Die Möglichkeiten der Milterschnittstelle

Andreas Schulze

DATEV eG

5. Mailserverkonferenz

Berlin, 2011

Agenda

- Historie
- Überblick über die Filtermöglichkeiten bei Postfix
- Vorteile von Miltern
- Design
- Produktübersicht
- Beispiel: Signatur-Milter
- (Nachschlag)

Historie

- Sendmail Milter ist ein Kunstwort aus „Mail“ und „Filter“
  - macht den Anspruch klar
- Ausgabentrennung
  - MTA -> MailTransport
  - Milter -> Inhaltsanalyse
- sendmail-8.10.0/RELASE_NOTES
  - um 1999/2000
- sendmail-8.13.0/RELEASE_NOTES
  - „enabled by default“
  - 2004

Unterstützung bei anderen MTAs

- EXIM
  - ${dlfunc} Interface
  - http://mta.org.ua/exim-conf/dlfunc/milter/
  - keine Trennung vom MTA
  - klingt nicht wirklich produktiv ...
- diverse kommerzielle Sendmail Produkte
- Postfix

Unterstützung durch Postfix

- Postfix unterstützt seit Version 2.3 die Milterschnittstelle
  - ca. 2006
- bis dahin bei Postfix
  - „SMTP Access Delegation“ Protokoll
  - seit postfix-2.3 keine signifikaten Erweiterungen
- erfreulicherweise: PreQueue Filterung

Milter und die Aufgaben eines MTA

- Mailtransport
  - Annahme vom Mails über verschiedene Eingänge
    - smtp, lokal, qmqp, (uucp)
  - Mailversand an entfernte Systeme
  - Zustellung von Mails in Postfächer
- Mails nicht annehmen
  - basierend auf Informationen aus einer SMTP-Verbindung
  - unerwünschte / schadhafte Inhalte
  - Mengenbeschränkungen

Filterung bei Postfix

- Interne Postfix Tests
- Access Policy Delegation
- Filterung **nach** der Mailannahme
- Filterung **während** der Mailannahme

interne Postfix Tests (1)

- Domainnamen korrekt ?
- Client / Helo / Sender / Recipient Checks
- flexibel, kreative und exotische Lösungen möglich:
  - wenn die Absenderdomain von einem Nameserver gehosted wird, dessen IP-Adresse in einem Netz liegt, welches SPAMHAUS kennt, ...
  - wenn die SMTP-Gegenstelle „localhost“ als Helo-Parameter nutzt, ...
  - mein Wunsch: wenn die Gegenstelle `$valid_destination_domain` als Helo nutzt ...
- Peers Musterlösung

interne Postfix Tests (2)

- Inhaltsanalyse durch Zugriff auf Mailheader und -body
  - header_checks = pcre://...
  - body_checks = regex://...
- Peers Antispam
  - http://www.postfixbuch.de/upload/header_checks
  - http://www.postfixbuch.de/upload/body_checks
  - @Peer: Status / Aktualität ???

Access Policy Delegation

- Delegation der Entscheidung über Mailannahme an einen externen Prozess
- postfix spezifisches Protokoll
  - textbasiert, einfach, sessionbezogen
  - auch in exim realisierbar
- prominente Vertreter
  - postgrey
  - policyd-weight
  - postfwd
- kein Zugriff auf den INHALT einer Mail
- keine Information über Parallelität

Filterung **nach** der Mailannahme

- „PostQueue“
  - einfach & unkompliziert
  - Mail wird einem Inhaltsfilter per SMTP oder LMTP weitergeleitet
  - dieser gibt die Mail abschließend an Postfix zurück
  - macht einen MX möglicherweise zur Quelle von Backscatter
  - sowas macht heute natürlich NIEMAND mehr !?
- typischer Vertreter: amavisd-new

Filterung **während** der Mailannahme

- „PreQueue“
  - einfach
  - erzeugt keinen Backscatter
  - unkompiziert ?
    - Timeout Problem
    - `-o smtpd_proxy_options = speed_adjust` (seit Postfix 2.7)
  - wer macht das nicht ???
- typischer Vertreter: amavisd-new

Nachteile ?

- „Advanced“ Setup
  - amavisd-new
    - mehrere Virenscanner
    - SpamAssassin
  - kommerzieller Spamfilter
  - kommerzieller Virenscanner
  - Überprüfung von DKIM Signaturen
  - Mailentschlüsselung

Herausforderungen

- Received-Zeilen sind unübersichtlich
- Timeouts
  - bei großen Mails
  - langsamen Clients
- Mailverfolgung in den Logdaten zu Supportzwecken

Vorteile von Miltern (1)

- Zugriff auf Verbindungsinformationen UND Inhalte
  - welcher Client
  - HELO-Parameter
  - Absender
  - Empfänger
  - Header
  - Mailbody

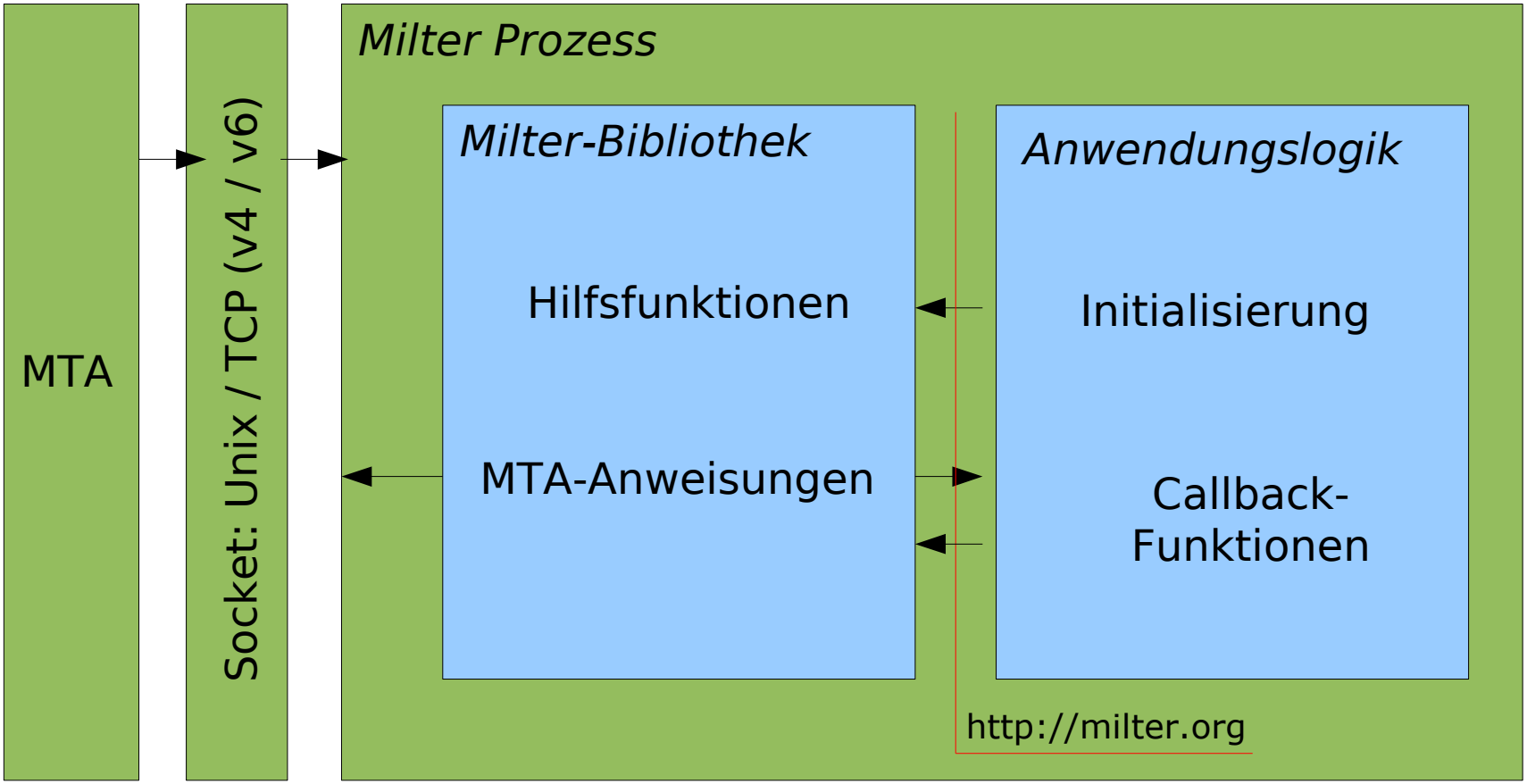
Vorteile von Miltern (2)

- Veränderungsmöglichkeiten
  - Absender ersetztbar
  - Emfänger umändern, hinzufügen und entfernen
  - Headerzeilen ändern, hinzufügen und entfernen
  - kompletter Mailbody ersetztbar
  - Steuerung des SMTP-Reply Code und -Text

Vorteile von Miltern (3)

- alles in einem Programm
- getrennt vom MTA über eine sauber definierte Schnittstelle
- auf externe Server auslagerbar
- Redundanz und Lastverteilung eingebaut
- großer Bestand an Miltern für verschiedenste Aufgaben
- http://milter.org
  - über 70 Milter verschiedenster Qualität für diverse Aufgaben

Design



Initialisierung

```
sfsistat callback_envfrom(SMFICTX* ctx, char** argv);
sfsistat callback_header(SMFICTX* ctx, char* headerf, char* headerv);

struct smfiDesc callbacks = {
    STR_PROGNAME,                          /* filter name        */
    SMFI_VERSION,                          /* version code       */
    SMFIF_ADDHDRS | SMFIF_CHGBODY,         /* filter actions     */
    NULL,                                  /* connection info    */
    NULL,                                  /* SMTP HELO command  */
    callback_envfrom,                      /* envelope sender    */
    callback_envrcpt,                      /* envelope recipient */
    callback_header,                       /* header             */
    callback_eoh,                          /* end of header      */
    callback_body,                         /* body block         */
    callback_eom,                          /* end of message     */
    callback_abort,                        /* message aborted    */
    callback_close,                        /* connection cleanup */
    NULL, NULL, NULL
};
```

Start

```
openlog(STR_PROGNAME, LOG_PID, LOG_MAIL);

if (smfi_setconn(„inet6:6570@[::1]“) != MI_SUCCESS) { log+exit(); }

if (smfi_register(callbacks) != MI_SUCCESS) { log+exit(); }

setgid(); setuid();

if ((c = smfi_main()) != MI_SUCCESS)
        logmsg(LOG_ERR, "Milter startup failed");
else
        logmsg(LOG_NOTICE, "stopping %s %s", STR_PROGNAME, STR_PROGVERSION);

exit (c);
```

Callbacks

- bekommen ein „SessionHandle“ mitgeliefert
  - Kontext
  - Optional: Platz für einen Zeiger auf einen privaten Speicherbereich zur freien Verwendung
- werden meist zu den SMTP-Kommandos aufgerufen
  - connect, helo, mail from, ...
- nur bestimmte Aktionen zulässig
  - Headerzeile löschen geht nicht im Status „Mail From“
- Rückgabewerte für den Mailserver
  - continue
  - accept / tempfail / reject

Callback Beispiel

```
sfsistat callback_envfrom(SMFICTX* ctx, char** argv) {
    if (mylookup(&badsender_table, argv[0])) {
        logmsg(LOG_INFO, "reject sender %s", argv[0]);
        return SMFIS_REJECT;
    }
    if (mylookup(&filtersender_table argv[0])) {
        logmsg(LOG_INFO, "starting vodoo for %s", argv[0]);
        return SMFIS_CONTINUE;
    }
    return SMFIS_ACCEPT;
}
```

Eigenheiten von einigen Callbacks

- Für jede Headerzeile erfolgt ein separater Aufruf des entsprechenden Callbacks
  - HeaderName und HeaderValue als getrennte Zeichenketten
- es gibt einen eigenen Callback „End of Header“
- der Mailbody kann in mehreren Teilen 'geliefert' werden
  - wie groß diese Teilblöcke sind, kann nicht gesteuert werden
  - bei kleineren Mails meist nur ein Block
- zum Abschluß gibt's einen Callback „End of Message“

weitere Details

- gibt’s auf milter.org

- Sendmail::PMilter
  - Pure-Perl Milter implementation
- Wrapper um die Milter-Bibliothek für mehrere Sprachen
  - Sendmail::Milter Perl Module
  - pymilter
  - (php)
  - (ruby)

Kontakt zum MTA

- Konfiguration erfolgt in der main.cf
  - `smtpd_milters = inet:foobar-milter.example.com:6570`
  - das kann IPv4 oder auch IPv6 sein ...
- oder in der master.cf als Option des smtpd
  - ```
    submission inet n - - - - smtpd
    -o smtpd_milters = unix:private/submission-milter
    ```

- zu beachten ist die unterschiedliche Notation des Sockets:
  - sendmail: inet:port@hostname
  - postfix: unix|inet:hostname:port
    ```

mehr bitte !

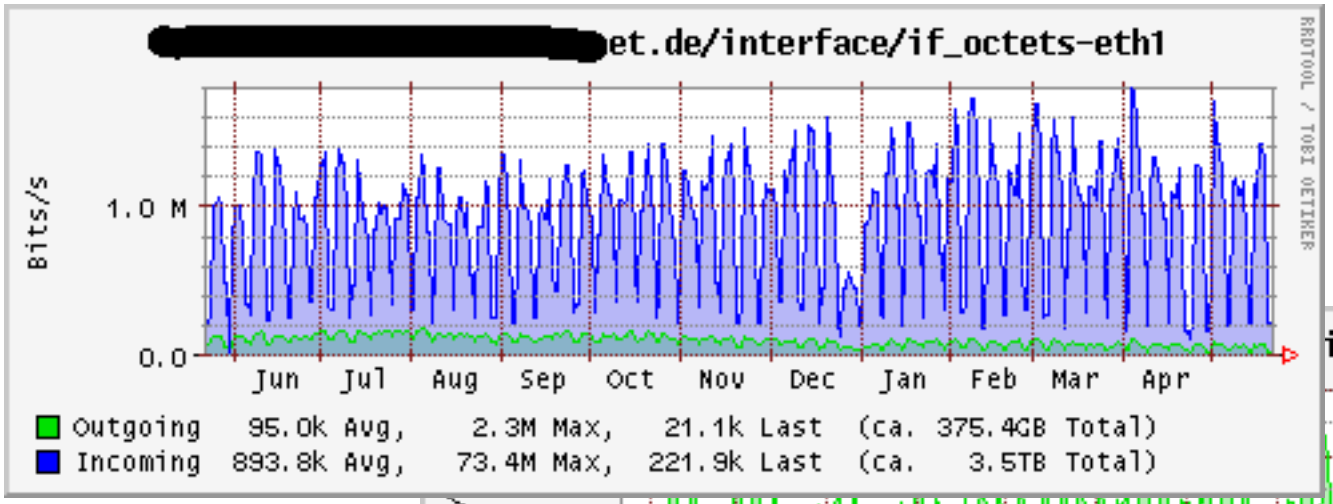
- mehrere Milter sind möglich
- sie werden einfach aneinandergereiht
  - `smtpd_milters = inet:localhost:3000,`
    `inet:localhost:4000`
  - Baukastenprinzip
- alle Änderungen des 1. Milters sind für den 2. Milter sichtbar!
  - veränderte Empfänger
  - eingefügte Headerzeilen
  - ersetzter Mailbody

und nochmehr !

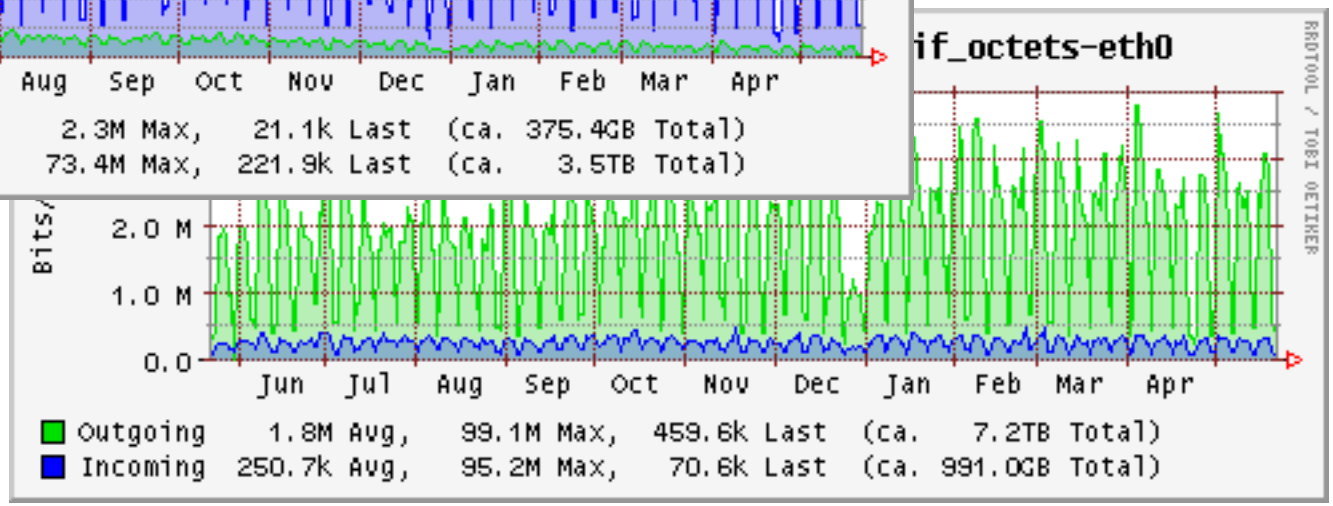
- sendmail hat das Milterprotokoll lediglich für SMTP-Verbindung ausgelegt.
- Postfix kann auch lokale Mails (+ QMQP-Server) an Milter umleiten
- Filterung von BounceMails möglich !
  - das ärgert die Sendmail-Jünger etwas :-)

Nachteile ?

- Netzlast im Auge behalten:



externes Interface:
eingehende Mails



internes Interface:
eingehende Mails
+ Mails zum Milter

welche Milter ?

- amavisd-new -> amavisd-milter
  - aktuelle Version 1.5.0 (Mai 2010) nötig, wenn amavisd-new-2.7.0 eingesezt wird.
  - postfix <-> inet-socket <-> milter <-> unix-Socket <-> amavis
  - amavisd.conf:

```
- $unix_socketname  = "$MYHOME/amavisd.sock";
  $interface_policy{'SOCK'} = 'AM.PDP-SOCK';
  $policy_bank{'AM.PDP-SOCK'} = {
    protocol => 'AM.PDP',
    forward_method => undef,
  };
```

  - @Mark: how to configure multiple policybanks?

welche Milter ?

- opendkim-milter
  - vergleichbare Funktionalität zu amavisd-new
  - Signatur und Verify auf verschiedene Instanzen verteilbar
  - Version > 2.3.x benutzen
  - aktive Mailing-Liste
  - Schlüsselmaterial aus dem DNS wird via DNSSEC validiert. (mittels libunbound)
  - Support für dkim-reputation.org

welche Milter ?

- clamav-milter
  - Virenscanner ClamAV scannt Mails direkt während der Mailannahme
  - keine Erfahrung / Empfehlung
- spamass-milter
  - „SpamAssassin ohne Amavis“
  - Vorsicht: Fehler in Version 0.3.1 -> CVE-2010-1132
  - Version 0.3.2 benutzen !
  - keine Erfahrung / Empfehlung

welche Milter ?

- milter-manager
  - nur ein Milter gegenüber dem MTA
  - dieser bedient dann weiter Milter
  - komplexes Regelwerk implementierbar

  - gar keine Erfahrung
  - aber klingt interessant !

Beispiel: Signatur-Milter

- Motivation
- bestehende Lösung
- Alternativen
- Lösung mittels Miltertechnik
- etwas Werbung ...

Motivation

- Mails mit S/MIME Signaturen versehen
- „ein echte Mail von DATEV ist signiert“
- schafft Vertrauen bei den Kunden
- wer bekommt von seiner Bank signierte Mails ???

bestehende Lösung

- Zustellung der Mails an ein externes Programm in der master.cf
  - http://www.postfix.org/FILTER_README.html#simple_filter
- externes Programm war richtig langsam
  - Vorgabe: 5000 Mails/Stunde
- keine DSN bei Zustellung mehr möglich
  - Mail gilt für postfix ja als zugestellt, sobald sie dem externen Programm übergeben wird

Plan B

- `cat plaintext \`
  `| openssl smime -sign -signer cert.pem ...`
- das geht also in Software :-)
- Beispielquelltext in openssl-0.x.y/apps/smime.c
- kein Projekt gefunden
- selbst programmiert
  - erst mit den Perl-Miltern
  - letztlich dann doch in C

signing-milter.org

- C-Programm
- Auswahl der Zertifikate je nach Envelope-Sender
- Alternative Steuerung über einen X-Header
- Signatur des kompletten Mailbodys
- Umbau der Header wegen geändertem Content-Type

Logging + Statistik

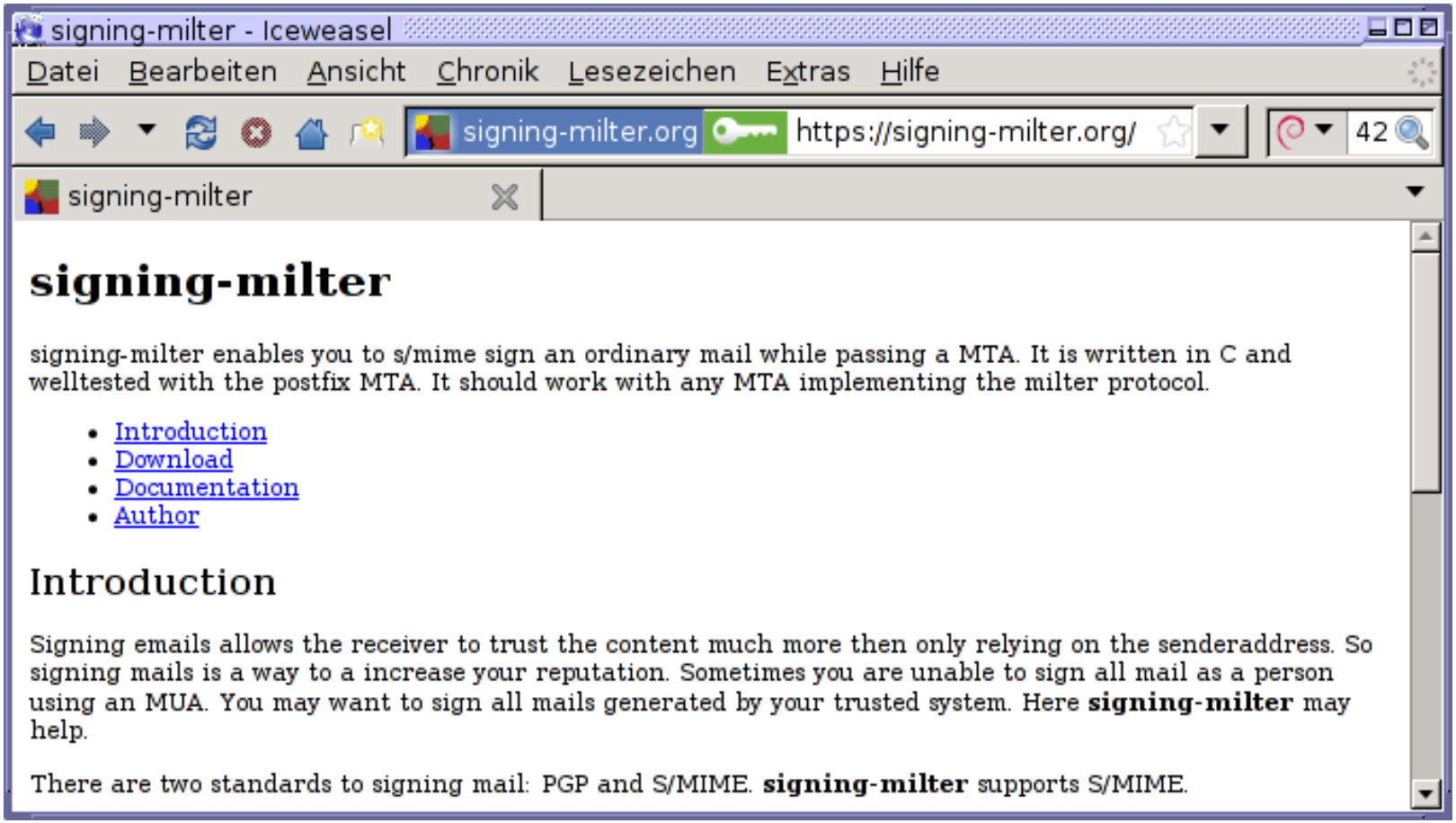
- Logging
  - enthält die QueueID
  - `May 23 11:43:47 debian signing-milter[5200]: 33458123D41: clearsigned with /etc/signing-milter/sender@example.com-cert+key.pem`
- Statistik
  - gemessen wird die Dauer der SSL-Operationen
  - `May 23 11:43:47 debian signing-milter[5200]: 33458123D41: signing 87 byte took 0.71760 sec`
  - `May 23 12:17:12 debian signing-milter[5200]: STATISTIK: 1/0.71`

Performance

- eigene Messungen auf Produktionsservern
  - Mails Sekunden Dauer pro Mail (in ms)

Mails	Sekunden	Dauer pro Mail (in ms)
699	32.28	46.19
719	32.26	44.87
2039	78.81	38.65
2043	76.73	37.56
2530	20.76	8.2
2539	20.42	8.04
2860	24.38	8.53
14925	123.97	8.31
2880	118.62	41.19
2889	114.21	39.53
5283	43.47	8.23
6084	48.87	8.03
6098	46.94	7.7
6788	51.67	7.61
6789	53.46	7.87

signing-milter.org



Danke

- Andreas Schulze
- DATEV eG
- andreas . schulze @ datev . de

Zukunft gestalten. Gemeinsam.

Nachschlag

- sendende Mailsysteme werden üblicherweise bei DNSWL.ORG registriert
- DNSWL.ORG wird als RBL im SpamAssassin abgefragt.
- ein gelisteter Mailserver bekommt einen positiven Bonus.
- ca. 100.000 Mailserver gelistet
- Annahme: ein Admin, der sich bei DNSWL.ORG einträgt, ist um seine Systeme bemüht und kann im Problemfall kontaktiert werden.
- Seit November 2010 nicht mehr komplett kostenfrei

Alternative: MTX

- Idee: jeder benennt seine Mailserver selber.
- 193.27.50.76
- -> mailout01.datevnet.de -> 193.27.50.76
- 76.50.27.193.mtx.mailout01.datevnet.de -> 127.0.0.1
- Kann doch jeder ...
- Genau !
- Keine zentrale Instanz nötig
- SA-Plugin vergibt Bonus
- Voraussetzung: sauberes DNS-Setup

Nutzen Spammer MTX ?

- unwahrscheinlich
- Fastflux-Netze zum Spamversand
- kein Zugriff auf rDNS
- Spammer wollen unerkannt bleiben
- falls doch: Blacklist ist eingebaut

wie geht’s genau

- kann sendende Systeme benennen
- kann nichtsendende Systeme benennen (WebServer)
- Policy beschreibt alle anderen Systeme
  - kein anderer Versender in meinem Netz
  - könnte sein, dass noch andere Systeme senden
  - auf jeden Fall sind da noch mehr Versender
  - keine Aussage
- Beschreibung der Ergebnisse an SPF angelehnt
  - pass, hardfail, softfail, neutral, none

Ergebnissoffen

- Mapping des Ergebnisses in Punkte durch ein SA-Plugin
- für den Abuse-Fall gibt’s dann doch eine zentrale Blacklist
- auch deren Ergebniss wird in SA-Punkte umgewandelt

Quelle und weitere Details:

- http://chaosreigns.com/mtx/
- DNSWL.ORG Admin
- das SA-Plugin **läuft** mit 3.3.2-rc1
- Patch f. IPv6 Hosts bei Interesse ...