Security by Any Other Name:
On the Effectiveness of Provider Based Email Security

•••

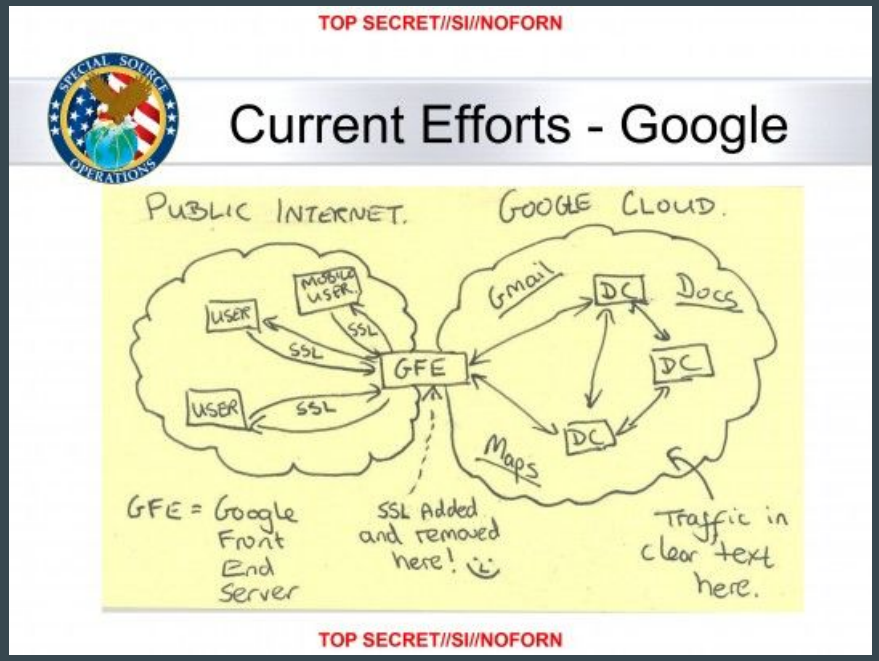
Ian Foster, Jon Larson, Max Masich, Alex C. Snoeren,
Stefan Savage, and Kirill Levchenko

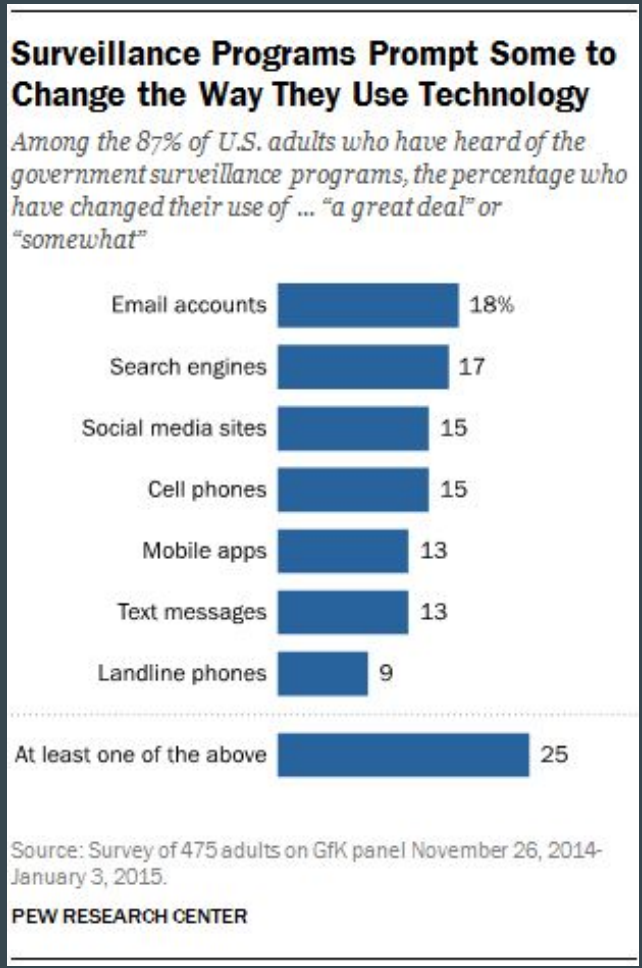
University of California, San Diego

UCSDCSE

Recent Email Communications Surveillance Revelations

- MUSCULAR (surveillance program)
- TAO QUANTUM (active attacks)
- Fairview (surveillance program)





Solved Problem

- Solved Problem: End-to-End Security
  - PGP
  - S/MIME
  - Very little adoption
- Lower-Level Security Extensions
  - TLS
    - SMTP
    - POP
    - IMAP
  - DKIM
  - SPF

Overview

- We examined the existing protocols used today and describe the level of security they provide
- We measured how these protocols are used today and determined if they provide the level of security in practice that they could in theory
  - hop-by-hop deployment and use of TLS with SMTP, POP3, IMAP across major providers
  - DKIM, SPF, and DMARC use
  - DNSSEC which ensures DKIM, SPF, and DMARC

- TLS deployment is on rise
  - no verification only offers protection from passive attackers
- DNSSEC has the lowest deployment
  - even among the top providers

Previous Studies

- **Facebook**
  - 2014 measurement of sending notification emails to users
  - **76%** of incoming MTAs offered TLS
  - **58%** of outgoing email used TLS
  - About half of the TLS certificates pass validation

- **Google**
  - Offers SMTP TLS stats on ongoing basis
  - At the time of our study (Febuary 2015)
    - **46%** outbound messages
    - **40%** inbound messages
  - Today
    - **81%** outbound messages
    - **59%** inbound messages

Security Properties

- Confidentiality
  - Can an attacker *read* a message?
- Integrity
  - Can an attacker *modify* a message?
- Authenticity
  - Can an attacker *forge* a message?

Assuming the provider is trusted, what guarantees can TLS, DKIM, SPF and DMARC provide?

In practice are these technologies used in a way that provides these guarantees?

Threat Model

Attackers:

- Active
  - man-in-the-middle attacker
  - can observe, inject, and modify all packets between a target and the rest of the Internet
- Passive
  - can observe but not modify the traffic between a target and the rest of the Internet
- Peer
  - ordinary host connected to the Internet
  - capable of sending arbitrary packets and receiving packets for which it is the destination

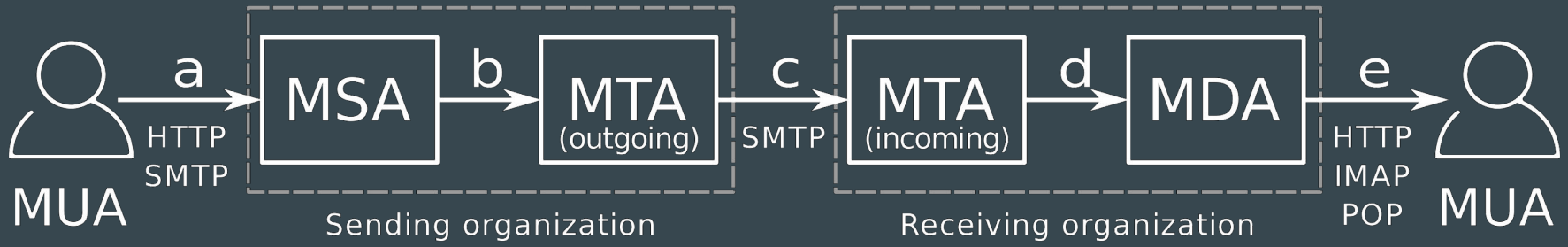
Email Security Extensions

- Transport Layer Security (TLS)
  - Encryption
  - STARTTLS - Upgrades SMTP, IMAP, and POP connections to TLS
- Sender Policy Framework (SPF)
  - DNS record listing hosts authorised to send mail on behalf of a domain
- DomainKeys Identified Mail (DKIM)
  - Digital signature included in message headers
  - Public key in domain's DNS record
- Domain Message Authentication, Reporting and Conformance (DMARC)
  - Defines policies (`none`, `quarantine`, `reject`) for messages that have invalid SPF or DKIM
  - Stored in DNS record
- Domain Name System Security Extensions (DNSSEC)
  - Adds origin authentication and Integrity to DNS records.

Security Properties

- Confidentiality
  - HTTP, SMTP, IMAP, POP can be protected using TLS encryption
  - Internal hops from MSA → MTA or MTA → MDA may be using a proprietary protocol and may or may not be encrypted
  - Use of TLS on all attacker accessible links can prevent a passive attacker
  - TLS with server certificate verification can prevent an active (MITM) attacker
- Authenticity
  - MTA → MTA link is most vulnerable
  - Sufficient to verify SPF and DKIM
    - SPF - identify authorized senders for a domain
    - DKIM - prevent message forgery and tampering by including a signature
- Integrity
  - DKIM signatures can be used to protect messages from tampering in transit
  - Required DNSSEC if an attacker can alter DNS traffic

Mail Path



a. The message is transmitted to the sender's mail provider using SMTP or HTTP
b. Processing inside the sending provider, may include adding SPF or DKIM headers
c. The message is transmitted to the recipient's provider using SMTP
d. Receiver processing, may include spam filtering
e. The message is delivered to the recipient using IMAP, POP, or HTTP

Email Providers & Generators

- Provider list
  - Top email providers for sending and receiving
  - Top providers from Adobe leak (2013)
    - 152m unique emails, 9.2m domains
    - Top 22 covers >75% of users
    - grouped domains owned by same provider together
- Generator list
  - Services that automatically generate email
  - 61 services from Alexa top 100
  - additional special interest sites such as banks and dating sites

Domain	*Country*	*Frequency*	*Cumulative*
hotmail.com		29.82%	29.82%
gmail.com		18.86%	48.68%
yahoo.com		14.22%	62.91%
aol.com	US	2.83%	65.74%
gmx.de	DE	1.06%	66.80%
mail.ru	RU	1.05%	67.85%
yahoo.co.in	IN	0.99%	68.84%
comcast.net	US	0.89%	69.73%
web.de	DE	0.88%	70.61%
qq.com	CN	0.71%	71.32%
yahoo.co.jp	JP	0.71%	72.02%
naver.com	KR	0.47%	72.49%
163.com	CN	0.46%	72.95%
twc.com	US	0.38%	73.33%
libero.it	IT	0.34%	73.67%
yandex.ru	RU	0.32%	73.99%
daum.net	KR	0.27%	74.26%
cox.net	US	0.26%	74.52%
att.net	US	0.22%	74.73%
wp.pl	PL	0.20%	74.93%
pacbell.net	US	0.08%	75.01%
sohu.com	CN	0.04%	75.05%

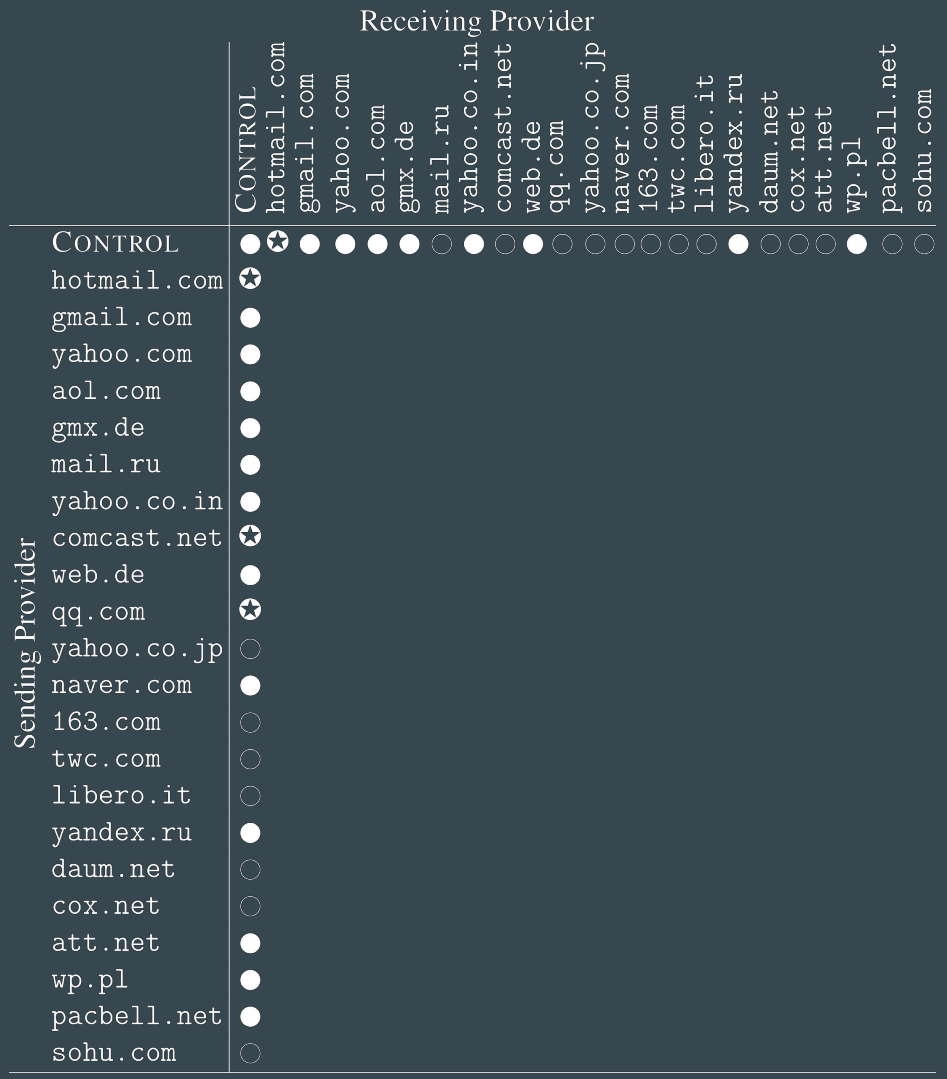
Results

Provider TLS Use

- Top million MTA
  - 50.5% supported TLS in 2014
  - 54.6% in 2015.
- Top 1000 MTAs
  - 43.7% in 2014
  - 59.2% in 2015

Provider TLS Use

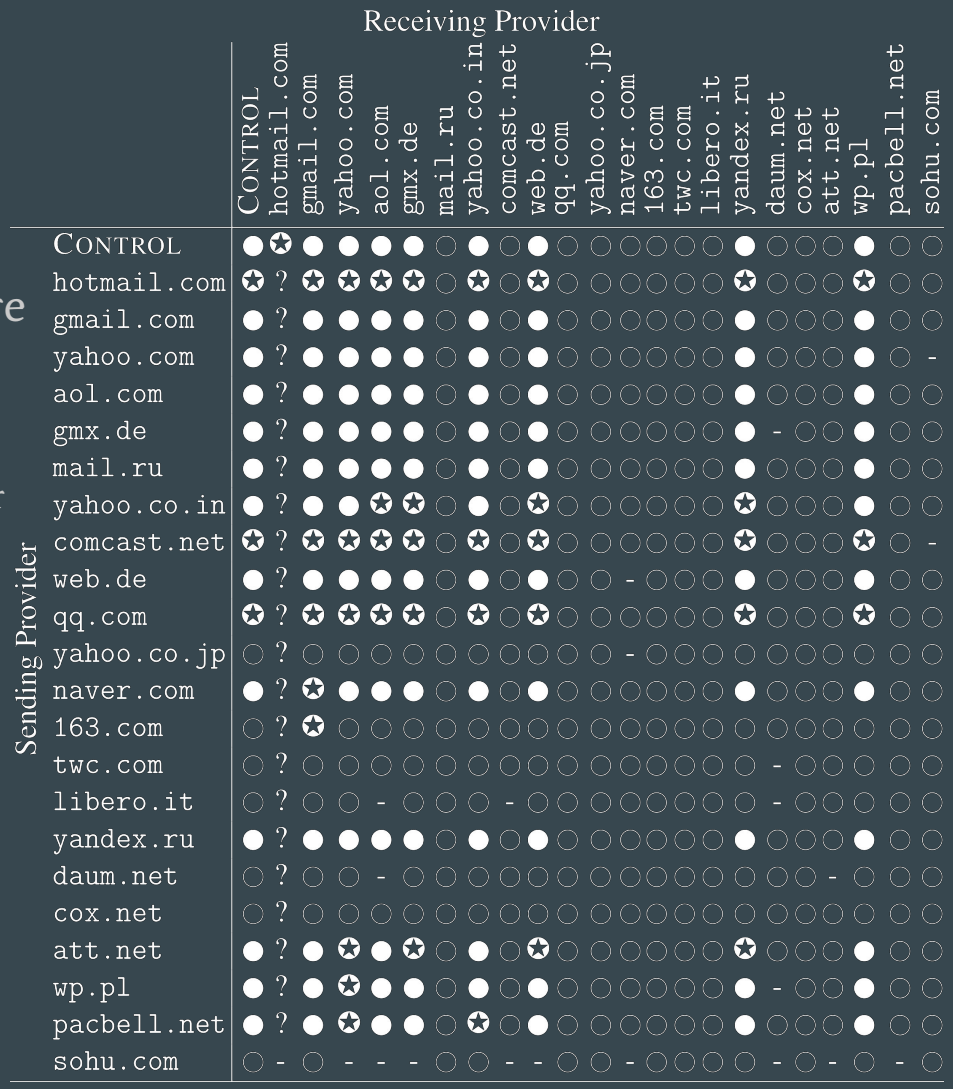
- Top million MTA
  - 50.5% supported TLS in 2014
  - 54.6% in 2015.
- Top 1000 MTAs
  - 43.7% in 2014
  - 59.2% in 2015
- Top 10 providers send with TLS



no TLS
TLS (2014 & 2015)
TLS added in 2015

Provider to Provider TLS

- Examined `Received` header to determine TLS use
- Some hosts particularly sohu.com were often blocked by the recieveding prociders
  - spam due to unauthenticated SMTP server
- hotmail.com recorded SMTPSVC for both TLS and non-TLS connections



Generator TLS

- Email generators from Alexa top 100
- Measured TLS to our control server
- Highest support by **Bank** sites
- Lowest support by **News** and **Dating** sites

Domain	*TLS*
Search	
google.com	●
yahoo.com	●
baidu.com	○
qq.com	○
live.com	○
hao123.com	○
sohu.com	○
yandex.ru	○
bing.com	○
163.com	○
mail.ru	●
Entertainment	
youtube.com	●
xvideos.com	○
imgur.com	●
xhamster.com	●
vube.com	○
youku.com	○
pornhub.com	○
vimeo.com	○
dailymotion.com	○
netflix.com	○
Government	
healthcare.gov	○
whitehouse.gov	○
Conferences	
easychair.org	●
hotcrp.com	●

Domain	*TLS*
Commerce	
amazon.com	●
ebay.com	●
adcash.com	○
neobux.com	○
godaddy.com	○
craigslist.org	○
aliexpress.com	○
alibaba.com	○
alipay.com	●
rakuten.co.jp	○
Misc	
ask.com	○
360.cn	●
microsoft.com	○
thepiratebay.se	○
kickass.to	●
imdb.com	●
stackoverflow.com	●
wikipedia.org	○
News	
sina.com.cn	○
msn.com	○
cnn.com	○
people.com.cn	○
gmw.cn	○
espn.go.com	○

Domain	*TLS*
Banks	
bankofamerica.com	●
paypal.com	○
chase.com	●
discover.com	●
usbank.com	○
americanexpress.com	●
Social	
wordpress.org	○
facebook.com	●
linkedin.com	●
twitter.com	●
blogspot.com	●
weibo.com	○
wordpress.com	○
vk.com	○
pinterest.com	○
instagram.com	●
tumblr.com	○
reddit.com	○
fc2.com	○
blogger.com	●
odnoklassniki.com	○
Dating	
match.com	○
zoosk.com	○
okcupid.com	○
pof.com	○

○ no TLS
● TLS

SMTP Certificate Status

- Incoming
  - 3 incoming MTAs had mismatched certs in top 10
  - valid certificates have risen
  - use of mismatched certificates also increased
- Outgoing
  - All but 3 providers did not perform certificate checking
  - 7/22 provided a client cert
    - comcast.com was expired

Status	*Freq. 2014*	*Freq. 2015*
Valid	75.86%	79.14%
Self Signed	20.47%	11.39%
Expired	3.41%	2.88%
Revoked	0.17%	0.04%
Non Matched	34.13%	37.26%

Incoming cert status of adobe top million

Provider Security Mechanisms

- SPF
  - Strict if ends in "`-all`", instructs the receiver to reject mail not from the correct origin
  - 5 providers rejected invalid SPF messages at the SMTP layer
- DMARC
  - strict if its policy is to reject invalid messages by setting "`p=reject`"

	Implementation				DNS Lookup			Enforcement		
Domain	*DNSSEC*	*SPF*	*DKIM*	*DMARC*	*SPF*	*DKIM*	*DMARC*	*SPF*	*DKIM*	*DMARC*
hotmail.com	○	●	○	●	●	●	●	✪	●	●
gmail.com	○	●	●	●	●	○	●	○	○	●
yahoo.com	○	○	●	◉	●	●	●	○	○	●
aol.com	○	●	○	◉	●	●	●	●	○	○
gmx.de	○	◉	○	○	●	○	○	●	○	○
mail.ru	○	●	●	●	●	●	○	○	○	○
yahoo.co.in	○	○	●	●	●	○	●	●	○	●
comcast.net	●	○	●	●	●	●	○	○	○	●
web.de	○	◉	○	○	●	●	○	●	●	●
qq.com	○	●	●	●	●	●	○	○	●	○
yahoo.co.jp	○	●	●	○	●	●	○	●	○	○
naver.com	○	●	○	○	●	○	○	✪	○	○
163.com	○	◉	●	○	●	●	●	✪	○	●
twc.com	○	●	○	○	○	○	○	○	○	○
libero.it	○	◉	●	●	●	○	○	○	○	○
yandex.ru	○	●	●	●	●	○	●	✪	○	○
daum.net	○	●	○	○	○	○	○	○	○	○
cox.net	○	○	○	○	●	●	○	○	○	○
att.net	○	○	●	○	●	●	●	○	○	○
wp.pl	○	○	●	○	●	○	○	✪	○	○
pacbell.net	○	○	●	○	●	○	●	○	○	○
sohu.com	○	◉	○	○	●	○	○	○	○	○

○ no support
● support
✪ provider rejected invalid messages
◉ strict policy implemented

Generator SPF and DKIM

- SPF
  - Very widely used
  - often strict
- DKIM
  - Widely used by commerce and all banks
  - about half implement a strict policy
    - mostly banks or social sites

Domain	SPF	DM
Search		
google.com	●	●
yahoo.com	●	◉
baidu.com	◉	○
qq.com	●	●
live.com	●	○
hao123.com	◉	○
sohu.com	◉	○
yandex.ru	●	●
bing.com	○	○
163.com	◉	○
mail.ru	●	●
Entertainment		
youtube.com	◉	●
xvideos.com	●	○
imgur.com	●	●
xhamster.com	○	○
vube.com	◉	●
youku.com	○	○
pornhub.com	◉	○
vimeo.com	◉	○
dailymotion.com	●	○
netflix.com	◉	◉
Government		
healthcare.gov	◉	○
whitehouse.gov	○	○
Conferences		
easychair.org	○	○
hotcrp.com	●	●

Domain	SPF	DM
Commerce		
amazon.com	◉	●
ebay.com	●	●
adcash.com	●	○
neobux.com	◉	◉
godaddy.com	◉	●
craigslist.org	◉	●
aliexpress.com	◉	●
alibaba.com	◉	●
alipay.com	◉	●
rakuten.co.jp	●	●
Misc		
ask.com	◉	○
360.cn	●	○
microsoft.com	◉	●
thepiratebay.se	○	○
kickass.to	●	○
imdb.com	○	○
stackoverflow.com	●	○
wikipedia.org	○	●
News		
sina.com.cn	◉	○
msn.com	◉	○
cnn.com	○	○
people.com.cn	○	○
gmw.cn	○	○
espn.go.com	○	○

Domain	SPF	DM
Banks		
bankofamerica.com	●	●
paypal.com	●	◉
chase.com	◉	◉
discover.com	○	●
usbank.com	◉	●
americanexpress.com	◉	◉
Social		
wordpress.org	○	○
facebook.com	◉	◉
linkedin.com	●	◉
twitter.com	◉	◉
blogspot.com	○	●
weibo.com	◉	○
wordpress.com	●	●
vk.com	●	○
pinterest.com	◉	◉
instagram.com	◉	◉
tumblr.com	●	○
reddit.com	◉	○
fc2.com	●	○
blogger.com	○	●
odnoklassniki.ru	●	○
Dating		
match.com	●	●
zoosk.com	●	○
okcupid.com	●	○
pof.com	●	○

○ no support
● basic support
◉ strict support

Security Mechanisms Across Top Million

Metric	*Alexa Hosts*	*Adobe Hosts*	*Adobe Users*
DNSSEC	3.40%	2.75%	4.92%
Valid	2.96%	2.12%	1.35%
Invalid	0.44%	0.63%	3.57%
DMARC	0.97%	0.90%	67.81%
None	0.73%	0.66%	51.29%
Quarantine	0.08%	0.06%	0.46%
Reject	0.16%	0.18%	16.06%
SPF	42.26%	43.60%	85.02%

Conclusion

- The current system offers no protection from an active adversary
- Postel's principle:
  - Senders won't enforce TLS use if deployment is poor
  - Receivers won't do it right if there is no penalty for non-compliance
- Fix:
  - Make authentication encryption use user-visible
    - Worked for HTTPS
  - **Integrity**: show if sender of message is authenticated for integrity
  - **TLS**: show whether message was sent using TLS
    - Offer TLS only option

Questions?

idfoster@cs.ucsd.edu

Recommendations

1. Use TLS
2. Fix Certificates
3. Verify Certificates
4. Require TLS
5. Certificate Pinning
6. Use DKIM and DMARC
7. Enforce SPF and DKIM policy
8. Use DNSSEC

Attacks

- Passive Eavesdropping
- Peer Forgery
- Active Eavesdropping
- Active Tampering

Minimum Protocol Requirements

Property	*Active*	*Passive*	*Peer*
Confidentiality	TLS with Cert Verif.	TLS	—
Authenticity	DKIM* and DNSSEC	—	SPF or DKIM*
Integrity	DKIM* and DNSSEC	—	—

Summary of each security policy required to protect aginst each class of attacker

* Note: while DKIM is theoretically sufficient, as used today, it is also necessary to advertise a strict policy using DMARC.

Submission and Delivery

- MUA → MSA
  - SMTP and HTTP
- MDA → MUA
  - POP3, IMAP, and HTTP
- 3 providers do not offer TLS over HTTP
- 6 providers used a certificate that did not match the hostname
  - ex: hotmail's SMTP server is `smtp-mail.outlook.com`, wth a certificate for `*.hotmail.com`

	SMTP	*POP3*	*IMAP*	*HTTP*
hotmail.com	◐	◐	◐	●
gmail.com	●	●	●	●
yahoo.com	●	◐	●	●
aol.com	●	◐	●	●
gmx.de	●	●	●	●
mail.ru	●	●	●	●
yahoo.co.in	◐	●	●	●
comcast.net	●	●	◐	●
web.de	●	●	●	●
qq.com	◐	●	◐	●
yahoo.co.jp	◐	●	●	●
naver.com	●	○	●	●
163.com	●	●	●	○
twc.com	◐	◐	◐	●
libero.it	●	●	●	○
yandex.ru	●	●	●	●
daum.net	●	●	●	○
cox.net	●	●	●	●
att.net	◐	●	●	●
wp.pl	●	●	●	●
pacbell.net	●	●	●	●
sohu.com	○	○	○	●

● valid certificate, valid hostname
◐ valid certificate, non-matching hostname
○ provider offers no TLS support
● provider rejected non-TLS connections

Inside the Provider

- Information gathered from **`Received`** headers
- **Out** measures inferred TLS use on MSA → MTA links
- **In** measures inferred TLS use on MTA → MDA links
- Internal hops may be on the same local network, or encrypted on an inter-datacenter VPN
- Providers which report no hops from the MTA → MDA may not be recording the internal hops to the message headers

	Out	*In*
hotmail.com	▶	
gmail.com	▷▶▷	▷
yahoo.com	· · ·	·
aol.com	▶	
gmx.de	▶▷	
mail.ru	▷	
yahoo.co.in	· · · · ·	·
comcast.net	▷▶	· ▷
web.de	▶	
qq.com	▶	
yahoo.co.jp	▷ · · · ·	
naver.com	▷	▷ ·
163.com	▷	
twc.com	▷	▷
libero.it	▷	▷ ·
yandex.ru	▷▷	▷
daum.net	▷▷	
cox.net	▷▷	▷
att.net	· · ·	·
wp.pl	▷	·
pacbell.net	· · ·	·
sohu.com	▷▷	▷

▶ TLS was used

· TLS was not used

▷ non-standard protocol was used

Methodology

- TLS (STARTTLS)
  - Tested top million provider's ability to accept SMTP TLS connections
  - TLS on POP, IMAP and HTTP for MUA→ MSA for top 22 providers
  - Examined `Received` headers of all messages received by control and providers for TLS use
- DKIM
  - Examined email headers for DKIM selector and examined DNS record for all messages
- SPF and DMARC
  - Queried for top million providers and generators
  - recorded policy (reject, quarantine, etc)
- DNSSEC
  - Checked for all DNS queries performed