Collateral Damage

Consequences of Spam and Virus Filtering for the E-Mail System

Peter Eisentraut

credativ GmbH

22C3

Introduction

- 12 years of spam. . .
- 24 years of SMTP. . .
- Things have changed:
  - SMTP is no longer enough.
  - Spam filters, virus filters are part of the system
  - But they are not standardized, verified, or predictable.
  - Getting e-mail through is a challenge.

Filtering Techniques

Examples of questionale defense mechanisms:

- DNS blackhole lists
- Bounce messages
- Greylisting
- SPF
- Blocking port 25
- Challenge/response systems
- Inventing your own

DNS Blackhole Lists: Concept

- Publish list of “problem” hosts via DNS
- Every mail server can query the lists
- First DNSBL MAPS did manual inspections
- Current DNSBLs are mostly automatic

DNS Blackhole Lists: Discussion

- Indiscriminate treatment of temporary problems
- Large ISPs often blocked
- Useless against dial-up accounts
- Low correlation with spam occurrence
- DNS is insecure
- Only usable as part of scoring system (SpamAssassin)

Bounce Messages: Concept

Original concept:

1. Host A sends message to host B.
2. Host B checks the message.
3. Host B accepts or rejects the message.

Problem: Checking took too long, host A timed out.
New concept:

1. Host A sends message to host B.
2. Host B accepts the message.
3. Host B checks the message and sends rejection message to the sender.

How to find the sender?

Bounce Messages: Discussion

Junk e-mail fakes sender addresses.

- Rejection messages go to innocent users.
  - Users now reject rejection messages.
- Alternatives: discard messages, quarantine
- Better: fix MTA time-outs, spam filter performance, go back to original concept

Greylisting: Concept

- Mail server sends temporary error on first contact
- Normal client tries again
- Spamming software, zombies doesn’t try again
- Extremely effective
- Spammers could react easily, but don’t. . . (?)

Greylisting: Discussion

Full of configuration pitfalls:

- Poorly implemented software
- Sender-side server pools
- Recipient-side load balancing
- Broken MTAs that don’t retry
- Mailing list software with variable sender addresses
- Time-critical e-mails (eBay)
- Multistage relays

Very hard to get right with diverse user populations

SPF: Concept

Sender Policy Framework:

- Domain owner publishes SPF record via DNS, identifying valid outgoing mail servers
- Mail recipient checks SPF records, rejects mail from invalid mail servers
- SPF checks envelope sender, Sender ID checks sender address in mail content

SPF: Discussion

- Does not stop spam, spammers just use a different domain
- Spammers can publish their own SPF records
- SPF does not stop phishing, the envelope address is hidden from the user (Sender ID is better)
- Does prevent certain kinds of e-mail forgery
- Breaks forwarding
- ISPs can control users' mail routes
- DNS is insecure

Don't use it!

Blocking Port 25: Concept

- Most junk e-mail is sent by zombies
  - Hard to track (DNSBL)
  - Spammers just switch to the next set of zombies
- Solution: block outgoing port 25 on dial-up accounts
  - Users are forced to go through ISP's mail server
  - Dial-up PCs no longer attractive targets for installing zombieware

Blocking Port 25: Discussion

Problems:

- Users want to use other e-mail accounts than the one provided by their ISP
- Workaround: ISP allows all customers to route through ISP's mail server
- Users cannot use their own mail server
  - Use your own mail server software
  - ISP's mail server is misconfigured (or blacklisted)
  - Privacy
- Incompatible with SPF!

Challenge/Response Systems: Concept

1. Receiving mail server intercepts message, sends challenge
2. Original sender must manually answer the challenge
3. Receiving mail server checks response, delivers original message

Challenge/Response Systems: Discussion

Major annoyance!

- Sender addresses are faked, innocent users get challenge messages.
  - Users of CR systems get blacklisted.
- Spam can fake already authenticated sender addresses.
- Two users of CR can never talk to each other.
- CR systems would require (exploitable) loopholes in e-mail filters.
- Facilitates phishing
- CR transaction tracking violates privacy.

Loses e-mail, quite useless against spam

Being Smarter Than Everyone Else

- Running a local DNSBL
- Running a local Pyzor server
- Forgetting the MX backup
- Random RFC purity checking
- Changing your e-mail address regularly
- . . .

Don’t invent your own filters.

Legal Issues: Privacy

- Bayesian filter word databases
- Insecure greylisting databases
- Distributed e-mail counting
- Challenge/response transaction records
- SPF + blocking port 25 forcing e-mail routes

Everything controlled at ISP's mail server, not by user!

Legal Issues: Database Building

Everyone is building databases:

- Spam filter manufacturers
- Industry associations (eco, Wettbewerbszentrale)
- Governments (FTC)
- to be shared internationally
- impossible to control

Legal Issues: Recourse

- Spam filtering not allowed without user's consent
- ISPs must inform users, or
- Users must activate the filters
- Most users don't care

Conclusion

- E-mail has become unreliable.
- Users accept it as such.
- Spammers and virus writers are to blame.
- But inappropriate junk mail filters as well.
- Check each filter technique thoroughly.
- Check what your ISP is doing.