Computer Security Concepts and Principles

NT101 – NETWORK SECURITY

Giảng viên: Nghi Hoàng Khoa | khoanh@uit.edu.vn

Outline

- **Computer Security concepts (Khái niệm)**
- Computer Security principles

CS book, chapter 1

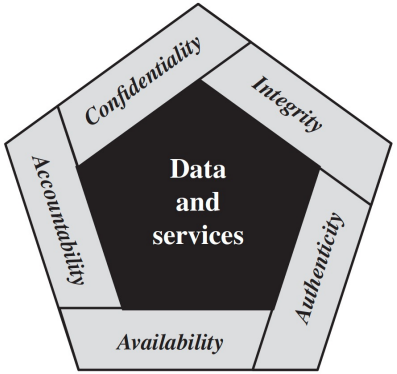
Computer Security Concepts

Computer Security Concepts

- **Computer Security** định nghĩa là (NIST):

*"Measures and controls that ensure **confidentiality, integrity, and availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated"*

- Ngoài "ba mục tiêu lớn" (bộ ba CIA), 2 mục tiêu phổ biến nhất là:
  - Tính xác thực (Authenticity): xác minh rằng người dùng có đúng như họ nói hay không và mỗi đầu vào đến hệ thống đều đến từ một nguồn đáng tin cậy.
  - Trách nhiệm giải trình (Accountability): lưu giữ hồ sơ về các hoạt động của người dùng để cho phép phân tích điều tra số sau này nhằm theo dõi các vi phạm an ninh hoặc hỗ trợ trong các tranh chấp giao dịch.



Lỗ hổng, Đe doạ và Rủi ro

- Lỗ hổng bảo mật: một điểm yếu đã biết của tài nguyên hệ thống có thể bị khai thác bởi một hoặc nhiều kẻ tấn công.
- Đe doạ: một sự cố mới hoặc mới được phát hiện có khả năng gây hại cho toàn bộ hệ thống hoặc công ty của bạn.
- Rủi ro: khả năng mất mát hoặc thiệt hại khi một mối đe dọa khai thác lỗ hổng.

Bạn có thể cho một ví dụ?

Tấn công và biện pháp đối phó

- Tấn công (Attack): một mối đe dọa được thực hiện (bởi tác nhân đe dọa hoặc kẻ thù), nếu thành công, dẫn đến vi phạm không mong muốn về bảo mật hoặc hậu quả của mối đe dọa.
  - Tấn công chủ động (Active): Cố gắng thay đổi tài nguyên hệ thống hoặc ảnh hưởng đến hoạt động của chúng, liên quan đến một số sửa đổi luồng dữ liệu hoặc tạo luồng giả (phát lại, giả mạo, sửa đổi thông báo, DOS)
  - Tấn công thụ động (Passive): Cố gắng tìm hiểu hoặc sử dụng thông tin từ hệ thống mà không ảnh hưởng đến tài nguyên hệ thống (phát hành nội dung thông báo, phân tích lưu lượng) => khó bị phát hiện
  - Phân loại khác: tấn công bên trong (insider) và tấn công bên ngoài (outsider)
- Countermeasure (biện pháp đối phó): bất kỳ phương tiện nào được thực hiện để đối phó với một cuộc tấn công bảo mật
  - Lý tưởng nhất: ngăn chặn các cuộc tấn công thành công
  - Nếu không thể: phát hiện cuộc tấn công => phục hồi hoặc giảm nhẹ tác động của cuộc tấn công

Đe doạ và Tấn công

Threat consequences (Hệ quả)	Threat Action (attack)
→ **Unauthorized Disclosure:** an entity gains access to data for which the entity is not authorized.	• **Exposure** • **Interception** • **Inference** • **Intrusion**
→ **Deception:** an authorized entity receiving false data and believing it to be true	• **Masquerade** • **Falsification** • **Repudiation**
→ **Disruption**: interrupts or prevents the correct operation of system services and functions.	• **Incapacitation** • **Corruption** • **Obstruction**
→ **Usurpation**: control of system services or functions by an unauthorized entity.	• **Misappropriation** • **Misuse**

RFC 4949: https://tools.ietf.org/html/rfc4949

Đe doạ và Tấn công

Threat consequences (Hệ quả)	Threat Action (attack)
→ **Unauthorized Disclosure:** an entity gains access to data for which the entity is not authorized.	• **Exposure** • **Interception** • **Inference** • **Intrusion**
→ **Deception:** an authorized entity receiving false data and believing it to be true	• **Masquerade** • **Falsification** • **Repudiation**
→ **Disruption**: interrupts or prevents the correct operation of system services and functions.	• **Incapacitation** • **Corruption** • **Obstruction**
→ **Usurpation**: control of system services or functions by an unauthorized entity.	• **Misappropriation** • **Misuse**

RFC 4949: https://tools.ietf.org/html/rfc4949

Đe doạ và Tấn công

Threat consequences (Hệ quả)	Threat Action (attack)
→ **Unauthorized Disclosure:** an entity gains access to data for which the entity is not authorized.	• **Exposure** • **Interception** • **Inference** • **Intrusion**
→ **Deception:** an authorized entity receiving false data and believing it to be true	• **Masquerade** • **Falsification** • **Repudiation**
→ **Disruption**: interrupts or prevents the correct operation of system services and functions.	• **Incapacitation** • **Corruption** • **Obstruction**
→ **Usurpation**: control of system services or functions by an unauthorized entity.	• **Misappropriation** • **Misuse**

RFC 4949: https://tools.ietf.org/html/rfc4949

Đe doạ và Tấn công

Threat consequences	Threat Action (attack)
→ **Unauthorized Disclosure:** an entity gains access to data for which the entity is not authorized.	• **Exposure** • **Interception** • **Inference** • **Intrusion**
→ **Deception:** an authorized entity receiving false data and believing it to be true	• **Masquerade** • **Falsification** • **Repudiation**
→ **Disruption**: interrupts or prevents the correct operation of system services and functions.	• **Incapacitation** • **Corruption** • **Obstruction**
→ **Usurpation**: control of system services or functions by an unauthorized entity.	• **Misappropriation** • **Misuse**

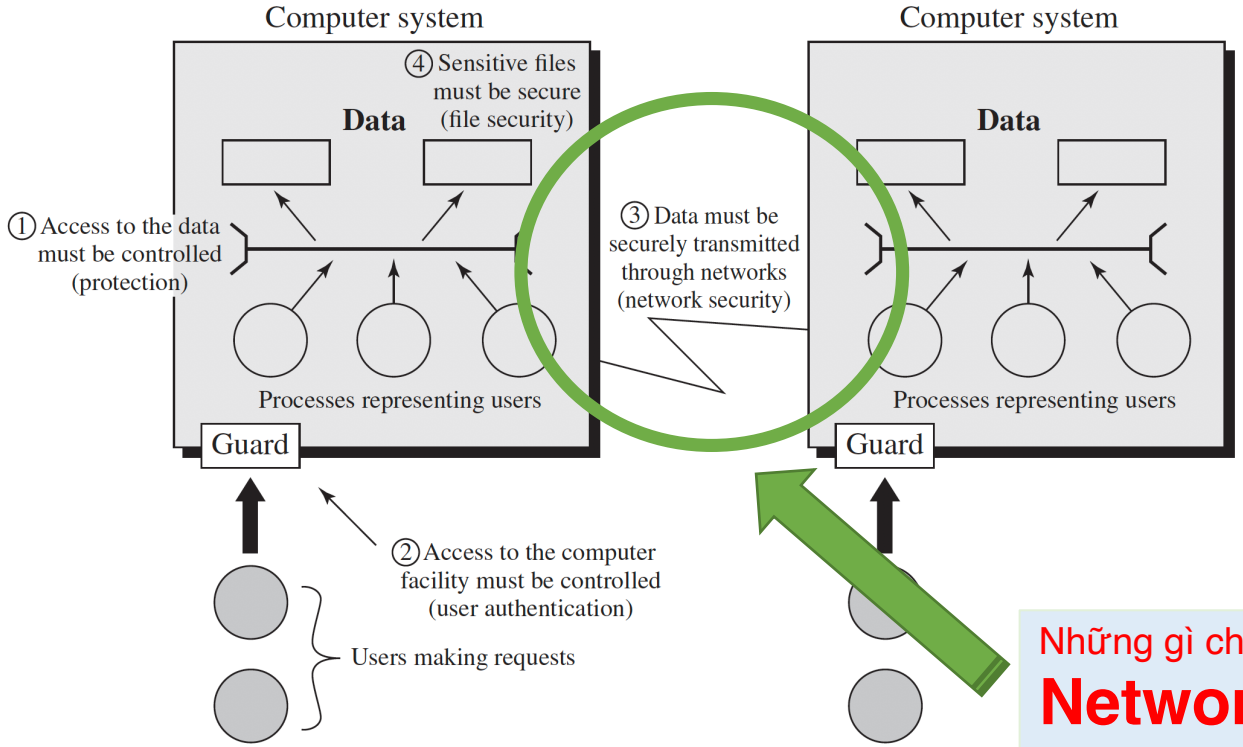
RFC 4949: https://tools.ietf.org/html/rfc4949

Đe doạ và tài nguyên hệ thống

	Tính sẵn sàng	Tính bí mật	Tính toàn vẹn
Phần cứng	Thiết bị bị đánh cắp hoặc bị vô hiệu hóa, do đó từ chối dịch vụ.	Một ổ USB không được mã hóa đã bị đánh cắp.	
Phần mềm	Các chương trình bị xóa, từ chối quyền truy cập của người dùng.	Một bản sao trái phép của phần mềm được tạo ra.	Một chương trình làm việc bị sửa đổi, có thể khiến nó bị lỗi trong khi thực thi hoặc khiến nó thực hiện một số tác vụ ngoài ý muốn.
Dữ liệu	Các tệp bị xóa, từ chối quyền truy cập của người dùng.	Việc đọc dữ liệu trái phép được thực hiện.	Các tập tin hiện có được sửa đổi hoặc các tập tin mới được tạo ra.
Communication Lines and Networks	Tin nhắn bị hủy hoặc bị xóa. Các đường dây hoặc mạng liên lạc không khả dụng	Tin nhắn được đọc. Lưu lượng tin nhắn được quan sát.	Tin nhắn được sửa đổi, trì hoãn, sắp xếp lại hoặc trùng lặp. Thông điệp sai là bịa đặt.

CS book – Chapter 1, Section 1.2

Phạm vi bảo mật máy tính



Những gì chúng ta sẽ tập trung:

Network Security

RFC 4949: https://tools.ietf.org/html/rfc4949

Sự tin cậy

Reflections on Trusting Trust

Chúng ta có thể tin tưởng vào chương trình "đăng nhập - login" trong bản phân phối Linux không? (ví dụ: Ubuntu)

- Không! Chương trình đăng nhập có thể có backdoor
  - ⇾ ghi lại mật khẩu khi nhập

→ Giải pháp: biên dịch lại chương trình đăng nhập từ mã nguồn

Chúng ta có thể tin tưởng mã nguồn đăng nhập không?

- Không! Nhưng chúng ta có thể kiểm tra đoạn mã, sau đó biên dịch lại

Chúng ta có thể tin tưởng trình biên dịch không?

Không! Ví dụ về mã trình biên dịch độc hại:

```
compile(s) {
    if (match(s, “login-program”)) {
        compile(“login-backdoor”);
        return
    }
    /*  regular compilation */
}
```

Để làm gì?

Giải pháp: kiểm tra mã nguồn trình biên dịch, sau đó biên dịch lại trình biên dịch

Vấn đề: Trình biên dịch C được viết bằng C, tự biên dịch

Điều gì sẽ xảy ra nếu trình biên dịch nhị phân (compiler binary) có backdoor?

Thompson's clever backdoor

Tấn công bước 1: Thay đổi mã nguồn của trình biên dịch.

```
compile(s) {
    if (match(s, "login-program")) {
        compile("login-backdoor");
        return
    }
    if (match(s, "compiler-program")) {
        compile("compiler-backdoor");
        return
    }
    /*  regular compilation */
}
```

(*)

Thompson's clever backdoor

Tấn công bước 2: Thay đổi mã nguồn của trình biên dịch.

- Biên dịch trình biên dịch đã sửa đổi ⇒ trình biên dịch nhị phân (compiler binary)
- Khôi phục mã nguồn trình biên dịch về trạng thái ban đầu

Bây giờ: kiểm tra mã nguồn trình biên dịch không thấy có gì bất thường

… nhưng biên dịch trình biên dịch cung cấp compiler binary bị hỏng

Phức tạp: compiler-backdoor cần bao gồm (*)

Chúng ta có thể tin tưởng điều gì?

Tôi đặt một chiếc Laptop qua đường bưu điện. Khi nó đến, tôi có thể tin tưởng vào điều gì?

- Các ứng dụng hoặc hệ điều hành có thể được cài sẵn backdoor.
  ⇒ **Giải pháp: cài đặt lại OS và ứng dụng**

- Làm thế nào để cài đặt lại? Không thể tin tưởng OS để cài lại OS.
  ⇒ **Boot *Tails* từ ổ USB (Debian)**

- Cần tin tưởng pre-boot BIOS, UEFI code. Chúng ta có thể tin tưởng?
  ⇒ **Không (e.g. ShadowHammer operation in 2018)**

- Chúng ta có thể tin motherboard? Cập nhật phần mềm?

Vì vậy, những gì chúng ta có thể tin tưởng?

- Tệ thay, không có gì **...** bất cứ điều gì có thể bị xâm phạm
  - nhưng sau đó chúng ta không thể đạt được tiến bộ
- **Trusted Computing Base** (TCB)
  - Giả sử một số phần nhỏ nhất của hệ thống không bị xâm phạm
  - Sau đó, xây dựng một môi trường an toàn trên đó

Security Design Principles

Clipped from CS155 – Stanford University (Spring 2020)

Bài tập trên lớp

1. Kể tên tất cả các thiết bị điện tử (có thể có kết nối Internet) mà bạn có trong nhà? Suy nghĩ và liệt kê các lỗ hổng tiềm ẩn, các mối đe dọa và rủi ro (vulnerabilities, threats and risks) của chúng.
2. Suy nghĩ và lập danh sách tất cả các lỗ hổng, mối đe dọa và rủi ro tiềm ẩn (vulnerabilities, threats and risks) của trang web **daa.uit.edu.vn**.

Bài tập về nhà

1. Tóm tắt tất cả các Nguyên tắc Thiết kế Bảo mật (Security Design Principles) và đưa ra ví dụ cho từng nguyên tắc.

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularitzy
- Layering
- Least astonishment

Hint: You can refer to Section 1.4, Chapter 1, **CS Book**

Bài tập về nhà

2. Hãy xem xét mã nguồn sau đây để cho phép truy cập vào một tài nguyên:

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
    //Security check failed
    //Inform user that access is denied
} else {
    //Security check OK.
    //Do something
}
```

a. Giải thích lỗi bảo mật trong chương trình này.
b. Viết lại mã để tránh lỗ hổng.

Hint: Hãy xem xét nguyên tắc thiết kế của **fail-safe defaults**.

Tài liệu tham khảo

- **Top Cyber Security Conferences**
  - IEEE Technical Committee on Security and Privacy (S&P)
  - USENIX Security Symposium (USENIX Sec)
  - …
- **NIST Computer Security Resource Center**
- **Center for Internet Security**
- **CS Book – Student Resources**
- **News – Articles:**
  - **DarkReading: https://www.darkreading.com/**
  - **TheHackerNews: https://thehackernews.com/**

Buổi kế tiếp

- Chuẩn bị
  - Chủ đề dự kiến: Tổng quan về các mối đe dọa Phần mềm độc hại
  - Tài liệu:
    - **CS book, Chapter 6**
    - **Một số tham luận, bài báo có liên quan (sẽ được giao)**
  - Chọn chủ đề cho đồ án

Hôm nay, **kết thúc!**

- Nghi Hoàng Khoa
- khoanh@uit.edu.vn
- inseclab.uit.edu.vn
- NT101 – An toàn Mạng máy tính