No Need for Black Chambers

Testing TLS in the E-mail Ecosystem at Large

Wilfried Mayer, **Aaron Zauner**, Martin Mulazzani, Markus Huber (FH St-Poelten)

Overview

Background

Methodology

Results

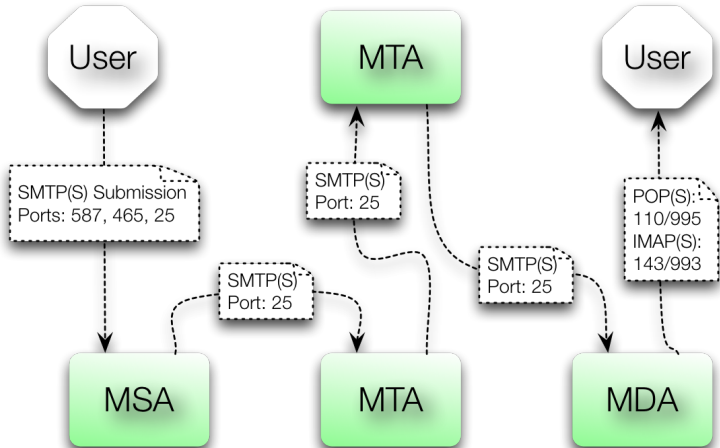Abuse-handling

Mitigation

Background

E-mail & TLS

- TLS in HTTP (aka HTTPS) is a well understood subject, lots of research
- We have't seen a lot of research into other application layer protocols
  - especially on high-confidentiality / traffic systems like E-mail protocols
- Many people use (at times moderately secured) public mail services (e.g. Gmail), but there're millions of mail-daemons around on the internet
- Misconfiguration and word-of-mouth considering crypto settings among admins
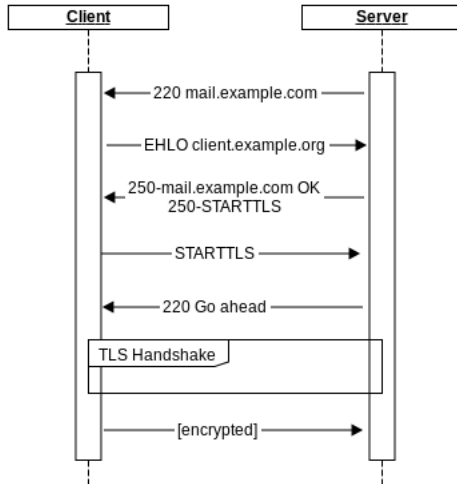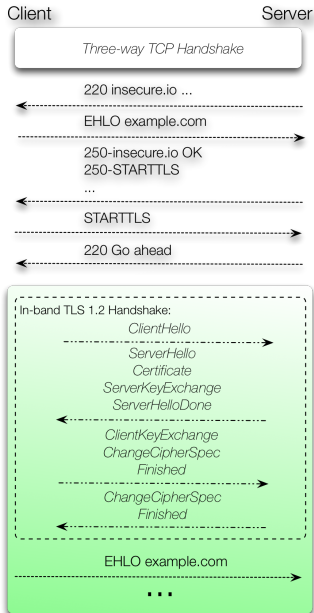
Recap: E-Mail protocols and their associated ports

Port	TLS	Protocol	Usage
25	STARTTLS	SMTP	E-mail transmission
110	STARTTLS	POP3	E-mail retrieval
143	STARTTLS	IMAP	E-mail retrieval
465	implicit	SMTPS	E-mail submission
587	STARTTLS	SMTP	E-mail submission
993	implicit	IMAPS	E-mail retrieval
995	implicit	POP3S	E-mail retrieval

Flow: mail submission until delivery

STARTTLS & SMTP

Client   Server

Three-way TCP Handshake

220 insecure.io ...
← -

EHLO example.com
- →

250-insecure.io OK
250-STARTTLS
...
← -

STARTTLS
- →

220 Go ahead
← -

In-band TLS 1.2 Handshake:
ClientHello
- →

ServerHello
Certificate
ServerKeyExchange
ServerHelloDone
← -

ClientKeyExchange
ChangeCipherSpec
Finished
- →

ChangeCipherSpec
Finished
← -

EHLO example.com
- →

● ● ●

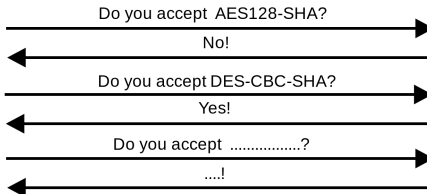# Methodology

So we scanned the entire IPv4 space!

- used `masscan` for discovery scans and X.509 Certificate collection
- customized `sslyze` and built a queueing framework around it
- More than 10 billion TLS handshakes over the course of a couple of months (not counting discovery scans)
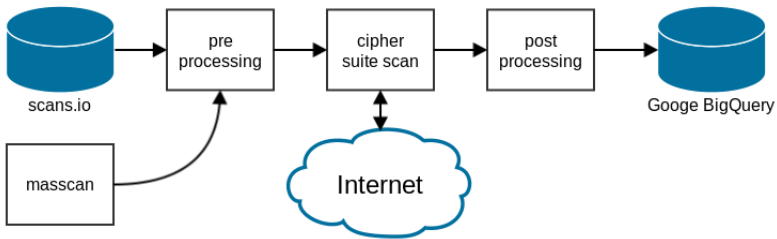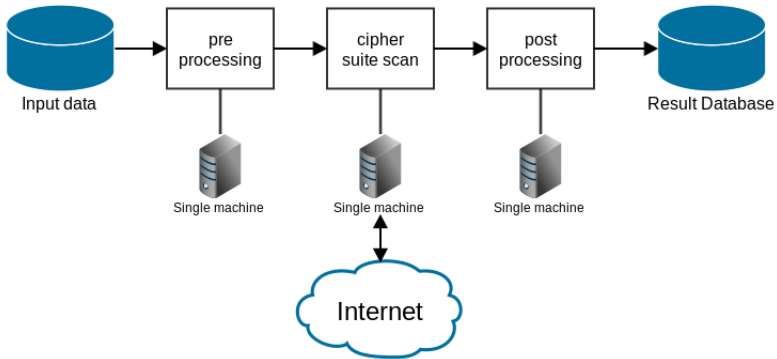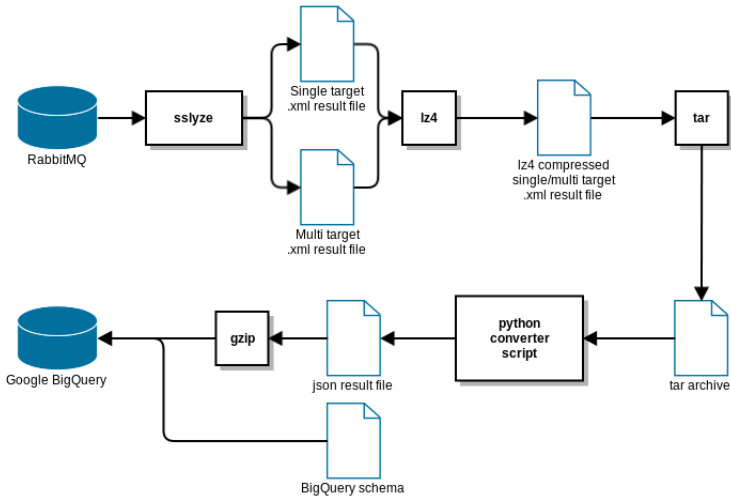
TLS enumeration

SSLyze

E-mail server

Do you accept AES128-SHA?

No!

Do you accept DES-CBC-SHA?

Yes!

Do you accept ....?

....!

Input dataset / collection

scans.io → pre processing → cipher suite scan → post processing → Google BigQuery

masscan → pre processing

cipher suite scan ↕ Internet

Scan flow

Processing flow

Results

- Conducted 20,270,768 scans over seven different TCP ports (april to august 2015)
- 18,381,936 valid reponses (551 TLS handshakes per host/port combination)
- 89.78% handshakes rejected, 8.26% accepted and 1.95% error (combinatorial explosion - protocols, ports, ciphersuites and SSL/TLS versions)

Protocol version support
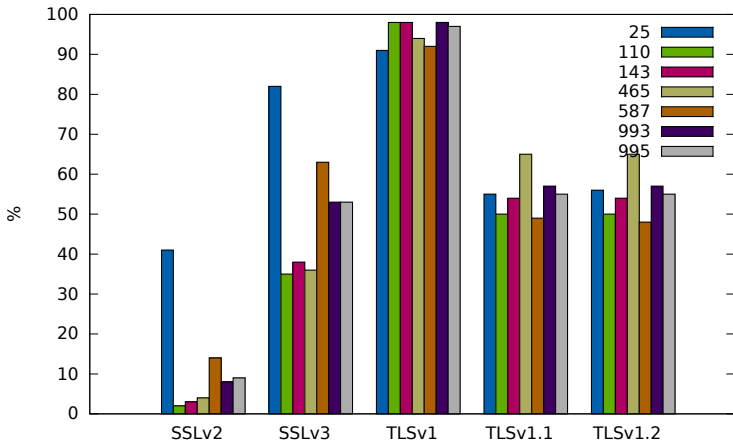
Key-exchange security

Diffie-Hellman - DH(E):

- Large amount of 512bit DH primes in SMTP (**EXPORT**!)
- DH group size below or equal to 1024 bit is very common in all protocols

Elliptic Curve Diffie-Hellman - ECDH(E):

- SMTP: 99% use `secp256r1` curve
- POP/IMAP: about 70% use `secp384r1` cuve
- Most use 256 bit group size

Key-exchange security: common primes

- SMTP: a 512 bit prime used by 64%, a 1024 bit prime used by 69% (Postfix)
- 512 bit Postfix prime:
  ```
  0x00883f00affc0c8ab835cde5c20f55d
  f063f1607bfce1335e41c1e03f3ab17f6
  635063673e10d73eb4eb468c4050e691a
  56e0145dec9b11f6454fad9ab4f70ba5b
  ```

Server-preferred TLS 1.0 ciphersuites

TLS 1.0 most widely supported (above 90% support in each mail protocol):

- `DHE-RSA-AES256-SHA`
  25: 49.64% 110: 68.03% 143: 67.89% 465: 79.32% 587: 47.72% 993: 68.39% 995: 69.65%

- `ECDHE-RSA-AES256-SHA`
  25: 43.67% 110: 6.44% 143: 6.84% 465: 11.49% 587: 23.01% 993: 7.43% 995: 6.13%

- `AES256-SHA`
  25: 4.94% 110: 17.67% 143: 17.89% 465: 7.17% 587: 16.41% 993: 17.23% 995: 17.25%
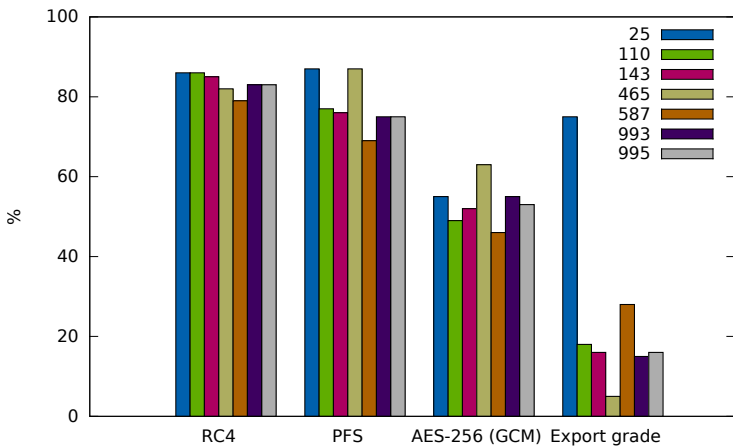
AUTH-PLAIN

- Not everything is crypto related
- If you do plaintext authentication *before* you upgrade to TLS, one can sniff/strip
- While some hosts offer `AUTH-PLAIN` without STARTTLS support, a lot offer it before doing an upgrade

Port	no STARTTLS	STARTTLS	Total Hosts
25	12.90%	24.21%	7,114,171
110	4.24%	63.86%	5,310,730
143	4.38%	66.97%	4,843,513
587	15.41%	42.80%	2,631,662

X.509 Certificates: self vs. CA-signed
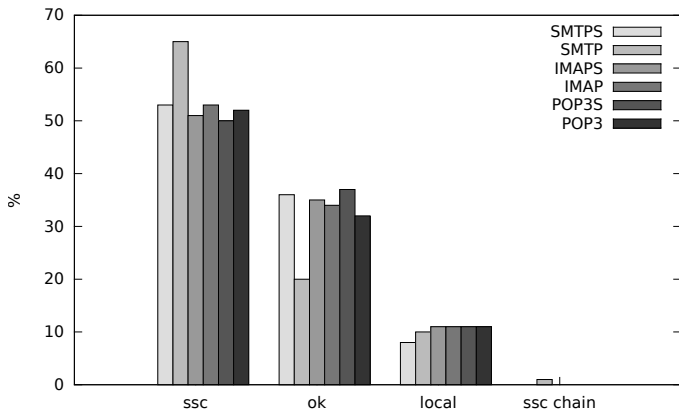
Compared to Mozilla Truststore:
ssc: self-signed, ok: CA signed, local: unable to get local issuer, ssc chain: self-signed in chain

X.509 Certificates (cont.)

- 99% of leafs use RSA (vs. e.g. ECDSA)
- Most SMTP(S) leafs and intermediates above 1024bit RSA (most 2k)
- Less than 10% use 4096bit RSA public keys
- SHA1 Fingerprint: `b16c...6e24` was provided on 85,635 IPs in 2 different /16 IP ranges

| Name	Key Size	IPs
Parallels Panel - Parallels	2048	306,852
imap.example.com - IMAP server	1024	261,741
Automatic...POP3 SSL key - Courier Mail Server	1024	87,246
Automatic...IMAP SSL key - Courier Mail Server	1024	83,976
Plesk - Parallels	2048	68,930
localhost.localdomain - SomeOrganizationalUnit	1024	26,248
localhost - Dovecot mail server	2048	13,134
plesk - Plesk - SWsoft, Inc.	2048	14,207

Common Name (Issuer Common Name)	Fingerprint	Port	IPs
*.nazwa.pl (nazwaSSL)	b16c…6e24	25	40,568
		465	81,514
		587	84,318
		993	85,637
		995	85,451
*.pair.com (USERTrust RSA Organization …)	a42d…768f	25	15,573
		110	60,588
		143	13,186
		465	63,248
		587	61,933
		993	64,682
		995	64,763
*.home.pl (RapidSSL SHA256 CA - G3)	8a4f…6932	110	126,174
		143	26,735
		587	125,075
*.home.pl (AlphaSSL CA - SHA256 - G2)	c4db…a488	993	128,839
		995	126,102
*.sakura.ne.jp (RapidSSL SHA256 CA - G3)	964b…c39e	25	16,573
*.prod.phx3.secureserver.net (Starfield …)	f336…ac57	993	61,307
		995	61,250

Table : Common leaf certificates

X.509 Certificates: weak RSA keys

- Analyzed 40,268,806 collected certificates similar to Heninger et al. "Mining Your Ps and Qs"
- 30,757,242 RSA moduli
- 2,354,090 uniques
- Fast-GCD (algo. due to djb, impl. due to Heninger et al.)
- 456 GCDs found (= RSA private keys recovered)

X.509 Certificates: volatility
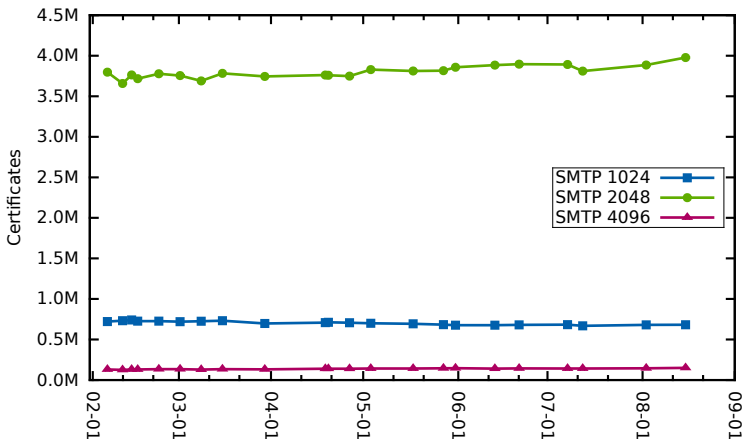
based on scans.io data

X.509 Certificates: volatility (cont.)
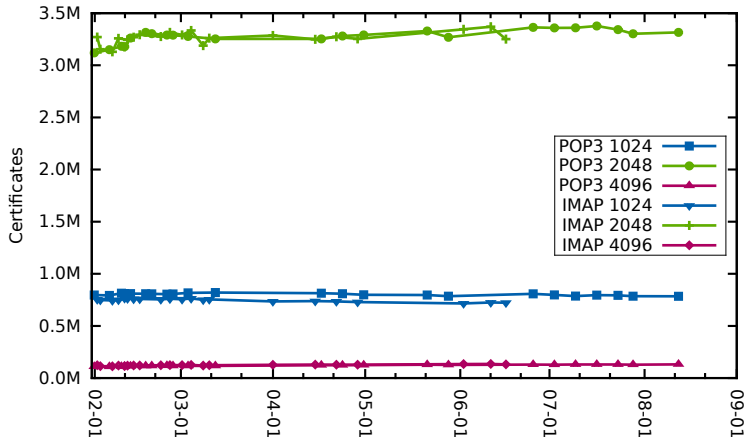
based on scans.io data

Collateral damage

- open-source mail daemons are easily DoS'ed - test carefully
- (re)discovered a `dovecot` bug: (CVE-2015-3420, investigated and reported by Hanno Boeck)
- `OpenSSL` will establish **EXPORT** ciphersuites with TLS 1.1 and 1.2 (although the spec explicitly says `MUST NOT`). Core-team reponse: confusion and finally "not a security issue". you are implementing a network security / crypto protocol the wrong way?! (AFAIK unfixed)

Abuse-handling

Scanning considerations

- Get an upstream ISP that is willing to help your research
- Depending on local law: maybe even a good team of lawyers
- People **will be pissed off**!
- ..they even might write to your management or unrelated 3rd parties
- WHOIS / RIPE entry explaining the research project - abuse contact
- webpage on the scan host explaining the research project - abuse contact
- handle each mail request professionally - regardless

Some statistics

- Recieved 89 mails in total (as of submitting the paper in august)
- 52 auto generated by IDS / ops tooling
- 16 simple blacklisting requests (sometimes large CIDR ranges)
- A few were blatantly rude
- A few very interested in our work
- We also recieve quite some amount of spam on our abuse address

You'll recieve these mails as well

From: ███████████████ secureserver.net
To: abuse@sba-research.org
Cc: abuse@ipax.at

Seriously. 617 connections to my mail server in 1 minute?

FUCK OFF.

─ asshole.txt

```
May  5 06:00:06 ip-████████/var/qmail/bin/relaylock[30532]: /var/qmail/bin/relaylock: mail from 93.189.25.174:13925 (scan.sba-research.org)
May  5 06:00:06 ip-████████/var/qmail/bin/relaylock[30533]: /var/qmail/bin/relaylock: mail from 93.189.25.174:15155 (scan.sba-research.org)
May  5 06:00:07 ip-████████/var/qmail/bin/relaylock[30536]: /var/qmail/bin/relaylock: mail from 93.189.25.174:16925 (scan.sba-research.org)
May  5 06:00:07 ip-████████/var/qmail/bin/relaylock[30535]: /var/qmail/bin/relaylock: mail from 93.189.25.174:16923 (scan.sba-research.org)
May  5 06:00:07 ip-████████/var/qmail/bin/relaylock[30537]: /var/qmail/bin/relaylock: mail from 93.189.25.174:16926 (scan.sba-research.org)
```

Mitigation

Solid server configurations & awareness

- `bettercrypto.org`
- Mozilla Server TLS Security guide:
  `https://wiki.mozilla.org/`
  `Security/Server_Side_TLS`
- RFC 7457 (Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)) and RFC 7525 (Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS))
- educating administrators, managers and operational people

Key pinning

- Public keys get pinned on first use (TOFU)
- Elegant solution but difficult deployment model (non-technies won't deploy)
- HPKP (for HTTPS) available, not really deployed yet
- TACK(.io) is a universal TLS extension that would also fit e.g. STARTTLS protocols (deadlocked in IETF)

DNSSEC / DANE

- DANE is a very nice protocol but:
- DNSSEC shifts trust to TLDs instead of CAs
- DNSSEC has huge deployment problems (especially on end-user devices)
- It's still one option that *could* work, so why not deploy in addition?

DKIM, SPF, DMARC

especially if you're hosting a large environment you *MUST* deploy:

- DKIM (DomainKeys Identified Mail)
- SPF (Sender Policy Framework)
- DMARC (Domain-based Message Authentication, Reporting, and Conformance)

New efforts in IETF and beyond

- DEEP (Deployable Enhanced Email Privacy) - similar to how HSTS works for HTTPS
- Let's Encrypt by EFF et al (beta live since tuesday!)
- `draft-ietf-uta-email-tls-certs-05`: Identity verification for SMTP/POP/IMAP/ManageSieve updates various RFCs
- IETF works on a new OpenPGP spec
- Continued scans necessary to track change over time
- Publish all data sets!

Questions?

abuse@sba-research.org