

CHƯƠNG 4

KIỂM SOÁT TRUY CẬP

(ACCESS CONTROL)

11/7/2020

ThS.Nguyễn Duy
duyn@uit.edu.vn

Nội dung

2

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- Kĩ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Nội dung

3

duyn@uit.edu.vn

- **Tổng quan về kiểm soát truy cập?**
- Mô hình kiểm soát truy cập
- Kĩ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Tổng quan về kiểm soát truy cập?

Khái niệm

4

duyn@uit.edu.vn

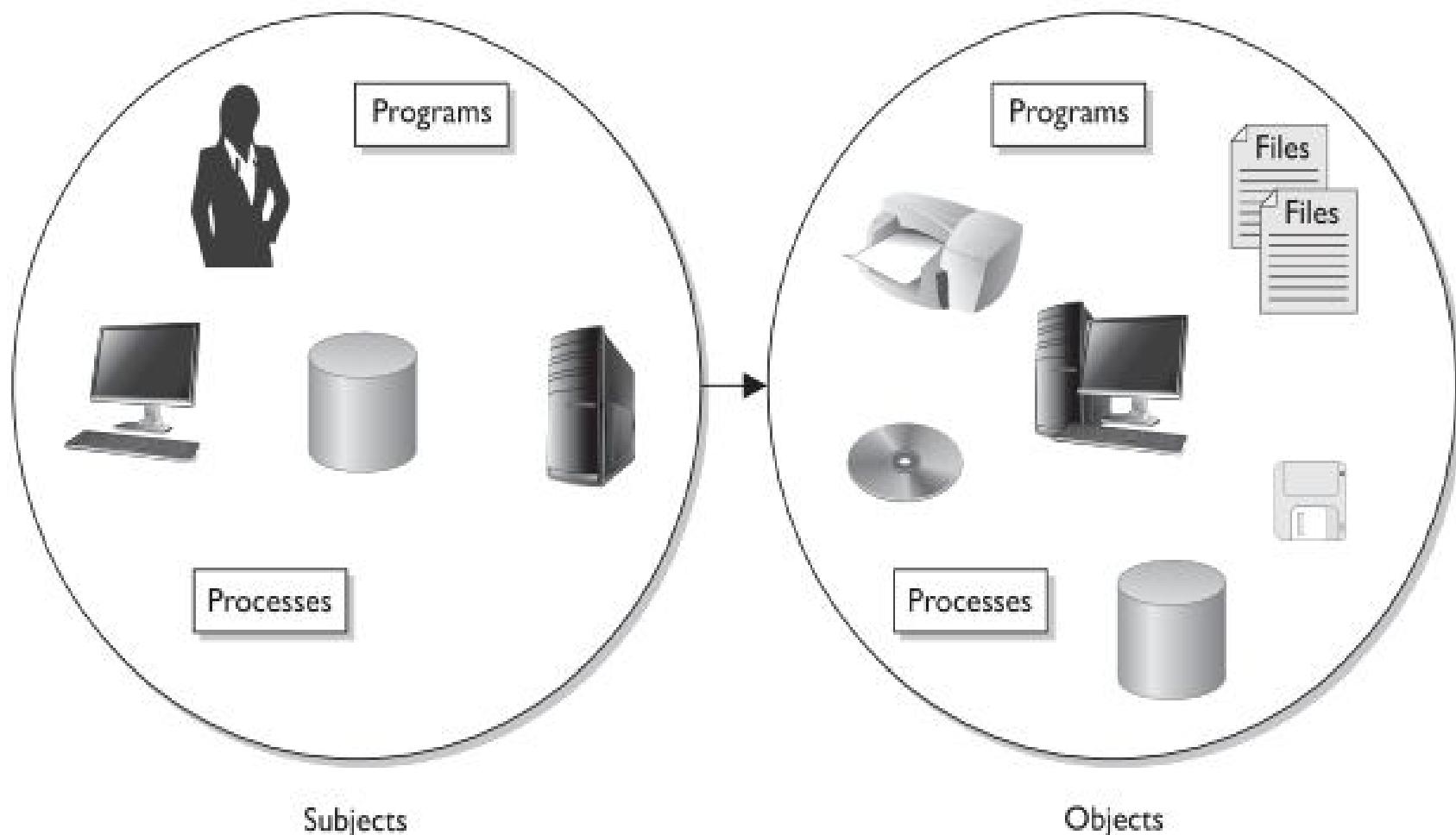
- Kiểm soát truy cập là kiểm soát cách người dùng và hệ thống giao tiếp và tương tác với các hệ thống và các tài nguyên khác.
- Mục đích: bảo vệ hệ thống và các tài nguyên từ các truy cập trái phép.
- Được chia thành 2 phần: Access và Control
 - Access là quá trình truy cập các tài nguyên của một chủ thể (Subject) tới một đối tượng (Object)
 - Control là hành động cho phép hoặc không cho phép truy cập, cũng như các phương thức áp dụng cho Access Control

Tổng quan về kiểm soát truy cập?

Khái niệm - tt

5

duyn@uit.edu.vn

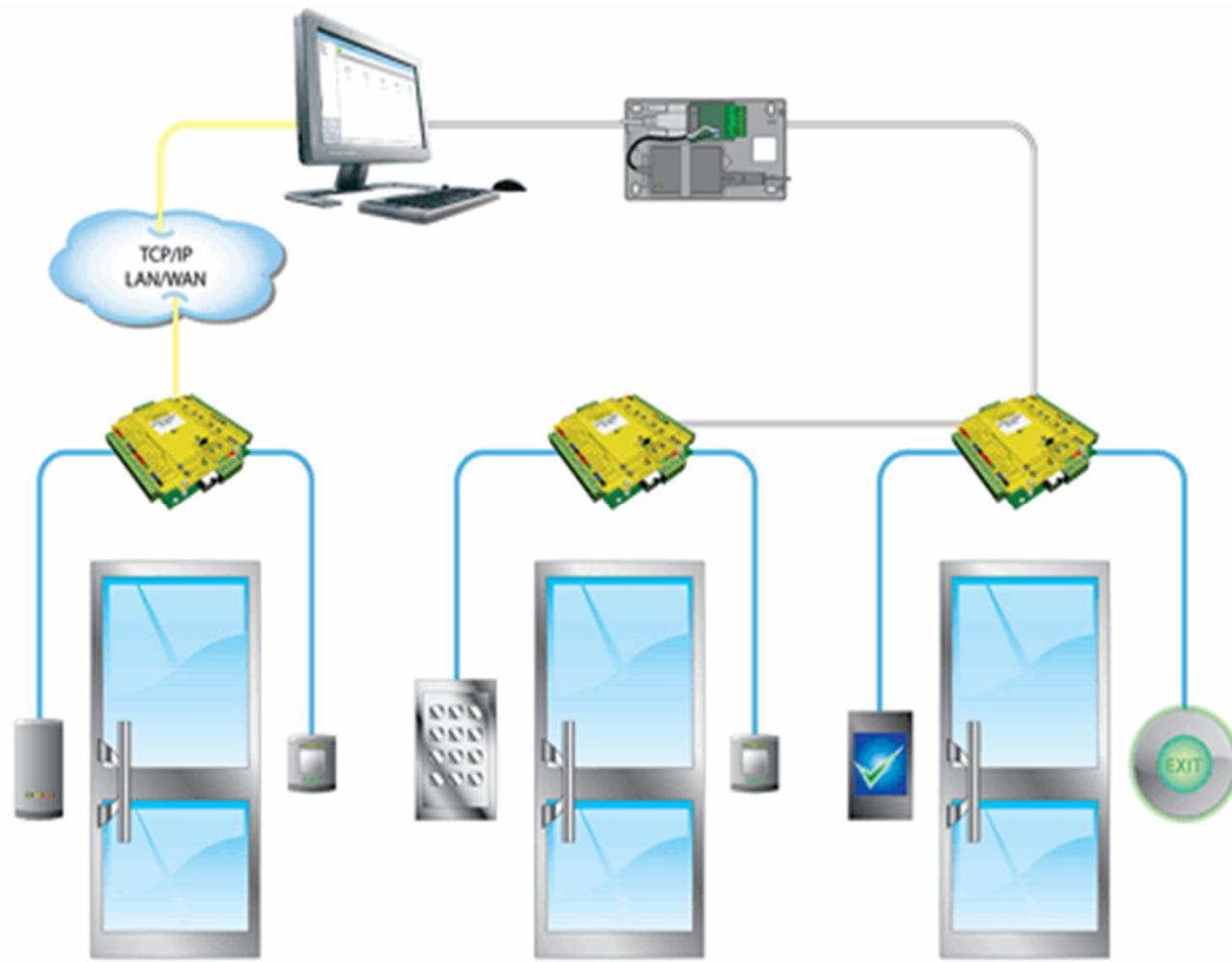


Tổng quan về kiểm soát truy cập?

Khái niệm - tt

6

duyn@uit.edu.vn

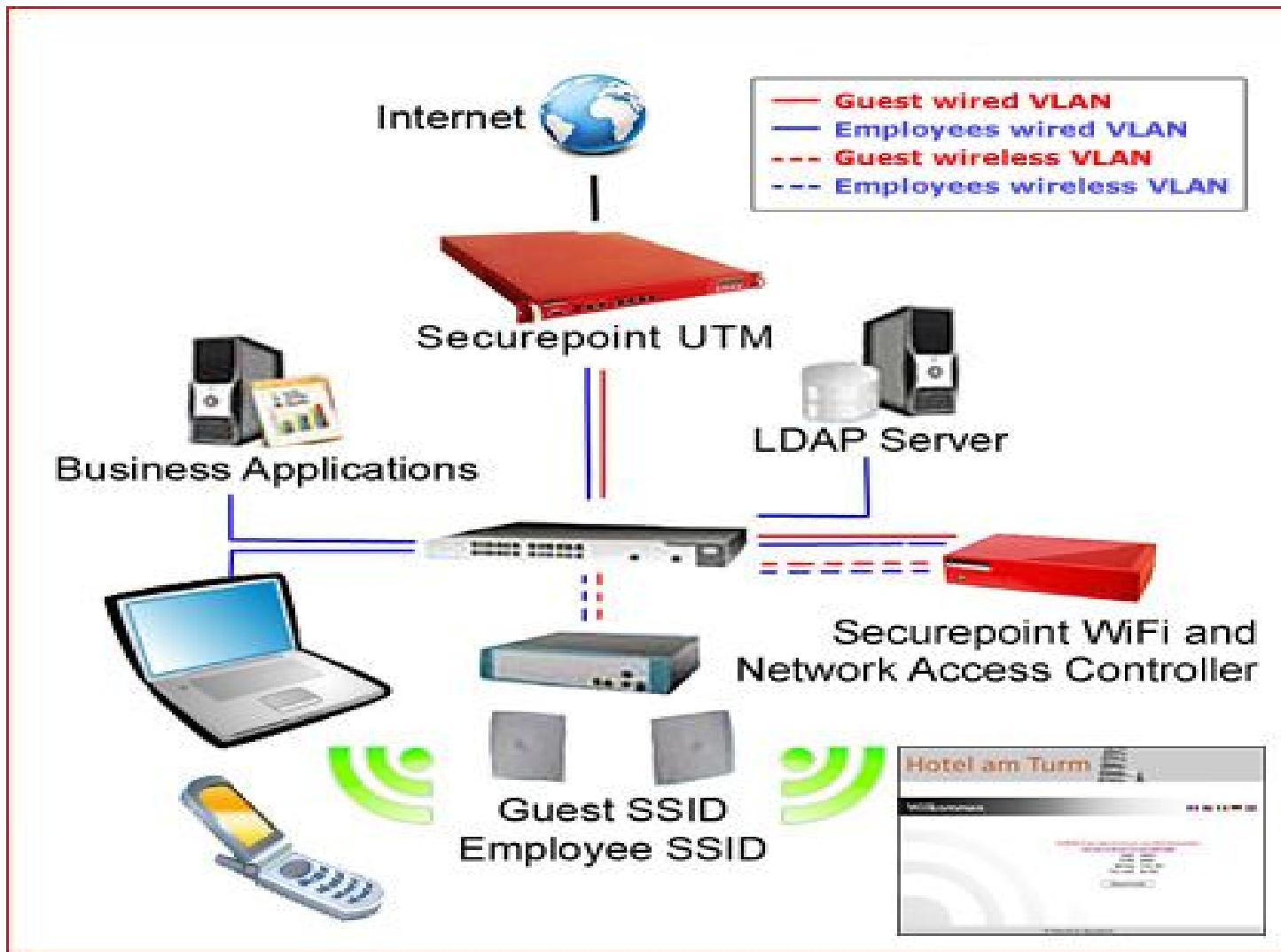


Tổng quan về kiểm soát truy cập?

Khái niệm - tt

7

duyn@uit.edu.vn



Tổng quan về kiểm soát truy cập?

Khái niệm - tt

8

duyn@uit.edu.vn

- Identification (định danh)
 - Subjects cung cấp thông tin nhận dạng
 - Username, user ID, account number,...
- Authentication (xác thực)
 - Xác minh thông tin định danh
 - Passphrase, PIN value, biometric, one-time password, password,...
- Authorization (Phân quyền)
 - Mức độ truy cập của các Subject lên các Object
- Accountability (Theo vết)
 - Theo dõi các hành động của các Subject lên các Object

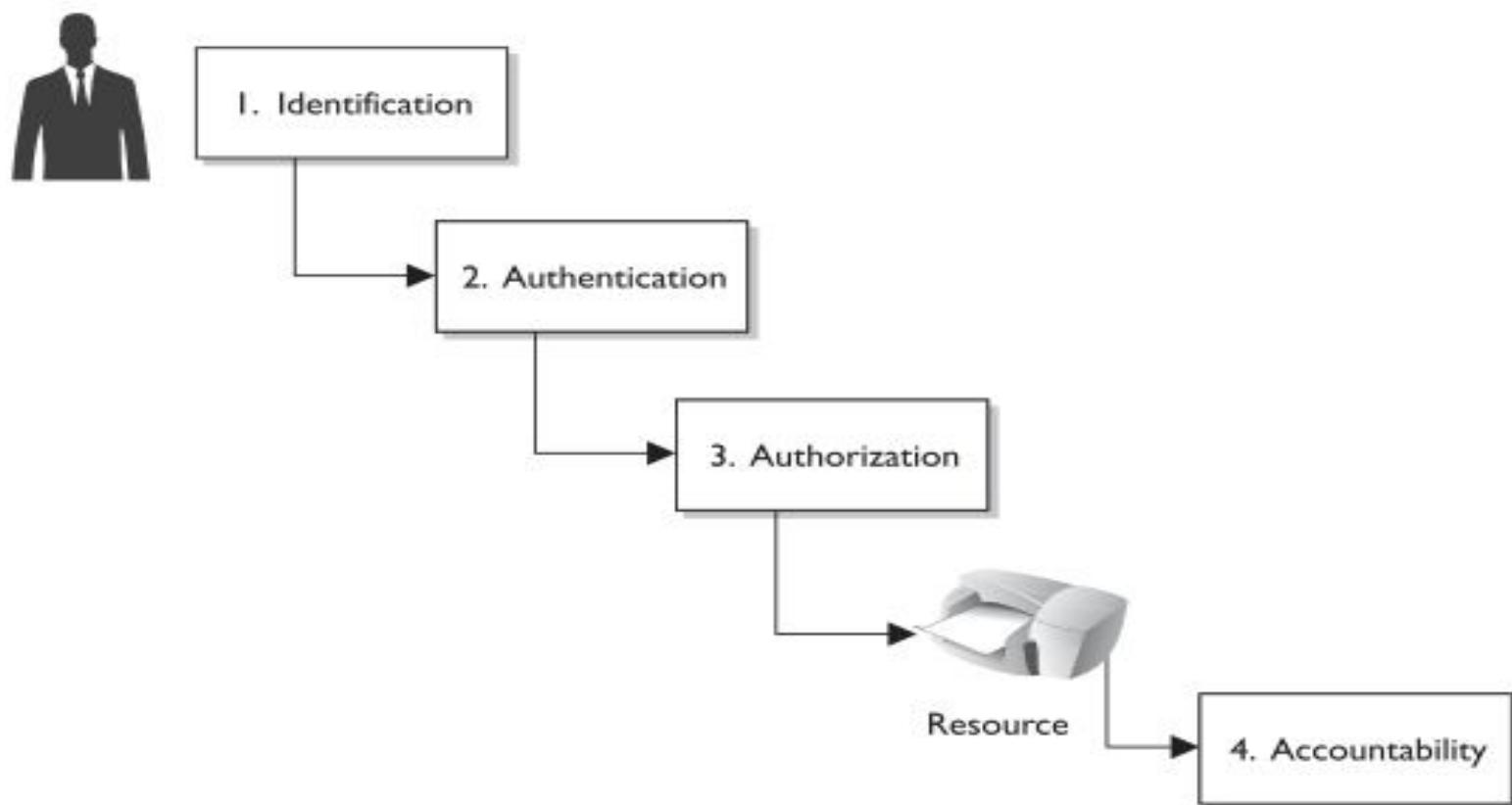
Tổng quan về kiểm soát truy cập?

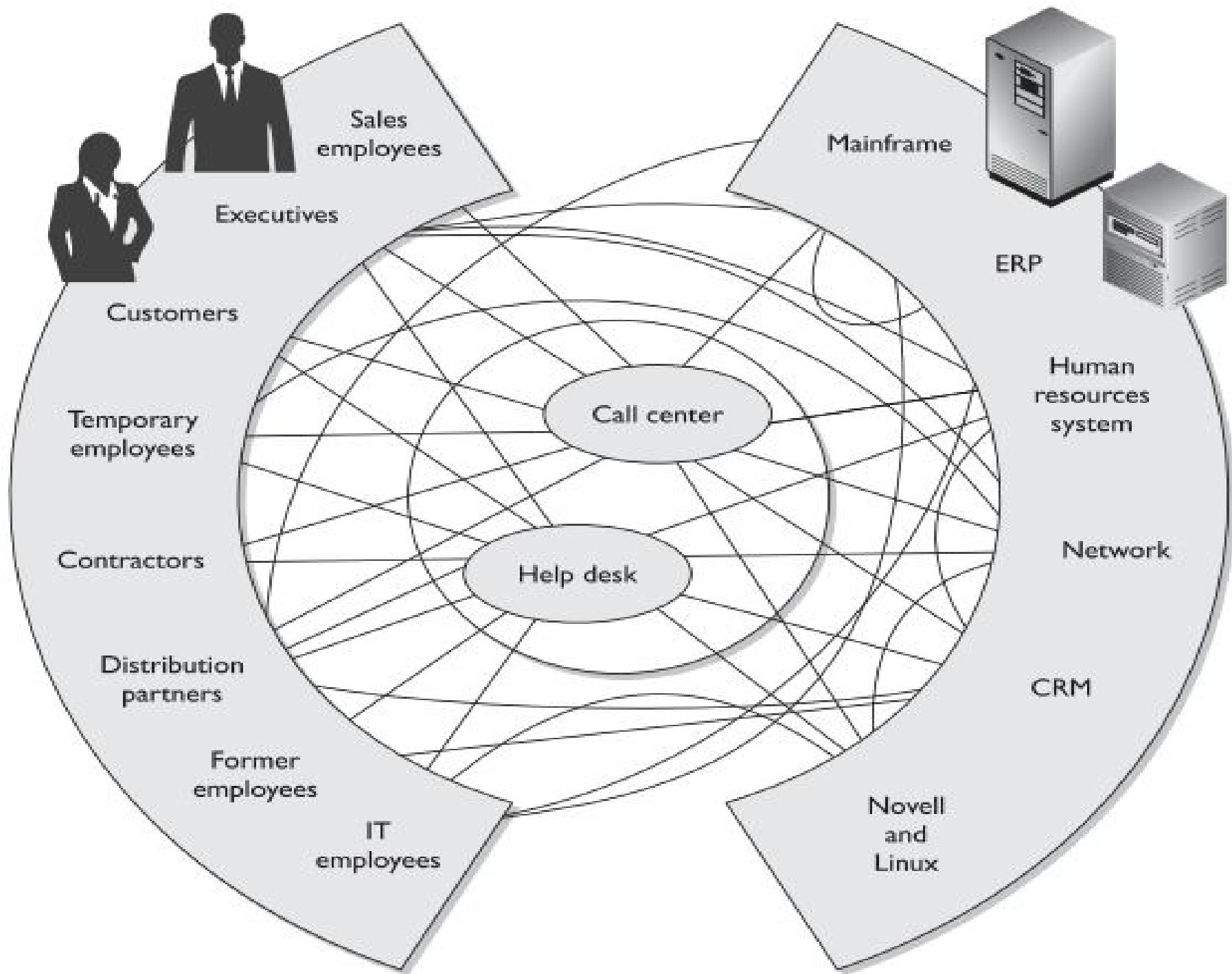
Khái niệm - tt

9

duyn@uit.edu.vn

- 4 bước diễn ra trong quá trình Subject truy cập Object





Tổng quan về kiểm soát truy cập?

Khái niệm - tt

11

duyn@uit.edu.vn

- Những câu hỏi phổ biến các doanh nghiệp ngày nay thường đặt ra để quản lý kiểm soát quyền truy cập vào tài sản:
 - Phân loại đối tượng truy cập (nhân viên, khách hàng và đối tác,...)
 - Yếu tố dùng để xác minh khi truy cập?
 - Phương thức xác thực khi truy cập?
 - Người dùng được truy cập vào đâu?
 - Ai là người phê duyệt cho phép truy cập?
 - Theo dõi quá trình truy cập của người dùng
 - Cách thức thu hồi quyền truy cập

Nội dung

12

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- **Mô hình kiểm soát truy cập**
- Kĩ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Mô hình kiểm soát truy cập

13

duyn@uit.edu.vn

- Mô hình kiểm soát truy cập là một khuôn khổ (framework) dùng để qui định như thế nào Subject truy cập Object.
- Có 3 mô hình kiểm soát truy cập chính
 - **Discretionary Access Control**
 - **Mandatory Access Control**
 - **Role-Based Access Control**
- Những mô hình này được xây dựng tích hợp vào lõi hoặc hạt nhân của hệ điều hành.

Mô hình kiểm soát truy cập

Discretionary Access Control (DAC)

14

duyn@uit.edu.vn

- Cho phép chủ sở hữu của tài nguyên chỉ định các đối tượng có thể truy cập tài nguyên của mình.
- Mô hình này được gọi là tùy ý (Discretionary) vì sự kiểm soát truy cập dựa trên quyết định của chủ sở hữu.
 - Network: ACLs, Rule of Firewall,...
 - System: Sharing Permission, NTFS,...

Mô hình kiểm soát truy cập

Mandatory Access Control (MAC)

15

duyn@uit.edu.vn

- Một hệ điều hành dựa trên một mô hình MAC làm giảm đáng kể số lượng quyền, quyền hạn, chức năng của người sử dụng cho các mục đích an ninh.
 - Người dùng bình thường không thể cài phần mềm
 - Không thể tạo, xóa và sửa thông tin người dùng khác
 - Không thể thay đổi cấu hình: IP, quyền hạn trên tài nguyên dùng chung,...

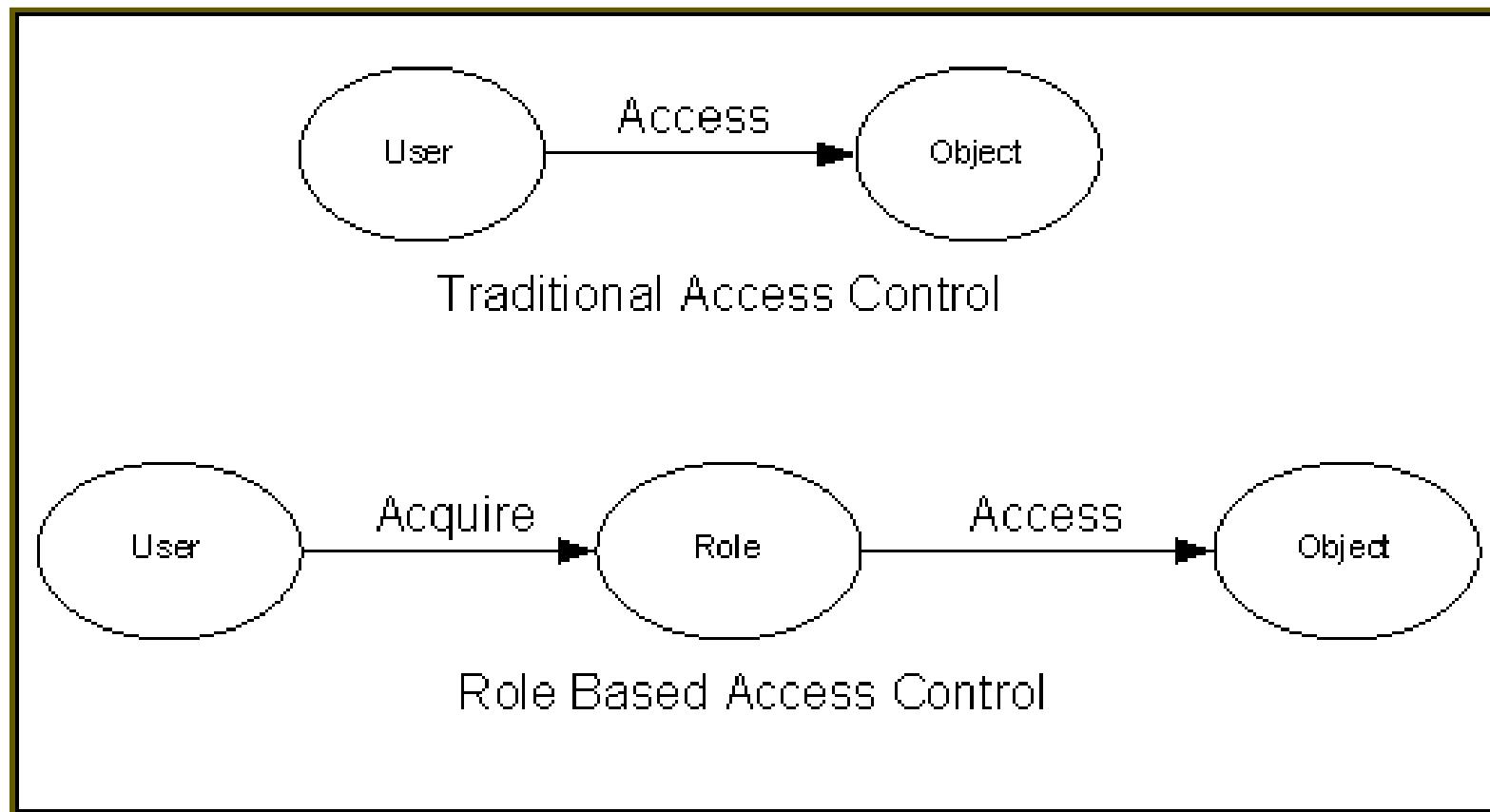
Mô hình kiểm soát truy cập

Role-Based Access Control (RBAC)

16

duyn@uit.edu.vn

- Mô hình quản lý tập trung và phân nhóm các quyền truy cập



Nội dung

17

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- **Kĩ thuật kiểm soát truy cập**
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Kĩ thuật kiểm soát truy cập

18

duyn@uit.edu.vn

- Sau khi quyết định hình mô hình kiểm soát truy cập sẽ sử dụng trong hệ thống bước tiếp theo cần phải xác định các kĩ thuật và công nghệ để hỗ trợ mô hình đó.
 - **Rule-Based Access Control**
 - **Constrained User Interfaces**
 - **Access Control Matrix**
 - **Content-Dependent Access Control**
 - **Context-Dependent Access Control**

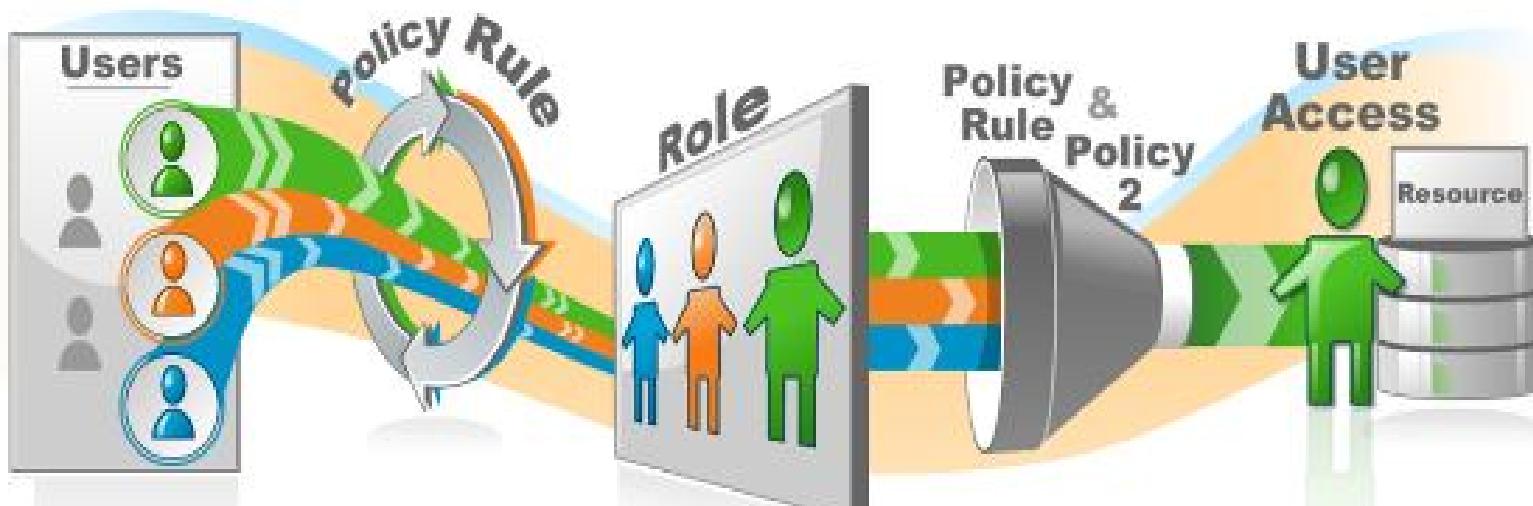
Kĩ thuật kiểm soát truy cập

Rule-Based Access Control

19

duyn@uit.edu.vn

- Sử dụng quy tắc cụ thể để chỉ định những gì có thể và không có thể xảy ra giữa một chủ thể và một đối tượng



Kĩ thuật kiểm soát truy cập

Constrained User Interfaces

20

duyn@uit.edu.vn

- Hạn chế khả năng truy cập của người sử dụng bằng cách không cho phép họ yêu cầu chức năng hoặc thông tin nào đó, hoặc có quyền truy cập vào tài nguyên hệ thống cụ thể.
- Ba loại chính của Constrained User Interfaces:
 - Menus và shells
 - Database views
 - Physically constrained interfaces

Kĩ thuật kiểm soát truy cập

Access Control Matrix

21

duyn@uit.edu.vn

- Ma trận kiểm soát truy cập là một bảng của các chủ thể và các đối tượng cho thấy những hành động chủ thể cá nhân có thể thao tác trên đối tượng cá nhân.

User	File1	File2	File3
Diane	Read and execute	Read, write, and execute	No access
Katie	Read and execute	Read	No access
Chrissy	Read, write, and execute	Read and execute	Read
John	Read and execute	No access	Read and write

Kĩ thuật kiểm soát truy cập

Content-Dependent Access Control

22

duyn@uit.edu.vn

- Kiểm soát việc truy cập vào đối tượng dựa vào nội dung của đối tượng đó.

Kĩ thuật kiểm soát truy cập

Context-Dependent Access Control

23

duyn@uit.edu.vn

- Dựa vào ngữ cảnh và thông tin thu thập được để kiểm soát truy cập
- Thường chỉ có ở những công nghệ mới sau này: Next Generation Firewall, IDS/IPS, Unified Threat Management,...

Nội dung

24

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- Kỹ thuật kiểm soát truy cập
- **Quản trị kiểm soát truy cập**
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Quản trị kiểm soát truy cập

25

duyn@uit.edu.vn

- Đầu tiên một tổ chức phải lựa chọn mô hình điều khiển truy cập (DAC, MAC, RBAC)
- Sau đó tổ chức phải lựa chọn và thực hiện công nghệ kiểm soát truy cập
- Quản lý điều khiển truy cập có hai hình thức cơ bản:
 - Centralized (tập trung)
 - Decentralized (không tập trung)

Quản trị kiểm soát truy cập

Tập trung

26

duyn@uit.edu.vn

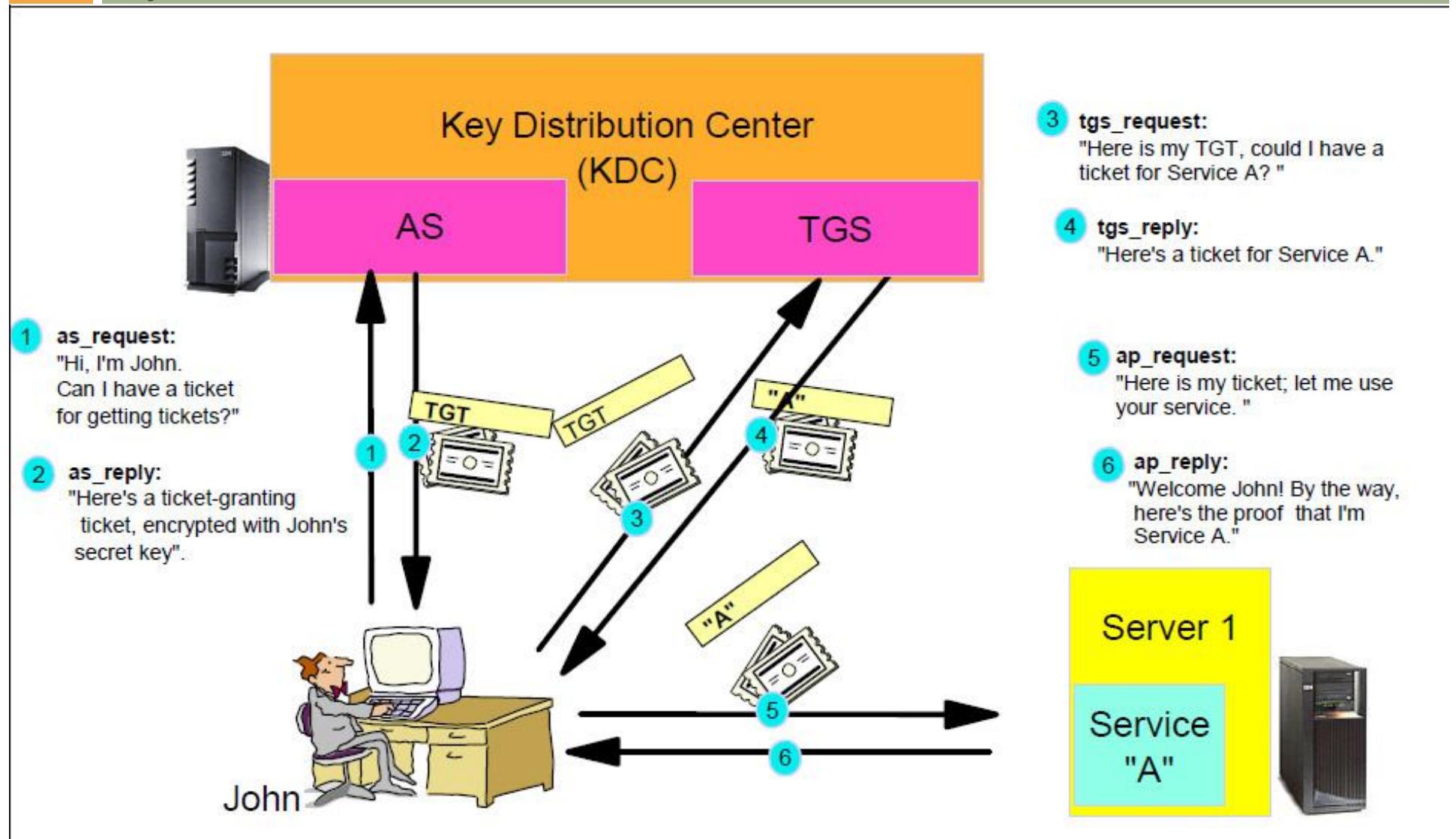
- Một thực thể có trách nhiệm giám sát truy cập vào tất cả các tài nguyên của tổ chức.
- Cung cấp một phương pháp phù hợp và thống nhất kiểm soát quyền truy cập.
- Mỗi một giao thức xác thực cần tham chiếu tới giao thức AAA (authentication, authorization, và auditing)
- Kiến trúc Client/Server: Kerberos, RADIUS, Terminal Access Controller Access Control System (TACACS),...

Quản trị kiểm soát truy cập

Tập trung - Kerberos

27

duyn@uit.edu.vn

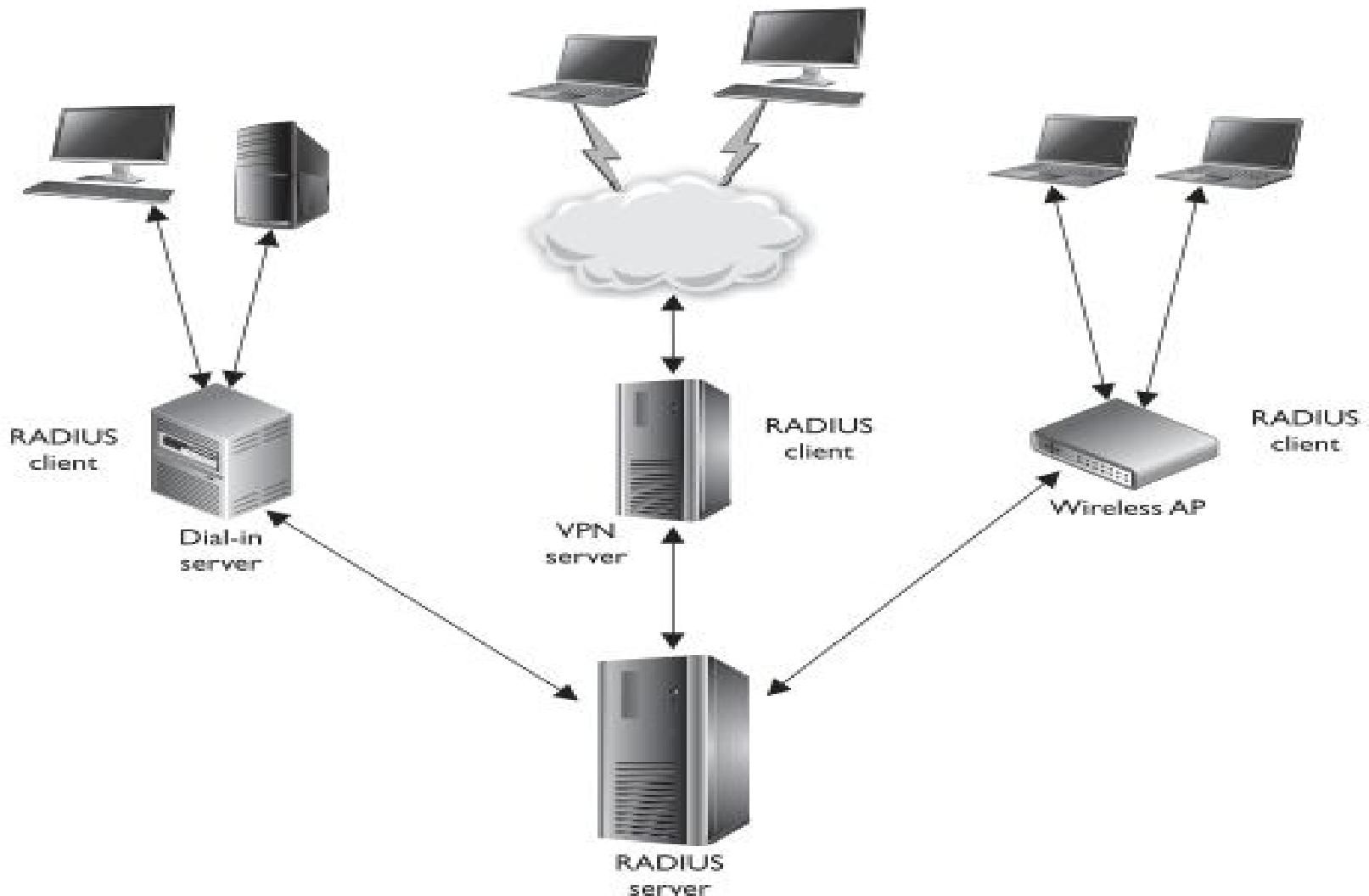


Quản trị kiểm soát truy cập

Tập trung - RADIUS

28

duyn@uit.edu.vn



Quản trị kiểm soát truy cập

Không tập trung

29

duyn@uit.edu.vn

- Cho phép người dùng tự kiểm soát truy cập
 - Tự chia sẻ dữ liệu
- Không có phương pháp kiểm soát phù hợp và thiếu nhất quán

Nội dung

30

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- Kĩ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- **Phương thức kiểm soát truy cập**
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Phương thức kiểm soát truy cập

31

duyn@uit.edu.vn

- Kiểm soát truy cập có thể được thực hiện ở các tầng khác nhau của một tổ chức, mạng lưới và hệ thống cá nhân.



Phương thức kiểm soát truy cập

Hành chính

32

duyn@uit.edu.vn

- Chính sách và qui trình truy cập
- Kiểm soát con người
- Cơ cấu giám sát
- Đào tạo nâng cao nhận thức an ninh
- Kiểm tra

Phương thức kiểm soát truy cập

Vật lý

33

duyn@uit.edu.vn

- Network Segregation
- Perimeter Security
- Computer Controls
- Work Area Separation
- Data Backups
- Cabling
- Control Zone

Phương thức kiểm soát truy cập

Kĩ thuật (logic)

34

duyn@uit.edu.vn

- System Access
- Network Access
- Network Architecture
- Encryption and protocols
- Auditing

Nội dung

35

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- Kĩ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- **Theo vết (Accountability) truy cập**
- Giám sát truy cập
- Những mối đe dọa với kiểm soát truy cập

Theo vết (Accountability) truy cập

36

duyn@uit.edu.vn

- Quá trình theo dõi hành động của Users, System và Applications
- Quá trình theo dõi hành động này sẽ được thực thi bởi hệ điều hành và ứng dụng
- Kết quả của quá trình theo dõi:
 - Phải được lưu trữ
 - Dung lượng lưu trữ
 - Thời gian lưu trữ
 - Ai được quyền truy cập
 - Ai được quyền xóa

Theo vết (Accountability) truy cập

37

duyn@uit.edu.vn

- System-level events
 - System performance
 - Logon attempts (successful and unsuccessful)
 - Logon ID
 - Date and time of each logon attempt
 - Lockouts of users and terminals
 - Use of administration utilities
 - Devices used
 - Functions performed
 - Requests to alter configuration

Theo vết (Accountability) truy cập

38

duyn@uit.edu.vn

- Application-level events
 - Error messages
 - Files opened and closed
 - Modifications of files
 - Security violations within application
- User-level events
 - Identification and authentication attempts
 - Files, services, and resources used
 - Commands initiated
 - Security violations

Nội dung

39

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- Kỹ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- **Giám sát truy cập**
- Những mối đe dọa với kiểm soát truy cập

Giám sát truy cập

40

duyn@uit.edu.vn

- Giám sát kiểm soát truy cập là một phương pháp theo dõi của những chủ thể (người dùng và ứng dụng) cố gắng để truy cập tài nguyên.
- Một trong những giải pháp giám sát truy cập nổi tiếng
 - Intrusion Detection
 - Intrusion Prevention
 - Honeypot
 - Packet Sniffer
 - Networking Activities

Giám sát truy cập - tt

41

duyn@uit.edu.vn

- Intrusion Detection có 3 thành phần chính
 - Sensor
 - Analyzers
 - Administrator Interface
- Intrusion Detection có 2 loại chính:
 - Network Based (NIDS)
 - Host Based (HIDS)
- Nhiệm vụ chính của IDS:
 - Giám sát
 - Phân tích
 - Cảnh báo
 - Báo cáo

Giám sát truy cập - tt

42

duyn@uit.edu.vn

- Intrusion Prevention có 3 thành phần chính
 - Sensor
 - Analyzers
 - Administrator Interface
- Intrusion Prevention có 2 loại chính:
 - Network Based (NIDS)
 - Host Based (HIDS)
- Nhiệm vụ chính của IDS:
 - Giám sát
 - Phân tích
 - Cảnh báo
 - Báo cáo
 - Phản ứng

Giám sát truy cập - tt

43

duyn@uit.edu.vn

➤ Honeypots

- Một máy tính được sử dụng để thu hút người tấn công
- Thu thập thông tin cuộc tấn công

➤ Network sniffers

- Các chương trình hoặc các thiết bị có khả năng kiểm tra gói tin trên một phân đoạn mạng LAN.

Nội dung

44

duyn@uit.edu.vn

- Tổng quan về kiểm soát truy cập?
- Mô hình kiểm soát truy cập
- Kĩ thuật kiểm soát truy cập
- Quản trị kiểm soát truy cập
- Phương thức kiểm soát truy cập
- Theo vết (Accountability) truy cập
- Giám sát truy cập
- **Những mối đe dọa với kiểm soát truy cập**

Những mối đe dọa với kiểm soát truy cập

45

duyn@uit.edu.vn

➤ **Dictionary Attack**

- Một số chương trình có thể cho phép kẻ tấn công (hoặc quản trị viên chủ động) xác định người sử dụng thông tin
- Biện pháp đối phó:
 - Mã hóa password (lưu trữ và khi truyền)
 - Băm password (hashing)
 - One-time password
 - Chính sách thay đổi password và lịch sử thay đổi
 - Bảo vệ hệ thống lưu trữ password
 - Giới hạn số lần logon sai
 - IDS

Những mối đe dọa với kiểm soát truy cập

46

duyn@uit.edu.vn

➤ Brute Force Attacks

- Có gắng kết hợp tất cả các yếu tố có thể cho đến khi Password được xác định
- Biện pháp đối phó:
 - Mã hóa password (lưu trữ và khi truyền)
 - Băm password (hashing)
 - One-time password
 - Chính sách thay đổi password và lịch sử thay đổi
 - Bảo vệ hệ thống lưu trữ password
 - Giới hạn số lần logon sai
 - IDS

Những mối đe dọa với kiểm soát truy cập

47

duyn@uit.edu.vn

➤ Spoofing at Logon

- Người tấn công sử dụng chương trình để đưa người dùng đến màn hình logon giả mạo với mục đích đánh lừa người dùng logon. Sau khi logon thì thông tin tài khoản đã được lưu trữ trên hệ thống của attacker.
- Biện pháp đối phó:
 - IPSecurity
 - SSL
 - Mutual authentication

Question ???

