Peningkatan Layanan Keamanan S/MIME

Andi Hasad
andihasad@yahoo.com
Sekolah Pascasarjana IPB, Departemen Ilmu Komputer
Jl. Raya Darmaga, Kampus IPB Darmaga, Wing 20 Level 5-6,
Bogor - Jawa Barat, Indonesia,16680
Telp. 0251-8625584, Fax. 0251-8625584

I. Pendahuluan

Untuk memahami S/MIME, diperlukan pemahaman umum format dasar dari email yang digunakan, yaitu MIME (*Multipurpose Internet Mail Extension*). MIME merujuk kepada protokol yang luas digunakan di dalam dunia internet yang memperluas protokol SMTP *(Simple Mail Transfer Protocol*) yang merupakan protokol dari format standar e-mail tradisional (RFC / Request For Comment 5322), untuk mengizinkan beberapa data selain teks dengan pengodean ASCII, seperti video, suara, dan berkas biner, agar dapat ditransfer melalui e-mail tanpa harus mentranslasikan terlebih dahulu data-data tersebut ke dalam teks berformat ASCII. MIME merupakan bagian dari protokol HTTP, dan *web browser* dan *server* HTTP akan menggunakan MIME untuk menginterpretasikan berkas-berkas e-mail yang dikirimkan dan diterima.

Pada dasarnya, sebuah pesan SMTP hanya boleh mengandung berkas teks saja yang dikodekan dengan menggunakan pengodean ASCII 7-bit saja. Berkas-berkas biner, seperti halnya program, dokumen pengolah kata, dan banyak lagi format lainnya, tidak dapat dikirimkan melalui SMTP. Dengan menggunakan MIME yang didefinisikan di dalam RFC 1521, hal tersebut bukan lagi masalah. Meskipun demikian, protokol ini tidaklah dibuat untuk menggantikan protokol SMTP, tapi hanya memperluas pada dua bagian yaitu : "*multipart message body*" dan "*non-ASCII message content*". MIME menambahkan dua jenis *header* SMTP tambahan, yakni sebagai berikut:

- *Content-Type* : menentukan jenis content yang dibawa oleh pesan-pesan SMTP.
- *Content-Transfer-Encoding* : menentukan metode apa yang digunakan untuk mengodekan pesan-pesan SMTP.

RFC 1521 menentukan tujuh buah jenis content dasar yang dapat dimasukkan ke dalam *header Content-Type* dalam pesan SMTP. Setiap jenis content dasar ini memiliki beberapa *Content Subtype* yang menentukan informasi apa yang dibawa oleh pesan-pesan SMTP, yakni sebagai berikut:

- *Text* : yang menentukan bahwa pesan yang dibawa oleh protokol SMTP merupakan teks biasa saja (*Text/plain*), teks kaya (*Text/richtext*), *Text/html*, dan beberapa jenis lainnya.
- *Application* : yang menentukan bahwa pesan yang dibawa oleh protokol SMTP merupakan data biner. Beberapa jenis subtype untuk type ini adalah *Application/octet-stream, Application/Postscript, Application/msword* (dokumen Microsoft Word 97-2003) dan masih banyak lagi.
- Berkas: yang menentukan bahwa pesan yang dibawa oleh protokol SMTP adalah gambar. Beberapa jenis *subtype* untuk *type* ini adalah Image/gif, Image/jpg, Image/png, Image/tiff dan lain-lain.
- *Audio* : yang menentukan bahwa pesan yang dibawa oleh protokol SMTP adalah berkas *audio*.

- *Video* : yang menentukan bahwa pesan yang dibawa oleh protokol SMTP adalah berkas *video*.
- *Message* : Beberapa jenis subtype antara lain Message/rfc5322 (pesan asli teks standar RFC 5322), *Message/HTTP* (untuk lalu lintas HTTP), dan beberapa lainnya
- *Multipart*

RFC 1521 juga mendefinisikan metode pengodean data tambahan yang dapat ditentukan pada *field Content-Transfer-Encoding* dalam *header* SMTP, yakni:

- 7 bit: pengodean yang digunakan adalah teks ASCII 7 bit, dengan batasan panjang hingga kurang dari 1000 karakter
- 8 bit
- *binary*
- *quoted-printable*
- *base64 (UUEncoded data)*
- *x-token*

S/MIME (*Secure / Multipurpose Internet Mail Extension*) adalah peningkatan keamanan standar format email internet MIME, yang didasarkan pada teknologi dari keamanan data RSA. Meskipun *Pretty Good Privacy* (PGP) dan S/MIME berada pada jalur standar *Internet Research Task Force* (IETF), kemungkinan S/MIME akan muncul sebagai standar industri untuk penggunaan komersial dan organisasi, sementara PGP akan tetap menjadi pilihan untuk keamanan e-mail pribadi untuk banyak pengguna. S/MIME didefinisikan dalam sejumlah dokumen, yang paling penting adalah RFC3369, 3370, 3850 dan 3851.

II. RFC 822 atau RFC 5322

Sebuah dokumen RFC adalah salah satu dari seri dokumen infomasi dan standar internet bernomor yang diikuti secara luas oleh perangkat lunak untuk digunakan dalam jaringan, internet dan beberapa sistem operasi jaringan, mulai dari Unix, Windows, dan Novell NetWare. RFC kini diterbitkan di bawah arahan *Internet Society* (ISOC) dan badan-badan penyusun-standar teknisnya, seperti *Internet Engineering Task Force* (IETF) atau *Internet Research Task Force* (IRTF). Semua standar Internet dan juga TCP/IP selalu dipublikasikan dalam RFC, meskipun tidak semua RFC mendefinisikan standar Internet. Beberapa RFC bahkan hanya menawarkan informasi, percobaan/eksperimen, atau hanya informasi sejarah saja. Sebelum menjadi sebuah dokumen RFC, sebuah dokumen yang diajukan akan dianggap menjadi draf Internet (Internet draft), yang merupakan sebuah dokumen yang umumnya dikembangkan oleh satu orang pengembang di dalam kelompok kerja IETF atau IRTF. Sebagai contoh, kelompok kerja IPv6 (IPv6 *working group*) mengkhususkan usahanya hanya untuk mengembangkan standar-standar yang akan digunakan pada IPv6, protokol calon pengganti IPv4. Setelah beberapa waktu, dokumen tersebut akan diulas dan akhirnya harus diterima secara konsensus oleh para penguji. Dan setelah diterima, maka IETF pun menerbitkan versi final dari draf Internet tersebut menjadi sebuah RFC dan kemudian memberikan nomor urut kepadanya, yang disebut sebagai *RFC Number*.

RFC 5322 mendefinisikan format untuk pesan teks yang dikirim menggunakan *mail* (surat) elektronik. RFC 5322 telah menjadi standar untuk pesan teks berbasis *internet mail* dan masih umum digunakan. Dalam konteks RFC 5322, pesan akan dipandang sebagai amplop dan isinya (Gambar 1). Amplop berisi informasi apa pun yang diperlukan untuk mencapai transmisi dan pengiriman sedangkan isi membentuk objek yang akan dikirim ke penerima.

Standar RFC 5322 hanya berlaku untuk isi. Namun, standar isi mencakup satu set *field header* yang dapat digunakan oleh sistem *mail* untuk membuat amplop, dan standar ini dimaksudkan untuk memudahkan perolehan informasi oleh program. Struktur keseluruhan dari sebuah pesan yang sesuai dengan RFC5322 sangat sederhana.

Gambar 1 Ilustrasi pesan dalam konteks RFC 5322

Sebuah pesan terdiri dari beberapa jumlah baris *header* (*the header*) diikuti oleh teks yang tidak dibatasi penggunaannya (*the body*). *Header* dipisahkan dari *body* oleh baris kosong.

Sebuah *header* biasanya terdiri dari sebuah kata kunci, diikuti oleh titik dua, diikuti oleh argumen kata kunci; format memungkinkan sebuah garis panjang untuk dipecah menjadi beberapa baris. Kata kunciyang paling sering digunakan adalah Dari, Untuk, Subjek, danTanggal. Berikut adalah contoh pesan :

```
Date: October 8, 2009 2:15:49 PM EDT
From: William Stallings <ws@shore.net>
Subject: The Syntax in RFC 5322
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual
message body, which is delimited from the
message heading by a blank line.
```

Bidang lain yang umum ditemukan dalam *header* RFC 5322 adalah *Message-ID*. Bidang ini berisi pengenal unik terkait dengan pesan ini.

III. Keterbatasan RFC 5322

MIME adalah perluasan untuk kerangka RFC 5322 yang dimaksudkan untuk mengatasi beberapa masalah dan keterbatasan penggunaan SMTP atau protokol transfer mail lain dan RFC 5322 untuk mail elektronik. Daftar keterbatasan antara lain :

1. SMTP tidak bisa mengirimkan file *executable* atau objek biner lainnya. Sejumlah skema sedang digunakan untuk mengkonversi file biner ke dalam bentuk teks yang dapat digunakan oleh sistem mail SMTP, termasuk UNIX populer *uuencode* / skema *uudecode*. Namun, tidak satupun dari hal iniyang merupakan suatu standar atau bahkan *standar de facto*.
2. SMTP tidak dapat mengirimkan data teks yang berisi karakter bahasa nasional karena ini diwakili oleh kode 8-bit dengan nilai desimal 128 atau lebih tinggi, dan SMTP terbatas untuk ASCII 7-bit.
3. *Server*SMTP mungkin menolak pesan email lebih dari ukuran tertentu.

4. *Gateway* SMTP yang menerjemahkan antara ASCII dan karakter kode EBCDIC tidak menggunakan satu set konsisten pemetaan yang berakibat pada masalah terjemahan.
5. *Gateway* SMTP ke jaringan mail elektronik X.400 tidak dapat menangani data *nontextual* termasuk dalam pesan X.400.
6. Beberapa implementasi SMTP tidak mematuhi sepenuhnya standar SMTP yang didefinisikan dalam RFC 821. Masalah umum meliputi:
   - Penghapusan, penambahan, atau pemesanan ulang dari *carriage return* dan*linefeed*
   - Memotong atau pembungkus garis lebih panjang dari 76 karakter
   - Penghapusan *trailing white space* (tab dan karakter spasi)
   - *Padding* baris dalam pesan dengan panjang yang sama
   - Konversi karakter tab ke beberapa karakter spasi

MIME dimaksudkan untuk menyelesaikan masalah-masalah ini dengan cara yang kompatibel dengan implementasi RFC 5322. Spesifikasi disediakan dalam RFC 2045 sampai 2049.

IV. MIME

Spesifikasi MIME mencakup unsur-unsur berikut :

1. Lima bidang *header* pesan baru didefinisikan, yang dapat dimasukkan dalam RFC 5322 header. Bidang ini memberikan informasi tentang *body* pesan.
2. Sejumlah format konten yang didefinisikan, sehingga standardisasi representasi multimedia yang mendukung *mail* elektronik.
3. Transfer *encoding* didefinisikan yang memungkinkan konversi format konten ke dalam bentuk yang dilindungi dari perubahan oleh sistem email.

Dalam subbagian ini, diperkenalkan bidang-bidang pesan lima *header*. Kesepakatan dua subbagian berikutnya dengan format isi dan pengodean transfer. Bidang *the fiveheader* didefinisi kan dalam MIME, sebagai berikut :

- **MIME-Version** : Harus memiliki nilai parameter 1.0. Bidang ini menunjukkan bahwa pesan tersebut sesuai dengan RFC 2045 dan 2046.
- **Content-Type** : Menjelaskan data yang terdapat dalam *body* dengan rincian yang memadai bahwa agen *user* penerima dapat mengambil seorang agen yang tepat atau mekanisme untuk mewakili data kepada *user* atau berurusan dengan data dalam cara yang tepat.
- **Content-Transfer-Encoding** : Menunjukkan tipe transformasi yang telah digunakan untuk mewakili *body* pesan dengan cara yang dapat diterima untuk transportasi *mail*.
- **Content-ID**: Digunakan untuk mengidentifikasi MIME entitas unik dalam beberapa konteks.
- **Content-Description** : deskripsi teks dari objek dengan *body*, ini berguna ketika objek tidak dapat dibaca (misalnya, data audio).

Salah satu atau semua bidang ini mungkin muncul dalam sebuah *header* normal RFC 5322. Implementasi yang sesuai harus mendukung *MIME-Version, Content-Type,* dan *Content-Transfer-Encoding,* sedangkan *Content-ID* dan bidang *Content-Description* adalah opsional

dan dapat diabaikan oleh implementasi penerima.

V. S/MIME

S/MIME memanfaatkan sejumlah tipe konten baru MIME yang ditunjukkan dalam Tabel 1. Semua tipe aplikasi baru menggunakan penandaan PKCS mengacu pada spesifikasi kriptografi kunci publik yang dikeluarkan oleh RSA Laboratories.

Tabel 1. Tipe-tipe konten S/MIME

Tipe	Subtipe	Parameter S/MIME	Deskripsi
Multipart	Signed		Pesan ditandatangani dalam dua bagian : pesan dan tanda tangan.
Application	pkcs7-mime	signedData	Menandatangani entitas S/MIME
	pkcs7-mime	envelopeData	Mengenkripsi entitas S/MIME
	pkcs7-mime	Degenerate signedData	Entitas hanya berisi sertifikat kunci publik
	pkcs7-mime	compressedData	Mengkompres entitas S/MIME
	pkcs7-signature	signedData	Tipe konten dari sub bagian tanda tangan pada pesan multipart/signed.

VI. Peningkatan Layanan Keamanan S/MIME

S/MIME melindungi entitas MIME dengan tanda tangan, enkripsi, atau keduanya. Entitas MIME merupakan pesan keseluruhan (kecuali untuk *header* RFC 5322), jika tipe konten MIME multipart, maka entitas MIME terdiri dari satu atau lebih dari subbagian pesan entitas MIME yang disusun menurut aturan normal untuk persiapan pesan MIME. Entitas MIME kemudian ditambah beberapa data yang berhubungan dengan keamanan, seperti algoritma identifikasi dan sertifikat yang diproses oleh S/MIME untuk menghasilkan apa yang dikenal sebagai objek PKCS. Sebuah objek PKCS kemudian diperlakukan sebagai konten pesan dan dibungkus di dalam MIME (disediakan dengan *header* MIME yang sesuai). Penerapan algoritma keamanan menggunakan *transfer encoding base64*.

Beberapa jasa peningkatan layanan keamanan yang dapat dilakukan, yaitu :

- *Signed receipt* : Sebuah tanda terima yang telah ditandatangani dapat diminta dalam objek *SignedData*. Mengembalikan tanda terima yang telah ditandatangani menyediakan bukti pengiriman pesan dan memungkinkan pengirim untuk menunjukkan kepada pihak ketiga bahwa penerima telah menerima pesan. Tanda tangan penerima pesan seluruhnya asli ditambah tanda tangan pengirim pesan asli dan menambahkan tanda tangan baru untuk membentuk pesan baru S/MIME.
- *Security labels* : Label keamanan dapat dimasukkan dalam atribut otentikasi objek *SignedData*.
- Penggunaan MLA S/MIME untuk membebaskan pengguna mengirim pesan ke beberapa penerima yang memerlukan pemrosesan tertentu per-penerima. MLA dapat mengambil satu pesan yang merupakan seperangkat keamanan informasi tentang sensitivitas dari konten yang dilindungi oleh enkapsulasi S/MIME. Label dapat digunakan untuk kontrol akses, dengan menunjukkan pengguna yang diizinkan akses ke objek. Kegunaan lain mencakup prioritas (kerahasiaan, konfidensial, dibatasi, dan sebagainya) atau berbasis

peran, yang menggambarkan jenis orang dapat melihat informasi (misalnya, tim pasien kesehatan, agen penagihan medis, dll).

- *Secure mailing lists* : Pemanfaatan Mail List Agent yang masuk, melakukan enkripsi penerima-spesifik untuk masing-masing penerima, dan *forward* pesan, pengirim pesan hanya perlu mengirim pesan ke MLA dengan enkripsi yang dilakukan dengan menggunakan kunci publik MLA tersebut.

Referensi :

Neyman Shelvie N., *Materi Kuliah Keamanan Informasi*, Sekolah Pascasarjana IPB, Bogor

Stalling William, 2005, *Cryptography and Network Security, Principles and Practices*, Prentice Hall, USA

Stalling William, 2011,*Network Security Essential, Applications and Standards*, Prentice Hall, USA

Andi Hasad menempuh pendidikan di program studi Teknik Elektro (S1) UNHAS, Makassar, kemudian melanjutkan di Ilmu Komputer (S2) IPB, Bogor. Penulis pernah menimba ilmu dan pengalaman di berbagai perusahaan / industri di Jakarta dan Bekasi. Saat ini menekuni profesi sebagai dosen tetap di Fakultas Teknik UNISMA Bekasi serta aktif dalam pengembangan ilmu di bidang *robotics, computational intelligence, electronic instrumentation, intelligent control, knowledge management system, network* dan *cryptography*. Info lengkap penulis dapat diakses di http://andihasad.wordpress.com/