# Bài 1. Tổng quan về an ninh mạng

## 1. Một số khái niệm

- Hai trạng thái dữ liệu:

+ Transmission state (truyền)

+ Storage state (lưu trữ)

- Bốn yêu cầu của dữ liệu:

+ Confidentiality (bảo mật)

+ Integrity (toàn vẹn)

+ Non-repudiation (không thể từ chối)

+ Availability (sẵn sàng)

Tam giác bảo mật: Security , Functionality và Usability (An ninh, chức năng và khả năng sử dụng)

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

- Eavesdropping (nghe trộm)

+ Nghe trộm là 1 phương pháp cũ hiệu quả.

+ Sử dụng thiết bị mạng (router, card mạng...) và chương trình (Tcpdump, Wireshark…) để giám sát lưu lượng mạng, bắt gói tin đi qua thiết bị.

+ Thức hiện dễ dàng hơn với mạng không dây.

+ Không thể ngăn chặn trong mạng công cộng.

+ Cách chống: mã hóa dữ liệu trước khi gửi đi trên mạng.

- Cryptanalysis (phá mã)

+ Tìm kiếm thông tin từ dữ liệu đã mã hóa mà ko cần khóa.

+ Sử dụng các công cụ toán học và máy tính có hiệu suất cao.

+ Cách chống:

1. Sử dụng những giải thuật mã hóa không thể hiện cấu trúc thống kê trong chuỗi mật mã (Vd: Ceasar…)
2. Khóa có độ dài lớn để chống Brute-force attack

- Password pilfering (ăn cắp mật khẩu)

+ Cơ chế chứng thực đc sử dụng rộng rãi nhất là dùng username và password.

+ Các phương pháp:

1. Guessing (đoán)
2. Social engineering (xã hội) – Vd: gửi mail lừa đảo để đánh cắp mật khẩu
3. Dictionary (từ điển) – 1 từ điển trong giới hacker lưu trữ các username và password thông dụng (chứa trong file SAM).
4. Password sniffing (nghe lén mật khẩu).

- Identity Spoofing

+ Cho phép kẻ tấn công mạo nhận nạn nhân mà không cần sử dụng mật khẩu nạn nhân

+ Các phương pháp:

1. Man-in-the-middle attacks. (kẻ tấn công chèn vào giữa để nghe lén)
2. Message replays attacks. (ngăn chặn chứng thực và giữ 1 bản sao chứng thực sử dụng nó sau này để mạo nhận (đóng vai) người dùng A để có được các dịch vụ từ hệ thống)
3. Network spoofing attacks. IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng

+ SYN flooding: 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: sử dụng các gói tin giả mạo để chiếm đoạt một kết nối giữa máy tính nạn nhân và máy đích

+ ARP spoofing (ARP poisoning): 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

1. Software explotation attacks.

- Buffer-Overflow Exploitations:

+ Quá trình ghi dữ liệu vào bộ đệm nhiều hơn kích thước khả dụng của nó

- Repudiation

+ Bác bỏ dữ liệu để tránh hậu quả pháp lý.

+ Sử dụng các thuật toán mã hóa và xác thực để giúp ngăn ngừa.

- Intrusion

+ Xâm nhập bất hợp pháp vào 1 mạng để truy cập vào hệ thống máy tính của người khác nhằm mục đích đánh căp thông tin, tài nguyên máy tính hoặc băng thông cá nhân.

+ Nguyên nhân: cấu hình sơ hở, giao thức sai, mở các cổng UDP hoặc TCP không cần thiết.

+ Cách khắc phục: đóng các cổng UDP và TCP không cần thiết.

+ Công cụ: IP scan và Port scan vừa là công cụ cho hacker vừa là công cụ giúp người dùng kiểm tra các lỗ hổng của hệ thống.

- Denial of Service Attacks (DoS): ngăn chặn người dùng hợp pháp sử dụng những dịch vụ mà họ thường nhận được từ các máy chủ bằng cách buộc máy tính mục tiêu phải xử lý một số lượng lớn thông tin, làm tiêu tụ tất cả nguồn tài nguyên quan trọng

+ Các hình thức tấn công cơ bản:  
 1) Smurf

1. Buffer overflow attack
2. Ping of death
3. Teardrop
4. SYN attack

- Distributed DoS (DdoS)

+ Các hình thức tấn công cơ bản:

1. Sử dụng Trojan kiểm soát nhiều máy tính nối mạng.
2. Hacker cài đặt phần mềm zombie lên các máy tính này để tạo ra 1 đội quân zombie để tấn công DDoS sau này trên máy nạn nhân.
3. Phát lệnh tấn công vào các máy tính zombie để khởi động 1 cuộc tấn công DoS trên cùng 1 mục tiêu cùng 1 lúc.

- Malicious Software

+ Các phần mềm độc hại bao gồm:

1. Virus. (Sao chép chính nó, không đứng 1 mình mà phải gắn vào tập tin khác, chạy khi chạy chương trình bị nhiễm, có thể lây lan)
2. Worms. (Giống Virus nhưng là chương trình độc lập, không cần vật chủ)
3. Trojan horses. (không lây lan, chỉ thực hiên khi người dung chạy chương trình bị nhiễm trojan)
4. Logic Bombs. (chương trình con được nhúng vào chương trình khác, tự kích hoạt sau khi thỏa những diều kiện nhất định)
5. Backdoors. (mã độc tạo cửa sau)
6. Spyware. (bao gồm Browser Hijacking: kĩ thuật thay đổi thiết lập trình duyệt người dùng và Zombieware: phần mềm biến máy tính người dùng trở thành zombie để tấn công DDoS.

**3. Lý lịch của những kẻ tấn công**

- Các attacker có thể là:

+ Black-hat hacker (một nhóm người ưu tú, có tri thức, chuyên môn tốt về máy tính, bao gồm hackers mũ đen, hackers mũ trắng và hackers mũ xám).

+ Script kiddies (chỉ biết sử dụng tool của người ta viết ra để tấn công chứ ko am hiểu)

+ Cyber spies (hackers hoạt động trên lĩnh vực quân sự, kinh tế…).

+ Vicious employees (hoạt động như gián điệp mạng để thu thập và bán bí mật công ty).

+ Cyber terrorrists (sử dụng máy tính và công nghệ mạng làm công cụ phá hoại tài sản công cộng và cuộc sống của nhiều người vô tội nên cực kì nguy hiểm).

**4. Mô hình bảo mật cơ bản**

- Bao gồm 4 thành phần:  
+Hệ thống mã hóa (Cryptosystem): sử dụng mật mã và các giao thức bảo mật (giao thức mã hóa, giao thứ chức thực, giao thức quản lý khóa) để bảo vệ dữ liệu.

+ Tường lửa (Firewall): gói phần mềm cài trên máy tính hoặc thiết bị mạng để kiểm tra các gói tin đi vào và đi ra trên mạng.

+ Hệ thống phần mềm chống độc hại (Anti-Malicious System software – AMS software): quét thư mục, hệ thống, tập tin, registry => Nhận diện, cách ly hoặc xóa các mã độc hại.

+ Hệ thống tìm kiếm xâm nhập (Intrusion Detection System – IDS): giám sát việc đăng nhập và hành vi của người dùng, phân tích file log để nhận diện và đưa ra cảnh báo khi phát hiện có sự xâm nhập.