Spam

Techniken zur Abwehr

Dirk Geschke

Linux User Group Erding

23. April 2008

Gliederung

1. Methoden der Spambekämpfung
2. Theoretische Verfahren
3. Abschluß

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*)

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*)

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*)

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*)

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*)

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*)

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*)

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*)

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- im Client vor Abholung
- im Client nach Abholung

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 Annahme
- 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!)

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!)

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!)

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!)

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!)

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 aufgrund von Datenschutzbestimmungen nicht möglich
- Filterung im Mailclient
- erkannter Spam kann zum Trainieren anderer Filter verwendet werden, siehe Bayes–Verfahren

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 aufgrund von Datenschutzbestimmungen nicht möglich
- Filterung im Mailclient
- erkannter Spam kann zum Trainieren anderer Filter verwendet werden, siehe Bayes–Verfahren

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 aufgrund von Datenschutzbestimmungen nicht möglich
- Filterung im Mailclient
- erkannter Spam kann zum Trainieren anderer Filter verwendet werden, siehe Bayes–Verfahren

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 aufgrund von Datenschutzbestimmungen nicht möglich
- Filterung im Mailclient
- erkannter Spam kann zum Trainieren anderer Filter verwendet werden, siehe Bayes–Verfahren

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 aufgrund von Datenschutzbestimmungen nicht möglich
- Filterung im Mailclient
- 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 eine 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, fehlerhafte Mailclients leider nicht.

Einhalten des Protokolls, Timeouts

- Prüfung des HELO-Strings: Ist der Hostname korrekt? Weist er auf eine 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, fehlerhafte Mailclients leider nicht.

Einhalten des Protokolls, Timeouts

- Prüfung des HELO-Strings: Ist der Hostname korrekt? Weist er auf eine 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, fehlerhafte Mailclients leider nicht.

Einhalten des Protokolls, Timeouts

- Prüfung des HELO-Strings: Ist der Hostname korrekt? Weist er auf eine 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, fehlerhafte Mailclients leider nicht.

Einhalten des Protokolls, Timeouts

- Prüfung des HELO-Strings: Ist der Hostname korrekt? Weist er auf eine 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, fehlerhafte Mailclients leider nicht.

Einhalten des Protokolls, Timeouts

- Prüfung des HELO-Strings: Ist der Hostname korrekt? Weist er auf eine 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, fehlerhafte Mailclients leider nicht.

Sender Policy Framework, SenderID

- 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

Sender Policy Framework, SenderID

- 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

Sender Policy Framework, SenderID

- 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

Sender Policy Framework, SenderID

- 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

Sender Policy Framework, SenderID

- 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

Sender Policy Framework, SenderID

- 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 viel gegen Bot–Netze, die sind in der Regel leistungsstark
- Als Kriterium eher sekundär geeignet, z.B. in Verbindung mit heuristischer Statistik

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 viel gegen Bot–Netze, die sind in der Regel leistungsstark
- Als Kriterium eher sekundär geeignet, z.B. in Verbindung mit heuristischer Statistik

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 viel gegen Bot–Netze, die sind in der Regel leistungsstark
- Als Kriterium eher sekundär geeignet, z.B. in Verbindung mit heuristischer Statistik

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 viel gegen Bot–Netze, die sind in der Regel leistungsstark
- Als Kriterium eher sekundär geeignet, z.B. in Verbindung mit heuristischer Statistik

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 viel 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

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

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

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

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? Wie schnell werden die Listen aktualisiert?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

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? Wie schnell werden die Listen aktualisiert?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

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? Wie schnell werden die Listen aktualisiert?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

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? Wie schnell werden die Listen aktualisiert?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

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? Wie schnell werden die Listen aktualisiert?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

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? Wie schnell werden die Listen aktualisiert?
- rechtlich nicht einwandfrei: Speicherung von IP-Adressen können personenbezogen sein
- generell aber recht effektiv

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? Wie schnell werden die Listen aktualisiert?
- 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 **SPAM** und **HAM**
- 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

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **SPAM** und **HAM**
- 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

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **SPAM** und **HAM**
- 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

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **SPAM** und **HAM**
- 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

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **SPAM** und **HAM**
- 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

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **SPAM** und **HAM**
- 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

Statistische Inhaltsanalyse

- Vorhersagbarkeit von **HAM** oder **SPAM** durch statistische Analyse alter E-Mails
- naive Bayes-Filter: Statistiken über einzelne Wörter (*token*)
- Trainingsphase notwendig für **SPAM** und **HAM**
- 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

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

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

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

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

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

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

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

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

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

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!

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!

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!

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!

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!

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!

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!

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!

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
- Vorsicht: Spammer verwenden manchmal derartige Adressen als Absender, bounces und Abwesenheitsnotizen können dann zu Problemen führen!

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
- Vorsicht: Spammer verwenden manchmal derartige Adressen als Absender, bounces und Abwesenheitsnotizen können dann zu Problemen führen!

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
- Vorsicht: Spammer verwenden manchmal derartige Adressen als Absender, bounces und Abwesenheitsnotizen können dann zu Problemen führen!

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
- Vorsicht: Spammer verwenden manchmal derartige Adressen als Absender, bounces und Abwesenheitsnotizen können dann zu Problemen führen!

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
- Vorsicht: Spammer verwenden manchmal derartige Adressen als Absender, bounces und Abwesenheitsnotizen können dann zu Problemen führen!

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
- Vorsicht: Spammer verwenden manchmal derartige Adressen als Absender, bounces und Abwesenheitsnotizen können dann zu Problemen führen!

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwendig, 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

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwendig, 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

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwendig, 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

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwendig, 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

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwendig, 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

Tokenbasierte und Challenge–Response–Verfahren

- spezieller Token innerhalb einer E-Mail notwendig, 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

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

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

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

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

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

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: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Elektronische Briefmarken

- Idee: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Elektronische Briefmarken

- Idee: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Elektronische Briefmarken

- Idee: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Elektronische Briefmarken

- Idee: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Elektronische Briefmarken

- Idee: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- interessante Idee: Empfänger bekommt das Geld, spamlesen wird lukrativ
- Variante: Whitelisten für bestätigte Kontakte
- Probleme: legitime Massenversendungen, Mailinglisten

Elektronische Briefmarken

- Idee: geringe Kosten pro E-Mail treffen hauptsächlich Spammer
- Gewinnreduzierung beim Spammer, diese verlieren Interesse
- Frage der Geldeintreibung offen: Micropayment
- Wer soll das Geld bekommen? Der ISP? Wer darf dann ISP werden?
- 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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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?

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

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

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

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

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

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