# AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình

Bộ môn Kỹ thuật máy tính & mạng

*http://dhthuyloi.blogspot.com*

# Chương 5:

## *AN NINH HỆ THỐNG*

- Những kẻ xâm nhập
- Phần mềm gây hại
- Firewall

# Bài 5.1 Những kẻ xâm nhập

- Sự xâm nhập bất hợp pháp vào một hệ thống máy tính hay mạng là một trong những mối đe dọa nghiêm trọng nhất đến an ninh hệ thống
- Hệ thống có thể bị xâm nhập bởi những người dùng trái phép, hoặc bởi các phần mềm gây hại (như virus, worm…)

# Phân loại người dùng trái phép

- **Giả dạng (Masquerader)**: Một cá nhân nào đó không có quyền sử dụng một máy tính nhưng đã lọt qua được hệ thống kiểm soát truy cập để khai thác tài khoản cá nhân của một người dùng hợp pháp.
- **Thông đồng (Misfeasor)**: Một người dùng hợp pháp truy xuất vào dữ liệu, chương trình hay các tài nguyên mà anh ta không có quyền; hoặc có quyền nhưng lạm dụng, dùng sai mục đích hợp pháp của mình.
- **Kẻ giấu mặt (Clandestine user)**: Một cá nhân nắm giữ quyền giám sát điều khiển hệ thống và sử dụng điều khiển này để lẩn tránh các kiểm soát, ghi chép an ninh hoặc vô hiệu hóa các ghi chép an ninh

# Các kỹ thuật xâm nhập

- Tìm cách lấy được mật khẩu người dùng
- Khai thác các lỗ hổng an ninh của hệ thống (ví dụ lỗi tràn bộ đệm..)
- Mua chuộc, dụ dỗ…

# Các kỹ thuật lấy mật khẩu

1. Thử các mật khẩu từng dùng với các tài khoản chuẩn gắn liền với hệ thống. Rất nhiều quản trị viên đã không bận tâm đến việc thay đổi các mật khẩu này.
2. Thử hết tất cả các mật khẩu ngắn (một đến ba ký tự).
3. Thử các từ trong từ điển trực tuyến của hệ thống, hoặc một danh sách mà rất có khả năng được sử dụng làm các mật khẩu.
4. Thu thập thông tin người dùng, chẳng hạn tên đầy đủ, tên vợ hoặc chồng cùng con cái, các bức tranh có trong văn phòng của họ, những cuốn sách ở văn phòng liên quan tới sở thích riêng…

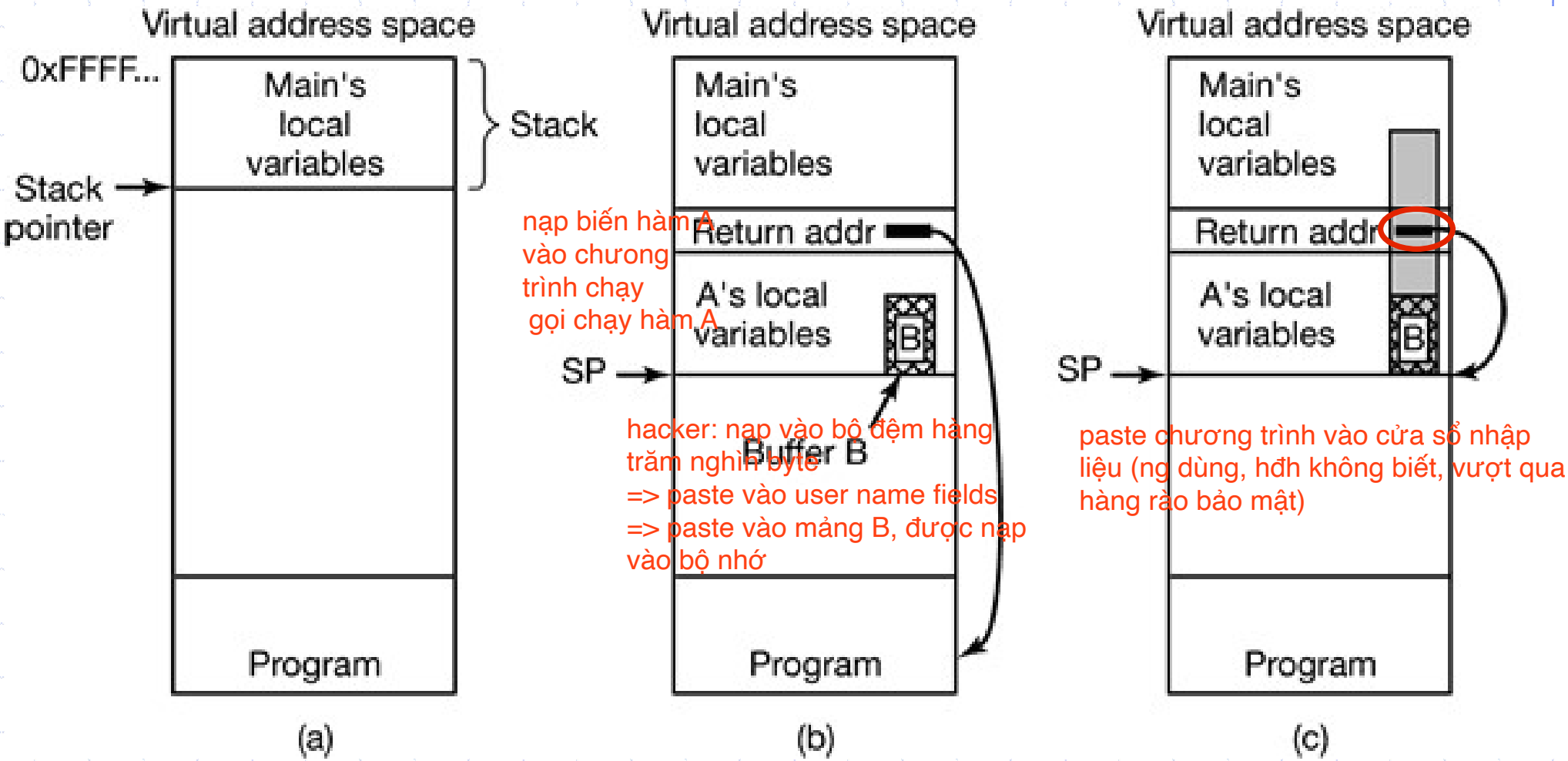
5. Thử số điện thoại của người dùng, các số An sinh xã hội và số phòng ở, phòng làm việc.
6. Thử tất cả các biển đăng ký xe hợp pháp của địa phương.
7. Dùng một Trojan horse để ăn cắp mật khẩu.
8. Đấu nối một đường truyền giữa người dùng từ xa với host hệ thống.

# Lỗi tràn bộ đệm

- Hầu hết các hệ điều hành và các chương trình hệ thống đều được viết bằng ngôn ngữ C, tuy nhiên các trình biên dịch C thường không kiểm tra giới hạn của mảng
- Ví dụ:

```
int i;
char c[1024];
i = 12000;
c[i] = 0;
```

- Đoạn chương trình trên bị lỗi vì ghi đè vào một ô nhớ nào đó nằm cách mảng *c* tới 10976 byte, và có thể tạo ra một hậu quả vô cùng tai hại
- Khi chạy chương trình, những lỗi như thế này sẽ không bị kiểm tra nên không thể ngăn chặn được. Hacker có thể lợi dụng lỗi này để tấn công

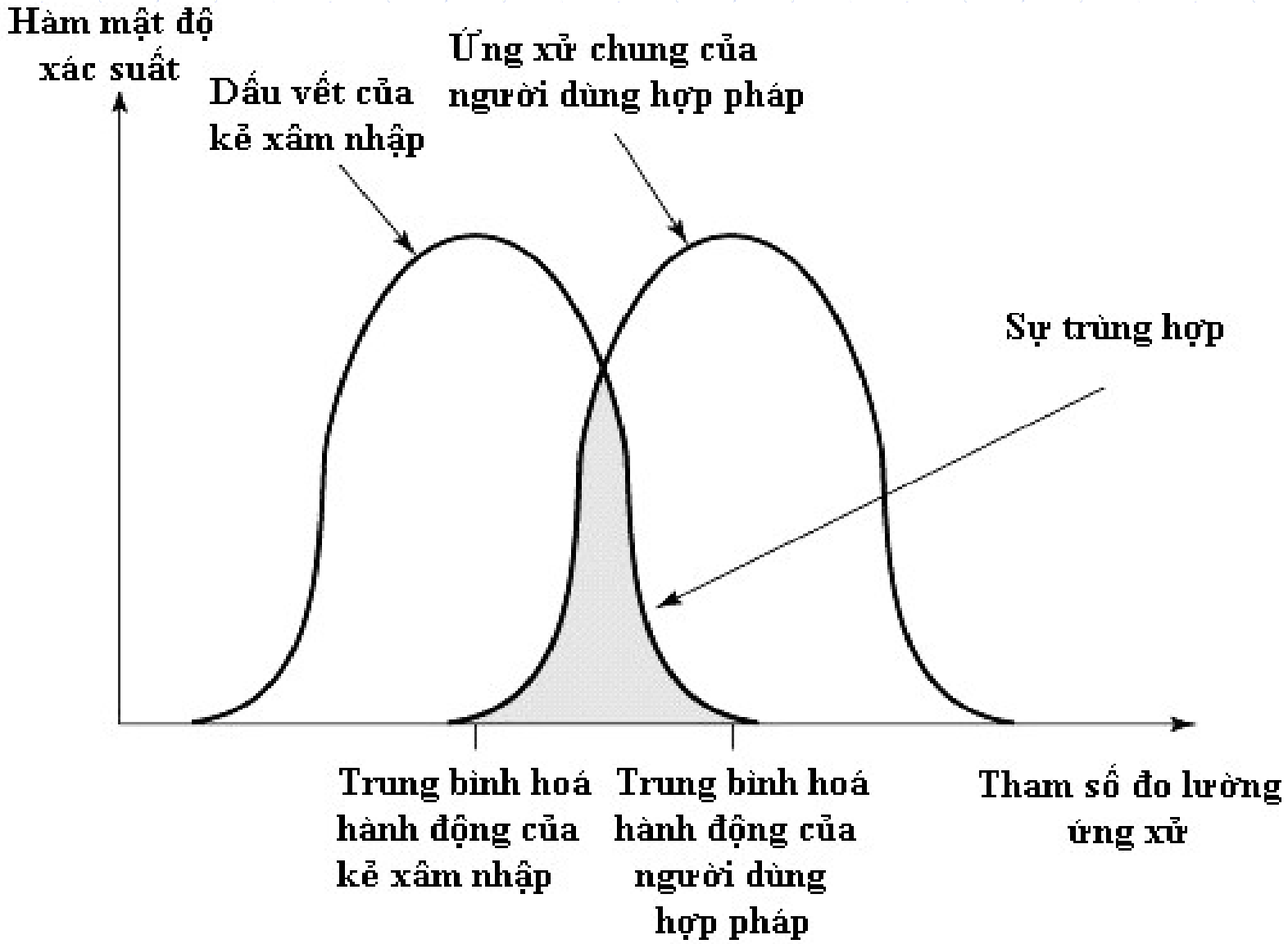



*(a) Tình huống khi chương trình chính đang chạy.*
*(b) Sau khi hàm A được gọi.*
*(c) Bộ đệm bị tràn (vùng tô màu xám).*

- Hacker sẽ chuẩn bị trước một chuỗi kí tự đặc biệt, chuỗi này có chứa địa chỉ của một chương trình do hacker viết.
- Địa chỉ đó được đặt ở một vị trí được tính toán cẩn thận, sao cho khi nạp chuỗi vào bộ đệm B thì địa chỉ đó sẽ ghi đè vào địa chỉ trở về của chương trình ban đầu.
- Kết quả là khi hàm A kết thúc, quyền điều khiển không được trả về cho chương trình ban đầu, mà lại được trao cho chương trình do hacker viết.

# Phát hiện xâm nhập

- Bằng cách theo dõi và ghi lại các hoạt động của người dùng, người ta có thể phát hiện ra kẻ xâm nhập bất hợp pháp nằm trong hệ thống
- Cách thức hoạt động của kẻ xâm nhập thường có sự khác biệt so với người dùng hợp pháp


Hàm mật độ xác suất
Dấu vết của kẻ xâm nhập
Ứng xử chung của người dùng hợp pháp
Sự trùng hợp
Trung bình hoá hành động của kẻ xâm nhập
Trung bình hoá hành động của người dùng hợp pháp
Tham số đo lường ứng xử

- Tuy nhiên, việc phát hiện sự khác biệt trong hành động của kẻ xâm nhập so với người dùng hợp pháp cũng không phải đơn giản.
- Người ta thường sử dụng hai phương pháp sau để phát hiện sự khác biệt:
  + Phát hiện bất thường bằng thống kê
  + Phát hiện bất thường bằng quy tắc

# Phát hiện bất thường bằng thống kê

- Cần xây dựng một bộ sưu tập dữ liệu liên quan tới hoạt động thông thường của người dùng hợp pháp trong một khoảng thời gian nào đó.
- Sau đó, các phép kiểm tra thống kê được áp dụng để giám sát hoạt động của người dùng ở mức độ cao.

- Ví dụ:

  Một người dùng thực hiện một hành động nào đó với tần suất vượt quá "ngưỡng" trung bình của các người dùng thông thường có thể sẽ bị nghi ngờ, và bị theo dõi chặt chẽ hơn.

# Phát hiện bất thường bằng quy tắc

- Cần định nghĩa một tập các quy tắc để quy định hành động nào là hợp lệ, hành động nào không hợp lệ, hành động nào là bình thường, hành động nào là đáng ngờ...
- Người dùng nào thường xuyên có các hành động không hợp lệ sẽ bị nghi ngờ.

# Bài 5.2 Phần mềm gây hại

- Có rất nhiều loại phần mềm gây hại khác nhau, với những đặc điểm và nguyên tắc hoạt động khác nhau.
- Có những phần mềm gây hại có khả năng lây lan, tự nhân bản nó từ máy này sang máy khác, như virus, worm…
- Có những phần mềm gây hại không tự lây lan được, chúng chỉ nhằm thực hiện một hành động định trước như ăn cắp dữ liệu hay phá hoại (ví dụ Trojan horse, Logic bomb…)

# Các phần mềm có khả năng lây lan

- ***Virus:***

  Virus là một đoạn mã chương trình có thể lây nhiễm tới các chương trình khác (bằng cách gắn bản sao của nó vào các chương trình mà nó tìm thấy)

- ***Worm:***

  Worm là một chương trình có thể tự nhân bản và gửi các bản sao của nó từ máy tính này đến máy tính khác qua các kết nối mạng.

# Phân loại virus

- Virus Boot
- Virus File thi hành
- Virus Macro

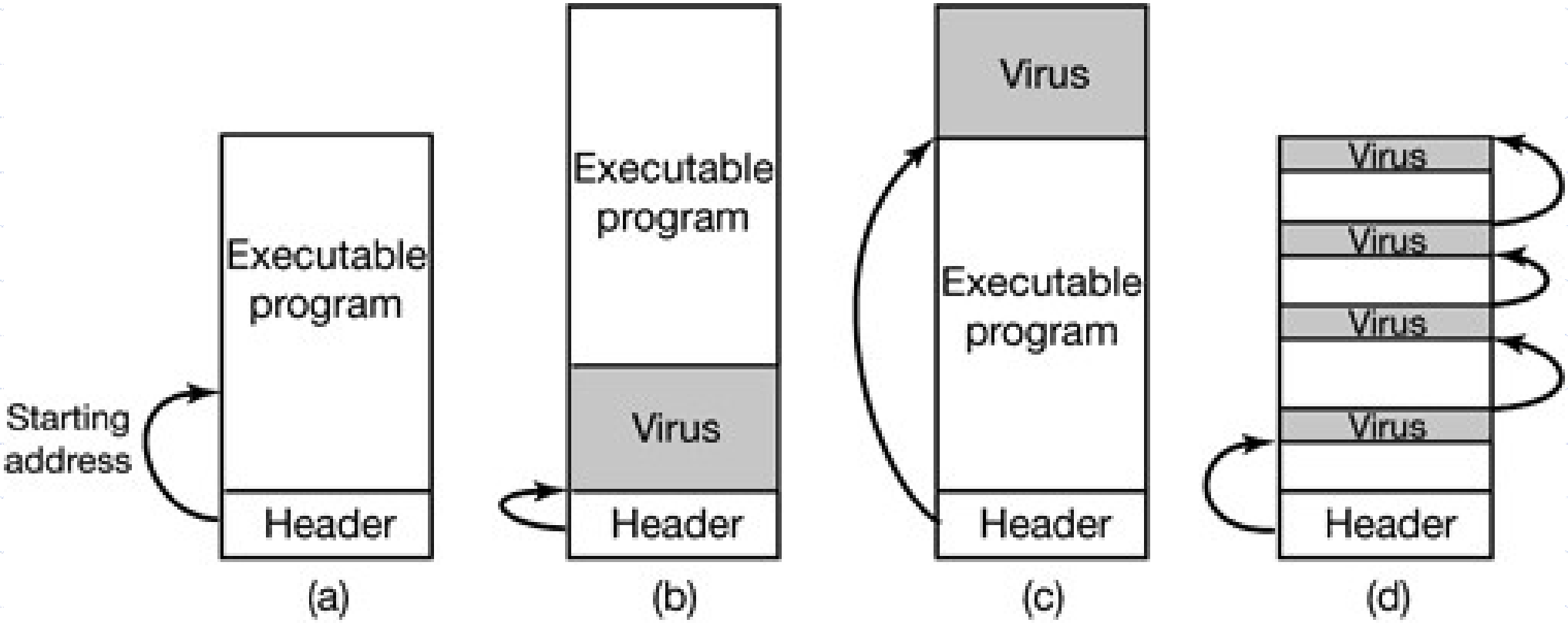
# Virus Boot

- Loại virus này lây lan vào đoạn mã khởi động trên Boot sector hay Master Boot Record của đĩa
- Khi máy tính khởi động, virus boot được kích hoạt. Nó sẽ thường trú trong bộ nhớ, chờ để lây vào một ổ đĩa mới
- Nếu đem ổ đĩa nhiễm virus lắp sang một máy tính khác, rồi khởi động máy từ ổ đĩa đó, máy tính sẽ bị nhiễm virus.

- Ví dụ:

# Virus File thi hành

- Loại virus này lây nhiễm vào các file nhị phân thi hành được (.EXE, .COM, .DLL, .BIN, .SYS…)
- Đoạn mã virus có thể được gắn vào đầu file, cuối file, hoặc giữa file
- Khi file được chạy, virus sẽ được kích hoạt, nó sẽ tìm cách lây vào các file khác trong máy




*(a) Câu trúc một file thi hành.*
*(b) Virus gắn vào đầu file.*
*(c) Virus gắn vào cuối file.*
*(d) Virus nằm rải rác ở các vùng trống trong file.*

- Ví dụ:

# Virus Macro

- Loại virus này lây nhiễm vào các macro trong các file tài liệu của MicroSoft Office (Word, Excel…)
- Một số macro có khả năng tự khi hành khi mở file, cất file… Virus Macro thường nằm trong các macro tự động đó.
- Khi file được mở, virus sẽ được kích hoạt, sau đó nó tìm cách lây vào các file tài liệu khác.

- Ví dụ:

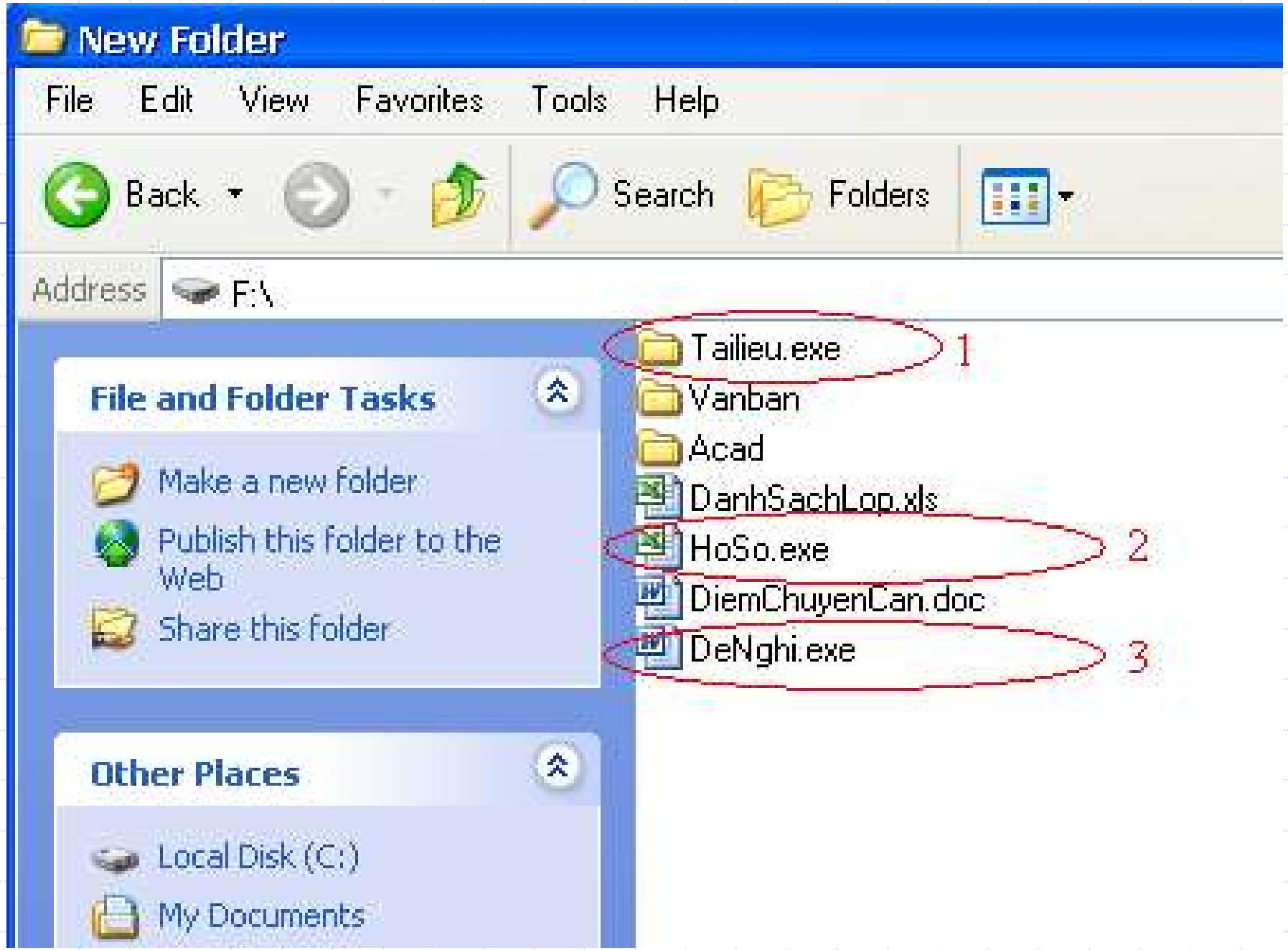
# Kỹ thuật lây lan của Virus

- Muốn lây lan thì virus phải được kích hoạt. Khi virus được kích hoạt, mã lệnh của nó sẽ tìm cách tự sao chép tới các file khác hoặc đĩa khác.
- Có nhiều cách để kích hoạt một virus, chủ yếu là lợi dụng các sơ hở của hệ thống, hoặc tìm cách "dụ" người dùng chạy file nhiễm virus.

- Hacker viết virus, gắn nó vào một chương trình (do anh ta tự viết hoặc ăn cắp), rồi phát tán chương trình đó (ví dụ bằng cách gửi nó lên một website cung cấp phần mềm miễn phí). Ai download và chạy chương trình này sẽ kích hoạt virus
- Có thể đính kèm file nhiễm virus vào email, rồi gửi cho mọi người. Khi mở file đính kèm thì virus sẽ được kích hoạt

- Virus "đóng giả" các file tài liệu hoặc Folder (bằng cách đổi tên, đổi icon…) để "lừa" người dùng bấm chuột vào
- Lợi dụng tính năng Auto Run của các ổ đĩa USB, CD để kích hoạt virus

…



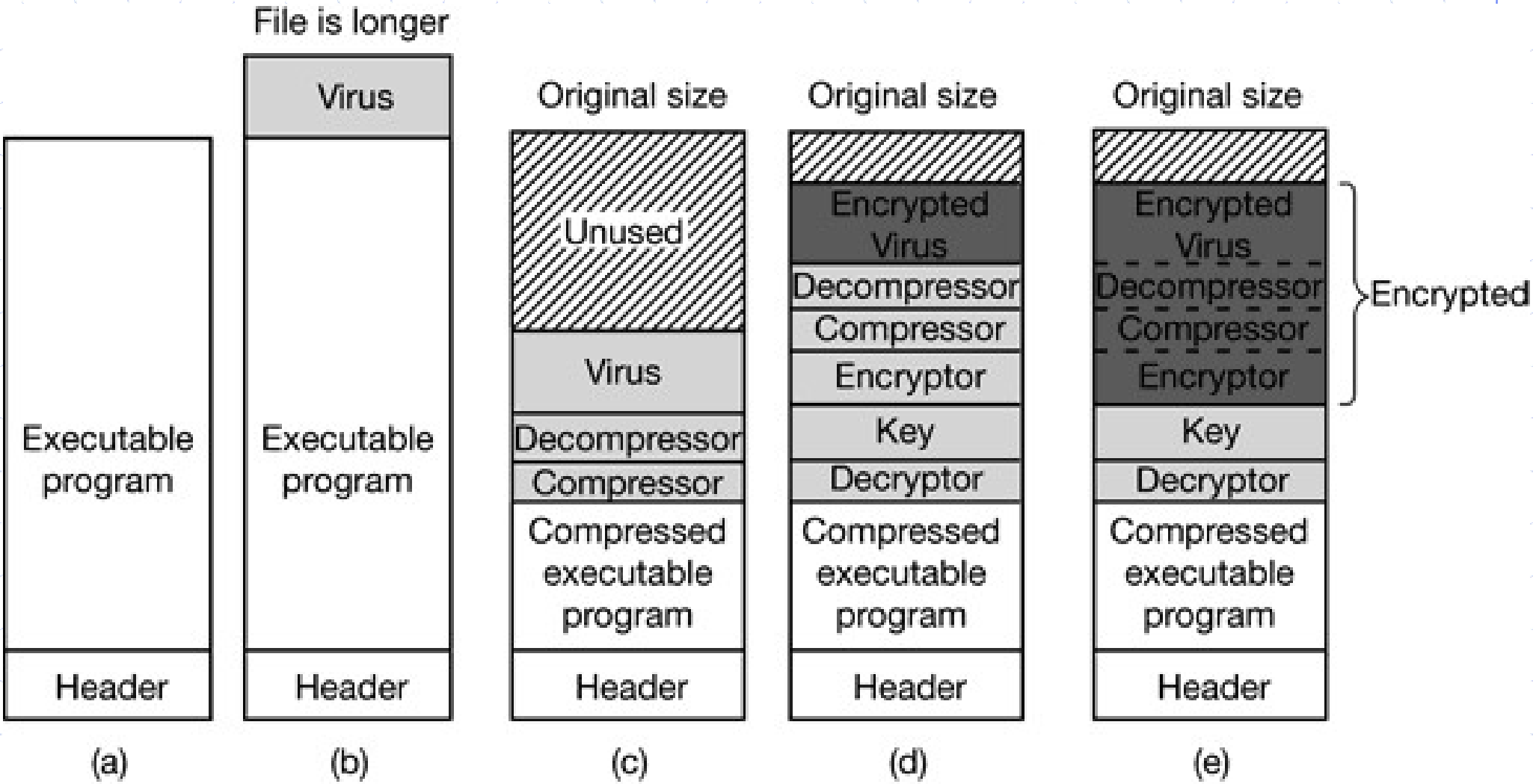

*1- Virus đóng giả Folder. 2- Virus đóng giả file Excel. 3- Virus đóng giả file Word. Tuy có biểu tượng của Word, Excel và Folder, nhưng các file này lại có đuôi là EXE.*

# Kỹ thuật nguỵ trang của Virus

- Để chống lại các phần mềm diệt virus, virus phải có giải pháp nguỵ trang, che dấu bản thân
- Sau khi lây vào một file mới, virus thường sửa đổi lại ngày, giờ, thuộc tính file… cho giống với file chưa bị lây nhiễm
- Có thể áp dụng phương pháp nén để giữ nguyên kích thước của file sau khi lây

- Dấu mã lệnh virus vào các vùng an toàn trên đĩa, và đánh dấu chúng là các sector hỏng (đối với virus boot hoặc virus lai).
- Liên tục biến đổi mã lệnh virus để thay đổi bản thân, tránh bị nhận dạng (virus đa hình).

…




*(a) Chương trình chưa nhiễm virus. (b) Chương trình đã bị nhiễm virus.*
*(c) Chương trình nhiễm virus đã được nén. (d) Virus được mã hoá.*
*(e) Mã hoá cả virus lẫn các hàm nén, giải nén, mã hoá.*

# Worm

*Worm cũng có khả năng lây lan giống virus, nhưng nó khác với virus ở hai điểm cơ bản sau:*

- Worm là một chương trình hoàn chỉnh (chứ không phải là một đoạn mã gắn vào chương trình khác như virus)
- Kỹ thuật lây lan từ máy này sang máy khác của Worm dựa vào các lỗ hổng bảo mật của mạng máy tính.

# Một số kỹ thuật lây lan của Worm

- **Tìm cách thi hành chương trình từ xa:** Một số máy cho phép chạy *chương trình shell* ở xa mà không yêu cầu xác thực. Nếu thành công, shell ở xa sẽ tải chương trình worm về và tiếp tục lây vào các máy khác kết nối với nó
- **Tìm cách đăng nhập từ xa:** Worm có thể sử dụng chương trình đoán mật khẩu, lần lượt thử đăng nhập với một danh sách mật khẩu được chuẩn bị từ trước. Nếu đoán mật khẩu thành công, Worm có thể đăng nhập được vào bất cứ máy tính nào người dùng đó có tài khoản.

- **Tận dụng lỗi tràn bộ đệm:** Worm Morris đã tận dụng lỗi tràn bộ đệm của chương trình finger (có trên một số website) để kích hoạt Worm trên máy bị tấn công.
- **Tận dụng lỗi của hệ thống email:** Một số hệ thống email cho phép chương trình worm gửi thư có chưa phần khởi động cho người khác và thi hành nó

…

# Tóm lại, Worm thường lây lan thông qua 3 bước sau đây:

- Tìm kiếm các hệ thống khác để lây nhiễm bằng cách khảo sát các bảng host hay những nơi chứa các địa chỉ các hệ thống từ xa.
- Thiết lập kết nối tới hệ thống từ xa.
- Tự sao chép đến hệ thống từ xa và kích hoạt để tự thi hành.

# Phòng tránh virus và các phần mềm gây hại

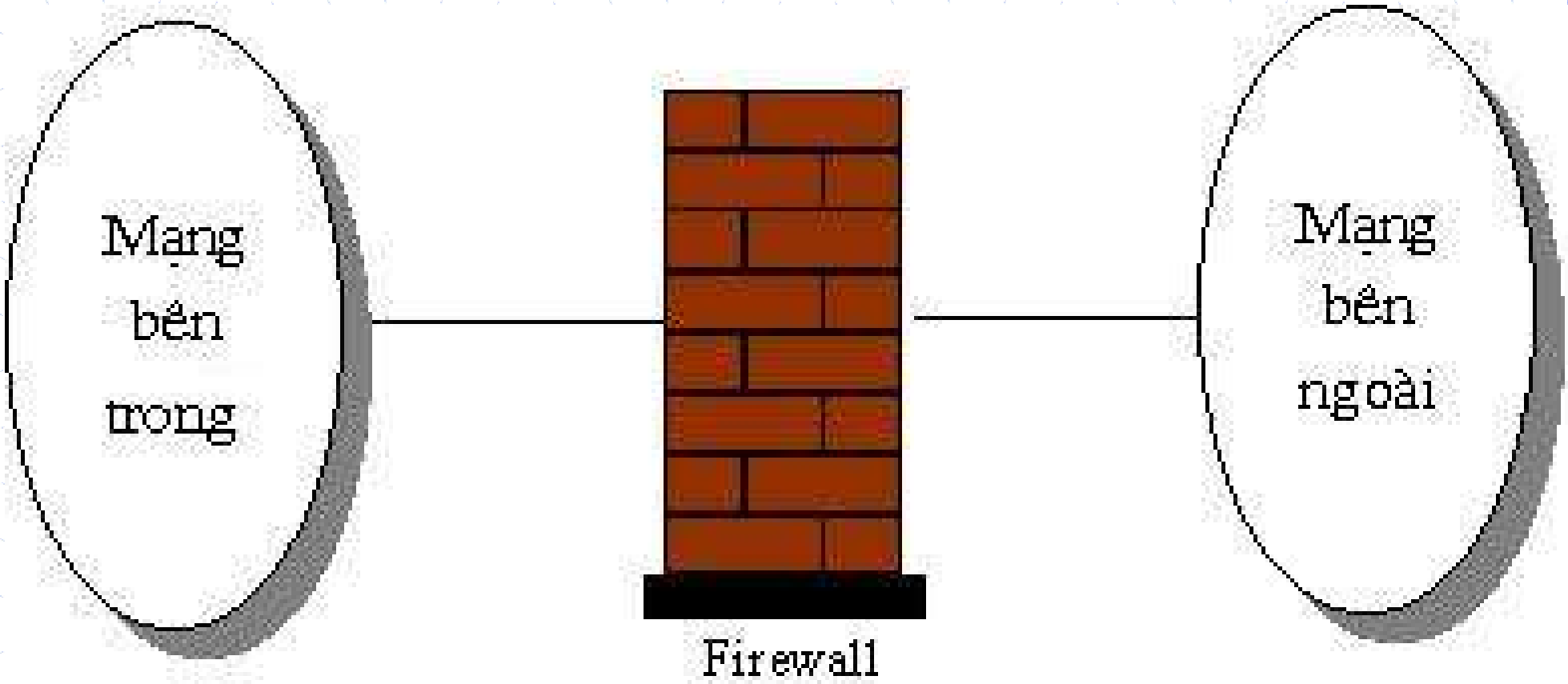
- Thứ nhất, hãy chọn một hệ điều hành có độ an toàn cao, chế độ kernel và chế độ người dùng có ranh giới rõ ràng, người dùng và người quản trị hệ thống phải có mật khẩu đăng nhập riêng. Khi đó, nếu virus có lẻn vào thì cũng khó có thể lây vào hệ thống nhị phân.
- Thứ hai, chỉ cài đặt các phần mềm chính thống mua từ các nhà sản xuất đáng tin cậy. Không download các phần mềm không rõ nguồn gốc từ Internet.

- Thứ ba, hãy mua một chương trình diệt virus tốt và sử dụng nó thường xuyên. Hãy luôn cập nhật phiên bản mới nhất của nó từ Website của nhà sản xuất.
- Thứ tư, đừng bao giờ bấm chuột vào các file thi hành đính kèm trong email, hay các file thi hành tự nhiên xuất hiện trong ổ đĩa USB của bạn. Nói chung, phải cận thận với tất cả các file có thể chứa mã lệnh!

- Thứ năm, thường xuyên sao lưu các file quan trọng ra bộ nhớ ngoài (như đĩa USB, đĩa CD), đề phòng trường hợp máy tính của bạn bị nhiễm virus, bạn vẫn có thể khôi phục lại các file về trạng thái ban đầu.
- Thứ sáu, thường xuyên cập nhật các bản vá lỗi mới nhất của hệ điều hành, của trình duyệt web, và các phần mềm khác.

# Bài 5.3 Firewall

- Firewall là một phương tiện hiệu quả để bảo vệ hệ thống khỏi các nguy cơ an ninh mạng, trong khi vẫn hỗ trợ các giao tiếp với bên ngoài qua các mạng diện rộng hay Internet.
- Firewall được chèn vào giữa nội mạng và Internet để tạo nên một "bức tường chắn" điều khiển được, hình thành một vành đai bảo vệ.




# Mô hình firewall đơn giản

- Một firewall có thể được thiết kế để hoạt động như một bộ lọc ở mức các gói tin IP, hoặc có thể hoạt động ở các tầng giao thức cao hơn
- Firewall có thể là một máy tính (hoặc một hệ thống máy tính), được cài đặt phần mềm phù hợp.

# Bốn hoạt động cơ bản của firewall

- **Kiểm soát dịch vụ**: Xác định các kiểu dịch vụ Internet có thể truy xuất, cả trong ra và từ ngoài vào. Firewall thi hành lọc các giao vận trên cơ sở địa chỉ IP và số hiệu cổng.
- **Kiểm soát hướng**: Xác định hướng xuất phát của các yêu cầu dịch vụ cụ thể và cho phép đi qua firewall thành luồng có kiểm soát.
- **Kiểm soát người dùng**: Kiểm soát việc truy xuất tới một dịch vụ mà một người dùng đang thi hành.
- **Kiểm soát ứng xử**: Kiểm soát cách thức mà các dịch vụ cụ thể được sử dụng. Ví dụ, firewall có thể lọc e-mail để loại trừ spam, hoặc chỉ cho phép các truy xuất từ bên ngoài đến được các vị trí cụ thể trong một server Web cục bộ

# Các hạn chế của firewall

1. Firewall không thể bảo vệ trước các tấn công đường vòng. Ví dụ, nếu hệ thống nội mạng kết nối ra ngoài bằng quay số trực tiếp tới một ISP (không đi qua firewall), thì firewall không thể bảo vệ được.
2. Firewall không thể bảo vệ trước các nguy cơ nội bộ, chẳng hạn một nhân viên bất mãn hay một nhân viên hai mặt, thông đồng với kẻ tấn công.

3. Firewall không thể bảo vệ trước các phiên truyền tập tin hay chương trình nhiễm virus, do các bộ lọc của firewall chủ yếu chỉ kiểm tra phần header của gói tin, chứ không kiểm tra phần data. Việc kiểm tra phần data của gói tin đòi hỏi chi phí thời gian rất lớn, làm chậm tốc độ hệ thống.

# Ba loại firewall cơ bản

- Bộ lọc gói tin (packet-filtering router)
- Cổng ứng dụng (application-level gateway hay proxy server)
- Cổng nối (circuit level gateway)

*Một firewall thực tế có thể bao gồm một hoặc nhiều chức năng của 3 loại firewall cơ bản nói trên*

# Bộ lọc gói tin

*Một bộ lọc gói tin áp dụng một tập quy tắc đối với từng gói tin IP vào/ra mạng để quyết định sẽ chuyển tiếp hoặc hủy bỏ nó. Các quy tắc lọc được dựa trên các thông tin chứa trong mỗi gói tin như:*

- Địa chỉ IP nguồn
- Địa chỉ IP đích
- Loại giao thức chuyển vận (ví dụ, TCP hay UDP)
- Số hiệu cổng ở tầng chuyển vận, số hiệu này xác định các ứng dụng như SNMP hay TELNET.

...

# Cổng ứng dụng

- Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng.
- Cơ chế hoạt động của nó dựa trên Proxy service. Proxy service là các bộ code đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall.

# Cổng nối

- Cổng nối là một chức năng đặc biệt có thể thực hiện được bởi một cổng ứng dụng. Cổng nối đơn giản chỉ chuyển tiếp các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.
- Cổng nối làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong và các kết nối bên ngoài. Vì sự kết nối này xuất hiện từ hệ thống firewall, nó giúp che dấu thông tin về mạng nội bộ.
- Cổng nối thường được sử dụng cho những kết nối ra ngoài, nơi mà các quản trị mạng thật sự tin tưởng những người dùng bên trong

# *Hết Phần 5*