Chuyên đề Thương mại điện tử

Bảo mật trong EC

Lê Thị Nhàn – Lương Vĩ Minh
lvminh@fit.hcmuns.edu.vn
8324467-801

Nội dung chi tiết

- Giới thiệu
- Các vấn đề bảo mật
- Các loại tấn công
- Một số mối đe dọa
- Chính sách bảo vệ

Nội dung chi tiết

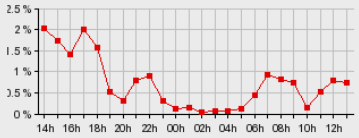
- Giới thiệu
- Các vấn đề bảo mật
- Các loại tấn công
- Một số mối đe dọa
- Chính sách bảo vệ

Next generation! NOD32 Antivirus System

Time interval: Day | Week | Month | Year

Total infection ratio in the last 24 hours

TOTAL THREATS
(Virus infection ratio percentage progress)



More information...

Top threats in the last 24 hours

Virus	Count
1. Win32/Stration.ABF worm	76 178
2. Win32/Netsky.Q worm	9 523
3. Win32/Mydoom.R worm	2 175
4. Win32/Bagle.gen.zip ...	448
5. Win32/Bagle.HE worm	357

More information...

Top virus in the last 24 hours

Info: Win32/Stration.ABF worm
Risk: Elevated

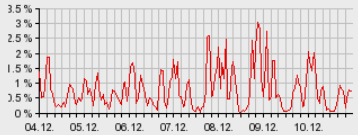
Date first captured:	2007-12-04 14:10
Date last captured:	2007-12-11 13:59
Total stopped to date:	491 005
Most active month:	2007-12
Most active date:	2007-12-09
Infection ratio (2007-12-09):	0.875 %

Virus Encyclopedia NOD32...
More information...

Time interval: Day | Week | Month | Year

Total infection ratio in the last 168 hours

TOTAL THREATS
(Virus infection ratio percentage progress)



More information...

Top threats in the last 168 hours

Virus	Count
1. Win32/Stration.ABF worm	491 005
2. a variant of Win32/S...	58 759
3. Win32/Netsky.Q worm	58 697
4. Win32/Stration.XW worm	15 152
5. Win32/Mydoom.R worm	8 647

More information...

Top virus in the last 168 hours

Info: Win32/Stration.ABF worm
Risk: Elevated

Date first captured:	2007-12-04 14:10
Date last captured:	2007-12-11 13:59
Total stopped to date:	491 005
Most active month:	2007-12
Most active date:	2007-12-09
Infection ratio (2007-12-09):	0.875 %

Virus Encyclopedia NOD32...
More information...

Time interval: Day | Week | Month | Year

Total infection ratio in the last 31 days

TOTAL THREATS
(Virus infection ratio percentage progress)

More information...

Top threats in the last 31 days

Virus	Count
1. Win32/Stration.XW worm	675 190
2. Win32/Stration.ABF worm	491 005
3. a variant of Win32/S...	270 712
4. Win32/Netsky.Q worm	246 218
5. Win32/TrojanDownload...	19 800

More information...

Top virus in the last 31 days

Info: Win32/Stration.XW worm
Risk: Elevated

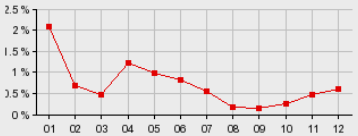
Date first captured:	2007-03-03 13:11
Date last captured:	2007-12-11 12:53
Total stopped to date:	1 300 113
Most active month:	2007-11
Most active date:	2007-11-25
Infection ratio (2007-11-25):	0.778 %

Virus Encyclopedia NOD32...
More information...

Time interval: Day | Week | Month | Year

Total infection ratio in the last 12 months

TOTAL THREATS
(Virus infection ratio percentage progress)



More information...

Top threats in the last 12 months

Virus	Count
1. a variant of Win32/S...	11 608 228
2. probably unknown New...	4 184 672
3. Win32/Netsky.Q worm	3 367 043
4. Win32/Nuwar.gen worm	2 965 119
5. Win32/Fuclip.B trojan	1 740 631

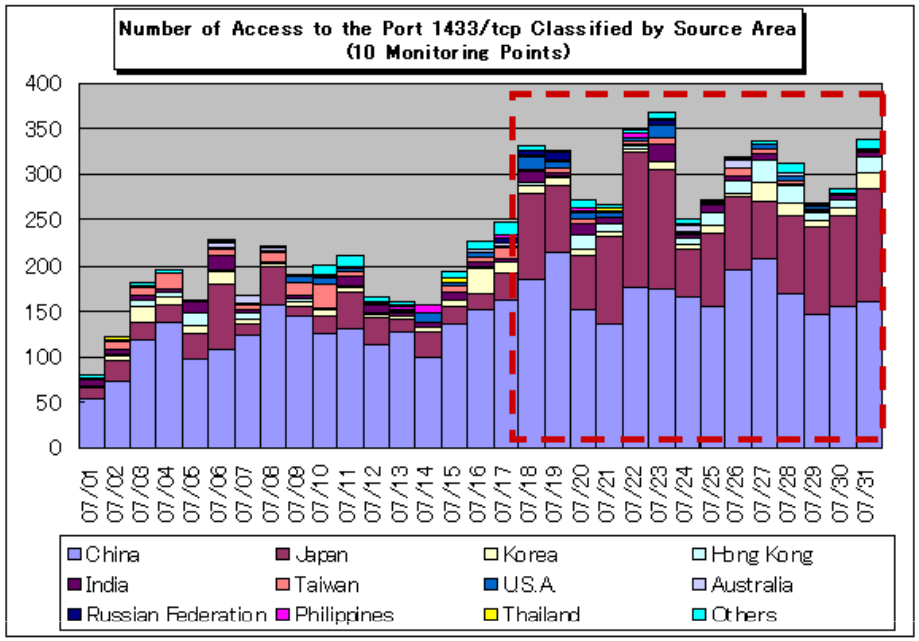
More information...

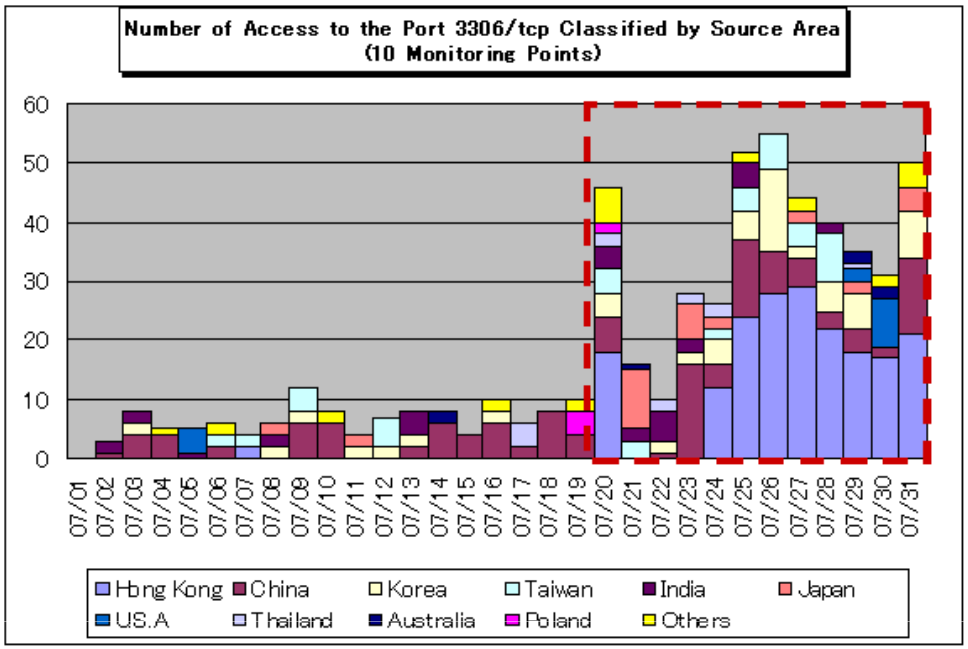
Top virus in the last 12 months

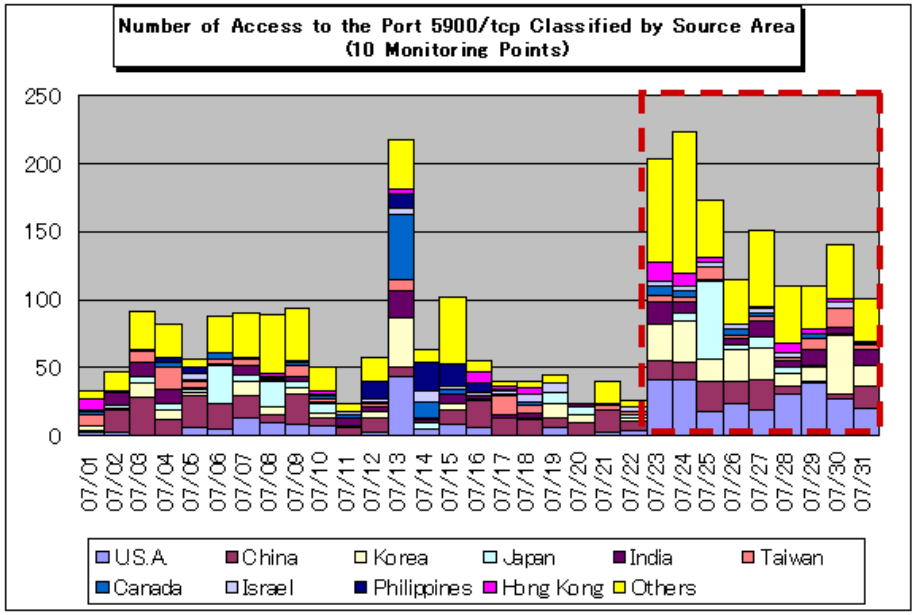
Info: a variant of Win32/Stration.XW worm
Risk: Critical

Date first captured:	2007-04-03 02:57
Date last captured:	2007-12-05 21:48
Total stopped to date:	11 608 228
Most active month:	2007-04
Most active date:	2007-04-19
Infection ratio (2007-04-19):	13.153 %

Virus Encyclopedia NOD32...
More information...







http://www.ipa.go.jp/security/english/virus/press/200707/E_PR200707.html

Giới thiệu - Virus

Hơn 10.000 loại

+200 loại / tháng

Chức năng

-Nhân bản

-Thực hiện n/vụ

Cơ chế

- Cơ chế nhân bản
- Cơ chế hoạt động
- Mục tiêu

Lây lan

- Thiết bị lưu trữ ngoại
- Bản tin điện tử
- Internet/intranet

Dấu hiệu

- Chương trình chạy chậm
-Truy xuất ổ cứng nhiều
- Truy xuất thiết bị khác
-Tốn tài nguyên hệ thống
-Mất dung lượng ổ cứng
-Kích thước tập tin bị thay đổi

Các loại khác

Spyware, trojan, Malware

Source : http://www.uhd.edu/computing/uss/virus.htm

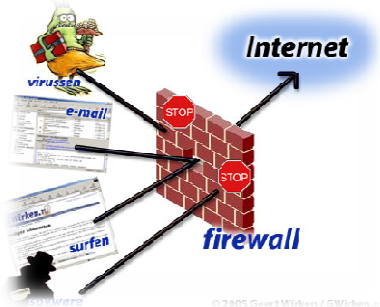
Giới thiệu (tt)

- Phishing
  - Mưu đồ sử dụng email, tin nhắn dạng pop-up hay các trang web để đánh lừa người dùng cung cấp các thông tin nhạy cảm
    - Số thẻ tín dụng, số tài khoản ngân hàng, mật mã
- Lợi dụng PC
  - Các hacker tấn công và sử dụng một số PC làm nơi gửi các spam mail
- PC bị nhiễm và làm lây lan virus, worm, trojan

Giới thiệu (tt)

- An toàn và bảo mật trên mạng có nhiều tiến triển
  - Bức tường lửa (firewall)
  - Mã hóa (encryption)
  - Chữ ký điện tử (digital signature)

  Nhưng vẫn còn 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 HĐH
  - Mở thư đã bị nhiễm virus
  - Xem những trang web chứa 1 số đoạn mã có ý xấu
  - …

Nội dung chi tiết

- Giới thiệu
- Các vấn đề bảo mật
- Các loại tấn công
- Một số mối đe dọa
- Chính sách bảo vệ

Các vấn đề bảo mật

- 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
  - Một khách hàng cần có thông tin của các sản phẩm trên website của 1 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?

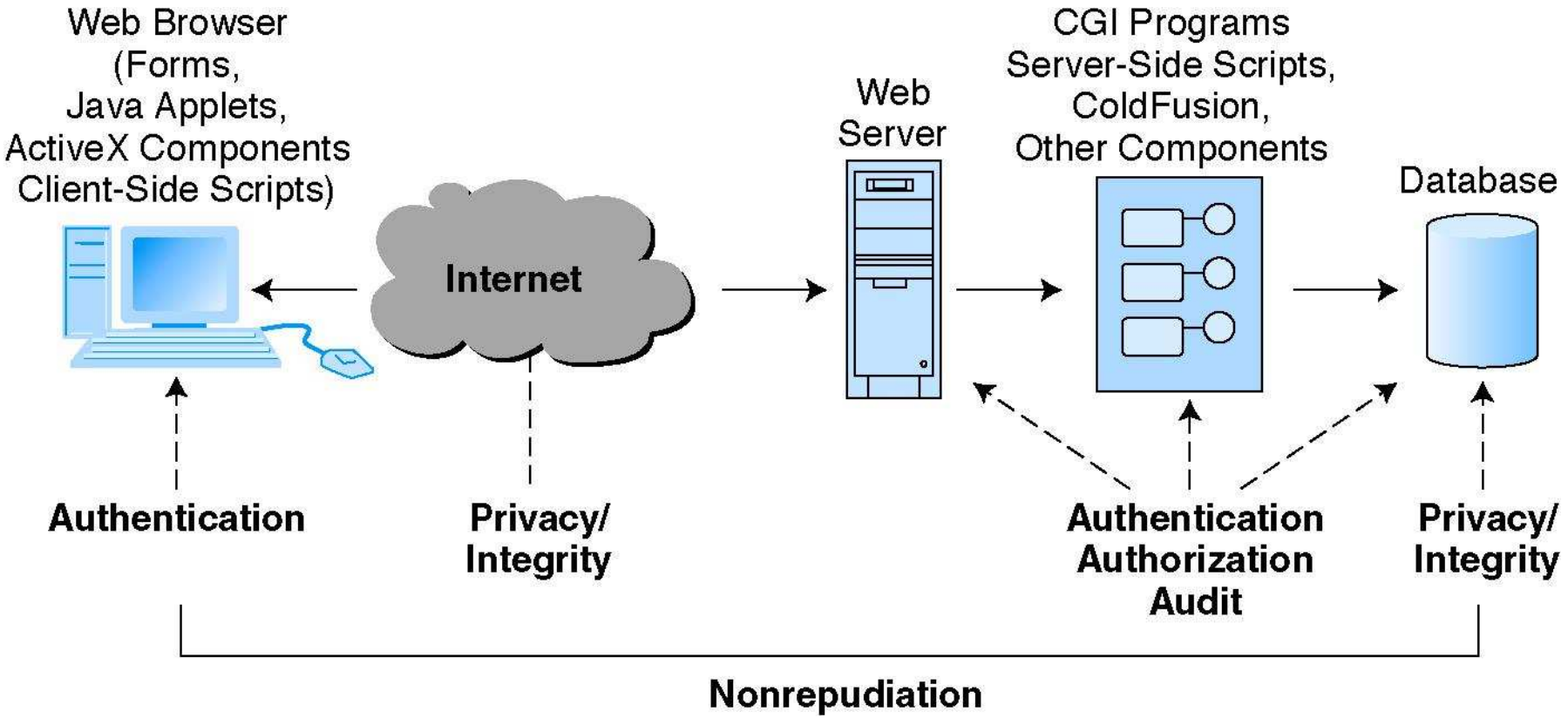
Các vấn đề bảo mật (tt)

- 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 (tt)

- 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
    - Mã hóa
  - Integrity – Toàn vẹn thông tin
  - Availability – Khả năng sẵn sàng đáp ứng
  - Nonrepudiation – Không thể từ chối trách nhiệm
    - Chữ ký

Các vấn đề bảo mật (tt)

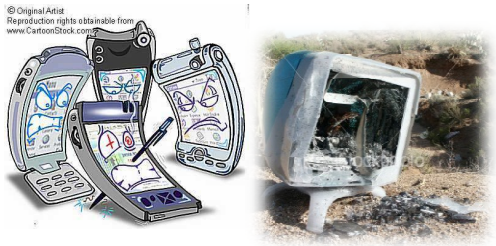


Nội dung chi tiết

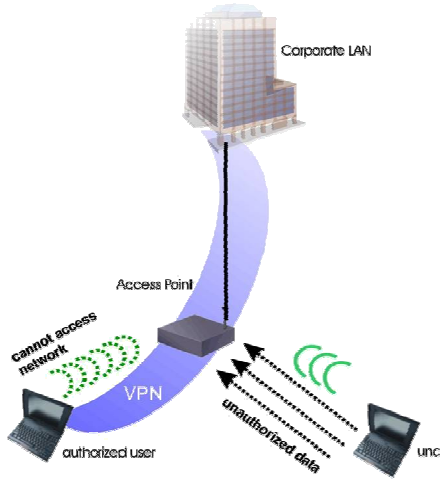
- Giới thiệu
- Các vấn đề bảo mật
- Các loại tấn công
- Một số mối đe dọa
- Chính sách bảo vệ

Các loại tấn công

- 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



Denial of Service Attack

Ví dụ

Dear user of xyz.com

We have detected that your e-mail account was used to send a large amount of spam during the recent week. Obviously, your computer had been compromised and now runs a trojan proxy server.

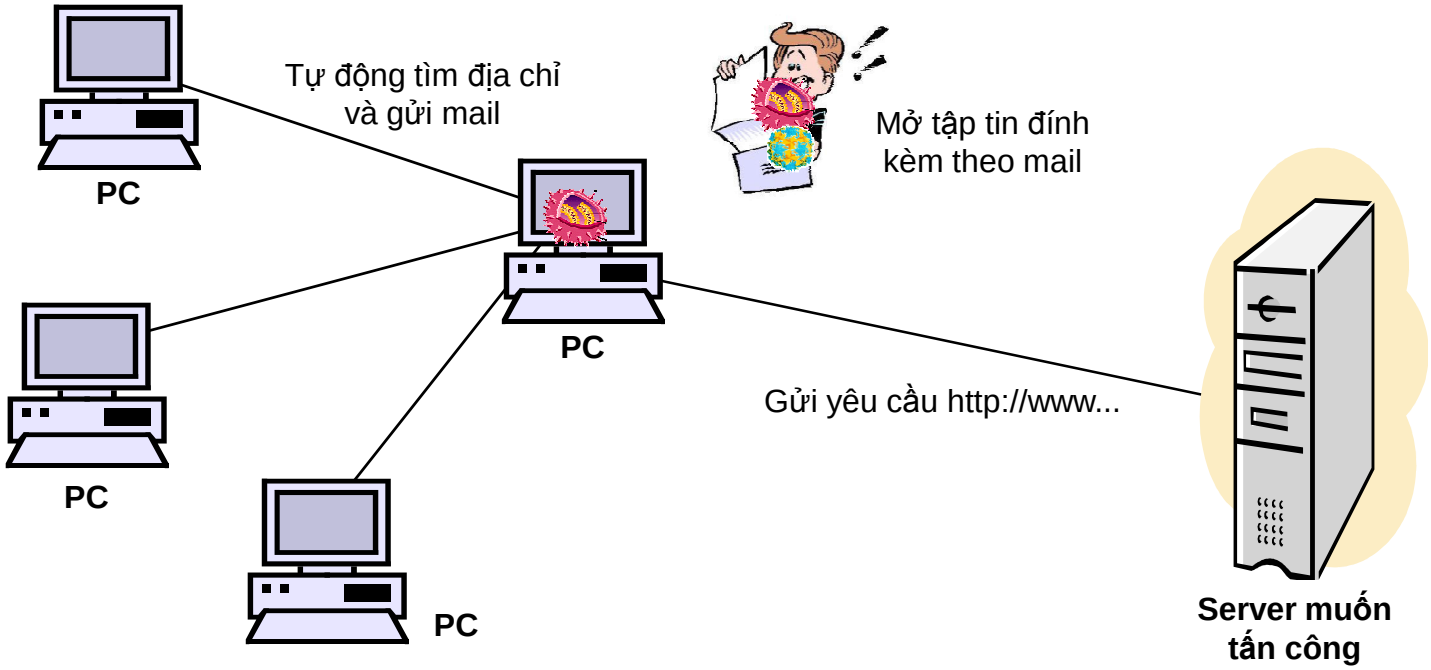
We recommend you to follow the instructions in the attachment (xyz.com.zip) in order to keep your computer safe.

Have a nice day,

xyz.com technical support team.

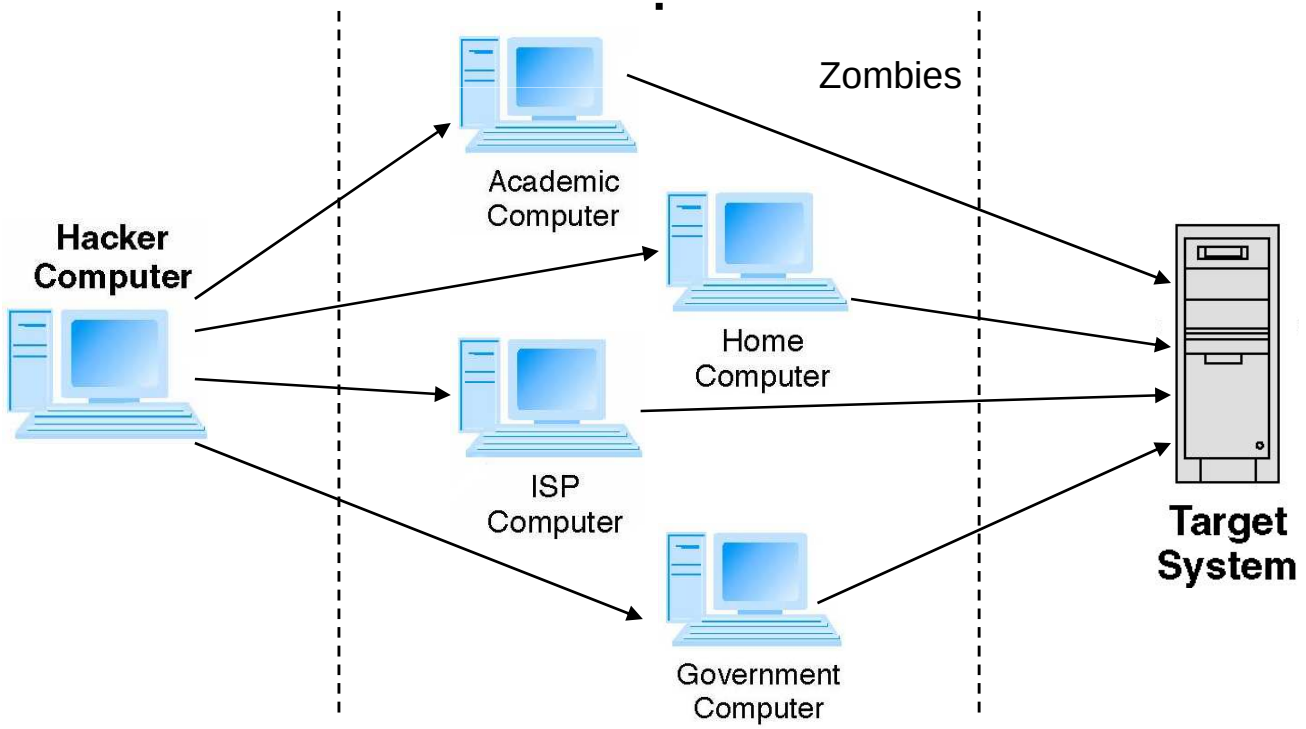
DoS

- 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



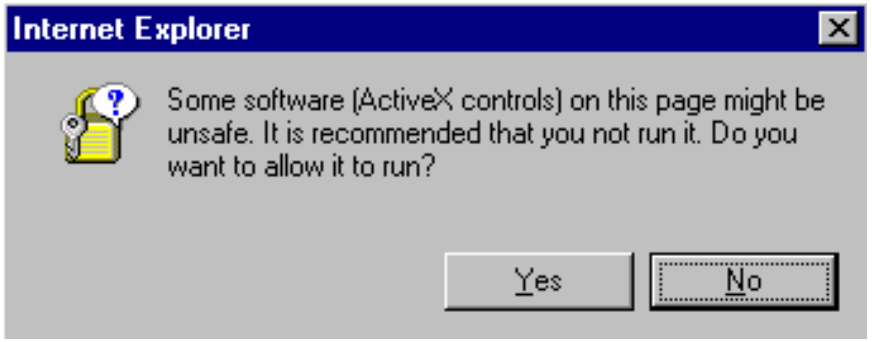
Nội dung chi tiết

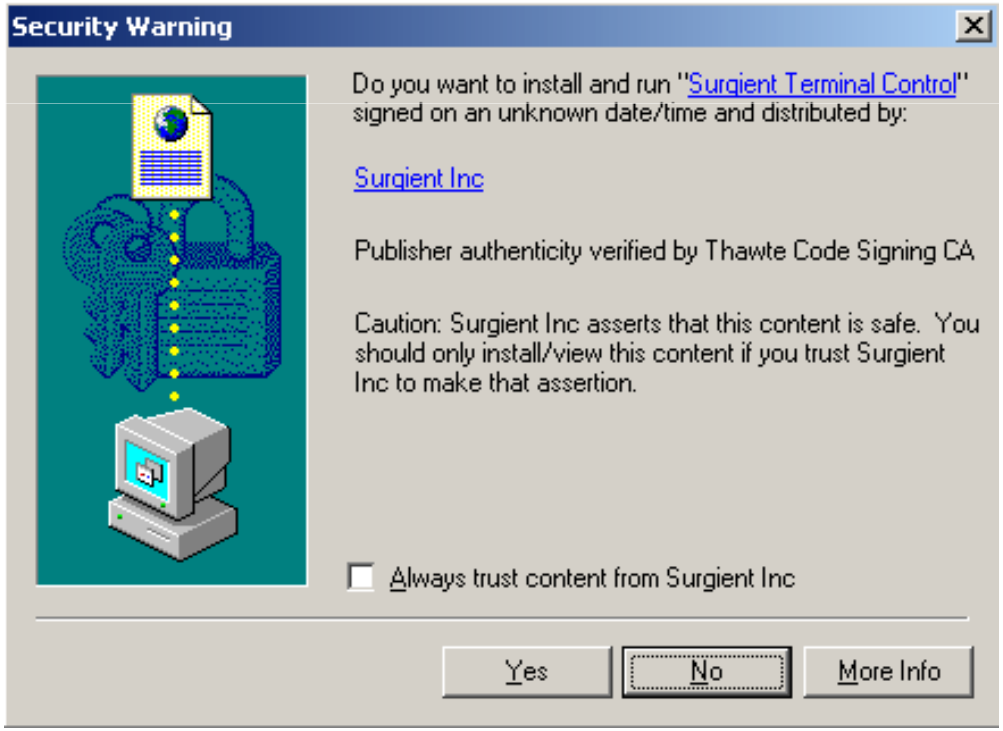
- Giới thiệu
- Các vấn đề bảo mật
- Các loại tấn công
- Một số mối đe dọa
  - Tại client
  - Môi trường Internet
  - Tại server
- Chính sách bảo vệ

Mối đe dọa – 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 – Client (tt)





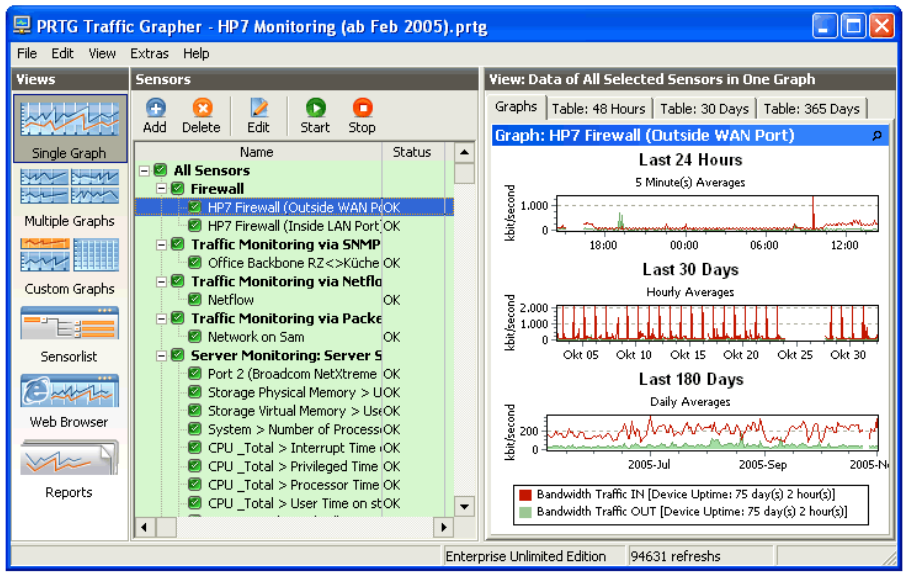
Mối đe dọa – Client (tt)

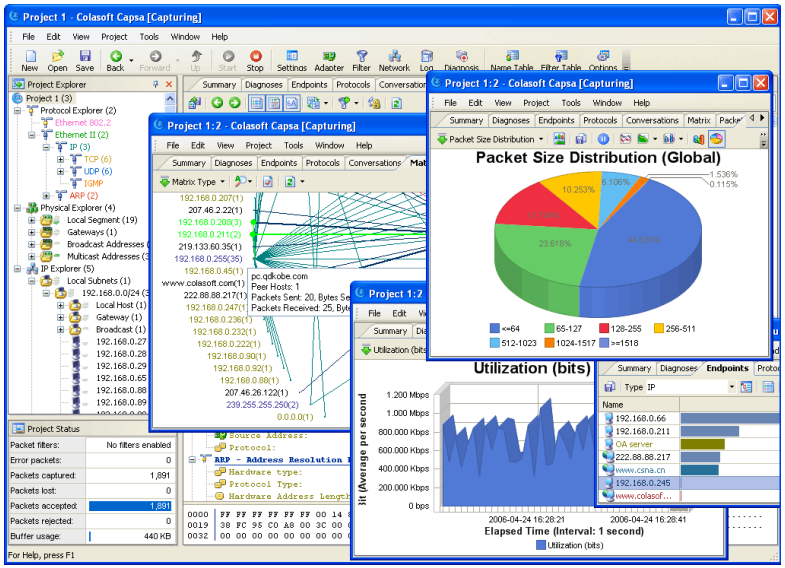
- Plug-in
  - Chương trình làm tăng khả năng trình bày của các trình duyệt (browser)
    - Mở nhạc, phim, animation
    - QuickTime, RealPlayer, FlashPlayer
  - Có thể nhúng các lệnh với mục đích xấu làm hư hại máy tính
- Tập tin đính kèm theo thư điện tử (e-mail)

Mối đe dọa – 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

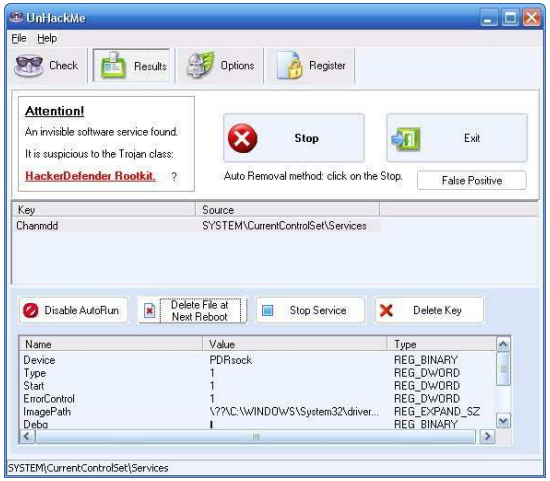
  → Gói tin bị đọc trộm, sửa đổi, xóa
  - "*sniffer program*" được sử dụng để bắt gói tin

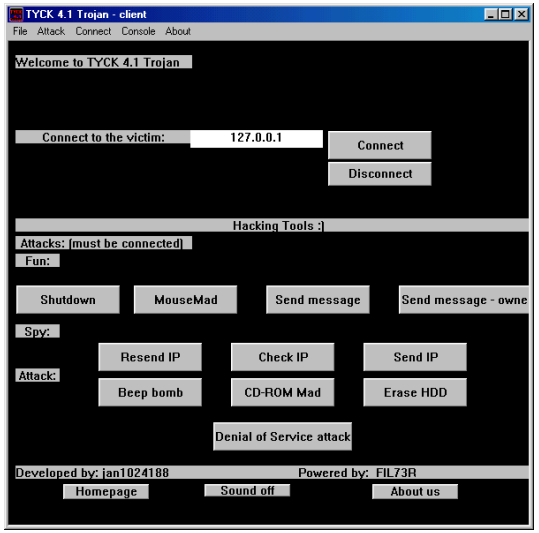




Mối đe dọa – Internet

- 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 – 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
  - 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 /baigiang/2524_701143

	Name	Last modified	Size	Description
	Parent Directory		-	
	701143_MayTinhKinhDo..>	14-Mar-2007 14:27	94K	
	HDTH_AHP.pdf	23-Mar-2007 10:34	529K	
	HDTH_NETMEETING.pdf	23-Mar-2007 10:34	171K	
	HDTH_OLAP.pdf	23-Mar-2007 10:34	500K	
	QDNhom3.ppt	23-Mar-2007 12:24	263K	
	btMohinh.xls	27-Mar-2007 15:19	27K	
	dss_lecture_notes_Un..>	23-Mar-2007 12:24	422K	
	dss_lecture_notes_Un..>	23-Mar-2007 12:24	526K	
	dss_lecture_notes_Un..>	23-Mar-2007 12:24	215K	
	unit_1.pdf	23-Mar-2007 10:22	367K	
	unit_2.pdf	23-Mar-2007 10:22	655K	
	unit_3.pdf	23-Mar-2007 10:22	429K	
	unit_4.pdf	23-Mar-2007 10:22	292K	
	unit_5.pdf	23-Mar-2007 10:34	136K	

Apache/2.0.48 (Win32) Server at www.sim.hcmut.edu.vn Port 80

Mối đe dọa – Server (tt)

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

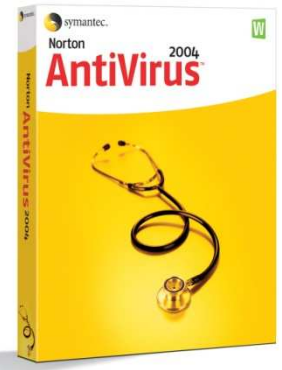
Nội dung chi tiết

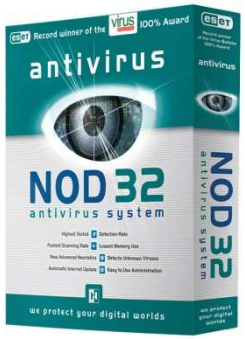
- Giới thiệu
- Các vấn đề bảo mật
- Các loại tấn công
- Một số mối đe dọa
- Chính sách bảo vệ
  - Tại client
  - Môi trường Internet
  - Tại server

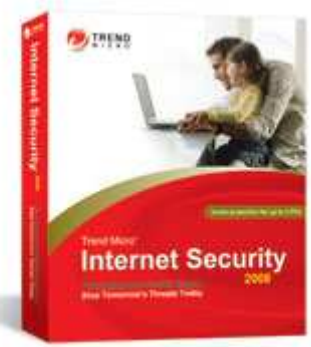
Bảo vệ – Client

- Trình duyệt 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)

- Phần mềm chống virus







Chứng nhận số

- 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

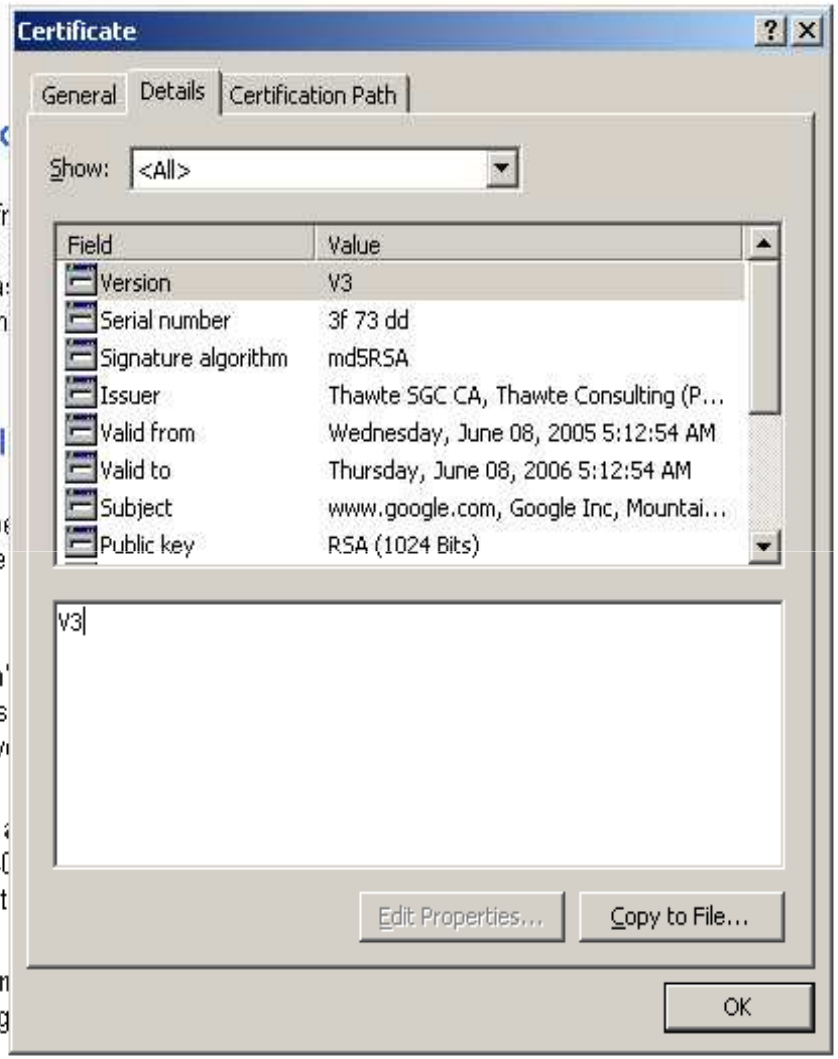
New! Gmail c

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



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.

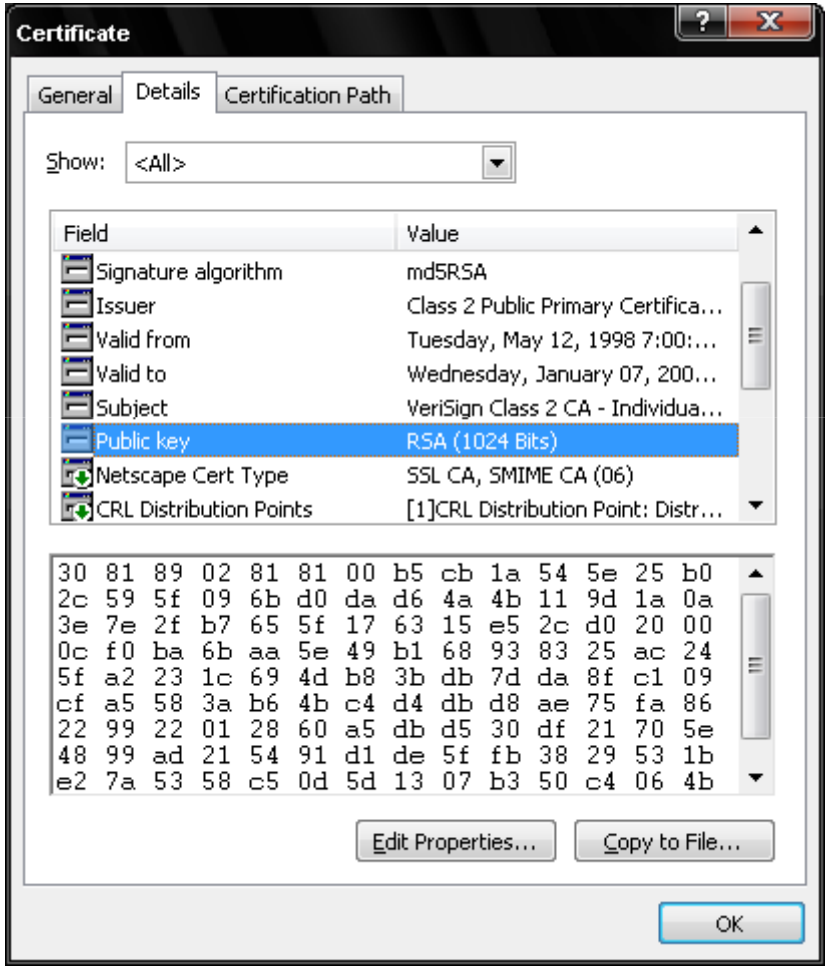
Internet

Chứng nhận (tt)

- Chứng nhận phải do một đơn vị có uy tín cấp
  - Certification Authority (CA)
  - VeriSign

- Gồm các thông tin
  - Tên, địa chỉ của nhà phát triển phần mềm
  - Public key của nhà phát triển phần mềm
  - Thời gian hợp lệ của chứng nhận
  - Số chứng nhận
  - Tên người cấp chứng nhận
  - Chữ ký điện tử của người cấp chứng nhận

Chứng nhận (tt)



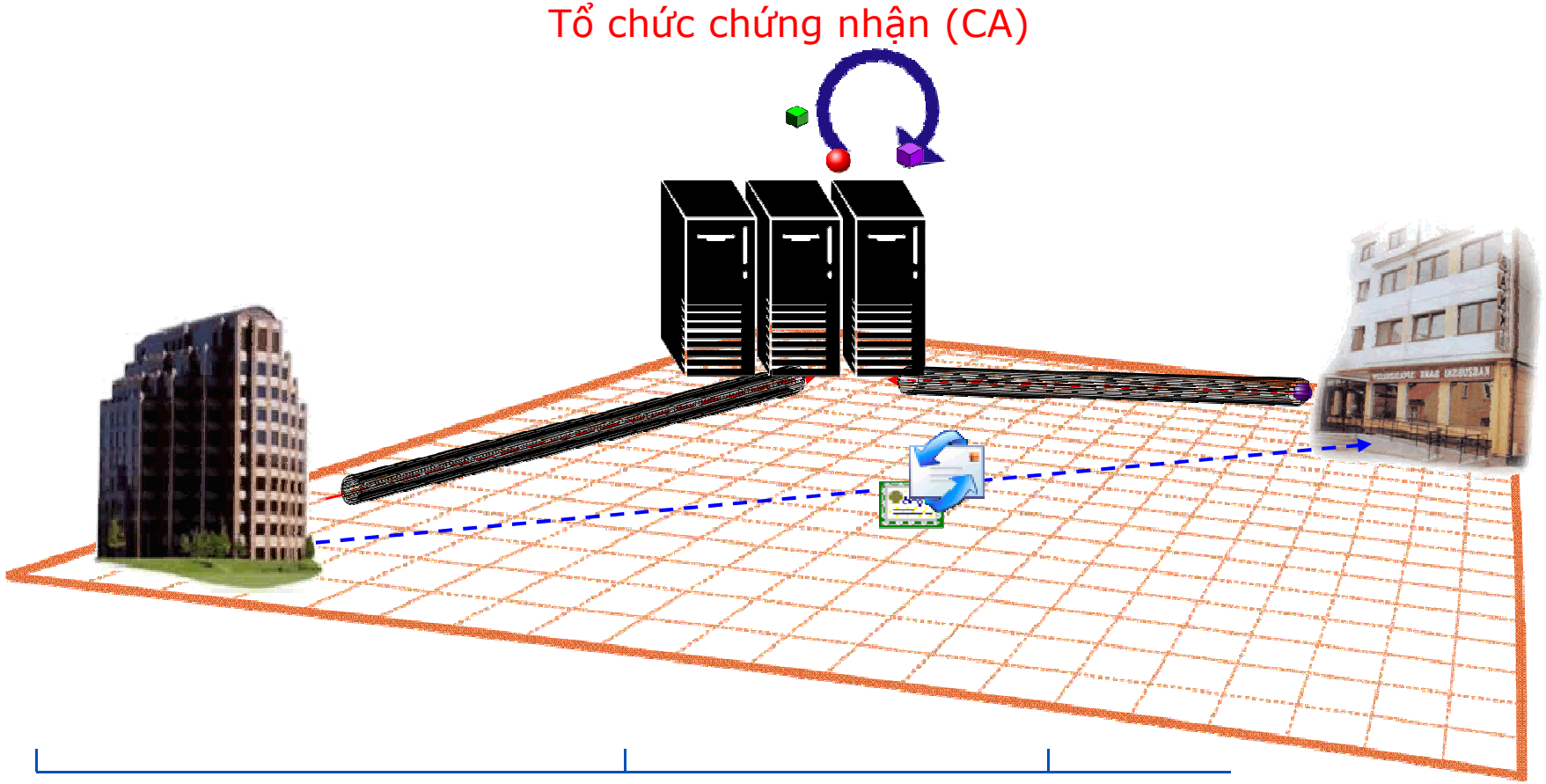
Microsoft IE

- Sử dụng kỹ thuật **Authenticode** để nhận diện các active content

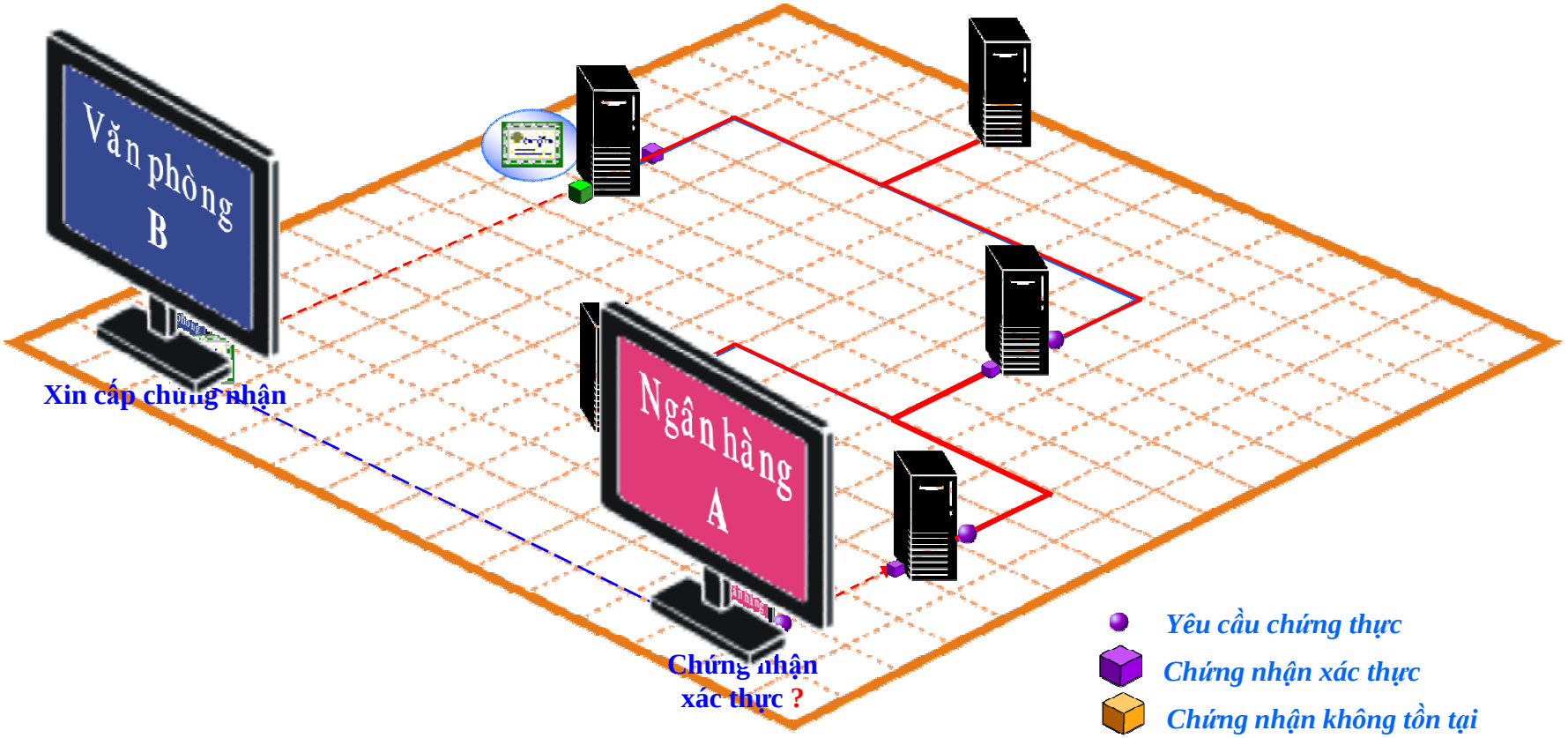
  - Ai ký xác nhận cho chứng nhận
    - Danh sách các CA và public key của CA được lưu trữ trong IE

  - Chứng nhận có bị thay đổi gì từ lúc được ký xác nhận không
    - Sử dụng public key của CA để mở chứng nhận
    - Nếu thông tin trong chứng nhận chứng minh được nhà phát triển phần mềm đã ký cho active content thì chứng nhận là hợp lệ

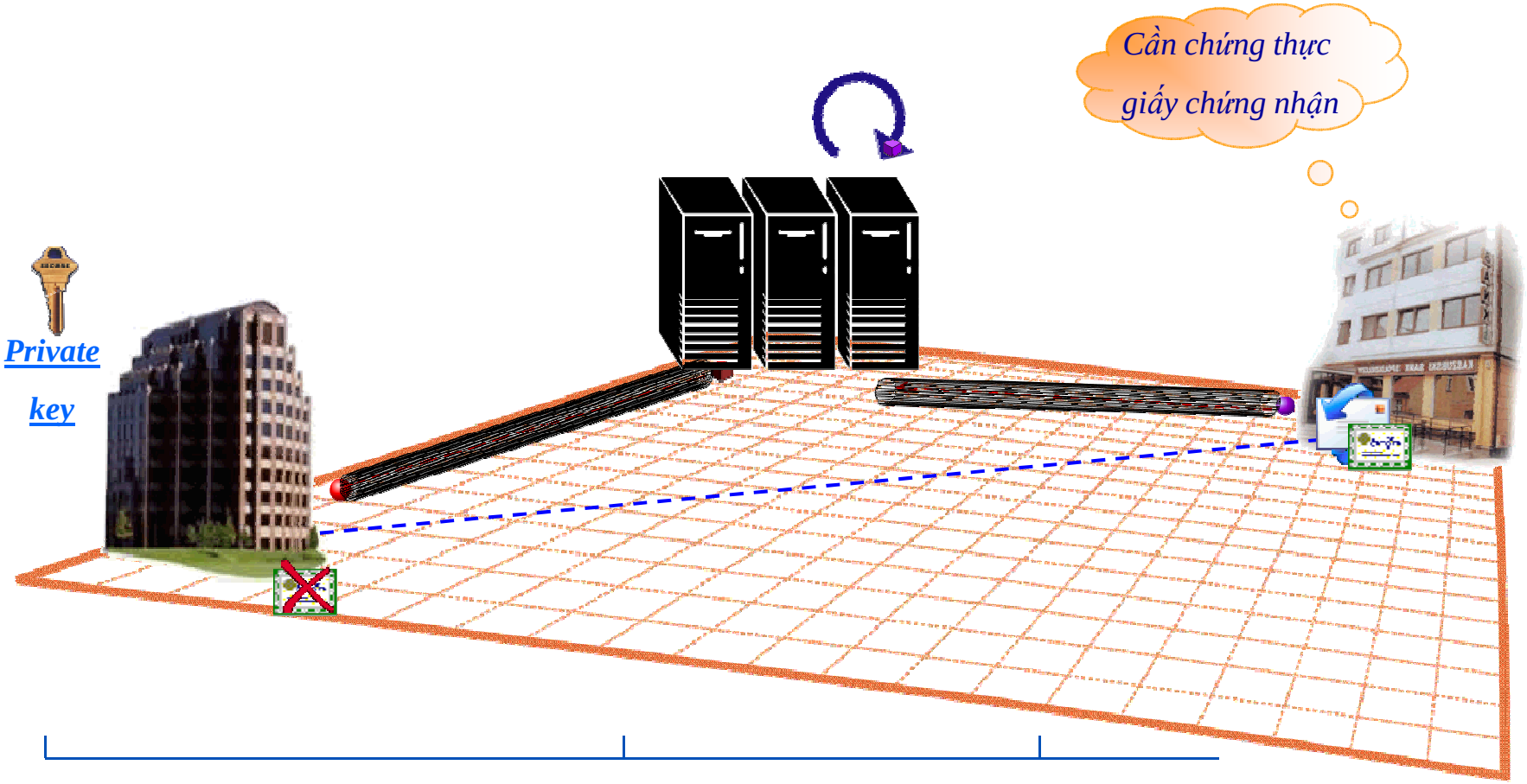
Demo4



Demo5


Văn phòng
B
Xin cấp chứng nhận
Ngân hàng
A
Chứng nhận
xác thực ?
Yêu cầu chứng thực
Chứng nhận xác thực
Chứng nhận không tồn tại

Demo6



Bảo vệ – Internet

- Mã hóa (Encryption)
- Nghi thức SSL (Secure Sockets Layer)
- Chữ ký điện tử

Bảo vệ – Internet

- Mã hóa (Encryption)
- Nghi thức SSL (Secure Sockets Layer)
- Chữ ký điện tử

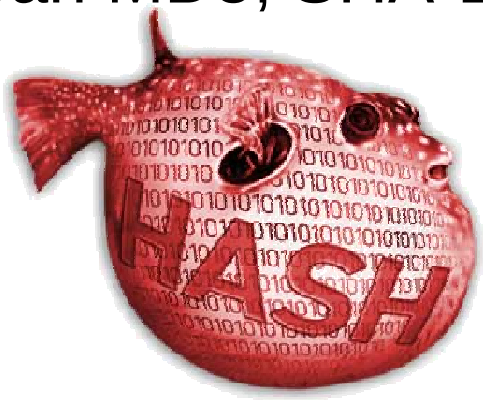
Mã hóa

- Chuyển dữ liệu sang dạng mã
  - Thuật toán
  - Khóa
- Có 3 kỹ thuật
  - Mã hóa Hash
  - Mã hóa không đối xứng (public key)
  - Mã hóa đối xứng (secret key)

Mã hóa Hash

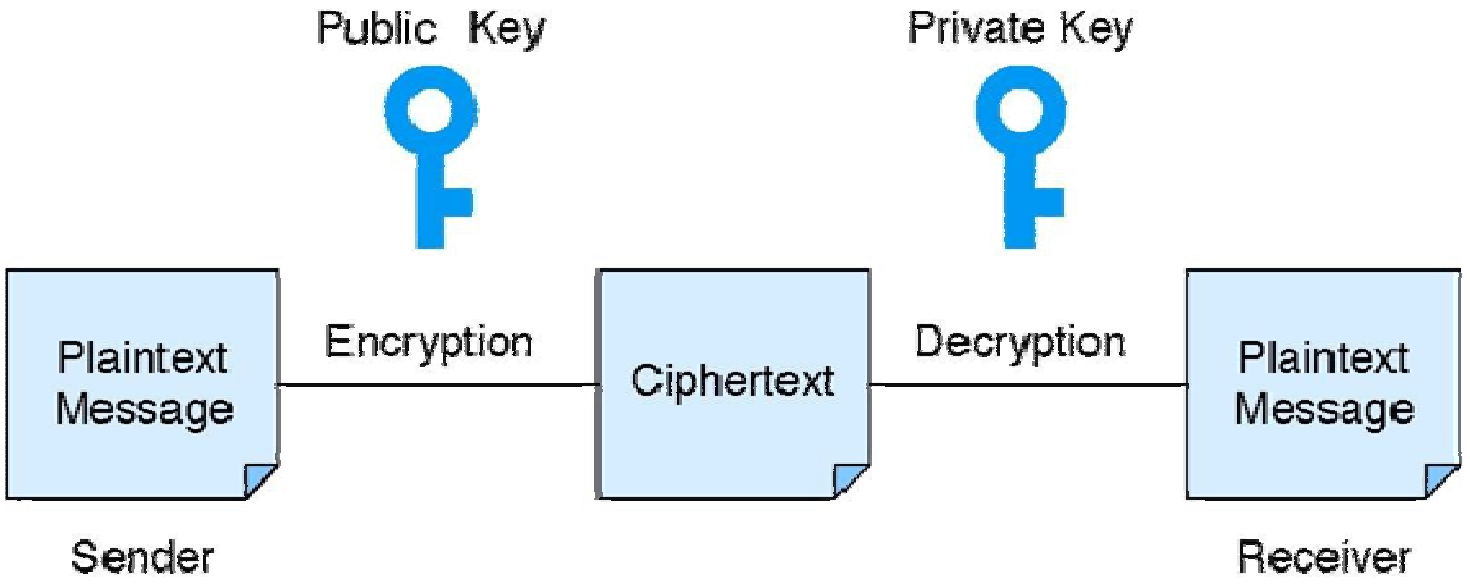
- Sử dụng thuật toán Hash để đưa ra một con số từ một thông điệp có độ dài bất kỳ
  - Xung đột giá trị băm rất hiếm xãy ra
  - Không sử dụng khóa
  - Chuỗi được mã hóa không thể giải mã thành chuỗi ban đầu

- Thuật toán MD5, SHA-1, SHA256, SHA512, …



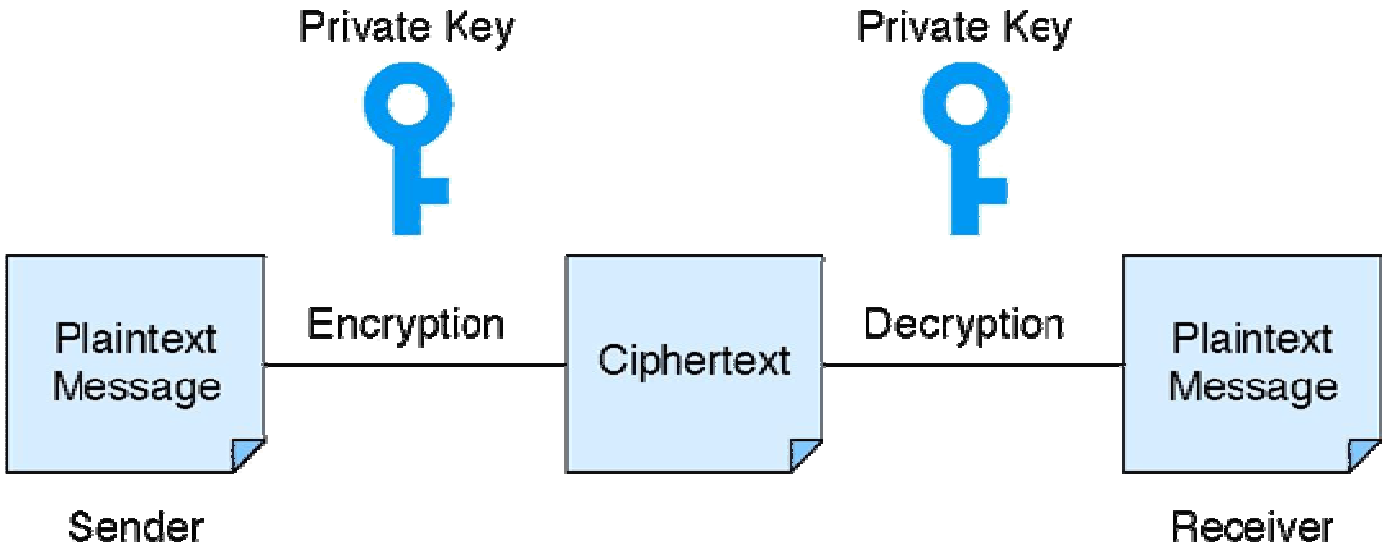
Mã hóa bất đối xứng

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



Mã hóa đối xứng

- Mã hóa chỉ sử dụng 1 loại khóa
  - Secret key – mã hóa và giải mã thông điệp
- Thuật toán 3DES, Rijndael (AES), blowfish, idea,…

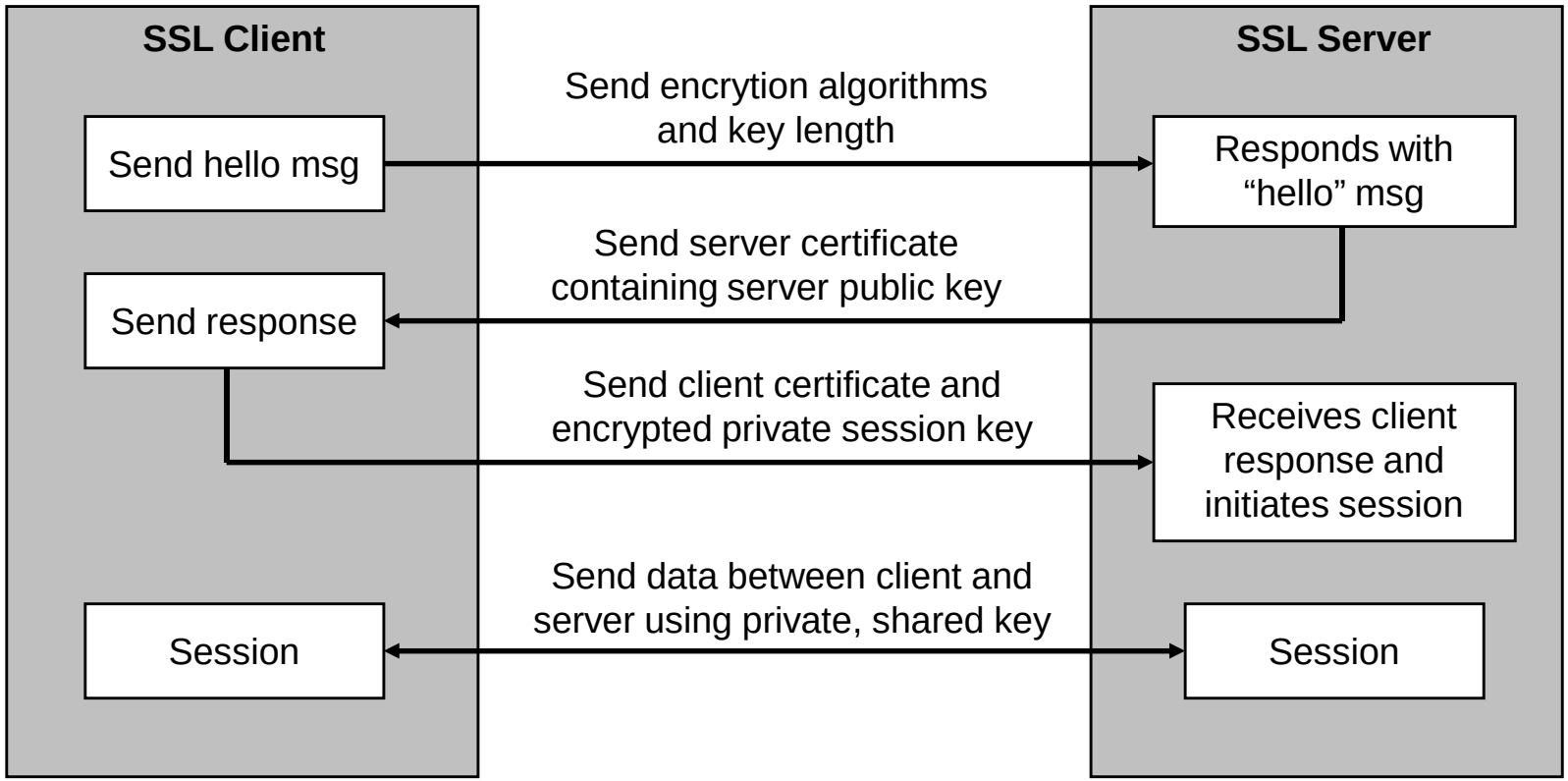


Bảo vệ – Internet

- Mã hóa (Encryption)
- Nghi thức SSL (Secure Sockets Layer)
- Chữ ký điện tử

SSL

- Nghi thức bảo mật kết nối giữa client và server

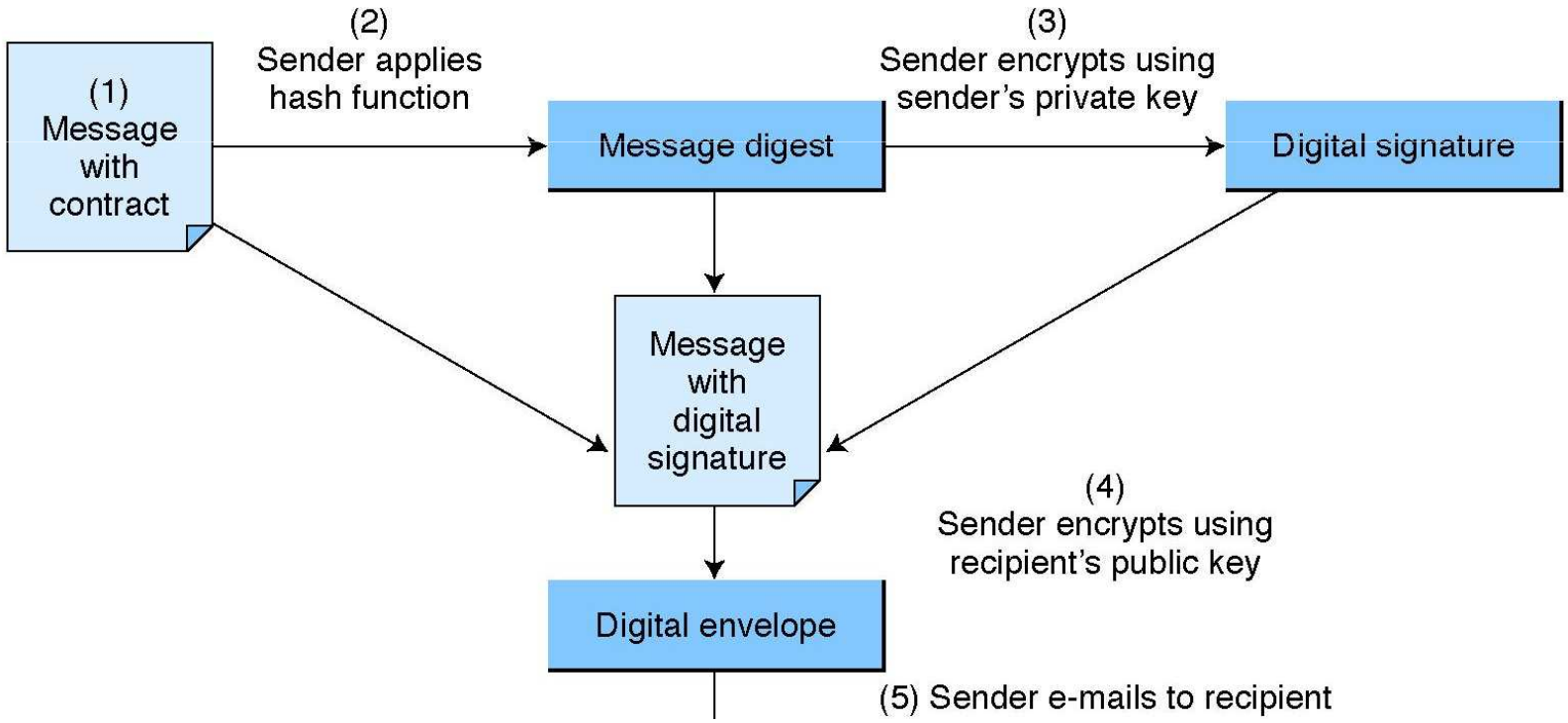


Bảo vệ – Internet

- Mã hóa (Encryption)
- Nghi thức SSL (Secure Sockets Layer)
- Chữ ký điện tử

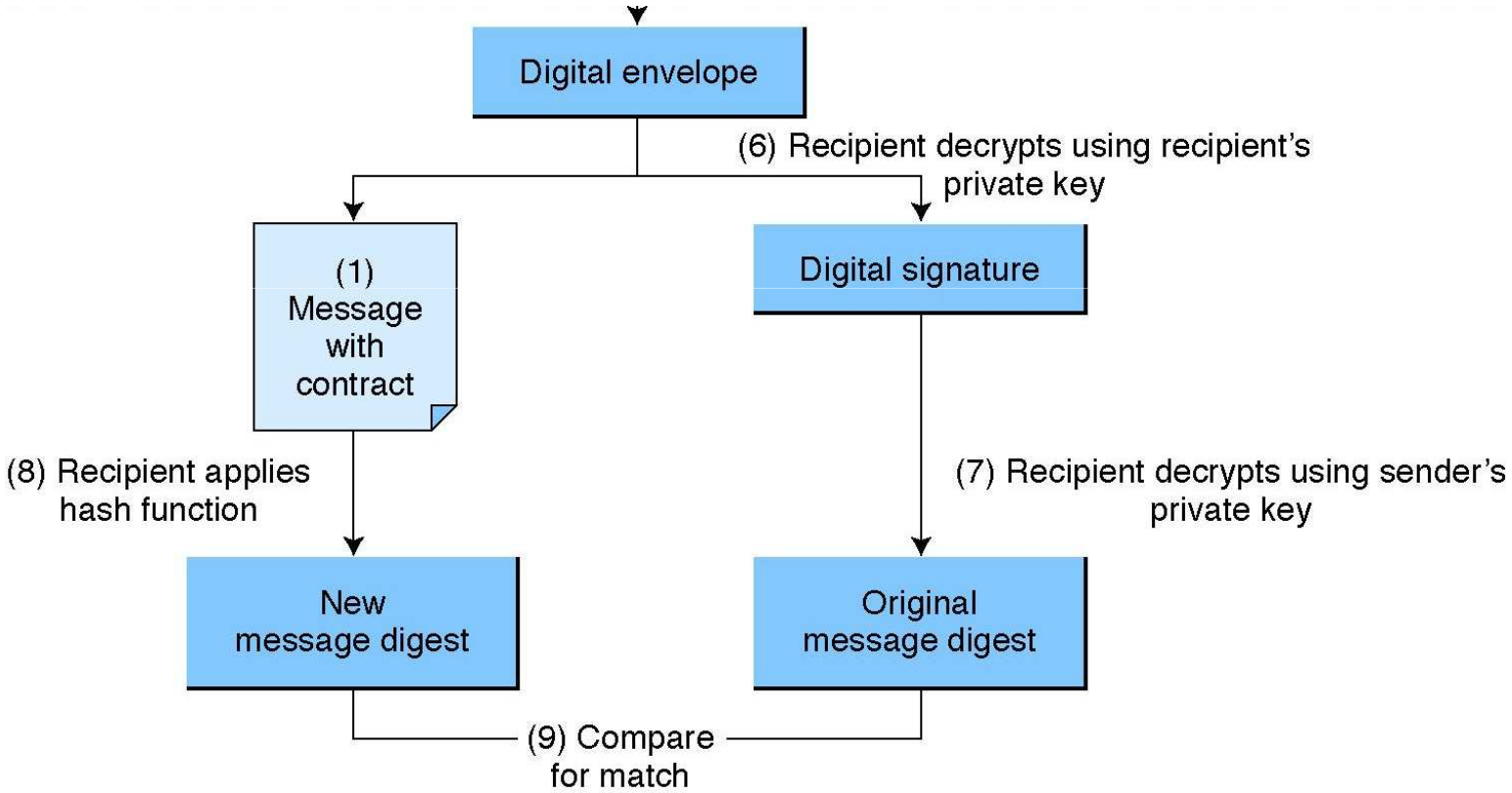
Chữ ký điện tử

- Sử dụng khóa công khai trong Chữ ký điện tử để mã hóa và xác thực thông tin

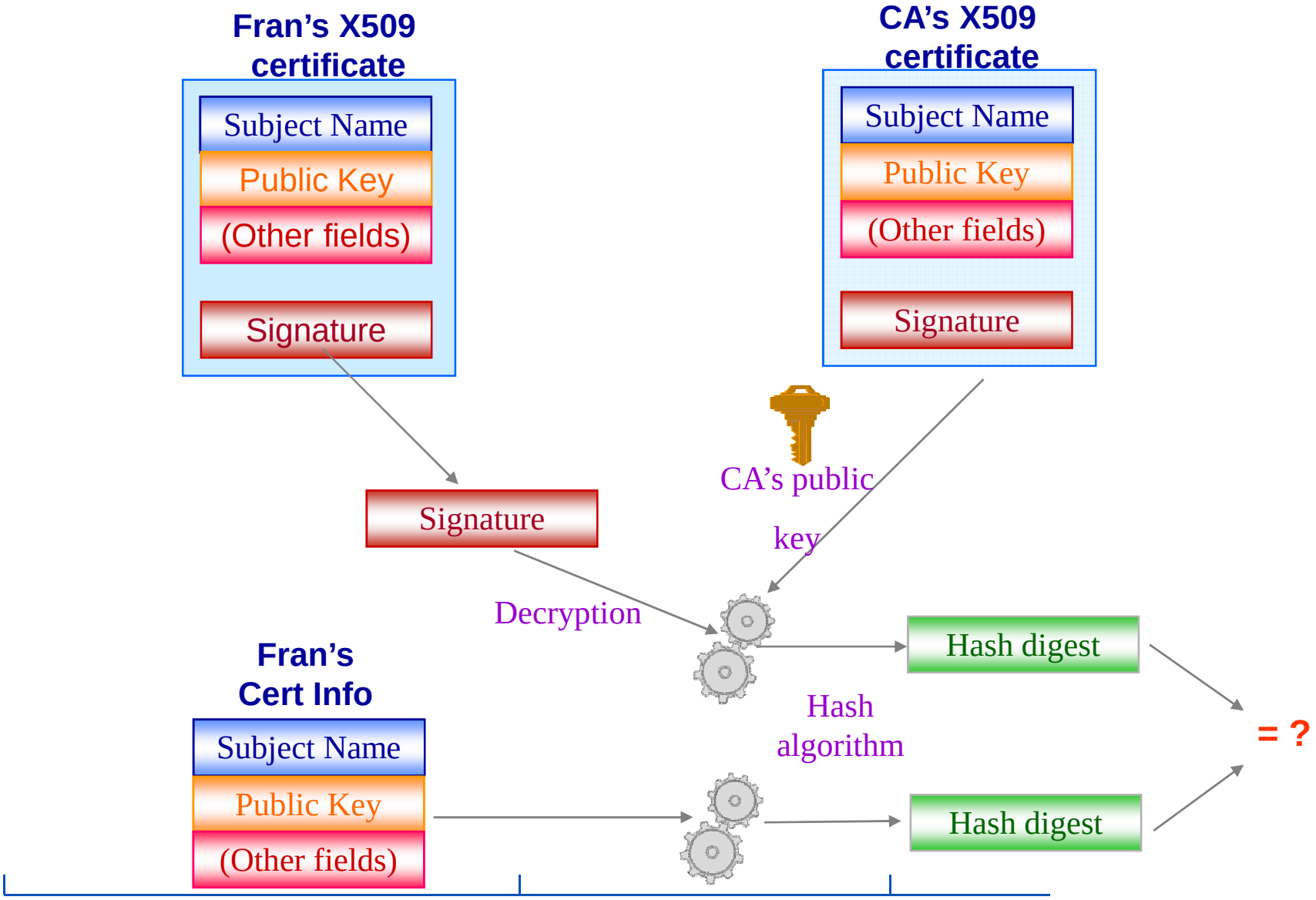


Chữ ký điện tử (tt)

- Nhận:



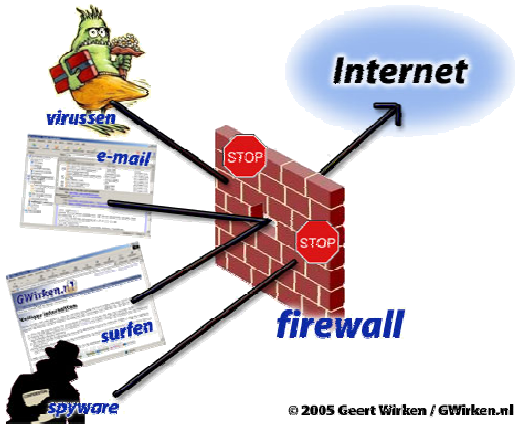
Kiểm tra chứng nhận



Bảo vệ – Web Server

- Điều khiển truy cập và xác thực người dùng
  - Ai đang truy cập vào server
  - Truy cập những gì

- Bức tường lửa (firewall)
  - Giải pháp gồm máy tính và phần mềm
  - Điểm đi ra ngoài Internet của hệ thống mạng
  - Ngăn chặn các tấn công từ Internet hay từ các mạng khác



- http://www.securitystats.com/tools/password.php

Password Security

A good password is one that cannot be easily guessed.

Enter a password, click submit, then we'll score it against best practices!

Submit

DO'S	DONT'S
• DO use a password with mixed-case letters. Use uppercase letters throughout the password.	• DO NOT use a network login ID in any form (reversed, capitalized, or doubled as a password).
• DO use a password that contains alphanumeric characters and include punctuation, where supported by the operating system.	• DO NOT use your first, middle or last name or anyone else's in any form. Do not use your initials or any nicknames you may have or anyone else's.
• DO use a password with mixed-case letters. Do not just capitalize the first letter, but add uppercase letters throughout the password.	• DO NOT use a word contained in English or foreign dictionaries, spelling lists, or other word lists and abbreviations.
• DO use at least six characters, eight characters for Windows NT.	• DO NOT use other information easily obtained about you. This includes pet names, license plate numbers, telephone numbers, identification numbers, the brand of your automobile, the name of the street you live on, and so on. Such passwords are very easily guessed by someone who knows the user.
• DO use a seemingly random selection of letters and numbers.	• DO NOT use a password of all numbers, or a password composed of alphabet characters. Mix numbers and letters.

Online Secure Hash Algorithm Calculator

Hash algorithms are fundamental to many cryptographic applications. Although widely associated with digital signature technology, the hash algorithm has a range of other uses. SHA-1 and MD5 are amongst the most widely known, trusted and used. When utilised with a password (the HMAC version), the potential uses of these algorithms extends further.

Enter a string in the box below and select the hash algorithm.

MD5 Submit

ALL
SHA1
MD5
MD4
NT
LANMAN
GOST
HAVAL256
HAVAL224
HAVAL192
HAVAL160
HAVAL128
RIPEMD160
TIGER
TIGER160
TIGER128
CRC32B
CRC32

Dictionary Based Hash Cracker

The "Golden Rule" of password security is **NOT** to choose a password that is easily guessable, or one that might be found in a dictionary. The reason for this is that many hacker tools can crack dictionary-based passwords in mere seconds.

This web based demonstration shows how truely easy it is to break dictionary based passwords, regardless of the type of encryption algorythm used to encrypt them. Simply paste in an encrypted password value, and then count the seconds it takes to return the password associated with that encrypted value (won't be long.....)

Here is an example:

LANMAN HASH: FDA95FBECA288D44AAD3B435B51404EE

-OR-

NTLM HASH: 066DDFD4EF0E9CD7C256FE77191EF43C

Will return a value of "hello", within about 5 seconds (even using this crude web interface.)

Not Sure? Submit