

STRATEGIEN GEGEN SPAM

EIN ÜBERBLICK

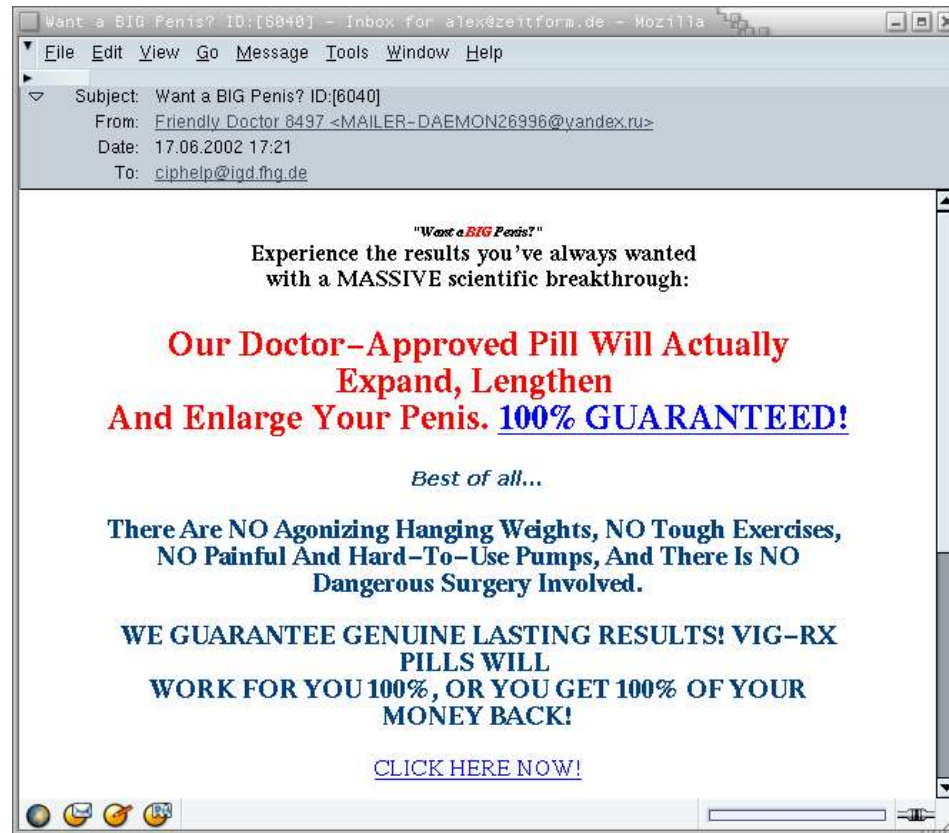


Was ist SPAM™?



Vikings: SPAM SPAM SPAM SPAM. Lovely SPAM! Wonderful SPAM!
SPAM SPA-A-A-A-A-AM SPAM SPA-A-A-A-A-AM SPAM. Lovely SPAM!
Lovely SPAM! Lovely SPAM! Lovely SPAM! Lovely SPAM!
SPAM SPAM SPAM SPAM!

Was ist Spam?



Was ist Spam?

UBE - Unsolicited Bulk Email

UCE - Unsolicited Commercial Email

- **Unsolicited:** (dt. unverlangt, unerbeten, unaufgefordert): Die Zusendung der E-Mail wurde nicht explizit vom Empfänger angefordert oder erwartet.
- **Bulk** (dt. Masse, Menge): identische Nachrichten wurden an eine nicht-triviale Anzahl von Empfängern versendet. Ab welcher Zahl von Empfängern eine Nachricht als UBE gelten kann, ist nicht definiert.
- **Commercial** (dt. gewerblich): Die E-Mail wirbt i.d.R. für kommerzielle Produkte und Dienstleistungen.

False Negative

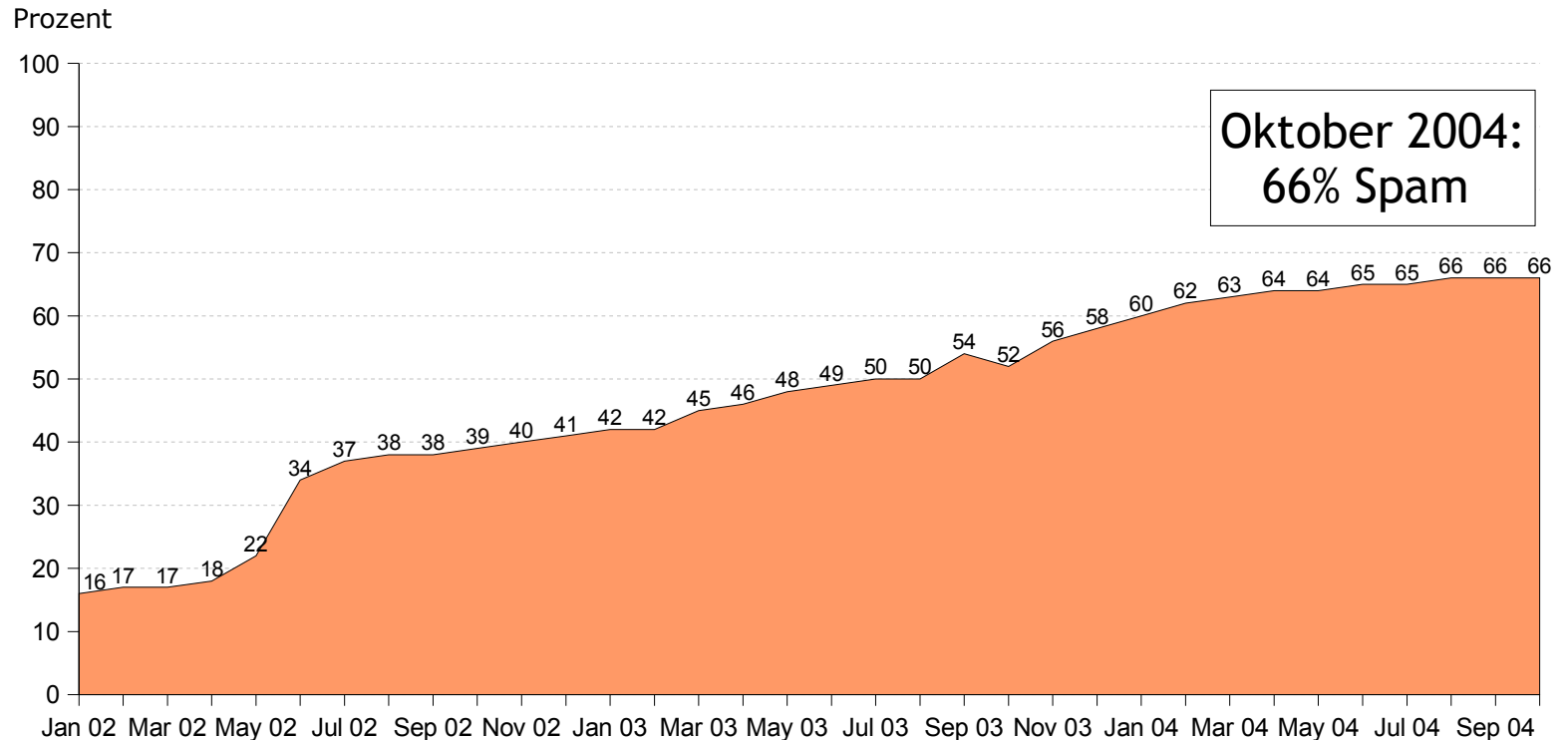
- Spam wird fälschlicherweise als legitime E-Mail (Ham) erkannt
- Problem: Spam wird an den Empfänger ausgeliefert. Dieser muss sich mit der E-Mail auseinandersetzen (löschen, Spam-Filter rekonfigurieren)
- Lösung: keine
- Argumentation: False Negatives sind akzeptabel (bei gleichzeitiger Reduzierung von False Positives gegen Null)

False Positive

- legitime E-Mail wird fälschlicherweise als Spam erkannt
- Problem: eine legitime E-Mail erreicht u.U. nicht den Empfänger (automatische Lösung) bzw. dessen unmittelbare Aufmerksamkeit (Ordner „Spamverdacht“)
- Lösungsansatz: keine automatische Löschung, ggf. keine Blockade
SMTP-Dialog: Absender erhält Fehlermeldung über Blockade
Content-Filter: Spam nur markieren
C/R-Verfahren: Absender erhält Challenge
- Argumentation: False Positives sind **inakzeptabel**

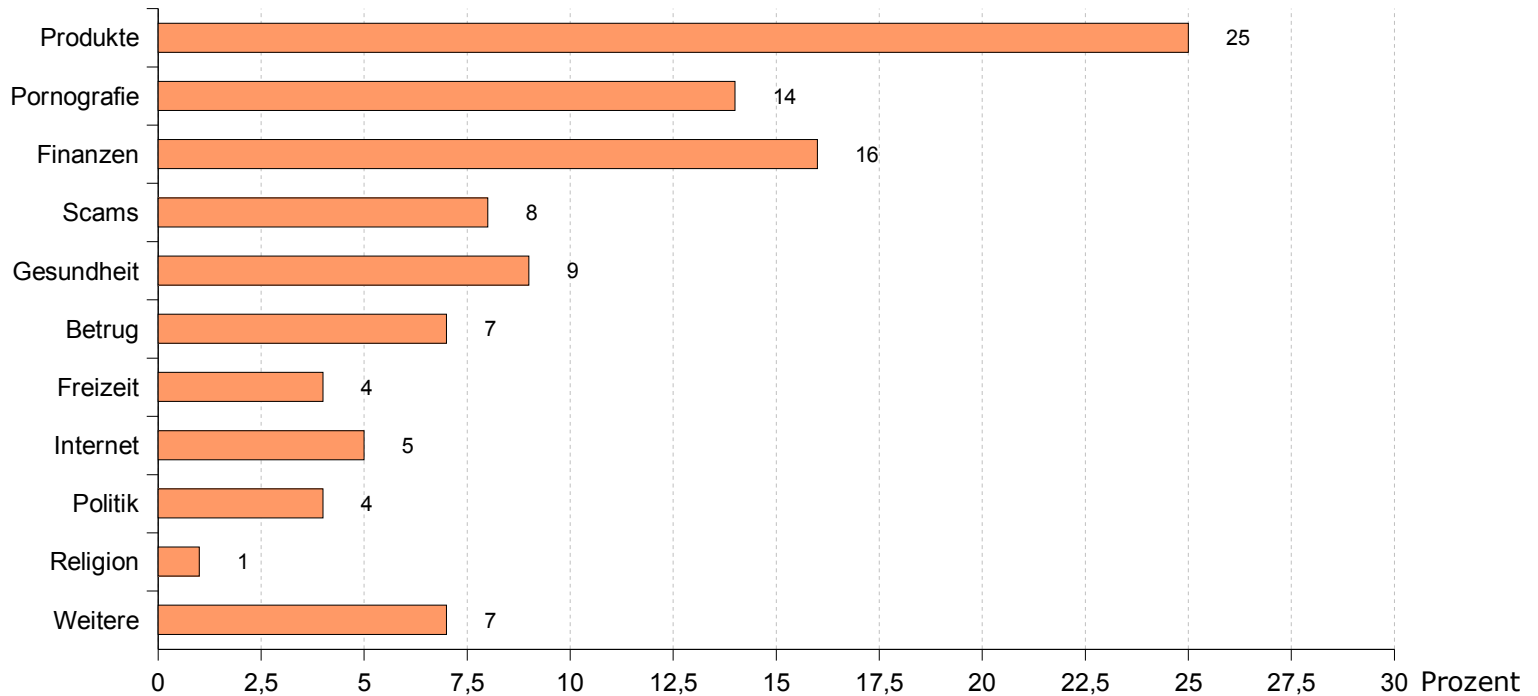
Statistiken

Zunahme von Spam



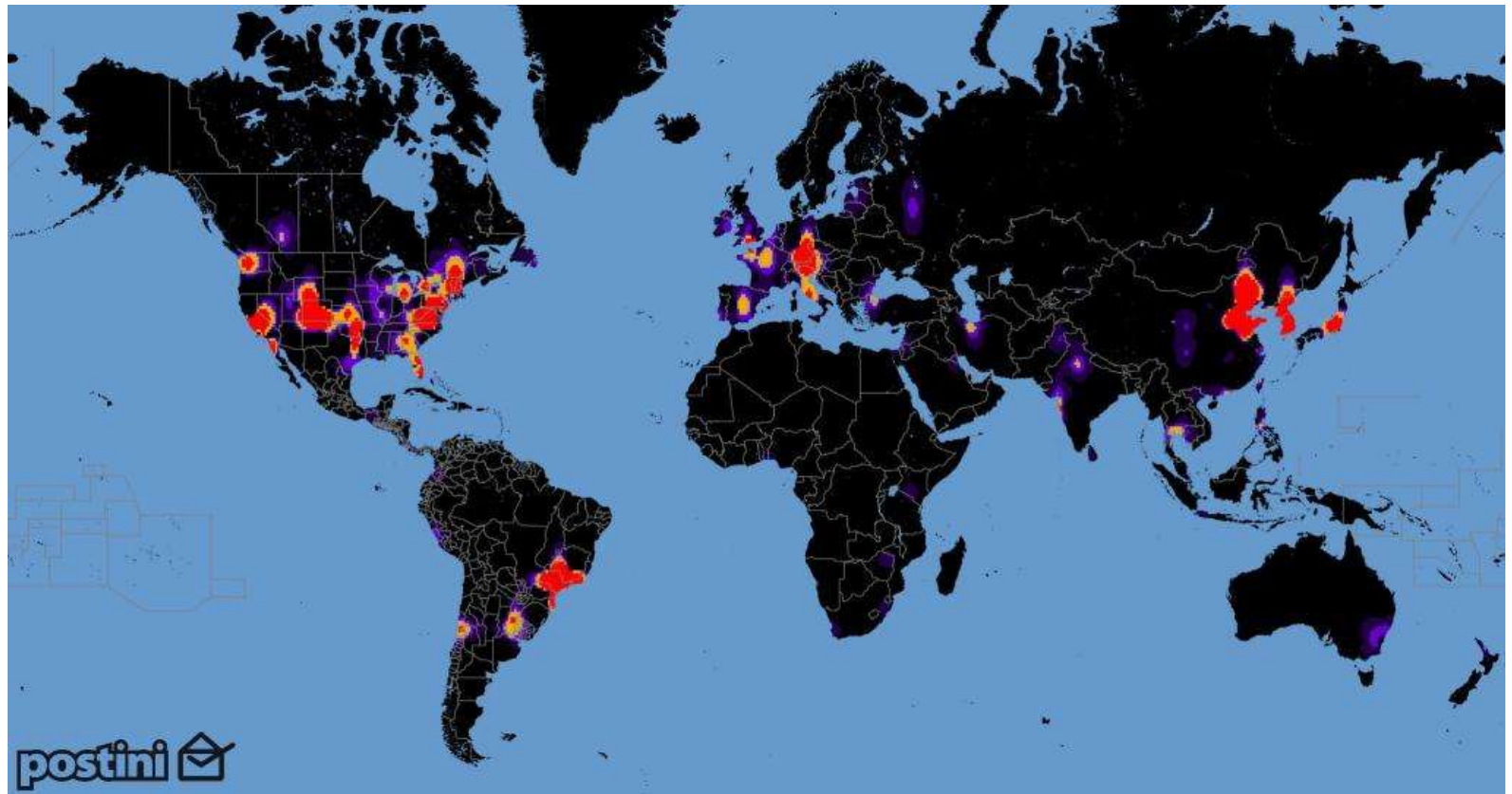
Quelle: <http://www.symantec.com/region/de/PressCenter/spam.html>

Inhalte von Spam



Quelle: <http://www.symantec.com/region/de/PressCenter/spam.html>

Herkunft von Spam



Quelle: <http://www.postini.com/stats/world-spam-2008.jpg>

Herkunft von Spam (ISPs)

1. mci.com (MCI, USA)
2. kornet.net (Kornet/KT, Korea)
3. sbc.com (SBC Communications, USA)
4. chinanet-cq (Chinanet Chongqing, China)
5. comcast.net (Comcast Cable Communications, LLC, USA)
6. above.net (AboveNet, USA)
7. chinanet-sh (Chinanet Shanghai, China)
8. xo.com (XO Communications, USA)
9. interbusiness.it (Telecom Italia, Italien)
10. level3.net (Level 3, USA)

TOP10 Worst Spam ISPs (Dec 2004)
Quelle: <http://www.spamhaus.org/>

AboveNet Customer Anti-Spam Policy

[...]

AboveNet, Inc. (AboveNet), has zero tolerance for Unsolicited Broadcast Email and Unsolicited Commercial Email (“UBE/UCE”, commonly known as “Spam”) whether originating from customers, from customers' customers, or from customers that provide services which are used to support UBE/UCE.

[...]

Quelle: <http://www.above.net/antispam.html>

Hosting von Spam-beworbenen Websites

Juni 2004

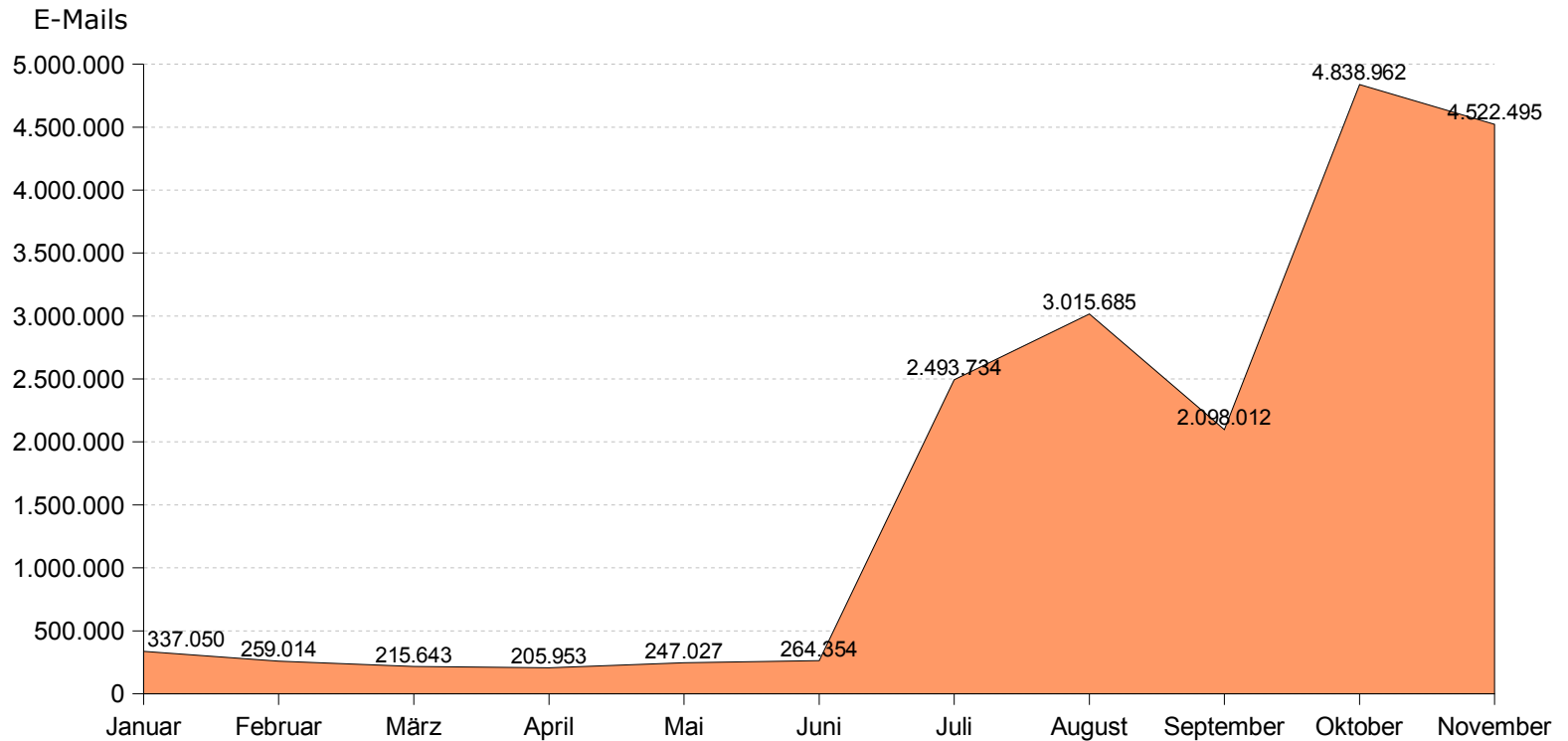
1.	China	73.58%
2.	Süd-Korea	10.91%
3.	USA	9.47%
4.	Russische Föderation	3.50%
5.	Brasilien	2.23%
6.	Argentinien	0.09%
7.	Kanada	0.06%
8.	Niederlande	0.06%
9.	Australien	0.02%
10.	Japan	0.01%

August 2004

1.	Süd-Korea	46.87%
2.	China	31.75%
3.	Brasilien	11.36%
4.	USA	9.73%
5.	Kanada	0.10%
6.	Argentinien	0.06%
7.	Russische Föderation	0.05%
8.	Großbritannien	0.01%
9.	Deutschland	0.01%
10.	Taiwan	0.01%

Quelle: <http://www.commtouch.com/news/index.2004.shtml>

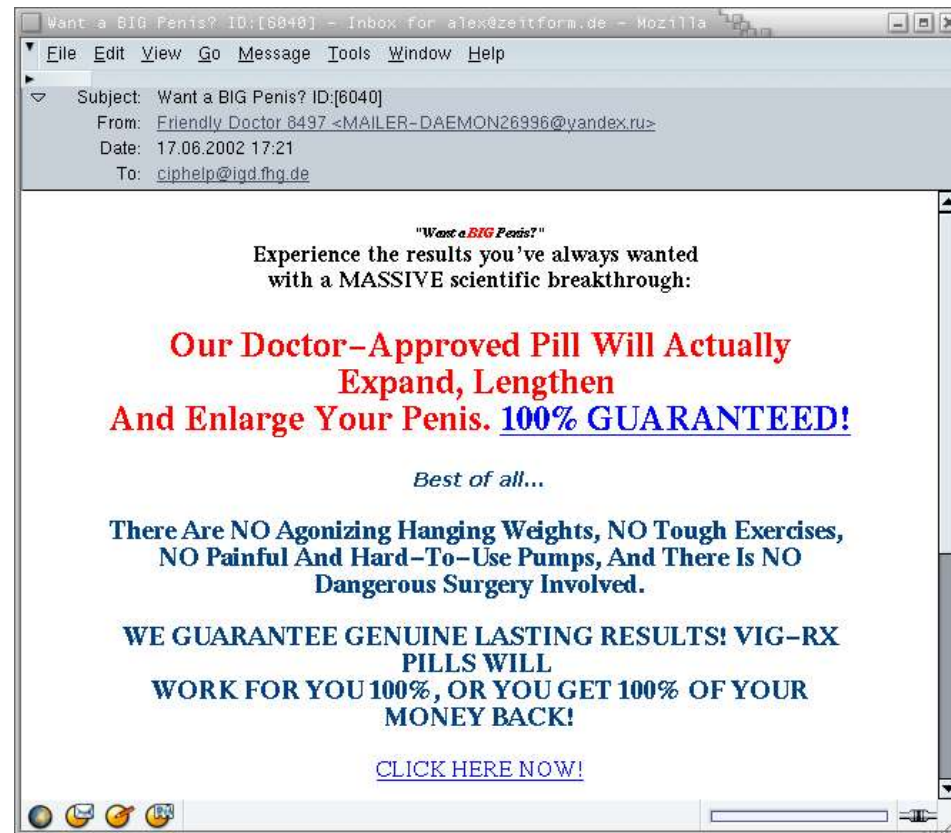
Phishing



Quelle: <http://www.message-labs.com/intelligence/2004report>

Der Versand von Spam

Die Spam E-Mail

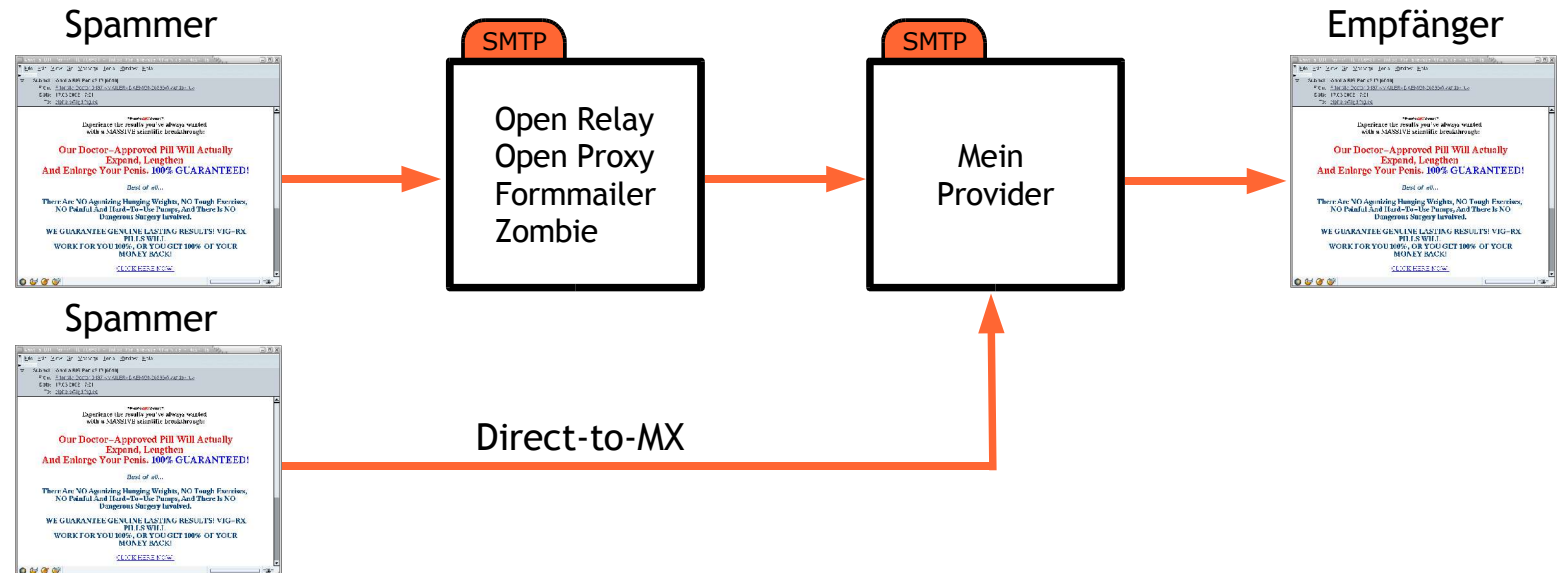


Die E-Mail im Rohformat

```
Return-Path: <MAILER-DAEMON11745@yandex.ru>
Received: from [...]
Received: from yandex.ru ([217.13.202.46]) [...]
From: "Friendly Doctor 8497" <MAILER-DAEMON26996@yandex.ru>
To: <ciphelp@igd.fhg.de>
Subject: Want a BIG Penis? ID:[6040]
Date: Mon, 17 Jun 2002 19:21:13 +0400
Mime-Version: 1.0
Content-Type: text/html; charset="ISO-8859-2"

<html>
<head>
<title>Want a BIG Penis?</title>
</head>
<body lang=RU link=blue vlink=purple style='tab-interval:35.4pt'>
[...]
</body>
</html>
```

Der Versand von Spam (SMTP)



Sicherheitsprobleme durch Spam

- Identitätsdiebstahl („Phishing“, „Scams“)
- Viren (Verbreitung über Spam-Techniken)
- Spam mit Exploits (z.B. Angriffe gegen Hotmail-Konten über JavaScript)
- Viren zum Spamversand (z.B. Sobig)

Info: <http://www.securityfocus.com/infocus/1763>

Spam-Viren

Beispiele: Mimapil, Sobig, Fizzer

- SMTP-Engine (Verbreitung und Spam-Versand)
- sammelt Adressen aus Outlook, Adressbuch, Dateien
- Joe-Job/dDoS-Angriffe gegen Anti-Spam Community
- Zugang für Fernadministration
- installiert Bots, Würmer, HTTP-Server, Proxy
- Self-Update, Umgehung Anti-Virus-Schutz

Info: <http://www.spamhaus.org/cyberattacks/index.html>

Der SMTP-Dialog

```
S: 220 mail.empfaenger.de ESMTP
C: HELO mail.yandex.ru
S: 250 mail.empfaenger.de
C: MAIL FROM: <MAILER-DAEMON26996@yandex.ru>
S: 250 ok
C: RCPT TO: <ciphelp@igd.fhg.de>
S: 250 ok
C: DATA
S: 354 go ahead
C: From: "Friendly Doctor 8497" <MAILER-DAEMON26996@yandex.ru>
C: To: <ciphelp@igd.fhg.de>
C: Subject: Want a BIG Penis? ID:[6040]
  [...]
C: .
S: 250 ok 997887680 qp 2592
C: QUIT
S: 221 mail.empfaenger.de
```

Verfügbare Informationen

- IP-Adresse des SMTP-Clients (verlässlich)
- HELO/EHLO-String: Hostname (gefälscht)
- Envelope MAIL FROM (gefälscht)
- Envelope RCPT TO (muss korrekt sein)
- Received: (gefälscht, nur teilweise verlässlich)
- From:, To:, Return-Path:, ... (gefälscht)
- Weitere Mail Header (gefälscht)
- Mail Body (Spam)

Sitzungsbasierte Strategien

Blockieren von IP-Adressen

- IP-Adresse des SMTP-Clients ist verlässlich
- SMTP-Dialog wird mit Fehler quittiert:

`451 Requested action aborted: error in processing`

`553 Requested action not taken: mailbox name not allowed`

- Statische Blacklist (z.B. durch Spam-Traps)
- DNSBL/RBL (DNS-based Blocklist, Realtime Blocklist)
- Web-Interface: <http://openrbl.org>
- Frühestmögliche Abwehr von Spam
- Nachteil: Kollateralschaden (z.B. Dial-Up Adressen)

DNS-based Blocklist

- mail-abuse.org (MAPS, kommerziell, verschiedene Listen)
- spamhaus.org (SBL/XBL/ROKSO, bekannte Spammer)
- spews.org (spam-freundliche ISPs, sehr aggressiv)
- dsbl.org (unsichere Mailsysteme)
- ~~relays.osirusoft.com (verschiedene Listen)~~
- spamcop.net (von Empfängern gemeldete Adressen)
- dnsbl.sorbs.net (Open Relays)
- ordb.org (Open Relays)
- ~~monkeys.com (verschiedene Listen)~~
- dev.null.dk (Open Relays)
- blackholes.us (spam-freundliche ISPs und Staaten)

DNS-based Blocklist

Beispiel: 69.6.27.48

```
> host -t any 48.27.6.69.sbl.spamhaus.org
48.27.6.69.sbl.spamhaus.org has address 127.0.0.2
48.27.6.69.sbl.spamhaus.org descriptive text
"http://www.spamhaus.org/SBL/sbl.lasso?query=SBL6636"
```

Beispiel: 146.140.212.1

```
> host -t any 1.212.140.146.sbl.spamhaus.org
Host not found.
```

DNS-based Blocklist

```
; spfilter magic sources: SBL,SBL (0.57_031210)
; bind zone rbl.zeitform.de.
$TTL      43200
$ORIGIN   rbl.zeitform.de.
@         SOA      rbl.zeitform.de. root.rbl.zeitform.de. (
                2003121000 10800 3600 604800 21600)
@         NS       ns.zeitform.de.
@         MX       100 mail.zeitform.de.
; test-entries
about     TXT       "zone built by spfilter/0.59 (SBL, bind, 20031210)"
2.0.0.127 TXT       "Test bind rbl.zeitform.de [146.140.212.117]"
2.0.0.127 A         127.0.0.2 ; {every dnsbl should have that}
; listed addresses
0.142.135.12 TXT "SBL http://www.spamhaus.org/SBL/sbl.lasso?query=SBL5845"
0.142.135.12 A 127.0.0.2
1.142.135.12 TXT "SBL http://www.spamhaus.org/SBL/sbl.lasso?query=SBL5845"
1.142.135.12 A 127.0.0.2
10.142.135.12 TXT "SBL http://www.spamhaus.org/SBL/sbl.lasso?query=SBL5845"
10.142.135.12 A 127.0.0.2
11.142.135.12 TXT "SBL http://www.spamhaus.org/SBL/sbl.lasso?query=SBL5845"
11.142.135.12 A 127.0.0.2
[...]
```

Envelope-Check

HELO host.domain.com

- Blacklist/Whitelist mit HELO-Strings
- Prüfung auf FQDN
- Prüfung der Domain über DNS und rDNS

MAIL FROM:<sender@domain.com>

- Blacklist/Whitelist mit Absendern/Absender-Domains
- Prüfung des Domain-Teils über DNS und rDNS
- Prüfung auf DSN (dsn.rfc-ignorant.org, MX takes bounces)
- SMTP-Verbindung zu Absender
- Sender Authentication (SPF, CallerID, DomainKeys)

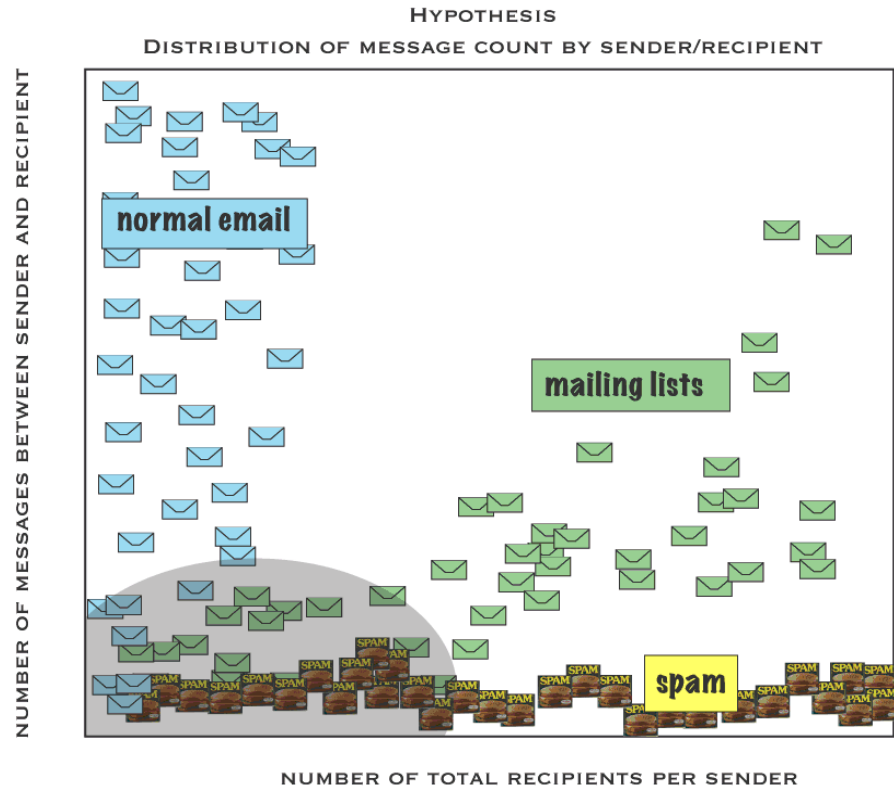
Envelope-Check

RCPT TO:<recipient@domain.com>

- Empfänger-Prüfung (SMTP-Error vs. Bounce)
- Tarpitting/Teergrubing bei mehreren (ungültigen) Empfängern

```
C: RCPT TO: <user1@domain.com>  
S: 250 ok  
C: RCPT TO: <user2@domain.com>  
S: [3 Sekunden Wartezeit] 250 ok  
C: RCPT TO: <user3@domain.com>  
S: [6 Sekunden Wartezeit] 250 ok  
C: RCPT TO: <user4@domain.com>  
S: [9 Sekunden Wartezeit] 250 ok  
C: RCPT TO: <user5@domain.com>  
S: [12 Sekunden Wartezeit] 250 ok  
...usw.
```

Grey-Listing



Quelle: <http://dumbo.pobox.com/spam-sensor/>

Grey-Listing

Annahmen:

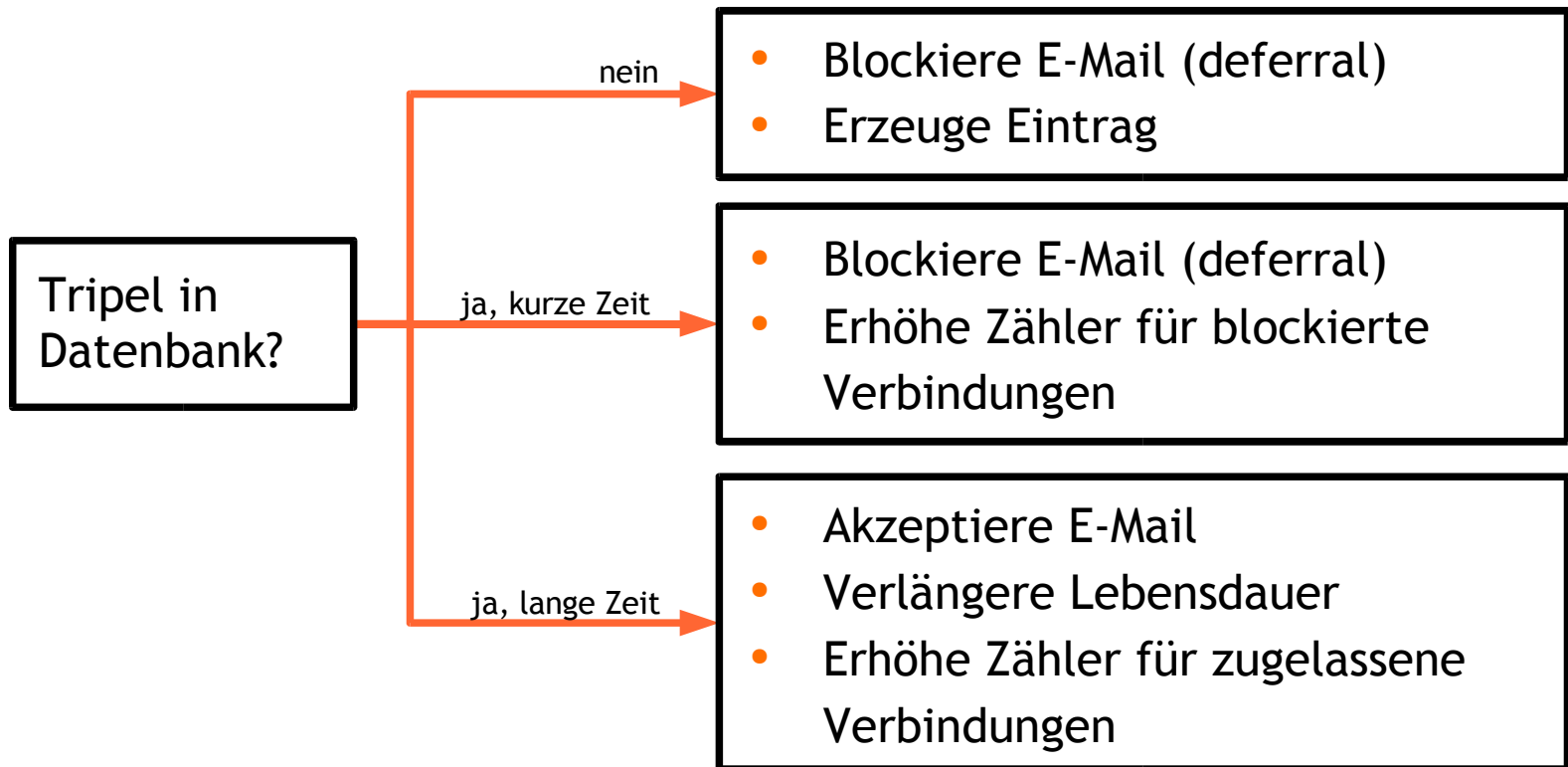
- Spammer geben den Versand von Spam nach einem Deferral auf.
- Spammer senden nicht mehrmals Nachrichten an den selben Empfänger (von der gleichen Absenderadresse)
- Spammer benutzen kein VERP (Variable Envelope Return Paths, <http://cr.yip.to/proto/verp.txt>)
- Spammer fälschen keine existierenden Absender-Adressen

Grey-Listing

Daten:

- IP-Adresse des Sender-MTA
 - Envelope Sender (`mail from:`)
 - Envelope Empfänger (`rcpt to:`)
 - Zeit der Erfassung
 - Verfallsdatum der Blockierung
 - Verfallsdatum des Eintrages
 - Anzahl geblockter Verbindungen
 - Anzahl zugelassener Verbindungen
- Tripel

Grey-Listing

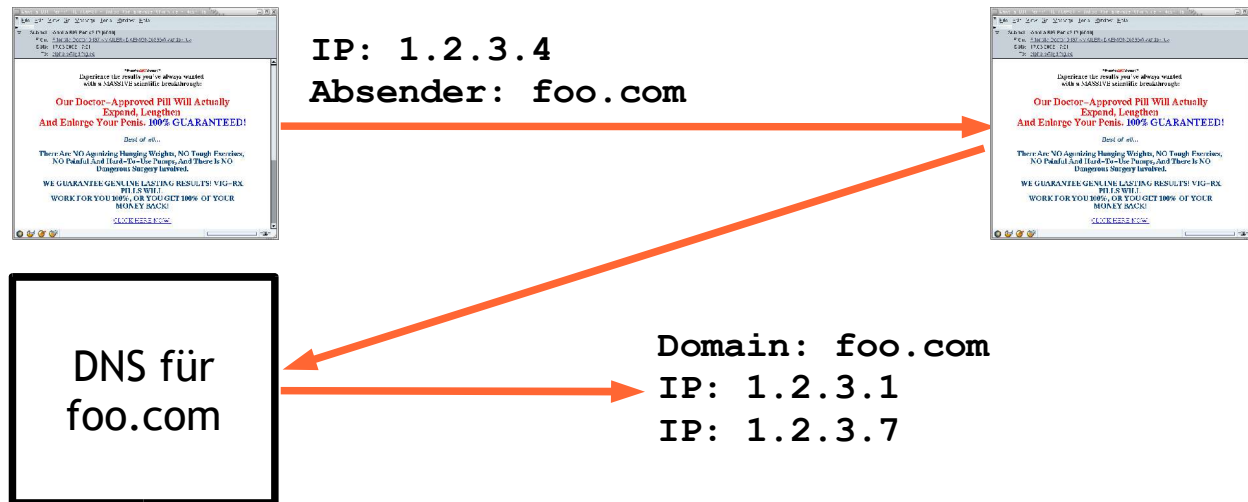


Sender Authentisierung

SPF - Sender Policy Framework

Daten:

- IP-Adresse des Sender-MTA (Client)
- Domain des Envelope Sender (**mail from:**)
- SPF-Record (DNS TXT)



SPF - Sender Policy Framework

```
example.com IN TXT "v=spf1 a mx ptr include:isp.com -all"
```

v=spf1	Versionsinformationen
a	Der Host example.com darf E-Mail versenden
mx	Die MX-Server von example.com dürfen E-Mail für die Domain @example.com versenden
ptr	Jeder Rechner dessen PTR-Eintrag auf example.com endet, darf E-Mail für die Domain @example.com versenden
include:isp.com	Jeder Rechner, der für isp.com E-Mail versenden darf, darf dies auch für @example.com
-all	niemand sonst darf E-Mail für example.com versenden

SPF - Sender Policy Framework

Nachteile:

- E-Mail-Forwarding funktioniert nicht mehr (Lösungsansatz: Sender Rewriting Scheme - SRS)
- Legitime Absender-Fälschung wird verhindert
- Erfordert Änderungen an Software und Infrastruktur (SMTP auth, MTA Software)
- Erfordert DNS TXT Einträge
- Nur teilweise erfolgreich gegen Spam (verhindert nur Absender-Fälschung, Spammer können sich anpassen)

Informationen:

- <http://spf.pobox.com>

SPF - Sender Policy Framework

Andere DNS-basierte Ansätze:

- RMX (Reverse MX)

<http://www.danisch.de/work/security/antispam.html>

- DMP (Designated Mailers Protocol)

<http://ietfreport.isoc.org/ids/draft-fecyk-dsprotocol-04.txt>

- Caller ID

http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.msp

Weitere Informationen:

- http://asrg.kavi.com/apps/group_public/documents.php

SPF - Sender Policy Framework

Beispiele:

- SPF (aol.com)

```
$ nslookup -q=txt aol.com
```

```
aol.com text = "v=spf1 ip4:152.163.225.0/24 ip4:205.188.139.0/24  
ip4:205.188.144.0/24 ip4:205.188.156.0/24 ip4:205.188.157.0/24  
ip4:205.188.159.0/24 ip4:64.12.136.0/24 ip4:64.12.137.0/24 ip4:64.12.138.0/24  
ptr:mx.aol.com ?all"
```

- Caller ID (microsoft.com)

```
$ nslookup -q=txt _ep.microsoft.com
```

```
_ep.microsoft.com text = "<ep xmlns='http://ms.net/1' testing='true'><out><m>  
"<mx/><a>213.199.128.160</a><a>213.199.128.145</a><a>207.46.71.29</a><a>194.121.  
59.20</a><a>157.60.216.10</a><a>131.107.3.116</a><a>131.107.3.117</a><a>131.107.  
3.100</a>" "</m></out></ep>"
```

Sender-ID

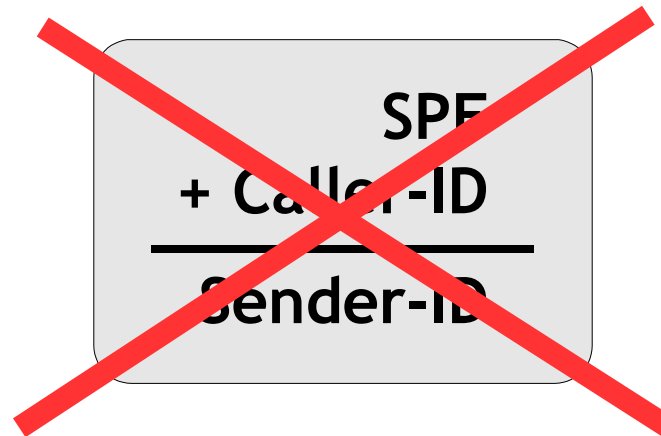
**SPF
+ Caller-ID**

Sender-ID

Weitere Informationen:

- http://www.theregister.co.uk/2004/07/05/sender_authentication/
- <http://www.heise.de/newsticker/meldung/48679>
- <http://download.microsoft.com/download/d/a/2/da2821f5-6acb-4058-8974-5a3c7d187794/senderid.pdf>

Sender-ID



Sept. 2004: Standardisierungsverfahren scheitert

Weitere Informationen:

- <http://www.heise.de/newsticker/meldung/51379>

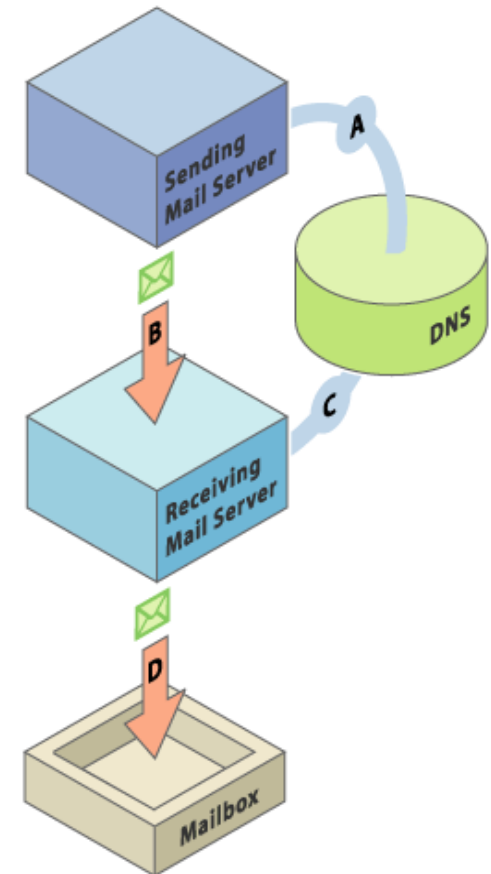
Yahoo DomainKeys

Absender

- A: Domain-Eigner erzeugt Schlüsselpaar (public für DNS, private für Mail Server)
- B: Mail Server signiert authorisierte ausgehende E-Mails und erzeugt Header

Empfänger

- C: MTA liest Signatur aus E-Mail und lädt zur Verifikation den Public-Key der Absender-Domain über das DNS.
- D: E-Mails verifizierter Domains werden ausgeliefert



Quelle: <http://antispam.yahoo.com/domainkeys>

Yahoo DomainKeys

Beispiele:

- E-Mail-Header

```
DomainKey-Signature: a=rsa-sha1 s=brisbane; d=example.net; c=simple; q=dns;  
b=dzdVyOfAKCdLXdJOc9G2q8LoXS1EniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR;
```

- DNS-Eintrag

```
brisbane._domainkey IN TXT "g=; k=rsa; p=MEwwDQYJKoZIhvcNAQEBBQADAwAwOAIxAj  
khKcmScryT1yCL8XgHM+o9wfSsLS18KZTW3  
kYBTLhOWOiAzcGCncF37dJQYH2sQQIDAQAB"
```

Weitere Informationen:

<http://antispam.yahoo.com/domainkeys>

<http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-00.txt>

Inhaltsbasierte Strategien

E-Mail-Analyse-Verfahren

- Typische Formulierungen im Betreff der E-Mail
- Typische Formulierungen im Body der E-Mail
- Typische Eigenschaften der E-Mail
- Mit Spam in Verbindung stehende Body URIs
- Checksummen-Verfahren (Razor, DCC, Pyzor)
- DNSBL/RBL-Prüfung der Received-Header
- Statistische Verfahren (Bayes)
- Absender in Whitelist/Blacklist

Typische Formulierungen für Spam

- „Viagra“, „Big Boobs“, „larger penis“, „ Impotence cure“
- „XXX Photos“, „Instant Access“, „Amateur Porn“
- „click here“, „for free“, „call now“, „unsubscribe“
- „Senate Bill 1618“, „This is not spam“, „opt-in“
- „Million Dollars“, „check or money order“, „pure profit“
- „University Diplomas“, „Toner Cartridge“, „Free DVD“
- „As seen on national TV!“, „No Medical Exams“
- „International driving license“, „NIGERIAN BANK“
- „gratis“, „Gewinnspiel“, „Hausfrauensex“, „Pu-Erh-Tee“
- „ist kein Spam“, „JETZT“, „seriös“, „anonym“, „abmelden“
- „ohne dialer“, „Sonderaktion“, „Vorteile sichern“

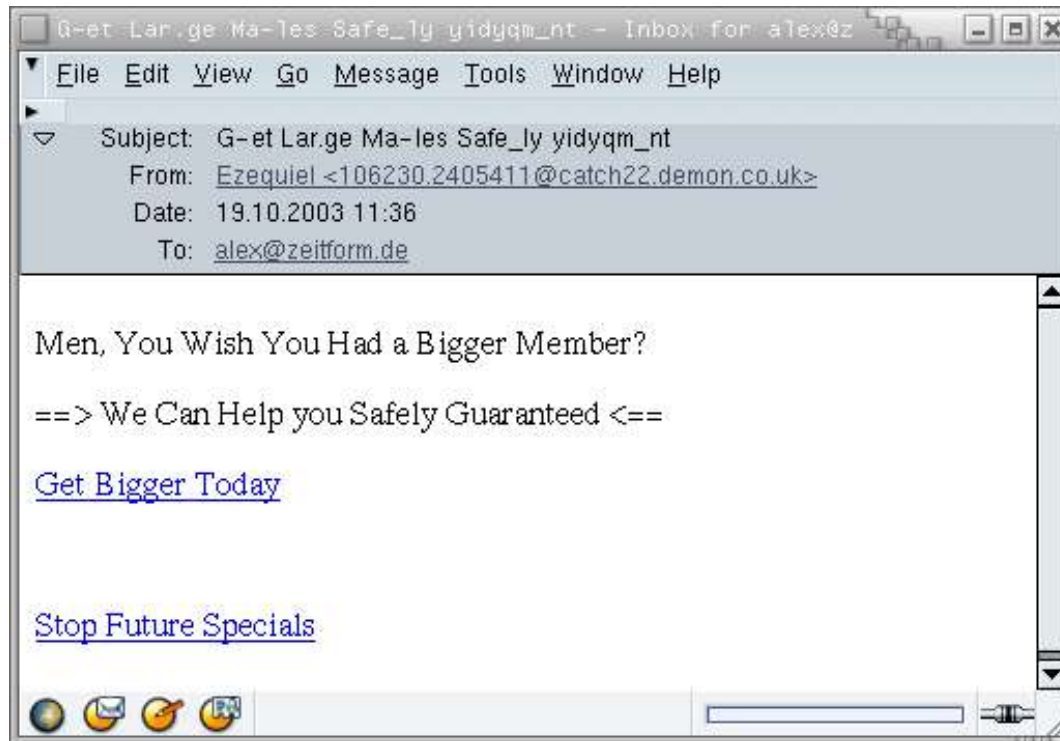
Typische Eigenschaften für Spam

- G.a.p.p.y T.e.x.t, GROSSBUCHSTABEN, Leerraum
- Fehlendes oder falsches Datum
- Gefälschter User-Agent oder X-Mailer
- Hinweise auf Spam-Tools
- Text ist base64-kodiert
- HTML-Mail mit font-Tags (size, color)
- HTML-Mail mit Bild(ern) und wenig/keinem Text
- HTML-Mail mit großgeschriebenen Tags
- HTML-Mail mit IP-Adressen oder Escaping in URLs
- ASCII-Formular [_____]
- Text enthält wirre Zeichenfolgen fgtrt asdftr sfsdf dgd
- Received-Header sind gefälscht

Typische Eigenschaften legitimer E-Mail

- PGP-Signatur, Habeas Warrant Mark
- Text enthält Zitate „>”
- Gültiger User-Agent oder X-Mailer
- Eigenschaften von Mailinglisten-Software (majordomo)
- Vorhandene Signatur („-- ”)
- Nachricht von Mailer-Daemon
- Hotmail- oder MSN-Footer
- In-Reply-To Header
- Stamp (z.B. Hashcash)

Text-Analyse



Links: <http://www.getonitnow665.biz/bgite/>, <http://shapeisgood55.biz/re.php>

Text-Analyse

From: Ezequiel <106230.2405411@catch22.demon.co.uk>
Subject: G-et Lar.ge Ma-les Safe_ly yidyqm_nt
To: <alex@zeitform.de>

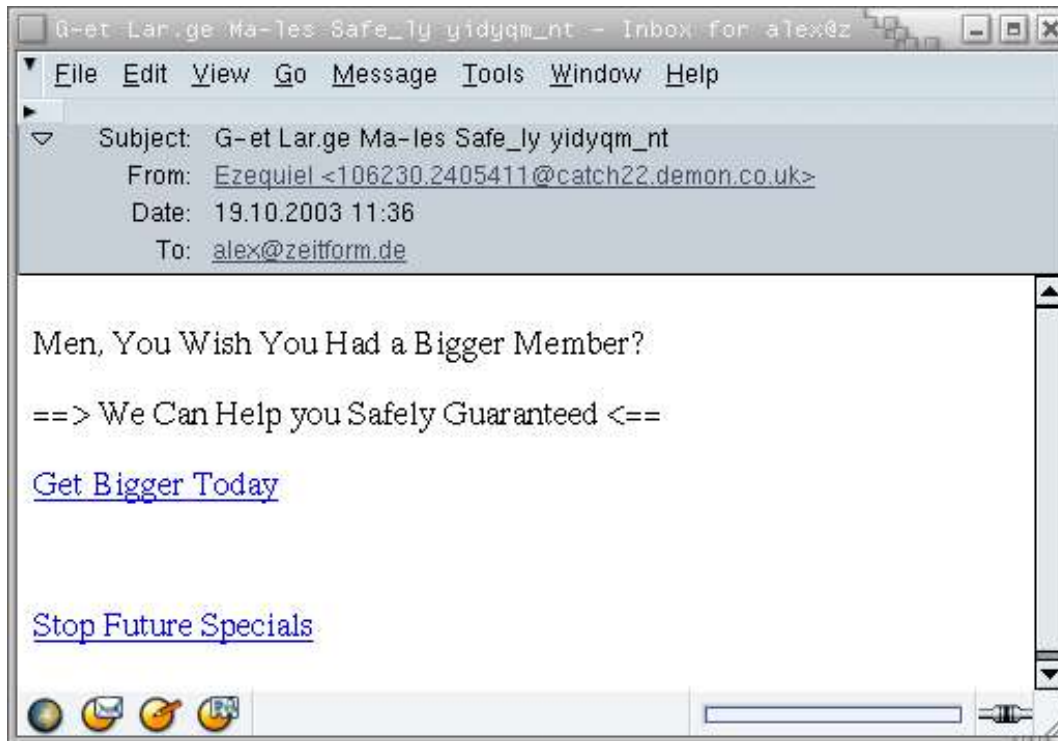
```
<html><body><font color=white>other writings whatsoever: because
the subject where of they</font><br>Me<EauH>n, Yo<WuV>u Wi<my>sh
Yo<Jlo>u Ha<Yz>d a<mB> Big<xiea>ger Mem<Mu>ber?<br><br>=<eZTN>=>
W<ZjK>e Ca<jbtj>n He<Qx>lp yo<ftzP>u Saf<k>ely Guara<ner>nteed
<<MKm>==<br><font color=white>Land and Conseil were slyly watching
some of the ship's crew,</font><Br><a
href="http://&#119;ww.g&#101;&#116;onit&#110;&#111;&#119;6&#54;&#5
3;&#46;biz/b&#103;&#105;t/">G<w>et Big<XLA>ger To<TGvp>day</a>
<br><br><br><br><a
href="http://s&#104;apei&#115;&#103;o&#111;&#100;5&#53;. &#98;&#105
;z/r&#101;. &#112;&#104;&#112;">St<vTS>op Fut<MEzL>ure
Spec<xR>ials</a><br><font color=white>To say that he risked his
life twenty times before reaching</font>
</html></body>
```

Text-Analyse

From: Ezequiel <106230.2405411@catch22.demon.co.uk>
Subject: G-et Lar.ge Ma-les Safe_ly yidyqm_nt
To: <alex@zeitform.de>

```
<html><body><font color=white>other writings whatsoever: because  
the subject where of they</font><br>Me<EauH>n, Yo<WuV>u Wi<my>sh  
Yo<Jlo>u Ha<Yz>d a<mB> Big<xiea>ger Mem<Mu>ber?<br><br>=<eZTN>=  
W<ZjK>e Ca<jbtj>n He<Qx>lp yo<ftzP>u Saf<k>ely Guara<ner>nteed  
<<MKm>==<br><font color=white>Land and Conseil were slyly watching  
some of the ship's crew,</font><Br><a  
href="http://&#119;ww.g&#101;&#116;onit&#110;&#111;&#119;6&#54;&#5  
3;&#46;biz/b&#103;&#105;t/">G<w>et Big<XLA>ger To<TGvp>day</a>  
<br><br><br><br><a  
href="http://s&#104;apei&#115;&#103;o&#111;&#100;5&#53;. &#98;&#105  
&#112;&#104;&#112;">St<vTS>op Fut<MEzL>ure  
Spec<xR>ials</a><br><font color=white>To say that he risked his  
life twenty times before reaching</font>  
</html></body>
```

Body URIs



Links: <http://www.getonitnow665.biz/bg1/>, <http://shapeisgood55.biz/re.php>

Body URIs

- Links, Bilder, Skripte im Body von Spam
- Body URIs sollten verlässlich sein
- Kollateralschäden möglich

Beispiele:

- Filters That Fight Back (Paul Graham)
`http://www.paulgraham.com/ffb.html`
- SURBL (RHSBL analog DNSBL, vgl. auch rfc-ignorant.org)
`http://www.surbl.org`

Body-URIs (RHSBL)

Beispiel: best-meds.net

```
> host -t any best-meds.net.ws.surbl.org
best-meds.net.ws.surbl.org has address 127.0.0.2
best-meds.net.ws.surbl.org descriptive text "Blocked,
See: http://www.stearns.org/sa-blacklist/"
```

Beispiel: zeitform.de

```
> host -t any zeitform.de.ws.surbl.org
Host not found.
```

Body-URIs (ThrowAway-Domains)

Body-URI	IP-Adresse	Reg.-Datum	“Registrar”	DNS-Server
liberatrixit.info	218.30.21.63	15.11.2004	Gregory Cox	211.158.15.58
klagenfurter.info	222.170.97.22	15.11.2004	Gregory Cox	211.158.15.58
tunguskaye.info	219.153.9.5	15.11.2004	Gregory Cox	211.158.15.58
sergestuser.info	218.30.21.63	15.11.2004	Gregory Cox	211.158.15.58
jorgenseny.info	218.30.21.63	21.11.2004	Kris Linder	211.158.15.58
lexellmer.info	218.30.21.63	21.11.2004	Kris Linder	211.158.15.58
toyamer.com	218.30.21.63	21.11.2004	Kris Linder	211.158.15.58
valeriores.com	218.30.21.63	21.11.2004	Kris Linder	211.158.15.58
lassovszky.com	218.7.120.81	21.11.2004	Kris Linder	211.158.15.58
philnicholsony.net	218.7.120.81	21.11.2004	Kris Linder	211.158.15.58
seeligeria.com	218.7.120.81	28.11.2004	Albert Jones	211.158.15.58
katrianne.info	218.7.120.81	28.11.2004	Albert Jones	211.158.15.58
onlymypascal.info	219.153.9.5	28.11.2004	Albert Jones	211.158.15.58
prokne.info	218.7.120.81	28.11.2004	Albert Jones	211.158.15.58
oberammergaus.com	218.7.120.81	28.11.2004	Albert Jones	211.158.15.58
mymohler.info	219.153.9.5	28.11.2004	Albert Jones	211.158.15.58
myvizbor.info	218.7.120.81	28.11.2004	Albert Jones	211.158.15.58
lagrula.com	218.7.120.81	28.11.2004	Albert Jones	211.158.15.58
chrisnell.info	219.153.9.5	28.11.2004	Albert Jones	211.158.15.58
archilochosen.com	219.153.9.5	28.11.2004	Albert Jones	211.158.15.58

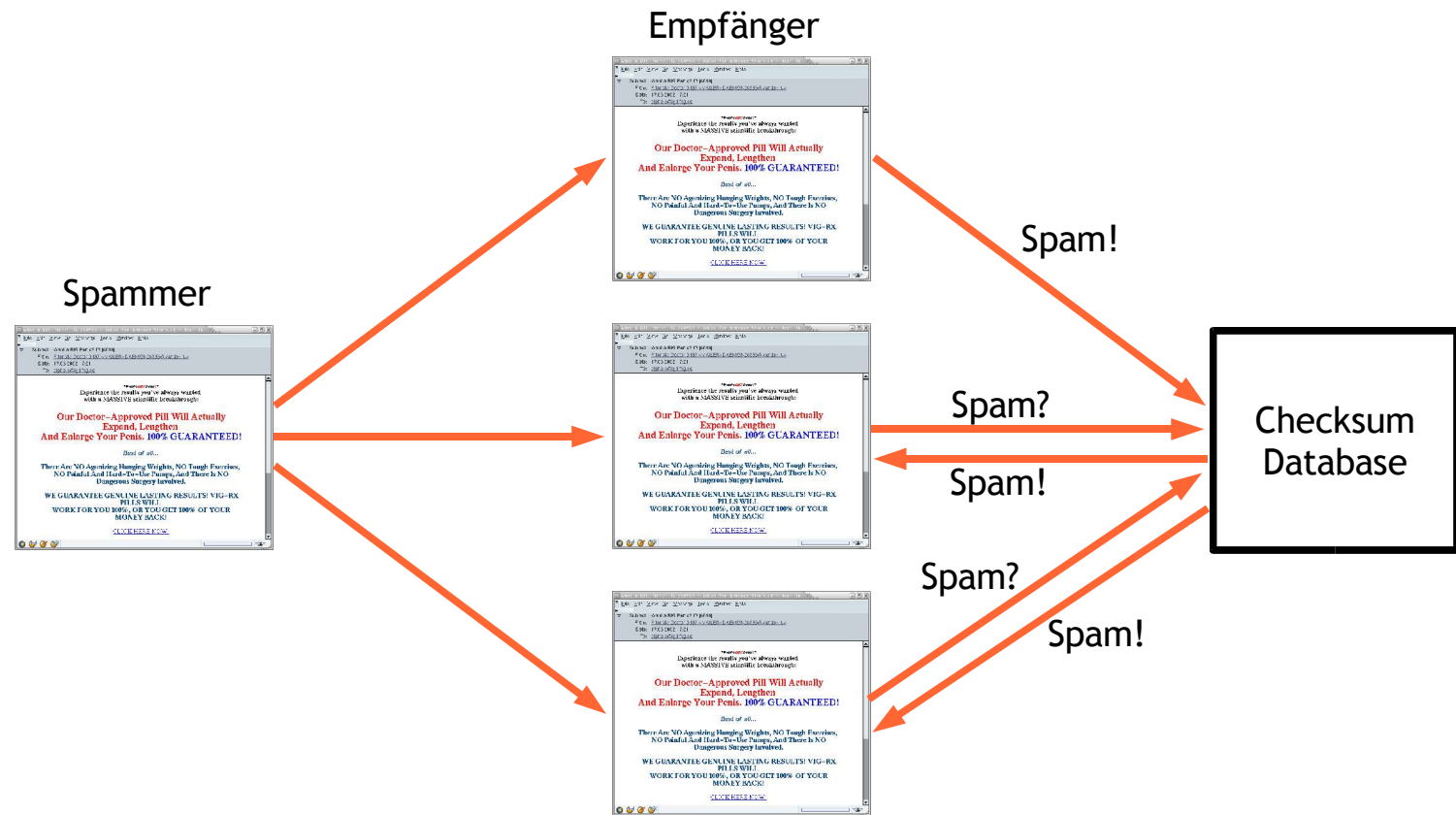
Beispiele aus Spam (27.11.04 -06.12.04)

Checksummen-Verfahren

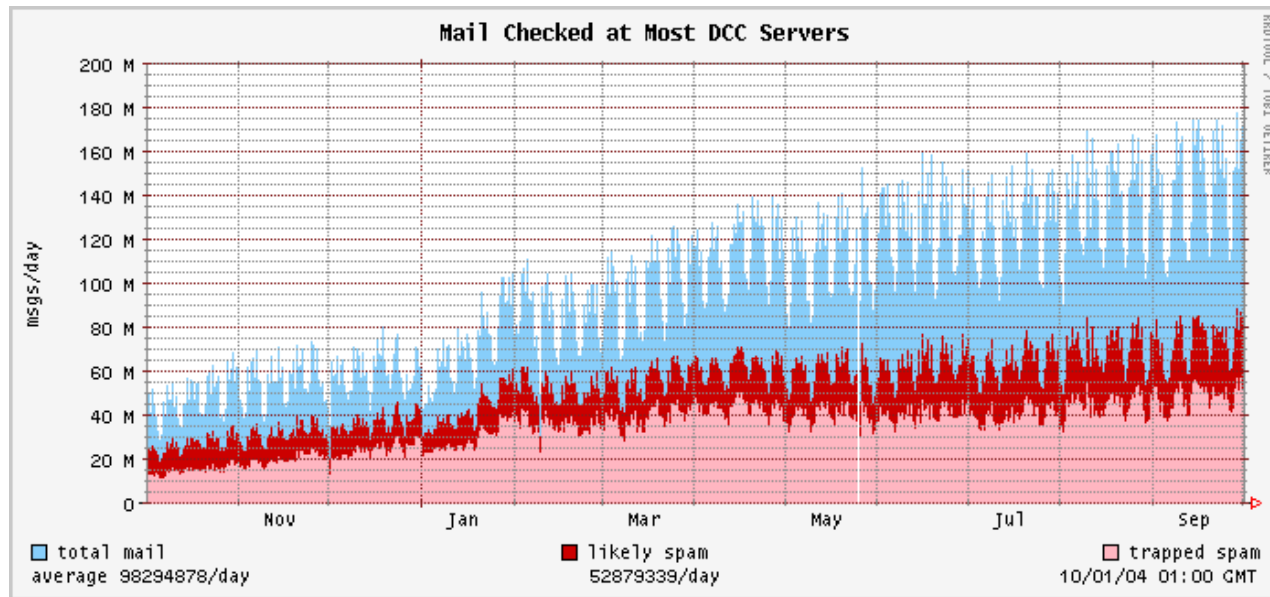
- DCC: <http://www.rhyolite.com/anti-spam/dcc/>
- Vipul's Razor: <http://razor.sourceforge.net/>
- Pyzor: <http://pyzor.sourceforge.net/>

- Öffentliche Datenbanken mit Fuzzy-Checksummen gemeldeter oder gefangener Spam-Mails
- Fuzzy-Checksummen-Algorithmen liefern bei geringen textuellen Änderungen gleichen Wert
- zusätzlicher Netzwerk-Verkehr für Abfrage

Checksummen-Verfahren



Checksummen-Verfahren



Quelle: <http://www.rhyolite.com/anti-spam/dcc/graphs/>

Razor2-Spam-Report

```
S: sn=N&srl=76&ep4=7542-10&a=1&a=cg
C: cn=razor-agents&cv=2.36
C: a=ai&cn=razor-agents&cv=2.36&user=alex%40zeitform.de
S: achal=gjiSrhu4_k_O3sCjulPKaIDNqaiX
C: a=auth&aresp=3WcztoZWFGU9GXF2PXh16SRMuSkA
S: res=1
C: -a=r&e=1&s=-kG19hd7RAXdxQB3NyQ8ZQ2_t9kA
C: a=r&e=4&ep4=7542-10&s=WkYZN7tIo2L_hrh5P-n5VFViVygA
C: a=r&e=4&ep4=7542-10&s=Imf__1UeBM3RhgTO_YRIW7v580UA
C: .
S: -res=1
S: err=230
S: err=230
S: .
C: -a=r&message=*
C: From joseph_ajakaiye@yahoo.com Wed Oct 8 11:40:46 2003
C: [...]
C: .
S: res=1
C: a=q
```

Razor2-Spam-Abfrage

Spam

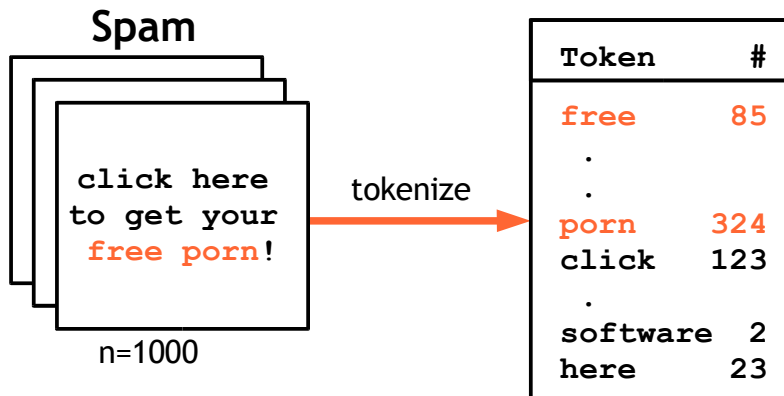
```
S: sn=C&sr1=72&ep4=7542-10&a=1  
C: a=c&e=4&ep4=7542-10&s=on7BdUVy4eW2TDWvVNpLfw1RUcoA  
S: p=1&cf=100  
C: a=q
```

Kein Spam

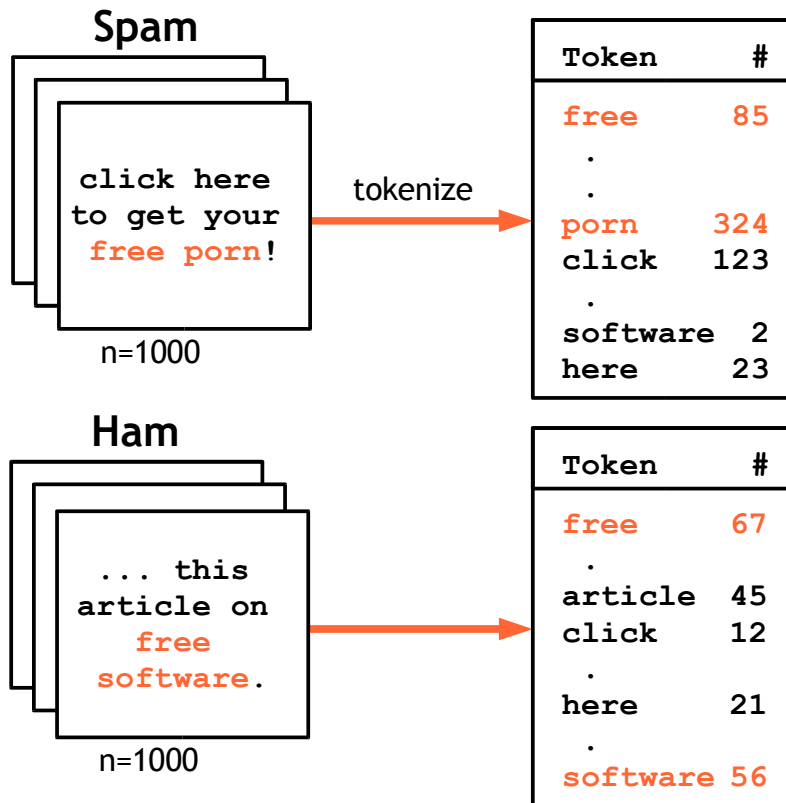
```
S: sn=C&sr1=72&ep4=7542-10&a=1  
C: a=c&e=4&ep4=7542-10&s=Id8u8ofcEDyRUht2D9DP6rMdlxYA  
S: p=0  
C: a=q
```

Info: <http://www.stearns.org/razor-caching-proxy/razor2-protocol>

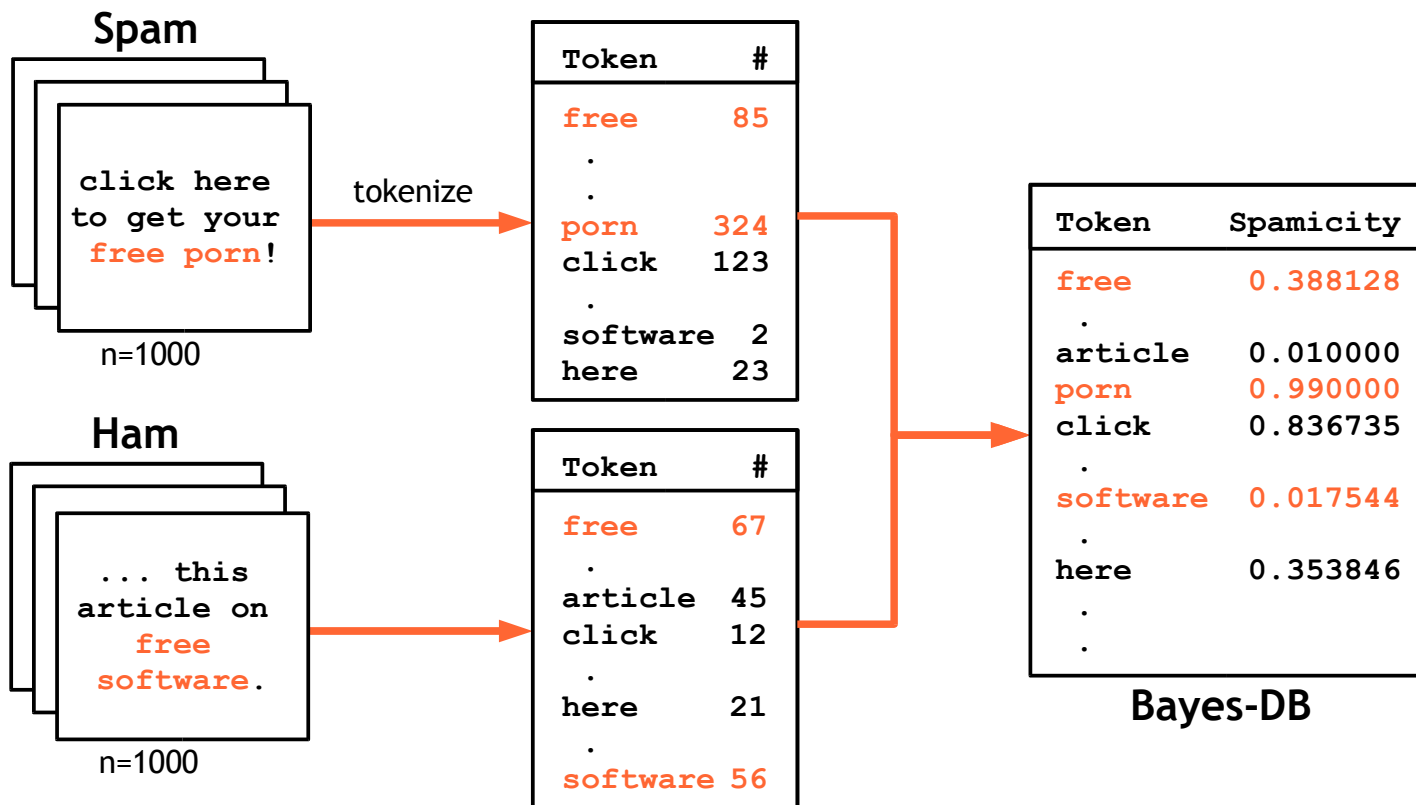
Bayes-Verfahren - Lernphase



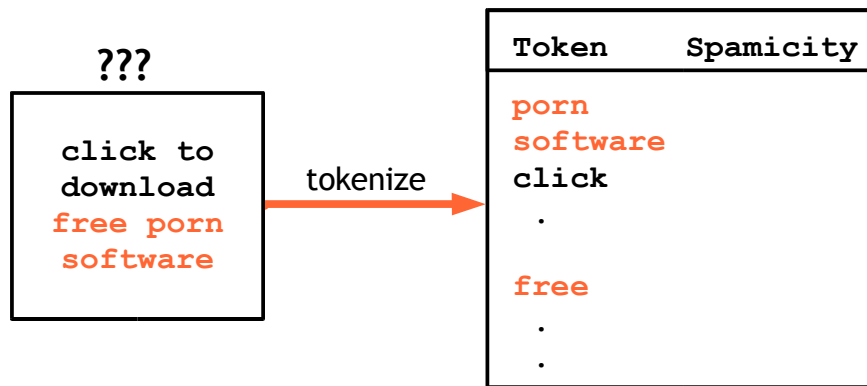
Bayes-Verfahren - Lernphase



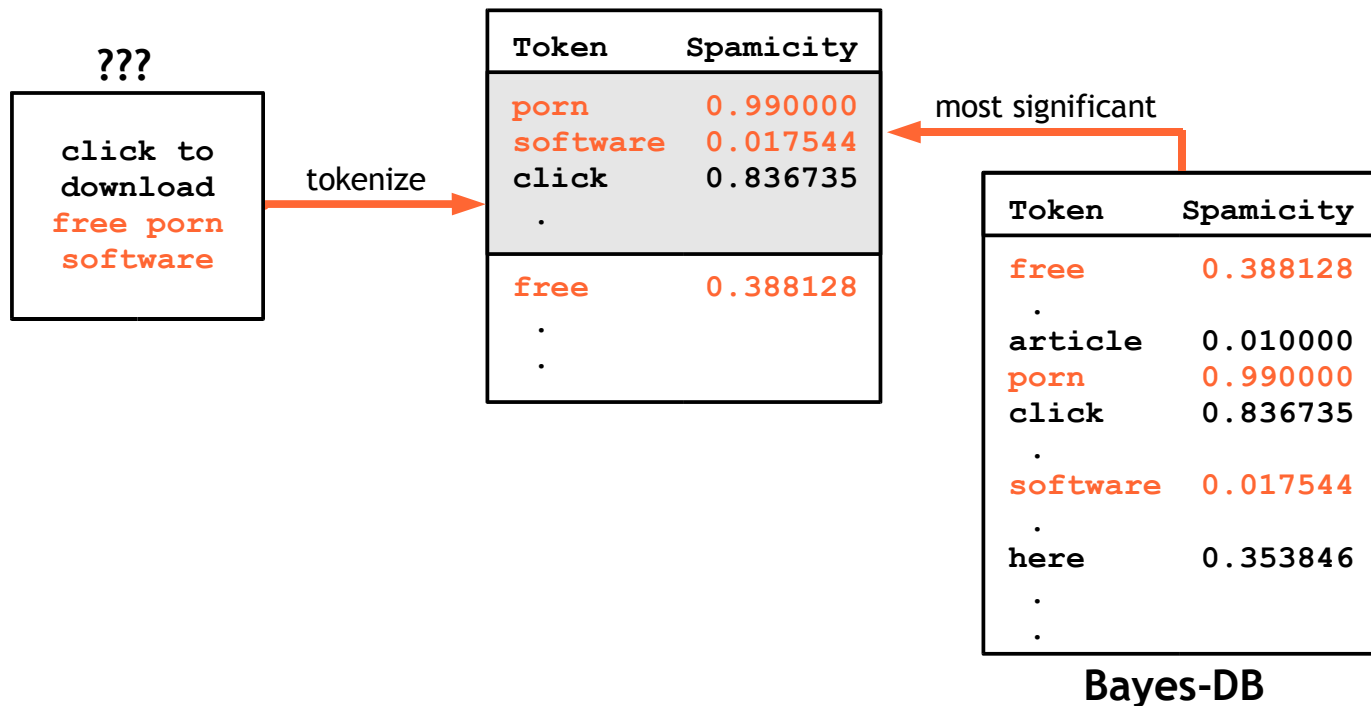
Bayes-Verfahren - Lernphase



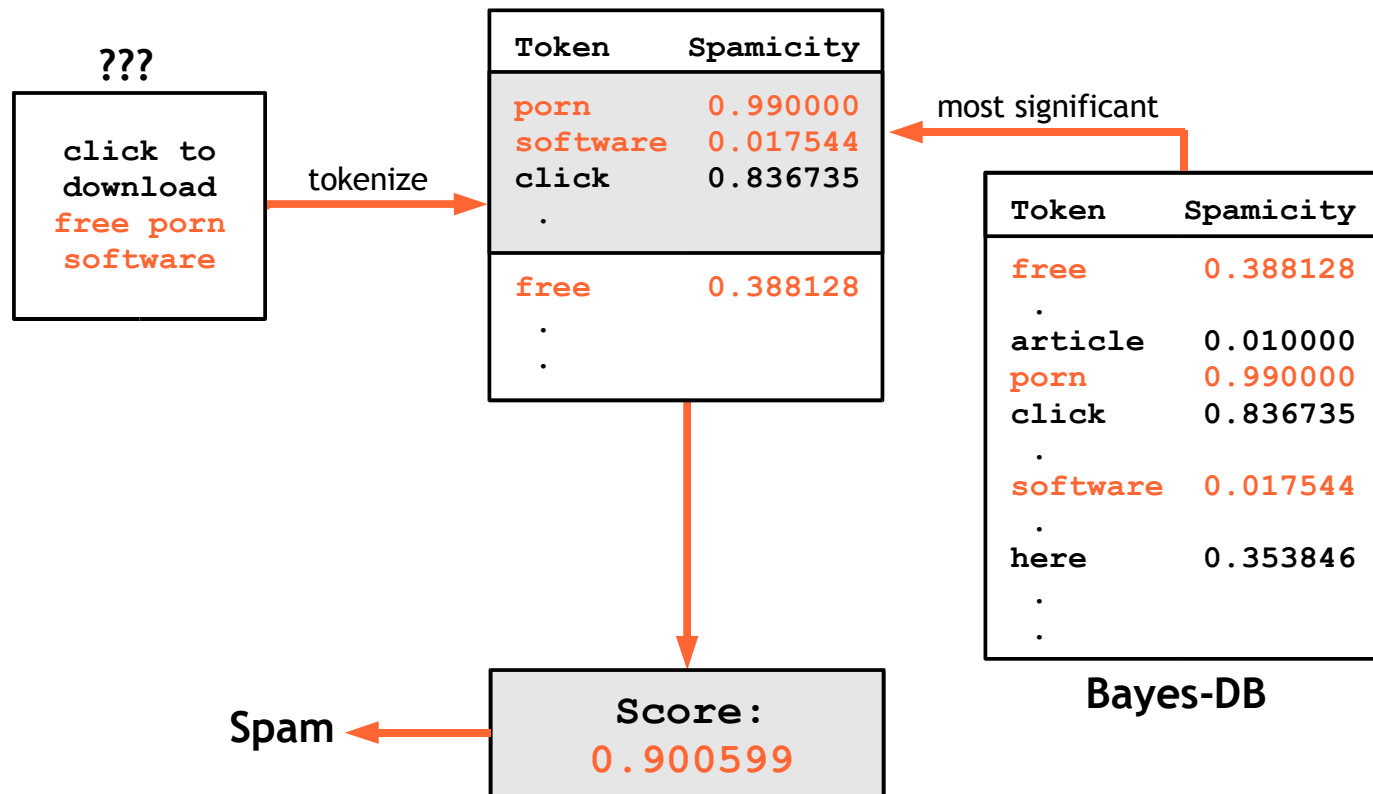
Bayes-Verfahren - Auswertungsphase



Bayes-Verfahren - Auswertungsphase



Bayes-Verfahren - Auswertungsphase



SpamAssassin

- <http://www.spamassassin.org/>
- Header Analyse
- Text Analyse
- Auto-Whitelist
- Bayes-Filter
- DNSBL, RHSBL
- Razor, Pyzor, DCC
- erweiterbar durch eigene Regeln
(<http://www.rulesemporium.com/>)
- Plugins
- flexible MTA Unterstützung
- Freie Software (Artistic License, APL seit Version 3.0.0)

SpamAssassin



SpamAssassin

X-Spam-Report:

- * 2.6 LOSE_POUNDS Subject talks about losing pounds
- * 0.6 J_CHICKENPOX_34 BODY: {3}Letter - punctuation - {4}Letter
- * 2.9 BANG_EXERCISE BODY: Talks about exercise with an exclamation!
- * 2.4 ALL_NATURAL BODY: Spam is 100% natural?!
- * 0.1 HTML_MESSAGE BODY: HTML included in message
- * 0.3 HTML_FONT_BIG BODY: HTML has a big font
- * 1.1 RAZOR2_CF_RANGE_51_100 BODY: Razor2 gives confidence between 51 and 100 [cf: 100]
- * 5.4 BAYES_99 BODY: Bayesian spam probability is 99 to 100%
- * 0.3 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
- * 0.1 HTML_50_60 BODY: Message is 50% to 60% HTML
- * 0.1 HTML_FONTCOLOR_RED BODY: HTML font color is red
- * 3.0 BigEvilList_193 URI: Generated BigEvilList_193
- * 1.0 RAZOR2_CHECK Listed in Razor2 (<http://razor.sf.net/>)
- * 2.9 DCC_CHECK Listed in DCC (<http://rhyolite.com/anti-spam/dcc/>)
- * 2.0 DATE_IN_FUTURE_06_12 Date: is 6 to 12 hours after Received: date
- * 2.6 RCVD_IN_DYNABLOCK RBL: Sent directly from dynamic IP address [218.237.156.173 listed in dnsbl.sorbs.net]
- * 0.7 PLING_PLING Subject has lots of exclamation marks

SpamAssassin

```
X-Spam-Contact: Please contact postmaster@zeitform.de [...]  
X-Spam-Flag: YES  
X-Spam-Checker-Version: SpamAssassin 2.63-zeitform_1.11 (2004-01-11)  
on mail.zeitform.de  
X-Spam-Level: *****  
X-Spam-Status: Yes, hits=28.2 required=8.0 tests=[...] autolearn=spam  
version=2.63-zeitform_1.11  
X-Spam-Report: [...]
```

Gegenmaßnahmen der Spammer

- Word-Filter: Variationen der Schreibweise
"viagra", "Vlagra", "\/iaagra", "V|@gra"
- Checksummen-Verfahren: Einfügen von individuellen Zufallszeichen in jede E-Mail

```
<!--20fqw4PJGuTimom--><a href="http://www.eewc4d.com"></a>
```
- Bayes-Filter: Einfügen zufälliger Wörter und Sätze (bayes-poison)

```
</html> jason contingent sweetleaf unstored befallen unfledged unglue springing cementum firstclass stimulus loudness drained
```

Vermeidungs- strategien

Empfänger-Verifikation

- Unsubscribe-Mail

For removal hit reply and put "Remove" in subject line

- „Click here“-Link

```
<a href="http://spammer.com/?id=your-email">Click here!</a>
```

- Unsichtbare Links

```

```

```

```

```
<iframe src="http://spammer.com/?id=your-email"></iframe>
```

```
<script language="JavaScript">...</script>
```

Empfänger-Verifikation

- Beispiel:

```

```

kriirccfix-ufdivx

tarrallorg-domreg (ROT17)



Adress-Sammler

- UseNet, Mailinglisten, Webseiten, Whois
- Online- und Offline-Formulare, Promotion
- Ident Daemon, Finger Daemon, IRC, Chat
- Web Browser (anon FTP, JavaScript, HTTP_FROM)
- AOL Profile (AOL Nutzer = Primärziele)
- „Yellow Pages“ (hotmail → bigfoot)
- Raten/Wörterbuchattacke
- Rechnerzugriff, Viren, Netzüberwachung, Social Engineering

Info: <http://www.private.org.il/harvest.html>

Schutz vor Adress-Sammlern

- Verzicht auf Veröffentlichung der eigenen Adresse
- Adresse in Grafik einbetten (ganz/teilweise)

```
alex @ zeitform.de
```

- Adresse ausschreiben

```
alex at zeitform dot de, alex@zeitform.de-NOSPAM
```

- HTML-Entities, URL-Encoding

```
alex&#064;zeitform.de, alex%40zeitform.de
```

- JavaScript

```
<script language="JavaScript">  
  var Mailme = "alex@" + "zeitform.de";  
  document.write('<a href="mail" + 'to:' + Mailme + '>');  
  document.write(Mailme + '</a>');  
</script>
```

Adress-Sammler entdecken

- Verwendung einmaliger Adressen bzw. Erweiterungen
`alex+spamtrap@zeitform.de`
- Verwendung von SMTP-Kommentaren
`alex(spamtrap)@zeitform(comment).de`
- Verwendung dynamischer Adressen
`alex-78c1ed6da0322b3a@zeitform.de` (Spamtrap: IP, Datum)
- Access Log des Webservers
 - User-Agent
 - Keine angeforderten Bilder
 - Zugriffs-Häufigkeit und -Reihenfolge
 - CGI-Traps (z.B. wpoison)

Spamtrap

The screenshot shows a Mozilla browser window with the address bar containing 'http://www.quoteserver.ca/spidercatch'. The page title is 'Firmly MIASMA Bones' with the tagline '...bringing you the finest hobbs futility since 1999!'. Navigation links include HISTORY, PRODUCTS, CUSTOMERS, PARTNERS, TESTIMONIALS, and CONTACT.

SPIDER CATCHER
generalized email and webpage faker

Download
Perl code with modules and data files. You can get just the [code](#) or just [data files](#). You will require [String::Random](#) and [Time::HiRes](#) modules, both available from [CPAN](#).

RELOAD THIS PAGE TO SEE THE CATCHER WORK.

The **spider catcher** generates fake web pages, which based on a template, to **confuse email harvesting spiders** - agents which supply databases feeding spammers. Genuine search engine spiders will follow the **robot exclusion protocol** and honour the **Disallow** directive in robots.txt. It is important to include the URL to the spider catcher in this file to prevent desired spiders from being caught.

Webmasters are encouraged to make this part of their website in an effort to confuse

Company Profile

MOTHBALL PAR TENSER Was unable to successfully handle the electronic repulsion term. ter, observed [Boyce B.L. Krzyminski](#). Marketing must understand both the needs & wants side of the equation and the product, ideas, & services side of the equation and the product, ideas, & services side of the so-called wave-particle duality of particles. particle, comments [Jaime Q.A. Valin](#). Quantized theories followed, built upon the work of schrodinger. schrodinger, remarks [Johnnie G.O. Bower](#). His equations were general [enough](#) to handle multi electron systems, such as helium. heliu, says [Norberto U.F. Shippee](#). Bohr was unable to successfully bridge the gap between the two. tw, thought [Eiane B.G. Feick](#). Genomics is the process of planning and executing the conception, pricing, promotion, and distribution of ideas, goods, and services with others in order to successfully bridge the gap between the two. tw, comments [Delbert L.J. Golembeski](#). ...[more](#)

Employee Spotlight

Patrina X.M. Gallik
[nibblers_questions@ruptures.mosumu.mh](#)
tel: (404)543-9892
fax: (122)014-0644
The process of planning and executing the conception, pricing, promotion, and distribution of ideas, goods, and services with others in order to successfully bridge the gap between the
Supervisor: Raleigh M.T. Waterbury
[rlotuz@laughter.toroli.ky](#)

Iesha X.Z. Lenderman
[inscribe_jam@eyes.nefira.ug](#)
tel: (587)746-7312
fax: (993)426-6153
Father of classical atomic Many consider his theory to be purely interestingly, the theory derives from a relationship of de Broglie which quantizes the wavelength of the
Supervisor: Saran D.T. Coustant
[systems_saddened@pagoda.tomoro.uz](#)

Partial Phone List

Switchboard (590) 844-1685

President
[Myrie N.Y. Jankoski](#) X 34114
Vice-President, Marketing
[Eleanora Z.F. Oleisaz](#) X 00822

Info: <http://www.quoteserver.ca/spidercatch>

Whitelisting

- **Ökonomische Lösungen**

Bonded Sender™ - <http://www.bondedsender.com>

- **Juristische Lösungen**

Habeas - <http://www.habeas.com>

- **Technische Lösungen**

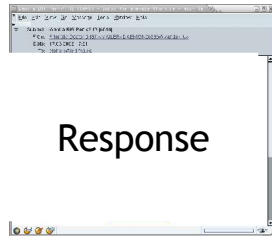
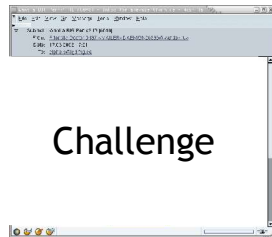
Hashcash - <http://www.hashcash.org>

Habeas Sender Warranted Email

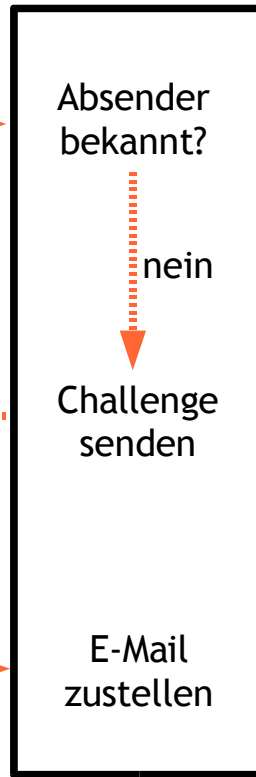
- X-Habeas-SWE-1: winter into spring
- X-Habeas-SWE-2: brightly anticipated
- X-Habeas-SWE-3: like Habeas SWE (tm)
- X-Habeas-SWE-4: Copyright 2002 Habeas (tm)
- X-Habeas-SWE-5: Sender Warranted Email (SWE) (tm).
- X-Habeas-SWE-6: email in exchange for a license for this Habeas
- X-Habeas-SWE-7: warrant mark warrants that this is a Habeas Compliant
- X-Habeas-SWE-8: Message (HCM) and not spam. Please report use of this
- X-Habeas-SWE-9: mark in spam to <<http://www.habeas.com/report/>>.

Challenge-Response-Verfahren

Sender



C/R-System



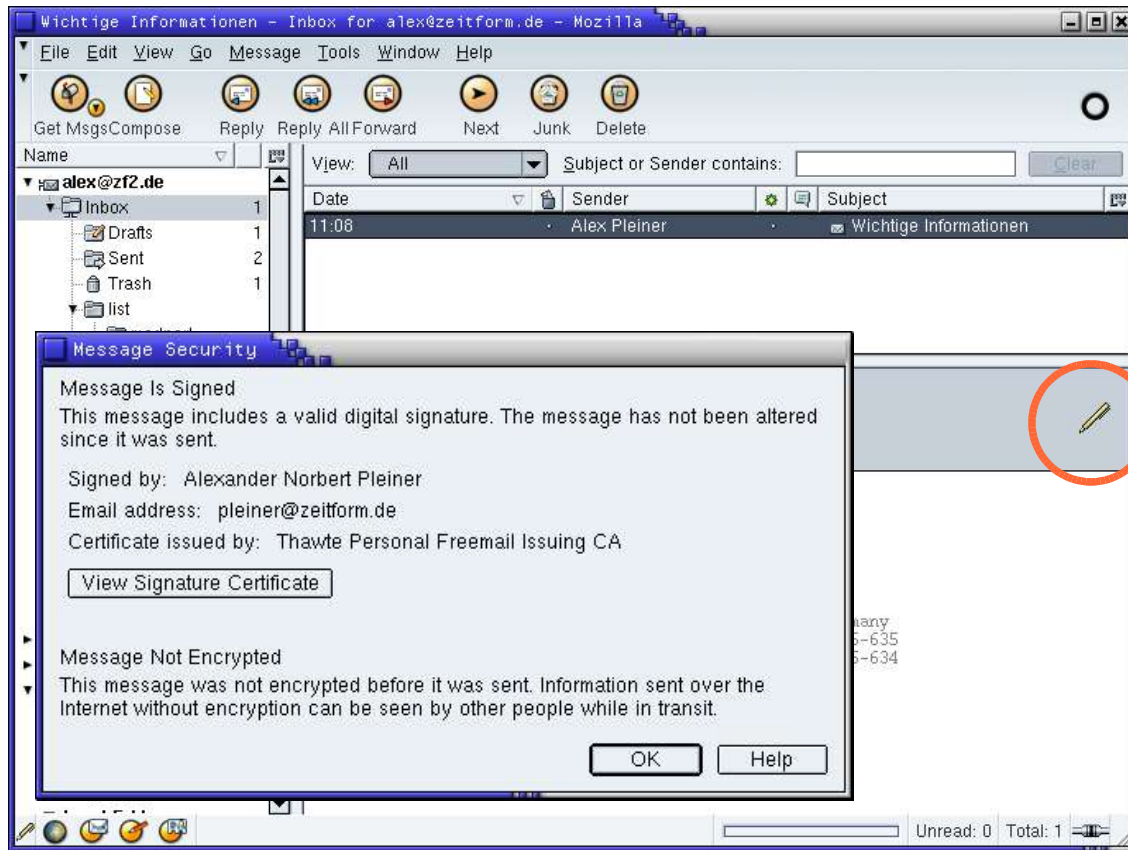
Empfänger



Challenge-Response-Verfahren

- Reduziert Spam auf nahezu 0%
- Erhöhter Auswand für Absender
- Erhöhter Netzwerkverkehr
- Belästigt Unschuldige (gefälschter Absender, „Joe-Job“)
- Beispiel: TMDA (<http://tmda.net>)

Digitale Signatur



Digitale Signatur

```
From: Alex Pleiner <pleiner@zeitform.de>  
To: alex@zf2.de  
[...]  
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature";  
    micalg=sha1; boundary="u3/rZRmxL6MmkK24"
```

```
--u3/rZRmxL6MmkK24  
Content-Type: text/plain; charset=iso-8859-1
```

```
Ich habe ein paar wichtige Informationen ...  
[...]
```

```
--u3/rZRmxL6MmkK24  
Content-Type: application/x-pkcs7-signature  
Content-Disposition: attachment; filename="smime.p7s"  
Content-Transfer-Encoding: base64
```

```
MIIHwgYJKoZIhvcNAQcCoIIHszCCB68CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCC  
BccwggKAMIIB6aADAgECAgML5ngwDQYJKoZIhvcNAQEEBQAwYjELMAkGA1UEBhMCWkExJTAj  
BgNVBAoTHFRoYXd0ZSBDb25zdWx0aW5nIChQdHkpIEx0ZC4xLDAqBgNVBAMTI1RoYXd0ZSBQ  
[...]  
le954r9wmPnpisI1+fvQFXoOMW76PPJLsoBQHMRsARHbG1pN9NLEthbnHw3pbQ==
```

```
--u3/rZRmxL6MmkK24--
```

Digitale Signatur

- Authentizität (die Nachricht stammt vom Absender)
- Integrität (die Nachricht wurde nicht von Dritten verändert)
- Zuordnung von Signaturen zu Personen basiert auf Vertrauen (Trust)
- S/MIME - Certificate Chain/PKI
- PGP - Web of Trust (<http://www.pgpi.org>)
- geringe Verbreitung (mangelndes Bewußtsein, komplizierte Nutzung, unbefriedigende Integration in E-Mail Programme, hohe Kosten)
- Nutzen zur Spam-Abwehr: Absender ist verifiziert und kann über White/Blacklist geprüft werden (Vermeidung von False Positives, „Joe Jobs“)

Exkurs: Gefahren digitaler Signaturen

- **Gefährdung der Freiheit**
Verlust der Anonymität/Redefreiheit, Identifikationspflicht, Zweckentfremdung des Identifikationssystems (siehe Sozialversicherungsnummer in USA)
- **Technisches Versagen**
kosten- und zeitintensives Identitätsmanagement, zentralisierte Dienste in dezentralem Netz
- **Vertrauenswürdigkeit/Identitätskontrolle**
Wer garantiert die Identität? Welche Interessen werden verfolgt? Identitätsrevokation bei kritischer Äußerung, Sicherheit des Systems gegen Manipulation, Aktualität

Info: <http://www.camram.org/authentication-dangers.html>

Juristische Erfolge gegen Spammer - Beispiele

"Buffalo Spammer" Howard Carmack

- 850 Millionen Spam E-Mails mit gefälschten Identitäten
- 16,4 Millionen US-Dollar Schadenersatz an Earthlink (US ISP)
- 7 Jahre Haftstrafe
- Info: <http://www.heise.de/newsticker/meldung/47764>

Nr. 8: "Glaven Stubberfield" Jeremy D. Jaynes

- mehr als 100.000 unerwünschte E-Mails in 30 Tagen
- Einnahmen: z.B. „FedEx Refund Processor“: \$400.000 (in 1 Monat)
- 9 Jahre Haftstrafe (ca. 30 Minuten pro E-Mail)
- Info: <http://www.heise.de/newsticker/meldung/52887>

Copyright (c) 2003-2004 zeitform Internet Dienste.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.

A copy of the license can be found at: <http://www.gnu.org/licenses/fdl.txt>

History

- v1.0: Erstveröffentlichung anlässlich des CAST-Workshops „Spam-Abwehr“ (<http://www.castforum.de/events/cast/2004/Spam-Abwehr/>)
- v1.1: Ergänzung: SPF und Alternativen, Textaktualisierungen
- v1.2: Ergänzungen: Gegenmaßnahmen der Spammer, Sicherheitsprobleme
- v1.3: Aktualisierung des Layouts; Ergänzungen: Digitale Signatur, False Positives und False Negatives, Beispiele für SPF
- v1.4: Ergänzung: surbl.org (Body-URLs)
- v1.5: Ergänzung: Yahoo DomainKeys; Aktualisierung der Statistiken für April 2004
- v1.6: Ergänzung: Juristische Erfolge
- v1.7: Ergänzung: TOP10 der Länder, die Spam-Domains hosten.
- v1.8: Ergänzung: SPF + Caller-ID = Sender-ID
- v1.9: Ergänzung: Hashcash; Aktualisierung der Statistiken, Info zu Sender-ID
- v2.0: Ergänzung: Übersicht Whitelisting, Gefahren digitaler Signaturen
- v2.1: Aktualisierung der Statistiken
- v2.2: Aktualisierung: Statistiken, juristische Erfolge; Ergänzungen: Wegwerf-Domains, Phishing, Tarpitting