



TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 10 – Keamanan E-mail



Menu

- Komponenten Email
- Email Spoofing
- PGP (Pretty Good Privacy)
- Spamming
- Mail Bombing
- Naïve Bayesian



E-Mail

- Pesan surat digital yang dapat dikirim secara instan, komposisinya mirip dengan surat di dunia nyata.
- Header berisi nama, dan alamat tujuan, serta pengirimnya
- Body berisi isi surat



E-Mail Pun Bermasalah?

- Di jaman modern ini tidak ada yang aman, bahkan e-mail saja bisa dijadikan alat untuk menyerang target lawan, bahkan mencuri data yang penting.
- Berbagai macam serangan dapat dilakukan melalui e-mail, salah satunya adalah spoofing.

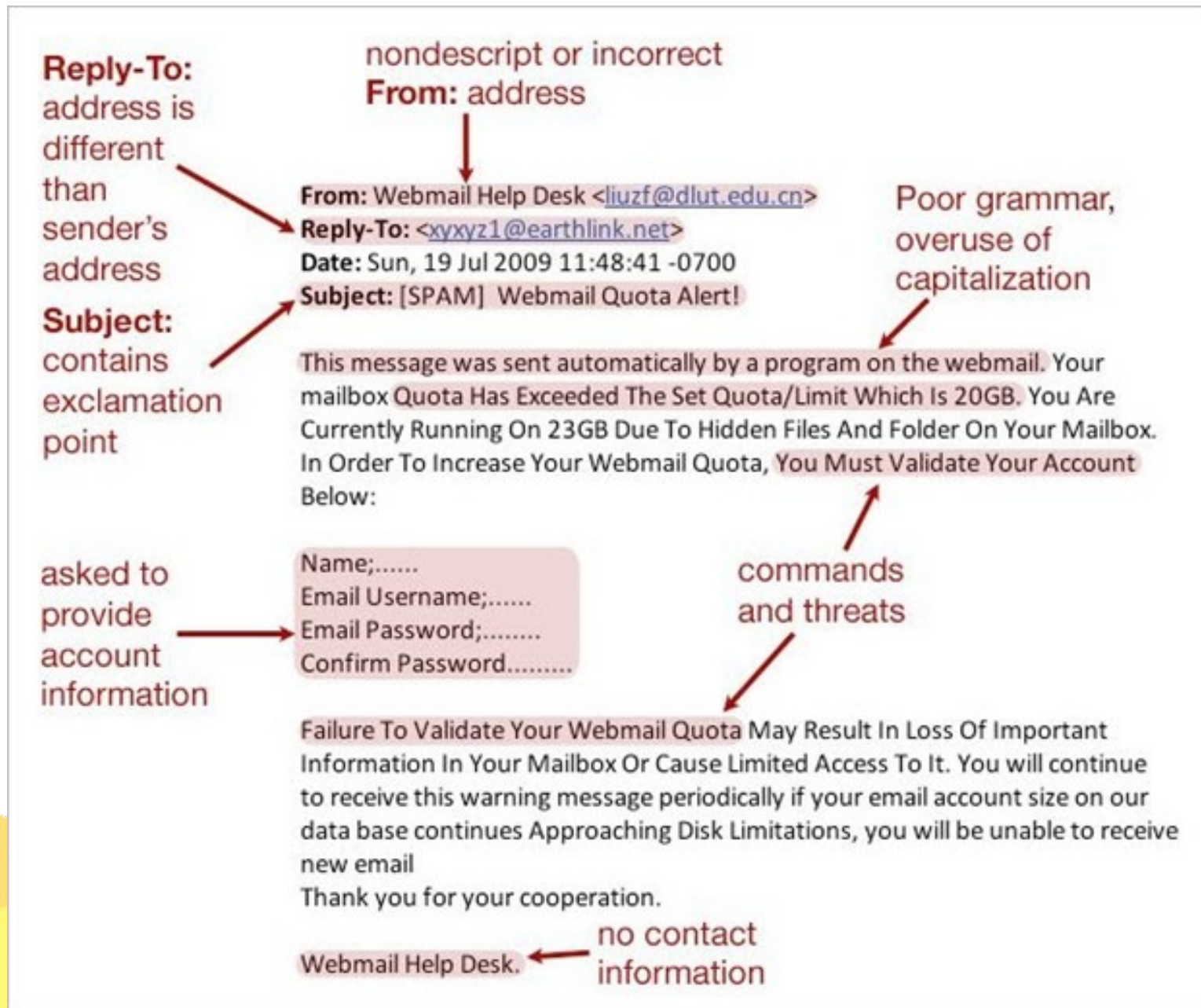


E-Mail Spoofing

- Email yang berupa spam atau virus umumnya dikirim menggunakan alamat email pengirim palsu (spoofing address).
- Email yang terlihat seolah-olah berasal dari alamat email orang lain. Hal ini bertujuan menyembunyikan identitas pengirim dan agar lolos dari filter pada software email



Contoh



Masalah Kerahasiaan

- 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.



Solusi nya?

- PGP (***pretty good privacy***) enkripsi dengan kunci asimetrik pada metode RSA
- PGP Dekstop
- Gunakan One Use Mail



PGP Online Encrypt Decrypt

Encrypt Your PGP Message

Please paste the Public PGP Key in here

PGP Public Key

Memerlukan Kunci Publik PGP, yang dapat dibuat hanya dengan nama dan e-mail saja.



Membuat Kunci PGP

- Bisa secara online, atau menggunakan tool
 - <https://pgpkeygen.com>
 - GNU Privacy Assistant (Linux)
 - GPG4Win



Menggunakan Klien untuk Privasi

- Klien E-Mail Thunderbird dengan Enigmail akan mengirimkan e-mail yang aman dengan PGP yang sudah dibuat.
- Thunderbird bisa didownload secara gratis di internet.



Contoh

From Me <maulanahirzan@yandex.com> ☆
Subject **Test PGP**
To Me <maulanahirzan@gmail.com> ★

PGP Test

Jika dilihat Source

To: maulanahirzan@gmail.com
From: "Alauddin Maulana Hirzan (Work)" <maulanahirzan@yandex.com>
Subject: Test PGP
Openpgp: preference=signencrypt
Autocrypt: addr=maulanahirzan@yandex.com; keydata=
xsBNBFvsE3oBCADObVy8BBCpOLlsCczl99256Plh5h6gxaX+xyd/r63qPfBMFdJp8nNaaW/G
YLdIs0+DVELAjEsow8TlvxYHxLV+LK53DXB0vWYLiPDpm2umQCveuZ8T9o1sFrtyB7lSpJjl
qQebyglfzxb0BnAngelWUaXLH0EsuEFw0XCinNnR0UGg3eRxr3yYA6sVcpZWfr6RS7dVZwUe
5XIlJl/Om9MLK1lxV3Tcvu/oAaBiX38jl68cI3WwBA0c5BdxYqj0h7i/YTPdwG6yTL2H1/O
ojZ9nWHA1K8XwLb9RcbgV0cWBBKGzRxvv/PU+V0a2D2raVa+lsr0jKI1pMMk1ZVSKIERABEB
AAHNMkFsYXVvkZgluIE1hdWxhbmEgSGlyemFuIDxtYXVsYW5haGlyemFuQHlhbmlleC5jb20+
wsB5BBMBCAAjBQJb7BN6AhsDBwsJCAcDAgEGFQgCCQoLBBYCAwECHgECF4AACgkQceCER9Jh
URD4yQgAl65a6gY6+MPVFUz8039r3AEcnV3Yaab/oa1qj0EbrvAyCnwTWg+SZYyS0dWrr/hi
GEagXob+eRJWmoBJFMHJOexys8Mx7jy6VAvpMHCcl/6clGuso42bfYI66ctGsumrHXwRSpWb
VEZ0wQ3xBzUqMTZD2fJBZvLLMN7eg2JL/Di2QUiJXVxA7WfkIk4pgw0oiiIphlR3Ux+a5RnJ
FuVqvLfNYUdM/TZ2UfV102uDmFJCLZhjwRwdtjJni+y0An4QZyA4gUqPmbpbFjgz3+OIyNjX
0a7b6i75s5e3zSV4g72U51SULvYF4fayXo+pyaNuLAYZ+D2+uVNL3Thm0VvcLs7ATQRb7BN6
AQgA5+J3fjdJB2+RvEJHx4dFF4G5cMkJh0QzX8+eazQZeokOKIa/cDR+zjodBP+Dg6DJIjaC
LBcQwjb0A1XQ08KW//jLX2j4X8fyY9iB08ygYZT9E0ztGjuEV79v9yUllTnnMdPS0XxlDRFh
UT2QQLel0Qahea9wA6S8+S5/D/6hZr2NFK+ISrHIaBU600q5SHixewEqpbJmltw8l0hdUS/W
2FraJXOSIPCSdmfWpWDgNxauee/3xnLPS26Aq4XndHoyzsD3mUMBT0QxtITRrSsX3oXho7ce
YF0h4V51aJw8i5K/c/pq57Ky13LP+d4E0nKYc34VWRNQFmfrI+4ZNcAzGwARAQABwsBfBBgB
CAAJBQJb7BN6AhsMAAoJEHHghEfSYVEQG18H+wQuvJmchcKo6lmnzcMfw4rGRumHqdGLlkxj
83uhuZSC7J30CAAdYM005qQ2L4PRRFbsNhjqYlztMQ3kDRePSxVypqiMAktgGUWe6ulttrmp6h
q0YmETAhHIB+OD/YgIAjk0NmduIopFokQqaD30c982MhNMRpXxJsZyrGjg8WG9BH0Vnw1Noz
Fg+s02AGcvPjybJvK20YzgRAteVrkBj+p0obfl8amx66WFld85szmgITxprMD8G0DmTF49tY
Q0lztSlnTAfjRTkCmomJIdS119swXfn+MpGtFwuB2wORfyKslL34Yy7gmORYi19u7CGfDSl
9NvJpR21/semvJDTbo=

E-Mail Spamming

- E-mail yang tidak diinginkan yang masuk ke inbox.
- Namun dalam penerapannya terkadang e-mail yang diharapkan pun masuk kategori Spam
- Contoh: E-Mail verifikasi
- Hal ini disebabkan oleh kita yang suka melakukan pendaftaran web tanpa kenal keamanannya




Contoh Spam

- E-mail Verifikasi
- E-mail Iklan
- E-mail MLM
- E-mail penipuan hadiah



Contoh

Re: How Are You Today .  Spam x



Cpt. Kate Lee <www.@ion.ocn.ne.jp>



Sun, Oct 28, 2:23 AM



Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam



I am indeed glad to be in contact with you even though this medium of communication (internet) has been grossly abused by criminal minded people making it difficult for people with genuine intention to correspond and exchange views without skepticism.

I am Cpt Kate Lee, an Army Nurse attached to the U.S. Army corps of engineers in Syria.I have decided that I seek your assistance in a matter that requires your urgent attention.I want you to assist me to receive some funds. Kindly e-mail me your contact information Which Should include Full name, address and phone number,occupation, so I can tell you what you need to do and also give you more details about myself and the project.

Regards

Cpt. Kate Lee



Reply



Forward



Mengapa Spam Terjadi?

- ***Ekonomi Internet*** yang aneh
- Biaya untuk mengirimkan 1 email sama dengan 1000 email, atau bahkan 1 juta email
- Sangat murah untuk mengirimkan *unsolicited emails*
- Kuota 1GB bisa mengirimkan jutaan e-mail yang hanya berukuran tidak lebih dari 100kb (tanpa attachment)



Efek Sampling

- Menghabiskan / memboroskan
- Disk (email storage)
- Jaringan
- **Waktu dan produktivitas kerja pengguna**
- Pengguna tertipu (phising)



Kesulitan Penanganan Spam

- Variasi Subjet
- Isi Konten yang berbeda-beda
- Sistem AI yang belum mumpuni untuk mendeteksi SPAM
- Kesengajaan penyedia layanan E-mail



Naive Bayesian

- Digunakanlah Naive Bayesian untuk mengatasi spam.
- Merupakan metode terbaru yang digunakan untuk mendeteksi *spam mail*. Algoritma ini memanfaatkan teori probabilitas yang dikemukakan oleh ilmuwan Inggris Thomas Bayes, yaitu memprediksi probabilitas di masa depan berdasarkan pengalaman di masa sebelumnya



Kelemahan

- Mail server berat
- Spammer menyisipkan kata-kata atau huruf yang tidak teratur guna mengacaukan statistik
- Spammer menggunakan gambar (image) untuk menyampaikan pesannya



Tool Anti Spam

- Spamassassin & spamd



MailBomb

- Mirip PING FLOOD tapi untuk e-mail saja
- Mengirim banyak email ke satu orang
- Proteksi: membatasi ukuran email, quota disk, menggunakan filter khusus yang dapat mendeteksi duplikasi isi content



Contoh Skrip

```
#!/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 terpakai untuk mengirim email tersebut (yang biasanya banyak)
- Mengelabui penerima email

