

Wirksame Spam-Abwehrtechniken mit OpenSource-Mitteln



Alexander von Gernler
ITS 2008 Unterhaching, 15. April

- Netzwerksicherheit, Datenschutz, Privatsphäre
- Mitglied im OpenBSD-Projekt
 - Mirror an der Uni Erlangen
 - <grunk@openbsd.org>
- Betreiber eines Internet-Servers
 - Weltweit bekannte Mailadresse
 - Trotzdem kein Spam in der Inbox



- Dieser Vortrag ist
 - Ein technischer Überblick über Spamabwehr
 - Eine Fallstudie mit Schwerpunkt OpenBSD
- Dieser Vortrag ist nicht
 - Eine umfassende Anleitung zum Bau eines Mailservers
 - Ein heiliger Kreuzzug



- Erfassung des Problems
 - Definition von Spam, Motivation der Beteiligten
- Vorstellung der theoretischen Prinzipien
 - White/Grey/Blacklisting und RBL
 - Patterns und bayesische Filter
 - SPF und Tipps aus den RFCs
- Spamabwehr am realen Beispiel
- Fazit und Ausblick



Erfassung des Problems: Spamversender und deren Motivation Angriffsszenarien

• **Definition: Spam**

- *Unsolicited bulk E-Mail*, also unerwünschte Massen-Mails
- Alles, worum ich nicht gebeten habe und wofür mein Einverständnis auch nicht in Zukunft zu erwarten ist
- Egal, welchem Zweck die Mail sonst dient
- Vgl. *cold calls* beim Telefonmarketing oder Werbung im Briefkasten trotz „Keine Werbung“-Schild
- Verursacher nicht feststellbar, also Selbsthilfe nötig

- Ziele von Spamversendern
 - Billiges Massenmarketing (Viagra, Cialis etc.)
 - Versenden von Trojanern
 - Aufbau von Botnetzen (Storm-Worm und Co.)
 - Gezieltes Ausspionieren von Personen
 - 22. März Heise: Trojaner-Angriffe auf Pro-Tibet-Gruppen
 - In Zukunft: Post vom Finanzamt -- Bundestrojaner?
 - Denial of Service, Verschmutzen von Filtern
 - Proof of Concept



- Vermutete Ausstattung von Spamversendern
 - Professionelle gewerbsmäßige Tätigkeit
 - Nutzung geknackter Rechner zum Versenden
 - Hoher Aufwand steckt in Botnetzen und verteiltem Mailversand
 - Gute finanzielle Ressourcen durch Einnahmen aus dem Spamversand

- Sammeln von Mailadressen
 - Webcrawler, Mailinglisten-Archive, GPG-Keyrings, gestohlene Firmendaten, Daten von geknackten Rechnern, Gewinnspiele, Opt-Out-Listen
- Aufbau einer Infrastruktur zum Versand
 - Rechner selber knacken oder knacken lassen, Botnet-Software zum Versand installieren
- Zurückschießen
 - Denial-of-Service gegen Anti-Spam-Anbieter

- Angreifer
 - Wechseln häufig IP-Adressen und Mailinhalte
 - Rechner in fremden Ländern
 - Selbst dann nicht die Rechner der eigentlichen Angreifer
 - Sind juristisch kaum belangbar
 - Mangelnde Nachweisbarkeit
 - International lückenhafte Gesetzgebung
 - Haben erhebliche Ressourcen
- Fazit: Lokale Maßnahmen einzige Möglichkeit

Theorie der Spamvermeidung

SMTP-Grundlagen

Techniken auf IP-Ebene und im SMTP-Dialog

Auf Mailinhalt basierende Techniken



- Mailversand-Schritte
 - Schreiben der Mail im Mail User Agent (MUA), z.B. Outlook, Eudora, mutt, Thunderbird
 - Übergabe an Mail Submission Agent (MSA), dieser übergibt an Mail Transport Agent (MTA) zur Auslieferung
 - MTA findet zuständigen Mailserver (remote MTA) heraus (MX-Lookup), kontaktiert diesen und führt den SMTP-Dialog mit ihm durch.
 - Remote MTA beauftragt MDA (mail delivery agent) mit der lokalen Zustellung der Mail.

```
$ dig -t MX genua.de
```

```
[...]
```

```
;; ANSWER SECTION
```

```
genua.de.          21600 IN MX      10 gg.genua.de.  
genua.de.          21600 IN MX      20 hh.genua.de.  
genua.de.          21600 IN MX      30 sauger.genua.de.
```

```
[...]
```

```
;; ADDITIONAL SECTION
```

```
gg.genua.de.       21600 IN MX      151.136.100.2
```

```
$ fgrep smtp /etc/services
```

```
smtp                25/tcp             mail
```

```
$
```



```
$ telnet mail.genua.de 25
220 mail.genua.de ESMTP smtprelay service ready
EHLO gernler.de
250-mail.genua.de pleased to meet you
250-SIZE
250-DSN
250 HELP
MAIL FROM:<alexander@gernler.de>
250 Sender ok.
RCPT TO:<info@genua.de>
250 Recipient ok.
DATA
354 Enter mail, end with . on a single line.
From: Alexander von Gernler <alexander@gernler.de>
To: <info@genua.de>

Hello,
I want information from you!
Bye
.
```

```
250 Recipient ok.
```

```
DATA
```

```
354 Enter mail, end with . on a single line.
```

```
From: Alexander von Gernler <alexander@gernler.de>
```

```
To: <info@genua.de>
```

```
Hello,
```

```
I want information from you!
```

```
Bye
```

```
.
```

```
250 Message accepted for delivery
```

```
QUIT
```

```
221-smtprelay closing connection.
```

```
221 Good bye.
```

```
Connection closed by foreign host.
```

```
$
```



```
$ telnet mail.genua.de 25
```

```
220 mail.genua.de ESMTP smtprelay service ready
```

```
EHLO gernler.de
```

```
250-mail.genua.de pleased to meet you
```

```
250-SIZE
```

```
250-DSN
```

```
250 HELP
```

```
MAIL FROM:<alexander@gernler.de>
```

RFC 2821
SMTP Envelope

```
250 Sender ok.
```

```
RCPT TO:<info@genua.de>
```

RFC 2821
SMTP-Dialog

```
250 Recipient ok.
```

```
DATA
```

```
From: Alexander von Gernler <alexander@gernler.de>
```

RFC 2822

```
To: <info@genua.de>
```

Internet Message Header

```
Hello,
```

```
I want information from you!
```

RFC 2822

```
Bye
```

Internet Message Body

```
.
```

- Standard: unverschlüsselt und unauthentifiziert
 - E-Mails schlechter als mit Bleistift beschriebene Postkarten
 - Informationen im Header beliebig fälschbar, im Envelope fast genauso
 - Absender-IP meist echt, aber nutzlos
 - Received-From-Header: Nur letzter Hop glaubwürdig
- Spammer nutzen ganz normales SMTP, nur in Massen, und mit gefälschten Daten

- Laut RFC 2821 sind wir für einmal akzeptierte Mails verantwortlich
- Daher Spam-Mails bereits relativ früh ablehnen, spart Ressourcen
- Ist die Mail erst akzeptiert, muss eine Bounce (Delivery Status Notification) generiert werden, falls die Mail nicht zugestellt werden kann.



- Wurden Spam-Mails identifiziert, könnte man sie...
 - Zustellen?
 - Ablehnen?
 - Löschen?
 - Markieren?



Techniken auf IP-Ebene und im SMTP-Dialog

Blacklisting
Whitelisting
Greylisting
HELO/EHLO Checks
PIPELINING
Stottern
Greytrapping
Absender-Authentifikation



- Absender-IP meist nicht gefälscht
- Also Sammeln von IPs, die Spam versenden in einer Blacklist
- Ablehnen aller Mails von IPs aus Blacklist
- Problem: Pflege der Listen
 - Irrtümlich gelistete IPs, blindes Vertrauen, Policy
 - Zu lange Reaktionszeiten, Spammer sind schneller
- Fazit: Blacklisting hilft, reicht aber nicht.

- Wie funktioniert DNS-basiertes Blacklisting?
 - Wir benutzen den (erfundenen) Blacklistserver `dnsbl.genua.de`
 - MTA namens `spambert.evil.org` kontaktiert uns zur Mailauslieferung, hat IP `11.22.33.44`
 - DNS-Lookup auf `44.33.22.11.dnsbl.genua.de` liefert positive Antwort (d.h. nicht den Fehler `NXDOMAIN`)
 - `spambert.evil.org` ist also ein Spammer!

- Schutz vor rigorosen Anti-Spam-Massnahmen
- Unser Kunde/Partner/Zulieferer betreibt den Mailserver `mail.partner.de`
 - Der Kunde ist vertrauenswürdig, d.h. sein Mailserver ist sicher kein Spamversender
 - Der Kunde legt Wert darauf, dass seine Mails zeitnah beantwortet werden
- Also die IP seines Mailservers dauerhaft von Anti-Spam-Maßnahmen ausnehmen



- Spammer haben Probleme
 - Millionen Mails innerhalb kürzester Zeit versenden
 - Sowas schon mal mit sendmail probiert?
 - Botnetz-Software darf nicht durch Last auffallen
 - Meist kein echter MTA hinter der ganzen Sache
 - Spooling von Mails viel zu teuer – Ein Versuch und ab damit
- Das müsste man doch ausnutzen können!

- Wir bringen also das Gegenüber zum Spoolen!
Aber wie?
- SMTP kennt u.a. diese Status-Codes
 - 2xx (Erfolg)
 - 5xx (Permanenter Fehler)
 - 4xx (Temporärer Fehler)
 - Out of diskspace, Load too high, etc.
- Wir simulieren einen temporären Fehler und warten darauf, dass der Client wiederholt



```
$ telnet mail.genua.de 25
220 mail.genua.de ESMTP smtprelay service ready
EHLO gernler.de
250-mail.genua.de pleased to meet you
250-SIZE
250-DSN
250 HELP
MAIL FROM:<alexander@gernler.de>
250 Sender ok.
RCPT TO:<info@genua.de>
451 Temporary failure, please try again later.
QUIT
221 Good bye.
```

- Ein normaler SMTP-MTA versucht es einfach nochmal => Kaum Beeinträchtigung des Dienstes für normale Nutzer



- Greylisting wirkt kurzfristig und sofort
- Spammer, die lange versuchen, kommen durch
- Schließt die Lücke, die vor Blacklisting besteht
- Spammer werden erst durch Greylisting aufgehalten, und landen inzwischen (hoffentlich) auf einer Blacklist



- Unterscheidung zwischen Greylisting in RCPT- und in DATA-Phase
 - Bei RCPT-Phase erlaubt einzelnes Annehmen/Ablehnen von Empfängern
 - Bei DATA-Phase kann nur noch ganze Mail angenommen oder abgelehnt werden
 - Aber bei DATA liegt auch Inhalt vor
- Unbedingt Backup-MXe auch mit Greylisting versehen, ansonsten wirkungslos!

```
220 mail.genua.de ESMTP smtprelay service ready
EHLO gernler.de
250 mail.genua.de pleased to meet you
```

- RFC 2821 verlangt eine HELO/EHLO-Zeile
- Bleibt diese aus, ist das Protokoll verletzt
- Ist diese verdächtig, kann abgelehnt werden (Achtung, nicht komplett RFC-konform):
 - Löst der angegebene Hostname im DNS auf?
 - Ist es eine echte IP, und keine private?
 - Wird etwa von vorne herein nur eine IP übergeben?
 - Besitzt die Domain einen MX? Löst dieser auf?



```
250 mail.genua.de pleased to meet you
MAIL FROM:<alexander@gernler.de>
250 Sender ok.
```

- Der Envelope-Absender kann geprüft werden, fast analog zum EHLO/HELO-Check
 - Existiert die Domain?
 - Besitzt sie einen MX-Eintrag?
- Falls nicht, kann das verdächtig sein
- Aber: Kaputte Mail-User-Agents von netten Leuten fallen hier auch raus



- Viele MTAs beherrschen heute RFC 2920
PIPELINING
 - 250-PIPELINING
 - Sender darf dann mehrere Befehle auf einmal absetzen
 - Niemals aber HELO/EHLO zusammen mit weiteren Befehle
 - Viele Spammer pipelinen auch andere verbotene Kombinationen
- Erkennen, ablehnen



- Spammer haben es eilig!
- Wir nicht.
 - Warum den SMTP-Dialog nicht mal laaaannngsam sprechen?
 - Ein normaler MTA merkt das gar nicht
 - Ein Spammer bricht ab, die 99999999 anderen Mails warten ja noch...
- In OpenBSD's `spamd` (8) implementiert



- Greytrapping fängt Spammer ein, die zufällige Adressen versuchen
- Wir richten uns eine geheime Adresse ein: `<oberzipfl@gernler.de>`
- Adresse wird **nirgendwo** bekanntgegeben
 - (oder in Hintergrundfarbe oder in Kommentar auf die eigene Webseite, für die Harvester...)
- Jeder, der an diese Adresse zustellt, muss ein Spammer sein, wird für 24h geblacklistet

- Vorsicht mit Greytrapping!
- Benutzt ein Spammer unsere Greytrap als Absenderadresse für Spam, landen die Bounces bei uns, also in der Greytrap
- Wir haben jetzt jemanden gesperrt, obwohl er selbst nur Ziel ist, wir sind daher auch Opfer
- Spammer ist der lachende Dritte.



- SPF, SenderID, DomainKeys und andere
- Idee: DNS-Einträge geben an, wer für diese Domain Mails versenden darf
- Problem: Konkurrierende Entwürfe (vgl. HD-DVD vs. BluRay), unklare Patentsituation, kein eindeutiger Sieger erkennbar
- Wird von GMX und Google für deren Mails gesetzt, aber Überprüfung auf Clientseite findet kaum statt

Auf Mailinhalt basierende Filtertechniken

Statische Filter (Heuristiken)

Bayesische Filter

Ähnlichkeits-Hashes



- Eines der ältesten Verfahren überhaupt
- Beurteilung einer Mail anhand von bestimmten fixen Merkmalen
- Jedes Merkmal gibt Punkte
- Ab einem bestimmten Punktestand ist die Mail als Spam klassifiziert
- Dann meist Kennzeichnung im Header für späteres Aussortieren



- Beispiele für Merkmale
 - Großbuchstaben/Ausrufezeichen im Subject
 - Kein Realname in der From:-Zeile
 - Vorkommen bestimmter Strings (Viagra, \$\$\$, Make Money Fast, ...)
 - Unsubscribe-Link für eine angebliche Mailingliste
 - Überlange Zeilen
 - Verdächtige andere Empfänger der Mail



- Heuristisch == Von Menschen anhand von Beobachtungen erstellte Regeln
- Liefern relativ vorhersehbare Ergebnisse
- Trefferrate heute niedriger als früher, aber immer noch signifikant
- Filtert vor allem die dummen Spammer heraus
- Verfügbare Software z.B. SpamAssassin



- Lernende Filter, d.h. müssen individuell trainiert werden
- Anfangs Füttern mit eigener Inbox und händisch gesammeltem Spam
- Im Betrieb selbstlernend anhand von selbst getroffenen Entscheidungen
- Entscheidungen müssen von Zeit zu Zeit korrigiert werden



- Mail wird nicht auf semantischer (also inhaltlicher) Ebene interpretiert, sondern nur als Muster
- Mails mit bestimmten Mustern entsprechen der erwünschten Post.
- Sehr individuell, hängt von Sprache, Jargon und Schreibstil des Bekanntenkreises ab.
- Bestimmter Spam ist hart an der Entscheidungs-Grenze, soll Filter verschmutzen



- Höherer Eigenaufwand zum Einrichten eines Bayes-Filters als für statischen Filter
- Von Zeit zu Zeit Korrektur der Entscheidungen nötig
- Liefert sehr gute Trefferquoten
- Verfügbare Software z.B. `bogofilter`

- Idee: Spam-Mails einer Sorte schauen fast immer gleich aus
 - Maschinelles Erkennen solcher Mails durch Fuzzy Hashing
 - Abgleich mit Prüfsummenliste verdächtiger Hashes
- Sowohl offline (d.h. beim User) als auch online (während des SMTP-Dialogs) möglich
- Beispiele: Nilsimsa, NiXSpam

Fallstudie

Spamvermeidung auf einem
realen Server im Internet



- Weltweit bekannte Mailadresse durch das OpenBSD-Projekt
- Gemeinsamer Server mit mehreren Kollegen
- Keiner von uns hat viel Lust auf Spam
- Wie löst man das?



- Pro Tag werden etwa 700 Mails am spamd abgewiesen: Greylisting, Blacklisting
- Etwa 1200 weitere Mails schaffen es durch
- Den Rest besorgen Inhaltsfilter auf meiner Maschine
- Spam in meiner Inbox? Praktisch keiner.
- Kleiner Mailserver, kleine Zahlen. Aber: skalierbar, mehr dazu später



- Mails mit Ziel auf SMTP-Port (tcp/25) treffen auf diese Paketfilter-Regeln (OpenBSD pf):

```
table <spamd-white> persist
no rdr on $ext_if proto tcp from <spamd-white> \
    to any port smtp
rdr pass on $ext_if proto tcp from any to any \
    port smtp -> 127.0.0.1 port spamd
```

- Auf Deutsch:
 - IPs im Whitelisting dürfen zum echten Sendmail
 - Alles andere landet bei OpenBSD's spamd



- OpenBSD's spamd behandelt zwei von drei Klassen von Mailversendern:
 - IPs im Blacklisting haben keine Chance auf Erfolg. Spamd ist nur eine *Teergrube* für sie.
 - IPs im Greylisting werden, falls sie in einem Tupel zum zweiten Mal gesehen werden, ins Whitelisting aufgenommen
 - IPs im Whitelisting landen wegen der Paketfilter-Regel gar nicht mehr beim spamd

- Typischer spamd-Dialog, dauert min. 10 sec:

```
$ telnet pestilenz.org 25
220 pestilenz.org ESMTP spamd IP-based SPAM blocker; Mon Mar 31
16:47:11 2008
EHLO gernler.de
250 Hello, spam sender. Pleased to be wasting your time.
MAIL FROM:<alexander@gernler.de>
250 You are about to try to deliver spam. Your time will be
spent, for nothing.
RCPT TO:<grunk@pestilenz.org>
250 This is hurting you more than it is hurting me.
DATA
451 Temporary failure, please try again later.
Connection closed by foreign host.
$
```

- Spamd ist ein sehr sparsames Programm
 - kommt ohne fork() aus, nur 3530 Zeilen C-Code
- Universität von Alberta, in Edmonton (Stand 2006, Daten von <beck@openbsd.org>)
 - Spamd für die komplette Mail der Universität
 - In 72 Stunden ca. 3.000.000 SMTP-Verbindungen
 - Davon kamen nur 450.000 Verbindungen durch
 - Läuft auf einem 1U-Server von Dell, der dabei 95% CPU Idle ist

- Was hier durchkommt, ist noch nicht spamfrei:
 - Mails, die per Forwarding von anderer Mailadresse ankommen (der an uns ausliefernde Server ist hier immer der gleiche)
 - Spammer, die es schaffen, Grey- und Blacklisting zu umgehen (eher geringer Anteil)
- Mit diesen Mails kann jeder User selbst umgehen



- Automatisierte Mailbearbeitung durch procmail
- Regeln für Bearbeitung jeder Mail mit bogofilter

```
:0fw
| /usr/local/bin/bogofilter -e -p -u
```
- Regeln zum Aussortieren bedenklicher Mails

```
:0 H
* ^X-Bogosity: Spam, tests=bogofilter
bogospam/
```
- Hotkeys im MUA zum Umsortieren der Mails und Umlernen von bogofilter





Ausblick



- Selbst in 90 min kein Gesamtüberblick möglich
- Noch nicht behandelt:
 - RHSBL, BATV, IIM, Tokenbasierte Verfahren, HashCash, Micropayments, Frequenzanalyse, URIDNSBL
 - Teils illusorische Konzepte
 - Teils patentbehafte
 - Teils einfach noch nicht durchgesetzt



- Spam wird es geben, solange es das Netz gibt
 - Geld ist viel zu einfach zu verdienen damit
- Wettlauf Spammer/Antispam-Software
 - Vergleichbar mit Viren/Antiviren-Software
- Spamfreies Leben ist trotzdem möglich
 - Trotz weltweit bekannter Mailadresse, q.e.d



- BSI Anti-Spam-Studie, sehr empfehlenswert
<http://www.bsi.de/literat/studien/antispam/index.htm>
- OpenBSD-Manpage zu spamd(8)
<http://www.openbsd.org/cgi-bin/man.cgi?query=spamd>
- Talk von Bob Beck zu OpenBSD spamd(8)
<http://www.ualberta.ca/~beck/nycbug06/spamd>
- <http://www.greylisting.org/>
- Wikipedia zu Grey-/White-/Blacklisting und anderen Konzepten



- Noch Fragen?
- Jobs bei GeNUA!
- Folien auf
<http://pestilenz.org/~grunk/vortraege/2008/04-ITS/its2008.pdf>
- Kritik und Anregungen zum Vortrag gerne willkommen:
<gernler@genua.de>

