Spam

Problematik und Lösungen

Dirk Geschke

Linux User Group Erding

22. August 2007

Gliederung

- Allgemeines zu Spam
- Juristische Aspekte
- Vorsorge und Ansatzpunkte
- Methoden der Spambekämpfung
- Theoretische Verfahren
- Abschluß

Historisches

- Dosenfleisch: SPiced hAM, auch Shoulder Pork and hAM
- Begriff stammt von Monthy Python-Sketch: Spam als etwas was man nicht haben will und trotzdem bekommt
- Jon Postel dachte schon in RFC-706 *On the Junk Mail Problem* aus dem Jahr 1975 über Spam nach
- Erste Spammail: 3. Mai 1978 - DEC Marketing TOPS-20
- Erste Verwendung des Begriffs Spam: Usenet, 31.3.1993 - Werbung für Greencard-Lotterie
- Folge: praktisches Ende der Newsgroups

Spam-Definition

- UCE: Unsolicited Commercial Email
- UBE: Unsolicited Bulk Email
- Kollateral-Spam: Bounces die an vermeintlichen Absender gesendet werden
- verwandte Probleme: Phishing, Viren, Tojaner, Kettenbriefe
- juristische Definition
  - werbender Inhalt mit kommerziellem Hintergrund
  - unverlangte Zusendung
  - kein bestehender geschäftlicher Kontakt

Spamprobleme

- Server überlastet
- Mailboxen werden verstopft
- Verschwendung von Arbeitszeit
- Kosten für Traffic
- verlangsamte Zustellung regulärer E-Mail, verspätetes Lesen

Motivation der Spammer

- guter Gewinn gegen geringen Aufwand, Kosten für Spamversand sind minimal
- bei Millionen von E-Mails gibt es immer welche die darauf anspringen
- Laut Spamhaus nur 200 professionelle Spammer
- Arbeiten im Auftrag anderer
- schwer juristisch belangbar

Techniken

- SMTP hat keine Sicherungen gegen Fälschungen von Adressen
- Envelope unabhängig von der eigentlichen E-Mail
- Betrieb eigener Mailserver
- Spamversand mit besonderen Mailclients: Fire & Forget
- Verwendung von open relays: bis in 90er Jahre gewünschte Funktionalität!
- Verwendung von open proxies, z.B. Webproxies
- unsichere CGI–Scripte (*formmail*)
- Zombie–PCs, Bot–Netze
- Mailserver der einzelnen Provider bei Botnetz

Sammeln von Adressen

- offline via CDs - käuflich erwerbbar
- von Webseiten und aus Newsgruppen (*harvester*)
- raten von Adressen (*local-parts*)
- Adreßaustragungs–Links, Gewinnspiele, Gratisproben
- FTP-Links: z.B. Outlook verwendet eigene E-Mail Adresse zur Authentisierung bei *anonymous*–Zugängen
- automatische Antworten, vacation– oder Abwesenheits-E-Mail
- whois–Datenbanken
- Adreßbücher von Zombie–PCs

Allgemeines

- juristisch sind nur E-Mails mit kommerziellem Hintergrund relevant
- Zusendung unverlangter E-Mails zu Werbezwecken verstößt gegen gute Sitten
- Klageberechtigt sind nur Konkurrenten, Verbraucher- und Wettbewerbsverbände und Handelskammern
- Ansonsten: Abmahnung und einstweilige Verfügung
- Deutschland und EU: opt-in, USA opt-out
- Probleme: Gerichtsstand und Prozeßkosten

Spam und Recht

- eigentlicher Spamversand ist nicht strafbar!
- allerdings kann der Inhalt strafbar sein
- gefälschte Adressen: Markenrecht gilt auch für Domainnamen!
- lahmlegen eines Mailservers durch Spam: Computersabotage
- Virenwarnungen mit Werbung für Virenscanner gelten als Spam

Recht und Filterung

- E-Mails fallen unter §206 StGB: Fernmeldegeheimnis
  - Ausnahme bei Unternehmen: Verbot privater Nutzung
  - E-Mail muß dem Server zur Übermittlung anvertraut sein
- Ebenfalls relevant ist §303a StGB: Datenveränderung

  (1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
  (2) Der Versuch ist strafbar
  (3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Recht und Filterung

- Folgen aus §303a:
  - ungenehmigte Löschung oder Unterdrückung von E-Mails ist verboten!
  - Zustimmung des Empfängers vorher notwendig!
  - Verschieben spamverdächtiger E-Mails in andere Ordner ist rechtlich bedenkenlos
- Notfallbetrieb (z.B. *DDoS*–Attacke): Hier darf Spam auch ohne Zustimmung gelöscht werden!
- Viren: Theoretisch auch §§206 Abs. 2 und 303a StGB. Abwehr drohender Virenangriffe reicht aber als Rechtfertigung einer Löschung, §109 TKG: Schutz gegen unerlaubte Zugriffe

Erlaubter Spam

- opt-in: Empfänger muß vorher dem Versand zugestimmt haben
- Zustimmung auch durch Kauf einer Ware oder Dienstleistung, dem kann aber widersprochen werden
- Online oft double-opt-in oder auch verified opt-in: doppelte Bestätigung gegen Mißbrauch, z.B. bei Newslettern und Eintragen fremder Adressen
- Variante: confirmed opt-in: schriftliche Bestätigung vor Zusendung z.B. eines Newsletters mit sofortiger Kündigungsmöglichkeit

Vermeidung von Spam

- Mailserver nicht als open relay betreiben, gleiches gilt für open proxies wie z.B. *Squid*
- Vorsicht bei mailversendenden CGI–Scripten (*formmail*)
- Umgang mit Mailadressen
  - keine E-Mail Adressen auf Webseiten
  - lange Namen, 1-2 Buchstaben werden schnell geraten
  - Vorsicht bei: Gewinnspielen, Newslettern, Gratisproben, Austragunglinks
  - keine vacation E-Mails.
  - Geheimhalten der Adresse, häufiger Adreßwechsel und Wegwerfadressen (unpraktisch)
  - Zusatzinformationen in der Adresse: auf *Displaynamen* achten!
  - Zusatzinformationen in mailto–Links (*Subject*)

Angreifpunkte bei Spam

- im Server beim Versand (MSA): *egress*–Filterung (ISPs)
- im Server vor der Annahme der E-Mail
  - IP-Filter vor Connect
  - vor **HELO/EHLO**
  - nach **HELO/EHLO**
  - nach **MAIL FROM**
  - nach **RCPT TO**
  - nach **DATA** und **CRLF . CRLF**
- im Server nach Abnahme
- im Client vor Abholung
- im Client nach Abholung

Nach Spamanalyse

- zustellen, spamverdächtige E-Mails markieren oder separaten Folder
- abweisen, ressourcensparend
- löschen: niemand merkt das, Fehler nicht erkennbar, Rekonstruktion der E-Mail nicht möglich $\longrightarrow$ nicht machbar!
- markieren, entweder unsichtbar im Header oder sichtbar im Subject
- unter Quarantäne stellen
- Ausnahmen: Postmaster (zwecks Beschwerden!)

Filterung durch Personen

- sehr effektives Verfahren, gewöhnlich wird Spam auf den ersten Blick erkannt
- wird von manchen Mailinglisten verwendet: moderated List
- im Unternehmenseinsatz an zentraler Stelle wegen Datenschutz nicht möglich
- Filterung im MUA
- erkannter Spam kann zum Trainieren anderer Filter verwendet werden, siehe Bayes–Verfahren

Einhalten des Protokolls, Timeouts

- Prüfung des HELO-Strings: Ist der Hostname korrekt? Weist er auf gültige Adresse hin?
- Test auf PTR–Eintrag: Existiert er und verweist dieser auf die gleiche IP-Adresse (reverse and forward lookup)
- Einhaltung der Sequenzen: Sendet der Client vor der Antwort des Servers? Vorsicht bei **PIPELINING**.
- Tests auf Korrektheit z.B. der Adressen, Vorsicht: es existieren nicht-RFC-konforme Mailserver.
- Verlangsamung, Ausnutzung von Timeouts: Spammer haben es eilig, sie wollen viele E-Mails durchschleusen. Eine bewußte Verlangsamung kann daher helfen.
- Spammer dürften bei Verbreitung des Verfahrens schnell darauf reagieren

Sender Policy Framework, SenderID, CallerID

- Verifikation des Absenders anhand von DNS–Einträgen
- Einschränkung des Kreises von sendeberechtigten Servern
- nur der Versender kann Einträge vornehmen: Spamvermeidung bei anderen und nicht bei einem selber
- Spammer können sich auch SPF-Einträge generieren
- Relaying über andere Server nur bedingt möglich
- Erfolg begrenzt, Einsatz eher nicht ratsam

S/MIME, PGP, STARTTLS

- Aufwand für Verschlüsselung recht hoch
- Existenz von Signaturen nicht ausreichend, Spammer können einmal signieren und mehrfach versenden
- STARTTLS hilfreich: Hohe CPU-Last durch Verschlüsselung, reduziert Durchsatz bei Spammern
- Allerdings hilft das nicht gegen Bot–Netze, die sind in der Regel leistungsstark
- Als Kriterium eher sekundär geeignet, z.B. in Verbindung mit heuristischer Statistik

Right Hand Side Blacklists RHSBL

- Blockierung aufgrund des Domainnamens des Absenders
- Absender leicht fälschbar $\longrightarrow$ schlecht für Blacklists
- sinnvoll nur bei bekannten Spam-Domains.
- hilfreich bei Whitelists, Anwendung muß gut durchdacht sein
- wenig hilfreich, höchstens in Verbindung mit DKIM

Realtime Blackhole Lists

- Sperrung anhand der IP-Adresse des Absenders
- Auch DNSBL genannt: Mißbrauch von DNS um Informationen zu IP-Adressen zu verteilen
- Vertrauen in Betreiber von RBLs notwendig
- diverse Policies: offene Relays, bekannte Spammer, dial-in Adressen
- Wer kommt alles auf die Liste? Wie verfährt man wenn jemand fälschlich auf die Liste gesetzt wurde?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

URI-Blacklists

- Filtern nach URIs innerhalb der E-Mail
- Bei Verwendung beliebiger Subdomains nur die unterste Domain verwenden
- Vorsicht: uk hat 3. Level
- Problem: Redirect-Dienste wie z.B. TinyURL
- Datenschutzproblem existiert auch hier
- Spammer umgehen dies durch z.B. GIF-Bilder mit URLs

Prüfsummenvergleiche

- statischer Inhalt: Prüfsummenvergleiche des Inhalts effektiv
- bei leichten Variationen: unscharfe Verfahren wie z.B. nilsimsa
- Varianten: Distributed Checksum Clearing (DCC), Vipul's Razor, Pyzor
- Brauchen eine breite Basis um effektiv zu sein: zentrales Register
- Da nur Metadaten abgefragt werden: unbedenklich aus Datenschutzgründen
- Können sehr effektiv sein, benötigen aber in der Regel übergeordnete Instanz

Frequenzanalyse

- Reputationsverfahren, Häufigkeit und Frequenz von E-Mails
- Grund-Maillast notwendig
- Verhältnis gültige zu ungültigen Adressen
- Größe der E-Mails: Alle ungefähr gleichgroß?
- temporäres Blacklisten von IP-Adressen
- recht einfaches und brauchbares Verfahren

Sperren SMTP-Port, MTAMARK

- nur für ISPs und Unternehmen interessant
- einige Provider wie z.B. AOL führen dies durch
- MUAs müssen Mailserver des Providers erreichen können oder MSP-Port verwenden
- Problem ist, daß man selber keinen eigenen Mailserver betreiben kann, viele Firmen wollen dies aber.
- könnte gegen viele Bot–Netze helfen

Heuristische Inhaltsanalyse

- Analyse nach Wörtern, Strukturen: rule-based filtering
- Suche nach bestimmten Begriffen im Body und Header
- Body: Großschreibung, Austragungsoptionen, Aufforderung URL aufzurufen, Mustern innerhalb von URLs, HTML-Verschleierungstricks, . . .
- Header: Absender, Empfänger, Versand-Datum, X-Mailer-Analyse, Zeitsprünge in Received-Zeilen, . . .
- Verwendung von Scores für verschiedene gefundene Eigenschaften, positiv wie negativ
- berühmter Vertreter: SpamAssassin
- Effektivität recht hoch, muß auf aktuellem Stand gehalten werden (Katz-und-Maus-Spiel), hoher Rechenaufwand durch viele Regeln und Regular-Expressions
- auf dem Server nur bedingt anwendbar

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **HAM** und **SPAM**
- Filter muß ständig aktualisiert werden
- Spamfallen können zum automatischem Training verwendet werden
- Probleme bereiten HTML-Verschleierungen, es gibt Ansätze die diese vorher rendern
- Erfolg hängt vom Training ab, gewöhnlich nur im MUA anwendbar

DomainKeys Identified Mails (DKIM)

- Validierung des Absenders und der E-Mail durch digitale Signierung auf dem Server
- keine Änderungen am MUA notwendig
- Replay–Attacken möglich, d.h. mehrfaches versenden einer einmal signierten E-Mail
- public key wird via DNS verteilt, ratsam nur mit DNSSec
- Spammer können auch DKIM einsetzen: Kombination mit RHSBL
- bislang keine große Verbreitung, derzeit nur als Whitelist verwendbar

SMTP-Callout

- Validierung des Absenders durch SMTP-Verbindung zum Mailserver des vermeintlichen Absenders
- auch: Sender–Address–Verification, Sender–Verify
- Problem: Bindung von Ressourcen, nachfragen kann länger dauern, manche Maliserver nehmen generell für alle E-Mails entgegen
- erhöhte Last auf Gegensystem kann zu Verstimmungen führen
- Einsatz nicht ratsam
- Variante: Testen ob Server überhaupt auf Port 25 reagiert. SYN, SYN-ACK

Greylisting

- Spammer ignorieren Antworten des Servers, sie lassen sich durch temporäre Fehlermeldungen abschrecken
- Funktionsweise:
  - 1. E-Mail wird durch 4xx-Fehlermeldung abgelehnt,
  - spätere E-Mails mit Tripel (Absender, Sender-IP-Adresse, Empfänger) werden temporär freigeschaltet: Greylist
  - jedes Auftreten des Tripels aktualisiert Greylist-Eintrag
- Zeiten relevant: sehr effektiv zusammen mit RBL
- nicht alle Mailserver sind RFC-konform: Whitelists notwendig
- alle MX-Server müssen Greylisting unterstützen
- derzeit noch die wirksamste Waffe gegen Spam!

Spamfallen, Greytrapping

- Spamfallen: versteckte, nicht-existierende Mailadressen
- alles was an diese Adresse gesendet wird ist Spam: gut für Analyse via Bayes
- Greytrapping: temporäres Sperren eines Mailservers der an eine Spamfalle E-Mails sendet
- beschäftigen Spammer mit unnötiger Arbeit
- dynamische Adressen und Weblogs können Beweise für Gerichtsverfahren liefern

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwending, wird über Bounce erhalten
- manchmal auch alternative Wege wie Webbestätigung erforderlich
- Vorgang meist nur einmal notwendig
- Verfahren ist sehr effektiv
- jedoch nicht ratsam, hohe Hürde für normale Mailversender
- Verwendung mit Mailinglisten hoffnungslos: Whitelists notwendig

Bounce Address Tag Validation (BATV)

- Vermeidung von falschen Bounces
- spezielle Tags in Envelope-From Adresse, individuelle Absenderadressen
- funktioniert nicht mit Greylisting
- local-part darf nur maximal 64 Zeichen lang sein
- BATV muß schwer ratbar und Tag ständig erneuert werden, Tracking der vergebenen Tags
- hilft nur gegen Kollateral–Spam
- möglicher Gewinn rechtfertigt nicht den Aufwand

Elektronische Briefmarken

- Idee: Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Proof-of-Work

- Idee ähnlich der elektronischen Briefmarke
- hohe CPU-Last vor dem Versenden erschwert Spammern das Leben
- wenig CPU-Last zur Verifizierung
- Bot–Netze haben viel Rechenleistung, daher wenig erfolgversprechend
- derzeit kaum Verbreitung, praktisch keine Verwendung
- mögliches Verfahren: HashCash
- Problem: Muß pro E-Mail unterschiedlich sein, was ist mit Relaying über mehrere Server?

Dedizierte Mailserver

- Zustellung nur über spezielle Mailserver möglich
- effektives Verfolgen von Spamversendern möglich
- Problem: alle ISPs müssen mitmachen und Port 25 entsprechend filtern
- Problem: zuviel Macht bei ISPs?
- Wer regelt wer Mailserver betreiben darf?

Verbot von Spam

- derzeit ist Spamversand erlaubt
- Verbot müßte weltweit gelten
- konsequente Verfolgung notwendig
- Sperrung von IP-Adressen aus Ländern die Spam erlauben denkbar
- mögliches Problem: zuviel Macht für den Staat?

Schlußbemerkungen

- eine perfekte Lösung gibt es nicht
- nicht alle Verfahren eignen sich überall
- Kombination mehrerer Verfahren ratsam
- juristische Aspekte dürfen nicht vergessen werden
- Reihenfolge mitunter wichtig (Ressourcenverbrauch)
- heute funktionierende Verfahren müssen nicht morgen auch noch erfolgreich sein, Spammer passen sich an

Was noch fehlt

- 4. Teil?
  - Mailboxformate: mbox, MH, Maildir und Varianten
  - POP: pop2, pop3, pop3s
  - IMAP, IMAPS
  - Sieve-Filter
- Diskussion — die darf nun beginnen