MAIL SECURITY AND THE DNS

John Levine

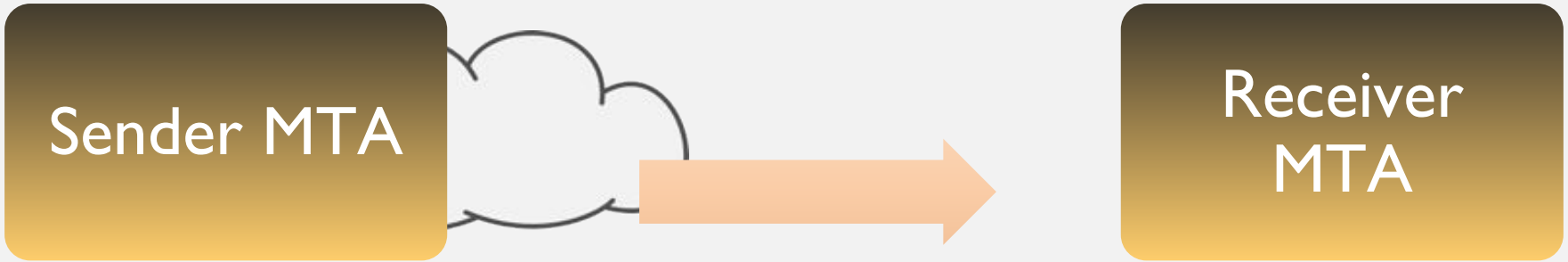
STANDCORE LLC

ICANN 65 | Marrakech

MAIL AND SMTP ARE VERY VERY OLD

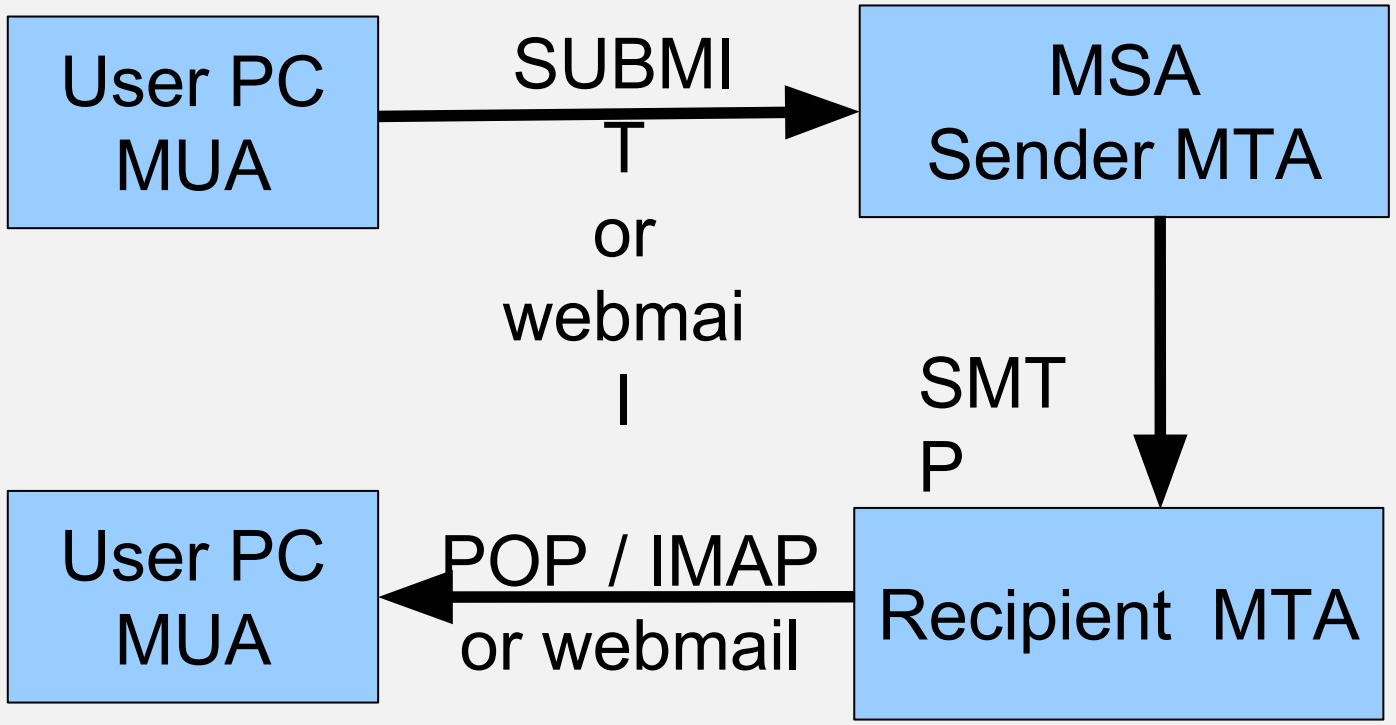
- Message format from RFC 733 in 1977
- SMTP from RFC 788 in 1981
  - Both pretty much the same today, with a lot of extensions
- DNS wasn't invented until RFC 881/2/3 in 1983
- MX records for mail routing in RFC 974 in 1986

INTERNET MAIL ARCHITECTURE



Sender MUA

INTERNET MAIL TLAS



WHAT PROBLEM ARE WE SOLVING?

- Spam started to be a problem in mid 1990s
- Phish and malware in the 2000s
- Identify unwanted mail by sender, malicious mail by content such as URLs
- Spam filters are complex: today we only look at bits that use the DNS

SMTP ENVELOPE AND BODY

connection from 203.0.113.1

220 mail1.example.com mh ESMTP

HELO mailout.example.com

250 mail1.example.com

MAIL FROM:<bob@example.com> *or* MAIL FROM:<>

250 2.1.0 Sender accepted.

RCPT TO:<mary@example.net>

250 2.1.5 Recipient accepted.

...

SMTP ENVELOPE AND BODY

DATA

354 End your message with a period on a line by itself.

--- message header including To:, From:. Cc: ---
--- and message body ---

.

250 2.6.0 Accepted message qp 50475 bytes 976

QUIT

221 2.0.0 Good bye.

MX AND A/AAAA RECORDS TO FIND MAIL SERVERS

To: bob@examp1e.com

- Look up MX records

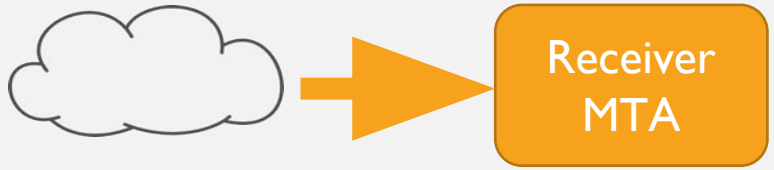
examp1e.com MX 10 mx1.example.net

- Look up A/AAAA records

mx1.example.net A 192.0.2.1
mx1.example.net AAAA 2001:db8:42::a3:f

- If no MX, fall back to A/AAAA
  - 30 years of backward compatibility

PTR VALIDATION OF SENDING IP ADDRESSES



- Mail server gets connection from 203.0.113.1
- Do rDNS lookup

  1.113.0.203.in-addr.arpa PTR mailout.example.net
- Then check forward lookup

  mailout.example.net A 203.0.113.1
- Do they match and look non-generic?
  - Matching forward/reverse says static allocation
  - Generic name says random residential user, e.g. cpe-74-66-241-88.nyc.res.rr.com

DNS BLACK/WHITELIST OF IPS

- Mail server gets connection from 203.0.113.1
- Look up IP in DNSBLs configured in inbound MTA:

1.113.0.203.bl.badguys.net NXDOMAIN ☞ OK

1.113.0.203.bl.badguys.net A 127.0.0.5 ☞ uh oh

- Low bits typically indicate why listed
- Sometimes used to block outright, sometimes in spam scoring
- DNS whitelists exist but aren't very interesting

DNS BLACK/WHITELIST OF DOMAINS

- Envelope or body URL domain name maybe.org
- Look up IP in DNSBLs configured in inbound MTA:

maybe.org.dbl.badguys.net NXDOMAIN ☞ OK

maybe.org.dbl.badguys.net A 127.0.0.5 ☞ uh oh

- Low bits typically indicate why listed
  - Newly registered, seen in phish, related to other malicious, ...
- Envelope often used to block outright, body URL in spam scoring

SPF PATH VALIDATION

HELO mailout.example.net

MAIL FROM:<bob@example.com>

- Check SPF record for sending or HELO domain

example.com TXT “v=spf1 mx ip4:203.0.113.0/25 ~all”

- No changes to mail sending
- Complex spec, can say yes, no, or two kinds of in between

SPF PATH VALIDATION

HELO mailout.example.net

MAIL FROM:<bob@example.com>

- Typically used in DMARC or to whitelist known senders
- Can’t describe a lot of valid mail
- **Doesn’t mean the mail is good**, only that it was sent by the purported envelope sender

DKIM MESSAGE CONTENT VALIDATION

- Cryptographic signature of hashes of message headers and content
- Validation key in the DNS

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple; d=example.com;
    h=date:message-id:from:to:cc:subject:in-reply-to;
    s=k1906; bh=3MVSYjdcf7HbxwaOvclgeGwI+is5VbRZigtSsm/jiUU=;
    b=R6ZT1a9kbCXfBBCWH0KbozQBbxSrKFLVThI7tHm...

k1906._domainkey.example.com TXT “v=DKIM1; h=sha256;
    p=MIHfMA0GCSqGSIb3DQEBA ...”
```

DKIM MESSAGE CONTENT VALIDATION

- Recipient recomputes the hashes to see if the message is "the same"
- If so, checks the signature against the DNS
- If OK, it means the d= domain takes responsibility for the message
  - **Still doesn't mean the mail is good**
- Multiple signatures with different d= are common
- Like SPF, used with DMARC and for local whitelisting
- Works better with forwarding, but much more work than SPF
  - Breaks when forwards edit the message, e.g. mailing list
  - But forwarders should re-sign to take responsibility

DMARC SENDER POLICY

- Publish sender policy for domain in the From header
  - From: Mr. Bob <bob@example.com>
- ”Alignment” depends on SPF and DKIM
  - SPF: aligned if envelope has same domain and SPF says yes
  - DKIM: aligned if valid DKIM signature with d=example.com
- If aligned, DMARC does nothing
- But if not aligned ...

DMARC SENDER POLICY

- From: Mr. Bob <bob@example.com>

- _dmarc.example.com TXT “v=DMARC1; p=none;
  rua=mailto:dmarc-a@example.com;
  ruf=mailto:dmarc-f@example.com”
- Policy advice to recipients on DMARC failure
  - None: deliver as normal
  - Quarantine: put in the spam folder
  - Reject: bounce back

DMARC SENDER POLICY

- Policy advice to recipients on DMARC failure
  - None / quarantine / reject
- Originally intended for phish targets like paypal.com
- Repurposed when AOL and Yahoo had millions of address books stolen
- Fails on a small fraction of high value mail, notably discussion mailing lists
- Lots of nonsense about how DMARC unaligned is “wrong”

DMARC SENDER POLICY

- _dmarc.example.com TXT “v=DMARC1; p=none;
  rua=mailto:dmarc-a@example.com;
  ruf=mailto:dmarc-f@example.com
- Reporting via rua=<address> and ruf=<address>
  - rua: daily aggregate reports, fairly common
  - ruf: individual failure reports, fairly rare
  - Interesting stuff about your mail even if you state no policy

ARC POLICY CHAINING

- Intended to undo DMARC damage to mailing lists and other forwarders
- DKIM-like signatures showing chain of custody

ARC POLICY CHAINING

ARC-Seal: i=1; a=rsa-sha256; cv=none; d=lists.iecc.com; s=9f5f.5d0bad5c.k1906;
t=1561046364; b=E/sM30VYN6xDl1K0s8F2YWt5Yr0F0J0L==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=lists.iecc.com;
h=from:date:message-id:to:content-type:subject:reply-to:sender;
s=k1906; bh=BbD0NyCbReUbOnx=; b=X6P15BozQ2HFNVdi92DCDkz==

ARC-Authentication-Results: i=1; iecc.com; arc=none;
smtp.remote-ip=209.85.208.44; spf=pass spf.mailfrom=sam@them.net
spf.helo=mail1.google.com; dmarc=pass header.from=them.net (p=none)

ARC POLICY CHAINING

- Recipient can check chain of custody in mail from credible senders, e.g. mailing lists
- Use chain info to do retroactive filtering
- If senders are credible, why not just whitelist them?
  - Lists often validate only by From: address, forged spam leaks through
  - Relatively easy to detect using Authentication-Results in the chain
- Sort of implemented at Google and VZ (Yahoo/AOL)

DANE TLSA SERVER CERTIFICATES

- TLSA originally used to validate certificates on web servers
- But can equally well validate certificates on anything

ARE YOU MY MAIL SERVER?

220 mail1.example.com mh ESMTP

ehlo mailout.example.com

250-mail1.example.com
250-SMTPUTF8
250-8BITMIME
250-PIPELINING
250 STARTTLS

STARTTLS

220 2.0.0 Ready to start TLS

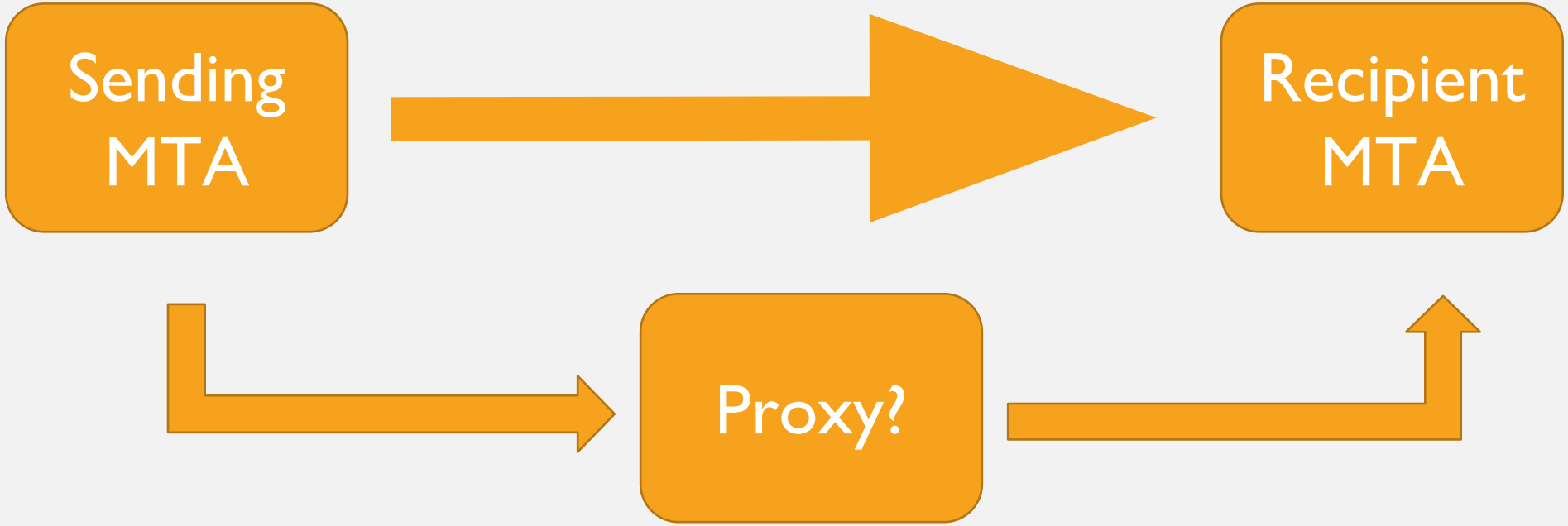
... negotiate TLS session ...

220 mail1.example.com mh ESMTP

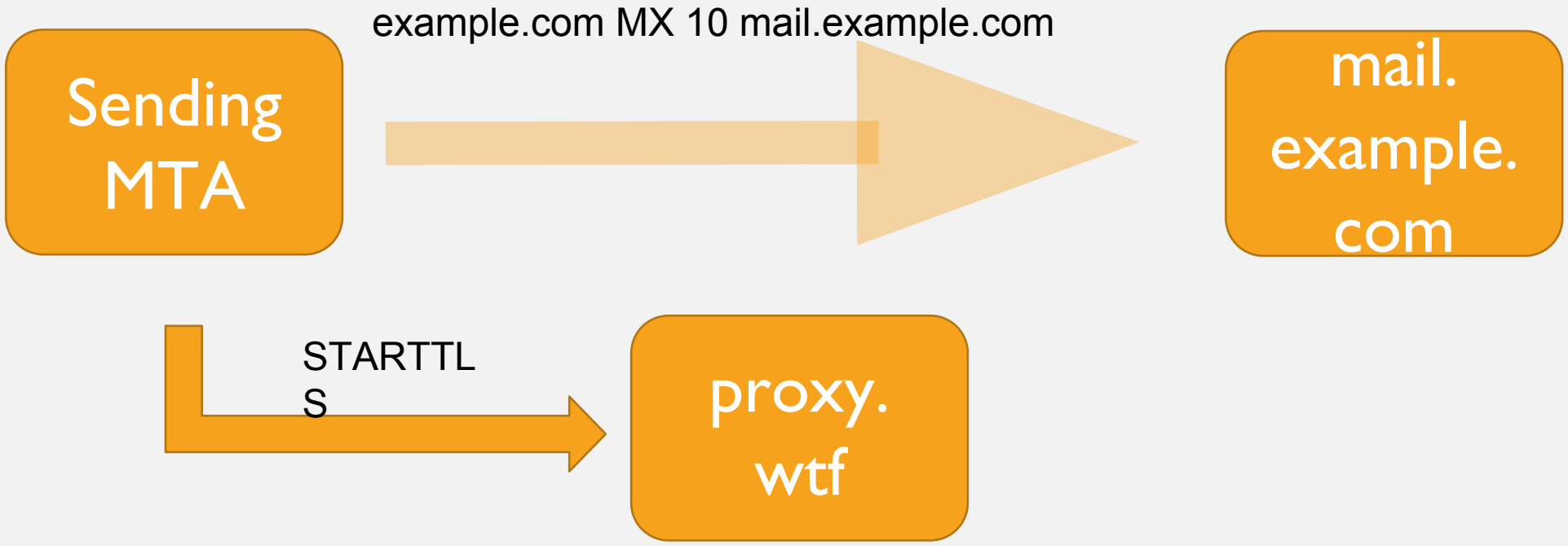
ehlo ...

TLS encrypted

ARE YOU MY MAIL SERVER?



ARE YOU MY MAIL SERVER?



ARE YOU MY MAIL SERVER?

- DNSSEC protects MX and A records
- STARTTLS retrieves server's certificate
- DANE TLSA validates server's certificate
- If no match, don't send the mail
- I know this works
  - Because I messed up my TLSA and Comcast wouldn't accept my mail

POSSIBLE FUTURE DIRECTIONS WITH DBOUND AND DMARC PSD

- The Mozilla Public Suffix List is a horrible kludge
- But it is very useful so we all use it
  - Cookie policy in browsers
  - CA's signing *.example.com certificates
  - DMARC *Organizational* Domain

DMARC ORGANIZATIONAL DOMAINS

From: <bob@sales.example.com>

From: <mary@support.example.com>

_dmarc.example.com TXT “v=DMARC1; p=reject; ...”

- Publishing a DMARC policy for every possible subdomain is hard
- So if there isn’t one, DMARC checks the “organizational” domain
- Which is the label below the next PSL public suffix above

PUBLIC SUFFIX DOMAINS

- Some branches of the DNS are under single management
  - *someone@something*.gov.uk is always part of HM government
  - *someone@something*.bananarepublic always works for Gap
- Some TLDs have strong agreements with their registrants
  - *anything*.bank has to be a bank, requires strong DMARC policy
- PSD: experimental DMARC extension applies policy to public suffix
  - Look one level up from the organizational domain

CAN WE DO BETTER THAN THE PSL?

- IETF **dbound** WG looked at ways to put PSL-like info in the DNS
- Questions of semantics and name management
  - Is boundary info in the zone itself or somewhere else?
  - How many kinds of boundaries are there?
  - Who controls the boundary info?
  - How expensive are lookups? (Big issue for web browsers)
- Several proposals, none got consensus
  - I really liked mine

MAIL SECURITY AND THE DNS

John Levine

STANDCORE LLC

ICANN 65 | Marrakech