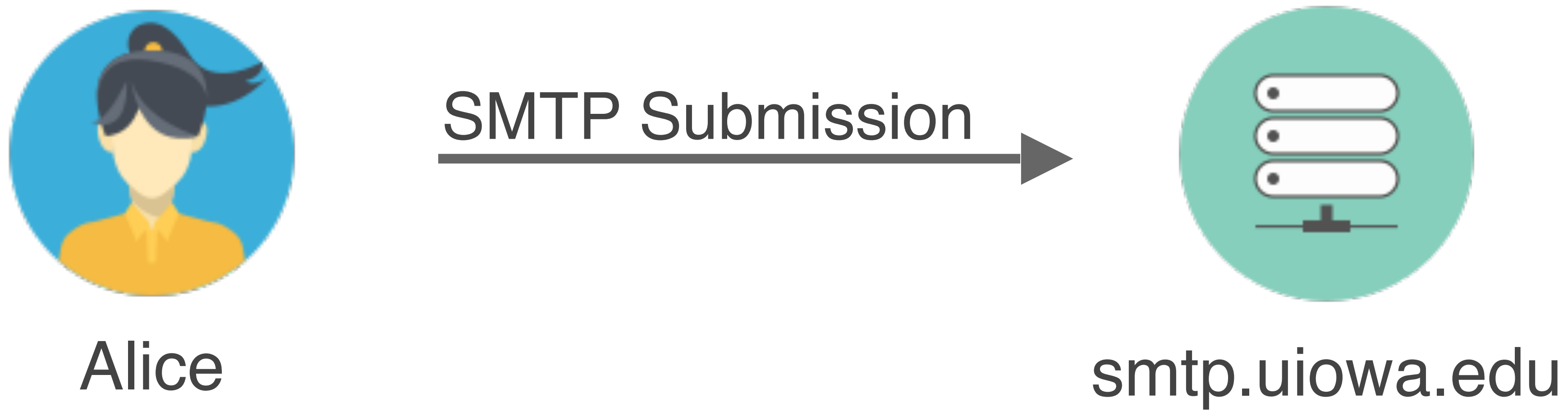
Secure (and Insecure) Messaging

CS249i: The Modern Internet

Before we talk about secure messaging…
let's talk about insecure messaging

Email Delivery

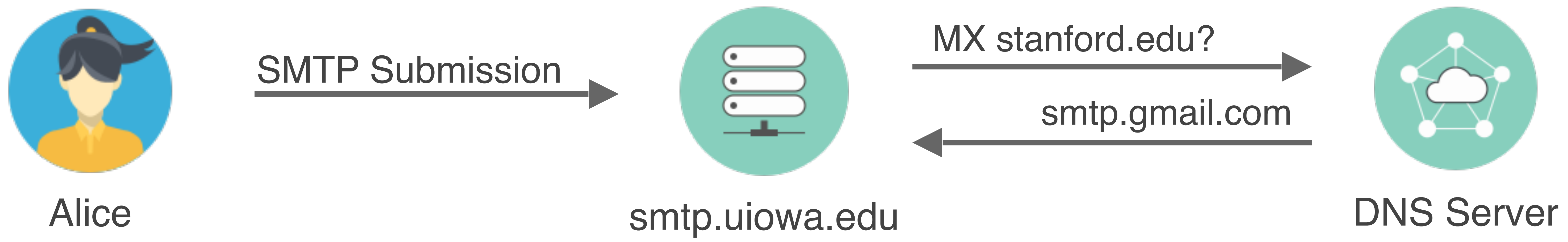


Alice

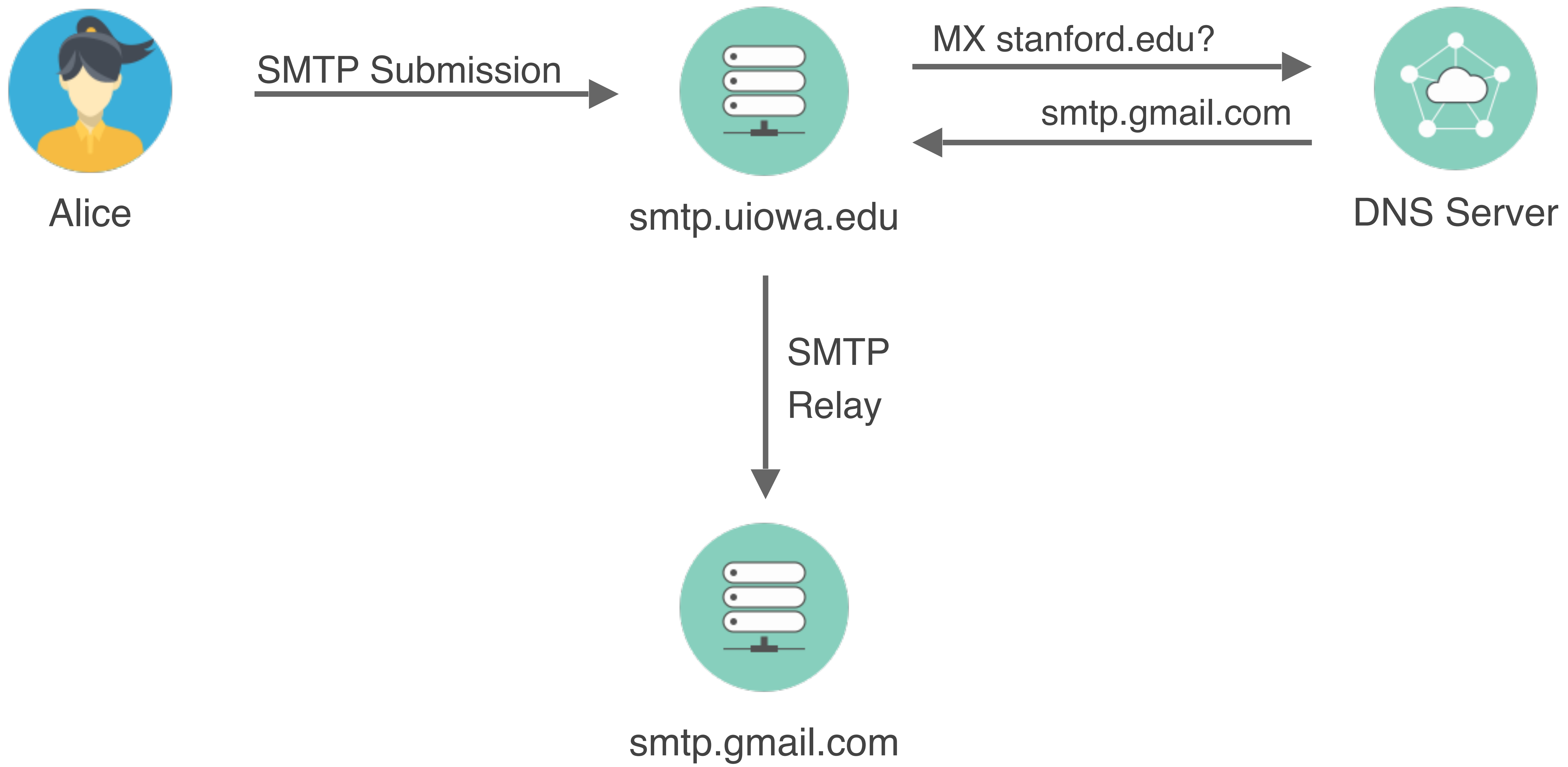
SMTP Submission

smtp.uiowa.edu

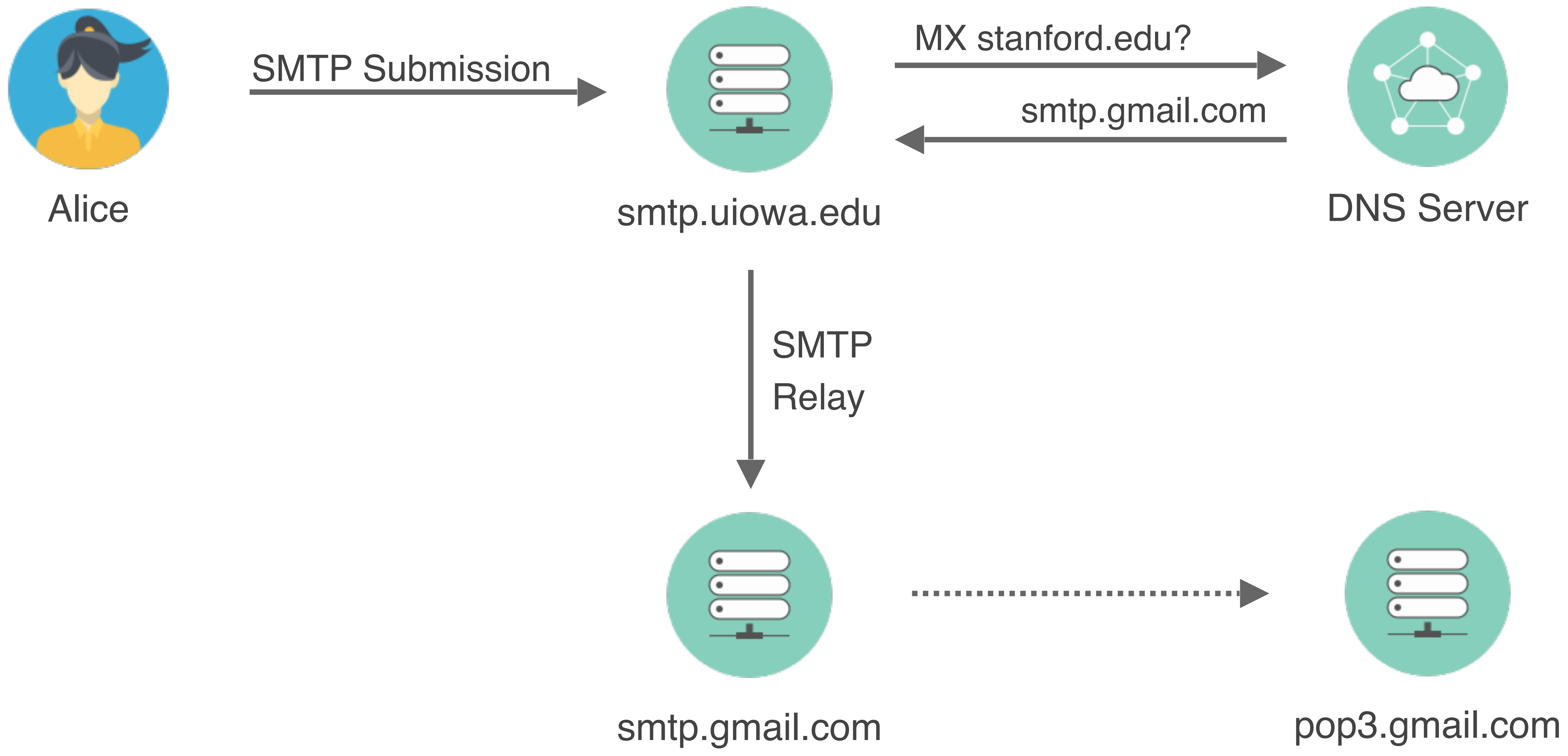
Email Delivery



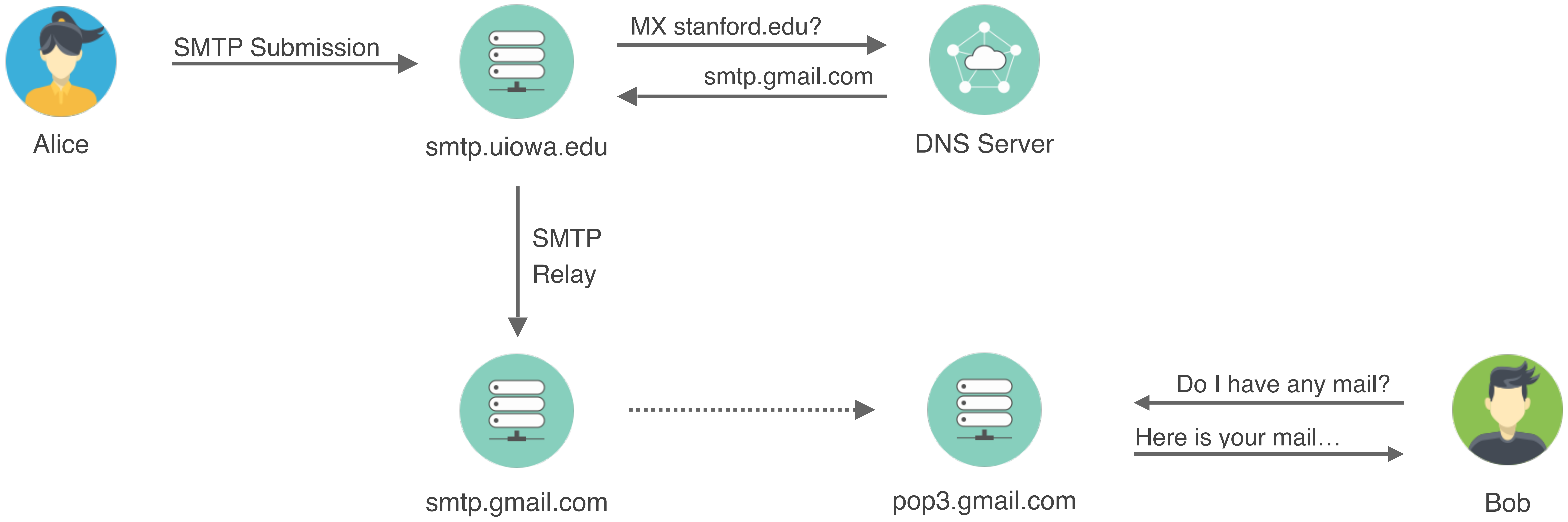
Email Delivery



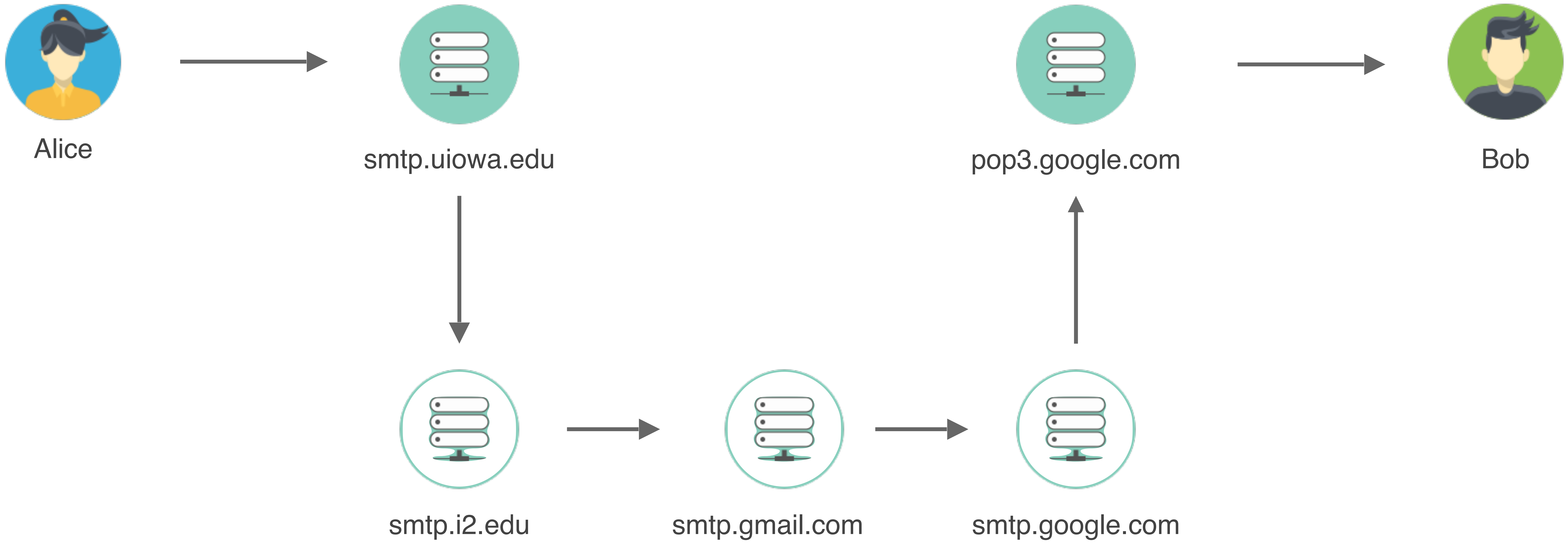
Email Delivery



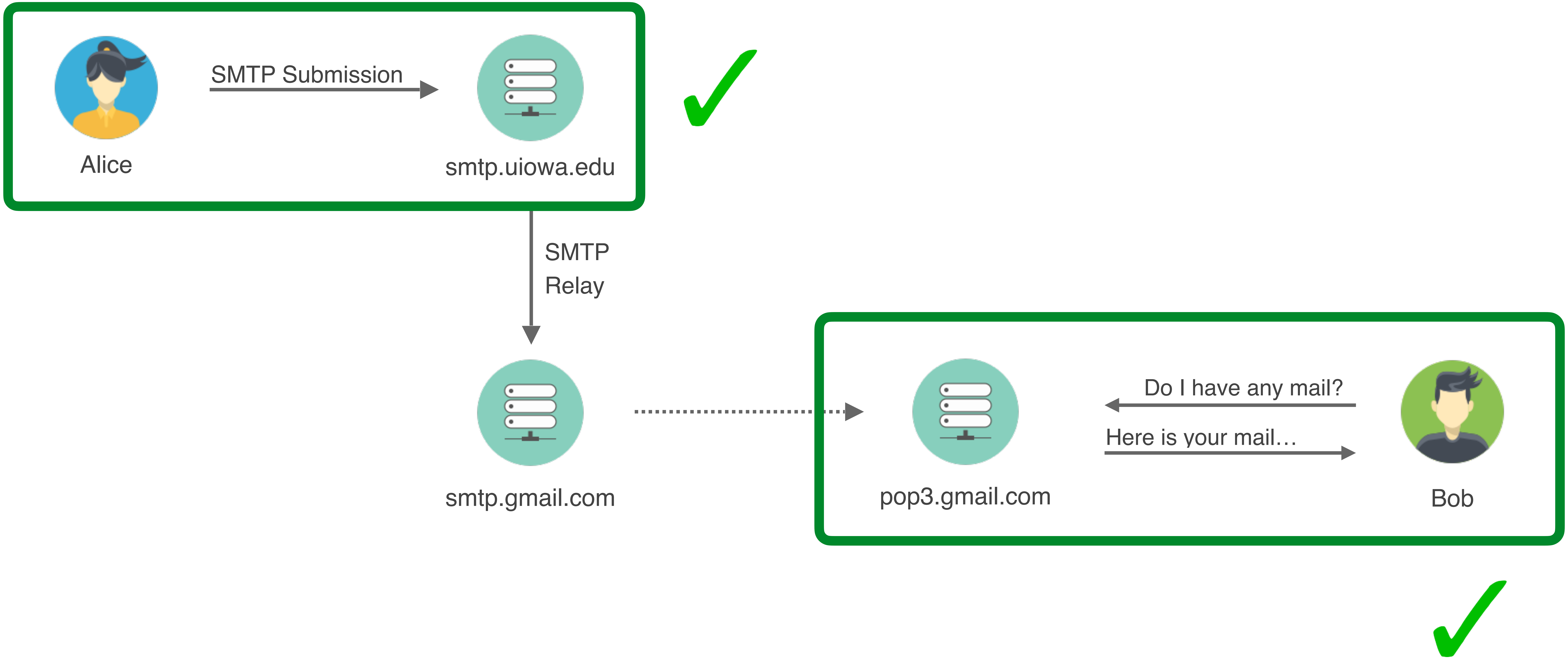
Email Delivery



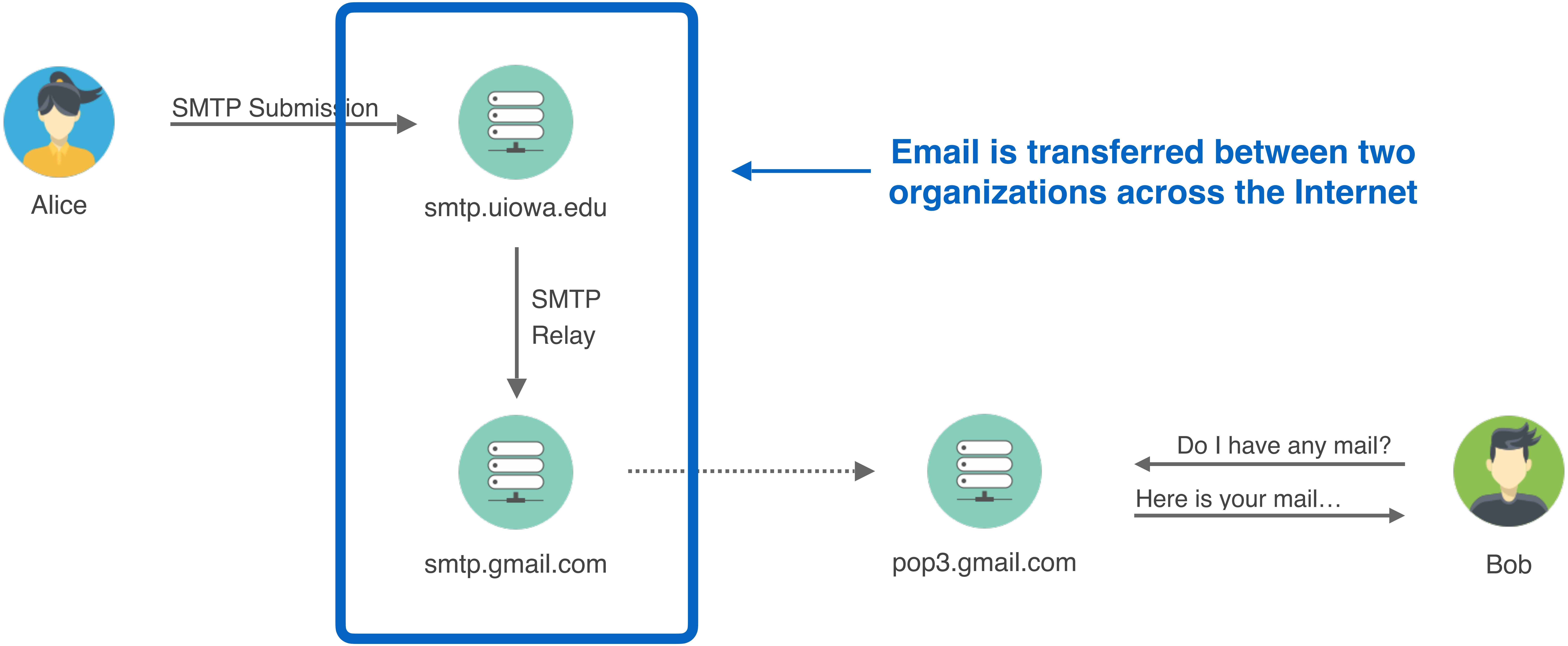
Email Delivery



Email Delivery Security



Email Delivery Security



Email is transferred between two organizations across the Internet

SMTP

SMTP — Simple Mail Transfer Protocol — is the protocol used for transferring email between servers on the Internet

The protocol was first introduced in 1982. A number of additional extensions were later added in 2008

As originally conceived, the protocol had no security features

SMTP Security

Confidentiality. No protection against eavesdropping for mail sent across the Internet. Anyone on path could read your message.

Integrity. Nothing prevented an *active* attacker from modifying your messages in transit, or spoofing emails as you.

Availability. Little guarantee of uptime or availability of email data (i.e., email delivery).

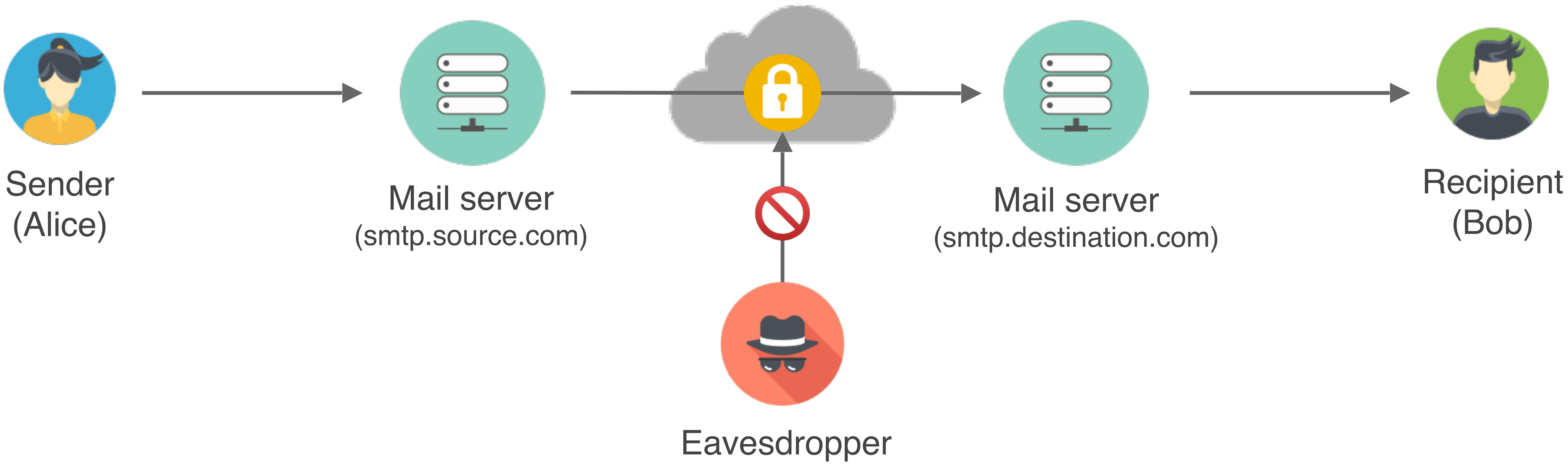
SMTP Extensions

Several extensions to SMTP were later introduced to provide email security, including STARTTLS, SPF, DKIM, and DMARC

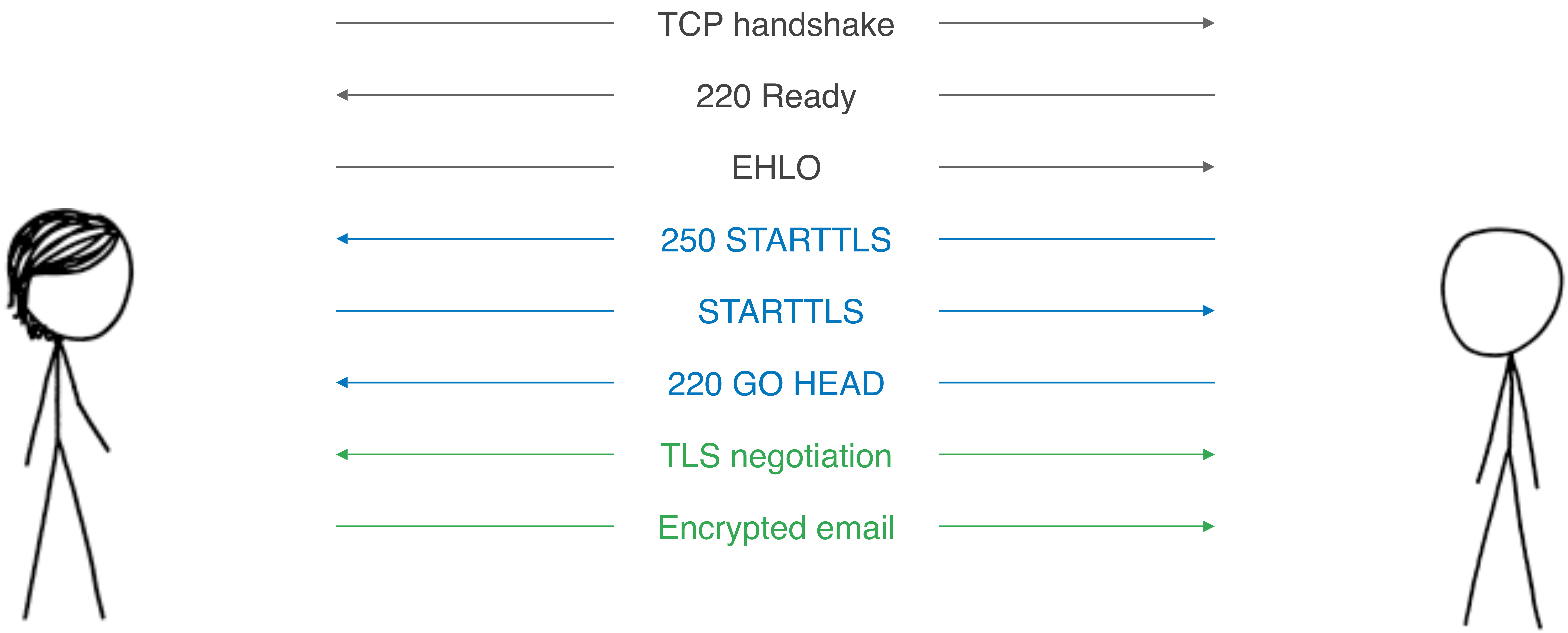
Their deployment has been largely hidden from sight

STARTTLS Extension

STARTTLS enables the sender to start an encrypted TLS session when delivering mail. Messages are transferred over the encrypted session.



STARTTLS Protocol



TCP handshake

220 Ready

EHLO

250 STARTTLS

STARTTLS

220 GO HEAD

TLS negotiation

Encrypted email

Opportunistic Encryption

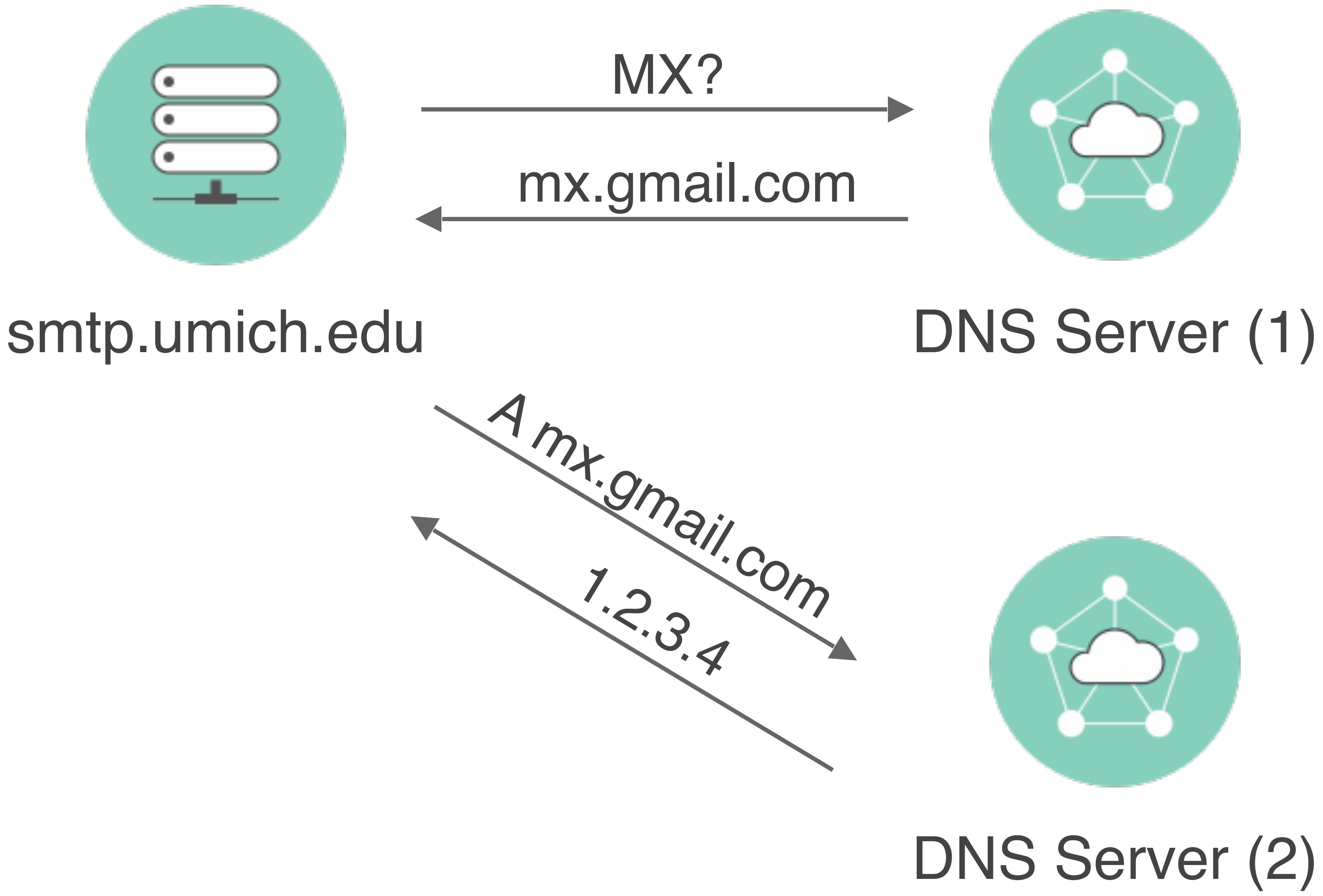
"A publicly-referenced SMTP server MUST NOT require use of the START TLS extension in order to deliver mail locally. This rule prevents the STARTTLS extension from damaging the interoperability of the Internet's SMTP infrastructure." (RFC3207)

Unlike HTTPS, STARTTLS is used *opportunistically*

Senders do not validate destination servers — the alternative is cleartext

Many servers do not support STARTTLS

What name do you 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 solution for cloud providers

Long Tail of Operators (2015)

These numbers are dominated by a small number of large providers

Of the Alexa Top 1M most popular domains:

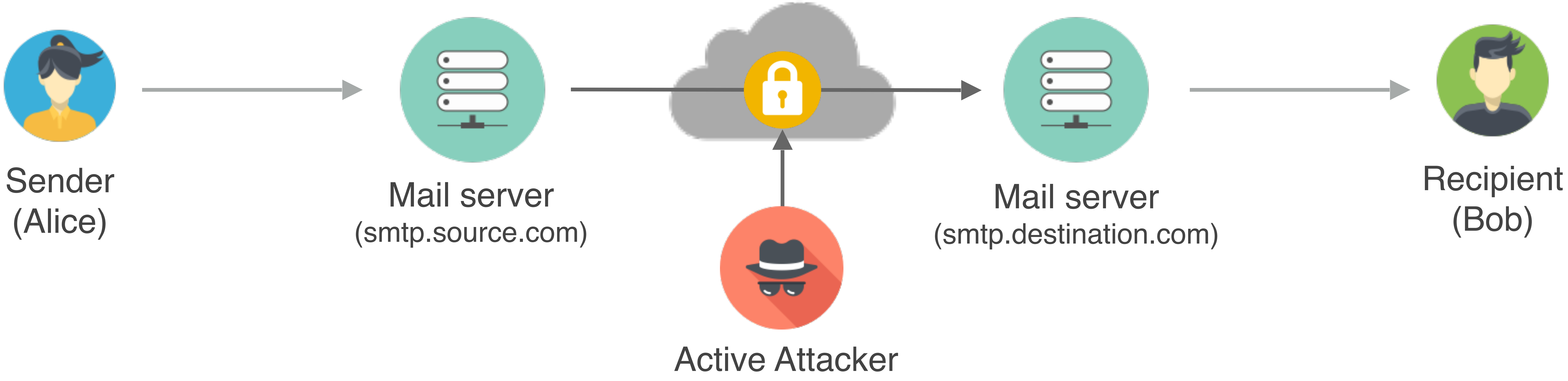
- 80% support STARTTLS
- 34% have certificates that match mail server
- 0.6% have certificates that match domain ✓

↖ This is the only case where you know you're sending mail to the right place.

Implications for Mail Providers

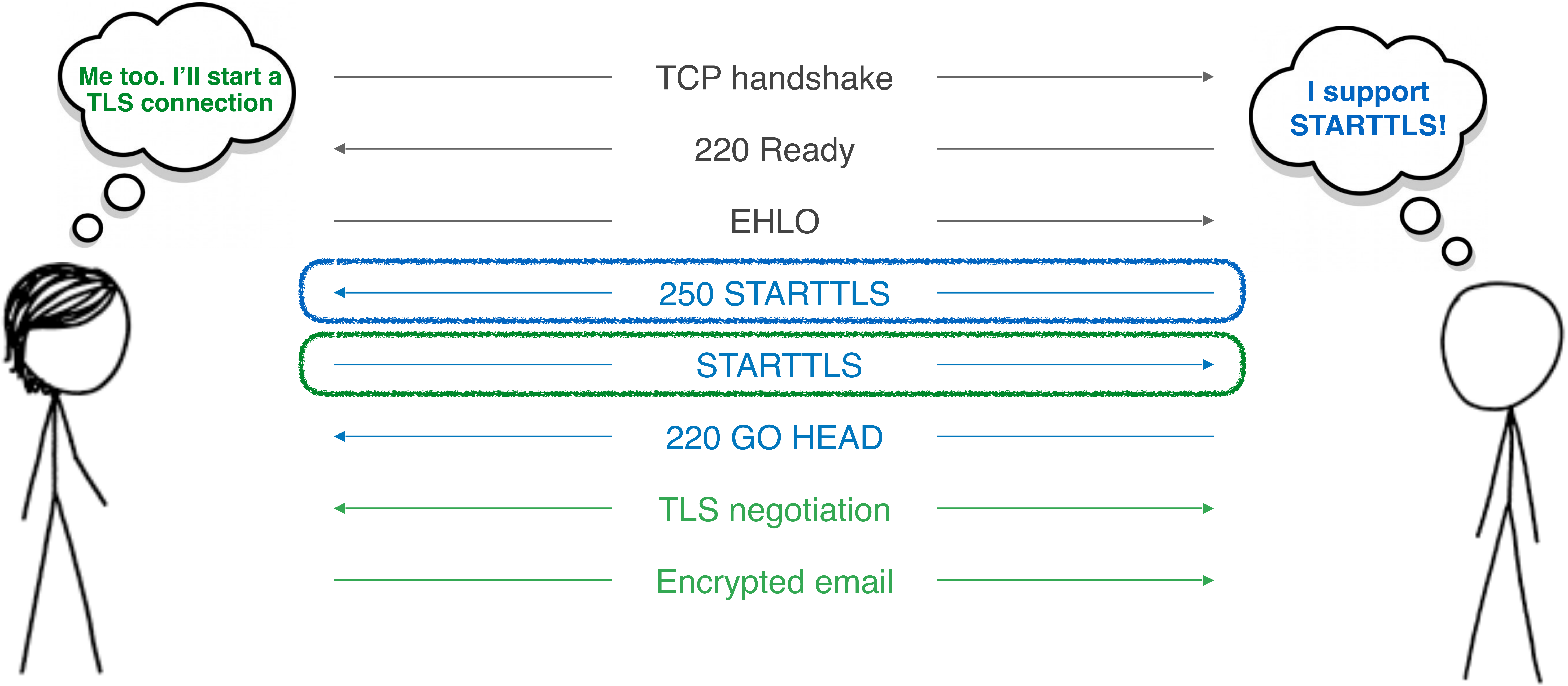
Because so many servers still do not support encryption, mail providers are forced to allow mail to be sent unencrypted

Doesn't that mean that an active attacker can eavesdrop if they can prevent a secure connection?



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

STARTTLS Protocol



TCP handshake

220 Ready

EHLO

250 STARTTLS

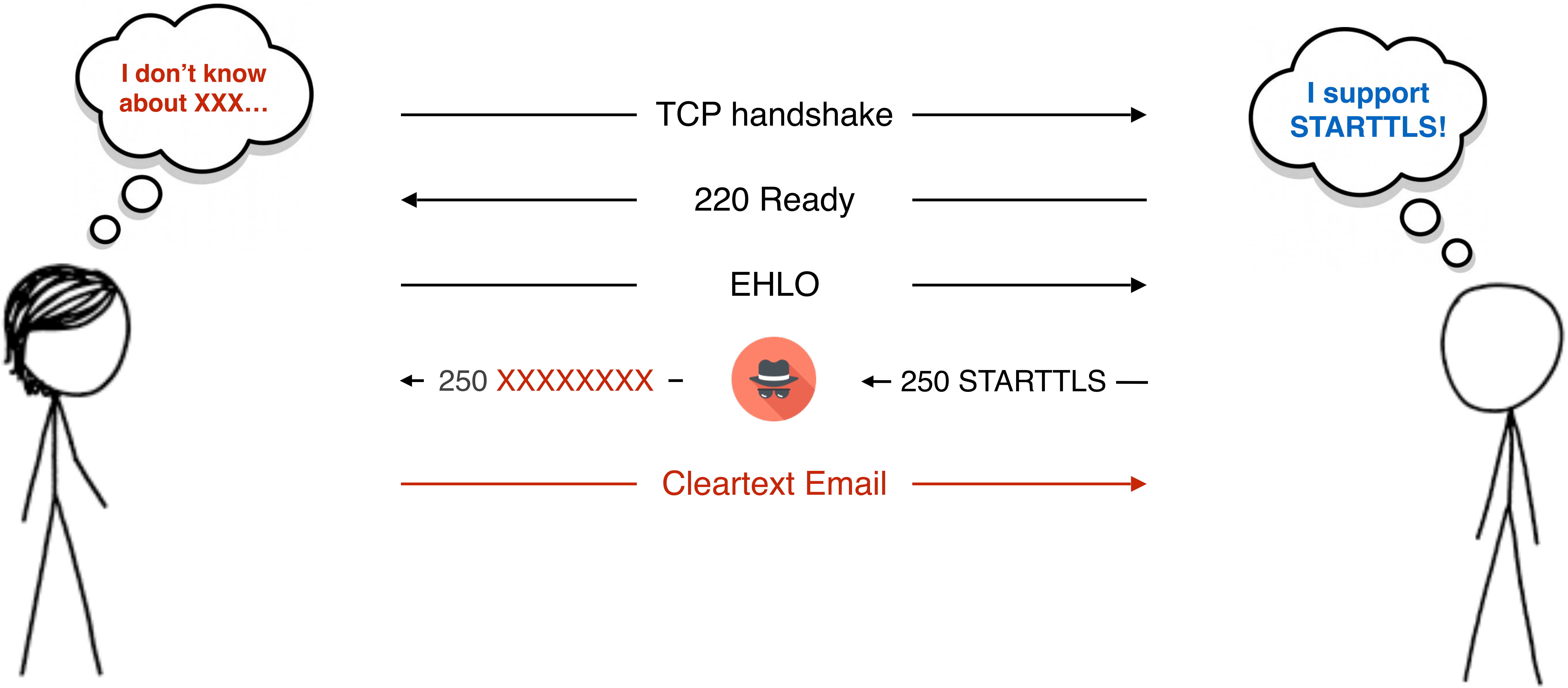
STARTTLS

220 GO HEAD

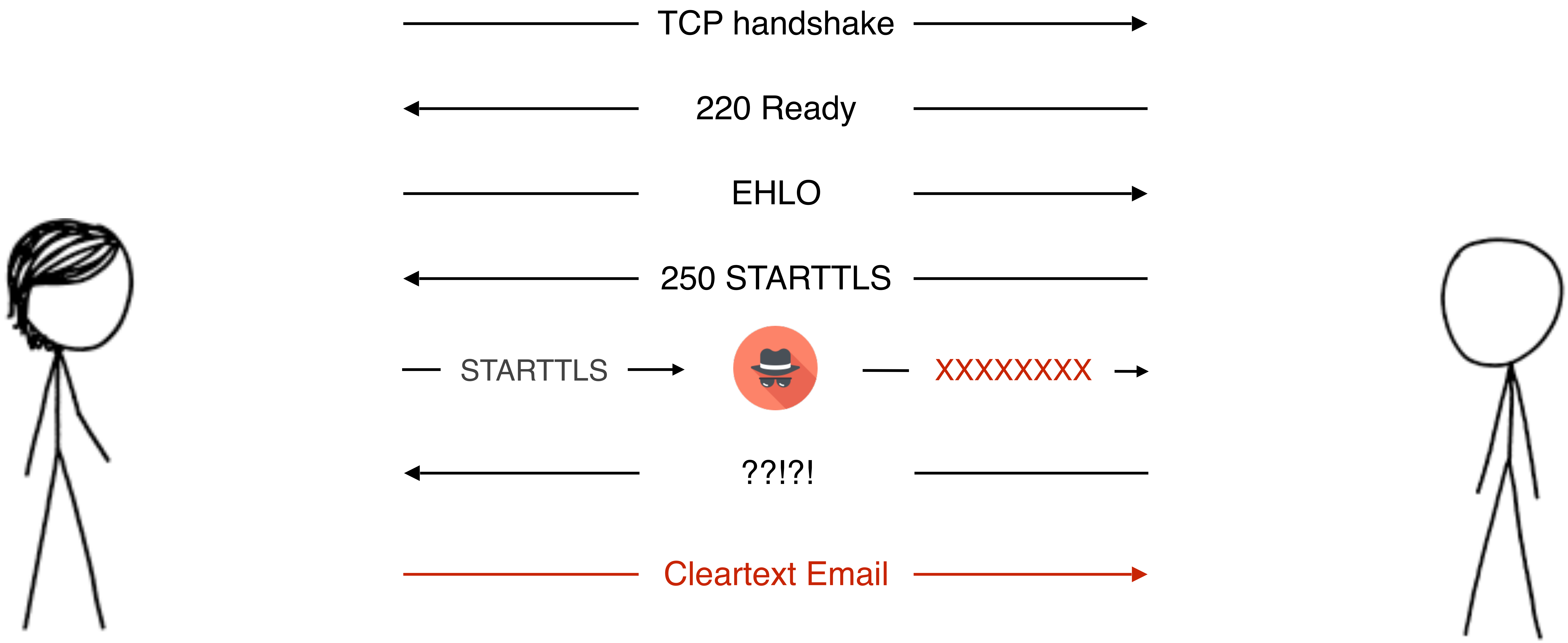
TLS negotiation

Encrypted email

STARTTLS Stripping (1)



STARTTLS Stripping (2)



TCP handshake

220 Ready

EHLO

250 STARTTLS

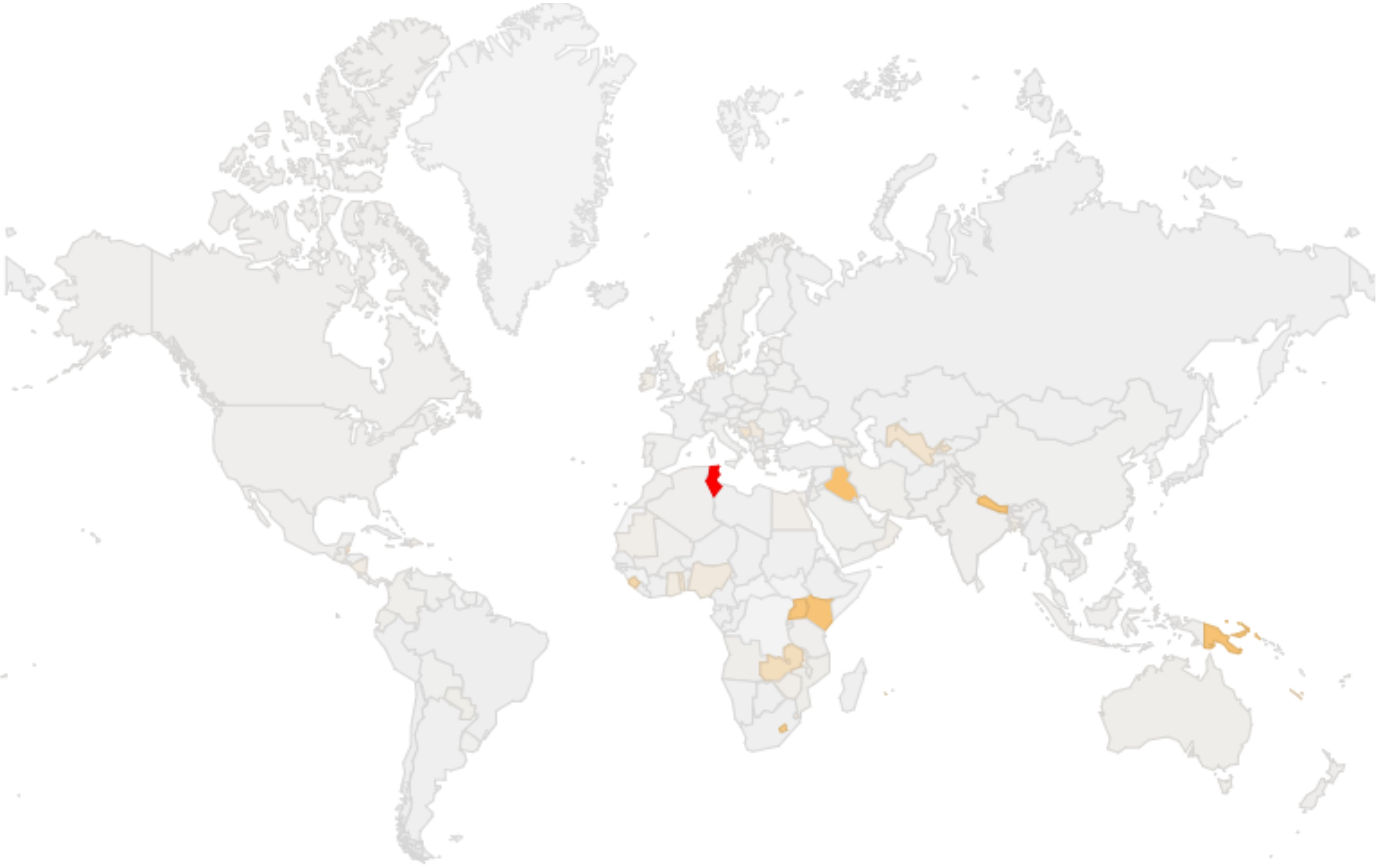
STARTTLS

XXXXXXXX

??!?!

Cleartext Email

Attacks 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%

Are these truly attacks?

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

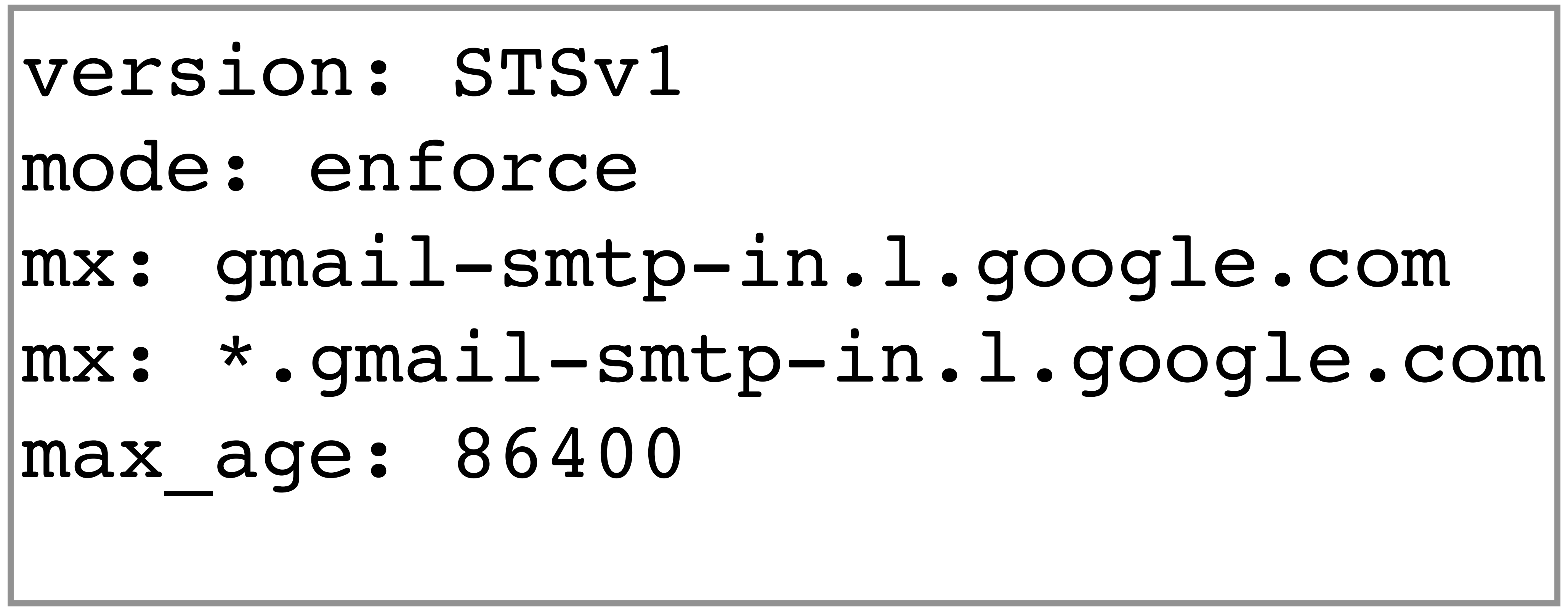
Cisco advertises this feature to prevent attacks and catch spam

Unclear if operators know they’re putting their users at risk

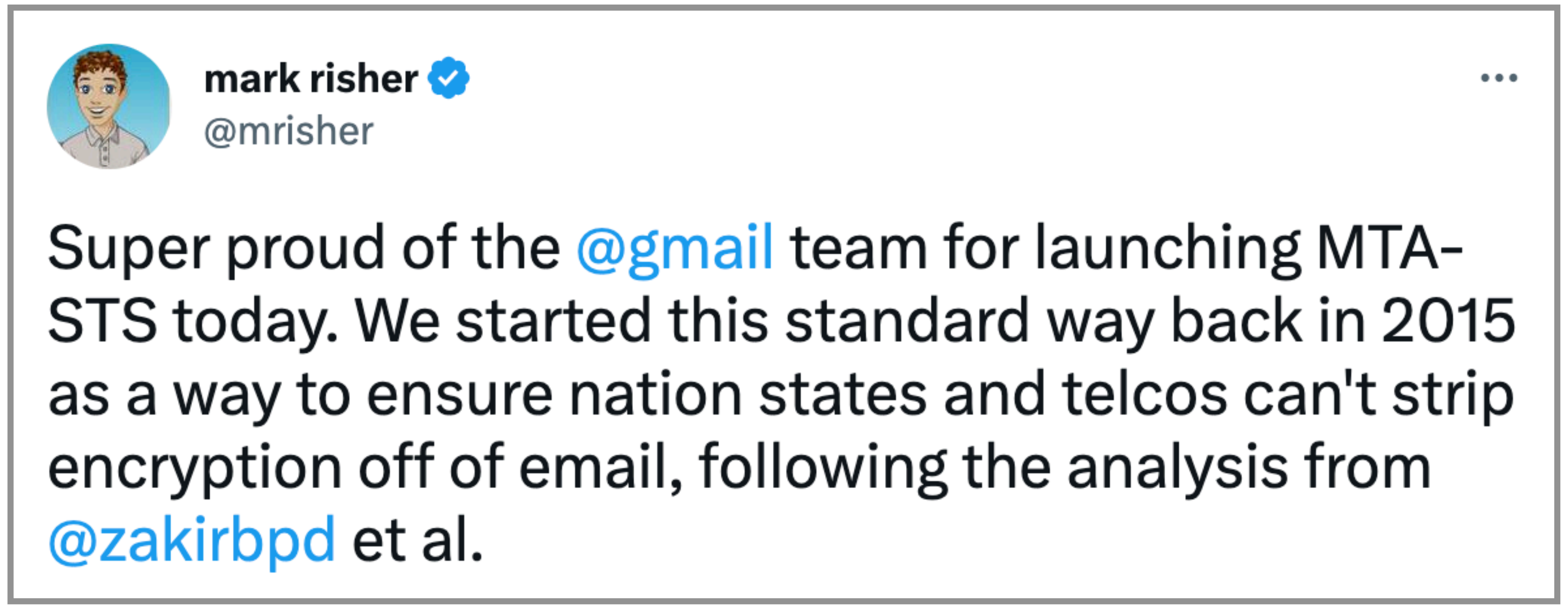
MTA-STS

SMTP MTA Strict Transport Security (MTA-STS) is a mechanism enabling mail service providers (SPs) to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate.

https://mta-sts.gmail.com/.well-known/mta-sts.txt



```
version: STSv1
mode: enforce
mx: gmail-smtp-in.l.google.com
mx: *.gmail-smtp-in.l.google.com
max_age: 86400
```



mark risher
@mrisher

Super proud of the @gmail team for launching MTA-STS today. We started this standard way back in 2015 as a way to ensure nation states and telcos can't strip encryption off of email, following the analysis from @zakirbpd et al.

How much of email is protected in practice?

STARTTLS as seen by Gmail

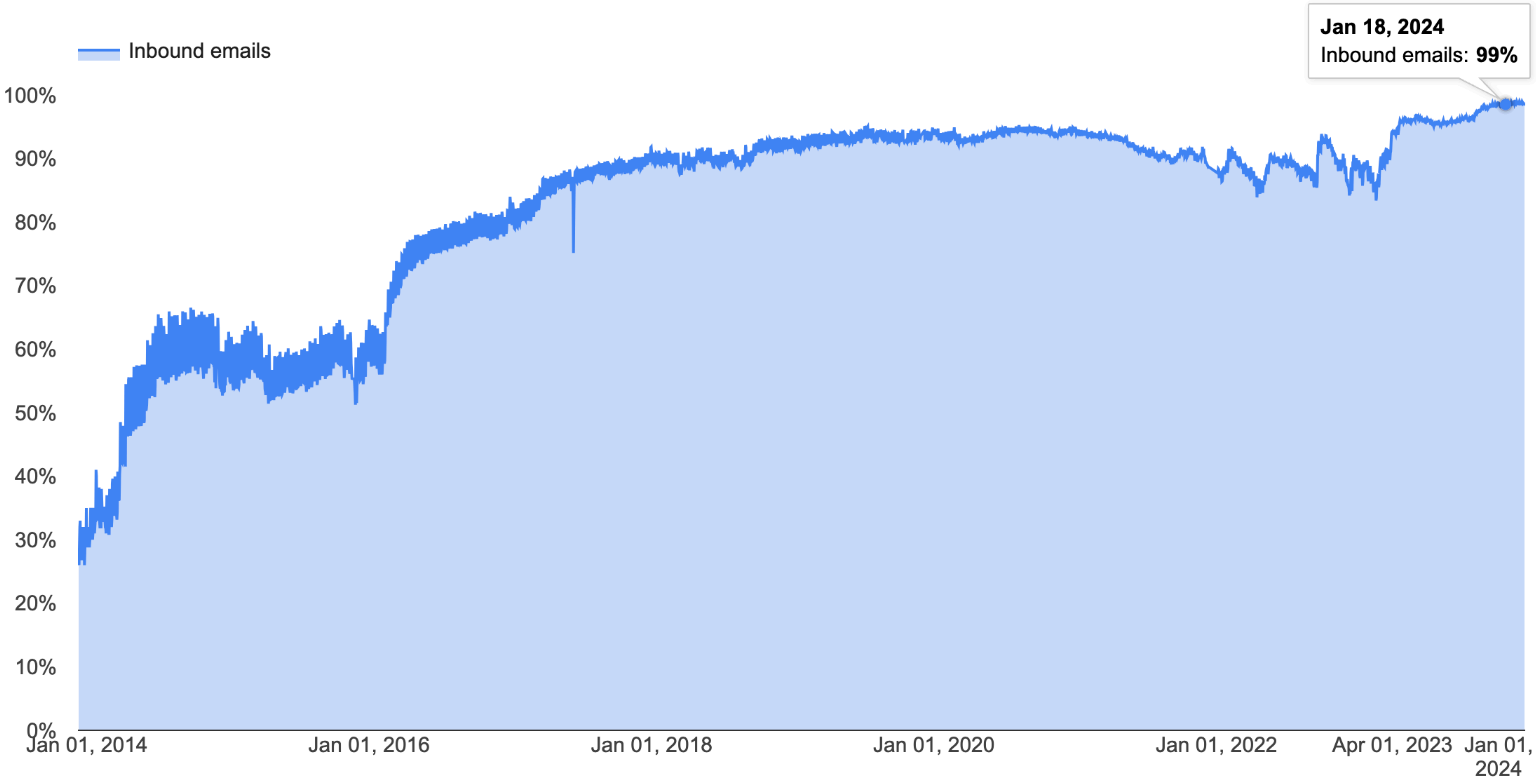
100%
75%
50%
25%
0%
2013
2015
2016
2017
2019
Gmail Inbound
Gmail Outbound

Yahoo and Hotmail deploy STARTTLS

Gmail rolls out 🔒 indicators

Today, 92-93% of messages are encrypted

Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security. IMC'15; Google


Inbound emails
Jan 18, 2024
Inbound emails: 99%
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Jan 01, 2014
Jan 01, 2016
Jan 01, 2018
Jan 01, 2020
Jan 01, 2022
Apr 01, 2023
Jan 01, 2024

Authenticating Email

Sender Policy Framework (SPF)

Sender publishes list of IPs authorized to send mail

DomainKeys Identified Mail (DKIM)

Sender signs messages with their cryptographic key

Domain Message Authentication, Reporting, and Conformance (DMARC)

Sender publishes DNS policy that specifies what to do if message validation fails

Example SPF and DMARC Records

dig -t _spf.google.com

```
;; ANSWER SECTION:
_spf.google.com.        125        IN        TXT        "v=spf1 include:_netblocks.google.com
                                                                include:_netblocks2.google.com
                                                                include:_netblocks3.google.com ~all"
```

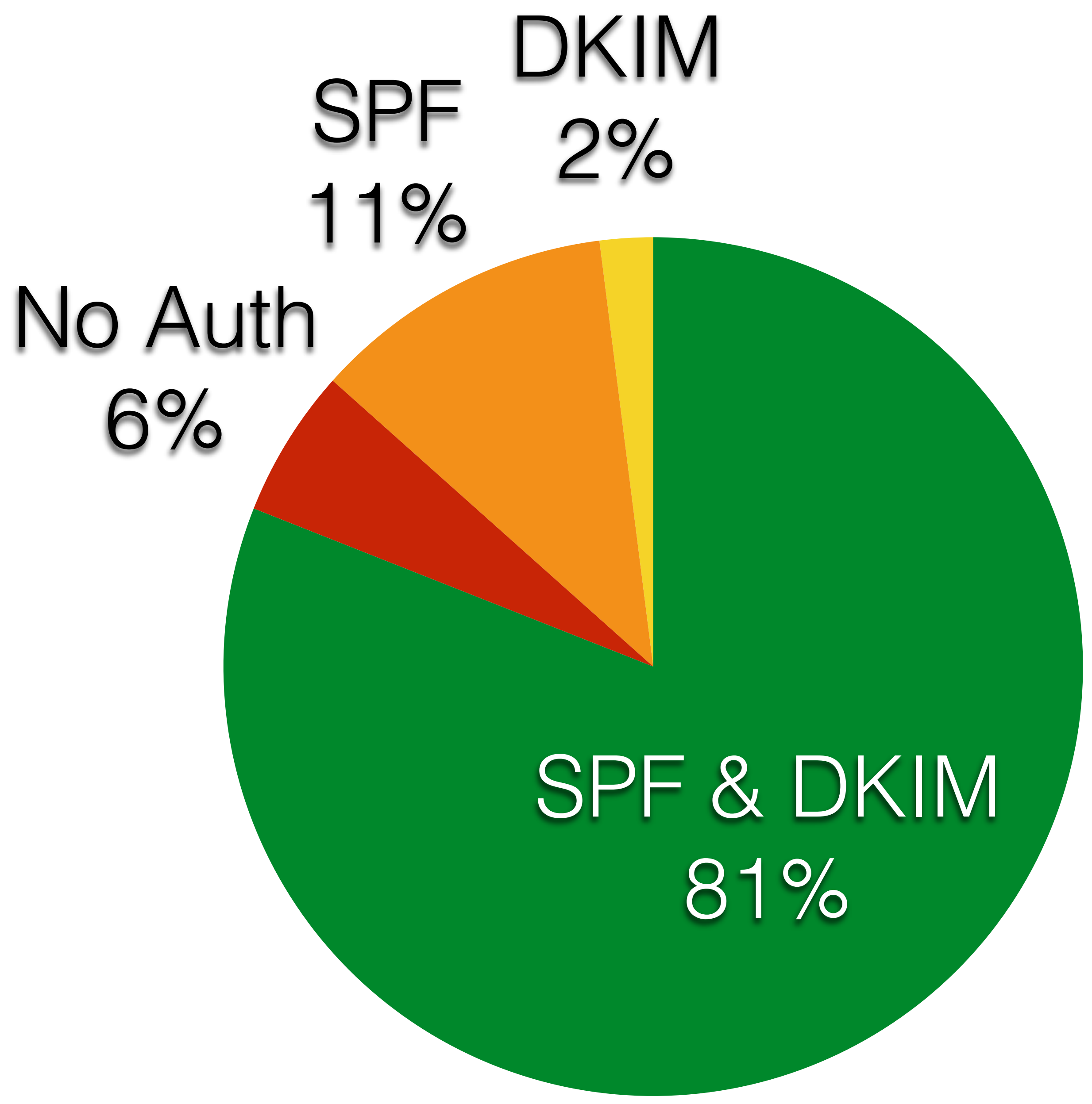
_netblocks:

```
"v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0.0/16
ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all"
```

dig -t txt _dmarc.google.com

```
"v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
```

Authentication for Gmail



Delivered Gmail Messages

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

DMARC Policy	Top 1M
Reject	20%
Quarantine	8%
None	72%

1M Most Popular Domains

PGP — Pretty Good Privacy

Third-Party Toolkit for encrypting and signing emails originally developed in 1991

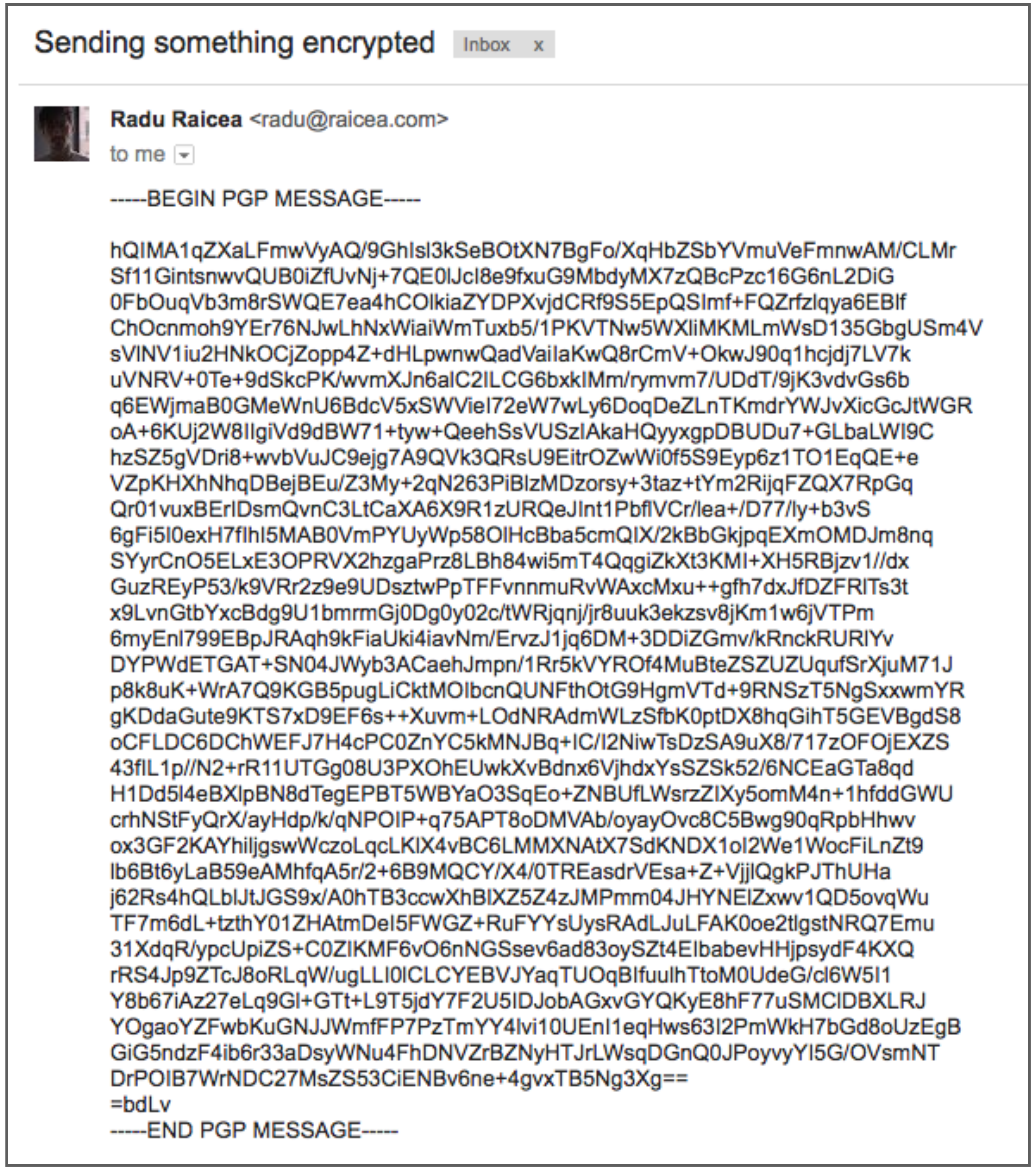
Tremendous Usability and Implementation Challenges

Most Recently: "Our attacks allow the spoofing of digital signatures for arbitrary messages in 14 out of 20 tested OpenPGP-capable email clients and 15 out of 22 email clients supporting S/MIME signatures."

“Johnny, you are fired!” – Spoofing OpenPGP and S/MIME Signatures in Emails (USENIX Security 2019)

Signatures prevent deniability.

tl;dr: Do Not Use PGP if you need security.



Sending something encrypted

Radu Raicea <radu@raicea.com>

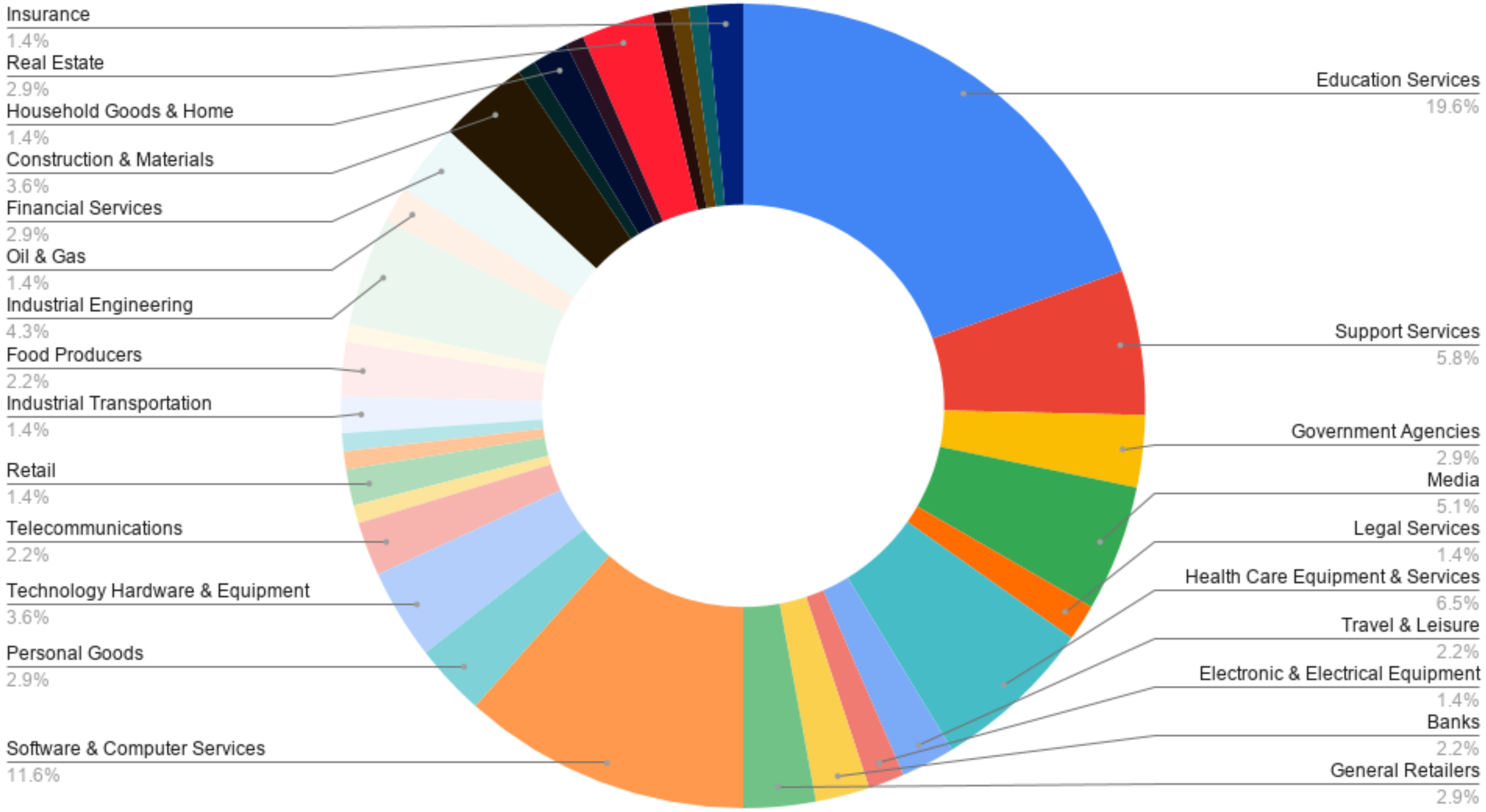
```
-----BEGIN PGP MESSAGE-----

hQIMA1qZXaLFmwVyAQ/9GhIsl3kSeBOtXN7BgFo/XqHbZSbYVmuVeFmnwAM/CLMr
Sf11GintsnwvQUB0iZfUvNj+7QE0lJcl8e9fxuG9MbdyMX7zQBcPzc16G6nL2DiG
0FbOuqVb3m8rSWQE7ea4hCOlkiaZYDPXvjdCRf9S5EpQSImf+FQZrfzlqya6EBlf
ChOcnmoh9YEr76NJwLhNxWiaiWmTuxb5/1PKVTNw5WXliMKMLmWsD135GbgUSm4V
sVlNV1iu2HNkOCjZopp4Z+dHLpwnwQadVailaKwQ8rCmV+OkwJ90q1hcjdj7LV7k
uVNRV+0Te+9dSkcPK/wvmXJn6alC2ILCG6bxkIMm/rymvm7/UDdT/9jK3vdvGs6b
q6EWjmaB0GMeWnU6BdcV5xSWVieI72eW7wLy6DoqDeZLnTKmdrYWJvXicGcJtWGR
oA+6KUj2W8IlgiVd9dBW71+tyw+QeehSsVUSzIAkaHQyyxgpDBUDu7+GLbaLWI9C
hzSZ5gVDri8+wvbVuJC9ejg7A9QVk3QRsU9EitrOZwWi0f5S9Eyp6z1TO1EqQE+e
VZpKHXhNhqDBejBEu/Z3My+2qN263PiBlzMDzorsy+3taz+tYm2RijqFZQX7RpGq
Qr01vuxBErIDsmQvnC3LtCaXA6X9R1zURQeJInt1PbflVCr/lea+/D77/ly+b3vS
6gFi5l0exH7fIhl5MAB0VmPYUyWp58OlHcBba5cmQIX/2kBbGkjpqEXmOMDJm8nq
SYyrCnO5ELxE3OPRVX2hzgaPrz8LBh84wi5mT4QqgiZkXt3KMI+XH5RBjzv1//dx
GuzREyP53/k9VRr2z9e9UDsztwPpTFFvnnmuRvWAxcMxu++gfh7dxJfDZFRITs3t
x9LvnGtbYxcBdg9U1bmrmGj0Dg0y02c/tWRjqnj/jr8uuk3ekzsv8jKm1w6jVTPm
6myEnl799EBpJRAqh9kFiaUki4iavNm/ErvzJ1jq6DM+3DDiZGmv/kRnckRURlYv
DYPWdETGAT+SN04JWyb3ACaehJmpn/1Rr5kVYROf4MuBteZSZUZUqufSrXjuM71J
p8k8uK+WrA7Q9KGB5pugLiCktMOlbcnQUNFthOtG9HgmVTd+9RNSzT5NgSxxwmYR
gKDdaGute9KTS7xD9EF6s++Xuvm+LOdNRAdmWLzSfbK0ptDX8hqGihT5GEVBgdS8
oCFLDC6DChWEFJ7H4cPC0ZnYC5kMNJBq+IC/I2NiwTsDzSA9uX8/717zOFOjEXZS
43fIL1p//N2+rR11UTGg08U3PXOhEUwkXvBdnx6VjhdxYsSZSk52/6NCEaGTa8qd
H1Dd5l4eBXlpBN8dTegEPBT5WBYaO3SqEo+ZNBUfLWsrzZIXy5omM4n+1hfddGWU
crhNStFyQrX/ayHdp/k/qNPOIP+q75APT8oDMVAb/oyayOvc8C5Bwg90qRpbHhwv
ox3GF2KAYhiljgswWczoLqcLKlX4vBC6LMMXNAtX7SdKNDX1ol2We1WocFiLnZt9
lb6Bt6yLaB59eAMhfqA5r/2+6B9MQCY/X4/0TREasdrVEsa+Z+VjjlQgkPJThUHa
j62Rs4hQLblJtJGS9x/A0hTB3ccwXhBlXZ5Z4zJMPmm04JHYNElZxwv1QD5ovqWu
TF7m6dL+tzthY01ZHAtmDel5FWGZ+RuFYYsUysRAdLJuLFAK0oe2tlgstNRQ7Emu
31XdqR/ypcUpiZS+C0ZlKMF6vO6nNGSsev6ad83oySZt4ElbabevHHjpsydF4KXQ
rRS4Jp9ZTcJ8oRLqW/ugLLI0lCLCYEBVJYaqTUOqBlfuulhTtoM0UdeG/cl6W5I1
Y8b67iAz27eLq9GI+GTt+L9T5jdY7F2U5lDJobAGxvGYQKyE8hF77uSMClDBXLRJ
YOgaoYZFwbKuGNJJWmfFP7PzTmYY4lvi10UEnI1eqHws63I2PmWkH7bGd8oUzEgB
GiG5ndzF4ib6r33aDsyWNu4FhDNVZrBZNyHTJrLWsqDGnQ0JPoyvyYI5G/OVsmNT
DrPOIB7WrNDC27MsZS53CiENBv6ne+4gvxTB5Ng3Xg==
=bdLv
-----END PGP MESSAGE-----
```

2021 Microsoft Exchange Server Vulnerability

Pre-authentication vulnerability allowed attackers to dump mailbox content and remotely execute code on Microsoft Exchange Servers

"Censys observed 251,211 Microsoft Exchange Servers (2013, 2016, or 2019 versions) across the Internet."

Actually, don't use email at all if you really need security.



Random Sampling U.S. Exchange Servers Mapped to Industries

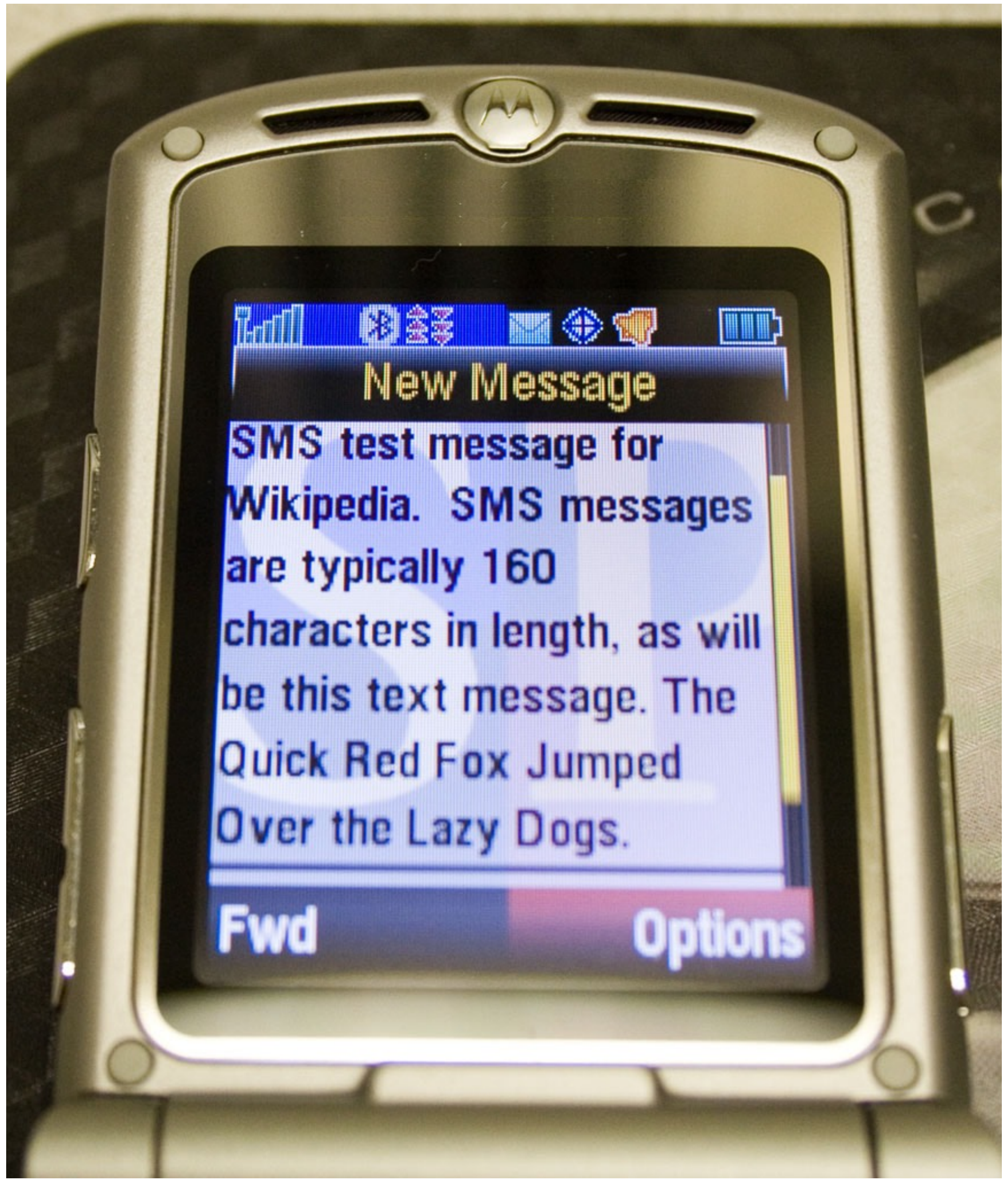
https://censys.io/blog/microsoft-exchange-vulnerabilities-mar2021/

SMS — Short Message Service

SMS allows sending 140 byte messages as part of the non-data cellular protocols (e.g., GSM, CDMA, HSPA, 4G, 5G)

Messages are sent using the same type of control messages that your phone uses to coordinate with cellular towers for service

No end-to-end security protections — provider sees everything. Messages are stored and forwarded by your provider.



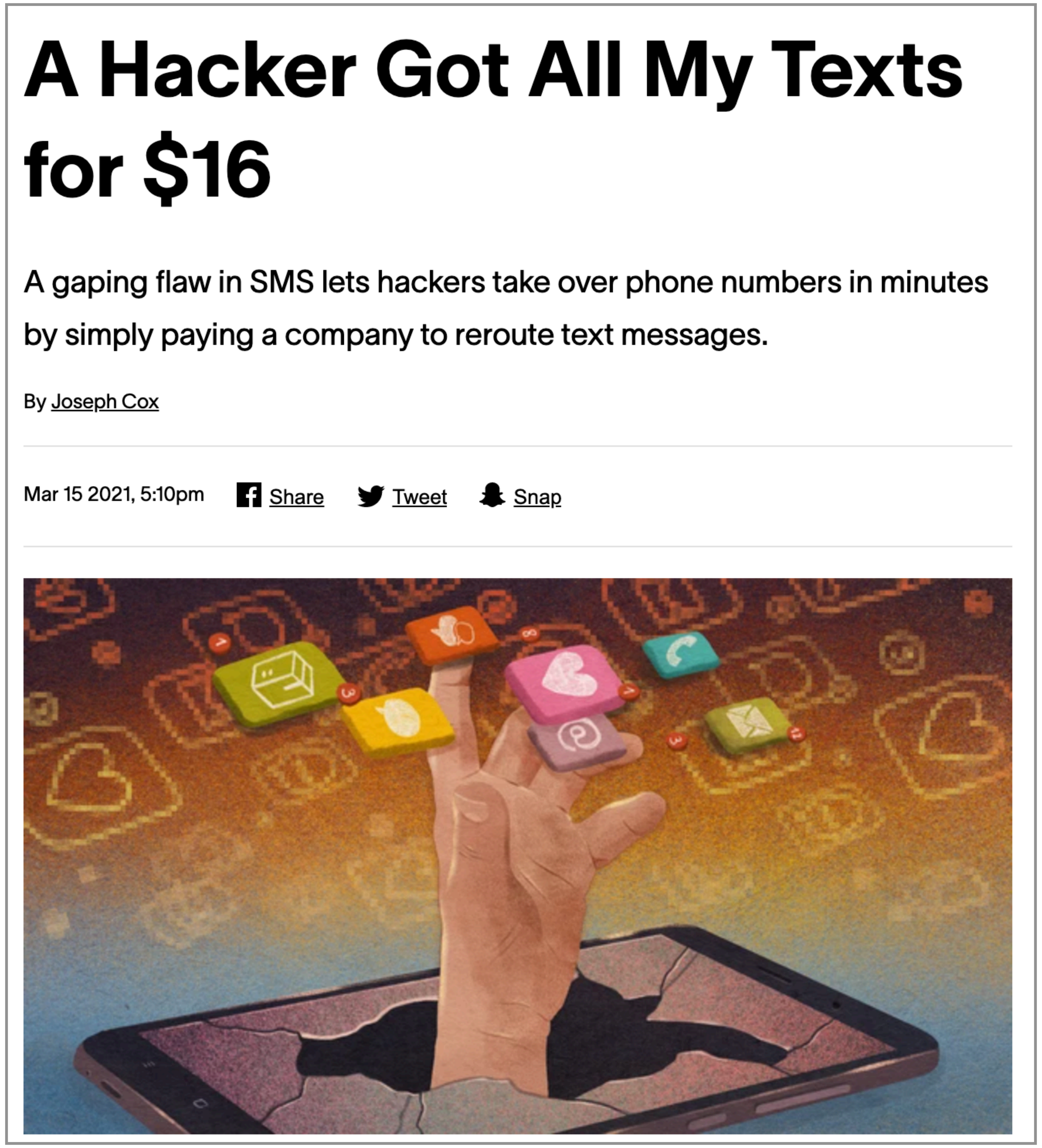
SMS test message for Wikipedia. SMS messages are typically 160 characters in length, as will be this text message. The Quick Red Fox Jumped Over the Lazy Dogs.

Phone Number and SMS Hijacking

Recent years have seen an increase in social engineering attacks to hijack phone numbers

An attack this year also showed how it's possible to hijack the SMS capabilities of a phone through a third provider

NetNumber — company that provides authoritative database of SMS redirections — allows some companies to change routing of numbers



A Hacker Got All My Texts for $16

A gaping flaw in SMS lets hackers take over phone numbers in minutes by simply paying a company to reroute text messages.

By Joseph Cox

Mar 15 2021, 5:10pm Share Tweet Snap

Alright… more secure alternatives

OTR: Off-the-Record Messaging

Cryptographic Protocol released in 2004 by Nikita Borisov, Ian Goldberg, and Eric Brewer

Alternative to PGP that runs on top of Instant Messaging Clients (e.g., Jabber)

Precursor to many of today's secure messaging protocols

Beyond Encryption and Authentication, introduced new ideas to messaging security:

> **Forward Secrecy:** Messages are encrypted with temporary per-message AES keys, negotiated using the Diffie-Hellman key exchange protocol. The compromise of any long-lived cryptographic keys does not compromise any previous conversations
>
> **Deniability:** Messages do not have digital signatures. Anyone is able to forge a message to appear to have come from one of the participants in the conversation.

Signal Protocol

Protocol created by creators of Signal App. Built on good parts of OTR and Silent Circle Instant Messaging Protocol (SCIMP)

Basis for Signal, WhatsApp, Google E2E Encryption

Based on notion of "double ratchet" between each message

The rain is pouring down and I'm sitting here just listening to it.
30m

That's what I did this morning

Tina Ukuku 11:11 AM
You set disappearing message time to 1...

Chairman Meow 11:11 AM
Missed call

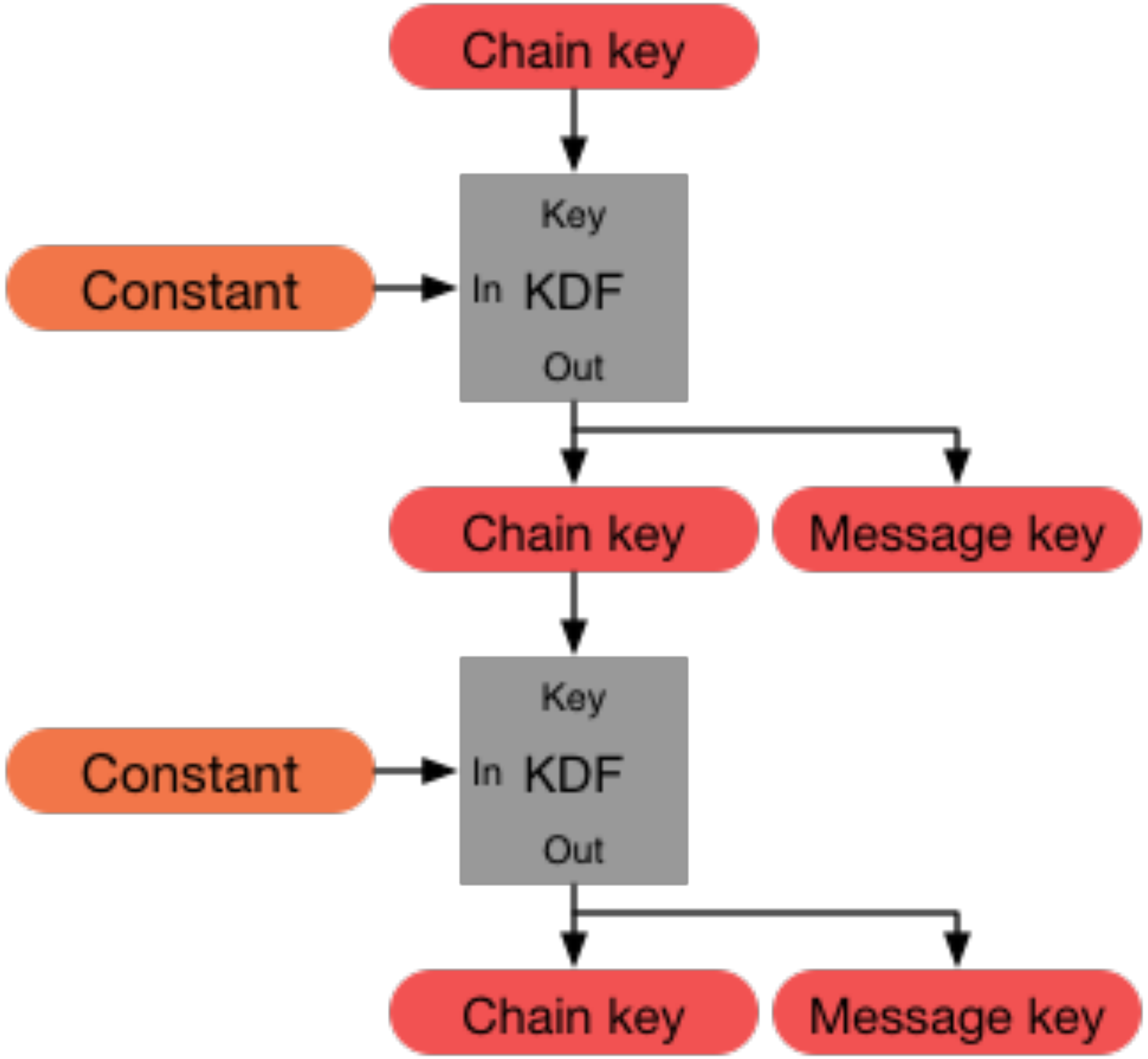
Myles Larson 11:07 AM
🎤 Voice Message

Cat Chat 🐈 🐱 11:02 AM
This is the instruction manual. 📎 Attac...

Ali Smith 10:38 AM
📷 Attachment

Kirk Family 9:13 AM
Happy birthday to you. Happy birthda...

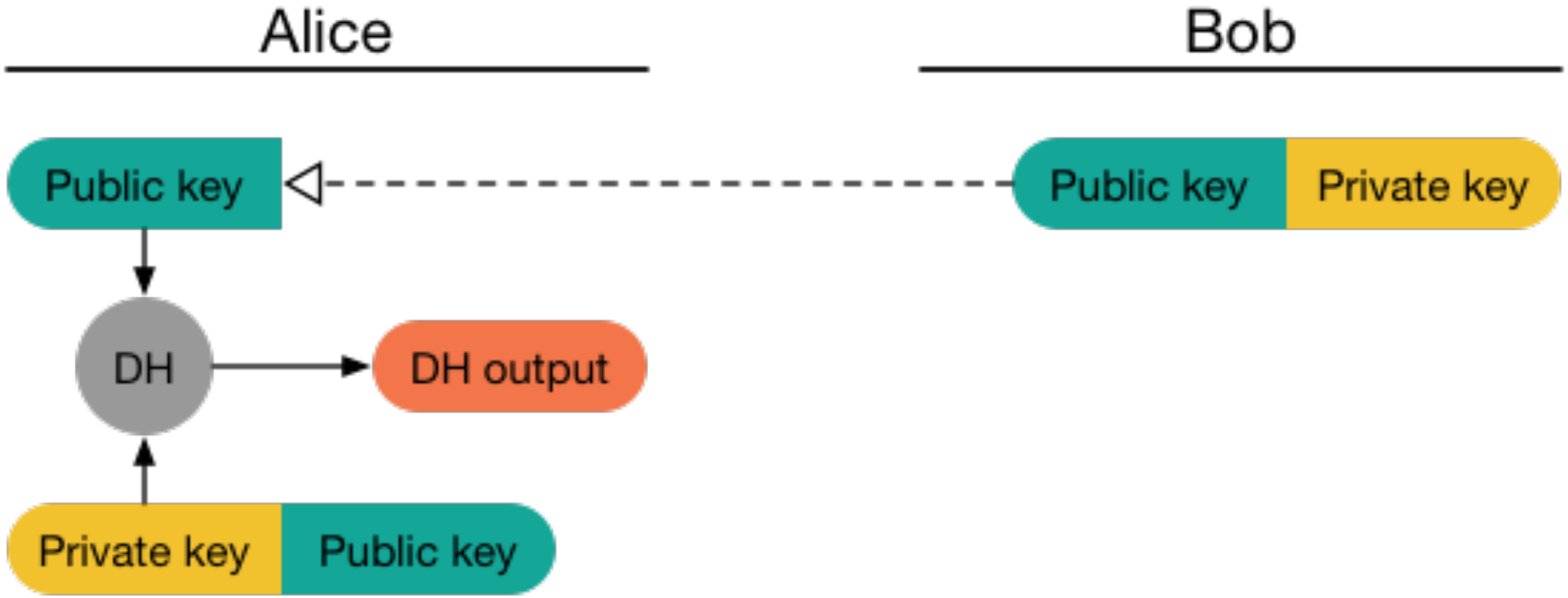
Symmetric-Key Ratchet



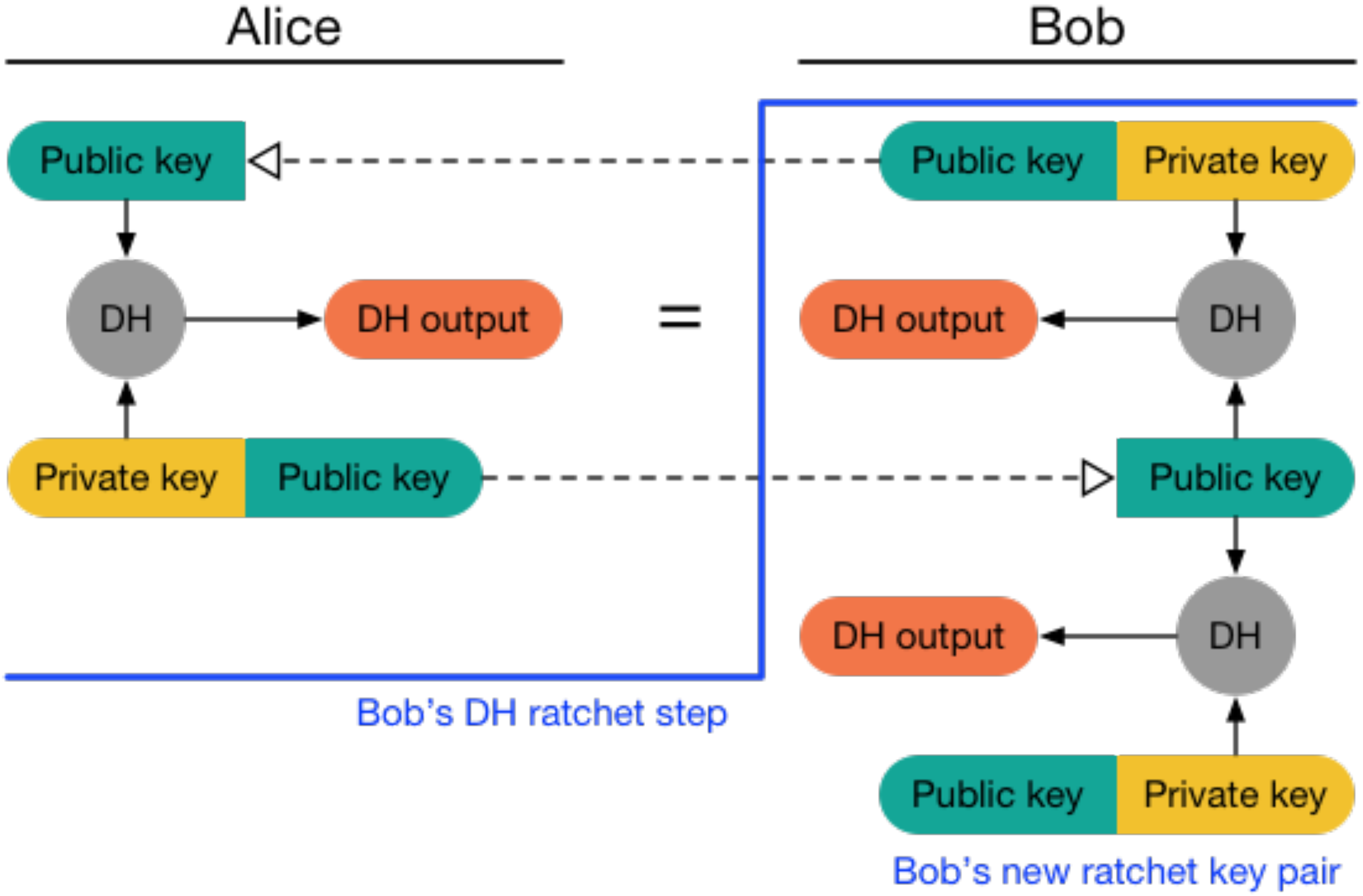
Different cryptographic key for each message.

Significant Downfall: If an attacker gets access to key, then they can decrypt all future messages.

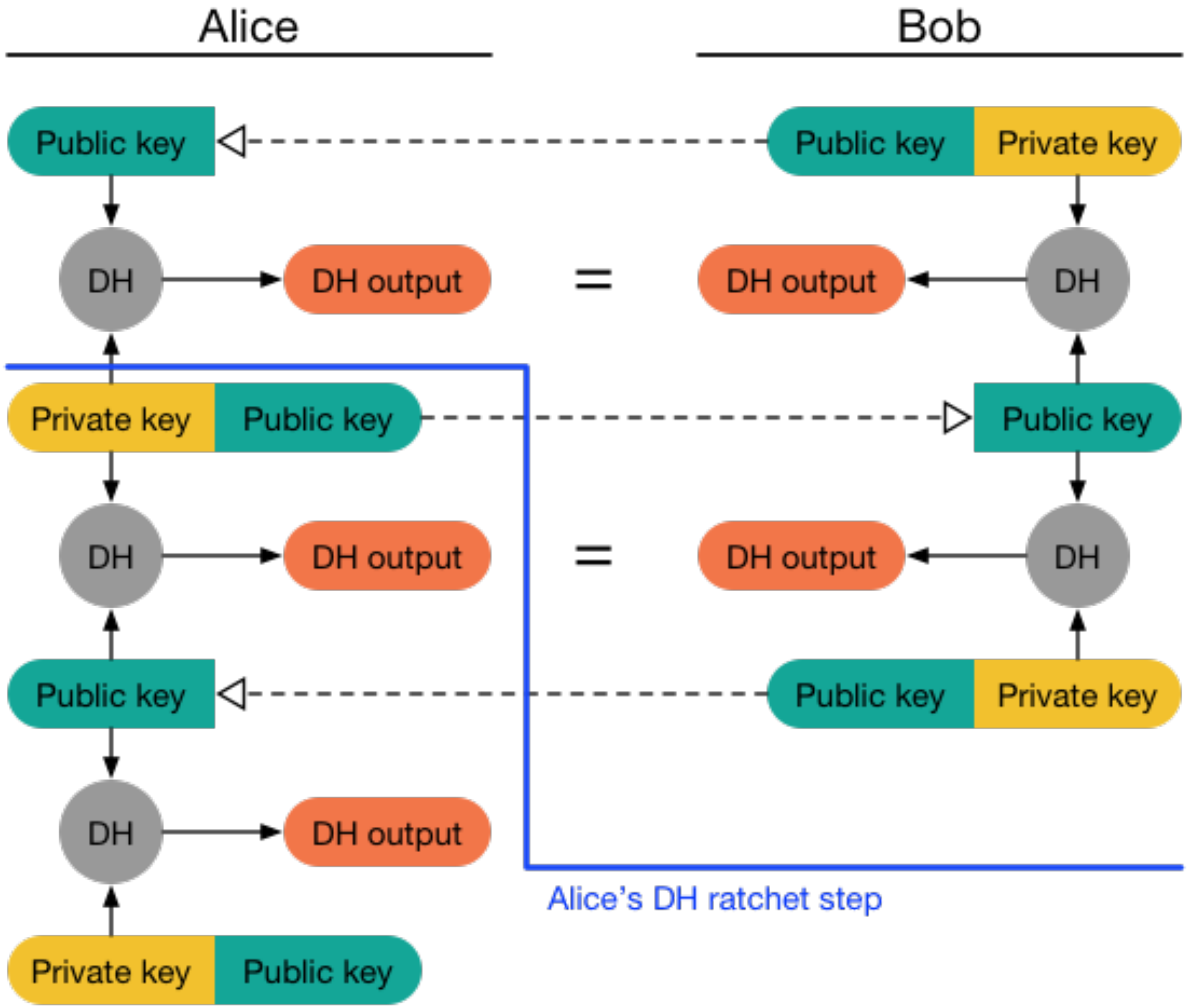
Diffie-Hellman Ratchet



Diffie-Hellman Ratchet



Diffie-Hellman Ratchet



Messaging Layer Security (MLS) Protocol

RFC in active development that sets out to create a protocol for asynchronous group keying with forward secrecy and post-compromise security

2 Party Solved: "For two parties, this problem has been studied thoroughly, with the Double Ratchet emerging as a common solution [doubleratchet] [signal]."

But group message situation remained unsolved:

Based on earlier work on "asynchronous ratcheting trees", the protocol presented here uses an asynchronous key-encapsulation mechanism for tree structures. This mechanism allows the members of the group to derive and update shared keys with costs that scale as the log of the group size

Details: https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/