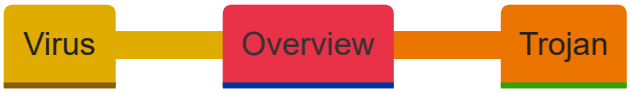
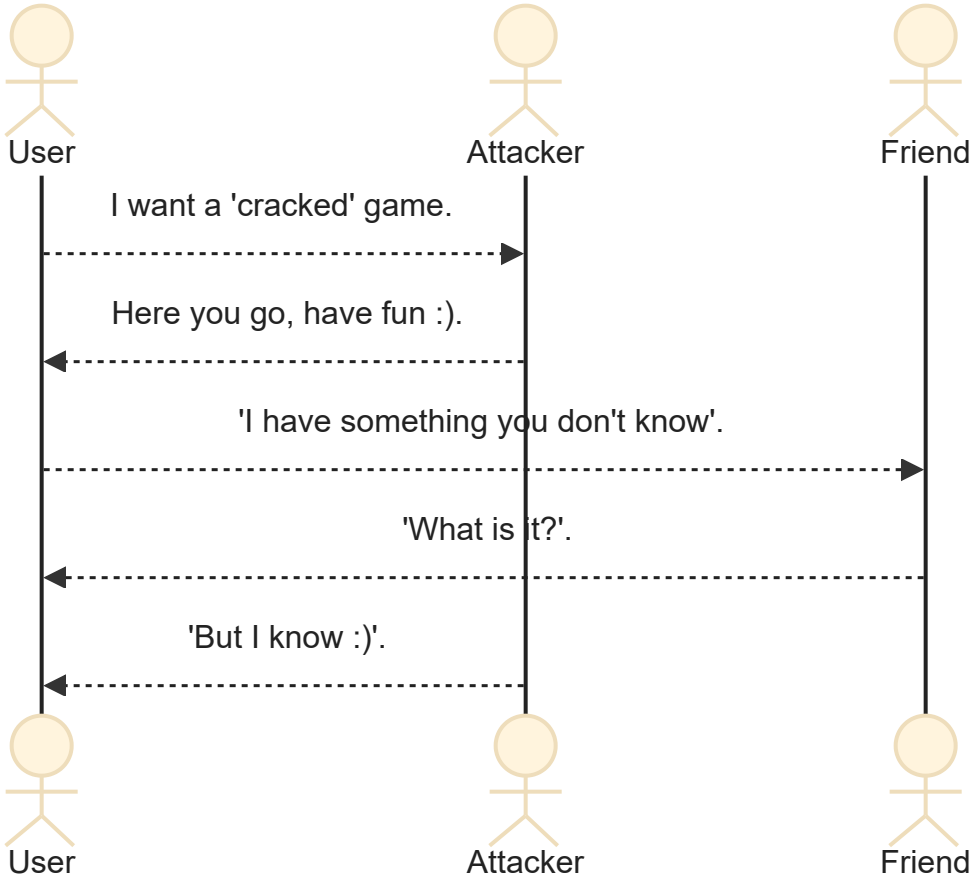
Ôn tập NT101 - An toàn mạng máy tính

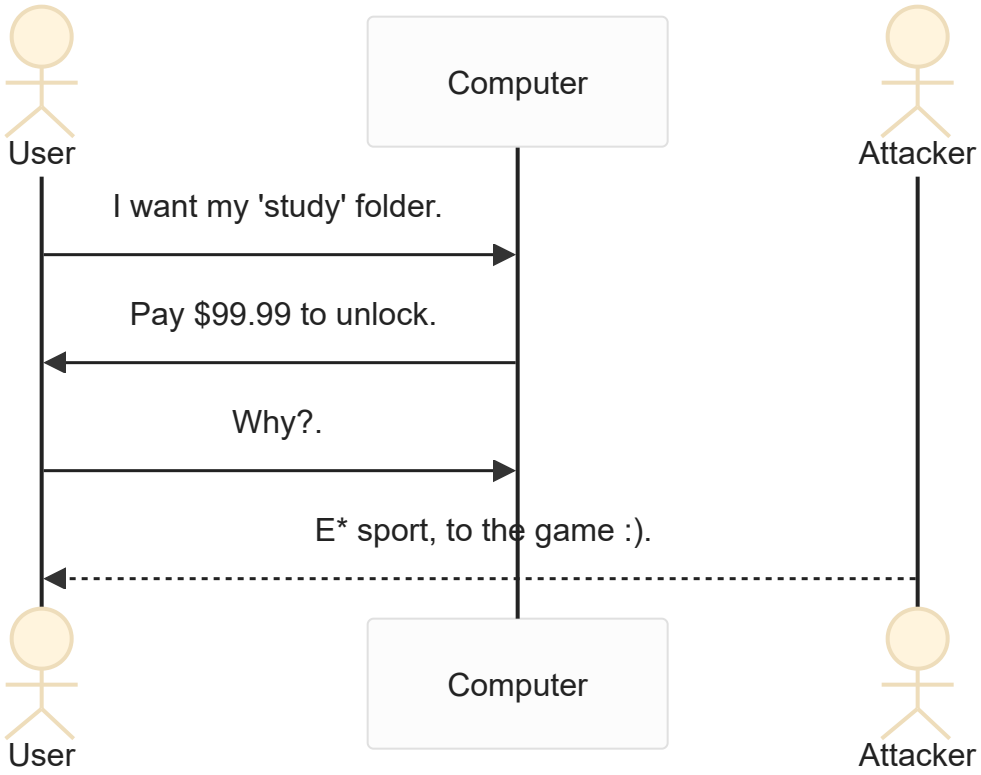
Trojan



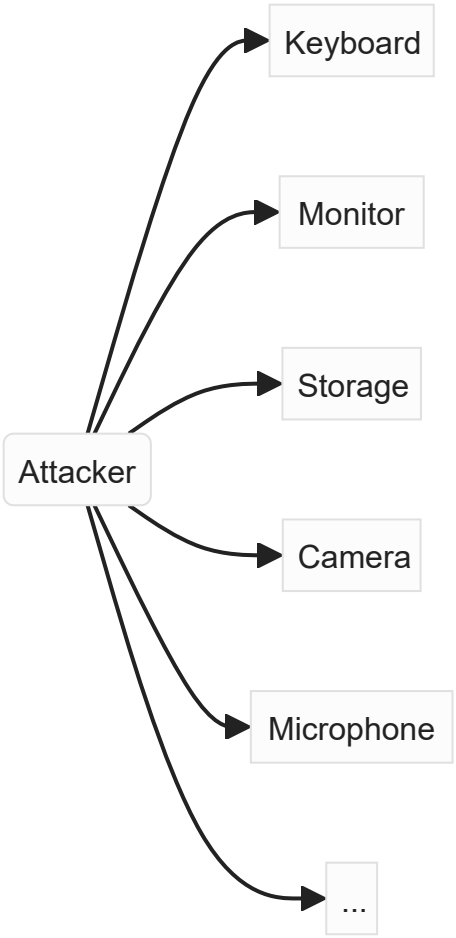
- Trojan:
  - A piece of malware or virus, attacker install on devices for malicious purposes.
  - Appear as a legit file.
  - A Trojan horse cannot manifest by itself, the executable (.exe) file should be implemented and the program installed for the Trojan to attack a device's system.
  - Zoombie computer: attackers have remote control of user computer without the user knowing.
  - Botnet: a network of infected devices.
  - Examples:
    - Backdoor trojan:



    - Ransomeware trojan:



- Remote Access Trojan (RAT):
  - Include 2 files: server, client.
  - Run in background, allow attackers to remote access through specific port.
  - Ex: Back orifice, Girlfriend, Netbus ...



- Keylogger:
  - Availible in 2 types: hardware, software.
  - Record keyboard typing.
  - Good: monitor children on the internet ...
  - Bad: Steal password.
  - 3 parts:
    - Program: monitor activities.
    - Hook file: record typing, screen capture.
    - Log file: record hook history.
- Trojan coutermeasures:
  - Avoid email from unknown.
  - Update OS.
  - Block unnecessary ports.
  - Use antivirus software.

Các kỹ thuật tấn công phổ biến

- Eavesdropping(nghe trộm):
  - Không chặn được việc nghe trộm trong mạng công cộng.

    - Cách chống: mã hóa đường truyền trước khi gửi.
        - Plaintext: văn bản gốc.
        - Cyphertext: chuỗi mật mã.
        - Key: khóa.
- Cryptanalysis(phân tích mã):
    - Tìm thông tìn từ dữ liệu mã hóa không cần giải mã.
    - Sử dụng toán học, máy tính hiệu suất cao ...
    - Các chống: sử dụng thuật giải mã hóa không thể hiện cấu trúc thống kê, khóa có độ dài đủ lớn.
- Password pilfering(đánh cắp mật khẩu):
    - Guessing(đoán mã):
        - Hiệu quả với mật khẩu ngắn hoặc người dùng quên đổi mật khẩu ngầm định.
    - Social engineering:
        - Mạo danh.
        - Lừa đảo.
        - Thu thập thông tin từ giấy tờ bỏ đi.
        - Tạo website giả mạo.
    - Dictionary attacks:
        - Duyệt tìm từ một từ điển (thu được từ các file SAM...) các username và password đã được mã hóa.
        - Chỉ những mật khẩu mã hóa mới được lưu trên máy tính.
    - Password sniffing:
        - Là một phần mềm bắt các thông tin đăng nhập từ xa đối với các ứng dụng mạng phổ biến như Telnet, FTP, SMTP, POP3.
        - Chống: Có thể dùng những chương trình đặc biệt (như SSH trong HTTPS) để mã hóa thông điệp truyền đi.
        -

        ...
- Identity spoofing:
    - Giả mạo nạn nhân không cần xác minh.
    - Man-in-the-middle: hacker dùng thiết bị mạng, nạn nhân kết nối vào, hacker sẽ nhận được message giữa 2 nạn nhân và có thể sửa đổi -> mã hóa, chứng thực cho chắc.
    - Message replays: hacker chặn gói tin chứa certificate, dùng nó để giả mạo nạn nhân.
    - Network spoofing:
        - SYN flooding: lấp đầy bộ đệm **TCP** gói SYN của nạn nhân -> không thể liên lạc máy khác.

        - TCP hijacking: sử dụng gói tin fake, chiếm kết nối của nạn nhân tới đích -> TCP Wrapper kiểm tra IP tại Transport.
        - ARP spoofing: thay địa chỉ MAC đích thành của hacker -> kiểm tra tên miền, make sure gói tin k đổi địa chỉ khi truyền.
- Buffer-overflow exploitation:
    - Data vô > buffer size -> tràn.
    - Các hàm **strcat, strcp, sprintf, vsprintf, bcopy, get, scanf ..** trong **C**.
- Repudiation:
    - Tấn công bác bỏ: thiếu tính pháp lý, xác thực -> someone có thể không thừa nhận việc làm của bản thân (trốn tội).
    - Dùng mã hóa, xác thực -> hết chối.
- Intrusion:
    - Xâm nhập trái phép máy tính của người khác, đánh cắp data và resouces...
    - Kiểm tra, đóng các cổng không dùng.
- DOS/DDOS:
    - Tấn công từ chối dịch vụ -> spam cho khỏi xài.
    - Smuft: gửi nhiều lệnh ping, short time -> Nhiều ICMP của nạn nhân được gửi -> Nhiều ICMP replay đến nạn nhân -> Quá tải.
    - Trojan -> 1 mạng Botnet -> nhiều máy Zombie
- Malicious software:
    - Virus: phần mềm, có thể tự sao chép, lây nhiễm, không đứng 1 mình.
    - Worms: chương trình, có thể tự sao chép, có thể đứng 1 mình, thực thi bất kỳ thời điểm.
    - Trojan horses: fake chương trình có ích, không tự sao chép, kích hoạt khi chạy chương trình, điều kiển từ xa, backdoor...
    - Logic boms: sub program/instruction, kích hoạt theo điều kiện.
    - Backdoors: đoạn chương trình bí mật, mở các port khác.
    - Spyware: phần mềm, theo dõi, browser hijacking, zombieware.

Mô hình bảo mật:

- Cơ bản:
    - Cryptosystem
    - Firewall
    - Anti-malicious system sofware
    - Intrusion detection system
- Defense in dept:
    - Application

    - Host
    - Internal network
    - Perimeter
    - Physical
    - Policies, procedures, awareness

Trojan:

- RAT: back orifice, girlfriend, netbus
- Keylogger: hard/soft, 3 thành phần:
    - Chương trình điều khiển: thiết lập
    - Hook file: nhận thao tác
    - Log file: ghi log

Virus:

- Tính chất:
    - Lây lan
    - Phá hoại
    - Nhỏ
    - Tương thích
    - Phát triển, kế thừa
- Phân loại:
    - Đối tượng:
        - Thường trú
        - Không thường trú
    - Đối tượng, môi trường:
        - Boot virus
        - File-system virus
        - File-format virus
        - Macro virus
        - Script virus
        - Registry virus
    - Phương pháp:
        - Ghi đè
        - Ghi đè bảo toàn
        - Dịch chuyển
        - Song hành

        - Nối thêm
        - Chèn giữa
        - Định hướng lệnh nhảy
        - Điền khoảng trống
    - Tính năng, bản chất:
        - Boot virus: trên boot
        - File virus: trên file
        - Macro virus: file microsoft...
        - Source code virus: trên code của file chủ
        - Network virus: theo mail, dùng lệnh và giao thức mạng
        - Stealth virus: có thể ẩn với chống virus
        - ...
- Kỹ thuật:
    - Lây nhiễm:
        - Trên boot record/master boot của ổ đĩa: thay thế trên phân vùng hoạt động.
        - File thực thi: nối thêm, chèn giữa, ghi đè trên file chủ.
        - Trên file **.COM**:
            - Mở file
            - Ghi lại thời gian/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/thuộc tính
            - Đóng file
    - Định vị vùng nhớ:
      - Chuyển virus, quyền tới vùng nhớ `segment:offset` mới
      - Boot và file cần có
      ...

Giải thuật mã hoá cổ điển:

- Mã thay thế đơn giản: hoán vị theo khoá.
- Mã thay thế n-gram: thay thế cụm n ký tự.
- Mã hoán vị bậc d
- Mã dịch chuyển
    - Vigenere: lặp lại ký tự của khoá đến khi = m
    - Caesar: chỉ có 1 cách, d = 1

- OTP:
  - Đưa m và k về binary (quy định trước)
  - XOR với nhau
  - Đưa về ký tự
- Mã tuyến tính:
  - e(x) = ax + b (mod 26), a: số nguyến tố từ 1 - 26, b: số bước nhảy từ 1 - 26
- Mã playfair:
  - Ma trận khoá: thêm các ký tự của khoá vào ma trận, nếu chưa đầy thì thêm ký tự theo tứ tự từ A -> Z. Trong đó I J được coi là 1 ký tự.
  - Giải thuật:
    - Từng cặp 2 ký tự
    - Dư 1 ký tự, thêm X vào cuối
    - Cùng dòng, shift phải
    - Cùng cột, shif dưới
    - Khác dòng, khác cột, shift 2 góc tạo thành tứ giác
- Mã hill:
  - Mã hoá từng chuỗi n ký tự trên plaintext (vector P) với n là kích thước ma trận vuông Hill: C = HP mod 26.
- Phá mã:
  - 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.

Giải thuật mã hoá hiện đại:

- DES:
  - Dùng khoá độ dài 56 bit để mã hoá dữ liệu 64 bit
  - Mã hoá, giải mã chung khoá
  - Hiện nay: 3DES
  - Giải thuật:
    - 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).

- AES:
  - Dữ liệu đầu vào 16 bytes
  - Kích thước khoá: 128, 192, 256
  - Mỗi khoá con gồm 4 byte
  - Các hàm:
    - SubBytes: mỗi byte thay thế bằng byte khác, sử dụng bảng tham chiếu s-box,
    - ShiftRows: hàng đầu không đổi, hàng thứ n dịch n-1 cột
    - MixColumns: mỗi cột 1 đa thức, nhân modulo $x^4 + 1$ với hàm cố định $c(x) = 3x^2 + x^2 + x + 2 $
    - AddRoundKey: mỗi byte $\oplus$ 1 byte trong khoá con