Simple Mail Transfer Protocol, Spam und IM2000

Vortrag von Ingo Blechschmidt

am 1. Dezember 2004

Gliederung

- Design
- Typischer Ablauf
- Spam, Spam-Abwehr, Spam-Verhinderung
- IM2000 als neues Mail-Protokoll

Design

- Eindeutige Identifizierung eines Nutzers durch `user@host`
- Leitung von RFC 822-Mails über viele Server: Client $\rightarrow$ Server $\rightarrow \ldots \rightarrow$ Server $\rightarrow$ Client
- „Store and forward“
- ASCII-basiertes Protokoll $\Rightarrow$ Eignung zum manuellen Testen mit Telnet

Typischer Ablauf

- Verbindung des Clients zu seinem SMTP-Server
- Übermittlung des Envelope-Headers (`From`, `To`)
- Akzeptanz?

  Ja $\Rightarrow$ Übermittlung der Mail
  Nein $\Rightarrow$ Sofortiges Schließen der Verbindung

- Übernahme der weiteren Zustellung durch den Server

MX-Records

- Erhalt einer Mail an `iblech@web.de`
- Wunsch einer Verbindung zu `web.de:25`
- Problem: Kein Lauschen eines SMTP-Daemons auf `web.de`

MX-Records

- Erhalt einer Mail an `iblech@web.de`
- Wunsch einer Verbindung zu `web.de:25`
- Problem: Kein Lauschen eines SMTP-Daemons auf `web.de`
- Lösung: Frage nach den MX-Records von `web.de`:

```
$ dig +noall +answer web.de MX
web.de. 32066 IN MX 110 mx-ha02.web.de.
web.de. 32066 IN MX 100 mx-ha01.web.de.
```

- Verbindung zu einem MX-Server

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
Trying 217.72.192.149...
Connected to mx-ha01.web.de.
Escape character is '^]'.
220 mx27.web.de ESMTP WEB.DE
```

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
220 mx27.web.de ESMTP WEB.DE
```

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
220 mx27.web.de ESMTP WEB.DE
EHLO localhost
250-mx27.web.de Hello localhost [80.81.9.175]
250-SIZE 70254592
250-PIPELINING
250 HELP
```

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
220 mx27.web.de ESMTP WEB.DE
EHLO localhost
250 mx27.web.de Hello localhost [80.81.9.175]
```

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
220 mx27.web.de ESMTP WEB.DE
EHLO localhost
250 mx27.web.de Hello localhost [80.81.9.175]
MAIL FROM: <abc@def.de>
250 <abc@def.de> is syntactically correct
```

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
220 mx27.web.de ESMTP WEB.DE
EHLO localhost
250 mx27.web.de Hello localhost [80.81.9.175]
MAIL FROM: <abc@def.de>
250 <abc@def.de> is syntactically correct
RCPT TO: <iblech@web.de>
250 <iblech@web.de> verified
```

SMTP-Sitzung

```
$ telnet mx-ha01.web.de 25
220 mx27.web.de ESMTP WEB.DE
EHLO localhost
250 mx27.web.de Hello localhost [80.81.9.175]
MAIL FROM: <abc@def.de>
250 <abc@def.de> is syntactically correct
RCPT TO: <iblech@web.de>
250 <iblech@web.de> verified
DATA
354-Enter message, ending with "." on
354 a line by itself
```

SMTP-Sitzung

```
DATA
354-Enter message, ending with "." on
354 a line by itself
```

SMTP-Sitzung

```
DATA
354-Enter message, ending with "." on
354 a line by itself
From: Jemand <hallo@test.com>
To: You <hi@pi++>
Subject: Hallo

Hi das ist eine gefälschte Mail.
cu
.
```

SMTP-Sitzung

```
DATA
354-Enter message, ending with "." on
354 a line by itself
...
.
250 OK id=1CTJrs-0005ZP-00
QUIT
221 mx27.web.de closing connection
Connection closed by foreign host.
$
```

Probleme bei tradit. SMTP

- Extrem leichte Fälschbarkeit des Absenders
- Möglichkeit der Angabe mehrerer Empfänger
  $\Rightarrow$ Versand von Massenmails simpel
- Leichte Kompromittierbarkeit
  von Windows-Clients $\Rightarrow$
  Viele freie Ressourcen für Spammer
- Nur wie beheben?

Client-seitige Abwehr

- SpamAssassin:
  Wenig False-Negatives,
  aber starres Regelwerk
- DSPAM:
  Lange Trainingszeit,
  dann aber sehr wenig Fehleinschätzungen
- Problem: Z.T. großer Verbrauch an CPU-Zeit

Server-seitige Abwehr

- Einsatz der Client-Tools direkt auf den Servern
- Server-Callback
- Greylisting z.B. durch SPONTS
- Sender Policy Framework, Microsoft Sender ID

Server-seitige Abwehr

- Einsatz der Client-Tools direkt auf den Servern
- Server-Callback:
  Validierung des Absenders beim für die Absenderadresse zuständigen MX-Server
- Greylisting z.B. durch SPONTS
- Sender Policy Framework, Microsoft Sender ID

Greylisting

- „Sorry, versuch’s bitte später nochmal.“
- Merken der Absender/Empfänger/Server-Kombination
- Beim zweiten Versuch: Mail akzeptieren
- Vorteil: Nachhaltig weniger Spam
  Problem: Anpassung der Spammer

Sender Policy Framework

- Vergleich eines TXT-Records der Absenderdomain mit dem Hostnamen des einliefernden Servers:

```
$ dig +noall +answer gmx.de TXT
gmx.de. 300 IN TXT \
    "v=spf1 ip4:213.165.64.0/23 ?all"
```

- Übereinstimmung?

  Ja ⇒ Annahme der Mail
  Nein ⇒ Annahmeverweigerung

Spam-Verhinderung

- Durchforstung des Internets nach E-Mail-Adressen durch Robots $\Rightarrow$

  Ziel: Erschwerung des automatischen Adressensammelns

- Angabe von Adressen nur in veränderter Form...:
  - `iblech (at) web.de`
  - `iblechNOSPAM@web.de`
- ...oder als Bilder

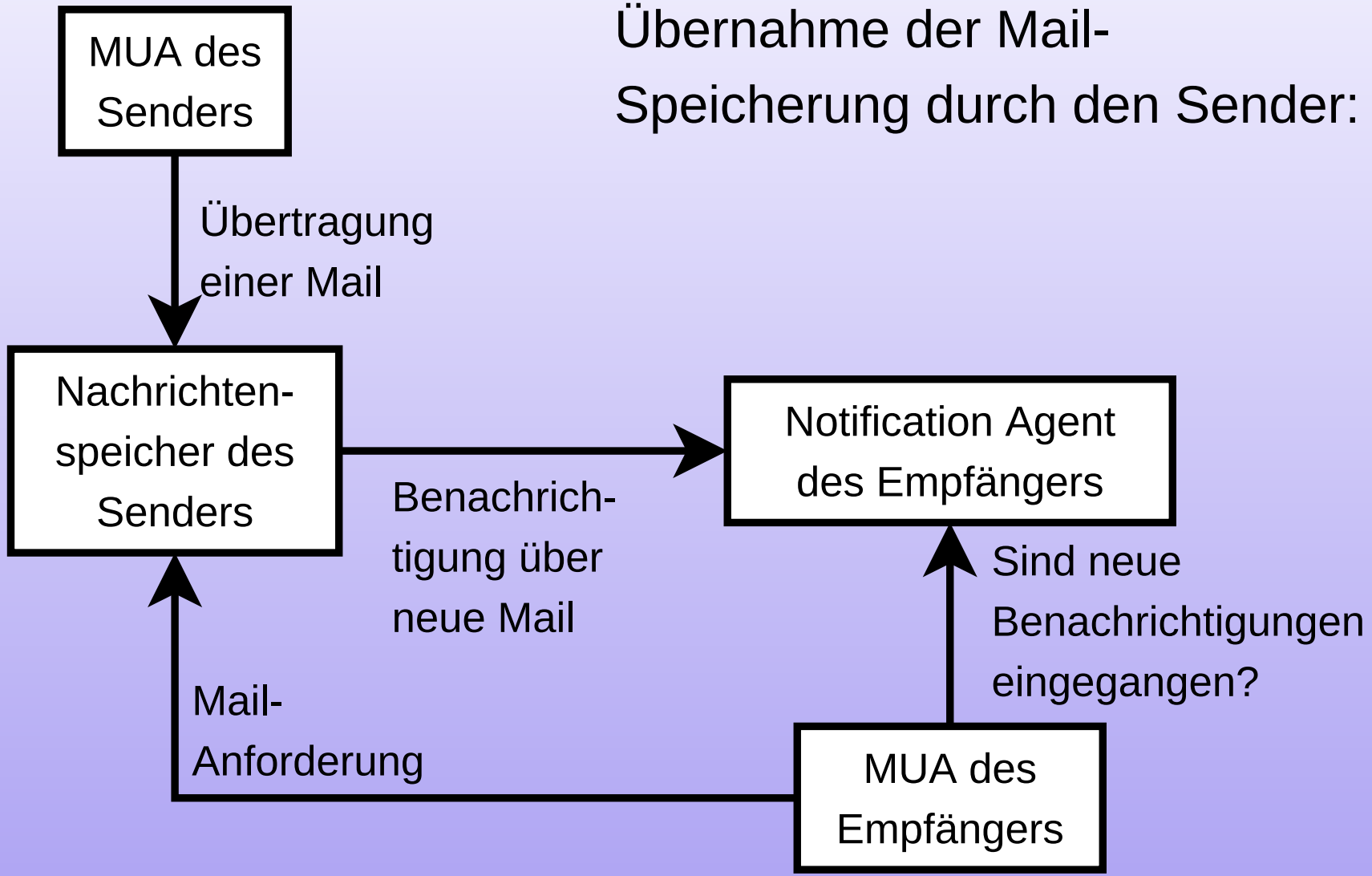
Spam-Verhinderung

- Durchforstung des Internets nach E-Mail-Adressen durch Robots $\Rightarrow$

  Ziel: Erschwerung des automatischen Adressensammelns
- Angabe von Adressen nur in veränderter Form...
- ...oder als Bilder
- Problem: Einmaliges Vergessen $\Rightarrow$ Eintrag seiner Mail-Adresse in Sendelisten

Internet Mail 2000

Übernahme der Mail-Speicherung durch den Sender:



IM2000: Vorteile

- Kein Problem: Ausfälle des Servers des Empfängers
- Keine Bounces
- Einfache Realisierung von Mailinglisten
- Übertragung nur vom Client ausgewählter Mails
- Sender für Mail-Speicherung verantwortlich
  $\Rightarrow$ Spam-Versand ressourcenverbrauchender

IM2000: Offene Fragen

- Wie erfolgt die Benachrichtigung der Empfänger?
- Wie sollen Mails heruntergeladen werden?
- Welches Format sollen die Mails und die Benachrichtigungen haben?
- Ist es vertretbar, dass der Sender erfährt, wann der Empfänger seine Mails herunterlädt/liest?

Siehe auch

- Hitchhiker's Guide to the Internet
  `http://linide.sf.net/theguide2/`
- Linux-Magazin 09/2004
- `http://cr.yp.to/smtp.html`
- `http://cr.yp.to/im2000.html`

Fragen?