Cyber Defense Organization

Fall 2020 - Email Forensics/Phishing

What this won't be

- This is not phishing signs 101
- This is not a definitive guide on email analysis (not even close)

What I am not:

- A 100% expert on email analysis

What this will be:

- A beginners look at email headers and analysis

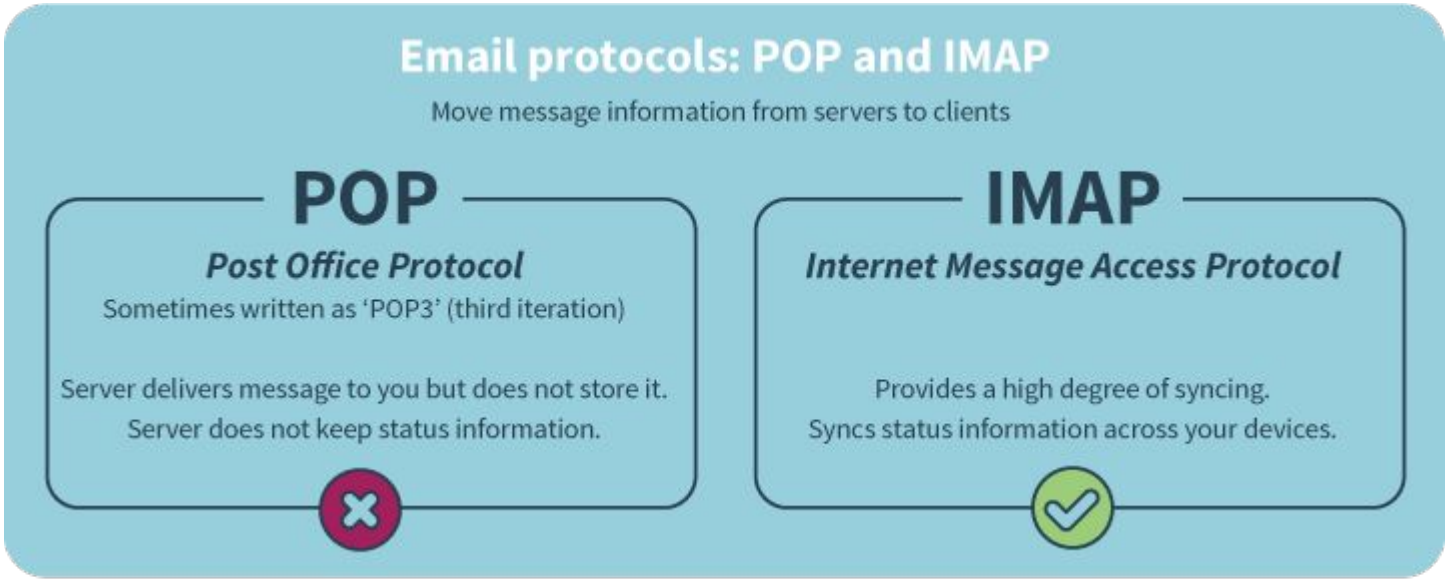
Word of the Week: KnowBe4

Why email is important

- They say if you compromise email, you compromised a lot of different accounts
- Some low tech insider threats use email as exfiltration
- Phishing/social engineering (today's topic)

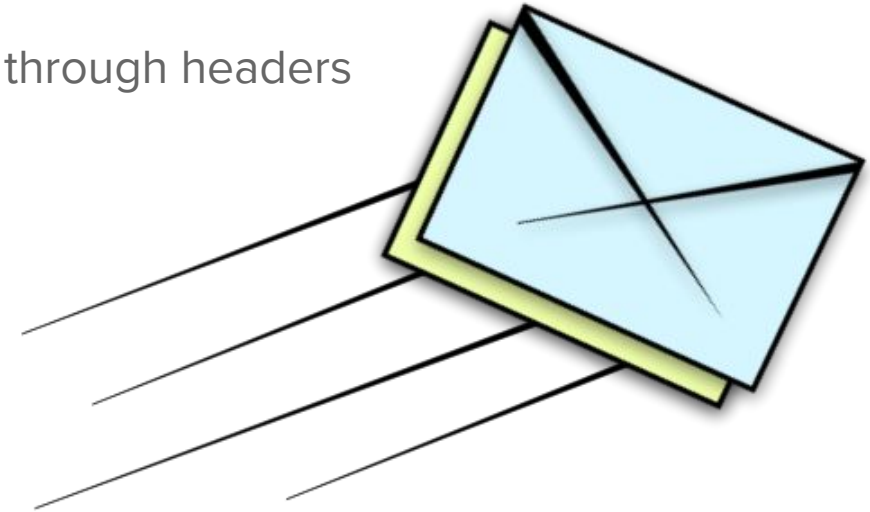
IMAP VS POP

Body

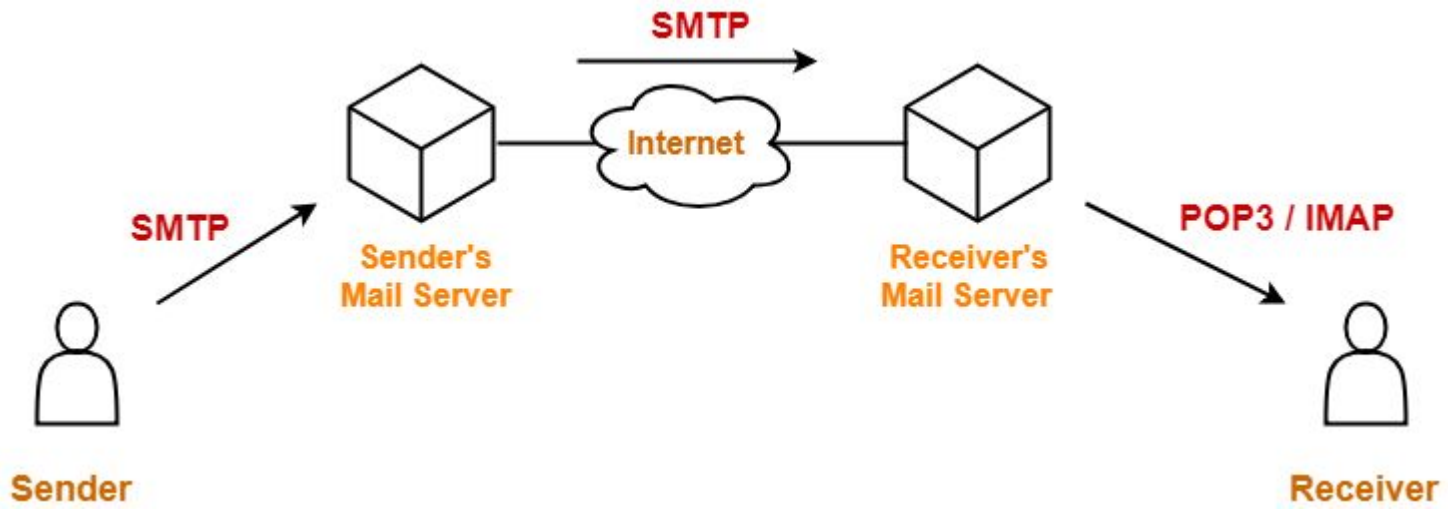


SMTP

- Stands for Simple Mail Transfer Protocol
- The method of sending emails between servers
- Insecure and extremely trusting
- You can see the history of smtp servers through headers
- Uses MX records



SMTP & POP/IMAP together



Email Anatomy

- Email Envelope Vs Email headers
  - Like a post office
  - Info DOES NOT need to match
- From address
- To address
- Reply-To (Should be the same as the From address)
- Subject

Why is phishing important

- Look at the figures: estimates range from 50% - 90% of incidents are caused by phishing
  - https://www.phishingbox.com/news/phishing-news/verizon-data-breach-investigations-report-dbir-2019
  - https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks
- Can get past firewalls and other defensive measures (degrades the secure walls, soft underbelly)

Phishing

- A social engineering attack that is used to steal user's data
- Can be aimed at credential harvesting, PII harvesting, delivering malware, etc.
- Usually thought of in terms of email but really is quite expansive

Different Types of phishing:

- Whaling: Aiming for big targets such as CEOs
- Vishing: Uses a phone call instead of an email
- Spear phishing: Aimed a specific individual with their identifying information
- Smishing: Using SMS/text instead of email

Case Study: Gathering info

Let’s see how we could get info to mount a credential harvesting attack

Choose a domain and enter it here: https://mxtoolbox.com/

What Phishing preys on

- A sense of urgency: “OH NO MY ACCOUNT GOT HACKED”
- A sense of legitimacy: If it uses your identifying information, or appears to be from a reputable source
- People not reading the from address (even though it can be spoofed, and is not 100% reliable)
- Curiosity

The Value of Email Headers

- Tells you info such as:
  - What SMTP servers it passed through
  - SPF, DMARC, DKIM, ARC auth results
  - Different headers that was sent with it
  - Timestamps
  - Unique message ID
- TLDR: A Lot

Why Default SMTP Kind of Sucks

- There is a lack of authentication measures in the original protocol
- Lack of encryption by default
- So.... there are some ways (besides SMTP Auth) that spam filters detect abuse of email measures

SPF

- Sun Protection Factor.... GLOBAL WARMING IS REAL
- Senders Policy Framework (type of authentication)
- Creates a list of IP addresses that are allowed to send from a domain
- Could break when forwarding an email address between servers
- Only checks the FROM on the envelope

So... can anyone guess what can be a problem with this?

SPF Policy Example

v=spf1 include:_spf_ipv4.netflix.com include:_spf.google.com include:amazonses.com include:servers.mcsv.net -all

- V: version
- Include: what domains to allow (spf_ipv4.netflix.com resolves to this spf rule: v=spf1 ip4:205.139.44.20 ip4:66.150.112.120 ip4:205.139.45.20 ip4:209.177.164.2 ip4:209.177.166.34 ip4:207.45.73.162/31)

DKIM (DomainKeys Identified Mail)

- Method of authentication of email headers
- Implemented with a DNS TXT record of a public key
- Takes a hash of headers and email body then encrypts it with private keys
- Receiving server reverses it

The value of this:

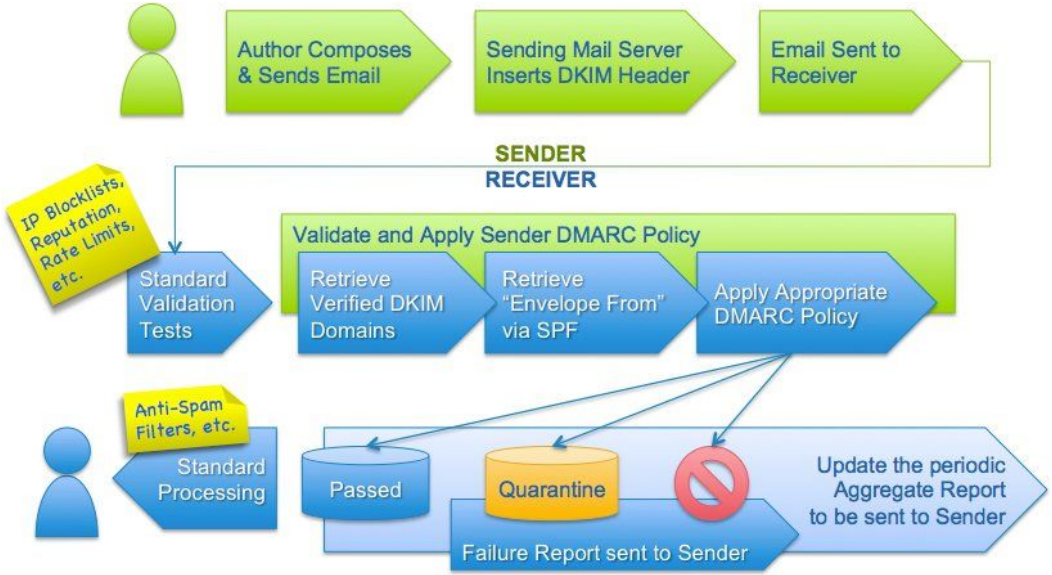
- Email headers are now authenticated
- Ensures email contents are not modified
- Provides for non repudiation

Example of a DKIM header

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

DMARC

- Stands for Domain-based Message Authentication
- SPF & DKIM are included in a DMARC “policy”
- What to do if email claiming to be from domain fails SPF & DKIM checks
- Used by email filters



Example DMARC Policy

v=DMARC1\;p=none\;rua=mailto:dmarc@sendgrid.com\;ruf=mailto:dmarc@sendgrid.com\;rf=afrf\;pct=100

Breakdown:

V is version

P is the policy (none, reject, quarantine) - this case no action would be taken

Rua: where to send high level DMARC reports to

Ruf: where to send low level DMARC reports

rf : reporting format

Pct: % of emails policy applies to

ARC Policy

- Authenticated Received Chain
- Designed in 2016 to help with mailing lists and forwarding
- Reduce false positives
- Yahoo, Gmail example

Arc Seal & Arc Message Signature

- Checks to ensure validity of ARC chain and adds its own signature

How to Defend

PEOPLE, PROCESS, TECHNOLOGY

People: Do trainings with them, use phishing tests

Process: what is the process people should take to report emails? Is it an easy repeatable process?

Technology: What is in place to prevent phishing emails from getting through? Spam filters? Technology like Proofpoint? What technology is used in the process to report emails?

How to read email headers

Example time (with my own personal email)

Non-Educational Videos

James Veitch on spam: Cuz why not

https://www.youtube.com/watch?v=mrh9KbhrXD8

https://www.youtube.com/watch?v=3MHDDSekvcE

Hands On

- Go through your email and look through the headers
- I will chill in Discord chat in case you want to look at any with me

Coming up next week!

Tuesday: Blue Team Practice @ 7pm

Wednesday: Security + @ 5pm

Thursday: Red Team Practice @ 7:30pm

Friday: Python Workshop @ 3:30pm

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!