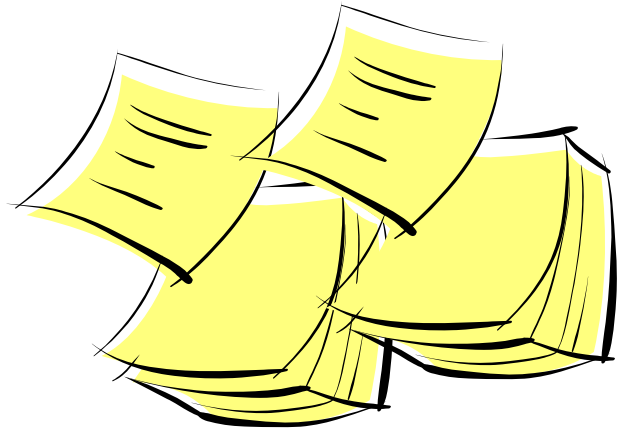


CHƯƠNG I

TỔNG QUAN VỀ BẢO MẬT
Hệ Thống Thông Tin

I.1 Giới thiệu chung

I.1.1 Mở đầu về bảo mật hệ thống thông tin

- Gồm ba hướng chính
  - **Bảo đảm an toàn thông tin tại máy chủ**
  - **Bảo đảm an toàn cho phía máy trạm**
  - **Bảo mật thông tin trên đường truyền**
- Có thể xem xét theo
  - **Hệ điều hành và ứng dụng**
  - **Cơ sở dữ liệu**
  - **Mạng**

Những yêu cầu về an toàn

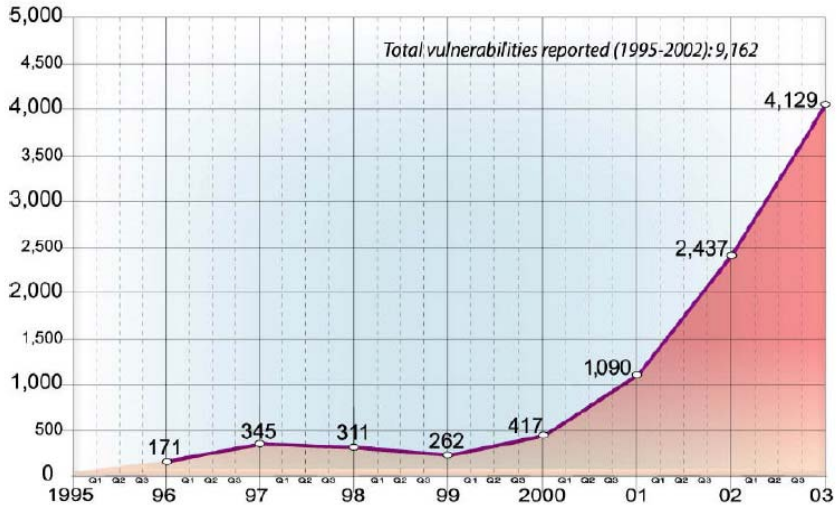
- Confidentiality (sự tin cậy)
- Integrity (tính toàn vẹn)
- Authentication (chứng thực)
- Non-repudiation (không thể từ chối)
- Availability (sẵn dùng)
- Access control (điều khiển truy cập)
- Combined
  - **User authentication used for access control**
  - **Non-repudiation combined with authentication**

Các yêu an toàn thông tin

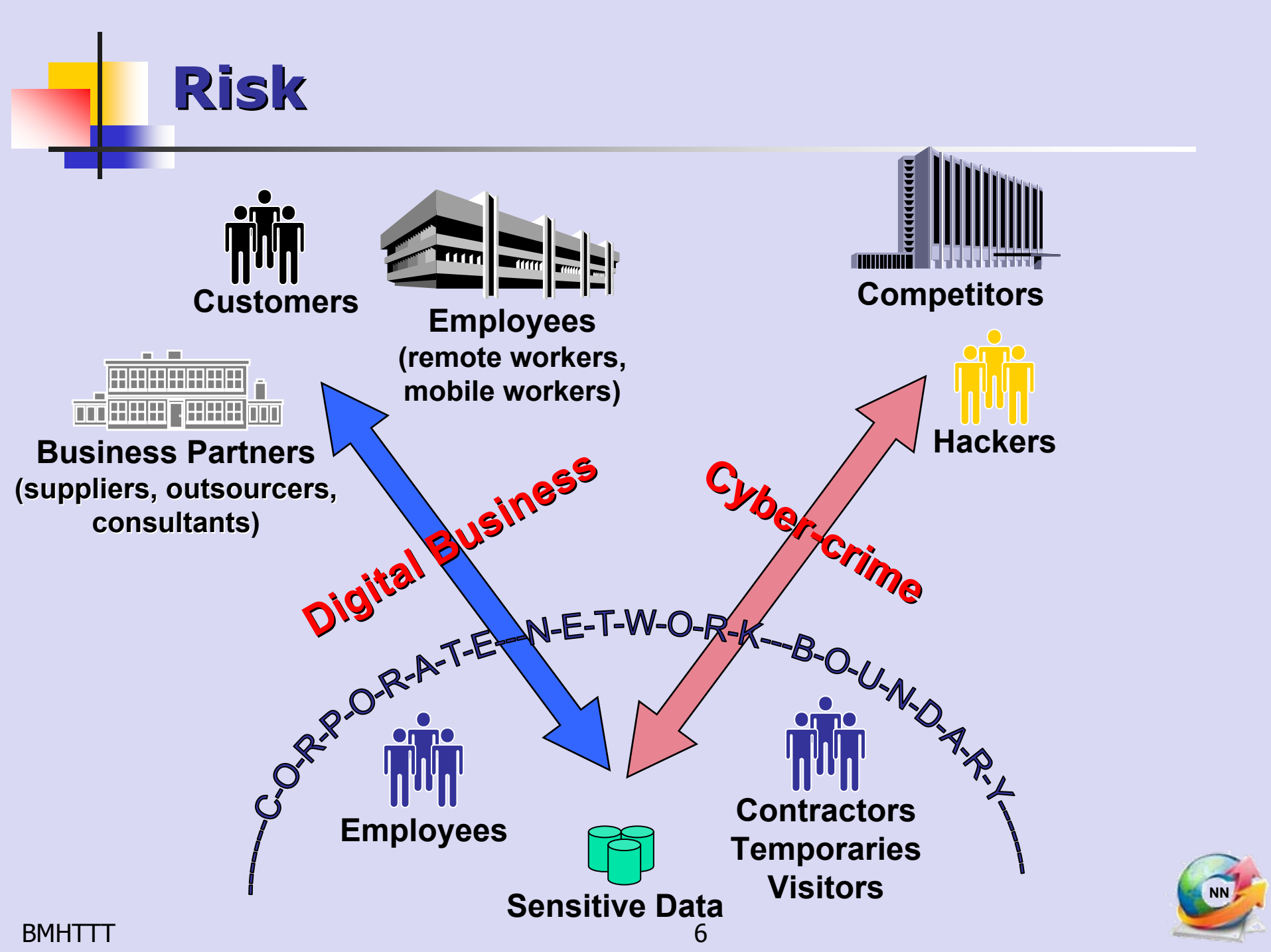
- Nhiều yêu cầu mới liên quan tới bảo mật hệ thống thông tin trên mạng
- Ngoài phương pháp vật lý còn cần các kỹ thuật bảo mật, chính sách bảo mật và các giải pháp bảo mật
- Phải có các công cụ hỗ trợ bảo đảm an toàn thông tin.
- Các yêu cầu mới: Bảo mật Outsourcing, bảo mật hệ thống phân bố, bảo mật trong Datamining, cơ sở dữ liệu thống kê, giao dịch thương mại điện tử, tính riêng tư, tội phạm và bản quyền số…

Attack


November 1988
Sunday
Monday
Tuesday
Wednesday
Friday
Saturday
Worm Attack
Morris Worm
Post Mortem
CERT/CC
created
CERT
Coordination
Center


Total vulnerabilities reported (1995-2002): 9,162
5,000
4,500
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
171
345
311
262
417
1,090
2,437
4,129
1995
96
97
98
99
2000
01
02
03

Risk


Customers
Employees
(remote workers,
mobile workers)
Competitors
Business Partners
(suppliers, outsourcers,
consultants)
Hackers
Digital Business
Cyber-crime
C-O-R-P-O-R-A-T-E---N-E-T-W-O-R-K---B-O-U-N-D-A-R-Y
Employees
Contractors
Temporaries
Visitors
Sensitive Data

I.1.2 Nguy cơ và hiểm họa

- **Hiểm họa vô tình:** khi người dùng khởi động lại hệ thống ở chế độ đặc quyền, họ có thể tùy ý chỉnh sửa hệ thống. Nhưng sau khi hoàn thành công việc họ không chuyển hệ thống sang chế độ thông thường, vô tình để kẻ xấu lợi dụng.
- **Hiểm họa cố ý:** như cố tình truy nhập hệ thống trái phép.
- **Hiểm họa thụ động:** là hiểm họa nhưng chưa hoặc không tác động trực tiếp lên hệ thống, như nghe trộm các gói tin trên đường truyền.
- **Hiểm họa chủ động:** là việc sửa đổi thông tin, thay đổi tình trạng hoặc hoạt động của hệ thống

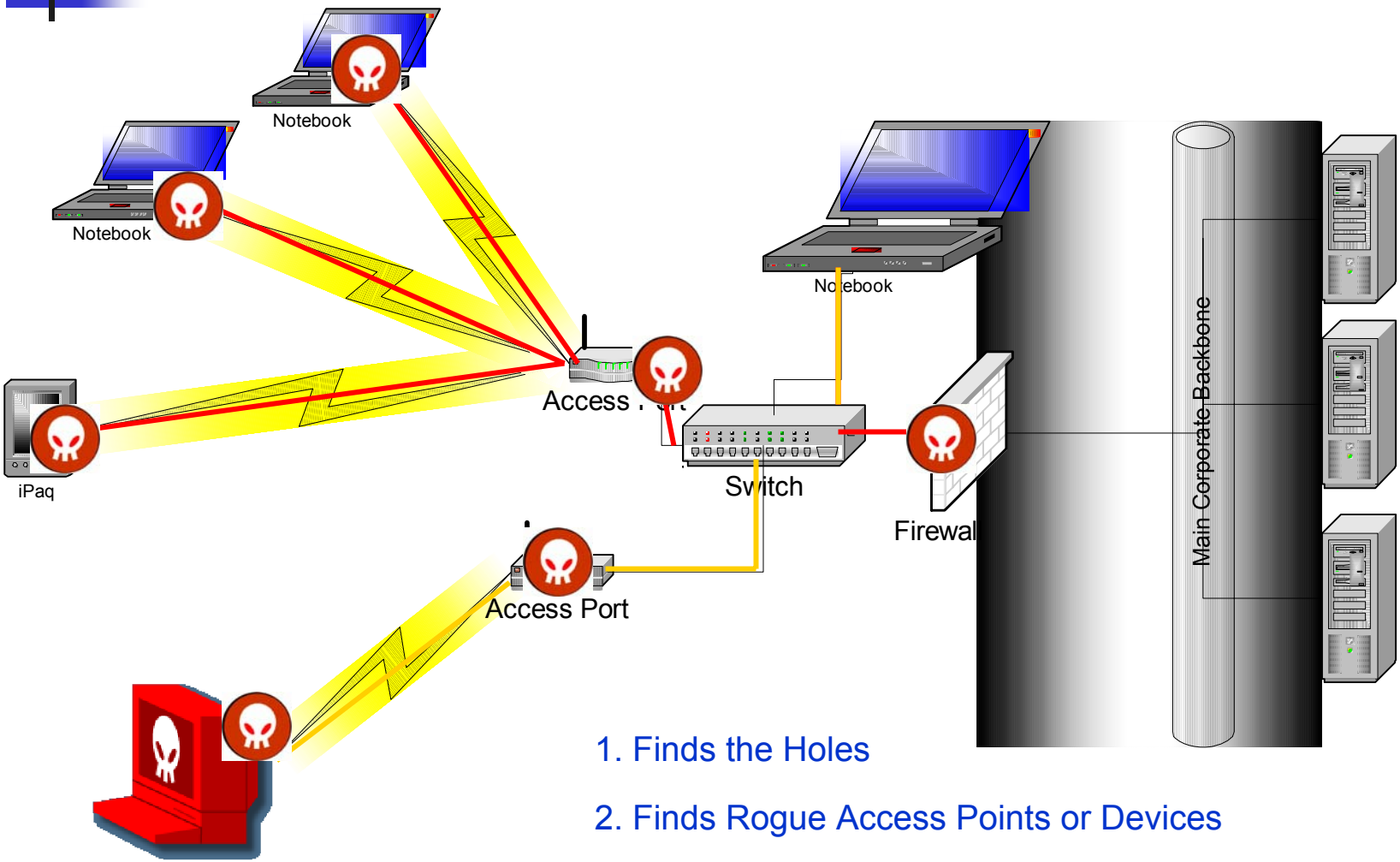
Nguyên nhân

- **Từ phía người sử dụng:** xâm nhập bất hợp pháp, ăn cắp tài sản có giá trị. Trong đó quan trọng nhất là những người dùng nội bộ
- **Kiến trúc hệ thống thông tin:** tổ chức hệ thống kỹ thuật không có cấu trúc hoặc không đủ mạnh để bảo vệ thông tin.
- **Chính sách bảo mật an toàn thông tin:** không chấp hành các chuẩn an toàn, không xác định rõ các quyền trong vận hành hệ thống.

Một số ví dụ

- Tin tặc, từ phía bọn tội phạm, dùng các kỹ thuật và các công cụ: phần mềm gián điệp, bẻ khóa, các phần mềm tấn công, khai thác thông tin, lỗ hổng bảo mật, theo dõi qua vai…
- Hãng sản xuất cài sẵn các loại 'rệp' điện tử theo ý đồ định trước
- Những chương trình ứng dụng chứa đựng những nguy hại tiềm ẩn: cửa sau, gián điệp…

Internet Scanner



1. Finds the Holes

2. Finds Rogue Access Points or Devices

Tấn công dữ liệu

I.1.3 Phân loại tấn công mạng

- **Tấn công giả mạo:** là một thực thể tấn công giả danh một thực thể khác. Tấn công giả mạo thường được kết hợp với các dạng tấn công khác như tấn công chuyển tiếp và tấn công sửa đổi thông báo.
- **Tấn công chuyển tiếp:** xảy ra khi một thông báo, hoặc một phần thông báo được gửi nhiều lần, gây ra các tác động tiêu cực.
- **Tấn công sửa đổi thông báo:** xảy ra khi nội dung của một thông báo bị sửa đổi nhưng không bị phát hiện.

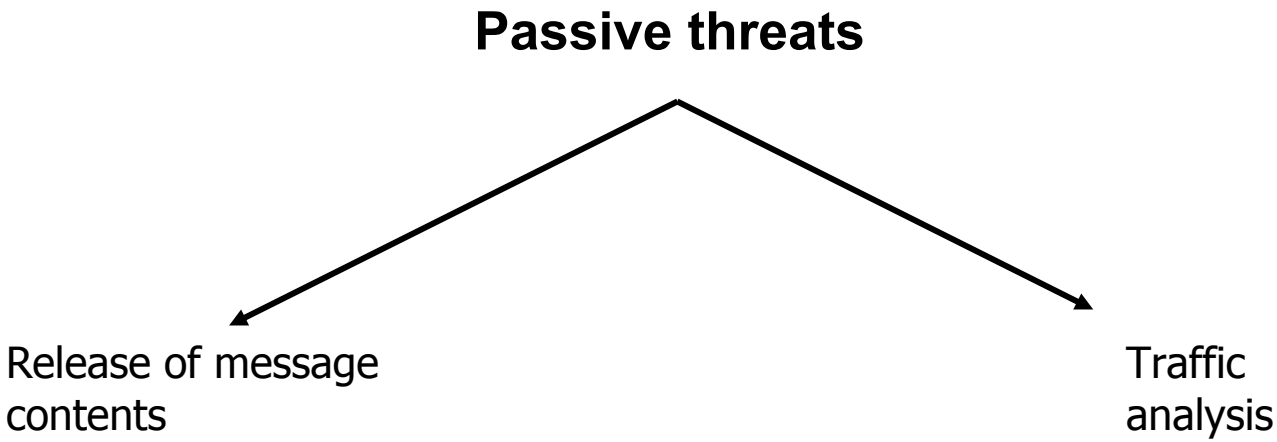
Phân loại tấn công mạng (tt)

- **Tấn công từ chối dịch vụ:** xảy ra khi một thực thể không thực hiện chức năng của mình, gây cản trở cho các thực thể khác thực hiện chức năng của chúng.
- **Tấn công từ bên trong hệ thống:** xảy ra khi người dùng hợp pháp cố tình hoặc vô ý can thiệp hệ thống trái phép.

Tấn công bị động/chủ động

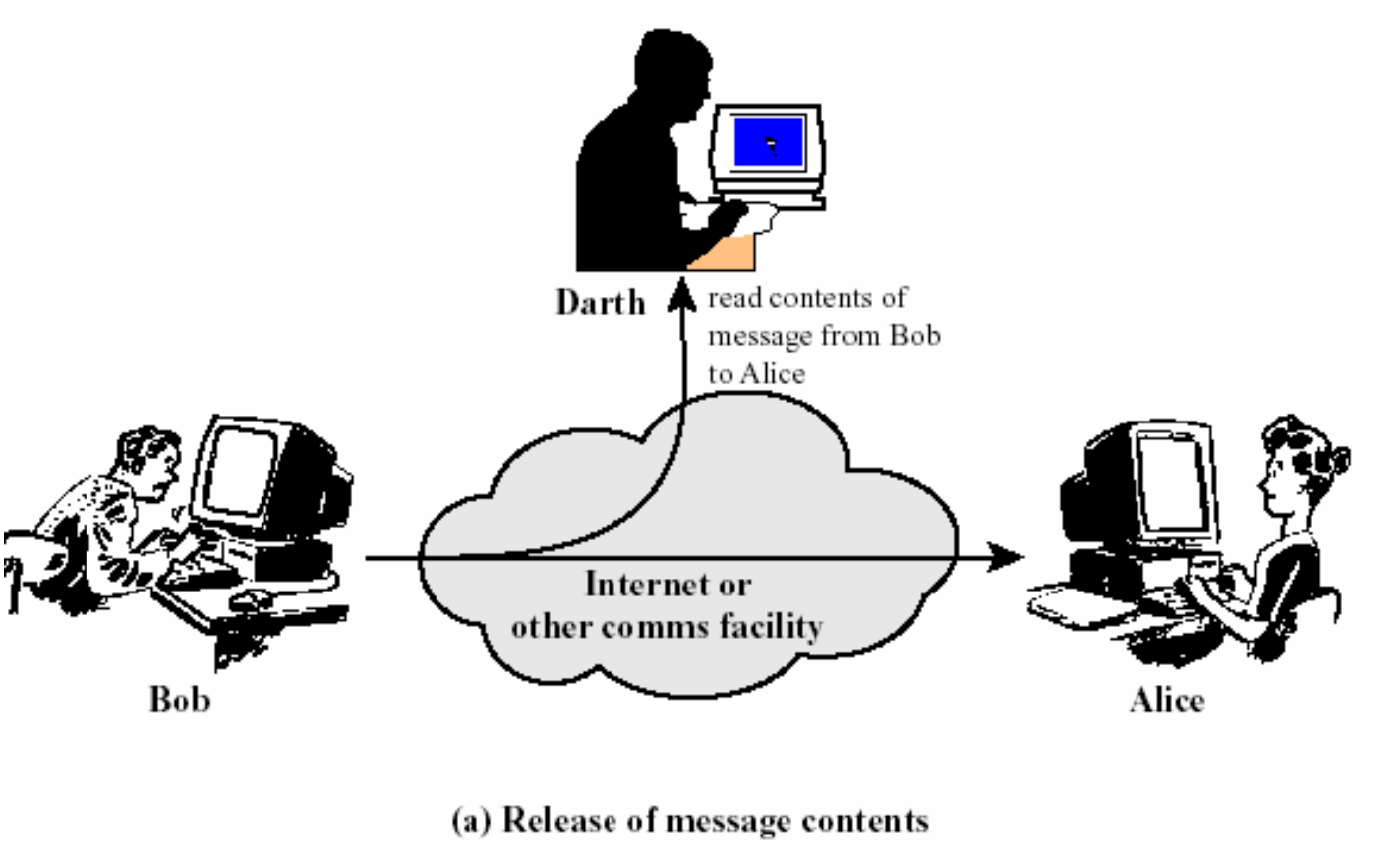
- **Tấn công bị động:** do thám, theo dõi đường truyền để:
  - **Nhận được nội dung bản tin hoặc**
  - **Theo dõi luồng truyền tin**
- **Tấn công chủ động:** thay đổi luồng dữ liệu để:
  - **Giả mạo một người nào đó.**
  - **Lặp lại bản tin trước**
  - **Thay đổi bản tin khi truyền**
  - **Từ chối dịch vụ.**

Security Attacks



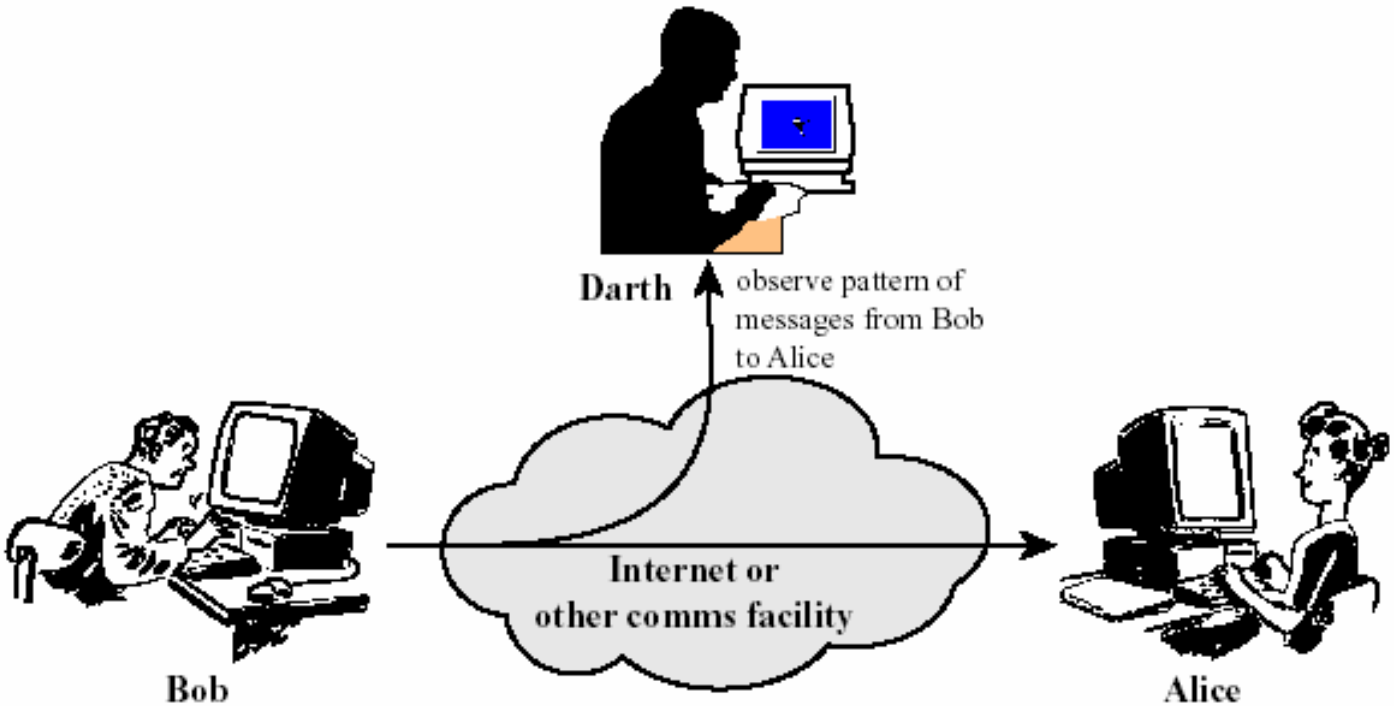
- eavesdropping (nghe lén), monitoring transmissions

Passive Attacks



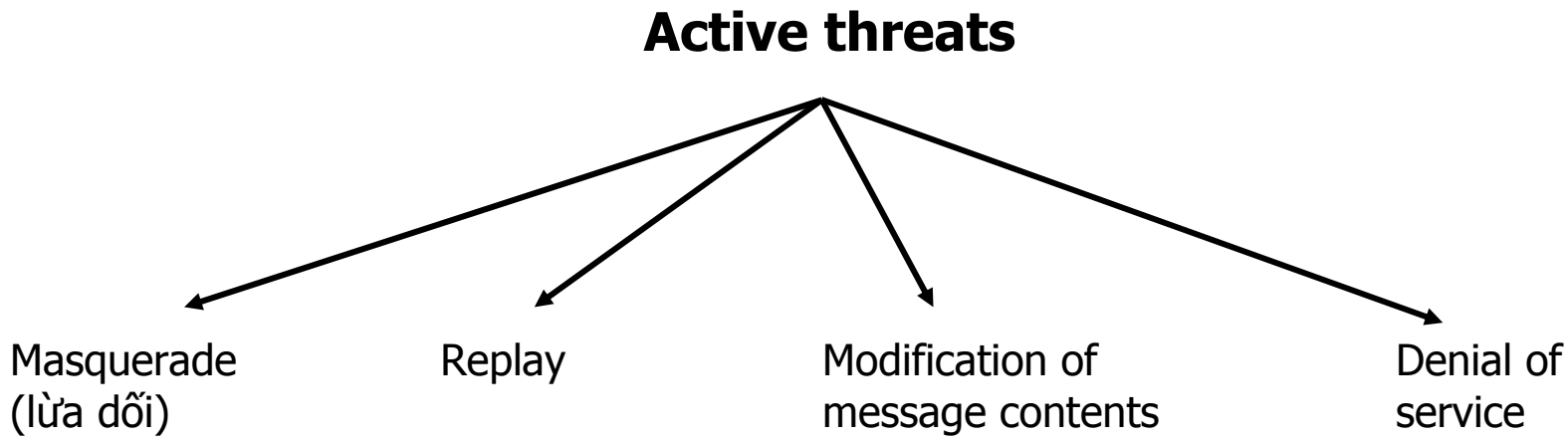
(a) Release of message contents

Passive Attacks



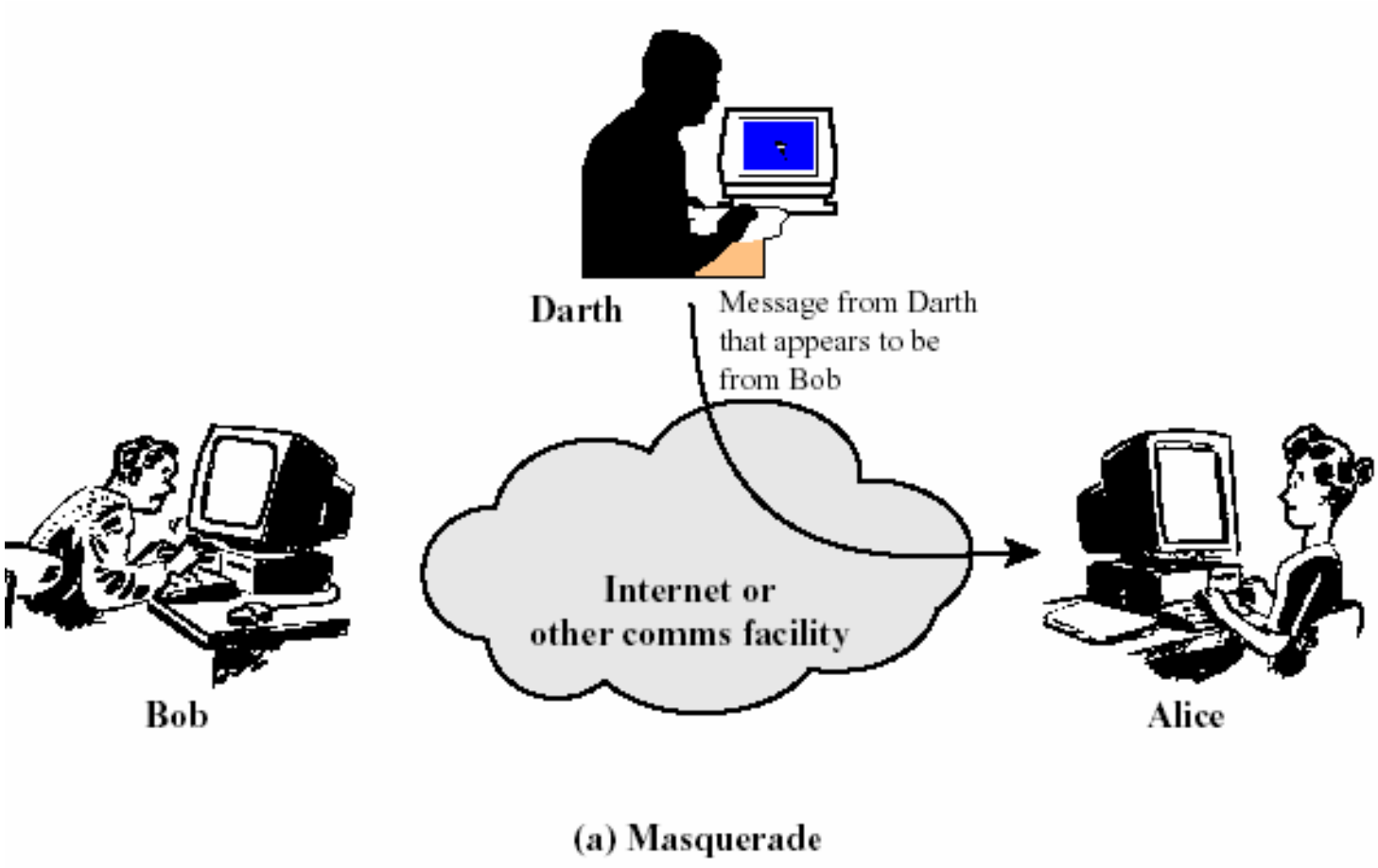
(b) Traffic analysis

Active Attacks



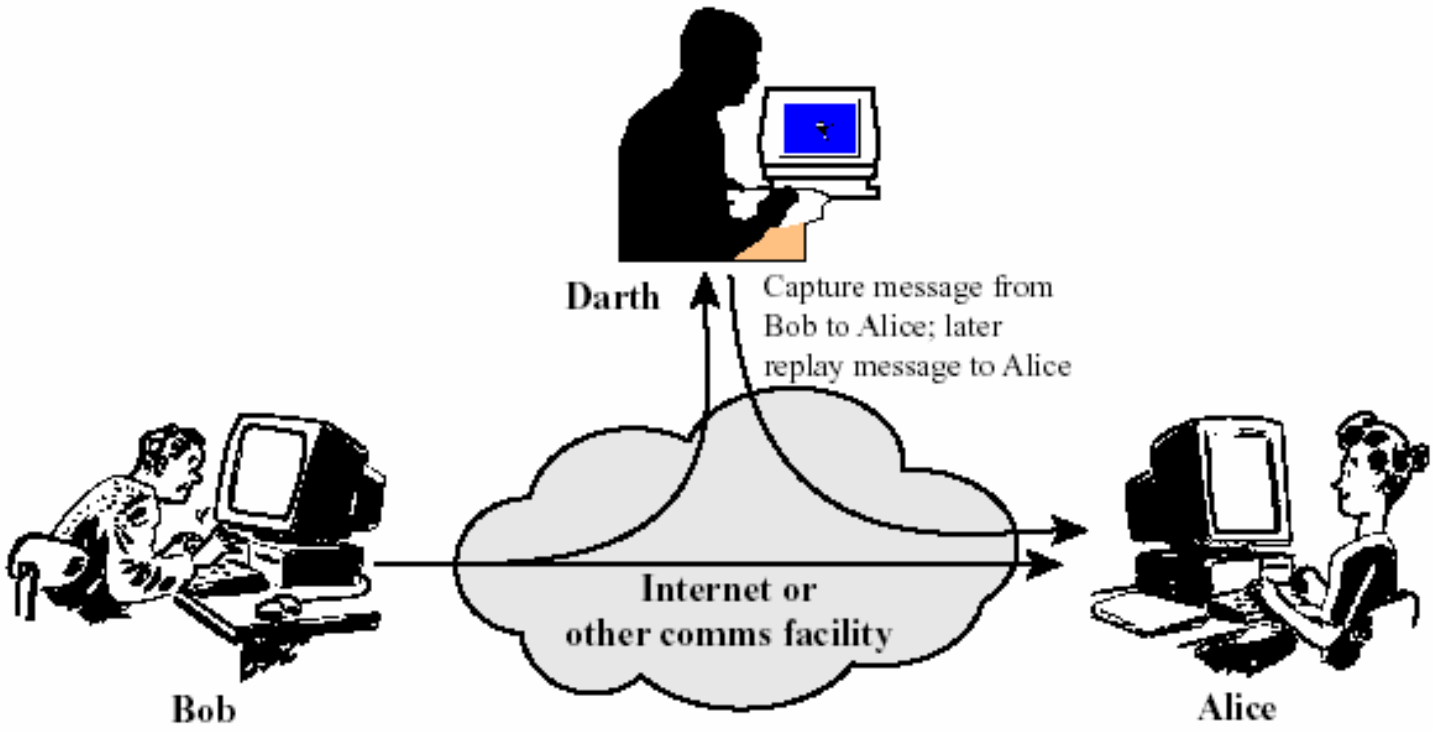
- some modification of the data stream

Active Attacks



(a) Masquerade

Active Attacks



(b) Replay

I.2 Ba khía cạnh của an toàn thông tin

- Bảo vệ tấn công
- Cơ chế an toàn
- Dịch vụ an toàn

Giải pháp an toàn

Bảo vệ tấn công

- Bảo vệ tấn công nhằm mục đích An toàn thông tin, cách thức chống lại tấn công vào hệ thống thông tin hoặc phát hiện ra chúng.
- Cần tập trung chống một số kiểu tấn công: thụ động và chủ động.

Các cơ chế an toàn

- Các cơ chế an ninh khác nhau được thiết kế để phát hiện, bảo vệ hoặc khôi phục do tấn công phá hoại.
- Không có cơ chế đơn lẻ nào đáp ứng được mọi chức năng yêu cầu của công tác an ninh. Tuy nhiên có một thành phần đặc biệt nằm trong mọi cơ chế an toàn đó là: kỹ thuật mã hoá.

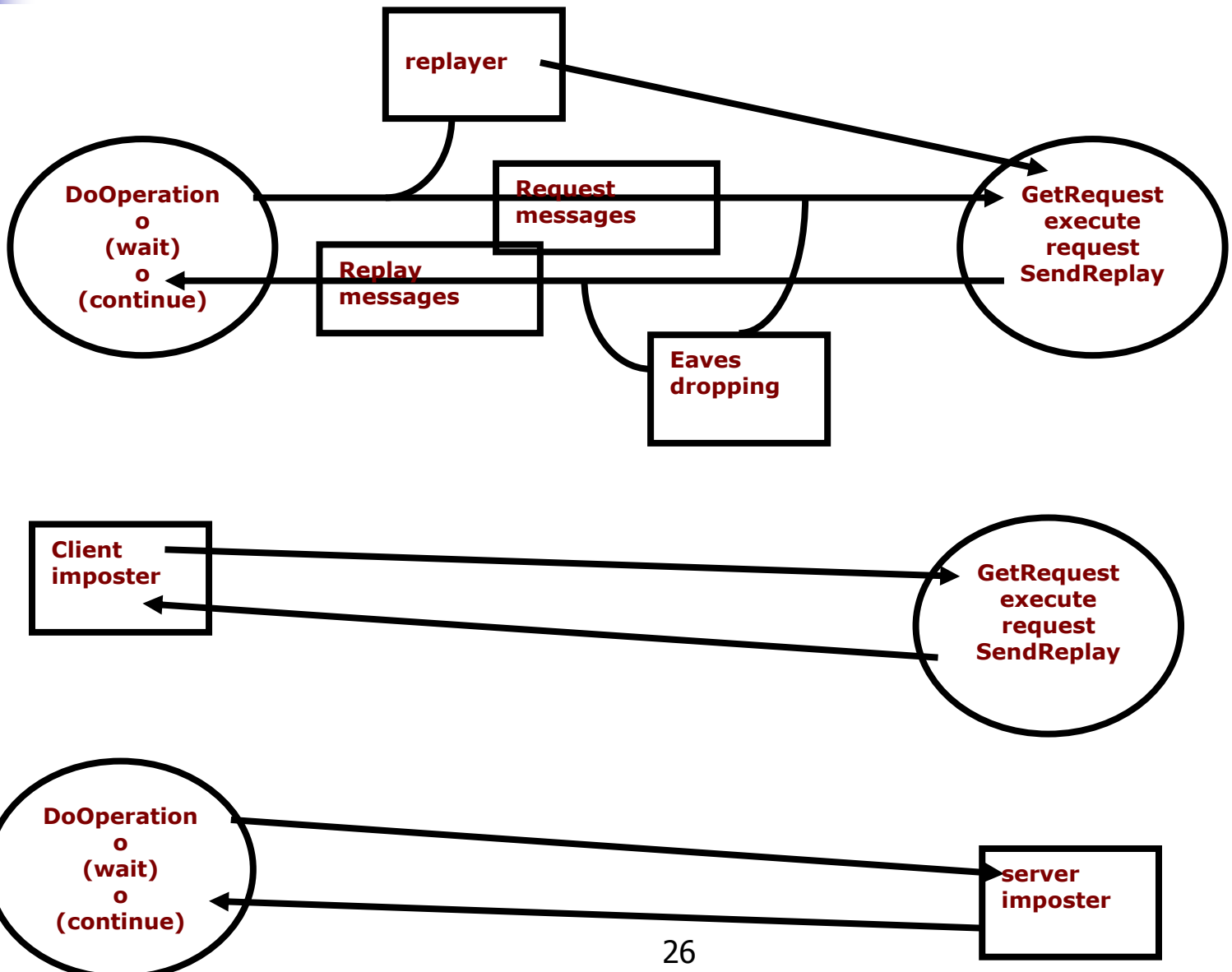
Các dịch vụ an toàn

- Có thể dùng một hay nhiều cơ chế an toàn để cung cấp dịch vụ.
- Người ta thường dùng các biện pháp tương tự như trong thế giới thực: chữ ký, công chứng, bản quyền…

Một số lưu ý về bảo mật

- Những đe dọa thường do mở rộng kênh thông tin
- Xem xét hệ thống trong mối quan hệ với môi trường
- Kỹ thuật bảo mật phải chứng tỏ được khả năng bảo vệ tốt hệ thống (logic authentication)

Mối đe doạ trong thông tin client-server



Những đòi hỏi về thông tin client-server

- Kênh thông tin phải an toàn để tránh việc chen vào mạng.
- Server phải nhận dạng được client
- Client phải nhận dạng được server
- Phải xác định được người là chủ thật sự của message và message đó không không hề có sự thay đổi (có thể nhờ vào tổ chức thứ ba)

I.3 Mô hình an toàn mạng

Kiến trúc an toàn của hệ thống truyền thông mở OSI

- Bộ phận chuẩn hóa tiêu chuẩn của tổ chức truyền thông quốc tế (International Telecommunication Union) đã đề ra Kiến trúc an ninh X800 dành cho hệ thống trao đổi thông tin mở OSI
- X800 là dịch vụ cung cấp nhằm đảm bảo an toàn thông tin thiết yếu và việc truyền dữ liệu của hệ thống
- RFC 2828 đã nêu định nghĩa cụ thể hơn: dịch vụ an toàn là dịch vụ trao đổi và xử lý, cung cấp cho hệ thống những bảo vệ đặc biệt cho các thông tin nguồn

Định nghĩa dịch vụ theo X800

- **Xác thực:** tin tưởng là thực thể trao đổi đúng là thực thể đã tuyên bố. Người đang trao đổi với mình đúng như tên của anh ta, không cho phép người khác mạo danh.
- **Quyền truy cập:** ngăn cấm việc sử dụng nguồn thông tin không không được phép. Mỗi đối tượng trong hệ thống được cung cấp các quyền nhất định và chỉ được hành động trong khuôn khổ các quyền được cấp.
- **Bảo mật dữ liệu:** bảo đảm dữ liệu không bị khám phá bởi người không có quyền.

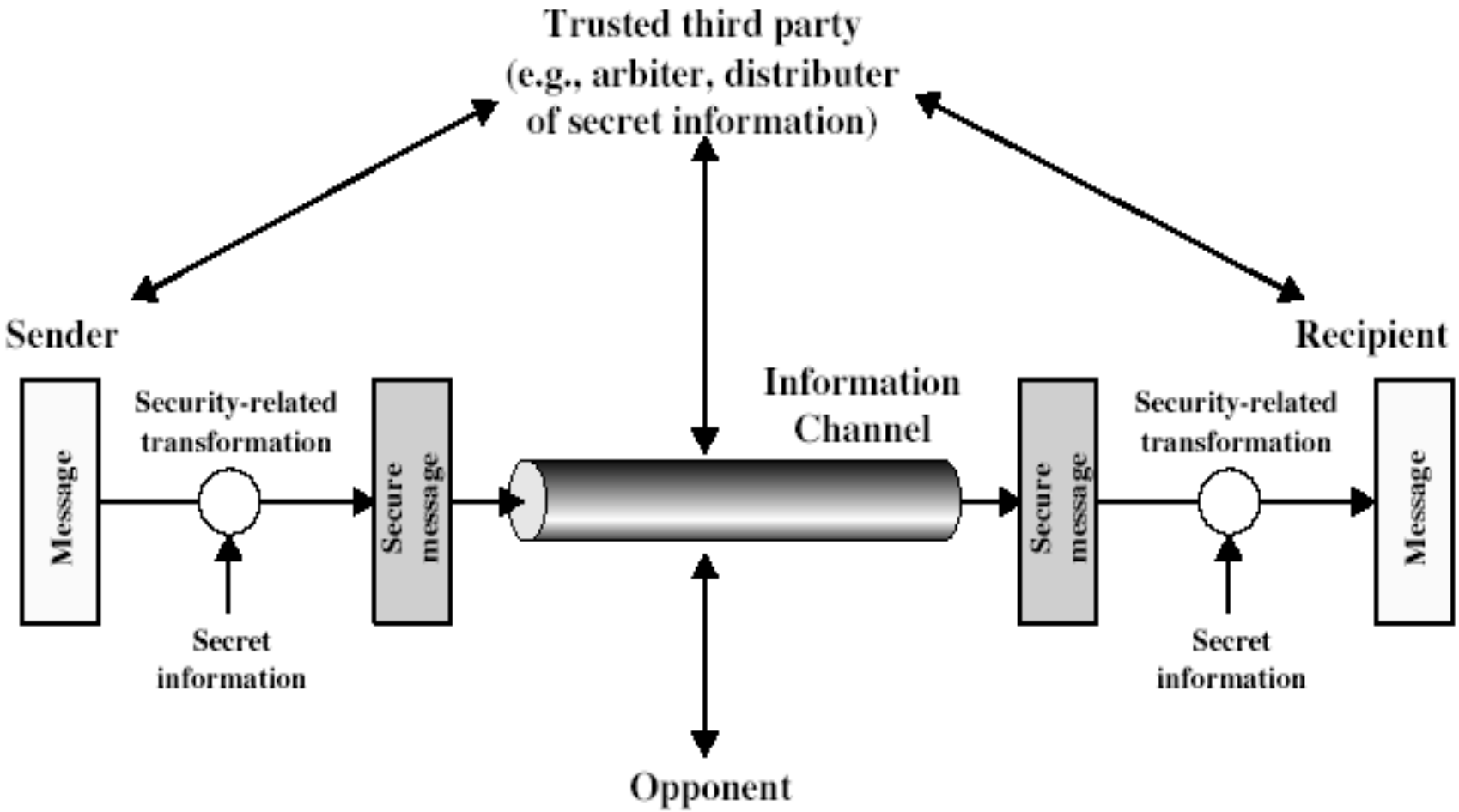
Định nghĩa dịch vụ theo X800

- **Toàn vẹn dữ liệu:** dữ liệu được gửi từ người có quyền. Nếu có thay đổi như làm trì hoãn về mặt thời gian hay sửa đổi thông tin, thì xác thực sẽ cho cách kiểm tra nhận biết là có các hiện tượng đó đã xảy ra.
- **Không từ chối:** chống lại việc phủ nhận của từng thành viên tham gia trao đổi. Người gửi không thể chối bỏ là mình đã gửi thông tin với nội dung như vậy và người nhận cũng không thể nói dối là tôi chưa nhận được thông tin đó.

Cơ chế an toàn theo X800

- **Cơ chế an toàn chuyên dụng** được cài đặt trong một giao thức của một tầng chuyển vận: mã hoá, chữ ký điện tử, quyền truy cập, toàn vẹn dữ liệu, trao đổi có phép, đệm truyền, kiểm soát định hướng, công chứng.
- **Cơ chế an toàn thông dụng** không chỉ rõ việc sử dụng cho giao thức trên tầng nào hoặc dịch vụ an ninh cụ thể nào: chức năng tin cậy, nhãn an toàn, phát hiện sự kiện, lần vết vết an toàn, khôi phục an toàn.

Mô hình truy cập mạng an toàn

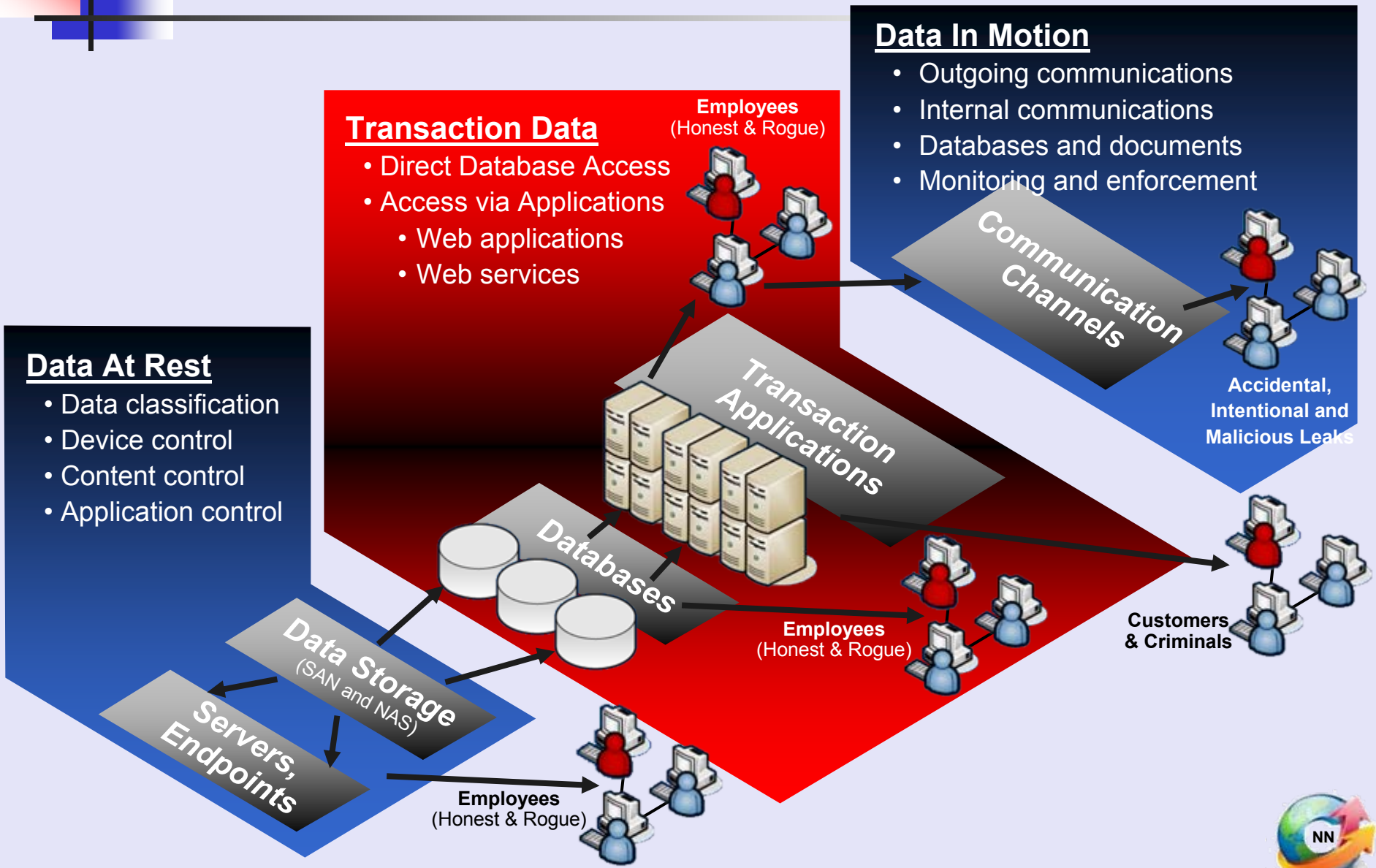


I.4 Bảo mật thông tin trong hệ cơ sở dữ liệu

- Các hệ cơ sở dữ liệu (CSDL) ngày nay như Oracle, SQL Server, DB2 đều có sẵn các công cụ bảo vệ tiêu chuẩn như hệ thống định danh và kiểm soát truy xuất. Tuy nhiên, các biện pháp bảo vệ này hầu như không có tác dụng trước các tấn công từ bên trong.

Data Security and Compliance

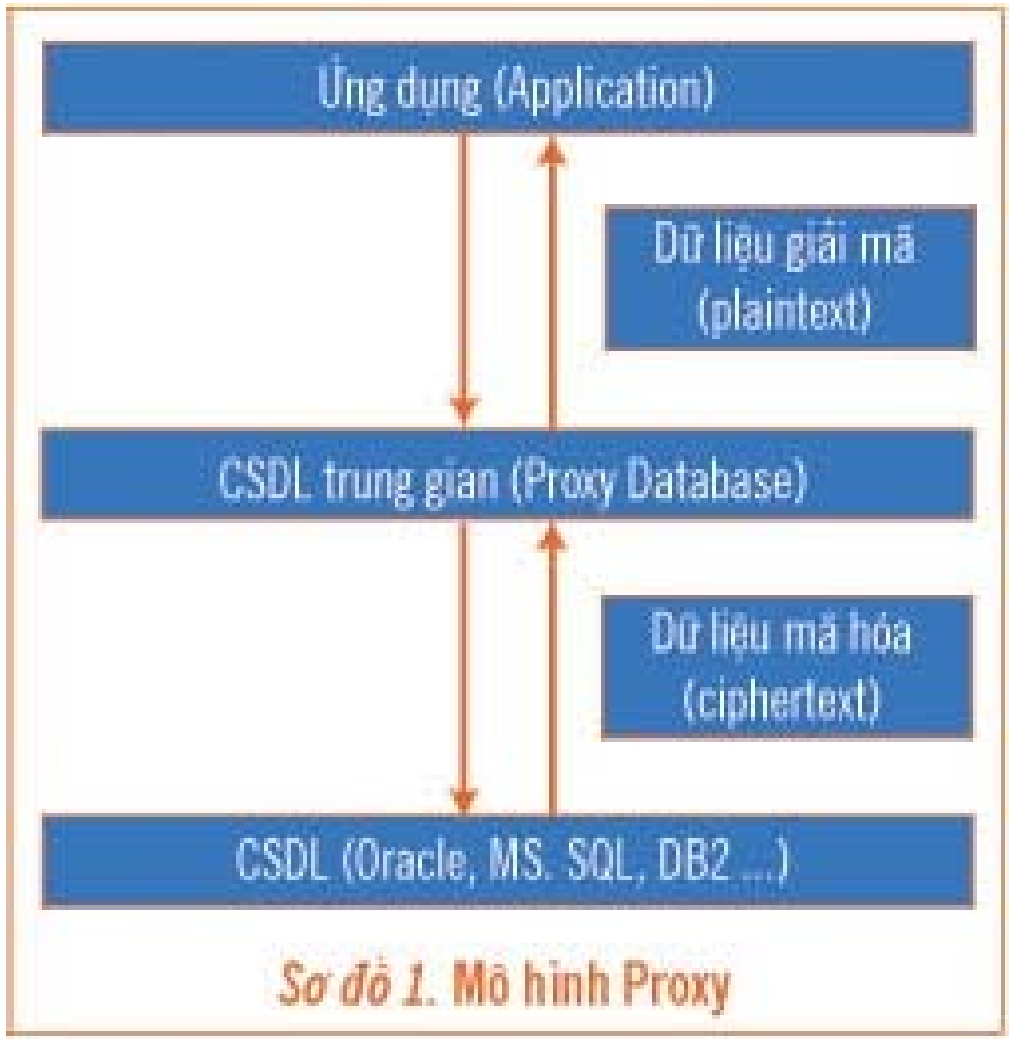
The Landscape



Bảo mật dựa vào tầng CSDL trung gian

- Một CSDL trung gian được xây dựng giữa ứng dụng và CSDL gốc. CSDL trung gian này có vai trò mã hóa dữ liệu trước khi cập nhật vào CSDL gốc, đồng thời giải mã dữ liệu trước khi cung cấp cho ứng dụng. CSDL trung gian đồng thời cung cấp thêm các chức năng quản lý khóa, xác thực người dùng và cấp phép truy cập.
- Giải pháp này cho phép tạo thêm nhiều chức năng về bảo mật cho CSDL. Tuy nhiên, mô hình CSDL trung gian đòi hỏi xây dựng một ứng dụng CSDL tái tạo tất cả các chức năng của CSDL gốc.

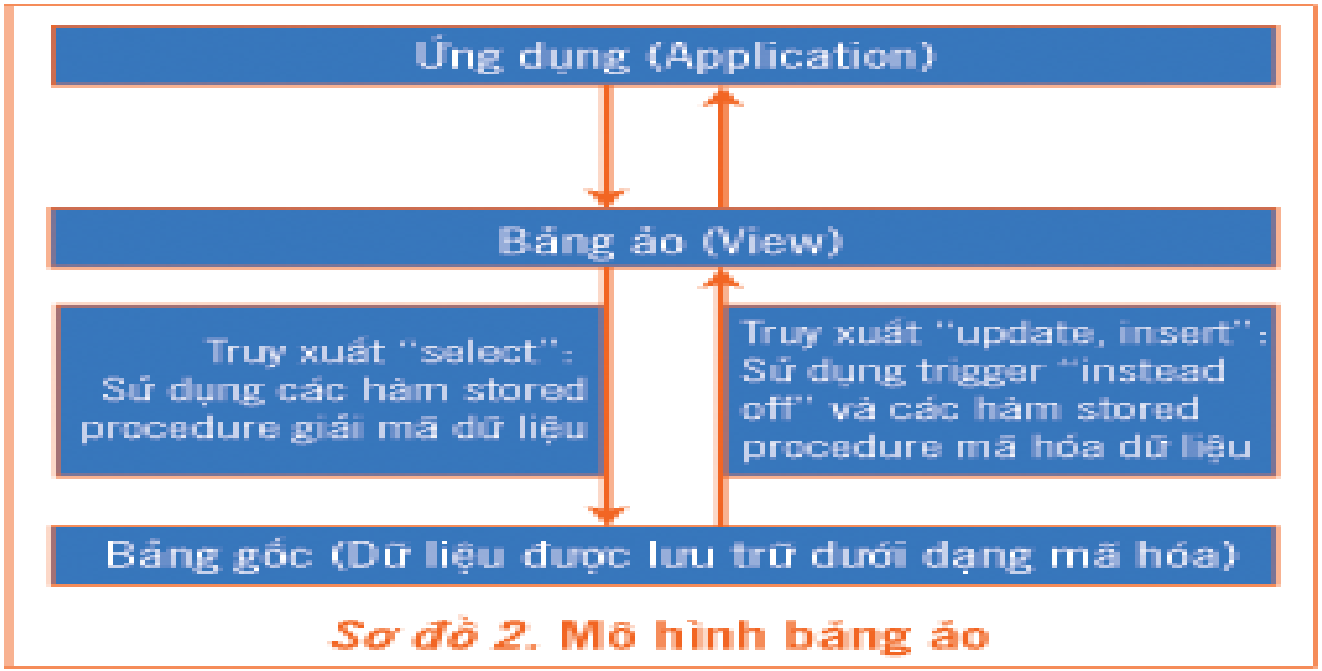
Bảo mật dựa vào tầng CSDL trung gian



Sơ đồ 1. Mô hình Proxy

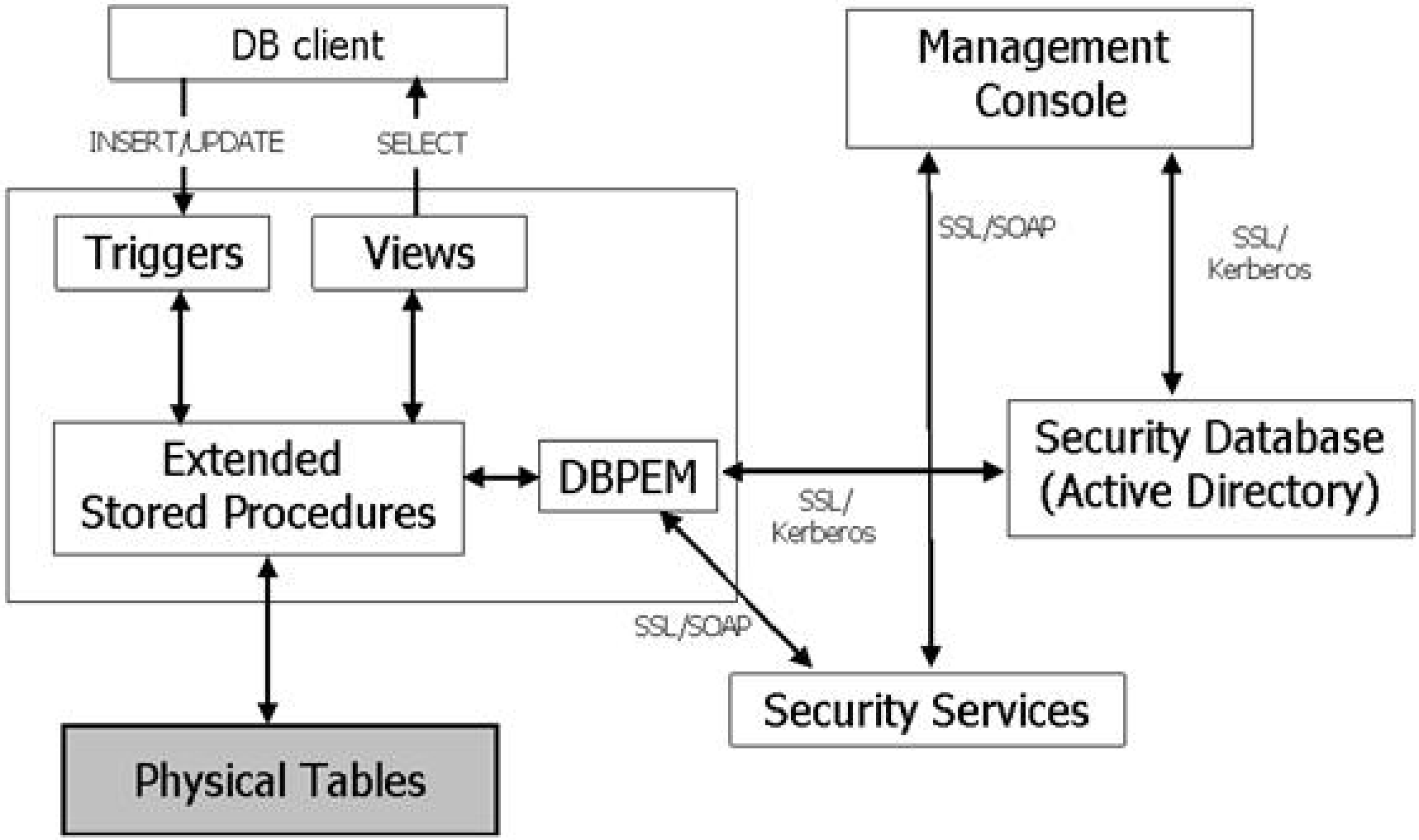
Mô hình bảng ảo

- **Ngoài các quyền cơ bản do CSDL cung cấp, hai quyền truy cập:**
  - **Người sử dụng chỉ được quyền đọc dữ liệu ở dạng mã hóa. Quyền này phù hợp với những đối tượng cần quản lý CSDL mà không cần đọc nội dung dữ liệu.**
  - **Người sử dụng được quyền đọc dữ liệu ở dạng giải mã.**



Sơ đồ 2. Mô hình bảng ảo

Kiến trúc một hệ bảo mật CSDL



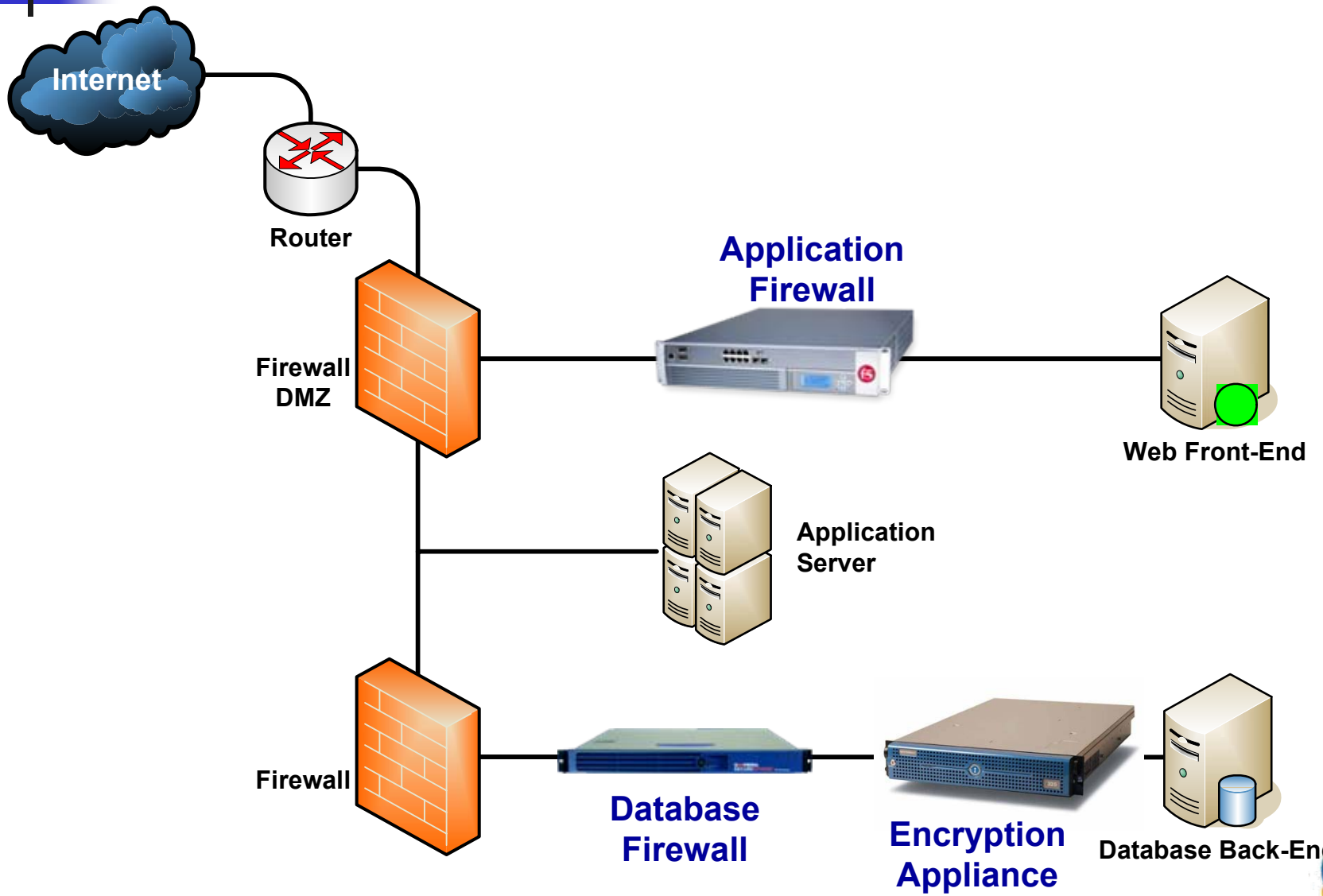
Hệ bảo mật CSDL

- **Trigger:** được sử dụng để lấy dữ liệu đến từ các câu lệnh INSERT, UPDATE (để mã hóa).
- **View:** các view được sử dụng để lấy dữ liệu đến từ các câu lệnh SELECT (để giải mã).
- **Extended Stored Procedures:** được gọi từ các Trigger hoặc View dùng để kích hoạt các dịch vụ được cung cấp bởi Modulo DBPEM từ trong môi trường của hệ quản tri CSDL.
- **DBPEM (Database Policy Enforcing Modulo):** cung cấp các dịch vụ mã hóa/giải mã dữ liệu gửi đến từ các Extended Stored Procedures và thực hiện việc kiểm tra quyền truy xuất của người dùng (dựa trên các chính sách bảo mật được lưu trữ trong CSDL về quyền bảo mật).

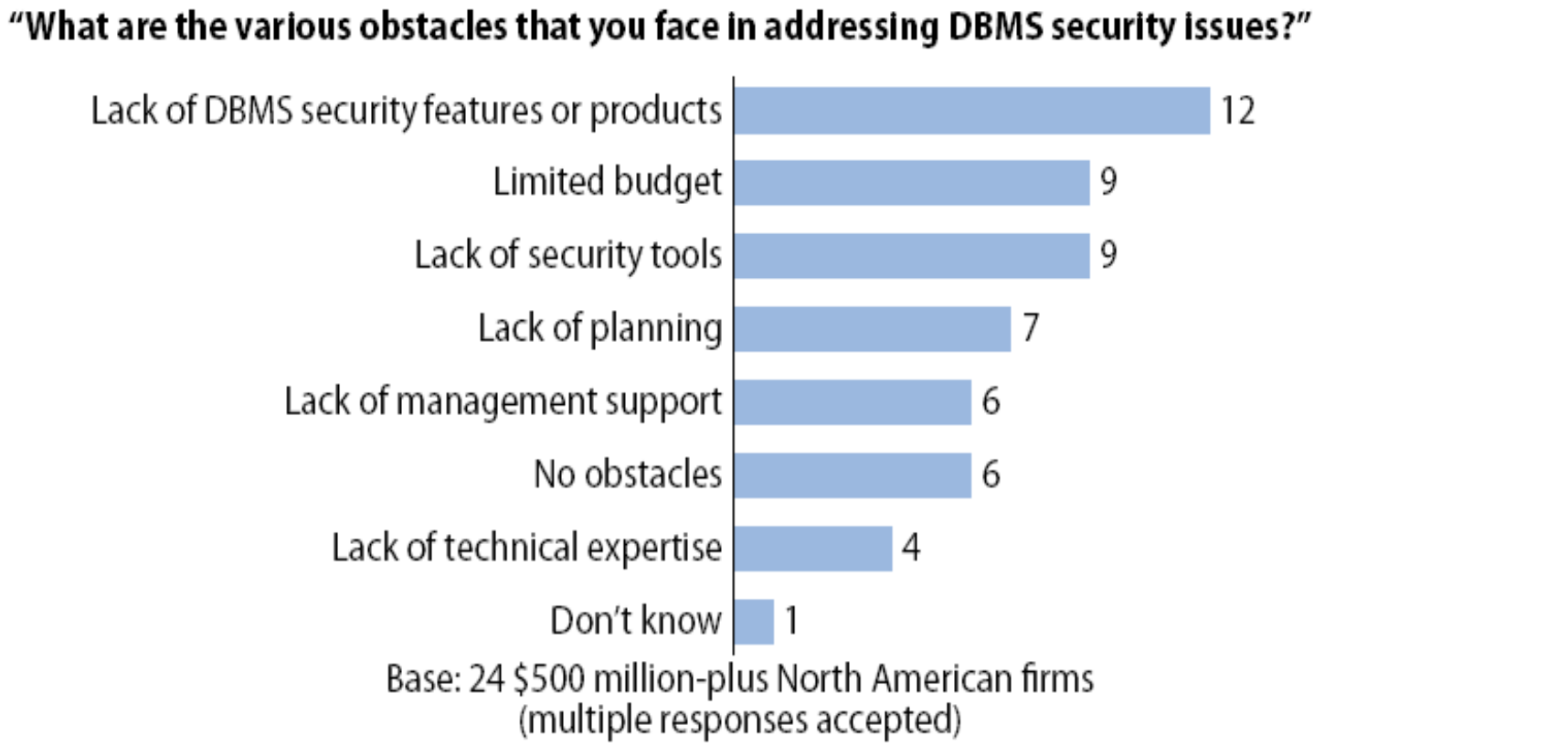
Hệ bảo mật CSDL

- **Security Database:** lưu trữ các chính sách bảo mật và các khóa giải mã. Xu hướng ngày nay thường là lưu trữ CSDL về bảo mật này trong Active Directory (một CSDL dạng thư mục để lưu trữ tất cả thông tin về hệ thống mạng).
- **Security Services:** chủ yếu thực hiện việc bảo vệ các khóa giải mã được lưu trong CSDL bảo mật.
- **Management Console:** dùng để cập nhật thông tin lưu trong CSDL bảo mật (chủ yếu là soạn thảo các chính sách bảo mật) và thực hiện thao tác bảo vệ một trường nào đó trong CSDL để đảm bảo tối đa tính bảo mật, thông tin được trao đổi.

Ecommerce Architecture



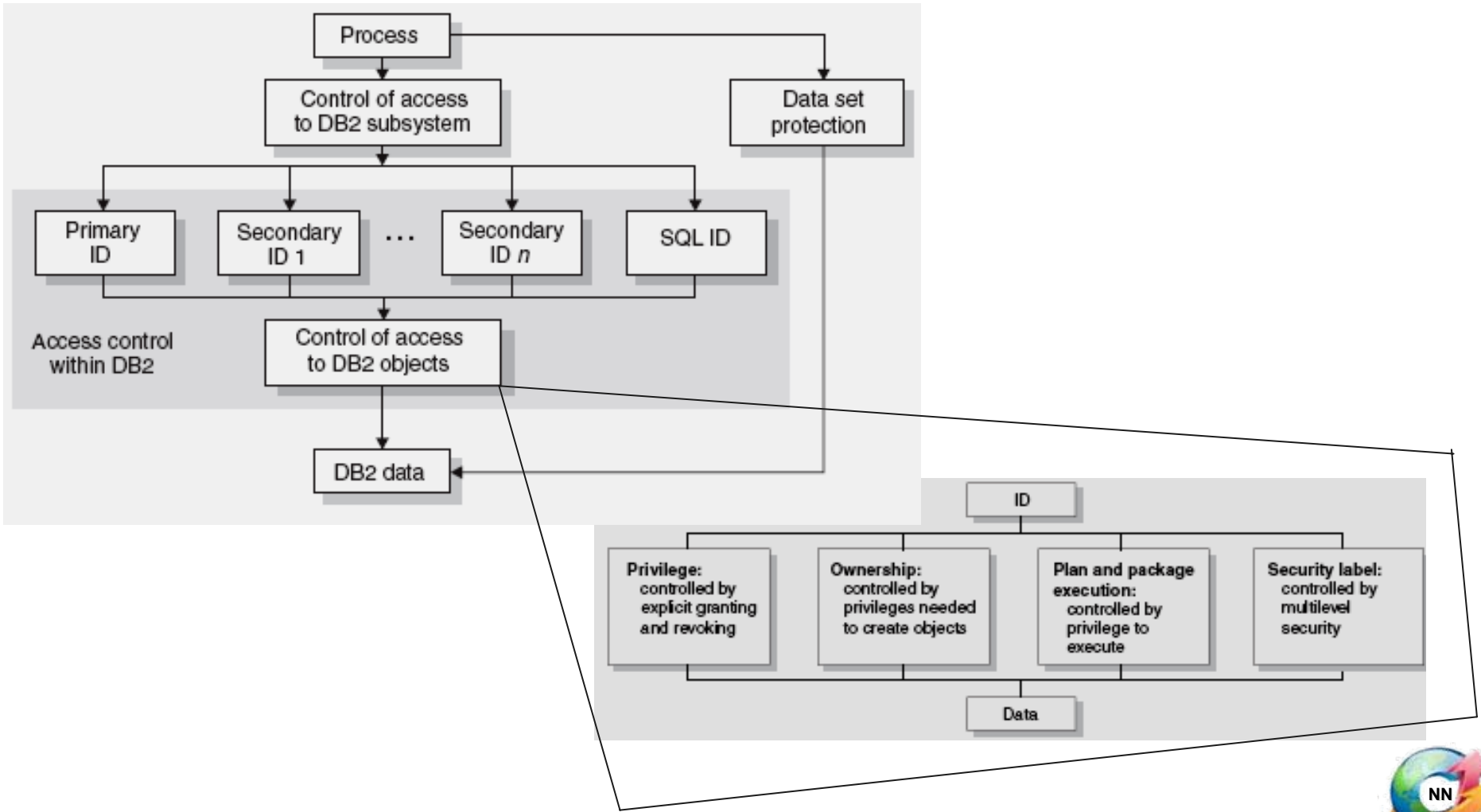
Những trở ngại cho Database Security



An toàn CSDL

- Authentication
  - **Who is it?**
- Authorization (sự cấp qu
  - **Who can do it?**
- Encryption
  - **Who can see it?**
- Audit (kiểm tra, kiểm toán)
  - **Who did it?**

DB2


Process
Control of access to DB2 subsystem
Data set protection
Primary ID
Secondary ID 1
...
Secondary ID n
SQL ID
Access control within DB2
Control of access to DB2 objects
DB2 data
ID
Privilege: controlled by explicit granting and revoking
Ownership: controlled by privileges needed to create objects
Plan and package execution: controlled by privilege to execute
Security label: controlled by multilevel security
Data

Kiểm tra sau khi tấn công

- You have discovered you have been attacked
  - **Now what???**
- Need to collect as much data about attack as possible
  - **When did it occur**
  - **How did it occur**
  - **Where did it come from**
- Databases write auditing data in numerous locations
  - **Collect all those locations into a single repository**
  - **Correlate events to get a better picture of what happened**

I.5 hệ thống tin cậy

Kiểm soát truy cập

- Hệ thống đã xác định được định danh như người sử dụng, xác định các nguồn gốc nào nó có thể truy cập. Mô hình tổng quát là ma trận truy cập với
  - **Chủ thể - thực thể chủ động (người sử dụng, quá trình)**
  - **Đối tượng - thực thể bị động (file hoặc nguồn)**
  - **Quyền truy cập – cách mà đối tượng được truy cập**
- Có thể được phân tách bởi
  - **Các cột như danh sách kiểm soát truy cập**
  - **Các hàng như các thẻ về khả năng**

Cấu trúc điều khiển truy cập

	Program1	...	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
. . .				

(a) Access matrix

Access control list for Program1: Process1 (Read, Execute)
Access control list for SegmentA: Process1 (Read, Write)
Access control list for SegmentB: Process2 (Read)

(b) Access control list

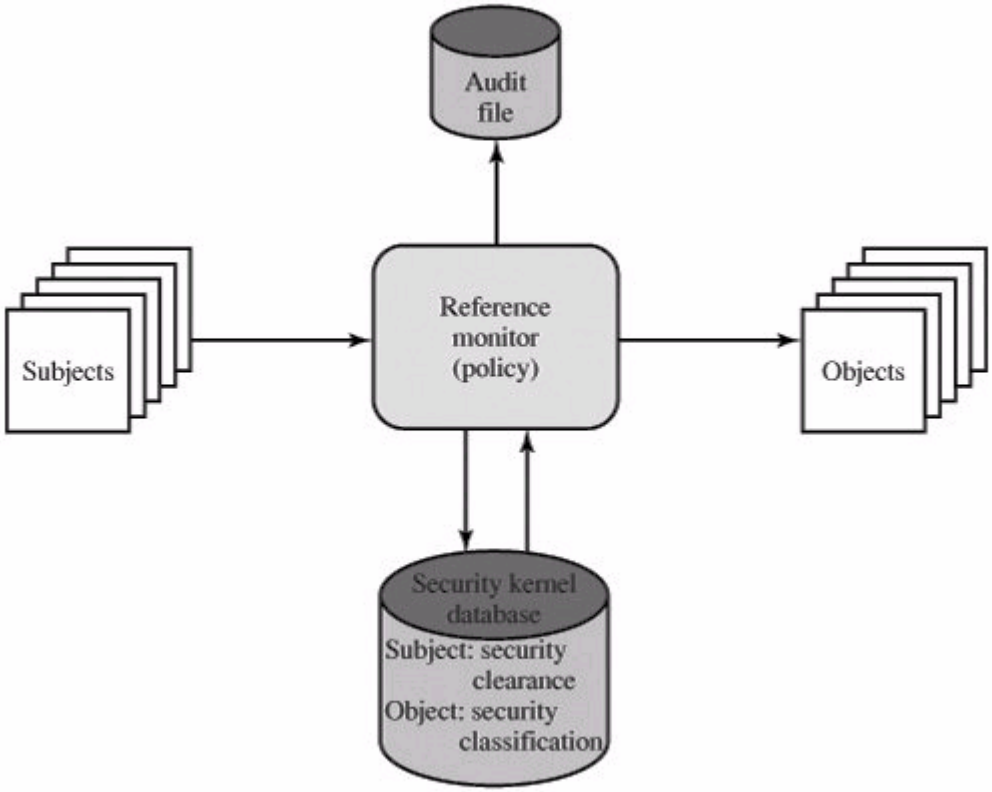
Capability list for Process1: Program1 (Read, Execute) SegmentA (Read, Write)
Capability list for Process2: Segment B (Read)

(c) Capability list

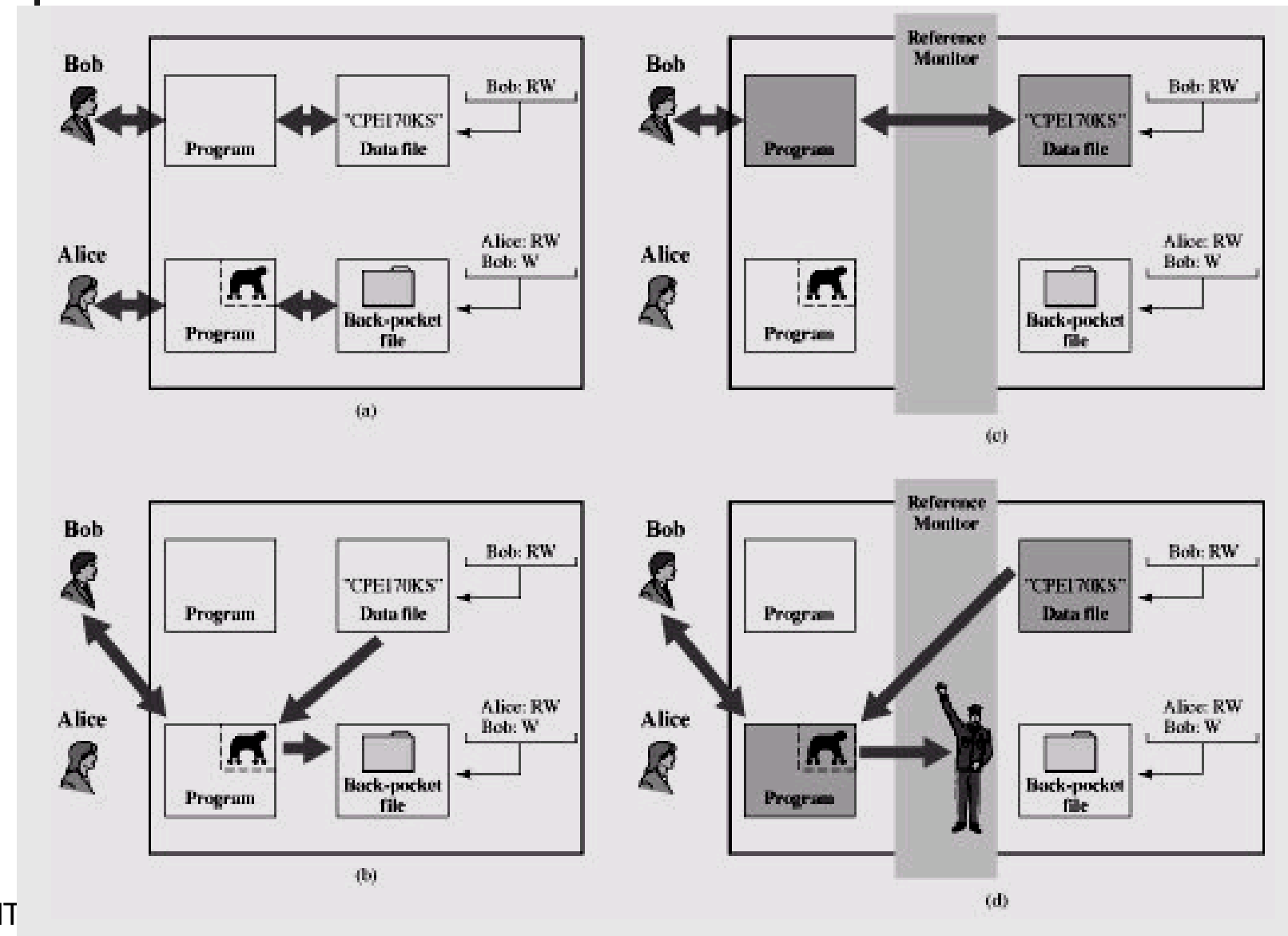
Các hệ thống tin cậy

- Phân loại: unclassified (U), confidential (C), secret (S), top secret (TS)…
- Hệ thống an toàn đa mức
  - No read up: chỉ có thể đọc những đối tượng ít hay bằng với quyền được truy cập
  - No write down: chỉ có thể viết những đối tượng nhiều hay bằng với quyền được truy cập
- Thuộc tính reference monitor (policy):
  - Phối hợp đầy đủ (Complete mediation)
  - Cô lập (Isolation)
  - Có thể kiểm tra (Verifiability)
- Hệ thống an toàn phải thỏa các tính chất trên

Reference Monitor



Phòng chống Trojan



I.6 Phần mềm có hại

- I.6.1 Virus và các chương trình xâm hại
- I.6.2 Antivirus
- I.6.3 Tấn công từ chối dịch vụ

I.6.1 Virus và các chương trình xâm hại

Thuật ngữ

Name	Description
Virus	Attaches itself to a program and propagates copies of itself to other programs
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	Program modification that allows unauthorized access to functionality
Exploits	Code specific to a single vulnerability or set of vulnerabilities
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely
Kit (virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e-mail
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (DoS) attack
Keyloggers	Captures keystrokes on a compromised system
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access
Zombie	Program activated on an infected machine that is activated to launch attacks on other machines

Virus

- 4 giai đoạn
  - **Nằm im - chờ sự kiện kích hoạt**
  - **Lan truyền – lặp sinh ra chương trình/đĩa**
  - **Kích hoạt - bởi sự kiện để thực hiện bộ tải**
  - **Thực hiện bộ tải**
- Cấu trúc

```
        program V :=

{goto main;
        1234567;

        subroutine infect-executable :=
                {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567)
                   then goto loop
                   else prepend V to file; }

        subroutine do-damage :=
                {whatever damage is to be done}

        subroutine trigger-pulled :=
                {return true if some condition holds}

main:   main-program :=
                {infect-executable;
                if trigger-pulled then do-damage;
                goto next;}
next:

}
```

Virus nén

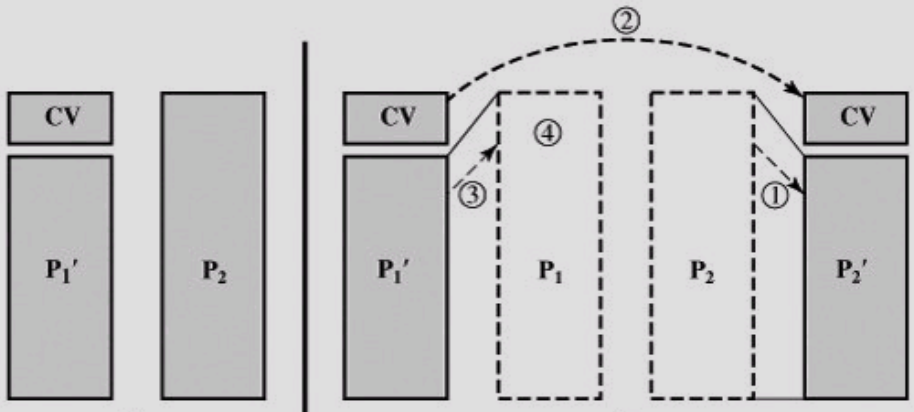
```
     program CV :=

{goto main;
     01234567;

     subroutine infect-executable :=
               {loop:
                    file := get-random-executable-file;
               if (first-line-of-file = 01234567) then goto loop;
          (1)  compress file;
          (2)  prepend CV to file;
          }

main:  main-program :=
               {if ask-permission then infect-executable;
          (3)  uncompress rest-of-file;
          (4)  run uncompressed file;}
          }
```

Figure 19.3. A Compression Virus



Các kiểu Virus

- Có thể phân loại dựa trên kiểu tấn công
  - **Virus cư trú ở bộ nhớ**
  - **Virus ở sector khởi động**
  - **Virus Lén lút: ẩn mình trước các chương trình AV**
  - **Virus nhiều hình thái (Polymorphic, không dùng signature được): thay đổi cách nhiễm**
  - **Virus biến hoá (Metamorphic): Viết lại chính nó, gia tăng việc khó nhận diện, thay đổi hành vi và sự xuất hiện**

Tìm hiểu thêm về virus

- **polymorphic virus**:
  - **Nhân đôi nhưng có những mẩu bit khác nhau.**
  - **Hoán vị các lệnh thừa hay các lệnh độc lập**
  - **Tạo ra phần mã hóa cho phần còn lại, khóa mã hóa sẽ thay đổi ngẫu nhiên khi nghiễm vào chương trình khác**
- **virus-creation toolkit**

Marco Virus

- Giữa thập niên 90
- Nhiễm MS WORD/Excel và những phần mềm hỗ trợ
- Macro nhiễm vào tài liệu
- Macro virus thường phát tán dựa vào email

Virus email

- Đây là loại virus lan truyền khi mở file đính kèm chứa marco virus (Melissa).
  - **Virus gởi chính nó tới những người dùng trong mail list**
  - **Thực hiện phá hoại cục bộ**
- Cuối 1999 những virus này có thể hoạt động khi người dùng chỉ cần mở email

Các chương trình xâm hại

- Có 2 loại
  - **Dựa vào các chương trình khác: Virus, logic bomb và backdoor**
  - **Chương trình độc lập: Worm and zombie**
- Tiến trình
  - **Hoạt động dựa vào trigger**
  - **Tạo bản copy**

Cửa sau (Backdoor)

- Điểm vào chương trình bí mật, cho phép những người biết truy cập mà không cần các thủ tục thông thường.
- Những người phát triển thường dùng để phát triển và kiểm tra chương trình
- Backdoor xuất phát từ ý tưởng của những người phát triển game
- Rất khó ngăn chặn trong hệ điều hành, đòi hỏi sự phát triển và cập nhật phần mềm tốt.

Bom logic

- Đây là một trong những phần mềm có hại kiểu cổ, code được nhúng trong chương trình hợp pháp. Nó được kích hoạt khi gặp điều kiện xác định
  - Có mặt hoặc vắng mặt một số file
  - Ngày tháng/thời gian cụ thể
  - Người sử dụng nào đó
- Khi được kích hoạt thông thường nó làm hỏng hệ thống
  - Biến đổi/xoá file/đĩa, làm dừng máy,...

Ngựa thành Tơ roa (Trojan horse)

- Là chương trình có thể hoàn thành những hoạt động gián tiếp mà những người không có quyền không thể thực hiện trực tiếp
- Có thể giả dạng các chương trình tiện ích, các chương trình ứng dụng, nó có thể thay đổi hoặc phá hủy dữ liệu
- Có thể một trình biên dịch insert thêm mã vào ứng dụng login để cho phép người viết có thể login vào hệ thống với 1 PWD đặc biệt

Zombie

- Đây là chương trình bí mật điều khiển máy tính khác trên mạng
- Sử dụng các máy tính bị nhiễm mà không bị nghi ngờ để tiến hành các tấn công.
- Rất khó để nhận ra người tạo ra Zombie
- Thông thường sử dụng để khởi động tấn công từ chối các dịch vụ phân tán (Ddos). Nó có thể sử dụng hàng trăm máy tính bị nhiễm để làm tràn ngập việc di chuyển thông tin trên Internet (traffic)

Sâu (Worm)

- Tương tự như virus email nhưng nó tự động lan truyền
- Khi trong hệ thống nó hoạt động như virus
- Nó có thể lan truyền bằng
  - **Email**
  - **Thực thi từ xa**
  - **Login từ xa**
- Nó có các giai đoạn như virus, trong giai đoạn lan truyền có thực hiện
  - **Tìm để nhiễm các hệ thống khác dựa vào host table hay remote system address**
  - **Thiết lập connect**
  - **Copy tới hệ thống từ xa và kích hoạt bản copy**

Sâu Morrris

- Sâu Morris là sâu được tạo bởi Robert Morris vào 1988, nhằm tới các hệ thống Unix. Đối với mỗi host được khám phá nó thực hiện
  - Crack file PWD
  - Phát hiện PWD và ID bằng chương trình crack mà cố thử
    - Tên người dùng và hòan vị đơn giản
    - Danh sách pwd có sẵn (432)
    - Tất cả những từ trong thư muc hệ thống cục bộ
  - Khám phá lỗi của giao thức mà cho biết nơi của người dùng từ xa
  - Khám phá cửa sau trong chọn lựa debug của quá trình remote mà nhận và gởi mail

Sâu Morrris

- Nếu một trong những cách trên thành công
  - **Nó đạt được việc truyền thông với bộ phiên dịch lện hệ điều hành**
  - **Gởi một chương trình tự phát triển ngắn (boostrap)**
  - **Thực thi chương trình**
  - **Log off**
  - **Chương trình boostrap gọi chương trình cha và download phần còn lại của worm**

Tấn công của sâu đương thời

Code Red

- 7-2001
- Dựa vào lỗ hỗng trong Microsoft Internet Information Server (IIS)
- Disable system file checker
- Thăm dò random IP address để vươn tới những host khác
- Tấn công denial-of-service
- Nó tạm hoãn và hoạt động theo một khoảng thời gian
- Trong làn sóng tấn công thứ 2, nó nhiễm 360.000 server trong 14 giờ

Code Red II

- Biến thể tấn công IIS, cài đặt Backdoor

Nimda

- Cuối 2001
- Kỹ thuật
  - **client to client qua e-mail**
  - **client to client qua network share**
  - **Web server to client qua duyệt Web**
  - **client to Web server qua duyệt thư mục Microsoft IIS 4.0 / 5.0**
  - **client to Web server qua backdoor**
- Thay đổi file Web và những file thực thi

SQL Slammer

Sâu SQL Slammer

- Đầu năm 2003
- Lỗi tràn bộ đệm của Microsoft SQL server

Sâu Sobig.f

- Khai thác open proxy server tạo động cơ spam từ những máy tính nhiễm

Mydoom

- 2004
- Cài đặt backdoor, tạo ra một lượng email khổng lồ

Kỹ thuật tạo sâu

- Chạy trên nhiều platform
- Khai thác nhiều phương tiện: Web servers, browsers, e-mail, file sharing, và những ứng dụng mạng
- Phân bổ cực nhanh
- Đa hình (Polymorphic)
- Biến hóa (Metamorphic)
- Transport vehicles
- Khia thác Zero-day

I.6.2 Antivirus

- Các bước
  - **Phát hiện virus nhiễm trong hệ thống**
  - **Định danh loại virus nhiễm**
  - **Loại bỏ khôi phục hệ thống về trạng thái sạch**
- Thế hệ
  - **First generation: simple scanners**
  - **Second generation: heuristic scanners**
  - **Third generation: activity traps**
  - **Fourth generation: full-featured protection**

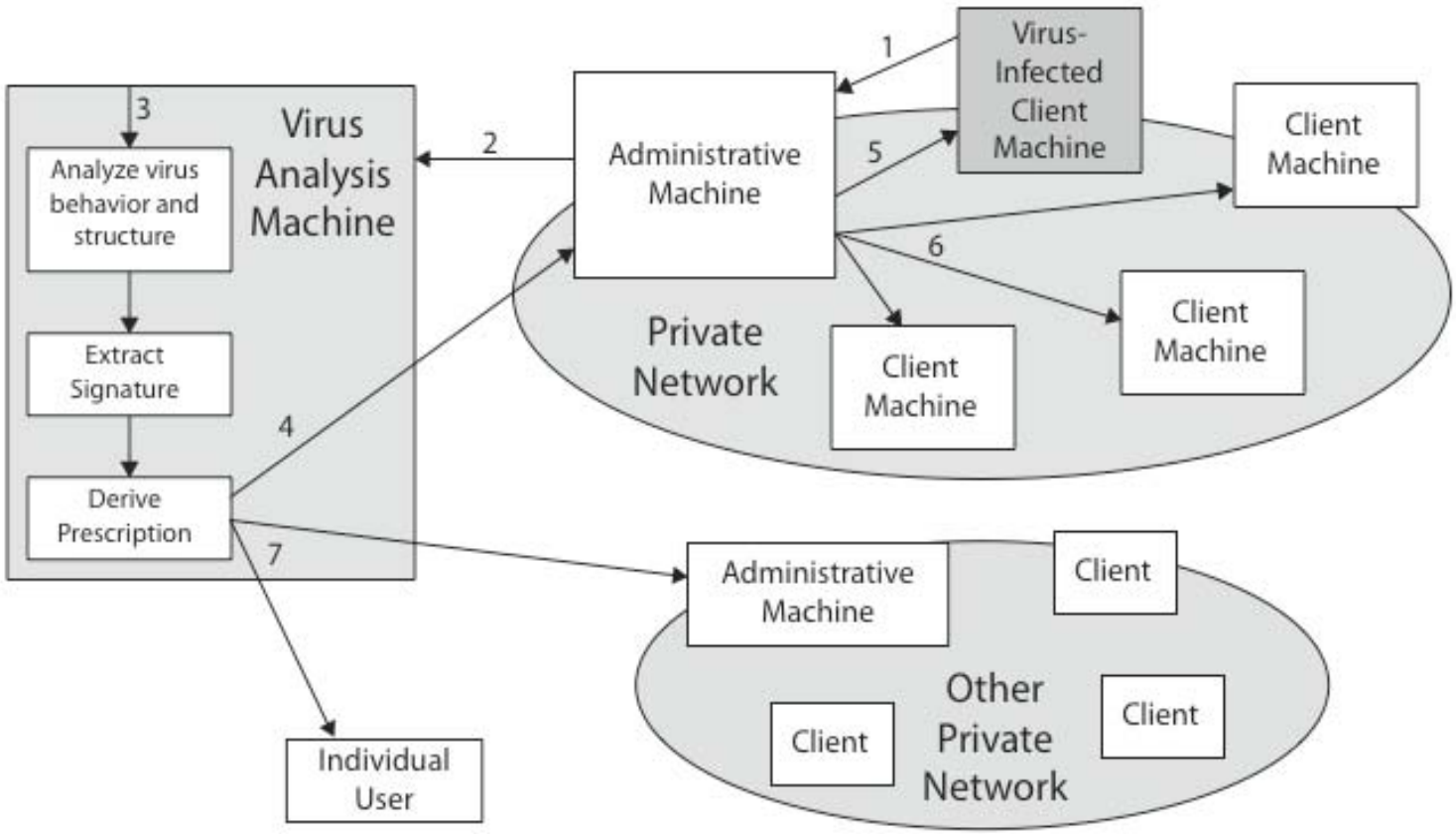
Các Thế hệ antivirus

- Thế hệ thứ 1
  - **Quét dấu hiệu (signature) virus**
  - **Độ dài chương trình**
- Thế hệ thứ 2
  - **Heuristic.**
  - **Kiểm tra checksum, dùng hàm hash mã hóa (ngoài chương trình)**
- Thế hệ thứ 3
  - **Chương trình thường trú kiểm tra hoạt động**
- Thế hệ thứ 4
  - **Đóng gói các kỹ thuật**
  - **Điều khiển truy cập (không cho phép virus update file)**

Kỹ thuật chống Virus nâng cao

- Giải mã giống loài
  - **Sử dụng mô phỏng CPU**
  - **Quyét chữ ký virus**
  - **Module kiểm tra hoạt động**

Hệ miễn dịch số (Digital Immune System)



Hệ thống miễn dịch số (IBM)

- **Hoạt động**
  - Chương trình theo dõi trên mỗi máy, phát hiện dấu hiệu thì chuyển máy quản trị trung tâm
  - Máy quản trị mã hóa và gởi đến trung tâm phân tích
  - Trung tâm phân tích đề ra cách nhận dạng và remove
  - Gởi mô tả trở lại máy quản trị
  - Máy quản trị chuyển tới client
  - Update

Phần mềm ngăn chặn hành vi

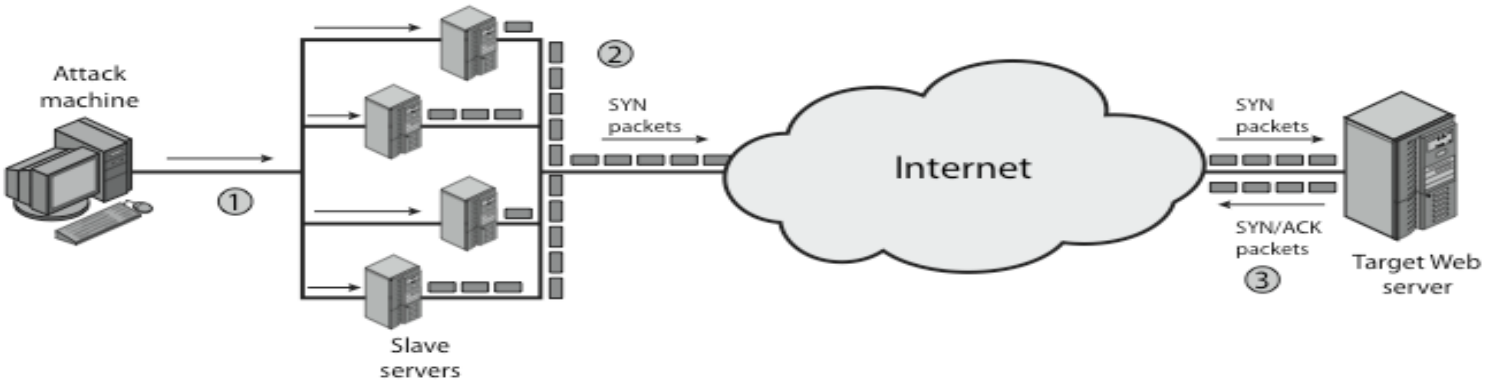
- Các phần mềm này được tích hợp với hệ điều hành của máy chủ. Chương trình theo dõi các hành vi trong thời gian thực
  - **Chẳng hạn truy cập file, định dạng đĩa, các chế độ thực hiện, thay đổi tham số hệ thống, truy cập mạng**
- Có ưu điểm so với quét, nhưng code có hại có thể chạy trước khi phát hiện.

I.6.3 Phòng chống Tấn công từ chối dịch vụ

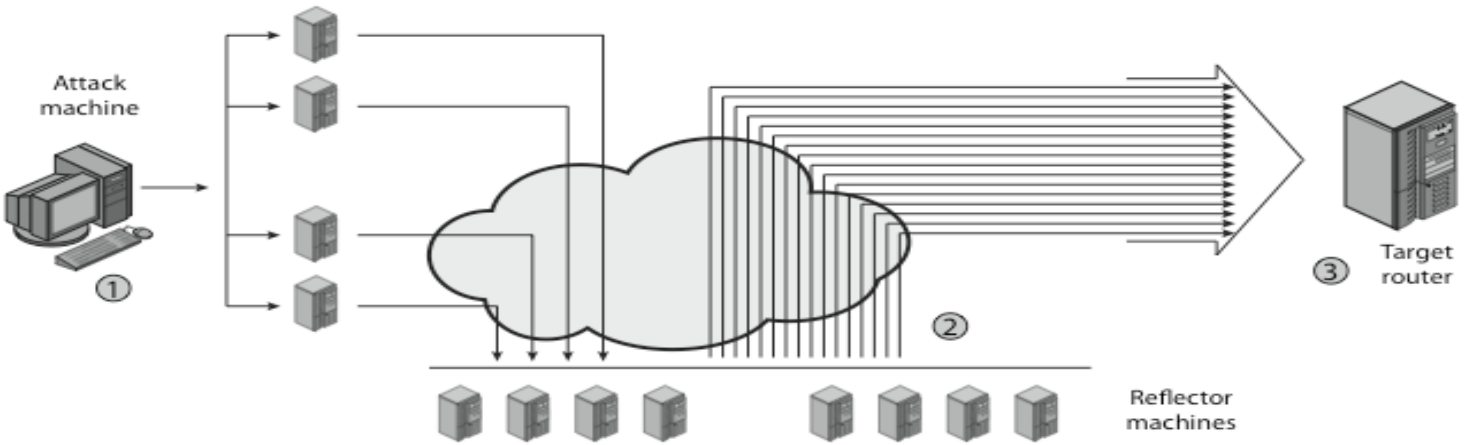
Tấn công từ chối dịch vụ

- Tấn công từ chối dịch vụ từ xa (DDoS) tạo thành đe dọa đáng kể, làm cho hệ thống trở nên không sẵn sàng, làm tràn bởi sự vận chuyển vô ích.
- Ví dụ
  - **Tấn công tài nguyên nội (tấn công đồng bộ)**
    - **Nhiều host giao tiếp với một máy chủ cần tấn công**
    - **Gởi TCP/IP SYN (synchronize/initialization) với địa chỉ giả**
  - **Tiêu thụ tài nguyên truyền dữ liệu**
    - **Điều khiển nhiều máy yêu cầu ICMP ECHO với địa chỉ giả**
    - **Nhận request và gởi echo rely**

Tấn công từ chối dịch vụ



(a) Distributed SYN flood attack

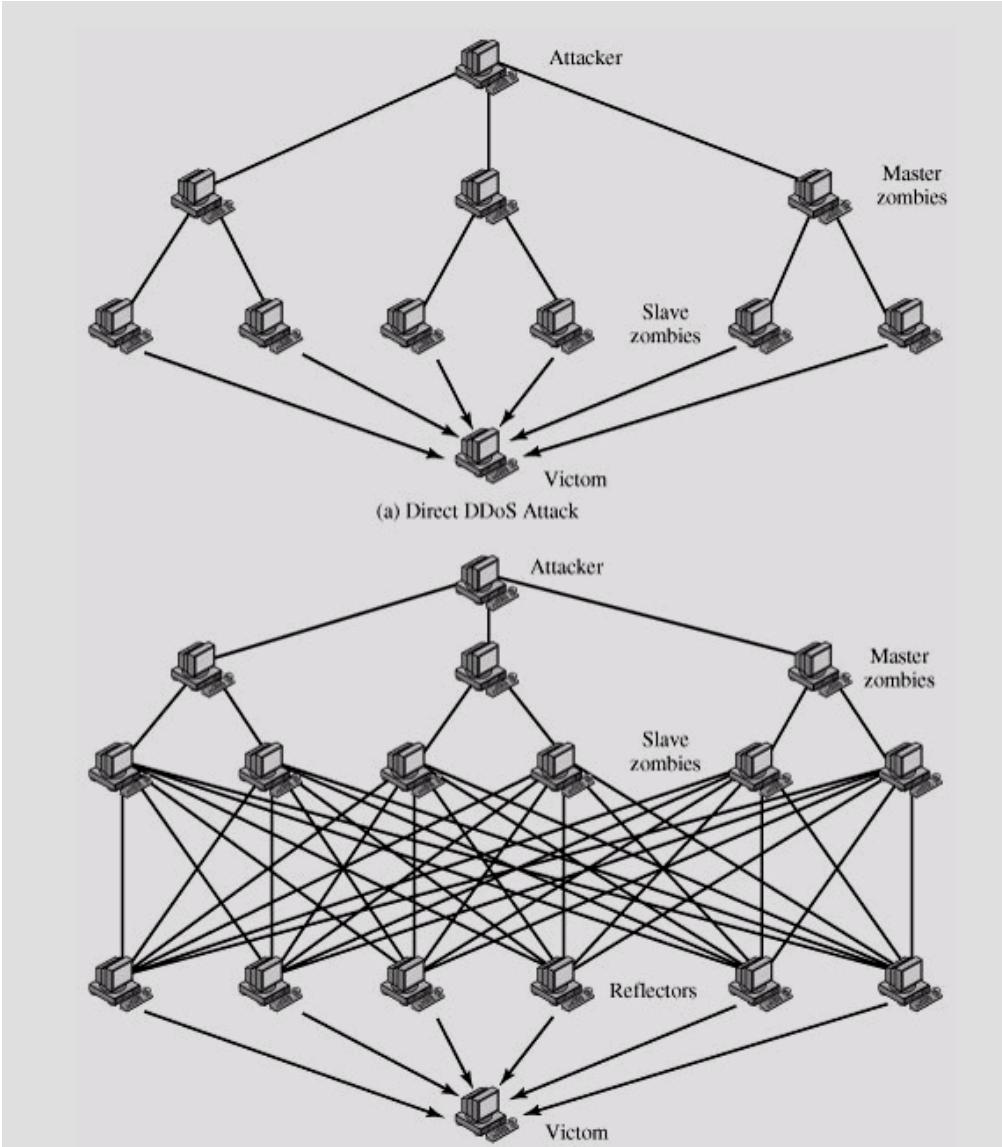


(a) Distributed ICMP attack

Một số cách tấn công

- Trong nhiều hệ thống những tài nguyên dữ liệu rất hạn chế: process identifiers, process table entries, process slots… Kẻ xâm nhập có thể viết những chương trình lặp tạo ra nhiều copy tiêu thụ tài nguyên này
- Kẻ xâm nhập cố tiêu thụ không gian đĩa
  - **Message mail**
  - **Tạo những lỗi mà được log**
  - **Ghi những file trong vùng anonymous ftp hay vùng chia sẻ**

Các hình thức tấn công



Xây dựng mạng tấn công

- Phần mềm zoobie phải chạy trên một số lớn máy, giấu sự tồn tại của nó, thông tin với máy chủ, có nhiều trigger để thực hiện tấn công tới máy đích
- Tấn công một số lớn hệ thống dễ xâm nhập
- Chiến lược sắp đặt dựa vào scan
  - **Random**
  - **Hit-list: danh sách máy dễ bị xâm nhập**
  - **Topological: dùng thông tin trong máy bị nhiễm**
  - **Local subnet: sau fireware**

Phòng chống tấn công DOS

- Ngăn ngừa: chính sách tiêu thụ tài nguyên, backup tài nguyên, điều chỉnh hệ thống và giao thức
- Phát hiện tấn công và lọc: dựa vào mẫu hành vi
- Xác định và lần vết