

Email Security and Spam Prevention

March 25, 2004

Tim Faltemier

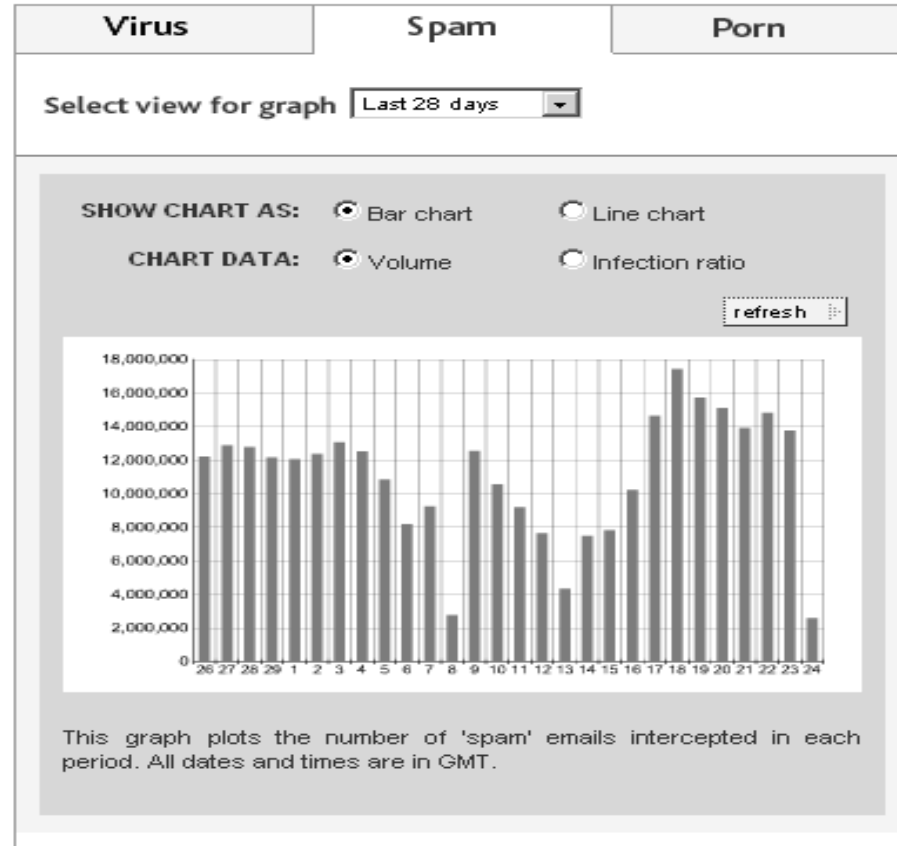
Saurabh Jain

Email Spam

(Impact)

- Spam- Unsolicited Email that lack affirmative consent from Receiver.
- America Online estimated that between 5% and 30% of its email server time at any given moment was exclusively dedicated to handling spam.
 - <http://content.techweb.com/wire/story/TWB19971218S0007>
- Between \$2-3 of a consumer's monthly Internet bill is for handling spam
 - <http://www.wa-state-resident.com/finalrpt.pdf>
- 7% of Internet users who switch ISPs do so because of spam which leads to \$250,000 per month for an ISP with 1 million subscribers.
 - http://www.brightmail.com/pdfs/gartner_rebuilt.pdf

Email Spam (Statistics)



* <http://www.message-labs.com/viruseye/threats/default.asp?tblt=spam>

Definitions

■ Mail User Agent (MUA)

- This allows the user to read and compose email messages. Often referred to as an email client (outlook, pine, etc.)

■ Mail Transfer Agent (MTA)

- Transfers email messages between machines using Simple Mail Transfer Protocol (SMTP). Often referred to as an email server (Sendmail)

Email Filtering

- One of the most readily available spam prevention techniques. (Currently available in most MUAs)
- Two main forms of filtering
 - Content Based Filters
 - Bayesian Spam Filters

Content Based Filters

- Broken into two main sections
 - Spam Filters
 - These are responsible for removing something on the basis of a rule previously set (ie. Any message with the text V-I-A-G-R-A would be filtered)
 - Anti-Filters
 - If special unusual key words or names were in a message (ie. Hippopotamus) then the email would be allowed. Sometimes known as “White Listing” a person or email address.

Bayesian Filtering

- Calculate the probability of a message being spam based on its contents.
- Learns from spam and good mail.
- Hardly returns any false positives.
- Keeps getting better and better according to the mail you classify as spam and non-spam.
- Examples of what is taken into account:
 - Words in the body, Headers, HTML code, Links, Word pairs and Phrases.

- Spam detection software, running on the system "neptune.lunarpages.com", has identified this incoming email as possible spam. The original message has been attached to this so you can view it (if it isn't spam) or block similar future email. If you have any questions, see the administrator of that system for details.

Content preview: Hi Tim, When you get time, please give me a call so we could proceed with update. Thank you! Rosie [...]

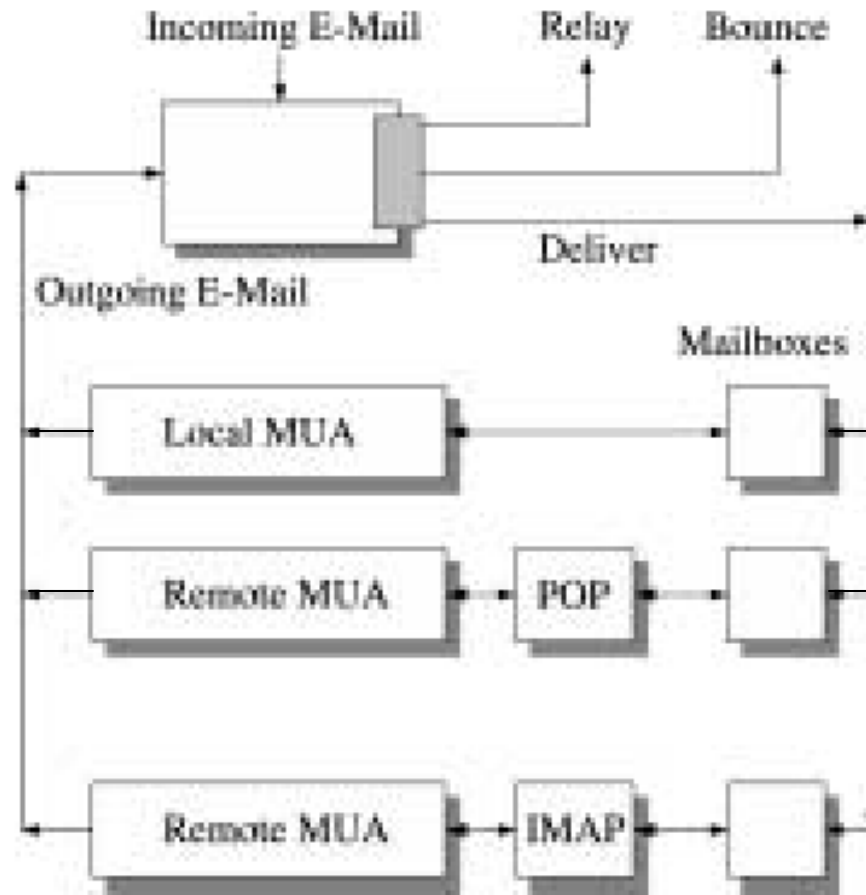
Content analysis details: (5.7 points, 5.0 required)

pts	rule name	description
0.2	NO_REAL_NAME	From: does not include a real name
1.0	FROM_ENDS_IN_NUMS	From: ends in numbers
-0.9	BAYES_30	BODY: Bayesian spam probability is 30 to 40% [score: 0.3590]
1.1	RCVD_IN_SORBS_HTTP	RBL: SORBS: sender is open HTTP proxy server [205.188.139.166 listed in dnsbl.sorbs.net]
1.5	RCVD_IN_BL_SPAMCOP_NET	RBL: Received via a relay in bl.spamcop.net [Blocked - see < http://www.spamcop.net/bl.shtml?205.188.139.166 >]
2.7	RCVD_IN_SORBS_SMTP	RBL: SORBS: sender is open SMTP relay [205.188.139.166 listed in dnsbl.sorbs.net]
0.1	RCVD_IN_SORBS	RBL: SORBS: sender is listed in SORBS [205.188.139.166 listed in dnsbl.sorbs.net]

Remailers [1]

- Integrates a challenge / response to traditional MTAs
- Also adds restrictive aliasing to current email accounts.
 - This allows a user to get many “one time use” email addresses to give when filling out forms on the internet.
 - Allows you also to know who is giving out your information.

Remailer Design



Aliasing

■ Good

- Allows you to have very good protection while filling out forms or giving out your email address on the web / business cards.

■ Bad

- Still does nothing to stop spam once your real address is ever known.
- Malicious users still know your subdomain (the aliasing proposed in the paper only changes the username component)

Challenge Response

- If sender's address is unknown or not validated, then the MTA will bounce the message and attach a "challenge word" [Fig 1] that will authenticate the user.



CAPTCHA challenge (original in color)

Pros and Cons of CR

■ Good:

- Notably reduces spam email from machine sources. (Almost 100%)

■ Bad:

- All mail still is transferred on the Internet so does not solve the problem of spam.
- Only stops spam from machine sources not human sources (assuming that machines are unable to read images – which may or may not be the case)
- Important non-verified email may be delayed until the sender has a chance to verify.
- Even MORE bandwidth is used than simple spam due to the attached image.

Malicious Email Tracking (MET)

- Malicious programs continue to threaten and damage computers.
- 80% virus spread through email.
- Popular defense mechanism include anti-virus software.
- Protection against new virus and tracking not possible.

MET

(Introduction)

- Logs and maintains database of attachments passing through a mail server.
- Provides:
 - Ability to track global spread of malicious software.
 - Capability to determine point of entry.
 - Reduce the spread of Self replicating viruses.
- Uses MET client and MET Server.

MET

(Architecture)

■ Client:

- Runs on mail server and logs email traffic.
- Computes the MD5 hash of attachment to create unique identifier for the attachment.
- Maintains a database of all email attachments

■ Server:

- Central server operated by trusted third party.
- Provides virus updates to clients and reports at global level.
- Maintains no information about the users so as to protect privacy.
- Warns all clients about the potential self replicating virus threats.

MET

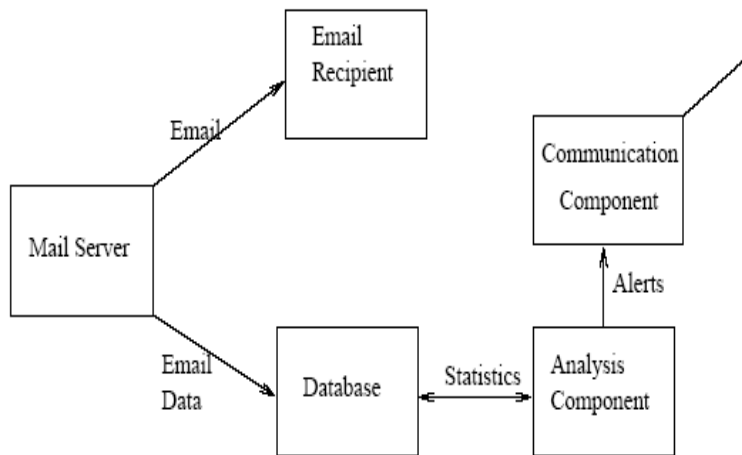


Figure 1: MET Client Architecture

Email Attachment Log Record:
Unique ID of every Attachment
Time Stamp
Attachment Classification (Malicious or Benign)
Sender Email
Receiver Email

Client

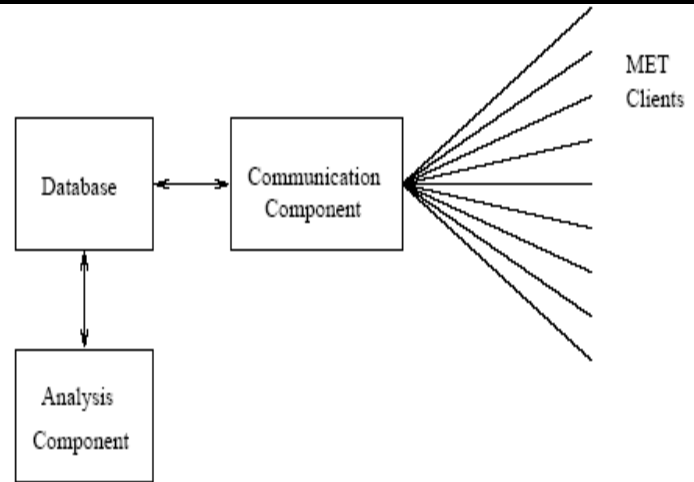


Figure 2: MET Server Architecture

Record reporting malicious attachment incident
ID of reporting server
Unique ID of attachment
Date/Time of report
Prevalence
Birth Rate

Server

MET

(Statistics)

- Virus Incident:
 - Fraction of total machine infected within an organization.
- Birth Rate:
 - Rate at which virus replicate.
- Lifespan:
 - Length of time virus is active.
- Incident Rate:
 - Rate at which virus incidents occur in a given population per unit time.
- Death Rate:
 - Rate at which virus is detected.
- Prevalence:
 - Measure of total number of local hosts infected.
- Spread:
 - Measure of global birth rate of a virus.

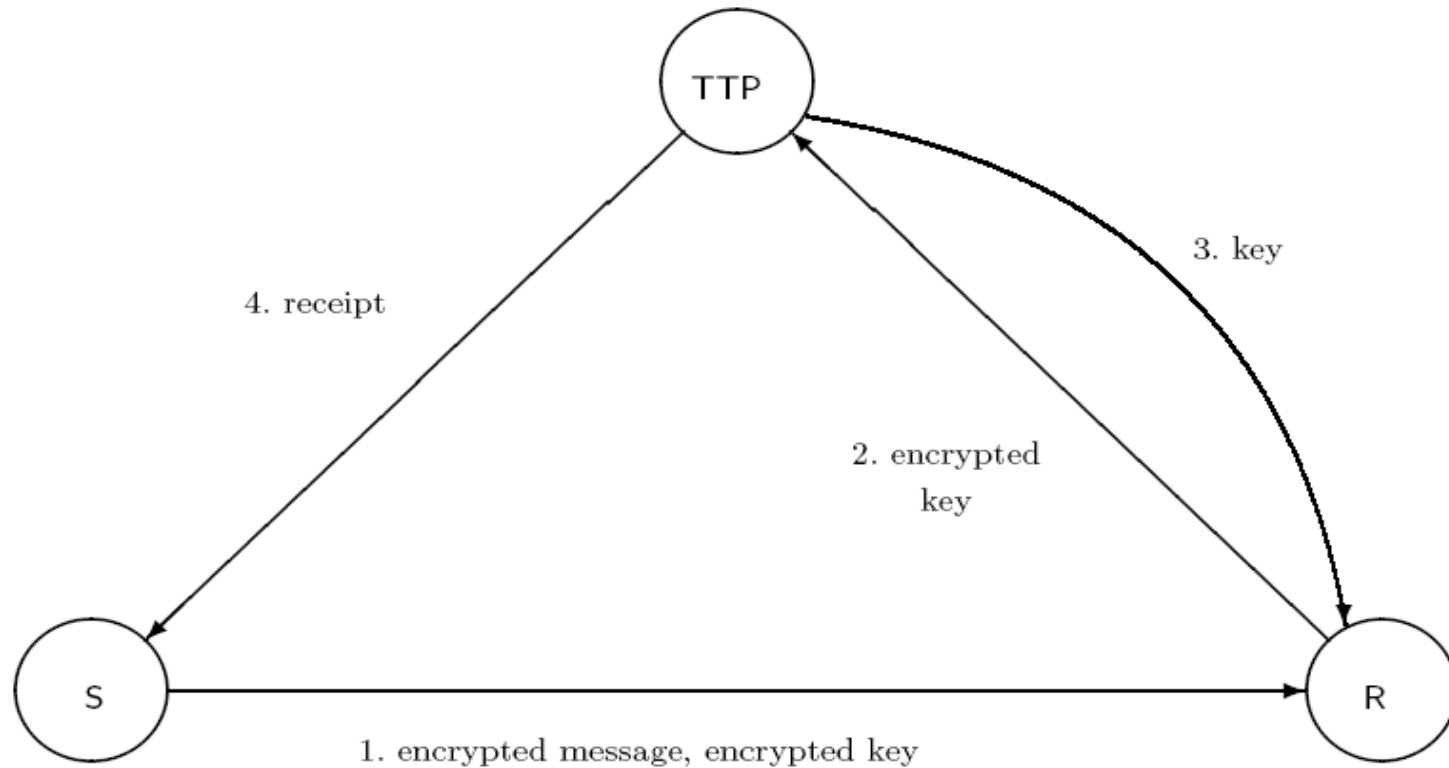
Certified E-mail

- Safeguards valuable messages in an organization.
- Goal is to produce a receipt certificate whether the receiver is honest and diligent or not.
- Secondary goal include authenticity and confidentiality.
- Designs may or may not include Trusted Third Party (TTP).
- Commercially available Systems:
 - Authentica, certifiedmail.com, sigaba etc.

Certified E-mail (Protocol)

- Sender 'S' encrypts message using fresh generated keys, encrypted the keys using public key of TTP.
- S sends the encrypted message and keys to Receiver 'R'
- R sends request to TTP to release key.
- TTP authenticates R, and sends key to R and receipt to S.

Certified E-mail (Protocol)



Possibilities for Future

- Technical: Some of the presented and other techniques.
 - Anti-Spam Research Group.
(<http://www.irtf.org/charters/asrg.html>)
- Legal and Economic Actions:
 - Amy Harmon, Digital Vandalism Spurs a Call for Oversight, New York Times, September 1, 2003.
 - Declan McCullagh, "Want to stop spammers? Charge 'em." May 5, 2003.

References

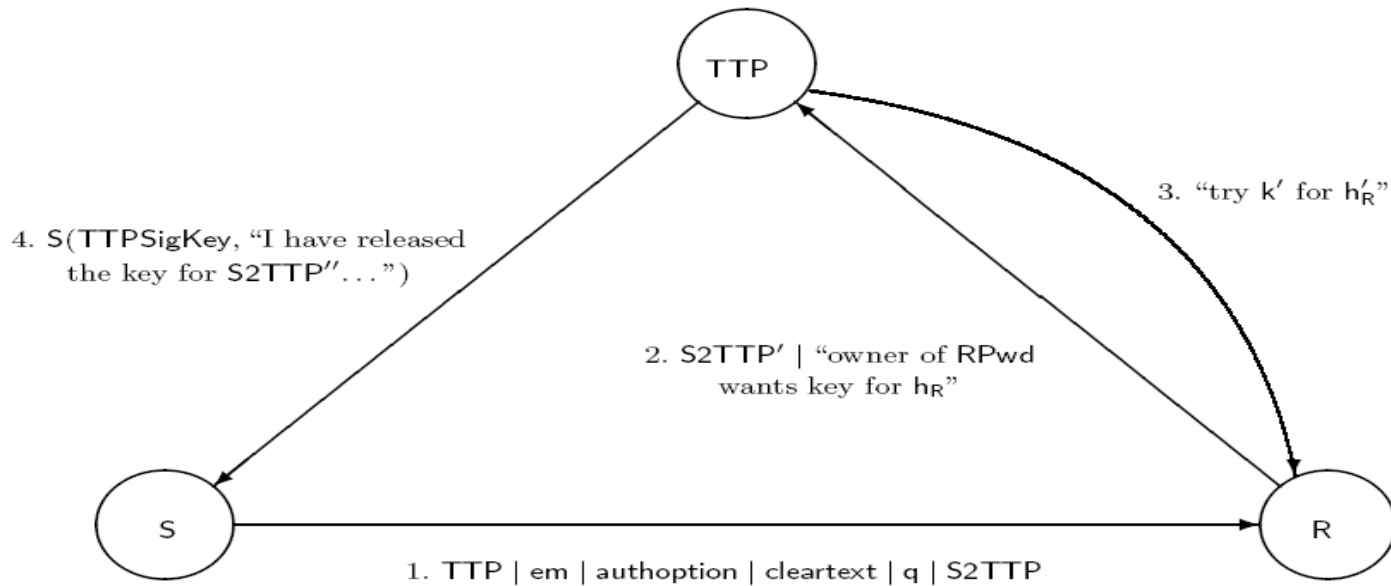
- [1] Gburzynski, Pawel. Fighting the Spam Wars: A Remailer Approach with Restrictive Aliasing, ACM Feb 2004.
- [2] Bhattacharyya, Schultz, Eskin, Hershkop, Stolfo, MET: An Experimental System for Malicious Email Tracking
- [3] Abadi, Glew, Horne, Pinkas. Certified Email with a Light On-line Trusted Third Party: Design and Implementation
- <http://www.icir.org/floyd/email.html>
- <http://certifiedmail.com>

Appendix - Certified Mail

- S generates fresh keys 'k' and encrypts message (AES in CBC)
- S computes hash: $hs = H(\text{cleartext} \parallel em)$
- S encrypts (RSA) using public Keys of TTP : $S2TTP = A(TTPEncKey, S \parallel \text{"give k to R for hs"})$
- S sends to R: $TTP \parallel em \parallel \text{cleartext} \parallel S2TTP$
- R computes hash: $hr = H(\text{cleartext}' \parallel em')$
- R sends to TTP: $S2TTP' \parallel \text{"owner of RPwd wants key for hr"}$
- TTP authenticates R using password.
- TTP decrypts $S2TTP'$ using $TTPDecKey$ (private key of TTP)
- TTP Verifies hs' equals hr'
- TTP sends keys to R and receipt to S using $TTPSigKey$.
- S verifies the signature and checks that $S2TTP'$ is same.

Appendix - Certified Mail

em = $E(k, m)$
 h_S = $H(\text{cleartext} \mid q \mid r \mid em)$
 h_R = $H(\text{cleartext}' \mid q' \mid r' \mid em')$
 $S2TTP$ = $A(TTPEncKey, S \mid \text{authoption} \mid \text{"give } k \text{ to } R \text{ for } h_S\text{"})$



Protocol sketch, in more detail