Email Security: Considering Spam

SMTP

- Simple Mail Transfer Protocol
  - Client connects to server on TCP port 25
  - Client sends commands to server
  - Server acks or notifies of error
- Security issues
  - Sender not authenticated
  - Message and headers transmitted in plain text
  - Message and header integrity not protected
  - Spoofing trivial to accomplish

Example SMTP session

```
HELO mail.university.edu
MAIL FROM: president@whitehouse.gov
RCPT TO: chancellor@university.edu
DATA
From: president@whitehouse.gov
To: chancellor@university.edu
Date: April 1, 2010
Subject: Executive order
You are hereby ordered to increase the stipend of all TAs by $10,000 per year.
Sincerely,
The President of the United States
```
What is Email Spam?

• Email spam is often defined as unsolicited bulk email
  – Forbidden by all major ISPs
  – Considered “acceptable business practice” by US Direct Marketing Association (DMA)
• Unsolicited email and bulk email are individually acceptable practices for people, business, and organizations
• Spam arises from the combination of unsolicited and bulk
• In classifying email as spam, content does not matter
• The US CAN-SPAM act (2004) regrettably protects commercial spam provided some requirements are satisfied, including:
  – Opt-out mechanism
  – Sender clearly identified and subject line not deceptive
  – Adult material labeled in subject line

Who Responds to Spam anyhow?

A princess in Nigeria wants to send me money!
Spam Conversion

- Empirical study [Kanich+ 2008]
  - Parasitic infiltration into botnet launching spam campaign for “Canadian drugs”
  - 28 conversions, yielding $3K, from 300M spam messages over 26 days

Blacklisting

- Spamhaus Black List (SBL)
  - Real-time database of IP addresses of verified spam sources
  - Eliminates about 10% of spam before transmission takes place
  - Formal listing and delisting procedures
  - More than 600M email users protected by SBL

- How to circumvent blacklisting
  - Powerful blacklisted spam server impersonates small unlisted zombie
  - Initiate TCP handshake from zombie
  - Send bulk email from spam server using spoofed source IP and TCP sequence numbers

TCP handshake

zombie

TCP sequence numbers

spam server

SMTP spam transmission

victim
Graylisting

- Spam servers typically do not resend messages after transmission errors
- Maintain database of trusted servers
- Respond with “Busy, please retry” to SMTP connection requests from servers not in database
- Server added to database if reestablishes connection
- Currently effective although simple to circumvent

Sender ID and Sender Policy Framework

- Store DNS records about servers authorized to send mail for a given domain
- Look up domain in From header to find IP address of authorized mail server

Source: Microsoft
DomainKeys Identified Mail (DKIM)

- Sender’s mail server signs email to authenticate domain
- Public key of server available in DNS record
- To be used in conjunction with other spam filtering methods

SenderID vs. DKIM

**SenderID**
- Sending MTA authentication
- Channel based
- Simple implementation
- Message integrity not protected
- Mail forwarding not supported
- Vulnerable to DNS cache poisoning
- Vulnerable to IP source spoofing

**DKIM**
- Sending MTA authentication
- Object based
- Cryptographic assurance
- Protection of message integrity
- Supports mail forwarding
- Vulnerable to DNS cache poisoning