***(Lưu ý: Chỉ mang tính tham khảo, không phải tất cả kiến thức đều nằm ở đây)***

**\* Slide bài học !!:** <https://drive.google.com/drive/u/0/folders/1gMPbnIHSLEm20e_SGUoG2_lUaPM2hH8z>

# **Chương 1: Introduce**

1. Định nghĩa Bảo mật máy tính là gì?
2. CIA Triad

Tính bảo mật:

Tính bảo mật dữ liệu:

Tính riêng tư

Tính toàn vẹn:

Toàn vẹn dữ liệu: đảm bảo rằng thông tin và chương trình chỉ được thay đổi bởi người được được chỉ định và được ủy quyền

Tính toàn vẹn của hệ thống: Đảm bảo rằng một hệ thống thực hiện

hoạt động một cách nguyên vẹn

Tính sẵn sàng: đảm bảo rằng các hệ thống hoạt động kịp thời, và dịch vụ không bị từ chối khi người dùng được ủy quyền sử dụng

1. Thách thức đối với bảo mật máy tính

Không đơn giản

Phải xem xét các cuộc tấn công ngầm (tấn công bất ngờ)

Thủ tục được sử dụng thường counter-intuitive

Phải xem xét nơi nào cần bảo mật

Liên quan đến khóa và thuật toán

Cuộc chiến không hồi kết của kẻ tấn công / quản trị viên – bên phòng thủ

Không nhận thức được sự cần thiết của tính bảo mật cho đến khi hệ thống xảy ra vấn đề

Yêu cầu giám sát liên tục

Bảo mật cần được cân nhắc “là quá trình được thực hiện sau cùng thay vì trong khi thiết kế” : Giải thích: nếu cứ thiết kế lắp đặt đến đâu cũng gắn bảo mật tới đó sẽ tạo nên 1 thể khó thống nhất

Bảo mật thường xuyên bị coi là trở ngại đối với vận hành hệ thống

1. Các thuật ngữ trong bảo mật máy tính

• Vulnerability(lỗ hổng): Thường được biết đến như điểm yếu hệ thống

• Threat(mối đe dọa): Đe dọa trực tiếp tới ATTT: virus,…

• Adversary (Threat Agent or Threat Actor)

• Attack(tấn công):

• Asset

• Countermeasure(biện pháp đối phó)

• Risk(Rủi ro)

• Security Policy(Chính sách bảo mật)

1. Các nguyên tắc thiết kế bảo mật cơ bản

Simplicity, Fail-Safe defaults, Complete Mediation, Open Design, Minimum Exposure, Separation of Privileges, Least Privilege, Maximize the Entropy of Secrets, Traceability, Usability.

1. Phương diện tấn công

Port đang mở

Dịch vụ ngoài tầm kiểm soát của tường lửa

Ai là người có thể truy cập vào dữ liệu quan trọng

1. Chiến lược bảo mật

Chính sách: Công việc cần làm là gì?

Thực hiện/Triển khai: Thực thi như thế nào?

Tính chính xác/đảm bảo: Hiệu quả?

# **Chương 2: OS**

1. Tổng quan về HĐH

Cung cấp sự tiện lợi khi sử dụng và high-level-abstractions: Ví dụ thay vì hiển thị các địa chỉ vùng nhớ khô khan thì cung cấp giao diện trực quan hơn

Cung cấp quyền truy cập có kiểm soát vào tài nguyên phần cứng

Cung cấp sự độc lập giữa các quy trình khác nhau và giữa các tiến trình đang chạy là sự kết hợp của phần cứng, phần mềm và kiểm soát để tạo thành 1 thể thống nhất và triển khai các chính sách bảo mật

Một phần cứng hoặc phần mềm nhất định là một phần của TCB(Trusted Computing Base) khi và chỉ khi nó được thiết kế để một phần của cơ chế cung cấp bảo mật cho hệ thống máy tính

1. Tại sao cần tin tưởng 1 HĐH
2. Tại sao HĐH bảo vệ tài nguyên

Kiểm soát truy cập của HĐH bảo vệ tài nguyên vì:

Phải xác thực yêu cầu truy cập/sử dụng tài nguyên

Kiểm soát truy cập thực hiện kiểm tra hoặc ủy quyền sử dụng

Các cơ chế cho phép các chính sách khác nhau được hỗ trợ

1. Tin tưởng HĐH ntn?
2. Nguyên tắc thiết kế HĐH
3. Các tính năng bảo mật chính được hỗ trợ từ TCB
4. Kiến trúc Kernel

# **Chương 3: Authentication**

1. Xác thực là gì
2. Mục đích của việc xác thực
3. Ba loại xác thực

Knowledge-based: những gì người dùng biết (mật khẩu)

Possession-based: những gì người dùng có (thẻ định danh)

Inheritance-based: những gì có trên người của người dùng (vân tay)

1. Yếu tố xác thực
2. Tầm quan trọng của Trusted Path
3. Mật khẩu xác thực là gì?

Là 1 quá trình mà người dùng nhập ID/tên người dùng duy nhất và khóa của họ, và hệ thống kiểm tra thông tin đăng nhập trong dữ liệu lưu trữ => Xác định có cho vào hay ko?

1. Tại sao “something you know” phổ biến hơn “something you have” và “something you are”?

Cost: passwords là free (Những gì người dùng biết thì không cần phải lưu trữ quá nhiều)

Convenience(sự tiện dụng): đơn giản cho quản trị viên khi khôi phục mật khẩu bị mất trong trường hợp xảy ra vấn đề

1. Vấn đề về bảo mật của mật khẩu

Kinh nghiệm bẻ khóa: mật khẩu dựa trên cụm từ liên quan, sử dụng công cụ chuyên dụng để bẻ các mk yếu

1. Các phương thức bảo vệ mật khẩu

9.1 Lưu trữ danh sách mk, mỗi user 1 cái trong tệp tin hệ thống

Tệp này chỉ có thể đọc bởi root/admin

Bất lợi:

Quyền set ràng buộc ko kĩ => người khác đọc được

Nếu hệ thống bảo mật bị đe dọa, mật khẩu dễ bị lộ ra

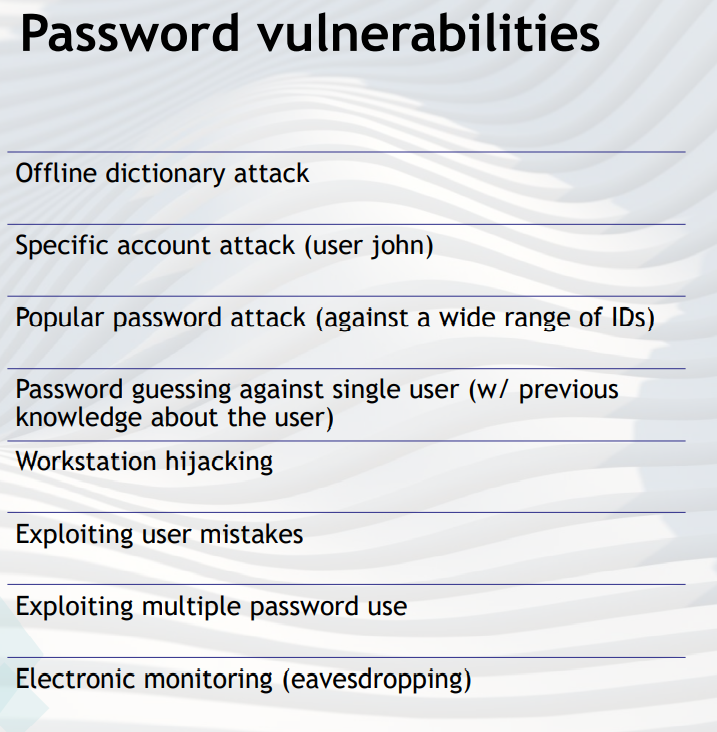
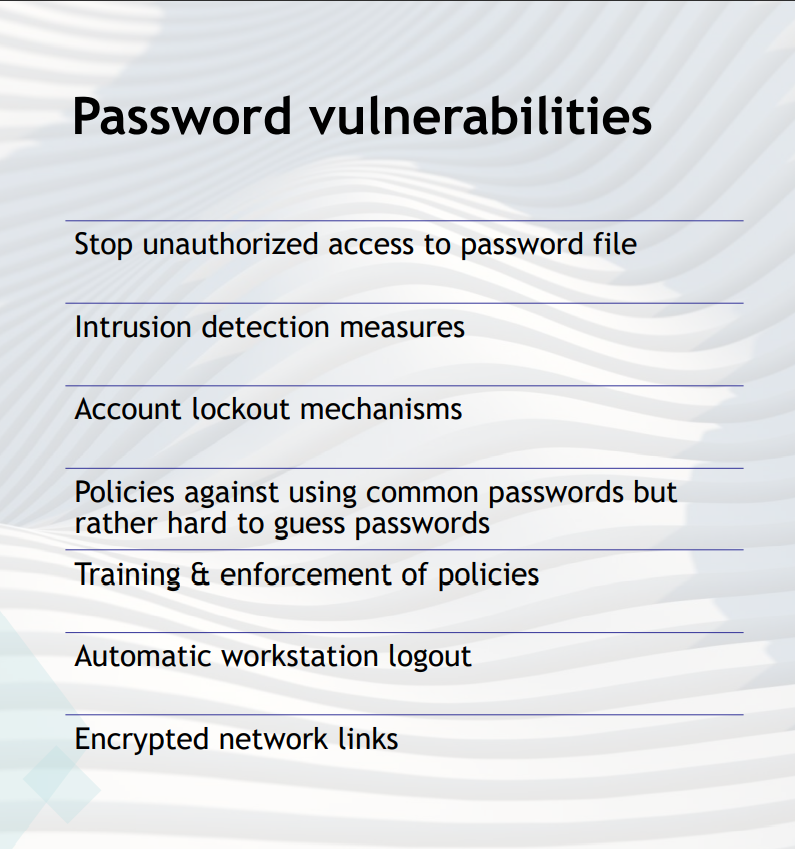
* 1. Không lưu mật khẩu, lưu thứ được tạo ra bởi mật khẩu (Hash?)

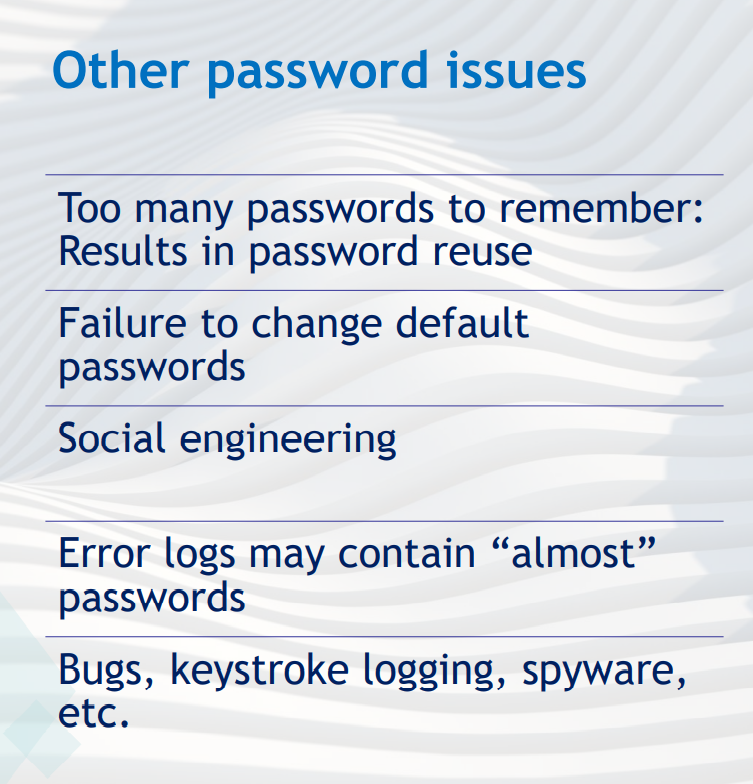
Sử dụng hàm băm 1 chiều và lưu trữ kết quả

File mk chỉ đc đọc bởi root/admin

Cách bẻ khóa mk hàm băm

1. Lỗ hổng của mk



# **Chương 4: Access Control**

(Slide for details)

# **Chương 5: Bảo mật Web**

(Lên mạng tìm hiểu)

1. Kiến trúc Web
2. Các tấn công phổ biến

CSRF

XSS

SQL Injection

# **Chương 6: Malicious Software**

1. Định nghĩa **Mal**icious Soft**ware** (Còn được gọi là Malware)

Là 1 chương trình khai thác lỗ hổng hệ thống, được biết đến như là phần mềm độc hại đe dọa trực tiếp tới hệ thống máy tính

1. Thuật ngữ

Virus: tự gắn vào một chương trình

Worm: lan truyền các bản sao của chính nó đến các máy tính khác

Logic bomb: “nổ” khi có điều kiện xảy ra

Trojan horse: giả mạo/chứa chức năng bổ sung

Backdoor/Trapdoor: cho phép truy cập trái phép

Mobile code: di chuyển không thay đổi sang các nền tảng không đồng nhất

Auto-rooter Kit (virus generator): bộ tạo mã độc (virus)

Spammer and flooder program: khối lượng lớn “packets” không mong muốn

Keylogger: ghi lại thao tác bàn phím

Rootkit: công cụ tin tặc tinh vi để có quyền truy cập cấp gốc

Zombie: phần mềm trên các máy tính bị nhiễm tấn công người khác (còn gọi là bot)

Thông tin chi tiết về các dạng này thì xem ở slide.

# **Chương 7.1: Cyber Security & Firewall**

Các phòng thủ thường được triển khai

* Perimeter defense: Firewall, IDS (Intrusion Detection System)
  + Bảo vệ mạng LAN và các host
  + Giữ external threats từ internal network
* Internal defense – Quét Virus: Bảo vệ host từ các mối đe dọa đã thâm nhập xuyên qua perimeter defenses

1. Tường lửa là gì

* Một điểm kiểm soát và giám sát
* Kết nối mạng tin tưởng khác nhau
* Áp đặt các hạn chế đối với dịch vụ mạng
* Kiểm toán và kiểm soát truy cập
* Cung cấp perimeter defense

1. Mục tiêu thiết kế

2.1 Thực thi các chính sách bảo mật

– Tất cả lưu lượng truy cập từ mạng nội bộ đến internet, và

ngược lại, phải vượt qua tường lửa.

– Chỉ lưu lượng truy cập được ủy quyền bởi chính sách mới được phép đi qua.

* 1. Mạnh mẽ: Tường lửa không được lỗi/sập bởi tấn công

1. Hạn chế của tường lửa

FW không thể bảo vệ:

* Các traffice mạng không đi qua nó
* Cấu hình sai => Tạo ra lỗi

1. Bốn kỹ thuật kiểm soát

• Kiểm soát dịch vụ

– Xác định các loại dịch vụ Internet có thể được được truy cập, in / outbound

• Điều khiển hướng

– Xác định hướng mà dịch vụ cụ thể yêu cầu được phép đi qua

• Kiểm soát người dùng

– Kiểm soát quyền truy cập vào một dịch vụ tùy theo người dùng nào

cố gắng truy cập nó

• Kiểm soát hành vi

– Kiểm soát cách sử dụng các dịch vụ cụ thể (ví dụ: lọc e-mail)

1. Chính sách truy cập của FW

Liệt kê các loại traffic được phép đi qua tường lửa, bao gồm: address range,giao thức, ứng dụng và các nội dung khác

Được phát triển bởi tổ chức đánh giá rủi ro an ninh và chính sách

1. FW và Filtering

* Cơ chế chính trong tường lửa là lọc lưu lượng.
* Mỗi gói bị dừng tại tường lửa và được kiểm tra nó có chống lại chính sách bảo mật hay ko. Và sau đó tường lửa sẽ quyết định có cho phép gói hay loại bỏ gói tin.
* Cả lưu lượng vào và ra đều được lọc hoặc được kiểm tra bởi chính sách bảo mật của tường lửa.

1. Các loại FW

Stateless packet filters

Stateful packet filters

Application Gateways

Circuit-level gateways

**(Chi tiết xem trong slide)**

1. Tường lửa cá nhân

Được triển khai như 1 phần mềm

Được cài đặt trên máy tính và kiểm tra lưu lượng mạng vào ra để xác định cái gì được truy cập hay chặn

Có thể sử dụng để bảo vệ máy tính tại nhà hoặc thiết bị cá nhân khác khỏi các mối đe dọa

# **Chương 7.2: Intrusion Detection System (IDS)**

(Slide for details)

1. Intruders
   1. Examples
   2. Behavior
      * Target acquisition/Information gathering
      * Initial access
      * Privilege escalation
      * System exploit
      * Maintaining access
      * Covering tracks
2. Intrusion Detection System (IDS)
   1. Components
      * Sensors
      * Analyzers
      * User interfaces
   2. Basic Principles
      * Intruder/Authorized user behavior
      * False positives/False alarms vs False negatives
   3. The Base-Rate Fallacy
   4. Requirements
   5. Detection Techniques
      * Anomaly detection (Statistical, Knowledge based, Machine-learning)
      * Signature/Rule-based detection
   6. HIDS vs NIDS

# **Chương 8: Mã hóa**

1. Mật mã học

* Mật mã học: liên quan đến việc bảo mật thực tế dữ liệu kỹ thuật số,

mối quan tâm với việc thiết kế các hệ thống mật mã

* Phân tích mật mã: liên quan đến việc nghiên cứu cơ chế mật mã

với ý định phá vỡ chúng, nghiên cứu sự phá vỡ của hệ thống mật mã

1. Security services of Cryptography

1. Confidentiality (privacy/secrecy)

2. Integrity

3. Authentication

4. Non-repudiation (Chống chối bỏ)

1. Mật mã nguyên thủy

Mã hóa

Hàm băm

Message Authentication codes – Mã truy cập

Chữ kí số

## **\* (Symmetric encryption)**

**(Slide for details)**

I. Modern Block Cipher

1. Components (P-box, S-box, XOR operation, swapping, splitting, shifting, combining)
2. Principles (confusion, diffusion)

II. Data Encryption Standard (DES)

1. Feistel structure
2. DES
3. 3DES

III. Advanced Encryption Standard (AES)

IV. Encrypting large message

1. Modes: ECB, CBC, CFB, OFB, CTR
2. Evaluation criteria (Identical messages, Chaining dependency, Error propagation, Efficiency)

## **\* Asymmetric encryption & Key management**

**(Slide for details)**

1. Modular Arithmetic
2. Modulo, modulus
3. Congruence modulo
4. Properties (addition, subtraction, multiplication, exponentiation)
5. Modular inverse (additive, multiplicative)
6. Totient (Euler’s phi) function
7. RSA
   1. Algorithm
   2. Encryption & Decryption
   3. Example
8. Diffie-Hellman Key exchange
9. Algorithm
10. Example
11. Man-in-the-middle attack on key exchange protocol
12. Key Management
13. Symmetric-key distribution

* Key-distribution center: KDC
* Multiple KDC
* Session key

1. Symmetric-key agreement

* Diffie-Hellman key agreement



1. Public-key distribution (Public announcement, CA, X.509)