
  - Kết nối đến một máy chủ Linux từ một router Cisco hay có thể kết nối đến một máy chủ Windows 2008 từ một máy khách sử dụng hệ điều hành Linux.
- Tạo kết nối bảo mật giữa 2 máy tính.
- Có khả năng nén, bảo mật dữ liệu khi truyền (SFTP) và sao chép file (SCP)
- Là giao thức ứng dụng client-server.SSH chia thành 3 lớp trong ứng dụng mô hình mạng TCP/IP:
  - Connection
  - User Authentication
  - Transport Layer



2. Cách thức hoạt động

- **Định danh Host:**
    - Thông qua trao đổi khóa,Mỗi máy tính có hỗ trợ kiểu truyền thông SSH có một khoá định danh duy nhất gồm khóa công khai và khóa riêng tư.Dữ liệu được mã hóa bằng khóa công khai và chỉ có khóa riêng tư mới giải mã được.
    - khi bắt đầu 1 phiên SSH, máy chủ sẽ gửi khóa công khai đến máy khách,máy khách sẽ sinh khóa ngẫu nhiên và mã hóa bằng khóa công khai và gửi về máy chủ ,Máy chủ sử dụng khóa riêng tư để giải mã và có được khóa của máy khách.Khóa này chính là khóa dùng để trao đổi dữ liệu giữa 2 bên.
- **Mã hóa:**
    - Sau khi định dạnh xong,dữ liệu trước khi trao đổi sẽ đươuc mã hóa.
    - Việc lựa chọn cơ chế mã hóa do **máy khách quyết định**.Cơ chế thường bao gồm: 3DES, IDEA và Blowfish.
- **Chứng thực:**
    - Mỗi định danh và truy nhập của người sử dụng có thể được cung cấp theo nhiều cách khác nhau. Chẳng hạn, kiểu chứng thực rhosts có thể được sử dụng, nhưng không phải là mặc định; nó đơn giản chỉ kiểm tra định danh của máy khách được liệt kê trong file rhost (theo DNS và địa chỉ IP).
    - Việc chứng thực mật khẩu là một cách rất thông dụng để định danh người sử dụng, nhưng ngoài ra cũng có các cách khác: chứng thực RSA, sử dụng ssh-keygen và ssh-agent để chứng thực các cặp khoá.

VII. Bảo mật mạng không dây

A. Tổng quan và phân loại

Công nghệ Wi-Fi được phát triển dựa trên bộ tiêu chuẩn IEEE 802.11 và được sử dụng rộng rãi trong truyền thông mạng không dây. Các điểm phát sóng Wi-Fi hay còn gọi là Wi-Fi Hotspots, có thể được tìm thấy dễ dàng ở các nơi công cộng hoặc có thể thiết lập ngay tại nhà dễ dàng.

1. Phân loại các mạng không dây

- Extension to a Wired Network - Mở rộng từ mạng dây
- Multiple Access Points - Đa điểm truy cập
- LAN-to-LAN Wireless Network - Mạng không dây giữa LAN với LAN
- 3G/4G/5G Hotspot

2. Các chuẩn trong mạng không dây

- 802.11a - Băng thông lên tới **54 Mbps**, hoạt động ở băng tần **5 Ghz**.
- 802.11b - Băng thông lên tới **11 Mbps**, hoạt động ở băng tần **2.4 Ghz**.
- 802.11g - Băng thông lên tới **54 Mbps**, hoạt động ở băng tần **2.4 Ghz**.
- 802.11i - Thường dùng trong các WLANs, cung cấp cơ chế mã hóa tối ưu hơn cho các mạng dùng 3 chuẩn ở trên.
- 802.11n - Sử dụng công nghệ MIMO - Multiple Input Multiple Output để tăng tốc độ Wi-Fi (lên đến **100 Mbps**) và tăng độ phủ sóng.
- 802.16 - Một nhóm các chuẩn mạng không dây dùng trong **MAN** - Metropolitan Area Network.
- Bluetooth - Độ phủ sóng bé (khoảng cách **dưới 10m**) và băng thông tương đối thấp (**1-3 Mbps**)

B. Các kiểu chứng thực

- Open System Authentication: Không có chứng thực, client chỉ việc gửi yêu cầu kết nối.
- Shared Key Authenticaion:
    - AP gửi một challenge cho client, client mã hóa nó bằng key mình đang có.
    - AP giải mã văn bản nhận được và nếu đúng, client đó được chứng thực.
    - CLient kết nối thành công tới AP.
- Centralized Authentication Server:
    - AP gửi EAP-Request (Extensible Authentication Protocol-Request) cho client đang yêu cầu kết nối để xác định danh tính. Sau khi nhận được phản hồi, sẽ chuyển tiếp về RADIUS Server
    - Trong suốt quá trình chứng thực, AP chỉ làm nhiệm vụ tiếp nhận yêu cầu kết nối và gửi các yêu cầu về cho RADIUS Server.
    - Mọi tác vụ chứng thực được xử lý bởi Server.

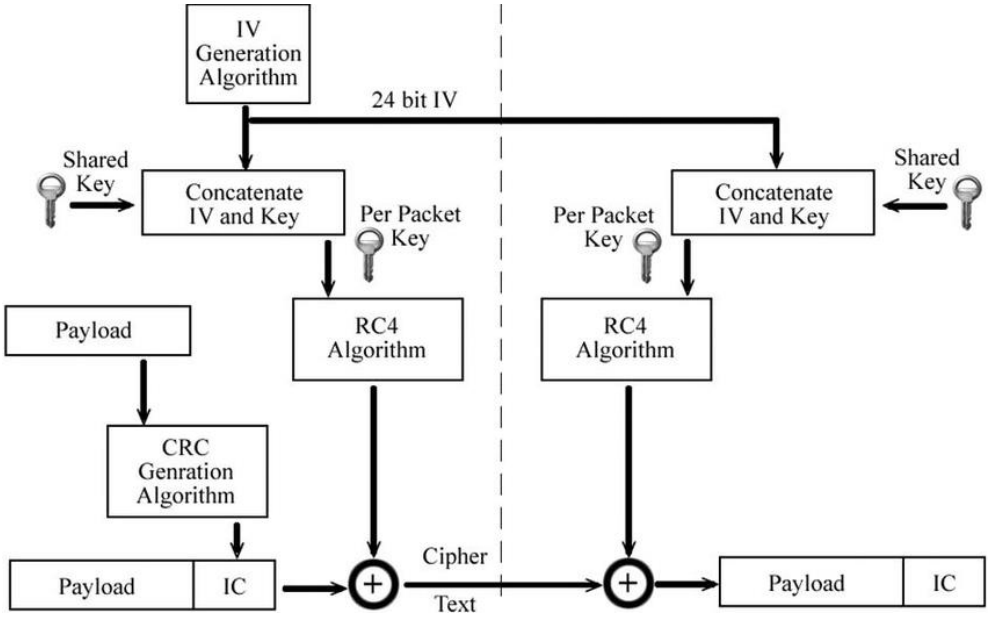
C. WEP, WPA và WPA2

1. WEP

Wired Equivalent Privacy là một giao thức không dây theo chuẩn 802.11 cung cấp thuật toán mã hóa cho quá trình truyền dữ liệu. WEP sử dụng một Initialization Vector (Vector khởi tạo) để hình thành các stream cipher - chuỗi mã hóa RC4 và có cơ chế checksum là CRC32.

- 64-bit WEP uses a 40-bit key

- 128-bit WEP uses a 104-bit key size
- 256-bit WEP uses 232-bit key size



Quy trình hoạt động của WEP

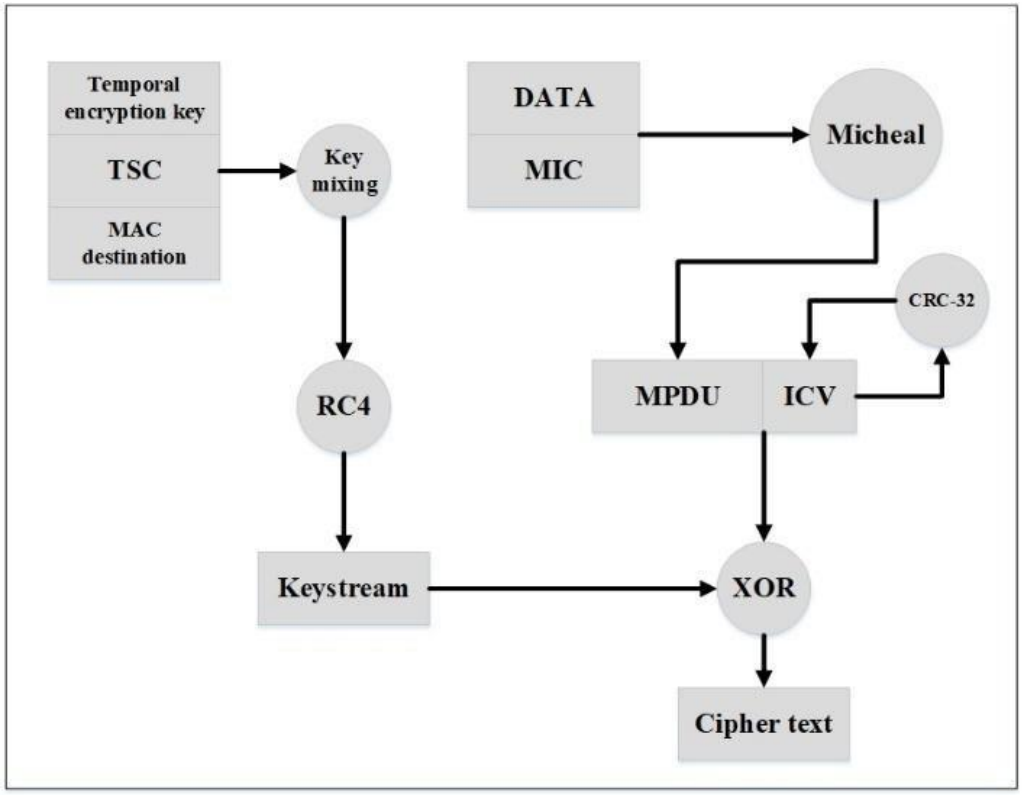
1. AP tạo ra một khóa mã hóa 40 bit (Shared key).
2. Nối khóa này với IV 24 bit được tạo ra từ thuật toán tạo IV để tạo chuỗi khóa mới cho mỗi gói (Per packet key) có kích thước 40 hoặc 104 bit.
3. Chuỗi khóa mới đi qua thuật toán mã hóa RC4.
4. Payload (dữ liệu cần được chuyển đi) sau khi được đính kèm checksum ở header từ thuật toán CRC sẽ tiếp tục được XOR với chuỗi khóa ở bước 3 => Cipher text.
5. Phía client nếu sở hữu Shared key sẽ thực hiện lại các bước 2,3,4 khi nhận được cipher text. Khi thực hiện phép XOR sẽ đưa cipher text về lại thành plain text.

Cách để crack WEP

1. Dùng aireplay-ng để giả mạo xác thực với AP.
2. Dùng airodump-ng để thu thập các IV từ AP đó.
3. Tiếp tục dùng aireplay-ng để liên tục gửi request đến AP.
4. Sử dụng tấn công từ điển để lấy được khóa giải mã từ các IV thu tập được.

2. WPA

Wi-FI Protected Access cũng là một giao thức bảo mật không dây dựa theo bộ tiêu chuẩn 802.11 nhưng với cải tiến so với WEP về thuật toán và cơ chế trao đổi khóa.

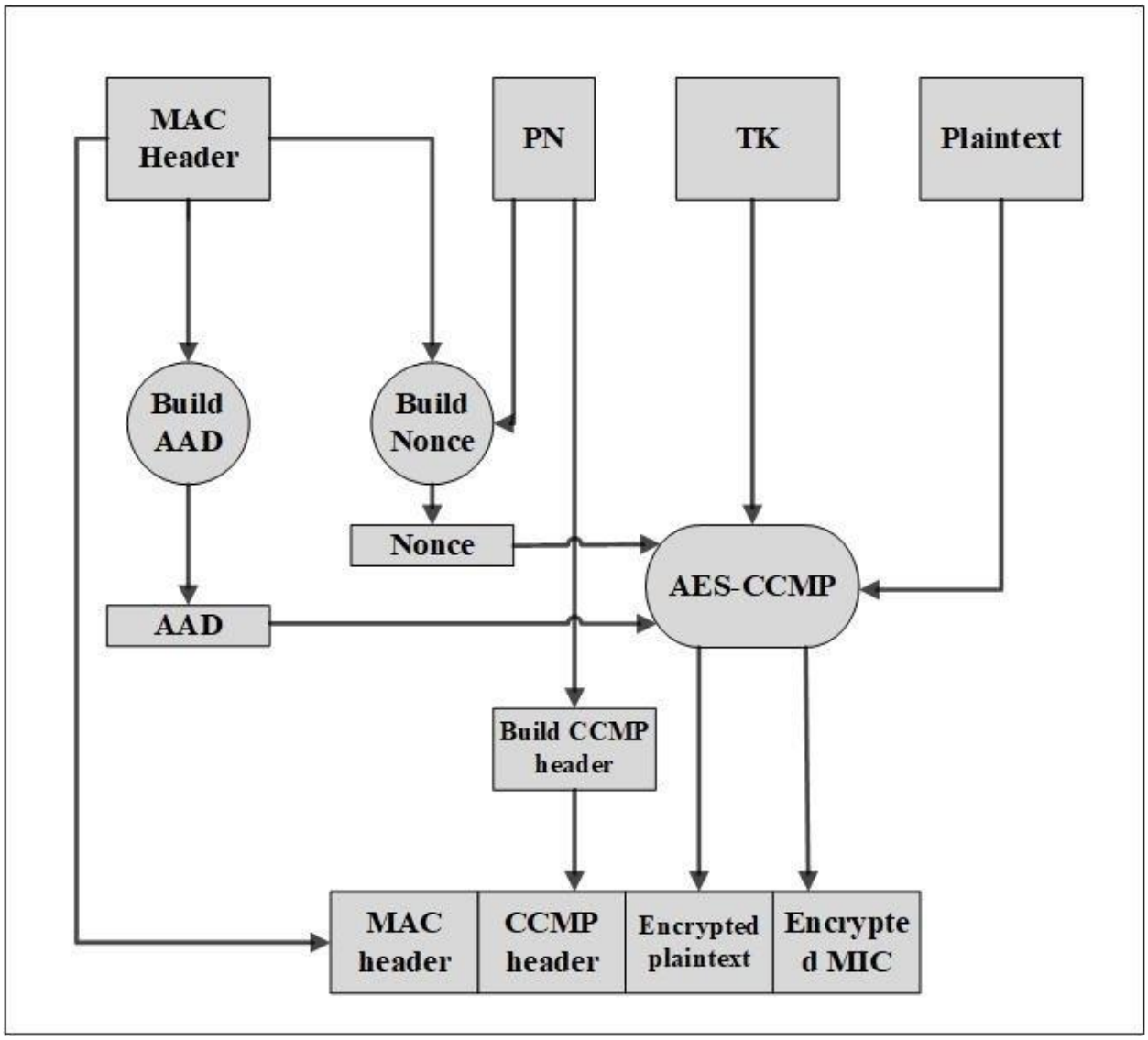


Quy trình hoạt động của WPA

1. AP khởi tạo PSK - Pre-Shared Key để từ đó tạo ra PMK - Pairwise Master Key dùng để gửi cho client. Từ PMK, tiếp tục tạo ra Temporal Encryption Key - Khóa mã hóa tạm thời cho mỗi gói tin.
2. Trộn các khóa lại với nhau bao gồm Temporal Encryption Key, TSC - TKIP Sequence Counter (Bộ đếm TKIP) và địa chỉ MAC đích.
3. Sử dụng thuật toán mã hóa RC4 để từ đó tạo ra keystream.
4. Dữ liệu được đính kèm MIC key (Message Integrity Check) được mã hóa với thuật toán Micheal. Sau đó, đính kèm thêm checksum từ CRC-32.
5. Thực hiện phép XOR giữa keystream và dữ liệu được mã hóa từ bước 3 => cipher text.
6. Client sau khi nhận được PMK từ AP sẽ thực hiện lại các bước như 1,2,3 để giải mã thay vì mã hóa. Sau đó, tự tính lại giá trị MIC để so sánh với giá trị MIC có trong gói tin nhận được để kiểm tra tính toàn vẹn của dữ liệu. Nếu bằng nhau, dữ liệu xem như là toàn vẹn và được giải mã thành công thành plaintext.

3. WPA2

Một giao thức bảo mật không dây tiếp tục cải tiến thêm từ WPA, được khuyến nghị sử dụng cho các mạng không dây hiện đại ngày nay.



Quy trình hoạt động của WPA2

1. Tạo AAD - Additional Authentication Data (Dữ liệu xác thực bổ sung) từ MAC header.
2. Tạo Nonce - Number used once (Số chỉ dùng một lần) từ MAC header và PN - Packet Number
3. Khởi tạo TK - Temporal Key (Khóa tạm thời) với kích thước 128 bit.
4. Plaintext cũng như AAD, Nonce và TK được mã hóa với thuật toán AES-CCMP - **A**dvanced **E**ncryption **S**tandard-**C**ounter Mode **C**BC-**M**AC **P**rotocol
5. PN được tiếp tục sử dụng để tạo CCMP Header.
6. Đính kèm MAC Header và CCMP Header vào payload
7. Cuối cùng thêm cipher text và MIC đã mã hóa từ AES-CCMP vài payload.

Phần này mình soạn nhưng cũng không chắc lắm do muốn giống sơ đồ trong slide bài giảng trên trường thì phải tìm lại mấy tài liệu đã rất cũ. Khối AES-CCMP cũng không có giải thích gì thêm nên coi như là nó làm phép thuật trong đó vậy.

Cách để crack WPA/WPA2

Trong slide bài giảng hiện không có cách hiệu quả, chỉ có việc bắt các gói tin trong quá trình handshake rồi brute force dựa trên thông tin có được.

4. Bảng so sánh tổng quan 3 giao thức

	WEP	WPA	WPA2
Mã hóa	RC4	RV4, TKIP	AES-CCMP
Kích thước IV	24 bit	48 bit	48 bit
Kích thước khóa	40/104 bit	128 bit	128 bit
Cơ chế checksum	CRC-32	Thuật toán Micheal và CRC-32	AES-CCMP
Độ bảo mật	Thấp	Trung bình	Cao

D. Các mối đe dọa

Ta có 5 nhóm mối đa dọa như sau:

1. Access Controls Attack - Tấn công kiểm soát truy cập
2. Integrity Attack - Tấn công tính toàn vẹn
3. Confidentiality Attack - Tấn công tính bảo mật
4. Availability Attack - Tấn công tính sẵn sàng
5. Authentication Attack - Tấn công xác thực

1. Access Controls Attack

Wireless access control attacks aims to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls

- MAC Spoofing
- Ad Hoc Associations
- AP Misconfiguration
- Client Misassociation
- Unauthorized Association
- Promiscuous Client
- Rogue Access Point
- War Driving

2. Integrity Attack

In integrity attacks, attackers send forged control, management or data frames over a wireless network to misdirect the wireless devices in order to perform another type of attack (e.g., DoS)

- Data Frame Injection
- WEP Injection
- Data Replay
- IV Replay
- Bit-Flipping
- Extensible AP Replay
- RADIUS Replay
- Virus trong mạng không dây

3. Confidentiality Attack

These attacks attempt to intercept confidential information sent over wireless associations, whether sent in the clear text or encrypted by Wi-Fi protocols

- Eavesdropping
- Traffic Analysis
- Cracking WEP key
- Evil Twin AP
- Man-In-The-Middle Attack
- Masquerading
- Session Hijacking
- Honeypot AP

4. Availability Attack

Denial of Service attacks aim to prevent legitimate users from accessing resources in a wireless network

- AP Theft
- DoS
- Beacon Flood
- Authenticate Flood
- ARP Cache Poisoning
- TKIP MIC Exploit
- De-authenticate Flood
- Disassociation Attack
- EAP-Failure
- Routing Attack
- Power Saving Attack

5. Authentication Attack

The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources

- Application Login Theft
- PSK Cracking
- Shared Key Guessing
- Domain Login Cracking
- Identity Theft
- VPN Login Theft
- Password Speculation
- LEAP Cracking

E. Phương pháp và công cụ tấn công

Quy trình tấn công mạng Wi-Fi gồm 5 bước:

1. **Wi-Fi Discovery** - Tìm kiếm và xác định mang Wi-Fi mục tiêu

2. **GPS Mapping** - Dùng GPS để xác định vị trí vật lý của vùng mạng đó, hacker có thể chia sẻ thông tin này hoặc bán để kiếm tiền.
3. **Wireless Traffic Analysis** - Phân tích lưu lượng mạng để tìm ra lỗ hỏng nhằm khai thác và tán công
4. **Launch wireless attack** - Bắt đầu tấn công với phương thức phù hợp
5. **Crack Wi-Fi encryption** - Crack được chuẩn mã hóa của Wi-Fi

Các công cụ có thể dùng trong mỗi bước:

1. Wi-Fi Discovery: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, WirelessMon…
2. GPS Mapping: WIGLE, Skyhook… (Dùng phương pháp War Driving kết hợp với các công cụ này)
3. Wireless Traffic Analysis: WireShark, OmniPeek Tool, CommView Tool, AirMagnet Wi-Fi Analyzer… (Dùng kết hợp với USB-WiFi)
4. Launch wireless attack: Bộ công cụ Aircrack-ng là thích hợp nhất để sử dụng một số phương pháp tấn công đã giới thiệu ở mục VII.D.1.Access Controls Attack.

F. Tấn công mạng Bluetooth

1. Phương pháp tấn công

1. **Bluesmacking** - Tấn công DoS bằng các gói tin ngẫu nhiên khiến thiết bị đang kết nối bị crash
2. **Blue Snarfing** - Đánh cắp dữ liệu thông qua kết nối Bluetooth
3. **Bluejacking** - Kỹ thuật gửi các thông điệp qua Bluetooth mà không cần bên kia yêu cầu hay chấp nhận (Kiểu ai hỏi mà bộ trưởng trả lời ấy).
4. **BlueSniff** - War driving nhưng mà là Bluetooth

2. Các công cụ tấn công

- **Super Bluetooth Hack** - Một Bluetooth Trojan khi lây nhiễm sẽ cho phép kẻ tấn công điều khiển và đọc thông tin từ điện thoại của nạn nhân.
- **PhoneSnoop** - Một spyware hoạt động trên các điện thoại Blackberry
- **BlueScanner** - Dùng để khám phá các mạng Bluetooth xung quanh và sẽ cố ghi lại mọi thông tin có thể từ các thiết bị Bluetooth sao cho không cần phải xác thực.

G. Biện pháp phòng chống

1. Các lớp bảo mật trong mạng không dây

- Lớp bảo mật tín hiệu không dây
- Lớp bảo mật kết nối
- Lớp bảo mật dữ liệu
- Lớp bảo mật người dùng cuối
- Lớp bảo mật mạng
- Lớp bảo mật thiết bị

2. Phòng chống Bluetooth Hacking

- Dùng các mã PIN bất thường, độc lạ.
- Luôn luôn bật chế độ mã hóa khi thiết lập kết nối.
- Thường xuyên kiểm tra xem các thiết bị nào đã từng ghép cặp với mình và xóa những thiết bị lạ.
- Chỉ bật chế Bluetooth lên khi cần thiết.
- Để thiết bị ở chế độ non-discoverable (chế độ ẩn)
- Không chấp nhận mọi yêu cầu kết nối từ thiết bị lạ mặt.

3. Phòng chống Wi-Fi Hacking

- Sử dụng các chuẩn WPA, WPA2 thay vì WEP.
- Thiết lập WPA2-Enterprise mỗi khi có thể.
- Đặt AP ở một vị trí an toàn.
- Thường xuyên cập nhật driver cho các thiết bị mạng.
- Sử dụng server cho việc chứng thực.
- Ngắt kết nối mạng khi không cần thiết sử dụng.

Còn một số thông tin khác liên quan đến thiết lập SSID mình sẽ không đề cập ở đây, các bạn có thể xem thêm trong slide chương 7.

H. Công cụ bảo mật Wi-Fi

WIPS - Wireless Intrusion Prevention System, thuật ngữ nói về các hệ thống ngăn ngừa và phát hiện xâm nhập cho mạng không dây.

Ta có các công cụ liên quan như sau:

- **AirMagnet Wi-Fi Analyzer Tool** - công cụ để kiểm tra và troubleshoot mạng. Nó có thể phát hiện các cuộc tấn công DoS hoặc tấn công xác thực. Ngoài ra, công cụ này còn hỗ trợ phát hiện ra các thiết bị kết nối không hợp pháp trong mạng.
- **AirDefense** - Một nền tảng GUI cho phép theo dõi và phát hiện xâm nhập. Nó hoạt đông thông qua các sensor phân tán để quan sát lưu lượng mạng 24/7, từ đó cho phép phân tích các lỗ hỏng zero-day trong thời gian thực. Hơn thế, công cụ này cho phép thực hiện các cuộc điều tra pháp chứng kỹ thuật số thông qua những bản ghi chi tiết mà nó lưu trữ.

Adaptive WIPS nói về các hệ thống không chỉ phát hiện mối nguy mà còn hỗ trợ giảm thiểu hậu quả của các cuộc tấn công.

Ta có các công cụ liên quan như sau:

- **Aruba RFProtect WIPS** - Gồm 2 tính năng chính là Automatic Threat Mitigation (Giảm thiểu mối nguy tự động) và Automated compilance reporting (Báo cáo tự động theo quy chuẩn)

I. Kiểm thử hệ thống

Kiểm thử hệ thống là quá trình đánh giá các chỉ số về an toàn thông tin trong một hệ thống để phân tích các điểm yếu trong thiết kế, các sai phạm về kỹ thuật và các lỗ hỏng còn tồn tại.

Các công việc chính khi kiểm thử hệ thống bao gồm:

- Threat Assesment - Xác định mối đe dọa.
- Upgrading Infrastructure - Nâng cấp hạ tầng của phần mềm, phần cứng hoặc trong thiết kế mạng (NT113 reference!!).
- Risk Prevetion and Response - Ngăn ngừa mối nguy và phản hồi, xử lý.
- Security Control Auditing - Kiểm thử lại mức độ hiệu quả của các quyền kiểm soát và truy cập trong bảo mật mạng không dây.
- Data Theft Detection - Phát hiện mất cắp dữ liệu nếu có.
- Information System Management - Thu thập thông tin và ghi nhận lại cho quá trình quản trị hệ thống thông tin.

Quy trình kiểm thử hệ thống

1. Khám phá các thiết bị không dây.
2. Nếu tìm thấy, ghi chép lại các thông tin tìm được.
3. Nếu thiết bị tìm thấy đang sử dụng Wi-Fi, thực hiện tấn công Wi-Fi căn bản để xem chúng có đang dùng mã hóa WEP hay không.
4. Nếu đúng là mã hóa WEP, thực hiện phương pháp pen test dành cho WEP. Nếu không, kiểm tra xem chúng có đang dùng mã hóa WPA/WPA2 không.
5. Nếu đúng là mã hóa WPA/WPA2, thực hiện phương pháp pen test dành cho các mã hóa này. Nếu không, kiểm tra xem chúng có đang dùng mã hóa LEAP.

6. Nếu đúng là mã hóa LEAP, thực hiện phương pháp pen test dành cho mã hóa này. Nếu không, kiểm tra xem WLAN này có phải là WLAN không có mã hóa.
7. Nếu không mã hóa, thực hiện phương pháp pen test dành cho các mạng không mã hóa. Nếu không, thực hiện cách tấn công dùng chung cho các mạng Wi-Fi.

Tóm gọn lại là tấn công nó trước, rồi check coi nó dùng loại mã hóa nào thì pen test theo loại đó. Nếu không xác định được thì dùng phương pháp tổng quan nhất.

1. Pen test tổng quan

1. Tạo một Rogue AP.
2. Gửi gói tin hủy xác thực người dùng.
3. Nếu người dùng bị hủy xác thực rồi cố gắng kết nối lại thì bắt gói tin trong quá trình đó. Kiểm tra xem có cần mật khẩu hay chứng thực gì không.
4. Nếu có cần mật khẩu, dùng công cụ **wzcook** để crack nó hoặc là tiếp tục hủy xác thực người dùng để kiếm thêm thông tin.

2. Pen test LEAP

1. Gửi gói tin hủy xác thực người dùng.
2. Nếu người dùng bị hủy xác thực rồi cố gắng kết nối lại thì bẻ mã hóa LEAP thông qua công cụ như **asleap** hoặc **THC-LEAP Cracker**.
3. Nếu chưa thành công, thực hiện lại bước 1.

3. Pen test WPA/WPA2

1. Gửi gói tin hủy xác thực người dùng.
2. Nếu người dùng bị hủy xác thực rồi cố gắng kết nối lại thì bắt gói tin rồi kiểm tra trạng thái **EAPOL handshake**
3. Nếu bắt được gói **EAPOL handshake**, thực hiện tấn công từ điển để dò ra mật khẩu.
4. Nếu chưa thành công, thực hiện lại bước 1.

4. Pen test WEP

1. Kiểm tra xem SSID có bị ẩn hay không.
2. Nếu không bị ẩn, bắt gói tin và kiểm tra trạng thái của chúng.
3. Sau khi bắt được, bẻ mã hóa WEP thông qua các công cụ như **Aircrack-ng**. Nếu chưa thành công, thực hiện lại bước 1.
4. Nếu là SSID ẩn, hủy xác thực client rồi đợi tiến hành xác thực lại để tìm ra SSID. Sau đó thực hiện bước 3.

5. Pen test WLAN không mã hóa

1. Kiểm tra xem SSID có bị ẩn hay không.
2. Nếu không bị ẩn, bắt gói tin để tìm dãy địa chỉ IP và kiểm tra trạng thái danh sách MAC filter.
3. Nếu có sử dụng MAC filter, giả thành địa chỉ MAC hợp lệ dùng tool như **SMAC** và kết nối tới AP sử dụng địa chỉ IP trong dãy kiếm được.
4. Nếu SSID ẩn, tìm kiếm SSID thông qua công cụ **Aireplay-ng** rồi thực hiện bước 3.

VIII. Bảo mật mạng ngoại vi

A. Tổng quan

Các thuật toán mã hoá không hiệu quả trong việc ngăn chặn các gói tin độc hại đi vào mạng cục bộ. Thay vào đó, Các giải thuật chứng thực có thể được sử dụng để xác định các gói tin đến từ các user tin cậy và giúp ngăn chặn các gói tin độc hại đi vào mạng. Một vấn đề khác lại phát sinh với cách này là các máy tính trong mạng đa số đều không có đủ tài nguyên, phương tiện… để thực hiện các giải thuật chứng thực trong mọi tình huống.

Giải pháp đưa ra: **Kỹ thuật tường lửa - firewall**

Tường lửa được sử dụng như một hàng rào ngăn cách giữa vùng không đáng tin cậy là **mạng Internet** (external network) và vùng có độ tin cậy cao là **mạng nội bộ** (internal network)

Tường lửa có thể là một thiết bị phần cứng, một gói phần mềm hoặc là sự kết hợp của cả hai. Tường lửa có thể được nhúng vào các thiết bị mạng phổ biến như router, switch, modem, wireless access point.

- Tường lửa cứng (phần cứng) nhanh nhưng khó cập nhật.
- Tường lửa mềm (phần mềm) linh hoạt hơn vì dễ dàng cập nhật.

Tường lửa phần cứng

1. Cisco Router
2. FortiNet
3. CheckPoint Safe@Office
4. Sonicwall PRO
5. WatchGuard Firebox

Tường lửa phần mềm

1. Comodo Firewall
2. ESET Smart Security
3. ZoneAlarm

4. Outpost Firewall Pro
5. F-Secure Internet Security

Phân loại theo tính năng đặc trưng

- **Packet filter**: kiểm tra cả IP header lẫn TCP header (Hoạt động ở tầng Network).
- **Circuit gateway** (Hoạt động ở tầng Transport).
- **Application gateway** (Hoạt động ở tầng Application).
- **Dynamic packet filter**: là tường lửa lai, kết hợp cả hai loại packet filter và circuit gateway vào trong một hệ thống tường lửa.

B. Bộ lọc gói tin (Packet Filters)

Là kỹ thuật tường lửa cơ bản. Kiểm tra các gói tin từ bên ngoài đi vào mạng nội bộ và từ mạng nội bộ đi ra bên ngoài.

Đặc điểm:

- Chỉ kiểm tra IP header và TCP header, không kiểm tra phần payload sinh ra từ lớp ứng dụng.
- Sử dụng một tập các quy tắc để quyết định xem gói tin nào được cho phép hoặc bị từ chối đi vào (ra).
- Gồm hai loại là **stateless filtering** (bộ lọc phi trạng thái) và **stateful filtering** (bộ lọc có trạng thái)

1. Stateless filtering

Là kỹ thuật tường lửa đơn giản nhất và được sử dụng rộng rãi nhất.

Đặc điểm:

- Xử lý mỗi gói tin như một đối tượng độc lập
- Kiểm tra một gói tin khi nó đến, ra quyết định phù hợp và không lưu lại bất kỳ thông tin nào về gói tin này.
- Đối với mỗi gói tin, thường kiểm tra Địa chỉ IP nguồn và đích trong IP header, Port nguồn và port đích trong một TCP header hoặc UDP header. Việc kiểm tra được thực hiện dựa theo một tập quy tắc gọi là Access control list (ACL).
- Bộ lọc này không đòi hỏi tính toán nhiều do mặc định tại lớp mạng đã có nhiệm vụ phải kiểm tra IP Header để phân phối gói tin.

Bên dưới là một bảng ví dụ đơn giản về các quy tắc ACL, trong đó int là internal - nội bộ, ext là external - ngoại vi:

int addr int port ext addr ext port action comment

int addr	int port	ext addr	ext port	action	comment
192.166.1.5	*	*	443	allow	Access HTTPS websites
*	*	200.5.12.7	*	block	Block packets to this address

Bộ lọc phi trạng thái thường chặn những kiểu gói tin:

- Một gói đi vào có địa chỉ IP nội bộ giống như địa chỉ IP nguồn nhằm mục đích che giấu chính nó như là một gói tin hợp pháp trong mạng nội bộ.
- Một gói (vào hoặc ra) có quy định cụ thể bộ định tuyến sẽ được sử dụng nhằm mục đích bỏ qua các tường lửa xác định.
- Một gói có phần payload rất nhỏ với mục đích làm TCP header trong phần payload sẽ bị ngắt thành hai hay nhiều phần. Ví dụ như đóng gói port nguồn và port đích trong những gói IP khác nhau. Đây là cách tấn công TCP fragmentation attack.

Ngoài việc chặn những gói tin độc hại đi vào, bộ lọc phi trạng thái còn chặn những gói tin nội bộ đi ra mạng ngoài có đặc tính là những gói điều khiển dùng cho việc thực thi truyền thông trong mạng nội bộ như **Bootp**, **DHCP**, **TFTP**, **NetBIOS**, **LRP** và **NFS**.

Ưu điểm: dễ thực hiện, không cần tính toán nhiều vì chỉ kiểm tra các IP header và TCP header.

Nhược điểm: Không ngăn chặn được các gói tin độc hại khai thác sơ hở của các phần mềm ở tầng ứng dụng; mỗi gói tin phải được kiểm tra đối với toàn bộ ACL, có thể gây nên một nút cổ chai trên một mạng tốc độ cao, dẫn đến thất thoát gói tin và giảm tốc độ truyền ngoài ý muốn.

2. Stateful filtering

Bộ lọc có trạng thái còn được gọi là bộ lọc trạng thái kết nối (connection-state filtering), giữ lại thông tin về kết nối giữa một host nội bộ và một host bên ngoài.

Một trạng thái kết nối chỉ ra đó là kết nối TCP hay UDP và kết nối này có được thiết lập hay không. Trạng thái kết nối được lưu trong một bảng trạng thái (state table).

Khi một gói tin đến (vào hay ra), bộ lọc sẽ kiểm tra xem gói tin này đã có trong bảng trạng thái hay chưa.

- Nếu có, tường lửa sẽ cho gói tin đi qua và lưu lại thông tin (TCP sequence number…) cho lần sau.
- Nếu gói tin này là gói SYN, tường lửa sẽ tạo một entry mới trong bảng trạng thái.
- Nếu gói tin không thuộc về một kết nối đã có và nó không phải là một gói SYN, tường lửa sẽ huỷ nó.

Bất kỳ một port nào được mở bởi một host nội bộ ngầm định sẽ có số port nhỏ hơn 1024 (Số port nhỏ hơn 1024 là port chuẩn). Ngầm định, host bên ngoài sẽ sử dụng số port giữa **1024** và **65535** để thực thi một kết nối với host nội bộ.

Bên dưới là ví dụ về một bảng trạng thái:

client addr	client port	server addr	server port	connection state	protocol
192.166.1.5	1030	129.63.24.84	443	established	TCP
192.168.1.25	1034	129.63.24.84	162	established	UDP

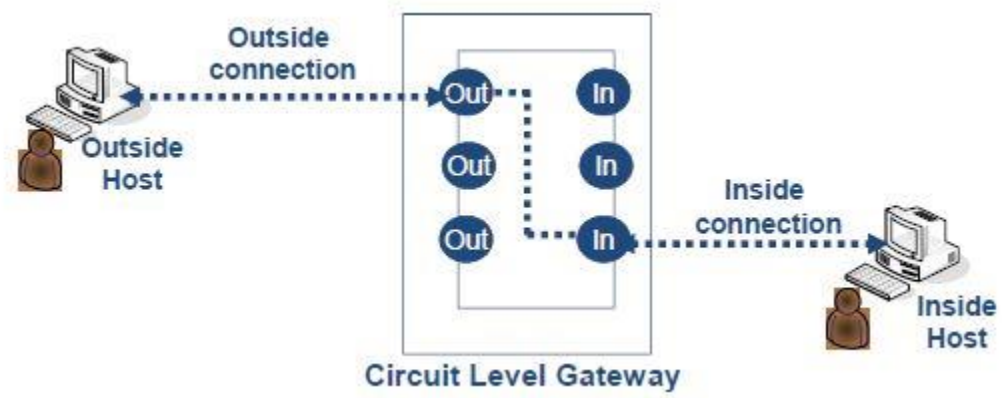
Bộ lọc có trạng thái và bộ lọc phi trạng thái thường được **sử dụng kết hợp với nhau**. Khi gặp khó khăn trong việc xác định chặn một gói dựa trên trạng thái kết nối, **ACL** sẽ được sử dụng để giúp ra quyết định chính xác.

Việc giữ lại các trạng thái kết nối cần đến các cấu trúc dữ liệu phức tạp và các giải thuật tìm kiếm. Thực hiện những công việc này đòi hỏi không gian lưu trữ lớn, hoạt động nhiều hơn của CPU, giảm lưu lượng mạng.

Attacker có thể đưa một số lượng lớn các gói tin vào tường lửa mục tiêu sử dụng bộ lọc có trạng thái, có thể làm ngắt các kết nối giữa mạng nội bộ và bên ngoài. Do đó, khi sử dụng bộ lọc có trạng thái, cần phải chắc chắn rằng có thể quản lý được sự phức tạp giữa thời gian và không gian.

Ví dụ: Thay vì giữ lại toàn bộ thông tin lịch sử của một kết nối, chỉ cần giữ lại thông tin của kết nối này trong một khoảng thời gian nào đó.

C. Cổng mạch (Circuit Gateways)



Cổng mạch (Circuit gateways, còn gọi là Circuit-level gateways), thực thi tại tầng Transport (đôi khi có ngoại lệ mà ngoại lệ khi nào thì mình không biết). Thường kết hợp các bộ lọc gói tin và cổng mạch để tạo ra một **bộ lọc gói tin động** (Dynamic Packet Filter – DFD).

Đối tượng của cổng mạch là chuyển tiếp một kết nối TCP giữa một host nội bộ và một host bên ngoài. Do đó, cổng mạch cũng được xem như là một Transparent Proxy Firewall.

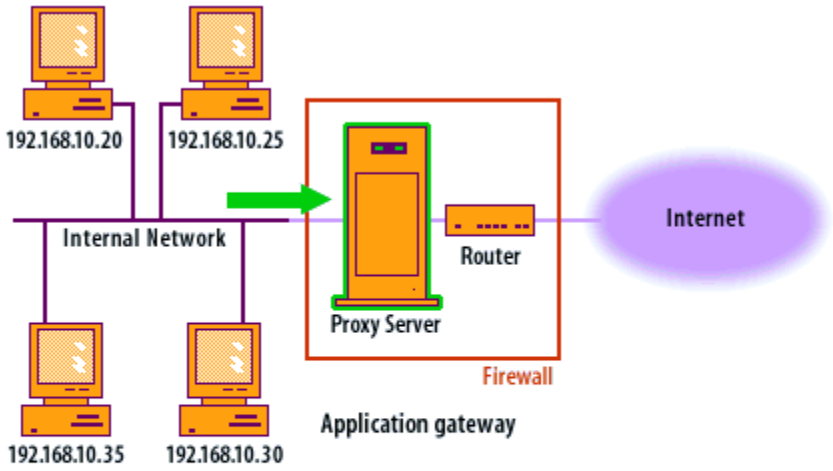
- Trước tiên, cổng mạch sẽ xác nhận một phiên TCP - TCP Session.
- Kế đó cổng mạch thực thi riêng biệt một kết nối với host nội bộ và một kết nối với host bên ngoài.
- Duy trì một bảng các kết nối hợp lệ và duy trì việc kiểm tra các gói tin đi vào với các thông tin chứa trong bảng.

- Cho phép gói tin đi qua nếu thuộc về một kết nối đã có duy trì trong bảng, ngược lại sẽ bị chặn.
- Khi phiên kết thúc, entry tương ứng sẽ bị huỷ khỏi bảng và mạch được đóng lại.

Trong thực tế, một tổ chức thường phân tách mạng nội bộ của mình với mạng ngoại vi bằng một cổng mạch có một địa chỉ IP public có thể kết nối với ngoại vi, và các host trong mạng nội bộ sẽ sử dụng địa chỉ IP private. Sau khi thực thi một kết nối mạng với host ngoại vi và một kết nối mạng với host nội bộ, cổng mạch sẽ đóng vai trò như là một node chuyển tiếp mà **không cần kiểm tra** các gói tin đi qua nó.

Do không cần kiểm tra như vậy, các gói tin độc hại có thể vào mạng nội bộ qua một kênh đã thiết lập sẵn. Vì vậy, cổng mạch nên được **sử dụng cùng với các bộ lọc gói tin** và cần có một tập tin log để ghi nhận lại thông tin của các gói tin (vào, ra) đã xác nhận, bao gồm địa chỉ IP nguồn, port nguồn, địa chỉ IP đích, port đích, và chiều dài của mỗi gói tin.

D. Cổng ứng dụng (Application Gateways)



Internal IP Addressing Scheme

When an internal node initiates a TCP/IP connection through a proxy server, the proxy server receives the request and checks it against a set of configurable filters.

Còn được gọi là **Application-level gateways** (ALG) hay Proxy Servers, là các gói phần mềm được cài đặt trên một máy tính được chỉ định. Một ALG hoạt động như một proxy cho một host nội bộ, xử lý các dịch vụ được yêu cầu bởi các clients ngoại vi.

ALG kiểm tra chi tiết trên mỗi gói IP (vào, ra), bao gồm việc kiểm tra những định dạng chương trình ứng dụng (ví dụ như định dạng MIME, định dạng SQL…) chứa trong gói và xem xét payload của nó có được cho phép hay không.

Giả sử một tổ chức muốn cài đặt một Web server và cho phép các user hợp pháp trên Internet có thể truy cập đến các trang Web này trên Web server.

- Để bảo vệ Web server khỏi bị tổn hại, một phương án phổ biến là cài đặt một cổng ứng dụng như là một proxy cho Web server này, gọi là **Web proxy server**.
- Web proxy server nhận các yêu cầu tại port 80 từ các client ngoại vi và thực hiện kiểm tra chi tiết phần payload của gói tin.
- Chỉ sau khi phần payload này **thoả yêu cầu kiểm tra**, Web proxy server sẽ chuyển gói này đến Web server.
- Web proxy server cũng kiểm tra các trang Web do Web server gửi đến các client ngoại vi và lưu chúng trong cache của nó. Nếu các client khác cũng yêu cầu những trang Web này, Web proxy server sẽ **chuyển trực tiếp** các trang này từ cache đến client mày không cần truy cập đến Web server. Loại Web proxy server này còn được gọi là **cổng ứng dụng** (Cache Gateways). Cổng ứng dụng thường sử dụng với một router có khả năng lọc gói tin. Router này được đặt phía sau gateway để bảo vệ các kết nối giữa gateway và các host nội bộ.

E. Bastion Hosts

Bastion hosts là các máy tính với cơ chế phòng thủ mạnh. Chúng thường được dùng làm cổng ứng dụng, cổng mạch, hoặc các kiểu tường lửa khác. Một bastion host được cài đặt với một hệ điều hành tin cậy và không chứa những chương trình hoặc chức năng không cần thiết nhằm giảm đi những lỗi không đáng có và dễ dàng kiểm tra tính bảo mật.

Gateways hoạt động trên bastion hosts cần phải thoả những điều kiện sau:

1. Phần mềm Gateway chỉ nên viết theo những module nhỏ để dễ dàng cho việc kiểm tra.
2. Một bastion host cần chứng thực các user tại tầng mạng bằng cách xác nhận địa chỉ IP nguồn và đích chứa trong gói IP. Gateways chạy trên bastion host nên chứng thực user độc lập tại một tầng **cao hơn**.
3. Một bastion host chỉ nên kết nối đến một **số lượng nhỏ** những host nội bộ.
4. Bastion hosts nên giữ lại các file log, lưu trạng thái của mỗi phiên TCP.
5. Nếu nhiều gateways đang chạy trên một bastion host, những gateways này cần phải được xử lý một cách độc lập để khi một gateway bất kì bị lỗi sẽ không ảnh hưởng đến phần còn lại.
6. Bastion hosts nên hạn chế ghi dữ liệu lên đĩa cứng của chúng nhằm giảm cơ hội các mã độc hại xâm nhập vào hệ thống.
7. Gateways chạy trên một bastion host không nên được dùng quyền admin hệ thống.

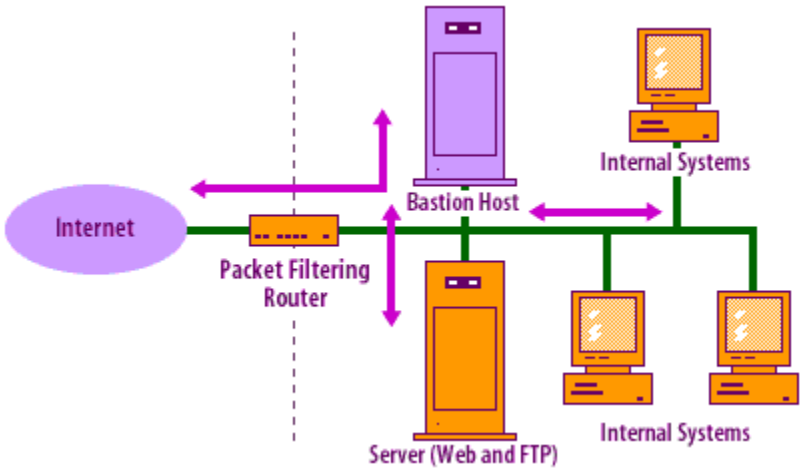
F. Cấu hình tường lửa

Gateways chạy trên một bastion host thườngđược sử dụng với bộ lọc gói tin.

Các cấu hình tường lửa thông dụng:

- Single-Homed Bastion Host System (SHBH)
- Dual-Homed Bastion Host System (DHBH)
- Screened Subnets (SS)
- Demilitarized Zones (DMZ)

1. Single-Homed Bastion Host System

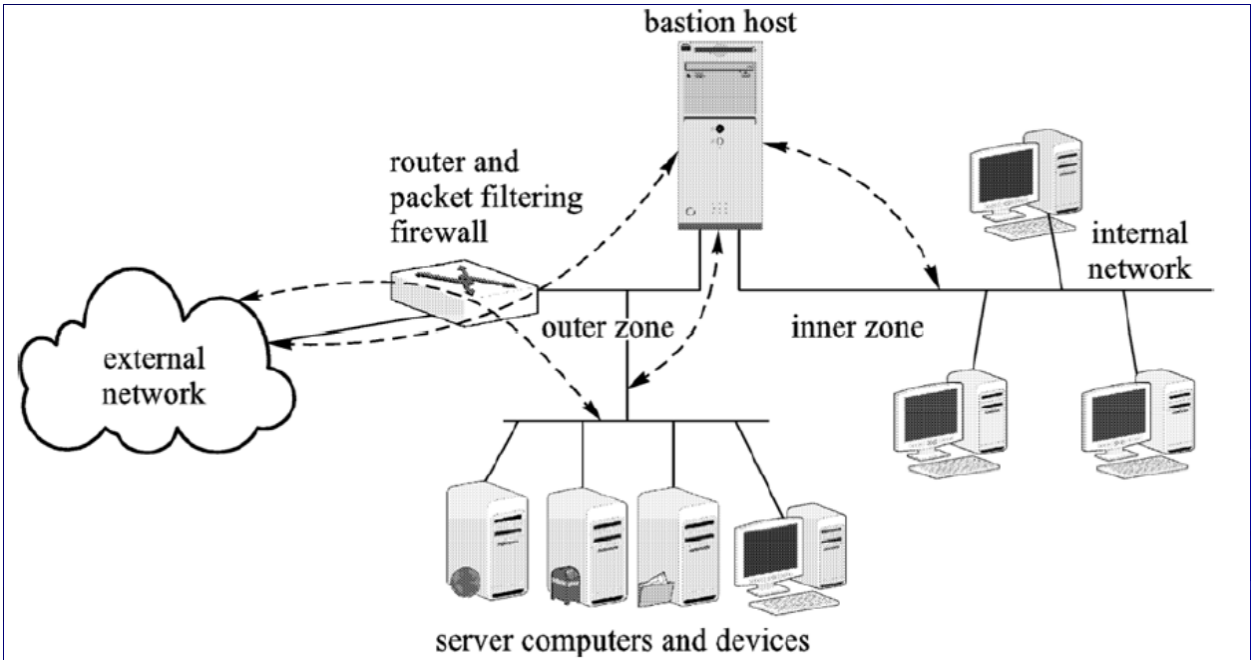


Bao gồm một **packet-filtering router** và một **bastion host**, trong đó router kết nối mạng nội bộ với mạng ngoại vi và bastion host nằm trong mạng nội bộ.

- Router sẽ thông báo ra bên ngoài địa chỉ IP và số port của các server nội bộ. Router sẽ không chuyển tiếp các gói tin đi vào trực tiếp đến các server mà sẽ kiểm tra các gói tin này, sau đó mới chuyển cho bastion host.
- Bastion host tiếp tục kiểm tra gói tin đi vào, nếu thoả, sẽ xác định server nội bộ nào gói tin muốn được chuyển tới.
- Các gói tin từ mạng nội bộ đi ra bên ngoài cũng phải qua bastion host. Bộ lọc gói tin của tường lửa kiểm tra mỗi gói tin đi ra ngoài và ngăn lại nếu địa chỉ nguồn của nó **không phải** là địa chỉ IP của bastion host hoặc không thoả các quy tắc lọc.

Trong một hệ thống SHBH, nếu attacker thoả hiệp được với packet-filtering router thì có thể sửa được các luật trong ACL để bỏ qua bastion host và truyền thông trực tiếp với các host nội bộ. Vấn đề này có thể giải quyết bằng cách sử dụng **Dual-Home Bastion Host** (DHBH).

2. Dual-Homed Bastion Host System

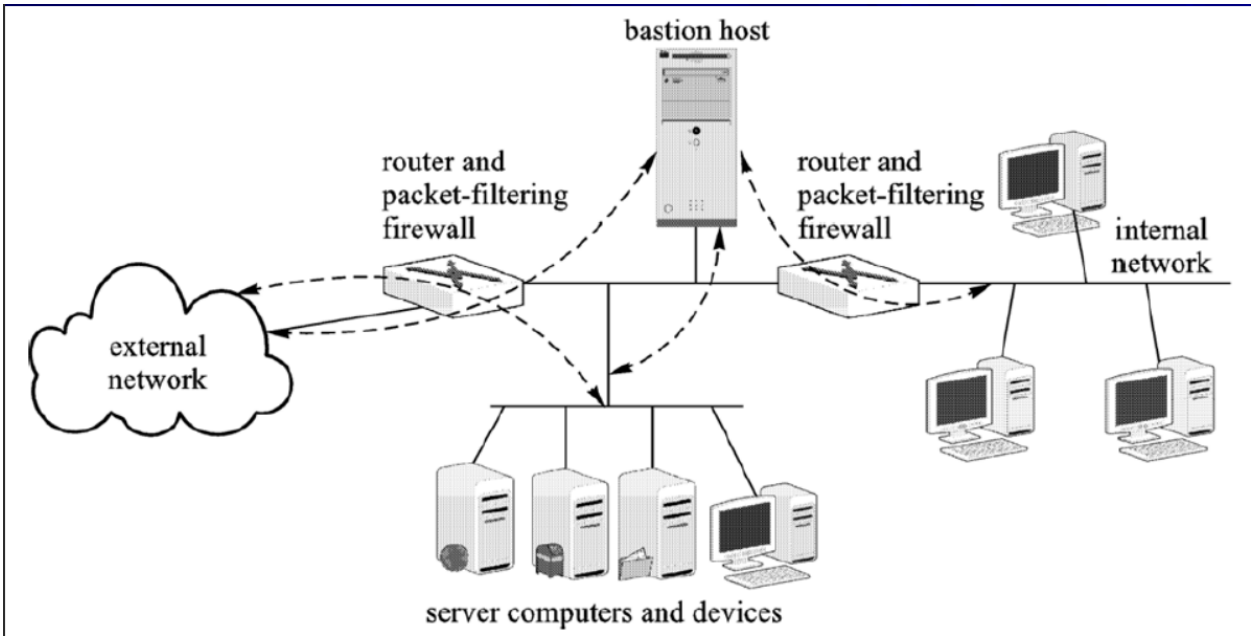


Một DHBH chia mạng nội bộ vào hai zones: inner zone (private zone) và outer zone.

- Địa chỉ IP của các host trong inner zone không thể vươn tới được từ các mạng ngoại vi.
- Địa chỉ IP của các host trong outer zone có thể vươn tới được trực tiếp từ các mạng ngoại vi.
- Router được đặt giữa mạng ngoại vi và outer zone, giữa mạng ngoại vi và bastion host.
- Inner zone trong DHBH chỉ được kết nối đến bastion host nên được bảo vệ bởi cả bastion host và packet-filtering router.
- Các server trong outer zone được bảo vệ bởi packet-filtering router.
- Tương tự như trong hệ thống SHBH, một DHBH cho phép các máy tính server trong outer zone có thể được truyền thông trực tiếp đến Internet mà không cần phải đi qua bastion host.
- ACL trong router cho phép các gói từ ngoài vào đi qua nó nếu địa chỉ nguồn được cho phép, và địa chỉ IP đích cùng số port thoả với địa chỉ IP của máy server cũng như một port đang mở của server này.

Trong hệ thống DHBH, attacker nếu thoả hiệp với packet-filtering router cũng vẫn không thể vượt qua được bastion host.

3. Screened Subnets



Là cấu hình tường lửa **bảo mật nhất**.

Bao gồm một bastion host và **hai** packet-filtering router, là một mạng SHBH với packet-filtering router thứ hai (inner router) chen vào giữa bastion host và mạng nội bộ.

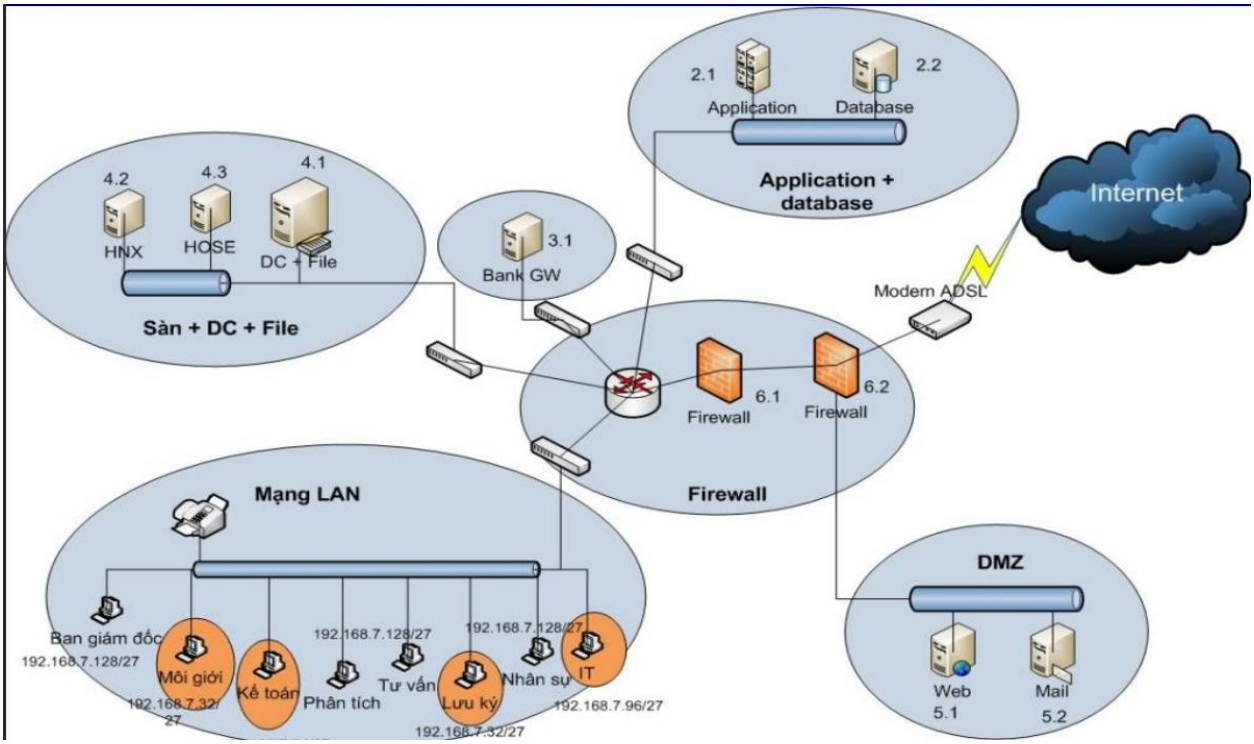
Nói cách khác, trong một Screened Subnet, một router đặt giữa Internet và bastion host, một router khác đặt giữa bastion host và mạng nội bộ. Hai tường lửa lọc gói sẽ tạo ra một screened subnetwork cô lập ở giữa. Các máy tính server và thiết bị nào không cần bảo mật mạnh thường được đặt trong screened subnetwork này.

Trong Screend Subnet:

- **Router ngoài (outer router)** sẽ thông báo cho mạng ngoại vi địa chỉ IP và số port của các máy tính server và thiết bị kết nối đến screened subnetwork.
- **Router trong (inner router)** sẽ thông báo cho mạng nội bộ địa chỉ IP và số port của các máy tính server và thiết bị kết nối đến screened subnetwork.
- Cấu trúc của mạng nội bộ là ẩn với thế giới bên ngoài.
- Có thể di chuyển một số server (database server…) từ screened subnetwork đến mạng nội bộ để cung cấp một sự bảo vệ mạnh hơn.
- Có thể đặt các proxy server tương ứng (chẳng hạn database server) trong screened subnetwork.

Cấu hình này làm tăng tính bảo mật của hệ thống nhưng cũng làm giảm tốc độ xử lý nên trong mỗi ứng dụng cụ thể, cần tìm kiếm những cấu hình tối ưu phù hợp.

4. Demilitarized Zones



Một subnetwork giữa hai tường lửa trong mạng nội bộ thường được xem như một Demilitarize zone (DMZ). Trong đó:

- Tường lửa bên ngoài bảo vệ vùng DMZ với mạng ngoại vi và tường lửa bên trong bảo vệ mạng nội bộvới vùng DMZ.
- Một DMZ có thể có hoặc không có bastion host.
- Các server không yêu cầu bảo mật mạnh được đặt trong vùng DMZ.
- Các máy tính cần phải được bảo mật cao nhất được đặt trong subnet kết nối đến tường lửa bên trong.

G. Chuyển dịch địa chỉ mạng (NAT)

NAT (Network Address Translation Protocol) chia địa chỉ IP vào hai nhóm:

- Nhóm 1 bao gồm các địa chỉ IP công cộng, có thể vươn tới được từ mạng ngoại vi.
- Nhóm 2 bao gồm các địa chỉ IP riêng và không thể vươn tới được một cách trực tiếp từ mạng ngoại vi.

Những thông tin thềm về NAT như NAT tĩnh, NAT động hay PAT, các bạn có thể xem thêm trong bài blog Ôn tập quản trị mạng của mình.

H. TMG – Threat Management Gateway

Forefront Threat Management Gateway 2010 là phiên bản của Microsoft thay thế cho ISA 2006

Những tính năng chính mà TMG cung cấp:

- Firewall
- Secure Web Access
- E-mail Protection
- Intrusion Prevention
- Remote Access
- Deployment and Management
- Subscription Services

Các điểm mới của TMG so với ISA:

- Hỗ trợ Windows Server 2008 R2.
- URL filter.
- E-mail anti-malware, anti-spam.
- Intrusion Prevention.
- Cải tiến UI tốt hơn cho việc quản trị và báo cáo.

Các mô hình mạng trong TMG:

- Edge Firewall
- 3-Leg Perimeter
- Front Firewall
- Back Firewall
- Single Network Adaptor

Chi tiết về các mô hình TMG này mình có thấy một bài viết tổng hợp tại https://securityzone.vn/t/chapter-2-microsoft-firewall-topology.600/. Anh em có thể tham khảo để nắm rõ hơn.

Bảng so sánh cơ chế hoạt động của một số TMG

	SecureNAT Client	**Forefront TMG**	**Web Proxy Client**
Yêu cầu cài đặt	Không cần cài đặt, chỉ cần trỏ default gateway về TMG Server	Phải cài đặt chương trình	Khai báo proxy server trong các trình duyệt web
Hệ điều hành hỗ trợ	Mọi hệ điều hành hỗ trợ TCP/IP	Windows only	Mọi trình duyệt web

	SecureNAT Client	Forefront TMG	Web Proxy Client
Giao thức hỗ trợ	Tất cả	Tất cả	HTTP, HTTPS và FTP
Hỗ trợ chứng thực	Không	Có	Có

Và nội dung trên cũng đã khép lại bài blog quá đỗi dài dòng này. Nếu bạn đọc được đến dòng này thì đáng khâm phục thật đấy, chúc bạn có một kỳ thi cuối kỳ đạt được kết quả cao hơn cả mong đợi!