Chương 1

# TỔNG QUAN VỀ AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG

Trình bày: Bùi Minh Quân - bmquan@ctu.edu.vn
Khoa MMT&TT – Trường CNTT&TT - ĐHCT

Chương 1

# TỔNG QUAN VỀ AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG

- Thế nào là an toàn hệ thống và an ninh mạng
- Tấn công trên mạng
- Các phần mềm có hại
- Các yêu cầu của một hệ thống mạng an toàn

# Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan về an toàn mạng và các vấn đề liên quan trong an toàn mạng.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Giải thích được thế nào là an toàn hệ thống và an ninh mạng.
  - Phân loại và trình bày được các mối đe dọa đối với hệ thống máy tính và hệ thống mạng.
  - Trình bày được các kỹ thuật tấn công trên mạng gồm: tấn công thăm dò, tấn công truy cập, tấn công từ chối dịch vụ.
  - Hiểu và phân loại được các phần mềm có hại và cách thức hoạt động của từng loại phần mềm có hại.
  - Mô tả được các yêu cầu cơ bản của 1 hệ thống an toàn mạng: chứng thực, phân quyền và giám sát.

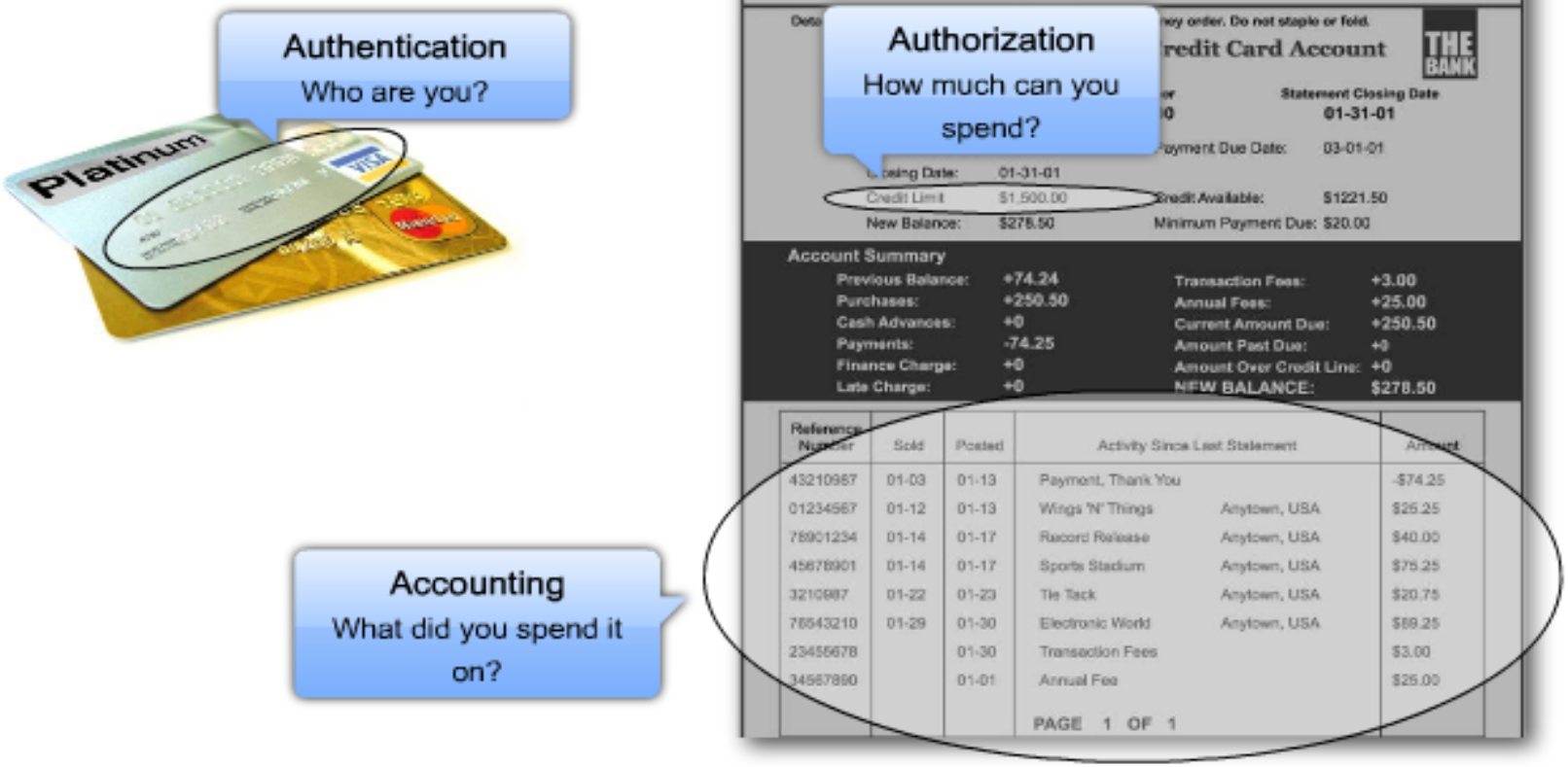
## Phần 4

# Yêu cầu cơ bản của một hệ thống mạng an toàn

- Giới thiệu về kiến trúc AAA
- Authentication
- Authorization
- Accounting

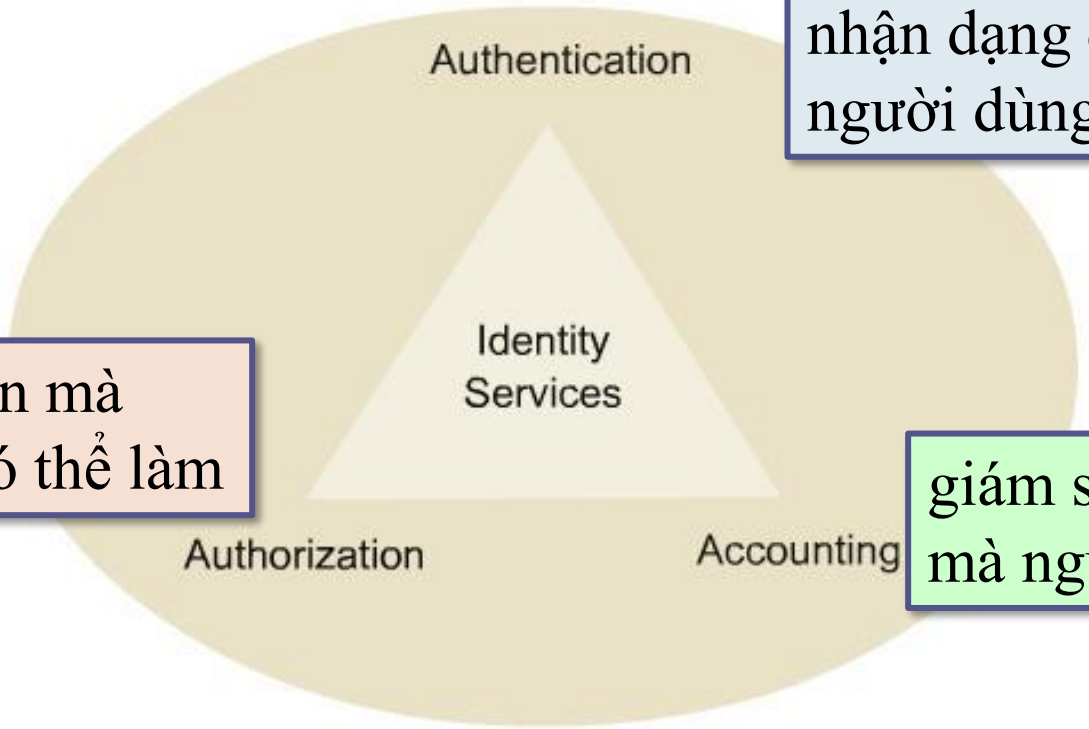
# Yêu cầu cơ bản của 1 hệ thống mạng an toàn

- Kiến trúc AAA



# Yêu cầu cơ bản của 1 hệ thống mạng an toàn

- Kiến trúc AAA




nhận dạng đúng người dùng

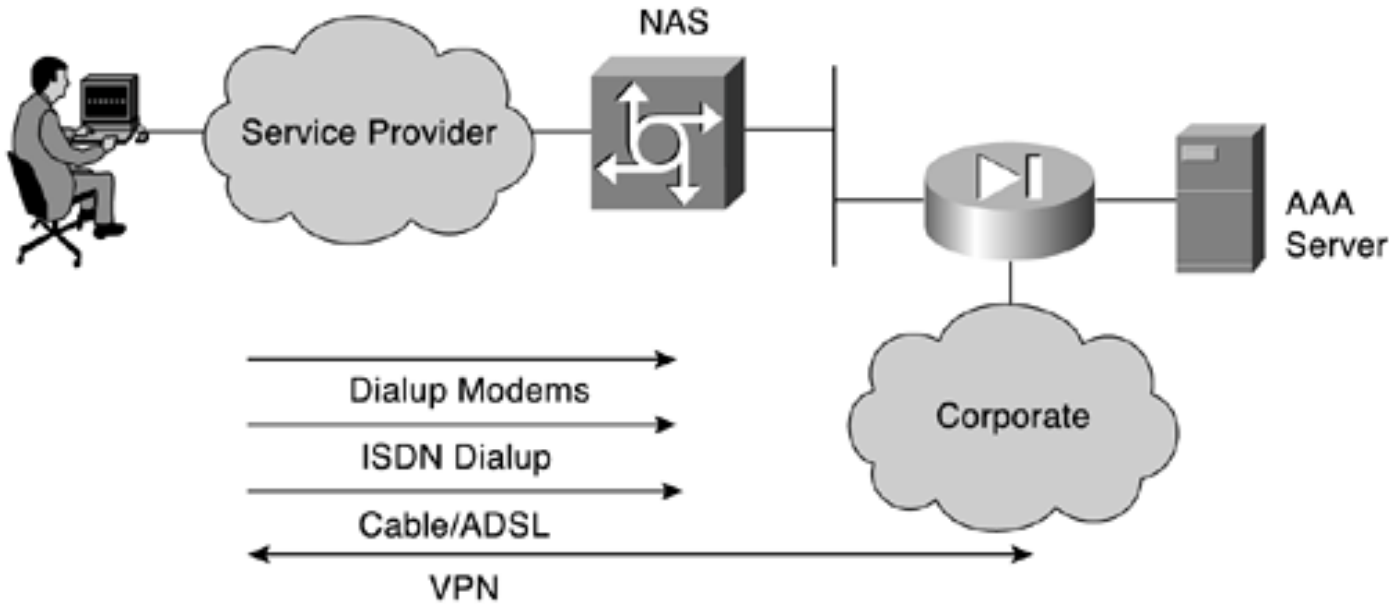
giới hạn quyền mà người dùng có thể làm

giám sát những gì mà người dùng làm

**Kiến trúc AAA** cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn của hệ thống mạng..

# Yêu cầu cơ bản của 1 hệ thống mạng an toàn

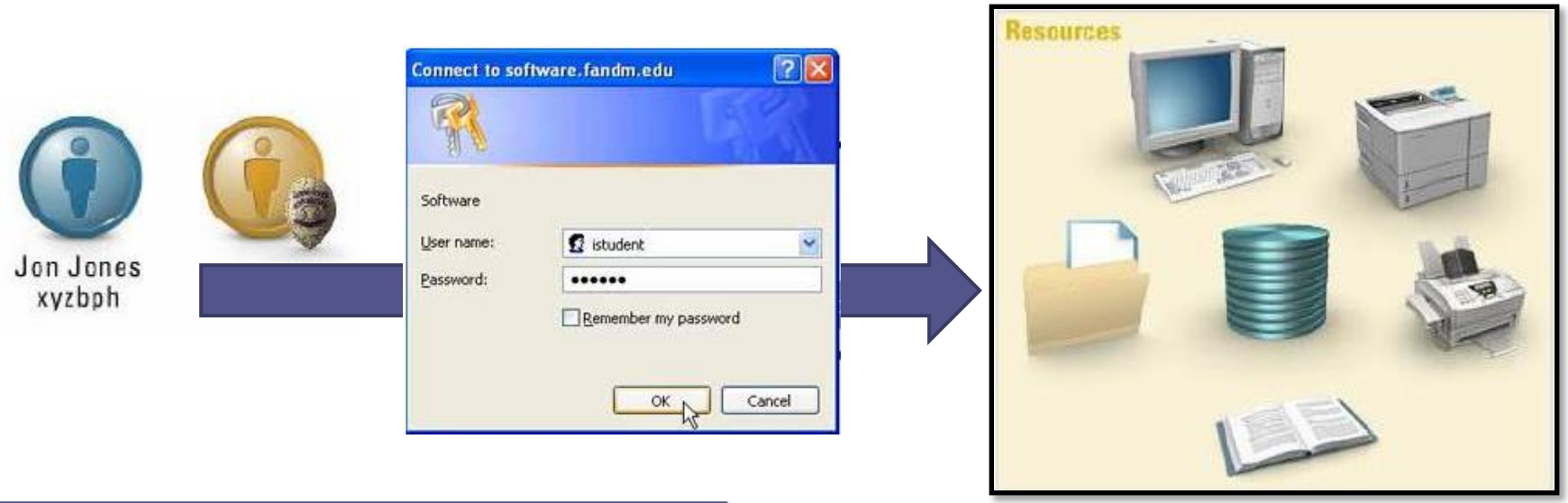
- Kiến trúc AAA




**AAA** thường cung cấp 1 phương thức **định danh người dùng**, xác định **mức độ truy cập** trong mạng và **giám sát hoạt động** của người dùng trong mạng.

# Chứng thực (Authentication)

- Khái niệm




**Chứng thực** là một quy trình nhằm cố gắng **xác minh** nhận dạng số (digital identity) của phần truyền gửi thông tin (sender) trong giao thông liên lạc.

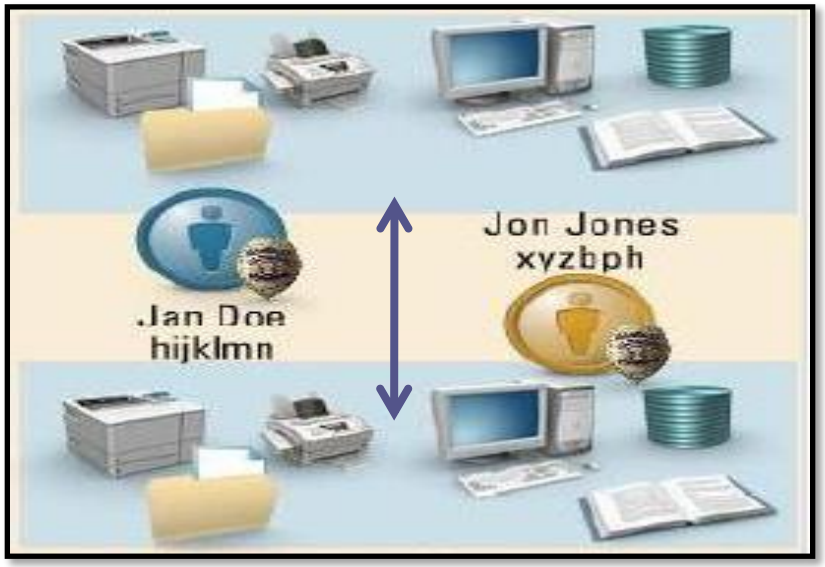
Điểm yếu của các hệ thống giao dịch bằng tài khoản-mật khẩu là:

- mật khẩu có thể bị quên
- mật khẩu bị lộ
- Dễ dàng dò tìm ra mật khẩu yếu.

# Chứng thực (Authentication)

- Chứng thực 1 chiều và 2 chiều

**Chứng thực 1 chiều**
**(1 way authentication)**



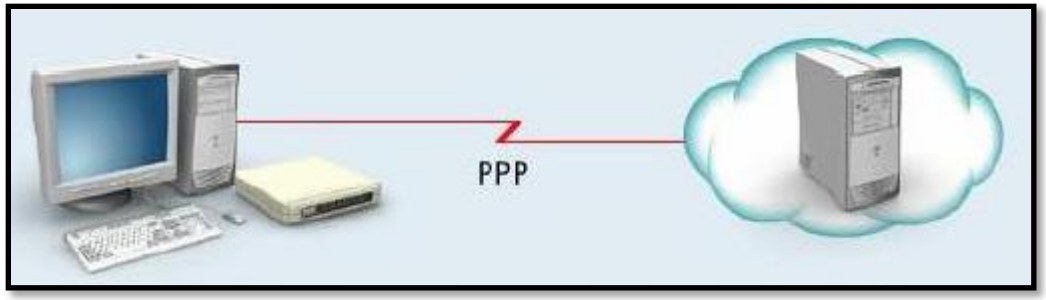

**Chứng thực 2 chiều**
**(2 way authentication)**

Client sẽ cung cấp cho Server tài khoản và mật khẩu.

Cả 2 bên sẽ phải xác nhận với nhau bằng username và password tương ứng

# Chứng thực (Authentication)

- PAP và CHAP




**Password Authentication Protocol (PAP):**

- Chứng thực 1 chiều hoặc 2 chiều.
- Gửi trực tiếp username và password đi trên đường truyền.
- Dữ liệu không mã hóa (dạng plaintext)
- Kém an toàn

**Challenge Handshake Authentication Protocol (CHAP):**

- Chứng thực 2 chiều.
- Không gửi trực tiếp username và password đi trên đường truyền.
- Dữ liệu được mã hóa theo MD5.
- An toàn hơn PAP.

# Chứng thực (Authentication)

- Hệ thống Kerberos – Mục tiêu


Một khoá mật mã càng được sử dụng lại nhiều lần thì nguy cơ bị giải mã càng lớn

Cần **một khoá được mã hoá có thời gian sống ngắn** mà không tạo ra sự bất tiện cho người sử dụng.

- Không truyền đi trên mạng mật khẩu "dưới dạng plaintext" (được mã hóa).
- Có khả năng chống lại dạng tấn công "sử dụng lại" (replay attack).
- Không yêu cầu người dùng lặp đi lặp lại thao tác nhập mật khẩu trước khi truy nhập vào các dịch vụ thường dùng.

# Chứng thực (Authentication)

- Hệ thống Kerberos – Khái niệm

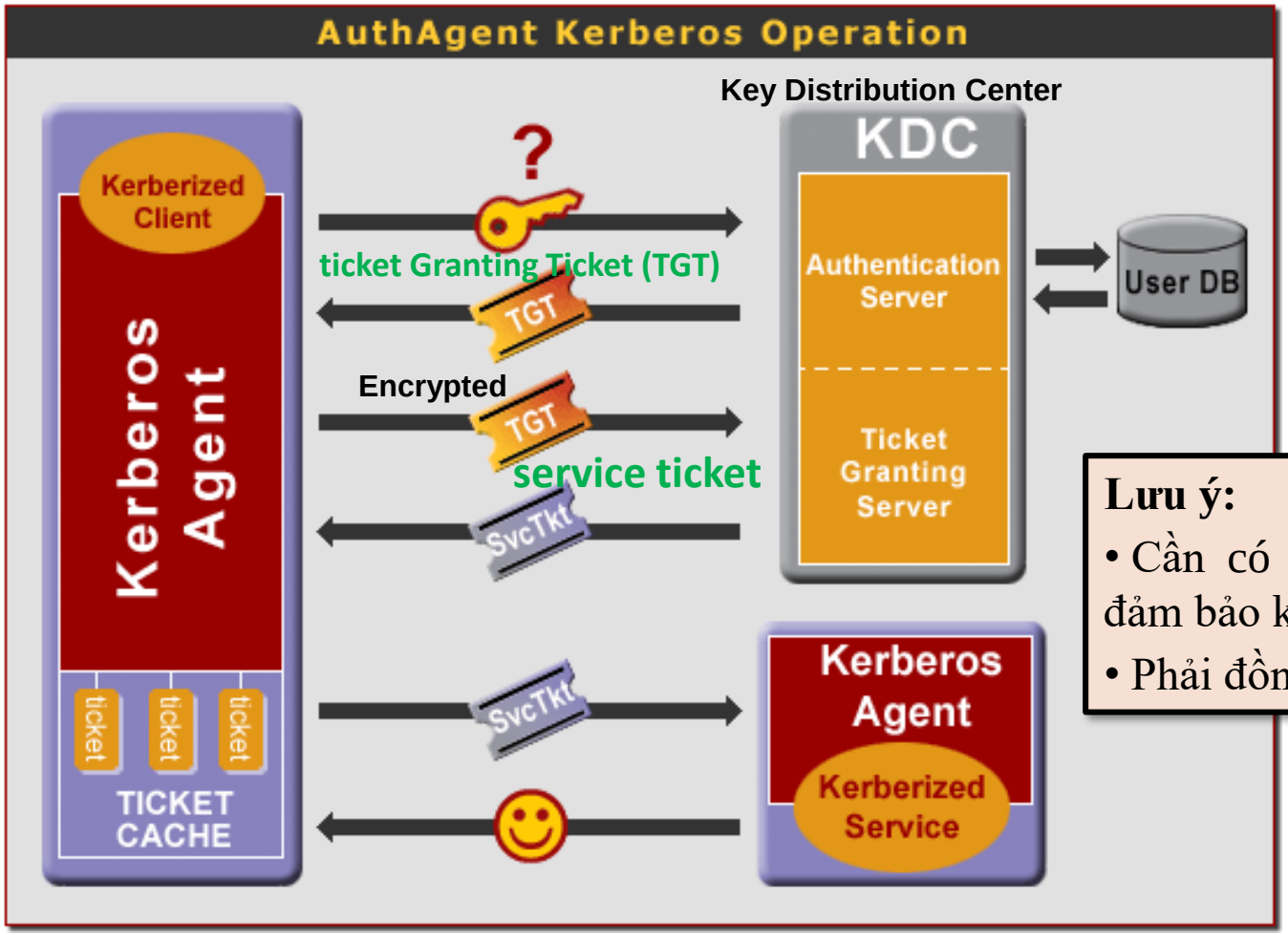

Là tên con chó ba đầu gác cổng địa ngục trong thần thoại Hy Lạp

**Kerberos** cung cấp dịch vụ chứng thực cho 1 mạng riêng lẻ hay nhiều mạng liên kết với nhau.

- Được phát minh bởi MIT từ những năm 1980.
- Một bên thứ ba (trusted third-party) được tin cậy cấp khóa phiên (**session key**) để người dùng và bên cung cấp dịch vụ có thể trao đổi thông tin trên mạng một cách an toàn.
- Hoạt động dựa trên nguyên lý mã hóa sử dụng khóa mật.
- Được tích hợp trong HĐH Solaris, Microsoft, router Cisco, …

# Chứng thực (Authentication)

- Hệ thống Kerberos – Hoạt động

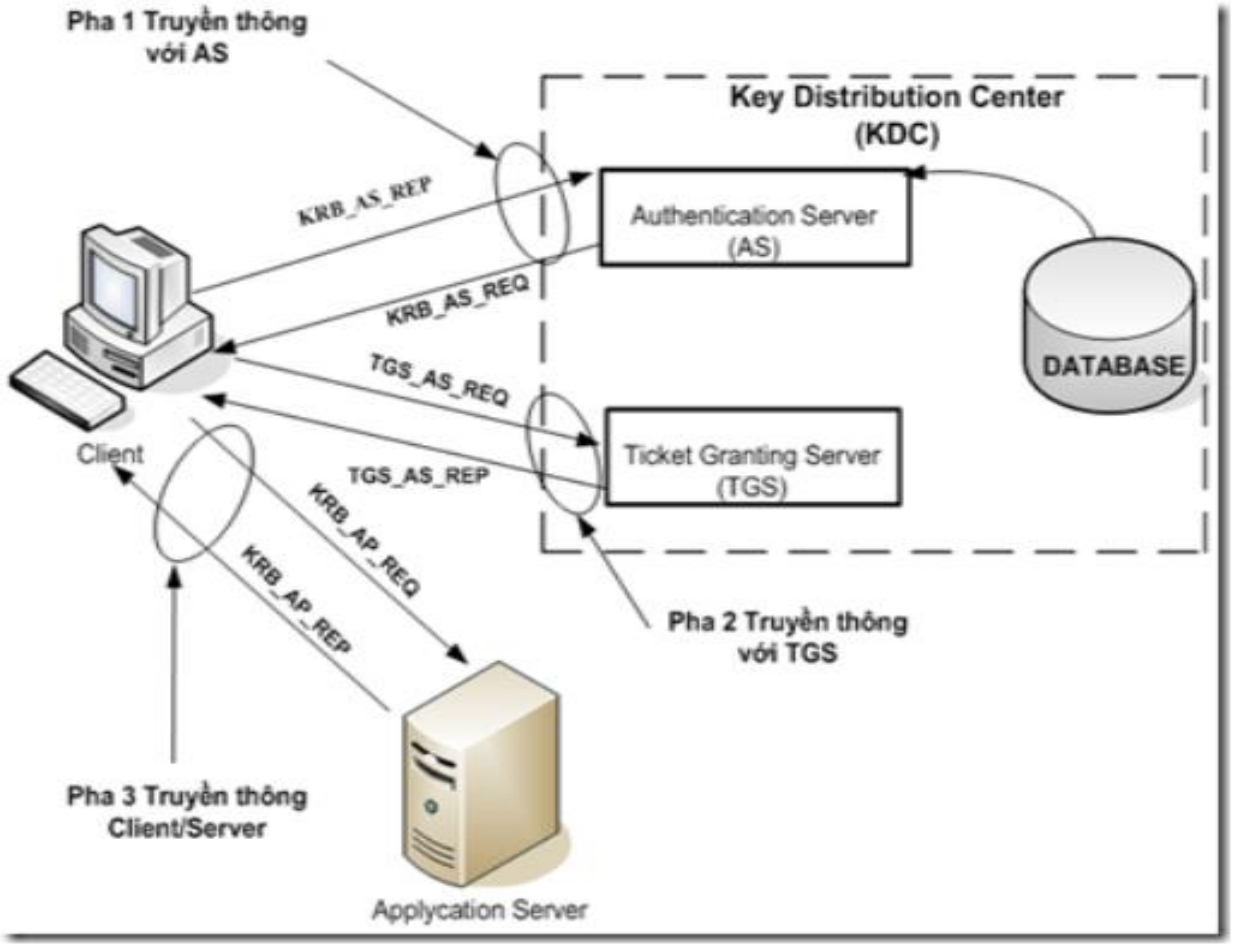



**Lưu ý:**

- Cần có nhiều máy chủ để đảm bảo không ngưng trệ.
- Phải đồng bộ hóa đồng hồ.

https://sec.vnpt.vn/2023/01/ky-thuat-attacking-kerberos-as-rep-roasting/

# Hệ thống Kerberos – Hoạt động




Hình 1 hoạt động của giao thức kerberos

# Chứng thực (Authentication)

- Mật khẩu sử dụng 1 lần

One time password (OTP)


Người dùng không cần lo lắng mật khẩu của mình bị đánh cắp hay bị mất

- OTP thường đi kèm với các thiết bị phần cứng
- Đồng hồ được đồng bộ thời gian với hệ thống Server xác thực
- Định sẵn một phương pháp tạo ra OTP như nhau: hàm toán học, tín hiệu đồng bộ thời gian, …

# Chứng thực (Authentication)

- Thẻ cứng (Token card)


Nhiều loại thiết bị có thể dùng cho token card là: thẻ cứng, PC card, thiết bị USB, thiết bị Bluetooth, …

- Là một trong các giải pháp bảo mật an toàn nhất.
- Được dùng kết hợp với một loại chứng thực khác (chẳng hạn như số PIN, mật khẩu)

# Chứng thực (Authentication)

- Sinh trắc học (biometrics)


Retinal Patterns


Finger/Palm Prints


Voice Patterns

- không thể làm mất
- Không thể quên
- Rất khó giả mạo

**Dùng để chứng thực người dùng thông qua:**

- Đặc điểm sinh học: khuôn mặt, bàn tay, mống mắt, võng mạc, dấu vân tay, DNA, …
- Hành vi bên ngoài: dáng đi, chữ ký, giọng nói, …

**Nhận dạng nhầm nếu:**

- Thiết bị đọc không chính xác
- Đặc điểm của người cũng có thể thay đổi theo năm tháng

# Phân quyền (Authorization)

- Khái niệm

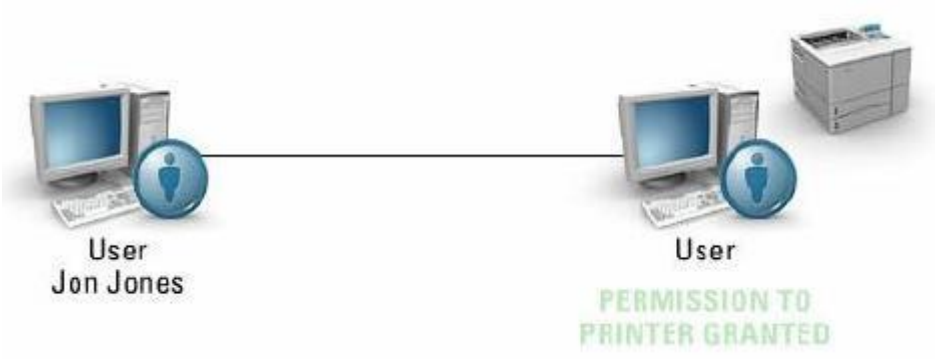
Sau khi được chứng thực, việc **phân quyền** chỉ định những gì mà người dùng đó có thể thi hành trên hệ thống


**Phân quyền**: định nghĩa các quyền (*rights*) và sự cho phép (*permission*) của người dùng trong một hệ thống

- Điều khiển truy cập sẽ cho phép hoặc từ chối một chủ thể (người , quá trình) sử dụng một đối tượng (chức năng, tập tin, ….).
- Điều khiển truy cập có 2 dạng chính là:
  - Điều khiển truy cập tùy quyền (**D**iscretionary **A**ccess **C**ontrol - **DAC**)
  - Điều khiển truy cập bắt buộc (**M**andarory **A**ccess **C**ontrol - **MAC**)

# Phân quyền (Authorization)

- Điều khiển truy cập tùy quyền (DAC)



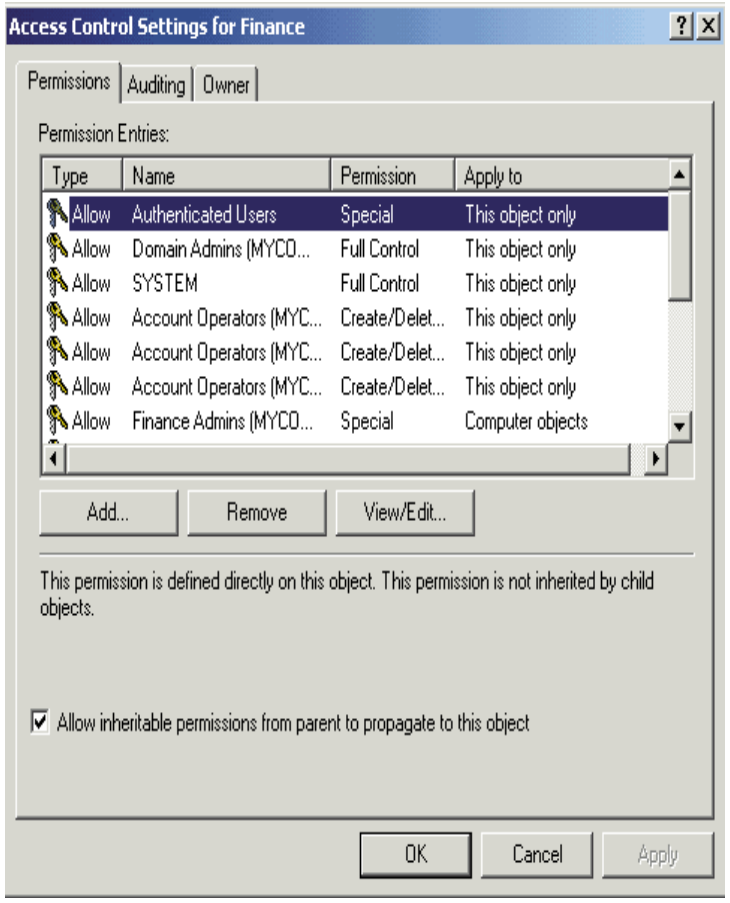

**Chủ nhân của tài nguyên** (file, dữ liệu, thiết bị, …) **quyết định ai** là người được phép truy cập và những **đặc quyền** (*privilege*) **nào** mà người đó được phép thi hành

**Hai khái niệm chủ yếu:**

- **Sở hữu của tập tin và dữ liệu:**
  - Tài nguyên nào cũng phải có chủ nhân (Owner).
  - Thông thường thì chủ nhân của tài nguyên chính là người đã tạo ra tài nguyên.
  - Chính sách truy cập trên tài nguyên là do chủ nhân tài nguyên đó quyết định.
- **Các quyền và phép truy cập**: là những quyền khống chế trên tài nguyên mà chủ nhân chỉ định cho từng người dùng hay nhóm người dùng.

# Phân quyền (Authorization)

- Điều khiển truy cập tùy quyền (DAC)




**DAC được áp dụng thông qua các kỹ thuật:**

- **Danh sách điều khiển truy cập (ACL):** định danh các quyền và phép được chỉ định cho **một chủ thể hoặc một đối tượng**.
- **Điều khiển truy cập dựa theo vai trò (RBAC):** chỉ định tư cách **nhóm hội viên** dựa trên vai trò của tổ chức hoặc chức năng của các vai trò.

**Linux và Windows dùng cách thức kiểm soát theo kiểu DAC:**

- Tùy theo quyền, mà user đăng nhập có thể truy cập những tài nguyên nào trong hệ thống.
- Root/Adminstrator sẽ có toàn quyền truy cập.

# Phân quyền (Authorization)

- Điều khiển truy cập bắt buộc (MAC)

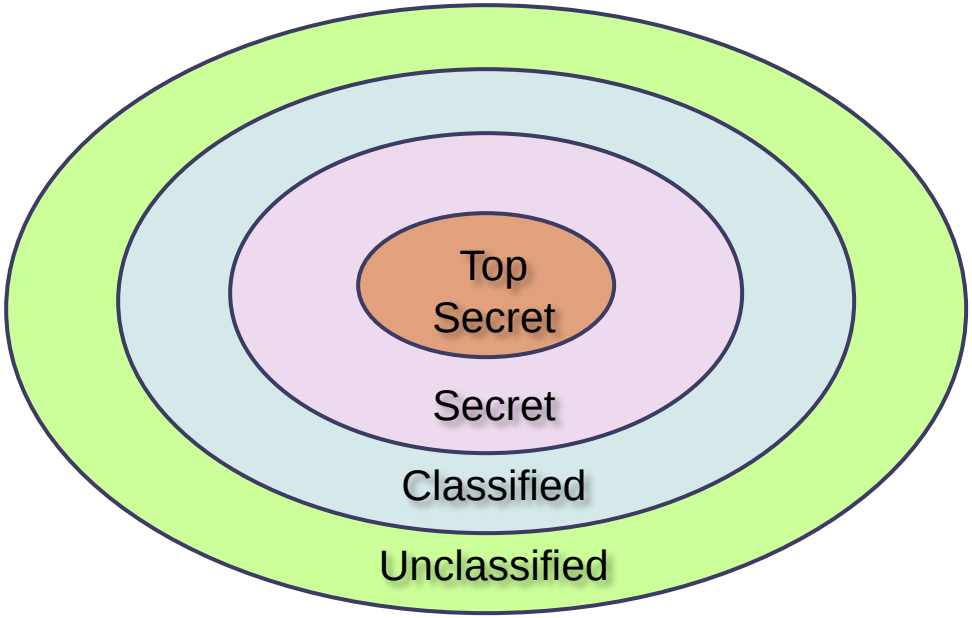

Điều khiển truy cập bắt buộc (MAC) là một chính sách truy cập **không do cá nhân sở hữu tài nguyên quyết định, mà do hệ thống quyết định**.

- MAC từ chối người dùng toàn quyền truy cập hay sử dụng tài nguyên do chính họ tạo ra.
- Quyền truy cập vào các tài nguyên được người quản trị chỉ định.

- MAC thường được thiết kế cho các ứng dụng.
- MAC cũng đã được xây dựng và cài đặt trong các hệ điều hành hiện tại như UNIX, Linux, MS Windows, OpenBSD, …

# Phân quyền (Authorization)

- Điều khiển truy cập bắt buộc (MAC)




MAC được dùng cho hệ thống đa tầng => phân loại các dữ liệu, thao tác thành nhiều mức độ nhạy cảm khác nhau.

Để truy cập một đối tượng nào đấy, chủ thể phải có một mức độ nhạy cảm (*tin cẩn*) tương đồng hoặc cao hơn mức độ của đối tượng yêu cầu

Một chương trình ứng dụng lạ, chưa từng thấy (*unknown program)* được phân loại vào các chương trình ứng dụng không đáng tin (*untrusted application*)

hệ thống phải theo dõi, giám sát và khống chế những truy cập của nó vào các thiết bị và các tập tin của hệ thống

# Phân quyền (Authorization)

- Điều khiển truy cập dựa trên vai trò (Role-Based Access Control - RBAC)


• Mỗi vai trò được gắn liền với một số quyền hạn (*permissions*) cho phép thao tác một số hoạt động cụ thể.

• Người dùng không được cấp quyền một cách trực tiếp, mà nhận được những quyền hạn **thông qua các vai trò** của họ => việc cấp quyền sẽ đơn giản hơn.

Việc nắm bắt các nhu cầu về quyền của người dùng trải rộng trên hàng chục, hằng trăm hệ thống và trên các chương trình ứng dụng, là một việc hết sức phức tạp => sử dụng RBAC còn nhiều tranh luận

# Phân quyền (Authorization)

- Các mô hình bảo mật thông tin (Information secure models)


• **Mô hình bảo mật thông tin** xác định cụ thể các khía cạnh thiết yếu của bảo mật và mối quan hệ của chúng với hiệu năng của hệ điều hành, **các mô hình sẽ hướng dẫn và xác định quy tắc đảm bảo tính bảo mật, cơ chế bảo vệ và tính toàn vẹn của thông tin.**

•**Chính sách bảo mật** (security policy) đề ra nhiều điểm chính như: dữ liệu được truy xuất như thế nào, số lượng các yêu cầu bảo mật, các bước thực hiện khi các yêu cầu bảo mật không thỏa mãn.

• **Mô hình bảo mật** (security model) mô tả sâu hơn, chi tiết hơn các yêu cầu và các nguy cơ của hệ thống thông tin để hỗ trợ các chính sách bảo mật và cách thức bảo vệ hệ thống đó. Một số các mô hình bảo mật thông tin gồm:

- Mô hình Clark-Wilson
- Mô hình Bell La-Padula
- Mô hình Biba

# Phân quyền (Authorization)

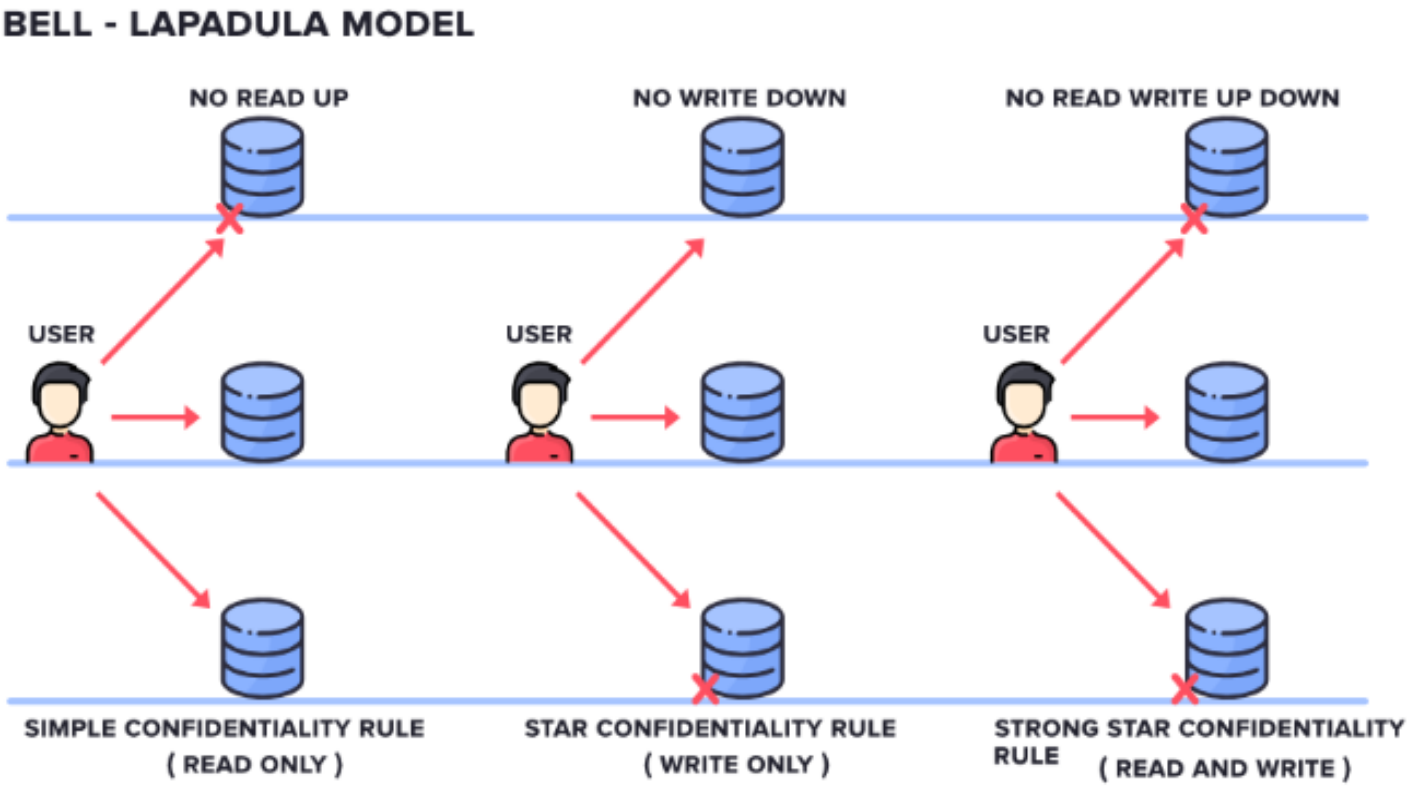
- Các mô hình bảo mật thông tin


**Mô hình Bell La-Padula**

- Hệ thống bảo mật đa mức: duy trì tính **bí mật** của dữ liệu
- Phân loại nhiều mức bảo mật dữ liệu và kiểm soát truy cập. Tùy thuộc vào mức bảo mật của mình mà người dùng có quyền truy xuất đến mức dữ liệu nào
- Điểm yếu của mô hình này là không đảm bảo tính toàn vẹn của dữ liệu

# Phân quyền (Authorization)

- Các mô hình bảo mật thông tin



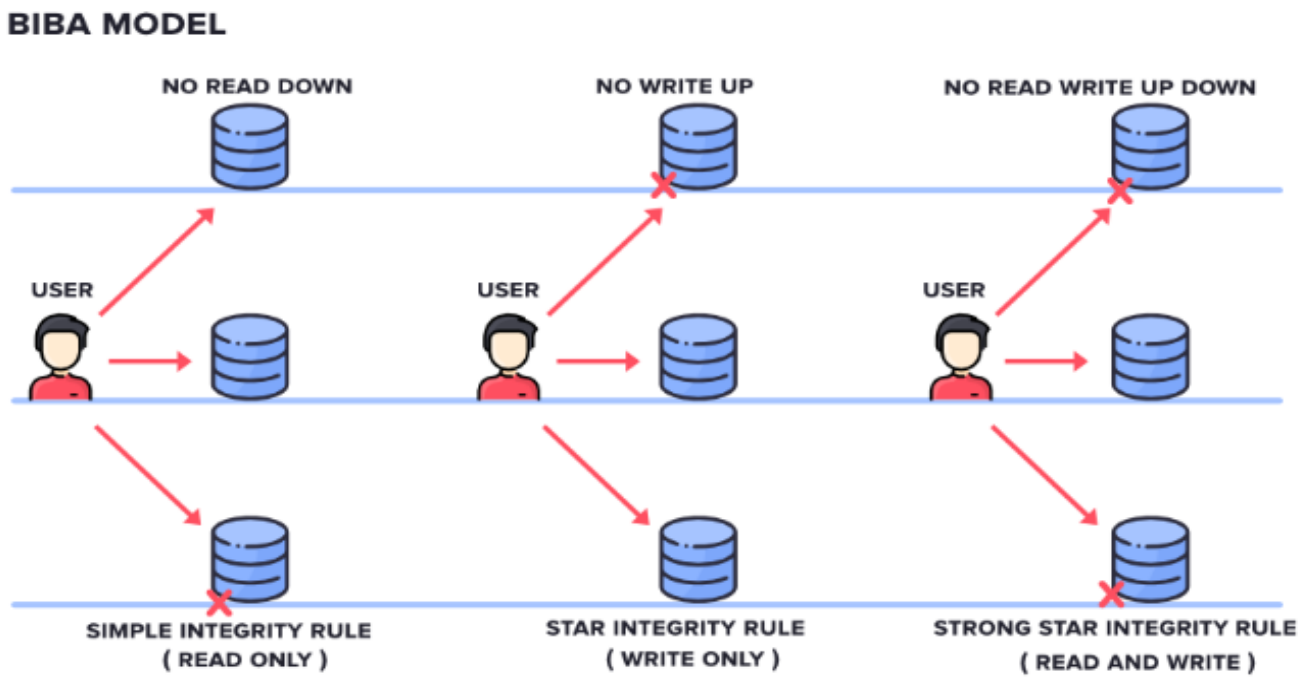

https://www.geeksforgeeks.org/introduction-to-classic-security-models/

# Phân quyền (Authorization)

- Các mô hình bảo mật thông tin

**Mô hình Biba**

- Đưa phần kiểm tra tính **toàn vẹn dữ liệu** vào mô hình Bell La-Padula
- Các đối tượng không thể sửa (ghi) đổi dữ liệu của cấp cao hơn nó




https://viblo.asia/p/mot-so-mo-hinh-an-toan-thong-tin-Qbq5QRBLKD8

# Phân quyền (Authorization)

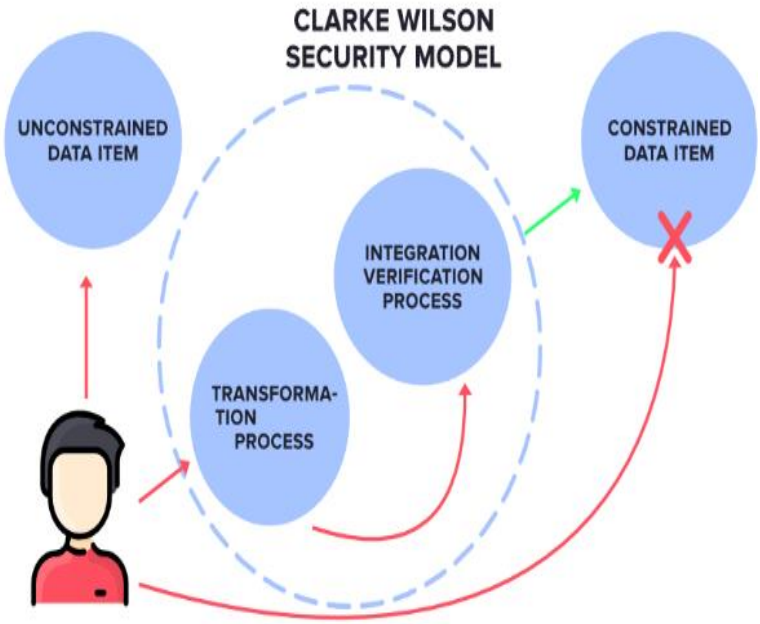
- Các mô hình bảo mật thông tin

**Mô hình Clark-Wilson**

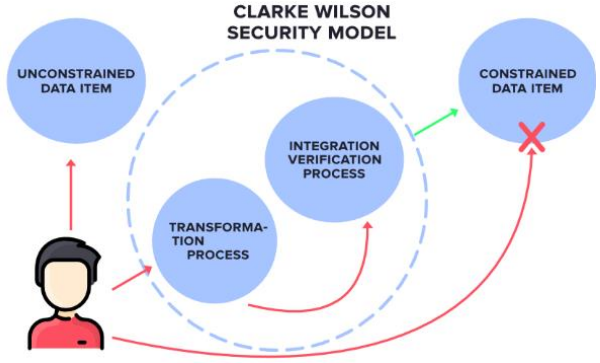
• Giải quyết sự **toàn vẹn** của dữ liệu.

• Trong mô hình này, dữ liệu được chia thành 2 loại:

- Có ràng buộc: chủ thể cần đáp ứng đủ điều kiện mới có thể truy cập. Truy cập thông qua mô hình **Clark-Wilson.**
- Không ràng buộc: mọi chủ thể có thể truy cập mà không cần điều kiện gì.



# Mô hình Clark-Wilson

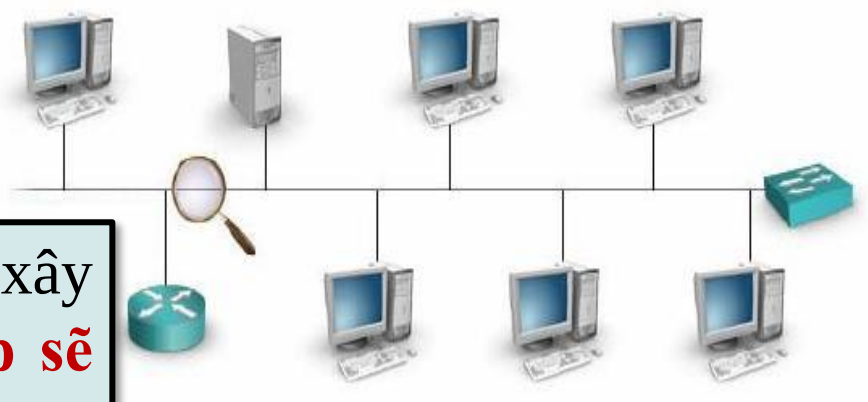



**Các thành phần của mô hình Clarke Wilson:**

- **Quy trình chuyển đổi** (Transformation Process): tiếp nhận yêu cầu truy cập dữ liệu có ràng buộc của chủ thể, chuyển đổi định danh chủ thể và định danh dữ liệu thành các mô tả quyền hạn. Sau đó chuyển thông tin này sang **Quy trình xác thực toàn vẹn**.
- **Quy trình xác thực toàn vẹn** (Integration Verification Process): thực hiện xác thực và trao quyền. Nếu quy trình này thực hiện thành công, chủ thể sẽ được chấp nhận truy cập tài liệu thông qua chương trình/dịch vụ xác định.

# Giám sát (Accounting)

- Khái niệm



Với một hệ thống giám sát được xây dựng, các **dấu vết của xâm nhập sẽ được ghi nhận lại** để cung cấp một bức tranh rõ ràng các sự kiện đã xảy ra trong hệ thống

**Các hình thức giám sát chính bao gồm:**

- Ghi file nhật ký (logging)
- Quét hệ thống (scanning)
- Kiểm soát (monitoring)

# Giám sát (Accounting)

- Ghi file nhật ký (Logging)


Log file ghi nhận lại các sự kiện và thời điểm xảy ra trong hệ thống

PR-PORTS-04-11-8-0-0-0.log - Notepad

File Edit Format View Help

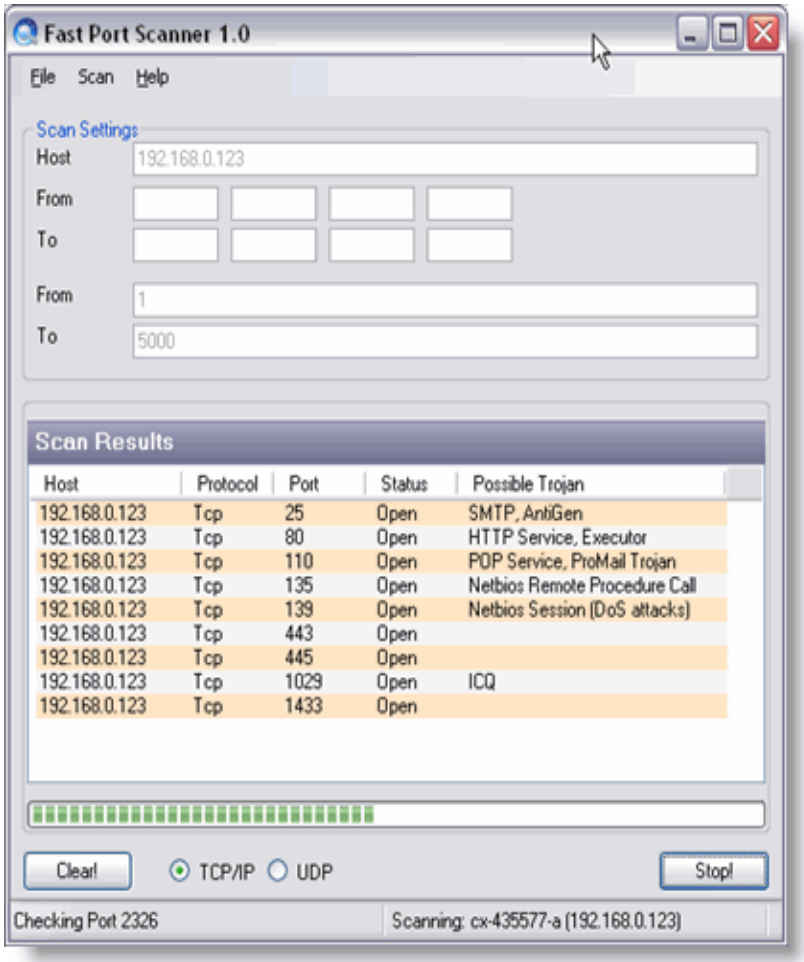
```
04/11/8,6:05:27,TCP,4842,192.168.11.11,110,68.1.17.2,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:10:33,TCP,4843,192.168.11.11,143,65.17.220.40,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:10:33,TCP,4844,192.168.11.11,110,68.1.17.2,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:13:42,TCP,4846,192.168.11.11,5431,192.168.11.1,1280,svchost.exe,<NT AUTHORITY\LOC
04/11/8,6:15:32,TCP,4847,192.168.11.11,139,192.168.11.12,0,System Idle,
04/11/8,6:15:38,TCP,4848,192.168.11.11,143,65.17.220.40,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:15:38,TCP,4849,192.168.11.11,110,68.1.17.2,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:18:36,TCP,4851,192.168.11.11,80,207.46.248.248,4860,IEXPLORE.EXE,<ASHTABULA\Al>
04/11/8,6:18:36,UDP,4850,127.0.0.1,*,*,4860,IEXPLORE.EXE,<ASHTABULA\Al>
04/11/8,6:18:39,TCP,4852,192.168.11.11,80,207.46.248.248,4860,IEXPLORE.EXE,<ASHTABULA\Al>
04/11/8,6:18:40,TCP,4853,192.168.11.11,80,207.46.248.248,4860,IEXPLORE.EXE,<ASHTABULA\Al>
04/11/8,6:18:40,TCP,4855,192.168.11.11,80,207.46.248.248,4860,IEXPLORE.EXE,<ASHTABULA\Al>
04/11/8,6:19:8,TCP,445,192.168.11.11,1383,192.168.11.12,4,System,
04/11/8,6:20:25,TCP,3389,192.168.11.11,1384,192.168.11.12,912,svchost.exe,<NT AUTHORITY\SYS
04/11/8,6:20:40,TCP,4857,192.168.11.11,110,68.1.17.2,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:20:40,TCP,4858,192.168.11.11,143,65.17.220.40,2540,OUTLOOK.EXE,<ASHTABULA\Al>
04/11/8,6:21:6,UDP,4859,0.0.0.0,*,*,4992,rdpclip.exe,<ASHTABULA\Al>
04/11/8,6:23:51,TCP,5679,0.0.0.0,,0.0.0.0,5456,WCESCOMM.EXE,<ASHTABULA\Al>
04/11/8,6:23:59,TCP,990,127.0.0.1,,0.0.0.0,5456,WCESCOMM.EXE,<ASHTABULA\Al>
04/11/8,6:24:5,TCP,1026,127.0.0.1,,0.0.0.0,5456,WCESCOMM.EXE,<ASHTABULA\Al>
04/11/8,6:24:11,UDP,4863,127.0.0.1,*,*,5992,Explorer.EXE,<ASHTABULA\Al>
04/11/8,6:24:20,UDP,4862,192.168.11.11,*,*,5992,Explorer.EXE,<ASHTABULA\Al>
04/11/8,6:24:30,TCP,999,0.0.0.0,,0.0.0.0,5668,WCESMgr.exe,<ASHTABULA\Al>
04/11/8,6:24:36,TCP,7438,0.0.0.0,,0.0.0.0,5456,WCESCOMM.EXE,<ASHTABULA\Al>
```

**Windows Firewall log file**

- Thường được ghi dưới dạng file Text, từng dòng là một sự kiện.
- Ghi nhận liên tục khi đang hoạt động.
- Có thể được ghi trên thiết bị, đĩa cục bộ, Server (SysLog) hay kết hợp nhiều nơi.
- Phải được lưu trữ trong 1 thời gian dài và bảo quản cẩn thận

# Giám sát (Accounting)

- Quét hệ thống (System scanning)



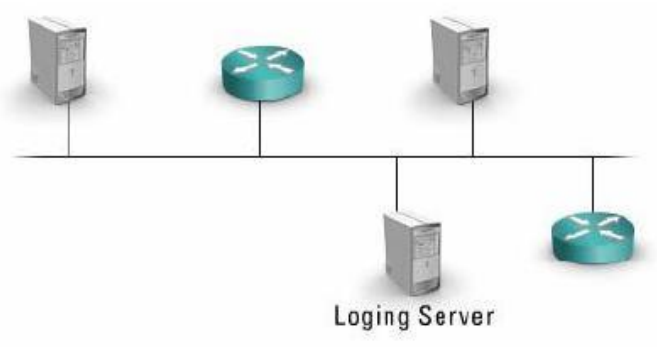

Theo dõi và kiểm tra các dịch vụ mạng nào đang hoạt động trên hệ thống

- Quét định kỳ rất quan trọng trong việc giám sát.
- Có rất nhiều các công cụ về bảo mật hỗ trợ quét hệ thống.

Kỹ thuật quét hệ thống có thể phát hiện ra những điểm yếu trong hệ thống mạng hay hệ thống máy tính để có hướng khắc phục và gia cố.

# Giám sát (Accounting)

- Kiểm soát (monitoring)




Một cách duy trì và kiểm soát hệ thống là thường xuyên xem lại các log file.

Khi có sự cố xảy ra thì quản trị mạng mới bắt đầu kiểm tra lại các log file và đôi khi điều này là đã quá muộn

Log Parser

Edit View Format

| TimeGenerated | Domain | User | SessionName | ClientName | ClientAddress | EventID |
|---|---|---|---|---|---|---|
| 2006-06-06 06:41:22 | SMB | sbunting | RDP-Tcp#8 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-06 07:08:11 | SMB | sbunting | RDP-Tcp#10 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-06 09:06:44 | SMB | sbunting | RDP-Tcp#11 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-06 09:18:11 | SMB | sbunting | RDP-Tcp#12 | 4N6NORTH | 128.175.95.41 | 682 |
| 2006-06-06 15:54:04 | SMB | sbunting | RDP-Tcp#13 | 4N6NORTH | 128.175.95.41 | 682 |
| 2006-06-06 16:34:21 | SMB | sbunting | RDP-Tcp#14 | 4N6NORTH | 128.175.95.41 | 682 |
| 2006-06-06 17:27:35 | SMB | sbunting | RDP-Tcp#15 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-06 18:43:52 | SMB | sbunting | Console | Unknown | Unknown | 682 |
| 2006-06-07 07:10:41 | SMB | sbunting | RDP-Tcp#16 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-07 08:16:29 | SMB | sbunting | RDP-Tcp#18 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-07 10:52:17 | SMB | sbunting | RDP-Tcp#19 | 4N6NORTH | 128.175.95.41 | 682 |
| 2006-06-07 13:52:55 | SMB | sbunting | RDP-Tcp#20 | 4N6NORTH | 128.175.95.41 | 682 |
| 2006-06-07 16:24:47 | SMB | sbunting | RDP-Tcp#21 | UDPD-R3YUAMBNI5 | 166.161.87.202 | 682 |
| 2006-06-07 17:46:32 | SMB | sbunting | Console | Unknown | Unknown | 682 |
| 2006-06-07 19:10:16 | SMB | sbunting | RDP-Tcp#22 | MOBILE4N6 | 166.161.87.201 | 682 |
| 2006-06-08 06:42:15 | SMB | sbunting | Console | Unknown | Unknown | 682 |

Auto Resize Close All rows Next 10 rows

Sử dụng các công cụ hỗ trợ trong việc phân tích các log file và có cảnh báo các nguy cơ.