Tài liệu tự đọc trước khi đến lớp

Kết hợp nội dung chương 7 trong tài liệu học tập học phần mạng máy tính và truyền số liệu.

Anh chị sinh viên đọc trước theo hướng dẫn ở nội dung dưới đây:

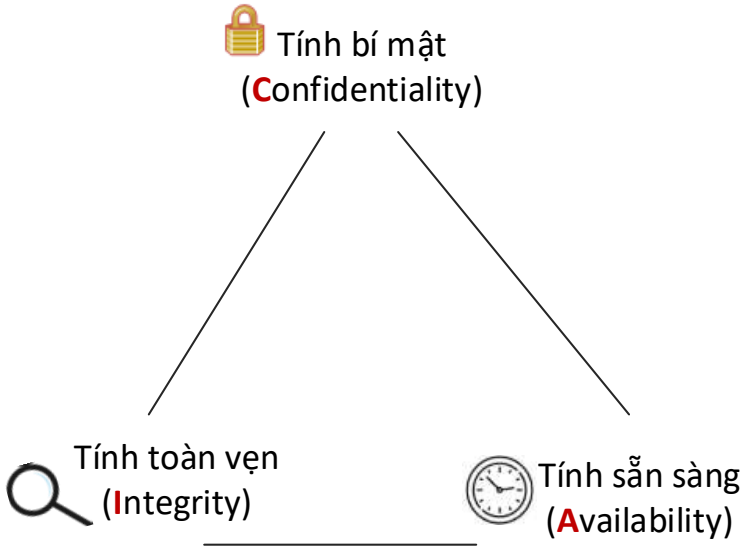
7.1. Giới thiệu

7.1.1. Khái niệm và đặc điểm của an ninh mạng

a) Định nghĩa : An ninh mạng (Cybersecurity) là tập hợp các biện pháp, công nghệ và quy trình nhằm bảo vệ hệ thống mạng, dữ liệu và thông tin khỏi các cuộc tấn công, truy cập trái phép, đánh cắp dữ liệu và các rủi ro khác. Mục tiêu của an ninh mạng là đảm bảo tính bảo mật (Confidentiality), toàn vẹn (Integrity) và sẵn sàng (Availability) của thông tin — gọi tắt là mô hình CIA[9].

Mô hình CIA trong an ninh mạng gồm:

- Confidentiality (Tính bảo mật): Thông tin chỉ được truy cập bởi người được phép.
- Integrity (Tính toàn vẹn): Dữ liệu không bị thay đổi trái phép.
- Availability (Tính sẵn sàng): Hệ thống hoạt động liên tục, truy cập được mọi lúc.



Hình 7.1. Mô hình an ninh mạng CIA

Ví dụ: Trang web ngân hàng bị tấn công DDoS → vi phạm Availability.

b) Vai trò của an ninh mạng (sinh viên tự tìm hiểu, xem chương 7 - TLHT)

7.1.2. Các mối đe dọa an ninh mạng phổ biến

Bảng 7.1. *Phân loại tấn công mạng*

Loại tấn công	Mô tả	Ví dụ thực tế
Malware	Mã độc làm hỏng hệ thống	WannaCry 2017

Loại tấn công	Mô tả	Ví dụ thực tế
Phishing	Email/website giả mạo	Giả mạo trang web ngân hàng
DDoS	Gửi ồ ạt gói tin, nghẽn máy chủ	Trang TMĐT ngừng hoạt động
Social Engineering	Dùng tâm lý người để khai thác	Giả mạo nhân viên IT

7.2.1. Kỹ thuật mã hóa

AES(**A**dvanced **E**ncryption **S**tandard) – *Mã hóa đối xứng:*

- Sử dụng cùng 1 khóa cho mã hóa và giải mã
- Nhanh, phù hợp truyền dữ liệu lớn
- 128/192/256-bit, dùng cho VPN, Wi-Fi

Ví dụ: Các thuật toán mã hóa đối xứng tiêu biểu gồm: DES, 3DES, AES, Blowfish, ChaCha20.

Đặc điểm của AES:

AES hoạt động dựa trên cấu trúc mạng thay thế và hoán vị với các bước lặp (rounds) để làm phức tạp dữ liệu ban đầu. Tùy thuộc vào độ dài khóa sử dụng, AES có thể có 10, 12 hoặc 14 vòng lặp tương ứng với các khóa có độ dài lần lượt là 128-bit, 192-bit và 256-bit. Độ dài khóa càng lớn thì càng đảm bảo tính bảo mật của dữ liệu. Tuy nhiên, AES có tốc độ mã hóa và giải mã rất nhanh, phù hợp với các ứng dụng yêu cầu xử lý dữ liệu thời gian thực như VPN, bảo mật Wi-Fi và các dịch vụ tài chính.

Chế độ hoạt động của AES:

- ECB (Electronic Codebook),
- CBC (Cipher Block Chaining),
- GCM (Galois/Counter Mode)

Trong đó CBC và GCM được ưa chuộng vì đảm bảo tính toàn vẹn của dữ liệu.

Ví dụ:

- Wi-Fi Security: Các chuẩn bảo mật Wi-Fi như WPA2 và WPA3 sử dụng AES với khóa 128-bit hoặc 256-bit để mã hóa lưu lượng mạng.
- Ngân hàng và thanh toán: Các giao dịch trực tuyến qua thẻ tín dụng đều sử dụng mã hóa AES để bảo vệ dữ liệu người dùng.

Ưu điểm và nhược điểm của AES:

- Ưu điểm: Tốc độ cao, bảo mật tốt, đã được kiểm chứng rộng rãi.
- Nhược điểm: Cần quản lý khóa hiệu quả để tránh bị đánh cắp hoặc lộ lọt.

RSA (**R**ivest-**S**hamir-**A**dleman) – *Mã hóa bất đối xứng:*

- 2 khóa: public key (mã hóa), private key (giải mã)
- Bảo mật khi trao đổi dữ liệu giữa 2 bên xa lạ

- Ứng dụng: SSL/TLS, email, chứng chỉ số

Bảng 7.2. So sánh AES vs RSA

Tiêu chí	AES	RSA
Loại mã hóa	Đối xứng (Symmetric)	Bất đối xứng (Asymmetric)
Số lượng khóa	01 (bí mật)	02(1 public, 1 private)
Độ dài khóa	128-bit, 192-bit, 256-bit	2048-bit đến 4096-bit
Tốc độ	Nhanh	Chậm hơn
Trao đổi khoa	Cần kênh an toàn	Không cần kênh an toàn
Ứng dụng	VPN, Wi-Fi, ngân hàng	SSL/TLS, email, chứng chỉ số
Bảo mật	Bảo mật cao nhưng phụ thuộc vào quản lý khóa	Bảo mật cao, không cần chia sẻ khóa riêng tư

Kết luận:

- AES phù hợp với các ứng dụng yêu cầu tốc độ xử lý cao và xử lý khối lượng dữ liệu lớn.
- RSA phù hợp với việc trao đổi khóa và các ứng dụng yêu cầu bảo mật cao nhưng không thường xuyên.

7.2.2. Kỹ thuật xác thực

- Mật khẩu: dễ dùng nhưng rủi ro cao, cần lưu dạng băm (SHA-256, bcrypt...)
- OTP: mã dùng 1 lần, thường gửi qua SMS, app Authenticator
- 2FA: kết hợp mật khẩu + OTP, hoặc vân tay + mã OTP → an toàn hơn

Câu hỏi tự kiểm tra

1. Tính "Availability" trong an ninh mạng là gì?
2. Khác nhau của AES và RSA là gì?
3. OTP khác mật khẩu thường như thế nào?
4. Tại sao dùng 2FA vẫn có thể bị hack?

Yêu cầu chuẩn bị trước khi đến lớp

- Cài Python 3 + VSCode
- Cài thư viện:

```
pip install pycryptodome
pip install pyotp
```

Thư viện **pycryptodome**:

PyCryptodome = “Python Cryptographic DOMEstic library”

Đây là phiên bản kế thừa và mở rộng của thư viện PyCrypto (đã lỗi thời), được phát triển mới để hỗ trợ tốt hơn Python 3.

Thư viện pycryptodome là một thư viện mã hóa mạnh mẽ cho Python, dùng để thực hiện các thuật toán mật mã hiện đại, bao gồm:

- Mã hóa đối xứng: AES, DES, ChaCha20...
- Mã hóa bất đối xứng: RSA, ECC...
- Băm (hashing): SHA256, SHA3...
- Chữ ký số (digital signature), xác thực (HMAC)...

Thư viện **pyotp**:

Thư viện pyotp là một thư viện Python mã nguồn mở dùng để tạo và xác thực OTP (One-Time Password) – tức mã xác thực dùng một lần, thường thấy trong các hệ thống xác thực hai yếu tố (2FA) như:

- Ngân hàng gửi mã SMS
- Google Authenticator sinh mã 6 chữ số mỗi 30 giây
- Xác minh bảo mật khi đăng nhập từ thiết bị lạ

Thực hiện cài đặt các thư viện pycryptohome và pyotp trên windows pro 10/11 như sau:

Trong cửa sổ cmd (chế độ Administrator) gõ lệnh:

C:\WINDOWS\system32>`python -m pip install pycryptodome`

Kết quả:

```
Collecting pycryptodome
  Downloading pycryptodome-3.23.0-cp37-abi3-win_amd64.whl.metadata (3.5 kB)
Downloading pycryptodome-3.23.0-cp37-abi3-win_amd64.whl (1.8 MB)
   ---------------------------------------- 1.8/1.8 MB 210.7 kB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.23.0
```

Cài thư viện **pyotp**

C:\WINDOWS\system32>`python -m pip install pyotp`

Kết quả thực hiện:

```
Collecting pyotp
  Downloading pyotp-2.9.0-py3-none-any.whl.metadata (9.8 kB)
Downloading pyotp-2.9.0-py3-none-any.whl (13 kB)
Installing collected packages: pyotp
Successfully installed pyotp-2.9.0
```

- Thực hiện file code mẫu bài thực hành trong TLHT chương 7.

Bài thực hành 1: Mã hóa đối xứng và bất đối xứng (AES và RSA).

Bài thực hành 2: Xác thực bằng mật khẩu, OTP và 2FA