Neither Snow Nor Rain Nor MITM…
An Empirical Analysis of Email Delivery Security

Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten,
Kurt Thomas, Vijay Eranti, Nicholas Lidzborski,
Elie Bursztein, Michael Bailey, J. Alex Halderman

University of Michigan, University of Illinois
Urbana-Champaign, Google

Who am I?

I am a Ph.D. Candidate at University of Michigan. My research focuses on measurement-driven security.

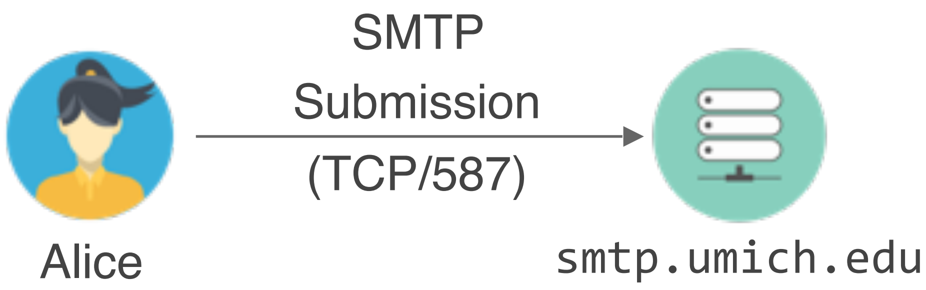
① Developing tools for researchers to better measure the Internet

zmap

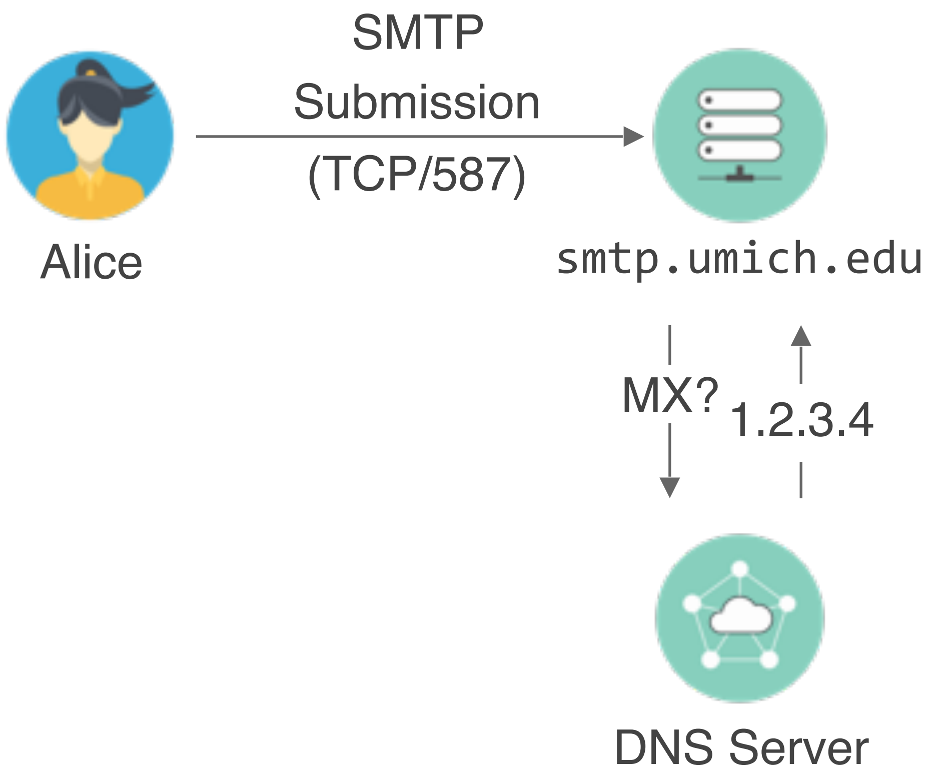
② Using this perspective to understand how systems are deployed in practice

censys

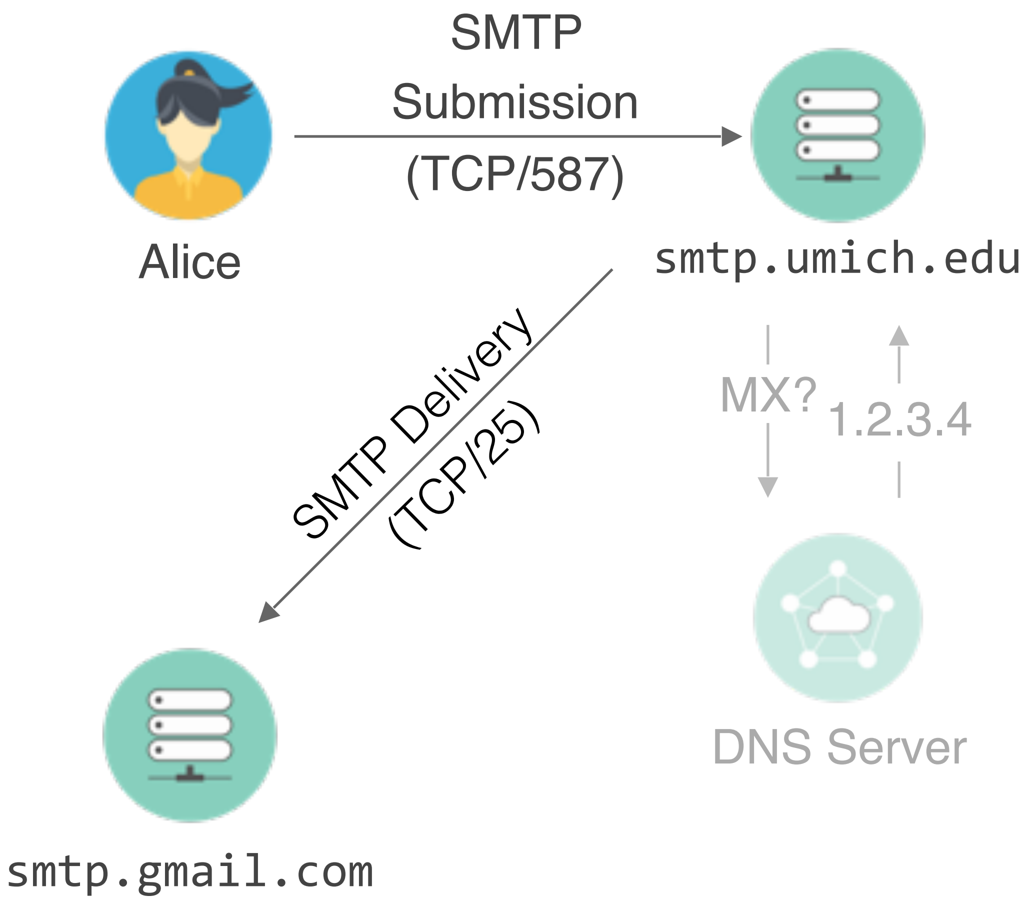
E-mail Security in Practice



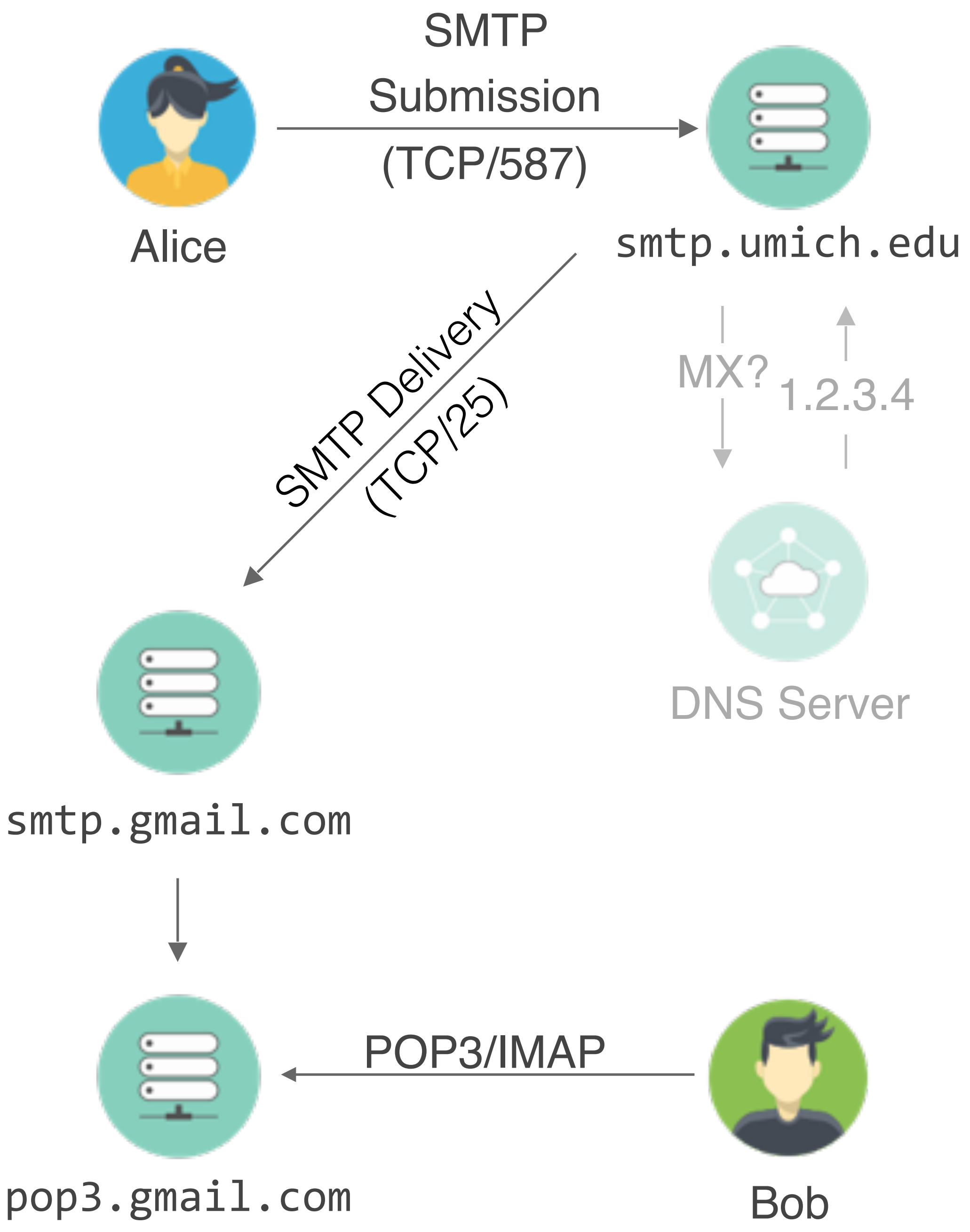
E-mail Security in Practice



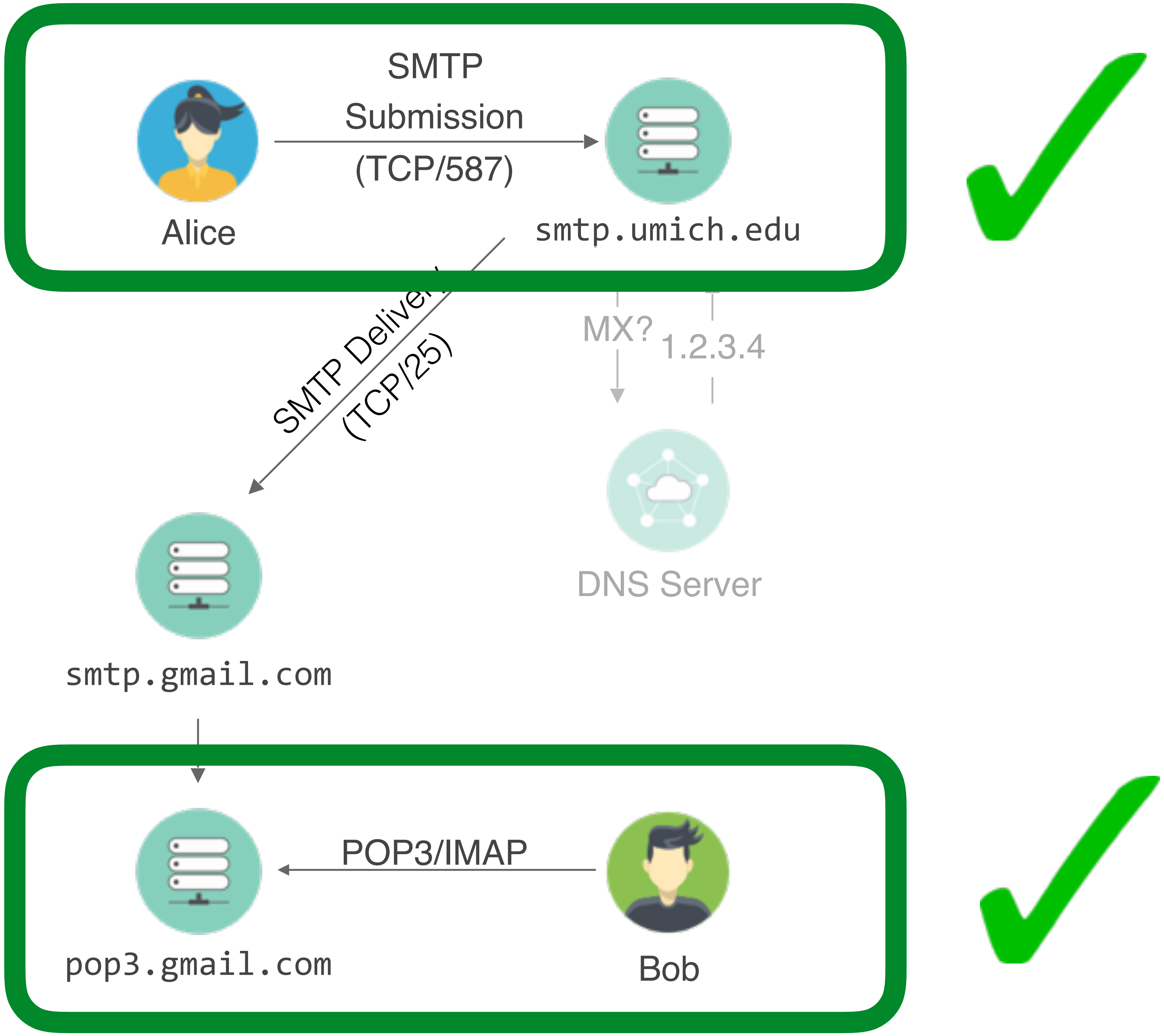
E-mail Security in Practice



E-mail Security in Practice



E-mail Security in Practice



SMTP Submission (TCP/587)

Alice

smtp.umich.edu

SMTP Delivery (TCP/25)

MX?

1.2.3.4

DNS Server

smtp.gmail.com

POP3/IMAP

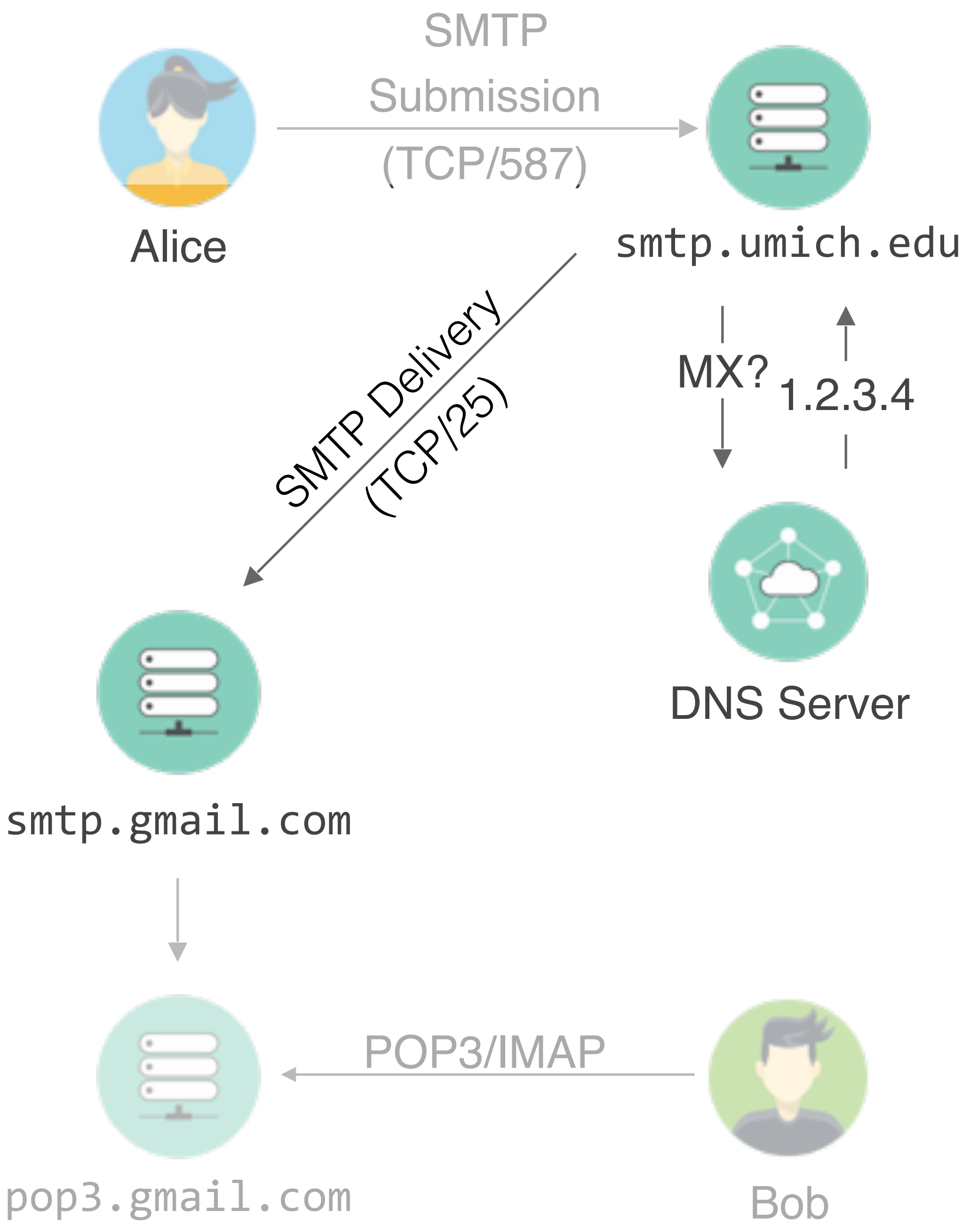
pop3.gmail.com

Bob

✓

✓

E-mail Security in Practice



Email Delivery (SMTP) has no built-in security

We've added SMTP extensions to:

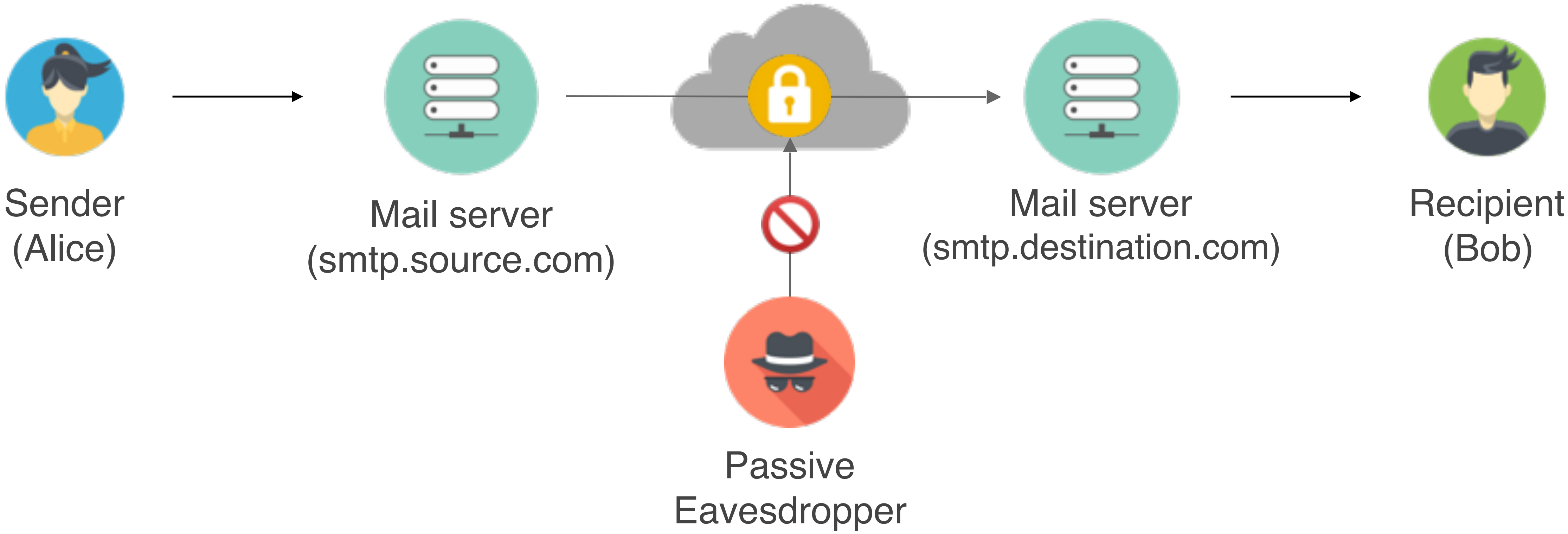
1. Encrypt email in transit
2. Authenticate email on receipt

Deployment is voluntary and invisible to end users

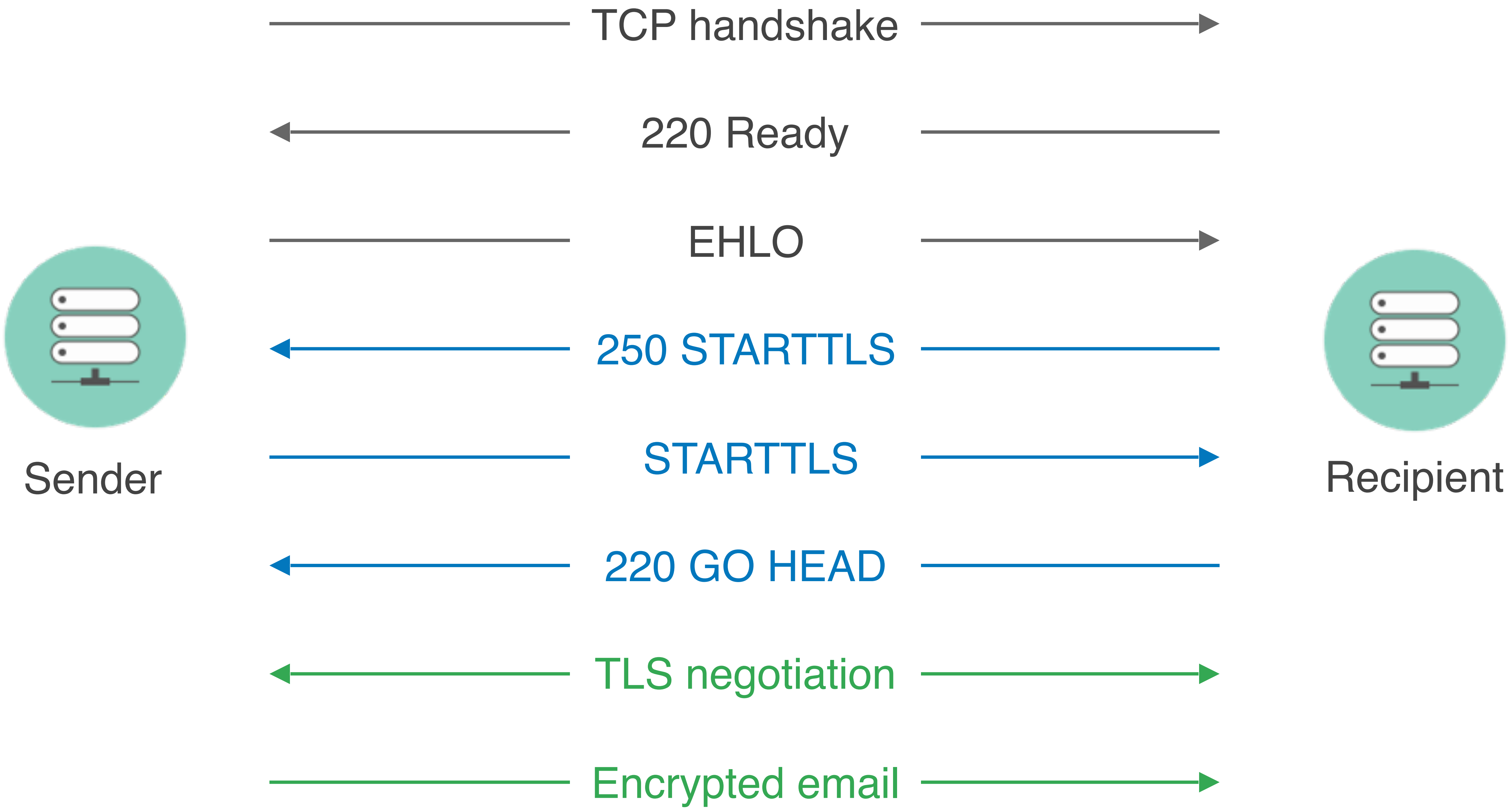
STARTTLS: TLS for SMTP

Allow TLS session to be started during an SMTP connection

Mail is transferred over the encrypted session



STARTTLS Protocol



Sender

Recipient

TCP handshake

220 Ready

EHLO

250 STARTTLS

STARTTLS

220 GO HEAD

TLS negotiation

Encrypted email

Opportunistic Encryption Only

Unlike HTTPS, STARTTLS is used opportunistically

Senders do not validate destination servers — the alternative is cleartext

Many servers do not support STARTTLS

“A publicly-referenced SMTP server MUST NOT require use of the STARTTLS extension in order to deliver mail locally. This rule prevents the STARTTLS extension from damaging the interoperability of the Internet's SMTP infrastructure.” (RFC3207)

What name to validate?

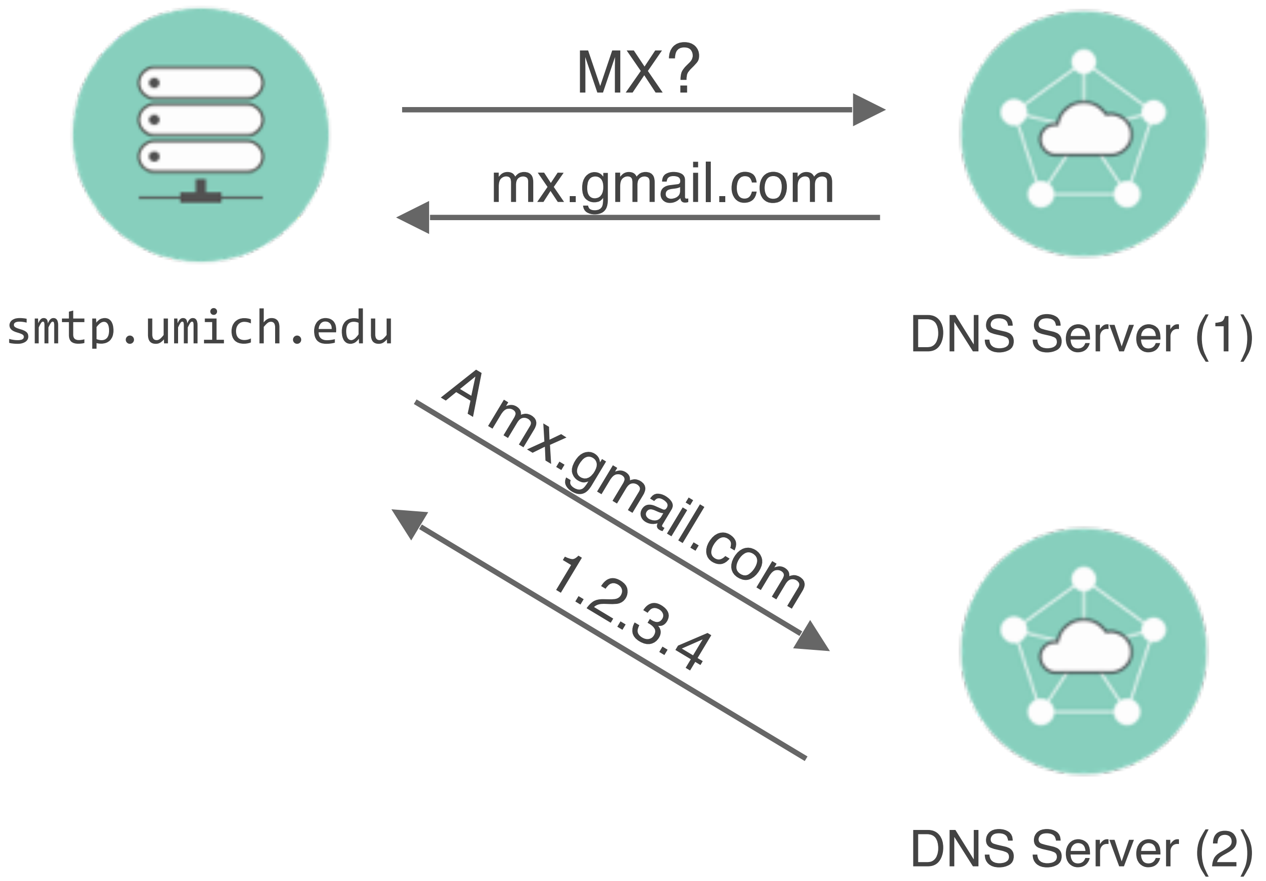
Unlike HTTPS, unclear what name should go on the certificate

MX Server (e.g., smtp.gmail.com)

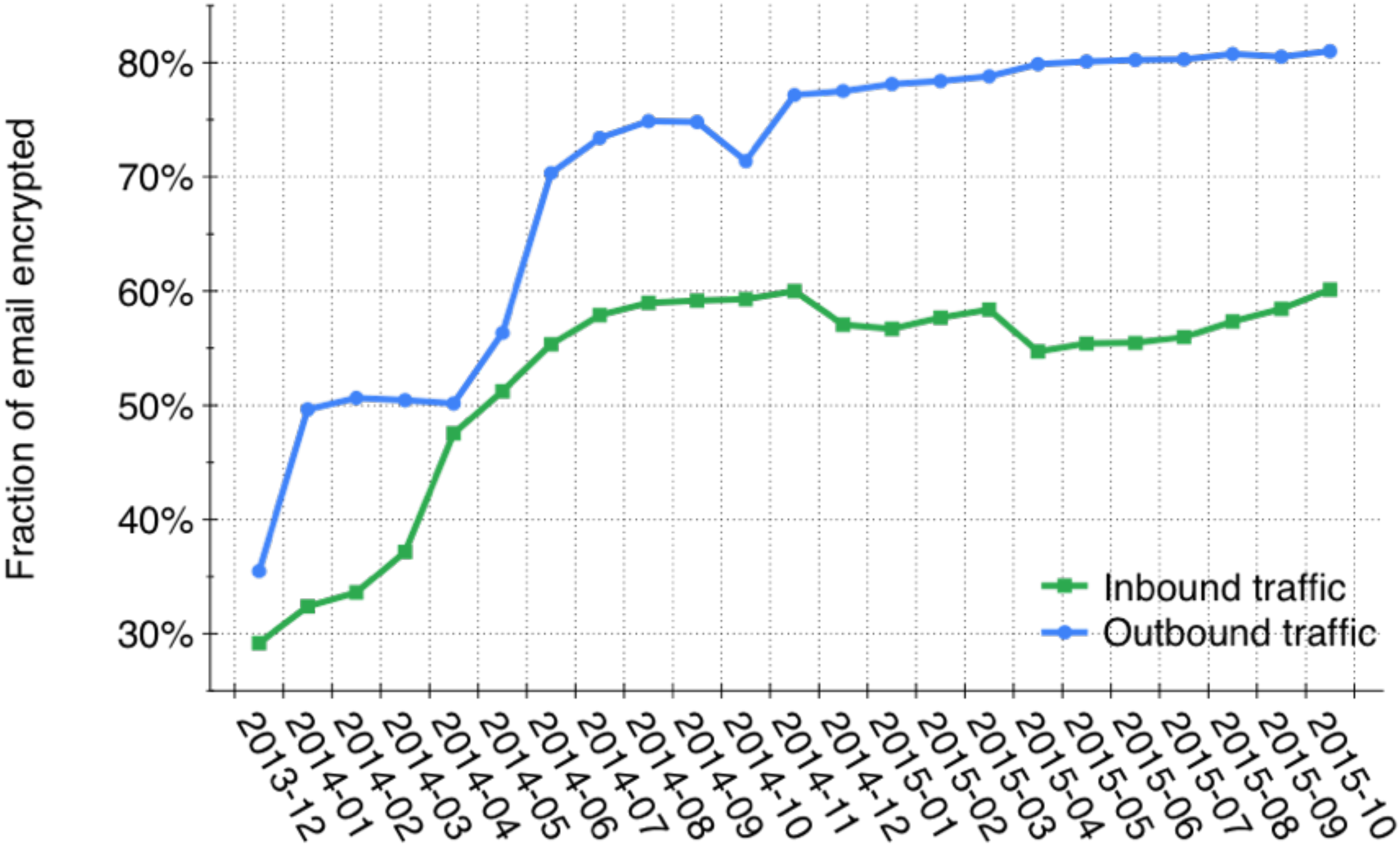
- No real security added
- MITM returns bad MX record

Domain (e.g., gmail.com)

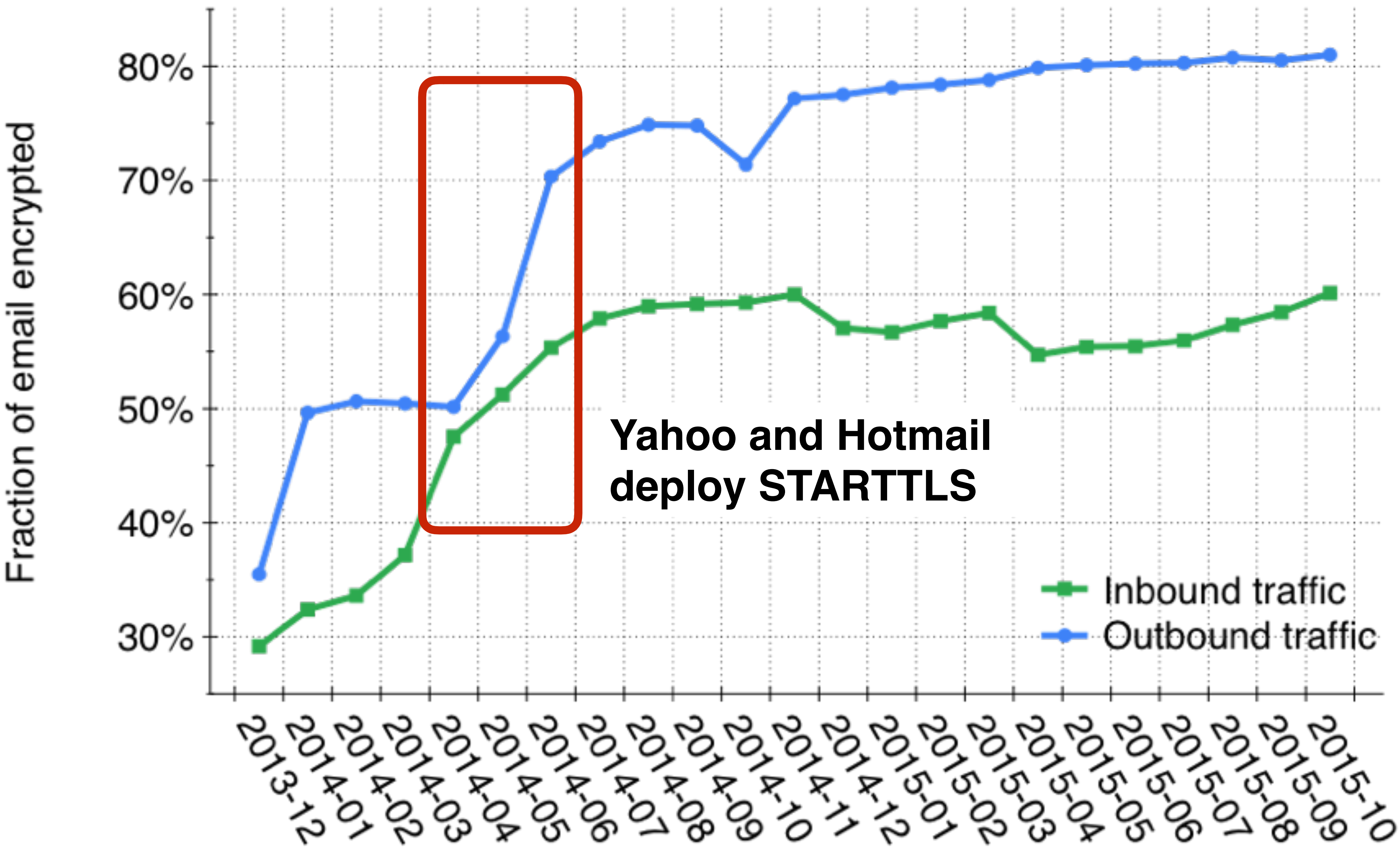
- No clear solution for large cloud providers



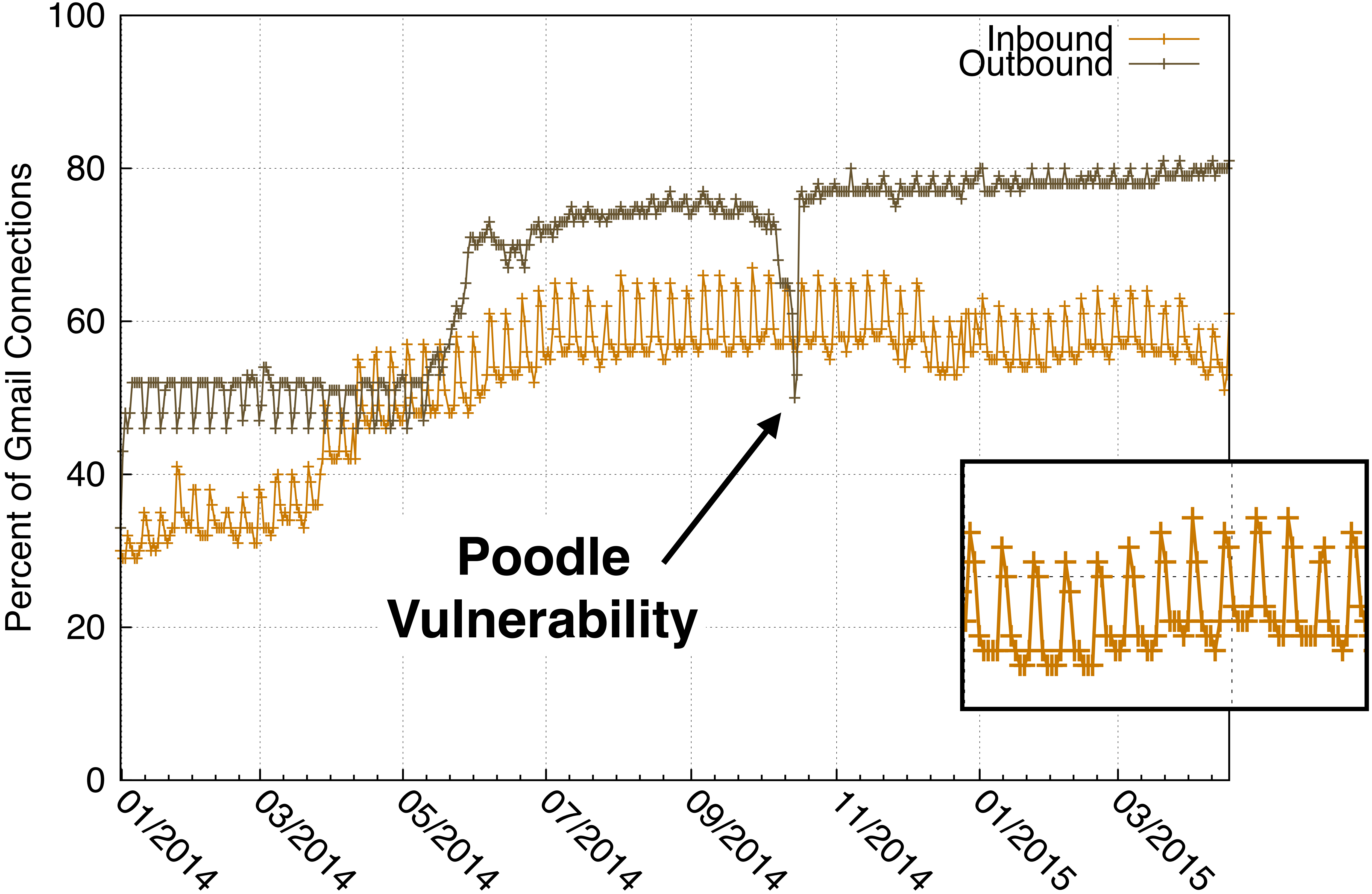
STARTTLS Usage as seen by Gmail



STARTTLS Usage as seen by Gmail



Yahoo and Hotmail deploy STARTTLS


Percent of Gmail Connections
100
80
60
40
20
0
Inbound
Outbound
01/2014
03/2014
05/2014
07/2014
09/2014
11/2014
01/2015
03/2015
Poodle
Vulnerability

Long Tail of Mail Operators

These numbers are dominated by a few large providers.

Of the Alexa Top 1M with Mail Servers:

- 81.8% support STARTTLS
- 34% have certificates that match MX server
- 0.6% have certificates that match domain (which would allow true authentication)

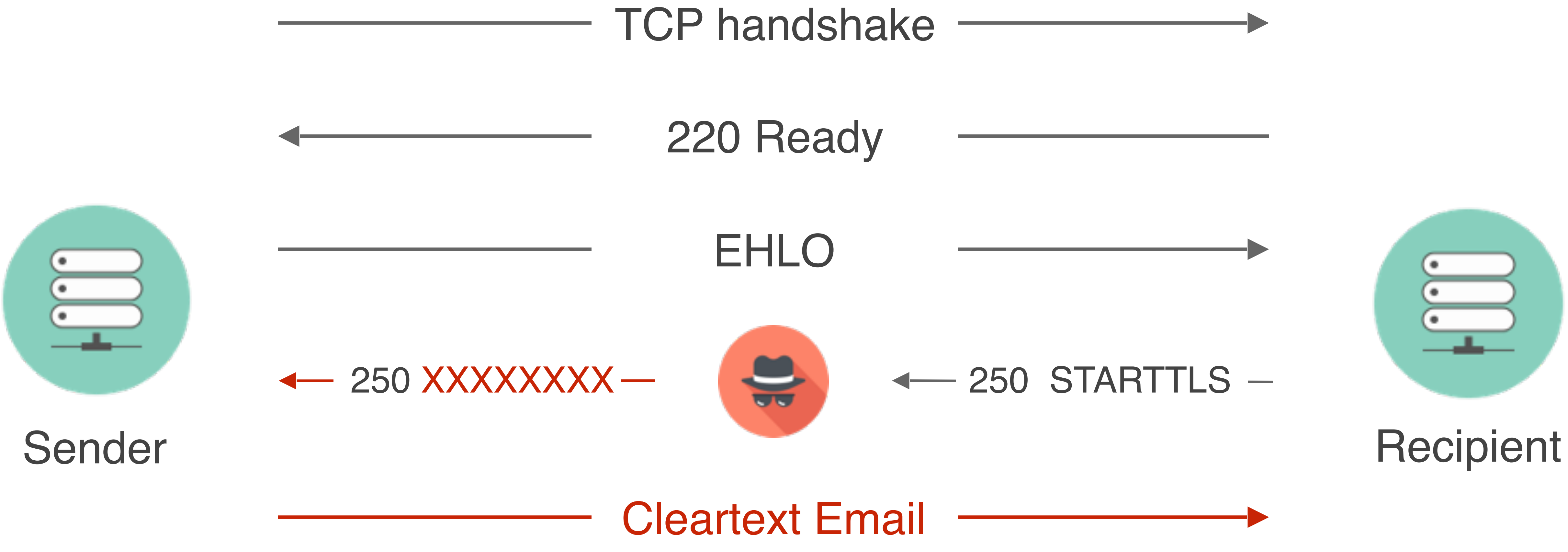
Not currently feasible to require STARTTLS

Common Implementations on Ubuntu

Software	Top Million Market	Public IPv4 Market Share	Default Incoming	Default Outgoing
Exim	34%	24%	✗	✓
Postfix	18%	21%	✓	✗
qmail	6%	1%	✗	✗
Sendmail	5%	4%	✗	✓
MS Exchange	4%	12%	✓	✓
Other/Unknown	33%	38%	?	?

What’s the simplest way to eavesdrop on servers that use STARTTLS?

Attack 1: STARTTLS Stripping



TCP handshake

220 Ready

EHLO

250 XXXXXXXX

250 STARTTLS

Sender

Recipient

Cleartext Email

STARTTLS Stripping in the Wild

Country	
Tunisia	96.1%
Iraq	25.6%
Papua New Guinea	25.0%
Nepal	24.3%
Kenya	24.1%
Uganda	23.3%
Lesotho	20.3%
Sierra Leone	13.4%
New Caledonia	10.1%
Zambia	10.0%

STARTTLS Stripping in the Wild

Country	
Tunisia	96.1%
Iraq	25.6%
Papua New Guinea	25.0%
Nepal	24.3%
Kenya	24.1%
Uganda	23.3%
Lesotho	20.3%
Sierra Leone	13.4%
New Caledonia	10.1%
Zambia	10.0%

Country	
Reunion	9.3%
Belize	7.7%
Uzbekistan	6.9%
Bosnia and Herzegovina	6.5%
Togo	5.5%
Barbados	5.3%
Swaziland	4.6%
Denmark	3.7%
Nigeria	3.6%
Serbia	3.1%

Not Necessarily Malicious

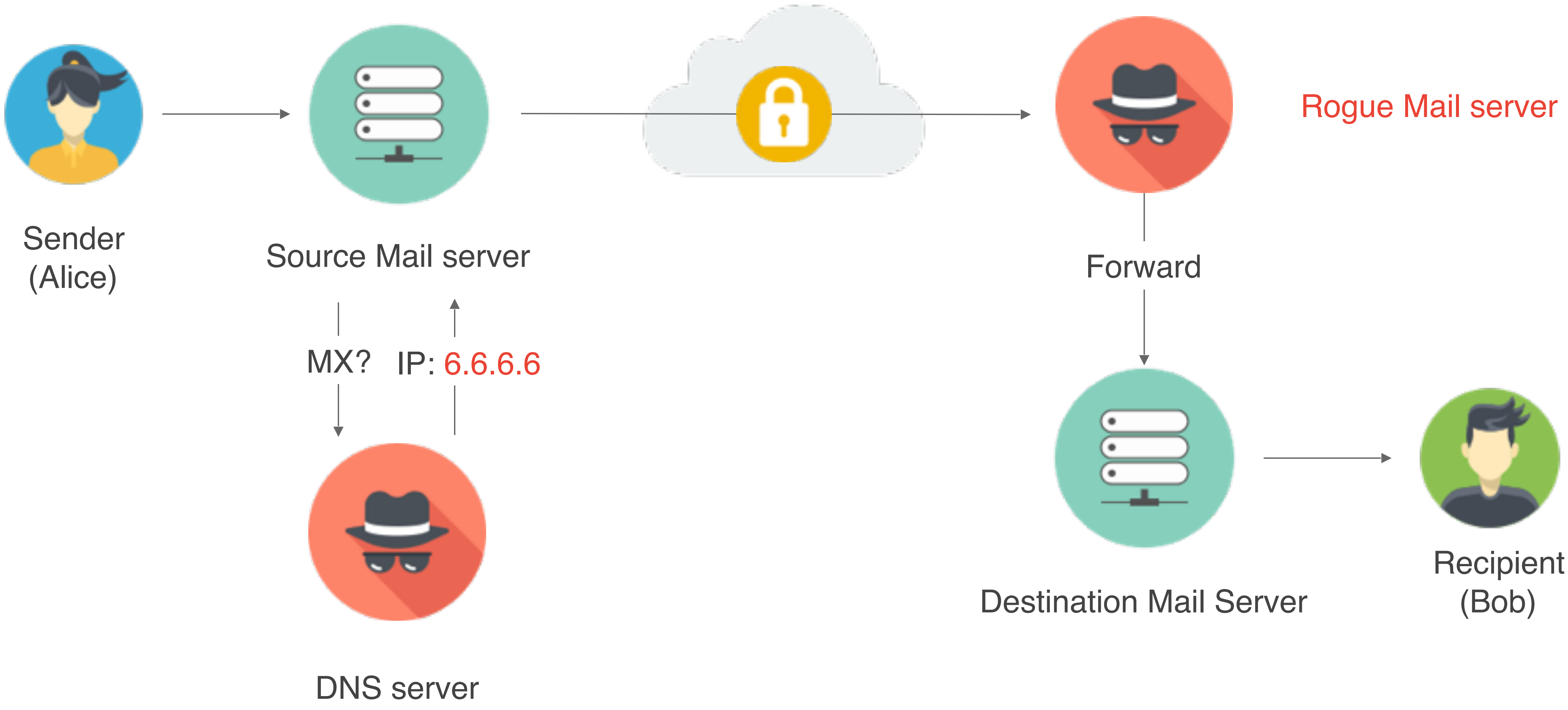
Organization Type	
Corporation	43%
ISP	18%
Financial Institution	14%
Academic Institution	8%
Healthcare Provider	3%
Unknown	3%
Airport	2%
Hosting Provider	2%
NGO	1%

Cisco advertises this feature to prevent attacks and catch spam

It’s unclear if operators know they’re inadvertently putting users at risk

Signal as to how vulnerable protocols currently are

Attack 2: Lying DNS Servers



Attack 2: Lying DNS Servers

Country	
Slovakia	0.08%
Romania	0.04%
Bulgaria	0.02%
India	0.01%
Israel	0.01%
Poland	0.01%
Switzerland	0.01%
Ukraine	0.01%
Others	10.1%

Authenticating Email

Authenticating Email

- **DomainKeys Identified Mail (DKIM)**

  Sender signs messages with cryptographic key

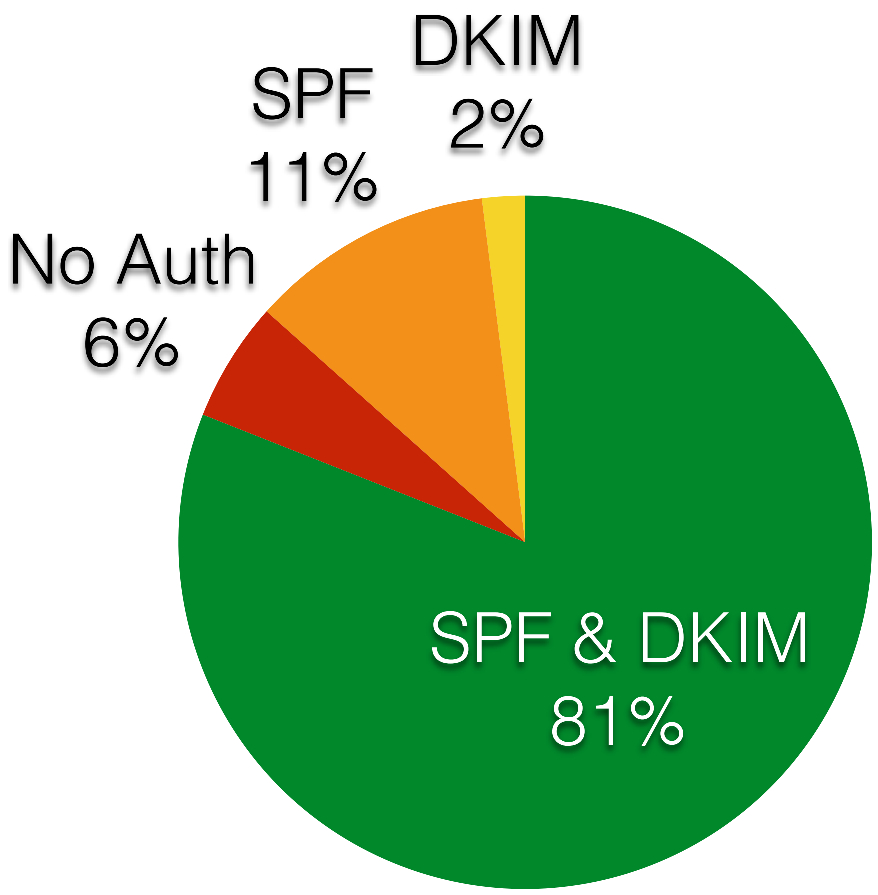
- **Sender Policy Framework (SPF)**

  Sender publishes list of IPs authorized to send mail

- **Domain Message Authentication, Reporting and Conformance (DMARC)**

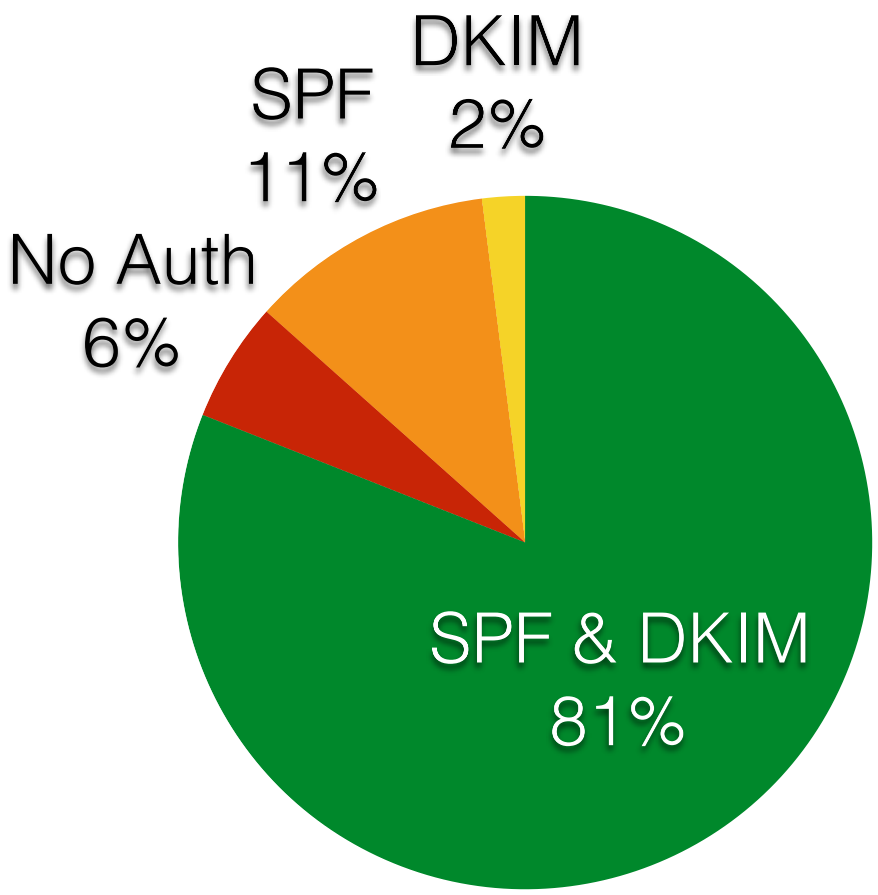
  Sender publishes policy in DNS that specifies what to do if DKIM or SPF validation fails

E-mail Authentication in Practice



Gmail Authentication

E-mail Authentication in Practice



Gmail Authentication

Technology	Top 1M
SFP Enabled	47%
DMARC Policy	1%

DMARC Policy	Top 1M
Reject	20%
Quarantine	8%
Empty	72%

Top Million Domains

Moving Forward

Two IETF proposals to solve real world issues:

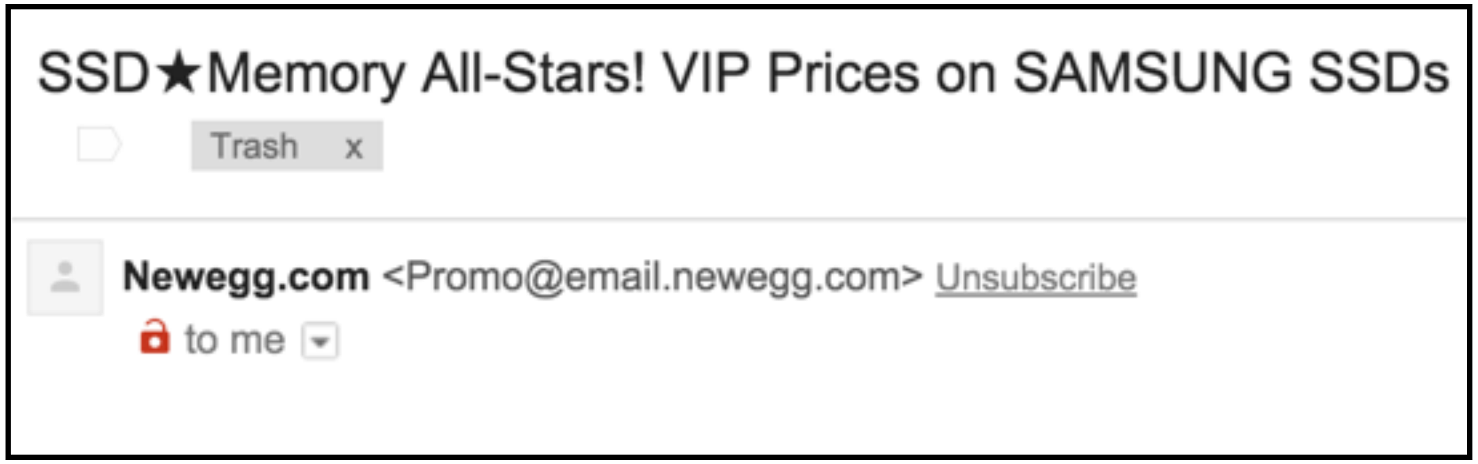
SMTP Strict Transport Security

Similar to HTTPS HSTS (key pinning)

Authenticated Received Chain (ARC)

DKIM replacement that handles mailing lists

Gmail STARTTLS Indication

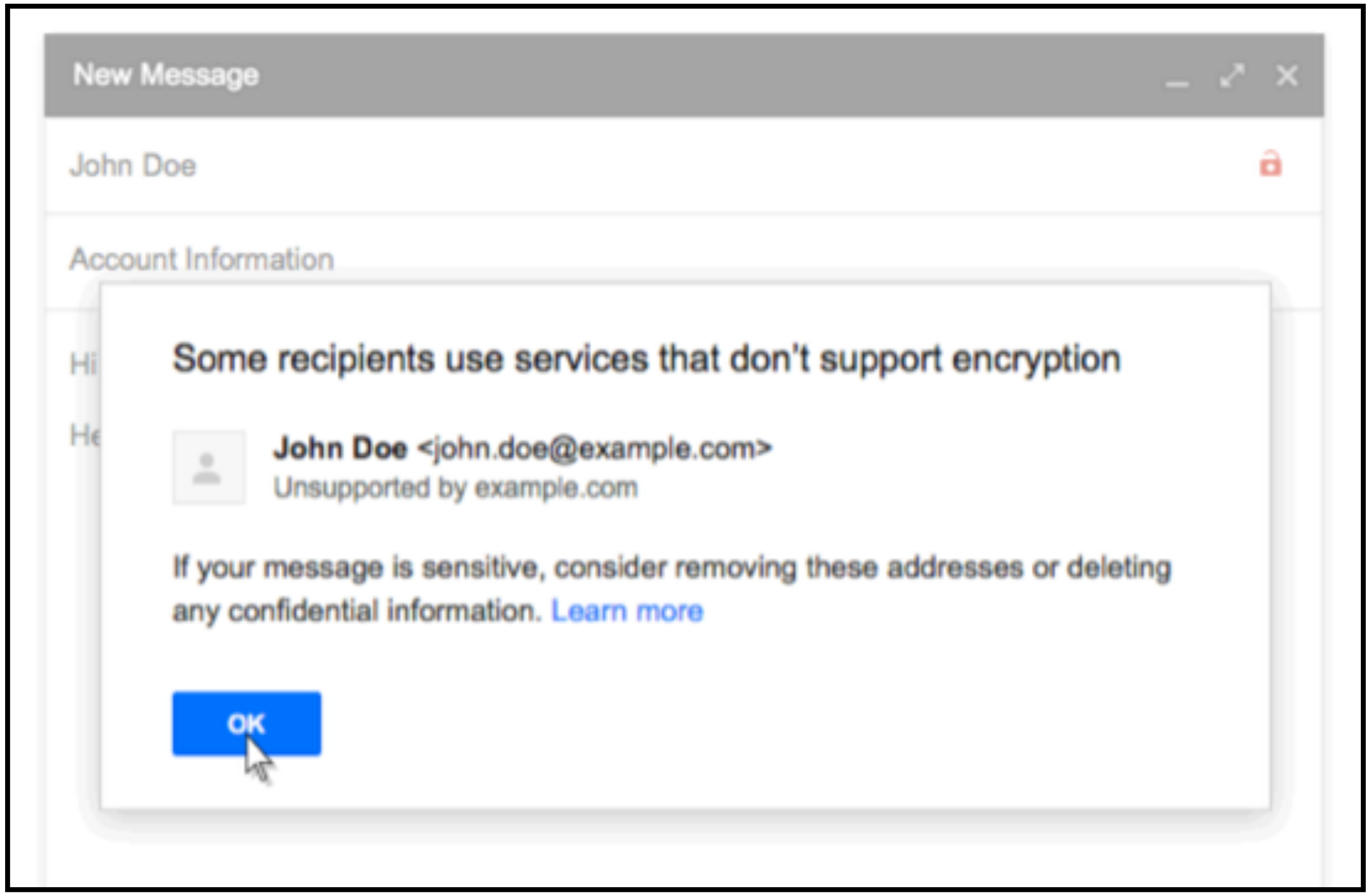


SSD★Memory All-Stars! VIP Prices on SAMSUNG SSDs

Newegg.com <Promo@email.newegg.com> Unsubscribe

🔓 to me

Insecure Received



John Doe

Account Information

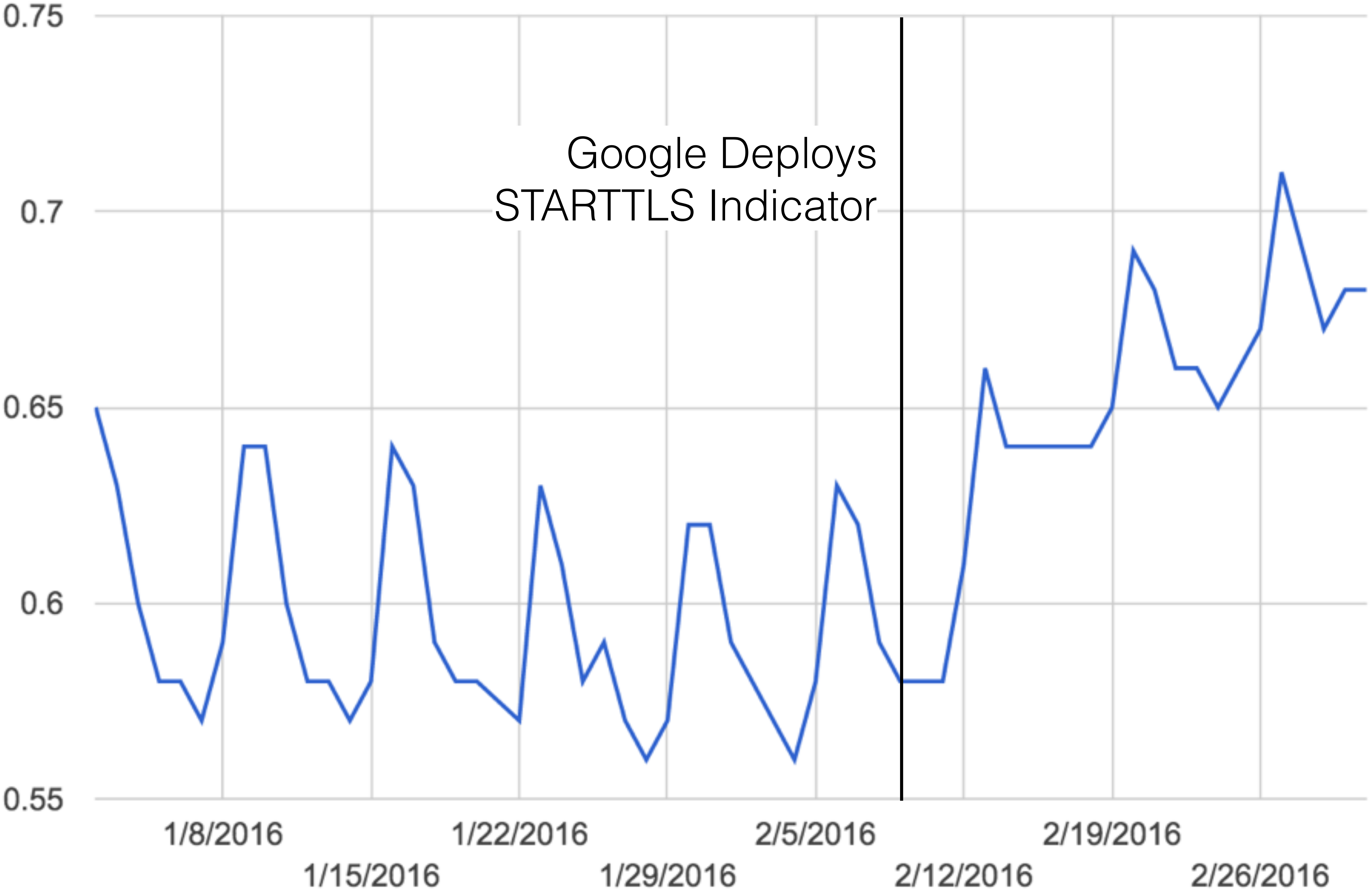
Some recipients use services that don't support encryption

John Doe <john.doe@example.com>
Unsupported by example.com

If your message is sensitive, consider removing these addresses or deleting any confidential information. Learn more

Insecure Sending

Inbound Gmail Protected by STARTTLS



Google Deploys
STARTTLS Indicator

Current State of Affairs

Providers are continuing to roll out transport security and authentication protocols, but many organizations lag in deployment

STARTTLS currently provides no protection against active adversaries

Several proposals in discussion for bridging these gaps

Mail is used to communicate sensitive data and despite being hidden from view, its security is equally important

Neither Snow Nor Rain Nor MITM…
An Empirical Analysis of Email Delivery Security

Zakir Durumeric
University of Michigan
zakir@umich.edu