Sender Authentication: Myths Revealed

Anti-phishing Working Group
Sept 28 Washington, DC
Miles Libbey
Anti-spam Product Manager
Yahoo! Mail

Fact or Fiction:
Sender Authentication will stop spam

Spammers can trivially authenticate

- CipherTrust: Spam currently 34% more likely to be SPF verified than legit mail
- Why do Sender Authentication?
  - To kill forgery
  - To use reputation and accreditation information to help fight spam
  - To help stop phishing
  - Increase traceability of spammers

Fact or Fiction: Sender Authentication will stop spam

Fiction

Fact or Fiction: I don’t need to worry about forwarding

Any sender can unknowingly send email to a forwarder

- Email providers that allow forwarding
  - Yahoo! Mail - SBC
  - Comcast - Mail.com
  - Earthlink - Juno
  - Verizon - many others
- If your company or users email users at any of these domains (and thousands of other domains that allow forwarding) forwarding may affect you

Why is forwarding an issue in email authentication?

- With a strict SPF/Sender ID record (”-all”), email sent to a user that forwards may be adversely affected
- Forwarders need to change to comply with SPF/Sender ID
  - Rewrite envelope from?
  - Add header?

The Sender's dilemma

- Publish strict (-all) SPF/Sender ID records
  - Stop forgery and phishing of your domain
  - Email to forwarders marked as forgery
- Publish 'weak' (?all) SPF/Sender ID records
  - Ensure email delivery
  - Doesn't stop forgery or phishing

Fact or Fiction: I don’t need to worry about forwarding

Fiction

Fact or Fiction:
SPF/Sender ID authenticates the sender

IP based solutions authenticate the last hop

- In a percentage of email, original sender is the only hop
- Email can traverse several hops
  - Forwarding
  - Mailing lists
  - Internal network topologies
- Do legitimate senders want someone else's reputation applied to their email?

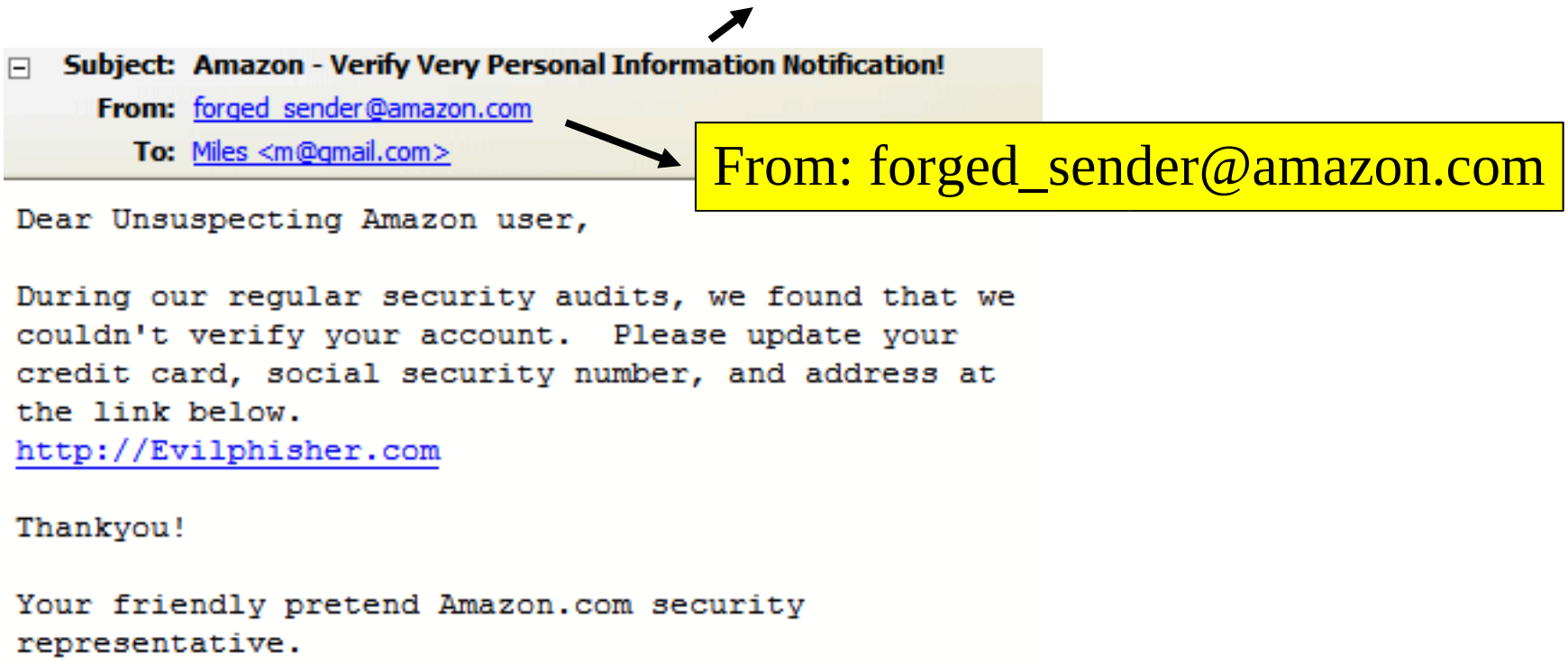
Fact or Fiction: SPF/Sender ID authenticates the sender

Fiction

Fact or Fiction:
SPF/Sender ID stops forgery and phishing

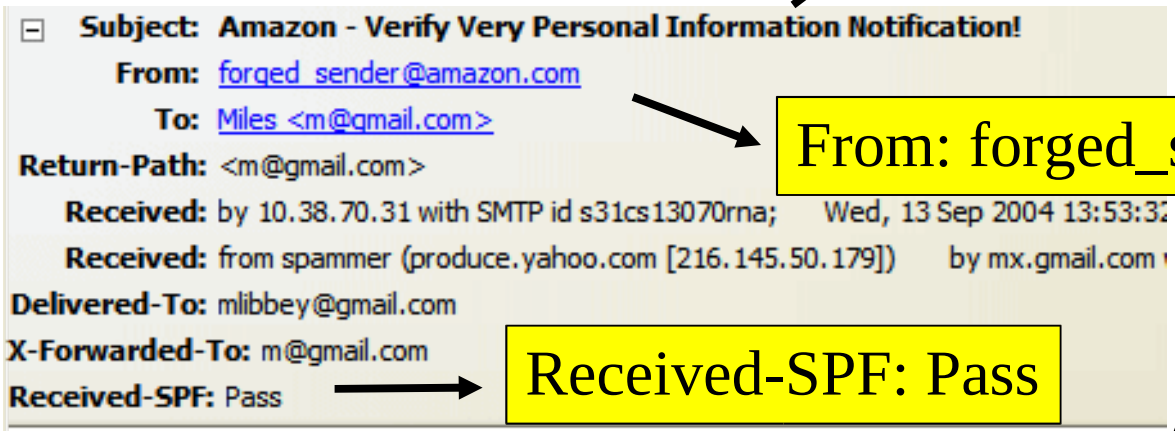
Is this a forged email?

Subject: Amazon - Verify Very Personal Information!



Is this a forged mail?

Subject: Amazon - Verify Very Personal Information!



From: forged_sender@amazon.com

Received-SPF: Pass

Dear Unsuspecting Amazon user,

During our regular security audits, we found that we couldn't verify your account. Please update your credit card, social security number, and address at the link below.
http://Evilphisher.com

Thankyou!

Your friendly pretend Amazon.com security representative.

According to SPF, this email is authenticated.

The spammer pretended to be a forwarder.

Forgers will adapt to pretend to be a forwarder

- BigBank.co publishes strict Sender ID records
- EvilPhisher.co does publish Sender ID record
- EvilPhisher.co pretends to forward a email from BigBank.co
- Reciever.co checks EvilPhisher.co’s Sender ID record: Pass - not forged

The Sender's dilemma, clarified

- Publish strict (-all) SPF/Sender ID records
  - ~~Stop forgery and phishing of your domain~~
  - Doesn't stop forgery or phishing
  - Email to forwarders marked as forgery
- Publish 'weak' (?all) SPF/Sender ID records
  - Ensure email delivery
  - Doesn't stop forgery or phishing

Fact or Fiction:
SPF/Sender ID stops forgery and phishing

Fiction

Fact or Fiction: SPF/Sender ID is lightweight, quicker to implement than DomainKeys

SPF/Sender ID has 2x more code, constant maintenance

- Compared 4 DomainKeys implementation to Sender ID implementations
  - DomainKeys averaged 2x less code than Sender ID
- Changing IP addresses results in Sender ID changes
  - In last 3 years, Yahoo! Mail has completely changed IP addresses >3 times
  - Cooperation between operations, email admin, DNS
- Sender ID is easier to implement for domains that ONLY send mail
  - Who sends email but does not receive it?
  - Spammers!
- IP based solutions constantly changing. Forwarders action items unclear and ever changing
- Sendmail benchmark: DomainKeys increases CPU by 8-15%

Fact or Fiction: SPF/Sender ID is lightweight, quicker to implement than DomainKeys

Fiction

Fact or Fiction: DomainKeys is the long term sender authentication solution

DomainKeys benefits

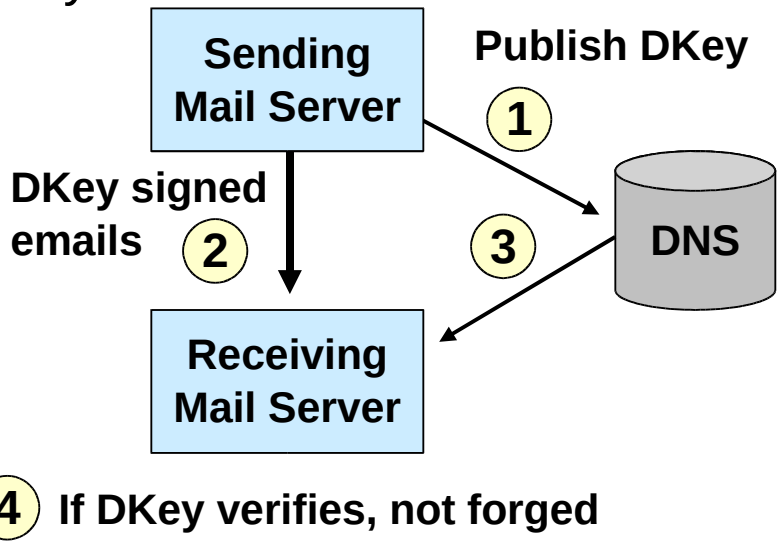
- Authenticates original sender
- Identifies forgery
- Message content tamper-proof
- Significantly less ongoing maintenance
  - Install and forget for years
  - 640 bit keys and bigger never been cracked (>$20k prize)
- Yahoo!, SBC, British Telecom, Rogers Cable implementing this year
- Long Term is now short term

Fact or Fiction: DomainKeys is the long term sender authentication solution

Fact

How DomainKeys works

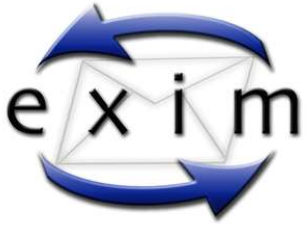
- Generate public-private key pair
- Publish the public key in DNS
- Using the private key, digitally sign the message and include in the headers
- Send the mail
- Receiver finds the domain from the Body From: or Sender:
- Receiver queries DNS for public key
- Checks signature
  - If signature verifies, know the message from the domain **and** is unaltered
  - If the signature does not verify, the message was altered or forged



MTAs and domains committed to testing DomainKeys

YAHOO! Mail

sendmail.org



port25 solutions, inc.

TUMBLEWEED COMMUNICATIONS

ROGERS

BT

Phisher attacks on DomainKeys

- Disposable or cousin domains
- Phisher authenticates domain using Sender: header
- Phisher inserts bogus signature
- Crack the key
- Attack domains not using DomainKeys

Myths Revealed

- Email Authentication does not stops spam
- Forwarding affects you
- Sender ID does not authenticate the original sender
- Sender ID neither stops forgery nor phishing
- Sender ID is neither light-weight, nor easy to implement
- DomainKeys is the long term solution