CSE508 Network Security

Stony Brook University

2024-04-16

Email

Michalis Polychronakis

Stony Brook University

Email Overview

MUA: Mail User Agent

Thunderbird, Apple Mail, …

MSA: Mail Submission Agent

SMTP (port 587)

Often same as initial MTA

MTA: Mail Transfer Agent

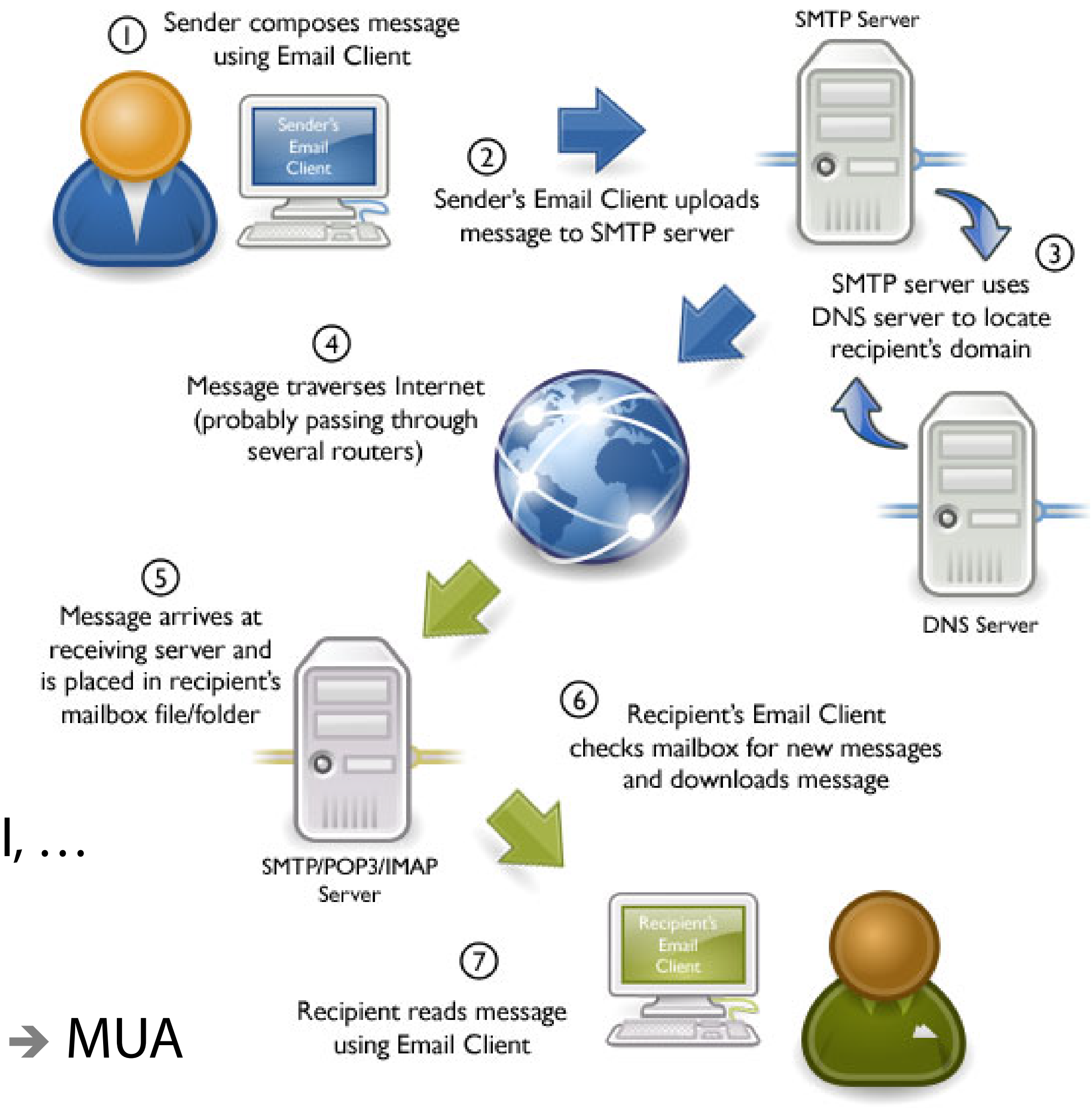
SMTP (port 25)

MDA: Mail Delivery Agent

IMAP (port 143), POP3 (port 110), local, …

Typical flow:

MUA → MSA → MTA → … → MTA → MDA → MUA



① Sender composes message using Email Client
Sender's Email Client
② Sender's Email Client uploads message to SMTP server
SMTP Server
③ SMTP server uses DNS server to locate recipient's domain
DNS Server
④ Message traverses Internet (probably passing through several routers)
⑤ Message arrives at receiving server and is placed in recipient's mailbox file/folder
SMTP/POP3/IMAP Server
⑥ Recipient's Email Client checks mailbox for new messages and downloads message
⑦ Recipient reads message using Email Client
Recipient's Email Client

©2010 OnlyMyEmail Inc. (ww.OnlyMyEmail.com) with many thanks to the Gnome project (www.gnome.org) for the images

SMTP Transport Example

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

Email/Messaging Security and Privacy Goals

Protect message content

Fight spam

Fight phishing

(future lecture: social engineering)

Verify communicating parties' identities

Hide communication patterns

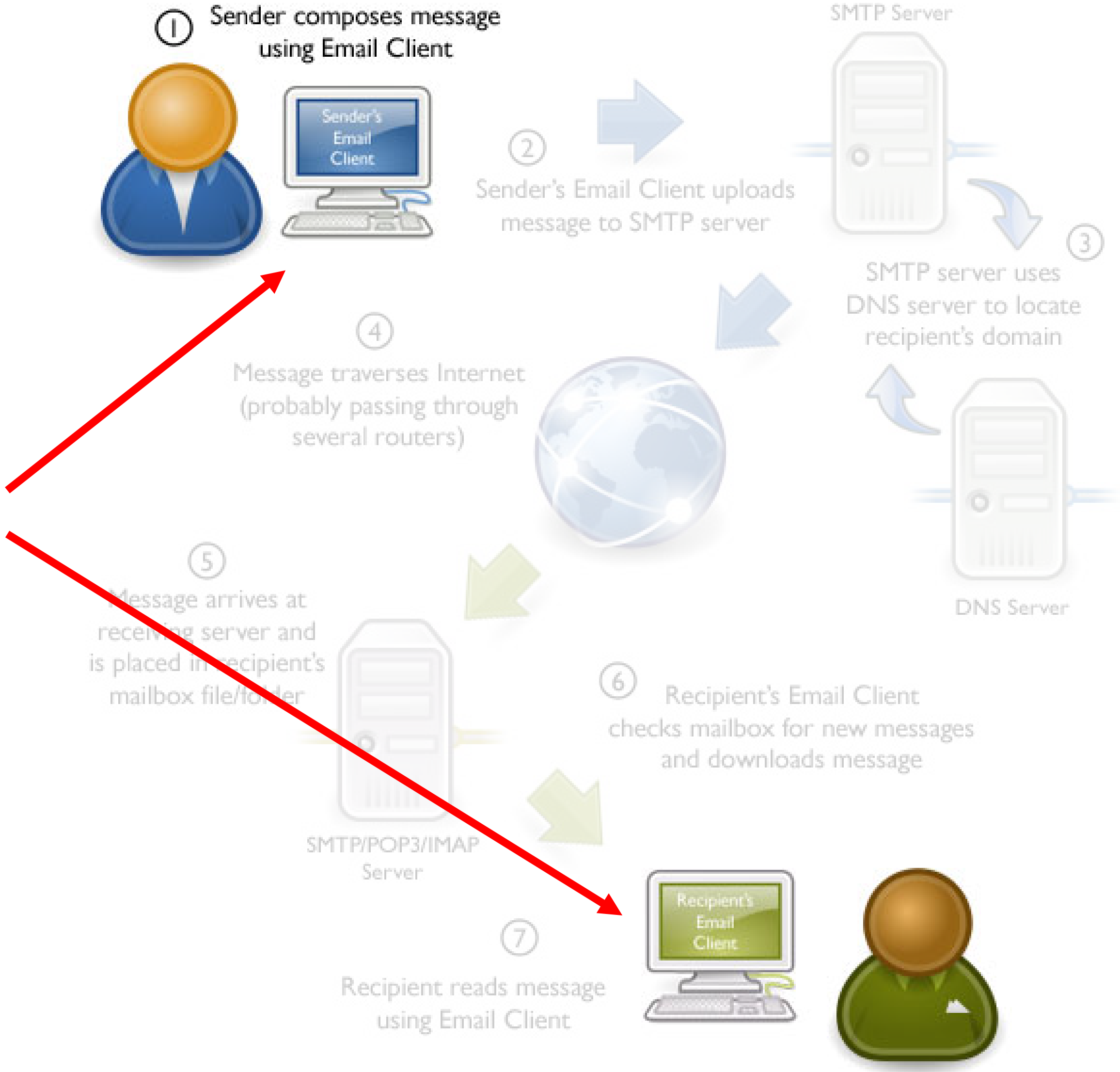
(future lecture: anonymity)

Who can read my email?

Adversaries with local or remote access to my devices

Intruders, spouse, system administrator, …

Malware, stolen credentials, physical access, …

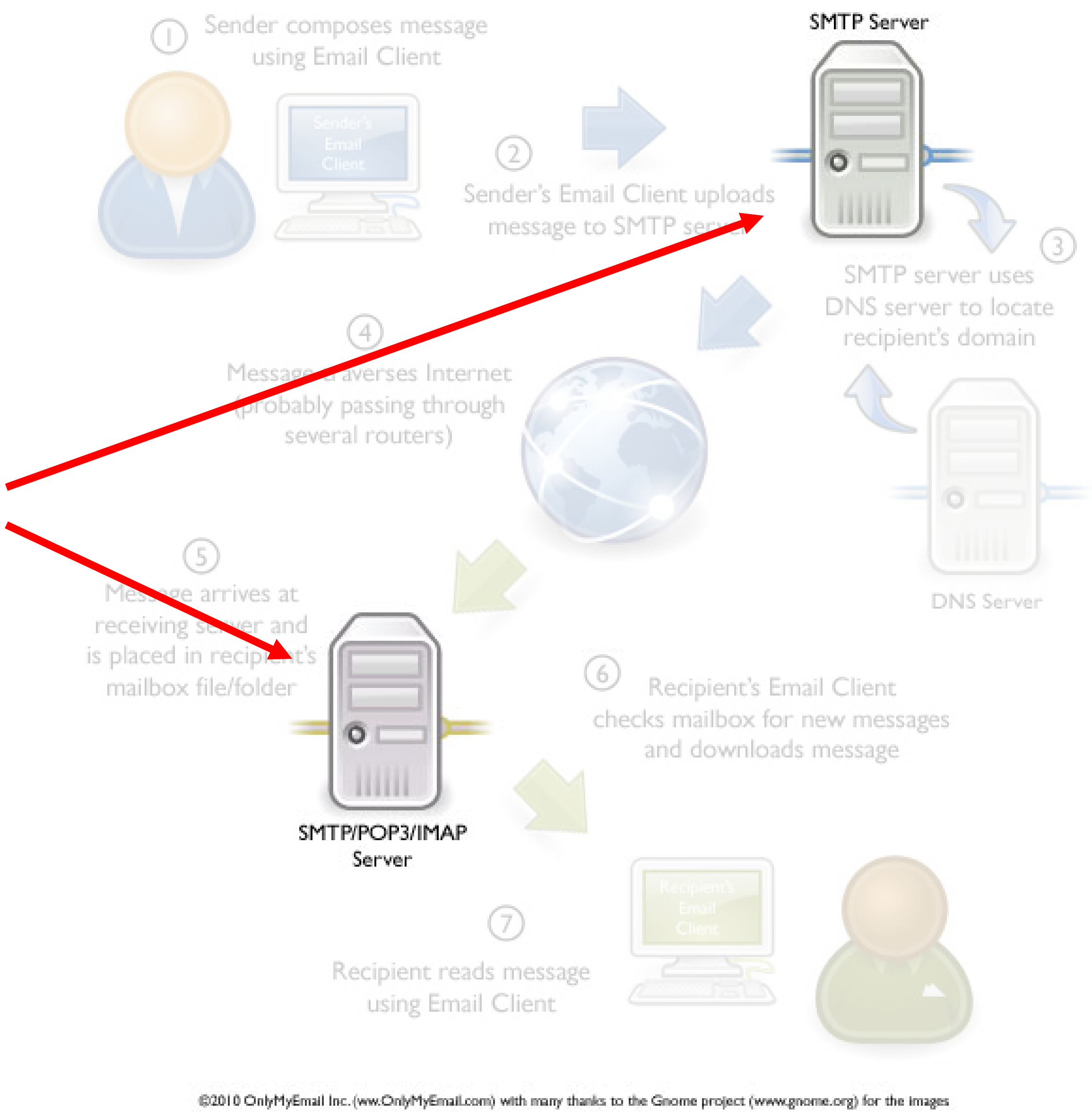

1 Sender composes message using Email Client
Sender's Email Client
2 Sender's Email Client uploads message to SMTP server
SMTP Server
3 SMTP server uses DNS server to locate recipient's domain
DNS Server
4 Message traverses Internet (probably passing through several routers)
5 Message arrives at receiving server and is placed in recipient's mailbox file/folder
SMTP/POP3/IMAP Server
6 Recipient's Email Client checks mailbox for new messages and downloads message
7 Recipient reads message using Email Client
Recipient's Email Client

©2010 OnlyMyEmail Inc. (ww.OnlyMyEmail.com) with many thanks to the Gnome project (www.gnome.org) for the images

Who can read my email?

Adversaries with local or remote access to MTAs and other intermediary servers

System administrators, other insiders, intruders, LEAs, …


SMTP Server
1 Sender composes message using Email Client
Sender's Email Client
2 Sender's Email Client uploads message to SMTP server
3 SMTP server uses DNS server to locate recipient's domain
4 Message traverses Internet (probably passing through several routers)
DNS Server
5 Message arrives at receiving server and is placed in recipient's mailbox file/folder
SMTP/POP3/IMAP Server
6 Recipient's Email Client checks mailbox for new messages and downloads message
7 Recipient reads message using Email Client
Recipient's Email Client

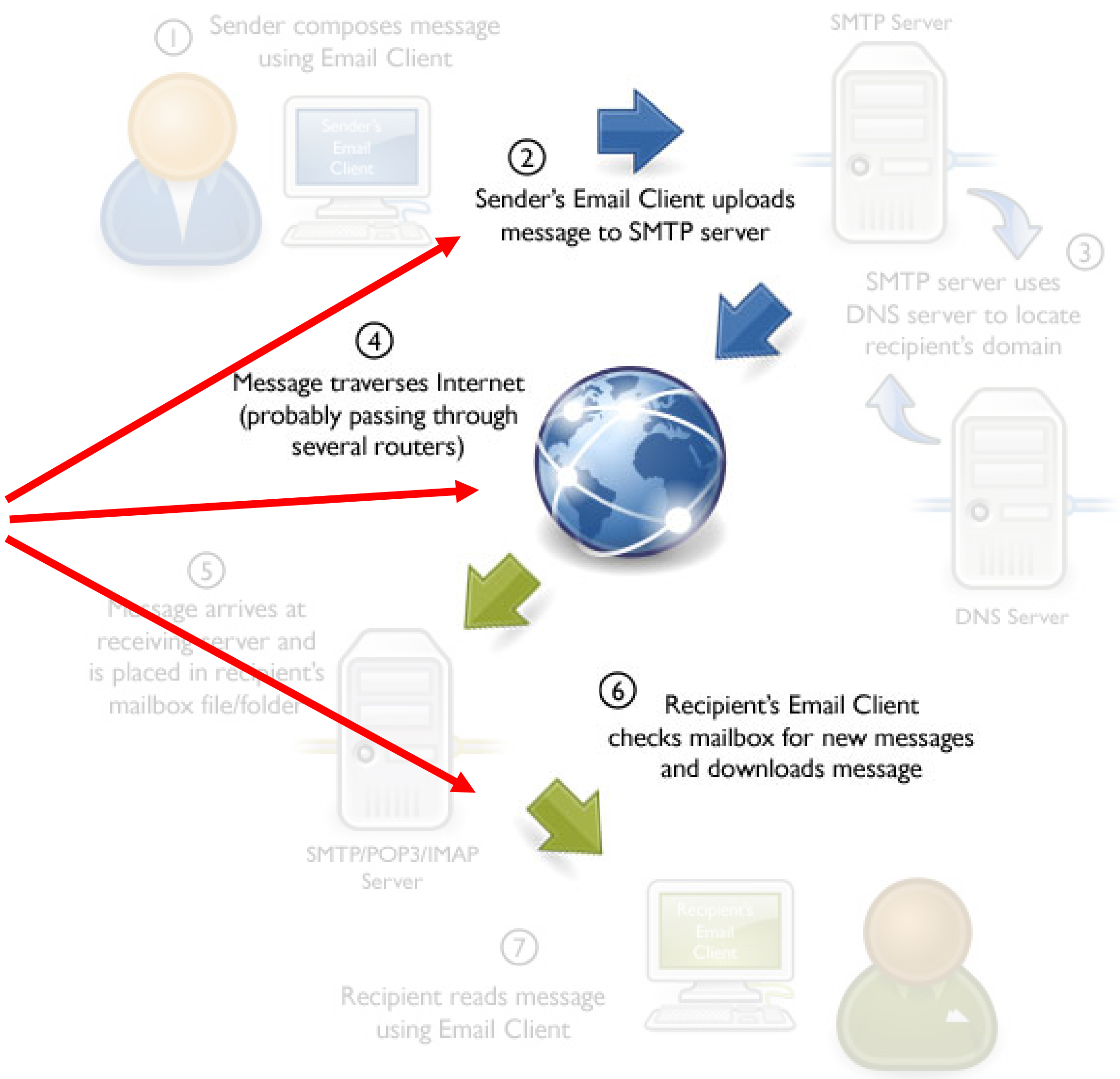
©2010 OnlyMyEmail Inc. (ww.OnlyMyEmail.com) with many thanks to the Gnome project (www.gnome.org) for the images

Who can read my email?

Adversaries with access to any intermediate network

System administrators, other insiders, intruders, LEAs, …

Passive eavesdropping, MitM, DNS poisoning, …



① Sender composes message using Email Client
Sender's Email Client
SMTP Server
② Sender's Email Client uploads message to SMTP server
③ SMTP server uses DNS server to locate recipient's domain
④ Message traverses Internet (probably passing through several routers)
DNS Server
⑤ Message arrives at receiving server and is placed in recipient's mailbox file/folder
⑥ Recipient's Email Client checks mailbox for new messages and downloads message
SMTP/POP3/IMAP Server
⑦ Recipient reads message using Email Client
Recipient's Email Client

©2010 OnlyMyEmail Inc. (ww.OnlyMyEmail.com) with many thanks to the Gnome project (www.gnome.org) for the images

Confidentiality Threats Recap:

Stored messages

Compromised system (either local user machine or remote email server)
Malware, intruder, insider, stolen/lost device, …

Compromised authentication
Password theft, phone unlock, …

Messages in transit

Eavesdropping and interception

Displayed messages

Screendump, reflections, shoulder surfing, …

Securing Email Transit

These days encryption is mandatory for client-to-server email transmission and retrieval

MUA → MSA: STARTTLS (port 587/25), SMTPS (port 465)

MDA → MUA: POP3S (port 995), IMAPS (port 993)

```
mikepo@capcom:~> nc smtp.gmail.com 25
220 mx.google.com ESMTP i185sm2356739qhc.49 - gsmtp
HELO foo.example.com
250 mx.google.com at your service
MAIL FROM:<mikepo@example.com>
530 5.7.0 Must issue a STARTTLS command first.
```

MTA → MTA relaying: *a different story…*

STARTTLS: Opportunistic Encryption

- Legacy MTAs may not support TLS
  - Fail-open design is necessary
- MTAs do their best to deliver messages
  - A recipient MTA may present a self-signed cert (common in antispam/AV systems)
  - There is no PKI for email…
- MitM is trivially easy
  - STARTTLS command is sent over a plaintext channel (!)
  - Analogous to SSL stripping, but in this case the client has no indication that downgrade has happened
  - Just assumes that the receiving MTA does not support TLS
- Message interception is still possible
  - Better than nothing: bulk passive eavesdropping not possible

I want to STARTTLS

```
mikepo@capcom:~> nc aspmx.l.google.com 25
220 mx.google.com ESMTP h126si17458667qhh.29 - gsmtp
EHLO foo.example.com
250-mx.google.com at your service, [128.59.23.41]
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
STARTTLS
220 2.0.0 Ready to start TLS
<TLS Handshake>
```

I want to STARTTLS

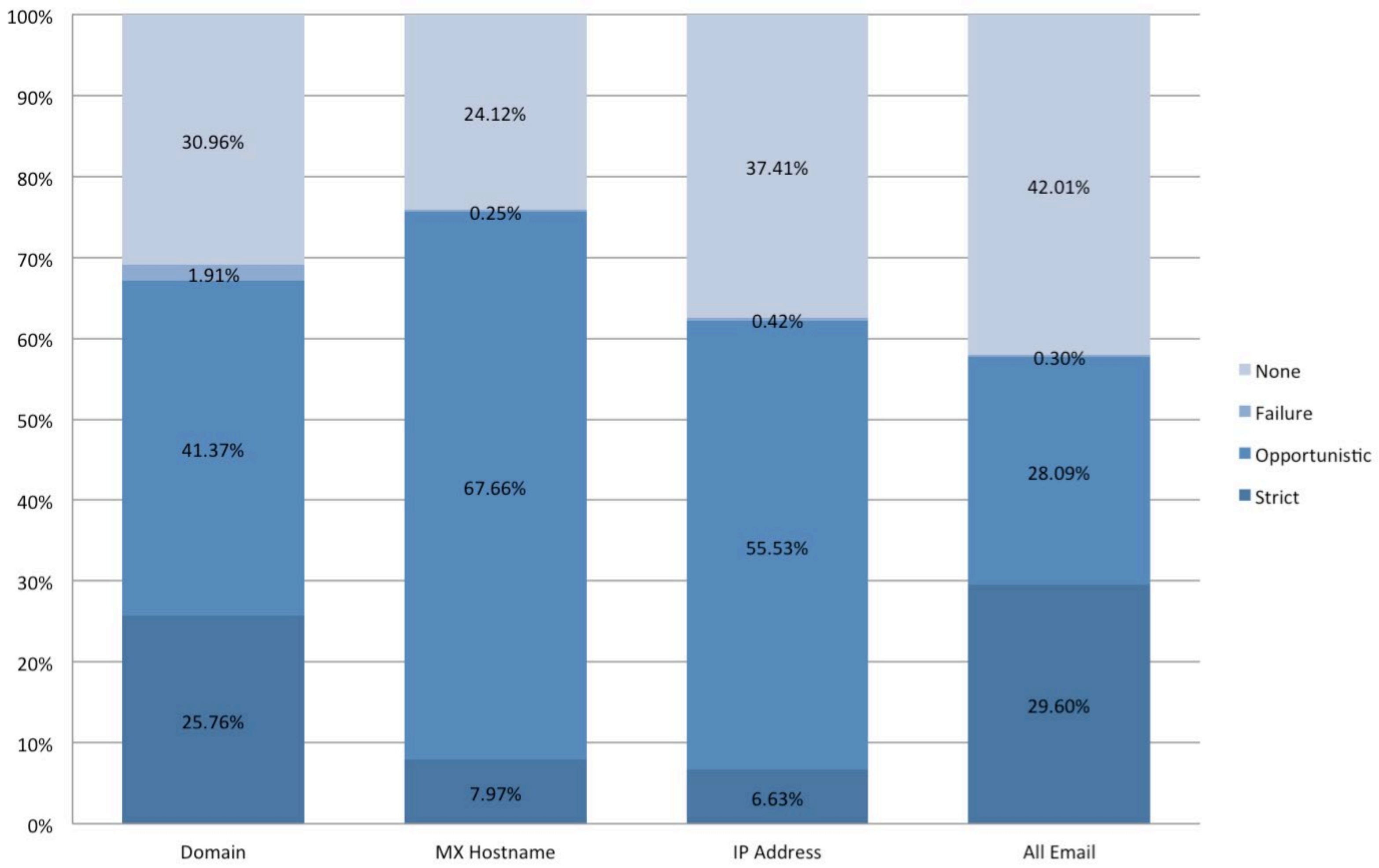
```
mikepo@capcom:~> nc aspmx.l.google.com 25
220 mx.google.com ESMTP h126si17458667qhh.29 - gsmtp
EHLO foo.example.com
250-mx.google.com at your service, [128.59.23.41]
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
STARTTLS
220 2.0.0 Ready to start TLS
<TLS Handshake>
```

Can be stripped off by a MitM attacker

Facebook STARTTLS Study: May 2014

~60% of all messages sent via encrypted connection

Only ~30% pass strict validation (mostly due to self-signed certs)

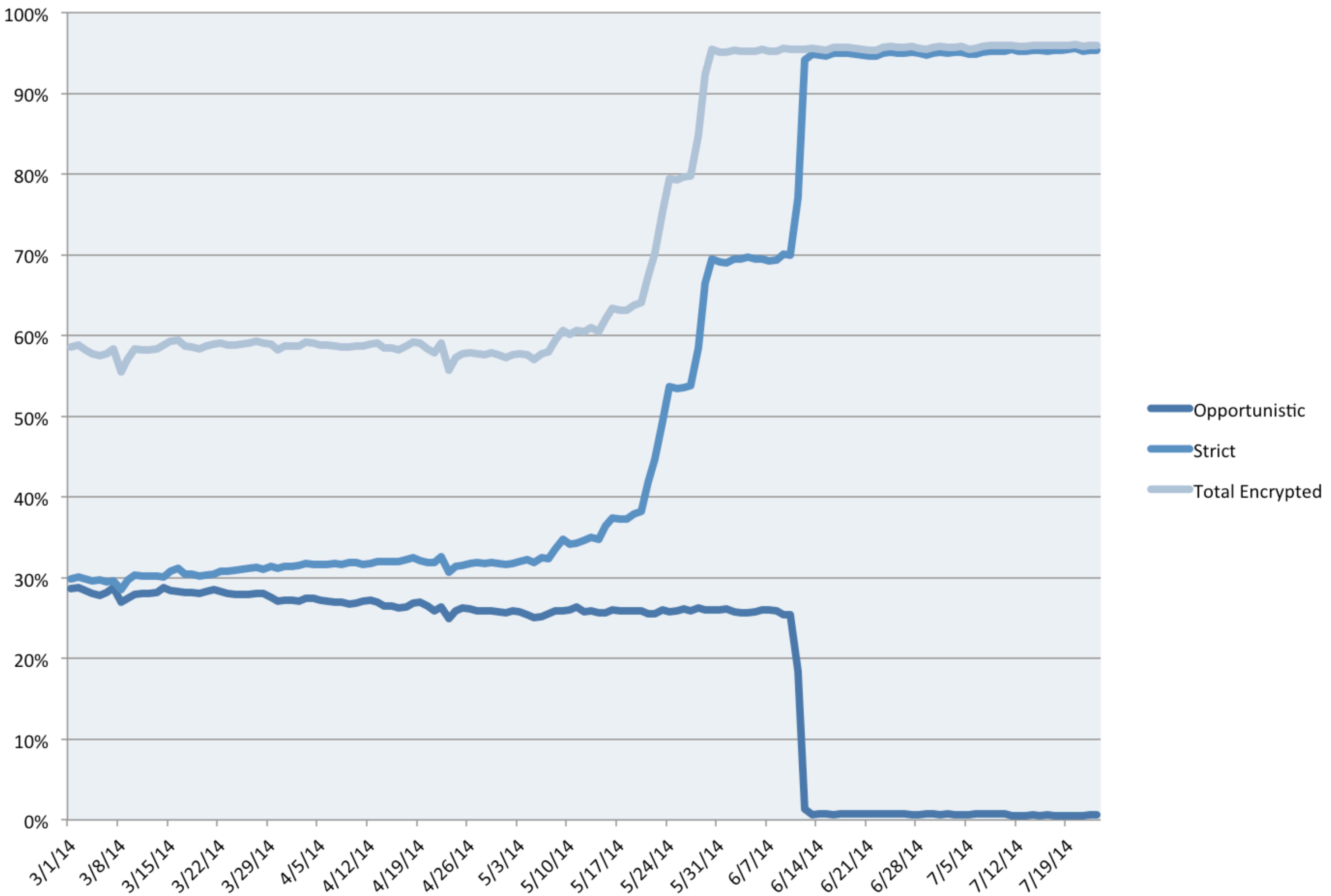


© Facebook - https://www.facebook.com/notes/protect-the-graph/the-current-state-of-smtp-starttls-deployment/1453015901605223/

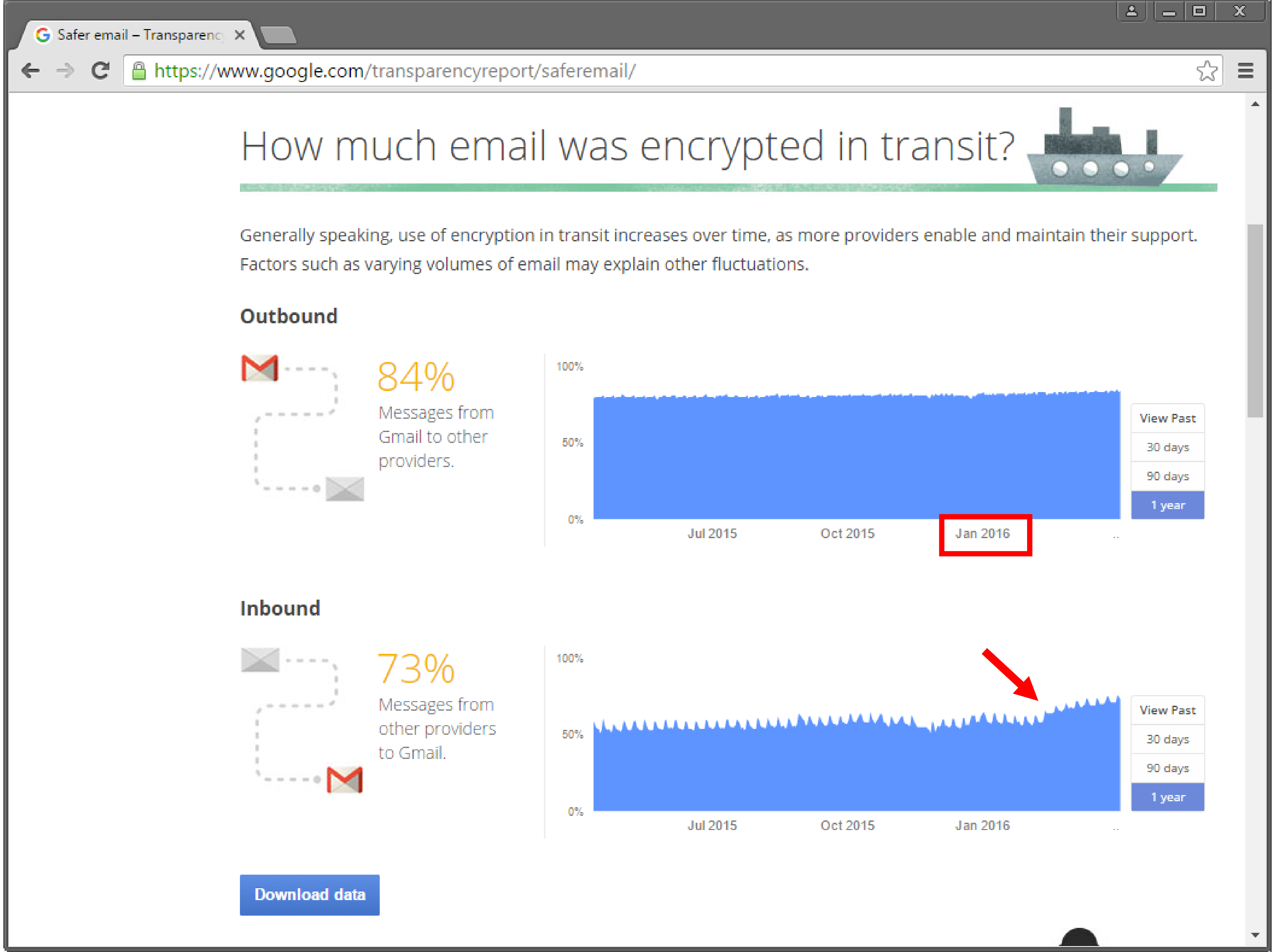
Facebook STARTTLS Study: August 2014

~95% of outgoing messages encrypted with PFS and strict certificate validation

Mostly due to changes by big recipient networks (Microsoft, Yahoo)



© Facebook - https://www.facebook.com/notes/protect-the-graph/massive-growth-in-smtp-starttls-deployment/1491049534468526/



Safer email – Transparenc
https://www.google.com/transparencyreport/saferemail/

How much email was encrypted in transit?

Generally speaking, use of encryption in transit increases over time, as more providers enable and maintain their support. Factors such as varying volumes of email may explain other fluctuations.

Outbound

84%

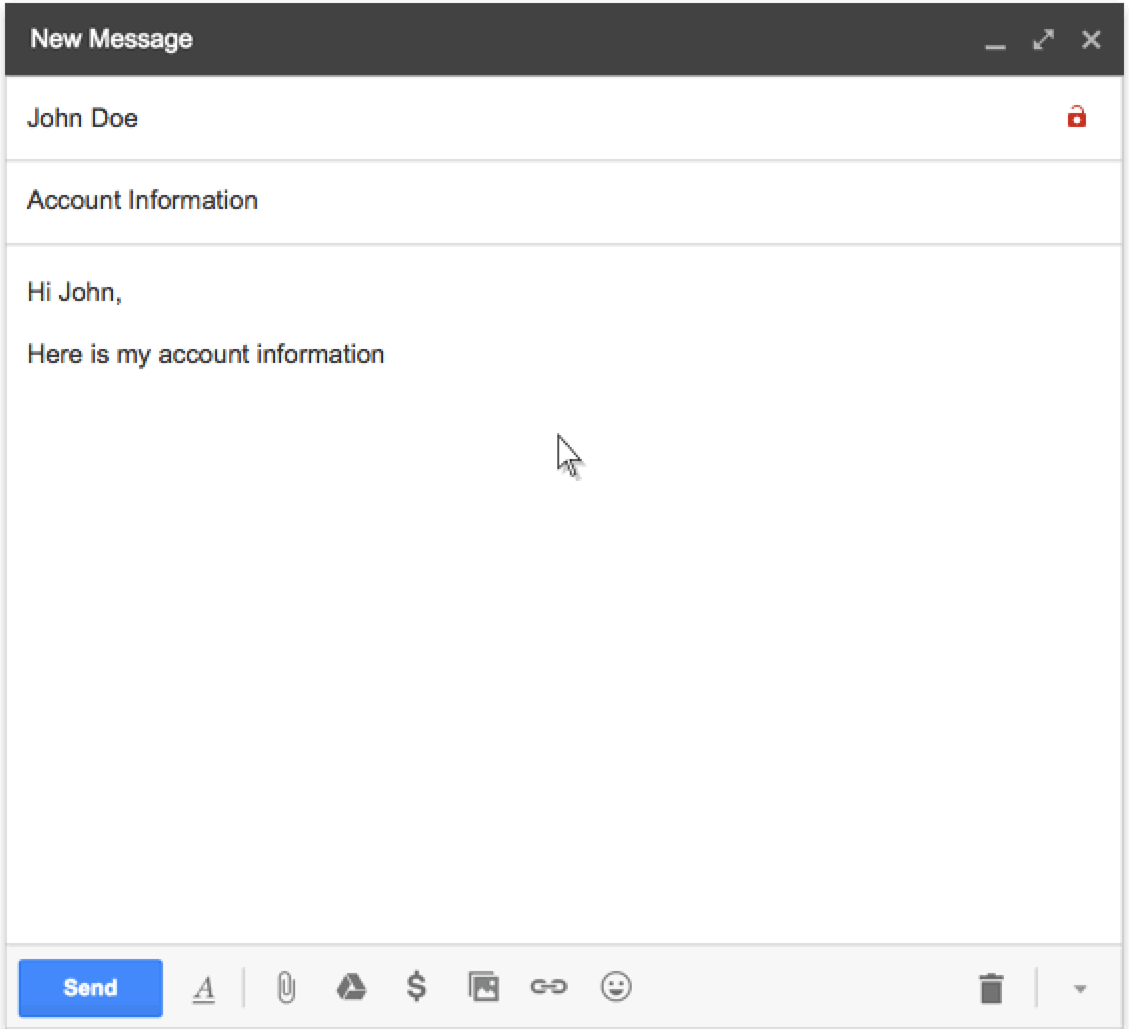
Messages from Gmail to other providers.

Inbound

73%

Messages from other providers to Gmail.

A tiny GUI change prompted many networks to deploy STARTTLS



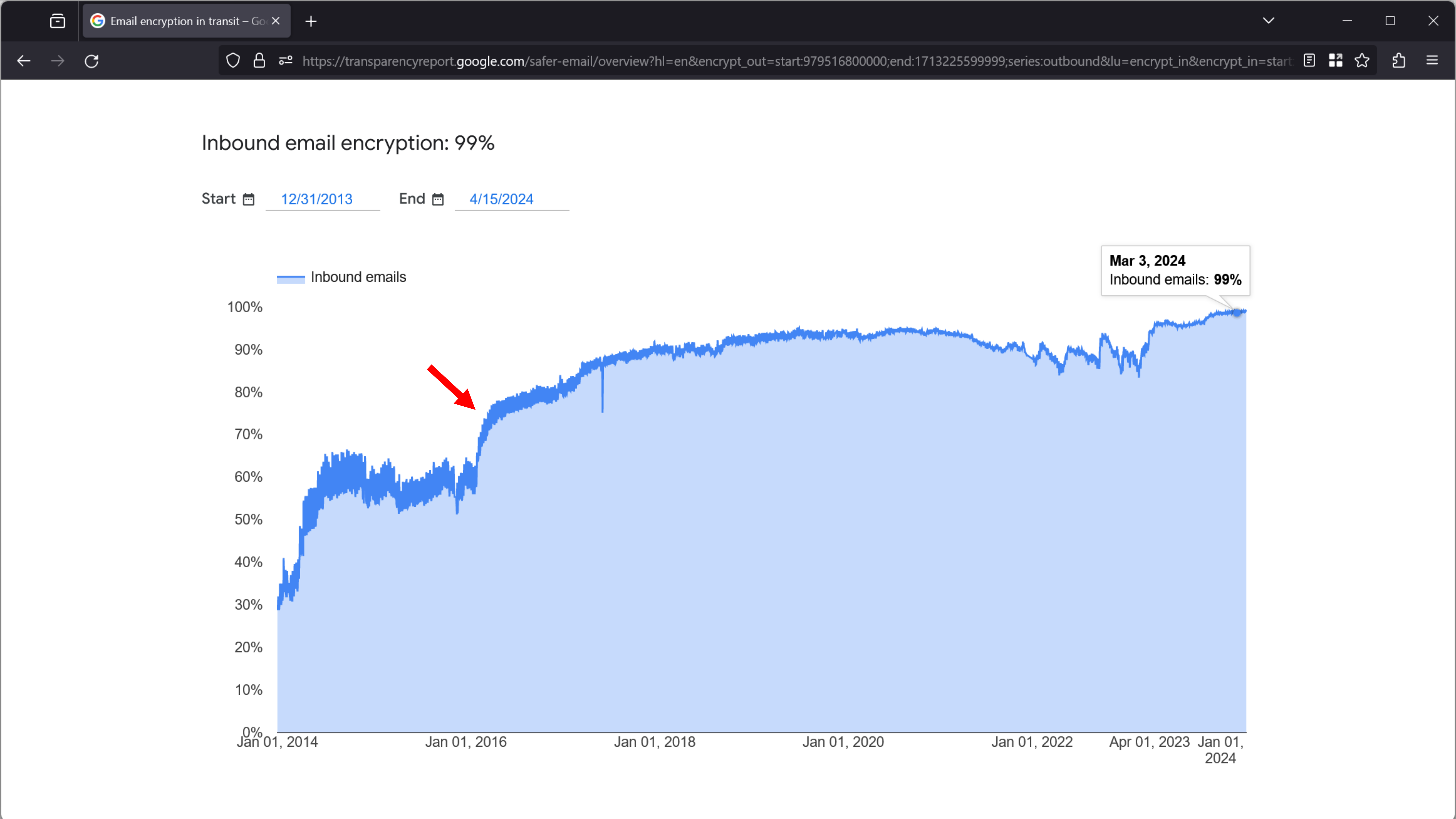
John Doe

Account Information

Hi John,

Here is my account information

© Google - https://googleblog.blogspot.com/2016/02/building-safer-web-for-everyone.html



https://transparencyreport.google.com/safer-email/overview?hl=en&encrypt_out=start:979516800000;end:1713225599999;series:outbound&lu=encrypt_in&encrypt_in=start

Inbound email encryption: 99%

Start 12/31/2013 End 4/15/2024

Defending against MitM

STARTTLS stripping is not the only way to intercept email

DNS MX record poisoning: spoofed MX response

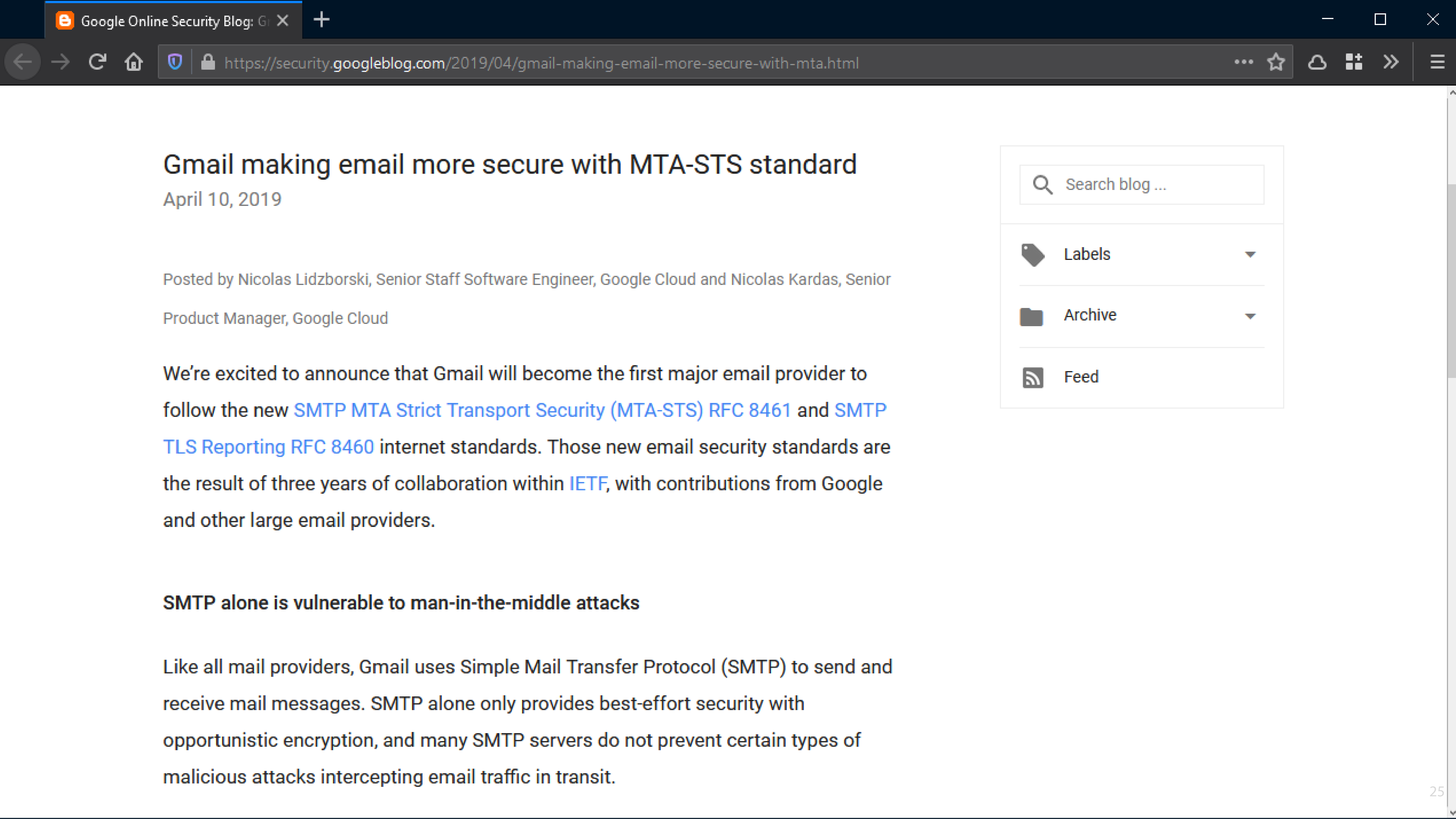
- Compromised name server, MotS DNS poisoning, …
- Messages are diverted through the attacker's mail server

DANE (DNS-based Authentication of Named Entities)

- Allow X.509 certs to be bound to DNS names through DNSSEC
- Provides a way to authenticate TLS clients/servers without a CA
- Enables downgrade-resistant TLS: advertise support for secure SMTP via a TLSA record

MTA-STS (MTA Strict Transport Security – RFC 8461)

- Allows recipient domains to tell senders whether they support TLS, how MTAs should validate certificates, and what to do if TLS negotiation fails
- Client-side policy cache provides TOFU-like protection (similar to HSTS for HTTPS)


Google Online Security Blog: G
https://security.googleblog.com/2019/04/gmail-making-email-more-secure-with-mta.html
Search blog ...
Labels
Archive
Feed

Gmail making email more secure with MTA-STS standard

April 10, 2019

Posted by Nicolas Lidzborski, Senior Staff Software Engineer, Google Cloud and Nicolas Kardas, Senior Product Manager, Google Cloud

We're excited to announce that Gmail will become the first major email provider to follow the new SMTP MTA Strict Transport Security (MTA-STS) RFC 8461 and SMTP TLS Reporting RFC 8460 internet standards. Those new email security standards are the result of three years of collaboration within IETF, with contributions from Google and other large email providers.

SMTP alone is vulnerable to man-in-the-middle attacks

Like all mail providers, Gmail uses Simple Mail Transfer Protocol (SMTP) to send and receive mail messages. SMTP alone only provides best-effort security with opportunistic encryption, and many SMTP servers do not prevent certain types of malicious attacks intercepting email traffic in transit.

I don't like
SPAM!

Spam Sources

Commercial entities

- Legitimate or "gray" businesses, advertisers, …

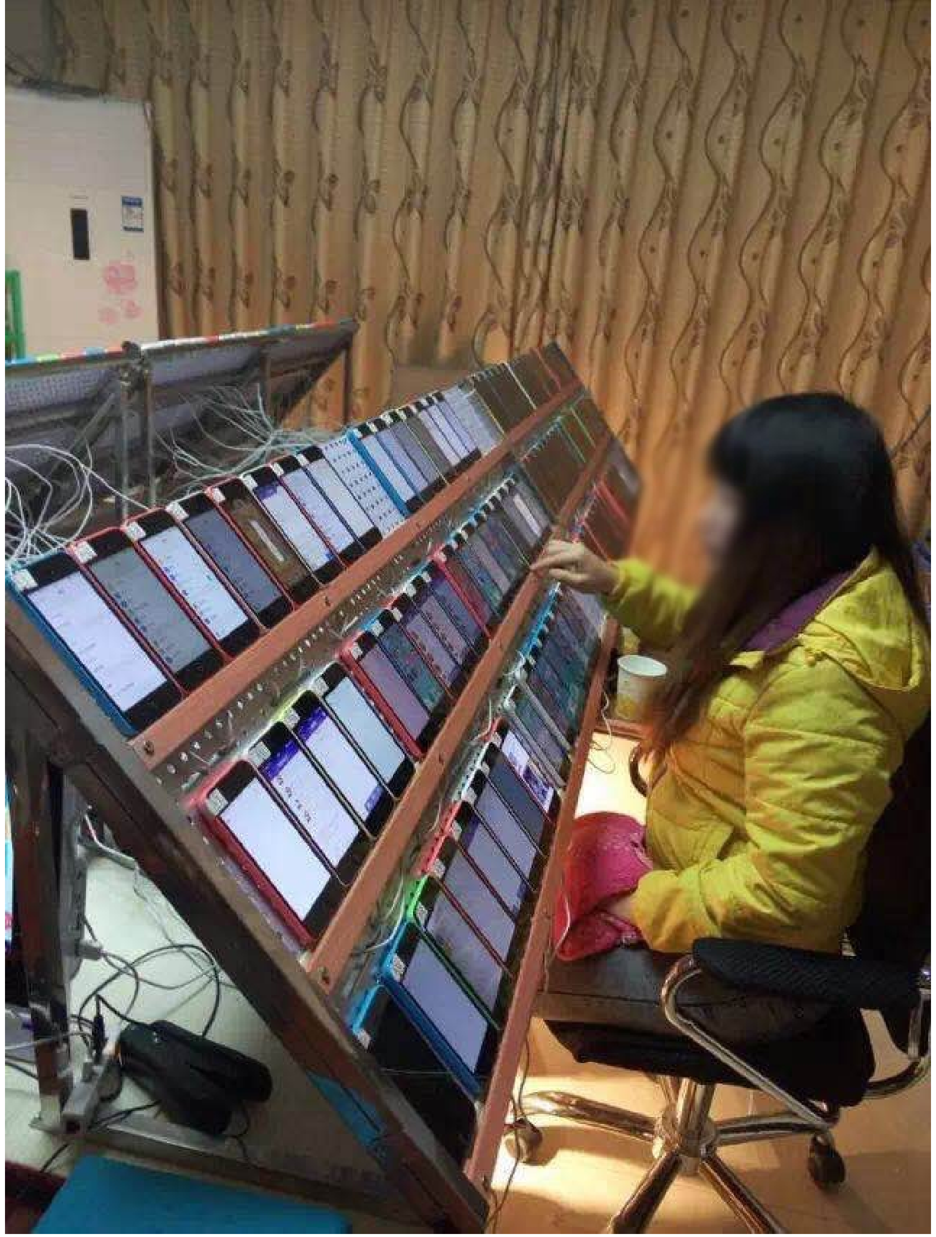
Spammers' own hosts or open relays ➔ easily blocked

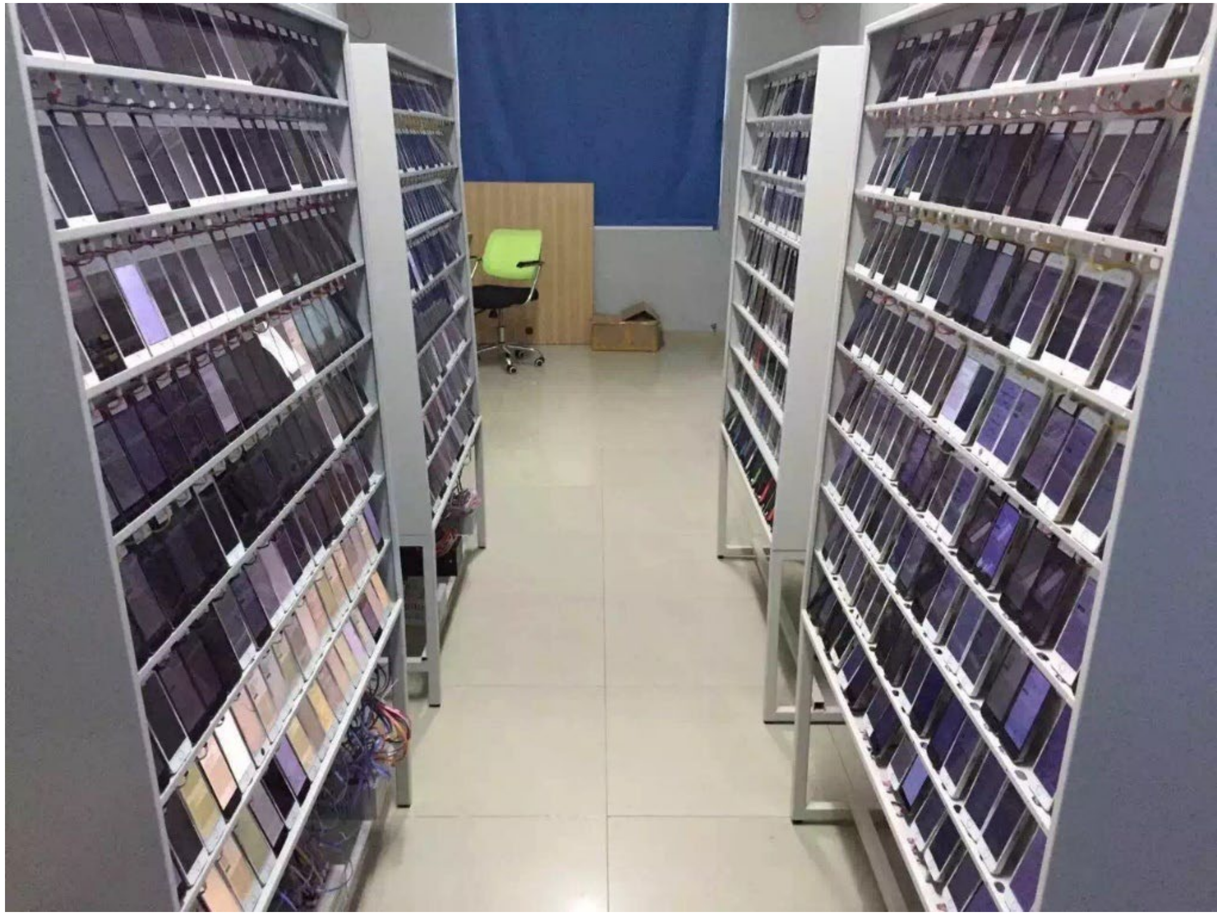
Botnets

- Abuse of ISPs and webmail providers
- Abuse of legitimate user email accounts
- Address harvesting from users' address books

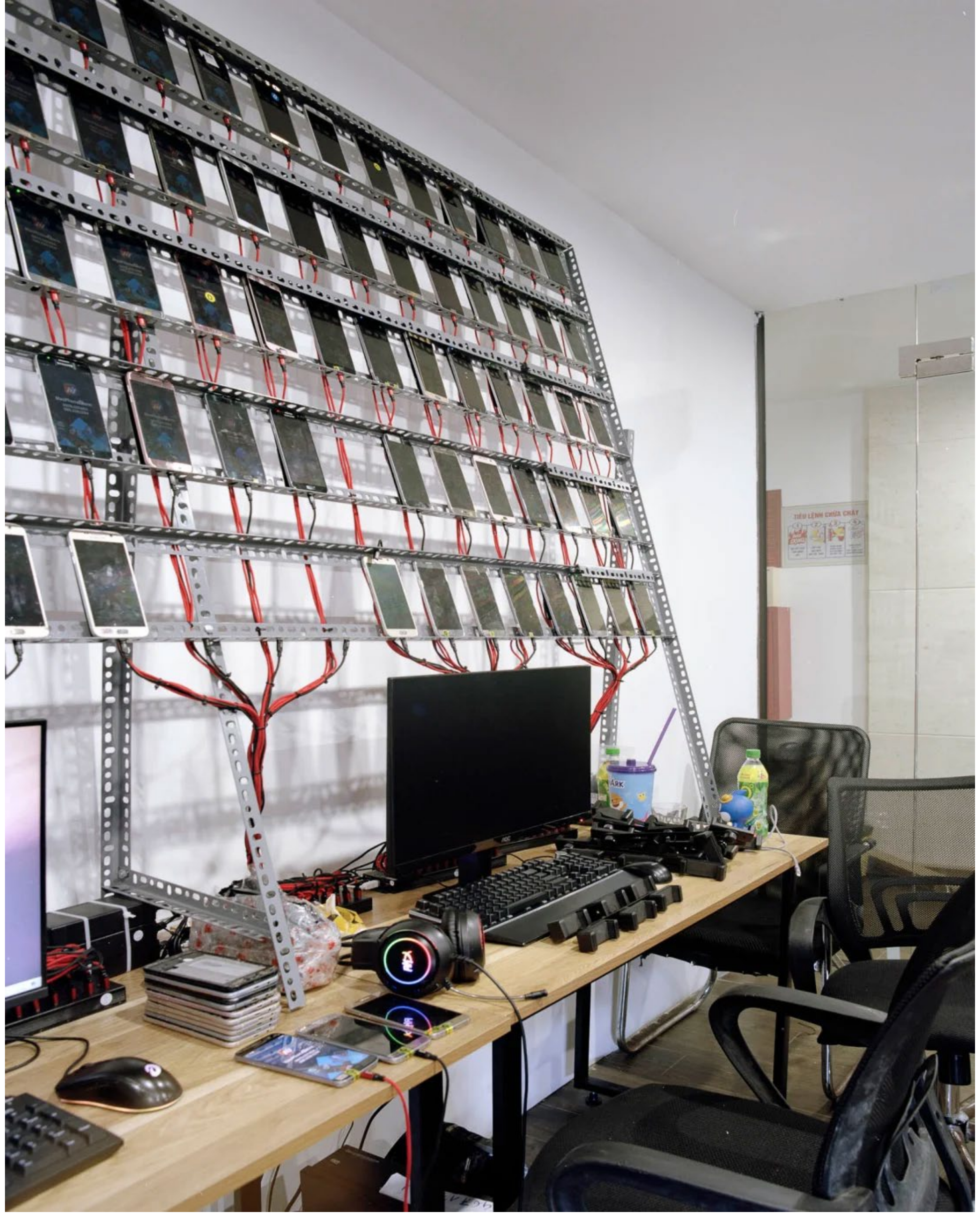
Beyond email

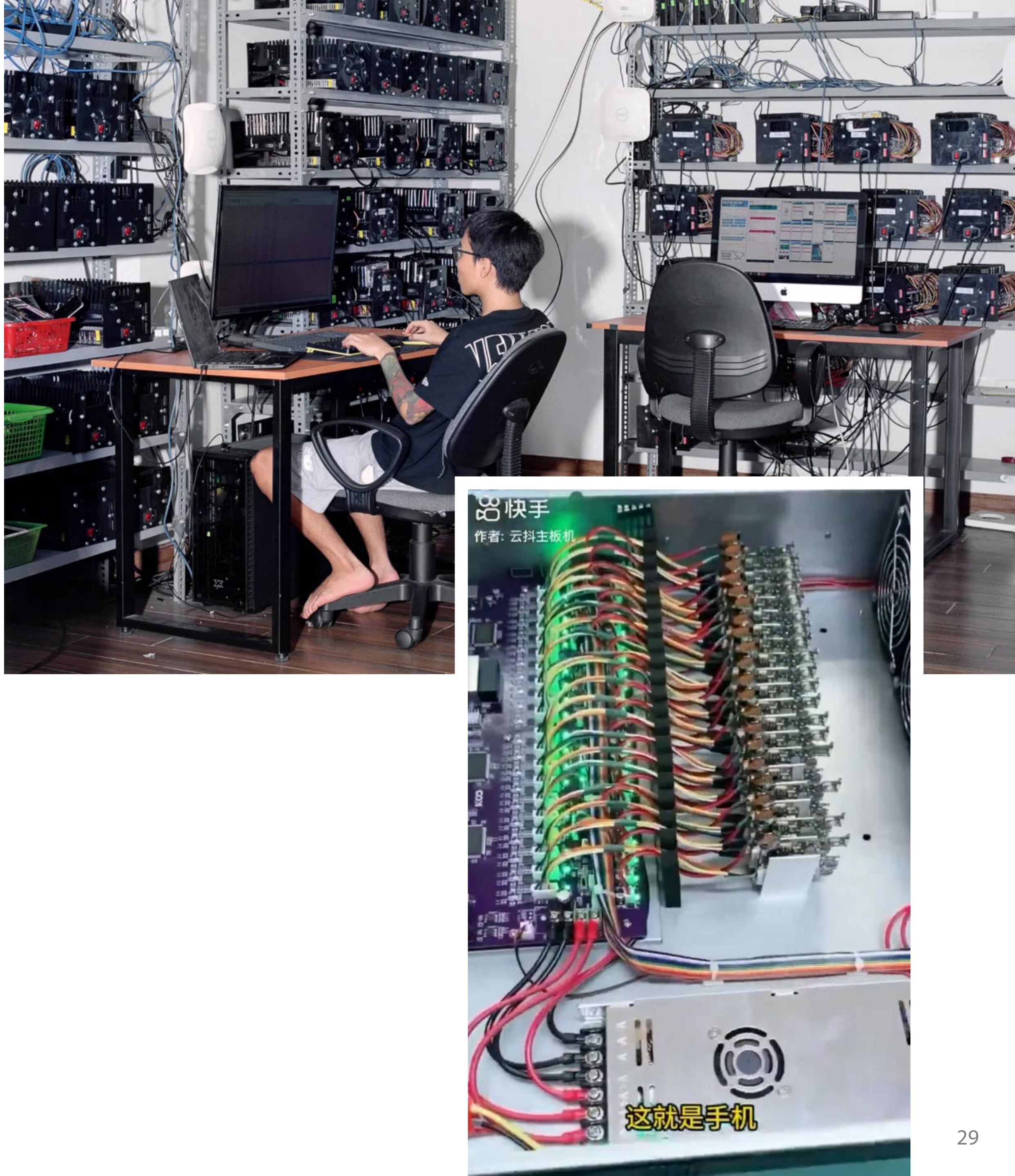
- *Fraudulent messages:* Facebook, Twitter, Yelp, Amazon, online comments, forum messages, Apple/Google Store, …
- *Fraudulent activities:* likes, retweets, clicks, app store rankings, fake reviews, …





© TechInAsia - https://www.techinasia.com/viral-photo-china-shows-manipulate-app-store-rankings-hard
© iFeng - http://tech.ifeng.com/a/20161024/44476050_0.shtml





https://www.cnn.com/style/vietnam-farms-jack-latham-beggars-honey/index.html

Email Spam Lifecycle

Gathering addresses

- Valid, actively used addresses are precious
- Stolen address books, web crawling, black market, …

Message content

- Advertising, 419 scams, fraud, phishing, malware, …
- Anti-spam filter evasion: content obfuscation

Spam email delivery

- Valid accounts: newly created (sweatshops), hijacked ones, …
- Fake social media accounts “primed” over time
- Open relays/proxies (not common anymore)
- Malware: most spam comes from infected machines/botnets

Email Address Protection

Keep it safe from automated address harvesting crawlers

Munging: `username [at] example.com`

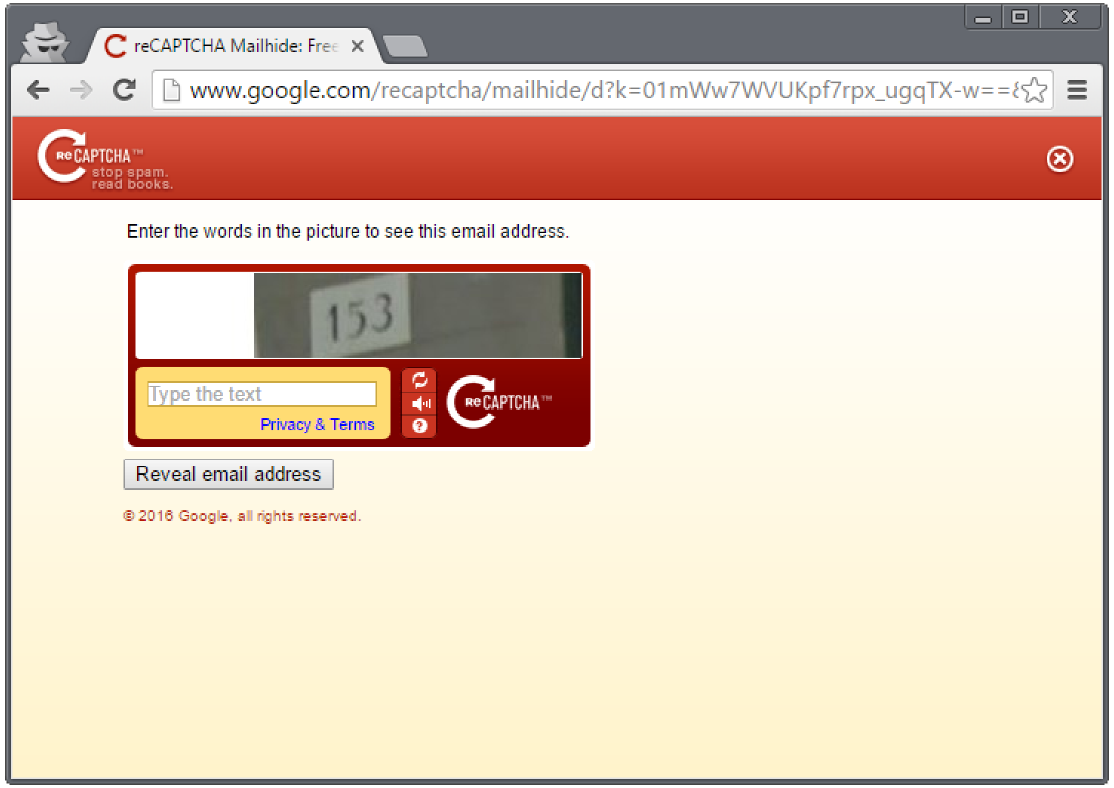
Image instead of text

CAPTCHAs

…

Limited effectiveness

Leaks, breaches, vendors, …



www.google.com/recaptcha/mailhide/d?k=01mWw7WVUKpf7rpx_ugqTX-w==

Enter the words in the picture to see this email address.

© 2016 Google, all rights reserved.

Fighting Spam

Content-based filtering

- False positives vs. false negatives
- Local vs. cloud-based

Block lists

- IPs/domains of known spammers, open relays, zombie machines, hosts that shouldn’t be sending emails (e.g., ISP DHCP pools), …

Honeypots

- Relays, proxies, spamtraps (fake email addresses)

Outbound filtering (block port 25)

- SMTP authentication is now mandatory by most ISPs

Email authentication

Content-based Filtering

Machine learning

- Training with labeled “spam” and “ham” messages
- Feedback from user activities (e.g., “not spam” button)

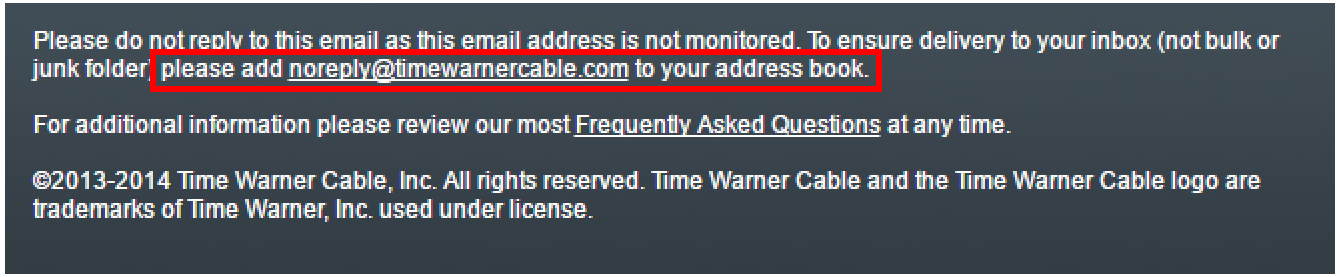
Rule-based systems

- Signatures, regular expressions, patterns, …
- Certain keywords, phrases, unusual text, …
- Example: SpamAssassin

Spam authors try to evade filters

- V1agra, Via'gra, Vi@graa, vi*gra, \/iagra
- Intentional spelling mistakes, symbols, weird punctuation, …
- Continuous arms race
- Example: attackers started using images, defenders started using OCR

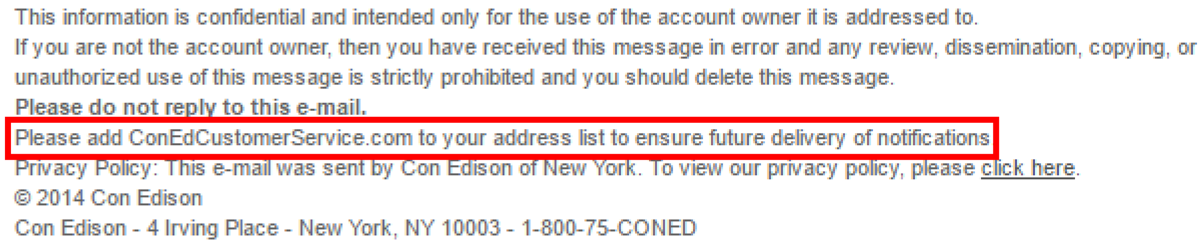
False positives are a challenging problem



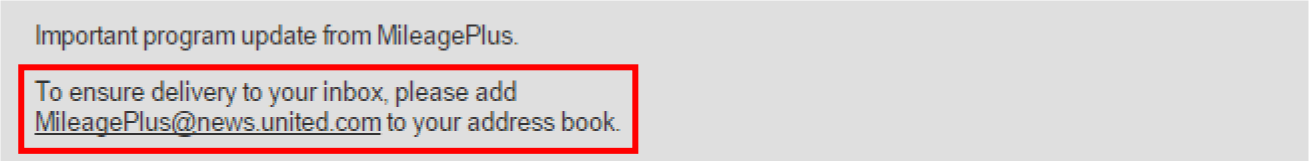
Please do not reply to this email as this email address is not monitored. To ensure delivery to your inbox (not bulk or junk folder) please add noreply@timewarnercable.com to your address book.

For additional information please review our most Frequently Asked Questions at any time.

©2013-2014 Time Warner Cable, Inc. All rights reserved. Time Warner Cable and the Time Warner Cable logo are trademarks of Time Warner, Inc. used under license.



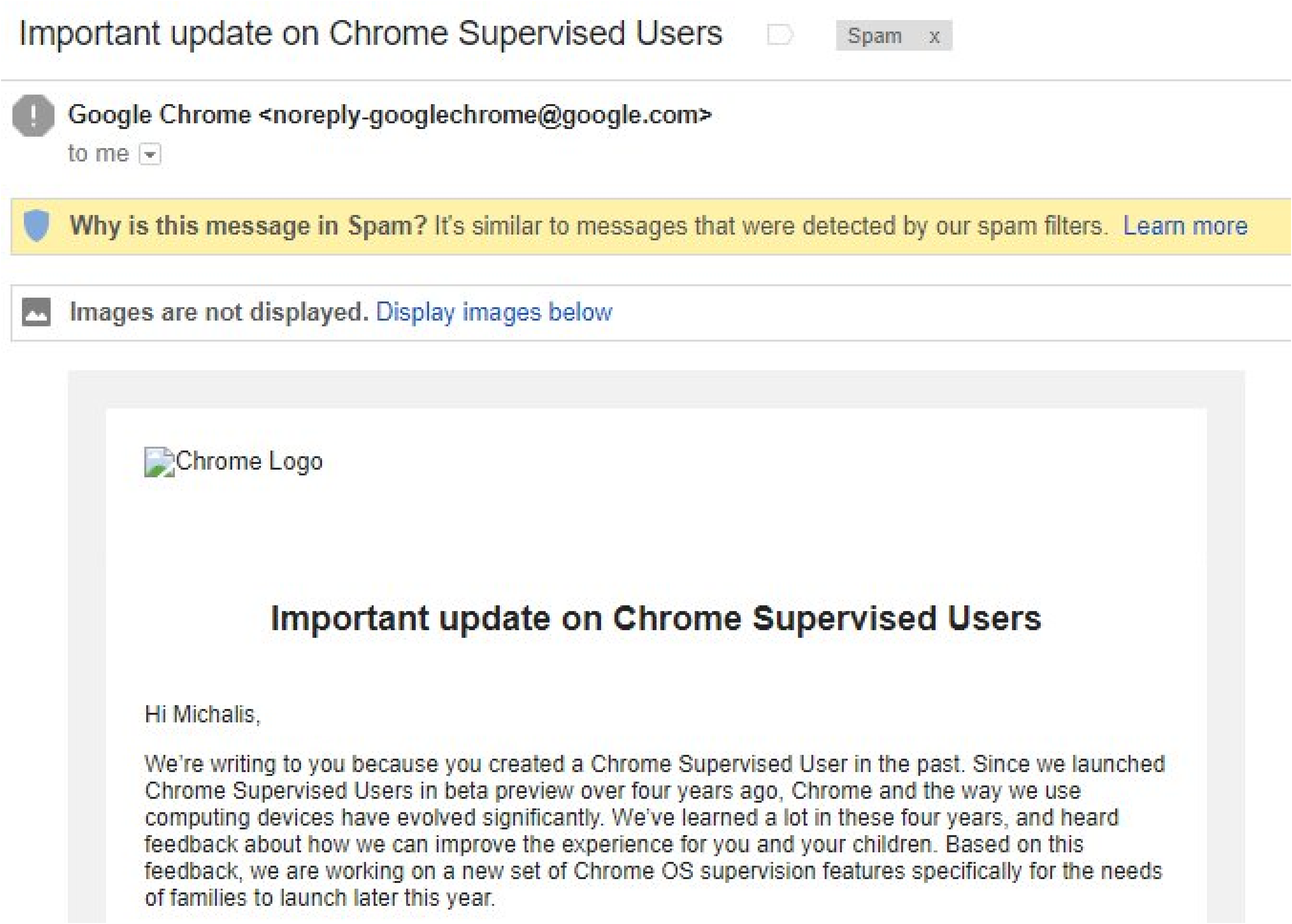
This information is confidential and intended only for the use of the account owner it is addressed to.
If you are not the account owner, then you have received this message in error and any review, dissemination, copying, or unauthorized use of this message is strictly prohibited and you should delete this message.
Please do not reply to this e-mail.
Please add ConEdCustomerService.com to your address list to ensure future delivery of notifications
Privacy Policy: This e-mail was sent by Con Edison of New York. To view our privacy policy, please click here.
© 2014 Con Edison
Con Edison - 4 Irving Place - New York, NY 10003 - 1-800-75-CONED



Important program update from MileagePlus.

To ensure delivery to your inbox, please add MileagePlus@news.united.com to your address book.

Personal example: Google's own message classified as spam by Gmail



Important update on Chrome Supervised Users

Google Chrome <noreply-googlechrome@google.com>

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

Images are not displayed. Display images below

Important update on Chrome Supervised Users

Hi Michalis,

We're writing to you because you created a Chrome Supervised User in the past. Since we launched Chrome Supervised Users in beta preview over four years ago, Chrome and the way we use computing devices have evolved significantly. We've learned a lot in these four years, and heard feedback about how we can improve the experience for you and your children. Based on this feedback, we are working on a new set of Chrome OS supervision features specifically for the needs of families to launch later this year.

https://twitter.com/polychronakis/status/950873453648850944

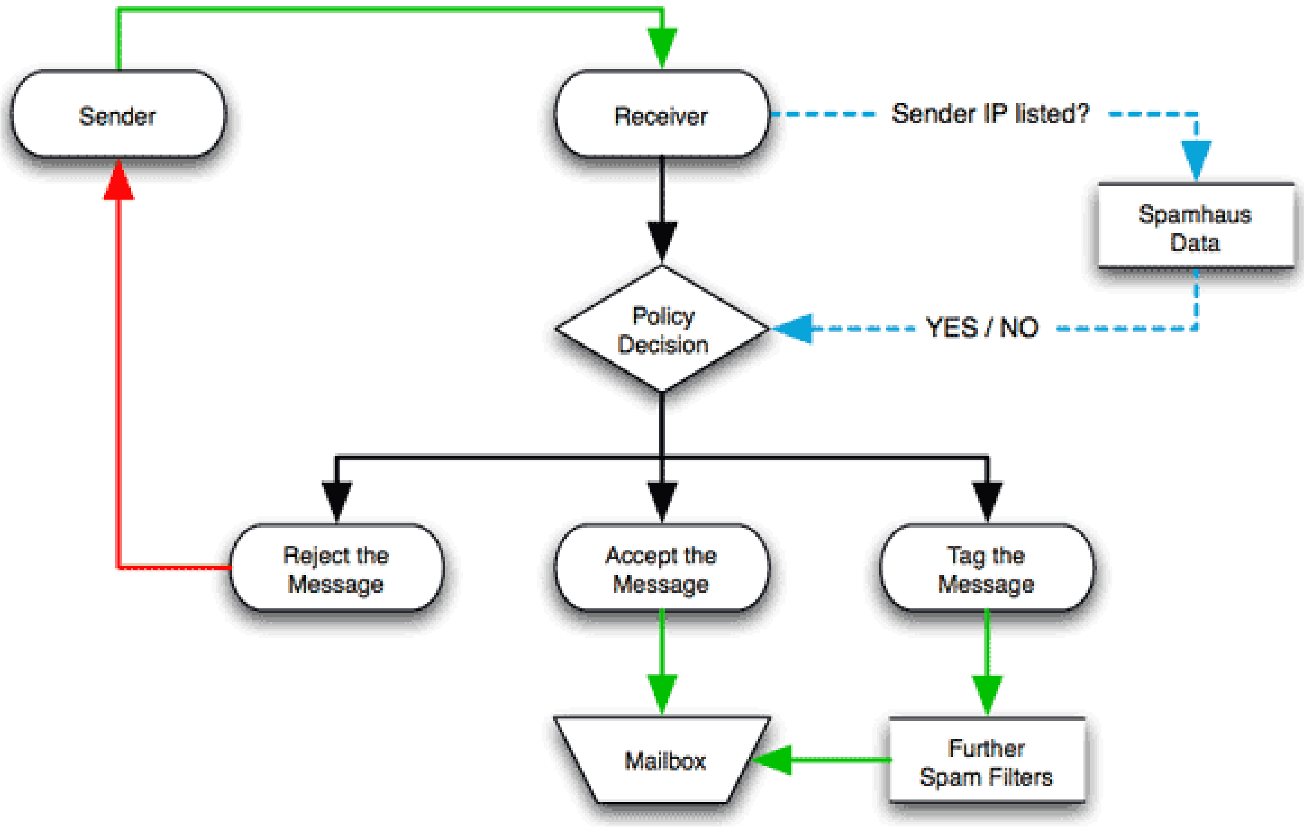
DNSBL Filtering

DNS Block List

- DB queried by mail servers to check the reputation of the origin of incoming email
- IP addresses, domain names, and other information compiled as a DNS zone

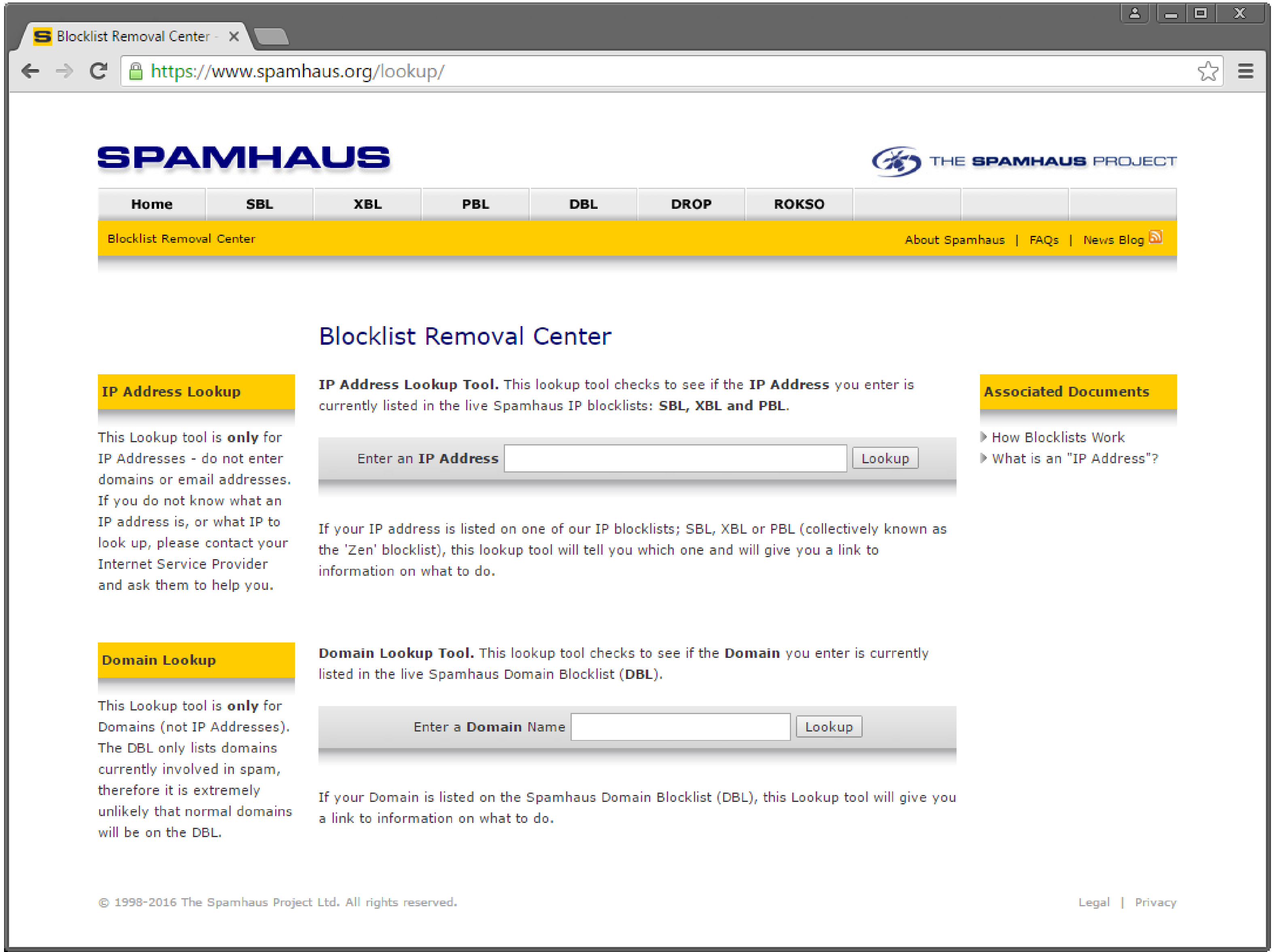
DNS-based

- Easy to query
- Light on bandwidth/resources



© Spamhaus - https://www.spamhaus.org/whitepapers/dnsbl_function/

False positives, IP addresses change owners, …


Blocklist Removal Center -
https://www.spamhaus.org/lookup/
SPAMHAUS
THE SPAMHAUS PROJECT
Home
SBL
XBL
PBL
DBL
DROP
ROKSO
Blocklist Removal Center
About Spamhaus | FAQs | News Blog
Lookup
Lookup

Blocklist Removal Center

IP Address Lookup

This Lookup tool is **only** for IP Addresses - do not enter domains or email addresses. If you do not know what an IP address is, or what IP to look up, please contact your Internet Service Provider and ask them to help you.

IP Address Lookup Tool. This lookup tool checks to see if the **IP Address** you enter is currently listed in the live Spamhaus IP blocklists: **SBL, XBL and PBL**.

Enter an **IP Address**

If your IP address is listed on one of our IP blocklists; SBL, XBL or PBL (collectively known as the 'Zen' blocklist), this lookup tool will tell you which one and will give you a link to information on what to do.

Associated Documents

- How Blocklists Work
- What is an "IP Address"?

Domain Lookup

This Lookup tool is **only** for Domains (not IP Addresses). The DBL only lists domains currently involved in spam, therefore it is extremely unlikely that normal domains will be on the DBL.

Domain Lookup Tool. This lookup tool checks to see if the **Domain** you enter is currently listed in the live Spamhaus Domain Blocklist (**DBL**).

Enter a **Domain** Name

If your Domain is listed on the Spamhaus Domain Blocklist (DBL), this Lookup tool will give you a link to information on what to do.

© 1998-2016 The Spamhaus Project Ltd. All rights reserved.

Legal | Privacy

SPF: Origin Authentication

SMTP allows anyone to send an email with an arbitrary "From" address

- "Envelop" sender: domain included in `HELO` and `MAIL FROM` commands

Sender Policy Framework (SPF)

- DNS TXT record pointing to the *hosts* that are allowed to send email from the domain
- Receiving SMTP servers compare the IP address attempting to send an email with the allowed (by SPF) addresses of the domain provided in the SMTP envelope
- Helps block spam at it source: cannot send spoofed emails from non-authorized IPs

```
mikepo@styx:~> dig google.com TXT
;; ANSWER SECTION:
google.com.           3599    IN      TXT     "v=spf1 include:_spf.google.com ~all"
```

DKIM: Email Validation

DomainKeys Identified Mail (DKIM): digitally sign some email headers and message body

Allows the recipient to verify that

- The message is sent from the domain it claims to be sent from
- The message has not been tampered with

Domain’s public key is stored in a DNS TXT record

```
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20161025;
h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
bh=0BSnrwLTQ7KblIwINxoPJN40a/K5PZCIV8atL6a1Dvg=;
b=Nch9yEorgibAjkh90ukDL6SU0FYn70qP6AMsWFfpLO+W3iroMoVdKIjKk8Cv6Gc1TW ...

mikepo@styx:~> dig 20161025._domainkey.1e100.net TXT
;; ANSWER SECTION:
20161025._domainkey.1e100.net. 21599 IN TXT     "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnOv6+Txyz+SEc7mT719QQtOj6g2MjpErYUGVrRGGc7f5rmE...
```

SPF + DKIM = DMARC

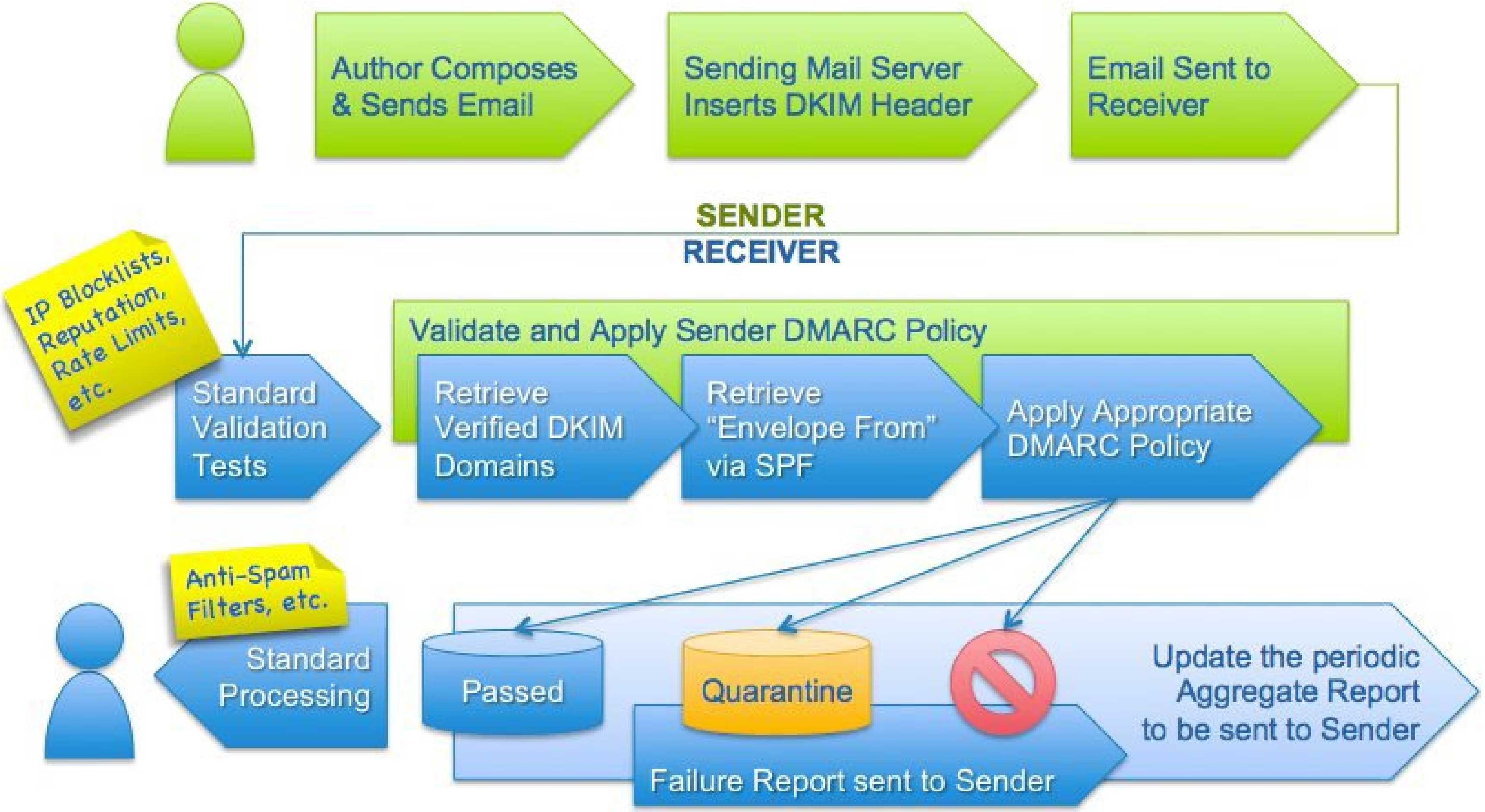
Domain-based Message Authentication, Reporting, and Conformance

- Standardizes how email receivers perform email authentication using SPF and DKIM
- Tells receivers what to do if neither of those authentication methods passes (possible actions: mark as junk, or reject the message)

DMARC policies are published as DNS TXT records

```
mikepo@styx:~> dig _dmarc.google.com TXT
;; ANSWER SECTION:
_dmarc.google.com.      299     IN      TXT     "v=DMARC1; p=reject;
rua=mailto:mailauth-reports@google.com"
```

DMARC Email Authentication Process



Author Composes & Sends Email

Sending Mail Server Inserts DKIM Header

Email Sent to Receiver

SENDER

RECEIVER

IP Blocklists, Reputation, Rate Limits, etc.

Standard Validation Tests

Validate and Apply Sender DMARC Policy

Retrieve Verified DKIM Domains

Retrieve "Envelope From" via SPF

Apply Appropriate DMARC Policy

Anti-Spam Filters, etc.

Standard Processing

Passed

Quarantine

Update the periodic Aggregate Report to be sent to Sender

Failure Report sent to Sender

http://dmarc.org/overview/

Recap: SPF, DKIM, DMARC

SPF validates MAIL FROM vs. its source server (“envelope” information)

- Prevents spammers from sending email on behalf of a domain from other IP addresses

DKIM cryptographically signs a message’s headers and body

- Ensures a message from a specific domain was indeed authorized by the owner of that domain
- Ensures the message content is authentic and has not been altered in transit

DMARC specifies how emails that fail SPF+DKIM should be treated

- Do nothing (just log), quarantine (place into spam/junk folder), reject

Not effective against spammers who

- Use their own domains
- Use legitimate email services (e.g., Gmail)
- Are legitimate users of (or have access to) the same domain as the victim

Good for allowlisting/verifying email from trusted sources (.gov, banks, …)

End-to-End Email Encryption

Two major standards: **PGP** and **S/MIME** (similar, but incompatible)

- Both rely on public key cryptography
- Both support signing and/or encryption
- Main difference: *how certificates are signed*

Typical workflow

- Encrypt message with a random symmetric key
- Encrypt symmetric key with the public key(s) of recipient(s)
- Digitally sign a hash of the message

Metadata still in the clear (!)

- Email headers, appended "Received:" records, subject line

Pretty Good Privacy

De facto standard for encrypted email

PGP (Phil Zimmermann) ➔ OpenPGP (RFC 4880)

- Gnu Privacy Guard (GPG): GPL implementation

Authentication

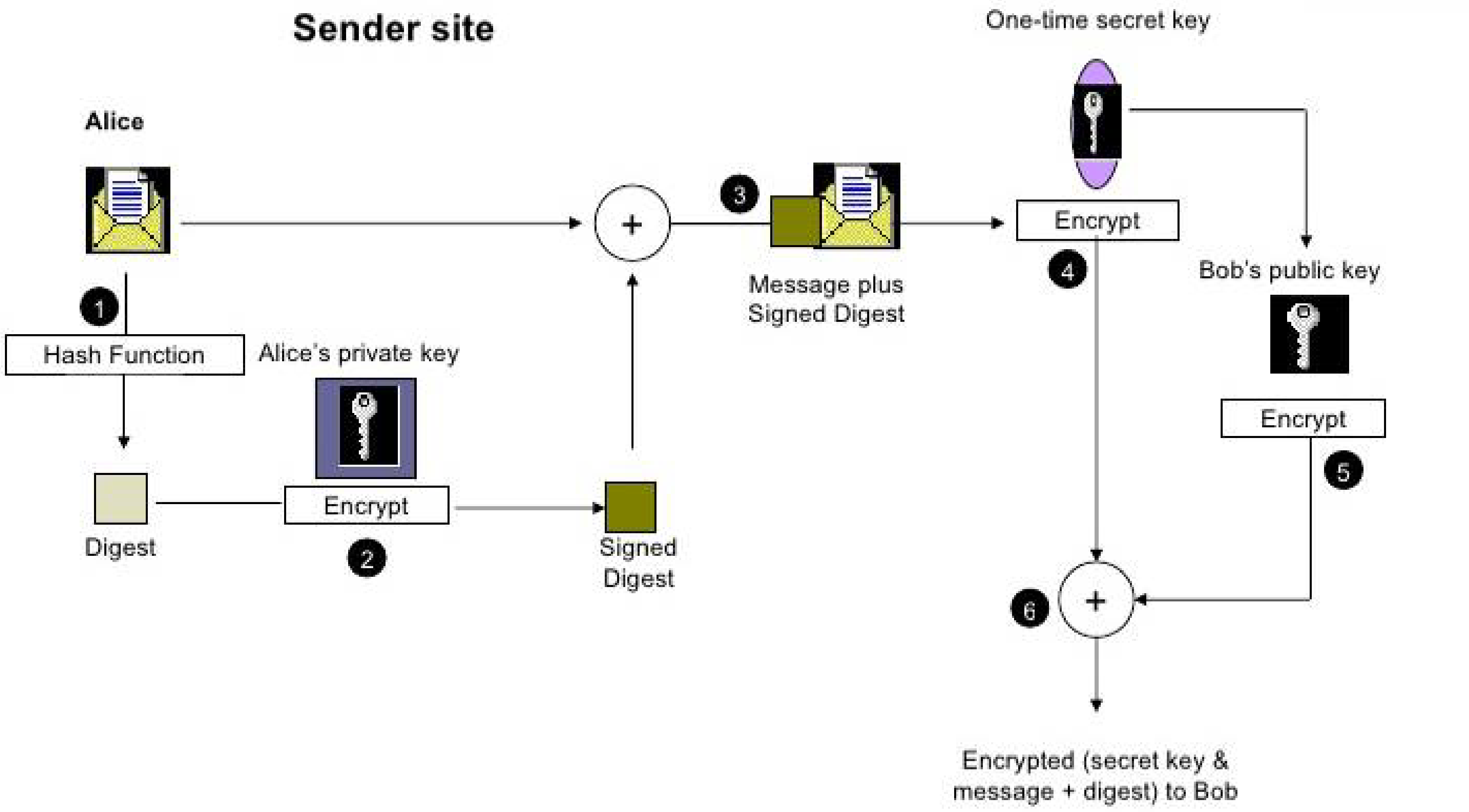
- Senders attach their digital signature to the message
- Receivers verify the signature using public-key cryptography

Confidentiality

- Symmetric key encryption
- Random session key generated for each message
- Session key is encrypted with recipient's public key

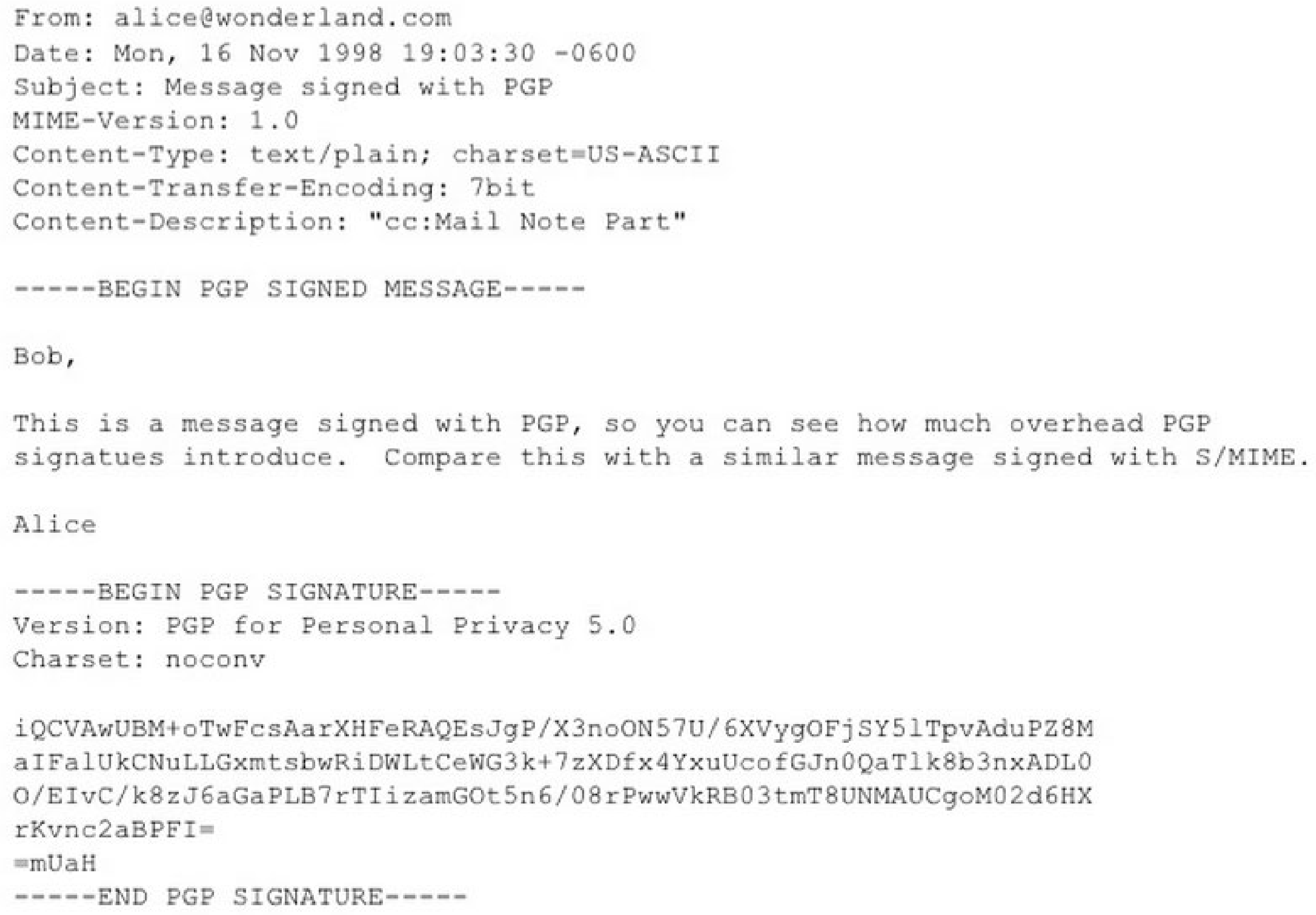
Both are typically used on the same message

PGP Encryption



http://www.slideshare.net/rvenkatesh25/network-security-primer

PGP Signed Message Example



```
From: alice@wonderland.com
Date: Mon, 16 Nov 1998 19:03:30 -0600
Subject: Message signed with PGP
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit
Content-Description: "cc:Mail Note Part"

-----BEGIN PGP SIGNED MESSAGE-----

Bob,

This is a message signed with PGP, so you can see how much overhead PGP
signatues introduce.  Compare this with a similar message signed with S/MIME.

Alice

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQCVAwUBM+oTwFcsAarXHFeRAQEsJgP/X3noON57U/6XVygOFjSY5lTpvAduPZ8M
aIFalUkCNuLLGxmtsbwRiDWLtCeWG3k+7zXDfx4YxuUcofGJn0QaTlk8b3nxADL0
O/EIvC/k8zJ6aGaPLB7rTIizamGOt5n6/08rPwwVkRB03tmT8UNMAUCgoM02d6HX
rKvnc2aBPFI=
=mUaH
-----END PGP SIGNATURE-----
```

http://www.slideshare.net/rvenkatesh25/network-security-primer

PGP Additional Features

Compression

Sign ➔ Compress ➔ Encrypt

Compression after encryption is pointless (no redundancy)

Signature does not depend on the compression algorithm

Email Compatibility

Ciphertext contains arbitrary 8-bit octects

Some email systems may interpret some of them as control commands

Solution: base64 encoding (33% space overhead)

Segmentation

Transparent message segmentation and reassembly for very large messages

Segments mailed separately

Encrypted Email: Two Main Challenges

Public key authenticity

Assurance that a public key is correct and belongs to the person or entity claimed

- Ensure it has not been tampered with or replaced by an attacker

Public key discovery

How can we find the public key of a person/entity?

- Especially the very first time we need to contact them

PGP: Web of Trust

Entirely decentralized authentication

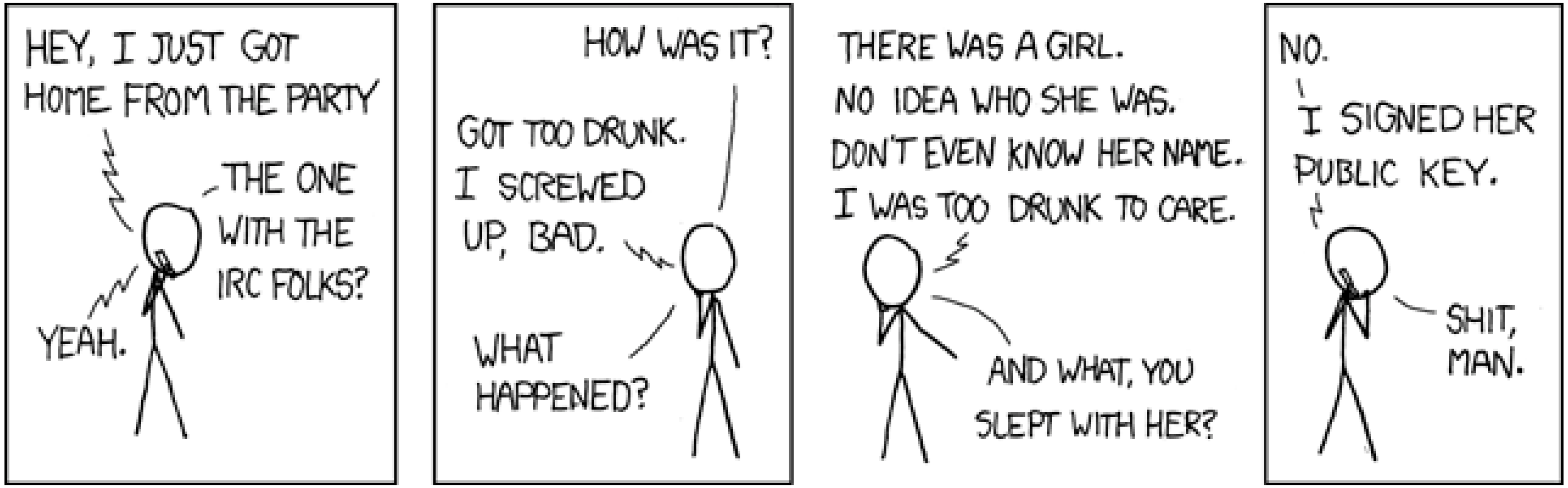
- No need to buy certs from CAs: users create their own certificates

Users validate other users' certificates, forming a "web of trust"

- No trusted authorities: trust is established through friends *(yay! key signing parties!)*

Main problems

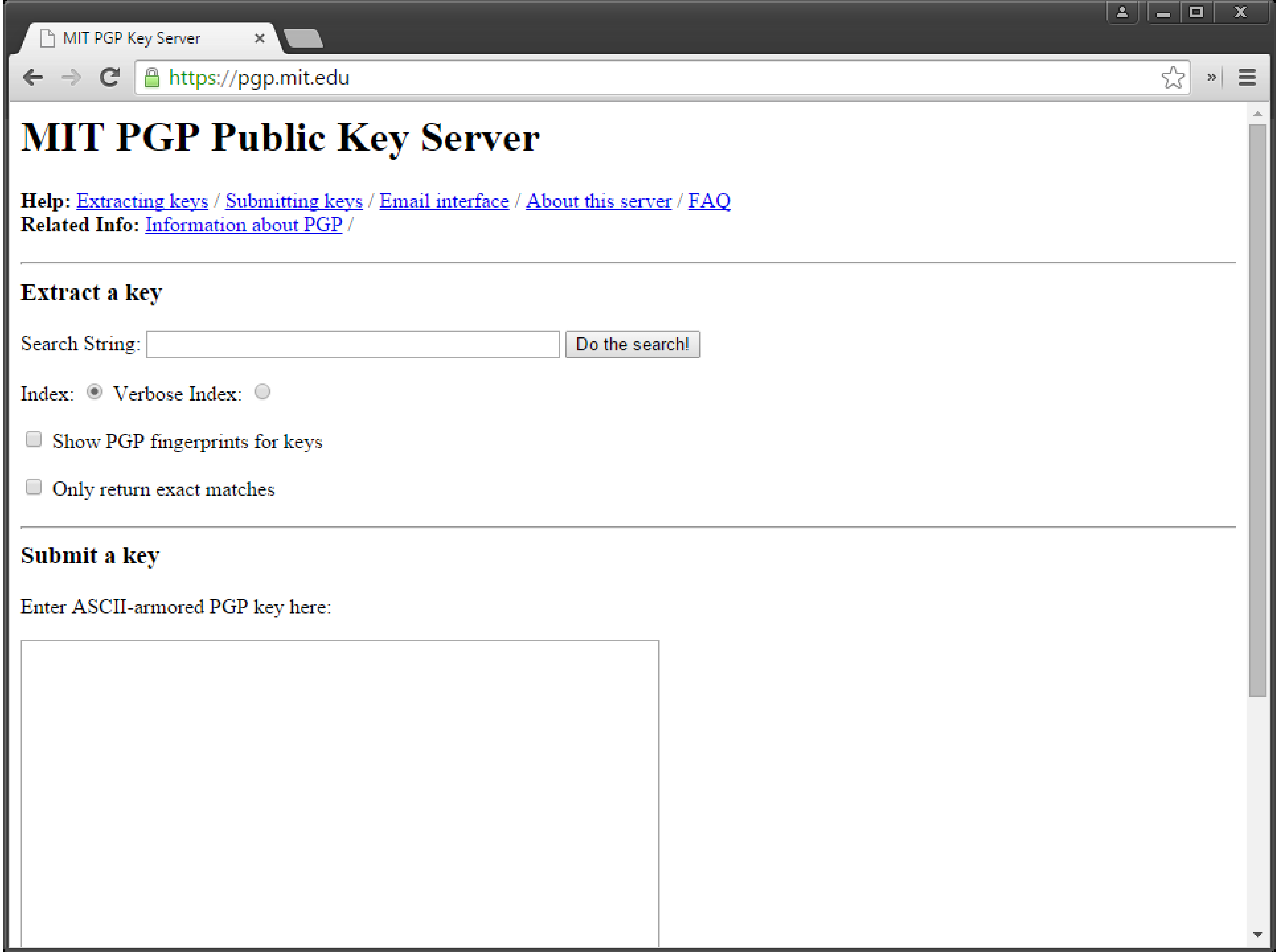
- Privacy issues: social graph metadata
- Bootstrapping: new users are not readily trusted by others
- When opinions vary, "stronger set" wins: impersonation through collusion/compromised keys
- Scalability: WoT for the whole world?


HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

https://xkcd.com/364/

Finding Public Keys

- Public PGP key servers
  - pgp.mit.edu
  - keyserver.pgp.com
- Cache certificates from received emails
- Integration with user management systems (LDAP)
- Ad-hoc approaches
  - List public key on home page
  - Print on business card
  - Exchange through another medium on a case-by-case basis
- Association with social profiles/identities
  - keybase.io



MIT PGP Public Key Server

Help: Extracting keys / Submitting keys / Email interface / About this server / FAQ
Related Info: Information about PGP /

Extract a key

Search String: [ ] Do the search!

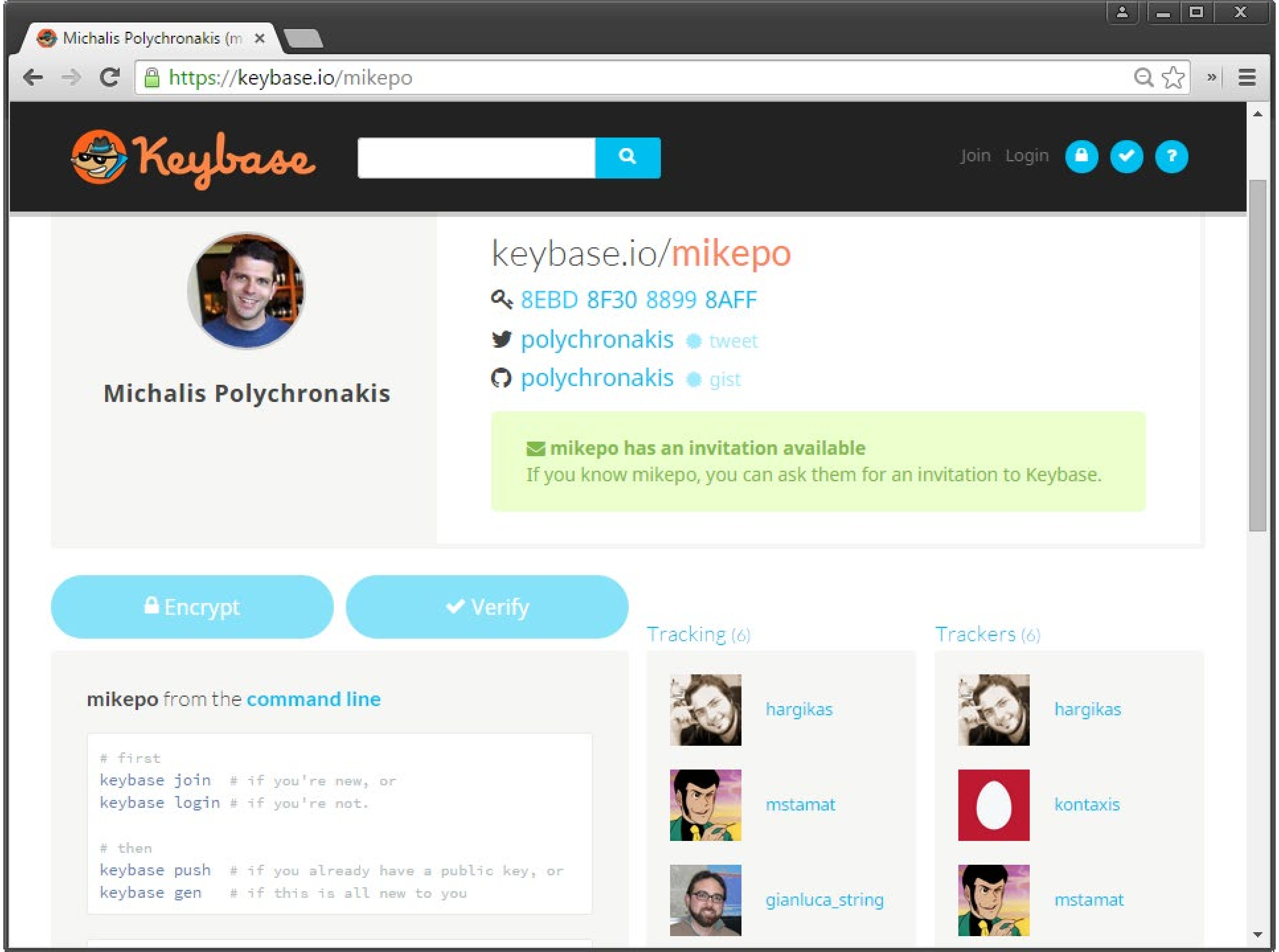
Index: ● Verbose Index: ○

□ Show PGP fingerprints for keys

□ Only return exact matches

Submit a key

Enter ASCII-armored PGP key here:



keybase.io/mikepo

8EBD 8F30 8899 8AFF

polychronakis tweet

polychronakis gist

Michalis Polychronakis

mikepo has an invitation available
If you know mikepo, you can ask them for an invitation to Keybase.

mikepo from the **command line**

```
# first
keybase join  # if you're new, or
keybase login # if you're not.

# then
keybase push  # if you already have a public key, or
keybase gen   # if this is all new to you
```

Tracking (6)	Trackers (6)
hargikas	hargikas
mstamat	kontaxis
gianluca_string	mstamat

Keybase.io

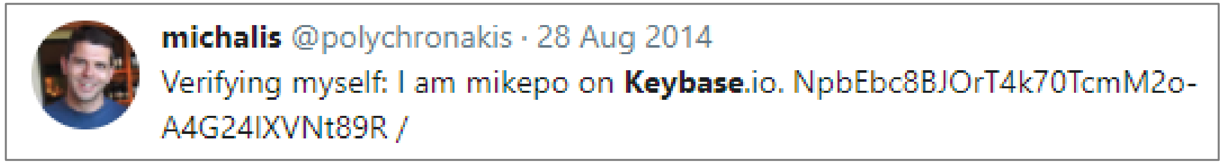
In essence, a directory associating public keys with names

Identity established through *public signatures*

- **Identity proofs**: *"I am Joe on Keybase and MrJoe on Twitter"*
- **Follower statements**: *"I am Joe on Keybase and I just looked at Chris's identity"*
- **Key ownership**: *"I am Joe on Keybase and here's my public key"*
- **Revocations**: *"I take back what I said earlier"*

Keybase identity = sum of public identities

- Twitter, Facebook, Github, Reddit, domain ownership, …



michalis @polychronakis · 28 Aug 2014
Verifying myself: I am mikepo on **Keybase**.io. NpbEbc8BJOrT4k70TcmM2o-A4G24IXVNt89R /

An attacker has to compromise all connected identities

- The more connected identities, the harder to impersonate a user

Biggest Issue: Usability

Non-trivial setup

PGP: users are responsible for everything

Key management

Key revocation

Public key fingerprints

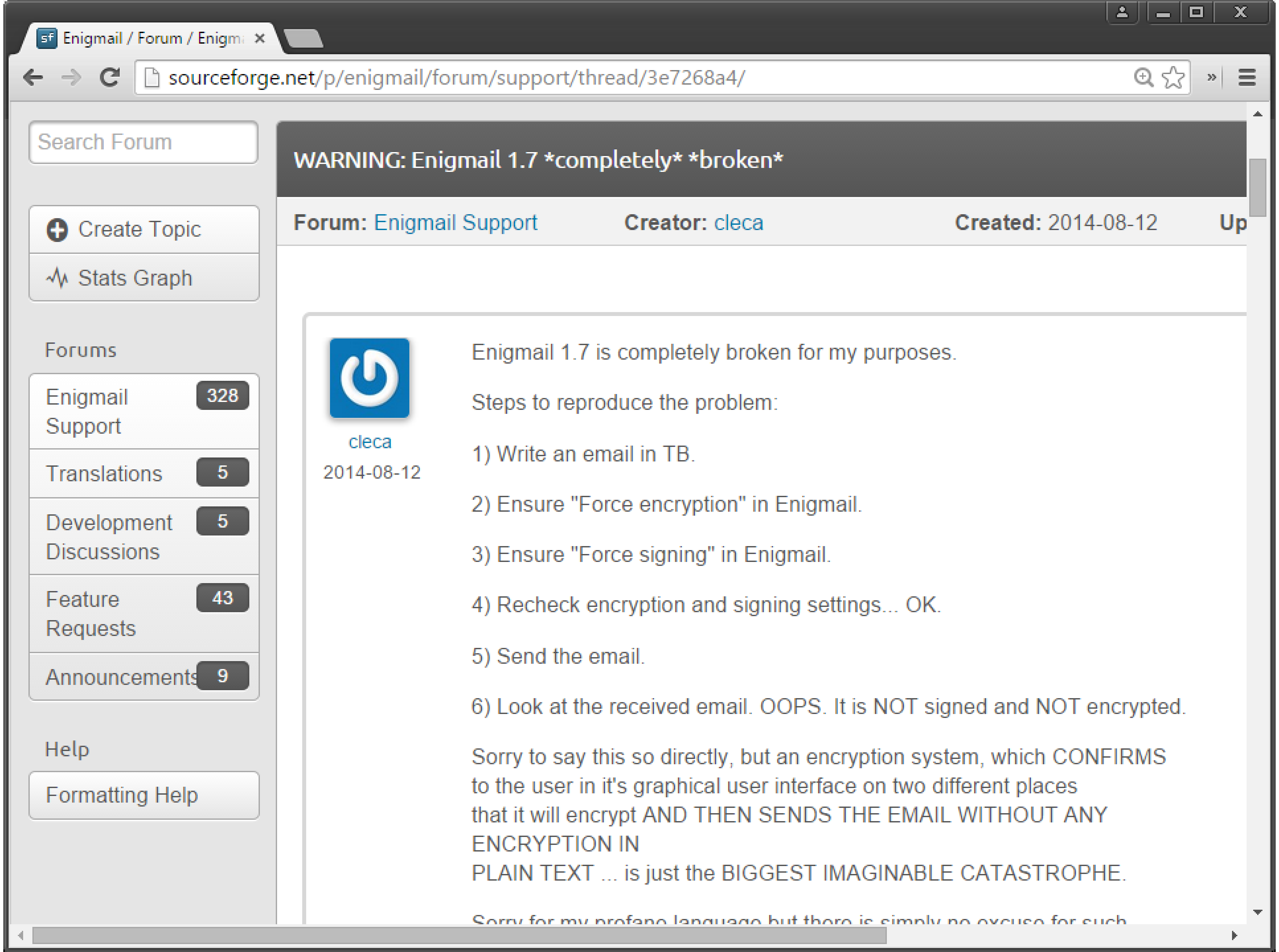
Poor mail client integration

Can lead to catastrophic failures: e.g., Enigmail+Thunderbird silent encryption failure

(Let alone key discovery and trustworthiness issues)

HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP:
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
FIRST OF ALL, THANKS FOR TAKING CARE OF
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

https://xkcd.com/1181/



WARNING: Enigmail 1.7 *completely* *broken*

Forum: Enigmail Support **Creator:** cleca **Created:** 2014-08-12 **Up**

cleca
2014-08-12

Enigmail 1.7 is completely broken for my purposes.

Steps to reproduce the problem:

1) Write an email in TB.

2) Ensure "Force encryption" in Enigmail.

3) Ensure "Force signing" in Enigmail.

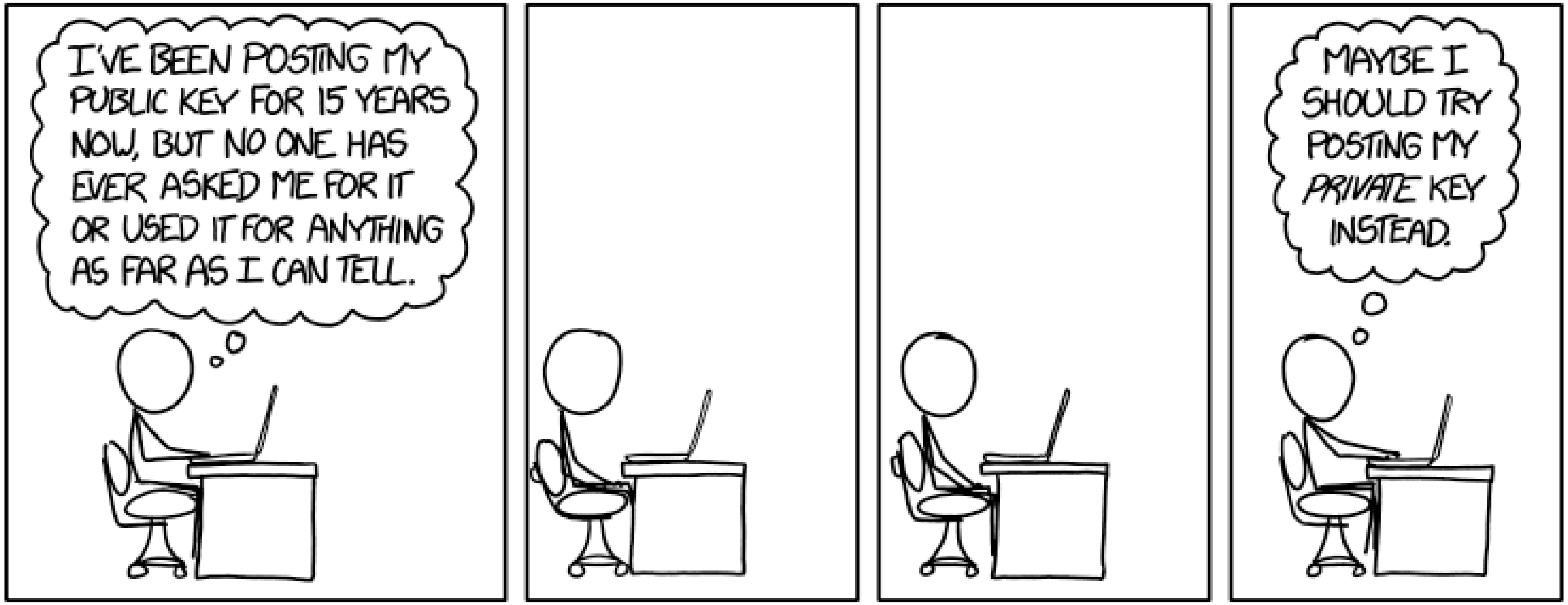
4) Recheck encryption and signing settings... OK.

5) Send the email.

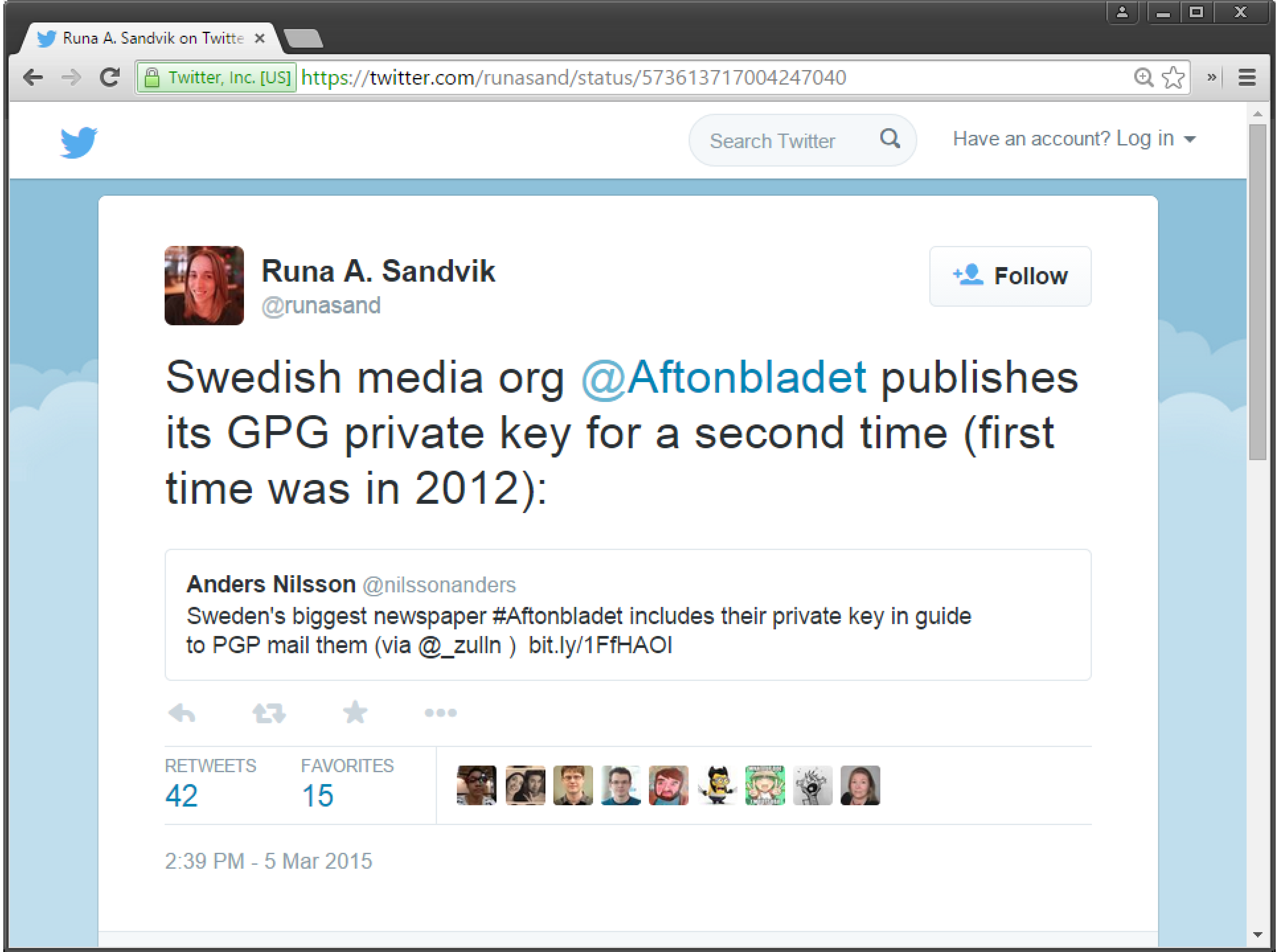
6) Look at the received email. OOPS. It is NOT signed and NOT encrypted.

Sorry to say this so directly, but an encryption system, which CONFIRMS
to the user in it's graphical user interface on two different places
that it will encrypt AND THEN SENDS THE EMAIL WITHOUT ANY ENCRYPTION IN
PLAIN TEXT ... is just the BIGGEST IMAGINABLE CATASTROPHE.

Sorry for my profane language but there is simply no excuse for such


I'VE BEEN POSTING MY PUBLIC KEY FOR 15 YEARS NOW, BUT NO ONE HAS EVER ASKED ME FOR IT OR USED IT FOR ANYTHING AS FAR AS I CAN TELL.
MAYBE I SHOULD TRY POSTING MY *PRIVATE* KEY INSTEAD.

https://xkcd.com/1553/



Runa A. Sandvik on Twitte
Twitter, Inc. [US]
https://twitter.com/runasand/status/573613717004247040
Search Twitter
Have an account? Log in
Follow

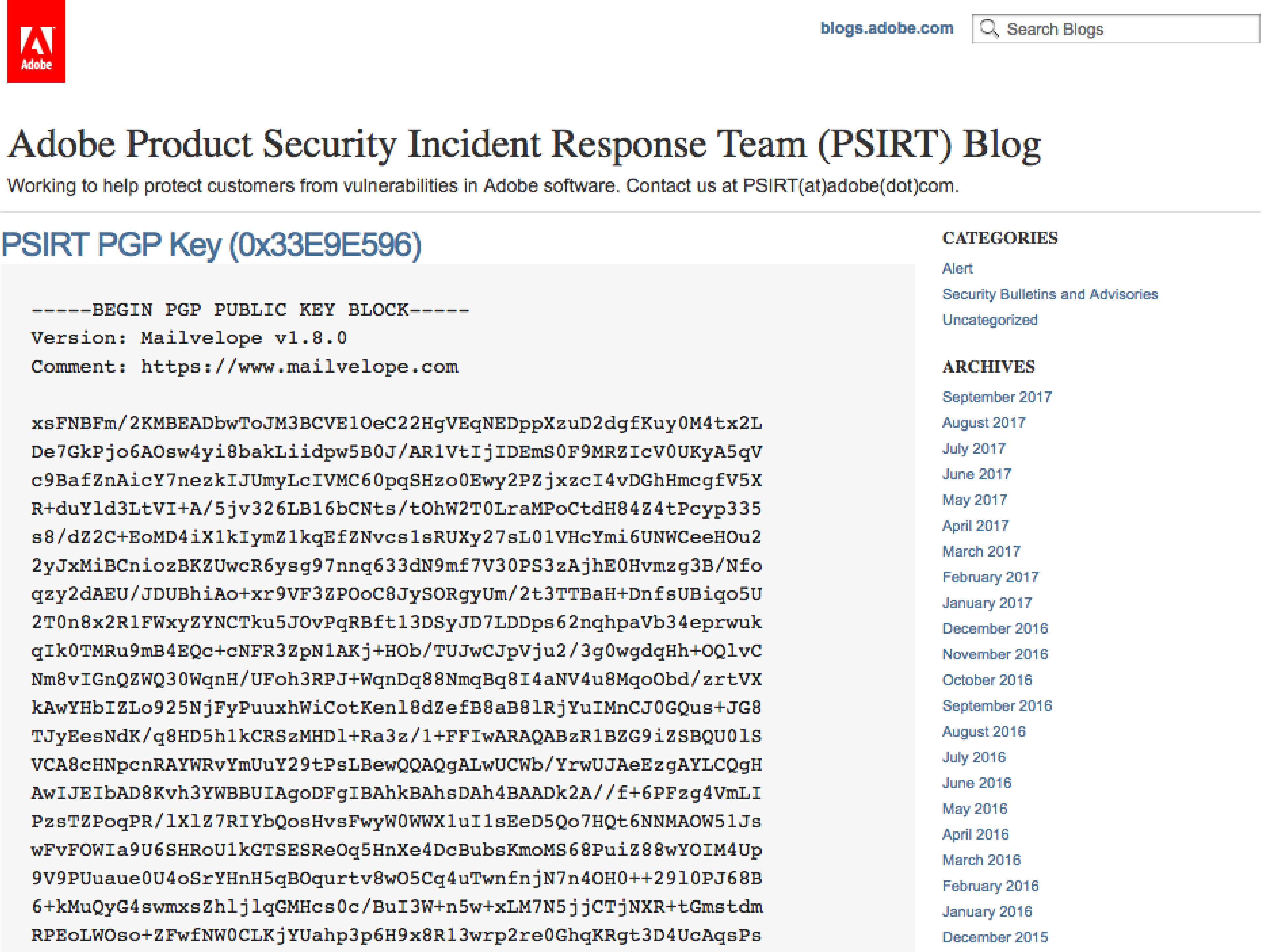
Runa A. Sandvik @runasand

Swedish media org @Aftonbladet publishes its GPG private key for a second time (first time was in 2012):

Anders Nilsson @nilssonanders
Sweden's biggest newspaper #Aftonbladet includes their private key in guide to PGP mail them (via @_zulln) bit.ly/1FfHAOI

RETWEETS 42 FAVORITES 15

2:39 PM - 5 Mar 2015



Adobe Product Security Incident Response Team (PSIRT) Blog

Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT(at)adobe(dot)com.

PSIRT PGP Key (0x33E9E596)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xsFNBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmqBq8I4aNV4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB8lRjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHDl+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPsLBewQQAQgALwUCWb/YrwUJAeEzgAYLCQgH
AwIJEIbAD8Kvh3YWBBUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lX1Z7RIYbQosHvsFwyW0WWX1uI1sEeD5Qo7HQt6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhljlqGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLWOso+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UcAqsPs
```

CATEGORIES

- Alert
- Security Bulletins and Advisories
- Uncategorized

ARCHIVES

- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- December 2016
- November 2016
- October 2016
- September 2016
- August 2016
- July 2016
- June 2016
- May 2016
- April 2016
- March 2016
- February 2016
- January 2016
- December 2015

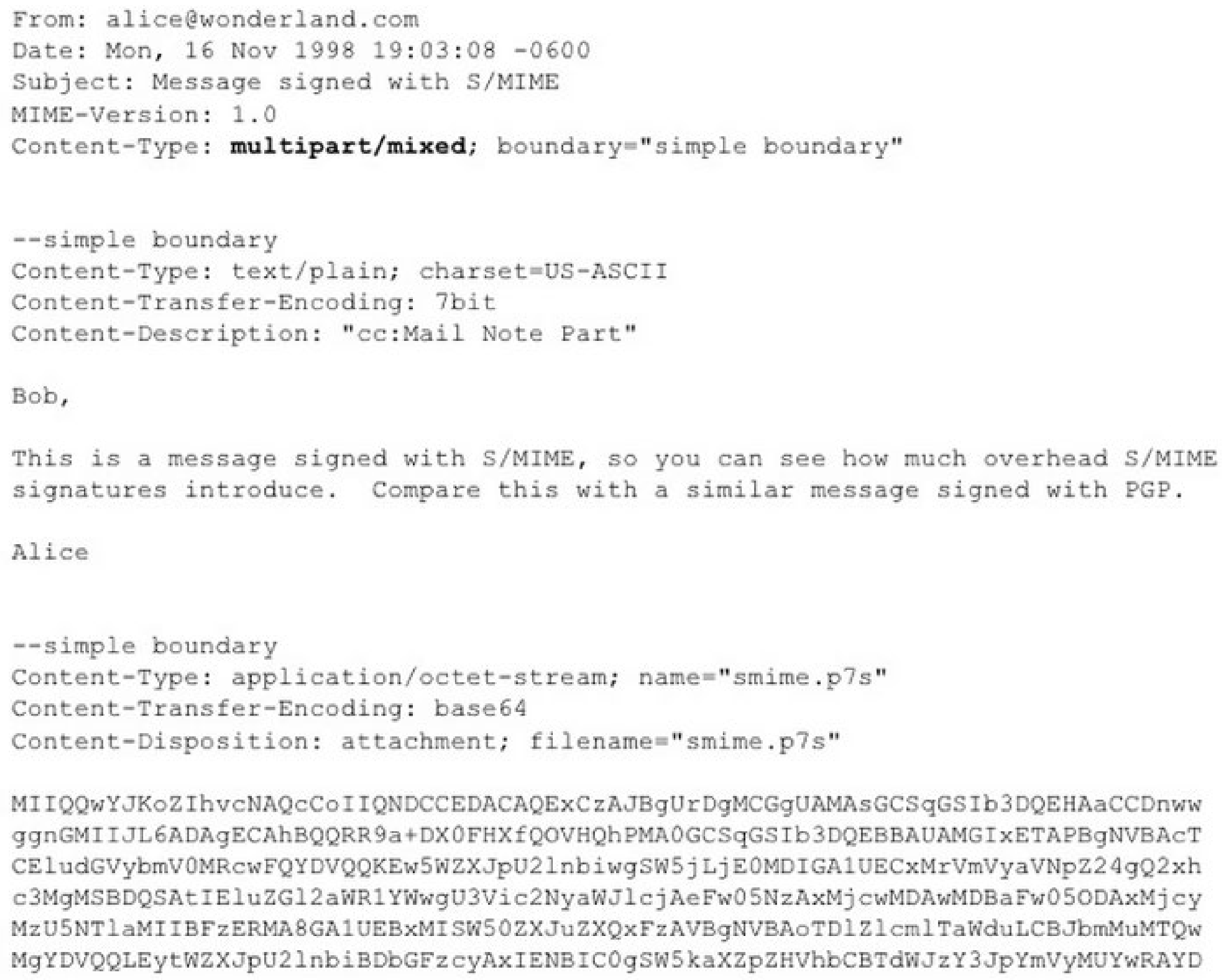
```
GAEIABkFAlm/2LAFCQHhM4AJEIbAD8Kvh3YWAhsMAACz+g/+KmbnChEUZXdo
ZIvPzphw3KvZQHWCY+5qGqdoxNkfkUSKhkzC0M51Kq7emVpvXYrMRdJRHxFP
83HIahA5UiufsDt7QlMwVRGtJYxhH+TNZBBbDBVQ1JQxuC3mH7F/tFHb9N1G
kURUwa2fdDBPw2+DOWa2+iVhcPhfB2iy9exs2txXjgPx67aZi70Jw44ixvpY
TWs/M5I6SXQsyuB5Qw0jtXKioQyTOLmeUFmJR2Ui5FK+t5SXus44mRCujEUn
YDqDmxKDnhssEVNWZ4KWs2uvNXNwlnZcHVSYXukf3FlCWp0TESCOecdqbvl0
Cs+vLivxiksh33xqZWnD78xv92t2Ggp2a41gBOaaCjx2irqZ9RHIv0YzNfQz
yz5XYEGI2iCrvdStrbZfX1Dqsllrqs/pZRbV48KbfubDvGZuNR3hrsfmfsgr
zkESOQmpuKhj/Es3CKjdafLDc8HOyVhJ+n4tvWXyRpYEhuDh/tzeDuuB9vfG
QA9TNhSpAp5lHFJklmd9knWbExJ0srUbK2QVmVn9CZx/sdUfwDWplGeANLsO
MRNlr3IrklbZ0bFH+nrcJQZ5+sDzHGNe4P9Dt30yvFHoyS1BkRndLuawSlqh
LJyYLUvFjL3i3jbiNT1NKldwqaL2i9OuRAuHthoFGOKIqr6hmtOYzUem/cl+
ZlRwd77Vmfc=
=QOc7
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xcaGBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmqBq8I4aNV4u8MqoObd/zrtVX
```

April 2014
March 2014
February 2014
January 2014
December 2013
November 2013
October 2013
September 2013
July 2013
June 2013
May 2013
April 2013
March 2013
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
June 2012
May 2012
April 2012
March 2012
February 2012
January 2012
December 2011
November 2011
October 2011
September 2011
August 2011
June 2011
May 2011
April 2011
March 2011
February 2011
December 2010

S/MIME

- Based on standard X.509 certificates
  - Analogous operation to TLS: trusted CA sign certificates
  - Traditional PKI
- Uses MIME to include cryptographic information in the message
  - Multipurpose Internet Mail Extensions: extends the format of email messages to support binary attachments, and text in non-ASCII character sets
- Works well within corporations
  - Certificate distribution through the existing Active Directory infrastructure
- Built-in support in most modern email clients
  - Seamless interoperability between them

S/MIME Signed Message Example



```
From: alice@wonderland.com
Date: Mon, 16 Nov 1998 19:03:08 -0600
Subject: Message signed with S/MIME
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="simple boundary"


--simple boundary
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit
Content-Description: "cc:Mail Note Part"

Bob,

This is a message signed with S/MIME, so you can see how much overhead S/MIME
signatures introduce.  Compare this with a similar message signed with PGP.

Alice


--simple boundary
Content-Type: application/octet-stream; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
```

```
MIIQQwYJKoZIhvcNAQcCoIIQNDCCEDACAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCDnww
ggnGMIIJL6ADAgECAhBQQRR9a+DX0FHXfQOVHQhPMA0GCSqGSIb3DQEBBAUAMGIxETAPBgNVBAcT
CEludGVybmV0MRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE0MDIGA1UECxMrVmVyaVNpZ24gQ2xh
c3MgMSBDQSAtIEluZGl2aWR1YWwgU3Vic2NyaWJlcjAeFw05NzAxMjcwMDAwMDBaFw05ODAxMjcy
MzU5NTlaMIIBFzERMA8GA1UEBxMISW50ZXJuZXQxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTQw
MgYDVQQLEytWZXJpU2lnbiBDbGFzcyAxIENBIC0gSW5kaXZpZHVhbCBTdWJzY3JpYmVyMUYwRAYD
```

http://www.slideshare.net/rvenkatesh25/network-security-primer

End-to-End vs. Cloud-to-Cloud

IMAP: one of the oldest "cloud" services!

- Keep messages on the server
- Conveniently access them from multiple devices (no file synchronization needed)

Useful modern cloud-based email features

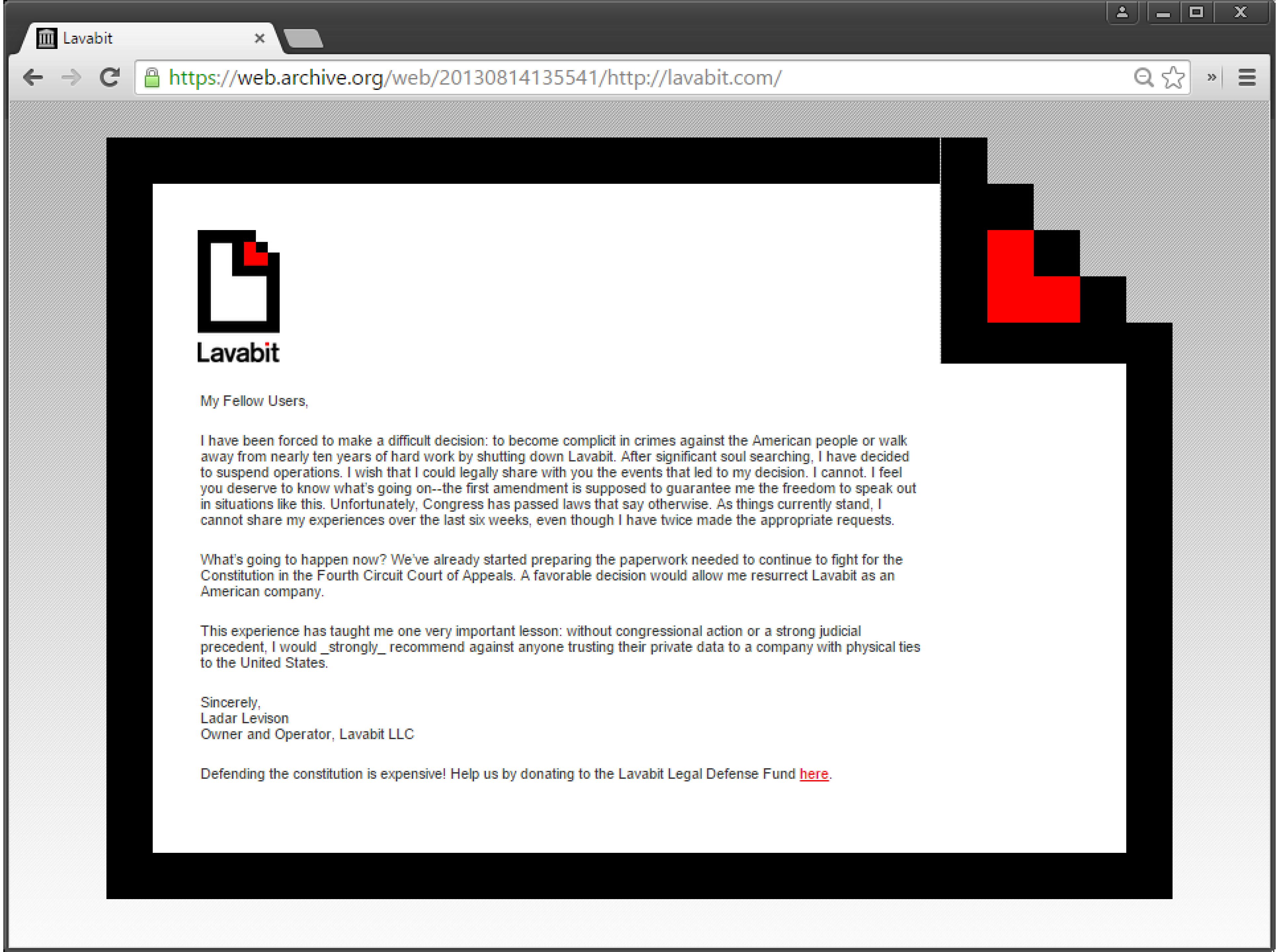
- Powerful and rapid search, collaborative SPAM filtering, …
- Need access to the **plaintext (!)** Gmail cannot index or filter encrypted messages

Tradeoff: privacy vs. convenience

- Active research on searchable encryption

Encrypted Webmail?

- Several recent efforts have focused on transparently combining the convenience of webmail with PGP encryption
  - Is this really possible in a *secure* way?
- JavaScript crypto is not a good idea
  - Secure JS code delivery?
  - Secure key storage?
  - Secure runtime (it’s a *web browser*!)?
- Google end-to-end: implement cryptographic functionality as part of a browser extension
  - More control, but still not trivial
  - After initial excitement, it seems the effort has been abandoned



Lavabit
https://web.archive.org/web/20130814135541/http://lavabit.com/
Lavabit

My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Defending the constitution is expensive! Help us by donating to the Lavabit Legal Defense Fund here.

Lavabit: *"so secure that even our administrators can't read your e-mail"*

But they *could*, if they wanted to…

"Basically we generate public and private keys for the user and then encrypt the private key using a derivative of the plain text password. We then encrypt user messages using their public key before writing them to disk."

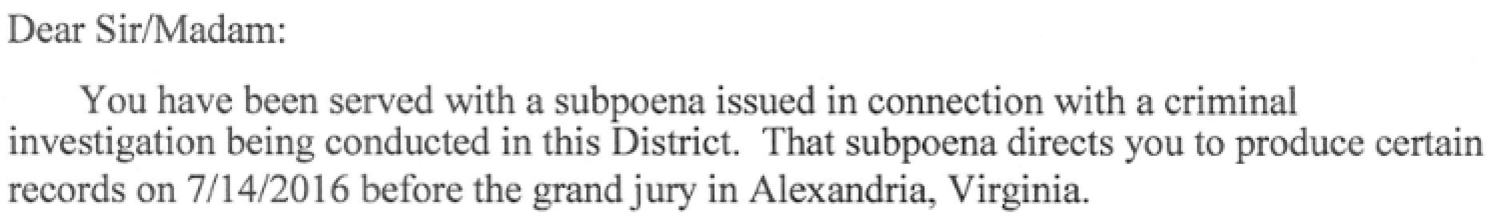
"Because we need the plain text password to decrypt a user's private key, we don't support secure password authentication. We decided to support SSL instead (which encrypts everything; not just the password)."

http://highscalability.com/blog/2013/8/13/in-memoriam-lavabit-architecture-creating-a-scalable-email-s.html
https://arstechnica.com/information-technology/2013/11/op-ed-a-critique-of-lavabit/
https://www.wired.com/2016/03/lavabit-apple-fbi/

Maybe rethink email altogether?

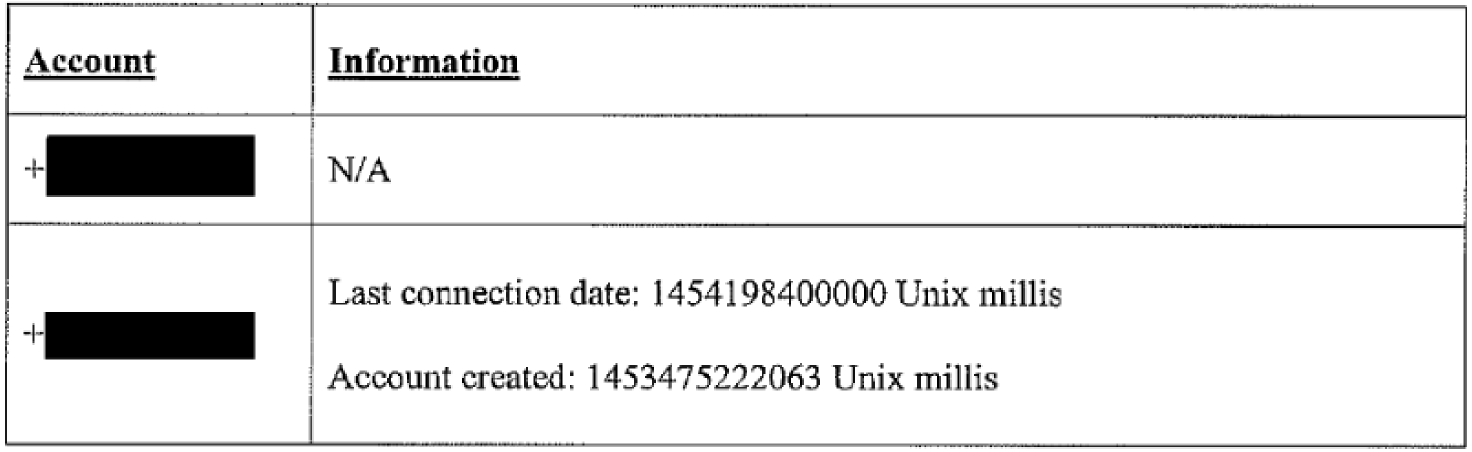
- Secure messaging apps offer many benefits
  - True end-to-end encryption: the provider cannot read message content
  - User-friendly verification of contacts' identities
  - Forward secrecy: past communications remain secure even if private keys are stolen
  - *No spam!* Only approved contacts can send messages
- Best option: **Signal**
  - Double Ratchet Algorithm (precursor: OTR protocol)
  - **Privacy-preserving contact discovery**
- OK alternatives (closed-source): WhatsApp (uses Signal protocol), iMessage
- Metadata is still there!
  - Signal is actively trying to minimize it

Grand jury subpoena for Signal user data (2016)



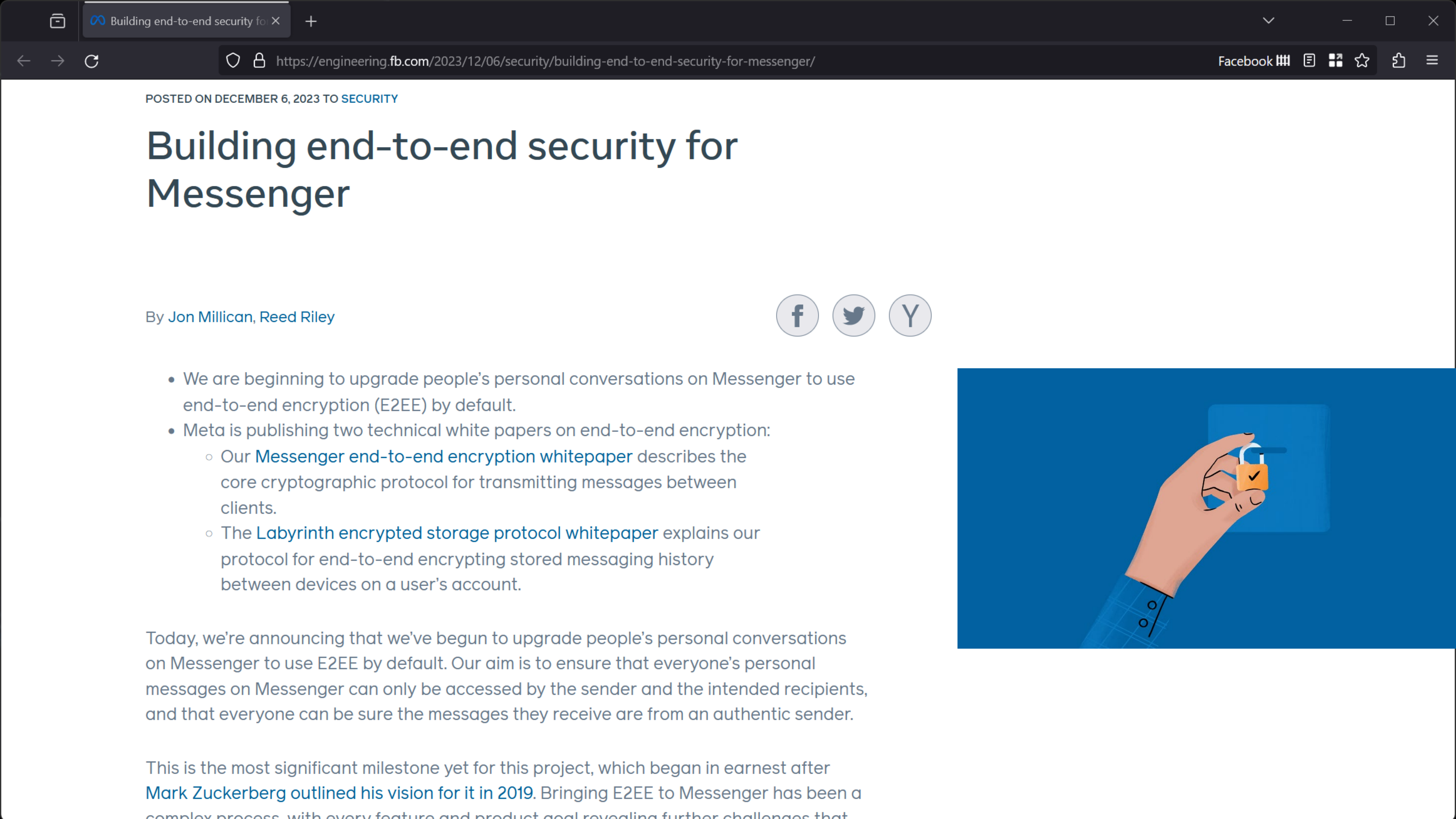
Dear Sir/Madam:

You have been served with a subpoena issued in connection with a criminal investigation being conducted in this District. That subpoena directs you to produce certain records on 7/14/2016 before the grand jury in Alexandria, Virginia.



Account	**Information**
+[redacted]	N/A
+[redacted]	Last connection date: 1454198400000 Unix millis Account created: 1453475222063 Unix millis

https://signal.org/bigbrother/eastern-virginia-grand-jury/


Building end-to-end security fo
https://engineering.fb.com/2023/12/06/security/building-end-to-end-security-for-messenger/
Facebook

POSTED ON DECEMBER 6, 2023 TO SECURITY

Building end-to-end security for Messenger

By Jon Millican, Reed Riley

- We are beginning to upgrade people's personal conversations on Messenger to use end-to-end encryption (E2EE) by default.
- Meta is publishing two technical white papers on end-to-end encryption:
  - Our Messenger end-to-end encryption whitepaper describes the core cryptographic protocol for transmitting messages between clients.
  - The Labyrinth encrypted storage protocol whitepaper explains our protocol for end-to-end encrypting stored messaging history between devices on a user's account.

Today, we're announcing that we've begun to upgrade people's personal conversations on Messenger to use E2EE by default. Our aim is to ensure that everyone's personal messages on Messenger can only be accessed by the sender and the intended recipients, and that everyone can be sure the messages they receive are from an authentic sender.

This is the most significant milestone yet for this project, which began in earnest after Mark Zuckerberg outlined his vision for it in 2019. Bringing E2EE to Messenger has been a complex process, with every feature and product goal revealing further challenges that