Analyse, Test und Bewertung von clientseitigen Spam-Filtern

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der
Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Schneider Vorname: Tobias

[redacted] [redacted] [redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 09.01.2008

Inhaltsverzeichnis

1 Einleitung

1.1 Problemstellung

Neben dem World Wide Web hat die Funktion E-Mail von den Internetdiensten die größte Bedeutung erlangt und sich neben herkömmlichen Kommunikationsmitteln wie Brief oder Telefon etabliert.

Als Erfinder der E-Mail gilt Ray Tomlinson. Er entwickelte 1971/72 ein Programm, mit dem sich innerhalb des ARPANET[1] elektronische Nachrichten versenden und empfangen ließen. Bis Mitte/Ende der 80er Jahre wurde das Medium E-Mail hauptsächlich für wissenschaftliche Zwecke genutzt, da der Großteil der vernetzten Rechner nur über universitäre Einrichtungen zugängig war. Anfang der 90er Jahre begann die Kommerzialisierung des Internets, wodurch ein größerer Personenkreis Zugang zu dem Medium E-Mail erhielt. Mit der Kommerzialisierung traten auch Mißbrauchsfälle der Funktion E-Mail auf: 1994 wurden Spam-Mails empfangen, in denen eine Anwaltskanzlei eine Lotterie für „Green Cards“ bewarb.[2]

Der Versand von Werbung per E-Mail fand aufgrund der minimalen Kosten zahlreiche Nachahmer. Heute beträgt der Anteil von Spam-Mails an den gesamten E-Mails 75-80%.[3] Spam ist aufgrund der verursachten Kosten (u. a. Produktivitätsausfälle aufgrund der zur Sortierung der E-Mails benötigten Arbeitszeit) zu einem ernstzunehmenden betriebs- und volkswirtschaftlichen Problem geworden. Einige Experten befürchten daher einen „Kollaps des Mediums E-Mail“[4].

Um gegen die Spamflut vorzugehen, wird u. a. versucht, das Geschäftsmodell der Spammer anzugreifen, das auf dem günstigen und massenhaften Versand von E-Mails fußt. Um aktuell eine effiziente Nutzung des Kommunikationsmittels E-Mail zu ermöglichen, werden Spam-Filter eingesetzt. Das Filtern der E-Mails kann auf Ebene des empfangenden Mail-Servers und/oder bei dem Abruf der auf dem Server gespeicherten E-Mails durch den Client vorgenommen werden. Gegenstand dieser Arbeit sind in clientseitige Spam-Filter.

Die ersten Spam-Filter durchsuchten die E-Mails nach Schlüsselwörtern. Wurde der Spam-Filter bei einer E-Mail fündig, wurde sie gelöscht bzw. in einen Spam-Ordner verschoben. Dieser Ansatz der Filterung brachte zwei Probleme mit sich: Einerseits genügte das Vorhandensein eines der Schlüsselwörter um eine erwünschte E-Mail fälschlicherweise zu löschen. Andererseits konnten die Spammer die Erkennung ihrer E-Mails relativ einfach vermeiden, indem sie die Schlüsselwörter verfälschten oder durch andere Wörter ersetzten.[5]

---

[1] Advanced Research Projects Agency Network. Dieses Netzwerk gilt als der Vorgänger des Internet. Vgl. Stahlknecht/Hasenkamp [2002, S. 113].

[2] Vgl. von der Helm.

[3] Vgl. Rossow [2007, S. 3 f.]. Andere Quellen gehen von einem noch höheren Anteil aus. Zu beachten ist, dass es sich einerseits um Schätzungen handelt und andererseits die verwendeten Definitionen von Spam nicht einheitlich sind.

[4] Bager/Bleich [2007, S. 85].

[5] Vgl. Zdziarski [2005, S. 26 f.].

1997 führte Paul Vixie die erste real-time blackhole list (RBL) ein. Die RBL ermöglichte E-Mails von Netzwerken, die sich in der Liste befanden, auf Serverebene abzuweisen.[6] Ein zweiter Meilenstein war die Übertragung des Bayes-Theorems auf die Spam-Filterung von Paul Graham im Jahr 2002. Hierdurch wurde die Grundlage für die Filterung anhand statistischer Methoden gelegt.[7]

Diese Arbeit soll verdeutlichen, warum Spam-Mails kein geringfügiges Ärgernis sind, sondern einen realen Schaden verursachen. Weiterhin wird betrachtet, warum der Versand von Spam-Mails ein lukratives Geschäft ist. Neben der ausführlichen Erläuterung clientseitiger Filtertechniken mit ihren Vor- und Nachteilen wird auch auf serverseitige Filtertechniken und andere Ansätze zur Bekämpfung von Spam eingegangen.

In dem praktischen Teil dieser Arbeit werden die Filter-Ergebnisse mehrerer Spam-Filter bzw. der einzelnen Filtertechniken analysiert und gegenübergestellt. Die Softwarequalität der Spam-Filter wird anhand mehrerer Kriterien evaluiert und miteinander verglichen.

1.2 Aufbau der Arbeit

Kapitel 2 geht auf die zum Verständnis der weiteren Kapitel erforderlichen Grundlagen ein. Dazu gehört die Definition des in dieser Arbeit zugrunde gelegten Spam-Begriffs sowie die Erläuterung der bei der Spam-Filterung auftretenden Fehlerarten. Kapitel 2.3 legt dar, warum Spammen ein lukratives Geschäft ist, bei dem auf Seite der Empfänger ein realer Schaden entsteht. Kapitel 2.4 erörtert die technischen Grundlagen von E-Mails.

Kapitel 3 stellt verschiedene clientseitige Filtertechniken dar und diskutiert ihre jeweiligen Vor- und Nachteile sowie die von den Spammern entwickelten Gegenmaßnahmen.

Kapitel 4.1 erläutert ausschließlich auf Serverebene verwendete Filtertechniken. Kapitel 4.2 beschreibt drei Ansätze gegen Spam, die nicht den Filtertechniken zuzuordnen sind.

Kapitel 5 beschreibt die Ergebnisse der mit den Spam-Filtern durchgeführten Tests. Kapitel 5.1 stellt die verwendeten Spam-Filter vor. Kapitel 5.2 und 5.3 erläutern, unter welchen Rahmenbedingungen die Tests durchgeführt wurden. Die Methoden, die zur Analyse der Testergebnisse verwendet wurden, stellt Kapitel 5.4 vor. Kapitel 5.5 legt die Ergebnisse der einzelnen Filtertechniken dar und Kapitel 5.6 fasst diese zusammen. Kapitel 5.7 erläutert, nach welchen Kriterien die Spam-Filter evaluiert wurden und wie sie dabei jeweils abgeschnitten haben. Kapitel 5.8 überführt die Kriterien in Schulnoten und vergibt für jeden Filter eine Durchschnittsnote.

Den Abschluss bilden das Fazit und der Ausblick in Kapitel 6.

---

[6] Vgl. Zdziarski [2005, S. 27 f.].
[7] Vgl. Zdziarski [2005, S. 49].

6 Fazit und Ausblick

Spam-Mails stellen ein ernsthaftes Problem dar, da sie einerseits das Medium E-Mail in seiner Existenz bedrohen und andererseits bei den Empfängern hohe Kosten verursachen. Für die Versender der Spam-Mails fallen dagegen praktisch keine Kosten an, wodurch das Spammen auch bei einer geringen Erfolgsquote profitabel ist.

Um die Profitabilität des Spam-Geschäftes zu senken, wurden in dieser Arbeit verschiedene Ansätze diskutiert. Ein grundsätzlich Erfolg versprechender Ansatz ist die Bestrafung und Verfolgung von Spammern. Problematisch ist, dass es Länder gibt, in denen Spammen kein Straftatbestand ist. Weiterhin ist es - trotz existierender Gesetze - keine Selbstverständlichkeit, dass Spammer zur Rechenschaft gezogen werden. Einerseits funktioniert die länderübergreifende Zusammenarbeit der Behörden häufig nicht reibungslos. Andererseits ist die Identität eines Spammer, der Botnetze zum Versenden von Spam einsetzt, relativ schwierig zu ermitteln. Trotzdem bietet ein gesetzliches Vorgehen gegen Spam - auf langfristige Sicht gesehen - gute Chancen, das Spammen unattraktiv zu machen.

Viele andere Ansätze sind entweder noch nicht völlig durchdacht (Challenge-Response-Verfahren, E-Mail-Gebühren), benachteiligen Versender legitimer Massen-E-Mails (Hashcash) oder sind von Spammern allzu leicht auszutricksen (SPF-Verfahren).

Der Einsatz von Spam-Filtern hat zwei Auswirkungen: Erstens werden weniger Spam-Mails zugestellt, wodurch der durchschnittliche Erfolg pro versandter Spam-Mail sinkt. Zweitens bleibt das Medium E-Mail in Abwesenheit einer Lösung, die die Ursache des Spam-Problems nachhaltig beseitigt, weiterhin effizient nutzbar.

Jede der aktuellen Filtertechniken hat ihre Vor- und Nachteile. Keine ist vollkommen immun gegenüber den Tricks der Spammer. Welche Filtertechnik am besten geeignet ist, lässt sich nicht pauschal beantworten, sondern ist abhängig von dem Ort der Filterung (Server- oder Clientebene), dem oder den Usern und den zu filternden E-Mails. Häufig werden ohnehin mehrere Filtertechniken miteinander kombiniert, um die Stärken mehrerer Techniken zu nutzen und ihre Schwächen zu kaschieren. Durch die Kombination von Filtertechniken können einerseits mehr Spam-Mails erkannt werden, andererseits werden weniger Ham-Mails fälschlicherweise als Spam eingestuft. Dies wurde durch die Tests von Spam-Filtern bestätigt, bei denen der Filter SpamAssassin, - der verschiedene Filtertechniken nutzt - die beste Filterleistung zeigte. Allerdings steigt mit der Zahl der verwendeten Filtertechniken auch die Laufzeit der Filterung, so dass in der Praxis häufig ein Kompromiss zwischen Filterleistung und Laufzeit eingegangen werden muss.

Bemerkenswert ist, dass Bilder-Spam von den Spam-Filtern relativ sicher erkannt wurde. Dies steht im Widerspruch zu einem Teil der Fachliteratur. Um diesbezüglich definitive Aussagen treffen zu können, war jedoch die für die Tests verwendete Anzahl an E-Mails zu gering. Insgesamt ist festzuhalten, dass die Testergebnisse von Spam-Filtern neben der Konfiguration auch immer stark abhängig von den für die Tests verwendeten E-Mails sind. Teilweise zeigten sich auch hier bei den Testergebnissen zwischen den einzelnen E-Mail-Korpora große Unterschiede.

Die Hersteller von Spam-Filter werden auch zukünftig bestehende Techniken verfeinern und neue Techniken entwickeln. Der Provider Strato arbeitet zurzeit mit dem Max-Planck-Institut Saarbrücken und der Humboldt-Universität Berlin zusammen an der Entwicklung eines Filtersystems, das auf Basis der Spieltheorie selbst Spam-Mails generiert, um die eigenen Filter auszutricksen. Durch die Anpassung der Filter an diese selbst generierten Spam-Mails soll sichergestellt werden, dass ähnlicher Spam zukünftig von den Filtern erkannt wird. Die Einführung ist für das Frühjahr 2008 vorgesehen.[281]

Die Spammer werden jedoch ebenfalls ihre bestehenden Techniken verfeinern und auf neuentwickelte Filtertechniken ihrerseits innovativ reagieren. Damit wird das „Wettrüsten“ zwischen den Entwicklern von Spam-Filtern und den Spammern fortgesetzt. Für die nähere Zukunft ist keine endgültige Lösung des Spam-Problems in Sicht.

[281] Vgl. Ziegler [2007, S.187].