Email Security

CS 166: Introduction to Computer Systems Security
E-mail Transport

Sender

MUA

MTA

SMTP

Recipient

MUA

MTA

POP/IMAP

Internet

• MUA: mail user agent, aka mail client
• MTA: mail transport agent, aka mail server
SMTP

• Simple Mail Transfer Protocol
  – Client connects to server
  – Client sends commands to server
  – Server acks or notifies of error

• Security issues
  – Sender not authenticated
  – Message transmitted in plain text
  – Message integrity not protected
  – Spoofing trivial to accomplish

HELO mail.cs.brown.edu
MAIL FROM: djt@whitehouse.gov
RCPT TO: rt@cs.brown.edu
DATA
From: djt@whitehouse.gov
To: rt@cs.brown.edu
Date: March 23, 2017
Subject: Executive order
You are hereby ordered to grade all
the students of CS166 class with A.
The President of the United States
What is Email Spam?

- Unsolicited email and bulk email are each acceptable
- Spam combines unsolicited and bulk
  - Forbidden by all major ISPs
  - Considered “acceptable business practice” by US Direct Marketing Association (DMA)
- In classifying email as spam, content does not matter
- US CAN-SPAM act (2004) protects commercial spam subject to requirements:
  - Opt-out mechanism
  - Sender clearly identified and subject line not deceptive
  - Adult material label in subject
Phishing

• Imitates legitimate websites
• Attempt to fraudulently acquire sensitive information (passwords, credit card numbers, etc.)
• Victim often lured to via email
• Relies on the user not inspecting page in depth
• Examples on www.phishtank.com
Unicode Phishing Attack

- Unicode characters may be rendered with ASCII ones
- E.g., www.STALLirectionalS.pαypal.com, where “α” is the Unicode character for the Greek letter alpha, may be displayed as www.paypal.com
- Another example: is this the real apple.com??
Falling Victim to Phishing Attacks

• Spear Phishing
  – Phishing attempts directed at specific individuals or companies
  – Attackers may gather personal information about their target to increase their probability of success

• Whaling
  – Attacks directed specifically at senior executives and other high profile targets within businesses,

• These attacks can be very successful and difficult to detect
Spam Conversion

- Who reads spam anyhow?
- Empirical study [Kanich+ 2008]
  - Parasitic infiltration into botnet launching spam campaigns
  - 28 conversions, yielding $3K, from 300M spam messages over 26 days
  - Spam business has small profit margin
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
Graylisting

• Spam servers typically do not resend messages after transmission errors
• Maintain database of trusted servers
• Respond with “Busy, please retry” to SMPT 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
DomainKeys Identified Mail (DKIM)

- Sender’s mail server signs email to authenticate domain
- Public key of server available in DNS record

**DomainKey-Signature:**
```
a=rsa-sha1; s=mail;
d=example.net; c=simple; q=dns;
b=Fg...5J
```

**Authentication-Results:**
```
from=bob@example.net; domainkeys=pass;
```
SenderID-SPF vs. DKIM

**SenderID - SPF**
- 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
DMARC

• What is DMARC
  – Domain-based Message Authentication Reporting and Conformance
  – Emerging standard
  – Supplements and works with DKIM and SPF

• Features
  – Additional DNS records
  – Description of sender’s email policies
  – Instructions to receiver on handling messages that do not conform to sender’s policies
What We Have Learned

• SMTP protocol and its limitations
• Spam and phishing attacks
• Spam conversion rates
• Blacklisting and graylisting
• Integrity protection and email policies via DKIM, SPF, and DMARC