Introduction to Email Spoofing and Prevention

Sumit Agrawal Piyush Lahoti

Indian Institute of Technology Indore

sumit4iit@gmail.com
piyush@iiti.ac.in

April 24, 2014

Overview

Email Protocols

Interaction between email servers is governed by email protocols.

- Simple Mail Transfer Protocol
- Internet Message Access Protocol
- Post Office Protocol

Post Office Protocol

- Oldest Protocol: (Recent- POP3[1984])
- Clients using POP generally connect, retrive all messages and store them on the user's PC as new message, delete from the server and then disconnect.
- POP3S
- No notion of folders.

Post Office Protocol

Working

```
S: <wait for connection on TCP port 110>
C: <open connection>
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:    +OK mrose's maildrop has 2 messages (320 octets)
C:    STAT
S:    +OK 2 320
C:    LIST
S:    +OK 2 messages (320 octets)
S:    1 120
S:    2 200
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <the POP3 server sends message 1>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    RETR 2
S:    +OK 200 octets
S:    <the POP3 server sends message 2>
S:    .
C:    DELE 2
S:    +OK message 2 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
C:  <close connection>
S:  <wait for next connection>
```

Internet Message Access Protocol

- Defaults to leaving message on email server. Simply downloads a local copy.
- Has notion of folders and hence mailbox is more organized.
- Can perform complex queries. Has ability to retrive partial messages. Allows labeling of emails e.g. read, unread.
- Designed to treat remote mailboxes as if they were local.
- In contrast to POP multiple clients can connect to server on same mailbox.

Internet Message Access Protocol

Working

```
C: <open connection>
S:   * OK IMAP4rev1 Service Ready
C:   a001 login mrc secret
S:   a001 OK LOGIN completed
C:   a002 select inbox
S:   * 18 EXISTS
S:   * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S:   * 2 RECENT
S:   * OK [UNSEEN 17] Message 17 is the first unseen message
S:   * OK [UIDVALIDITY 3857529045] UIDs valid
S:   a002 OK [READ-WRITE] SELECT completed
C:   a003 fetch 12 full
S:   * 12 FETCH (FLAGS (\Seen) INTERNALDATE "17-Jul-1996 02:44:25 -0700"
      RFC822.SIZE 4286 ENVELOPE ("Wed, 17 Jul 1996 02:23:25 -0700 (PDT)"
      "IMAP4rev1 WG mtg summary and minutes"
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      ((NIL NIL "imap" "cac.washington.edu"))
      ((NIL NIL "minutes" "CNRI.Reston.VA.US")
      ("John Klensin" NIL "KLENSIN" "MIT.EDU")) NIL NIL
      "<B27397-0100000@cac.washington.edu>")
      BODY ("TEXT" "PLAIN" ("CHARSET" "US-ASCII") NIL NIL "7BIT" 3028
      92))
S:   a003 OK FETCH completed
```

Figure : Demonstration of IMAP.

Internet Message Access Protocol

Working

```
C:   a004 fetch 12 body[header]
S:   * 12 FETCH (BODY[HEADER] {342}
S:   Date: Wed, 17 Jul 1996 02:23:25 -0700 (PDT)
S:   From: Terry Gray <gray@cac.washington.edu>
S:   Subject: IMAP4rev1 WG mtg summary and minutes
S:   To: imap@cac.washington.edu
S:   cc: minutes@CNRI.Reston.VA.US, John Klensin <KLENSIN@MIT.EDU>
S:   Message-Id: <B27397-0100000@cac.washington.edu>
S:   MIME-Version: 1.0
S:   Content-Type: TEXT/PLAIN; CHARSET=US-ASCII
S:
S:   )
S:   a004 OK FETCH completed
C    a005 store 12 +flags \deleted
S:   * 12 FETCH (FLAGS (\Seen \Deleted))
S:   a005 OK +FLAGS completed
C:   a006 logout
S:   * BYE IMAP4rev1 server terminating connection
S:   a006 OK LOGOUT completed
```

Figure : Demonstration of IMAP.

Simple Mail Transfer Protocol

- We use IMAP and POP to *receive emails*. We *send* emails using SMTP
- Email is submitted by client using MUA *(Mail User Agent)* which is delivered to MTA *(Mail Transfer Agent)*.
- MTA performs DNS lookup to lookup MX *(Mail eXchanger)* records. MTA next connects to MX server as SMTP client.
- Once target MX accepts the message it hands it over to MDA *(Mail Delivery Agent)*. MDA further saves message in relevant message format.
- Further end user clients connect to server using POP or IMAP to access emails.

Simple Mail Transfer Protocol

Working

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

Figure : Demonstration of SMTP.

Open Mail Relay

- An *open mail relay* is an SMTP server configured such that it allows any one on the Internet to send emails through it.
- Spammers would sent one email to openrelay and include a large bcc list, then the open relay would spam the entire list.
- Hashbusters
- Closing relays: Mailboxes should not accept and forward arbitrary e-mails from non-local ip addresses to non-local mailboxes by an unauthenticated or unauthorized user.

Sender Policy Framework

- SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific spf record (can be specified using TXT as well).
- example.net TXT "v=spf1 mx a:p.example.net include:aspmx.googlemail.com -all"

Sender Policy Framework: Contd.

- If domain publishes a SPF record, spammers and phishers are less likely to forge e-mails from that domain.
- Issues in case of forwarding:
- Forwarder does not rewrite a return path.
- The next hop does not white list the forwarder

Domainkeys Identified Mail

- DKIM is a way to associate domain name with email. This association is set up by means of digital signature which can be verified by recepients.
- Similar to PK Infrastructure.
- Singer claims responsibility by adding a DKIM signature field to message's header. The verifier recovers singer's public key using dns lookup and verifies that signature matches message's contents.

Domainkeys Identified Mail: Working

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
     c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
     h=from:to:subject:date:keywords:keywords;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
              VoG4ZHRNiYzR
```

Figure : Demonstration of SMTP.

- b: body + headers [signature]
- bh: body [Hash]
- d: signing domain
- s: selector

Domainkeys Identified Mail: Working

- v: version
- a: signing algorithm
- c: canonicalization algorithm
- q: default query method
- l: length of the canonicalized part of the body that has been signed.
- t: signature time
- x: expire time
- h: list of signed header fields.