PENGGUNAAN KRIPTOGRAFI DALAM SISTEM PENGAMANAN EMAIL

Wulandari – NIM : 13506001

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if116001@students.if.itb.ac.id

Abstrak

Sumber daya Internet yang paling penting dan paling banyak dipakai adalah surat elektronis atau yang lebih dikenal dengan sebutan e-mail. Dengan menggunakan e-mail, setiap orang di Internet dapat mentransmisikan suatu pesan teks ke siapapun juga yang ada di Internet.

Electronic mail adalah salah satu sarana komunikasi yang cukup handal. Hal ini diperoleh berdasarkan waktu pengirimannya yang sangat cepat. Proses penyampaian electronic mail dapat dianalogikan dengan penyampaian surat oleh Kantor Pos dan Giro.

Namun, penggunaan email tidaklah menjamin keamanan pesan. Bahkan pengiriman pesan melalui email cenderung tidak aman karena email dikirim melalui jaringan yangberarti melewati komputer-komputer lain sebelum mencapai alamat tujuan.

Makalah ini membahas tentang penggunaan kriptografi dalam sistem pengamanan email menggunakan metode pengamanan Secure / Multi purposa Internet Msil Extensions (S/MIME), MIME Object Security Services (MOSS), Privacy Enhanced Mail (PEM), dan Pretty Good Privacy(PGP).

Sebelum membahas mengenai metode pengamanan email, makalah ini terlebih dahulu membahas mengenai email, baik menyangkut struktur maupun proses pengiriman email untuk mengetahui bagaimana proses penyadapan email dapat terjadi.

***Kata kunci**: Secure / Multi purpose Internet Mail Extenxions(S/MIME), MIME Object Security Services (MOSS), Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP).*

1. Pendahuluan

Internet saat ini sudah menjadi sebuah teknologi yang sangat berkembang. Penggunaan internet sudah merambah di berbagai kalangan, mulai dari masyarakat kelas atas, maupun menengah ke bawah. Hal ini terjadi karena internet memiliki manfaat dan peran yang sangat besar, yaitu sarana penyebaran informasi. Akses dan cara penggunaannya pun tidak lagi dirasa sulit. Oleh sebab itu, penggunaan internet sudah menjadi seperti kebutuhan sehari-hari bagi masyarakat.

Dalam menjalankan perannya sebagai media penyebaran informasi, internet menyediakan berbagai layanan-layanan. Salah satunya yang paling banyak digunakan adalah layanan email (electronic mail). Seperti namanya, layanan ini berfungsi layaknya surat yang dapat mengirimkan pesan dari pengirim kepada penerima. Hanya saja karena layanan ini terhubung dengan internet, proses pengiriman pesan tidak lagi dilakukan secara manual melainkan di proses dalam sebuah jaringan.

Pesan yang dikirim dalam sebuah email terkadang mengandung informasi-informasi yang rahasia sehingga sangat diperlukan sebuah jaminan keamanan bahwa pesan tersebut dapat sampai kepada penerima tanpa dapat dilihat ataupun diubah oleh pihak lain. Hal ini merupakan sesuatu yang sulit mengingat sistem pengiriman melalui jaringan sangat tidak aman. Oleh karena itu, diperlukan sebuah sistem yang dapat meningkatkan pengamanan email.

Pengamanan yang dimaksud meliputi :

- Integritas pesan
  Pesan yang dikirimkan harus dijamin integritasnya, yang berarti tidak ada data yang diubah, ditambah, ataupun dikurangi.
- Verifikasi pengirim
  Sistem pengamanan ini bertujuan untuk memastikan bahwa pesan benar-benar dikirimkan oleh pengirim yang tertulis dalam pesan, bukan merupakan email palsu.
- Verifikasi penerima
  Dalam proses pengiriman pesan harus terdapat verifikasi penerima untuk memastikan bahwa pesan diterima oleh pihak yang berhak menerimanya.

Pengamanan – pengamanan di atas dapat diwujudkan dengan sebuah sistem pengamanan email yang memanfaatkan kriptografi sebagai dasar metodenya. Terdapat banyak metode pengamanan yang tersedia, empat diantaranya yang paling sering ditemukan adalah metode Secure / Multi purpose Internet Mail Extensions (S/MIME), MIME Object Security Services (MOSS) , Privacy Enhanced Mail (PEM) , dan Pretty Good Privacy (PGP) yang akan kita bahas lebih lanjut dalam makalah ini.

2. Kriptografi

Kriptografi merupakan ilmu dan seni untuk menjaga agar pesan aman. Lebih detilnya, kriptografi adalah suatu cara bagaimana agar pengiriman suatu pesan dapat dilakukan dengan aman.

Kriptografi berasal dari kata Crypto yang berarti secret (rahasia) dan graphy yang berarti writing (tulisan).

Cara yang dilakukan dalam menjaga pesan adalah dengan menyandikan informasi dengan suatu kode tertentu (encryption) sehingga tidak bisa terbaca (ciphertext) dan mengembalikan hasil sandi tersebut (decryption) sehingga dapat dibaca oleh penerima pesan (plaintext).

Tugas utama kriptografi adalah untuk menjaga agar baik plaintext maupun kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap. Namun selain untuk keamanan, kriptografi juga memiiliki manfaat lain, diantaranya:

- Authentification
  Penerima pesan dapat memastikan keaslian pengirimnya. Penyerang tidak dapat berpura-pura sebagai orang lain.
- Integritas pesan
  Penerima harus dapat memeriksa apakah pesan telah dimodifikasi ditengah jalan atau tidak.
  Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau merubah pesan selama data berada diperjalanan.
- Nonrepudiation
  Pengirim pesan tidak dapat menyangkal bahwa dialah pengirim pesan sesungguhnya.
- Authority
  Informasi yang berada pada sistem jaringan seharusnya hanya dapat dimodifikasi oleh pihak yang berwenang. Modifikasi yang tidak diinginkan, dapat berupa penulisan tambahan pesan, pengubahan isi, pengubahan status, penghapusan, pembuatan pesan baru (pemalsuan), atau menyalin pesan untuk digunakan oleh penyerang.

3. Email

Seperti yang telah dijelaskan sebelumnya, email merupakan aplikasi yang paling populer di internet. Hal ini dikarenakan email memiliki banyak kelebihan dibandingkan dengan mengirimkan surat secara fisik, diantaranya :

- Cepat. Pengiriman pesan melalui email memerlukan waktu yangsangat sedikit, bahkan untukpesan yang didkirimkan ke negara lain.
- Pesan yang dikirmkan tidak hanya berupa teks. Email dapat pula mengirimkan pesan dalam bentuk gambar, lagu, atau format lainnya.
- Biaya yang dikirimkan sangat murah bila dibandingkan dengan mengirimkan surat fisik.

Namun, pengiriman pesan melalui email memiliki beberapa permasalahan terutama dalam hal pengamanan pesan. Beberapa diantaranya adalah email dapat disadap, dipalsukan, spamming, mailbomb, ataupun relay.

Berdasarkan RFC 882, arsitektur email terdiri dari dua bagian :

- Header
  Layaknya sebuah amplop, sebuah header berisi tentang identitas pengirim dan alamat

email yang dituju. Header sebuah email juga dapat menyimpan host(s) mana saja yang dilalui untuk mengirimkan email tersebut. Contoh header sebuah email dapat dilihat pada Gambar 1. Dapat kita lihat bahwa dalam gambar ini terdapat beberapa kata "received" yang menunjukkan kemana saja email ini dilewatkan.

- Body
  Body sebuah email dipisahkan dengan header dengan sebuah baris kosong. Body merupakan isi email yang ingin dikirimkan.

```
Received: from nic.cafax.se (nic.cafax.se [192.71.228.17])
       by alliance.globalnetlink.com (8.9.1/8.9.1) with ESMTP id QAA31830
       for <budi@alliance.globalnetlink.com>; Mon, 26 Mar 2001 16:18:01 -0600
Received: from localhost (localhost [[UNIX: localhost]])
       by nic.cafax.se (8.12.0.Beta6/8.12.0.Beta5) id f2QLSJVM018917
       for ietf-provreg-outgoing; Mon, 26 Mar 2001 23:28:19 +0200 (MEST)
Received: from is1-55.antd.nist.gov (is1-50.antd.nist.gov [129.6.50.251])
       by nic.cafax.se (8.12.0.Beta5/8.12.0.Beta5) with ESMTP id f2QLSGiM018912
       for <ietf-provreg@cafax.se>; Mon, 26 Mar 2001 23:28:17 +0200 (MEST)
Received: from barnacle (barnacle.antd.nist.gov [129.6.55.185])
       by is1-55.antd.nist.gov (8.9.3/8.9.3) with SMTP id QAA07174
       for <ietf-provreg@cafax.se>; Mon, 26 Mar 2001 16:28:14 -0500 (EST)
Message-ID: <04f901c0b63b$16570020$b9370681@antd.nist.gov>
From: "Scott Rose" <scottr@antd.nist.gov>
To: <ietf-provreg@cafax.se>
Subject: confidentiality and transfers
Date: Mon, 26 Mar 2001 16:24:05 -0500
MIME-Version: 1.0
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4133.2400
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4133.2400
Sender: owner-ietf-provreg@cafax.se
Precedence: bulk
```

Gambar 1. Header sebuah email

Proses pengiriman email memiliki dua komponen, yaitu :

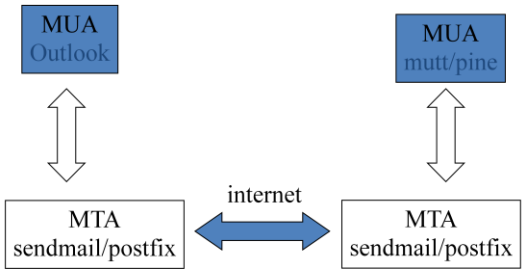
- Mail User Agent (MUA)

MUA adalah komponen yang berhubungan langsung dengan pengguna. MUA menyusun isi header dan body email yang ingin dikirimkan. MUA biasanya merupakan program compose email. Program MUA yang umum digunakan antara lain :

UNIX: elm, mail, mailtool, mush, mutt, netscape mail, pine, dan sebagainya.

MS Windows: Eudora, Microsoft Outlook Express, Netscape Mail, Pegasus seperti Outlook, Eudora, Netscape, Pegasus, Outlook, dan sebagainya.

- Mail Transfer Agent (MTA)
  MTA, atau lebih sering dikenal dengan mail server merupakan komponen yang melakukan perngiriman email.
  Contoh: sendmail, qmail, postfix, exchange



Gambar 2. Hubungan MUA dan MTA

4. Secure / Multi purpose Intenet Mail Extensions (S/MIME)

Secure / Multi purpose Intenet Mail Extensions atau biasa disebut S/MIME, yang saat ini merupakan standar dari secure messaging, adalah sebuah protokol yang menambahkan tanda tangan digital dan enkripsi pada pesan-pesan Internet MIME (Multipurpose Internet Mail Extensions) yang didekripsikan pada RFC 1521. MIME adalah format standar resmi yang diajukan untuk email.

MIME menjelaskan bagaimana srtuktur body dari email. Format MIME mengijinkan e-mail untuk berisi teks, grafik, audio, dan lebih dalam cara standar melalui sistem mail MIME-compliant. MIME sendiri tidak menyediakan layanan keamanan apapun. Tujuan S/MIME adalah untuk menyediakan layanan semacam itu, mengikuti sintaks yang ada pada PKCS #7 untuk tanda tangan digital dan enkripsi. Bagian body dari MIME membawa pesan PKCS #7, dimana ia sendiri adalah hasil dari pemrosesan kriptografi pada bagian body.

S/MIME menggunakan teknik kriptografi kunci publik yang bersifat centralized, artinya sertifikat yang mengikat kunci publik pada nama seseorang harus ditandatangani secara digital oleh CA (Certificate Authority). CA sendiri harus disahkan oleh RA (Regional Authority) yang juga harus disahkan oleh root. Body yang terenkripsi pada email yang menggunakan S/MIME memiliki MIME type sendiri yaitu application/pkcs7-mime. Sementara tanda tangan digital pada S/MIME sama seperti tanda tangan digital pada umumnya yaitu merupakan hasil enkripsi hash dari pesan dengan menggunakan kunci privat pengirim. Tanda tangan digital tersebut dipisah dari body email sebagai bagian tersendiri yang memiliki MIME subtype application/(x-) pkcs7-signature.

Berikut ini adalah langkah-langkah autentikasi e-mail melalui tanda tangan digital S/MIME:

1. Pihak yang berwenang dalam hal sertifikasi publik (contohnya VeriSign, Thawte, GlobalSign, dsb) menerbitkan sertifikat digital bagi alamat e-mail tersebut.
2. E-mail yang dikirimkan melalui alamat yang telah disertifikasi akan dibubuhkan tanda tangan digital dengan kunci privat. Tanda tangan digital ini menyediakan sebuah cara untuk membuktikan keabsahan alamat e-mail pada isian FROM.
3. Penerima e-mail yang dilengkapi dengan fitur S/MIME memvalidasi tanda tangan digital tersebut. Jika tanda tangan tersebut valid, alamat e-mail pada isian FROM dinyatakan sah dan penerima dapat mempercayai isi e-mail tersebut.

Keuntungan dari teknik ini adalah :

1. Teknik ini dapat dijalankan tanpa membutuhkan instalasi software tambahan
2. Alamat FROM tidak mungkin dapat disamarkan karena selalu dilakukan validasi tanda tangan digital.
3. Phisher harus terdaftar dan memiliki certificate authority untuk bisa mengirim phishing e-mail. Akan tetapi hal tersebut tidak akan bermanfaat karena identitas dapat dilacak dan diaudit sehingga mudah dituntut ke pengadilan
4. E-mail dari perusahaan legitimasi dapat dengan mudah diidentifikasi oleh pihak end-user

Sedangkan kerugian dari teknik ini adalah :

1. Tidak semua e-mail client mendukung teknologi S/MIME
2. Terdapat kemungkinan bahwa penerima e-mail tidak memeriksa certificate revocation status.
3. Teknik ini menuntut biaya yang cukup tinggi bagi pengguna.
4. Harus ada informasi tentang tanda tangan digital pada gateway dari pihak pengirim dan penerima.

5. MIME Object Security (MOSS)

MOSS menyediakan layanan keamanan email yang lebih fleksibel dengan mendukung model kepercayaan yang berbeda. Diperkenalkan pada tahun 1995, MOSS menyediakan otentikasi, integritas, kerahasiaan, dan non repudiasi untuk email. MOSS menggunakan MD2/MD5, kunci publik RSA, dan DES. MOSS juga mengijinkan identifikasi pengguna diluar standar X.509.

6. Pretty Good Privacy (PGP)

PGP adalah sebuah program enkripsi yang dikembangkan oleh Phil Zimmerman pada awal tahun 90-an. PGP dapat digunakan untuk mengenkripsi e-mail maupun file. Pada awalnya, Phil Zimmerman menyediakan PGP secara free untuk siapapun, namun hal ini diprotes oleh pemerintah USA dengan alasan batasan ekspor terhadap teknologi enkripsi. PGP dipasarkan oleh Network Associates..

Pada PGP, cipher simetris IDEA digunakan untuk mengenkrip pesan, dan RSA digunakan untuk pertukaran kunci simetris dan untuk tanda tangan digital. Selain menggunakan CA, PGP menggunakan Web of Trust. Pengguna dapat mensertifikasi satu sama lain dalam mesh model, yang baik diterapkan untuk kelompok yang lebih kecil.

Sistem infrastruktur kunci publik pada PGP tidak bersifat centralized seperti pada S/MIME namun

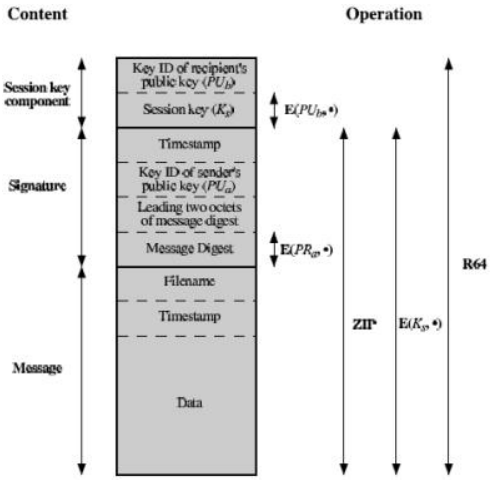
skema uncentralized yang bernama vetting scheme, sementara model trust-nya disebut web of trust. Pendistribusian publik key membutuhkan identity certificate yang dibuat sedemikian rupa sehingga perubahan sertifikat ini oleh pihak yang tidak berhak akan terdeteksi. identity certificate menyatakan bahwa publik key terikat pada nama tertentu dan ditandatangani secara digital oleh pihak ketiga.

Sistem enkripsi PGP merupakan sistem hybrid menggabungkan kecepatan enkripsi sistem kunci simetri dan keamanan sistem kunci publik. Untuk mengenkripsi suatu pesan mula-mula PGP memampatkan pesan tersebut untuk dengan tujuan menghemat bandwidth dan disk space sekaligus menghilangkan pola pesan yang biasanya dimanfaatkan kriptanalis, kemudian PGP membuat suatu session key untuk sistem kunci simetri, pesan yang telah dimampatkan kemudian dienkripsi dengan session key tersebut yang hanya dipergunakan sekali, terakhir session key tersebut dienkripsi dengan kunci publik penerima pesan dan dimasukkan dalam pesan. Untuk mendekripsi pesan dilakukan kebalikannya penerima pesan mendekripsi session key menggunakan kunci privatnya, kemudian session key itu digunakan untuk mendekripsi pesan.

Tanda tangan digital pada PGP memiliki format yang sama yaitu merupakan hasil enkripsi hash dari pesan dengan menggunakan kunci privat pengirim. Namun berbeda dengan S/MIME tanda tangan digital ini dimasukkan sebagai body dari email dan dienkripsi bersama body email.

Proses penggunaan PGP dapat dijabarkan secara singkat sebagai berikut:

1. Pengirim dan penerima harus sudah memiliki kunci publik satu sama lain.
2. Sebuah kunci simetris untuk sesi yang akan dilakukan, dibuat secara acak oleh perangkat lunak PGP. Pesan yang akan dikirim kemudian dienkripsi dengan kunci simetris.
3. Kunci simetris sesi tadi kemudian dienkripsi dengan kunci publik penerima.
4. Pesan yang telah dienkripsi beserta kunci simetris yang telah dienkripsi tadi dikirim kepada penerima
5. Penerima mendekripsi kunci simetris tadi menggunakan kunci privatnya guna mendapatkan kunci simetris.
6. Berbekal kunci simetris itu, penerima kemudian dapat mendekripsikan pesan yang tersandikan.



Gambar 3. Format Umum Pesan PGP

7. Privacy Enhanced Mail (PEM)

PEM merupakan standar pengamanan email yang diusulkan oleh Internet Engineering Task Force (IETF) untuk menjadi compliant dengan standar kriptografi kunci publik (PKCS), yang dikembangkan oleh konsorsium yang terdiri dari Microsoft, Novell, dan Sun Microsystems. PEM mendukung enkripsi dan otentikasi Internet email. Untuk enkripsi pesan, PEM menggunakan Triple DES-EDE menggunakan sepasang kunci simetris. Algoritma hash RSA MD2 atau MD5 digunakan untuk menghasilkan message digest, dan enkripsi kunci publik TSA mengimplementasi tanda tangan digital dan distribusi kunci rahasia. PEM menggunakan sertifikat yang berdasar pada standar X.509 dan dihasilkan oleh CA formal.

8. Kesimpulan

Tak dapat dipungkiri, penggunaan email sangat erat dalam kehidupan manusia dalam era sepertisekarang dimana teknologi mengalami kemajuan yang pesat tiap waktunya. Namun penggunaan email tidak dapatterlepas dari ancaman-ancaman yang terjadi dalam proses pengiriman email.

Terdapat banyak metode yang bertujuan untuk meningkatkan keamanan dari pesan yang dikirmkan. Empat diantaranya adalah Secure / Multi purposa Internet Msil Extensions (S/MIME), MIME Object Security Services (MOSS), Privacy Enhanced Mail (PEM), dan Pretty Good Privacy(PGP).

Melalui makalah ini, dapat disimpulkan bahwa keempat metode di atas memiliki kelebihan dan

kekurangan masing-masing. Sampai saat ini belum ada metode yang benar-benar dapat menjamin keamanan dari email yang dikirimkan. Namun, keempat metode diatas dirasa sudah cukup baik dan sangat membantudalam hal pengamanan email.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung.

[2] An Introduction to Cryptography. (2002). PGP Corporation.

[3] Callas, "OpenPGP Message Format", RFC 2440, November 1998.

[4] M. Elkins, "MIME Security with Pretty Good Privacy (PGP)", RFC 2015, Oktober 1996.

[5] William Stallings, "Cryptography and Network Security: Principles and Practices" , 3rd edition, Pearson Education International, 2003.

[6] Alfred J. Menezes, Paul C. Van Oorschot, dan Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[7] Aguirre, Jorge Ramió. (2005). Electronic Book About Computer Security and Crypthography.http://www.criptored.upm.es/guiateoria/gt_m001a.htm.

[8] NAI. (1999). Network Associates, Inc. http://www.nai.com.

[9] Kak, Avinash. (2006). Security for Internet Application. Purdue University