EC Security

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Nội dung

- Giới thiệu
- Các vấn đề bảo mật trong EC
- Các loại hình tấn công
- Một số mối đe dọa đến hệ thống EC
- Chính sách bảo vệ hệ thống

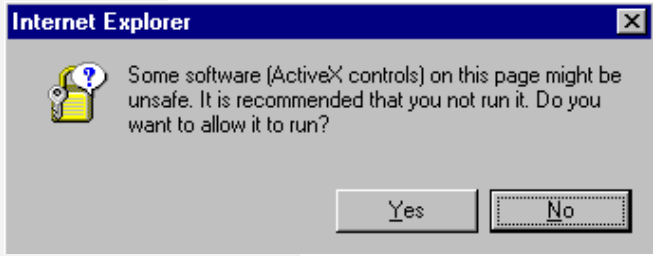
Một số mối đe dọa đến hệ thống EC

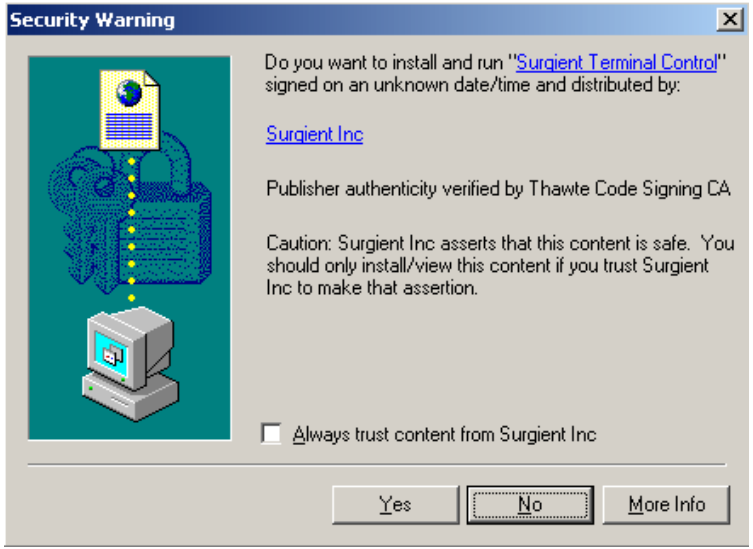
Bảo mật trong EC

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



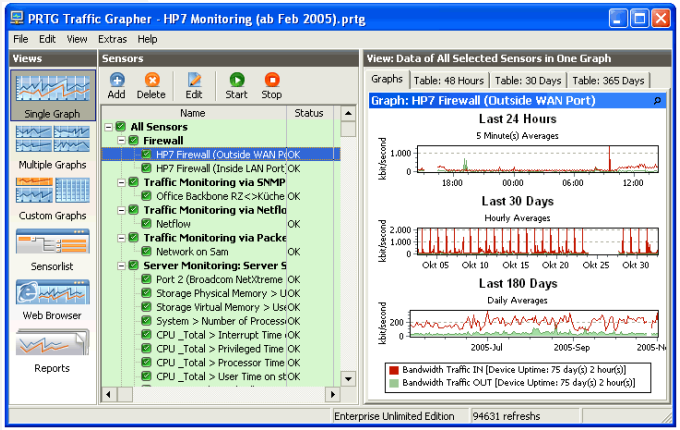


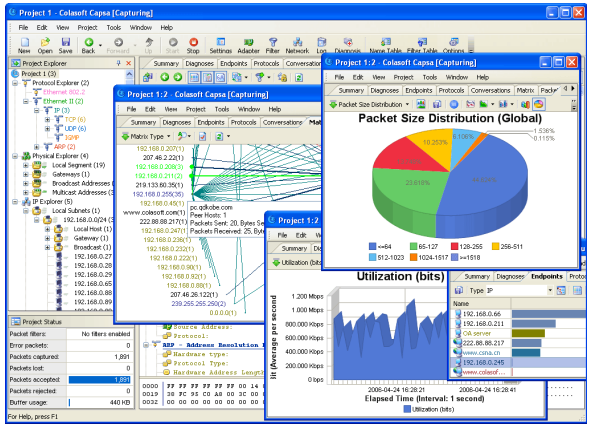
Mối đe dọa – Client

- 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 – Internet

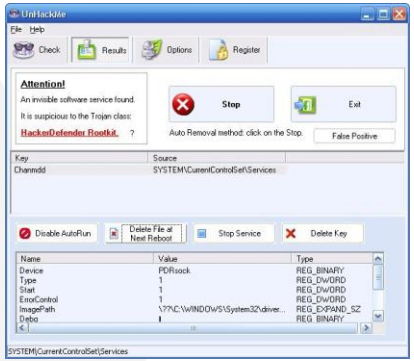
- Các gói tin di chuyển trên Internet theo một con đường không dự kiến trước
  - Người dùng không biết gói tin sẽ lưu lại ở nơi nào
  - → Gói tin bị đọc trộm, sửa đổi, xóa
  - *"sniffer program"* được sử dụng để bắt gói tin

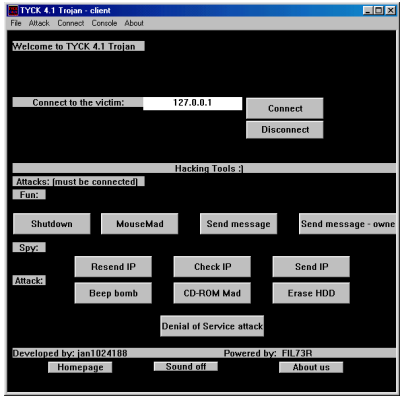




Mối đe dọa – Internet

- 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

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

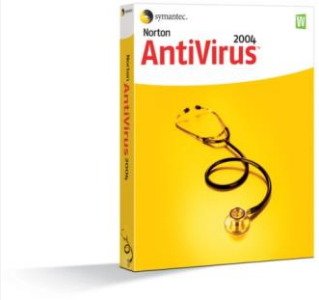
Chính sách bảo vệ

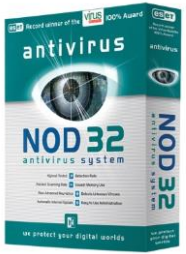
Bảo mật trong EC

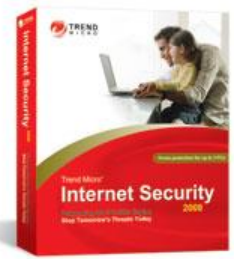
Bảo vệ Client – Phần mềm antivirus

- 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



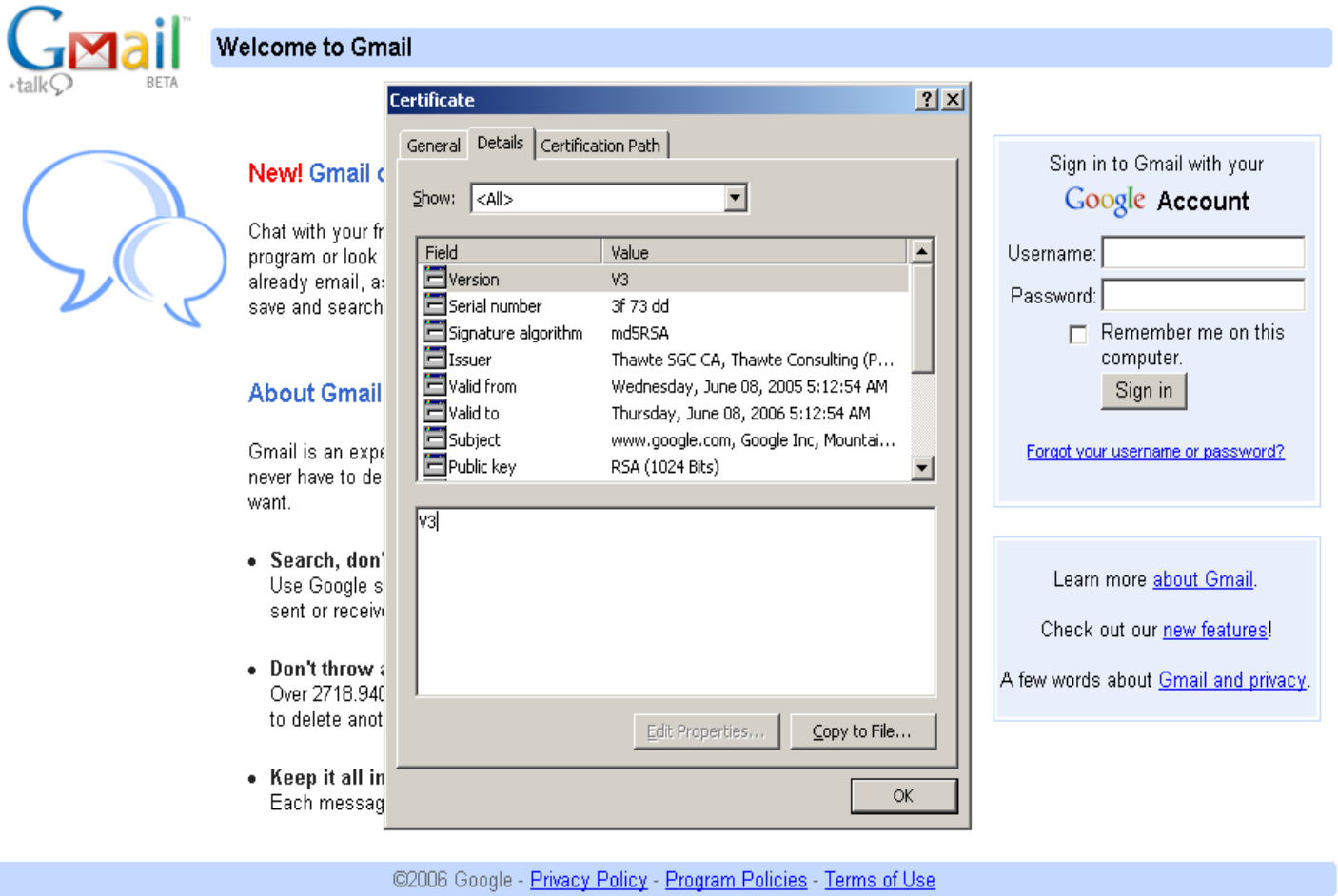




Bảo vệ Client – Chứng nhận số

- 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

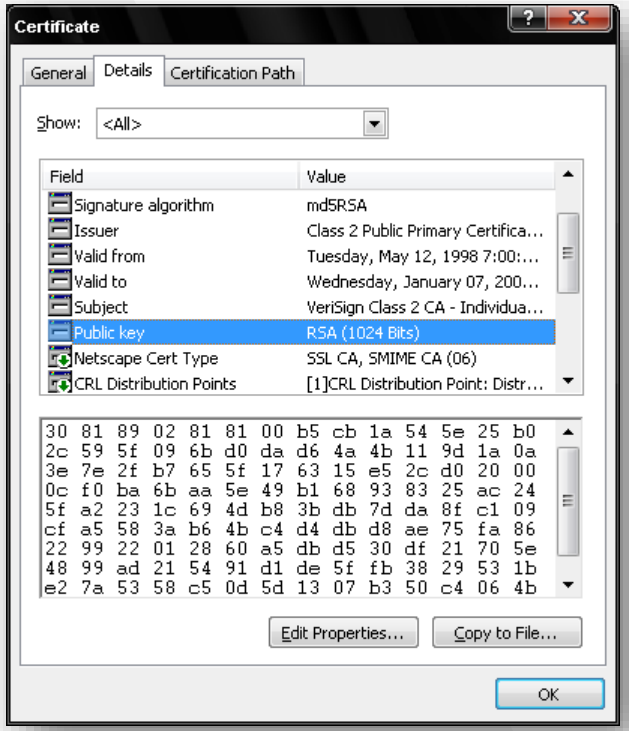


Bảo vệ Client – Chứng nhận số

- 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 / tổ chức cấp chứng nhận
  - Chữ ký điện tử của người / tổ chức cấp chứng nhận

Bảo vệ Client – Chứng nhận số



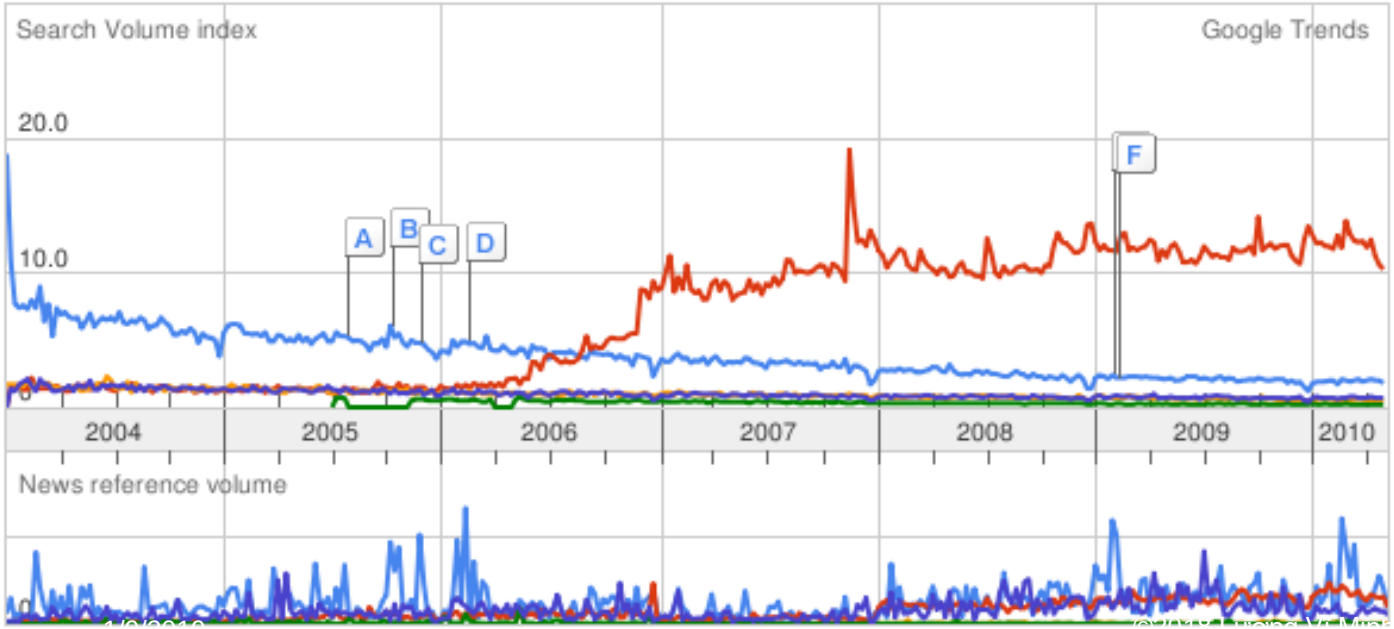

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

Google trends

Searches Websites

Scale is based on the average worldwide traffic of **entrust** in all years. Learn more

verisign 3.90 comodo 6.80 thawte 1.00 geotrust 0.20
entrust 1.00



Certification Practice Statement

- Mỗi CA cấp giấy chứng nhận dựa trên các chính sách và quy trình do CA đó đưa ra.
- Private keys của CA được lưu trữ trên phần cứng an toàn (hardware cryptomodules)
- View Verisign Certification Practice Statement
- INFN (Istituto Nazionale di Fisica Nucleare) CPS

CHRYSALIS LUNA CA3
TRUSTED ROOT KEY SYSTEM

IBM S/390 SECURE
CRYPTOGRAPHIC MODULE

LITRONIC 440
CIPHERACCELERATOR

Bảo vệ Client – Trình duyệt

- 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

Bảo vệ Internet

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

Bảo vệ Internet – Mã hóa

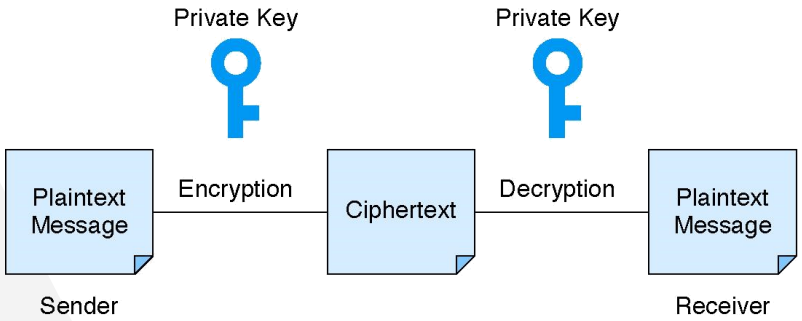
- Mã hóa – Encryption
- Chuyển dữ liệu sang dạng thể hiện khác
  - Thuật toán
  - Khóa
- Có 3 kỹ thuật
  - Mã hóa Hash
  - Mã hóa không đối xứng (public key)
  - Mã hóa đối xứng (secret key)

Bảo vệ Internet – 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, …

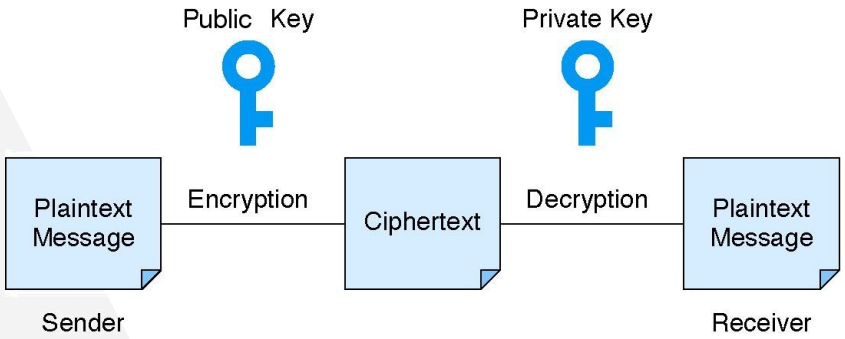
Bảo vệ Internet – Mã hóa đối xứng

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

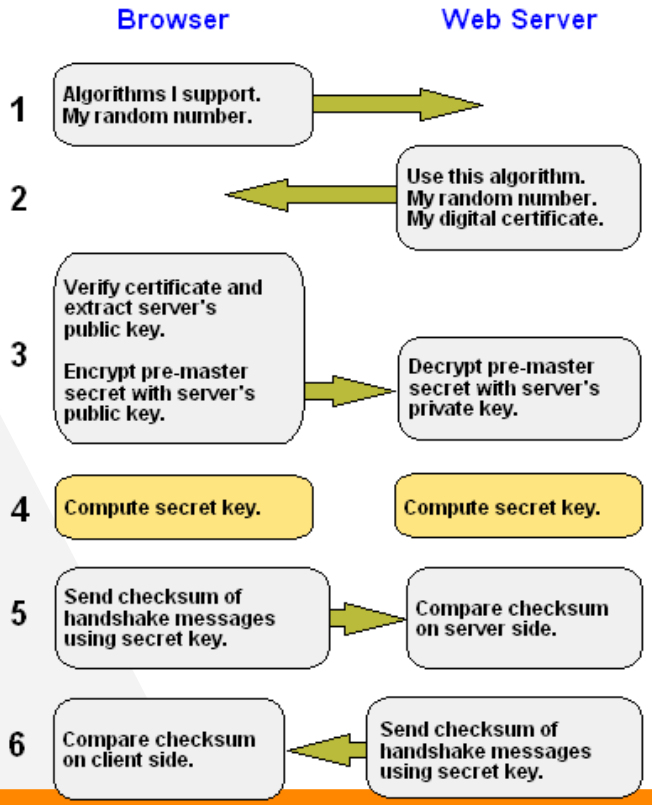


Bảo vệ Internet – Mã hóa bất đối xứng

- Mã hóa dựa vào 1 cặp khóa
  - Public key – mã hóa thông điệp
  - Private key – giải mã thông điệp
- Thuật toán RSA, DSA,…



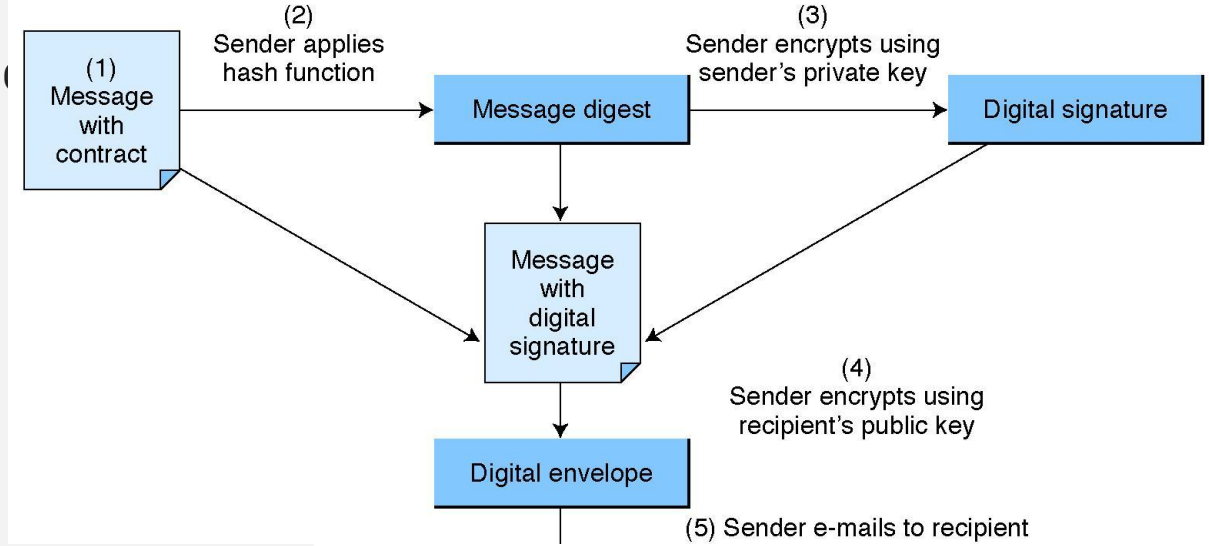
Bảo vệ Internet – Nghi thức SSL



- Nghi thức bảo mật kết nối giữa client và server

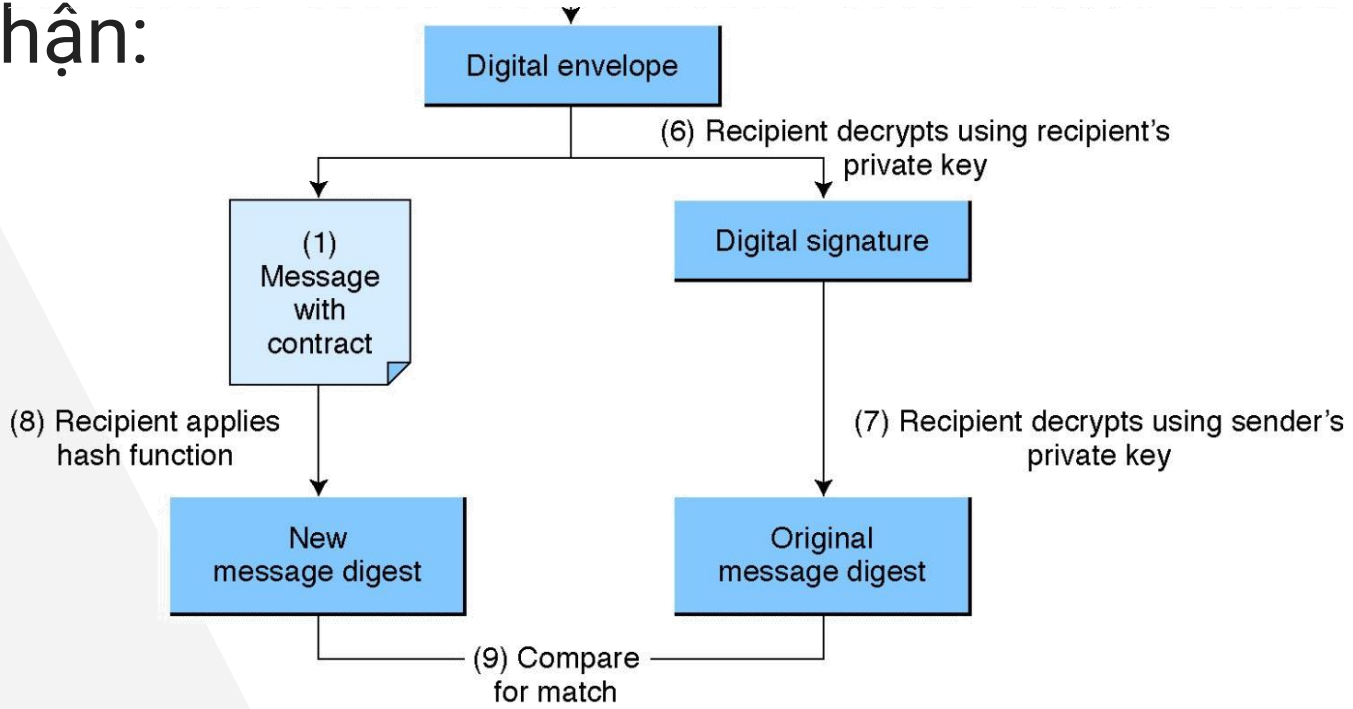
Bảo vệ Internet - Chữ ký điện tử

- Ứng dụng Mã hóa bất đối xứng
- Sử dụng khóa Private để ký nhận thông tin;
- Sử dụng khóa Public trong Chữ ký điện tử để xác thực thông tin
-



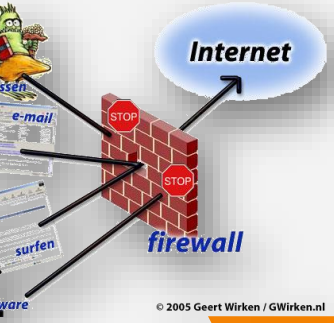
Bảo vệ Internet – Chữ ký điện tử

- 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



Các lời khuyên có ích

Always update your anti-virus software at least weekly

Back up your important files and ensure that they can be restored.

Change the computer's boot sequence to always start the PC from its hard drive

Don't share Drive C: without a password and without read-only restrictions.

Empty floppy drives of diskettes before turning on computers, especially laptops.

Forget opening unexpected e-mail attachments, even if they're from friends

Get trained on your computer's anti-virus software and use it.

Have multiple backups of important files. This lowers the chance that all are infected.

Install security updates for your operating system and programs as soon as possible.

Source: War between Good and Evil. The battlefield is your PC (2003-Dragon Lee)

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