Effektivität von Lösungsansätzen zur Bekämpfung von Spam

Der Autor

Guido Schryen

Dr. Guido Schryen
Lehrstuhl für Wirtschaftsinformatik und Operations Research
der Rheinisch-Westfälischen Technischen Hochschule Aachen
Templergraben 64
52062 Aachen
schryen@winfor.rwth-aachen.de

1 Einführung

Das Ziel dieses Beitrags besteht darin, einen Überblick über die Effektivität von Lösungsansätzen zur Bekämpfung von Spam zu vermitteln. Dieser einführende Abschnitt zeigt die Charakteristika von Spam auf und vermittelt die aus Spam resultierende ökonomische Problematik. Im zweiten Abschnitt werden die derzeit bedeutendsten Verfahren zur Bekämpfung von Spam erläutert, klassifiziert und hinsichtlich ihrer Effektivität beleuchtet. Im letzten Abschnitt finden sich die wesentlichen Aspekte dieses Beitrags zusammengefasst und ist die Notwendigkeit zukünftiger Anti-Spam-Bemühungen skizziert.

Es existieren zahlreiche Definitionen von Spam (verbreitete Auffassungen finden sich bei [CNIL99, 1], [GaDr01, 14], [Muel04]), [NOIE02, 6] und [OECD04]), die als „definitorische Schnittmenge" von einer elektronischen (Post-)Nachricht sprechen, die (1) vielen Empfängern zugestellt wird, von denen (2) einige oder keiner ein vorheriges Einverständnis zum Empfang erteilt hat. In der englischsprachigen Literatur wird dann alternativ zu Spam auch von „Unsolicited Bulk Email" (UBE) gesprochen. Der Inhalt der E-Mail kann religiöser, sozialer, politischer oder wirtschaftlicher Art sein. Ist er wirtschaftlicher Art, indem für den Kauf von Produkten oder die Inanspruchnahme von Dienstleistungen geworben wird, spricht man von „Unsolicited Commercial Email" (UCE). Einige der oben referenzierten Quellen reduzieren den Begriff Spam auf eine Teilmenge von UCE, diejenige, bei denen die E-Mail-Adresse des Absenders vorsätzlich verfälscht wurde. Im Folgenden wird mit UBE ein breiteres Verständnis von Spam zu Grunde gelegt, da einerseits ungeachtet des Inhalts und der Adresse des Absenders UBE unerwünscht ist und die Internet-Infrastruktur belastet und andererseits die vorgestellten Lösungsansätze generell UBE adressieren.

Die vorgestellten Daten zeigen auf, dass es sich bei Spam nicht mehr lediglich nur um ein Ärgernis handelt, sondern dass mittlerweile eine nennenswerte ökonomische Bedeutung vorliegt. Spam hat in der Internetkommunikation die Grenze von der Belästigung, der man sich einfach mit dem Löschen der Nachrichten entledigt, zur ökonomischen Relevanz längst überschritten. Beispielsweise berichtet der Mailprovider Microsoft Hotmail, dass Mitte 2003 der Spam-Anteil bei ungefähr 83 % lag; dies bedeutete eine tägliche Flut von ungefähr 2,5 Milliarden E-Mails [Micr04]. Nach Angaben des US-amerikanischen Unternehmens Brightmail, das nach eigenen Auskünften im Jahr 2003 mit 800 Milliarden E-Mails ungefähr 15 % des weltweiten E-Mail-Aufkommens hinsichtlich Spam untersucht hat, übertraf die Anzahl der Spam-E-Mails die der Nicht-Spam-E-Mails: Mehr als 56 % aller gefilterten E-Mails wurden 2003 als Spam klassifiziert, 2002 waren es noch 40 % [Brig03a]. Der Betreff der sechs meist versendeten Spam-E-Mails findet sich bei [Brig03a], eine Aufteilung nach beworbenen Produktkatego-

Kernpunkte

Spam als unerwünschte Massen-E-Mail hat eine beachtliche ökonomische Relevanz erreicht. Die praktisch bedeutendsten Ansätze gegen Spam adressieren das Problem auf technischer Ebene.

- Filtern und Blockieren gehört zu den technischen und am häufigsten angewandten Verfahren, die als Heuristiken jedoch unter fehlerhaften Klassifizierungen leiden.
- Neue Konzepte basieren auf der Authentifizierung der sendenden Organisation, lassen jedoch technische Möglichkeiten zum Spammen offen, sodass der Erfolg fraglich ist.
- Das Spam-Problem ist nicht gelöst. Es besteht weiterer Bedarf nach neuen und kombinierten Ansätzen.

Stichworte: Spam, E-Mail, Spoofing, Blockieren, Filtern, Lightweight Mail Transfer Agent Authentication Protocol (LMAP)

rien kann [Brig03b, 14] entnommen werden. Weitere Statistiken bietet [OECD04] an.

Ökonomische Betrachtungen können sich zum einen auf die Kosten beziehen, die Spam während des Transports und beim Empfänger verursacht, zum anderen bei UCE auch auf die Wirtschaftlichkeit aus Sicht des Spammers und seines Auftraggebers. Die OECD [OECD04, 9] berichtet hinsichtlich des zweiten Aspekts, dass bereits eine Erfolgsquote von 0,001 % – im Durchschnitt bestellt nur einer von 100.000 Empfängern das beworbene Produkt –, zu einem wirtschaftlichen Gewinn führen kann; bzgl. konkreter Szenarien sei auf diese Quelle verwiesen. Solange eine Profitabilität gegeben ist, ist kommerzielles Spamming nicht ursächlich verhinderbar.

Auf der anderen Seite sind die Kosten zu betrachten, die unfreiwillig Beteiligten entstehen. Dazu gehören die Internet Service Provider (ISP), E-Mail Service Provider (ESP) und die adressierten Organisationen. Eine Studie der EU-Kommission schätzte, dass bereits im Jahr 2002 Spam-Empfängern weltweit jährliche Kosten in Höhe von 10 Mrd. Euro entstanden [GaDr01]. Nach einer im OECD-Bericht aufgegriffenen Studie von Ferris Research, Inc. verursachten 2002 kommerzielle Spam-E-Mails bei US-Unternehmen 8,9 Mrd. US-$ Kosten und in Europa 2,5 Mrd. US-$. Für diese Kosten sind vor allem folgende Phänomene verantwortlich:

1. Die Arbeitsproduktivität sinkt, wenn Mitarbeiter Spam-E-Mails lesen, als Spam klassifizieren und löschen. Nach einer nicht-repräsentativen Studie von Nucleus Research [NuRe03] erhalten Mitarbeiter täglich durchschnittlich 13,3 Spam-E-Mails und verwenden darauf 6,5 Minuten. Es liegt eine Produktivitätseinbuße von 1,4 % vor, die pro Arbeitnehmer jährlich 874 US-$ Personalkosten verursacht. Zugrunde gelegt sind eine tägliche Arbeitszeit von 8 Stunden und Personalkosten in Höhe von 30 US-$ pro Stunde.
2. Aufgrund der Masse der Spam-Nachrichten entsteht ein Bedarf nach größeren Datenübertragungsraten und Bandbreiten sowie nach Prozessorzeit zur Verarbeitung oder Weiterleitung der E-Mails. Ferner benötigen Filter- und andere Anti-Spam-Programme Rechenzeit. Daher entstehen Spam zurechenbare Hardwarekosten und Kosten zur Reservierung von Bandbreiten.
3. Im Bereich der Anti-Spam-Software fallen Kosten für den Erwerb, den Betrieb und die Administration an. Diese enthalten Software- und Personalkosten.
4. Für Unternehmen, insbesondere ISP und ESP, die rechtliche Schritte gegen Spammer prüfen oder einleiten, entstehen Rechtskosten.
5. Schadhafte Software (Viren, Würmer und Trojanische Pferde) wird auch über Spam-Nachrichten verbreitet. Die Kosten für deren Identifizierung und Entfernung gehören zu den indirekten Schäden, für die Spam verantwortlich ist.

Weitere Probleme im Zusammenhang mit Spam (z. B. Identitätsdiebstahl und reduziertes Konsumentenvertrauen) werden in [OECD04] diskutiert.

2 Anti-Spam-Ansätze

Viele Privatpersonen, nicht-kommerzielle Organisationen und Unternehmen haben sich dem Kampf gegen Spam bereits gewidmet. [OECD04] gibt einen Überblick über ungefähr 40 nicht-kommerzielle nationale und internationale Anti-Spam-Organisationen. Neben ökonomischen, sozialen und rechtlichen Ansätzen gegen Spam existieren zahlreiche technische Lösungen, die in der Praxis derzeit am bedeutendsten sind. Eine zweite Dimension zur Klassifizierung der Ansätze besteht darin zu unterscheiden, ob es sich um präventive oder erkennende Maßnahmen handelt, wobei die erste Klasse zu präferieren ist, da eine Spam-E-Mail, die ggf. erst bei der Organisation des Empfängers als solche erkannt wird, bereits mehrere E-Mail-Knoten durchlaufen und dabei Hardware-, Software- und Netzwerk-Ressourcen gebunden hat. Die beiden Klassen werden im Folgenden auch als Abwehrarten bezeichnet.

2.1 Rechtliche Ansätze

Eine rechtliche Prävention haben bereits viele Staaten vorgenommen. Prinzipiell ist zwischen zwei Varianten zu differenzieren: (1) Anwendung existierender Regelungen und Gesetze, die Aspekte von Spam adressieren, beispielsweise Gesetze zum Schutz der Verbraucher gegen irreführende Werbung oder gegen die Distribution pornographischer Bilder, (2) Spam-spezifische Erweiterung oder Schaffung neuer gesetzlicher Bestimmungen. Der OECD-Bericht zum Spam-Workshop [OECD04] gibt einen ausführlichen Überblick über die länderspezifischen gesetzlichen Regelungen der OECD-Mitgliedstaaten. Dort wird eine heterogene Rechtslandschaft beschrieben, die sich darin manifestiert, dass einige Staaten oder Bundesstaaten das „Opt-out-Modell“ wählen, nach dem unaufgeforderte E-Mail-Werbung grundsätzlich legal ist, solange der Empfänger nicht widerspricht, während andere das „Opt-in-Modell“ zugrunde legen, bei dem ohne vorherige Zustimmung des Empfängers unaufgeforderte E-Mail-Werbung illegal ist. [Köch04] diskutiert den Versuch globaler rechtlicher Lösungsansätze detaillierter. Einige Staaten hatten 2003 noch keine spezifischen Anti-Spam-Gesetze, hierzu gehörten u. a. die Türkei und Neuseeland. Es ist anzunehmen, dass auch viele Länder, die nicht Mitglieder der OECD sind, weder Anti-Spam-Gesetze haben noch planen. Solange rechtliche Schlupflöcher bestehen, ist es zweifelhaft, ob rechtliche Ansätze effektiv Spam adressieren können. Ferner erscheint unklar, welche rechtlichen Regelungen gelten, wenn sich ein Spammer, der sich im Land A aufhält, in einen Computer in Land B einloggt, um von dort aus einen offenen MTA (mail transfer agent), auch offenes E-Mail-Relay genannt, in Land C zu verwenden. Dem globalen Phänomen „Spam“ mit unterschiedlichen nationalen Regelungen zu begegnen, erscheint wenig erfolgversprechend.

2.2 Soziale Ansätze

Soziale Ansätze können Spam zwar generell nicht verhindern, aber sie können E-Mail-Teilnehmer über Spam und den Umgang damit informieren. Zahlreiche Verbraucherschutzorganisationen und Regierungsbehörden haben Spam und Schutzmöglichkeiten in der Öffentlichkeit verstärkt thematisiert. Beispiele sind das „Center for Democracy and Technology“ [CfDT03] und das australische Finanzministerium, welches das „Australian E-commerce Best Practice Model“ [ADT00] entwickelt hat. Die US-amerikanische „Federal Trade Commission“ betreibt eine verbraucherorientierte Webseite zu Spam (http://www.ftc.gov/bcp/conline/edcams/spam/coninfo.htm). Wie bereits oben erwähnt, listet ein OECD-Bericht [OECD04] zahlreiche weitere Anti-Spam-Organisationen auf.

Der Ansatz, E-Mail-Adressen vor Spammern zu verbergen, ist kaum erfolgversprechend, wenn man deren (nicht oder kaum vermeidbare) Möglichkeiten betrachtet, an gültige E-Mail-Adressen zu gelangen [CfDT03].

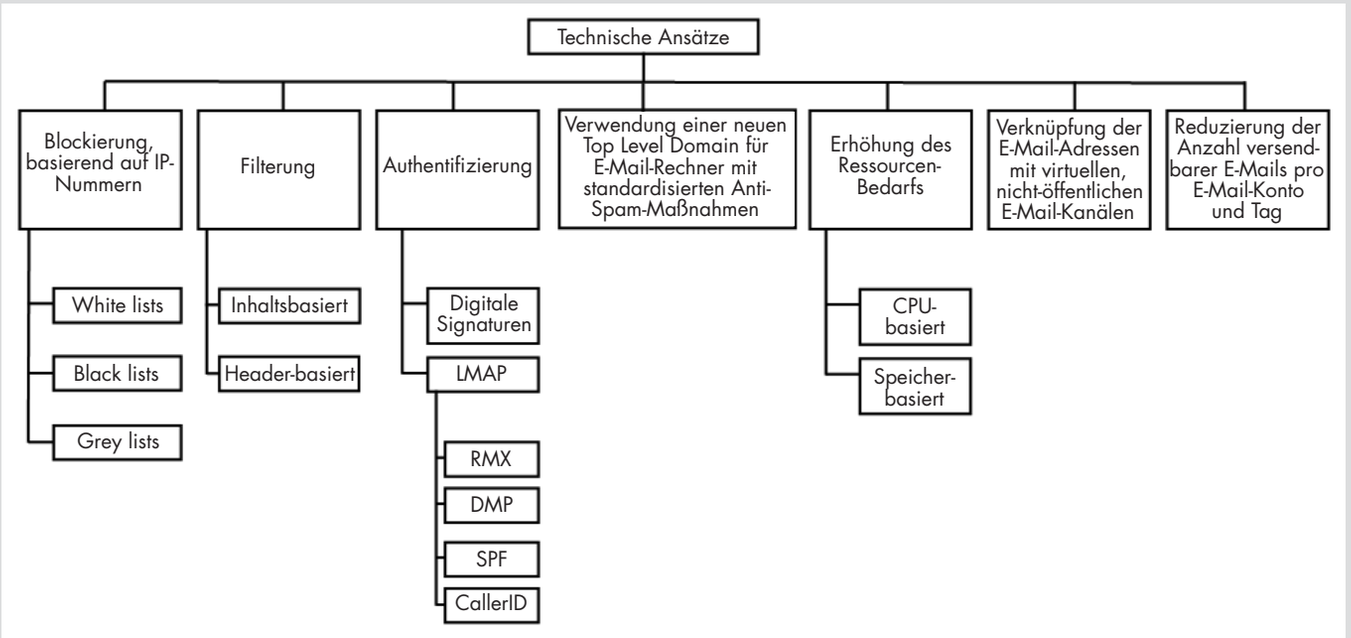

Bild 1 Technische Anti-Spam-Ansätze

2.3 Ökonomische Ansätze

Es finden sich ökonomische Ansätze, bei denen E-Mail-Versender bezahlen müssten. Beispielsweise ließen sich E-Mail-Briefmarken einführen. Generell lassen sich die Verfahren, bei denen jede E-Mail bezahlt werden muss, von den Verfahren unterscheiden, bei denen ausschließlich die vom Empfänger als unerwünscht deklarierten E-Mails vom Versender bezahlt werden müssen. ECT News Networks™ [ENN04] berichtet von Microsofts and Yahoos Interesse an einem Ansatz, *„[. . .] that would charge bulk e-mailers 1 U.S. cent for each piece of e-mail in an effort to differentiate legitimate e-mail marketing from spam.“* [Fahl02] schlägt vor, dass ein E-Mail-Versender dem Empfänger vor der Zustellung einer E-Mail einen Geldbetrag anbieten muss, den der Empfänger festlegt. Der Empfänger kann frei über die Annahme oder Ablehnung des Betrags entscheiden. Derartige Verfahren beeinträchtigen jedoch die Kommunikationsfreiheit im Internet, ferner sind mit der Einführung von E-Mail-Gebühren nennenswerte technische Veränderungen verbunden, da die Infrastruktur (Protokolle, E-Mail-Programme usw.) zu adaptieren ist. Drittens sind internationale Bezahlmechanismen zu entwickeln, zu implementieren und soziotechnisch zu etablieren.

2.4 Technische Ansätze

Der größte Teil der Anti-Spam-Ansätze ist technischer Natur (s. Bild 1), wobei die Ansätze oftmals auch komplementär implementiert werden. Beispielsweise vereint die Open-Source-Software SpamAssassin (http://www.au.spamassassin.org), die vom Rechenzentrum der RWTH Aachen eingesetzt wird, die Anwendung unterschiedlicher Filter und „black lists“.

Bevor die dargestellten Ansätze diskutiert werden, wird kurz der technische Ablauf der Versendung einer SMTP-E-Mail skizziert: Der Absender nutzt meist einen E-Mail-Client, der auch als MUA (mail user agent) bezeichnet wird. Dieser Client sendet die E-Mail an einen lokalen SMTP-Knoten, auch als MTA (mail transfer agent) bezeichnet. Im Folgenden werden seriell ggf. weitere MTAs durchlaufen, bis der erste MTA der Zielorganisation erreicht wird. Von dort wird die E-Mail (meist über weitere lokale MTAs) zum MDA (mail delivery agent) weitergereicht , der sie in dem Postfach des Adressaten ablegt. Schließlich ruft der lokale MUA die E-Mail über ein Protokoll wie POP oder IMAP ab. Der Weg einer E-Mail wird im E-Mail-Header protokolliert und kann vom Empfänger mithilfe seines E-Mail-Clients eingesehen werden.

2.4.1 Blockierung

Die Blockierung von E-Mails ist ein weit verbreiteter Mechanismus, bei dem die Weiterleitung von der IP-Adresse des versendenden MTA abhängt. Solche (sendenden) MTAs, die dem empfangenden MTA aufgrund eigener Historie, aufgrund der Historie anderer, kooperierender MTAs oder aufgrund eines Eintrags in einer globalen Anti-Spam-Liste als (potenzielle) Spam-Quelle bekannt sind, werden auf eine so genannte „black list“ gesetzt. E-Mails von MTAs dieser Liste werden nicht weitergeleitet. Spamhaus Block List [SpPr04] ist ein Beispiel für einen Internet-Dienst, der aktuelle IP-Listen bekannter Spam-MTAs zur Verfügung stellt und diese über eine Maschine-Mensch-Schnittstelle (als WWW-Seiten) und eine technische Schnittstelle für E-Mail-Server anbietet. Listen offener E-Mail-Relays und damit potenzieller Spam-MTAs finden sich unter http://www.ordb.org, http://www.spammingbureau.com/email-blacklist.php und http://www.mail-abuse.org. Analog enthalten so genannte „white lists“ die IP-Adressen vertrauenswürdiger E-Mail-MTAs. Kompromittiert werden können beide Listenarten mittels IP-Spoofing (und TCP-Hijacking), bei dem ein Spam versendender E-Mail-MTA die IP-Pakete mit gefälschten IP-Nummern versieht. Dabei kann er aufgrund des 3-Wege-Handshaking, das bei TCP zum Verbindungs-

aufbau erfolgt, nur schwer eine TCP-Verbindung mit einer falschen IP-Nummer initiieren – dann würde die vom Client zum endgültigen Verbindungsaufbau benötigte TCP-Antwort des Servers nicht beim Spammer, sondern beim Server mit der angegebenen IP-Adresse ankommen –, er kann jedoch eine regulär initiierte TCP-Verbindung zwischen zwei MTAs übernehmen (Hijacking), indem er die dazu benötigte(n) Sequenz- und Bestätigungsnummer(n) mitliest (sniffing) oder errät (guessing). Außerdem wechseln Spammer oft ihre MTAs und damit auch die Quell-IP-Nummern. Das Blockieren aller E-Mails eines ISP oder ESP mag noch akzeptabel erscheinen, auch wenn dabei viele reguläre E-Mails der Heuristik zum Opfer fallen, das Blockieren der MTAs ganzer Regionen oder Länder kann hingegen leicht zu einer digitalen Spaltung führen.

Derzeit werden neben den vorgestellten Listen so genannte „grey lists“ diskutiert und eingesetzt [Harr03]: Es ist gängige Praxis, dass MTAs eine E-Mail (ggf. mehrfach) erneut zuzustellen versuchen, wenn der erste Versuch gescheitert ist, um temporäre Ausfälle von E-Mail-Servern auf der Empfängerseite aufzufangen. Viele Spam versendende MTAs hingegen verzichten auf diese Wiederholungsfunktion, wenn (aufgrund einer Wörterbuch- oder „brute force“-Attacke) mit einer großen Anzahl abgelehnter Spam-Mails gerechnet wird, deren Zieladressen nicht existieren. Das erneute Versenden ist in diesem Fall mit einer geringen Erfolgsaussicht verbunden und würde Rechenzeit und Übertragungskapazität des Spammers in Anspruch nehmen, die er für das Verschicken weiterer E-Mails benötigt. Dieses Verhalten können sich empfangende MTAs zu Nutze machen, indem sie beim ersten Eintreffen einer E-Mail deren Empfang zunächst verweigert, den Zustellwunsch jedoch für einen vorher festgelegten Zeitraum – meist einige Minuten – speichert, innerhalb dessen ein erneuter Zustellversuch derselben E-Mail akzeptiert wird und diese zu einem anderen MTA weitergeleitet oder im Postfach des Benutzers abgelegt wird.

2.4.2 Filterung

Während die Blockierung nur herkunfts- bzw. IP-basiert vorgeht, ist eine Filterung flexibler, da alle Daten einer E-Mail einbezogen werden können. Werden ausschließlich Daten des Headers berücksichtigt, also vor allem die Inhalte des FROM-Eintrags, des SUBJECT-Eintrags, der RECEIVED-Einträge und auch des verwendeten Zeichensatzes als CONTENT-TYPE-Eintrag – manche Filter sehen in E-Mails mit chinesischem Zeichensatz ein Indiz für das Vorliegen einer Spam-E-Mail –, können Spammer diese Einträge analog zur Blockierung fälschen (Spoofing) und damit Filtermechanismen umgehen. Diese leichte Fälschbarkeit der Metadaten ist darauf zurückzuführen, dass SMTP als reguläres Internet-E-Mail-Protokoll die Integrität und Authentizität des E-Mail-Headers nicht adressiert.

Inhaltsbasiertes Filtern bezieht den E-Mail-Text ein, indem üblicherweise nach „verdächtigen“ Worten oder Phrasen gesucht wird, die in vielen Spam-E-Mails bislang auftraten. Die MTA-spezifische Historie von Spam-E-Mails kann auch Spam-typische Sequenzen von Satzzeichen und Kontrollzeichen (die ersten 32 Zeichen des ASCII-Zeichensatzes wie beispielsweise „CR“ (carriage return)) einbeziehen. Als effektiv gelten weit verbreitete, auf der Bayes-Regel basierende statistische Filter, die historische Daten zur Klassifizierung neuer E-Mails nutzen. Um diese Filter anwenden zu können, wird für bestimmte Worte und Token (Dollar-Zeichen, IP-Adressen etc.) jeweils eine Wahrscheinlichkeit bestimmt, mit der eine neu eintreffende E-Mail eine Spam-E-Mail ist. Diese wird dann auf die Worte und Token hin untersucht und es wird basierend auf den Einzelwahrscheinlichkeiten eine Spam-Gesamtwahrscheinlichkeit ermittelt, wobei unterschiedliche Aggregationsfunktionen zu verschiedenen Filtern führen. Geht man bei der Aggregation davon aus, dass das Auftreten von Worten und Token einer stochastischen Unabhängigkeit unterliegt, spricht man von einem naiven Bayes-Filter. Falls die Gesamtwahrscheinlichkeit einen festzulegenden Schwellenwert überschreitet (oft wird 90 % oder mehr gewählt), wird die E-Mail als Spam klassifiziert. Folgendes Beispiel zeigt die Bayes-Regel-basierte Ermittlung der Wahrscheinlichkeit, mit der eine E-Mail Spam ist, wenn sie das Wort „Hypothek“ enthält:

Die Bayes-Regel lautet

$$P(S \mid H) = \frac{P(H \mid S) \cdot P(S)}{P(H)},$$

die Ereignisse A und B seien wie folgt definiert:

S: eine E-Mail ist Spam
H: in einer E-Mail tritt das Wort „Hypothek“ auf

Folgende historische Daten seien gegeben:

- Es traten bislang 5000 Spam-E-Mails auf; 600 davon enthielten das Wort „Hypothek“.
- Es traten bislang 500 Nicht-Spam-E-Mails auf; 9 davon enthielten das Wort „Hypothek“.

Die Anwendung der Bayes-Regel ergibt folgende Wahrscheinlichkeit:

$$P(S \mid H) = \frac{(600/5000) \cdot (5000/5500)}{(609/5500)} \approx 98{,}52\,\%$$

Bemerkenswert ist, dass die Bayes-Spamwahrscheinlichkeit einer konkreten E-Mail, die dieses Wort enthält, mehr als 98 % beträgt, obwohl das Wort „Hypothek“ nur in 12 % aller Spam-E-Mails vorkommt. Bedeutsam ist hier, dass dieses Wort nur selten (in weniger als 2 % aller gespeicherten Fälle) in Nicht-Spam-E-Mails auftritt. Ein ausführlicheres Beispiel findet sich bei [Trei04]; einen guten Überblick gewährt [Link03].

Die historischen Daten können nicht aus öffentlichen Datenbanken entnommen werden, sondern sind unternehmensspezifisch zu erfassen und auszuwerten. Bei einem Finanzdienstleistungsunternehmen dürfte sich für das obige Beispiel eine deutlich geringere Wahrscheinlichkeit ergeben als für eine Hochschule. Bayes-Filter, die sich auf der Basis neuer Spam-E-Mails und Nicht-Spam-E-Mails kontinuierlich aktualisieren, werden auch als lernend bezeichnet.

Sowohl die Blockierung als auch die Filterung leiden als Heuristiken unter zwei möglichen Klassifikationsfehlern (Fehler erster und zweiter Ordnung): So genannte „false negatives“ liegen vor, wenn Spam-E-Mails als solche nicht erkannt werden, so genannte „false positives“, wenn Nicht-Spam-E-Mails fälschlicherweise als Spam klassifiziert werden. Letztgenannter Fehler ist der kritischere, da wichtige Informationen ungelesen bleiben können. Ein prominentes Beispiel ist der Fall, in dem einige Abgeordnete des britischen „House of Commons“ Diskussionspapiere bezüglich des „Sexual Offences Bill“ aufgrund eines zu restriktiven Filtermechanismus nicht erhielten [BBC03].

2.4.3 Authentifizierung

Spammer nutzen oft den Umstand aus, dass derzeit keine Authentifizierung des Absenders erforderlich ist, indem sie eine falsche E-Mail-Adresse vortäuschen („spoofen“). Ein Lösungsansatz besteht in der Verwendung digitaler Signaturen, die seit den 70er Jahren bekannt sind und die auf der Pub-

lic-Key-Kryptographie basieren. Digitale Signaturen ermöglichen eine Überprüfung der Absenderidentität und adressieren damit wirksam das „Spoofen“ von E-Mail-Adressen und IP-Nummern. Yahoo entwickelt derzeit das System „Domain Key“, das für jede Domäne, jedoch nicht für jeden Benutzer ein Schlüsselpaar vorsieht. Vor dem E-Mail-Versand wird eine domänenspezifische Signatur mithilfe des privaten Schlüssels erstellt und in die E-Mail integriert. Der empfangende MTA kann dann mithilfe des öffentlichen Schlüssels prüfen, ob die Nachricht authentisch ist, und sie bei negativem Ergebnis ablehnen. Entsprechende Realisierungen benötigen bei einer größeren Teilnehmeranzahl jedoch eine einheitliche Public-Key-Infrastruktur (PKI), deren Aufbau und Betrieb oft kostenintensiv ist. Von der Existenz einer weltweit verfügbaren PKI sind wir derzeit weit entfernt.

Ohne den Aufbau einer PKI kommen LMAP-Ansätze (Lightweight MTA Authentication Protocol) aus [LeDe04]. Es handelt sich dabei um eine Familie DNS-basierter (Domain Name System) Ansätze, die überprüfen, ob eine E-Mail, die beispielsweise als Absenderadresse `buffy@sunnydale.com` besitzt, auch von einem MTA der Organisation `sunnydale.com` versendet wurde. Ist dies nicht der Fall, so wurde die Absender-E-Mail-Adresse verändert oder es wurde ein intermediärer MTA als E-Mail-Relay verwendet. Es liegt dann ein Spam-Verdacht vor und das empfangende E-Mail-System (MTA, MDA oder MUA) kann die Annahme der E-Mail ablehnen. Damit dieser Ansatz in der Praxis tragfähig ist, müssen zulässige MTAs aller Organisationen als solche in DNS-Datensätzen abgelegt werden. Offen ist die Frage, wie mit Organisationen verfahren wird, die ihre MTAs nicht derartig registrieren. Auch das so genannte „Forwarden“ von E-Mails ist zu adressieren: Wird beispielsweise dem E-Mail-Server `yoda.winfor.rwth-aachen.de` eine (reguläre) E-Mail mit dem Absender `schryen@gmx.net` und dem Adressaten `determann@winfor.rwth-aachen.de` zugestellt und wird diese E-Mail an die Adresse `lorenz.determann@rewe.de` weitergereicht, so erhält der Rewe-MTA diese E-Mail versehen mit einem GMX-Absender von einem WINFOR-MTA. Der DNS-Test zeigt dies auf und die reguläre E-Mail wird ggf. nicht akzeptiert. Dies kann umgangen werden, wenn die Absenderadresse im SMTP-Envelope an den jeweiligen sendenden MTA angepasst wird. Der SMTP-Envelope lässt sich wie folgt beschreiben: Bei jedem E-Mail-Transfer zwischen zwei MTAs wird der E-Mail bestehend aus Header und dem eigentlichen Inhalt ein so genannter „Envelope“ vorangestellt, der die E-Mail-Adressen des Absenders und des Adressaten, die IP-Nummer des sendenden MTAs und den Fully Qualified Domain Name (FQDN) des sendenden MTAs enthält. Es handelt sich dabei um einen virtuellen Umschlag, da sich dessen Inhalt aus den Kommunikationsdaten zwischen zwei MTAs ergibt.

Reverse MX (RMX) [Dani03], *Designated Mailers Protocol* (DMP) [Fecy03], *Sender Policy Framework* (SPF) [LeWo04], das von AOL getestet wird, und Microsofts *Caller ID for E-Mail* [MiCo04] gehören zu den derzeit meist diskutierten Ansätzen. Die *Anti-Spam Research Group* (ASRG) der *Internet Research Task Force* (IRTF) hat bislang noch keine Standardisierungsentscheidung gefällt.

Wie der Ablauf eines DNS-basierten Ansatzes aussehen kann, wird am Beispiel von SPF und einem konkreten Szenario illustriert, wobei der empfangende MTA (`relay.rwth-aachen.de`) als SPF-Client bezeichnet wird, der die Authentizität des sendenden MTAs (`spielbar.com` gibt vor, `darth-vader.winfor.rwth-aachen.de` zu sein) mithilfe des SMTP-Envelope überprüft, der sich aus der in Bild 2 dargestellten SMTP-Kommunikation ergibt.

1. Der SPF-Client ist `relay.rwth-aachen.de`, der die zu authentifizierende Domäne der Sender-E-Mail-Adresse `guido.schryen@rwth-aachen.de` entnimmt.
2. Der SPF-Client führt für `rwth-aachen.de` eine SPF-Abfrage durch (spezifische DNS-Abfrage) und erhält einen SPF-Datensatz, der angibt, welche IP-Nummern zum Versenden von E-Mails verwendet werden dürfen.
3. Der SPF-Client stellt fest, dass die IP-Nummer `193.178.169.200` des sendenden MTAs, der vorgibt, ein RWTH-Rechner zu sein, nicht als zulässig im SPF-Datensatz zu `rwth-aachen.de` vermerkt ist.
4. Der SPF-Client antwortet mit der folgenden Fehlermeldung:
   `250 <guido.schryen@rwth-aachen.de>... Sender denied`

DNS-basierte Ansätze adressieren zwei Kernprobleme des Spamming nicht:

1. Sie sind kompromittierbar, wenn sich Viren oder Trojanische Pferde in „unbescholtene“ Rechner einnisten [Garf04] und die E-Mail-Daten lokaler Benutzerkonten (E-Mail-Adresse und die Zugangsdaten zum SMTP-Server) missbrauchen, um Spam zu versenden. In diesem Fall greifen DNS-basierte Ansätze nicht, vielmehr kann das Spammen auf den lokalen Benutzer zurückfallen. Das IT-Magazin „c't“ berichtet von Spammern, die Adressen infizierter Rechner von den Distributoren Trojanischer Pferde erwerben [Heis04].
2. Die Verfahren können nicht verhindern, dass ein Spammer sich regulär bei einem E-Mail-Provider ein Konto mit einem SMTP-Zugang verschafft, falsche Adressdaten hinterlegt, um nicht identifiziert werden zu können, und dann über diesen SMTP-Zugang Spam-E-Mails versendet.

2.4.4 Verwendung einer neuen Top Level Domain

Spamhaus hat der *ICANN* (Internet Corporation for Assigned Names and Numbers) kürzlich ein Vorgehen vorgeschlagen, mit dem sowohl eine technische als auch eine organisatorische Veränderung verbunden sind [ICAN04]. Die technische Veränderung bietet u. a. zwar eine neue Filter-Möglichkeit, der Top-Level-Domain-Ansatz wird jedoch in der Klassifikation (s. Bild 1) nicht unter Filterung subsumiert, da mit dem Ansatz weitergehende Möglichkeiten verbunden sind.

```
220 relay.rwth-aachen.de ESMTP Sendmail 8.12.10/8.12.7-1; Tue, 4
May 2004 16:42:16 +0200 (MEST)
HELO darth-vader.winfor.RWTH-Aachen.DE
250 relay.rwth-aachen.de Hello spielbar.com [193.178.169.200],
pleased to meet you
MAIL From:<guido.schryen@rwth-aachen.de>
```

Bild 2 Beispiel einer SMTP-Kommunikation

Nach dem Vorschlag von Spamhaus soll eine neue sTLD (sponsored Top Level Domain) eingerichtet werden, für die mit `.mail`, `.tmail` und `.mta` mehrere Namensvorschläge existieren und die nur in Zusammenhang mit dem E-Mail-Verkehr Verwendung findet. Eine existierende Domäne key – key hat die Form sld.tld (second-level-domain.top-level-domain), z. B. `rwth-aachen.de` – kann diejenigen E-Mail-MTAs, über die E-Mails versendet werden können, in einem neuen DNS-Datensatz zum Eintrag key.sTLD, z. B. rwth-aachen.de.mail, speichern lassen. E-Mails von MTAs, die keine derartige Kennzeichnung aufweisen, können vom empfangenden MTA herausgefiltert werden.

Um einen sTLD-Eintrag zu erhalten, muss nachgewiesen werden, dass derjenige, der die Domäne registriert hat (im Folgenden Registrierter genannt), für seine Domäne key bzw. die sendenden MTAs ausreichende Anti-Spam-Mechanismen implementiert hat. Die zu beachtenden Regeln werden von einer nicht-kommerziellen Organisation SO (Sponsoring Organization) festgelegt und beinhalten die folgenden Anforderungen an die Domäne key:

1. Zu jeder Domäne existieren derzeit Registrierungsinformationen, die auch als „whois"-Informationen bezeichnet werden und die über weltweit verfügbare Datenbanken (z. B. `http://www.allwhois.com`) von jedem Internetteilnehmer abgerufen werden können. Diese Informationen sollen (auf Antrag) auch für die Domäne `key.sTLD` gelten und validiert werden, sodass Registrierte, die Spamming nicht ausreichend verhindern oder sogar unterstützen, identifiziert werden können.
2. Die Domäne muss vor mindestens sechs Monaten registriert worden sein.
3. Es wird eine E-Mail-Adresse `abuse@key.sTLD` eingerichtet, an die E-Mail-Empfänger sich wenden können, wenn eine Spam-Nachricht von einem MTA der Domäne key eintrifft. Jede Nachricht an diese Adresse wird der SO zugeleitet – dies kann über einen (MX-)Eintrag im DNS sichergestellt werden –, sodass ein zentrales Beschwerde- und Kontrollsystem existiert.
4. Es wird eine WWW-Seite zu key.sTLD eingerichtet, die der Kontrolle der SO unterliegt und auf der sich Informationen über den Registrierten und dessen E-Mail-Politik finden. Außerdem muss der Registrierte auf dieser WWW-Seite die IP-Nummern und Host-Namen aller MTAs seiner Domäne angeben, die dann von der SO in das DNS eingetragen werden.
5. Wenn ein MTA der Domäne key sich bei einem externen MTA mit dem SMTP-Kommando HELO oder EHLO (Extended HELO) anmeldet, so muss er `key.sTLD` verwenden, damit der empfangende MTA ihn als sTLD-registriert erkennen und mit einer DNS-Abfrage überprüfen kann: Ist die IP-Adresse des sendenden MTAs unter `key.sTLD` registriert, so ist der MTA vertrauenswürdig im Sinne der geforderten SO-Politik.
6. Alle registrierten MTAs müssen die Versendung von Spam unterbinden.

Ferner wird die Verwendung von Authentifizierungstechniken wie den oben vorgestellten LMAP-Ansätzen empfohlen.

Die SO überprüft regelmäßig, ob die Registrierten den Anforderungen noch genügen, wobei das oben dargestellte Kontrollsystem verwendet werden kann. Für die Durchführung des operativen Betriebs beauftragt die SO einen „Registry Operator" und einen „Extra Services Operator". Mit einer sTLD-Registrierung ist nicht nur der Erwerb eines Qualitätsstatus verbunden, sondern es fällt auch eine Registrierungsgebühr an, welche die Kosten der oben geschilderten Maßnahmen decken soll.

Die Effektivität dieses Ansatzes hängt entscheidend davon ab, ob und mit welchen technischen Maßnahmen sich MTAs vor der Versendung von Spam-Nachrichten schützen lassen. Hierzu werden keine Angaben gemacht, sodass dieser Ansatz bislang nur ein technisch-organisatorisches Gerüst ist.

2.4.5 Erhöhung des Ressourcenbedarfs

Diese Ansätze zielen auf eine geringe Erhöhung des Ressourcenbedarfs ab, der für die Versendung einer einzelnen E-Mail erforderlich ist. Erst bei einer großen Anzahl von E-Mails werden die benötigten Ressourcen relevant.

CPU-basierte Ansätze sehen vor, dass ein E-Mail-Client pro E-Mail eine mathematische Funktion („pricing function") ausführen muss. Spammer, für die das preiswerte, millionenfache Versenden von E-Mails existenziell ist, müssen dann in CPU-Ressourcen investieren. Bereits 1992 haben Dwork und Naor [DwNa93] diesen Ansatz vorgeschlagen, der in der Open-Source-Software „hashcash" [HashoJ] praktisch umgesetzt wurde. Dieser Ansatz differenziert rein technisch über die CPU-Performanz von E-Mail-Clients, bezüglich der es große Unterschiede gibt. E-Mailer mit Zugang zu performanten Rechnern können weiterhin spammen, während reguläre E-Mailer mit sehr langsamen Rechnern benachteiligt werden. Da im Gegensatz zur CPU-Performanz die Speichergröße keine derart große Varianz aufweist, wird vorgeschlagen, an Stelle von rechenintensiven Funktionen speicherplatzintensive zu verwenden [DwGN02]. Beiden Ansätzen gemein sind die mit ihnen verbundenen hohen Umsetzungskosten, da alle E-Mail-Clients ersetzt oder zumindest aktualisiert werden müssten.

2.4.6 Verknüpfung von E-Mail-Adressen mit E-Mail-Kanälen

Die Idee, elektronische E-Mail-Kanäle zu verwenden [Hall96], ist mit E-Mail-Adressen der Form `Username-ChannelID-@Host` verbunden. Im Wesentlichen ist ein E-Mail-Konto mit einer Menge von virtuellen Kanälen zu assoziieren, die der Kontrolle des Konto-Inhabers unterliegt. Um dem Inhaber eine E-Mail zu senden, ist nicht nur die Kenntnis von `Username` und `Host` erforderlich – aus diesen besteht eine traditionelle E-Mail-Adresse –, sondern dem Versender muss auch eine nicht ableitbare `ChannelID` (Kanal-Identifikator) eines aktivierten Kanals bekannt sein; Kanäle können demzufolge auch deaktiv sein. Es obliegt dem Kontoinhaber zu entscheiden, wem er eine aktive `ChannelID` mitteilt, Spammer würden dann an der Unkenntnis eines aktiven E-Mail-Kanals scheitern. Ein offensichtliches Problem dieses Vorgehens ist der Aufwand zur Geheimhaltung und sicheren Distribution von Kanal-Identifikatoren. Des Weiteren müsste die Infrastruktur stark verändert werden, da E-Mail-Software und -Protokolle angepasst werden müssten.

2.4.7 Reduzierung der E-Mail-Anzahl

Ein Anti-Spam-Ansatz kann darin bestehen, die Anzahl der E-Mails zu begrenzen, die ein Konteninhaber täglich versenden darf. Die Erfolgsfaktoren für dieses Vorgehen bestehen darin, dass

- ESP die kontenspezifischen Zähler korrekt und sicher vor unautorisierten Zugriffen verwalten,
- die reguläre E-Mail-Kommunikation nicht beeinträchtigt wird – für legitime Massen-E-Mail wie Newsletter sind Sonderbehandlungen vorzusehen –,
- Konten nicht unautorisiert verwendet werden können und

– Spammer sich nicht kostengünstig viele Konten zulegen können oder die Erfassung gesendeter E-Mails umgehen können, indem sie einen lokalen MTA einrichten und die Verwendung eines ESP vermeiden.

Das Einrichten von E-Mail-Konten darf demnach nicht automatisiert erfolgen, sondern muss mit einem geringen, aber nicht substituierbaren manuellen Aufwand verbunden sein. Beispielsweise kann einem Bild mit einer Zufallsnummer oder Text diese(r) entnommen und zur Aktivierung in ein Formular eingegeben werden. Dieses Vorgehen stellt einen visuellen CAPTCHA-Prozess (Completely Automated Public Turing test to tell Computers and Humans Apart) dar, der von einigen E-Mail-Providern wie Yahoo und Hotmail eingesetzt wird. Derzeitige Realisierungen erweisen sich jedoch als unzureichend: [MoMa03] stellen ein Verfahren vor, mit dem 92 % aller von Yahoo erzeugten Bilder automatisch ausgelesen und damit E-Mail-Konten letztendlich maschinell angelegt werden können. Ein weiterer möglicher Angriff auf CAPTCHA besteht darin, dass derartige Bilder in andere Webseiten integrierbar sind, auf denen Benutzer aufgefordert werden, die gewünschte Information in ein Textfeld einzugeben, um sich ihrerseits Zugang zu einer Webseite zu verschaffen. Diese Eingabe wird dann automatisch in das Textfeld der ursprünglichen Anmeldemaske übertragen.

Setzt man die Lösung dieses Problems voraus und dürfen im Rahmen der vorgeschlagenen Begrenzung beispielsweise 200 E-Mails pro Tag und Konto versendet werden, müsste ein Spammer 5000 E-Mail-Konten manuell einrichten (lassen), um an einem Tag eine Million Spam-E-Mails versenden zu können, eine für Spammer nicht ungewöhnliche E-Mail-Anzahl.

Tabelle 1 fasst die vorgestellten Ansätze mit ihren Grenzen und Nachteilen zusammen.

3 Zusammenfassung und Ausblick

Spam ist nicht mehr bloß ein Ärgernis, sondern hat mittlerweile eine nennenswerte ökonomische Bedeutung erfahren, da jährlich geschätzt mehrere Milliarden US-$

Tabelle 1 Grenzen, Nachteile und Abwehrarten von Anti-Spam-Ansätzen

Ansatz			Grenzen und Nachteile	Abwehrart	
				Prävention	Erkennung
Rechtlich			– weltweite Homogenisierung schwierig – manche Länder besitzen keine Anti-Spam-Gesetze	X	
Sozial			– wenig effektiv – flankierende Maßnahme	(X)	
Ökonomisch			– starker Einfluss auf Infrastruktur und Client-Software	X	
Technisch	Blockierung	White lists	– Spoofing		X
		Black lists	– E-Mail-MTAs werden häufig gewechselt		
		Grey lists			
	Filterung	Inhaltsbasiert	– Heuristiken mit Fehlern erster und zweiter Art („false negatives" und „false positives")		X
		Header-basiert			
	Authentifizierung	Digitale Signaturen	– Notwendigkeit einer kostenintensiven Public-Key-Infrastruktur (PKI) – schwierige Etablierung einer weltweiten PKI	X	X
		Lightweight MTA Authentication Protocols (LMAP)	– Infizierung von Rechnern Dritter – Verwenden regulär eingerichteter Konten		X
	Verwendung einer neuen Top Level Domain für E-Mail-Rechner mit standardisierten Anti-Spam-Maßnahmen		– Rahmengerüst, das voraussetzt, dass MTAs registrierter Domänen das Versenden von Spam-E-Mails verhindern können	X	X
	Erhöhung des Ressourcenbedarfs	CPU-basiert	– starker Einfluss auf Infrastruktur und Client-Software	X	
		Speicherbasiert			
	Verknüpfung der E-Mail-Adresse mit virtuellen, nichtöffentlichen E-Mail-Kanälen		– starker Einfluss auf Infrastruktur	X	
	Reduzierung der Anzahl versendbarer E-Mails pro E-Mail-Konto und Tag		– Zwang zur Kontenführung bei allen ESP ist schwer zu erreichen – geringere Flexibilität, da die Verwendung eines ESP bei der Versendung obligatorisch wird	X	

Schaden auftreten. Neben rechtlichen, ökonomischen und sozialen Ansätzen wurden zahlreiche technische vorgeschlagen und praktisch umgesetzt. Leider zeigt die tägliche Spam-Flut, dass die implementierten Ansätze nicht ausreichend greifen. Vielmehr ist die weltweite Anti-Spam-Gemeinschaft weiterhin fragmentiert und es werden (wirtschaftlich motivierte) Standardisierungskämpfe ausgefochten. Es besteht weiterhin ein akuter Bedarf nach effektiven und langfristigen Lösungen, wollen wir das Internet als weltweit preiswertes und flexibles Kommunikationssystem nicht in Gefahr sehen.

Literatur

[ADT00] *Australian Department of the Treasury:* Australian E-commerce Best Practice Model. http://www.ecommerce.treasury.gov.au/html/ecommerce.htm, 2000, Abruf am 2004-05-25

[BBC03] *BBC:* E-mail vetting blocks MPs' sex debate. http://news.bbc.co.uk/1/hi/uk_politics/2723851.stm, 2003, Abruf am 2004-05-01.

[Brig03a] *Brightmail:* Brightmail Reports on Spam Trends of 2003. http://www.brightmail.com/pressreleases/121803_spam_2003.html, 2003, Abruf am 2004-05-01.

[Brig03b] *Brightmail:* The State of Spam – Impact & Solutions. http://www.brightmail.com/press/state_of_spam.pdf, 2003, Abruf am 2004-05-01.

[CfDT03] *Center for Democracy & Technology:* Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report. http://www.cdt.org/speech/spam/030319spamreport.shtml, 2003, Abruf am 2004-05-01.

[CNIL99] *Commission Nationale de l'Informatique et des Libertés:* Le Publipostage Électronique Et La Protection Des Données Personnelles. http://www.cnil.fr/thematic/docs/publpost.pdf, 1999, Abruf am 2004-05-01.

[Dani03] *Danisch, H.:* The RMX DNS RR and method for lightweight SMTP sender authorization. Internet Draft. http://www.ietf.org/internet-drafts/draft-danisch-dns-rr-smtp-03.txt, 2003, Abruf am 2004-05-01.

[DwGN02] *Dwork, C.; Goldberg, A.; Naor, M.:* On Memory-Bound Functions for Fighting Spam. Microsoft Research Report. http://research.microsoft.com/research/sv/PennyBlack/demo/ lbdgn.pdf, 2002, Abruf am 2004-05-01.

[DwNa93] *Dwork, C.; Naor, M.:* Pricing Via Processing Or Combatting Junk Mail. In: Lecture Notes in Computer Science (1993) 740, S. 137–147, Proceedings of CRYPTO'92. http://research.microsoft.com/research/sv/PennyBlack/junk1.pdf, Abruf am 2004-05-01.

[ENN04] *ECT News Network:* ISPs Consider Digital Stamps To Fight Spam. http://www.technewsworld.com/perl/story/32760.html, 2004-02-03, Abruf am 2004-05-25.

[Fahl02] *Fahlman, S. E.:* Selling Interrupt Rights: a way to control unwanted e-mail and telephone calls. In: IBM Systems Journal 41 (2002) 4, S. 759–766. http://www.research.ibm.com/journal/sj/414/forum.pdf, Abruf am 2004-05-01.

[Fecy03] *Fecyk, G.:* Designated Mailers Protocol – A Way to Identify Hosts Authorized to Send SMTP Traffic. Internet Draft. http://asrg.kavi.com/apps/group_public/download.php/24/DMP, 2003, Abruf am 2004-05-01.

[Garf04] *Garfinkel, Simon:* False Hope for Stopping Spam. MIT Enterprise Technology Review. http://www.technologyreview.com/articles/wo_garfinkel020404.asp, 2004-04-02, Abruf am 2004-05-01.

[GaDr01] *Gauthronet, S.; Etienne Drouard, E.:* Unsolicited Commercial Communications and Data Protection. Commission Of The European Communities. http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_en.pdf, 2001, Abruf am 2004-05-01.

[Hall96] *Hall, R.:* Channels: Avoiding Unwanted Electronic Mail. Proceedings DIMACS Symposium on Network Threats DIMACS, 1996. ftp://ftp.research.att.com/dist/hall/papers/agents/channels-long.ps, Abruf am 2004-05-01.

[Harr03] *Harris, E.:* The Next Step in the Spam Control War: Greylisting. http://projects.puremagic.com/greylisting/, 2003, Abruf am 2004-05-01.

[HashoJ] *Hashcash.org:* Hashcash. http://www.hashcash.org/, Abruf am 2004-05-01.

[Heis04] *Heise:* Uncovered: Trojans as Spam Robots. http://www.heise.de/english/newsticker/news/44879, 2004-02-21, Abruf am 2004-05-01.

[ICAN04] ICANN: New sTLD RFP Application .mail. http://www.icann.org/tlds/stld-apps-19mar04/mail.htm, 2004, Abruf am 2004-05-01.

[Köch04] *Köcher, J.:* Anti-Spam-Gesetze: Der Versuch globaler rechtlicher Lösungsansätze. In: DFN Mitteilungen 64 (2004) 3, S. 29–30.

[LeDe04] *Levine, J.; DeKok, A. et al.:* Lightweight MTA Authentication Protocol (LMAP) Discussion and Comparison. Internet Draft. http://asrg.kavi.com/apps/group_public/download.php/31/draft-irtf-asrg-lmap-discussion-00.txt, 2004, Abruf am 2004-05-01.

[LeWo04] *Lentczner, M.; Wong, M. W.:* Sender Policy Framework (SPF) – A Convention to Describe Hosts Authorized to Send SMTP Traffic. Internet Draft. http://spf.pobox.com/draft-mengwong-spf-00.txt, 2004, Abruf am 2004-05-01.

[Link03] *Linke, A.:* Spam oder nicht Spam? E-Mail sortieren mit Bayes-Filtern. In: c't magazin für computertechnik (2003) 17, S. 150–153.

[MiCo04] *Microsoft Corporation:* Caller ID for E-Mail: The Next Step to Deterring Spam. http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx, 2004, Abruf am 2004-05-01.

[MoMa03] *Mori, G.; Malik, J.:* Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 16.–22.06.2003, Wisconsin. http://www.cs.berkeley.edu/~mori/research/papers/mori_cvpr03.pdf, 2003, Abruf am 2004-05-01.

[Muel04] *Mueller, S. H.:* What is spam? Website of abuse.net. http://spam.abuse.net/overview/whatisspam.shtml, 2004, Abruf am 2004-05-01.

[NOIE02] *National Office for the Information Economy:* Final Report Of The NOIE Review Of The Spam Problem And How It Can Be Countered. http://www.noie.gov.au/publications/NOIE/spam/final_report/index.htm, 2002, Abruf am 2004-05-01.

[NuRe03] *Nucleus Research:* Spam: The Silent ROI Killer. Research Note D59, 2003. http://www.gwtools.com/sales/pdf/spam_roi_analysis.pdf, Abruf am 2004-05-01.

[OECD04] *OECD:* Background Paper For The OECD Workshop On Spam, 2003. http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp(2003)10-final, 2004-01-22, Abruf am 2004-05-01.

[SpPr04] *The Spamhaus Project:* The Spamhaus Block List (SBL) Advisory Frequently Asked Questions. http://www.spamhaus.org/sbl/sbl-faqs.lasso, 2004, Abruf am 2004-05-01.

[Trei04] *Treiber, M.:* Bayes Spamfilter. http://141.30.51.183/~treiber/statistik2/folien13_spamfilter.pdf, 2004-02-23, Abruf am 2004-05-17.

Abstract

Effectiveness of Anti-Spam Approaches

Spam as unsolicited email has certainly crossed the border of just being bothersome. In 2003, it surpassed legitimate email – growing to more than 50% of all Internet emails. Annually, it causes economic harms of several billion Euros. Fighting spam, beside legal approaches especially technical means are deployed in practical systems, mainly focussing on blocking and filtering mechanisms.

This article introduces into the spam field and describes, assesses, and classifies the currently most important approaches against spam.

Keywords: Spam, Email, Spoofing, Blocking, Filtering, Lightweight Mail Transfer Agent Authentication Protocol (LMAP)