Workshop E-Mail

Reisestationen elektronischer Post

Frank Becker <fb@alien8.de>

Linux-Info-Tag Dresden 2004

2004-10-30

Agenda

- Was ist E-Mail
- How Hackers do it...
- Mail Transfer Agent (MTA)
- Mail Delivery Agent (MDA)
- Mail User Agent
- Spam
- Archivierung

Was ist E-Mail?

Was ist E-Mail?

- Mein erstes Ma(i)l?
- Store and Forward System
  - Ich bestimme, wann ich E-Mails lese!
  - z. B. wie Anrufbeantworter
- gut archivierbar (speichern, indizieren, suchen)

Schreibregeln aka Netiquette

- TOFU
- zu viel Quote
- Quoting von Signaturen
  - „-- “
- Wer wird zitiert?
- keine HTML E-Mails
- Header ganz lassen!
- file:///home/becke/workfolder/computer/lit/2004/w

How Hackers do it...

SMTP RFCs

http://www.networksorcery.com/enp/protocol/smtp.htm

Hinter den Kulissen, SMTP

```
maul:~# host -t mx skyhub.de
skyhub.de mail is handled by 10 mail.skyhub.de.
skyhub.de mail is handled by 100 robot.first-ns.de.

maul:~# nc mail.skyhub.de 25
220 mail.skyhub.de ESMTP ZX Spectrum (128k)
vrfy fb@skyhub.de
252 fb@skyhub.de
vrfy fb@mail.skyhub.de
450 <fb@mail.skyhub.de>: Recipient address rejected: User unknown in
local recipient table
quit
221 Bye
```

vrfy

SMTP Kommandos (Auswahl)

• HELO <FQDN>	Klient stellt sich vor
• EHLO <FQND>	Klient stellt sich vor + Frage nach ESMTP-Befehle
• VRFY <Adr>	Adresse auf Server überprüfen
• MAIL FROM: <Adr>	Envelope-Adresse (Absender-Adresse)
• RCPT TO: <Adr>	Empfängeradresse
• DATA	es folgt der E-Mail Inhalt
• AUTH <Methode>	Authentifizierung
• STARTSSL	SSL-Verbindung aufbauen
• QUIT	Und Tschüß

SMTP

```
maul:~# nc mail.skyhub.de 25
220 mail.skyhub.de ESMTP ZX Spectrum (128k)
HELO maul.localhost
250 mail.skyhub.de
MAIL FROM:<fb@alien8.de>
250 Ok
RCPT TO:<fb@skyhub.de>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
To: Frank Becker <fb@skyhub.de>
From: Frank Becker <fb@alien8.de>
Subject: SMTP Handarbyte

Na was wohl, etwas testen ;)

cu
.
250 Ok: queued as 9A2E9D0012
quit
221 Bye
```

Hinter den Kulissen, SMTP

```
-[~:] swaks -t fb@alien8.de -f
fb@alien8.de -s mail.skyhub.de
=== Trying mail.skyhub.de:25...
=== Connected to mail.skyhub.de.
<-  220 mail.skyhub.de ESMTP ZX Spect
 -> EHLO maul.local
<-  250-mail.skyhub.de
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250 8BITMIME
 -> MAIL FROM:<fb@alien8.de>
<-  250 Ok
 -> RCPT TO:<fb@alien8.de>
<-  250 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Thu, 14 Oct 2004 01:03:55 +0200
 -> To: fb@alien8.de
 -> From: fb@alien8.de
 -> Subject: test
 -> X-Mailer: swaks v20040404.1
 ->
 -> This is a test mailing
 ->
 -> .
<-  250 Ok: queued as 946EFD0012
 -> QUIT
<-  221 Bye
=== Connection closed by foreign host.
```

SMTP 2, No relaying

```
-[~:] swaks -t Frank.Becker@web.de -f fb@alien8.de -s mail.skyhub.de
=== Trying mail.skyhub.de:25...
=== Connected to mail.skyhub.de.
<-  220 mail.skyhub.de ESMTP ZX Spectrum (128k)
 -> EHLO maul.local
<-  250-mail.skyhub.de
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250 8BITMIME
 -> MAIL FROM:<fb@alien8.de>
<-  250 Ok
 -> RCPT TO:<Frank.Becker@web.de>
<** 454 <Frank.Becker@web.de>: Relay access denied
 -> QUIT
<-  221 Bye
```

swaks

SMTP SSL

```
-[~:] swaks -tls -t Frank.Becker@web.de \
-f fb@alien8.de -s mail.skyhub.de
=== Trying mail.skyhub.de:25...
=== Connected to mail.skyhub.de.
<-  220 mail.skyhub.de ESMTP ZX Spectrum
(128k)
 -> EHLO maul.local
<-  250-mail.skyhub.de
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250 8BITMIME
 -> STARTTLS
<-  220 Ready to start TLS
=== TLS started w/ cipher DHE-RSA-AES256-SHA
 ~> EHLO maul.local
<~  250-mail.skyhub.de
<~  250-PIPELINING
<~  250-SIZE 10240000
<~  250-VRFY
<~  250-ETRN
<~  250-AUTH PLAIN
<~  250-AUTH=PLAIN
<~  250 8BITMIME
 ~> MAIL FROM:<fb@alien8.de>
<~  250 Ok
 ~> RCPT TO:<Frank.Becker@web.de>
<~* 454 <Frank.Becker@web.de>: Relay
access denied
 ~> QUIT
<~  221 Bye
```

SMTP Mail Header

```
Return-Path: lug-dd-bounces@schlittermann.de
Received: from localhost (localhost [127.0.0.1])
        by mail.kruitzer.net (SuperMail on ZX Spectrum 128k) with ESMTP id BF9BA3B9A8
        for <fb@alien8.de>; Thu, 14 Oct 2004 23:10:39 +0200 (CEST)
Received: from mail.kruitzer.net ([127.0.0.1])
        by localhost (p15107656 [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id 03442-06 for <fb@alien8.de>;
        Thu, 14 Oct 2004 23:10:35 +0200 (CEST)
Received: from pu.schlittermann.de (pu.schlittermann.de [212.80.235.130])
        (using TLSv1 with cipher RC4-SHA (128/128 bits))
        (No client certificate requested)
        by mail.kruitzer.net (SuperMail on ZX Spectrum 128k) with ESMTP id 0FE143B9A7
        for <fb@alien8.de>; Thu, 14 Oct 2004 23:10:35 +0200 (CEST)
Received: from localhost ([127.0.0.1])
        by pu.schlittermann.de with esmtp (Exim 4.34)
        id 1CICrj-0004ec-Lc; Thu, 14 Oct 2004 23:10:27 +0200
Received: from pu.schlittermann.de ([127.0.0.1])
        by localhost (pu [127.0.0.1]) (amavisd-new, port 10024) with ESMTP
        id 11085-07; Thu, 14 Oct 2004 23:10:26 +0200 (CEST)
[...]
Received: from pu.schlittermann.de ([127.0.0.1])
        by localhost (pu [127.0.0.1]) (amavisd-new, port 10024) with ESMTP
        id 14887-02 for <lug-dd@schlittermann.de>;
        Thu, 14 Oct 2004 23:08:53 +0200 (CEST)
Received: from dell.sachsenprovider.de ([80.86.168.10])
        by pu.schlittermann.de with esmtp (Exim 4.34) id 1CICqD-0004XW-DU
        for lug-dd@schlittermann.de; Thu, 14 Oct 2004 23:08:53 +0200
Received: from A5291.a.pppool.de (A5291.a.pppool.de [213.6.82.145])
        by dell.sachsenprovider.de (dell.sachsenprovider.de) with ESMTP id
        5A9C83982E9
        for <lug-dd@schlittermann.de>; Thu, 14 Oct 2004 23:08:41 +0200 (CEST)
From: Olli Mörtel <olli@moertel.de>
To: Linux-User-Group Dresden <lug-dd@schlittermann.de>
Date: Thu, 14 Oct 2004 23:18:39 +0200
User-Agent: KMail/1.7.1
References: <200311132213.44116.fm@moertel.de>
```

Dinge zum Ausprobieren

- leere From Adresse
- @ mit % ersetzen: RCPT TO:aa%bb.com
- lokale IP des Servers, MAIL FROM:aa@192.168.1.1
- Adresse in Gänsefüßchen, MAIL FROM: “aa@192.168.1.1“

POST request via proxy server

```
POST http://localhost:25/ HTTP/1.1
Host: victim
(empty line)
HELO spammer
MAIL FROM: <[...]>
RCPT TO: <[...]>
DATA
e-mail
.
```

```
CONNECT http://localhost:25/ HTTP/1.0
HELO spammer
MAIL FROM: <[...]>
RCPT TO: <[...]>
DATA
e-mail
.
```

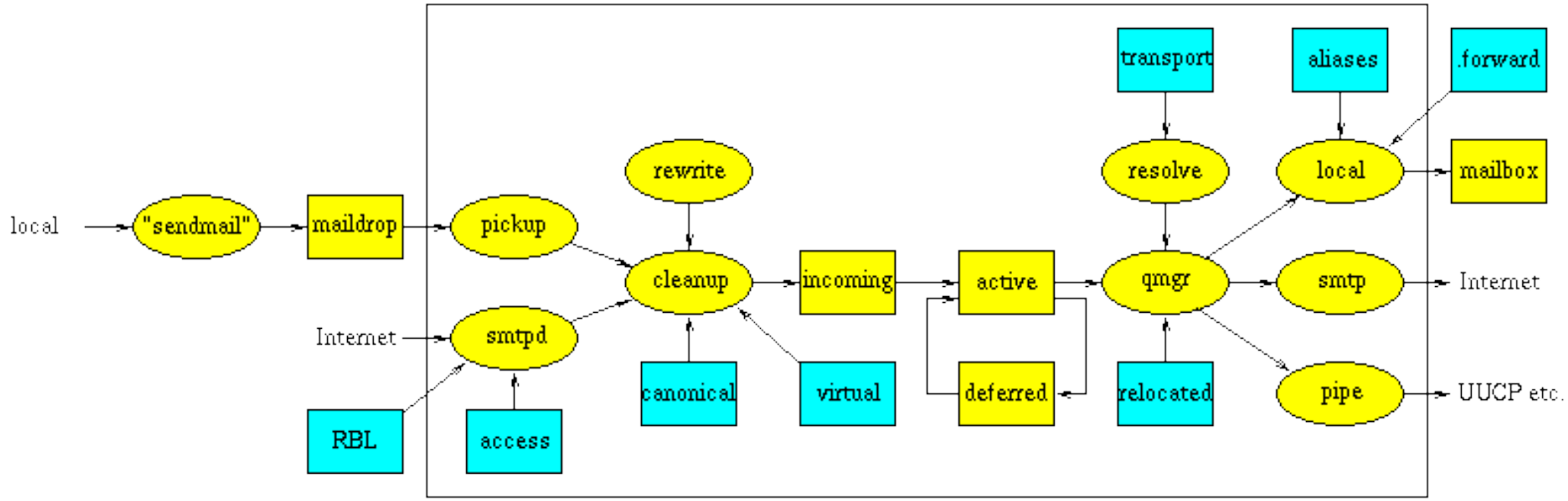
MTA

Postfix

http://www.postfix.org/ http://www.postfix.org/docs.html

- erwachsener MTA / äußerlich Sendmail-kompatibel
- einfache Konfiguration
- Einsatzgebiete:
  - lokaler MTA
  - Mailbackup (MX-Backup)
  - Relay in DMZ
  - Mailserver (SMTP-Auth, Multi-Domains ...)

Postfix: The big picture



Postfix: lokaler MTA

man 5 postconf

/etc/postfix/main.cf

myhostname = maul.alien8.de FQDN des Servers

mydomain = alien8.de muss nicht gesetzt sein

mydestination = alien8.de zuständig für Domain

mynetworks: Wer darf versenden

defer_transports = smtp Transport queue

relayhost = mail.alien8.de Weiterleitungsserver (MX-Abfrage)

smtp_use_tls = yes Verschlüsselung?

smtp_sasl_auth_enable = yes Authentifizierung?

smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd

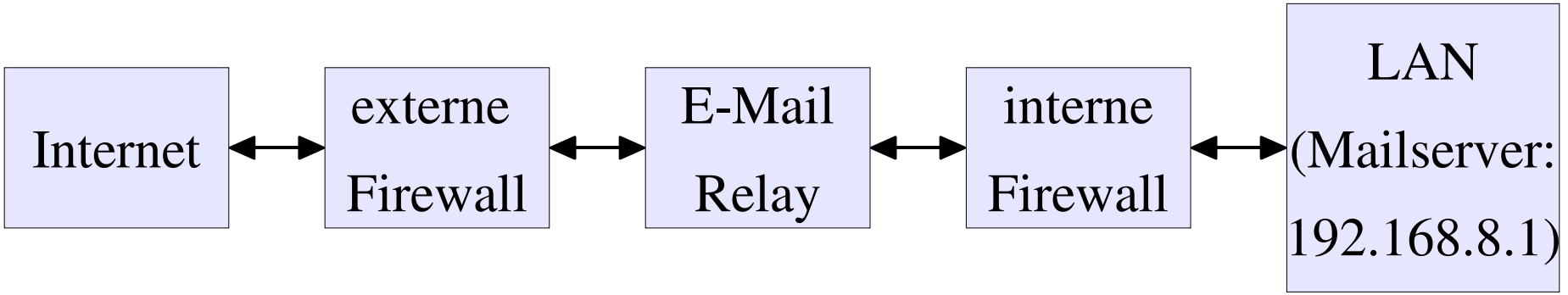
smtp_sasl_security_options = noanonymous

smtp_tls_CAfile = /etc/postfix/ca-certs/cacert.pem

Postfix: MX-Backup

- nimm E-Mail für ausgefallenen Hauptserver an
- Backup-Server kann gleichzeitig Hauptserver für andere Domain sein (Load-Sharing)
- wie lokalen MTA konfigurieren +
  - smtpd_recipient_restrictions = permit_mynetworks, **permit_mx_backup,** reject_unauth_destination
- evtl. `postsuper -r ALL`, falls sich IP des Hauptservers geändert hat

Postfix: Mail-Relay in DMZ



- interner Mailserver nicht aus Inet erreichbar
- Transport-Tabelle /etc/postfix/transport:
  alien8.de smtp:[192.168.8.1]
  - `postmap /etc/postfix/transport`
  - [] fragen A-Records ab (nicht MX-Records)

Postfix: Kommandos

- postfix flush — Warteschlange (Queue) ausliefern
- mailq — listet Warteschlange
- postconf — ändert Postfix Konfig-Parameter
- postsuper -r — Requeueing aller Mails (DNS wird neu aufgelöst)
- postsuper -d — löscht Einträge in der Mailqueue
- postcat — zeigt Inhalt einer Mail in d. Queue
- postlog — was in die Logdatei schreiben
- mailq — zeigt Inhalt der Mailqueue an

MDA

Mail Delivery Agent

- lokale Zustellung
  - /var/spool/mail/$user
  - procmail

Cyrus IMAP Server

http://asg.web.cmu.edu/cyrus/cyrus-overview-TOC.html

- IMAP und POP3-Server
- Cyrus IMAP entwickelt an der Carnegie Mellon University.
- Unterstützt SSL
- SASL-Login
- Quota Support
- jede E-Mail eine Datei
- Sieve E-Mail-Filtersprache

Serverseitige E-Mail Filter

http://asg.web.cmu.edu/cyrus/sieve/

- Sieve, einfache Scriptsprache zum filtern, RFC 3028

```
if
header :contains "List-Id" "Chaostreff Dresden"
{
fileinto "INBOX.c3d2";
stop;
}
if
anyof (header :contains "From" "tux",
header :contains "From" "daemon",
header :contains "To" "me@alien8.de")
{
fileinto "INBOX.me-folder";
addflag "\\Deleted";
keep;
notify :method "sms" :options "" :id "es kam was" :high :message "Da ist
eine E-Mail in der neuen Filterregel aufgeschlagen.";
}
```

E-Mail abholen

- übliche Protokolle
  - POP3
  - IMAP
- übliche Programme
  - getmail
  - offlineimap

Post Office Protokoll 3 am Bsp:

```
becke@p15107656:~$ nc localhost 110
+OK mail.kruitzer.net Cyrus POP3 v2.1.
IPv6-Debian-2.1.16-10 server ready
<1458821411.1098996103@mail.kruitzer.n
USER user1
+OK Name is a valid mailbox
PASS supergeheim
+OK Maildrop locked and ready
STAT
+OK 54 3288262
LIST
+OK scan listing follows
1 3073
2 2882
3 3049
4 1485718
5 2304
6 25878
```

```
NOOP
+OK
TOP 51 10
+OK Message follows
Return-Path: <cyrus@mail.kruitzer.net>
Received: from mail.kruitzer.net ([unix
socket]) by mail.kruitzer.net (Cyrus
...
Am Donnerstag, 28. Oktober 2004 19:24,
schrieb Nando:
> Also nachdem ich heute mit Christian

DELE
RETR
RSET
QUIT
```

E-Mail abholen

- fetchmail
  - zieht E-Mails von einem POP3/IMAP Server
  - liefert z. B. an procmail aus
- offlineimap
  - gleicht Mailboxen lokal und auf Server ab
  - Redundanz!

Procmail snippets

```
# Correct wrong sig-dashes, ie add a space for lines with only "--" in
# them:
# from: ^--$
# to:   ^-- $
:0 fBw
* ^--$
| sed -e 's/^--$/-- /'

# Correct wrong sig-dashes, ie add a space for lines with only "--" in them:
# from: ^--$
# to:   ^-- $
:0 fBw
* ^--$
| sed -e 's/^--$/-- /'

:0:
* ^TOc3d2
"c3d2-`date +%Y-%m`"
```

MUA

mutt

- Konsolen MUA
- macht das, was er soll
- kann fast alles
- file:///usr/share/doc/mutt/html/manual-4.html#ss4.

- Prinzip von Hooks

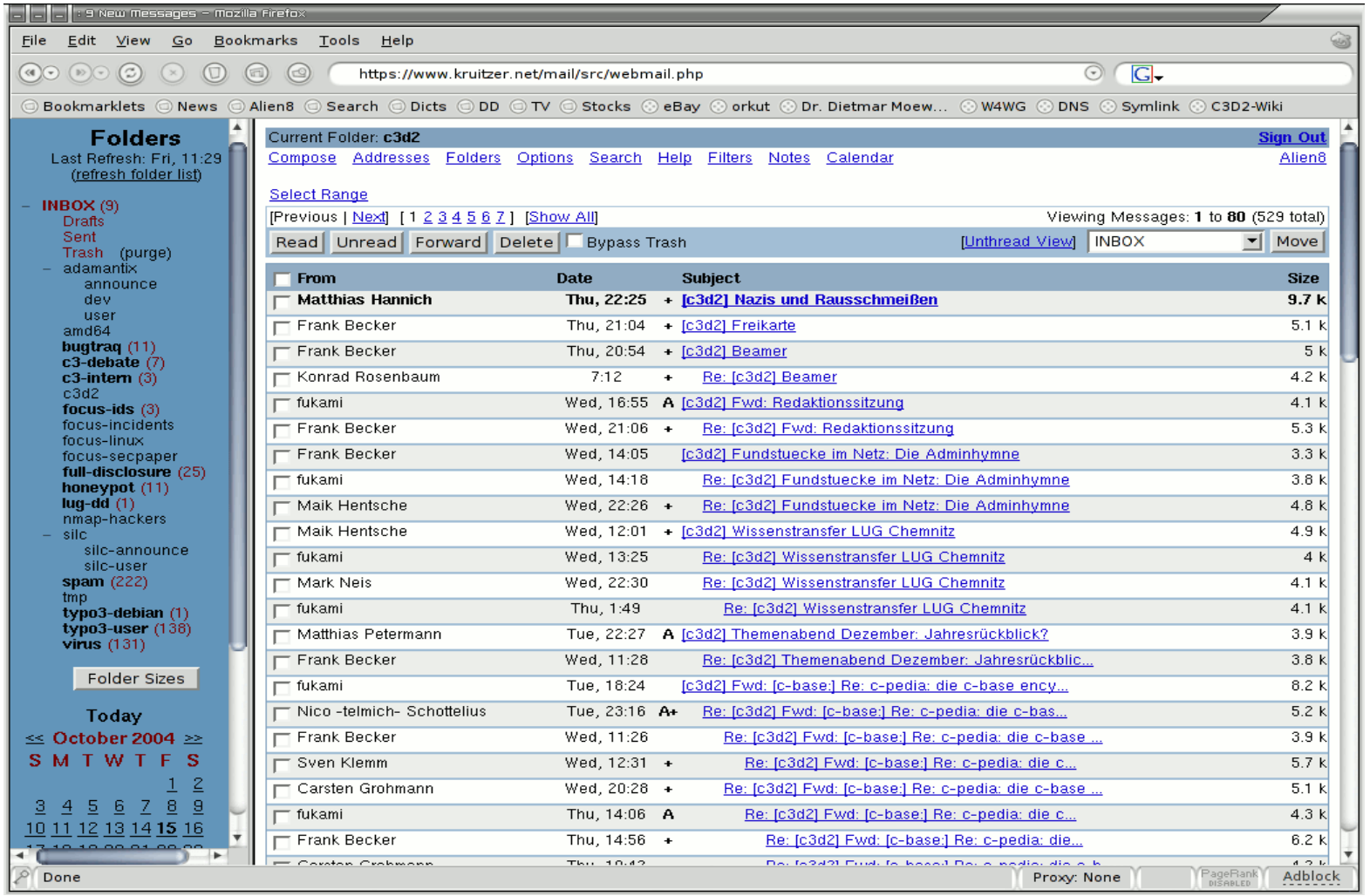
-> Demo

mutt Addons

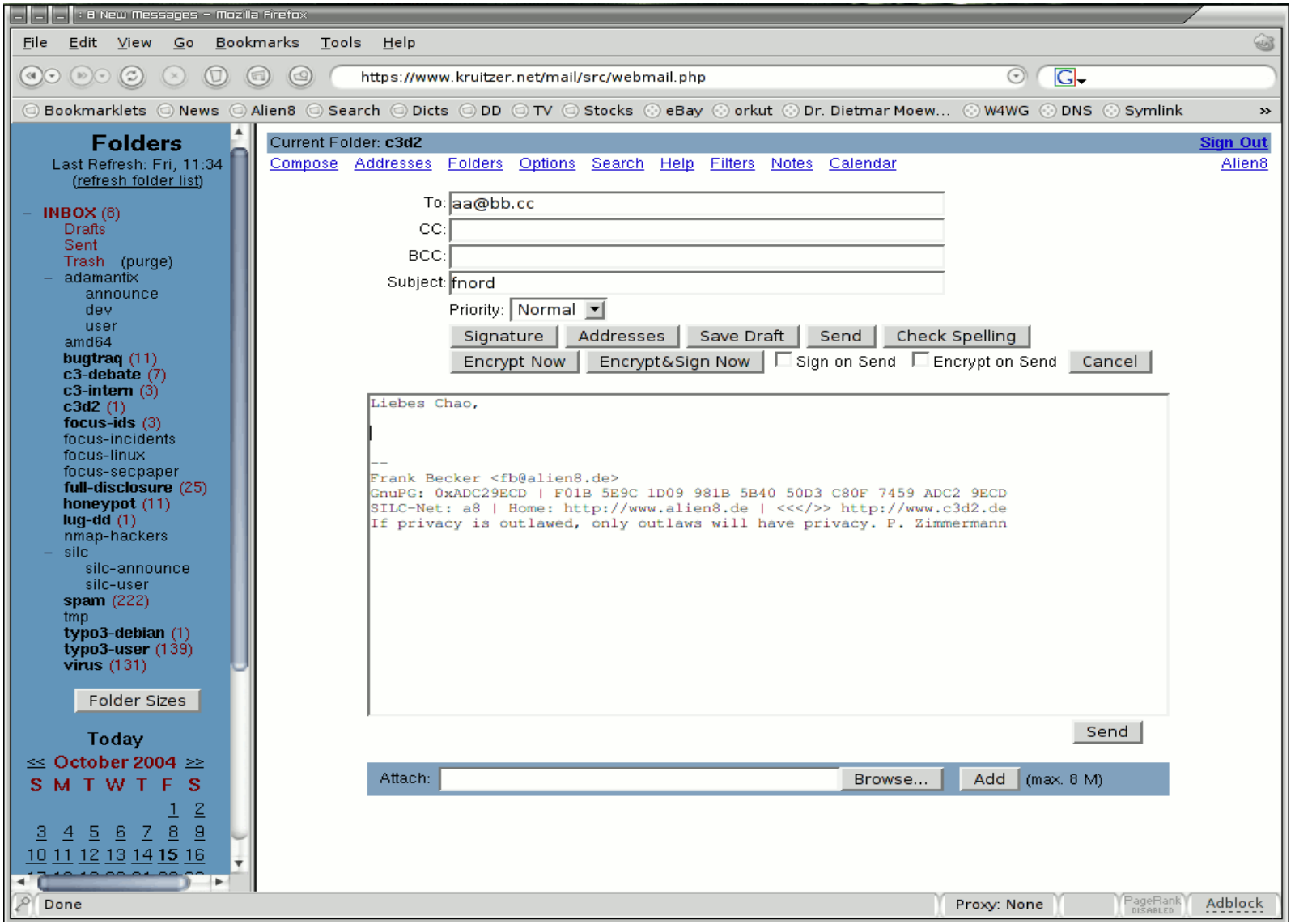
- muttprint
- t-prot
- abook
- msmtp

Web-Mailer: Squirrelmail

- The one and only!



Squirrelmail: Neue Nachricht



SPAM

Historie

- Hormel Foods
  - Shoulder pork and ham SPiced hAM
- Monty Python Serie
  - spam, spam, spam, lovely spam, wonderful spam
- RPG, flooding wurde Spam genannt
- IRC
- 1978 erster Spam durch DEC ins Arpanet (kauft DEC-20)
- 1994 erstmals im Usenet
  - Anwaltskanzlei wirbt für Green-Card

Wie wird SPAM hergestellt?

Challenge-response

- Absender bekommt „Bitte um Bestätigungsanforderung“, wenn nicht
  - Bestätigung gesendet wurde
  - E-Mail Adresse nicht bekannt ist
- für Mailinglisten gut
- sonst eher nervig

Greylisting

- Voraussetzung:
  - Spammer-Server eingeschränkte Funktionalität
- Funktion:
  - bei neuer E-Mail merkt sich der MTA:
    - IP, MAIL FROM und RCPT TO
  - Sender wird vertröstet, soll in 1h nochmal probieren (Code 450)
- geht gut, TU Chemnitz verwendet es

Anti-Spam Netze

- Prüfsummen (Hashes) über bekannte Spam E-Mails
- Bekannte Dienste
  - Vipul's Razor 2.x
  - DCC
  - Pyzo

Heuristische Analyse

- Wörter in E-Mails (Header & Body) werden mit *Ham* und *Spam* Datenbanken verglichen.
  -> Scoring der E-Mail
- Datenbanken müssen nachgepflegt werden
- ressourcenhungrig

Bayes Filter

- benannt nach Thomas Bayes (brit. Mathematiker)
- ähnlich wie heuristische Analyse, aber
  - Filter wird selbst „trainiert“
  - Filter wird mit als „falsch“ klassifizierten E-Mails gefüttert
- bessere Performance, als heuristische Analyse

Beispiel: Spamassasin

- Features:
  - Blacklist
  - RBLs (DNS Blacklists)
  - Bayesian Filter
  - Anti-Spam Netze
  - Scoring

Beispiel: Spamassasin

- Spamassassin Rules
- Whitelist
  - whitelist_from fb@alien8.de (-100 Punkte)
  - whitelist_to *@skyhub.de
  - more_spam_to
  - all_spam_to (wird nie Spam)
  - unwhitelist_[from|to]
- selbe mit blacklists

Beispiel Spamassassin

- Bayesian Filter
  - sa-learn --ham --mbox ~/Mail/inbox
  - sa-learn --spam ~/Maildir/INBOX/cur
  - sa-learn --forget --mbox

Spamassassin

- Schwellwert einstellen:
  - required_hits
- eigene Rulesets:

Virenabwehr

- GPL virus scanner, kann u. a.:
  - command-line scanner
  - fast, multi-threaded daemon
  - database updater with support for digital signatures
  - on-access scanning (Linux and FreeBSD)
  - detection of over 20000 viruses, worms and trojans
  - built-in support for RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (Compressed HTML), MS SZDD
  - built-in support for mbox, Maildir and raw mail files
  - support for built-in support Portable Executable files compressed with UPX, FSG, and Petite

ClamAV Beispiel

```
clamscan /var/lib/amavis/virusmails/

/var/lib/amavis/virusmails//virus-20041017-060150-19553-01:  \
    Trojan.Dropper.JS.Zerolin-6 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 24813
Scanned directories: 1
Scanned files: 3090
Infected files: 524
Data scanned: 141.54 MB
I/O buffer size: 131072 bytes
Time: 48.236 sec (0 m 48 s)
```

AMaViS A Mail and Virus Scanner

http://www.amavis.org/

- Wrapper für E-Mail Scanner
  - Anit-Virus
  - Spam
- Zentrale Konfiguration
- kümmert sich um:
  - auspacken
  - dekomprimieren
  - Integration div. Tools

Dos and Don'ts für Scanner

- Viren
  - wegspeichern (Quarantäne)
  - Empfänger informieren
  - Nicht Absender / sicher gefälscht
- Spam
  - nie löschen sondern markieren
  - nie Absender informieren, eh gefälscht
  - besser nicht erkennen, als falsch erkennen

Zusammengebaut!

der Mailserver

Mailserver: Überblick