# Tổng quan

Đầu tiên, chúng ta sẽ tìm hiểu về tam giác CIA nó ko phải là tên viết tắt của tổ chức tinh báo Mỹ :v. Nó là Confidentiality( bí mật), Integrity(toàn vẹn) and Availability(sẵn sàng).

Confidentiality (bí mật): dữ liệu cần được bí mật và riêng tư, nếu bạn không phải là chủ sở hữu bạn sẽ không xem được nó.

Integrity (toàn vẹn): dữ liệu chỉ được thay đổi bởi tác giả, trong quá trình truyền dữ liệu không được thêm vào hay xóa đi.

Availability (sẵn sàng): khi người dùng yêu cầu dữ liệu phải được đáp ứng.

Ví dụ bạn đặt password kết hợp chữ, số, ký tự đặt biệt nó sẽ tăng tính bảo mật nhưng bạn sẽ rất khó để nhớ vì vậy khi cần sử dụng bạn sẽ rất khó khăn.

Authenticity ( xác thực): xác thực người dùng và xác thực đầu vào là đáng tin cậy.

Accountability (trách nhiệm): các hành động của thực thể sẽ được truy tìm khi cần thiết và khi đó kết quả là thực thể duy nhất.

Có 2 dạng tấn công:

Passive (bị động): thu thập thông tin về hệ thống nhưng không ảnh hưởng đến tài nguyên hệ thống. 2 loại thường gặp trong dạng này là: lấy cắp nội dung các tin nhắn và phân tích lưu lượng truy cập. dạng này phòng là chính.

**Dễ ngừng khó phát hiện -> chú trọng phòng chống.**

Active (chủ động): thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến hoạt động của nó. Các loại thường gặp của dạng này: (Masquerade) giả danh, (Replay) gửi lại gói tin, (Modification of mesages) thay đổi nội dung tin nhắn, (Denial of service) từ chối dịch vụ. dạng này cần phải phát hiện xâm nhập và khôi phục lại hệ thống.

**Khó ngừng nhưng dễ phát hiện. -> chú trọng detect và recovery.**

## Security Services (X.800)

Authentication ( Xác thực): đảm bảo rằng thực thể đang giao tiếp là một điều chính xác. Trong trường hợp 1 tin nhắn duy nhất, đảm bảo rằng tin nhắn đó từ một nguồn xác thực. Trong trường hợp tương tác liên tục, đảm bảo rằng 2 thực thể là xác thực và trong kết nối không có sự can thiệp của bên thứ ba, người có thể giả mạo một trong 2 bên giao tiếp.

Hai dịch vụ chứng thực cụ thể được quy định trong X.800:

- Xác thực thực thể Peer
- Xác thực nguồn gốc dữ liệu

Access Control ( kiểm soát truy cập): ngăn ngừa việc sử dụng tài nguyên trái phép. Có khả năng hạn chế và kiểm soát truy cập vào hệ thống máy chủ và ứng dụng bằng các liên kết thông tin. Vì vậy, quyền truy cập phải được xác định và xác thực, phân quyền cho cá nhân.

Data Confidentiality ( Bí mật dữ liệu): bảo vệ dữ liệu không bị tiết lộ trái phép.Bảo vệ truyền dữ liệu khỏi kiểu tấn công thụ động: dịch vụ rộng là bảo vệ tất cả dữ liệu truyền giữa 2 user trong 1 khoảng thời gian; dạng hẹp là bảo vệ một tin nhắn đơn hoặc 1 trường cụ thể trong tin nhắn.

Data Integrity ( toàn vẹn dữ liệu): đảm bảo rằng dữ liệu nhận được là được gửi một thực thể có thẩm quyền. Áp dụng cho 1 dòng tin nhắn, 1 tin nhắn đơn, hoặc trường được chọn trong tin nhắn. Đảm bảo rằng tin nhắn được nhận không bị trùng lặp, thêm, thay đổi, sắp xếp lại, replay.

Non-Repudiation (chống chối bỏ): bảo vệ chống việc chối bỏ trong giao tiếp. Khi một thông điệp được gửi, người nhận có thể chứng minh rằng người gửi bị cáo buộc trên thực tế đã gửi tin nhắn. Khi nhận tin nhắn, người gửi có thể chứng minh rằng người nhận cáo buộc trên thực tế nhận được tin nhắn.

Availability(sẵn sàng): tài nguyên có thể truy cập/ sử dụng.

**Câu 1: What is the OSI security architecture ?**

Kiến trúc bảo mật OSI là khuôn khổ mà cung cấp một cách có hệ thống quy định các yêu cầu cho bảo mật và mô tả đặc tính phương pháp tiếp cận để đáp ứng những yêu cầu.

Tài liệu này định nghĩa các cuộc tấn công an ninh, cơ chế, dịch vụ, và các mối quan hệ giữa các loại

**Câu 2: What is the difference between passive and active security threats ?**

Sol : Các cuộc tấn công thụ động phải thực hiện với nghe trộm, hoặc giám sát, truyền đi. Thư điện tử, chuyển file, và trao đổi giữa client / server (Electronic mail, file transfers, and client/server exchanges ) là những ví dụ của truyền có thể được theo dõi.

Các cuộc tấn công chủ động : bao gồm những việc như sửa đổi các dữ liệu được truyền và nỗ lực để đạt được quyền truy cập trái phép vào hệ thống máy tính.

**Câu 3: List and briefly define categories of passive and active security attacks.**

Sol :

các cuộc tấn công thụ động: release nội dung tin nhắn và phân tích lưu lượng.

các cuộc tấn công chủ động: giả danh (masquerade), phát lại (replay), sửa đổi các thông điệp (modification messages), và từ chối dịch vụ (denial of service).

**Câu 4 : liệt kê và định nghĩa ngắn gọn các loại dịch vụ an ninh ?**

+ Authentication (Sự xác thực) : đảm bảo rằng giao tiếp đối tượng được tuyên bố.

+ Access Control (Kiểm soát truy cập): Phòng chống việc sử dụng trái phép tài nguyên

+ Data Confidentiality (Bảo mật dữ liệu) – bảo vệ dữ liệu không bị tiết lộ trái phép.

+ Data Integrity (Toàn vẹn dữ liệu) - Đảm bảo rằng dữ liệu nhận được khi gửi bởi một đơn vị có thẩm quyền.

+ Non-Repudiation (Không thoái thác) - bảo vệ chống lại sự từ chối của một trong các bên trong một giao tiếp

+ Availability – tài nguyên truy cập / hữu dụng

Câu 5 : liệt kê và định nghĩa ngắn gọn loại **cơ chế bảo mật** ? (security mechanisms)

 Security mechanisms: Được biết đến như là kiểm soát (control).

 Security mechanisms: Tính năng được thiết kế để phát hiện (detect), ngăn chặn (prevent), hoặc phục hồi (recover) từ một cuộc tấn công an ninh.

 Không có cơ chế duy nhất mà sẽ hỗ trợ tất cả các dịch vụ cần thiết

 Tuy nhiên một yếu tố đặc biệt làm nền tảng cho rất nhiều các cơ chế bảo mật được sử dụng: các kỹ thuật mã hóa

# Chương 2 **Kỹ thuật mã hóa cổ điển**

Tìm hiểu về: **mã hóa đối xứng**, **kỹ thuật thay thế**, **kỹ thuật chuyển vị**, **Steganography** (loại này là chèn thông điệp vào bức thư, hình ảnh, chèn vào những thứ quen thuộc mà không ai ngờ tới).

**Có 2 yêu cầu cho việc bảo mật mã hóa:**

Cần 1 giải thuật mã hóa hóa mạnh.

Người gửi và người nhận phải trao đổi khóa 1 cách an toàn và phải giữ bí mật khóa. Nếu 1 người khám phá ra khóa và biết giải thuật, tất cả giao tiếp sẽ bị phá vỡ.

**Phân loại:**

**Theo tổ chức mã hóa**: thay thế và chuyển vị, kết hợp.

Theo khóa: 1, 2.

Theo  xử lý plaintext: block(khối), stream(bit).

Tân công Crytanalysis (phân tích mã hóa) và Brute-force(Quét cạn):

Crytanalysis: Tấn công dựa vào tính chất của thuật toán cộng với một số kiến thức về các đặc điểm chung của các bản rõ. Tấn công khai thác các đặc điểm của thuật toán để cố gắng để suy luận một bản rõ cụ thể hoặc để suy ra khóa được sử dụng.( dựa vào điểm yếu của thuật toán)

Brute-force: Kẻ tấn công cố gắng mỗi khóa có thể trên một phần của ciphertext  cho đến khi thu được 1 plaintext. Tính trung bình, một nửa trong số tất cả các khóa có thể phải cố gắng để đạt được thành công.( dựa vào điểm yếu của khóa).

**Kỹ thuật thay thế:**

Là một trong đó các chữ cái của plaintext được thay thế bằng chữ cái khác hoặc bằng các con số hoặc ký hiệu

Plaintext được xem như là một chuỗi các bit, sau đó thay thế bao gồm việc thay thế các mẫu bit plaintext với các mẫu ciphertext bit.

Kỹ thuật chuyển vị:

Một loại rất khác nhau của bản đồ là đạt được bằng cách thực hiện một số loại hoán vị trên các chữ cái trên plaintext.

**Rail Fence:**

For example, to encipher the message “meet me after the toga party” with rail fence of depth 2, we write the following(chuyển vị)

m e m a t r h t g p r y

e t e f e t e o a a t

 The encrypted message is:

MEMATRHTGPRYETEFETEOAAT

**Caesar Cipher(thay thế):**

plain: meet me after the toga party .

cipher: PHHW PH DIWHU WKH WRJD SDUWB .

**Monoalphabetic Ciphers:**

Dễ phá vì ảnh hưởng tần suất xuất hiện của chữ cái.

**Playfair Ciphers:**

Dựa vào matrix 5x5.

**Vigenère Cipher:**

Ma trận bảng chữ cái.

**Steganography:**

Một thay thế cho mã hóa.

Giấu sự tồn tại của tin:

sử dụng mực vô hình, trốn trong LSB trong hình ảnh đồ họa hoặc file âm thanh, ẩn trong "tiếng ồn" .

Block Ciphers + DES

**Phân biệt Block cipher và Stream cipher:**

1 block cipher là 1 khối plaintext được mã hóa tạo ra ciphertext có độ dài bằng nhau. 1block thường 64 hoặc 128 bits.

1 stream cipher là mã hóa dữ liệu số dòng 1bit hoặc 1byte tại 1 thời điểm.

**Nguyên lý Block Cipher:**

Dựa vào a Feistel Cipher Structure.

Cần thiết vì phải giải mã ciphertext để khôi phục tin  nhắn hiệu quả.

Giống như  thay thế trên vùng rộng lớn.

Cần $2^{64}$ entries cho 64-bit block.

DES sinh ra từ năm 1977.

DES sử dụng 64bits-block nhưng khóa 56bits-key + 8 bit khác có thể được sử dụng như là các bit chẵn lẻ hoặc chỉ đơn giản là thiết lập tùy tiện.

Sử dụng 16 Round cho mã hóa.

Ngày nay, thì AES thay thế cho DES.

**Chapter 03: Mã hóa key công khai**

Người dùng sẽ có 2 khóa 1 public và 1 private.

**Khi A gửi dữ liệu cho B**, **A sẽ dùng public key của B để mã hóa**. B sẽ dùng private key của B để giải mã dữ liệu nhận được.

Khi A muốn ký chữ ký số cho mình: A sẽ dùng private key cuả mình ký vào, bên B sẽ dùng public key của A để kiểm tra chữ ký số.

Ngày nay, thường dùng khóa công khai để mã hóa key của mã hóa đối xứng**. Vì giải thuật mã hóa khóa công khai sử dụng tốt khi mã hóa lượng dữ liệu nhỏ, dữ liệu lớn thường tốn nhiều thời gian**.

Giải thuật RSA dựa trên độ khó của việc "phân tích số nguyên tố".

**Chapter 04A: Hàm Hash.**

**Đặc điểm:**

Giá trị của hàm Hash là giá trị có độ dài xác định dù cho độ dài tin nhắn như thế nào.

Hàm Hash dùng để xác định toàn vẹn dữ liệu.

**Hash functions dùng để chức năng khác:**

**Phát hiện xâm nhập hay virus.**

**Tạo one-way password file.**

**Collision Resistant Attacks:**

Bằng cách nào đó tìm ra H(x)=H(y); có xác suất khi thực hiện $2^{m/2}$.

**SHA1: là 160bits.**

## Chapter 04B: Message Authetication Codes(MAC)

Message authentication là 1 cơ chế hoặc dịch vụ được sử dụng để xác minh tính toàn vẹn của thông điệp.

**Xác định dữ liệu không bi sửa đổi, xóa hoặc replay và danh tính người gửi là xác thực.**

MAC là một thuật toán mà yêu cầu sử dụng 1 khóa bí mật. một MAC có một thông điệp có độ dài biến đổi và một khóa bí mật như là đầu vào và tạo ra mã xác thực.

**Cách Một:** một MAC kết hợp một hàm băm trong 1 số trường hợp với 1 khóa bí mật.

Cách khác**: sử dụng mã hóa khối đối xứng** trong như cách 1 mà nó tạo ra output có độ dài cố định từ input độ dài biến đổi.

**Message Authentication Requirements:**

**Disclosure:** phát hành nội dung tin nhắn cho bất kỳ người nào hoặc quá trình không sở hữu chìa khóa mã hóa thích hợp.

**Traffic analysis**: phát hiện mô hình lưu lượng giữa các bên.

Masquerade: đầu vào của tin nhắn từ 1 nguồn gian lận.

Content modification: Những thay đổi nội dung của một tin nhắn, bao gồm chèn, xóa, chuyển vị, và sửa đổi.

Sequence modification: Bất kỳ sửa đổi cho một chuỗi các thông điệp giữa các bên, bao gồm chèn, xóa, và sắp xếp lại.

Timing modification: Delay hoặc phát lại các tin nhắn.

Source repudiation: nguồn thoái thoát.

Destination repudiation: đích thoái thoát.

MAC : đảm bảo message từ nguồn không bị sửa đổi; xác thực trình tự và thời hạn;chữ ký số đảm bảo chống chối bỏ từ nguồn và đích.

| Hash function: | Message authentication code (MAC) |
|---|---|
| Một chức năng mà ánh xạ một tin nhắn có độ dài bất kỳ  thành một giá trị hash độ dài dài cố định phục vụ như là xác thực. | Một function của thông điệp và một khóa bí mật tạo ra một value độ dài cố định phục vụ như là xác thực. |

**Brute-Force Attacks(Two lines of attack):**

**Attack the key space**

- If an attacker can determine the MAC key then it is possible to generate a valid MAC value for any input x

**Attack the MAC value**

- Objective is to generate a valid tag for a given message or to find a message that matches a given tag.

**Cryptanalysis**

Cryptanalytic attacks seek to exploit some property of the algorithm to perform some attack other than an exhaustive search.

An ideal MAC algorithm will require a cryptanalytic **effort greater than** or equal to the brute-force effort.

There is much more variety in the structure of MACs than in hash functions, so it is **difficult to generalize about the cryptanalysis of MACs**.

Chapter 05: Chữ ký số.

Chữ ký số là một công cụ xác thực để người tạo ra message đính kèm 1 code mà nó hoạt động như 1 chữ ký ngoài đời thật.

Thông thường chữ ký được tạo bằng cách hash of the message and encrypting the message with the creator's private key.

**Chữ ký số đảm bảo nguồn và toàn vẹn của tin nhắn, sử dụng secure hash algorithm(SHA).**

Attacks and Forgeries(tấn công và giả mạo chữ ký):

Attacks:key-only attack, known message attack,generic(chung) chosen message attack, directed(hướng) chosen message attack, adaptive(thích nghi) chosen message .attack

Break success levels: total break,selective forgery(giả mạo chọn lựa), existential forgery(giả mạo hiện hữu).

Digital Signature **Requirements**:

phải phụ thuộc vào thông điệp ký.

phải sử dụng thông tin duy nhất cảu người gửi.

- để ngăn chặn cả hai giả mạo và phủ nhận.

phải tương đối dễ dàng để sản xuất

phải tương đối dễ dàng để nhận ra và xác minh

được tính toán để không thể giả mạo(computationally infeasible to forge):

- với message mới trong trường hợp tồn tại chữ ký số.
- với chữ ký số giả mạo cho thông điệp được đưa.

be practical save digital signature in storage.

**Direct** Digital Signatures:

chỉ liên quan đến người gửi và người nhận.

giả định người nhận có khóa công khai của người gửi.

chữ ký số được thực hiện bởi người gửi ký toàn bộ tin nhắn hoặc băm với private key.

có thể mã hóa bằng cách sử dụng khóa công khai người nhận.

quan trọng là dấu hiệu đầu tiên sau đó mã hóa tin nhắn & chữ ký.

security phụ thuộc vào private-key của người gửi.

**Digital Signature Algorithm** (DSA):

tạo ra một chữ ký 320 bit

với 512-1024 bit an ninh

nhỏ hơn và nhanh hơn so với RSA

a digital signature scheme only

an ninh phụ thuộc vào độ khó của máy tính logarit rời rạc

biến thể của ElGamal & Schnorr án

## Chapter 06: Electronic Mail Security.

**Electronic Mail Security**

Trong hầu như tất cả các môi trường phân phối, thư điện tử là ứng dụng dựa trên mạng **được sử dụng nhiều nhất**.

Người dùng mong đợi để có thể, và làm, gửi e-mail cho những người khác được kết nối trực tiếp hoặc gián tiếp với Internet, **không phụ thuộc host operating system or communications suite.**

Với sự phụ thuộc ngày càng bùng nổ vào e-mail, có mọc một nhu cầu cho các dịch vụ xác thực và bảo mật.

**Hai phương án sử dụng: Pretty Good Privacy (PGP) và S/MIME.**

**Hiện nay nội dung tin nhắn không an toàn:**

- có thể bị kiểm tra hoặc trên đường vận chuyển.
- hoặc bởi người dùng đặc quyền trên hệ thống đích.

**PGP** cung cấp một dịch vụ **bảo mật (confidentiality) và xác thực (authentication)** cái mà có thể được sử dụng đối với thư điện tử và các ứng dụng lưu trữ file.

Những nỗi bật (Enhancements) Email Security:

Confidentiality (Bảo mật): bảo vệ không bị tiết lộ.

Authentication (xác thực): của người gửi tin nhắn.

Message integrity( toàn vẹn tin nhắn): bảo vệ khỏi sửa đổi.

Non-repudiation of origin(Không thoái thác xuất xứ): bảo vệ từ chối bởi người gửi.

**Pretty Good Privacy (PGP):**

sử dụng rộng rãi trên thực tế email an toàn

phát triển bởi Phil Zimmermann

được chọn là **thuật toán mật mã khả dụng tốt nhất** để sử dụng

đc tích hợp vào **một chương trình duy nhất**

**trên Unix, PC, Macintosh và các hệ thống khác**

ban đầu miễn phí, bây giờ cũng có các phiên bản thương mại có sẵn

PGP Operation - **Xác thực(Authentication):**

1. sender creates message
2. make SHA-1160-bit **hash of message**
3. gắn RSA signed hash to message
4. người nhận giải mã và khôi phục hashcode
5. người nhận verifies received message hash.

PGP Operation – **bảo mật (Confidentiality):**

1. sender forms 128-bit random session key
2. encrypts message with session key
3. attaches session key encrypted with RSA
4. receiver decrypts & recovers session key
5. session key is used to decrypt message

PGP – **Authentication & Confidentiality**

Can use both services on same message: ( có thể dùng cả hai dịch vụ trên cùng tin nhắn )

create signature & attach to message

encrypt both message & signature

attach RSA/ElGamal encrypted session key

PGP Operation - Nén ( Compression )

bởi PGP mặc định nén tin nhắn **sau khi ký nhưng trước khi mã hóa**

- để có thể lưu trữ thông điệp không chưa nén & chữ ký để xác minh sau
- & vì nén là không xác định

sử dụng thuật toán nén ZIP

PGP **Operation - Tương thích Email**

Khi PGP được sử dụng, **ít nhất là một phần của khối được truyền đi được mã hóa**

Tuy nhiên email **chỉ được thiết kế cho văn bản**

Do đó PGP phải **mã hóa dữ liệu nhị phân** thành các ký tự ASCII in được

**Sử dụng radix-64 thuật toán**

- bản đồ 3 byte đến 4 ký tự in được
- cũng gắn thêm một CRC

PGP cũng phân đoạn tin nhắn nếu quá lớn

**S / MIME**

- **Secure / Multipurpose Internet Mail Extensions**
- tăng cường bảo mật cho MIME email
  - gốc email Internet RFC822 chỉ là văn bản
  - MIME cung cấp hỗ trợ cho các loại nội dung và tin nhắn đa phần khác nhau
  - với **mã hóa dữ liệu nhị phân** đến **hình thức văn bản**
  - S / MIME **đc thêm tăng cường bảo mật**
- **Có hỗ trợ S / MIME trong nhiều đại lý email**
  - ví dụ như ***MS Outlook, Mozilla, Mac Mail***, vv

**Các Chức năng S / MIME :**

- Dữ liệu đc bao bọc:
  - nội dung và các key liên kết được mã hóa
- Đữ liệu đc ký:
  - encoded message + signed digest
- DDữ liệu đc ký rõ ràng :
  - message cleartext + mã hóa ký digest
- Đữ liệu được ký & đc bao bọc:
  - làm tổ của các thực thể ký & mã hóa

**S/MIME Cryptographic Algorithms:**

Digital signatures: DSS & RSA

Hash functions: SHA-1 & MD5

Session key encryption: ElGamal & RSA

Message encryption: AES, Triple-DES, RC2/40 and others

MAC: HMAC with SHA-1

Have process to decide which algorithms to use

**S / MIME Tin nhắn**

S / MIME bảo mật một thực thể MIME với một chữ ký, mã hóa, hoặc cả hai

Hình thành một MIME bọc đối tượng PKCS

Có một loạt các nội dung loại:

- Dữ liệu được bao bọc
- Dữ liệu được ký kết
- dữ liệu rõ ràng ký
- yêu cầu đăng ký
- Giấy chứng nhận chỉ có tin nhắn

**S / MIME Certificate Processing:**

S / MIME sử dụng giấy chứng nhận X.509 v3

Đc quản lý bằng cách sử dụng một hỗn hợp của một hệ thống cấp bậc nghiêm ngặt X.509 CA & PGP web của niềm tin

mỗi khách hàng có một danh sách các chứng chỉ CA tin cậy

và own public/private key pairs & chứng chỉ

Giấy chứng nhận phải có chữ ký của CA đáng tin cậy

**Certificate Authorities**

đã một số nổi tiếng của CA

Verisign một trong những phổ biến nhất được sử dụng

Verisign vấn đề một số dạng của kỹ thuật số ID

tăng mức độ kiểm tra và do đó tin tưởng

**S / MIME nâng cao Dịch vụ bảo vệ**

3 đề xuất các dịch vụ bảo mật nâng cao:

- ký chứng từ: signed receipts
- nhãn an ninh: security labels
- danh sách gửi thư an toàn: secure mailing lists

**Domain Keys Identified Mails:**

- một đặc điểm kỹ thuật cho các tin nhắn email mã hóa ký
- nên ký miền nhận trách nhiệm
- người nhận / đại lý có thể xác minh chữ ký
- đề xuất tiêu chuẩn Internet RFC 4871
- đã được áp dụng rộng rãi

**Các mối đe dọa email (Email Threats):**

xem RFC 4684- Phân tích các mối đe dọa Tạo động lực cho Thư DomainKeys Identified

mô tả không gian vấn đề về:

- phạm vi : thấp end , kẻ gửi thư rác, những kẻ lừa đảo
- Khả năng về nơi gửi, ký kết, khối lượng, định tuyến đặt tên vv

- kẻ tấn công ngoài vị trí (outside located attackers)

Chapter 07: Transport-Level Security(bảo mật tầng Transport)

Ôn lại:

Secure Socket Layer(SSL) cung cấp security services giữa TCP và Ứng dụng mà sử dụng giao thức TCP.

The Internet standard version is called Transport Layer Service (TLS).

SSL/TLS cung cấp **confidentiality (bảo mật)** sử dụng **symmetric encryption(mã hóa đối xứng)** và **message integrity(toàn vẹn tin nhắn) sử dụng message authentication code(MAC).**

SSL/TLS gồm **protocol mechanisms** (kỹ thuật giao thức) to enable two TCP users to determine the security mechanisms and services they will use.(giữ bảo mật giữa TCP người dùng và dịch vụ họ dùng)

HTTPS tổng hợp giữa HTTP và SSL để hiện thực bảo mật giao tiếp giữa Web browser và Web server.

Secure Shell (SSH) cung cấp đăng nhập từ xa an toàn và tạo điều kiện thuận lợi của khách hàng / máy chủ an toàn khác.

**Web Security**

Bây giờ, Web được sử dụng trong kinh doanh, chính phủ, cá nhân. Internet & Web có lỗ hổng; gặp những đe dọa: toàn vẹn, bảo mật, từ chối dịch vụ, xac thực. Vì vậy, cần thêm vào các kỹ thuật bảo mật.

Phân loại tấn công:

Thụ động: nghe trộm (**eavesdropping**) trên đường truyền browser và server; tiếp cận các thông tin trên 1 trang web. Điều này phải được hạn chế.

Chủ động: **mạo danh (impersonating)** người dùng khác; thay đổi **(altering)** thông điệp trên đường truyền giữa client và server;thay đổi thông tin (**altering information**) trên 1 website.

Phân loại theo vị trí đe dọa: máy chủ Web, trình duyệt Web, và đường truyền mạng giữa các trình duyệt và máy chủ.

**Web Traffic Security Approaches(Phương pháp):**

Một cách là dùng **IP security(IPsec).** Lợi thế của IPsec : transparent (trong suốt) với người dùng cuối và ứng dụng; cung cấp giải pháp general-purpose. Hơn nữa, IPsec bao gồm một khả năng lọc để lưu lượng chỉ được lựa chọn cần phải chịu các chi phí IPsec processing.

Một giải pháp general-purpose khác là hiện thực bảo mật trên tầng TCP. Ví dụ quan trọng nhất của phương pháp này là **Secure Sockets Layer(SSL)** và theo tiêu chuẩn Internet Transport Layer Security (TLS). Ở cấp độ này, có hai lựa chọn thực hiện. Cho tổng quát đầy đủ, SSL (hoặc TLS) có thể được cung cấp như một phần của bộ giao thức cơ bản và do đó được minh bạch để các ứng dụng. Ngoài ra, SSL có thể được nhúng vào trong các gói cụ thể. Ví dụ, Netscape và Microsoft Explorer trình duyệt được trang bị với SSL, và hầu hết các máy chủ Web đã thực hiện các giao thức

**SSL:**

Netscape originated SSL.

Phiên bản 3 của giao thức được thiết kế với công chúng xem xét và đóng góp của ngành công nghiệp và đã được xuất bản như là một dự thảo tài liệu Internet.

Sau đó, khi một sự đồng thuận đã đạt được để nộp cho giao thức chuẩn Internet, các nhóm làm việc TLS đã được hình thành trong IETF để phát triển một **tiêu chuẩn(standard)** chung.

**SSL Architecture**

SSL được thiết kế để sử dụng TCP để cung cấp một dịch vụ đáng tin cậy end-to-end an toàn.

SSL không phải là một giao thức duy nhất mà là hai lớp giao thức.

Cung cấp hai dịch vụ:

• **Bảo mật**: The Handshake Protocol xác định một khóa bí mật chia sẻ đó là sử dụng để mã hóa thông thường trọng tải SSL.

• **Message Integrity**: The Handshake Protocol cũng định nghĩa một khóa bí mật được chia sẻ được sử dụng để tạo thành một mã xác thực thông điệp (MAC).

SSL chia ra SSL session và SSL connection:

Connection: **peer to peer relationships;**

Connection: client and server; được tạo bởi the Handshake protocol.

**SSL Record Protocol Services:**

**Confidentiality:** mã hóa với key tạo bởi Handshake Protocol; thông điệp được nén trước khi mã hóa. AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128.

**message integrity:** MAC; similar to HMAC but with different padding.

**Change Cipher Spec Protocol:**

The Change Cipher Spec Protocol là một trong ba giao thức SSL-cụ thể mà sử dụng SSL Record Protocol, và nó là đơn giản nhất.

Mục đích duy nhất của tin nhắn này là để gây ra các trạng thái chờ đợi để được sao chép vào tình trạng hiện tại, trong đó cập nhật các bộ mật mã được sử dụng trên kết nối này.

**SSL Alert Protocol:**

Được sử dụng để chuyển tải các thông báo SSL-liên quan đến các thực thể ngang hàng.

Như với các ứng dụng khác có sử dụng SSL, các thông điệp cảnh báo được nén và mã hóa.

**SSL Handshake Protocol: ( bắt tay):**

most complex part of SSL is the Handshake Protocol.

Cho phép server và client:

- để **xác nhận lẫn nhau** và
- để **đàm phán một mật mã và thuật toán MAC** và
- **Đàm phán các khóa mật mã** được sử dụng để bảo vệ các dữ liệu được gửi trong một bản ghi SSL.

Bao gồm một loạt các tin nhắn trong giai đoạn

- Thiết lập khả năng bảo mật.
- Authentication Server và Exchange Key
- Client Authentication và Exchange Key
- Finish.

**Cryptographic tính toán**

Hai hạng mục tiếp tục được quan tâm:

việc tạo ra một bí mật tổng thể được chia sẻ bởi các phương tiện của các trao đổi khóa và

- một lần giá trị 48-byte
- tạo ra bằng cách sử dụng trao đổi khóa an toàn (RSA / Diffie Hellman) và sau đó băm thông tin

thế hệ của các thông số mật mã bí mật từ bậc thầy.

- khách hàng bí mật ghi MAC, một máy chủ viết bí mật MAC, một khách hàng ghi chính, một máy chủ ghi trọng, một khách hàng ghi IV, và một máy chủ ghi IV

• tạo ra bằng cách băm mật chủ.

**TLS**

TLS là một sáng kiến tiêu chuẩn IETF mà mục đích là để tạo ra một phiên bản tiêu chuẩn Internet của SSL

với những khác biệt nhỏ

• in record format version number

• sử dụng HMAC cho MAC

• một hàm giả ngẫu nhiên bí mật mở rộng

dựa trên HMAC sử dụng SHA-1 hoặc MD5

• có mã cảnh báo thêm

• một số thay đổi trong thuật toán mã hóa được hỗ trợ

• Những thay đổi trong các loại giấy chứng nhận và các cuộc đàm phán

• Những thay đổi trong tính toán mật mã & đệm.

**HTTPS**

HTTPS (HTTP over SSL)

• combination of HTTP & SSL/TLS to secure communications between browser & server

documented in RFC2818

no fundamental change using either SSL or TLS

use https:// URL rather than http://

• and port 443 rather than 80

encrypts

• URL, document contents, form data, cookies, HTTP headers

connection initiation

• TLS handshake then HTTP request(s)

connection closure

• have “Connection: close” in HTTP record

• TLS level exchange close_notify alerts

• can then close TCP connection

• must handle TCP close before alert exchange sent or completed

SH (Secure Shell)

 protocol for secure network communications

• designed to be simple & inexpensive

 SSH1 provided secure remote logon facility

• replace TELNET & other insecure schemes

• also has more general client/server capability

 SSH2 fixes a number of security flaws

 documented in RFCs 4250 through 4254

 SSH clients & servers are widely available

 method of choice for remote login/ X tunnels

**SSH Transport Layer Protocol**

 server authentication occurs at transport layer, based on server/host key pair(s)

- server authentication requires clients to know host keys in advance

 packet exchange

- establish TCP connection
- can then exchange data

 identification string exchange, algorithm negotiation, key exchange, end of key exchange, service request

- using specified packet format

SSH User Authentication Protocol

 authenticates client to server

 three message types:

- SSH_MSG_USERAUTH_REQUEST
- SSH_MSG_USERAUTH_FAILURE
- SSH_MSG_USERAUTH_SUCCESS

 authentication methods used

- public-key, password, host-based

SSH Connection Protocol

 runs on SSH Transport Layer Protocol

 assumes secure authentication connection

 used for multiple logical channels

- SSH communications use separate channels
- either side can open with unique id number
- flow controlled

• have three stages:

 opening a channel, data transfer, closing a channel

• four types:

 session, x11, forwarded-tcpip, direct-tcpip.

**Port Forwarding**

 convert insecure TCP connection into a secure SSH connection

• SSH Transport Layer Protocol establishes a TCP

connection between SSH client & server

• client traffic redirected to local SSH, travels via tunnel, then remote SSH delivers to server

 supports two types of port forwarding

• local forwarding – hijacks selected traffic

• remote forwarding – client acts for server

Chapter 08: IP Security

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

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

Chức năng xác thực sử dụng HMAC message authentication code.

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

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

IP Security Tổng quan

 Năm 1994, Hội đồng Kiến trúc Internet (IAB) đã đưa ra một báo cáo có tựa đề "An ninh trong kiến trúc Internet" (RFC 1636).

 Báo cáo xác định các khu vực quan trọng cho cơ chế bảo mật.

 Trong số đó là sự cần thiết để bảo đảm cơ sở hạ tầng mạng từ giám sát trái phép và kiểm soát lưu lượng truy cập mạng và sự cần thiết để đảm bảo người dùng cuối của người sử dụng lưu lượng truy cập bằng cách sử dụng xác thực và kỹ thuật mã hóa.

 Để đảm bảo an ninh, IAB bao gồm xác thực và mã hóa như các tính năng bảo mật cần thiết trong các thế hệ tiếp theo IP, mà đã được ban hành như IPv6

 May mắn thay, những khả năng bảo mật được thiết kế để sử dụng được cả với IPv4 hiện tại và IPv6 trong tương lai.

 Điều này có nghĩa rằng các nhà cung cấp có thể bắt đầu cung cấp các tính năng bây giờ, và nhiều nhà cung cấp hiện nay có một số khả năng IPsec trong các sản phẩm của họ.

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

Các ứng dụng của IPsec

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

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

**Lợi ích của IPsec**

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

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

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

 IPsec có thể được minh bạch cho người dùng cuối.

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

ứng dụng định tuyến

IPsec có thể đảm bảo rằng

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

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

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

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

Tài liệu IPsec

 IPsec bao gồm ba khu chức năng:

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

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

 The documents can be categorized into the following groups

- Architecture
  - o RFC4301 Security Architecture for Internet Protocol
- Authentication Header (AH)
  - o RFC4302 IP Authentication Header
- Encapsulating Security Payload (ESP)
  - o RFC4303 IP Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE)
  - o RFC4306 Internet Key Exchange (IKEv2) Protocol
- Cryptographic algorithms

Dịch vụ IPsec

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

 RFC 4301 liệt kê các dịch vụ sau đây:

- Kiểm soát truy cập

• toàn vẹn hướng kết nối

• xác thực nguồn gốc dữ liệu

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

• Tính bảo mật (mã hóa)

• lưu lượng giao thông bảo mật giới hạn

• Other

Chế độ Transport

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

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

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

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

• có thể làm phân tích giao thông nhưng hiệu quả

• tốt cho ESP lưu lượng host-to-host

Chế độ đường hầm(Tunnel mode)

 Tunnel mode cung **cấp bảo vệ cho toàn bộ gói tin IP.**

 Để đạt được điều này, sau khi **các lĩnh vực AH hoặc ESP được thêm vào** gói tin IP, toàn bộ các lĩnh vực gói cộng với an ninh được coi là **payload** của gói IP mới bên ngoài với **một tiêu đề IP mới bên ngoài**

 Toàn bộ ban đầu, nội, gói tin **đi qua một đường hầm** từ một điểm của một mạng IP khác; không có các router trên đường đi có thể kiểm tra các tiêu đề IP bên trong

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

Điểm khác nhau giữa transport mode và tunnel mode:

Transport : bảo vệ upper-layer protocol.

Tunnel: entire IP packet.

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

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

IP Security Policy

 cơ bản để các hoạt động của IPsec là khái niệm về một chính sách an ninh áp dụng cho mỗi gói IP đi qua từ một nguồn đến đích.

 chính sách IPsec được xác định chủ yếu bởi sự tương tác của hai cơ sở dữ liệu,

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

 Security Associations

 Cơ sở dữ liệu Hiệp hội An toàn

 Database Security Policy

 IP Traffic Processing

Hiệp hội bảo mật (SA)

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

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

 xác định bởi 3 thông số:

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

Cơ sở dữ liệu Hiệp hội An toàn (SAD)

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

- Security Parameter Index
- Sequence Number Counter
- Sequence Counter Overflow
- Anti-Replay Window
- AH Information
- ESP Information
- Lifetime of this Security Association
- IPsec Protocol Mode

- Path MTU

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

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

Đóng gói An Ninh Payload (ESP)

 ESP có thể được sử dụng **để cung cấp bảo mật, xác thực nguồn gốc dữ liệu, toàn vẹn phi kết nối, và dịch vụ chống phát lại** (một hình thức toàn vẹn xếp từng phần), và (giới hạn) lưu lượng dòng chảy bảo mật.

 Tập hợp các dịch vụ cung cấp **phụ thuộc vào tùy chọn** đã chọn tại thời điểm Hiệp hội An toàn (SA) thành lập và vào vị trí của việc thực hiện trong một topo mạng.

 ESP **có thể làm việc với một loạt các thuật toán mã hóa và xác thực.**

Mã hóa và xác thực Algs

 Các **Payload Data, Padding, Pad Length, và Next Header** lĩnh vực được **mã hóa** bằng các dịch vụ ESP.

 Nếu thuật toán được sử dụng để mã hóa dữ liệu đồng bộ tải trọng yêu cầu mật mã, chẳng hạn như là một vector khởi tạo (IV), sau đó các dữ liệu có thể được thực hiện một cách rõ ràng vào đầu của trường Payload Data.

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

Padding

 Các trường Padding phục vụ nhiều mục đích:

- mở rộng plaintext đến chiều dài yêu cầu
- để sắp xếp thời gian pad và các lĩnh vực tiêu đề tiếp theo

- Cung cấp một phần bảo mật lưu lượng giao thông

Dịch vụ chống Replay

 replay là khi kẻ tấn công gửi một bản sao của một gói tin xác thực

 số thứ tự sử dụng để ngăn chặn các cuộc tấn công này

 sender khởi tạo chuỗi số 0 khi một SA mới được thiết lập

- tăng cho mỗi gói
- không được vượt quá giới hạn của (2mũ 32) -1

 nhận sau đó chấp nhận các gói tin với số seq trong cửa sổ của (N -W + 1)

Kết hợp Hiệp hội An Ninh

 SA có thể thực hiện một trong hai AH hoặc ESP

 thực hiện cả hai cần phải kết hợp SAs

- tạo thành một bó hiệp hội an ninh
- có thể chấm dứt ở thiết bị đầu cuối khác nhau hoặc cùng
- kết hợp bởi
    - o giao kề
    - o hầm lặp

 kết hợp xác thực và mã hóa

- ESP với xác thực, đi kèm bên trong ESP & AH ngoài, gói vận chuyển bên trong & ngoài ESP

IPSec Key Management

 xử lý thế hệ & phân phối chính

 thường cần 2 cặp phím

- 2 mỗi hướng cho AH & ESP

 dẫn quản lý khoá

- quản trị Sys tay cấu hình mỗi hệ thống

 quản lý khoá tự động

- hệ thống tự động cho vào việc tạo ra nhu cầu của các phím cho SA trong các hệ thống lớn

- có Oakley & ISAKMP yếu tố

**Specific Security Mechanisms (Cơ chế bảo mật cụ thể)**

- Encipherment (Mã hóa)
- Digital signatures (chữ ký số)
- Access controls (kiểm soát truy cập)
- Data integrity (Toàn vẹn dữ liệu)
- Authentication exchange ( Trao đổi xác thực)
- Traffic padding ( đệm lưu lượng)
- Routing control (Kiểm soát định tuyến)
- Notarization (Công chứng)

**Pervasive Security Mechanisms (Cơ chế bảo mật phổ biến )**

- trusted functionality (chức năng đáng tin cậy)
- security labels (nhãn an ninh)
- event detection (phát hiện sự kiện)
- security audit trails (con đường kiểm tra an ninh)
- security recovery (phục hồi an ninh)

## A Model for Network Security

Sử dụng mô hình này đòi hỏi chúng ta:

- Thiết kế một thuật toán thích hợp cho việc chuyển đổi an ninh
- Tạo ra các thông tin bí mật (các khóa) được sử dụng bởi các thuật toán
- Phát triển các phương pháp để phân phối và chia sẻ các thông tin bí mật