THƯƠNG MẠI ĐIỆN TỬ

Chương 7.
BẢO MẬT VÀ AN TOÀN TRONG TMĐT

ThS. Nguyễn Thị Thanh Trúc

Nội dung

- Giới thiệu
- Các vấn đề bảo mật cơ bản
- Các loại tấn công trên mạng
- Một số mối đe dọa
- Chính sách bảo vệ
- An toàn mạng dành cho doanh nghiệp VN tham gia TMĐT.

Giới thiệu

- Sự xuất hiện mạng internet cho phép mọi người có thể truy cập, chia sẻ và khai thác thông tin một cách dễ dàng và hiệu quả.
- Tuy nhiên lại nảy sinh các vấn đề an toàn thông tin, các nguy cơ dẫn đến việc thông tin của bạn bị tiết lộ, hư hỏng hoặc phá hủy hoàn toàn.

Giới thiệu

- Theo CERT (Computer Emegency Respones Team), số lượng các vụ tấn công trên internet ngày càng tăng, bên cạnh đó các phương pháp tấn công cũng ngày càng tinh vi, hoàn thiện.
- Chính vì vậy, việc bảo mật an ninh mạng là vấn đề nóng hổi trong hoạt động thương mại điện tử.

Giới thiệu

- Ngày này, việc an toàn và bảo mật trên mạng đã có nhiều tiến triển:
  - Bức tường lửa (firewall)
  - Mã hóa (encryption)
  - Chữ ký điện tử (digital signature)

Giới thiệu

- Tuy nhiên, vẫn còn tồn tại nhiều nguy cơ đe dọa:
  - Điểm yếu là ý thức và hành vi của người dùng
  - Đánh lừa người khác để lấy thông tin
  - Tấn công hay phá hoại thông qua lỗ hổng của hệ điều hành
  - Mở thư đã bị nhiễm virus
  - Xem những trang web chứa một số đoạn mã có ý đồ xấu
  - …

Giới thiệu

- Làm thế nào để khách hàng tin tưởng khi thực hiện các giao dịch trên mạng?

- Nhà cung cấp dịch vụ giao dịch trực tuyến + ISP có đảm bảo các giao dịch trên mạng được an toàn?

Các vấn đề bảo mật cơ bản

- Trong EC, vấn đề bảo mật không chỉ là ngăn ngừa hay đối phó với các cuộc tấn công và xâm nhập.
- Xét ví dụ sau:
  - Một khách hàng cần có thông tin của các sản phẩm trên website của một công ty nào đó
  - Máy chủ yêu cầu khách hàng điền thông tin cá nhân
  - Sau khi cung cấp thông tin cá nhân, khách hàng mới nhận được thông tin của sản phẩm
  - Giải pháp bảo mật cho trường hợp này là gì?

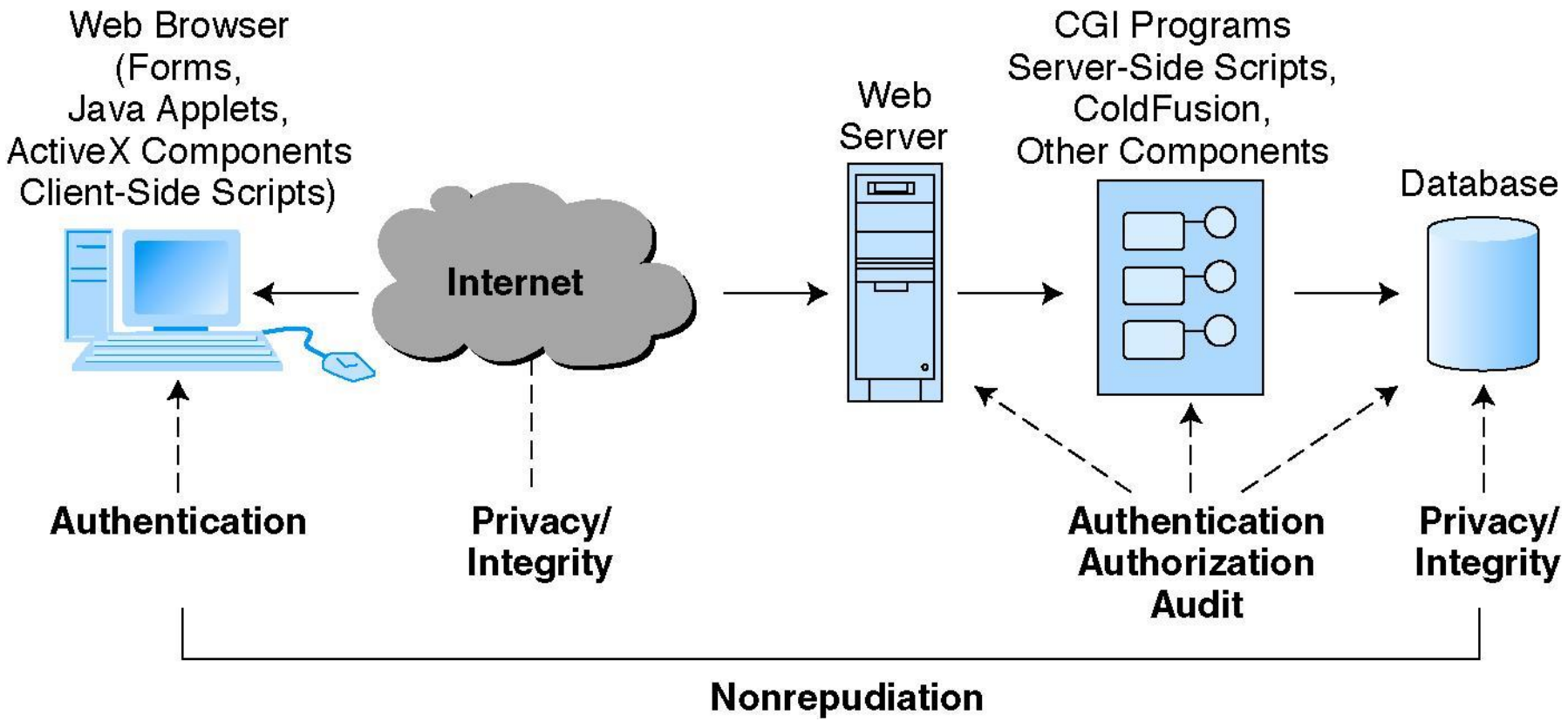
Các vấn đề bảo mật cơ bản

- Về phía khách hàng:
  - Trang web này là của một công ty hợp pháp?
  - Có chứa các đoạn mã nguy hiểm?
  - Có cung cấp thông tin cá nhân cho một website khác?
- Về phía công ty:
  - Người dùng có ý định phá server hay sửa nội dung của trang web?
- Khác:
  - Có bị ai nghe lén trên đường truyền?
  - Thông tin được gửi và nhận có bị sửa đổi?

Các vấn đề bảo mật cơ bản

- Bảo mật trong EC:
  - Authentication – Chứng thực người dùng
    - Sự ủy quyền thông qua mật mã, thẻ thông minh, chữ ký
  - Authorization – Chứng thực quyền sử dụng
  - Auditing – Theo dõi hoạt động
  - Confidentiality (Privacy) – Giữ bí mật nội dung thông tin
  - Integrity – Toàn vẹn thông tin
  - Availability – Khả năng sẵn sàng đáp ứng
  - Nonrepudiation – Không thể từ chối trách nhiệm

Các vấn đề bảo mật cơ bản



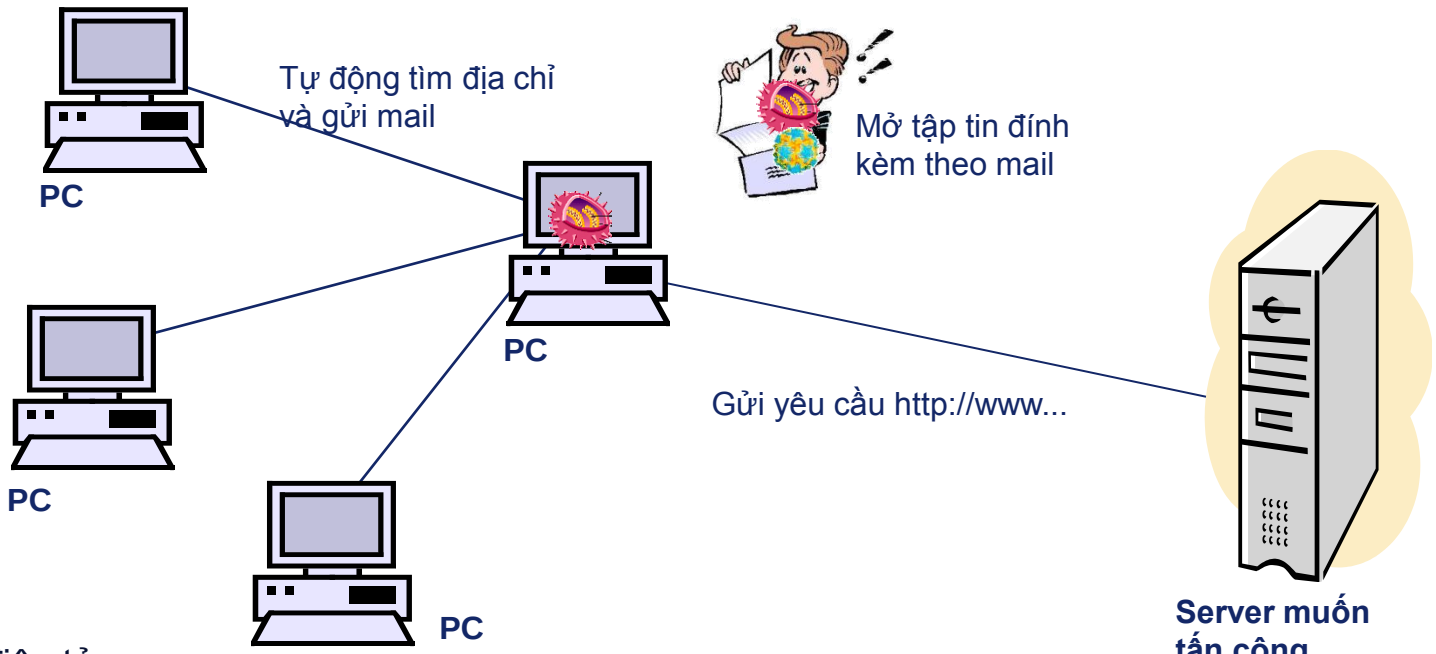
Các loại tấn công trên mạng

- Không sử dụng chuyên môn:
  - Lợi dụng sức ép, tâm lý để đánh lừa người dùng và làm tổn hại đến mạng máy tính
  - Hình thức: Gọi điện thoại, gửi mail, phát tán links
- Sử dụng chuyên môn:
  - Các phần mềm, kiến thức hệ thống, sự thành thạo
  - Hình thức:
    - DoS, DDoS
    - Virus, worm, trojan horse

DoS

Denial-of-Service

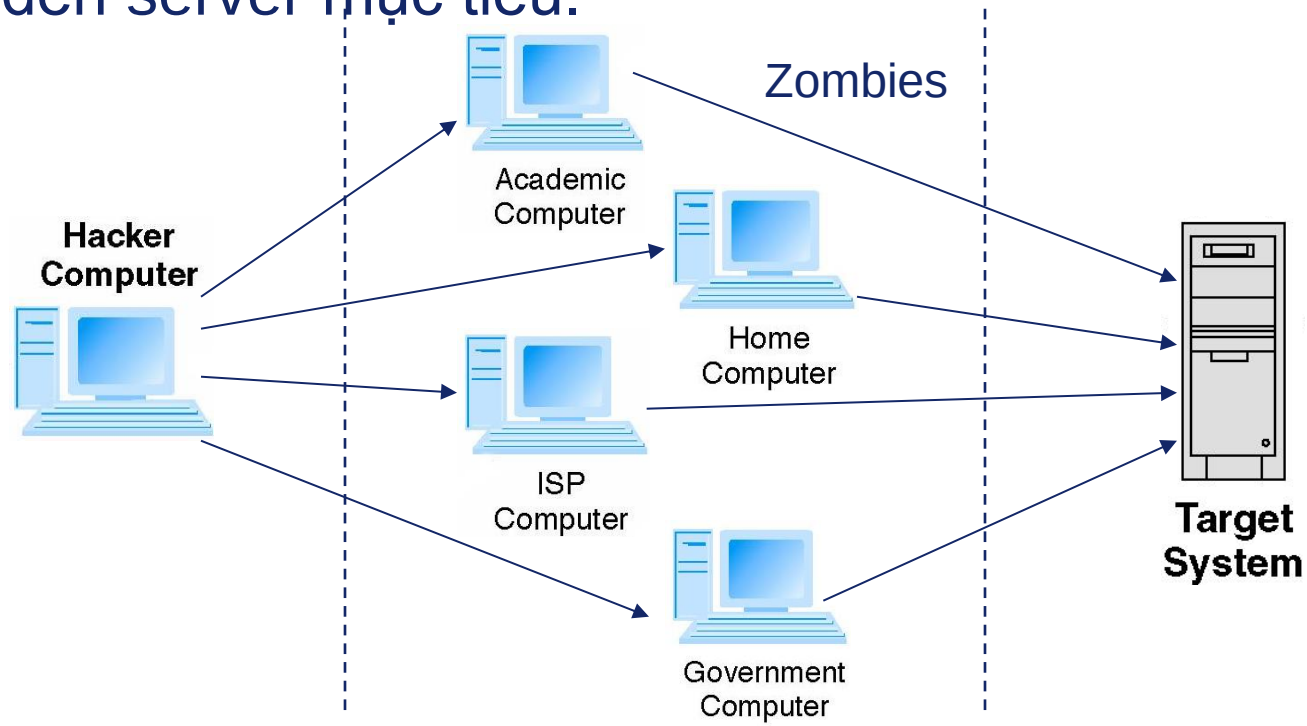
- Các hacker lợi dụng một máy tính nào đó gửi hàng loạt các yêu cầu đến server mục tiêu với ý định làm quá tải tài nguyên của server đó



DDoS

❖ Distributed Denial-of-Service

- Các hacker xâm nhập vào nhiều máy tính và cài phần mềm. Khi có lệnh tấn công, các phần mềm sẽ gửi yêu cầu đến server mục tiêu.



Hacking

- Bị tấn công từ chối phục vụ (DoS).
- Bị cướp tên miền:
  - Tìm email quản lý tên miền.
  - Lừa chủ tài khoản email để lấy được password.
  - Yêu cầu nhà cung cấp dịch vụ quản lý tên miền cung cấp password để quản lý tên miền.
  - Thay đổi thông số tên miền, chuyển tên miền sang website quản lý khác, thay đổi password quản lý,…

Hacking

- Bị xâm nhập host hoặc dữ liệu trái phép:
  - Tấn công nội bộ (local attack) tức hacker mua một host trên cùng một server với host “nạn nhân”.
  - Tìm kẽ hở để đột nhập thông qua việc tìm kiếm trên các search engine.
  - Tìm cách có được password của host.
  - Nghiên cứu kẽ hở trong lập trình để thâm nhập vào host.
  - Thâm nhập vào cơ sở dữ liệu của website.

Các loại tấn công trên mạng

- Spam (thư rác):
  - Người nhận mỗi ngày có thể nhận vài chục, đến vài trăm thư rác: dung lượng, thời gian tải về...

- Virus:
  - Là một chương trình máy tính có khả năng tự nhân bản và lan tỏa: chiếm tài nguyên, tốc độ xử lý máy tính chậm đi, có thể xóa file, format lại ổ cứng,…

Các loại tấn công trên mạng

- Sâu máy tính (worms):
  - Khác với virus ở chỗ sâu không thâm nhập vào file mà thâm nhập vào hệ thống.
  - Ví dụ: sâu mạng (network worm) tự nhân bản trong toàn hệ thống mạng, sâu email tự gửi nhân bản của chúng qua hệ thống email.

Các loại tấn công trên mạng

- Trojan:
  - Là một loại chương trình nguy hiểm được dùng để thâm nhập vào máy tính mà người sử dụng máy tính không hay biết.
  - Ví dụ: cài đặt chương trình theo dõi bàn phím (keyloger)

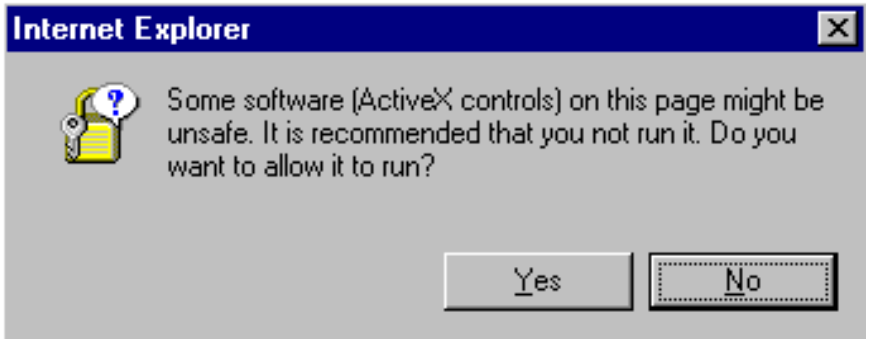
Các loại tấn công trên mạng

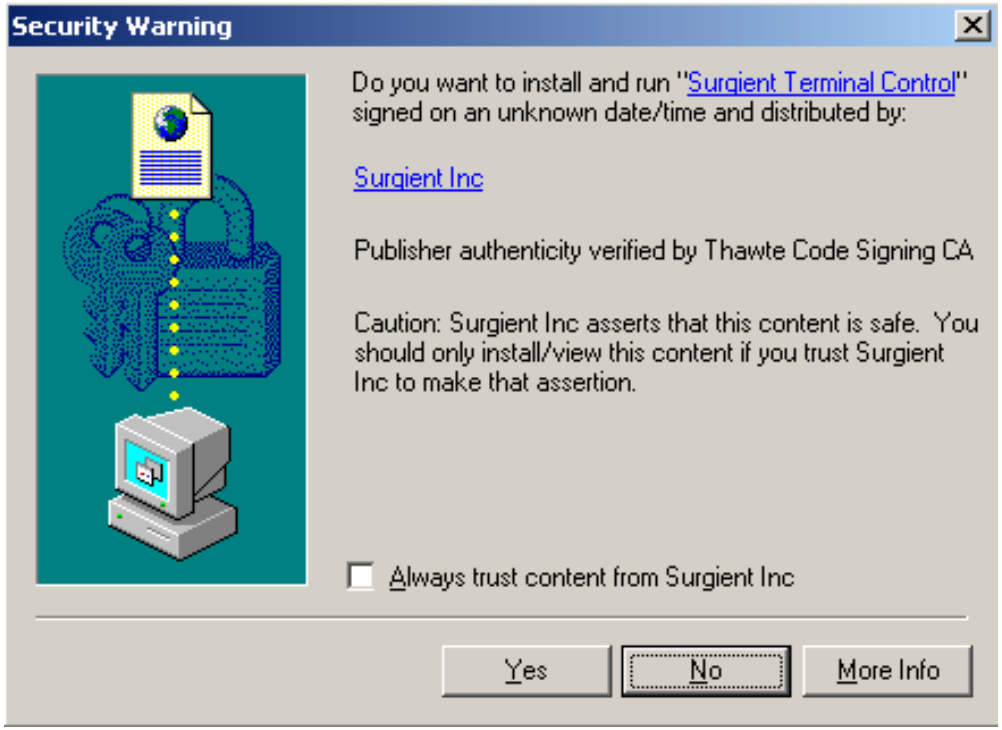
- Phishing: giả dạng những tổ chức hợp pháp như ngân hàng, dịch vụ thanh toán qua mạng,...
  - Gửi email yêu cầu người nhận cung cấp thông tin cá nhân và thông tin tín dụng.
  - Tuyên bố người nhận đã may mắn trúng giải thưởng rất lớn.
  - Tạo ra những website bán hàng, bán dịch vụ "y như thật" trên mạng.

Mối đe dọa tại client

- Trang web
  - Hiển thị nội dung
  - Cung cấp các liên kết (link)
  - Active content
    - Đoạn chương trình được nhúng vào trang web và tự động thực hiện
    - Tự động tải về và mở file
    - Cookie, java applet, java script, activeX control
    - Tùy vào mức độ bảo mật tại Client, trình duyệt hiện thị hộp thoại cảnh báo

Mối đe dọa tại client





Mối đe dọa tại client

- Plug-in
  - Chương trình làm tăng khả năng trình bày của các trình duyệt (browser)
  - Mở nhạc, phim, animation
  - QuickTime, RealPlayer, FlashPlayer
  - Có thể nhúng các lệnh với mục đích xấu làm hư hại máy tính
- Tập tin đính kèm theo thư điện tử (e-mail)

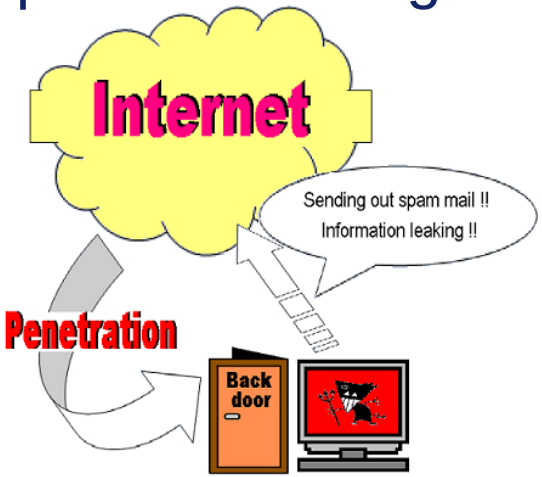
Mối đe dọa môi trường internet

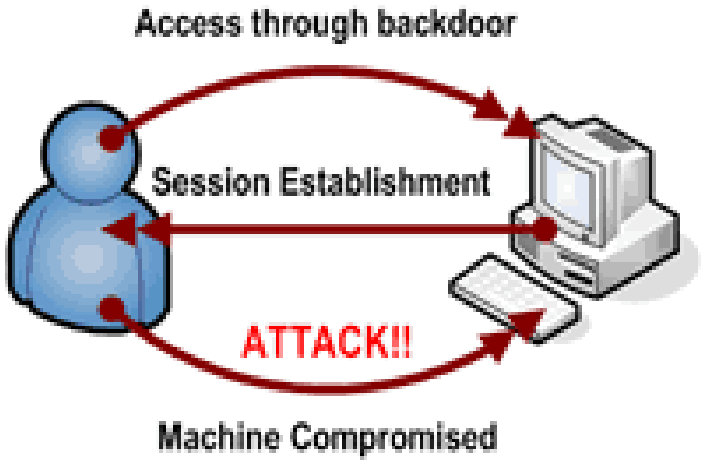
- Các gói tin di chuyển trên Internet theo một con đường không dự kiến trước:
  - Người dùng không biết gói tin sẽ lưu lại ở nơi nào

  → Gói tin bị đọc trộm, sửa đổi, xóa
  - "sniffer program" được sử dụng để bắt gói tin

Mối đe dọa môi trường internet

- Một số các phần mềm EC vẫn còn nhiều lỗ hổng (backdoor):
  - Lỗi lập trình ngẫu nhiên hay cố ý của người phát triển phần mềm
  - Nếu có kiến thức và phát hiện được backdoor, kẻ xấu có thể quan sát các giao dịch, xóa hay đánh cắp dữ liệu





Mối đe dọa tại server

- Web Server
  - Có thể được cấu hình chạy ở nhiều cấp độ quyền
    - Quyền cao nhất – cho phép thực thi các lệnh cấp thấp, truy xuất bất kỳ thành phần nào trong hệ thống
    - Quyền thấp nhất – chỉ có thể thực thi chương trình, không cho phép truy xuất nhiều các thành phần trong hệ thống

  →Quyền càng cao, web server càng bị nguy hiểm

Mối đe dọa tại server

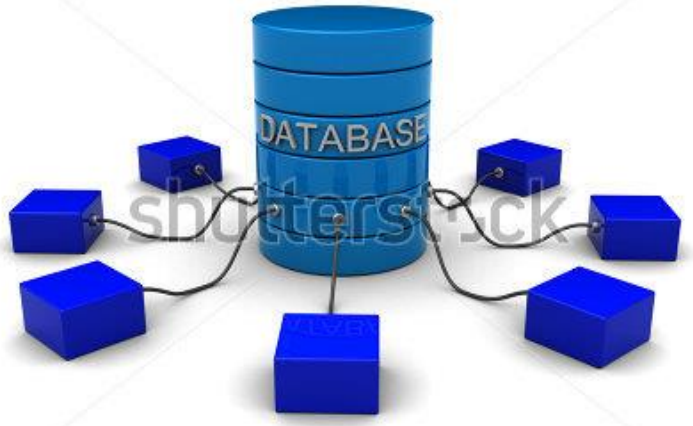
- Web Server
  - Nội dung của các thư mục có thể thấy được từ browser
    - Trang web mặc định không được cấu hình chính xác : Index.html, Index.htm
  - Yêu cầu người dùng nhập tên và mật mã ở một số trang
    - Sử dụng cookie

Index of /musiclsx

Name	Last modified	Size	Description
Parent Directory		-	
01 - Dau co loi lam.mp3	08-Dec-2005 00:55	2.3M	
01 - Khanh Ngoc - Mong thuy tinh.mp3	08-Dec-2005 00:51	3.4M	
04 - Em Se La Nguoi Ra Di.mp3	08-Dec-2005 00:49	4.9M	
04 - Roi Mai Thuc Giac.mp3	08-Dec-2005 00:48	3.1M	
DuaBe.wma	06-Jan-2006 09:16	3.2M	
artist/	26-Apr-2006 15:29	-	
bactinh.mp3	08-Dec-2005 00:47	4.6M	
binhthuongthoi.mp3	19-Jan-2006 16:50	8.7M	
cambay.mp3	08-Dec-2005 00:51	4.1M	
chimtrangmocoi.mp3	08-Dec-2005 00:48	5.5M	
demnghetiengmua.mp3	08-Dec-2005 00:52	3.4M	
divangcuoctinh.mp3	07-Feb-2006 16:28	6.2M	
duongnhutada.mp3	26-Apr-2006 15:09	7.7M	
emve.mp3	03-Jan-2006 14:47	3.8M	
kedungsautinhyeu.mp3	10-Mar-2006 09:38	5.5M	
loinguyencautinhyeu.mp3	07-Apr-2006 09:55	7.2M	
mattroitrongem.mp3	29-Mar-2006 11:13	10M	

Mối đe dọa tại server

- Database Server
  - Tập tin chứa dữ liệu có thể được truy xuất bằng quyền hệ thống
    - Quyền quản trị của hệ điều hành
  - Dữ liệu trong CSDL có thể bị lộ nếu không được mã hóa



Chính sách bảo vệ

- Kỹ thuật WaterMarking và 1 số công ty cung cấp giải pháp
- Thiết lập bảo vệ trong trình duyệt Web
- Chứng nhận số (chứng thực số)
- Bảo mật khi truyền gửi thông tin
- Các giải thuật mã hóa, các nghi thức truyền thông mã hóa
- Văn bản với chữ ký điện tử
- Proxy, FireWall

Kỹ thuật WaterMarking

- Cho phép nhúng thông tin tác giả vào các tài liệu số hóa sao cho chất lượng trực quan của tài liệu không bị ảnh hưởng và khi cần có thể dò lại được watermark đã nhúng nhằm xác nhận bản quyền.
- Đây là kỹ thuật ẩn giấu thông tin (steganography) đặc biệt nhằm đưa các dấu hiệu vào ảnh số.
- Ngoài ra, kỹ thuật watermarking còn đòi hỏi sự mạnh mẽ trong việc chống lại các thao tác tấn công nhằm xóa bỏ thông tin được nhúng.

Kỹ thuật WaterMarking

- Có hai hướng áp dụng chính của kỹ thuật watermarking:
  - Xác nhận (chứng thực) thông tin
  - Đánh dấu bảo vệ bản quyền
- Sử dụng Liquid Audio áp dụng công nghệ của Verance Corporation (âm nhạc).
- Photoshop: với Digimarc.
- Ngày nay, các công ty chuyên kinh doanh các hệ thống watermarking đã tăng đáng kể.

Kỹ thuật WaterMarking

- Một số công ty cung cấp các phần mềm bảo vệ bản quyền:
  - SoftLock Services
    - Cho phép khóa các tập tin
    - Gửi các tập tin lên mạng
    - Sử dụng 1 khóa giải mã (sau khi trả tiền) để có thể sử dụng

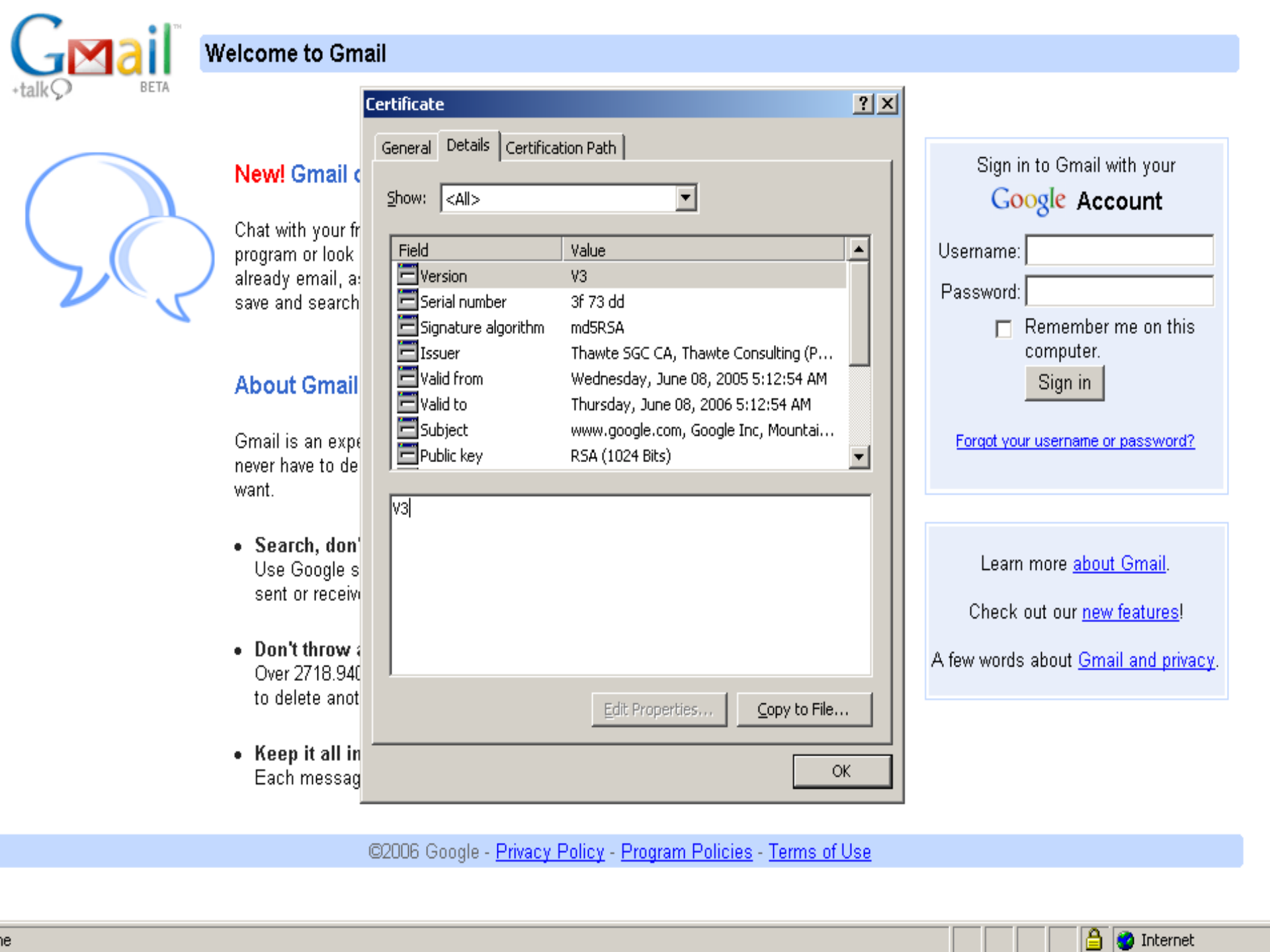
Bảo vệ trong trình duyệt Web

- Trình duyệt phải có khả năng nhận ra các trang web có chứa Active content
  - Cho phép người dùng xác nhận active content có đáng tin cậy hay không
    - Chứng nhận số (Digital Certificate)
- Các trình duyệt Netscape Navigator,Microsoft Internet Explorer,.. cho phép người sử dụng kiểm soát và quyết định tải về các thông tin dạng Active
- Phần mềm chống virus

Chứng nhận số (DC)

- Là một thông điệp đính kèm theo thư điện tử hay active content nhằm mục tiêu cho biết người gửi thư hoặc trang web đó là ai
  - Chứng nhận không nói lên được chương trình cần cài đặt là chất lượng hay có ích
  - Chứng nhận cho biết một điều chắc chắn chương trình là thật

  →Nếu người sử dụng tin tưởng vào các nhà phát triển phần mềm, thì sản phẩm của họ cũng có thể được tin tưởng


Gmail
talk
BETA
Welcome to Gmail
New! Gmail c
Chat with your fr
program or look
already email, a
save and search
About Gmail
Gmail is an expe
never have to de
want.
Search, don'
Use Google s
sent or receiv
Don't throw
Over 2718.94
to delete anot
Keep it all in
Each messag
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
3f 73 dd
Signature algorithm
md5RSA
Issuer
Thawte SGC CA, Thawte Consulting (P...
Valid from
Wednesday, June 08, 2005 5:12:54 AM
Valid to
Thursday, June 08, 2006 5:12:54 AM
Subject
www.google.com, Google Inc, Mountai...
Public key
RSA (1024 Bits)
V3
Edit Properties...
Copy to File...
OK
Sign in to Gmail with your
Google Account
Username:
Password:
Remember me on this computer.
Sign in
Forgot your username or password?
Learn more about Gmail.
Check out our new features!
A few words about Gmail and privacy.
©2006 Google - Privacy Policy - Program Policies - Terms of Use
Internet

Chứng nhận số (DC)

- Chứng nhận số phải do một đơn vị có uy tín cấp
- Trung tâm Chứng thực kỹ thuật số - CA:
  - Cấp và quản lý chứng thực số cho tất cả các đối tượng tham gia trong môi trường giao dịch điện tử.
  - Chứng thực số cho các cá nhân và tổ chức thực hiện an toàn các giao dịch trong môi trường điện tử, như gửi nhận e-mail, mua bán hàng hoá, trao đổi thông tin, phát triển phần mềm...

Chứng nhận số (DC)

- Một số chức năng chính của Trung tâm chứng thực số:
  - Đăng ký xin cấp chứng thực số
  - Xác thực và cấp chứng thực số
  - Truy lục và tìm kiếm thông tin về chứng thực số
  - Yêu cầu thay đổi, gia hạn,…
  - Quản lý chứng thực số

Chứng nhận số (DC)

- Công cụ an toàn, bảo mật và xác thực hợp pháp cho các hệ thống hoạt động thương mại điện tử: các website giao dịch B2B, các website bán hàng, hệ thống thanh toán trực tuyến,...
- Sử dụng chứng thực số giúp cho bảo đảm an toàn các giao dịch điện tử. Tránh được các nguy cơ, giả mạo thông tin, lộ các thông tin nhậy cảm, mạo danh, xuyên tạc và thay đổi nội dung thông tin.

Câu hỏi 1

Xin cấp chứng thực số ở đâu?

Đã có cơ quan cấp chứng thực số tại VN?

Bảo vệ khi truyền thông

- Bảo vệ thông tin, tài sản trong quá trình chuyển tải giữa các máy khách và máy phục vụ
- Bao gồm các yêu cầu:
  - Bảo mật kênh truyền
  - Bảo đảm toàn vẹn dữ liệu
  - Bảo đảm hợp lệ, phù hợp
  - Xác nhận - Authentication

Phương pháp bảo vệ

❖ Mã hóa - Encryption

- Chuyển đổi thông tin bằng phương pháp toán học: dựa trên 1 chương trình + khóa bí mật để tạo ra các ký tự khó hiểu
- Ẩn giấu thông tin – Steganography
- Thông tin vô hình trước người sử dụng
- Mã hóa thông tin – Cryptography
- Chuyển đổi dữ liệu gốc sang dạng không thể đọc, không có ý nghĩa,...

Mã hóa – Encryption

- Mã hóa là quá trình trộn văn bản với khóa mã tạo thành văn bản không thể đọc được trên mạng.
- Khi nhận được, dùng khóa mã giải mã thành bản gốc.
- Mã hóa và giải mã gồm 4 phần cơ bản:
  1. Văn bản nhập vào – plaintext
  2. Thuật toán mã hóa – Encryption
  3. Văn bản đã mã – ciphertext
  4. Giải mã – Decryption

Mã hóa – Encryption

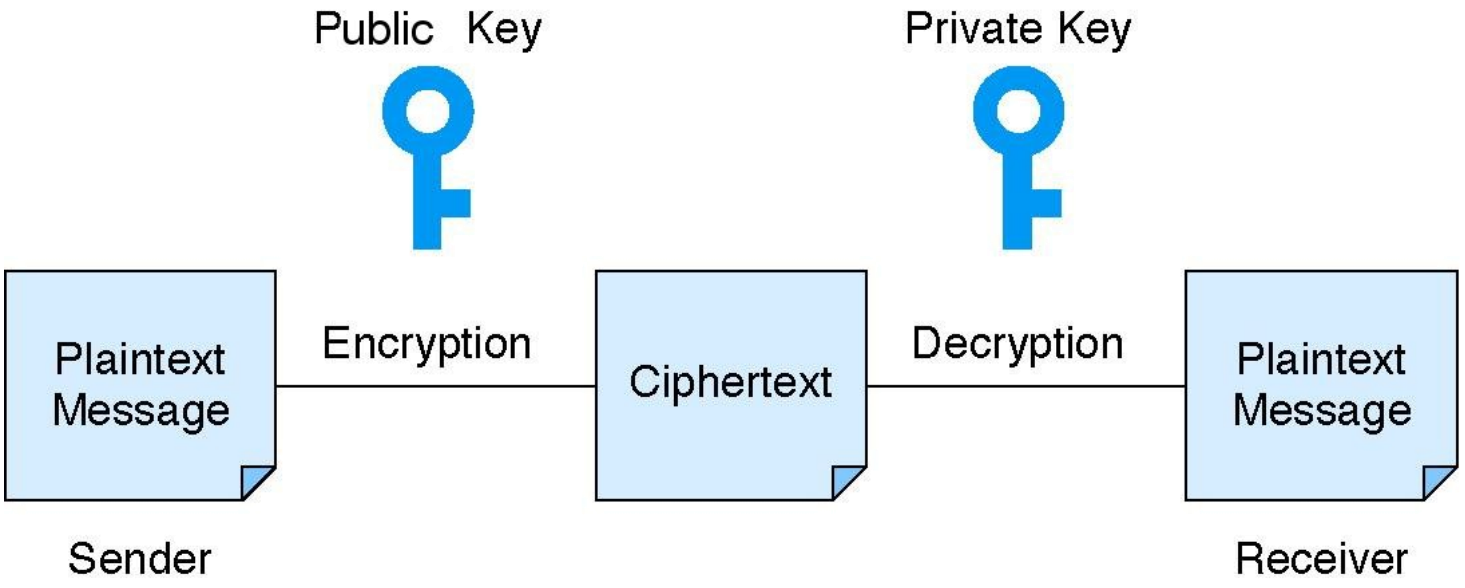
- Các giao thức bảo mật thông dụng:
  - Cơ chế bảo mật SSL
  - Cơ chế bảo mật SET
- Có thể phân thành 3 nhóm:
  - Mã hóa Hash
  - Mã hóa bất đối xứng – Asymmetric (Public-key) Encryption
  - Mã hóa đối xứng – Symmetric (Private-key) Encryption

Mã hóa Hash

- Sử dụng thuật toán Hash để đưa ra một con số từ một thông điệp có độ dài bất kỳ
  - Xung đột giá trị băm rất hiếm khi xảy ra
  - Không sử dụng khóa
  - Chuỗi được mã hóa không thể giải mã thành chuỗi ban đầu
- Một số thuật toán:
  - MD2, MD4, MD5
  - …

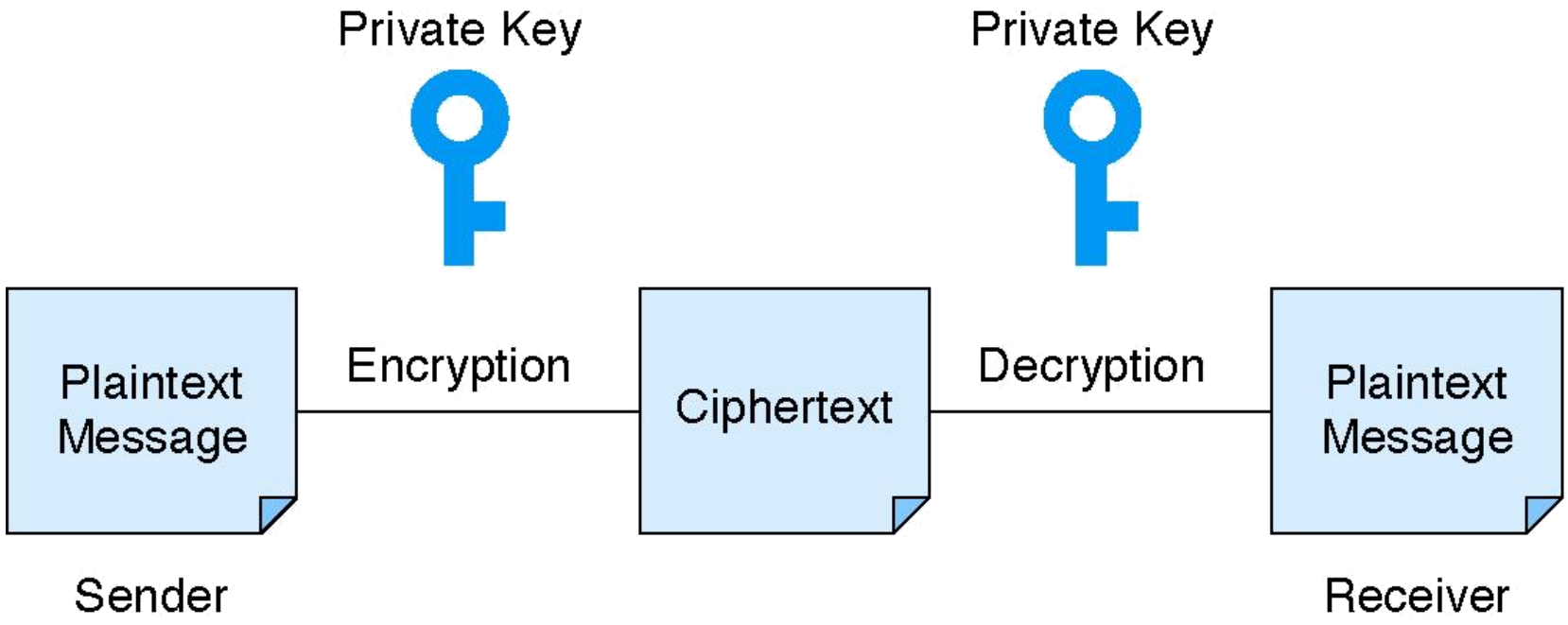
Mã hóa bất đối xứng

- Mã hóa dựa vào 2 loại khóa:
  - Public key – mã hóa thông điệp
  - Private key – giải mã thông điệp
- Thuật toán RSA



Mã hóa đối xứng

- Mã hóa chỉ sử dụng 1 loại khóa:
  - Private key – mã hóa và giải mã thông điệp
- Thuật toán: 3DES, Rijndael,…



Cơ chế bảo mật SSL

- Là nghi thức bảo mật kết nối giữa client (máy khách) và server (máy chủ).
- Máy khách và máy chủ qui ước cấp độ bảo mật, các qui ước xác nhận và các cơ chế bảo vệ thông tin liên lạc khác
- Nhiều cơ chế, kiểu loại bảo mật cho việc thông tin liên lạc giữa các máy tính

Câu hỏi 2

Các vấn đề nảy sinh khi gửi một tài liệu quan trọng, một đơn hàng, một hợp đồng,...

Chữ ký điện tử được thực hiện với một văn bản, tài liệu như thế nào?

Chữ ký điện tử

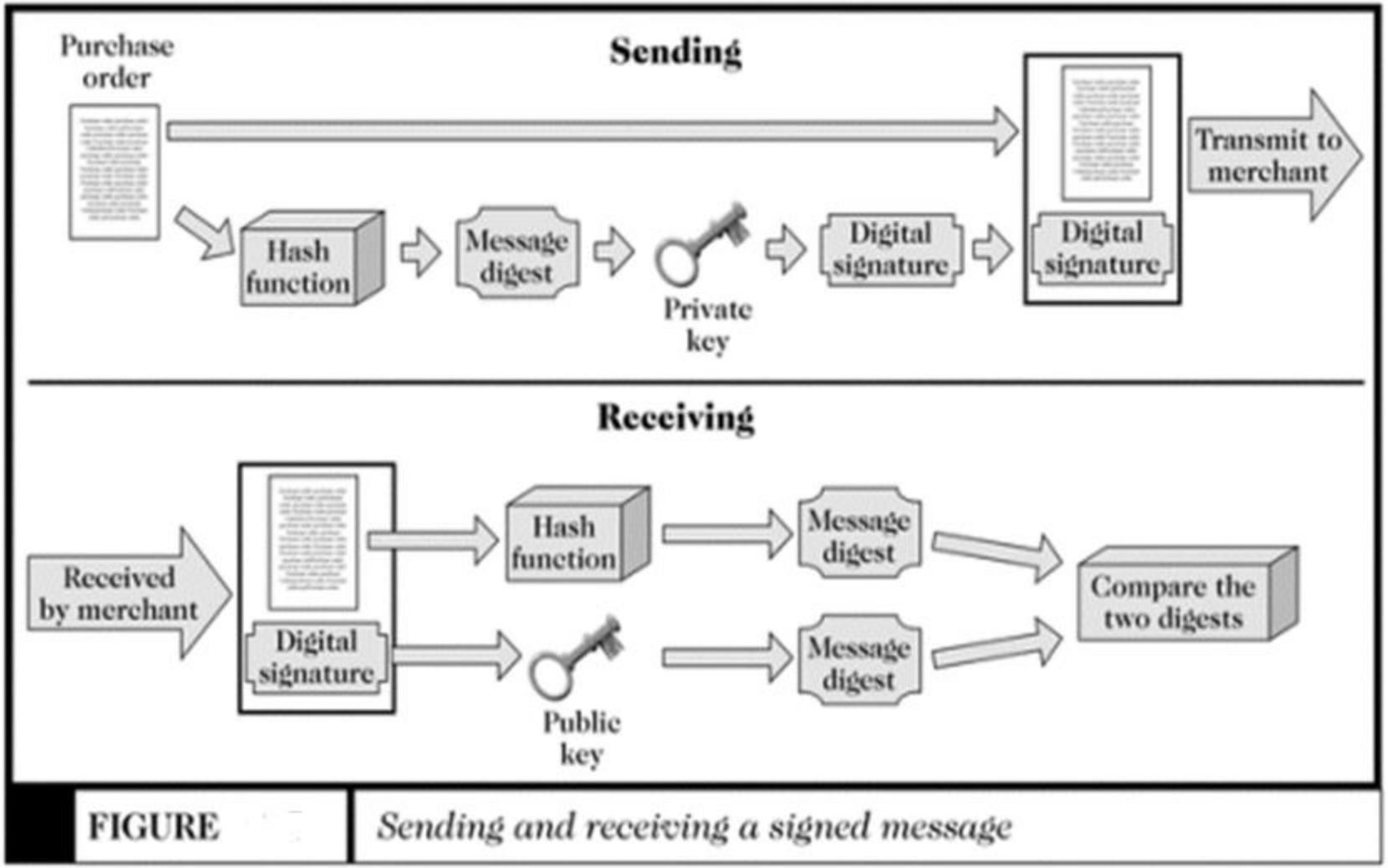


FIGURE *Sending and receiving a signed message*

Chữ ký điện tử

- Là đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.
- Được tạo ra bằng cách áp dụng thuật toán băm một chiều trên văn bản gốc để tạo ra bản phân tích văn bản (message digest) hay còn gọi là fingerprint, sau đó mã hóa bằng private key tạo ra chữ ký số đính kèm với văn bản gốc để gửi đi.

Chữ ký điện tử

- Dữ liệu dưới dạng điện tử (từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác)
- Gắn liền hoặc kết hợp một cách logic với thông điệp dữ liệu
- Có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp được ký.

Chữ ký điện tử

- Các cách tạo chữ ký điện tử:
  - Vân tay
  - Sơ đồ võng mạc
  - Sơ đồ tĩnh mạch trong bàn tay
  - ADN
  - Các yếu tố sinh học khác
  - Công nghệ mã hóa
  - …

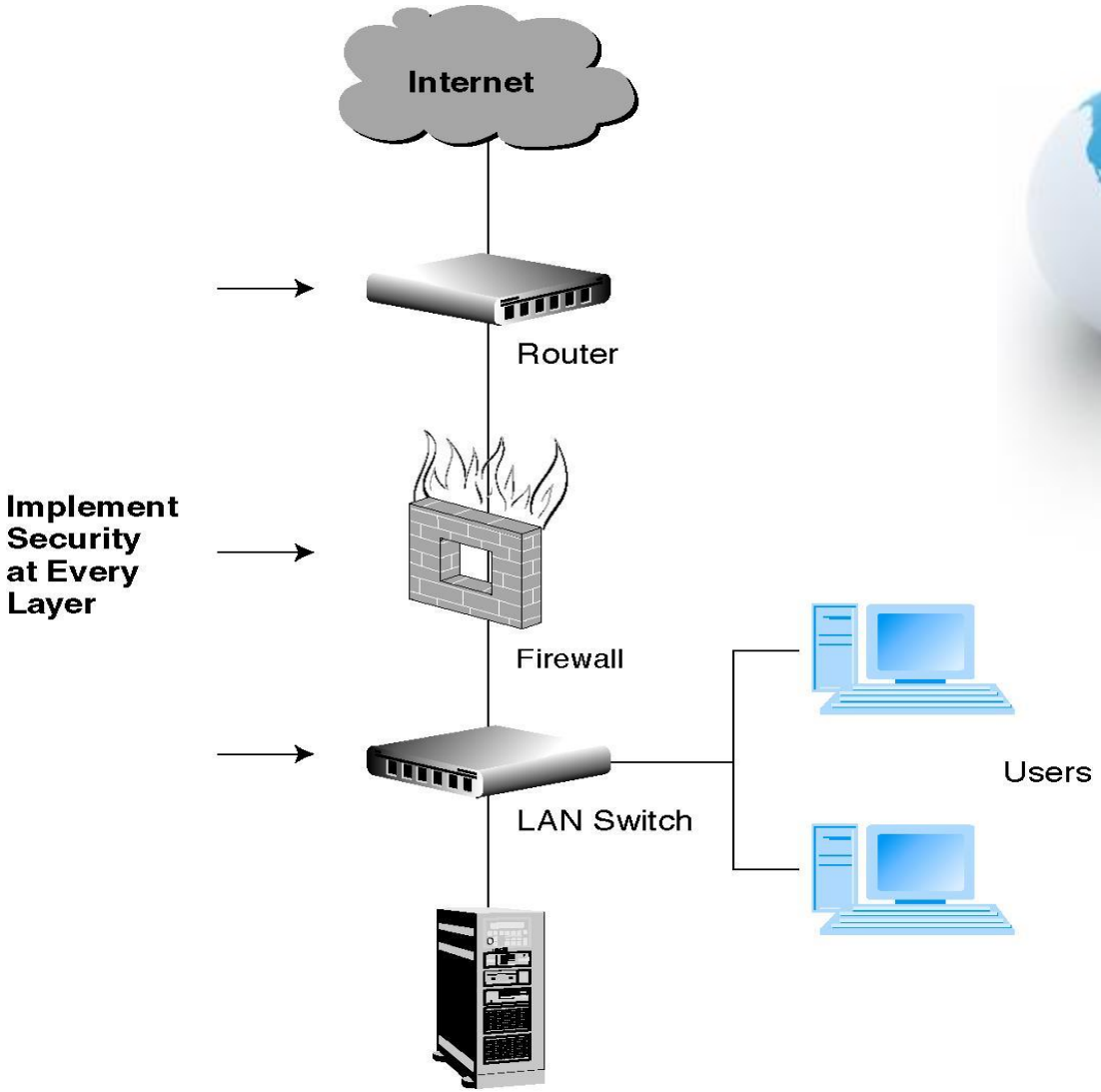
Bảo vệ máy chủ Commerce Server

- Điều khiển truy cập và xác thực người dùng:
  - Những ai có thể đăng nhập và có quyền sử dụng trên máy chủ (server)
  - Yêu cầu máy khách gửi một “xác nhận” (certificate) để định danh
  - Server kiểm tra “timestamp” của giấy xác nhận: thời gian hiệu lực
  - Có thể sử dụng một hệ thống callback nhằm kiểm tra địa chỉ và tên máy khách với một danh sách

Bảo vệ với chức năng của Hệ điều hành

- Phần lớn các hệ điều hành sử dụng cơ chế chứng thực: tài khoản/mật khẩu
- Phương án thường sử dụng: Firewall
- Mọi thông tin vào/ra khỏi mạng đều phải đi qua tường lửa
- Chỉ cho phép các gói thông tin xác định
- Firewall phải cấu hình tốt nhằm chống lại các cuộc xâm nhập

Tường Lửa – Firewalls



Tường Lửa – Firewalls

- Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet.
- Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet.
- Ngăn chặn các tấn công từ Internet hay từ các mạng khác

Tường Lửa – Firewalls

- Kiểm soát những dịch vụ truy nhập ra ngoài.
- Kiểm soát những dịch vụ phép truy nhập vào trong.
- Theo dõi luồng dữ liệu mạng.
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
- Kiểm soát người sử dụng và việc truy nhập NSD.
- Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.

An toàn mạng dành cho doanh nghiệp VN tham gia TMĐT

- Hacking: DN thường xuyên kiểm tra website để kịp thời phát hiện sự cố:
  - Bị tấn công từ chối phục vụ: Nếu thuê dịch vụ host, DN yêu cầu nhà cung cấp dịch vụ xử lý.
  - Bị cướp tên miền: DN có thể tự quản lý password của tên miền hoặc giao cho nhà cung cấp dịch vụ quản lý.

	DN tự quản lý tên miền	Nhà cung cấp dịch vụ quản lý tên miền
Thuận lợi	DN chủ động quản lý tên miền	DN không bận tâm về việc bảo mật password của tên miền
Vấn đề	DN chịu trách nhiệm bảo mật password của tên miền	DN có thể bị mất tên miền vì lỗi sơ suất hoặc cố ý của nhà cung cấp dịch vụ

An toàn mạng dành cho doanh nghiệp VN tham gia TMĐT

- Hacking: DN thường xuyên kiểm tra website để kịp thời phát hiện sự cố:
  - Bị xâm nhập host hoặc dữ liệu trái phép:
    - Khi xảy ra sự cố, doanh nghiệp yêu cầu nhà cung cấp dịch vụ host nêu rõ phương thức xử lý.
    - Yêu cầu nhà cung cấp dịch vụ host sao lưu (backup) dữ liệu website thường xuyên.
    - Nhà cung cấp dịch vụ phải có ít nhất 2 server để kịp thời chuyển sang server khác khi có sự cố.

An toàn mạng dành cho doanh nghiệp VN tham gia TMĐT

- Tự bảo vệ mật khẩu:
  - Khi có nhiều tài khoản (TK quản lý tên miền, TK quản lý website,…) thì ít người biết password của TK càng tốt.
- An toàn mạng nội bộ:
  - Nên có quy định sử dụng mạng nội bộ, quy định về phòng chống virus,…
- An toàn dữ liệu, thông tin
  - Không lưu trong mạng nội bộ những thông tin không cần chia sẻ nhiều người.
  - Sao lưu dữ liệu ra đĩa CD thường xuyên.

An toàn mạng dành cho cá nhân

- Khi có spam?
- Email yêu cầu cung cấp thông tin?
- Nếu mua qua mạng bằng thẻ tín dụng?
- Khi có mail lạ gởi file đính kèm?
- Khi duyệt web?
- Đăng nhập tài khoản sử dụng?
- Sử dụng máy tính dùng chung?

Sai lầm của tổ chức về an ninh TMĐT

- Đánh giá thấp vai trò của thông tin
- Chỉ tập trung vào an toàn nội bộ
- Quản trị an toàn TMĐT bị động
- Không chú trọng vào đào tạo và huấn luyện nhân viên thực hiện các biện pháp an toàn TMĐT
- Coi vấn đề an toàn TMĐT là trách nhiệm riêng của bộ phận IT

Qui trình quản trị rủi ro an toàn TMĐT

- Xác định những mục tiêu cần bảo vệ: máy tình, dữ liệu, website, thông tin,…
- Xác định những nguy cơ, rủi ro mà những mục tiêu này có thể gặp phải.
- Thực hiện các giải pháp an toàn TMĐT tùy theo mức độ ưu tiên.

Q/A?