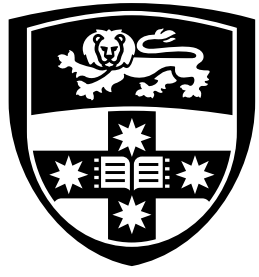
TLS in the wild

An Internet-wide analysis of TLS-based protocols for electronic communication

Ralph Holz

School of Information Technologies
Faculty of Engineering & Information Technologies



THE UNIVERSITY OF SYDNEY

Team

This is joint work with

- Johanna Amann—ICSI
- Olivier Mehani, Dali Kafaar—Data61
- Matthias Wachs—TUM

Electronic communication

Email

- Email: 4.1B accounts in 2014; 5.2B in 2018
- Most prevalent, near-instant form of communication

Chat

- Once dominant instant-messaging (IRC!)
- Newer: XMPP (also proprietary use)

Research question: how secure are these?

Securing email and chat

SSL/TLS is the common solution

- Responder authenticates with certificate
- Initiator usually uses protocol-specific method
- Direct SSL/TLS vs. STARTTLS in-band upgrade
  - Susceptible to active man-in-the-middle attack

Email protocols

- Email submission: SMTP, SUBMISSION (= SMTP on 587)
- Email retrieval: IMAP, POP3

Investigated properties

In this talk:

- Deployment numbers
- STARTTLS
- Versions
- Ciphers used/negotiated
- Responder authentication
- Initiator authentication

Focus mostly on email. There is more in the paper.

Data collection (July 2015)

Active scans

- To determine state of *deployment*
- `zmap` in the 'frontend', `openssl`-based 'backend'

Passive monitoring

- To determine *actual use*
- Bro monitor, UCB network

Active scans (July 2015)

Protocol (port)	No. hosts	SSL/TLS	Certs	Interm. (unique)
SMTP†,‡ (25)	**12.5M**	3.8M	**1.4M**	2.2M (1.05%)
SMTPS‡ (465)	**7.2M**	3.4M	**801k**	2.6M (0.4%)
SUBMISSION†,‡ (587)	**7.8M**	3.4M	**754k**	2.6M (0.62%)
IMAP†,‡ (143)	**8M**	4.1M	**1M**	2.4M (0.54%)
IMAPS (993)	**6.3M**	4.1M	**1.1M**	2.8M (0.6%)
POP3†,‡ (110)	**8.9M**	4.1M	**998k**	2.3M (0.44%)
POP3S (995)	**5.2M**	2.8M	**748k**	1.8M (0.44%)
IRC† (6667)	2.6M	3.7k	3k	0.6k (13.17%)
IRCS (6697)	2M	8.6k	6.3k	2.5k (12.35%)
XMPP, C2S†,‡ (5222)	2.2M	54k	39k	5.9k (32.28%)
XMPPS, C2S (5223)	2.2M	70k	39k	33k (8.5%)
XMPP, S2S†,‡ (5269)	2.5M	9.7k	6.2k	5.9k (32.28%)
XMPPS, S2S‡ (5270)	2M	1.7k	1.1k	0.8k (18.77%)
HTTPS (443)	42.7M	27.2M	8.6M	25M (0.93%)

† = STARTTLS, ‡ = fallback to SSL 3.

Passive observation (July 2015)

Protocol	Port	Connections	Servers
SMTP†	25	**3.9M**	**8.6k**
SMTPS	465	37k	266
SUBMISSION†	587	**7.8M**	**373**
IMAP†	143	26k	239
IMAPS	993	**4.6M**	**1.2k**
POP3†	110	19k	110
POP3S	995	**160k**	**341**
IRC†	6667	50	2
IRCS	6697	18k	15
XMPP, C2S†	5222	14k	229
XMPPS, C2S	5223	**911k**	**2k**
XMPP, S2S†	5269	175	2
XMPPS, S2S	5270	0	0

† = STARTTLS.

STARTTLS support and use

	Active probing	Passive monitoring		
Protocol	**Supported & upgraded**	**Supporting servers**	**Offering connections**	**Upgraded connections**
SMTP	30.82%	59%	97%	94%
SUBMISSION	43.03%	98%	99.9%	97%
IMAP	50.91%	77%	70%	44%
POP3	45.62%	55%	73%	62%

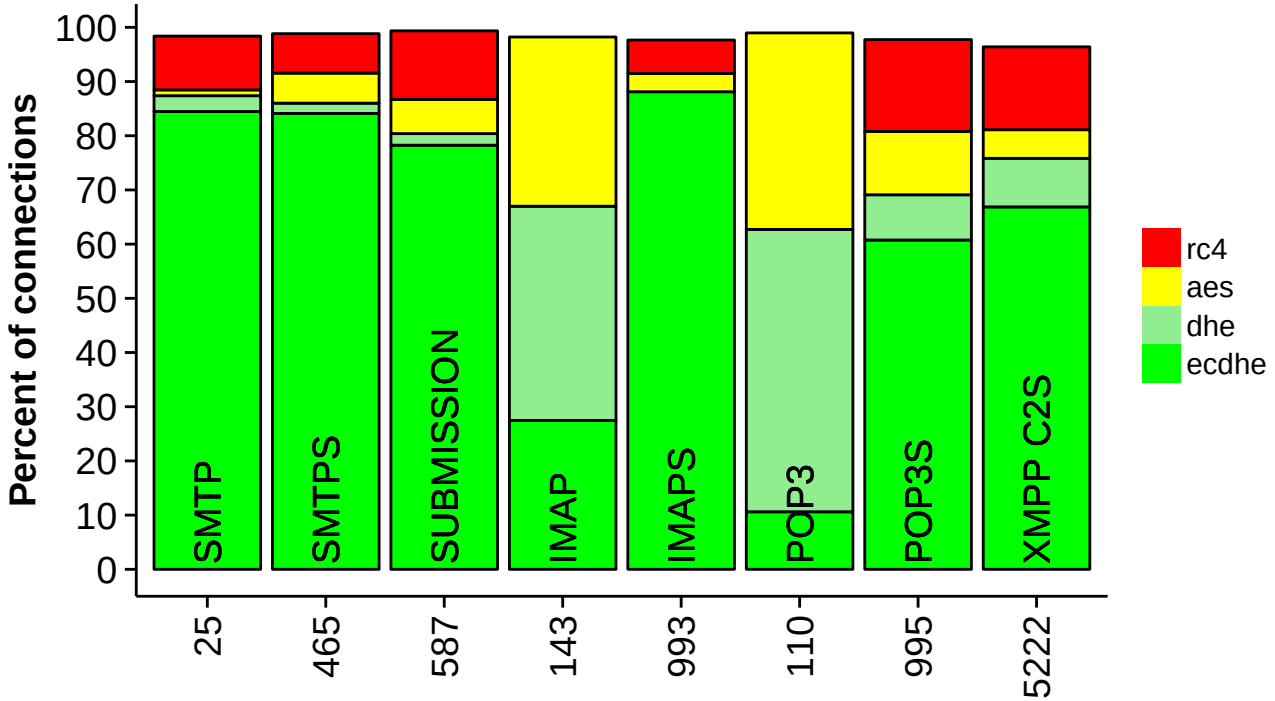
- **Deployment** as scanned: 30-50%—not good
- **Use** as monitored: better, but still not very good
  - SMTP: almost all connections upgrade
  - But not in IMAP/POP3

SSL/TLS versions in use (passive observation)

Version	Active probing Negotiated with server	Passive monitoring Observed connections
SSL 3	0.02%	1.74%
TLS 1.0	39.26%	58.79%
TLS 1.1	0.23%	0.1%
TLS 1.2	60.48%	39.37%

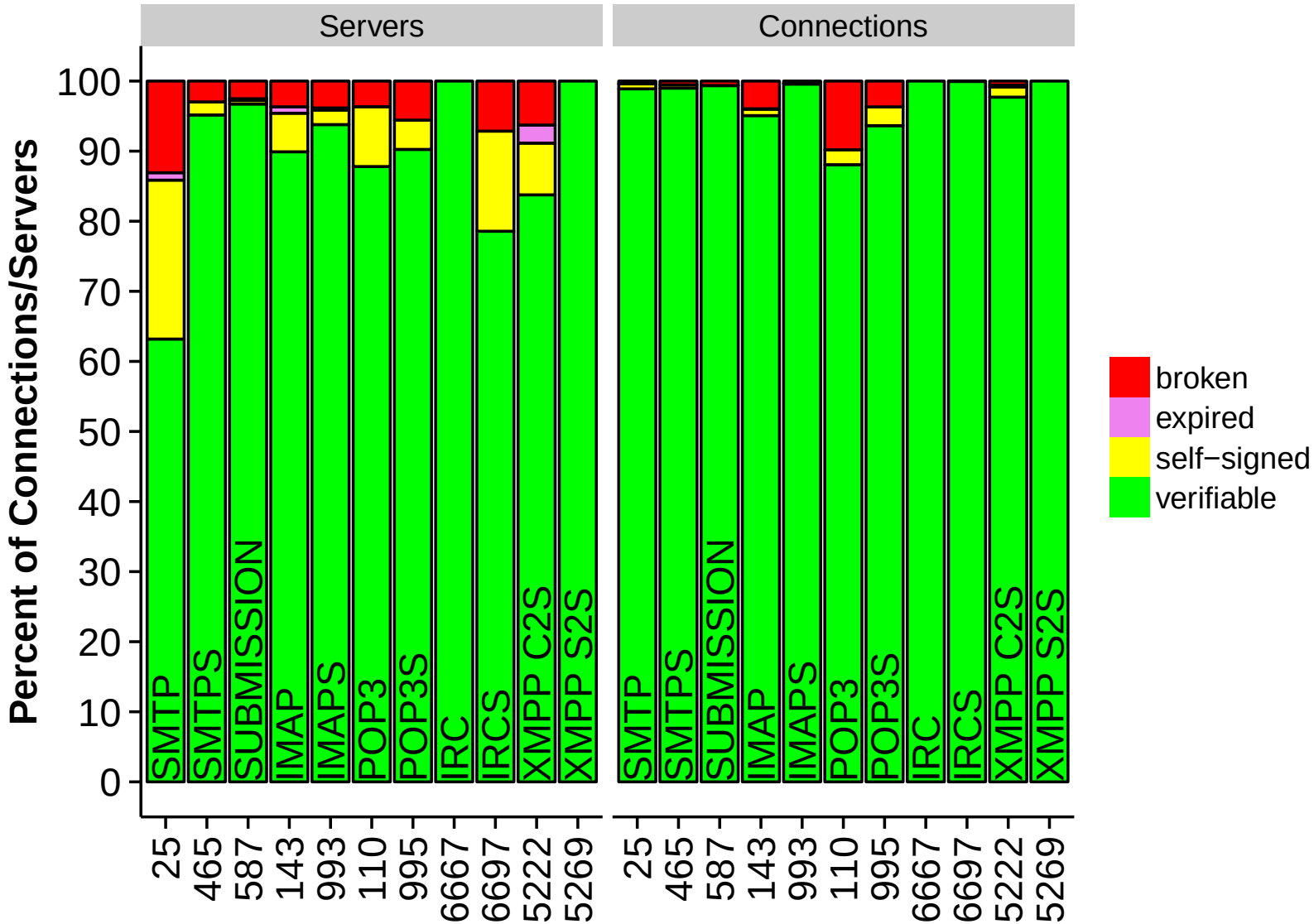
- SSL 3 is almost dead, some use left—are these old clients?
- TLS 1.2 most common in deployments, but not in use (not good)

Ciphers and forward secrecy (from monitoring)

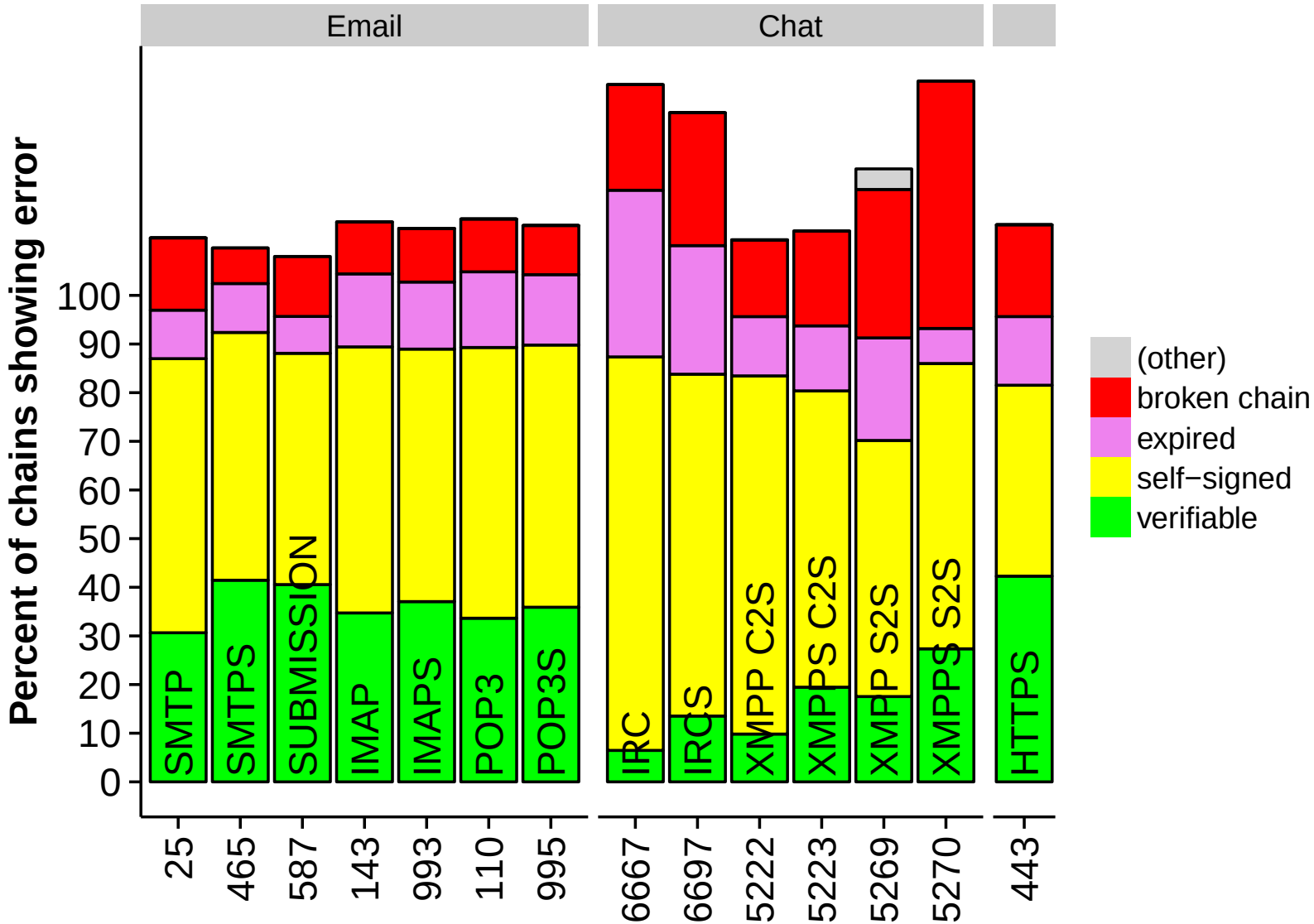


- RC4 has use (up to 17%, not good)
- ECDHE has much use
- DHE: 76% are 1024 bit, 22% 2048 bit, 1.4% are 768 bit

Responder authentication (monitored → use)



Responder authentication (scanned → deployed)



Initiator authentication: SUBMISSION

Combinations offered	Advertised	Servers
PLAIN, LOGIN	**2.1M**	**75.15%**
LOGIN, PLAIN	**224k**	**8.51%**
LOGIN, CRAM-MD5, PLAIN	96k	3.45%
LOGIN, PLAIN, CRAM-MD5	45k	1.63%
DIGEST-MD5, CRAM-MD5, PLAIN, LOGIN	36k	1.30%
CRAM-MD5, PLAIN, LOGIN	29k	1.04%
PLAIN, LOGIN, CRAM-MD5	25k	0.89%
...	...	...

- Plaintext-based methods the vast majority
- Even where CRAM is offered, it's usually not first choice
- No SCRAM

Risks and threats: SSL/TLS-level

STARTTLS

- Less than 50% of servers support upgrade
- But big providers do, have large share of traffic
- MITM vulnerability (reported to be exploited)

Ciphers

- For some protocols, 17% of RC4 traffic (WWW: 10%)
- For some protocols, $\approx$ 30% of connections not forward-secure
- Diffie-Hellman keys $\leq$ 1024 bit in $>$ 60% of connections

Risks and threats: authentication

Responder

- Many self-signed or expired certs, broken chains
- Big providers have correct setups
- Sending mail to 'small' domain/provider means risks of MITM
- We know from Foster *et al.* that mail servers do not verify certs in outgoing connections

Initiator

- Plain-text login pervasive
- CRAM not used much (and no implementations for SCRAM?)

Recommendations

A few things we can do

- Warnings in user agents that mail will be sent in plain
  $\rightarrow$ Google has implemented this now
- Flag-day for encryption (as for XMPP)
- Combine setup with automatic use of, *e.g.*, Let's Encrypt
- Ship safe defaults
- Follow guides, *e.g.*, `bettercrypto.org`
- More in the paper

Questions?

email: `ralph.holz@sydney.edu.au`

Recommendations

A few things we can do

- Warnings in user agents that mail will be sent in plain
  $\rightarrow$ Google has implemented this now
- Flag-day for encryption (as for XMPP)
- Combine setup with automatic use of, *e.g.*, Let's Encrypt
- Ship safe defaults
- Follow guides, *e.g.*, `bettercrypto.org`
- More in the paper

Questions?

email: `ralph.holz@sydney.edu.au`

Summary

We found light and shadow

- Connections between big providers are already (reasonably) secure
- The risk lies with mail from/to remaining providers
- User has no indication of security level at which email will be sent
- Authentication mechanisms (initiator) are very poor

Questions?

email: ralph.holz@sydney.edu.au

Summary

We found light and shadow

- Connections between big providers are already (reasonably) secure
- The risk lies with mail from/to remaining providers
- User has no indication of security level at which email will be sent
- Authentication mechanisms (initiator) are very poor

Questions?

email: ralph.holz@sydney.edu.au

On XMPP

Majority of certs for XMPP are self-signed.

- Inspection of Common Names shows: proprietary use
  - Content Distribution Network (`incapsula.com`)
  - Apple Push
  - Samsung Push
  - Unified Communication solutions

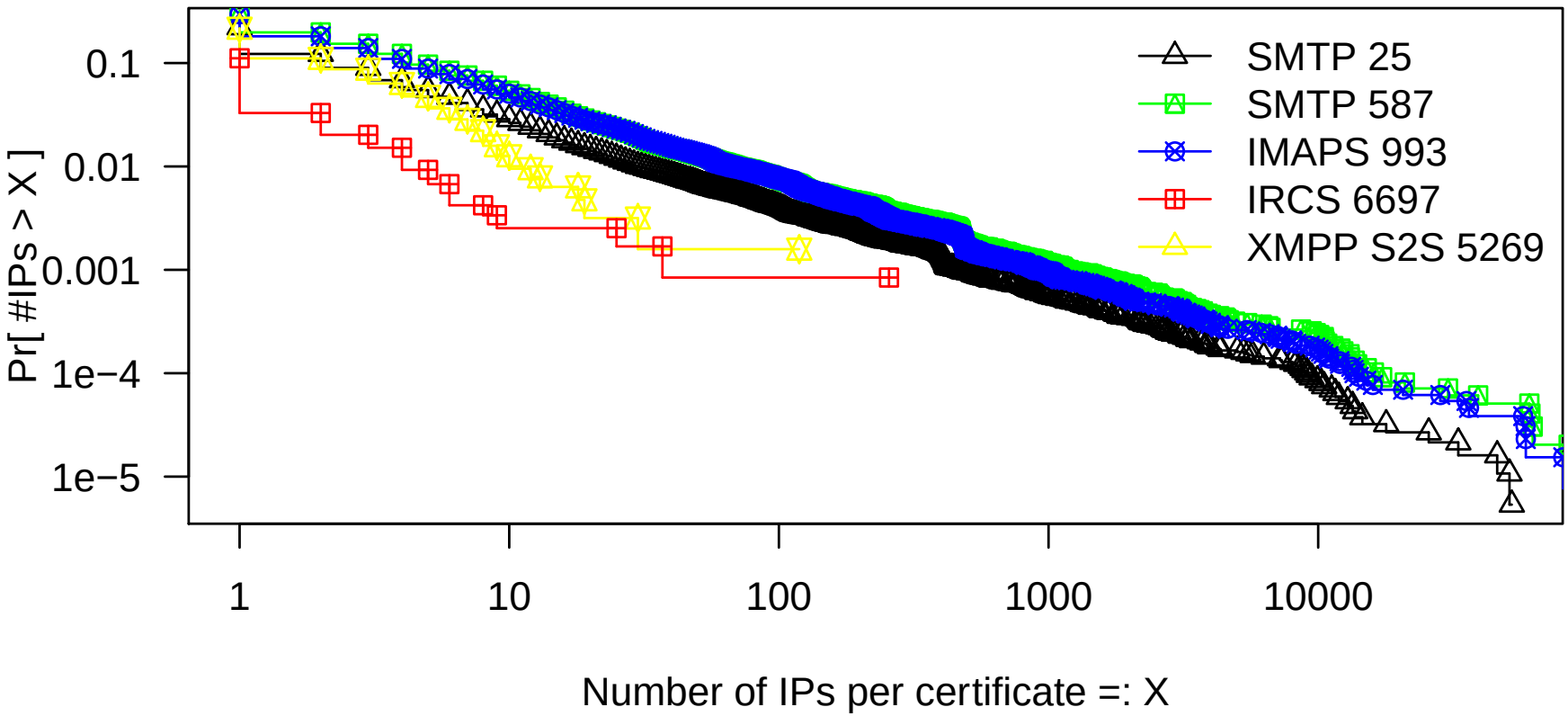
Oddity of scans

The Internet has background noise.

- Independent of port you scan, about 0.07-0.1% of IPs reply with SYN/ACK, but do not carry out a handshake
- Confirmed with authors of `zmap`
- Important to keep in mind when investigating protocols with smaller deployments, where SSL/TLS does not seem to succeed very often

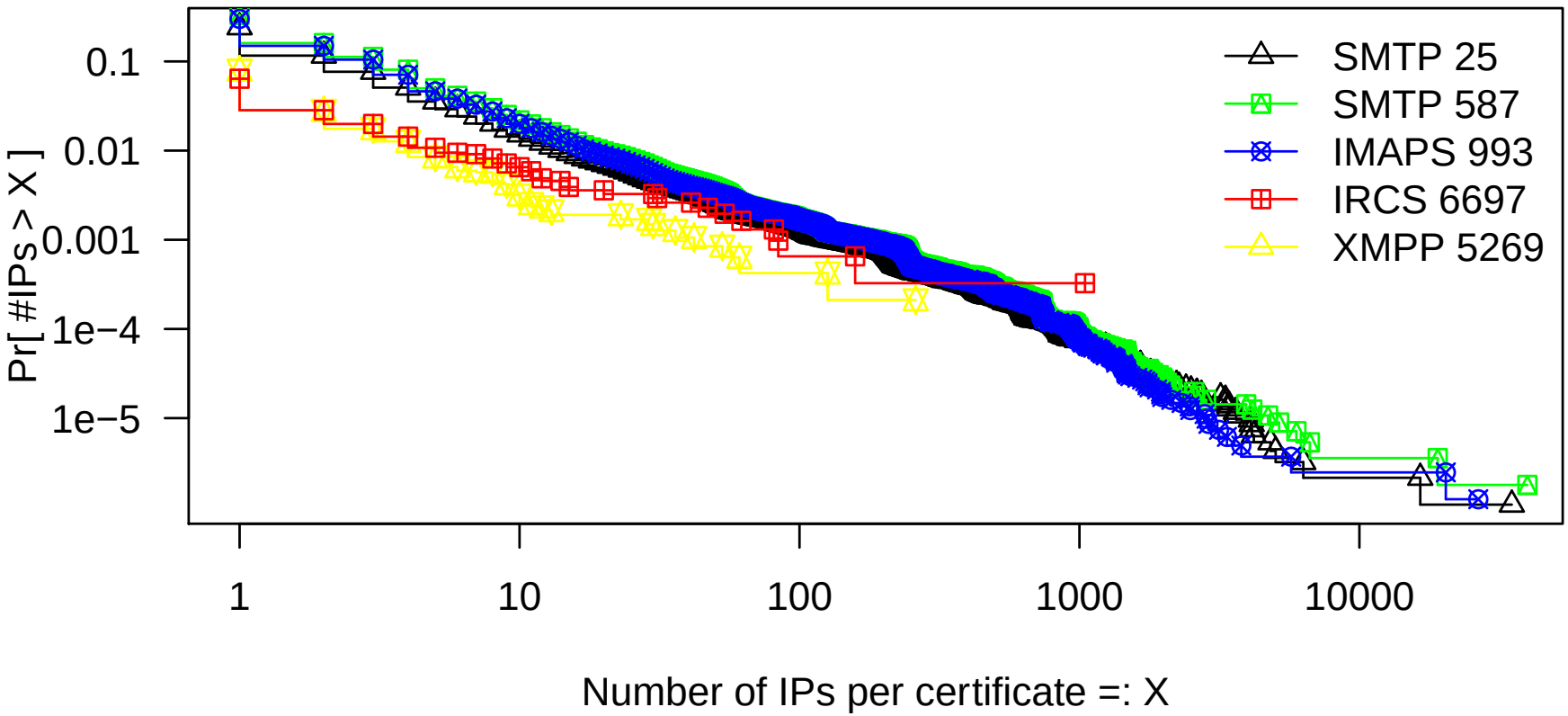
Certificate reuse—valid certs

Much reuse, even among valid certs

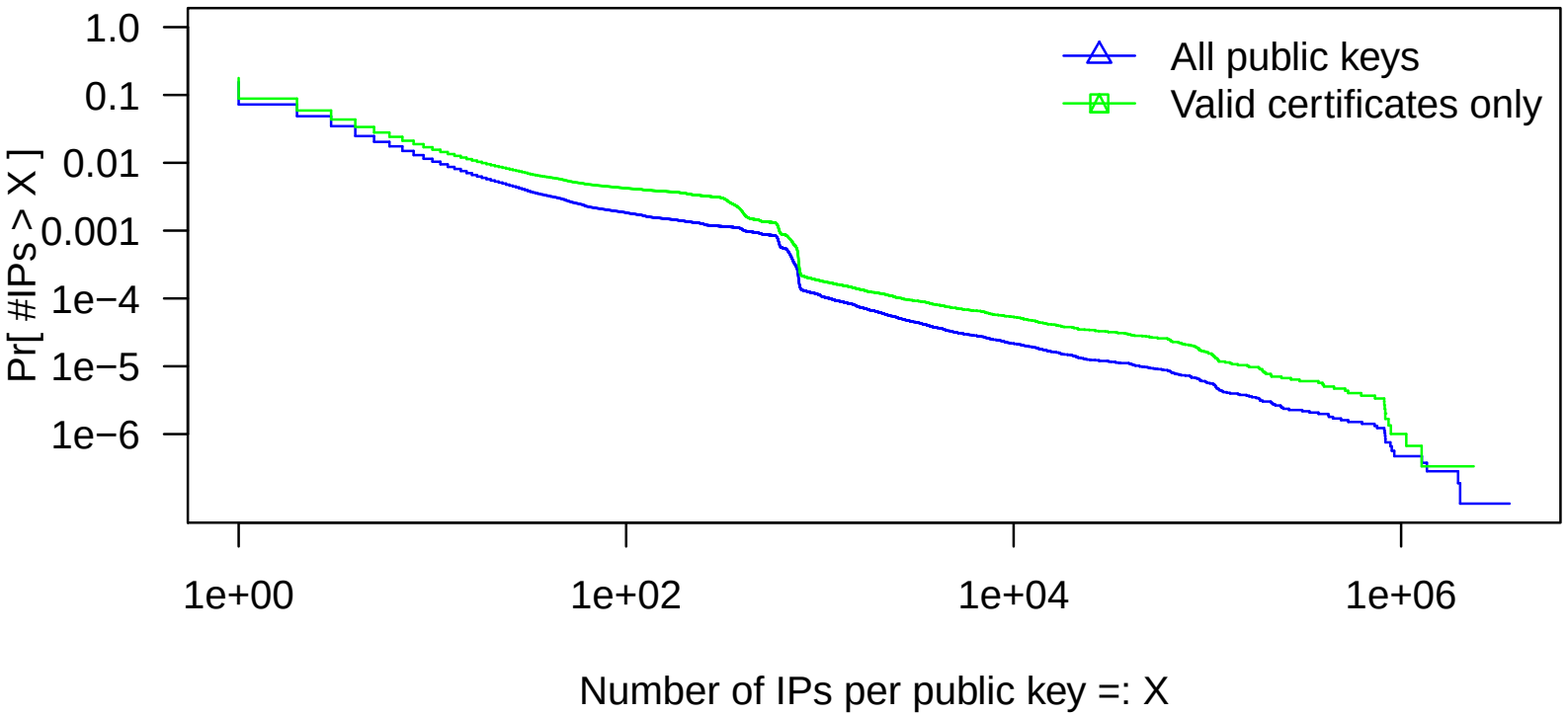


Certificate reuse—self-signed

Many default certs from default configurations



Key reuse across *all* protocols



Oddity in IMAPS...

Common name	Occurrences
*.securesites.com	88k
*.sslcert35.com	31k
localhost/emailAddress=webaster@localhost	27k
localhost/emailAddress=webaster@localhost	21k
*.he.net	19k
www.update.microsoft.com	19k
*.securesites.net	11k
*.cbeyondhosting2.com	11k
*.hostingterra.com	11k
plesk/emailAddress=info@plesk.com	6k

Table: Selected Common Names in IMAPS certificates.

Oddity in IMAPS...

Common name	Occurrences
*.securesites.com	88k
*.sslcert35.com	31k
localhost/emailAddress=webaster@localhost	27k
localhost/emailAddress=webaster@localhost	21k
*.he.net	19k
www.update.microsoft.com	19k
*.securesites.net	11k
*.cbeyondhosting2.com	11k
*.hostingterra.com	11k
plesk/emailAddress=info@plesk.com	6k

Table: Selected Common Names in IMAPS certificates.

Mapping to ASes

AS number	Registration information	CIRCL rank
3257	TINET-BACKBONE Tinet SpA, DE	9532
3731	AFNCA-ASN - AFNCA Inc., US	4804
4250	ALENT-ASN-1 - Alentus Corporation, US	9180
4436	AS-GTT-4436 - nLayer Communications, Inc., US	10,730
6762	SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT	11,887
11346	CIAS - Critical Issue Inc., US	557
13030	INIT7 Init7 (Switzerland) Ltd., CH	6255
14618	Amazon.com Inc., US	4139
16509	Amazon.com Inc., US	3143
18779	EGIHOSTING - EGIHosting, US	4712
21321	ARETI-AS Areti Internet Ltd.,GB	2828
23352	SERVERCENTRAL - Server Central Network, US	11,135
26642	AFAS - AnchorFree Inc., US	–
41095	IPTP IPTP LTD, NL	6330
54500	18779 - EGIHosting, US	–