AN TOÀN MẠNG MÁY TÍNH

#03: Trust

ThS. Lê Đức Thịnh, UIT

Nội dung

1. Trust?
2. Least Privilege, Privilege Separation?
3. Defense in Depth?

1. Trust?

Reflections on Trusting Trust:

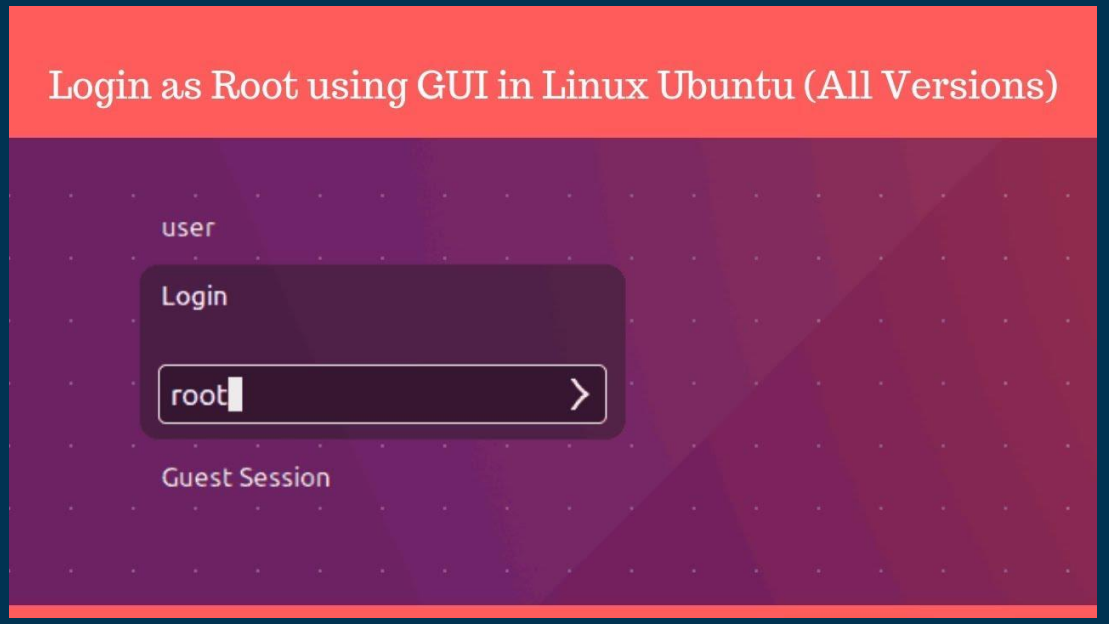
"To what extent shoud one trust a statement that a program is free of trojan horses? Perhaps it is more important to trust the people who wrote the software"

Ken Thompson, 1984

1. Trust?

Bạn có thể tin tưởng một chương trình login trên Linux Distribution?

- Không!
- Giải pháp?
  - Build lại từ source code? Bạn có tin tưởng source code?
    - Không! Nhưng chúng ta có thể kiểm tra mã nguồn và biên dịch lại chúng.
  - Bạn có thể tin tưởng trình biên dịch?
    - Không! Backdoor trong trình biên dịch?



Ken Thompson, 1984

1. Trust?

- Khi bạn mua 1 thiết bị mới (Laoptop/Mobile), Bạn có thể tin tưởng những điều gì trên đó?
  - App?
  - OS?
  - BIOS?
  - Mainboard?
  - …

  → No…! ☹

1. Trust?

Không có gì là đảm bảo

1. Trust?

… Nhưng chúng ta có thể tiến bộ!

Để tin rằng bạn an toàn, bạn phải tin từng phần nhỏ có phần mềm và phần cứng đã được sử dụng để tạo ra hệ thống của bạn!

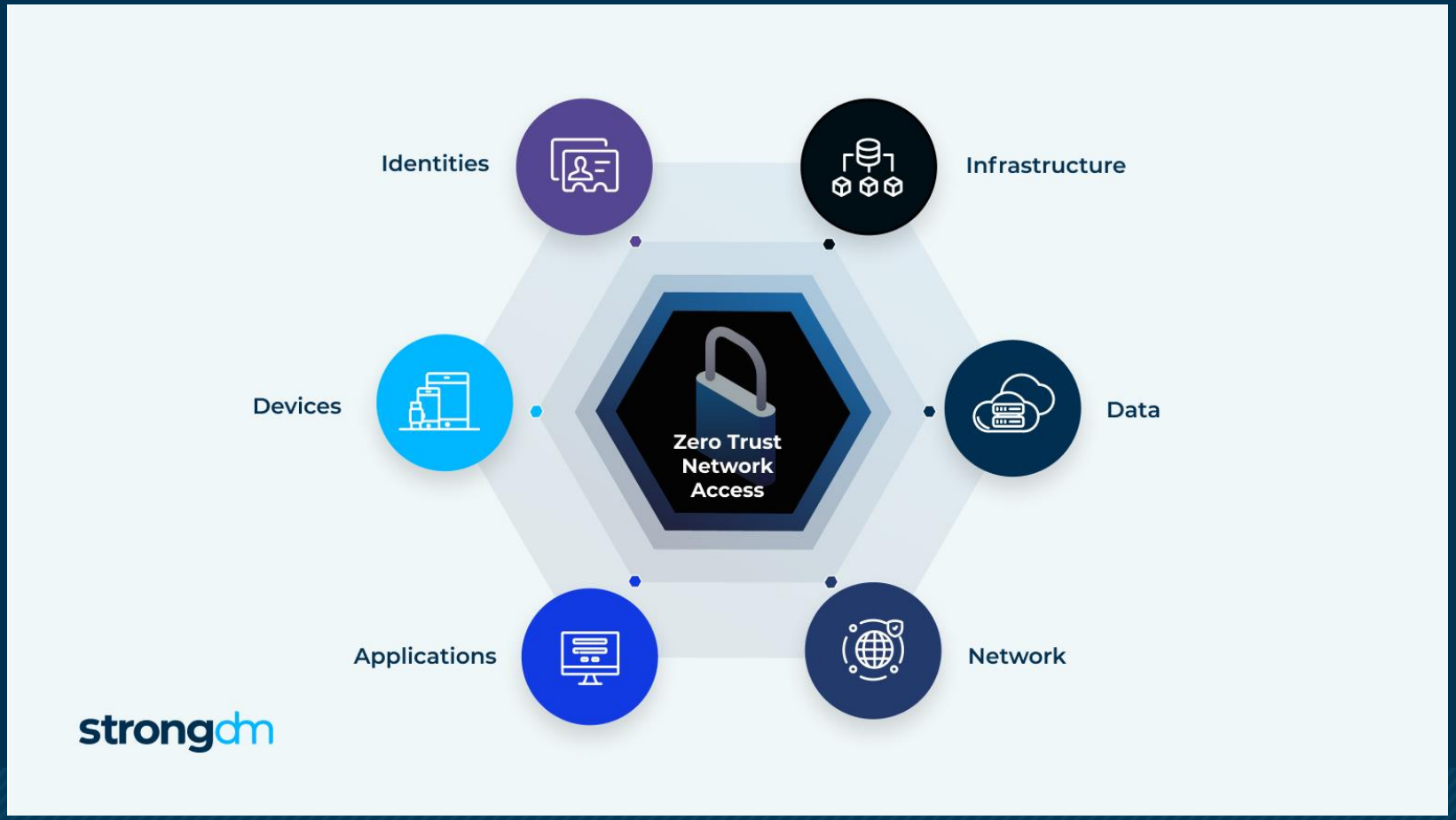
1. Zero Trust?

Traditional IT network security is based on the **castle-and-moat** concept

Cloudflare

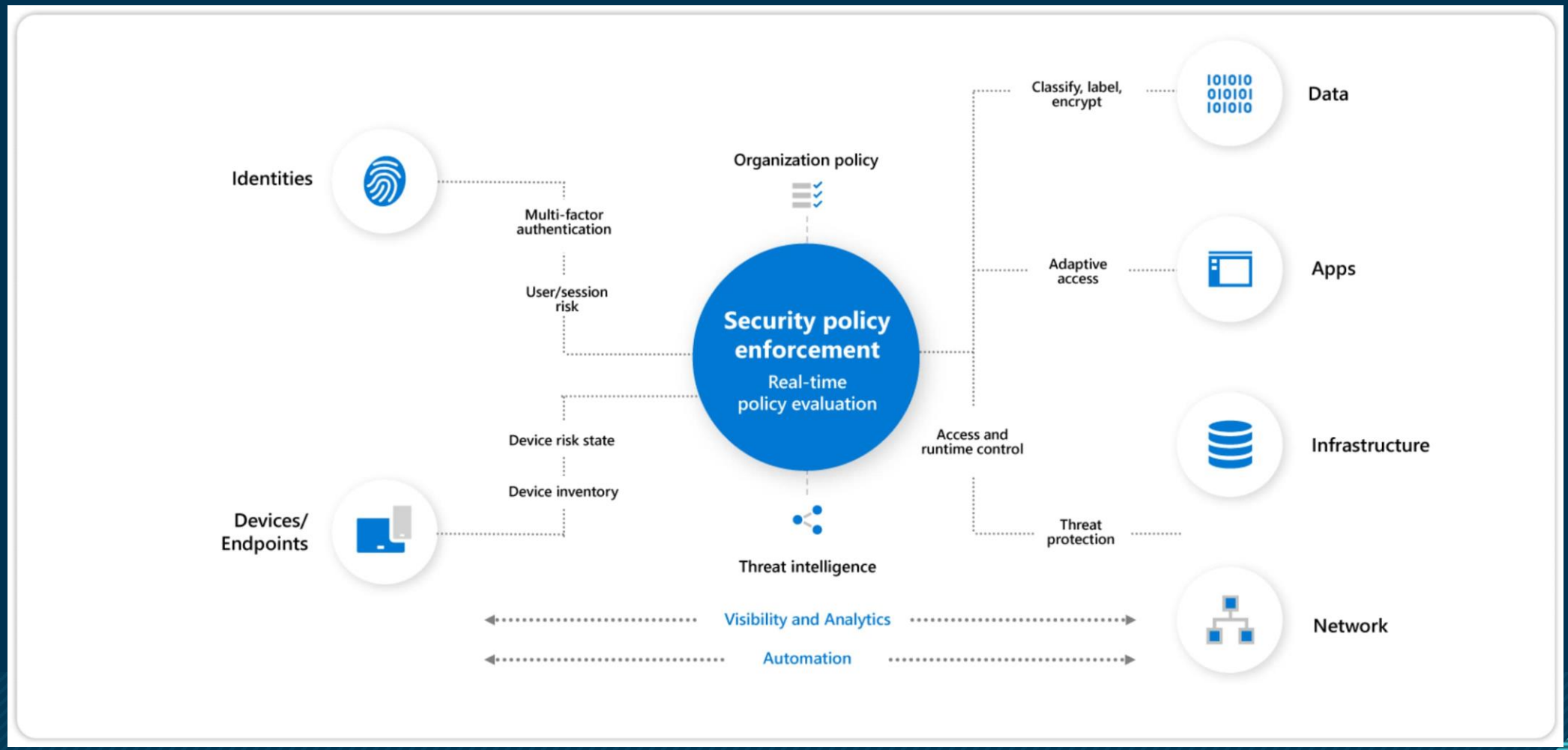
1. Zero Trust?

Zero Trust is a security concept of **“never trust, always verify”**



1. Zero Trust?

https://www.microsoft.com/vi-vn/security/business/zero-trust



1. Zero Trust?

- “Zero Trust”, “Zero Trust Network Access (ZTNA)” or “Zero Trust Architecture (ZTA)”
- “Zero Trust is a security concept of “never trust, always verify” that requires all devices and users, regardless of whether they are inside or outside an organization's network, to be authenticated, authorized, and regularly validated before being granted access.” (strongdm)

- “Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to “never trust, always verify.” Every access request is fully authenticated, authorized, and encrypted before granting access. Microsegmentation and least privileged access principles are applied to minimize lateral movement. Rich intelligence and analytics are utilized to detect and respond to anomalies in real time.” (Microsoft)

2. Least Privilege, Privilege Separation?

- Phân quyền tối thiểu (least privilege) là gì?

  "Users should only have access to the data and resources needed to perform routine, authorized tasks"

- Ví dụ:
  - Chỉ có GV mới có thể thay đổi điểm các lớp GV đó dạy.
  - Chỉ có những nhân viên được kiểm tra và quyền mới có thể truy cập được các tài liệu/tài nguyên được phân loại tương ứng với công việc của họ

2. Least Privilege, Privilege Separation?

- Sự phân chia Quyền là gì?

“Least Privilege requires dividing a system into parts to which we can limit access”

- Việc chia nhỏ 1 hệ thống thành các thành phần với phân quyền tối thiểu cần thiết có thể ngăn chặn kẻ tấn công kiểm soát toàn bộ hệ thống.

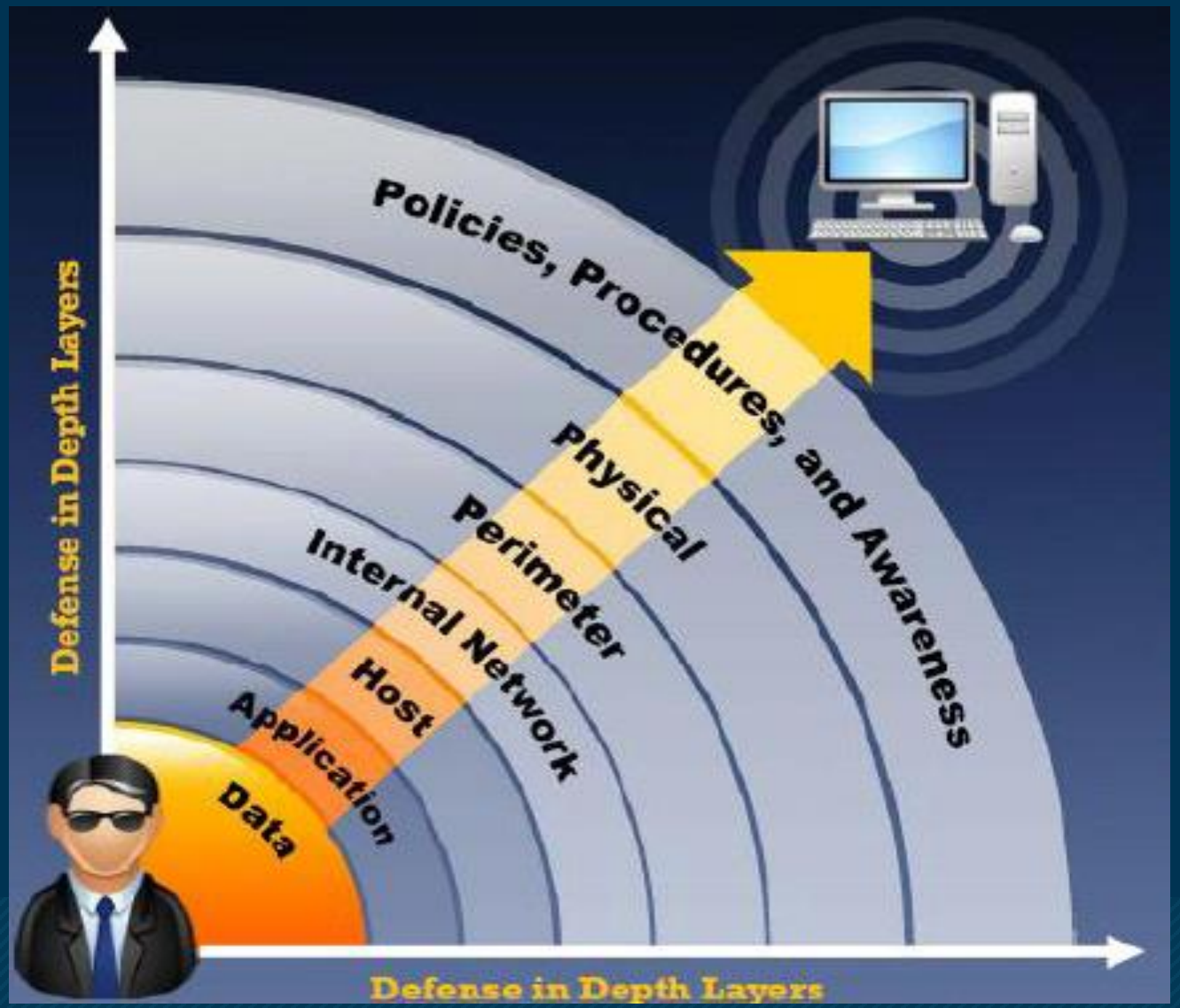
2. Least Privilege, Privilege Separation?

- **Chủ thể (Subjects)** của phân chia, phân quyền tối thiểu?
  - UNIX: Một **User** chỉ nên có thể đọc được các file mà họ chủ sở hữu
  - UNIX: Một **Process** không nên đọc được tiến trình bộ nhớ của Process khác
  - Mobile: Một **App** không nên chỉnh sửa được dữ liệu của ứng dụng khác
  - Web: Một **Domain** chỉ nên đọc được các cookies của nó.

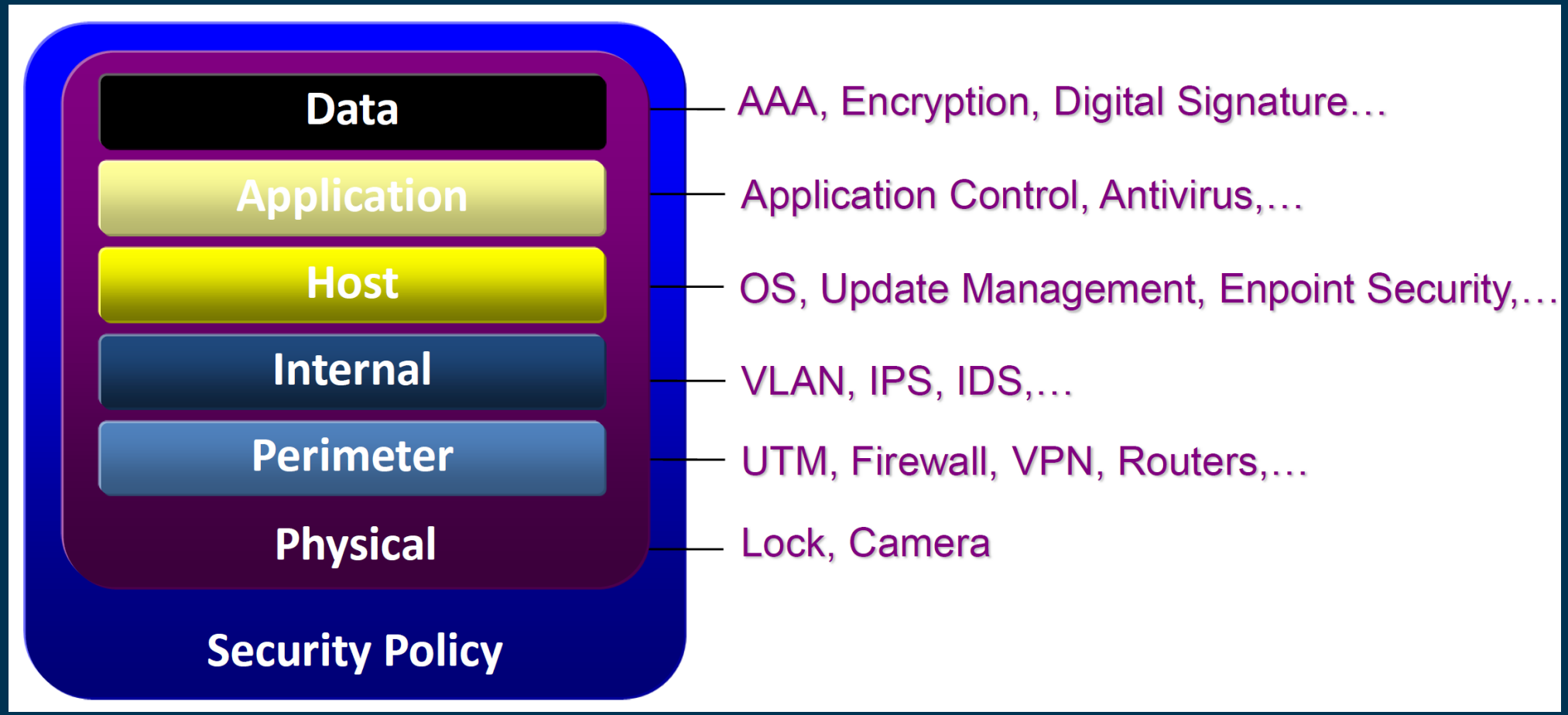
2. Least Privilege, Privilege Separation?

- Security policies:
  - Subject (Who?): acting system principals (e.g., user, app, process)
  - Object (What?): protected resources (e.g., memory, files, HW devices)
  - Operation (How?): how subjects operate on objects (e.g., read, delete)

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu



3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu



3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- **DATA Layer:** Mã hóa thông tin
  - Mã hóa?
  - Mã hóa đối xứng
  - Mã hóa bất đối xứng
  - Chữ kỹ điện tử
  - Hệ thống chứng nhận khóa công cộng
  - …

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- **Application Layer:**
  - Quy trình triển khai phần mềm
  - Ứng dụng bảo mật
  - Application Control

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- *Quy trình triển khai phần mềm:*
  - Phần mềm là ứng dụng truy cập trực tiếp vào dữ liệu nên cần phải có cơ chế kiểm tra và bảo mật.
  - Ưu tiên tối đa việc phát triển nội bộ.
  - Phần mềm mua từ bên ngoài cần có chính sách cam đoan nhất định.
  - Hạn chế tối đa việc sử dụng phần mềm không rõ nguồn gốc (download từ Internet) → Kiểm tra ứng dụng
  - Phân loại ứng dụng: networking hay local, System hay Non-System, Lincense?
  - Cơ chế truy xuất vào dữ liệu: nắm rõ cơ chế truy xuất dữ liệu của ứng dụng, phân quyền (xóa, sửa, full, …)

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- *Ứng dụng bảo mật:* Antivirus, Endpoint Security, Firewall, HIDS
  - Phát hiện và ngăn chặn những mã độc khi truy cập web
  - Phát hiện những kênh truyền thông giữa những ứng dụng bên trong, bên ngoài.
  - Hạn chế việc lây lan Virus trong hệ thống thống

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- *Application Control:* việc cho phép hay cấm những ứng dụng nào?
  - IM
  - Web
  - FTP
  - Game
  - …

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- **Host Layer:** Host = Computer
  - Cập nhật thường xuyên OS cũng như các ứng dụng chạy trên đó.
  - Hạn chế việc trao đổi dữ liệu giữa host và thiết bị ngoại vi
  - Kiểm tra vật lý theo định kỳ

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- Internal Layer:
  - Thiết kế, quản lý mạng nội bộ một cách chặt chẽ, khoa học (chú ý cân bằng các thành phần trong tam giác bảo mật)
    - Phân vùng rõ ràng
    - VLAN
    - IPS/IDS
    - Port Security
    - …

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- **Perimeter Layer:**
  - Được bảo vệ chủ yếu Firewall và Router
    - Router : thiết lập Access Control List
    - Firewall : thiết lập những chính sách (Rule) để quản lý việc truy cập thông tin giữa các Zone
  - Unified Threat Management – UTM:
    - Sophos
    - Checkpoint
    - Astaro security gateway
    - Cyberoam
    - Fortinet

3. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- **Physical Layer:**
  - Cơ chế quản lý thiết bị phần cứng.
  - Cơ chế xác thực khi truy cập vào thiết bị phần cứng chuyên dụng
  - Chính sách bảo hành thiết bị phần cứng
  - Chính sách hỗ trợ khi phần cứng xảy ra sự cố
  - Đảm bảo các thiết bị phần cứng chuyên dụng phải có giấy tờ xác mình hợp chuẩn.

4. Mô hình bảo mật cơ bản
Phương thức phòng thủ theo chiều sâu

- Policy Layer:
  - Chính sách con người
  - Quy trình

Bài tập

- Tìm hiểu và giải thích chi tiết (trình bày tương tự như phần 3. Mô hình phòng thủ theo chiều sâu trong slide) về kiến trúc “Zero Trust”? Ưu, nhược điểm và tính ứng dụng của kiến trúc này?
  - Trình bày và nộp .pptx
  - Làm theo nhóm đồ án
  - Deadline: 15g30, ngày 02/10/2021
  - Nộp trên moodle môn học

1. An toàn Mạng máy tính, Duy Nguyen, UIT
2. Security Principles and OS Security, CS155 Computer and Network Security, Stanford University.
3. Reflections on trusting trust, Ken Thompson, 1984
4. Microsoft Corp
5. …

Thank You

AN TOÀN MẠNG MÁY TÍNH

#03: Trust

ThS. Lê Đức Thịnh, UIT