**Chapter 06: Electronic Mail Security.**

**Electronic Mail Security**

Trong hầu như tất cả các môi trường phân phối, thư điện tử là ứng dụng dựa trên mạng **được sử dụng nhiều nhất**.

Người dùng mong đợi để có thể, và làm, gửi e-mail cho những người khác được kết nối trực tiếp hoặc gián tiếp với Internet, **không phụ thuộc host operating system or communications suite.**

Với sự phụ thuộc ngày càng bùng nổ vào e-mail, có mọc một nhu cầu cho các dịch vụ xác thực và bảo mật.

**Hai phương án sử dụng: Pretty Good Privacy (PGP) và S/MIME.**

**Hiện nay nội dung tin nhắn không an toàn:**

• có thể bị kiểm tra hoặc trên đường vận chuyển.

• hoặc bởi người dùng đặc quyền trên hệ thống đích.

**PGP** cung cấp một dịch vụ **bảo mật (confidentiality) và xác thực (authentication)** cái mà có thể được sử dụng đối với thư điện tử và các ứng dụng lưu trữ file.

Những nỗi bật (Enhancements) Email Security:

Confidentiality (Bảo mật): bảo vệ không bị tiết lộ.

Authentication (xác thực): của người gửi tin nhắn.

Message integrity( toàn vẹn tin nhắn): bảo vệ khỏi sửa đổi.

Non-repudiation of origin(Không thoái thác xuất xứ): bảo vệ từ chối bởi người gửi.

**Pretty Good Privacy (PGP):**

sử dụng rộng rãi trên thực tế email an toàn

phát triển bởi Phil Zimmermann

được chọn là **thuật toán mật mã khả dụng tốt nhất** để sử dụng

đc tích hợp vào **một chương trình duy nhất**

**trên Unix, PC, Macintosh và các hệ thống khác**

ban đầu miễn phí, bây giờ cũng có các phiên bản thương mại có sẵn

PGP Operation - **Xác thực(Authentication):**

1. sender creates message

2. make SHA-1160-bit **hash of message**

3. gắn RSA signed hash to message

4. người nhận giải mã và khôi phục hashcode

5. người nhận verifies received message hash.

PGP Operation – **bảo mật (Confidentiality):**

1. sender forms 128-bit random session key

2. encrypts message with session key

3. attaches session key encrypted with RSA

4. receiver decrypts & recovers session key

5. session key is used to decrypt message

PGP – **Authentication & Confidentiality**

Can use both services on same message: ( có thể dùng cả hai dịch vụ trên cùng tin nhắn )

create signature & attach to message

encrypt both message & signature

attach RSA/ElGamal encrypted session key

PGP Operation - Nén ( Compression )

bởi PGP mặc định nén tin nhắn **sau khi ký nhưng trước khi mã hóa**

• để có thể lưu trữ thông điệp không chưa nén & chữ ký để xác minh sau

• & vì nén là không xác định

sử dụng thuật toán nén ZIP

PGP **Operation - Tương thích Email**

Khi PGP được sử dụng, **ít nhất là một phần của khối được truyền đi được mã hóa**

Tuy nhiên email **chỉ được thiết kế cho văn bản**

Do đó PGP phải **mã hóa dữ liệu nhị phân** thành các ký tự ASCII in được

**Sử dụng radix-64 thuật toán**

• bản đồ 3 byte đến 4 ký tự in được

• cũng gắn thêm một CRC

PGP cũng phân đoạn tin nhắn nếu quá lớn

**S / MIME**

* + **Secure / Multipurpose Internet Mail Extensions**
  + tăng cường bảo mật cho MIME email
    - gốc email Internet RFC822 chỉ là văn bản
    - MIME cung cấp hỗ trợ cho các loại nội dung và tin nhắn đa phần khác nhau
    - với **mã hóa dữ liệu nhị phân** đến **hình thức văn bản**
    - S / MIME **đc thêm tăng cường bảo mật**
  + **Có hỗ trợ S / MIME trong nhiều đại lý email**
    - ví dụ như ***MS Outlook, Mozilla, Mac Mail***, vv

**Các Chức năng S / MIME :**

* + Dữ liệu đc bao bọc:
    - nội dung và các key liên kết được mã hóa
  + Đữ liệu đc ký:
    - encoded message + signed digest
  + DDữ liệu đc ký rõ ràng :
    - message cleartext + mã hóa ký digest
  + Đữ liệu được ký & đc bao bọc:
    - làm tổ của các thực thể ký & mã hóa

**S/MIME Cryptographic Algorithms:**

Digital signatures: DSS & RSA

Hash functions: SHA-1 & MD5

Session key encryption: ElGamal & RSA

Message encryption: AES, Triple-DES, RC2/40 and others

MAC: HMAC with SHA-1

Have process to decide which algorithms to use

**S / MIME Tin nhắn**

S / MIME bảo mật một thực thể MIME với một chữ ký, mã hóa, hoặc cả hai

Hình thành một MIME bọc đối tượng PKCS

Có một loạt các nội dung loại:

• Dữ liệu được bao bọc

• Dữ liệu được ký kết

• dữ liệu rõ ràng ký

• yêu cầu đăng ký

• Giấy chứng nhận chỉ có tin nhắn

**S / MIME Certificate Processing:**

S / MIME sử dụng giấy chứng nhận X.509 v3

Đc quản lý bằng cách sử dụng một hỗn hợp của một hệ thống cấp bậc nghiêm ngặt X.509 CA & PGP web của niềm tin

mỗi khách hàng có một danh sách các chứng chỉ CA tin cậy

và own public/private key pairs & chứng chỉ

Giấy chứng nhận phải có chữ ký của CA đáng tin cậy

**Certificate Authorities**

đã một số nổi tiếng của CA

Verisign một trong những phổ biến nhất được sử dụng

Verisign vấn đề một số dạng của kỹ thuật số ID

tăng mức độ kiểm tra và do đó tin tưởng

**S / MIME nâng cao Dịch vụ bảo vệ**

3 đề xuất các dịch vụ bảo mật nâng cao:

• ký chứng từ: signed receipts

• nhãn an ninh: security labels

• danh sách gửi thư an toàn: secure mailing lists

**Domain Keys Identified Mails:**

* một đặc điểm kỹ thuật cho các tin nhắn email mã hóa ký
* nên ký miền nhận trách nhiệm
* người nhận / đại lý có thể xác minh chữ ký
* đề xuất tiêu chuẩn Internet RFC 4871
* đã được áp dụng rộng rãi

**Các mối đe dọa email (Email Threats):**

xem RFC 4684- Phân tích các mối đe dọa Tạo động lực cho Thư DomainKeys Identified

mô tả không gian vấn đề về:

• phạm vi : thấp end , kẻ gửi thư rác, những kẻ lừa đảo

• Khả năng về nơi gửi, ký kết, khối lượng, định tuyến đặt tên vv

• kẻ tấn công ngoài vị trí (outside located attackers)