Email Security

Girindro Pringgo Digdo

Whoami

- Seven years in Information Security
- Lecturer
- Author

Agenda

- Introduction
- Email Format
- Email Problems

Introduction

- MUA (Mail User Agent)
  - Netscape, outlook, thunderbird, etc
- MTA (Mail Transfer Agent) → Mailer
  - Postfix, qmail, sendmail, etc

Email Format

Accroding to RFC 822 → 2822

- Header
- Body

From: Girin Digdo <girindigdo@gmail.com>

To: mahasiswa@unikom.ac.id

Subject: Final Task KSI

Final Task can be seen in online course. Thank You.

-- Girin Digdo

Email Format

```
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)
```

Email Format

```
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 Problem

- Tapping
- Fake Email
- Virus Infiltration
- Spam
- Mail Bomb
- Mail Relay

Email Problem: Tapping

- No encryption in SMTP Port 25

Email Problem: Tapping

How to prevent from Tapping?

Encryption.

Email Problem: Fake Email

Post Office Analogy:

Everyone can send letter with fake address without rechecked

Email Problem: Fake Email

Peringatan!!

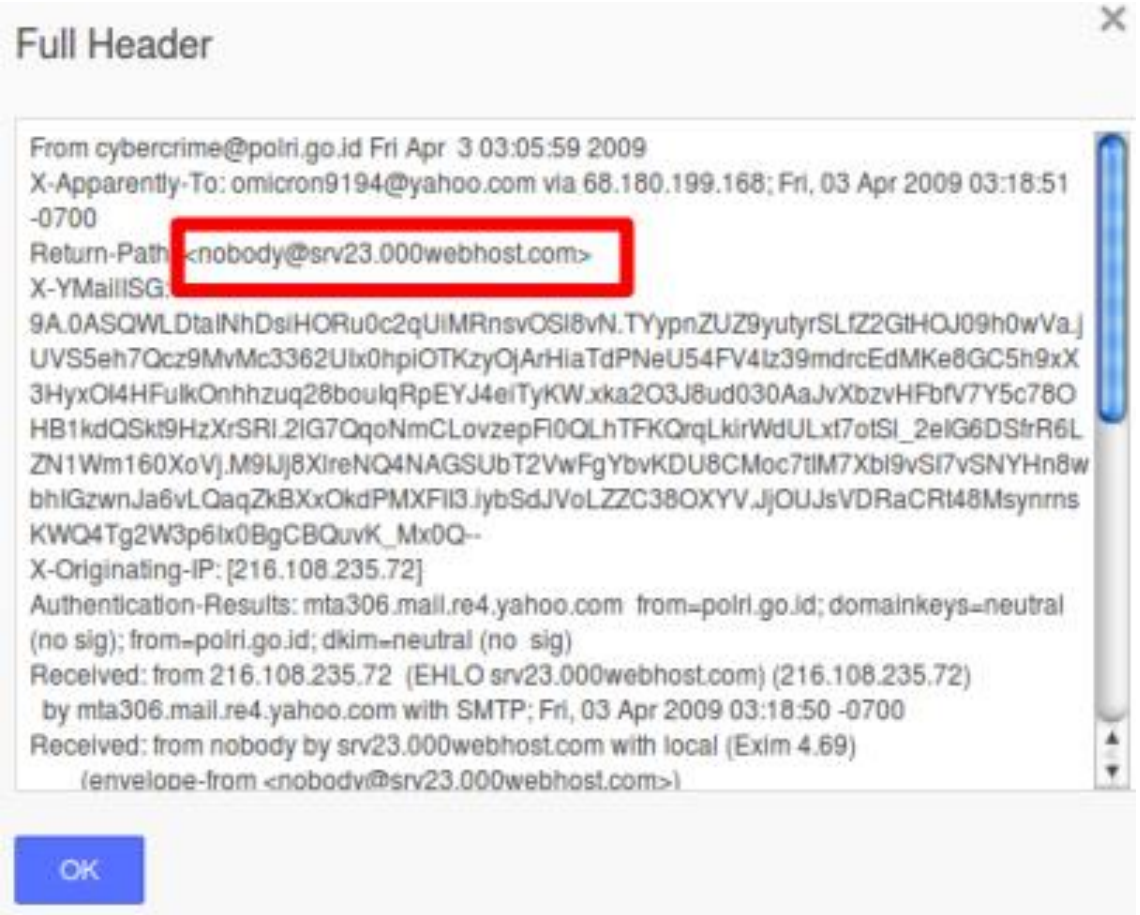
Fri, Apr 3, 2009 at 5:18 PM

From cybercrime@polri.go.id

To omicron9194@yahoo.com

Kami mendapat kabar bahwa anda adalah salah seorang hcker yang kami cari akrena telah banyak me-hack banyak situs, jika anda merasa tidak bersalah, silahkan kirim email berisi pembelaan ke email staff kami..
Anda juga merupakan sekelompok orang yang sedang kami cari salah satu teman anda yang mungkin anda kenal yaitu ciebal, vYc0d, dkk..
Mohon jujur kepada kami, adapa yang sering anda dan teman anda perbuat!!
Kami tunggu jawaban selama 3 hari..
Terima Kasih..

Email Problem: Fake Email



Email Problem: Fake Email

How to prevent from Fake Email?

- See the Header
- Use Digital Signature

Email Problem: Virus Infiltration

- Social Engineering
  - Nilai-UAS.pdf
  - Creditnumber.xlsx
  - etc

Email Problem: Spam

- Unsolicited email
- Spam != Virus

Email Problem: Mail Bomb

- Send emails with the number of lots
- Mailbox become full of emails
- Easy to do

Email Problem: Mail Bomb

How to prevent from Mail Bomb?

- Limit the quota

Email Problem: Mail Relay

- A Mail Relay is a server, normally on the Internet, which can forward mail from its users to other mail servers.
- Usually done by spammers