Mailen Sie doch einfach mit Ihrem guten Namen…

Businesskritische E-Mail mit
DKIM, ADSP und ARF sichern

stateofmind()

Wir leben in der Anti-Spam Steinzeit

BÖSE SPAM! BÖSE SPAM! SITZ! JA, SO IST‘S GUT…

Die drei Worte der Anti-Spam Welt

- **„Böse!“**
  - Mail wurde als Spam klassifiziert
  - Mail soll nicht zugestellt werden
- **Ähh…?**
  - Mail wurde nicht als Spam klassifiziert
  - Mail soll zugestellt werden
- **Hmmm…?**
  - Mail wurde nicht als Spam klassifiziert
  - Mail soll zugestellt werden

Status Quo Anti-Spam Methoden

- Unerwünschtes Verhalten wird bestraft
- Neutrales Verhalten führt zu nichts
- Gutes Verhalten wird nicht belohnt

Was eine Mail vor der Zustellung so durchmachen muss…

TYPISCHE MAIL POLICIES

SMTP Session Policies

- **RFC-Konformität**
  - HELO-Name erforderlich
  - Envelope-Sender muss gültig sein
  - Envelope-Recipient muss gültig sein
  - Sender-Domain muss existieren
  - Recipient-Domain muss existieren
  - HELO-Name muss gültig sein
  - HELO-Name muss vollständig (FQDN) sein

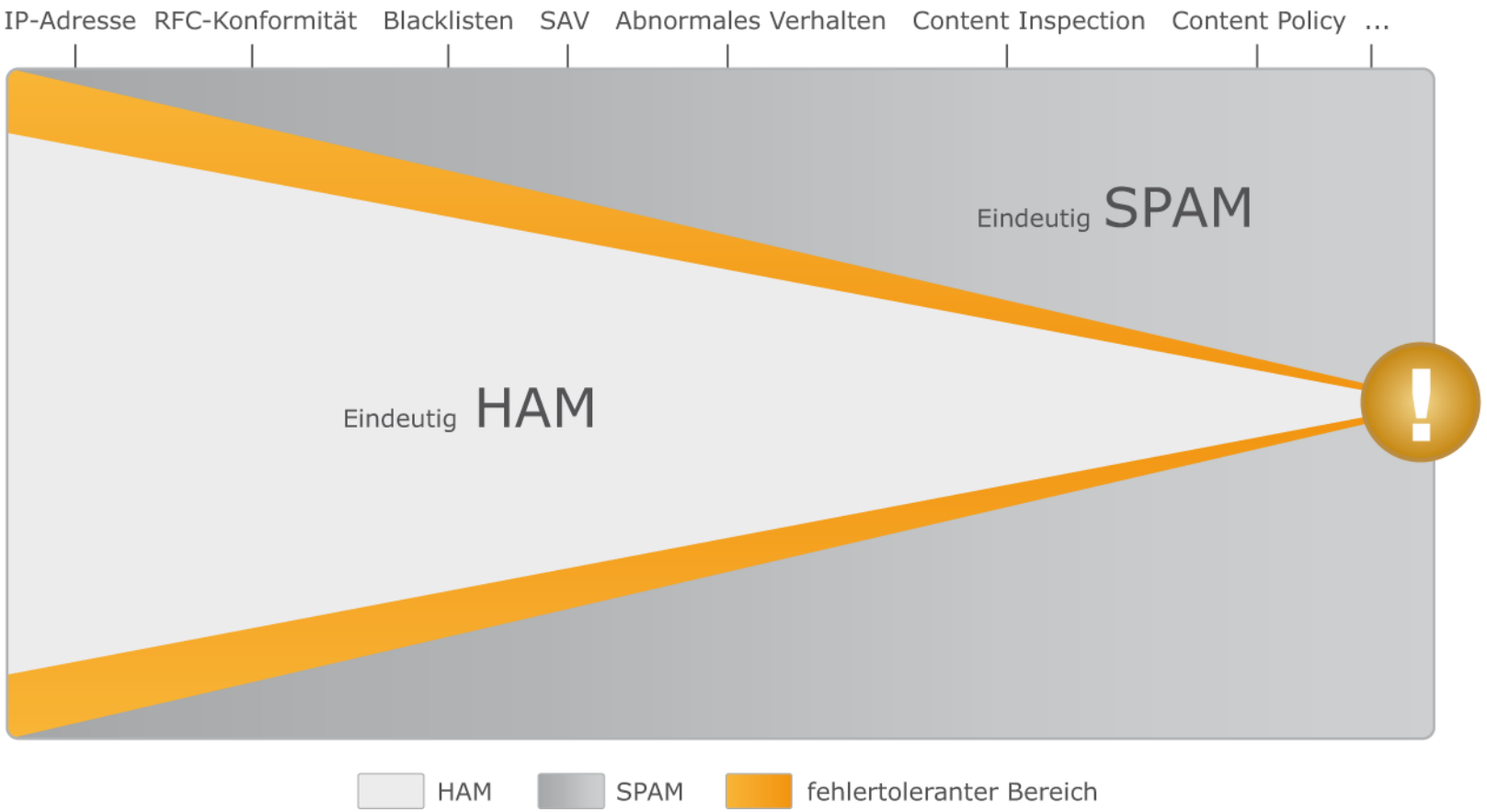
- **Blacklisten**
  - IP-Adressen
  - lokale Listen (manuell)
  - DNS-basierte Listen (automatisch)
- **Sender-Address-Verification**
- **Abnormale Verbindungen**
  - begrenzen
  - ablehnen

- **RFC-konform**
  - Subject-Header-Encoding
  - Match Envelope- und Header-Angaben
- **Content-Analyse**
  - Pattern Matching
  - Wortkombinationen
  - Worthäufungen
- **MIME-Formate**
- **Attachment-Typen**
- **Attachment-Analyse**
- **Verhaltensanalyse**
  - Sender – Empfänger
  - Ort
  - Uhrzeit

„Und als es wieder nicht geklappt hat, haben wir uns einfach noch mehr angestrengt…“

STATUS QUO

Worauf steuern diese Methoden zu?



- **Sender werden zu schnell als böse identifziert**
  - Der Korridor innerhalb dessen wir uns mit legitimer E-Mail Fehler erlauben dürfen, ist sehr schmal geworden.
- **False Positives sind teuer**
  - Fehltritte haben schnell weitreichende, uns selbst schädigende Folgen
- **Schutzbedürfnis pervertiert Use Case „E-Mail“**
  - Anti-Spam-Methoden, die businesskritische E-Mail-Eigenschaften einschränken, werden akzeptiert und etablieren sich

Womit wir heute schon E-Mail ruinieren

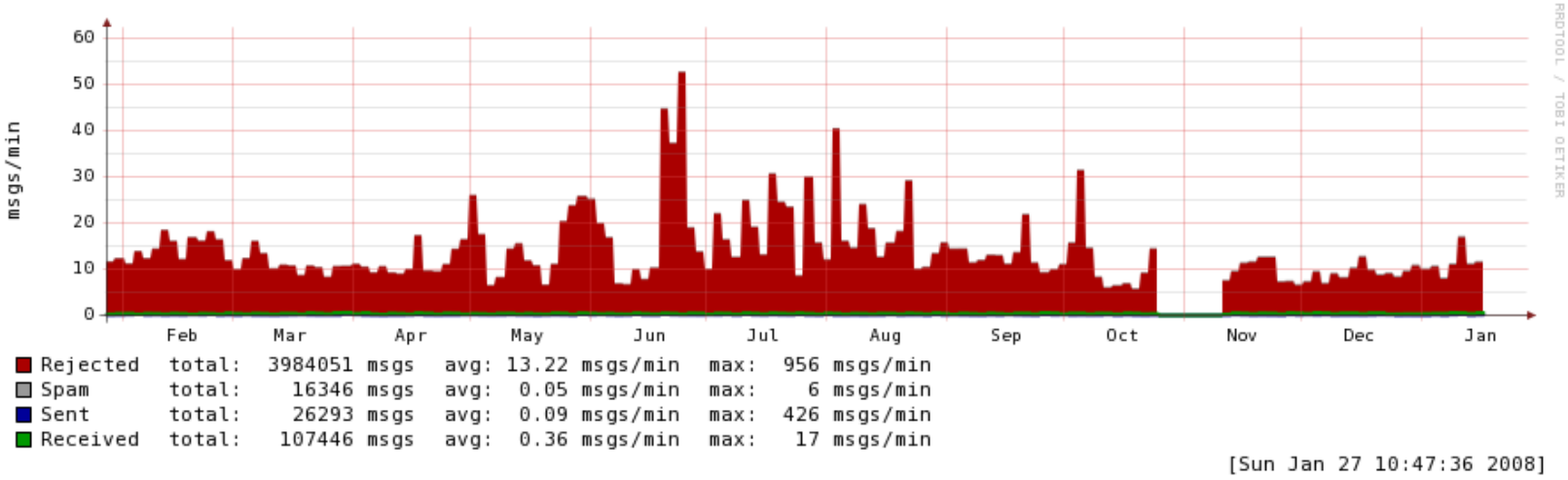
FRIENDLY FIRE

Greylisting

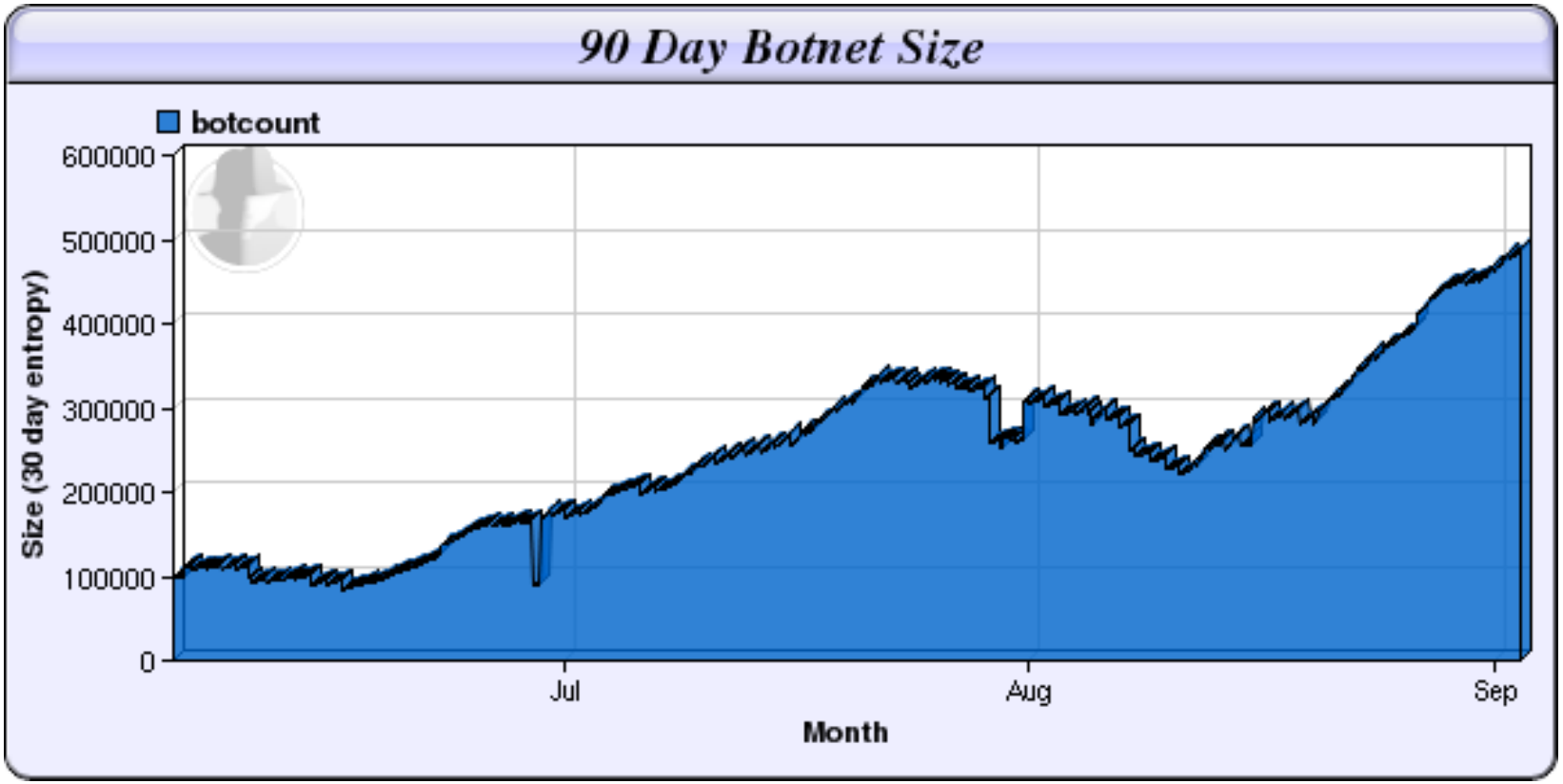
- **Kennkriterien**
  - Triplet aus IP des Clients, Envelope-Sender und Envelope-Recipient
- **Ziel**
  - Botnet-Dronen ausgrenzen
- **Methode**
  - Erstmalig ablehnen und Triplet merken
  - Durchlassen wenn Triplet nach Karenzzeit wiederkommt
  - Ablehnen wenn Triplet vorher wiederkommt
  - Triplet nach einer Weile wieder vergessen

- **Probleme**
  - Spontane Verfügbarkeit geht verloren
  - Client bestimmt wann erneuter Zustellversuch unternommen wird
  - Deadlock mit Sender-Address-Verification
  - Greylisting wird bereits erfolgreich unterlaufen

Botnetze durchbrechen Greylisting



Wachstum Botnetze 2008/Q3



Sender Policy Framework (SPF)

- **Kennkriterien**
  - DNS-Eintrag
- **Ziel**
  - Ungültige Server (Rechner) ausfiltern
- **Methode**
  - DNS-Eintrag benennt Server von denen E-Mail einer Domain „entspringen“ darf
  - Server prüft eingehende E-Mail auf korrekten Ursprung

- **Probleme**
  - User werden auf einen Server gezwungen
  - Company Policies verbieten Verbindungen zu den notwendigen Servern
  - Legitime Mail wird als illegal „gebrandmarkt“
  - SPF ist broken by design
- **Aber…**
  - … als Policy Tool für Reputation brauchbar

Tagged Message Delivery Agent (TMDA)

- **Kennkriterien**
  - Lokale Liste/Datenbank legitimer User
- **Ziel**
  - Alles verbieten was nicht explizit gestattet ist
- **Methode**
  - Envelope-Sender sendet E-Mail
  - Server hält E-Mail auf
  - Server sendet Challenge
  - User beantwortet Challenge erfolgreich

- Server trägt Envelope-Sender in (temporäre) Whitelist ein
- Server läßt originäre E-Mail passieren

- **Probleme**
  - Hohe Eintrittsbarriere für Neukontakte
  - Einsatz in Unternehmen mit viel Neukontakten schwierig
  - Widerspricht der Idee der freien Kommunikation im Internet

Status Quo Anti-Spam-Methoden

- **Effiziente Spambekämpfung ist auf Automatisierung angewiesen**
- **Der Anti-Spam-Wortschatz kennt nur die Kategorien „Neutral“ oder „Feind“**
- **Wer nicht neutral ist, wird als Feind behandelt!**
- **Der Interpretationsspielraum muss erweitert werden**
- **E-Mail muss lernen, was einen „Freund“ ausmacht**

Perspektiven, die aus der reinen Schwarzmalerei führen

NEUE FREUNDE

Ein Freund ist …

- **… solide**
  - Er ist ortsfest
- **… immer für uns da**
  - Er ist immer erreichbar
- **… ehrlich zu uns**
  - Wir wissen wir können ihnen vertrauen
- **… verantwortungsbewusst**
  - Er achtet auf sich selbst und läßt sich nicht missbrauchen
- **… nett zu den Nachbarn**
  - Er wird auch von den anderen so wahrgenommen

Wie Freunde automatisiert erkennen?

- **Zwei Aufgaben**
  - Freund von Feind unterscheiden
  - Vorgang automatisieren
- **Zwei (bis drei) Probleme**
  - Host-Adressen ändern sich
  - Host-Namen ändern sich
  - Spammer mißbrauchen Hostnamen

Richtige™ Vorgehensweise

1. Identität zweifelsfrei bestimmen
2. Identität kategorisieren
3. Reputation errechnen

Identität ist die Voraussetzung für Reputation

DKIM

D-WAS ?!?

- **DKIM ist ein zentralisierter Ansatz zum Signieren von E-Mail**
- **Eine DKIM-Signatur**
  - bestätigt die legitime Nutzung des Servers
  - bestätigt einen bestimmten Zustand der E-Mail zum Zeitpunkt der Unterschrift
- **Ein DKIM signierender Server kann**
  - sich im Internet „einen guten Namen“ machen
  - seinen guten Ruf bei der Beurteilung der Spamhaftigkeit in „die Waagschale werfen“

- mit seiner gültigen Signatur den Absender legitimieren und
  - die Glaubwürdigkeit seiner Anfrage untermauern bzw.
  - den Missbrauch einer Sender-Domain (Phising) aufdecken

Wer hat‘s erfunden?

- **DKIM ist der legitime Nachfolger von Domainkeys, einer Erfindung von Yahoo und Cisco.**
- **DKIM ist in einem RFC standardisiert (RFC 4871 und 5672)**
  - Sendmail
  - PGP
  - Yahoo
  - Cisco

Wie funktioniert DKIM?

1. Ausgehende E-Mail wird zentralisiert auf dem Mailserver (oder Mail-Gateway) durch einen Vermerk im Header signiert
2. Der öffentliche Teil des Signierschlüssels wird über DNS im Internet publiziert
3. Eingehende E-Mail wird auf DKIM-Header untersucht

Wie funktioniert DKIM?

4. Gefundene Signaturen werden auf ihre Gültigkeit geprüft (-> Identität)
5. Das Resultat der Prüfung wird zur Einstufung des Servers herangezogen (-> Reputation)
6. Das Ergebnis wird auf die weitere Zustellung angewendet

SMTP
Client

SMTP
Server

DNS
Server

Ablauf

Die Teilnehmer

SMTP
Client

SMTP
Server

DNS
Server

Ablauf

Besitzer von Private und Public key

SMTP
Client

SMTP
Server

DNS
Server

Ablauf

Ausgehende Nachricht wird mit DKIM-Signatur versehen

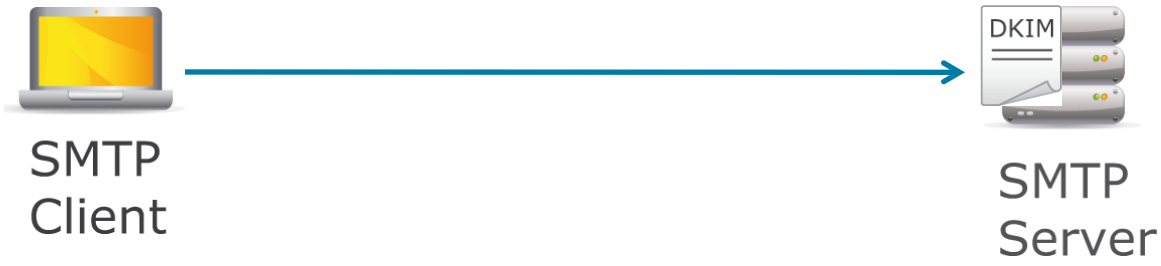
SMTP
Client

SMTP
Server

DNS
Server

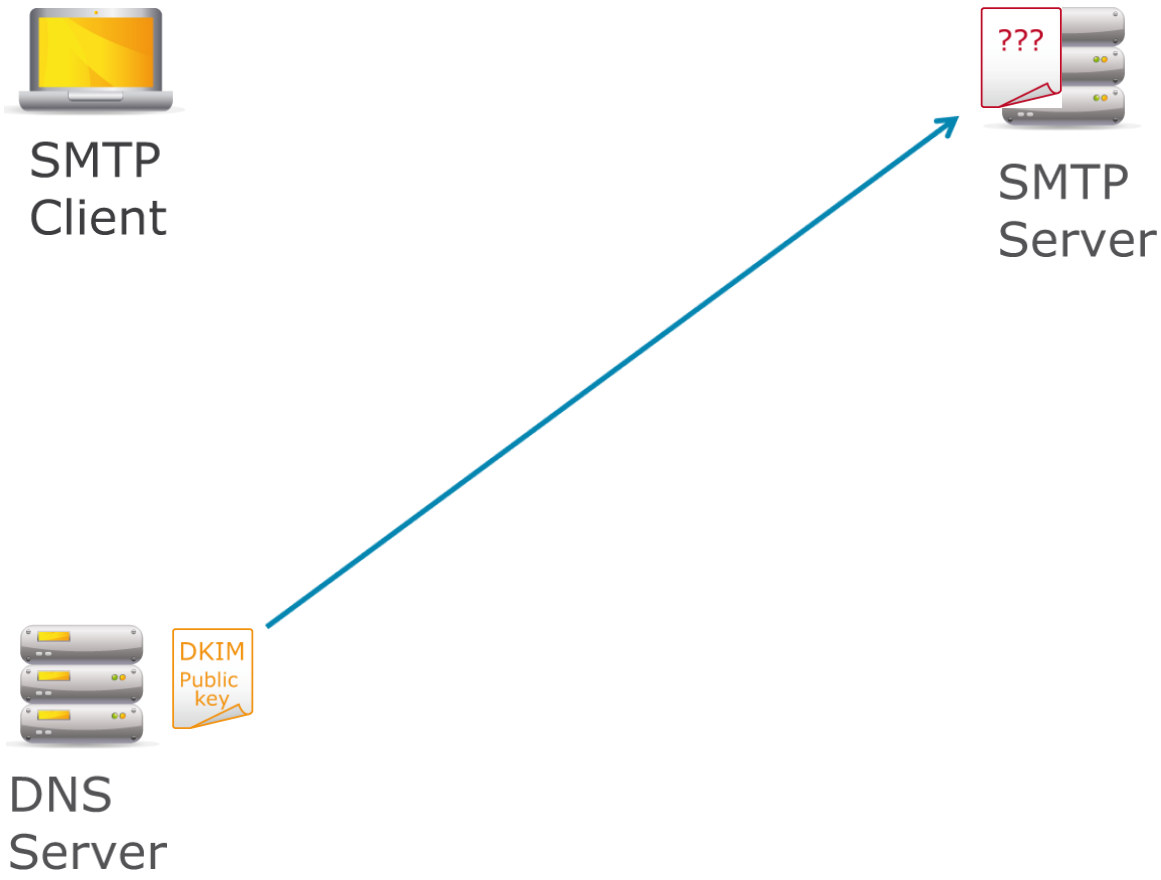
Ablauf

Signierte E-Mail



Ablauf

Server findet und analysiert DKIM-Signatur



Ablauf

Server bezieht Public key der signierenden Domain

SMTP
Client

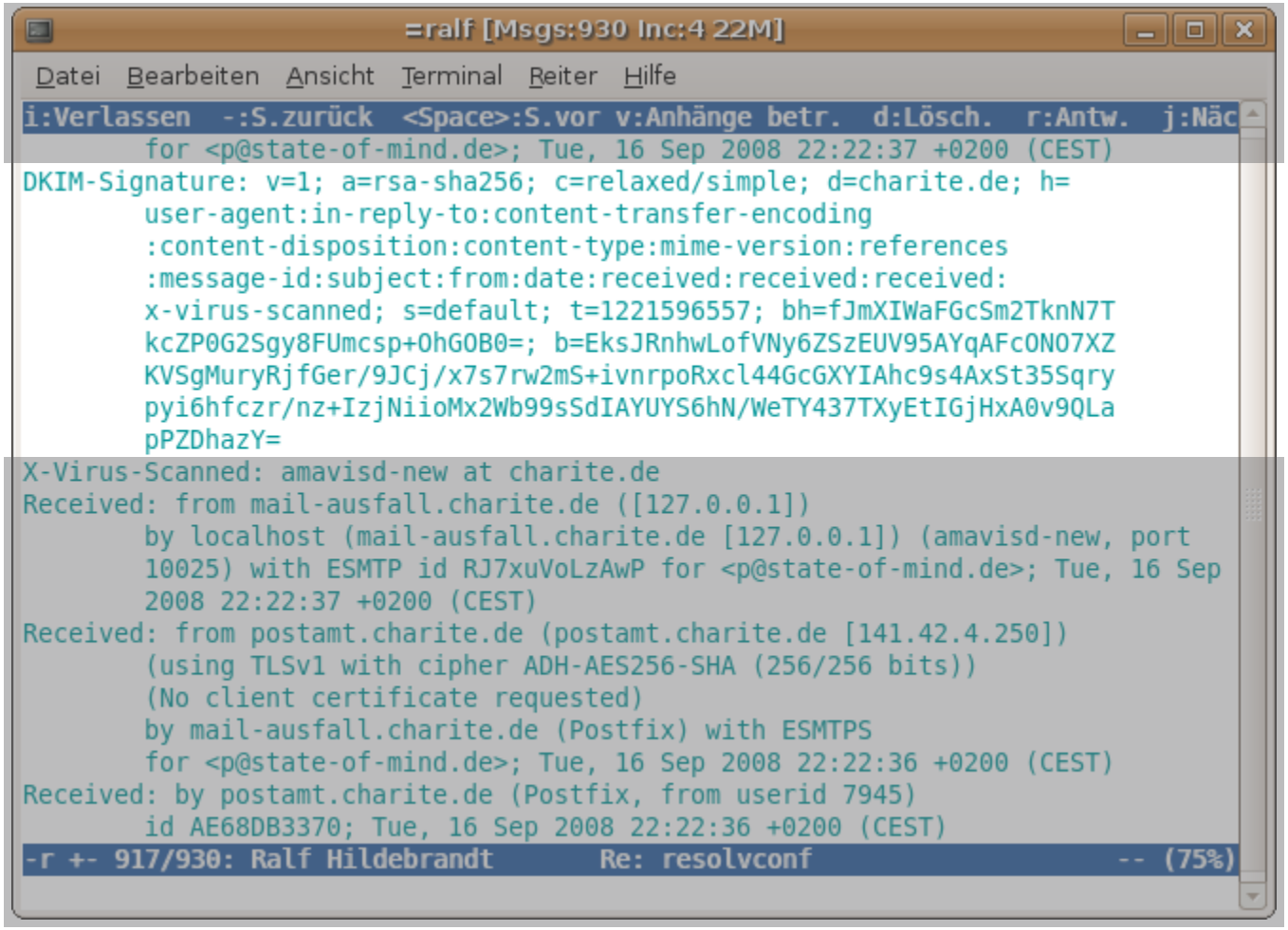
SMTP
Server

DNS
Server

Ablauf

Signatur verifiziert gültig

DKIM-Signatur in einer E-Mail



Wie implementiert man DKIM?

- Signier-Schlüssel generieren
- Public Key in DNS veröffentlichen
- Ort im Zustellprozess und Applikation zum Verifizieren und Handeln bestimmen
- Ort im Zustellprozess und Applikation zum Signieren bestimmen

Verifizieren und Signieren in getrennten Applikationen

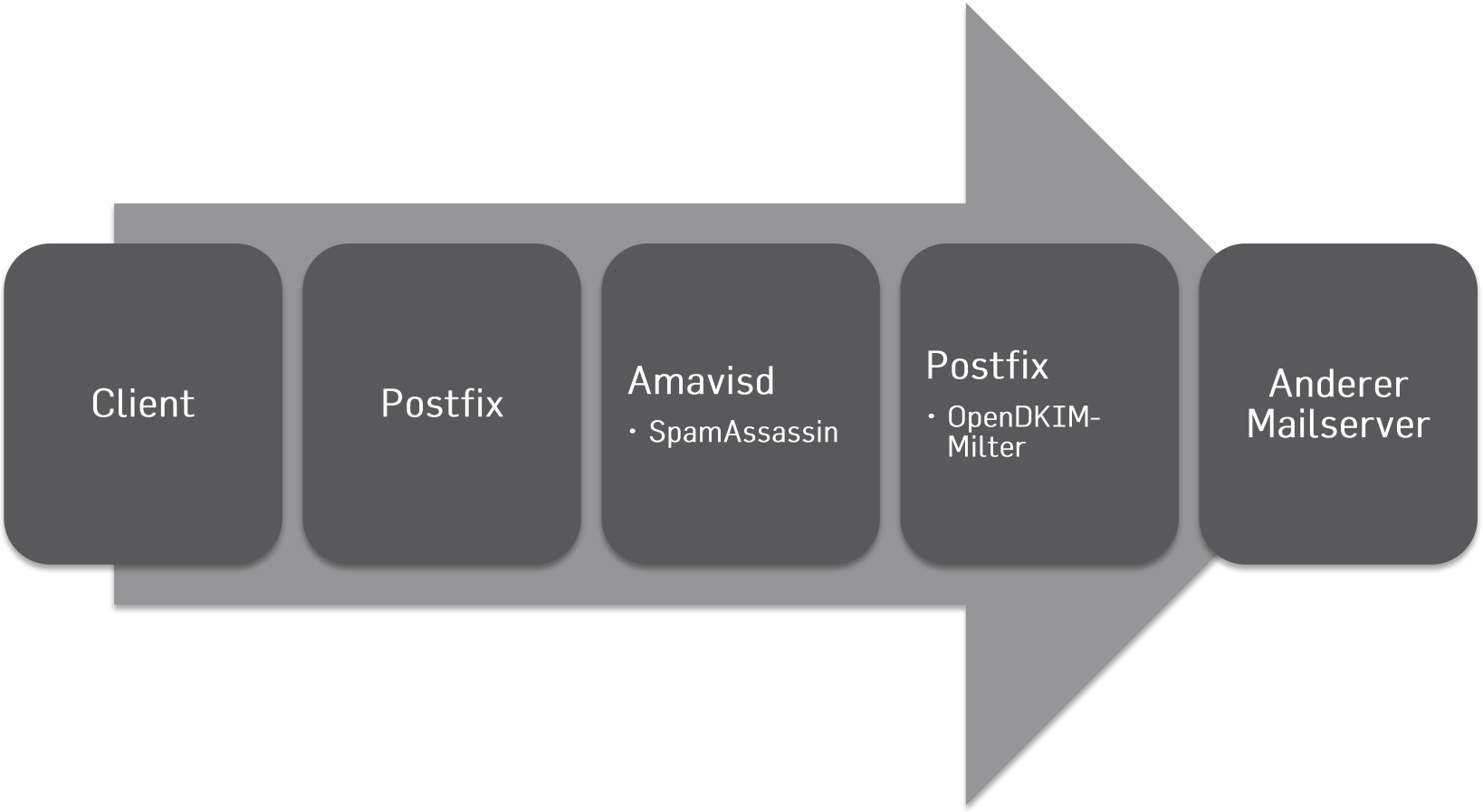
- **Software**
  - Postfix
  - DKIM-Milter (OpenDKIM)
  - SpamAssassin

- **Milter sind Sendmail Mail Filter**
- **Postfix implementiert weite Teile des Milter-API**

Arbeitsverteilung

- Postfix nimmt E-Mail an und gibt sie zur Prüfung an amavisd-new
- Amavisd-new übergibt E-Mail an SpamAssassin
- SpamAssassin prüft auf DKIM-Header
- SpamAssassin wendet Regeln auf DKIM-Signaturen an
- DKIM-Filter signiert ausgehende Mail, nachdem sie von amavisd-new ins Postfix-Mailsystem zurückgegeben wurde.

Sendeprozess



Schlüssel generieren

Openssl-Kommando oder bequem Skript verwenden, z.B. http://postfix.state-of-mind.de/patrick.koetter/dkim/mkdkim.sh

```
$ ./mkdkim.sh mail01
# TXT-Record
mail01._domainkey       IN       TXT       "v=DKIM1\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDlxOhKnVWipt5crkPVPmVVQvAdVZrBK/
YyAgvosQFWP3gEImaRyqsv5AKfG8XpQ0b8Lpxb7AvYvGc/nf/Pc8nfwa9WUEZ9D66igPFWc5
uXkcH+JryVC+D30/E45bxDFDpArwS93jwFiZsl44naTjqlsHy5ebYSyVmjbz+9uA5fEwIDAQ
AB"

# RSA-Keys
Private key stored in file \'mail01.key\'
Public cert stored in file \'mail01.pub\'
```

Verifizieren und Reagieren

SpamAssassin

- **Perl-Modul für DKIM laden**

```
loadplugin Mail::SpamAssassin::Plugin::DKIM
```

- **Regeln eintragen**

```
score DKIM_VERIFIED -1.3
score DKIM_POLICY_TESTING 0
score USER_IN_DKIM_WHITELIST -4.0

whitelist_from_dkim  *@state-of-mind.de state-of-mind.de
whitelist_from_dkim  *@intl.paypal.com paypal.com
```

Signieren

Postfix

```
127.0.0.1:10025 inet n    -     n       -       -     smtpd
     -o content_filter=
     -o smtpd_delay_reject=no
     -o smtpd_client_restrictions=permit_mynetworks,reject
     -o smtpd_helo_restrictions=
     -o smtpd_sender_restrictions=
     -o smtpd_recipient_restrictions=permit_mynetworks,reject
     -o smtpd_data_restrictions=reject_unauth_pipelining
     -o smtpd_end_of_data_restrictions=
     -o smtpd_restriction_classes=
     -o smtpd_milters=inet:localhost:8891
     -o mynetworks=127.0.0.0/8
     -o smtpd_error_sleep_time=0
     -o smtpd_soft_error_limit=1001
     -o smtpd_hard_error_limit=1000
     -o smtpd_client_connection_count_limit=0
     ...
```

Signieren

dkim-filter

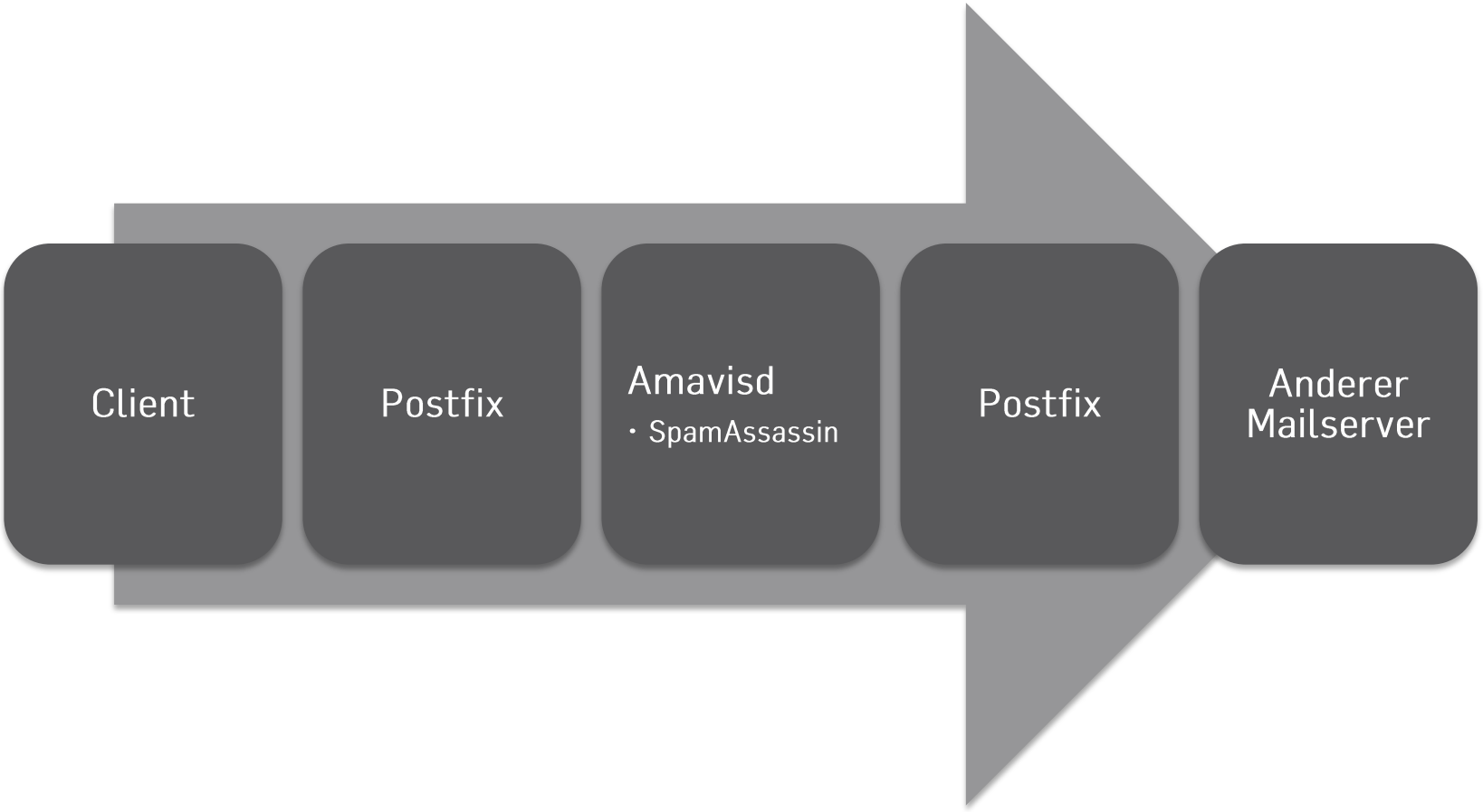
```
UMask                   002
Domain                  state-of-mind.de
KeyFile                 /etc/mail/mail0801.key
Selector                mail0801
AutoRestart             yes
Background              yes
Canonicalization        relaxed/simple
Mode                    s
SignatureAlgorithm      rsa-sha256
SubDomains              no
X-Header                no
BodyLengths             No
```

Verifizieren und Signieren in einer Applikation

Software: Amavisd-new > 2.6, Perl-Modul DKIM > 0.31

- **Verifizierung aktivieren**
  ```
  $enable_dkim_verification = 1;
  ```
- **Schlüssel generieren**
  ```
  # amavisd genrsa /var/db/dkim/a.key.pem
  ```
- **Signieren aktivieren**
  ```
  $enable_dkim_signing = 1;
  ```
- **Signatur konfigurieren**
  ```
  #       signing domain   selector  private key  options
  dkim_key('example.org',   'abc',    '/var/db/dkim/a.key.pem');
  ```

Sendeprozess



Reputation automatisiert einholen

- **Reputationsprovider prüft DKIM-signierte E-Mail**
- **Die Ergebnisse fliessen in eine Reputationsdatenbank ein**
- **Die Datenbank kann über DNS abgefragt werden**
- **Beispiel: dkim-reputation.org**
  - Perl-Modul für SpamAssassin
  - „NiX Spam“ füttert dkim-reputation.org

Lessons Learned

- E-Mail darf nach Signieren nicht mehr modifiziert werden
- Name des Selectors sollte inkrementierbar sein
- DKIM hat Rechte und Pflichten
  Mißbrauch ist kein Zeichen für das Scheitern der Methode
- Sites mit guter Reputation haben bessere Zustellquoten
- Achtung: Hohe Zustellquote ist für Spammer attraktiv!

Lessons Learned

- Spammer “phishen” Login-Daten für E-Mail-Accounts
- Accounts werden zum Spam-Versand mißbraucht
- Die Reputation der Site sinkt
- **Reputation ist nicht nur für DKIM brauchbar**

„Und wie bist Du sonst so…?“

ADSP

Von DKIM absichtlich ausgelagert…

- **Eine verifizierte Signatur ergibt eine Identität**
- **Eine verifizierte Signatur enthält keine Aussage über den Gebrauch der Identität**
- **„Author Domain Signing Practices“ (ADSP) lösen das Problem**

ADSP-Antworten

- Signierst Du?
- Signierst Du manchnal?
- Signierst Du immer?
- Was soll ich tun, wenn es Widersprüche gibt?

ADSP Policies

- **Publikation über DNS TXT-Record**
- **Wortschatz**
  - Unknown
    „Manchmal signier ich, manchmal nicht.“
  - All
    „Ich signiere alles. Nicht signierte E-Mail ist verdächtig!“

ADSP Policies

- Discardable
  „Wir signieren alles auf Absender-Ebene. Du mußt nicht signierte E-Mail löschen!“
- **Signier-Praxis**
  - Domain
  - Subdomains

ADSP ist schnell implementiert

http://www.sendmail.org/dkim/wizard

Wozu es auch noch gut ist!

DKIM & ADSP

Reject Handling

- **Grosse Mail-Provider blocken potentielle Spamversender rigoros**
  - AOL
  - Yahoo
  - ...
- **Reporting der Gründe nur nach Akkreditierung**
- **Provider fordern DKIM als Teil der Akkreditierung ein**
- **Das Reporting erfolgt automatisch**

Automatisierter Spam-Report

```
Date: Sat, 20 Feb 2010 13:49:36 -0800From: Yahoo! Mail AntiSpam Feedback <feedback@arf.mail.yahoo.com>
To: abuse@python.org
Subject: FW:Tutor Digest, Vol 72, Issue 101
X-Spam-Status: No, score=0.255 required=6.31 tests=[AWL=-0.154,
        DKIM_SIGNED=0.001, FORGED_YAHOO_RCVD=1.408, RCVD_IN_DNSWL_LOW=-1]

[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.1K --]

This is an email abuse report for an email message received from python.org  on Sat, 20 Feb 2010 07:55:17 PST

[-- Attachment #2 --]
[-- Type: message/feedback-report, Encoding: 7bit, Size: 0.3K --]

[-- Autoview using less ''/home/p/.mutt/tmp/muttbcvRTn'' --]
Feedback-Type: abuse
User-Agent: Yahoo!-Mail-Feedback/1.0
Version: 0.1
Original-Mail-From: <tutor-bounces+someone=yahoo.com@python.org>
Original-Rcpt-To: someone@yahoo.com
Received-Date: Sat, 20 Feb 2010 07:55:17 PST
Reported-Domain: python.org
Authentication-Results:

[-- Attachment #3 --]
[-- Type: message/rfc822, Encoding: 7bit, Size: 13K --]
…
```

Format zum Austausch von Abuse-Complaints

ARF

Hund? Katze? Maus?

- **Standardisiertes Format für Mißbrauch-Meldung**
- **Eigener MIME-Typ: *message/feedback-report***
  - Maschinenlesbar
  - Automatisierbar
  - Syntax-Element „Feedback-Type“ beschreibt Art des Mißbrauchs

Feedback Typen

- **abuse**
  spam oder anderer email abuse
- **dkim**
  DKIM Signatur Verifizierungsfehler
- **fraud**
  Betrug und/oder Phishing
- **miscategorized**
  Aufgrund Zertifizierung oder Reputation falsch eingestuft

- **not-spam**
  Nachricht ist nicht Spam
- **opt-out**
  Mailing-Listen opt-out
- **virus**
  Virus in Nachricht
- **other**
  Passte nicht in obige Kategorien

Abusix.org – ARF Clearing House

- *"Our mission is to help ISPs and Internet companies solving the rapidly growing problems of spam and and all kind of other security issues in a solid, accurate and reliable way."*
- *"Shutting down abusive systems as fast as possible thus is the only way to tackle the problem in an appropriate way."*

- **Provider senken Spam aus ihrem Netz**
  - Weniger Traffic reduziert Kosten
  - Weniger Spam erhöht ISP-Reputation
  - Hartes Vorgehen gegen Spam vergrault Spammer
  - Sauberes Netz lockt Neukunden an
- **Libraries und Software für ARF-Handling ist unterwegs**

Digitale Kommunikation
www.state-of-mind.de