HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Chương 5. Những vấn đề về an toàn thông tin, tội phạm tin học và tác chiến mạng

Học phần: LẬP TRÌNH CƠ BẢN

Tài liệu tham khảo

- **An ninh hệ thống mạng máy tính**, Chương 1, Nguyễn Hiếu Minh (Chủ biên), Nhà xuất bản QĐND, 2013.
- **Network Security Foundations**, Chương 1, 2, 4, 8, Matthew Schebe, 333p, 2004.
- **Network Security Bible**, Phần 1, 3, 5, Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, 697p, 2005.
- **Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network**, Chương 2, 7, 670p.
- **Cryptography and Network Security**, phần 6 chương 21

Mục tiêu của bài học

1. Tổng quan về an toàn thông tin
2. Mục tiêu của an toàn thông tin
3. Các loại hình tấn công và nguy cơ mất ATTT hiện nay
4. Giải pháp đảm bảo an toàn thông tin.
5. Cơ bản về tác chiến mạng
6. Pháp luật về an toàn thông tin
7. Tin tặc, tội phạm kỹ thuật
8. Một số tội phạm tin học liên quan đến lạm dụng Internet với mục đích xấu
9. Vấn đề sở hữu trí tuệ và bản quyền
10. Luật tội phạm tin học ở Việt Nam
11. Các phần mềm độc hại

1. Tổng quan về an toàn thông tin

- **An toàn thông tin mạng:** ATTTM là sự bảo vệ hệ thống thông tin và thông tin truyền đưa trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin (theo định nghĩa trong Luật An toàn thông tin mạng – 19/11/2015).

Tổng quan về an toàn thông tin (tiếp)

- Mục tiêu hướng tới của ATTT là bảo vệ các tài sản thông tin. Tuy nhiên, các sản phẩm và hệ thống thường luôn tồn tại những điểm yếu dẫn đến những rủi ro có thể xảy ra.
- Các đối tượng tấn công (tin tặc) có chủ tâm đánh cắp, lợi dụng hoặc phá hoại tài sản của các chủ sở hữu, tìm cách khai thác các điểm yếu để tấn công, tạo ra các nguy cơ và các rủi ro cho các hệ thống thông tin.

Tổng quan về an toàn thông tin (tiếp)

- **Đảm bảo ATTT** là đảm bảo an toàn kỹ thuật cho hoạt động của các cơ sở HTTT, trong đó bao gồm đảm bảo an toàn cho cả phần cứng và phần mềm hoạt động theo các tiêu chuẩn kỹ thuật do nhà nước ban hành; ngăn ngừa khả năng lợi dụng mạng và các cơ sở HTTT để thực hiện các hành vi trái phép; đảm bảo các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng.

Tổng quan về an toàn thông tin (tiếp)

- Với các biện pháp đảm bảo ATTT người dùng có được công cụ trong tay để nhận thức được các điểm yếu, giảm thiểu các điểm yếu, ngăn chặn các nguy cơ tấn công, làm giảm các yếu tố rủi ro.
- Như vậy, các biện pháp và kỹ thuật đảm bảo ATTT chính là mang lại sự tin cậy cho các sản phẩm và hệ thống thông tin.

Tổng quan về an toàn thông tin (tiếp)

- Vào hai thập niên cuối của thế kỷ 20, sự giải thích thuật ngữ *ATTT* (*information security*) đã có hai sự thay đổi quan trọng. Trước khi có sự phổ biến rộng rãi của các thiết bị tự động xử lý số liệu, các biện pháp bảo vệ an toàn thông tin mà các tổ chức thực hiện thường dựa trên:
- Các giải pháp vật lý;
- Các giải pháp hành chính.

Tổng quan về an toàn thông tin (tiếp)

- Các giải pháp vật lý – như bổ sung thêm các khóa cho các két sắt trong đó có lưu giữ các tài liệu quan trọng.
- Các giải pháp hành chính – kiểm tra hồ sơ của các cá nhân khi thu nhận vào làm việc.

Tổng quan về an toàn thông tin (tiếp)

- Với sự phát triển và phổ biến rộng rãi của của máy tính đã xuất hiện yêu cầu về các phương pháp tự động bảo vệ các máy tính.
- Vì thế để mô tả tổng hợp các phương pháp và phương tiện dùng để bảo vệ thông tin chống lại các hành động vi phạm, đã sử dụng thuật ngữ *an toàn máy tính* (*computer security*).

Tổng quan về an toàn thông tin (tiếp)

- Sự thay đổi lớn thứ hai, xuất hiện do sự hình thành các xu thế mới về ATTT, chúng là kết quả của sự xuất hiện các hệ thống xử lý dữ liệu phân tán và các trung tâm chuyển mạch dùng để trao đổi dữ liệu giữa các các người sử dụng đầu cuối và các máy tính trung tâm.
- Trong mối liên hệ này đã xuất hiện thuật ngữ *an toàn mạng* (*network security*), được hiểu không chỉ cho một mạng cục bộ riêng lẻ mà cho cả một tổ hợp các mạng (mạng internet).

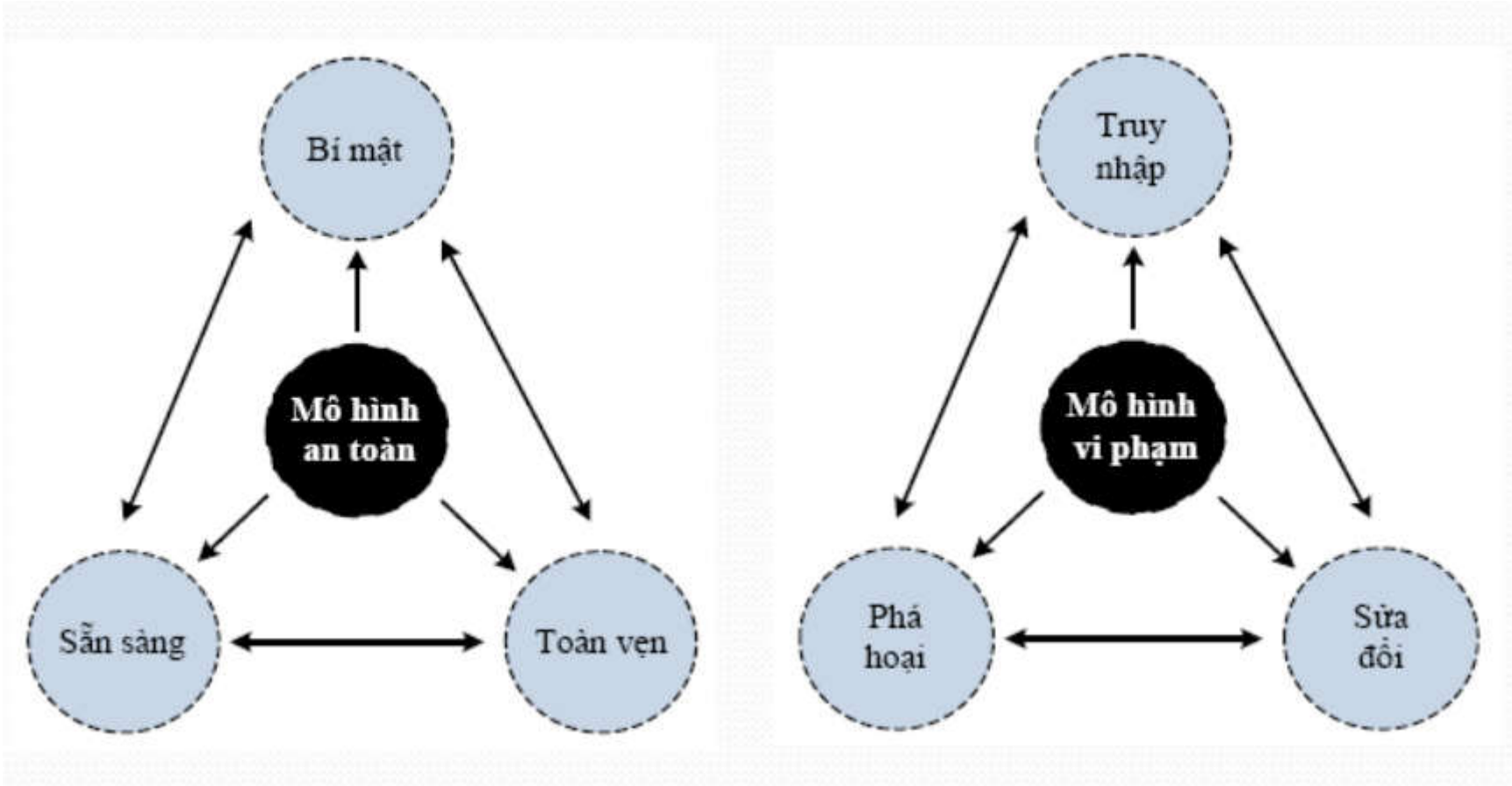
Tổng quan về an toàn thông tin (tiếp)

- ATTT là một trong những lĩnh vực hiện đang rất được quan tâm. Một khi internet ra đời và phát triển thì nhu cầu trao đổi thông tin đã trở nên cần thiết và phát triển không ngừng.
- Mục tiêu của việc nối mạng là để cho mọi người có thể dùng chung và trao đổi tài nguyên từ những vị trí địa lý khác nhau. Cũng chính vì vậy mà tài nguyên sẽ bị phân tán, dẫn đến một điều hiển nhiên là chúng sẽ dễ bị xâm phạm. Càng giao thiệp nhiều thì càng dễ bị tấn công, đó là một quy luật. ***Từ đó, vấn đề ATTT cũng xuất hiện.***

Tổng quan về an toàn thông tin (tiếp)

- ATTT nhằm đảm bảo 3 đặc điểm quan trọng nhất của thông tin (hình 1), đó là:
  - tính bí mật;
  - tính toàn vẹn;
  - tính sẵn sàng.
- Ba nguyên tắc này là tiêu chuẩn cho tất cả các hệ thống an ninh
- Tùy thuộc vào ứng dụng và hoàn cảnh cụ thể, mà một trong ba nguyên tắc nãy sẽ quan trọng hơn những cái khác

2. Các mục tiêu của ATTT



Mô hình CIA

Tính bí mật

Bí mật là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. Đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhạy cảm đó được che giấu với người dùng không được cấp phép.

Tính bí mật(tiếp)

- Một giải pháp đảm bảo an toàn là xác định quyền được truy cập đối với thông tin đang tìm kiếm, đối với một số lượng người sử dụng nhất định và một số lượng thông tin là tài sản nhất định. Trong trường hợp kiểm soát truy cập, nhóm người truy cập sẽ được kiểm soát xem họ đã truy cập những dữ liệu nào. Tính bí mật là sự đảm bảo rằng các chức năng kiểm soát truy cập có hiệu lực.
- Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất

Tính toàn vẹn

- Toàn vẹn là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó đảm bảo được sự chính xác của thông tin và hệ thống.
- Có ba mục đích chính của việc đảm bảo tính toàn vẹn:
  - Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.
  - Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chủ tâm của những người sử dụng được phép.
  - Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

Tính sẵn sàng

- Tính sẵn sàng của thông tin cũng là một đặc tính rất quan trọng.
- Tính sẵn sàng bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và tới mạng.

Tính sẵn sàng

- Tính sẵn sàng đảm bảo độ ổn định đáng tin cậy của thông tin, cũng như đảm nhiệm chức năng là thước đo, xác định phạm vi tới hạn an toàn của một hệ thống thông tin.

3. Các loại hình tấn công và nguy cơ mất ATTT

A. ĐỊNH NGHĨA

- ✓ Hiện nay vẫn chưa có định nghĩa chính xác về thuật ngữ "tấn công" (xâm nhập, công kích). Mỗi chuyên gia trong lĩnh vực ATTT luận giải thuật ngữ này theo ý hiểu của mình.
- ✓ Xâm phạm an toàn thông tin mạng là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin và hệ thống thông tin (Luật ATTTM – 19/11/2015).

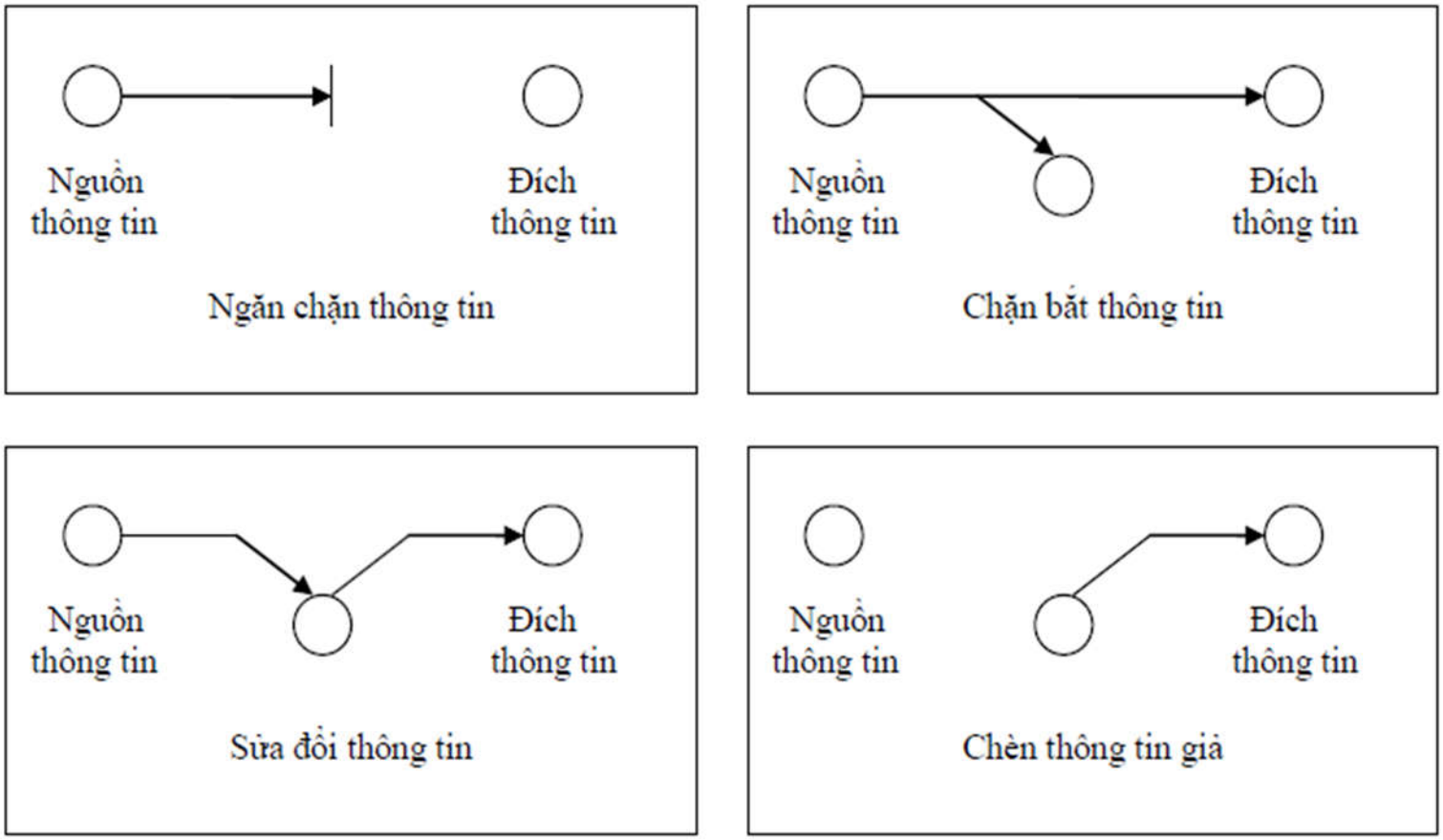
Các loại hình tấn công

- **Định nghĩa chung**: Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.

Các loại hình tấn công (tiếp)

- Tấn công HTTT là các tác động hoặc là trình tự liên kết giữa các tác động với nhau để phá huỷ, dẫn đến việc hiện thực hoá các nguy cơ bằng cách lợi dụng đặc tính dễ bị tổn thương của các hệ thống thông tin này.
  - Nghĩa là, nếu có thể bài trừ nguy cơ tổn thương (lỗ hổng) của các hệ thống thông tin chính là trừ bỏ khả năng có thể thực hiện tấn công.

Các loại hình tấn công (tiếp)



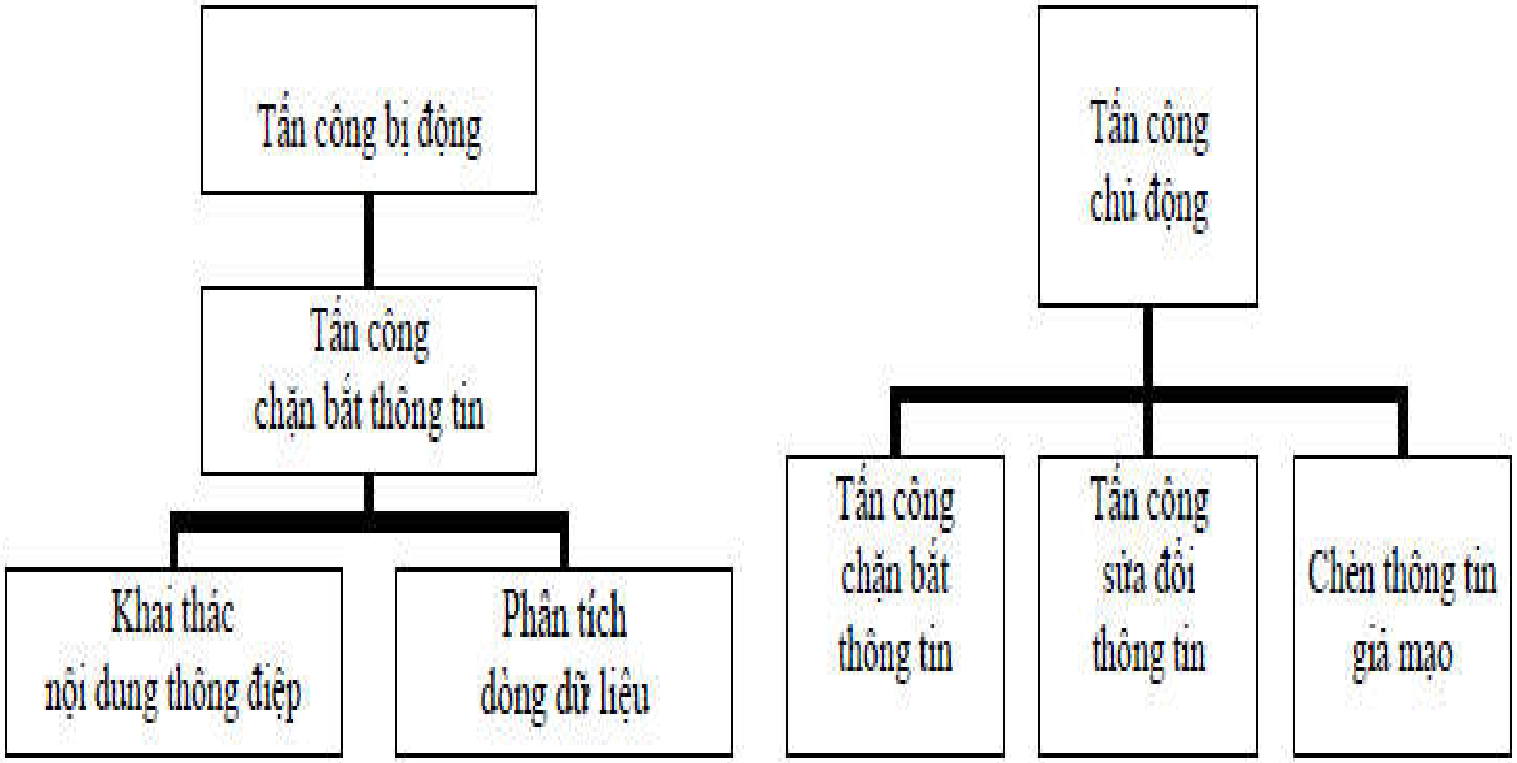
Các loại hình tấn công (tiếp)

- **Tấn công ngăn chặn thông tin (interruption)**
  - Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- **Tấn công chặn bắt thông tin (interception)**
  - Kẻ tấn công có thể truy nhập tới tài nguyên thông tin. Đây là hình thức tấn công vào tính bí mật của thông tin.

Các loại hình tấn công (tiếp)

- **Tấn công sửa đổi thông tin (Modification)**
  - Kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng.
  - Đây là hình thức tấn công vào tính toàn vẹn của thông tin.
- **Chèn thông tin giả mạo (Fabrication)**
  - Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống.
  - Đây là hình thức tấn công vào tính xác thực của thông tin.

Tấn công bị động và chủ động (Tự học)



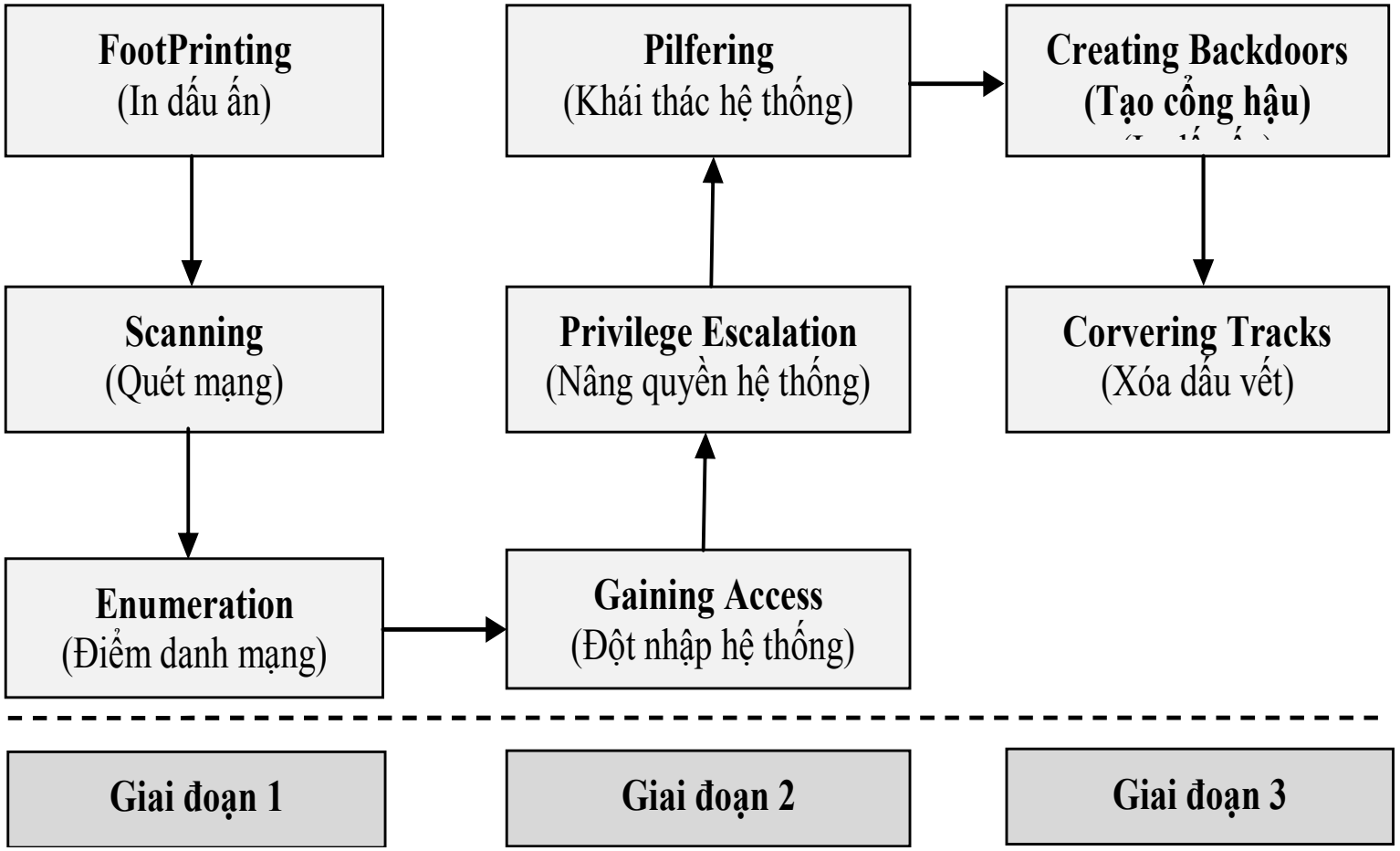
Tấn công bị động (passive attacks)

- Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.
- Có hai kiểu tấn công bị động là **khai thác nội dung thông điệp** và **phân tích dòng dữ liệu**.
- Tấn công bị động rất khó bị phát hiện vì nó không làm thay đổi dữ liệu và không để lại dấu vết rõ ràng. Biện pháp hữu hiệu để chống lại kiểu tấn công này là ngăn chặn (đối với kiểu tấn công này, ngăn chặn tốt hơn là phát hiện).

Tấn công chủ động (active attacks)

- Tấn công chủ động được chia thành 4 loại sau:
  - **Giả mạo** (Masquerade): Một thực thể (người dùng, máy tính, chương trình…) đóng giả thực thể khác.
  - **Dùng lại** (replay): Chặn bắt các thông điệp và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
  - **Sửa thông điệp** (Modification of messages): Thông điệp bị sửa đổi hoặc bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.
  - **Từ chối dịch vụ** (Denial of Service - DoS): Ngăn cấm việc sử dụng bình thường hoặc làm cho truyền thông ngừng hoạt động.

Các bước tấn công mạng



Một số kỹ thuật tấn công mạng

1) Tấn công thăm dò.
2) Tấn công sử dụng mã độc.
3) Tấn công xâm nhập.
4) Tấn công từ chối dịch vụ.
5) Tấn công sử dụng kỹ nghệ xã hội

Tấn công thăm dò

- Thăm dò là việc thu thập thông tin trái phép về tài nguyên, các lỗ hổng hoặc dịch vụ của hệ thống.
- Tấn công thăm dò thường bao gồm các hình thức:
  - Sniffing
  - Ping Sweep
  - Ports Scanning

Tấn công từ chối dịch vụ (Denial of Service)

- Về cơ bản, tấn công từ chối dịch vụ là tên gọi chung của kiểu tấn công làm cho một hệ thống nào đó bị quá tải không thể cung cấp dịch vụ, gây ra gián đoạn hoạt động hoặc làm cho hệ thống ngừng hoạt động.

Tấn công từ chối dịch vụ (Denial of Service)

- Tùy theo phương thức thực hiện mà nó được biết dưới nhiều tên gọi khác nhau.
- Khởi thủy là lợi dụng sự yếu kém của giao thức TCP (Transmision Control Protocol) để thực hiện tấn công từ chối dịch vụ DoS (Denial of Service), mới hơn là tấn công từ chối dịch vụ phân tán DDoS (Distributed DoS), mới nhất là tấn công từ chối dịch vụ theo phương pháp phản xạ DRDoS (Distributed Reflection DoS).

Tấn công sử dụng mã độc (malicious code)

- **Khái niệm:** Mã độc là những chương trình khi được khởi chạy có khả năng phá hủy hệ thống, bao gồm Virus, sâu (Worm) và Trojan, ...
- Tấn công bằng mã độc có thể làm cho hệ thống hoặc các thành phần của hệ thống hoạt động sai lệch hoặc có thể bị phá hủy.

Tấn công xâm nhập (Intrusion attack)

- Là hình thức tấn công, nhằm truy nhập bất hợp pháp vào các HTTT.
- Kiểu tấn công này được thực hiện với mục đích đánh cắp dữ liệu hoặc thực hiện phá hủy bên trong HTTT.

Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

- Là một nhóm các phương pháp được sử dụng để đánh lừa người sử dụng tiết lộ các thông tin bí mật.
- Là phương pháp tấn công phi kỹ thuật, dựa trên sự thiếu hiểu biết của người dùng để lừa gạt họ cung cấp các thông tin nhạy cảm như password hay các thông tin quan trọng khác.

Xu hướng tấn công HTTT

1. Sử dụng các công cụ tấn công tự động

- Những kẻ tấn công sẽ sử dụng các công cụ tấn công tự động có khả năng thu thập thông tin từ hàng nghìn địa chỉ trên Internet một cách nhanh chóng, dễ dàng và hoàn toàn tự động.
- Các HTTT có thể bị quét từ một địa điểm từ xa để phát hiện ra những địa chỉ có mức độ bảo mật thấp. Thông tin này có thể được lưu trữ, chia sẻ hoặc sử dụng với mục đích bất hợp pháp.

Xu hướng tấn công HTTT (tiếp)

2. Sử dụng các công cụ tấn công khó phát hiện

- Một số cuộc tấn công được dựa trên các mẫu tấn công mới, không bị phát hiện bởi các chương trình bảo mật, các công cụ này có thể có tính năng đa hình, siêu đa hình cho phép chúng thay đổi hình dạng sau mỗi lần sử dụng.

Xu hướng tấn công HTTT (tiếp)

3. Phát hiện nhanh các lỗ hổng bảo mật

- Thông qua các lỗ hổng bảo mật của hệ thống, phần mềm kẻ tấn công khai thác các lỗ hổng này để thực hiện các cuộc tấn công.
- Hàng năm, nhiều lỗ hổng bảo mật được phát hiện và công bố, tuy nhiên điều này cũng gây khó khăn cho các nhà quản trị hệ thống để luôn cập nhật kịp thời các bản vá. Đây cũng chính là điểm yếu mà kẻ tấn công tận dụng để thực hiện các hành vi tấn công, xâm nhập bất hợp pháp.

Xu hướng tấn công HTTT (tiếp)

4. Tấn công bất đối xứng và tấn công diện rộng

- Tấn công bất đối xứng xảy ra khi bên tấn công mạnh hơn nhiều so với đối tượng bị tấn công.
- Tấn công diện rộng thực hiện khi kẻ tấn công tạo ra một mạng lưới kết hợp các hoạt động tấn công.

Xu hướng tấn công HTTT (tiếp)

- 5. *Thay đổi mục đích tấn công*
- Thời gian trước, các tấn công chỉ từ mục đích thử nghiệm, hoặc khám phá hệ thống an ninh.
- Hiện nay, mục đích tấn công với nhiều lý do khác nhau như về tài chính, giả mạo thông tin, phá hủy, và đặc biệt nguy hiểm đó là mục đích chính trị, chính vì vậy mà độ phức tạp của các cuộc tấn công đã tăng lên và tác hại lớn hơn rất nhiều so với trước đây.

Các nguy cơ mất ATTT

- ***Cơ sở hạ tầng mạng***: Cơ sở hạ tầng không đồng bộ, không đảm bảo yêu cầu thông tin được truyền trong hệ thống an toàn và thông suốt.
- ***Thông tin*:** Dữ liệu chưa được mô hình hóa và chuẩn hóa theo tiêu chuẩn về mặt tổ chức và mặt kỹ thuật. Yếu tố pháp lý chưa được trú trọng trong truyền đưa các dữ liệu trên mạng, nghĩa là các dữ liệu được truyền đi trên mạng phải đảm bảo tính hợp pháp về mặt tổ chức và mặt kỹ thuật.

Các nguy cơ mất ATTT (tiếp)

- ***Công nghệ***: Chưa chuẩn hóa cho các loại công nghệ, mô hình kiến trúc tham chiếu nhằm đảm bảo cho tính tương hợp, tính sử dụng lại được, tính mở, an ninh, mở rộng theo phạm vi, tính riêng tư vào trong HTTT.
- ***Con người*****:** Sự hiểu biết của những người trực tiếp quản lý, vận hành các HTTT, xây dựng và phát triển hệ thống phần mềm, hệ thống thông tin còn chưa đồng đều và chưa theo quy chuẩn của các cơ quan tổ chức đó.

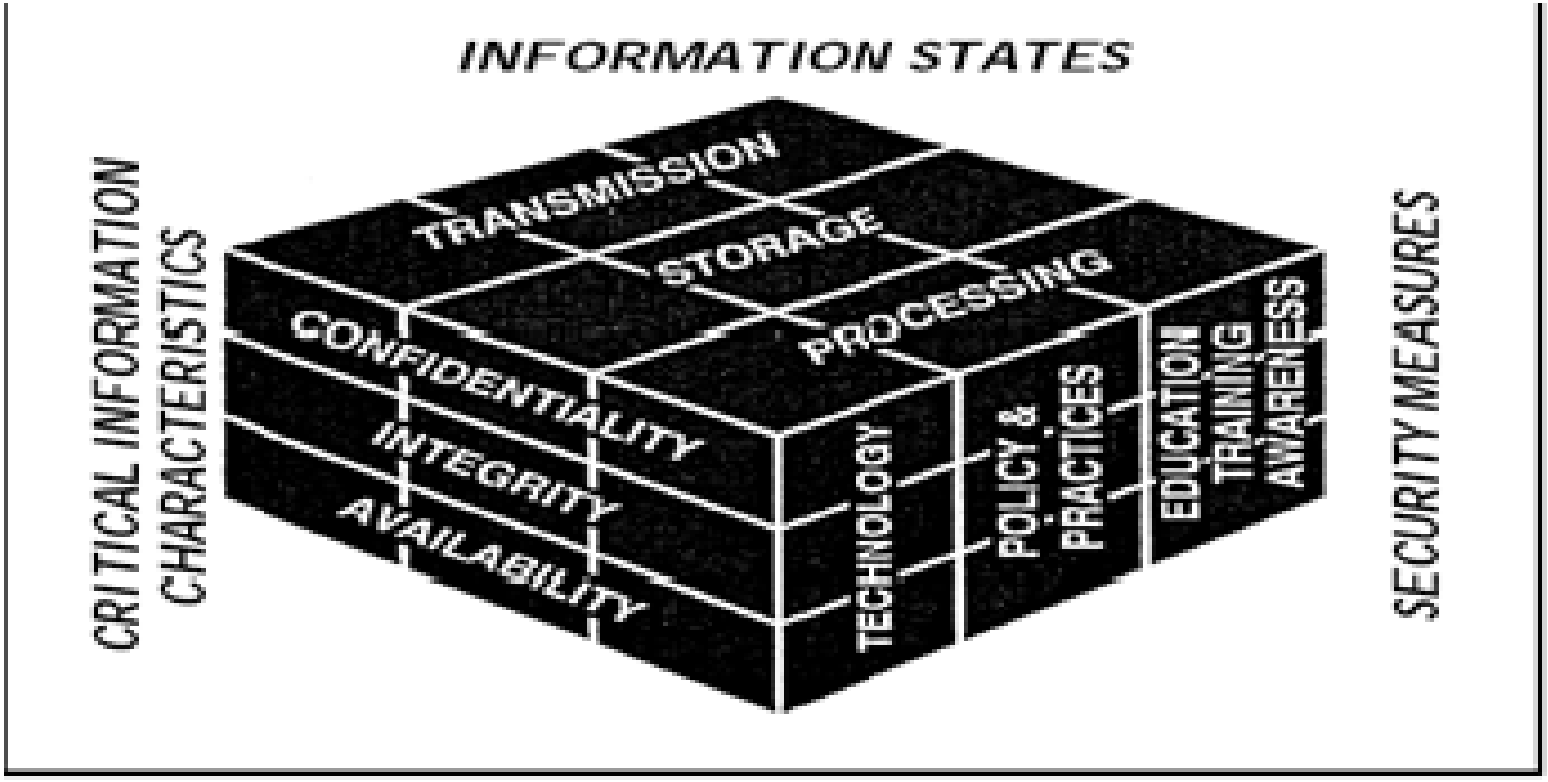
Các nguy cơ mất ATTT (tiếp)

- ***Quy trình, quản lý***:
- Chưa chuẩn hóa qui trình nghiệp vụ trong vận hành HTTT.
- Chưa chuẩn hóa các thủ tục hành chính, các qui định pháp lý trong việc đảm bảo ATTT.
- Tổ chức quản lý thay đổi hệ thống, ứng dụng chưa đúng cách, chưa chuẩn hóa và có chế tài mang tính bắt buộc thực hiện.
- Như vậy để đảm bảo ATTT thì các cơ quan tổ chức phải làm tốt và hạn chế tối đa 5 yếu tố trên.

4. Giải pháp đảm bảo an toàn thông tin

- Bộ ba các đặc tính then chốt của thông tin đề cập đến ở trên bao trùm toàn bộ các mặt của việc đảm bảo an toàn thông tin.
- Một ma trận được tạo nên bởi 3 yếu tố là 3 trạng thái của thông tin (truyền dẫn, lưu giữ, xử lí) được minh họa ở trục hoành (hình 2).

Hình 2
Mô hình tổng quát về an toàn thông tin



Giải pháp đảm bảo an toàn thông tin (tiếp)

- Ba đặc tính then chốt của thông tin (tính bí mật, tính toàn vẹn, tính sẵn sàng) được minh họa trên trục tung có thể được sử dụng làm nền tảng cho mô hình thể hiện các biện pháp an toàn thông tin (hình 2).

Giải pháp đảm bảo an toàn thông tin (tiếp)

- Các biện pháp ATHTTT được phân loại thành 3 lớp như sau, tạo thành chiều thứ 3 của không gian ma trận:
- **Các biện pháp công nghệ (Technology):** Bao hàm tất cả các biện pháp phần cứng, các phần mềm, phần sụn cũng như các kỹ thuật công nghệ liên quan được áp dụng nhằm đảm các yêu cầu an toàn của thông tin trong các trạng thái của nó.

Giải pháp đảm bảo an toàn thông tin (tiếp)

- **Các biện pháp về chính sách và tổ chức (Policy & Practices):** Đưa ra các chính sách, quy định, phương thức thực thi.
- Thực tế cho thấy, ATTT không chỉ đơn thuần là vấn đề thuộc phạm trù công nghệ, kỹ thuật. Hệ thống chính sách và kiến trúc tổ chức đóng một vai trò hữu hiệu trong việc đảm bảo an toàn thông tin.

Giải pháp đảm bảo an toàn thông tin (tiếp)

- **Các biện pháp về đào tạo, tập huấn, nâng cao nhận thức (Education, training & Awarenness):** Các biện pháp công nghệ hay các biện pháp về tổ chức thích hợp phải dựa trên các biện pháp đào tạo, tập huấn và tăng cường nhận thức để có thể triển khai đảm bảo an toàn thông tin từ nhiều hướng khác nhau.

Giải pháp đảm bảo an toàn thông tin (tiếp)

- Các nhà nghiên cứu và các kỹ sư cũng cần phải hiểu rõ các nguyên lý an toàn hệ thống thông tin, thì mới mong các sản phẩm và hệ thống do họ làm ra đáp ứng được các nhu cầu về an toàn thông tin của cuộc sống hiện tại đặt ra.

Giải pháp đảm bảo an toàn thông tin (tiếp)

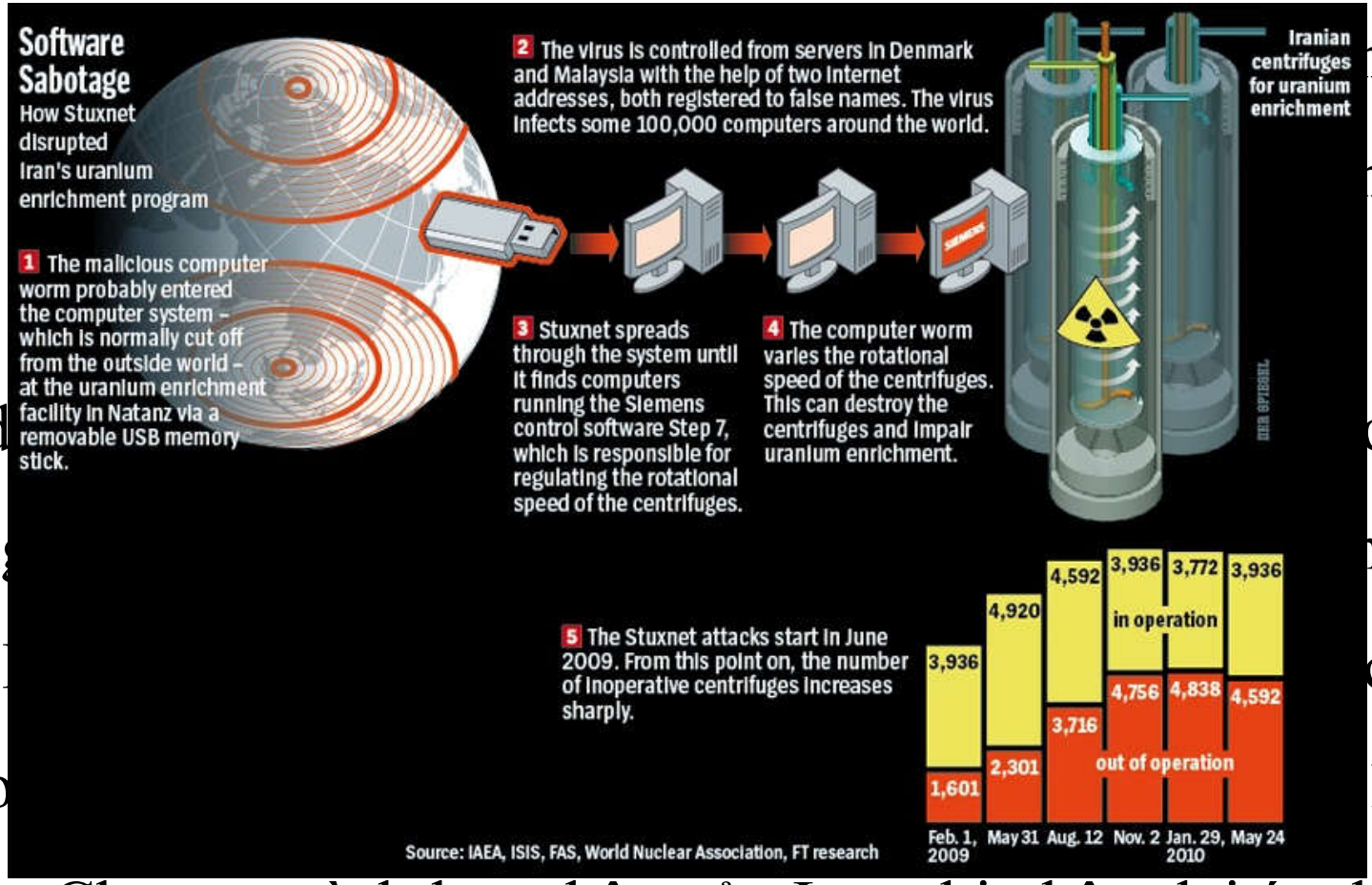
- ***Biện pháp hợp tác quốc tế***
- Hợp tác với các quốc gia có kinh nghiệm, kế thừa những thành tựu khoa học của các quốc gia đi trước trong vấn đề đảm bảo ATTT.
- Xây dựng các quy chế phối hợp với các cơ quan tổ chức quốc tế trong ứng phó các sự cố về ATTT.

5. Cơ bản về tác chiến mạng

- Tác chiến mạng (tác chiến không gian mạng) là hành vi các bên tham chiến sử dụng mạng Internet hoặc các mạng khác để thu thập, phá hoại thông tin trong hệ thống tổ chức, chỉ huy, điều khiển, hệ thống vũ khí… của nhau.
- Là phương thức tác chiến "không tiếng súng" trên cơ sở công nghệ thông tin mà các bên có thể tác chiến trong điều kiện không nhìn thấy nhau.

5. Cơ bản về tác chiến mạng

- Đặc hông chịu hông gian
- Ví d o hệ thốn nium của c vụ chươ hoạt động. Chương trình hạt nhân của I-ran bị chậm lại ít nhất 2 năm.



Cơ bản về tác chiến mạng (tiếp)

- Đối tượng của TCM là thông tin trên mạng máy tính, các quá trình vận hành trên mạng máy tính, cơ sở hạ tầng mạng máy tính.
- Nhiệm vụ của TCM là gây trở ngại hoặc làm mất khả năng chỉ huy, phối hợp các lực lượng, điều khiển vũ khí, phá hủy vật lý cơ sở hạ tầng đảm bảo cho các khả năng đó của đối phương, trong khi bảo vệ các khả năng đó của quân mình.

Cơ bản về tác chiến mạng (tiếp)

- Các hoạt động của tác chiến mạng bao gồm cả **tấn công** và **phòng thủ**.
- **Tấn công mạng máy tính** là các hoạt động phá vỡ tổ chức thông tin, ngăn cản truy cập và cung cấp thông tin, làm suy giảm khả năng hay phá hủy thông tin lưu trong các máy tính và lưu trong các mạng máy tính, hoặc phá hoại chính các máy tính và các mạng máy tính.
- Sử dụng các phương pháp xâm nhập là để lấy trộm các số liệu của đối phương cho phép quân nhà có quyết định chính xác hơn, sửa đổi cơ sở dữ liệu của địch làm cho chúng có những quyết định sai lầm, làm cho mạng của địch bị treo không thể truy cập được.
- Sử dụng virus để tấn công mạng làm cho đối phương sử dụng không hiệu quả các phương tiện thông tin liên lạc và xử lý thông tin, làm chậm quá trình suy luận và ra quyết định của đối phương, có thể bí mật lập trình lại các máy tính của đối phương nhằm phá hỏng các quá trình mà các máy tính đó điều khiển.

Cơ bản về tác chiến mạng (tiếp)

- Các hoạt động của tác chiến mạng bao gồm cả **tấn công** và **phòng thủ**.
- **Phòng thủ mạng** là các hoạt động phát hiện các cuộc tấn công mạng, ngăn chặn các cuộc xâm nhập trái phép vào các tài nguyên mạng, bảo vệ thông tin, các cơ sở dữ liệu, bảo vệ các chương trình phần mềm chạy trên mạng, bảo vệ các thiết bị, cơ sở hạ tầng của mạng, khôi phục nhanh chóng hoạt động bình thường của mạng do ảnh hưởng của các đợt tấn công mạng từ phía địch.

Cơ bản về tác chiến mạng (tiếp) - Chiến tranh thông tin

- Trong chiến tranh, ưu thế thông tin chính là ưu thế trong hoạt động tác chiến. Ưu thế thông tin có được từ việc tăng cường thu thập, xử lý, phân tích thông tin nhận được làm cơ sở ra quyết định đúng, đồng thời truyền đạt thông tin về quyết định đó đến các cơ quan, đơn vị cũng như điều khiển tổ hợp vũ khí khí tài (tự động hóa) một cách kịp thời, chính xác, bí mật, an toàn. Do vậy, ưu thế thông tin của ta chính là bất lợi cho đối phương, từ đó, khái niệm về "chiến tranh thông tin" ra đời.
- Chiến tranh thông tin là một phương thức tiến hành chiến tranh, gồm tổng thể các hoạt động nhằm giành quyền làm chủ (kiểm soát và điều khiển) thông tin giữa các bên tham chiến. Bản chất của chiến tranh thông tin là sử dụng thông tin để đánh vào thông tin. Chiến tranh thông tin gồm 3 thành phần chính đó là chiến tranh tâm lý, tác chiến điện tử và tác chiến KGM (KGM)

Cơ bản về tác chiến mạng (tiếp) - Tác chiến không gian mạng (KGM)

Một số khai niệm

- + *KGM* là không gian bao gồm các thành phần vật chất và phi vật chất được đặc trưng bởi việc sử dụng máy tính và các phổ điện từ, để tạo lập, lưu trữ, xử lý, chuyển nhận và hiển thị thông tin qua mạng.
- + *Tác chiến KGM*: Là các hoạt động trinh sát, giám sát, phòng thủ, tiến công của lực lượng tác chiến KGM.
- + *Đối tượng tác chiến KGM*: Đối tượng tác chiến KGM (đối phương) là các quốc gia, vùng lãnh thổ, tổ chức, cá nhân có âm mưu và hành động xâm nhập, phá hoại chủ quyền của nước ta trên KGM.

Cơ bản về tác chiến mạng (tiếp) - Tác chiến không gian mạng (KGM)

- Các hình thức tác chiến KGM:

- + *Trinh sát KGM:* Là hoạt động nhằm thu thập, nghiên cứu về hạ tầng mạng và các thông tin trên KGM đối phương nhằm phục vụ hoạt động tác chiến KGM và bảo vệ chủ quyền quốc gia trên KGM.
- + *Phòng thủ KGM:* Là hoạt động triển khai các giải pháp tổ chức, kỹ thuật nhằm bảo vệ chủ quyền quốc gia trên KGM trước các cuộc xâm nhập, tiến công của đối phương.
- + *Tiến công trên KGM:* Là hành động đáp trả lại các hoạt động tiến công có chủ đích của đối phương nhằm vào chủ quyền quốc gia trên KGM.

Hiện nay, KGM đã thực sự trở thành hoạt động tác chiến thứ năm sau các hoạt động tác chiến trên bộ, trên biển, trên không và trên vũ trụ. Nhiều quốc gia coi nguy cơ tấn công từ KGM là một trong những nguy cơ lớn, quan trọng hàng đầu đối với an ninh quốc gia.

Cơ bản về tác chiến mạng (tiếp) (tự đọc)

- Một số số liệu công khai:

- Ngày 21-5-2010, Bộ trưởng Quốc phòng Mỹ Robert Gates chính thức trao quyết định bổ nhiệm tướng K.Alexander, Cục trưởng Cục An ninh quốc gia kiêm nhiệm chức Tư lệnh, Bộ tư lệnh Tác chiến mạng quân đội Mỹ. Sự kiện này đánh dấu việc Bộ tư lệnh Tác chiến mạng quân đội Mỹ, một cơ quan được thai nghén từ lâu, nay chính thức đi vào hoạt động.
- Năm 2012, Hàn Quốc thành lập một Bộ tư lệnh Tác chiến mạng độc lập để đối phó với mối đe dọa tấn công các mạng máy tính quốc phòng của họ ngày một tăng. Hàn Quốc cho biết Triều Tiên đã thành lập một đơn vị đặc biệt gồm 3.000 hacker xuất sắc dưới sự kiểm soát trực tiếp của nhà lãnh đạo Kim Jong-Un và đánh giá "Triều Tiên là quốc gia mạnh thứ ba trên thế giới về chiến tranh không gian mạng sau Nga và Mỹ"

Cơ bản về tác chiến mạng (tiếp) (tự đọc)

- Một số số liệu công khai:

- Từ một thập kỷ nay, Trung Quốc đã chính thức thành lập lực lượng đặc nhiệm mạng, là lực lượng tác chiến mạng chuyên trách của quân đội Trung Quốc. Trung Quốc cũng đã phát triển chiến lược "Tác chiến điện tử mạng tích hợp-INEW"- một học thuyết quân sự tích hợp tác chiến điện tử và hoạt động mạng máy tính. Ngoài ra quân đội Trung Quốc cũng thành lập các đơn vị dân quân tại các quân khu có chức năng tiến hành chiến tranh thông tin, trong đó có thực hiện nhiệm vụ tác chiến mạng.
- Israel đã áp dụng nhiều tiến bộ công nghệ dân sự của mình để tăng cường khả năng chiến tranh mạng vì "sử dụng mạng lưới máy tính gián điệp có vai trò quan trọng trong tác chiến hiện đại giống như yểm trợ không quân trong tác chiến thế kỷ 20". Đây cũng là lần đầu tiên giới chức quân sự nước này công khai về chương trình bí mật cho lực lượng tác chiến mạng.

6. Pháp luật về an toàn thông tin

- Với việc kết nối máy tính vào mạng, con người có thể mở rộng phạm vi hoạt động của mình thì điều đó cũng có nghĩa là những tác hại có thể được nhân lên qua mạng. Vì thế trong một xã hội "nối mạng", mọi cá nhân phải nhận thức được trách nhiệm với cộng đồng.
- Pháp luật về ATTT là các quy định, nghị định, chính sách nhằm đưa ra các yêu cầu và luật về đảm bảo ATTT.

Pháp luật về an toàn thông tin (tiếp)

- Ngày 19/11/2015, Quốc hội nước CHXHCN Việt Nam thông qua luật ATTT mạng.
- Luật ATTT mạng quy định về hoạt động an toàn thông tin mạng, quyền và trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng.

Pháp luật về an toàn thông tin (tiếp)

- Trong đó, an toàn thông tin mạng được hiểu là sự bảo vệ hệ thống thông tin và thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.
- Các nội dung chính: Bảo đảm an toàn thông tin mạng (Bảo vệ thông tin mạng, Bảo vệ thông tin cá nhân, Bảo vệ hệ thống thông tin, Ngăn chặn xung đột thông tin trên mạng), Phát triển nguồn nhân lực an toàn thông tin mạng…

7. Tin tặc, tội phạm kỹ thuật

- Tin tặc (Hacker): Là một người hay nhóm người sử dụng sự hiểu biết của mình về cấu trúc máy tính, hệ điều hành, mạng, các ứng dụng trong cơ sở HTTT ... để tìm lỗi, lỗ hỗng, điểm yếu an toàn của nó và tìm cách xâm nhập, thay đổi hay chỉnh sửa HTTT với mục đích tốt xấu khác nhau.

Tin tặc, tội phạm kỹ thuật (tiếp)

- **Có hai loại Hacker:**
- **Hacker mũ trắng** là những người mà hành động tấn công, xâm nhập và thay đổi, chỉnh sửa hệ thống phần cứng, phần mềm với mục đích tìm ra các lỗi, lỗ hổng, điểm yếu bảo mật và đưa ra giải pháp ngăn chặn và bảo vệ hệ thống chẳng hạn như những nhà phân tích An ninh mạng.

Tin tặc, tội phạm kỹ thuật (tiếp)

- **Hacker mũ đen** là những người mà hành động tấn công, xâm nhập, thay đổi, chỉnh sửa hệ thống phần cứng, phần mềm với mục đích phá hoại, hoặc vi phạm pháp luật.

8. Một số tội phạm tin học liên quan đến lạm dụng Internet

- Mạo danh, xâm nhập máy tính trái phép để đánh cắp và huỷ hoại thông tin.
- Lừa đảo qua mạng (Phishing): Là loại lừa đảo hấp dẫn nhất với tin tặc và trở thành hiểm hoạ đe doạ thương mại điện tử, làm giảm lòng tin vào các giao dịch điện tử.

Một số tội phạm tin học liên quan đến lạm dụng Internet (tiếp)

- **Spamming (thư rác) và việc vi phạm tính riêng tư của người khác:** Email là hệ thống giúp marketting rất tốt với khả năng quảng bá nhanh chóng và rộng rãi. Tuy nhiên có những người lạm dụng hệ thống email để quấy rối, đe dọa, xúc phạm đến người khác.
- Nhiều nước đang xem xét những đạo luật liên quan đến spamming có được phép hay không. Ở Việt nam, nạn spamming đang bùng nổ rất mạnh mẽ.

Một số tội phạm tin học liên quan đến lạm dụng Internet (tiếp)

- **Tấn công từ chối dịch vụ.**
- **Phát tán hoặc gieo rắc các tài liệu phản văn hoá, vi phạm an ninh quốc gia:** Internet là môi trường công cộng, ai cũng có thể sử dụng. Một số người lợi dụng khả năng của Internet để phổ biến các tài liệu phản văn hoá như kích động bạo lực, phổ biến văn hoá đồi truỵ, kích động bạo loạn, kích động các xu hướng dân tộc hay tôn giáp cực đoan, hướng dẫn các phương pháp khủng bố.

9. Vấn đề sở hữu trí tuệ và bản quyền

- Luật bản quyền được quy định trong Bộ luật dân sự của nước Cộng hoà Xã hội chủ nghĩa Việt Nam.
- Về cơ bản, quyền tác giả (quyền tinh thần) được cấp cho những người trực tiếp sáng tạo ra phần mềm; quyền sở hữu (quyền thương mại) được cấp cho người đầu tư; quyền sử dụng (licence) do chủ sở hữu cấp phép cho người sử dụng.

Vấn đề sở hữu trí tuệ và bản quyền (tiếp)

- Về mặt luật, phần mềm hiện đang được đối xử như một tác phẩm viết và còn rất nhiều điều bất cập. Chắc chắn luật sở hữu trí tuệ phải được tiếp tục hoàn thiện, nhất là đối với phần mềm.
- Tình trạng dùng phần mềm sao chép không có bản quyền rất phổ biến không chỉ riêng ở các nước đang phát triển. Ngay ở Mỹ cũng có đến 1/3 số phần mềm được dùng không có bản quyền.

Vấn đề sở hữu trí tuệ và bản quyền (tiếp)

- Theo thống kê của các tổ chức có trách nhiệm tình trạng dùng phần mềm không có bản quyền đã gây thiệt hại cho những người làm phần mềm nhiều tỷ đô la mỗi năm.
- Các nhà sản xuất phần mềm đã tìm các phương pháp chống sao chép nhưng "không lại" được với dân tin tặc. Cho đến nay, chưa một phần mềm nào của Việt Nam chống được nạn bẻ khoá.

10. Luật tội phạm tin học ở Việt Nam

- Bất cứ một nước phát triển nào cũng phải có quy định dưới dạng các văn bản pháp luật để chống lại các tội phạm tin học.
- Ở Việt Nam, nhận thức được tính nghiêm trọng của các tội phạm tin học, Quốc hội Cộng hoà Xã hội Chủ nghĩa Việt Nam đã ban hành luật ATTT mạng (2015) và một số điều luật chống tội phạm tin học trong bộ luật hình sự (13/1/2000)

Luật tội phạm tin học ở Việt Nam (tiếp)

- *Điều 224*. Tội tạo ra và lan truyền, phát tán các chương trình virus tin học
- *Điều 225*. Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử
- *Điều 226*. Tội sử dụng trái phép thông tin trên mạng và trong máy tính

Luật tội phạm tin học ở Việt Nam (tiếp)

- **Nghị định 55/2001/NĐ-CP**
- Ngày 23/8/2001 Chính phủ ban hành nghị định 55/2001/NĐ-CP quy định một số mức xử phạt các vi phạm khi sử dụng Internet.

10. Các phần mềm độc hại

Nội dung:

- Các dạng của phần mềm độc hại
- Giới thiệu về Virus

10.1 Các dạng của phần mềm độc hại

Loại virus			Ví dụ
Mã độc hại	Virus	Compliled Virus	Stoned, Jerusalem
		Interpreted Virus	Melisa
	Worm	Network Service Worm	Sasser
		Mass Malling Worm	Netsky, Mydoom
	Trojan Horse		
	Maliciuos		Nimda
	Tracking Cookie		
	Attacker Tool	Backdoor	Trino, Turkojan
		KeyLogger	Perfect Keylogger
		Rootkit	LRK5, Adore, Hack Defender
		Web Browser Plug-in	
		Email Generator	

10.1 Các dạng của phần mềm độc hại

- *Trojan horse:* Là những đoạn mã được "cắm" vào bên trong một phần mềm, cho phép xuất hiện và ra tay phá hoại một cách bất ngờ.
- Là một đoạn mã hoàn toàn không có tính chất lây lan, chỉ nằm trong những phần mềm nhất định, nó sẽ phá hoại và một thời điểm nhất định được hacker xác định trước. Đối tượng của chúng là thông tin trên đĩa như Format lại đĩa, xóa FAT, Root…

10.1 Các dạng của phần mềm độc hại

- **Virus**: là một chương trình máy tính luôn cố gắng mô phỏng theo một loại mã khác được hệ thống hay người dùng cho phép hoạt động. Khi mã này được sử dụng, virus cũng sẽ được kích hoạt song song với nó.
- Virus có khả năng tự sao chép chính nó lên những đĩa, file khác mà người dùng không hề hay biết.

10.1 Các dạng của phần mềm độc hại

- **Worm**: là một chương trình máy tính có thể tự chạy độc lập và tự hoàn thành mục đích của nó khi tấn công một máy chủ trong một hệ thống.
- Worm cũng là một chương trình có khả năng tự nhân bản và tự lây nhiễm trong hệ thống tuy nhiên nó có khả năng "tự đóng gói", điều đó có nghĩa là worm khác virus không cần phải có "file chủ" để mang nó khi nhiễm vào hệ thống

10.1 Các dạng của phần mềm độc hại

- *Malicious Mobile Code* : là một dạng mã phần mềm có thể được gửi từ xa vào để chạy trên một hệ thống mà không cần đến lời gọi thực hiện của người dùng hệ thống đó
- Malicious Mobile Code khác với virus, worm ở đặc tính nó không nhiễm vào file và không tìm cách tự phát tán. Thay vì khai thác một điểm yếu bảo mật xác định nào đó, kiểu tấn công này thường tác động đến hệ thống bằng cách tận dụng các quyền ưu tiên ngầm định để chạy mã từ xa

10.1 Các dạng của phần mềm độc hại

- ***Attacker Tool :*** là những bộ công cụ tấn công có thể sử dụng để đẩy các phần mềm độc hại vào trong hệ thống. Các bộ công cụ này có khả năng giúp cho kẻ tấn công có thể truy nhập bất hợp pháp vào hệ thống hoặc làm cho hệ thống bị lây nhiễm mã độc hại
- Attacker tool thường gặp là backdoor và keylogger.

10.1 Các dạng của phần mềm độc hại

- **Backdoor (Trapdoor)**: là một thuật ngữ chung chỉ các phần mềm độc hại thường trú và đợi lệnh điều khiển từ các cổng dịch vụ TCP hoặc UDP. Một cách đơn giản nhất, phần lớn các backdoor cho phép một kẻ tấn công thực thi một số hành động trên máy bị nhiễm như truyền file, dò mật khẩu, thực hiện mã lệnh,... Backdoor cũng có thể được xem xét dưới 2 dạng: Zoombie và Remote Administration Tool

10.1 Các dạng của phần mềm độc hại

- **Keylogger** là phần mềm được dùng để bí mật ghi lại các phím đã được nhấn bằng bàn phím rồi gửi tới hacker. Keylogger có thể ghi lại nội dung của email, của văn bản, user name, password, thông tin bí mật, ...
- Ví dụ về keylogger như: KeySnatch, Spyster, ...

10.1 Các dạng của phần mềm độc hại

- **Rootkits** là tập hợp của các file được cài đặt lên hệ thống nhằm biến đổi các chức năng chuẩn của hệ thống thành các chức năng tiềm ẩn các tấn công nguy hiểm. Ví dụ như trong hệ thống Windows, rootkit có thể sửa đổi, thay thế file, hoặc thường trú trong bộ nhớ nhằm thay thế, sửa đổi các lời gọi hàm của hệ điều hành. Rootkit thường được dùng để cài đặt các công cụ tấn công như cài backdoor, cài keylogger. Ví dụ về rootkit là: LRK5, Knark, Adore, Hack Defender

10.1 Các dạng của phần mềm độc hại

- **Web Browser Plug-in** là phương thức cài mã độc hại thực thi cùng với trình duyệt web. Khi được cài đặt, kiểu mã độc hại này sẽ theo dõi tất cả các hành vi duyệt web của người dùng (ví dụ như tên web site đã truy nhập) sau đó gửi thông tin ra ngoài. Một dạng khác là phần mềm gián điệp có chức năng quay số điện thoại tự động, nó sẽ tự động kích hoạt modem và kết nối đến một số điện thoại ngầm định mặc dù không được phép của chủ nhân

10.1 Các dạng của phần mềm độc hại

- **Email Generator** là những chương trình cho phép tạo ra và gửi đi một số lượng lớn các email. Mã độc hại có thể gieo rắc các email generator vào trong hệ thống. Các chương trình gián điệp, spam, mã độc hại có thể được đính kèm vào các email được sinh là từ email generator và gửi tới các địa chỉ có trong sổ địa chỉ của máy bị nhiễm.

10.2 Viruses

- Bản chất của Virus
- Phân loại Virus

10.2.1 Bản chất của Virus

- Về bản chất virus là một chương trình máy tính nhưng có khả năng tự sao chép chính nó lên những đĩa, file khác mà người sử dụng không hay biết. Bên cạnh đó, virus còn có tình chất phá hoại .

10.2.1 Bản chất của Virus

Một Virus máy tính bao gồm 3 phần:

- **Cơ chế lây nhiễm**: Virus được nhân rộng ra theo một cơ chế nhất định
- **Điều kiện kích hoạt**: Điều kiện hay sự kiện quyết định khi nào thì virus bắt đầu thực hiện các hoạt động của mình.
- **Payload**: Hoạt động của virus đã được lập trình sẵn.

10.2.2 Ví dụ (tự tìm hiểu)

```
        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:

}
```

10.2.2 Ví dụ (tự tìm hiểu)

```
     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;}
          }
```

10.2 Phân loại Virus

Dựa vào mục tiêu, virus được chia thành các loại sau:

- **Nhiễm khởi động: boot virus**
- **Nhiễm File: File-virus**

10.2 Phân loại Virus

- **Nhiễm khởi động**: Khi máy tính khởi động, một đoạn chương trình nhỏ trong ổ đĩa khởi động sẽ được thực thi. Đoạn chương trình này có nhiệm vụ nạp hệ điều hành (Windows, Linux hay Unix...). Sau khi nạp xong hệ điều hành, mới có thể bắt đầu sử dụng máy. Đoạn mã nói trên thường được để ở vùng trên cùng của ổ đĩa khởi động, và chúng được gọi là "Boot sector".

10.2 Phân loại Virus

- Boot virus sẽ tấn công vào Boot sector, nghĩa là nó sẽ thay một Boot sector chuẩn bằng một đoạn mã virus, quyền điều khiển lúc này sẽ được trao cho virus trước khi boot record được nhận quyền điều khiển.

10.2 Phân loại Virus

- **Nhiễm file: file virus**

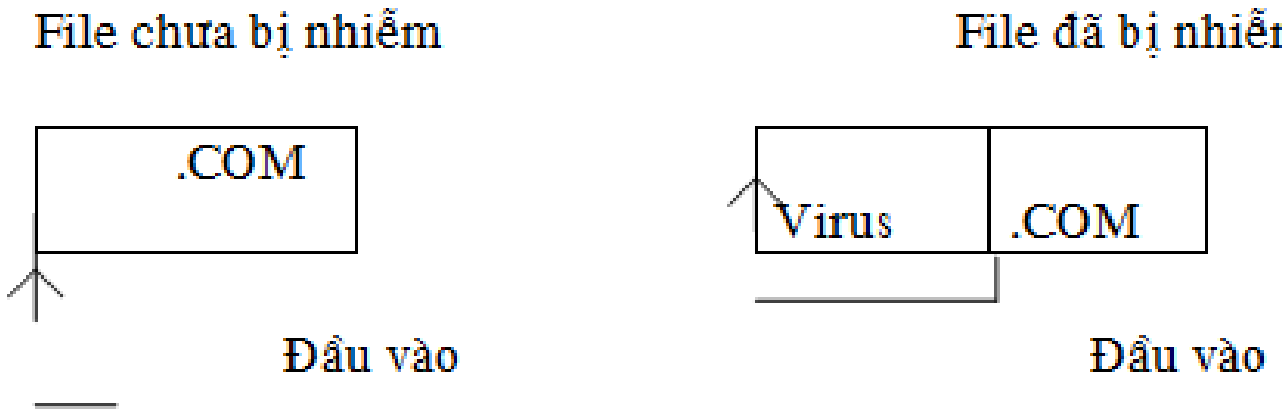
Là những virus lây vào những file chương trình, phổ biến nhất là trên hệ điều hành Windows, như các file có đuôi mở rộng .com, .exe, .bat, .pif, .sys... Khi chạy một file chương trình đã bị nhiễm virus cũng là lúc virus được kích hoạt và tiếp tục tìm các file chương trình khác trong máy để lây vào.

10.2 Phân loại Virus

- Giống như một nguyên tắc của B - virus, F - virus cũng phải tuân theo nguyên tắc sau: Quyền điều khiển phải nằm trong tay virus trước khi virus trả nó lại cho file bị nhiễm, Tất cả các dữ liệu của file phải được bảo toàn sau khi quyền điều khiển thuộc về file.

10.2.Phân loại Virus

- Một số phương pháp lây lan của F-virus:
- **1/ Chèn đầu**: Thông thường phương pháp này chỉ áp dụng với các file .COM



10.2.Phân loại Virus

- **2/ Append file**: Phương pháp này được thấy trên hầu hết các loại F - virus, phạm vi lây lan của nó rộng rãi hơn phương pháp trên. Theo phương pháp này Progvi sẽ được gắn ngay sau chương trinh đối tượng, Do đó progvi không nằm đúng đầu vào chương trình.

10.2.Phân loại Virus

- **3/ Overwrite**: Nhược điểm của hai phương pháp trên đều ở chỗ làm tăng kích thước file.
- Phương pháp này đề ra để khắc phục hai phương pháp trên, virus sẽ tìm một vùng trống trong file đối tượng (có thể là stack hoặc buffer) để ghi đè chương trình virus vào.

Tóm tắt nội dung

- Các vấn đề về ATTT
- Các nguy cơ ATTT
- Các mục tiêu ATTT
- Các loại hình tấn công HTTT
- Một số giải pháp đảm bảo ATTT
- Một số vấn đề liên quan đến luật ATTT
- Các phần mềm độc hại

Thảo luận

- Vai trò của ATTT trong xã hội?
- Tình hình ATTT trên thế giới và tại Việt Nam?
- Các mục tiêu của ATTT?
- Các nguy cơ về mất ATTT?
- Một số kỹ thuật tấn công mạng?
- Một số vấn đề liên quan đến luật ATTT?

CÂU HỎI VÀ BÀI TẬP

- Câu 1: Trình bày các khái niệm về tính bí mật, tính sẵn sàng và tính an toàn trong ATTT?
- Câu 2: Trình bày một số kiểu tấn công mạng?
  - Tấn công quét mạng
  - Tấn công từ chối dịch vụ
  - Tấn công mã độc
  - Tấn công kỹ nghệ xã hội

CÂU HỎI VÀ BÀI TẬP (tiếp)

- Câu 3: Trình bày và phân tích các nguy cơ về ATTT?
- Câu 4: Trình bày và phân tích các giải pháp bảo đảm ATTT?
- Câu 5: Trình bày tổng quan về thực trạng ATTT trên thế giới và tại Việt Nam?
- Câu 6: Trình bày các khái niệm về tin tặc và tội phạm kỹ thuật?

CÂU HỎI VÀ BÀI TẬP (tiếp)

- Câu 7: Trình bày vấn đề tội phạm tin học liên quan đến lạm dụng mạng?
- Câu 8: Trình bày một số vấn đề về sở hữu trí tuệ và luật bản quyền?
- Câu 9: Trình bày một số hiểu biết về luật tội phạm tin học ở Việt Nam?

HỎI VÀ ĐÁP