Trường Đại Học Công Nghệ Thông Tin
Khoa Mạng Máy Tính và Truyền Thông

AN TOÀN MẠNG MÁY TÍNH

ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan về an ninh mạng
2. Các phần mềm gây hại
3. Các giải thuật mã hoá dữ liệu
4. Mã hoá khoá công khai và quản lý khoá
5. Chứng thực dữ liệu
6. Một số giao thức bảo mật mạng
7. Bảo mật mạng không dây
8. Bảo mật mạng vành đai
9. Tìm kiếm phát hiện xâm nhập

BÀI 1

TỔNG QUAN VỀ AN NINH MẠNG

Tổng quan về an ninh mạng

1. Một số khái niệm
2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ
3. Lý lịch của những kẻ tấn công
4. Mô hình bảo mật cơ bản
5. Bài tập

1. Một số khái niệm

- Dữ liệu là gì?
- Hai trạng thái của dữ liệu:
  - Transmission state
  - Storage state
- Bốn yêu cầu của dữ liệu:
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Availability

1. Một số khái niệm

- An ninh mạng là một thành phần chủ yếu của an ninh thông tin.
- Ngoài an ninh mạng, an ninh thông tin còn có mối quan hệ với một số lãnh vực an ninh khác, bao gồm chính sách bảo mật, kiểm toán bảo mật, đánh giá bảo mật, hệ điều hành tin cậy, bảo mật cơ sở dữ liệu, bảo mật mã nguồn, ứng phó khẩn cấp, luật máy tính, luật phần mềm, khắc phục thảm họa…
- Môn học này tập trung vào an ninh mạng, nhưng vẫn có liên hệ với những lãnh vực còn lại.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

1. *Eavesdropping*
   - Nghe trộm là một phương pháp cũ nhưng hiệu quả.
   - Sử dụng một thiết bị mạng (router, card mạng…) và một chương trình ứng dụng (Tcpdump, Ethereal, Wireshark…) để giám sát lưu lượng mạng, bắt các gói tin đi qua thiết bị này.
   - Thực hiện dễ dàng hơn với mạng không dây.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

1. *Eavesdropping*

- Không có cách nào ngăn chận việc nghe trộm trong một mạng công cộng.
- Để chống lại việc nghe trộm, cách tốt nhất là mã hoá dữ liệu trước khi truyền chúng trên mạng.
  - Plaintext: văn bản gốc
  - Cyphertext: chuỗi mật mã
  - Key: khoá mã hoá hoặc giải mã

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

2. *Cryptanalysis*

- Là nghệ thuật tìm kiếm thông tin hữu ích từ dữ liệu đã mã hoá mà không cần biết khoá giải mã.
- Ví dụ: phân tích cấu trúc thống kê của các ký tự trong phương pháp mã hoá bằng tần suất.
- Phương pháp này thường sử dụng các công cụ toán học và máy tính có hiệu suất cao.
- Cách chống lại phá mã:
  - Sử dụng những giải thuật mã hoá không thể hiện cấu trúc thống kê trong chuỗi mật mã.
  - Khoá có độ dài lớn để chống Brute-force attacks.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Cơ chế chứng thực được sử dụng rộng rãi nhất là dùng username và password.
- Các phương pháp thông dụng bao gồm:
  - Guessing
  - Social engineering
  - Dictionary
  - Password sniffing

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Guessing: hiệu quả đối với các mật khẩu ngắn hoặc người dùng quên đổi mật khẩu ngầm định.

  10 mật khẩu phổ biến nhất trên internet (theo PC Magazine):

  1. Password
  2. 123456
  3. qwerty
  4. abc123
  5. letmein
  6. monkey
  7. myspace1
  8. password1
  9. blink182
  10. the user's own first name

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Social engineering: là phương pháp sử dụng các kỹ năng xã hội để ăn cắp thông tin mật của người khác.
  - Mạo danh (Impersonate)
  - Lừa đảo (Physing) qua email, websites…
  - Thu thập thông tin từ giấy tờ bị loại bỏ
  - Tạo trang web đăng nhập giả…

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Dictionary Attacks:
  - Chỉ những mật khẩu đã được mã hoá mới được lưu trên hệ thống máy tính.
  - Hệ điều hành UNIX và LINUX: mật khẩu đã được mã hoá với dạng mã ASCII của các user được lưu trong /etc/passwd (các versions cũ) và /etc/shadows (các versions mới hơn).
  - Hệ điều hành Windows NT/XP: tên user và mật khẩu của user đã được mã hoá được lưu trong registry của hệ thống với tên file là SAM.
  - Dictionary attacks: duyệt tìm từ một từ điển (thu được từ các file SAM…) các username và password đã được mã hoá.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Password Sniffing:
  - Là một phần mềm dùng để bắt các thông tin đăng nhập từ xa như username và password đối với các ứng dụng mạng phổ biến như Telnet, FTP, SMTP, POP3.
  - Để gây khó khăn cho việc Password Sniffing, có thể dùng những chương trình đặc biệt (như SSH trong HTTPS…) để mã hoá tất cả các thông điệp truyền.
  - Cain & Abel là một công cụ khôi phục mật khẩu trong hệ điều hành Microsoft và cũng là một công cụ password sniffing có thể bắt và phá mã các password đã được mã hoá sử dụng từ điển hoặc brute-force. Có thể download công cụ này tại http://www.oxid.it/cain.html.

OXID.IT

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

Cain & Abel has been developed in the hope that it will be useful for network administrators, teachers, security consultants/professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons. The author will not help or support any illegal activity done with this program. Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data. Please carefully read the License Agreement included in the program before using it.

The latest version is faster and contains a lot of new features like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS, and contains filters to capture credentials from a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders and some not so common utilities related to network and system security.

Download Cain & Abel v2.0 for Windows 9x (discontinued and not supported anymore)
MD5 - A14185FAFC1A0A433752A75C0B8CE15D
SHA1 - 8F310D3BECC4D18803AF31575E8035B44FE37418

Download Cain & Abel v4.9.36 for Windows NT/2000/XP
MD5 - 1C483952D48F9F97781A992A74ADCCE5
SHA1 - FAEF22138E58B4DB44B56CF081B53AB2F46DF2A5

Cain & Abel User Manual is included in the installation package and also available on-line so you can view all the program's features without the need to install the program. The on-line version of the manual requires a JavaScript enabled browser

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Một số phương pháp chứng minh danh tính người dùng đang được sử dụng:
  - Sử dụng mật khẩu bí mật (secret passwords): phổ biến nhất. Sử dụng tên người dùng và mật khẩu của người dùng.
  - Sử dụng sinh trắc học (biometrics): sử dụng các tính năng độc đáo của sinh học như vân tay, võng mạc… nhờ việc kết nối các thiết bị sinh trắc học (khá đắt tiền, chỉ dùng tại những nơi yêu cầu bảo mật ở mức độ cao) vào máy tính như máy đọc dấu vân tay, máy quét võng mạc…
  - Sử dụng chứng thực (authenticating items): dùng một số giao thức xác thực như Kerberos…

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Một số quy tắc bảo vệ mật khẩu:
  - Sử dụng mật khẩu dài kết hợp giữa chữ thường, chữ hoa, số và các ký tự đặc biệt như $ # & %. Không dùng các từ có trong từ điển, các tên và mật khẩu thông dụng.

    -> gây khó khăn cho việc đoán mật khẩu (guessing attacks) và tấn công sử dụng từ điển (dictionary attacks).
  - Không tiết lộ mật khẩu với những người không có thẩm quyền hoặc qua điện thoại, thư điện tử… -> chống lại social engineering.
  - Thay đổi mật khẩu định kỳ và không sử dụng trở lại những mật khẩu cũ để chống lại những cuộc tấn công từ điển hoặc mật khẩu cũ đã được nhận diện.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Một số quy tắc bảo vệ mật khẩu:
  - Không sử dụng cùng một mật khẩu cho các tài khoản khác nhau nhằm đảm bảo các tài khoản khác vẫn an toàn khi mật khẩu của một tài khoản bị lộ.
  - Không sử dụng những phần mềm đăng nhập từ xa mà không có cơ chế mã hoá mật khẩu và một số thông tin quan trọng khác.
  - Huỷ hoàn toàn các tài liệu có lưu các thông tin quan trọng.
  - Tránh nhập các thông tin trong các cửa sổ popup.
  - Không click vào các liên kết trong các email khả nghi.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Là phương pháp tấn công cho phép kẻ tấn công mạo nhận nạn nhân mà không cần sử dụng mật khẩu của nạn nhân.
- Các phương pháp phổ biến bao gồm:
  - Man-in-the-midle attacks
  - Message replays attacks
  - Network spoofing attacks
  - Software exploitation attacks

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

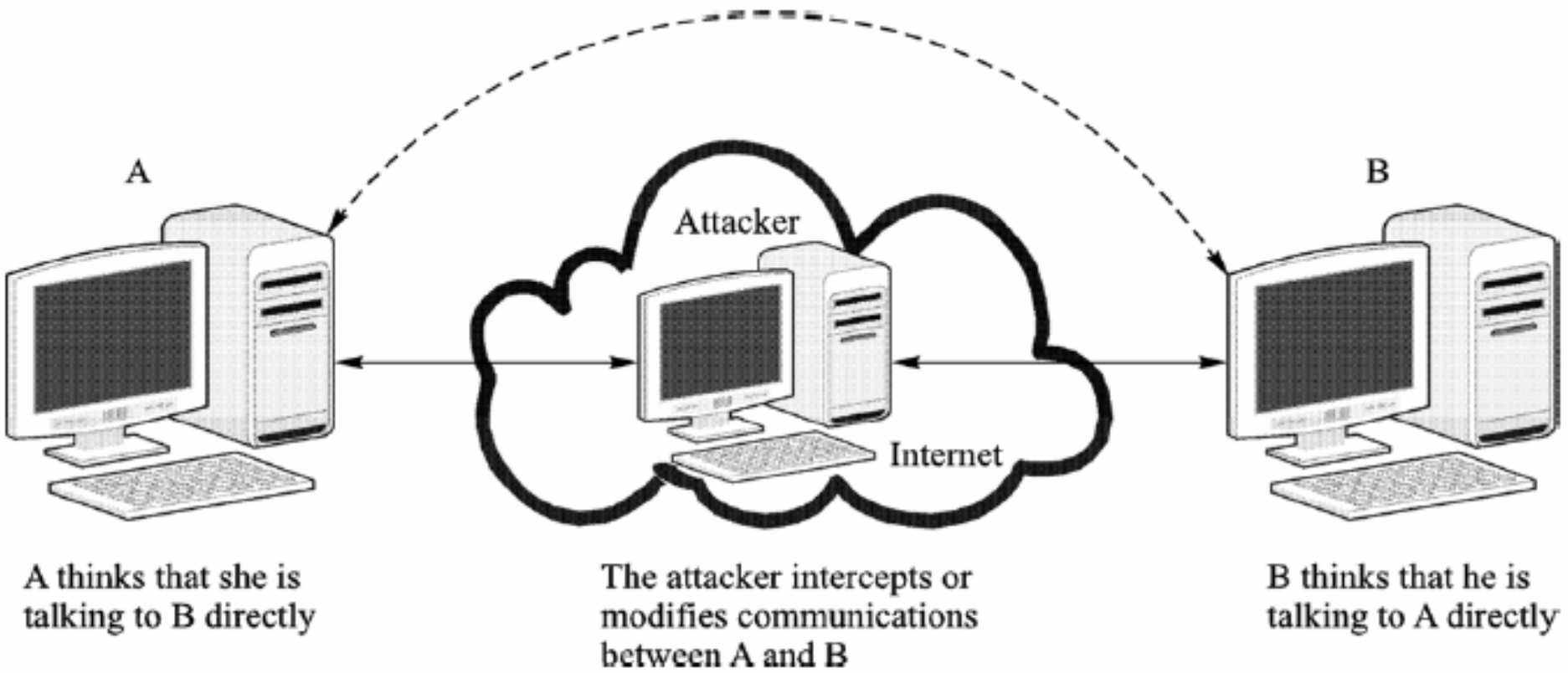
4. *Identity Spoofing*

- Man-in-the-midle attacks
  - Kẻ tấn công cố gắng dàn xếp với thiết bị mạng (hoặc cài đặt một thiết bị của riêng mình) giữa hai hoặc nhiều người sử dụng, sau đó chặn và sửa đổi hay làm giả dữ liệu truyền giữa những người sử dụng rồi truyền chúng như chưa từng bị tác động bởi kẻ tấn công.
  - Các người dùng vẫn tin rằng họ đang trực tiếp nói chuyện với nhau, không nhận ra rằng sự bảo mật và tính toàn vẹn dữ liệu của các gói tin IP mà họ nhận được đã không còn.
  - Mã hoá và chứng thực các gói IP là biện pháp chính để ngăn chận các cuộc tấn công Man-in-the-midle. Những kẻ tấn công không thể đọc hoặc sửa đổi một gói tin IP đã được mã hoá mà không phải giải mã nó.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Man-in-the-midle attacks



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

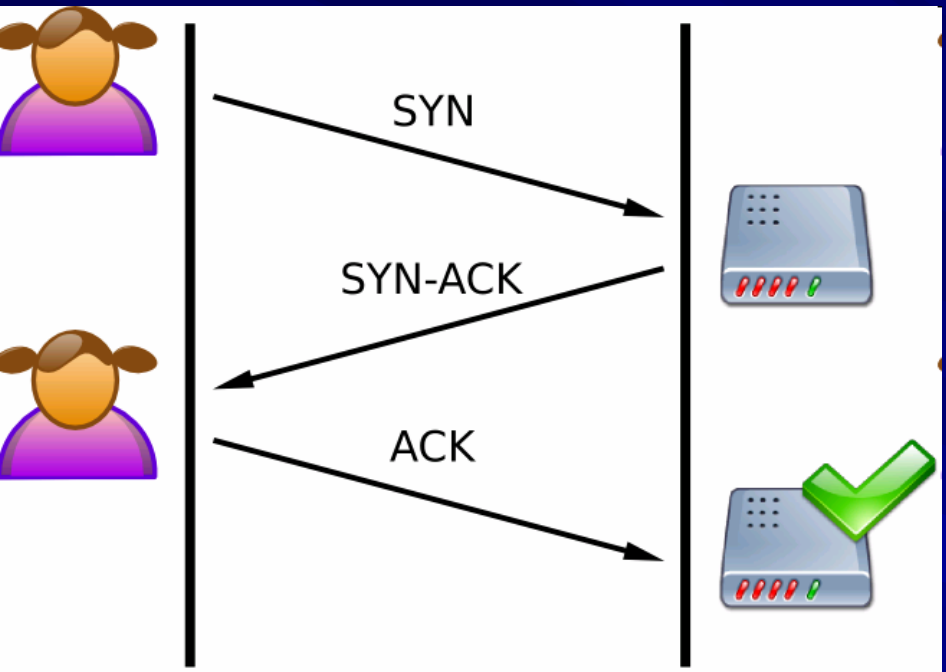
- Message replays:
  - Trong một số giao thức xác thực, sau khi người dùng A chứng thực mình với hệ thống là một người dùng hợp pháp, A sẽ được cấp một chứng thực (giấy phép) thông qua. Với giấy phép này, A sẽ nhận được những dịch vụ cung cấp bởi hệ thống. Giấy phép này đã được mã hóa và không thể sửa đổi.
  - Tuy nhiên, những kẻ tấn công có thể ngăn chặn nó, giữ một bản sao, và sử dụng nó sau này để mạo nhận (đóng vai) người dùng A để có được các dịch vụ từ hệ thống.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

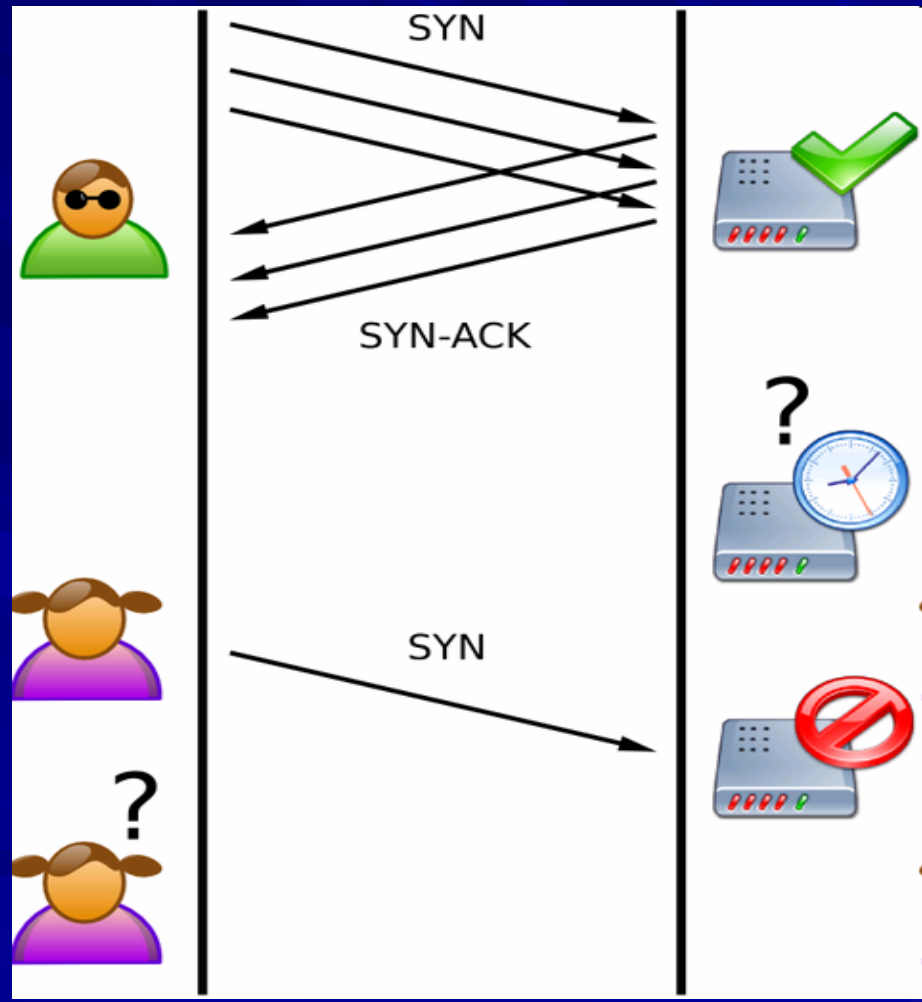
4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
  - SYN flooding: Trong một cuộc tấn công SYN flooding, kẻ tấn công lấp đầy bộ đệm TCP của máy tính mục tiêu với một khối lượng lớn các gói SYN, làm cho máy tính mục tiêu không thể thiết lập các thông tin liên lạc với các máy tính khác. Khi điều này xảy ra, các máy tính mục tiêu được gọi là một máy tính câm.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



A normal connection between a user and a server. The three-way handshake is correctly performed.

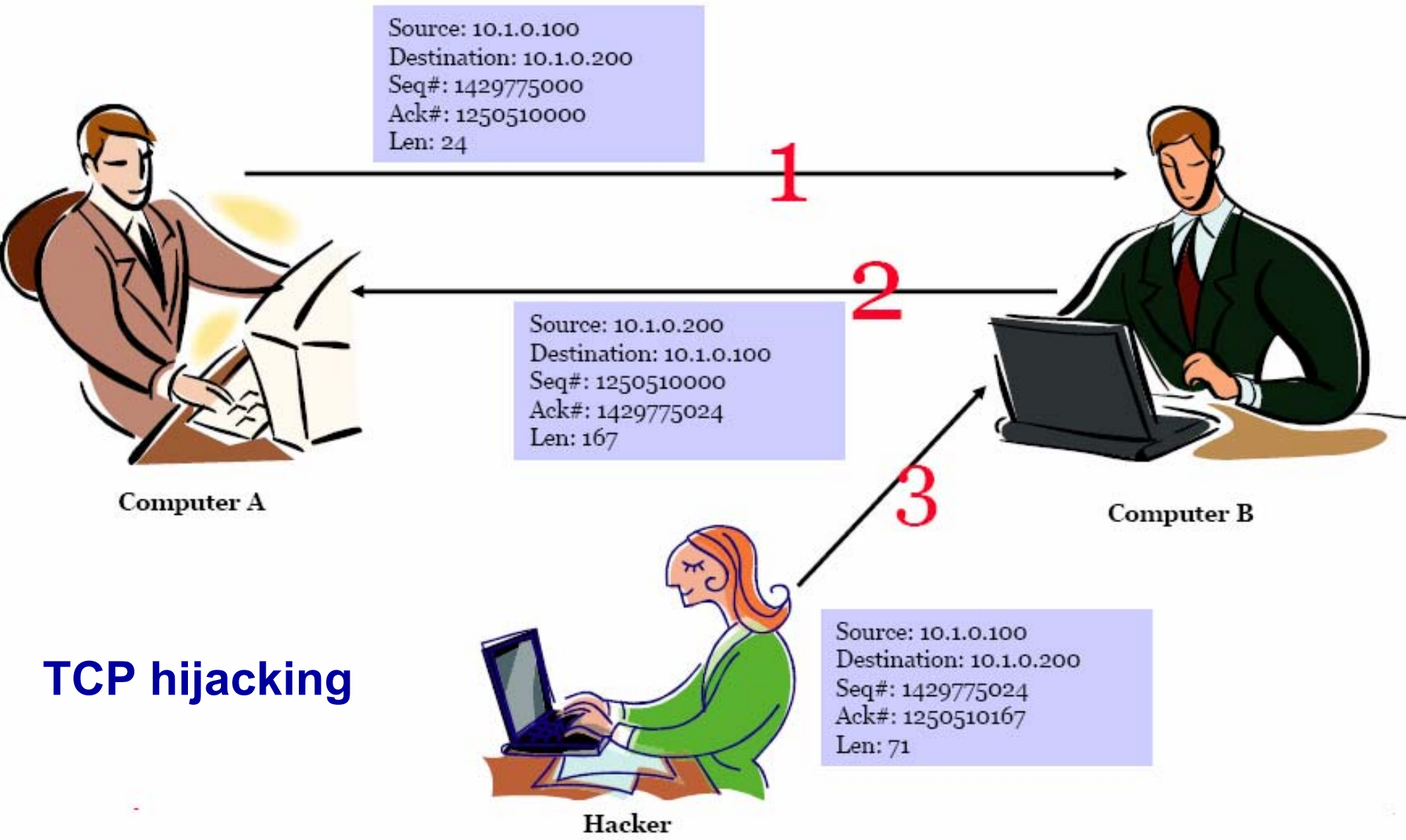


2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Network Spoofing: là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
  - TCP hijacking:
    - Là một kỹ thuật sử dụng các gói tin giả mạo để chiếm đoạt một kết nối giữa máy tính nạn nhân và máy đích. Máy nạn nhân bị treo và hacker có thể truyền thông với máy đích như hacker chính là nạn nhân.
    - Để ngăn chặn TCP hijacking, có thể sử dụng phần mềm như TCP Wrappers để kiểm tra địa chỉ IP tại tầng TCP (tầng Transport).

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



TCP hijacking

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

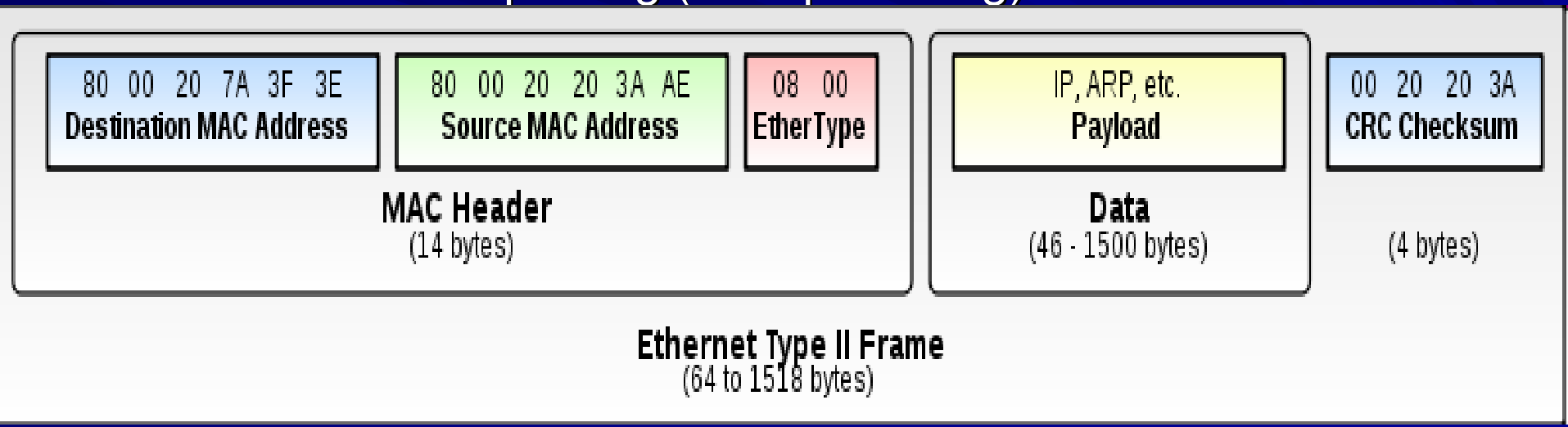
4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
  - ARP spoofing (ARP poisoning): ARP là một giao thức phân giải địa chỉ tại tầng liên kết có thể chuyển đổi địa chỉ IP đích trong header IP đến địa chỉ MAC của máy tính tại mạng đích. Trong một cuộc tấn công giả mạo ARP, kẻ tấn công thay đổi địa chỉ MAC đích hợp pháp của một địa chỉ IP đến một địa chỉ MAC khác được lựa chọn bởi những kẻ tấn công. Để ngăn chặn các cuộc tấn công ARP spoofing, cần phải tăng cường kiểm tra các tên miền, và chắc chắn rằng địa chỉ IP nguồn và địa chỉ IP đích trong một gói tin IP không được thay đổi trong khi truyền.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
  - ARP spoofing (ARP poisoning):

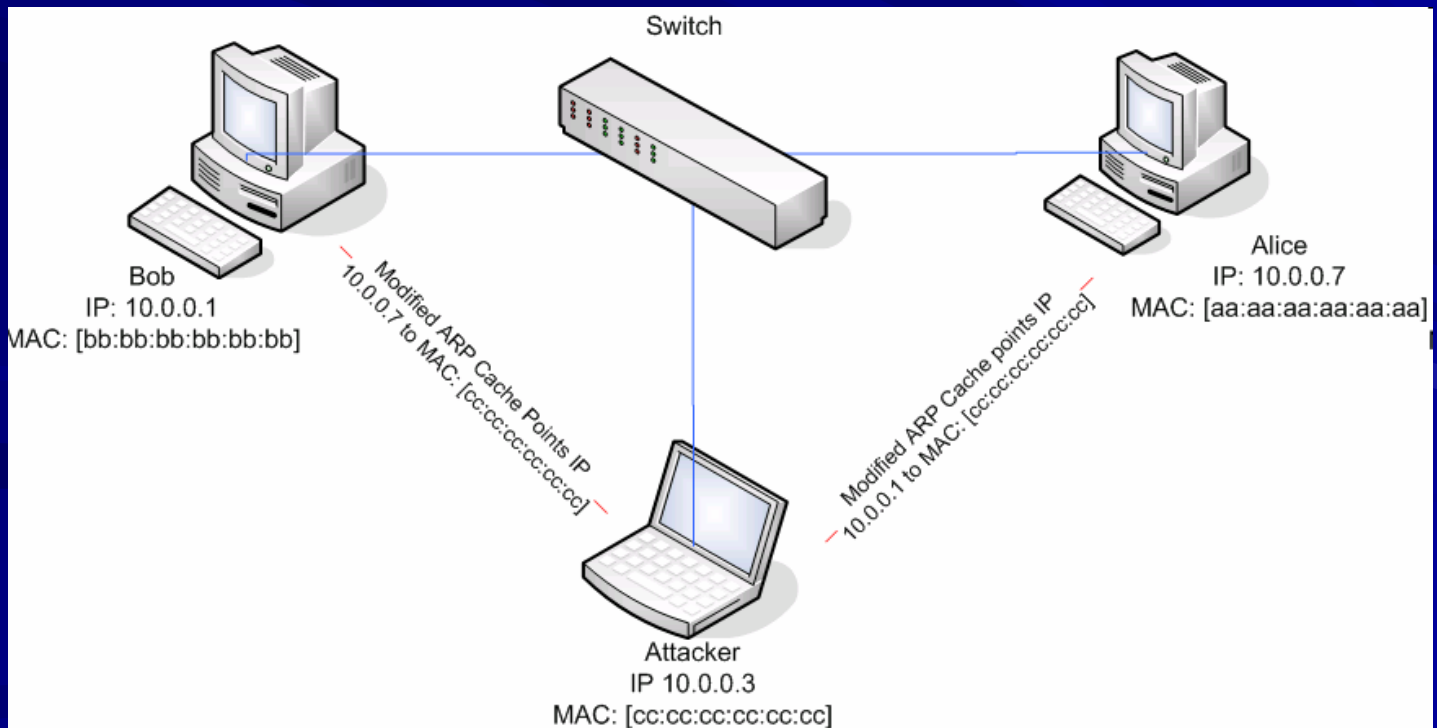


Một frame Ethernet tiêu biểu. Một frame giả mạo có địa chỉ MAC nguồn sai có thể đánh lừa các thiết bị trên mạng.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
  - ARP spoofing (ARP poisoning):



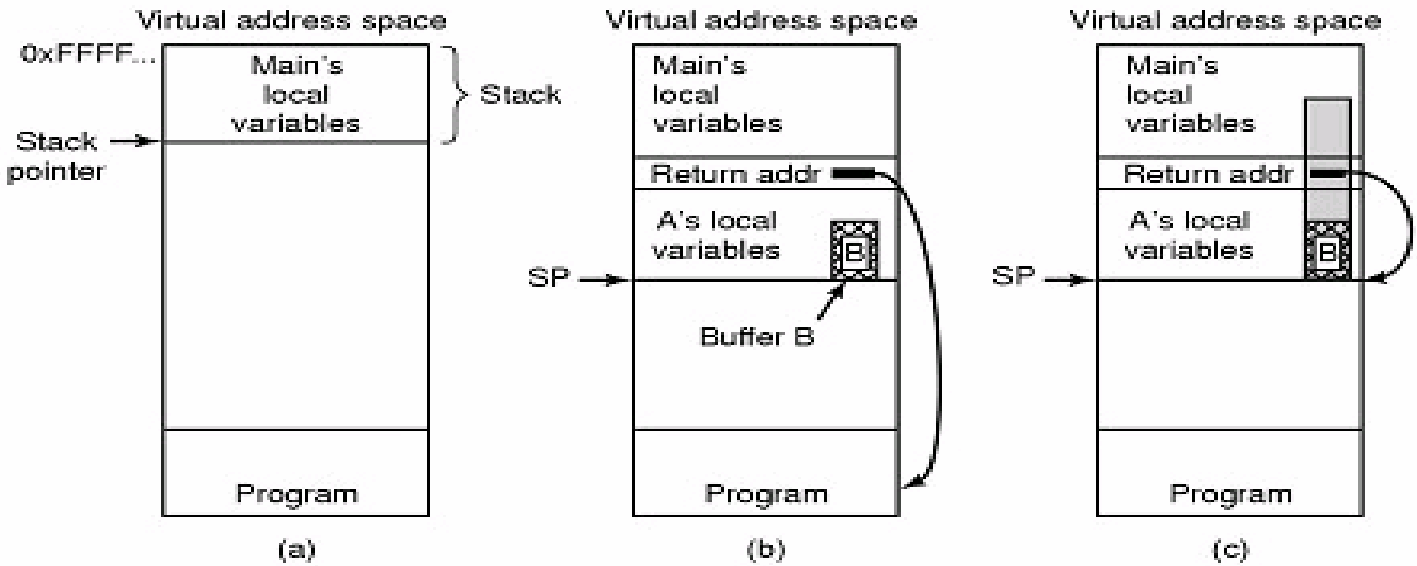
2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

5. *Buffer-Overflow Exploitations*

- Là một lỗ hổng phần mềm phổ biến. Lỗi này xảy ra khi quá trình ghi dữ liệu vào bộ đệm nhiều hơn kích thước khả dụng của nó.
- Các hàm strcat(), strcpy(), sprintf(), vsprintf(), bcopy(), get(), scanf()… trong ngôn ngữ C có thể bị khai thác vì không kiểm tra xem liệu bộ đệm có đủ lớn để dữ liệu được sao chép vào mà không gây ra tràn bộ đệm hay không.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

Buffer Overflow



- (a) Situation when main program is running
- (b) After program *A* called
- (c) Buffer overflow shown in gray

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

6. *Repudiation*

- Trong một số trường hợp chủ sở hữu của dữ liệu có thể không thừa nhận quyền sở hữu của dữ liệu để tránh hậu quả pháp lý. Người này có thể cho rằng chưa bao giờ gửi hoặc nhận các dữ liệu đó.
- Ngay cả khi dữ liệu đã được chứng thực, chủ sở hữu của dữ liệu xác thực có thể thuyết phục quan tòa rằng vì những sơ hở, bất cứ ai cũng có thể dễ dàng chế tạo tin nhắn và làm cho nó trông giống như thật.
- Sử dụng các thuật toán mã hóa và xác thực có thể giúp ngăn ngừa các cuộc tấn công bác bỏ.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

7. *Intrusion*

- Là kẻ xâm nhập bất hợp pháp vào một mạng với mục đích truy cập vào hệ thống máy tính của người khác, đánh cắp thông tin và tài nguyên máy tính hoặc băng thông của nạn nhân.
- Cấu hình sơ hở, giao thức sai sót, tác dụng phụ của phần mềm đều có thể bị khai thác bởi kẻ xâm nhập.
- Mở các cổng UDP hoặc TCP không cần thiết là một sơ hở phổ biến. Đóng các cổng này lại có thể giảm thiểu việc xâm nhập.
- IP scan và Port scan là những công cụ hack phổ biến thuộc dạng này và cũng là những công cụ giúp người dùng kiểm tra được các lỗ hổng trong hệ thống.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*

- Mục tiêu của cuộc tấn công từ chối dịch vụ là ngăn chặn người dùng hợp pháp sử dụng những dịch vụ mà họ thường nhận được từ các máy chủ.
- Các cuộc tấn công như vậy thường buộc máy tính mục tiêu phải xử lý một số lượng lớn những thứ vô dụng, hy vọng máy tính này sẽ tiêu thụ tất cả các nguồn tài nguyên quan trọng.
- Một cuộc tấn công từ chối dịch vụ có thể được phát sinh từ một máy tính duy nhất (DoS), hoặc từ một nhóm các máy tính phân bố trên mạng Internet (DDoS).

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*
   - DoS có các hình thức cơ bản sau:
     - Smurf
     - Buffer Overflow Attack
     - Ping of death
     - Teardrop
     - SYN Attack
   - Công cụ để thực hiện tấn công DoS có thể là Jolt2, Bubonic.c, Land and LaTierra, Targa, Blast20, Nemesy, Panther2, Crazy Pinger, Some Trouble, UDP Flood, FSMax…

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

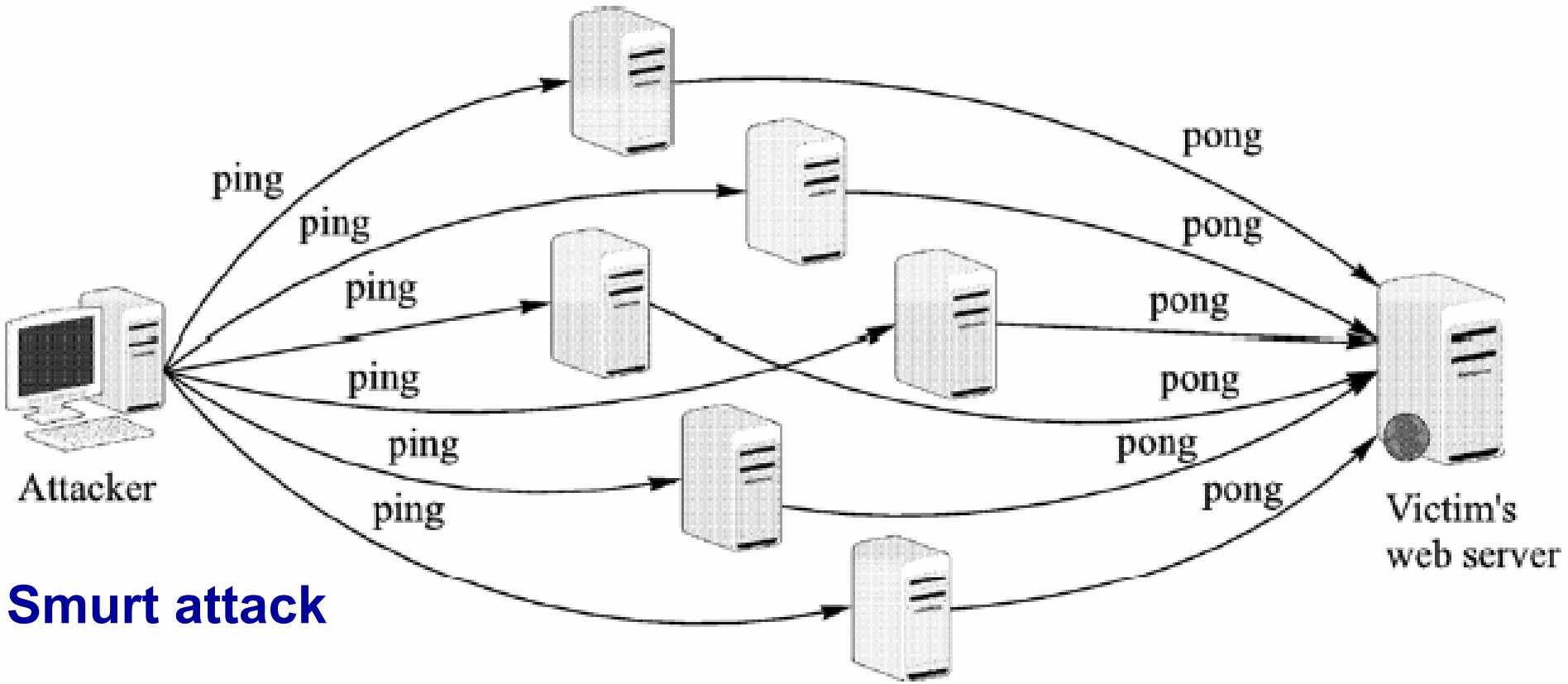
8. *Denial of Service Attacks*

- DoS: Smurf là một loại tấn công DoS điển hình. Máy của attacker sẽ gởi rất nhiều lệnh ping đến một số lượng lớn máy tính trong một thời gian ngắn trong đó địa chỉ IP nguồn của gói ICMP echo sẽ được thay thế bởi địa chỉ IP của nạn nhân. Các máy tính này sẽ trả lại các gói ICMP reply đến máy nạn nhân. Buộc phải xử lý một số lượng quá lớn các gói ICMP reply trong một thời gian ngắn khiến tài nguyên của máy bị cạn kiệt và máy sẽ bị sụp đổ.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*

– DoS:



Smurt attack

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*

– DDoS (Distributed DoS) có cơ chế hoạt động:

- Attackers thường sử dụng Trojan để kiểm soát cùng lúc nhiều máy tính nối mạng.
- Attacker cài đặt một phần mềm đặc biệt (phần mềm zombie) lên các máy tính này (máy tính zombie) để tạo ra một đội quân zombie (botnet) nhằm tấn công DoS sau này trên máy nạn nhân.
- Phát hành một lệnh tấn công vào các máy tính zombie để khởi động một cuộc tấn công DoS trên cùng một mục tiêu (máy nạn nhân) cùng một lúc.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

Hacker in Russia

1

John (end user in Boston)

Downloads and executes **chess.zip** from freeware site

John's machine is infected with Agabot

5 Commands

Attacker sends commands to the Bots

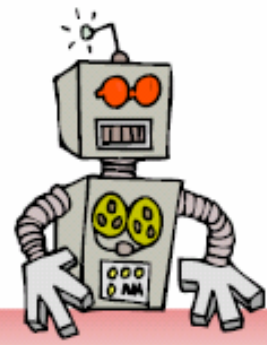
4

Bot

- Bots connect to the "Master" using IRC channel and waits for instructions

3

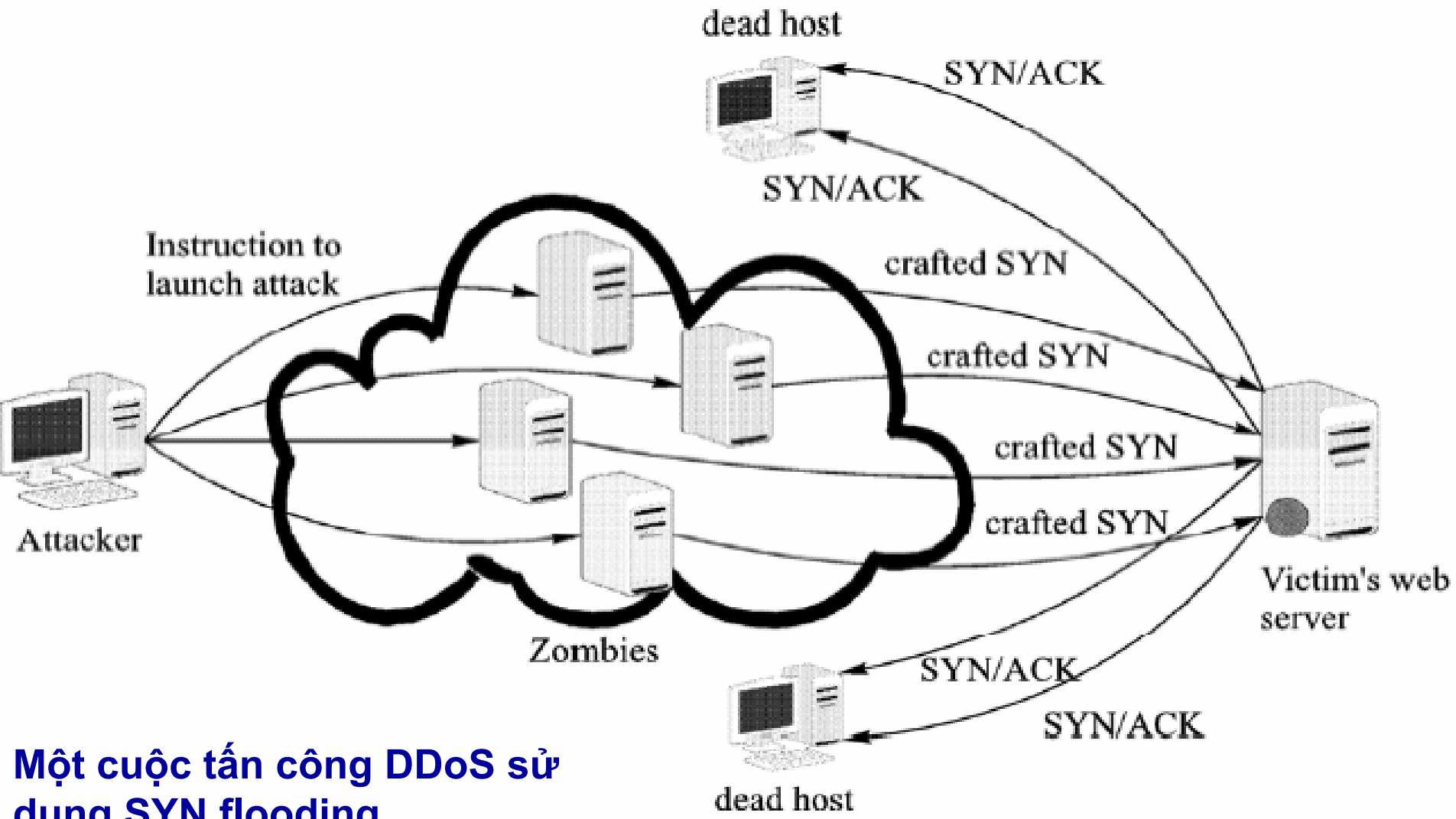
2



Bot

- Bot looks for other vulnerable systems and infects them

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



Một cuộc tấn công DDoS sử dụng SYN flooding

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

Các phần mềm độc hại bao gồm:

- Virus,
- Worms,
- Trojan horses,
- Logic bombs,
- Backdoors
- Spyware.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Virus***
  - Là một phần mềm có thể sao chép chính nó. Nó không đứng một mình mà phải gắn vào một tập tin hoặc một chương trình khác.
  - Khi một chương trình bị nhiễm virus máy tính được thực hiện hoặc một tập tin bị nhiễm được mở ra, loại virus chứa trong nó sẽ được thực thi.
  - Khi thực hiện, virus có thể làm hại máy tính và sao chép chính nó để lây nhiễm sang máy khác trong hệ thống.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Worms***
  - Cũng là một chương trình có thể tự sao chép chính nó. Nhưng không giống như virus, Worm là một chương trình đứng một mình (stand alone program). Nói cách khác là nó không cần vật chủ để ký sinh.
  - Một Worm có thể tự thực thi tại bất kỳ thời điểm nào nó muốn.
  - Khi thực thi, Worm có thể gây nguy hiểm cho hệ thống nơi nó thường trú hoặc tái sinh chính nó trên các hệ thống qua mạng.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Trojan horses***:
  - Thường nguỵ trang mình kèm theo những chương trình ứng dụng thông thường và vô hại như trò chơi hoặc những công cụ miễn phí để người dùng tải về máy.
  - Trojan không tự sinh sản như virus hay worm và chỉ thực hiện khi người dùng chạy chương trình có đính kèm Trojan.
  - Chức năng chính của Trojan là điều khiển máy tính từ xa, ăn cắp thông tin của nạn nhân hoặc làm nhiệm vụ backdoor.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Logic bombs***
  - Bom logic là chương trình con hoặc lệnh được nhúng trong một chương trình. Sự thi hành của nó được kích hoạt bởi câu lệnh điều kiện.
  - Ví dụ, một nhân viên công ty làm việc trên một dự án phát triển có thể cài đặt một quả bom logic bên trong một chương trình. Quả bom được kích hoạt chỉ nếu nhân viên này đã không chạy chương trình trong một thời gian nhất định. Khi điều kiện được đáp ứng, có nghĩa là nhân viên này đã bị sa thải một thời gian trước đó. Quả bom logic trong trường hợp này được sử dụng để trả thù chống lại chủ nhân.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Backdoors***
  - Backdoors là những đoạn chương trình bí mật thường được đính kèm vào những chương trình khác nhằm giúp kẻ tấn công sau khi đã xâm nhập được vào hệ thống mở sẵn những lối vào (cổng hậu)..
  - Khi được chạy trên máy nạn nhân, Backdoors sẽ thường trực trong bộ nhớ, mở một port (mặc định hoặc do kẻ tấn công quy định) giúp kẻ tấn công dễ dàng đột nhập vào máy nạn nhân thông qua port này.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Spywares***
  - Spyware là một loại phần mềm tự cài đặt chính nó trên máy tính của người dùng. Spyware thường được sử dụng để theo dõi xem người dùng làm gì và quấy rối họ với những thông điệp thương mại xuất hiện trong những cửa sổ popup.
  - Thường gồm các loại Browser hijacking và Zombieware.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Spywares***
  - Browser Hijacking: là một kỹ thuật có thể thay đổi các thiết lập của trình duyệt của người dùng. Nó có thể thay thế Website mặc định của người dùng với một trang web khác được lựa chọn bởi kẻ tấn công. Hoặc nó có thể ngăn chặn người dùng truy cập vào các Websites họ muốn đến thăm.
  - Zombieware: là phần mềm có trên máy tính của người dùng và biến nó thành một zombie để khởi động các cuộc tấn công DDoS hoặc thực hiện các hoạt động có hại như gửi thư rác hoặc phát tán virus.

3. Lý lịch của những kẻ tấn công

- Các attacker có thể là:
  - Black-hat hackers
  - Script kiddies
  - Cyber spies
  - Vicious employees
  - Cyber terrorists

3. Lý lịch của những kẻ tấn công

- Black-hat hackers
  - Hackers là những người có tri thức đặc biệt về hệ thống máy tính. Họ quan tâm đến những chi tiết tinh tế của phần mềm, giải thuật, mạng máy tính và cấu hình hệ thống. Họ là một nhóm người ưu tú, năng động, được đào tạo tốt.
  - Tùy theo mục đích, hackers được chia thành hackers mũ đen, hackers mũ trắng và hackers mũ xám.

3. Lý lịch của những kẻ tấn công

- Script kiddies
  - Là những người sử dụng các script hoặc các chương trình được phát triển bởi các hacker mũ đen (những công cụ hack) để tấn công các máy tính và gây thiệt hại cho người khác.
  - Script kiddies chỉ biết sử dụng công cụ hack để tấn công các mục tiêu chứ không hiểu cách thức hoạt động và cũng không có khả năng viết ra những công cụ tương tự.
  - Đa số Script kiddies chỉ là những thanh thiếu niên, không đủ nhận thức và chín chắn để hiểu hết những hậu quả do mình gây ra.

3. Lý lịch của những kẻ tấn công

- Cyber spies
  - Có thể hoạt động trên lãnh vực quân sự, kinh tế…
  - Đánh chặn truyền thông trên mạng và phá mã các thông điệp đã được mã hoá.
  - Nhiều tổ chức tình báo lớn trên thế giới đã thuê các nhà toán học, các nhà khoa học máy tính, các giáo sư đại học làm việc cho họ để phát triển các công cụ nhằm chống lại loại tội phạm này.

3. Lý lịch của những kẻ tấn công

- Vicious employees
  - Là những người cố tình vi phạm an ninh để làm hại những người sử dụng họ.
  - Tấn công máy tính công ty để kiếm sự quan tâm từ những người lãnh đạo.
  - Hoạt động như gián điệp mạng để thu thập và bán bí mật của công ty.

3. Lý lịch của những kẻ tấn công

- Cyber terrorists:
  - Là những kẻ khủng bố cực đoan sử dụng máy tính và công nghệ mạng làm công cụ.
  - Phá hoại tài sản công cộng và cuộc sống của những người vô tội nên cực kỳ nguy hiểm.
  - Vẫn chưa có những báo cáo đầy đủ về loại tội phạm này.

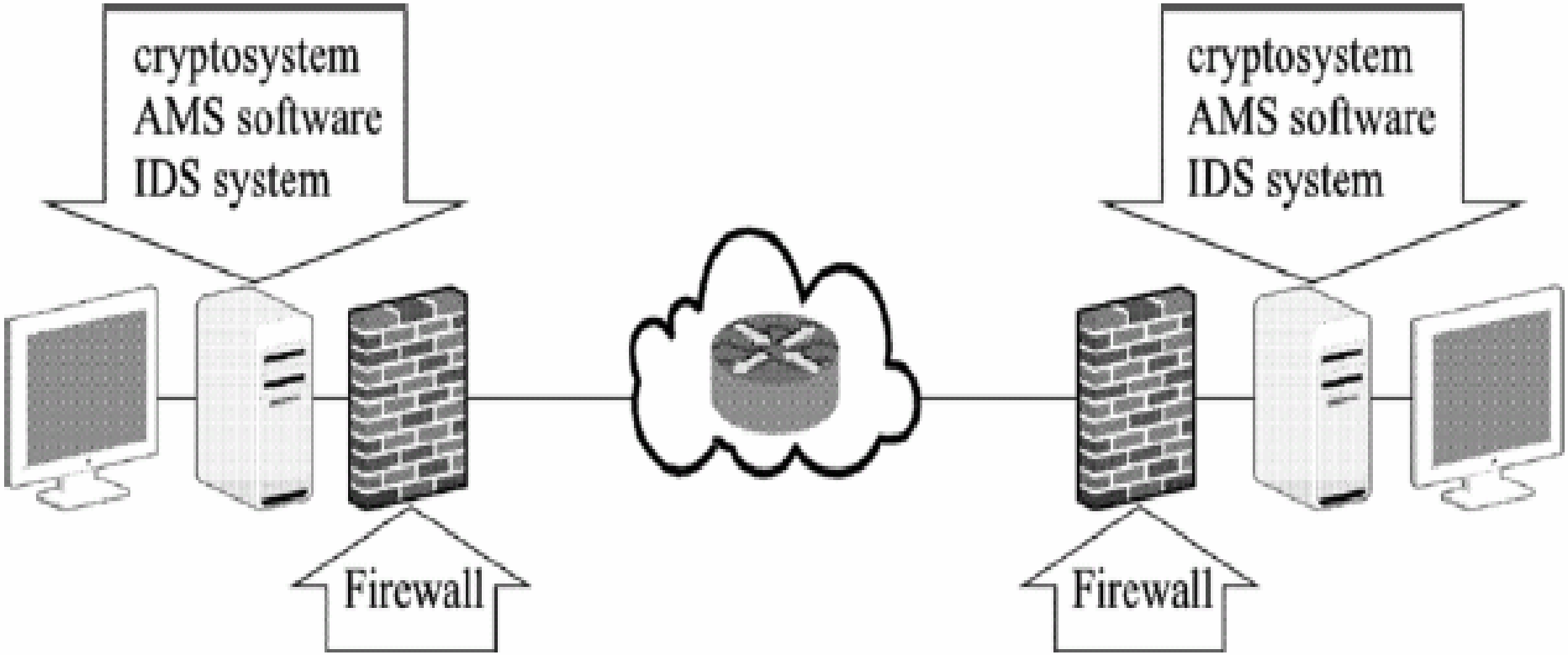
4. Mô hình bảo mật cơ bản

- Mô hình bảo mật cơ bản gồm 4 thành phần:
  - **Hệ thống mã hoá** (Cryptosystem):
    - Sử dụng mật mã và các giao thức bảo mật để bảo vệ dữ liệu.
    - Các giao thức bảo mật bao gồm các giao thức mã hoá, các giao thức chứng thực, các giao thức quản lý khoá.
  - **Tường lửa** (Firewalls): là những gói phần mềm đặc biệt cài trên máy tính hoặc thiết bị mạng để kiểm tra các gói tin đi vào và đi ra trên mạng.

4. Mô hình bảo mật cơ bản

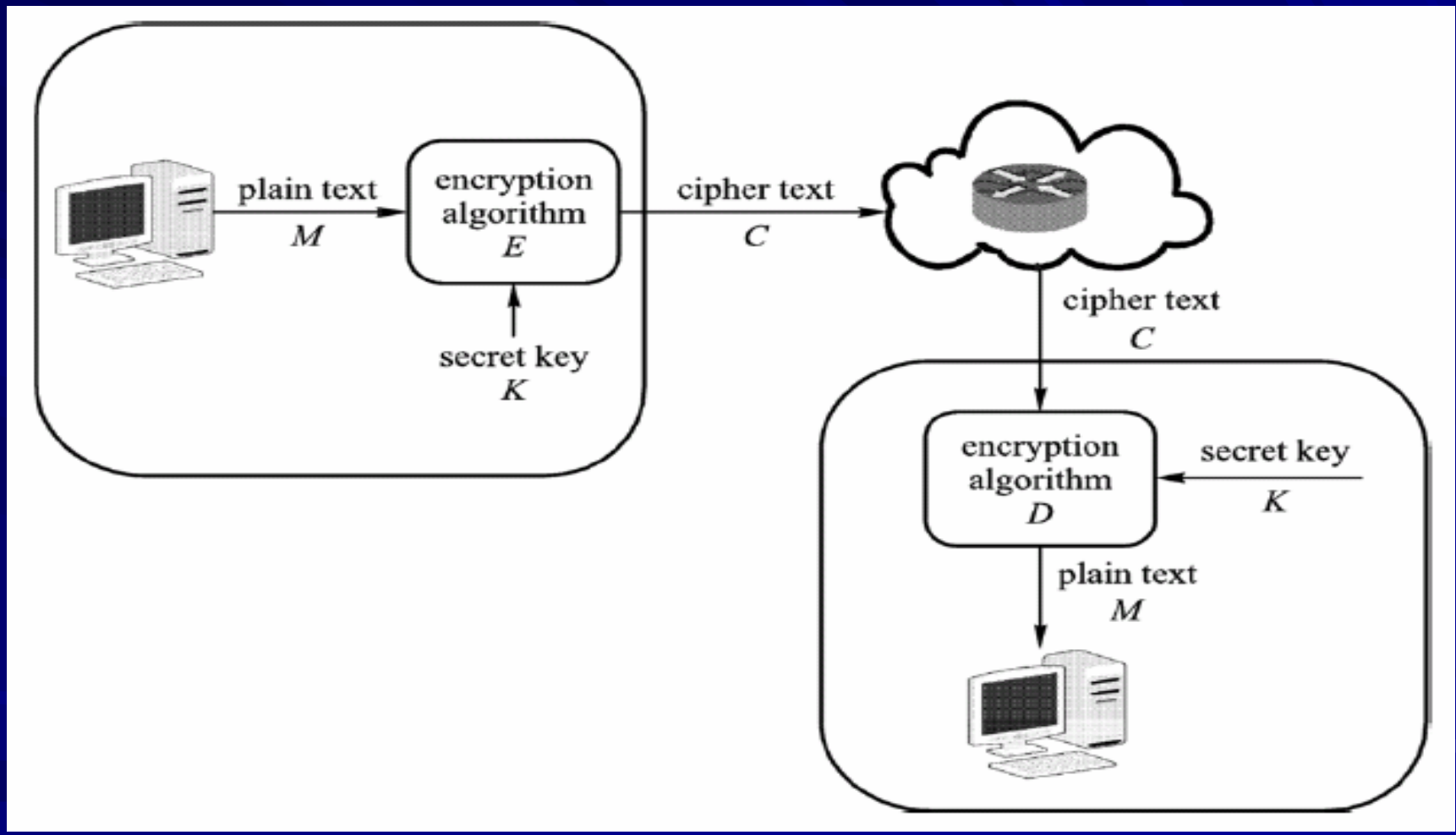
- Mô hình bảo mật cơ bản gồm 4 thành phần:
  - **Hệ thống phần mềm chống độc hại** (Anti-Malicious System software – AMS software): quét các thư mục hệ thống, tập tin, registry, sau đó nhận diện, cách ly hoặc xoá các mã độc hại.
  - **Hệ thống tìm kiếm xâm nhập** (Intrusion Detection System – IDS): giám sát việc đăng nhập vào hệ thống và hành vi của người dùng, phân tích file log để nhận diện và đưa ra cảnh báo khi khi phát hiện có sự xâm nhập.

4. Mô hình bảo mật cơ bản



Bốn thành phần của mô hình bảo mật cơ bản

4. Mô hình bảo mật cơ bản



Mô hình mạng của hệ thống mã hoá

5. Bài tập

1. **Kiến thức cơ bản về mạng máy tính**
    1. Mô tả cấu trúc của một gói TCP và giải thích các chức năng của TCP header.
    2. Mô tả cấu trúc của một gói IP và giải thích các chức năng của IP header.
    3. Trình bày chức năng chính của giao thức ARP.
    4. Trình bày chức năng chính của giao thức ICMP.
    5. Trình bày chức năng chính của giao thức SMTP.
    6. Mô tả giao thức bắt tay ba bước (Three-way handshake).
    7. Nêu sự khác biệt giữa giao thức TCP và UDP.
    8. So sánh những khác biệt chính giữa IPv4 và IPv6.
    9. Trình bày chức năng cơ bản của router và switch.

5. Bài tập

2. Sử dụng các công cụ quản trị mạng

1. Nêu công dụng và cách sử dụng các lệnh *ipconfig, ping, tracert, nslookup, netstat* trong hệ điều hành Windows.
2. Trong hệ điều hành UNIX hay LINUX, nêu cách sử dụng các lệnh *ping, nlslookup, netstat, arp* và giải thích các kết quả thu được.
3. Nêu cách tìm một số thông tin như host name, địa chỉ MAC, địa chỉ IP, subnet mask, default gateway trên máy PC trong hệ điều hành Windows và Linux.
4. Mở cửa sổ cmd trong hệ điều hành Windows và nhập lệnh *netstat –ano*. Giải thích các kết quả thu được. Từ số port và PID thu được nhờ lệnh netstat, dùng Windows Task Manager để nhận diện chương trình đang chạy trên port đó là chương trình nào.

5. Bài tập

3. **Sử dụng các công cụ Network sniffer.**
   1. Download TCPdump từ www.tcpdump và Wireshark từ www.wireshark.org và tiến hành cài đặt các phần mềm này.
   2. Sử dụng Wireshark, sniff các gói ARP từ việc mở một trình duyệt và thăm một số trang web nào đó. Trình bày cách thực hiện và nêu nhận xét.
   3. Tự tìm hiểu rồi nêu cách sử dụng công cụ TCPdump.
   4. Tự gởi 1 email rồi lọc các gói tcp từ cổng 25. Nhận xét?
   5. Thăm vài Websites và lọc tcp ở cổng 80. Giải thích kết quả thu được.
   6. Tìm cách để bắt các gói tcp ở cổng 443. Nhận xét?

5. Bài tập

4. **Sử dụng Scan port để kiểm tra các port đang mở trên máy tính**
    1. Sử dụng một phần mềm scan port bất kỳ để tìm các port đang mở trên máy tính.
    2. Xác định các chương trình đang chạy ứng với những port đang mở.
    3. Đóng lại một số cổng đang mở. Nhận xét.

5. Bài tập

5. Cài đặt phần mềm tường lửa ISA 2006 trên máy Windows Server 2003 và thực hiện các yêu cầu sau:
   1. So sánh System Policy và Access Rule.
   2. Cho biết chức năng các thành phần trên giao diện ISA Management Console.
   3. Nêu cách cấu hình ISA trên máy chủ ISA và trên máy tính khác kết nối từ xa.
   4. Thực hiện tạo một số Access Rule cơ bản.

5. Bài tập

5. So sánh các loại ISA client:
   - SecureNAT client
   - Web Proxy client
   - Firewall client
6. So sánh công dụng và cách hoạt động của các loại Network Templates:
   - Edge Firewall
   - 3-Leg Perimeter
   - Front Firewall
   - Back Firewall
   - Single Network Adapter
7. Web caching là gì và hoạt động như thế nào?

5. Bài tập

8. Thực hiện việc giám sát và lập báo cáo trong ISA server:
   - Cấu hình Intrusion Detection and IP Preferences.
   - Cấu hình giám sát và cảnh báo (Logging and alerts).
   - Cấu hình và chạy báo cáo (Report).
9. Giới hạn dịch vụ và lọc nội dung:
   - Giới hạn mạng nội bộ truy cập Internet.
   - Lọc nội dung trang Web.
   - Cấm Internal Network truy xuất đến trang Web.

Thank You !