Fighting SPAM: Whitelisting Revisited

David Erickson derickso@stanford.edu
Martin Casado casado@cs.stanford.edu
Nick McKeown nickm@stanford.edu

Member project of the
Stanford Clean Slate Program
http://cleanslate.stanford.edu
Motivation

- In 2007, 74-95% of all email was SPAM

- 1.2% of employee time
  - $713 per year per employee
  - $200 billion cost to companies worldwide
Whitelisting

- **What is it?**
  - Email must match a whitelist entry to be delivered
  - Entries contain email addresses / domains
- **Often paired with** challenge-response
  - Shifts some burden from user to sender
  - Has its own list of complaints
- **Is it feasible?**
  - Lots of opinions, little data
Methodology

- Built an operational system
  - Default Off Email (DOEmail)
- Heavily instrumented
  - Email and user behavior
- Running for nearly 2 years
  - ~800,000 emails processed to date
- Real users
  - 120+ accounts have received email
Default Off Email

- Create an account
  - E.g. derickso@doemail.org
- Forward existing email
- Set destination for cleaned email
- Install Mozilla Thunderbird
  - And use our custom add-on!
  - … or use the web interface
- Populate white/black lists
Whitelisting Revisited

Sender Categories

**Whitelist**

Blacklist

Unknown

DoEmail

Whitelisting Revisited

http://www.doemail.org
Stanford Integration

RCPT TO:
derickso@stanford.edu

stanford.edu

RCPT TO:
derickso@derickso.pobox.stanford.edu

derickso.pobox.stanford.edu

Delivered
Stanford w/DOEmail Whitelist

- Is sender on my blacklist?
  - No
- Is sender on my whitelist?
  - Yes
Stanford w/DOEmail Unknown

- Is sender on my blacklist?  
  - No
- Is sender on my whitelist?  
  - No

RCPT TO: derickso@stanford.edu
RCPT TO: derickso@doemail.org

stanford.edu
DOEmail.org
derickso.pobox.stanford.edu
Stanford w/DOEmail Unknown

DOEmail Confirmation Result

Success! Added email address someone@somewhere.com to the accept list for David Erickson. Your email will be delivered shortly.

Tired of receiving SPAM? - DOEmail is a highly effective, user-friendly, and FREE anti-SPAM system operated at Stanford University, click here to learn more!

Is sender on my blacklist?  
-No

Is sender on my whitelist?  
-No

DOEmail.org

Whitelisting Revisited

http://www.doemail.org
Stanford w/DOEmail Unknown

Is sender on my blacklist?
- No

Is sender on my whitelist?
- Yes
Tools

- Mozilla Thunderbird and Web Interfaces
- Import your whitelist
- Whitelist your email recipients
- Detect mailing lists
- View and manage pending email
- Monitor your statistics
Thunderbird Add-on

- Import email addresses and domains from existing mail folders
Thunderbird Add-on

- Manage white and blacklists
Thunderbird Add-on

- View and manage pending email
Thunderbird Add-on

- View the type of rule the email matched

<table>
<thead>
<tr>
<th>Subject</th>
<th>Sender</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 15</td>
<td>Connie</td>
<td>6/15/2007 2:46 PM</td>
</tr>
<tr>
<td>test3</td>
<td>David Erickson</td>
<td>6/15/2007 4:30 PM</td>
</tr>
<tr>
<td>[WE] test4</td>
<td>David Erickson</td>
<td>6/15/2007 4:32 PM</td>
</tr>
</tbody>
</table>

- Add/remove entries by right clicking addresses
Thunderbird Add-on

- See if recipients are on your lists, if not, add them!
Thunderbird Add-on

Whitelisting Revisited  http://www.doemail.org
Lists

❖ To: / CC: Whitelist
❖ Auto Detection

Message-ID: <20080122194451.-wnll7edr4soc8o6@webmail.utoronto.ca>
Date: Tue, 29 Jan 2008 19:44:51 -0500
From: auser@utoronto.ca

To: netfpga-beta@mailman.stanford.edu
Subject: Re: [netfpga-beta] Simulation.
Precedence: list,
List-Id: <netfpga-beta.lists.stanford.edu>
List-Unsubscribe: <https://mailman.stanford.edu/mailman/listinfo/netfpga-beta>,
 mailto:netfpga-beta-request@lists.stanford.edu?subject=unsubscribe>,
List-Archive: <http://mailman.stanford.edu/pipermail/netfpga-beta>,
List-Post: <mailto:netfpga-beta@lists.stanford.edu>,
List-Help: <mailto:netfpga-beta-request@lists.stanford.edu?subject=help>,
List-Subscribe: <https://mailman.stanford.edu/mailman/listinfo/netfpga-beta>,
 mailto:netfpga-beta-request@lists.stanford.edu?subject=subscribe>,
Sender: netfpga-beta-bounces@mailman.stanford.edu.
Errors-To: netfpga-beta-bounces@mailman.stanford.edu.

Netfpga-beta mailing list
netfpga-beta@lists.stanford.edu.
Limitations

- Backscatter
- Header spoofing
  - DomainKeys/DKIM • Hash/Sign Email
- Mailing list detection
  - Poor standardization
- Challenge Emails
  - Filtered

```
myth21:~> telnet smtp.stanford.edu 25
Trying 171.67.22.28...
Connected to smtp.stanford.edu (171.67.22.28).
Escape character is '^]'.
220 smtp1.stanford.edu ESMTP Postfix
EHLO myth21.stanford.edu
250-smtp1.stanford.edu
250-PIPELINING
250-SIZE 51200000
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<president@stanford.edu>
250 2.1.0 Ok
RCPT TO:<derickso@stanford.edu>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
FROM: John Hennessey <president@stanford.edu>
TO: David Erickson <derickso@stanford.edu>
SUBJECT: Hello

Hello David.

-John

250 2.0.0 Ok: queued as CBA6427013E
```
Results

- Measured from 7/13/07 – 2/29/08
- 112 user accounts received email
- 592,794 emails processed
- Two main questions:
  - What are DOEmail’s detection rates?
    - Compare with Spam Assassin
  - How much effort is required?
    - Track user behavior
Spam Assassin Comparison CDF

97.2%

98.9%

% of Email

Spam Assassin Score

DOEmail Accepted

DOEmail Deleted
Pending Email

- 9180 (1.55%) pending emails confirmed
  - 4382 (0.74%) by sender
  - 4798 (0.81%) by user (False Positive Rate)
    - 3864 (0.65%) sent challenges
    - 934 (0.16%) not sent challenges
- 58+% sender confirmation rate
Pending Email Delay

- 90% in 21 hours
- 66% in 1 hour

% of email vs. Time

Sender Confirmed (Red) vs. User Confirmed (Green)
User Events First 90 days

*smoothed to 1 sec granularity
Conclusions

- **Whitelisting enables powerful filtering**
  - Can achieve high degrees of accuracy
    - Based on user’s rule preferences
  - Low rate of false positives
  - Content filtering limitations
    - Fundamental tradeoff between FPs and FNs

- **Negligible email delay**
  - Applies only to first email from a new sender

- **Low user overhead**