

# KEAMANAN EMAIL

Email Security



## Tentang email

- Email merupakan aplikasi yang paling populer di Internet
- Masalah email
  - Disadap
  - Dipalsukan
  - Disusupi (virus)
  - Spamming
  - Mailbomb
  - Mail relay

Email security

-2-



## masih tentang email

- Sistem email memiliki dua komponen
  - **Mail User Agent (MUA)**  
Berhubungan dengan pengguna.  
Contoh: mutt, pine, pegasus, eudora, netscape, outlook, thunderbird
  - **Mail Transfer Agent (MTA)**  
Yang melakukan pengiriman email.  
Contoh: sendmail, qmail, postfix, exchange

## Format email

- Di definisikan oleh RFC 822
  - **header**  
Seperti amplop, berisi informasi tentang alamat pengirim dan yang dituju.
  - **body**  
Isi dari surat. Dipisahkan dari header dengan sebuah baris kosong.

## Contoh email

### ■ header - *body*

**From:** Budi Rahardjo <budi@cert.or.id>  
**To:** br@paume.itb.ac.id  
**Subject:** Kelas EL776 hari ini

*Kelas hari ini dibatalkan dan akan  
digantikan pada hari lain.*

*-- budi*

*--*

Email security

-5-



```
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 isl-55.antd.nist.gov (isl-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 isl-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-Mailer: Microsoft Outlook Express 5.50.4133.2400
Sender: owner-ietf-provreg@cafax.se
Precedence: bulk
```

Email security

-6-



## Bagaimana dengan berkas biner?

- Berkas biner (misalnya dokumen yang dihasilkan oleh wordprocessor) diubah dalam bentuk teks baru dikirimkan
  - uuencode/uuencode, base64
  - Dalam bentuk attachment
  - Standar MIME. RFC?

Email security

-7-



## Penyadapan email - confidentiality problem

- Email seperti kartu pos (postcard) yang dapat dibaca oleh siapa saja. Terbuka.
- Email dikirimkan oleh MTA ke “kantor pos” terdekat untuk diteruskan ke “kantor pos” berikutnya. Hopping. Sampai akhirnya di tujuan.
- Potensi penyadapan dapat terjadi di setiap titik yang dilalui.

Email security

-8-



## Proteksi terhadap penyadapan

- Menggunakan enkripsi untuk mengacak isi surat
- Contoh proteksi: PGP, GnuPG, PEM

## Email palsu

- Mudah membuat email palsu dengan membuat header sesuka anda.
- Email palsu ini kemudian dikirimkan via MTA atau langsung via SMTP
- Tapi, aktivitas tercatat di server dalam berkas log

## Email Palsu

Isi berkas "email-palsu.txt"

To: [siapasaja@dimanasaja.com](mailto:siapasaja@dimanasaja.com)

From: saya@hotmail.com

Subject: email palsu

Saya akan coba kirim email palsu. Perhatikan header dari email ini.

```
/usr/sbin/sendmail user01@training < email-palsu.txt
```

Email security

-11-



## Email via SMTP

```
Unix% telnet mailserver 25
HELO localhost
MAIL FROM: saya@hotmail.com
RCPT TO: user01
DATA
354 Enter mail, end with "." on a line by itself
To: haha@hotmail.com
From: hoho@hotmail.com
Subject: palsu

nih palsu
.

250 HAA20290 Message accepted for delivery
QUIT
```

Email security

-12-



## Proteksi: email palsu

- Lihat header untuk mengetahui asal email
- Menggunakan *digital signature*
- Namun keduanya jarang dilakukan

## Disusupi virus

- Email sering dijadikan media yang paling efektif untuk menyebarkan virus (melalui attachment)
- Isi email pada mulanya tidak diperiksa oleh firewall (karena firewall konvensional bukan pada layer aplikasi)
- Email langsung menuju pengguna yang seringkali teledor. (The weakest link)
- Email client langsung mengeksekusi program berdasarkan jenis berkas yang diterima untuk kenyamanan pengguna. Kepercayaan ini diabuse oleh virus
- Solusi:
  - Menggunakan anti virus dengan data terbaru
  - Tidak memperkenankan email client langsung menjalankan aplikasi
  - Melakukan pemeriksaan virus di level mail server

## Spamming

- Mengirim satu email ke banyak orang
- Biasanya digunakan untuk melakukan promosi (MLM, jualan)
  - Cost untuk mengirim email sangat murah
- Tidak bisa terfilter oleh anti-virus
- Asal kata “spam” dari skit Monty Python
  - Kemudian digunakan untuk menjual layanan greencard

Email security

-15-



## Proteksi Terhadap Spam

- Proteksi:
  - MTA dipasang proteksi terhadap spamming
    - » Dengan keyword dan karakteristik khusus
    - » Dengan statistik, Bayesian. Tapi email diubah secara dinamik dan mengandung huruf / karakter yang mengacaukan statistik
    - » Tools: spamassasin, spamd
  - Jumlah sangat banyak sehingga mail server kewalahan
  - Masih merupakan masalah besar
  - CAUCE.org – (Coalition Against Unsolicited Commercial Email)

Email security

-16-



## Mailbomb

- Mengirim banyak email ke satu orang
- Proteksi:
  - membatasi ukuran email,
  - quota disk (di direktori spool),
  - menggunakan filter khusus yang mendeteksi duplikasi isi (content) email

## Contoh Skrip Mailbomb

```
#!/usr/local/bin/perl
#
for ($i=0; $i < 10 ; $i++) {
    system("/usr/sbin/sendmail
target@somedomain.com < junkmail.txt");
}
```

## Mail relay

- Menggunakan server orang lain untuk mengirimkan email
- Akibat:
  - Bandwidth orang lain (pemilik server yang dapat di-relay) terpakai untuk mengirim email tersebut (yang biasanya jumlahnya sangat banyak)
  - Mengelabui penerima email dengan alamat palsu
  - Kena marah (dan *terfilter*) karena server kita digunakan untuk melakukan spamming

## Mail Relay [2]

- Proteksi
  - Mail Abuse Prevention System  
<http://mail-abuse.org/>
  - ORBZ – Open Relay Blackhole Zone  
<http://www.orbz.org/>
  - ORDB – Open Relay Database  
<http://www.ordb.org/>
  - RBL-type services  
<http://www.ling.helsinki.fi/users/reriksso/rbl/rbl.html>
  - SPF

## Penutup

- Email merupakan aplikasi yang paling penting
  - Mail server down, bikin masalah
- Ada banyak masalah yang terkait dengan security & reliability dari sistem email
- Masalah terbesar saat ini adalah spam dan virus