SMTP [in]Security

Ian Foster
Jon Larson

Goals

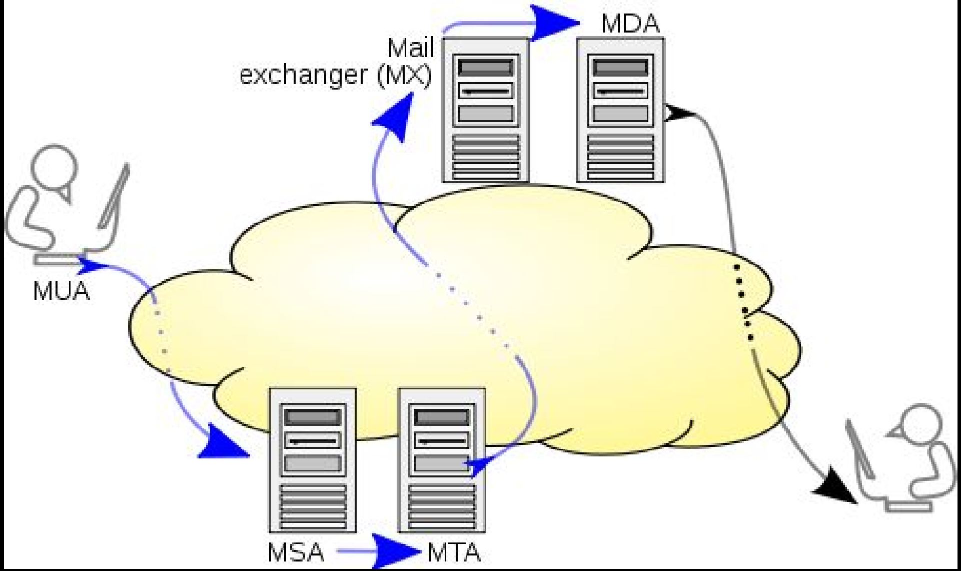
1. Does the global email system currently provide security against passive adversary (eavesdropper)?
2. Against an active adversary (man in the middle)?

Brief History of SMTP

- Many standards used on ARPAnet in 1970s
- Combined into SMTP by RFC 821 in 1982
- Support for extensions (ESMTP) added by RFC 1869 in 1995

SMTP Primer

1. Mail User Agent (MUA) sends message to Mail Submission Agent (MSA) using SMTP, HTTP, etc.
2. MSA sends to intra-domain Mail Transfer Agent (MTA) using SMTP
3. MTA queries DNS server to find MX records for destination user
4. MTA of one domain sends to MX server of another using SMTP
5. MX server passes message to Mail Delivery Agent (MDA)
6. User retrieves email using POP3/IMAP



If encryption happens, it is done *per-link*

Source: http://en.wikipedia.org/wiki/File:SMTP-transfer-model.svg

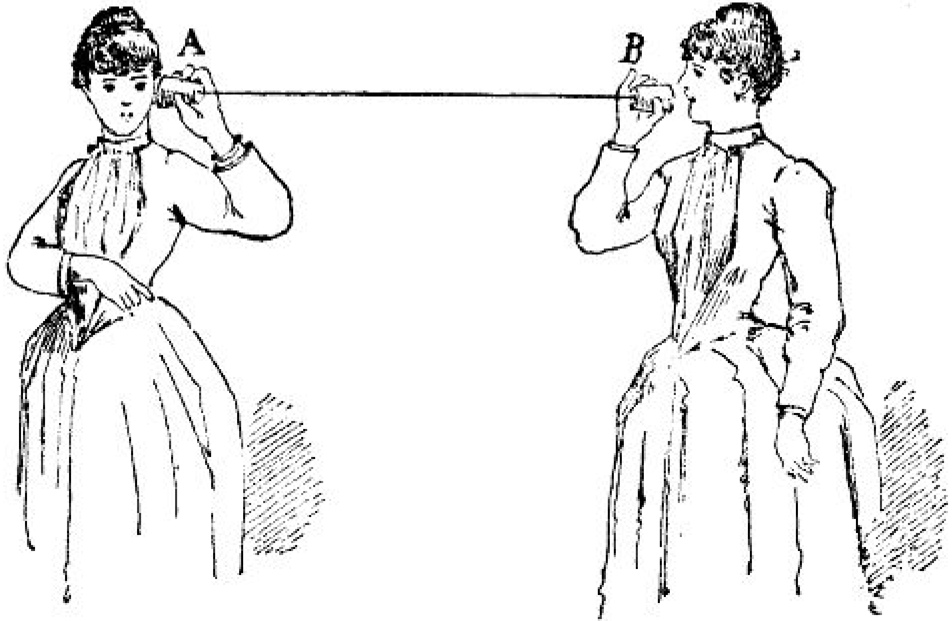


FIG. 76. Trådtelefon.

Alice and Barbara

Source: http://commons.wikimedia.org/wiki/File:Tr%C3%A5dtelefon-illustration.png

Security in SMTP

- Early versions had no built in security
  - All emails sent in plaintext
- RFC 3207 in 2002 added support for TLS
  - Encrypts connection between SMTP servers
  - Use of TLS is not required
- Only encrypts link between servers
  - Violates end-to-end principle

NSA Red Team

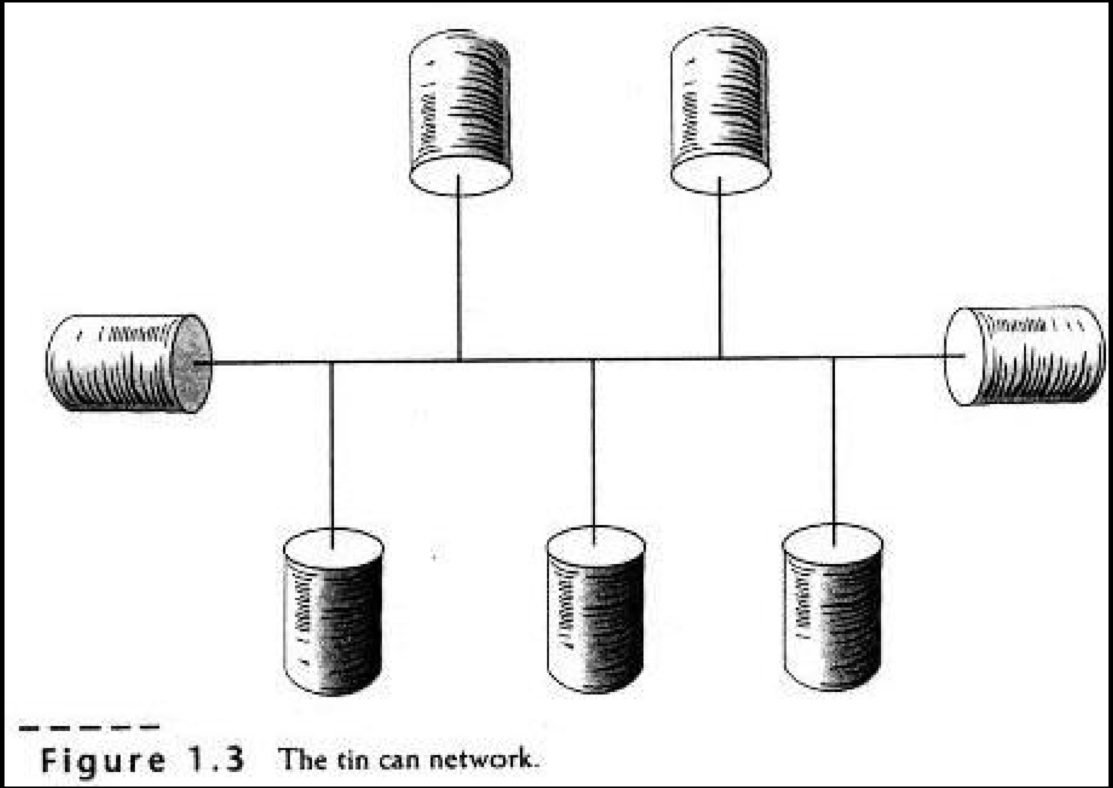


Figure 1.3 The tin can network.

Alice

Barbara

Anonymous

Eve

LRRR

Ruler of the planet
Omicron Persei 8

Source:

Methodology

1. Query DNS to determine IP addresses of domain’s MX servers
2. Establish connection on port 25
3. Issue *EHLO* command
   a. Valid response indicates server supports ESMTP
4. Issue *STARTTLS* command
   a. Valid response indicates server supports encryption
5. Start SSL connection and collect cipher information

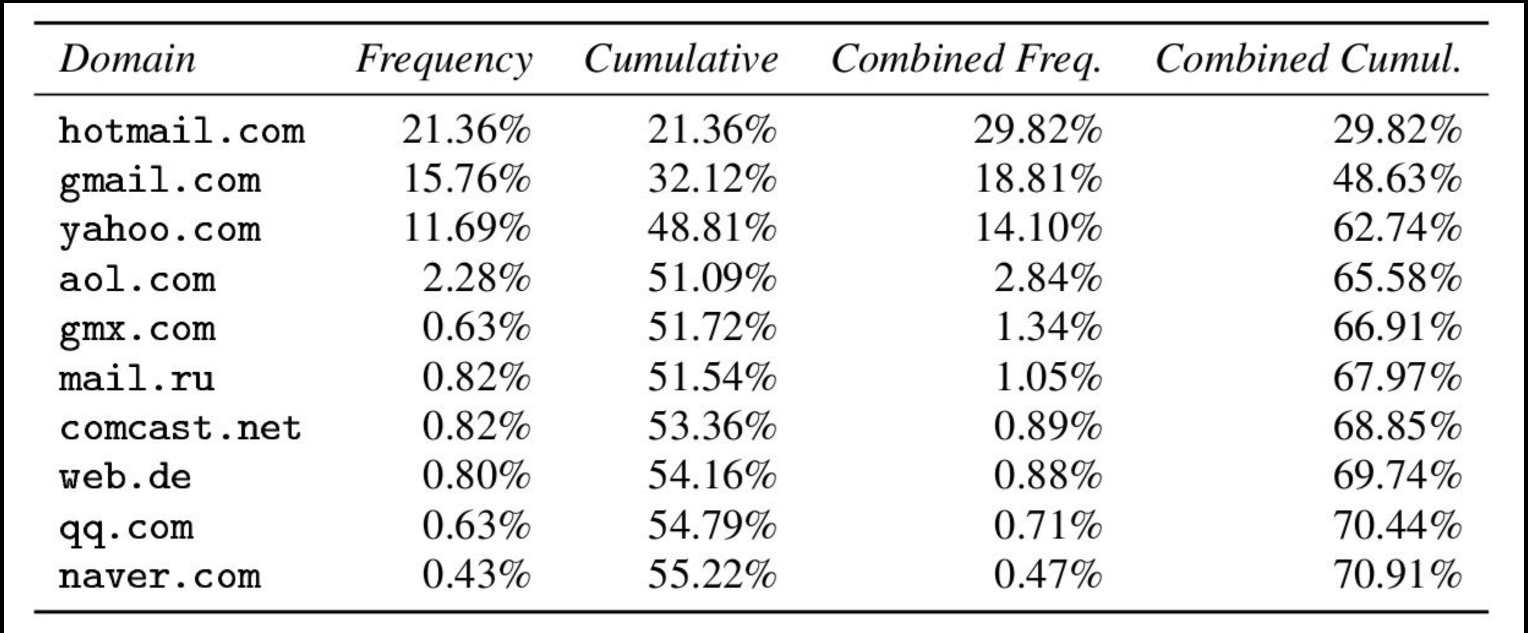
Methodology

```
$ host ucsd.edu
  ucsd.edu has address 132.239.180.101
  ucsd.edu mail is handled by 5 inbound.ucsd.edu.
$ telnet inbound.ucsd.edu 25
  Trying 132.239.0.173...
  Connected to 132.239.0.173.
  Escape character is '^]'.
  220 iport-acv2-in.ucsd.edu ESMTP
  > EHLO ucsd.edu
  250-iport-acv2-in.ucsd.edu
  250-8BITMIME
  250-SIZE 262144000
  250 STARTTLS
  > STARTTLS
  220 Go ahead with TLS
```

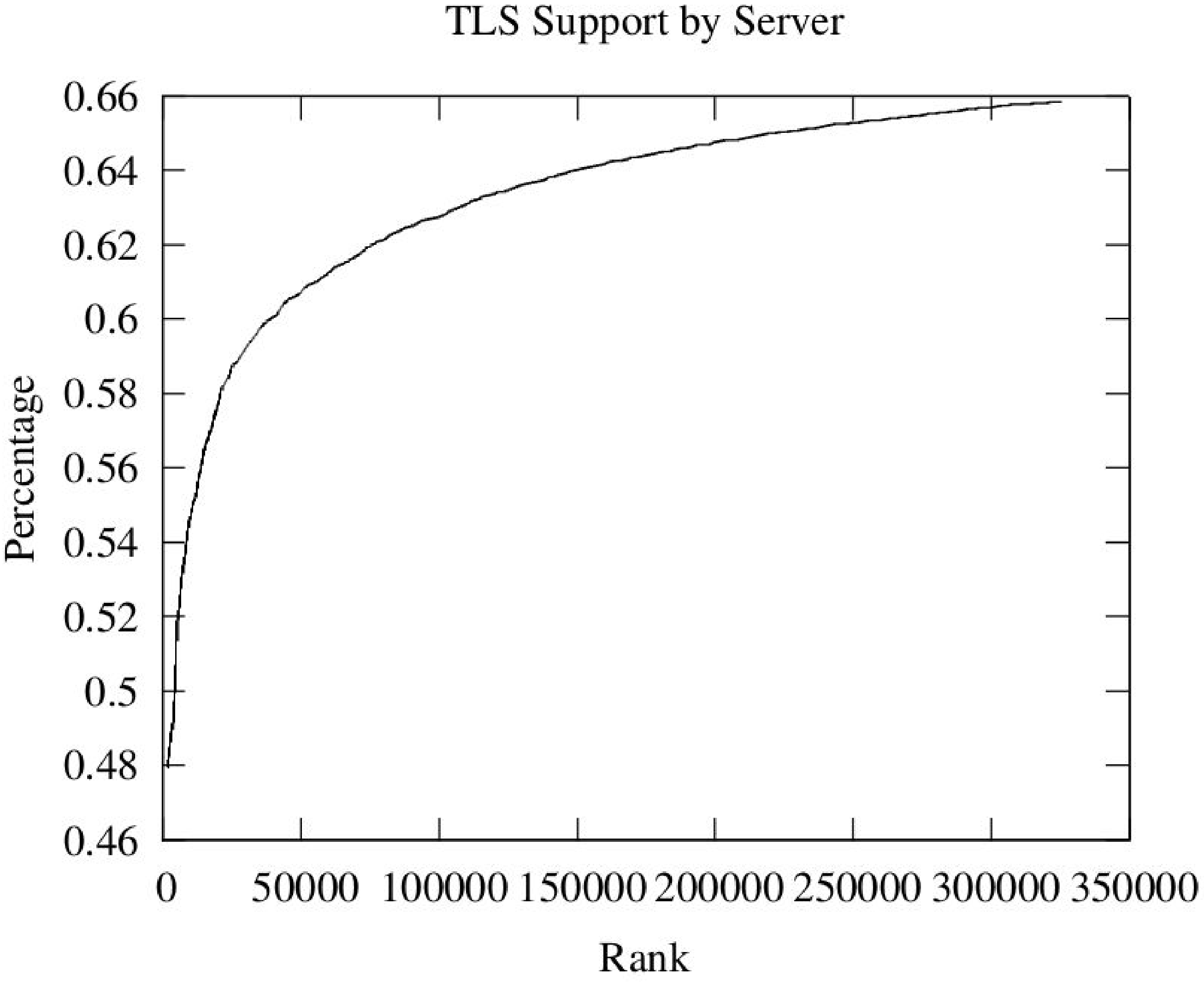
```
$ host hotmail.com
  hotmail.com has address 65.55.85.12
  hotmail.com has address 157.55.152.112
  hotmail.com mail is handled by 5 mx1.hotmail.com.
  hotmail.com mail is handled by 5 mx2.hotmail.com.
$ telnet mx1.hotmail.com 25
  Trying 65.55.37.88...
  Connected to mx1.hotmail.com.
  220 COL0-MC2-F22.Col0.hotmail.com Sending
  unsolicited  commercial or bulk e-mail to Microsoft's
  computer network is prohibited. Other restrictions are
  found at ...
  Wed, 19 Mar 2014 16:13:46 -0700
  > EHLO ucsd.edu
  250-COL0-MC2-F22.Col0.hotmail.com (3.19.0.77) Hello
  [137.110.222.250]
  250-SIZE 36909875
  250-PIPELINING
  250-8bitmime
  250-BINARYMIME
  250-CHUNKING
  250-AUTH LOGIN
  250-AUTH=LOGIN
  250 OK
  > STARTTLS
  554 Unable to initialize security subsystem
```

Data Sources

- Alexa Top Domains
- Leaked lists of email addresses
  - Adobe (141M, Nov ‘13), Gawker (500K, Dec ‘10)
  - Top 20 domains account for > 60% of users
  - Gives us the distribution of users among email providers



Domain	*Frequency*	*Cumulative*	*Combined Freq.*	*Combined Cumul.*
`hotmail.com`	21.36%	21.36%	29.82%	29.82%
`gmail.com`	15.76%	32.12%	18.81%	48.63%
`yahoo.com`	11.69%	48.81%	14.10%	62.74%
`aol.com`	2.28%	51.09%	2.84%	65.58%
`gmx.com`	0.63%	51.72%	1.34%	66.91%
`mail.ru`	0.82%	51.54%	1.05%	67.97%
`comcast.net`	0.82%	53.36%	0.89%	68.85%
`web.de`	0.80%	54.16%	0.88%	69.74%
`qq.com`	0.63%	54.79%	0.71%	70.44%
`naver.com`	0.43%	55.22%	0.47%	70.91%


TLS Support by Server
Percentage
0.66
0.64
0.62
0.6
0.58
0.56
0.54
0.52
0.5
0.48
0.46
0
50000
100000
150000
200000
250000
300000
350000
Rank

Determining Security

gmx.de -> aol.com

```
Return-Path: <username@gmx.de>
Received: from mout.gmx.net (mout.gmx.net [212.227.15.19])
   (using TLSv1 with cipher DHE-RSA-AES128-SHA (128/128 bits))
   (No client certificate requested)
   by mtain-dk12.r1000.mx.aol.com (Internet Inbound) with ESMTPS
          id 264DF38000098
   for <username@aol.com>; Tue, 18 Mar 2014 20:58:36 -0400
(EDT)
Received: from [128.54.46.25] by 3capp-gmx-bs51 with HTTP; Wed,
          19 Mar 2014  01:58:35 +0100
```

Secure!

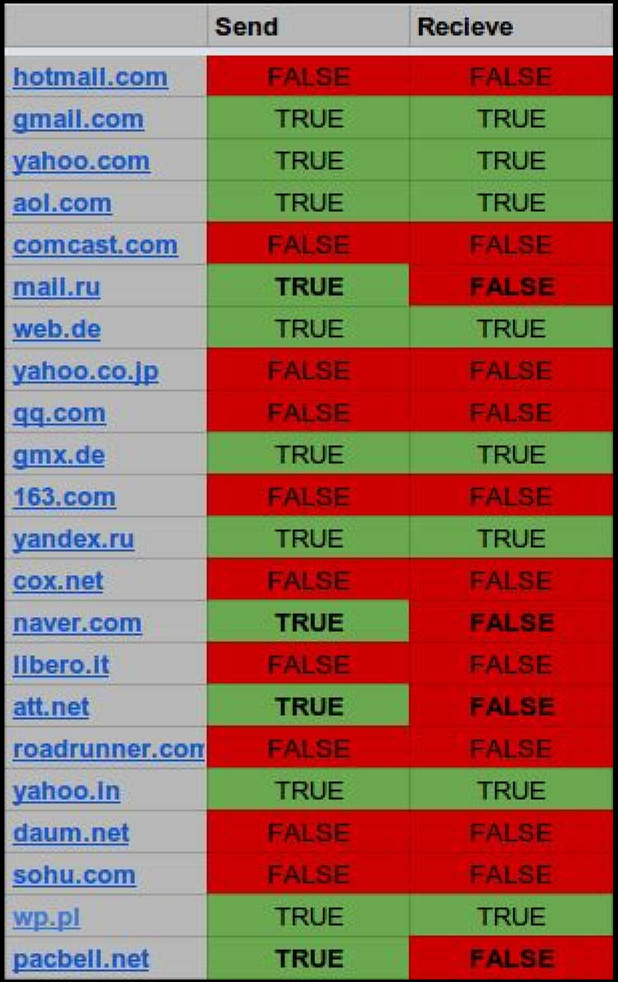
gmx.de -> outlook.com

```
x-store-info:J++/JTCzmObr++wNraA4Pa4f5Xd6uensydyekesGC2M=
Authentication-Results: hotmail.com; spf=pass (sender IP is 212.227.17.21)
smtp.mailfrom=username@gmx.de; dkim=none header.d=gmx.de; x-hmca=pass
header.id=username@gmx.de
X-SID-PRA: username@gmx.de
X-AUTH-Result: PASS
X-SID-Result: PASS
X-Message-Status: n:n
X-Message-Delivery:
Vj0xLjE7dXM9MDtsPTE7YT0xO0Q9MTtHRD0xO1NDTD0y
X-Message-Info: NhFq/7gR1vRIVO7c89UihwXoLMcdpm5/xh6Uow5+...
Received: from mout.gmx.net ([212.227.17.21]) by
BAY0-MC1-F41.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4900);
    Tue, 18 Mar 2014 17:56:07 -0700
Received: from [128.54.46.25] by 3capp-gmx-bs51 with HTTP; Wed, 19 Mar
2014 01:56:07 +0100
```

Not secure!

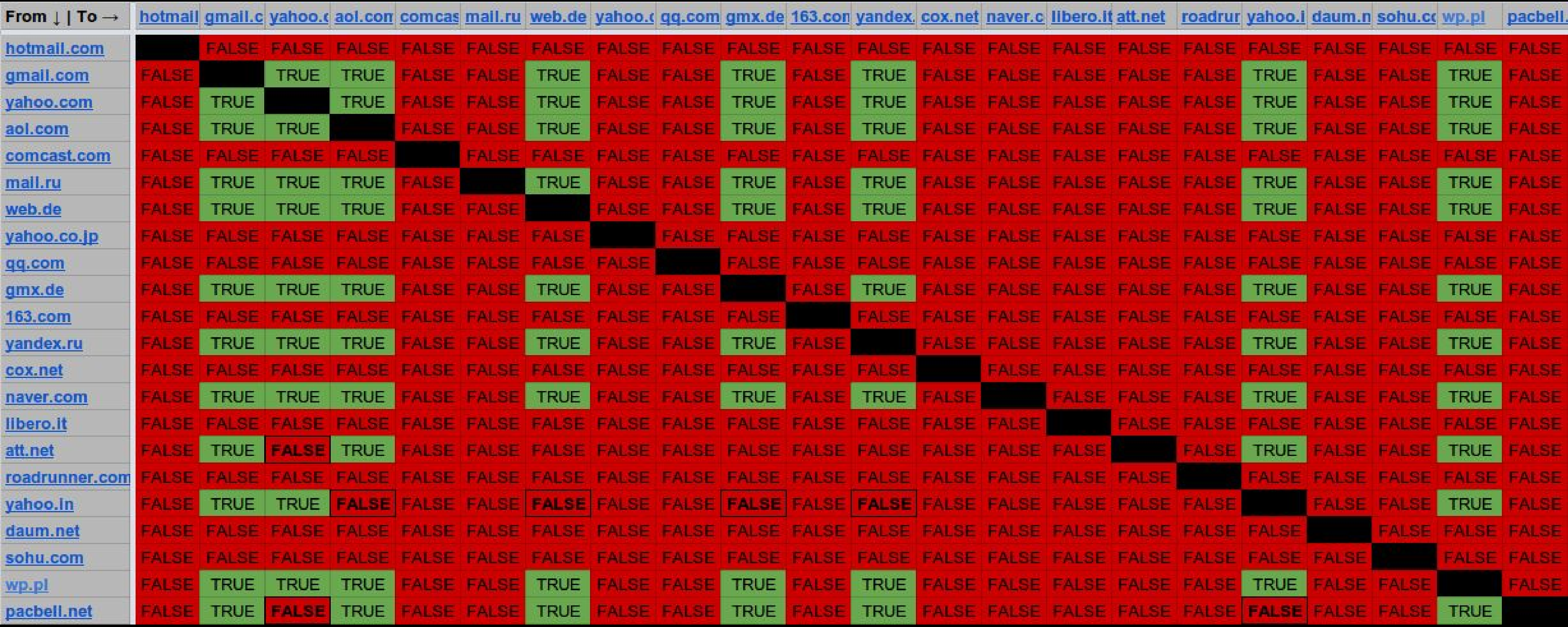
(using public records and standard protocols)

TLS Support



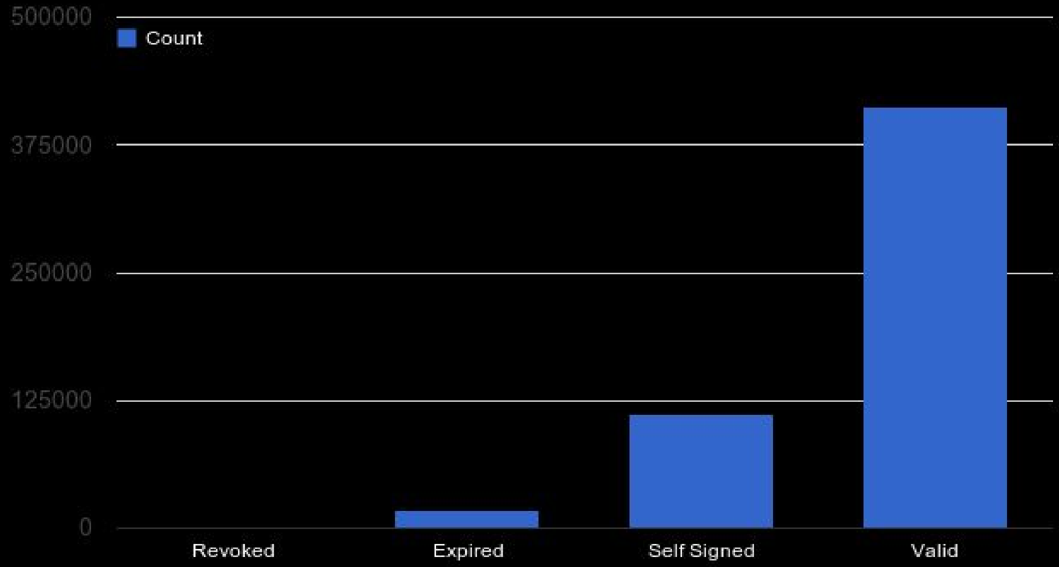
	Send	Recieve
hotmail.com	FALSE	FALSE
gmail.com	TRUE	TRUE
yahoo.com	TRUE	TRUE
aol.com	TRUE	TRUE
comcast.com	FALSE	FALSE
mail.ru	**TRUE**	**FALSE**
web.de	TRUE	TRUE
yahoo.co.jp	FALSE	FALSE
qq.com	FALSE	FALSE
gmx.de	TRUE	TRUE
163.com	FALSE	FALSE
yandex.ru	TRUE	TRUE
cox.net	FALSE	FALSE
naver.com	**TRUE**	**FALSE**
libero.it	FALSE	FALSE
att.net	**TRUE**	**FALSE**
roadrunner.com	FALSE	FALSE
yahoo.in	TRUE	TRUE
daum.net	FALSE	FALSE
sohu.com	FALSE	FALSE
wp.pl	TRUE	TRUE
pacbell.net	**TRUE**	**FALSE**

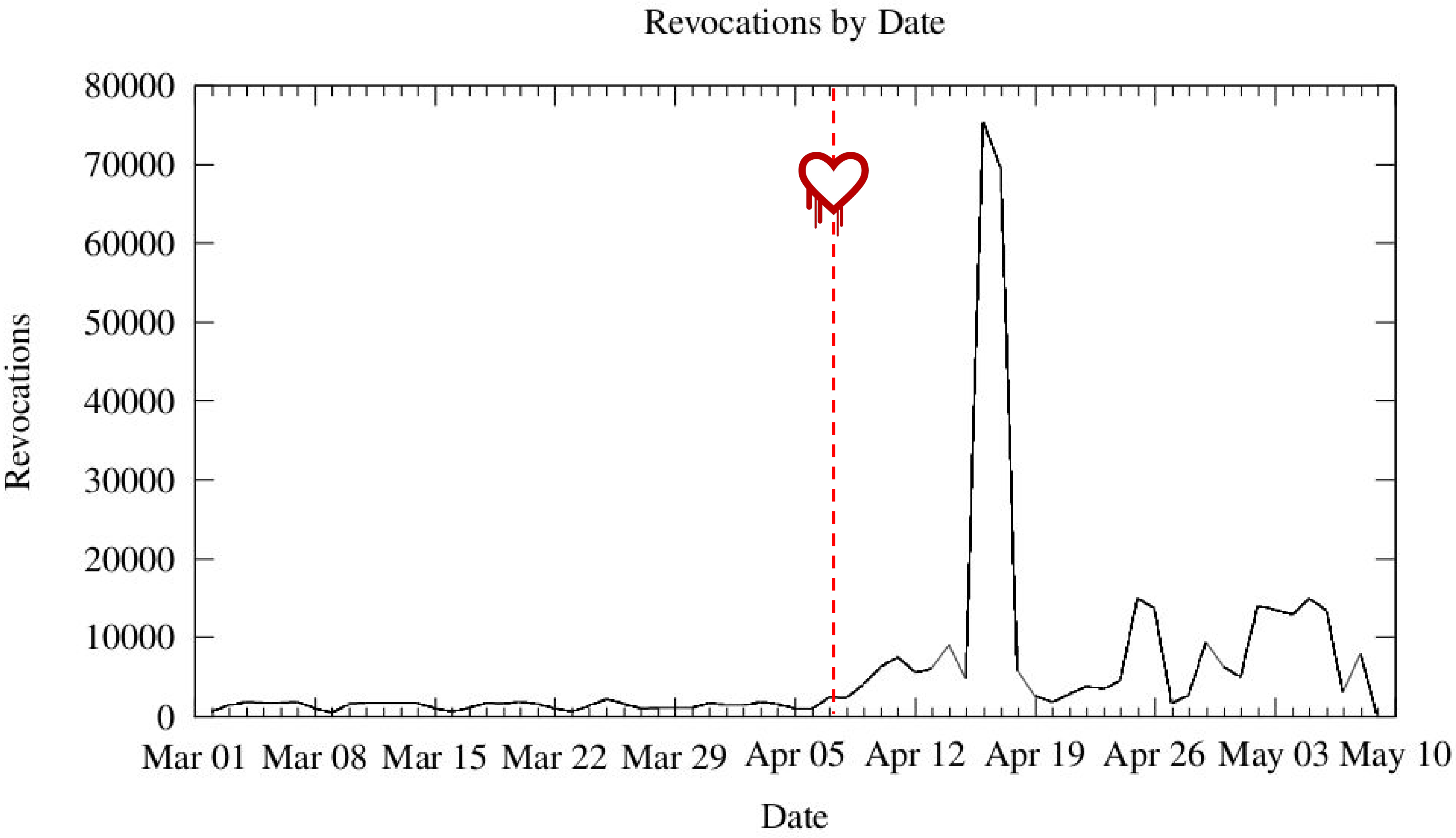
TLS Support For Top Mail Providers



From ↓ | To →	hotmail	gmail.c	yahoo.c	aol.con	comcas	mail.ru	web.de	yahoo.c	qq.com	gmx.de	163.con	yandex.	cox.net	naver.c	libero.it	att.net	roadrur	yahoo.i	daum.n	sohu.cc	wp.pl	pacbell.
hotmail.com		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
gmail.com	FALSE		TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
yahoo.com	FALSE	TRUE		TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
aol.com	FALSE	TRUE	TRUE		FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
comcast.com	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
mail.ru	FALSE	TRUE	TRUE	TRUE	FALSE		TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
web.de	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE		FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
yahoo.co.jp	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
qq.com	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
gmx.de	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
163.com	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
yandex.ru	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
cox.net	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
naver.com	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE		FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
libero.it	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
att.net	FALSE	TRUE	**FALSE**	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
roadrunner.com	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE	FALSE	FALSE
yahoo.in	FALSE	TRUE	TRUE	**FALSE**	FALSE	FALSE	**FALSE**	FALSE	FALSE	**FALSE**	FALSE	**FALSE**	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	TRUE	FALSE
daum.net	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE	FALSE
sohu.com	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE		FALSE	FALSE
wp.pl	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE		FALSE
pacbell.net	FALSE	TRUE	**FALSE**	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	**FALSE**	FALSE	FALSE	TRUE	

Certificate Status




Revocations by Date
Revocations
80000
70000
60000
50000
40000
30000
20000
10000
0
Mar 01
Mar 08
Mar 15
Mar 22
Mar 29
Apr 05
Apr 12
Apr 19
Apr 26
May 03
May 10
Date

Conclusion

- Does the global email system currently provide security against and passive adversary (eavesdropper)?
  - Yes, if both providers support STARTTLS and you trust each MTA

Conclusion

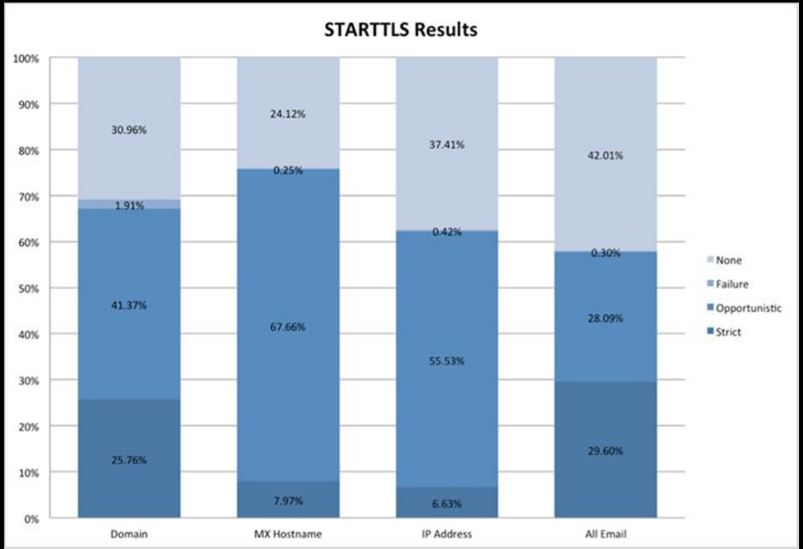
- Does the global email system currently provide security against an active adversary (man in the middle)?

Conclusion

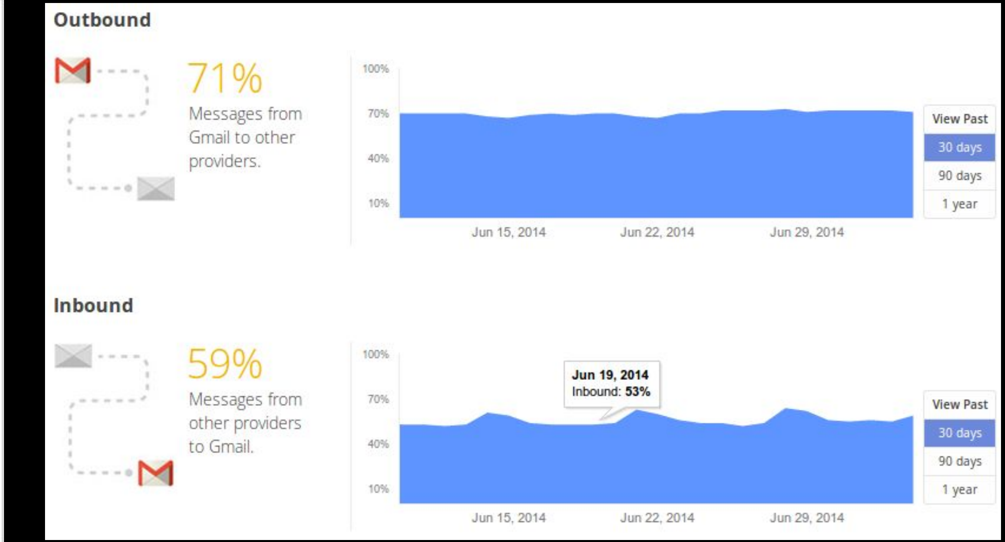
- SMTP is inherently insecure
  - violates end-to-end principle
- Difficult to assess secure practices
- Most email hosted by small set of providers
  - these don’t all follow secure practices
- Only takes one weak link to break security

Other Studies

Facebook Study



Google Study



Outbound

71%

Messages from Gmail to other providers.

Inbound

59%

Messages from other providers to Gmail.

Jun 19, 2014
Inbound: 53%

Questions?