# Exploiting the Trust Hierarchy among Email Systems

***Pablo Ximenes and André dos Santos***
***Information Security Research Team (INSERT)***
UPR at Mayaguez (USA)
UECE (Brazil)

## Outline

- Introduction
- Spam Fighting approaches
- Problem Definition
- Exploiting the trust Hierarchy: Gmail's Case
- Proof of Concept Experiments
- Remarks
- Acknowledgements
- Questions

## Introduction

- 95% of all email is SPAM
- System admins started dealing with the problem by closing their open relays
- This was associated with white/black listing
- This has generated a type of ad-hoc trust hierarchy that represents a serious threat
- We will present a clear case where this is true with Gmail

## Spam Fighting Approaches

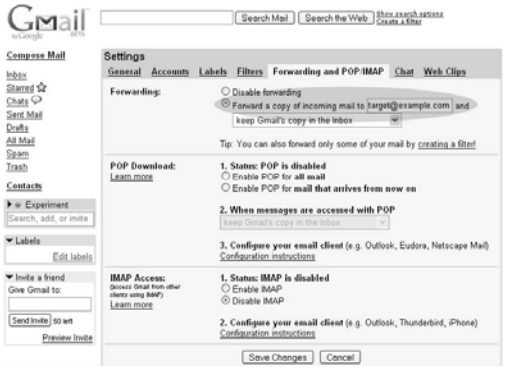
- Border Level Filtering
  - Source Authentication (SPF – RFC4408)
  - Black Lists
  - White lists
- Deep Inspection Filtering
  - Bayesian Filtering

## Problem Definition

- The volume of SPAM is enormous to be dealt exclusively with deep inspection filters
- There is no clear organization in border level filters
- System admins convenience plays an important role
- This generates a trust hierarchy prone to severe failures: either the security premise is no longer valid or attacker get free pass

## The Case of Gmail: Exploiting the Trust Hierarchy

- Gmail's Message Forwarding:



## The Case of Gmail: Exploiting the Trust Hierarchy

- Gmail's Message Forwarding:
  1. Message Received by Google's Incoming MTA server
  2. Not Spam and Matches Forwarding Rule?
  3. Message is modified to account forwarding process
  4. Return path set to the form '**GMAILUSER+caf_=TARGETUSER=TARGETDOMAIN @gmail.com**' Ex.:'attacker+caf_=target=example.com@gmail.com'
  5. Google's Outgoing MTA relays the modified message to the final destination

## The Case of Gmail: Exploiting the Trust Hierarchy

- Spam Message Whitelisting:
  - Used to fine tune Gmail's spam filters
  - Has tiny effect against global filters, but has powerful effect against local filter
  - After whitelisting messages following the same patterns are treated as good mail.

## The Case of Gmail: Exploiting the Trust Hierarchy

- The vulnerability: Using Gmail as an Open Relay
  - No proof of ownership of the email address that is used as target for the message forwarding option in Gmail accounts is required. A Gmail user can easily setup her account to forward messages to any email address in the Internet, since no verification of ownership is done.
  - No limit is imposed on the number of times a Gmail user can change the email address used as target in the message forwarding configuration.
  - Gmail users can whitelist a spam message.

## The Case of Gmail: Exploiting the Trust Hierarchy

- The attack:
  1. Whitelist the attack message. Since the attack message will probably originate from a blacklisted IP address and might contain other indicators that will make Gmail flag it as spam, the message needs to first be whitelisted (i.e. marked as 'not spam') before it can be forwarded.
  2. Change the email address destination in the message forwarding option.
  3. Deliver the attack message addressed to the compromised Gmail account using one of Google's MTA servers.
  4. Repeat steps 2 and 3 for every email address in the list of addresses to be spammed effectively sending the attack message to all addresses.

## Proof of Concept Experiments

- Assessing Gmail's Protections against Bulk Messages
  - Send same message many times to different addresses using regular interface (no attacks here)
  - Gmail blocked us at 500

## Proof of Concept Experiments

- Assessing Gmail's behavior against the described attack
  - Send same message many times to different addresses using attack vector
  - 4,000+ messages sent
  - Time taken: aprox. 6 hours / Rate: 11 messages/Min.
  - Important Notice: Only one Gmail account was used

## Proof of Concept Experiments

- Assessing the Trust Relationship between Gmail and other systems
  - Accounts created in two major providers (Yahoo and hotmail)
  - Sending messages coined as SPAM directly to test account: Messages Dropped entirely or Marked as SPAM
  - Sending messages in Google's behalf using the attack: Messages accepted in victims inbox

## Proof of Concept Experiments

- Attack Message after final delivery
  - See file
- **Assessing the limit on message forwarding setup change**
  - We have run 10,000 changes (with double check)
  - No countermeasures took place to avoid more changes

## Remarks

- Mitigation of the Flaw
  - Limiting the number of forwarding setup changes
  - Limiting the number of forwarded messages
  - Asking for proof of ownership
  - Forwarding Header Checking
- The Trust Hierarchy Problem
  - Disorganization of trust
  - Gmail gets special treatment not for its security, but for its message volume

## Acknowledgements

- This research was sponsored in part by the United States Army Research Office (ARO) grant number W911NF-07-1-0271.

## Questions?

- Emails:

pablo@ximenes.info

andre@dossantos.org