HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Bài 2. Những vấn đề trong an ninh thông tin

Học phần: BẢO ĐẢM VÀ AN TOÀN THÔNG TIN

Tài liệu tham khảo

1. Principles of Information Security - Michael E. Whitman and Herbert J. Matord

2.Information Security Fundamentals - Thomas R. Peltier, Justin Peltier

3.Google, Wikipedia, ...

NỘI DUNG

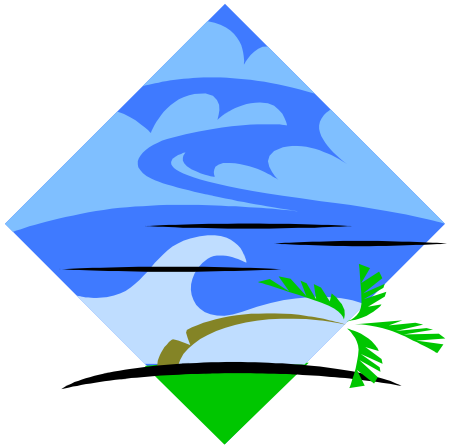
1. Chức năng của an toàn thông tin
2. Các mối đe dọa
3. Tấn công
4. Thảo luận và bài tập

1. Chức năng của An toàn thông tin

- Bảo vệ khả năng hoạt động của tổ chức
- Cho phép hoạt động an toàn của các ứng dụng chạy trên hệ thống CNTT của tổ chức
- Bảo vệ dữ liệu mà tổ chức thu thập và sử dụng
- Bảo vệ tài sản công nghệ của tổ chức

2. Các mối đe dọa

Khái niệm: Mối đe dọa là một đối tượng, một người, hoặc một thực thể khác có thể gây nguy hại đối với tài sản của một hệ thống thông tin.



- Nhà quản lý phải được thông báo về các loại mối đe dọa khác nhau mà tổ chức phải đối mặt.

- Bằng cách kiểm tra từng loại mối đe dọa, người quản lý bảo vệ hệ thông của mình thông qua chính sách, giáo dục và đào tạo và kiểm soát công nghệ.

Phân loại các đe dọa

CÁC ĐE DỌA	VÍ DỤ
1. Hành vi của con người	Tai nạn, lỗi của nhân viên
2. Sở hữu trí tuệ	Bản quyền cá nhân, sao chép
3. Hành vi gián điệp, xâm phạm	Truy cập bất hợp pháp, thu thập data bất hợp pháp
4. Hành vi tống tiền	Giả mạo thư điện tử, lấy cắp mật khẩu, mã hóa, tống tiền ...
5. Hành vi phá hoại	Phá hủy hệ thống thông tin
6. Hành vi trộm cắp	Lấy cắp các trang bi hoặc thông tin
7. Hành vi tấn công phần mềm	Virus, worm, backdoor,…
8. Thảm họa tự nhiên	Lũ, hỏa hoạn, động đất…
9. Chất lượng dịch vụ được cung cấp	Nguồn điện, mạng,…
10. Lỗi phần cứng	Trang bị phận cứng lỗi
11. Lỗi phần mềm	Bugs, lỗi lập trình, …
12. Công nghệ lỗi thời	Công nghệ lỗi hoặc chưa cập nhập mới

Hành vi của con người

Bao gồm các hành động được thực hiện mà không có mục đích xấu nguyên nhân:

- Thiếu kinh nghiệm
- Đào tạo không đúng
- Giả định không chính xác
- Các trường hợp khác

Nhân viên là mối đe dọa lớn nhất đối với bảo mật thông tin - Họ gần gũi nhất với dữ liệu tổ chức

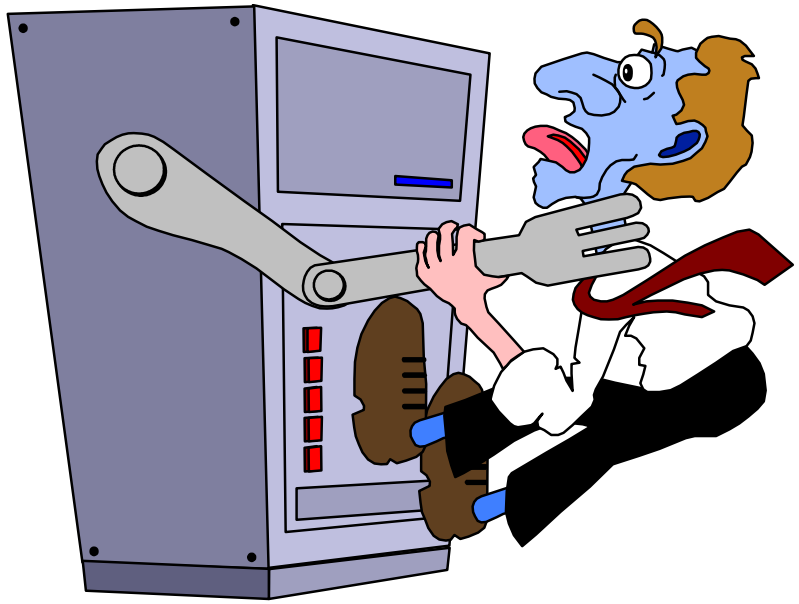
Hành vi của con người

Lỗi của nhân viên có thể dễ dàng dẫn đến những điều sau đây:

- Phân lớp dữ liệu sai
- Nhập dữ liệu sai
- Vô tình xóa hoặc sửa đổi dữ liệu

lưu trữ dữ liệu ở các khu vực không được bảo vệ

- Không bảo vệ được thông tin



Giải pháp: **Nhiều mối đe dọa có thể được ngăn chặn bằng các điều khiển, phân quyền**

Con người là mối đe dọa lớn nhất cho hệ thống thông tin

FIGURE 2-1 Acts of Human Error or Failure

Chất lượng dịch vụ cung cấp

- Các tình huống của sản phẩm hoặc dịch vụ không được phân phối như mong đợi
- Hệ thống thông tin phụ thuộc vào nhiều hệ thống hỗ trợ phụ thuộc lẫn nhau
- Ba vấn đề dịch vụ ảnh hưởng đáng kể đến hệ thống:
    - Dịch vụ Internet
    - Vấn đề truyền thông
    - Mạng lưới điện không ổn định

Dịch vụ Internet

- Mất dịch vụ Internet có thể dẫn đến mất mát đáng kể trong sự sẵn có của thông tin

  Ví dụ: tổ chức có nhân viên bán hàng và kết nối làm việc tại các địa điểm từ xa

- Khi một tổ chức thuê ngoài các máy chủ web của mình, người được thuê tự chịu trách nhiệm:
  - Tất cả dịch vụ Internet
  - Phần mềm hệ điều hành và phần cứng được sử dụng để vận hành trang web

Vấn đề truyền thông và các vấn đề khác

Các dịch vụ tiện ích khác có tác động tiềm năng tới hệ thống:

- Điện thoại
- Truyền hình cáp...

Các vấn đề khác:

- Nước và nước thải
- Rác thải
- Điều hòa….

Nguy cơ mất dịch vụ có thể dẫn đến hệ thống hoạt động sai lệch

Nguồn điện không ổn định

Mức điện áp có thể tăng, giảm hoặc dừng:

- Tăng đột biến - tạm thời
- Tăng gia tăng
- Mất điện tạm thời
- Mất điện kéo dài

Thiết bị điện tử dễ bị biến động, có thể áp dụng các biện pháp kiểm soát để quản lý chất lượng điện dùng UAC

Hành vi gián điệp, xâm phạm

- Truy cập trái phép thông tin

- Tin tặc sử dụng kỹ năng, lừa gạt hoặc gian lận để ăn cắp tài sản của người khác

Hành vi gián điệp, xâm phạm

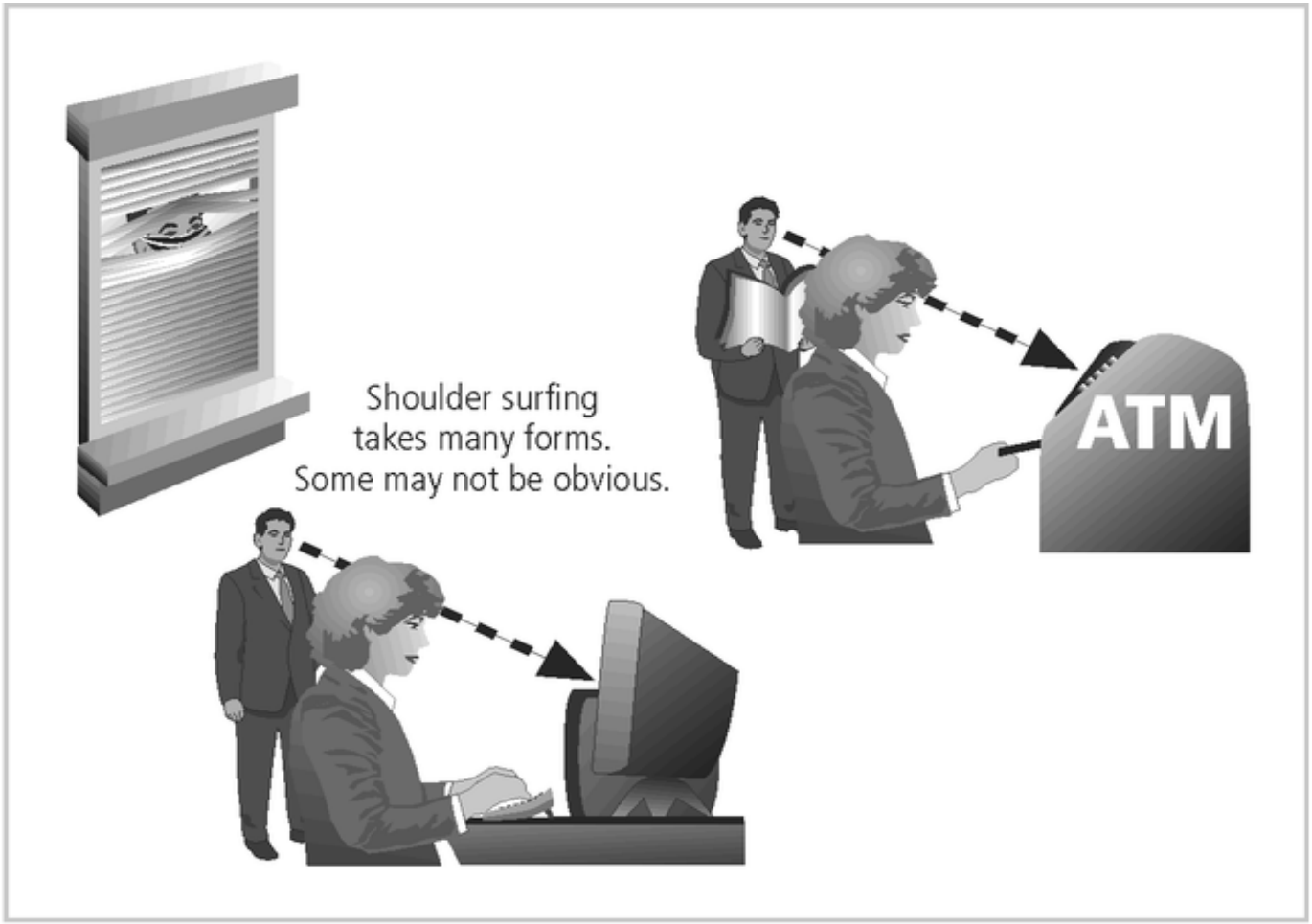


FIGURE 2-2 Shoulder Surfing

Hành vi gián điệp, xâm phạm

Traditional hacker profile:
Age 13-18, male with limited parental supervision spends all his free time at the computer

Modern hacker profile:
Age 12-60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization

FIGURE 2-3 Hacker Profiles

Hành vi gián điệp, xâm phạm

Hacker chuyên gia:
- Phát triển các kịch bản phần mềm và khai thác mã
- Có thể sẽ tạo phần mềm tấn công và chia sẻ

Kịch bản kiddies:
- Kỹ năng hạn chế
- Thường chạy script
- Sử dụng phần mềm có sẵn, thường không hiểu đầy đủ các hệ thống

Hành vi tống tiền

- Là hành vi đánh cắp thông tin từ hệ thống máy tính và yêu cầu bồi thường cho việc trả lại hoặc không sử dụng

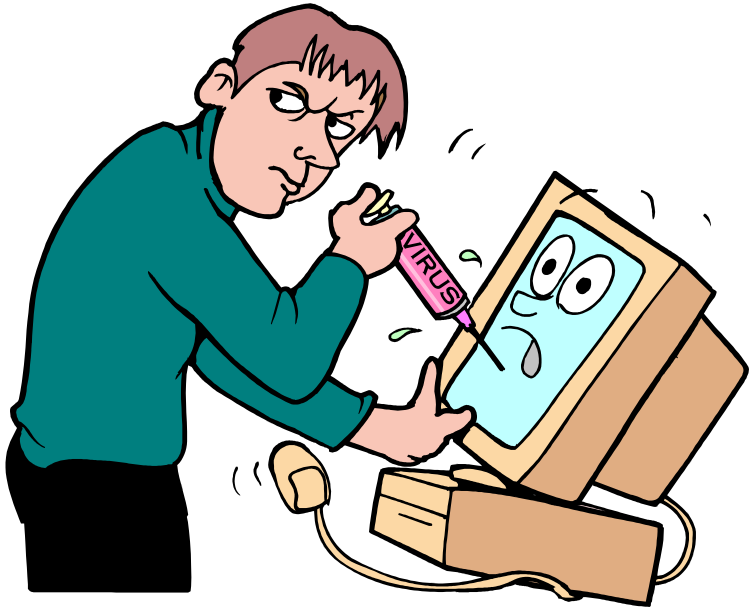
- Tống tiền tìm thấy trong trộm cắp số thẻ tín dụng

Hành vi phá hoại

- Cá nhân hoặc nhóm người muốn cố ý phá hoại các hoạt động của một hệ thống máy tính hoặc doanh nghiệp, hoặc thực hiện các hành vi phá hoại để phá hủy tài sản hoặc làm hỏng hình ảnh của tổ chức

- Những mối đe dọa này có thể dao động từ sự phá hoại nhỏ đến phá hoại có tổ chức

- Mối đe dọa gia tăng của các hoạt động tấn công hoặc chiến tranh mạng, hoặc khủng bố mạng



Hành vị trộm cắp

- Sử dụng bất hợp pháp tài sản của người khác - vật lý, điện tử hoặc trí tuệ
- Giá trị của thông tin bị ảnh hưởng khi được sao chép và lấy đi mà không được sự cho phép của chủ sở hữu
- Trộm cắp vật lý có thể được kiểm soát - sử dụng khóa, thuê bảo vệ hoặc hệ thống báo động
- Trộm cắp điện tử là một vấn đề phức tạp hơn để quản lý và kiểm soát - các tổ chức có thể thậm chí không biết nó đã xảy ra

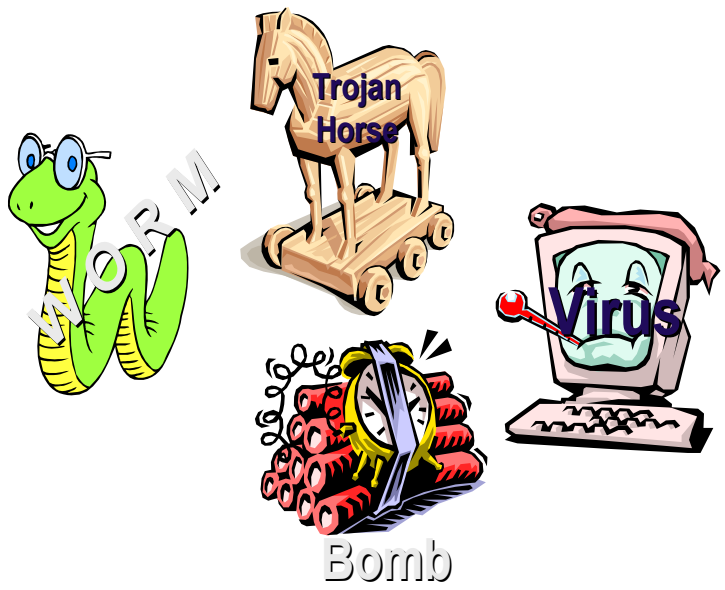
Tấn công phần mềm

- Khi một cá nhân hoặc nhóm thiết kế tạo phần mềm mã độc để tấn công hệ thống
- Được thiết kế để làm hỏng, phá hủy hoặc từ chối dịch vụ cho các hệ thống đích:

Ví dụ:

- macro virus
- boot virus
- worms
- Trojan horses
- logic bombs
- back door or trap door
- denial-of-service attacks

….



Tấn công phần mềm

- Virus là một chương trình máy tính tự gắn nó vào một tệp hoặc ứng dụng có thể chạy được.

Đặc điểm của virus:

- Lây lan
- Định vị
- Phá hoại

- Ngăn chặn virus bằng phần mềm, các kỹ năng sử dụng máy tính

Tấn công phần mềm

Phòng chống:

- Tìm hiểu các lỗ hổng hệ thống, phần mềm
- Cài đặt phần mềm diệt virus
- Cập nhập bản vá phần mềm
- Nâng cao kỹ năng sử dụng máy tính an toàn

Tấn công phần mềm

Sâu máy tính (worm): là một chương trình máy tính sao chép và truyền tải chính nó mà không cần phải đính kèm chính nó vào một tệp khác.

Vi dụ: Code Red và Nimda.

Tấn công phần mềm

- Trojan là một chương trình mà trong đó chứa đựng nhưng mã nguy hiểm và độc hại ẩn dưới dạng nhưng dữ liệu hay nhưng chương trình dường như vô hại (Sự tích thành Troy).
- Backdoor là một chương trình được sử dụng để cài đặt trên hệ thống đích, nhằm mục đích truy cập trở lại hệ thống vào lần sau.
- Thường sử dụng những cổng phổ biến để gây hiểu lầm cho người dùng

Tấn công phần mềm

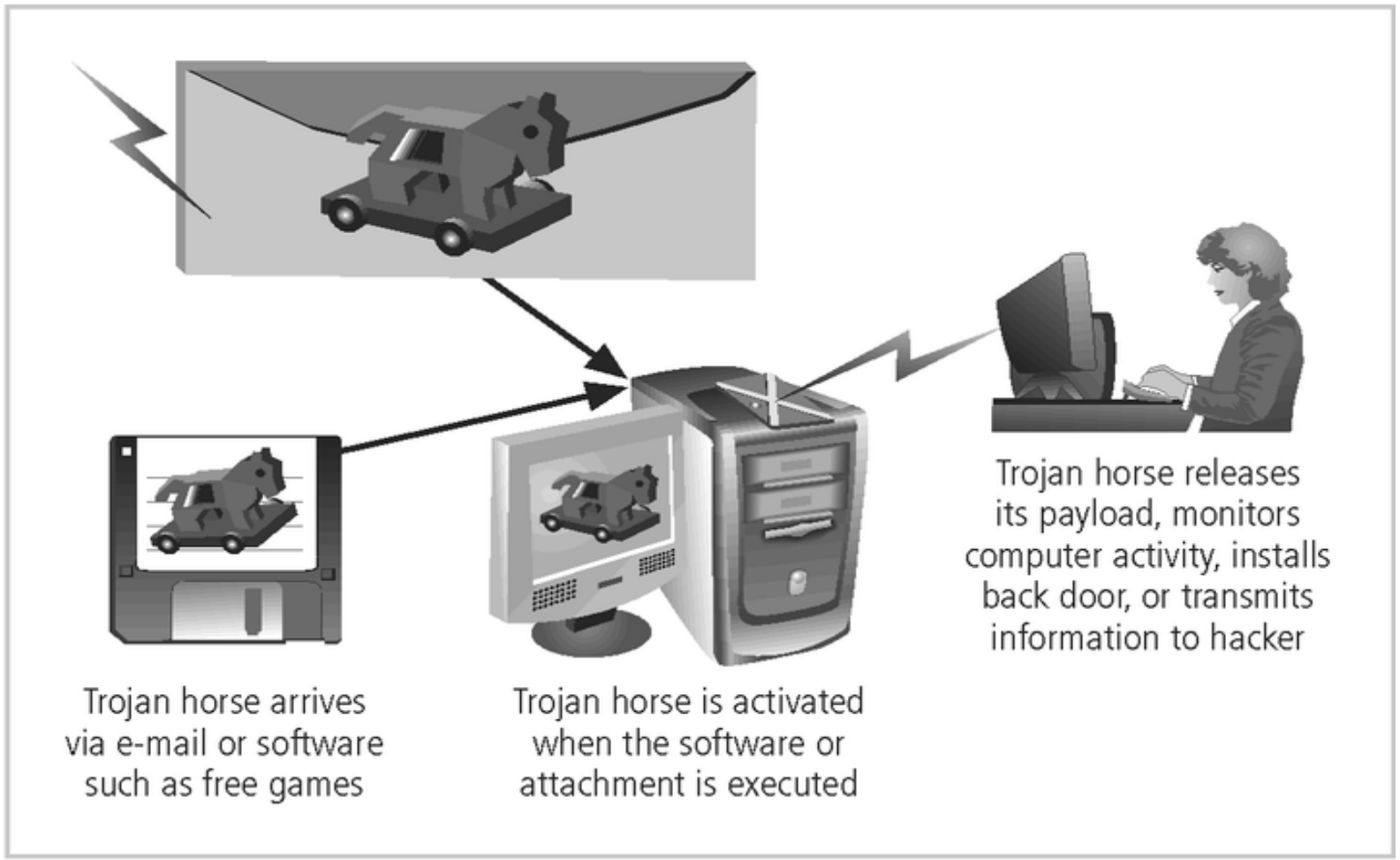


FIGURE 2-8 Trojan Horse Attack

Tấn công phần mềm

- Phần mềm gián điệp (spyware): là một chương trình phần mềm gián điệp gửi thông tin từ máy tính bị nhiễm tới máy chủ

Ví dụ: keylogger

- Phần mềm quảng cáo (adware): xác định thói quen mua của người dùng để trình duyệt web, hoặc nền tảng di động để có thể hiển thị quảng cáo phù hợp với người dùng đó.

Hệ quả: làm chậm máy tính đang chạy.

- Cả hai chương trình đều có thể được cài đặt ngoài ý muốn của người dùng

Bảo vệ việc Tấn công phần mềm

- Giáo dục bản thân, nâng cao nhận thức

+ Nâng cao kỹ năng sử dụng máy tính an toàn
+ Cài đặt phần mềm diệt virus
+ Tìm hiểu lỗ hổng bảo mệt
+ Sử dụng phần mềm bản quyền

….

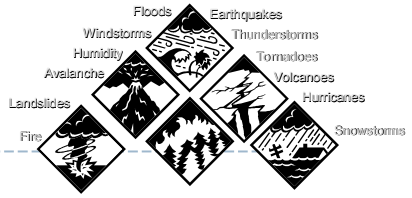
Sở hữu trí tuệ

Sở hữu trí tuệ là "quyền sở hữu các ý tưởng và kiểm soát đối với các đại diện hữu hình hoặc vô hình của những ý tưởng đó"

Sản phẩm trí tuệ:

- Bí mật thương mại
- Bản quyền
- Thương hiệu
- Bằng sáng chế

Thảm họa tự nhiên



- Thảm họa thiên nhiên, bất khả kháng như bão, lũ, cháy nổ... có thể gây hại tới hệ thống thông tin

- Vì không thể tránh được nhiều mối đe dọa này, quản lý phải thực hiện các biện pháp kiểm soát để hạn chế thiệt hại và cũng chuẩn bị các kế hoạch dự phòng cho hệ thống hoạt động liên tục

Lỗi phần cứng

- Lỗi phần cứng kỹ thuật là lỗi khi nhà sản xuất phân phối cho người dùng thiết bị chứa lỗi
- Những lỗi này có thể làm cho hệ thống hoạt động bên ngoài các tham số dự kiến, dẫn đến dịch vụ không đáng tin cậy

Ví dụ máy tính chứa backdoor...

- Một số lỗi là thiết bị đầu cuối, trong đó chúng dẫn đến mất thiết bị không thể khôi phục (ví dụ OE)

Công nghệ lỗi thời

- Khi cơ sở hạ tầng trở nên lỗi thời hoặc hết hạn sử dụng, nó dẫn đến các hệ thống sử dụng nó không đáng tin cậy.

- Người quản lý phải nhận ra rằng khi công nghệ trở nên lạc hậu, có nguy cơ mất tính toàn vẹn dữ liệu đối với các mối đe dọa và tấn công.

- Cách khắc phục: lập kế hoạch giám sát, cập nhập thay thế mới các công nghệ lỗi thời, hết hạn sử dụng.

3. Tấn công

- Tấn công là hành động có chủ ý nhằm khai thác lỗ hổng của một hệ thống nhằm mục đích đe dọa, gây thiệt hại, hoặc ăn cắp thông tin hoặc tài sản vật chất của hệ thống.

- Lỗ hổng là điểm yếu đã được xác định của hệ thống

Mã độc

- Tấn công này bao gồm các loại tấn công phần mềm như virus, worms, trojan, , backdoor và web scripts nhằm phá hủy hoặc ăn cắp thông tin hệ thống.
- Tấn công có thể kết hợp nhiều loại tấn công phần mềm ở trên nhằm khai thác các lỗ hổng của một hệ thống dựa trên các lỗ hổng phần mềm hệ thống được tìm thấy.

TABLE 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection
Shares	Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach
Mass mail	By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems
Simple Network Management Protocol (SNMP)	In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002

Mô tả tấn công

IP Scan and Attack – Hệ thống bị xâm nhập quét phạm vi địa chỉ IP, thường phục vụ cho công tác thăm dò của người tấn công

Virus - máy bị nhiễm virus có thể lây nhiễm mốt số tệp thực thi trên chính nó hoặc lây sang các máy khác

Mass Mail - gửi thư điện tử đến các địa chỉ được tìm thấy trong danh sách thư của người dùng một cách trái phép

Mô tả tấn công

Back Doors - sử dụng mở cổng trên máy bị tấn công để có thể truy cập, điều khiển, thực thi trái phép

Password Crack - tìm mật khẩu

Brute Force - thực hiện tấn công mật khẩu bằng phương pháp vét cạn, sử dụng từ điển

Dictionary - thử dụng từ điển để có thể thử các mật khẩu phổ biến mà người dùng sử dụng. Ví dụ – 123456, hello, admin,...

Mô tả tấn công

Denial-of-service (DoS) – tấn công từ chối dịch vụ là tấn công mà người tấn công gửi số lượng lớn các yêu cầu tới mục tiêu làm cho hệ thống quá tải và không thể đáp ứng được các yêu cầu từ người dùng khác.

Distributed Denial-of-service (DDoS) - là tấn công DoS nhưng sử dụng nhiều máy khác tấn công trong cùng một thời điểm.

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

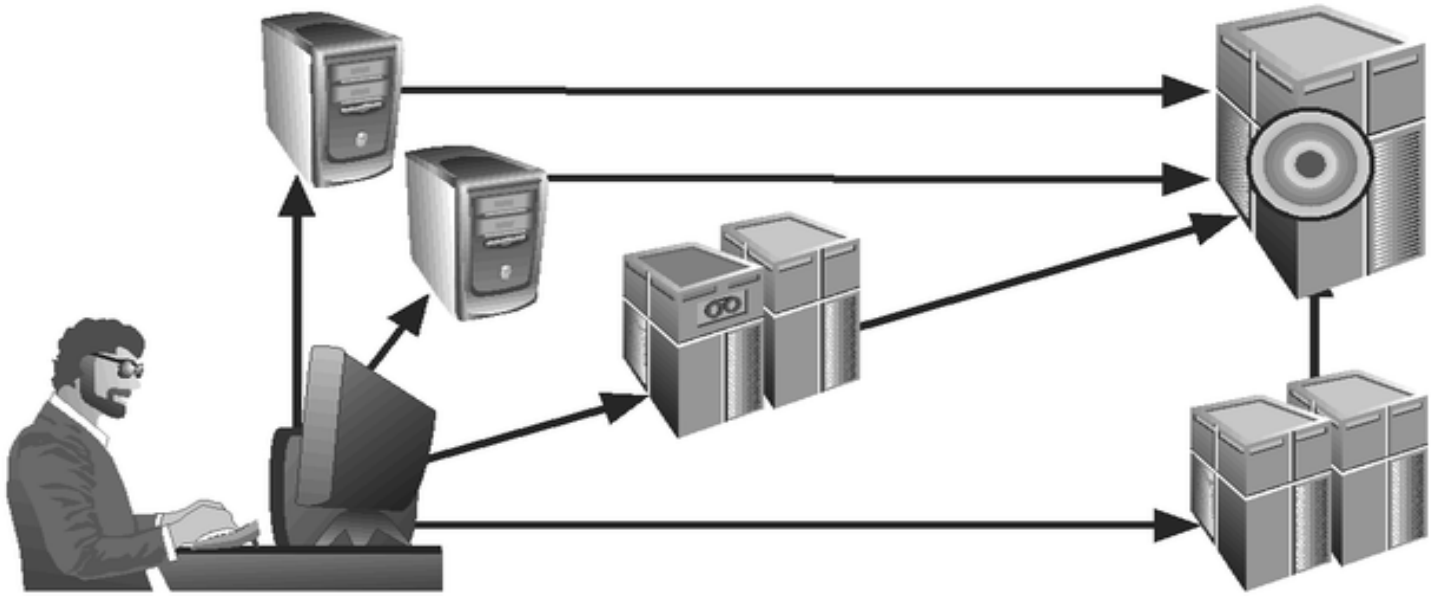


FIGURE 2-9 Denial-of-Service Attacks

Mô tả tấn công

Spoofing - giả mạo là kỹ thuật được sử dụng để truy cập trái phép, kẻ xâm nhập sử dụng thông tin thật của máy nạn nhân để tiến hành các hoạt động như gửi thư, tống tiền...

Man-in-the-Middle - tấn công sử dụng việc chặn bắt gói tin giữa đường truyền, sửa, sau đó gửi tiếp đến người dùng

Spam - có thể nhận mail không mong muốn từ những người lạ khi sử dụng dịch vụ

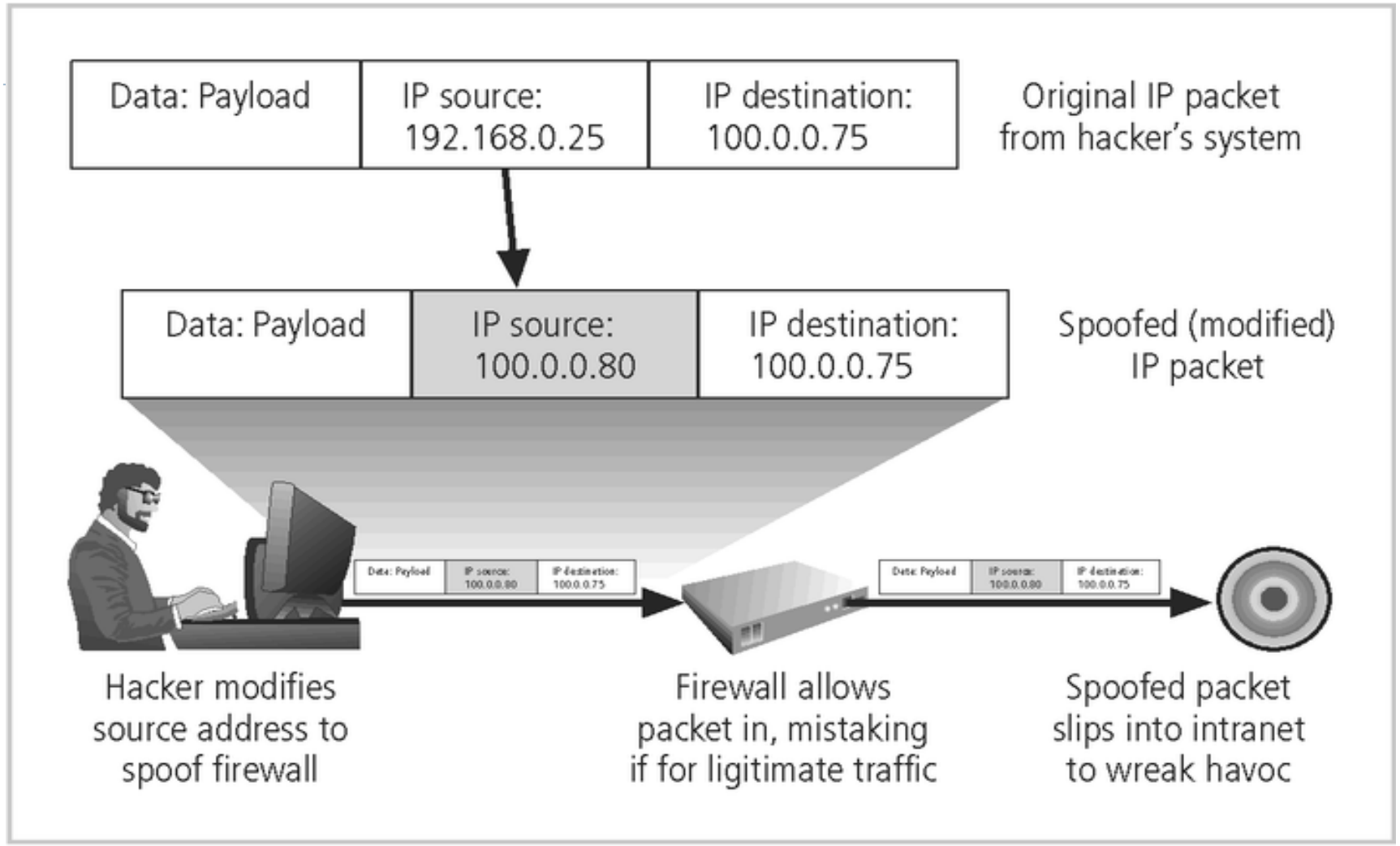


FIGURE 2-10 IP Spoofing

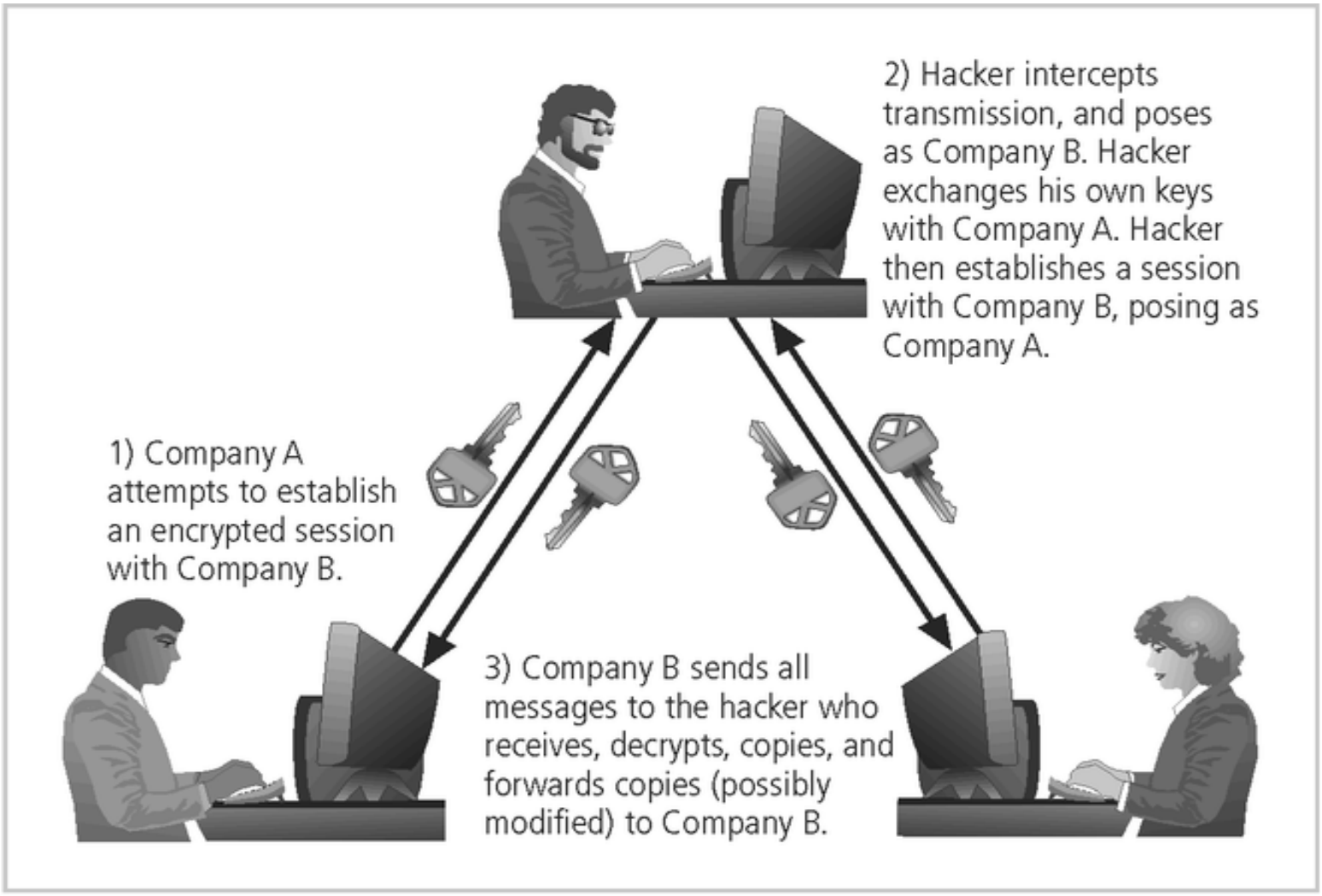


FIGURE 2-11 Man-in-the-Middle Attack

Mô tả tấn công

Mail-bombing - tương tự tấn công DoS sử dụng thư điện tử, kẻ tấn công gửi 1 lượng lớn mail đến máy chủ thư điện tử hoặc thư cá nhân

Sniffers - là một chương trình có thể giám sát chặn bắt dữ liệu truyền trên mạng. Ví dụ – tcpdump, tshark, wireshark...

Social Engineering - sử dụng các kỹ năng xã hội để thuyết phục mọi người tiết lộ thông tin xác thực truy cập hoặc thông tin giá trị khác cho kẻ tấn công

Mô tả tấn công

Buffer Overflow – tấn công tràn bộ đệm là tấn công xảy ra khi nhiều dữ liệu được gửi đến bộ đệm lớn hơn là nó có thể xử lý

- Khi tràn bộ đệm, kẻ tấn công có thể làm cho hệ thống đích thực hiện các lệnh ngoài kiểm soát của người dùng. Ví dụ: mở cổng cho backdoor hoạt động
- Phân tích lỗ hổng chương trình bên

```
#include <string.h>

int main(int argc, char *argv[])
{
 char buffer[10];
 if (argc < 2)
 {
 fprintf(stderr, "USAGE: %s string\n", argv[0]);
 return 1;
 }
 strncpy(buffer, argv[1], sizeof(buffer));
 buffer[sizeof(buffer) - 1] = '\0';
 return 0;
}
```

Mô tả tấn công

Ping of Death Attacks – Là loại tấn công tạo ra một gói ICMP có dữ liệu lớn hơn mức tối đa cho phép 65.535 byte. Các gói lớn được phân mảnh thành các gói nhỏ hơn và tập hợp lại tại đích đến của nó. Máy đích không thể xử lý gói quá khổ đã được tập hợp lại, do đó làm cho hệ thống bị treo hoặc đóng băng.

4. Thảo luận và bài tập

1. Tại sao vấn đề bảo mật thông tin lại là vấn đề quản lý?

2. Việc triển khai công nghệ mạng có tạo ra ít hoặc nhiều rủi ro cho

doanh nghiệp sử dụng công nghệ thông tin? Tại sao?

1. Tống tiền thông tin là gì? Mô tả cách tấn công như thế có thể gây ra tổn thất, nêu ví dụ.

2. Tại sao nhân viên lại là một trong những mối đe dọa lớn nhất đối với an ninh thông tin?

3. Nhận thức của hacker đã thay đổi như thế nào trong những năm gần đây? Hồ sơ của một hacker hôm nay là gì?

4. Sự khác biệt giữa một hacker có kỹ năng và một hacker không có kỹ năng (ngoài các cấp độ kỹ năng) là gì?

5. Các loại phần mềm độc hại khác nhau là gì? Trojan horses khác virus và worm ở điểm nào?

4. Thảo luận và bài tập

8. Hình thức vi phạm quyền sở hữu trí tuệ phổ biến nhất là gì? Làm thế nào để tổ chức bảo vệ chống lại nó? Cơ quan nào chống lại nó?

9. Làm thế nào để công nghệ lỗi thời là một mối đe dọa cho an ninh thông tin? Làm sao một tổ chức có thể bảo vệ chống lại nó không?

10. Các loại tấn công mật khẩu là gì? Quản trị viên hệ thống có thể làm gì bảo vệ hệ thống?

11. Sự khác biệt giữa cuộc tấn công từ chối dịch vụ và từ chối dịch vụ phân tán là gì? Loại nào nguy hiểm hơn? Tại sao?

12. Đối với một cuộc tấn công sniffer để thành công, kẻ tấn công phải làm gì? Làm thế nào kẻ tấn công có thể đạt được truy cập vào mạng để sử dụng hệ thống sniffer?

13. Các hacker kỹ thuật xã hội sử dụng phương pháp nào để thu thập thông tin về người dùng id đăng nhập và mật khẩu?

14. Tràn bộ đệm là gì, và nó được sử dụng như thế nào đối với một máy chủ ứng dụng hoặc máy chủ Web?

Tóm tắt

1. Chức năng của an toàn thông tin
2. Các mối đe dọa
3. Tấn công
4. Thảo luận và bài tập

HỎI VÀ ĐÁP