Proseminar:

"Ethische Aspekte der Informationsverarbeitung"

Der Kampf gegen Spam

von

Sebastian Zech

Matrikel-Nummer: 2502665

Gliederung:

Der Kampf gegen Spam

- Was ist Spam?
- Warum Spam bekämpfen?
- Wie Spam bekämpfen?
  - Analyse von Spam/ Das Spam-Profil
  - Analyse von Spammern/ Das Spammer-Profil
  - Taktiken und Tools der Spammer
  - Maßnahmen gegen Spam

Was ist Spam ?

- Definition: „Spam“ ursprünglich Markenname für Dosenfleisch, der 1936 in einem Sketsch von Monty Python an Bedeutung gewann

- 80er Jahre „Multi User Dungeons“ überfluten mit Text (durch Ähnlichkeit mit Sketch entsteht „Spam“)

- im USENET erstmals Zusammenhang mit Werbung

- später auch auf Dienste wie E-Mail, News, Fax und SMS übertragen

Warum Spam bekämpfen ?

- Zahlen (2003):
  - Anti-Spam-Firma „Brightmail“ blockt **60 Millionen** Spam / Monat
  - „MSN-Hotmail“ blockt mehr als **2 Millionen** / Tag
  - „AOL“ **1 Million** pro Tag

  → Spam-E-Mails überstieg die Anzahl normaler E-Mails (spamhaus.org)

- Spam- Aufkommen stieg in den letzten Jahren exponentiell

- Massenhafter Mail-Versand kostet viele Ressourcen:
  - Speicher
  - Rechnerleistung
  - Zeit (der User)
  - Folgeschäden für User/ Unternehmen (Geld)
    (2003: weltweit 8 – 10 Millionen Euro
    2004: in Europa 25 Milliarden Euro)

Wie Spam bekämpfen ?

❖ erst mal „verstehen“:

- Analyse von Spam
  ➔ Spam-Profil
- Analyse von Spammern
  ➔ Spammer-Profil
- Technik / Tools die Spammer verwenden

➔ dann erst:

- Gegenmaßnahmen (wie Filter) entwickeln
- Gesetze verabschieden, die Spam verhindern/ verringern
- Benutzerverhalten anpassen

ZIEL: Spams ganz verhindern

realistischer:

- Systeme die Emails vorsortieren
- Gesetze die Spammer abschrecken

Analyse von Spam / Das Spam-Profil

Definition von Spam:

- jede Organisation, die sich mit Spams beschäftigt hat ihre eigene Definition
- aber allgemein akzeptiert ist:

UCE **(unsolicited commercial e-mail)**	**UBE** **(unsolicited bulk e-mail)**
▪ unaufgefordert, unerwünscht an eine große Anzahl von Personen geschickt	
▪ Inhalt werbender Natur	▪ keine Werbung ▪ z.B. Massenmails von Würmern und Trojanern

➔ sehr schwer „Spam“ zu definieren

typische Eigenschaften von Spam:

- Extra E-Mail Konten zum Sammeln von Spams

- Archiv: „Spamarchiv.org“
  (im 1. Jahr: 1,5 Mio Spams,
  aktuelle Zahlen: 5000 Spams pro Tag ≈ 1,8Mio Spam/Jahr)

→ Eigenschaften:

- ❖ Absender-Adresse ist falsch
- ❖ Identität des Empfängers unwichtig
- ❖ E-Mail wird an mehrere Varianten einer gleichen Mailadresse geschickt
- ❖ Inhalt der Betreff-Zeile hat meistens nichts mit dem Inhalt der Mail zu tun
- ❖ E-Mail von dubiosen Quellen
- ❖ Links in Spams funktionieren entweder nicht oder dienen dazu, die E-Mail-Adresse als echt zu kennzeichnen
- ❖ enthalten manchmal versteckten Quelltext z.B. JavaScript

- Aufteilung von Spam:
  - 5% Scam
  - 12% pornographischen/sexuellen Inhalt
  - 24% Geldwerbung (billige Kredite etc.)
  - 33% Werbung für Produkte
  - 26% sind verschiedenen Inhalts
    (z.B. Pishing Mails, Würmer und Viren, Kettenbriefe,…)

Kosten einer Spam-E-mail:

- 0,00032 Cent
- genügt einfaches Modem zum verschicken
- Hauptkosten trägt der Empfänger

Analyse von Spammern / Das Spammer-Profil

❖ Kategorien von Spammern:

- Gelegenheits-Spammer:
  - geringer Anteil
  - z.B. Verfasser von Kettenbriefen
- „unwissender“ Spammer:
  - auch „Spamkiddies“ genannt
  - benutzen fertige Software und Mail Listen
  - wissen aber nicht wie diese funktionieren
- „Hacker“ Spammer:
  - anspruchsvolle Spammer, die auch Software entwickeln
- professionelle Spammer:
  - verursachen den meisten Schaden im Netz
  - und die meisten Spams

❖ Motivation:

- zum größten Teil Geld (2005: 7,3 Mio Dollar Geschäft)

Taktik und Tools der Spammer

- Beschaffen von E-Mail-Adresen:
  - E-Mail-Listen kaufen
  - von Webseiten
  - aus Mailinglists
  - Chat-Rooms
  - durch „dictionary attack“
  - aus Gastbüchern und Foren
  - durch Antworten auf Spam

- verschicken von Spam mit Spamware, die im Internet erworben werden kann (auch kostenlose Tools)

- Tools:
  - E-Mail-Harvester/-Extractor oder Spambot:
    - entnimmt E-Mails aus Internetseiten und Newsgroups
  - Desktop Server 2000:
    - verschickt Spams
    - kann Namen und E-Mail-Adressen verbinden (E-Mail wird persönlicher)
  - E-Mail List Verifier
    - überprüft Gültigkeit einer Mail
  - E-Mail List Manager
    - Verwalten von Adressen

- Kommunikation unter Spammern über sichere Server in Ländern wie China (keine rechtlichen Folgen zu befürchten)

Maßnahmen gegen Spam

- ❖ Filter:
  - Blacklist-Methode
    - sortiert Spams mit Hilfe einer Liste mit Schlüsselwörtern aus
  - Bayes-Filter-Methode
    - beruht auf Wahrscheinlichkeit
    - muss vom Benutzer trainiert werden
  - Datenbank-basierter Filter
    - Schlüsselwörter(Adressen, Tel., …) aus einer Datenbank zum aussortieren

- ❖ rechtliche Möglichkeiten:
  - USA:
    - jeder Staat eigene Gesetze
    - Florida keine, obwohl meisten Spams von dort kommen
    - verbieten meistens nur einzelne Mittel des Spammers (dictionary attacks, unechte Absenderadressen, …)
  - Europa:
    - Durch Richtlinie (2002/58/EG) geregelt, wurde 2003 von Mitgliedsstaaten in allgemeines Recht umgesetzt
    - Zusendung von E-Mail-Werbung nur mit Zustimmung
    - EU will künftig mit 13 asiatischen Ländern zusammenarbeiten

- Deutschland:
  - Möglich sind Unterlassungsklagen oder Verstoß gegen Wettbewerbsrecht
  - Anti-Spam-Gesetz (2005):
    besagt, dass kommerzieller Charakter der Email und Absender nicht verschleiert werden dürfen (bis 50000€ Strafe)

- Weltweit:
  - OECD (Organisation for Economic Co-operation and Development) brachte 2003 Richtlinien gegen Spam heraus, zielen hauptsächlich auf die Taktiken der Spammer

  - 11 Staaten (darunter Deutschland) haben einen „opt-in“-Gesetz beschlossen

❖ <u>Verhalten des Nutzers</u>:

- Email-Adressen nur an vertraute Personen weitergeben, nicht im Internet veröffentlichen

- Wegwerf-Email-Adressen zur Anmeldung z.B. in Foren verwenden

- Eine Email an viele Empfänger an sich selbst schicken und die Empfänger ins BCC-Feld schreiben

- weitere Tipps im Netz

The 10 Worst Spam Origin Countries		As at 29 May 2006
Rank	Country	Number of Current Known Spam Issues
1	United States	2477
2	China	388
3	Japan	331
4	Russia	308
5	Canada	185
6	Taiwan	181
7	South Korea	162
8	United Kingdom	152
9	Netherlands	141
10	Hong Kong	139

Source: Spamhaus Blocklist (SBL) database. Data is compiled automatically every 24 hours from the SBL database using the number of currently listed SBL records for each network (ISP/NSP) sorted by country. The source data, including listings of each country's current known spam issues, sorted by local network, can be viewed by clicking on any country hyperlink above.

The 10 Worst ROKSO Spammers			As at 29 May 2006
Rank	Photo	Spammer or Spam Gang	Country
1		**Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov** So many Alex's/Alexey's. Alex "Blood" tied to Pilot Holding & bbasafehosting.com long ago. Then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring. May be part of of same as Pavka/Artofit & Leo Kuvayev spam gangs.	**Ukraine**
2		**Michael Lindsay / iMedia Networks** Lindsay's iMedia Networks is a full-fledged criminal spam-hosting operation serving well known ROKSO-listed spammers. They sell "spammer hosting" at high premiums.	**United States** California
3		**Leo Kuvayev / BadCow** Russian/American spammer. Does "OEM CD" pirated software spam, illegal pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus infected PCs that it is assumed his gang create.	**Russia**
4		**Pavka / Artofit** A Russian gang who have been spamming for years. Started with porn, now into many types of spam, always via hijacked PCs. Part of a large criminal group involving ROKSO spammers Leo Kuvayev & Alex Blood. Also see "Yambo Financials" ROKSO.	**Russia**
5		**Amichai Inbar** Full scale criminal operation. Spamming porn, illegal drugs and pump-&-dump stock using botnets. Partnered with many of the worst US and Russian ROKSO spammers.	**Israel**
6		**Jeffrey Peters - JTel / CPU Solutions** Convicted felon, hard-core spammer host, Peters is also behind a fake Russian "ISP" serving many criminal ROKSO spammers. Forged documents seem to be among his specialties.	**United States** Florida
7		**Ruslan Ibragimov / send-safe.com** Stealth spamware creator. One of the larger criminal spamming operations around. Runs a CGI mailer on machines in Russia and uses hijacked open proxies and virus infected PCs to flood the world with spam.	**Russia**
8		**Tim Goyetche / Bulkers.net / Bulkbarn.com** Long time operator of Bulkbarn.com "secret" spammer chat forum. Behind a lot of the criminal method spamming that goes on in the world. Caught in 2005 spamming "pump & dump" stock scams.	**Canada** Nova Scotia
9		**Alexey Panov - ckync.com** Spamming, spammer hosting, spamware peddlers. Author of the DMS spamware that uses hijacked open proxies and virus infected PC to flood the world with spam.	**Russia**
10		**Ivo Ottavio Reali Camargo** A spammer and an "off shore" partner to many other spammers including Alan Ralsky and Michael Lindsay. Provides hosting, domains and spam services from Brazil where enforcement is lax.	**Brazil**

Source: Register Of Known Spam Operations (ROKSO) database + Spamhaus Blocklist (SBL) database. Detailed records on each spammer or spam gang listed can be viewed by clicking on the hyperlinks above.

Quellenangabe:

Texte:

- Anselm Lambert: Analysis of Spam. M.Sc. Thesis, University of Dublin, 2003. Darin S. 1–38.

Ergänzendes Material:

- http://www.spamfaq.net/spam-evils.shtml (25.05.06).
- http://de.wikipedia.org/wiki/Spam (25.05.06)
- http://de.wikipedia.org/wiki/Spamfilter (25.05.06)
- http://www.spamhaus.org/statistics/countries.lasso (29.05.06)
- http://www.spamhaus.org/statistics/spammers.lasso (29.05.06)
- spamarchiv.org (27.05.06)