KEAMANAN EMAIL

Subianto | AMIK JTC SEMARANG

Pendahuluan

- Email merupakan aplikasi yang paling utama di jaringan Internet.
- Hampir setiap orang yang menggunakan Internet memiliki alamat email.
- Saat ini akan aneh jika anda tidak memiliki alamat email.
- Kemampuanmenggunakan email sama esensialnya dengan kemampuan menggunakan telepon.

masalah keamanan yang terkait dengan sistem email

- disadap
- dipalsukan
- disusupi (virus)
- spamming
- mailbomb
- mail relay

Sistem email

- ***Mail User Agent* (MUA)**
  - MUA merupakan komponen yang digunakan oleh pengguna email.
  - Biasanya dia yang disebut program mail. Contoh MUA adalah Eudora, Netscape, Outlook, Pegasus, Thunderbird, pine, mutt, elm, mail, dan masih banyak lainnya lagi.
  - MUA digunakan untuk menuliskan email sepertihalnya mesin ketik digunakan untuk menulis surat jaman dahulu.

Sistem email

- ***Mail Tranfer Agent* (MTA)**
  - MTA merupakan program yang sesungguhnya mengantar email.
  - Biasanya dia dikenal dengan istilah mailer.
  - MTA ini biasanya bukan urusan pengguna, akan tetapi merupakan urusan dari administrator.
  - Contoh MTA antara lain postfix, qmail, sendmail, exchange, MDaemon, Mercury

Format Email

- HEADER, Berisi alamat tujuan, alamat pengirim dan hal-hal yang perlu diketahui untuk mengantarkan email

- BODY, merupakan isi dari surat itu

From: Subianto Masbianto<masbianto1@gmail.com>
To: amikjtc@amikjtc.com
Subject: Ujian diundur

Ujian kuliah saya akan diundur sampai ada pengumuman berikutnya. Mohon maaf atas ketidaknyamanan.

Penyadapan

- Potensi penyadapan ini dapat terjadi karena pengiriman emailmenggunakan protokol SMTP (Simple Mail Transport Protocol)1 yang tidak menggunakan enkripsi sama sekali. Jika kita berada pada satu jaringan yang sama dengan orang yang mengirim email, atau yang dilalui oleh e maka kita bisa menyadap email dengan memantau port 25, yaitu port yang digunakan oleh SMTP.mail

- Demikian pula untuk mengambil email, biasanya digunakan protokol POP (Post Office Protocol)1. Protokol yang menggunakan port 110 ini juga tidak menggunakan enkripsi dalam transfer datanya. Ketika seorang pengguna mengambil email melalui POP ke mail server, maka kita bisa menyadap data yang melewati jaringan tersebut.

Pengaman Penyadapan

- Agar email aman dari penyadapan maka perlu digunakan enkripsi untuk mengacak isi dari email.
- Header dari email tetap tidak dapat dienkripsi karena nanti akan membingungkan MTA.
- Dahulu, proses enkripsi dari email harus dilakukan secara manual oleh pengguna. Dia harus mengenkripsi pesan atau data yang ingin dia kirimkan dengan sebuah program, kemudian menyisipkan (attach) berkas tersebut ke dalam email.
- Saat ini sudah ada beberapa program (tools) yang dapat mempermudah atau mengotomasinya
- Contoh program tersebut antara lain Pretty Good Privacy (PGP), GnuPG, dan PEM.

Email Palsu

- Demikian pula membuat email palsu tidak terlalu sukar. Kita tinggal
- menuliskan informasi yang salah di header dari email. (Misalnya kita konfigurasikan sistem email kita dengan mengatakan bahwa kita adalah si-doel@hotmail.com.) Email yang palsu ini kemudian kita serahkan kepada MTA untuk dikirimkan ke tempat yang dituju. Maka MTA akan melakukan perintah tersebut.
- Namun perlu diingat bahwa aktivitas kita tercatat oleh MTA.

Pengaman Email Palsu

- Sebagaipenerima email, kita bisa melihat header dari email. Kita lihat tempat tempat yang dilalui oleh email tersebut.
- Sayangnya jarang sekali pengguna email melihat isi dari header email sehingga mereka mudah tertipu dengan email palsu.
- Cara lain untuk memastikan bahwa email berasal dari orang yang bersangkutan adalah dengan menggunakan digital signature
- **Digital Signature adalah** salah satu teknologi yang digunakan untuk meningkatkan keamanan jaringan.
- **Digital Signature** memiliki fungsi sebagai penanda pada data yang memastikan bahwa data tersebut adalah data yang sebenarnya (tidak ada yang berubah).

Penyusupan Virus

- Email sering dijadikan medium yang paling efektif untuk menyebarkan virus.
- Hal ini disebabkan email langsung menuju pengguna yang umumnya merupakan titik terlemah (weakest link) dalam pertahanan sebuah perusahaan atau institusi.
- program mail (MUA) dahulu sering dikonfigurasi untuk secara otomatis menjalankan program aplikasi yang sesuai dengan attachment yang diterima

Pencegahan Penyusupan Virus

- Solusi untuk mengurangi impak terhadap penyusupan virus adalah dengan menggunakan anti-virus dengan data (signature) yang terbaru.

- Melakukan pemeriksaan terhadap virus pada level mail server.

Spam

- Spam1 adalah didefinisikan sebagai “unsolicited email”, yaitu email yang tidak kita harapkan.
- Spam ini berupa email yang dikirimkan ke banyak orang.
- Biasanya isi dari email ini adalah promosi.
- Spam ini tidak terfilter oleh anti-virus karena memang dia bukan virus.

Pencegahan Spam

- Spam Filter

  Filter terhadap spam harus dilakukan secara khusus. Namun mekanisme untuk melakukan filtering spam ini masih sukar karena kesulitan dalam membedakan antara email biasa dan email yang spam.

- Statistik (Bayesian)

  statistik (Bayesian) yang menghitung kata-kata di dalam email. Jika ada banyak kata yang merupakan kata kunci dari spammer, maka statistik akan menunjukan probabilitas bahwa email tersebut merupakan spam.

Mailbomb

- Salah satu bentuk kejahatan di internet dengan cara membanjiri email korban dengan data atau kiriman email yang banyak. Sehingga ada kemungkinan email korban tidak bisa diakses lagi.
- Email yang tidak dapat di akses bisa saja berhari-hari, berjam-jam atau mungkin selamanya.

Pencegahan Mailbomb

- **Tarpitting**: tarpitting mendeteksi pesan masuk yang ditujukan untuk pengguna yang tidak diketahui. Jika server e-mail Anda mendukung tarpitting, dapat membantu mencegah spam atau DoS serangan terhadap server Anda. Jika ambang batas yang telah ditetapkan terlampaui - mengatakan, lebih dari sepuluh pesan - fungsi tarpitting efektif shuns lalu lintas dari alamat IP pengirim untuk jangka waktu.
- **E-mail firewall**: E-mail firewall dan aplikasi konten-filtering dari vendor seperti Symantec dan Barracuda Networks dapat pergi jauh menuju mencegah berbagai serangan e-mail. Alat-alat ini melindungi hampir setiap aspek dari sistem e-mail.
- **Perlindungan perimeter**: Meskipun tidak e-mail tertentu, banyak firewall dan IPS sistem dapat mendeteksi berbagai serangan e-mail dan mematikan penyerang secara real time. Hal ini dapat berguna selama serangan.

Mail Relay

- Mail relay Adalah fasilitas untuk mengirimkan email dengan menumpangkan kepada server yang di sebut relay. Server tersebutlah yang nantinya mengirimkan email ke alamat tujuan.
- Mail relay merupakan software SMTP Proxy sederhana dan Relay MTA yang berfungsi sebagai filter.
- Jenis Mail Relay
- *Closed Relay* yang berarti *secure* atau aman dalam artian pesan email hanya akan di relay oleh mail server untuk pengguna-pengguna yang terverifikasi memiliki akses untuk ke server relay. *Closed Relay* adalah pengaturan umumnya yang diberlakukan server internal untuk mencegah penyalahgunaan internet. Kedua,
- *Open Relay* merupakan server SMTP yang digunakan untuk

Penyalahgunaan Mail Relay

- Disabotase untuk mengirimkan junk mail, yang disebut spamming, dengan menumpang mail server milik orang lain.