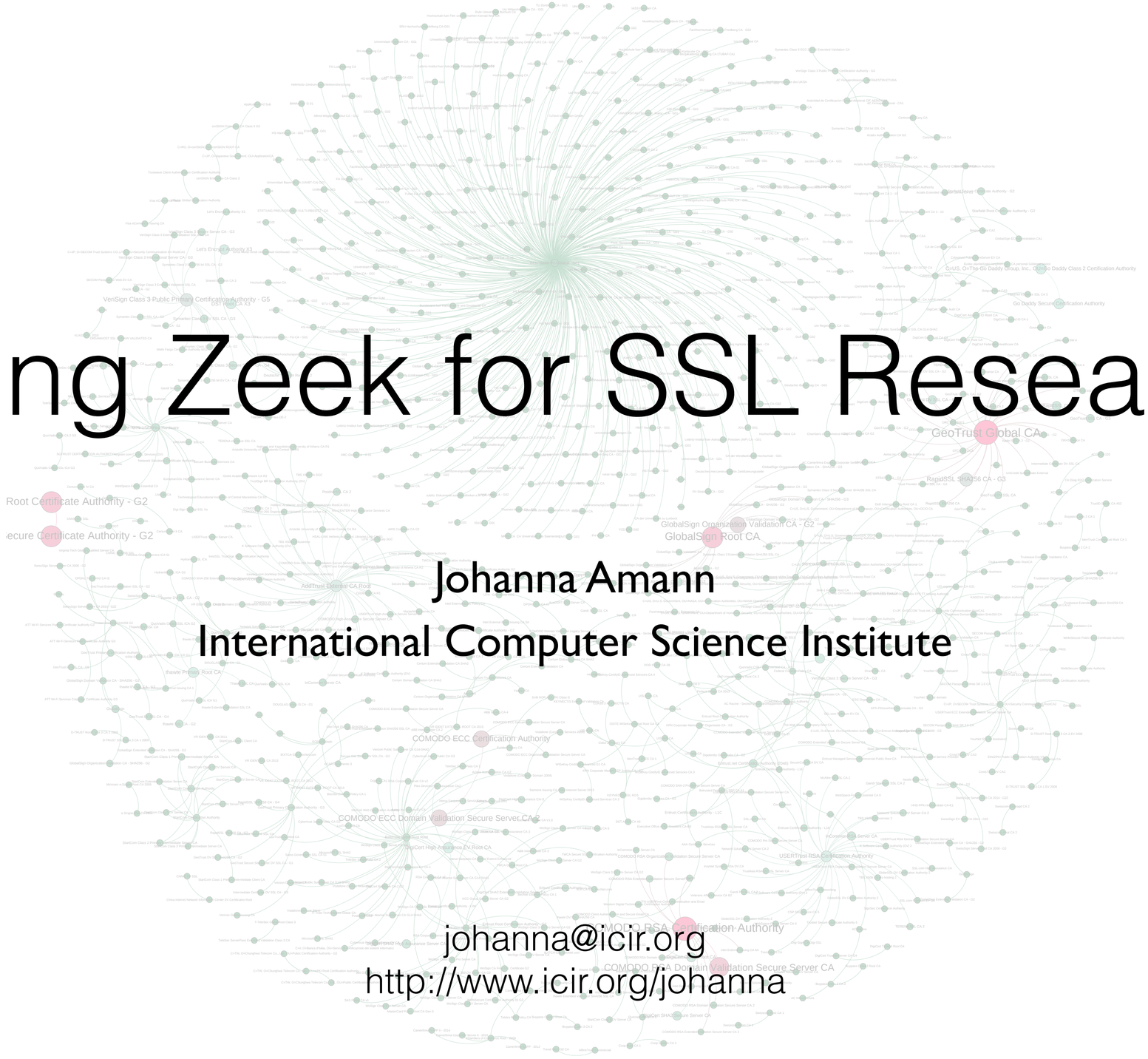
Using Zeek for SSL Research



Johanna Amann

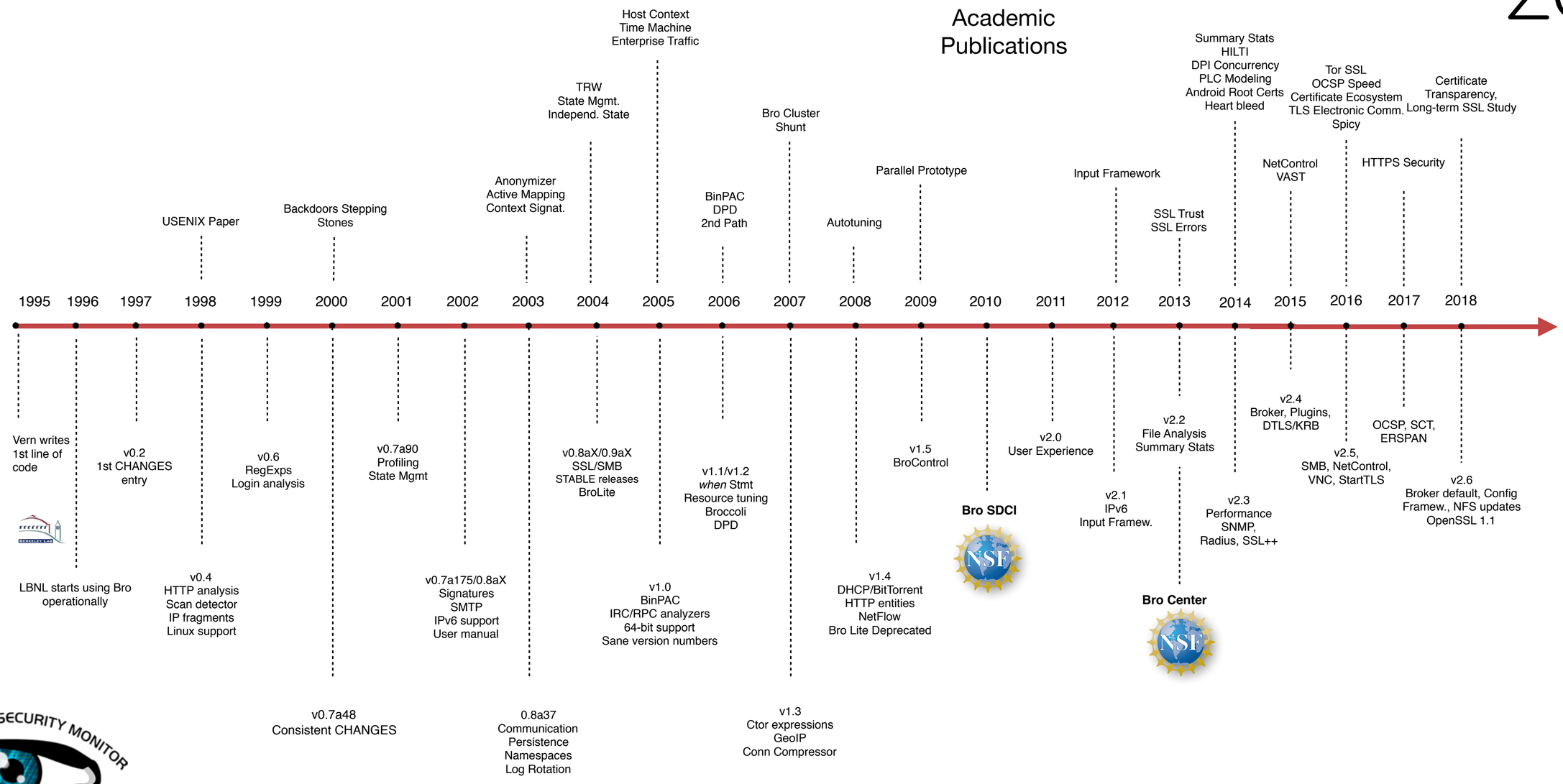
International Computer Science Institute

johanna@icir.org

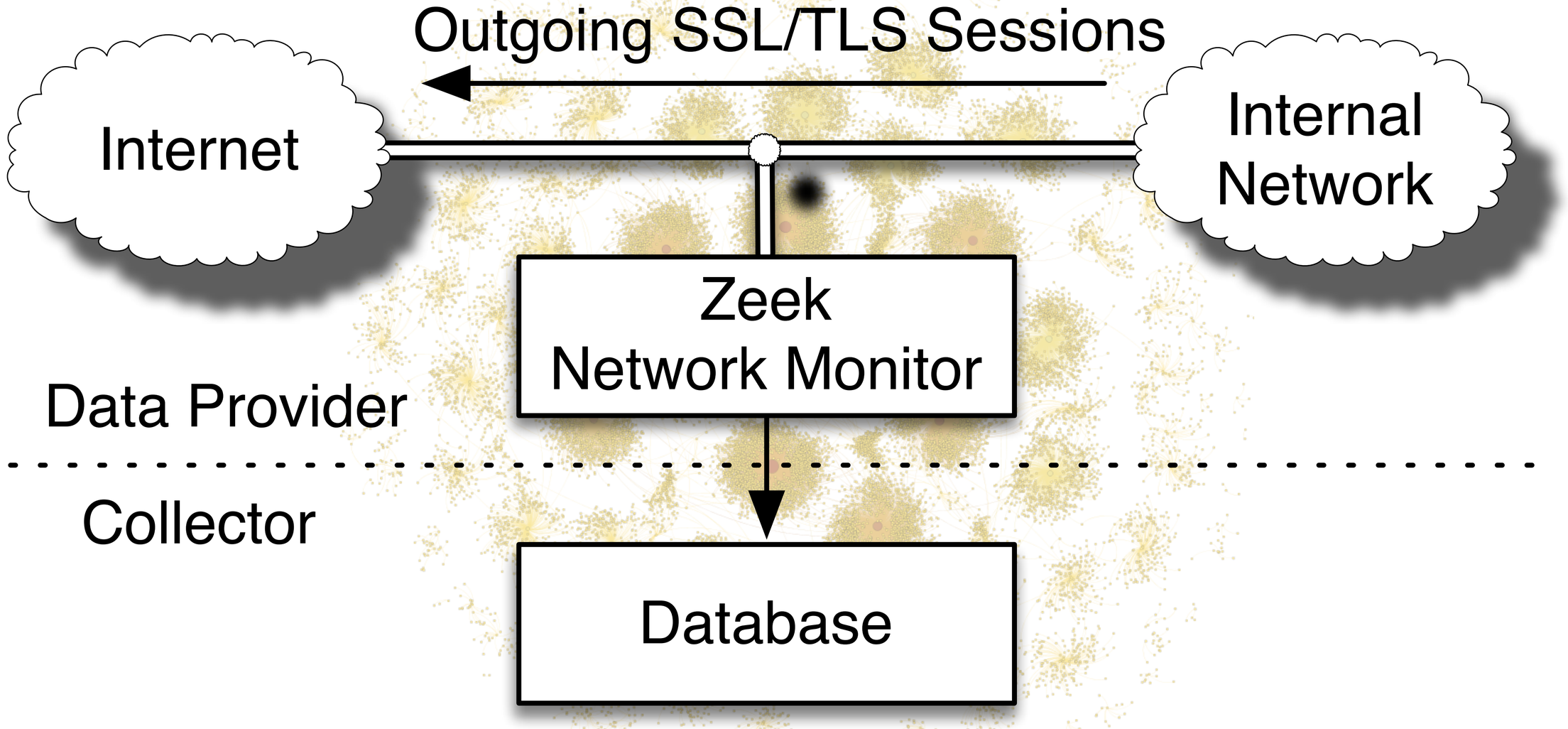
http://www.icir.org/johanna

ICSI
INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Zeek History

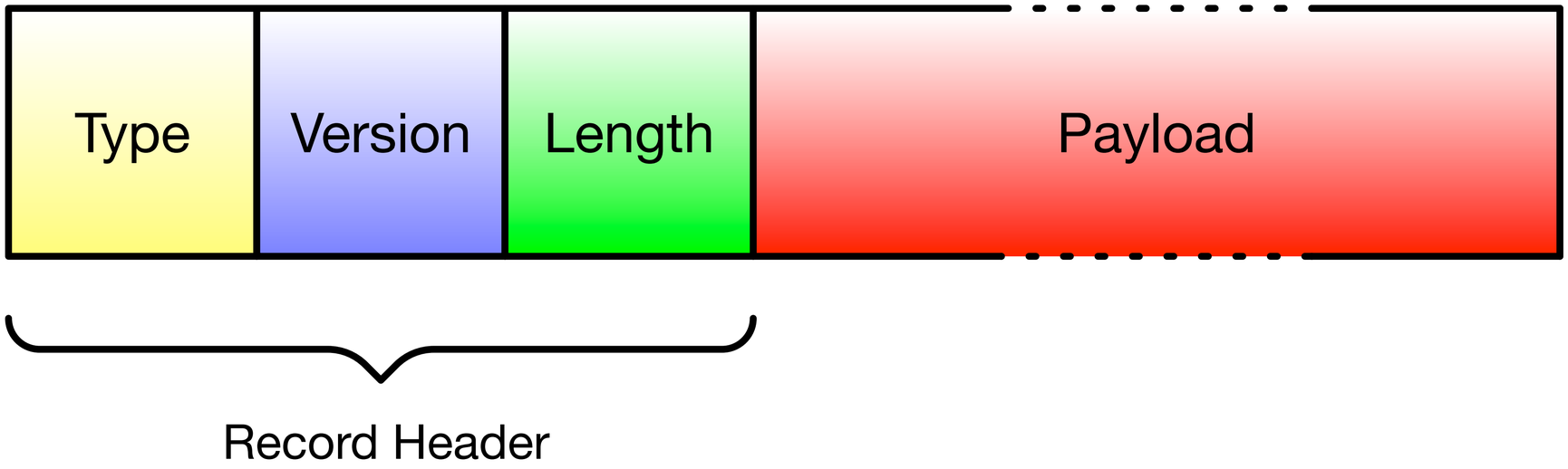


ICSI Notary


Outgoing SSL/TLS Sessions
Internet
Internal Network
Zeek Network Monitor
Data Provider
Collector
Database

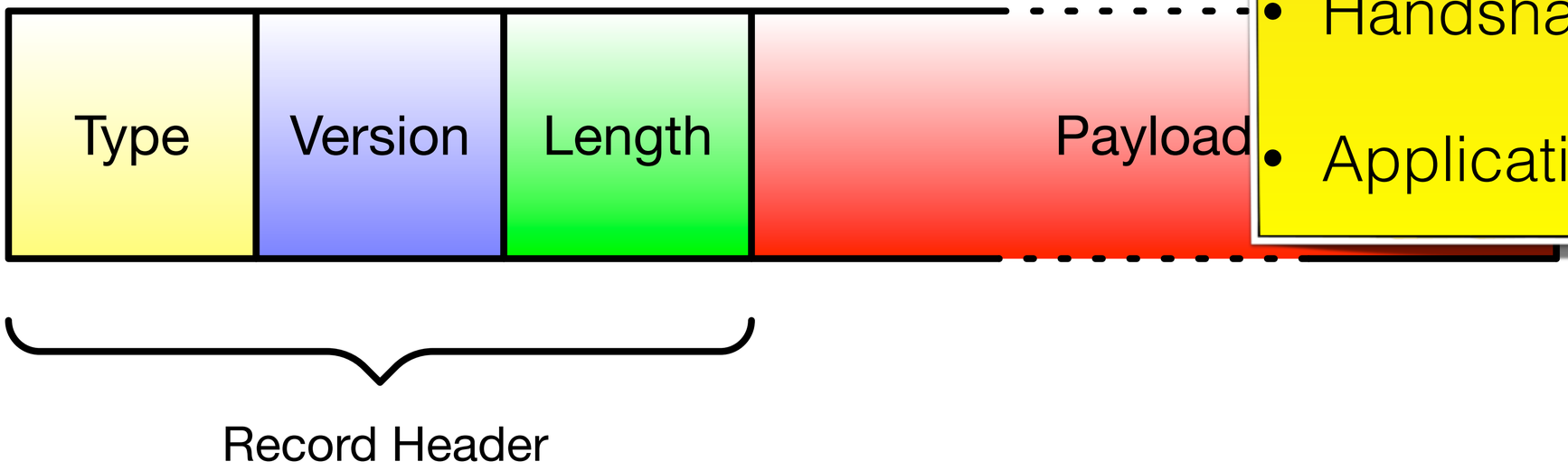
SSL/TLS Protocol

- Record based protocol
- Record header is never encrypted, only payload is (after the handshake is done)



SSL/TLS Protocol

- Record based protocol
- Record header is never encrypted, only payloa
  (after the handshake is done)

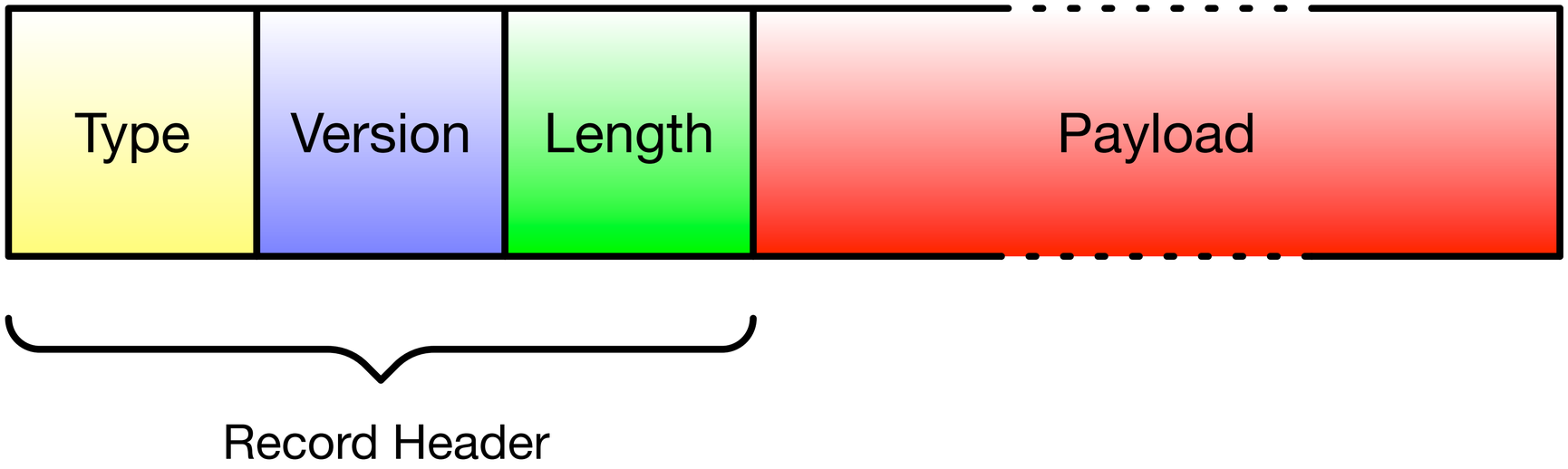


Common record types:

- Change Cipher Spec
- Alert
- Handshake
- Application Data

SSL/TLS Protocol

- Record based protocol
- Record header is never encrypted, only payload is (after the handshake is done)



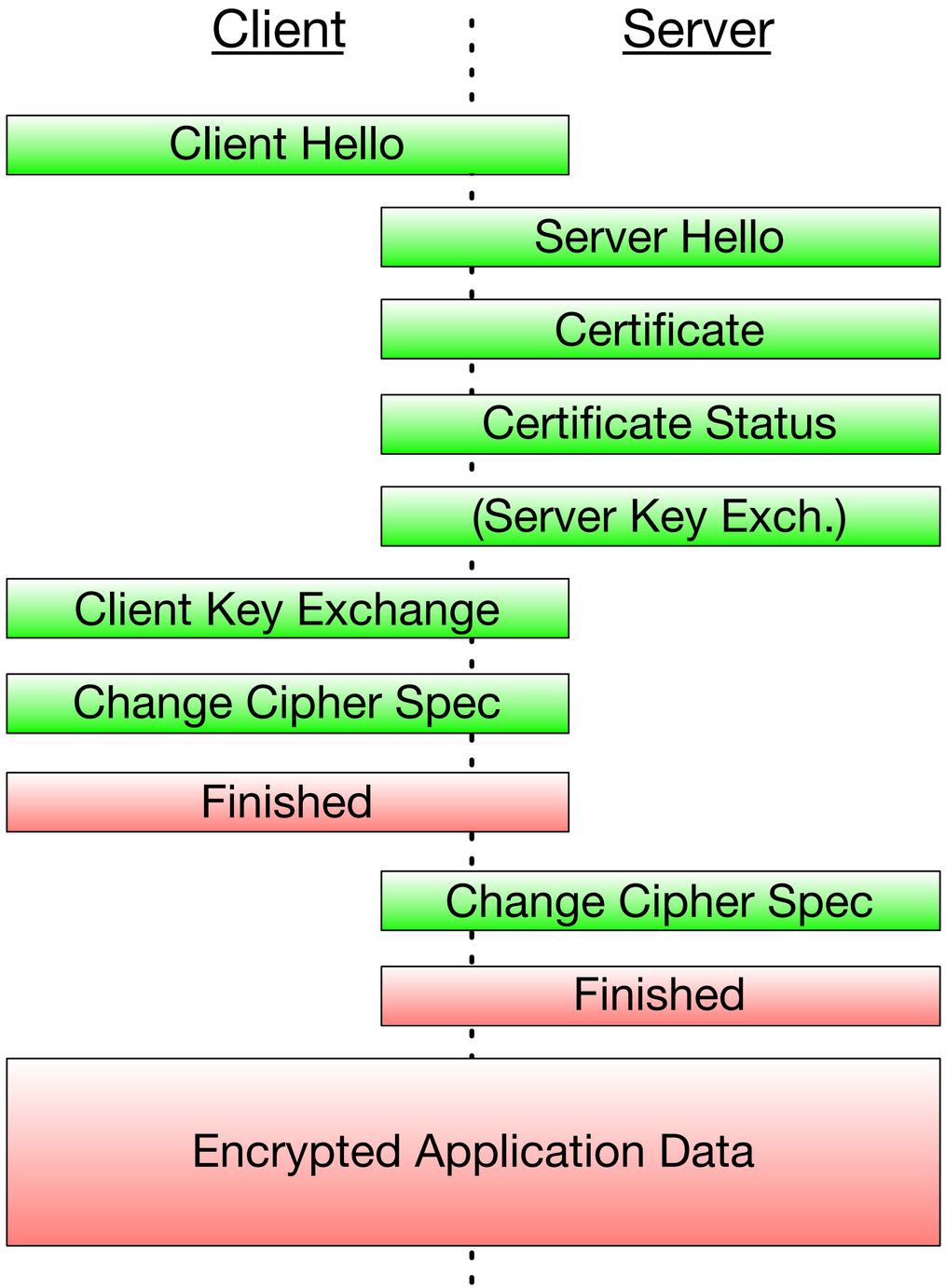
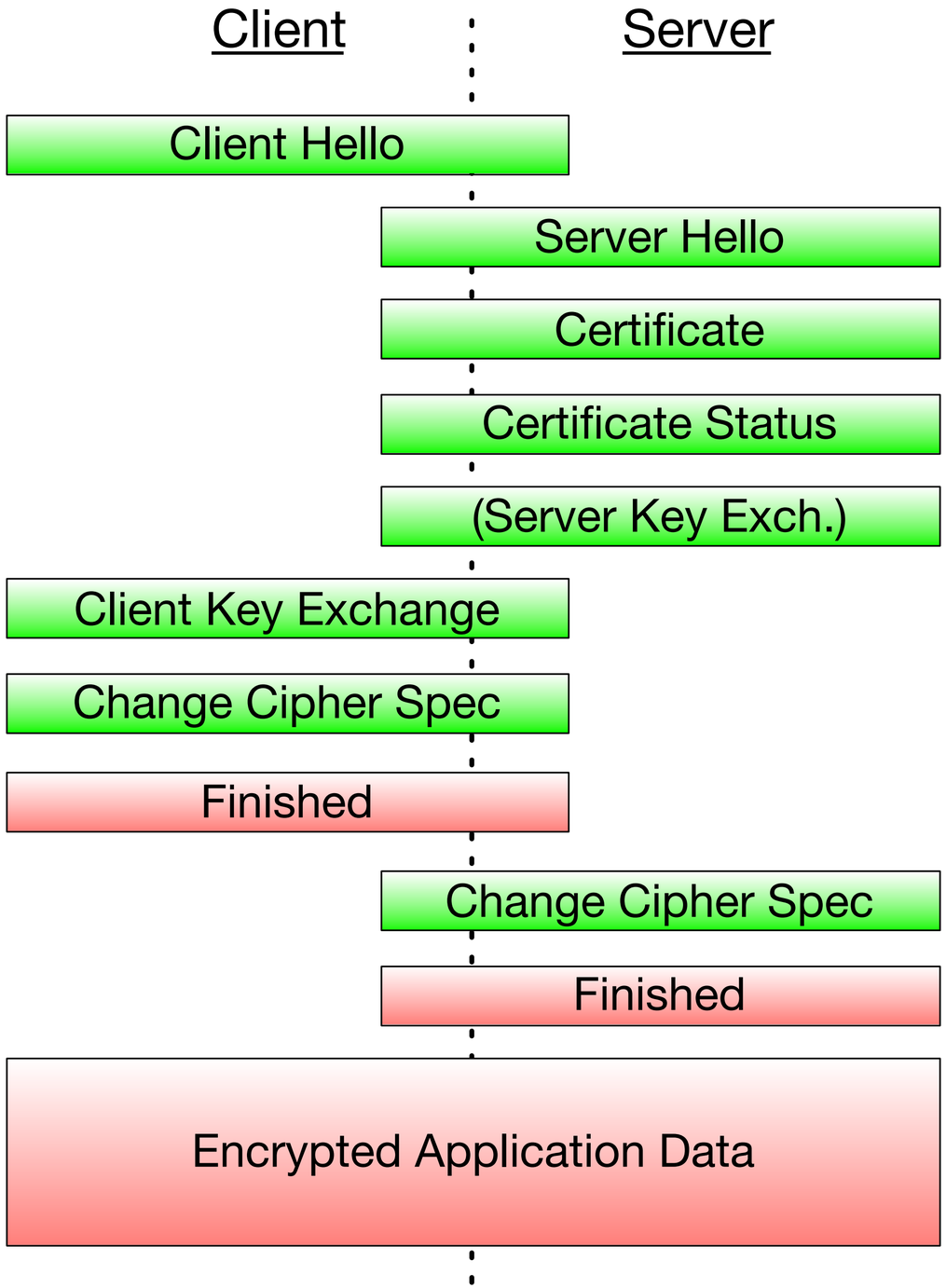
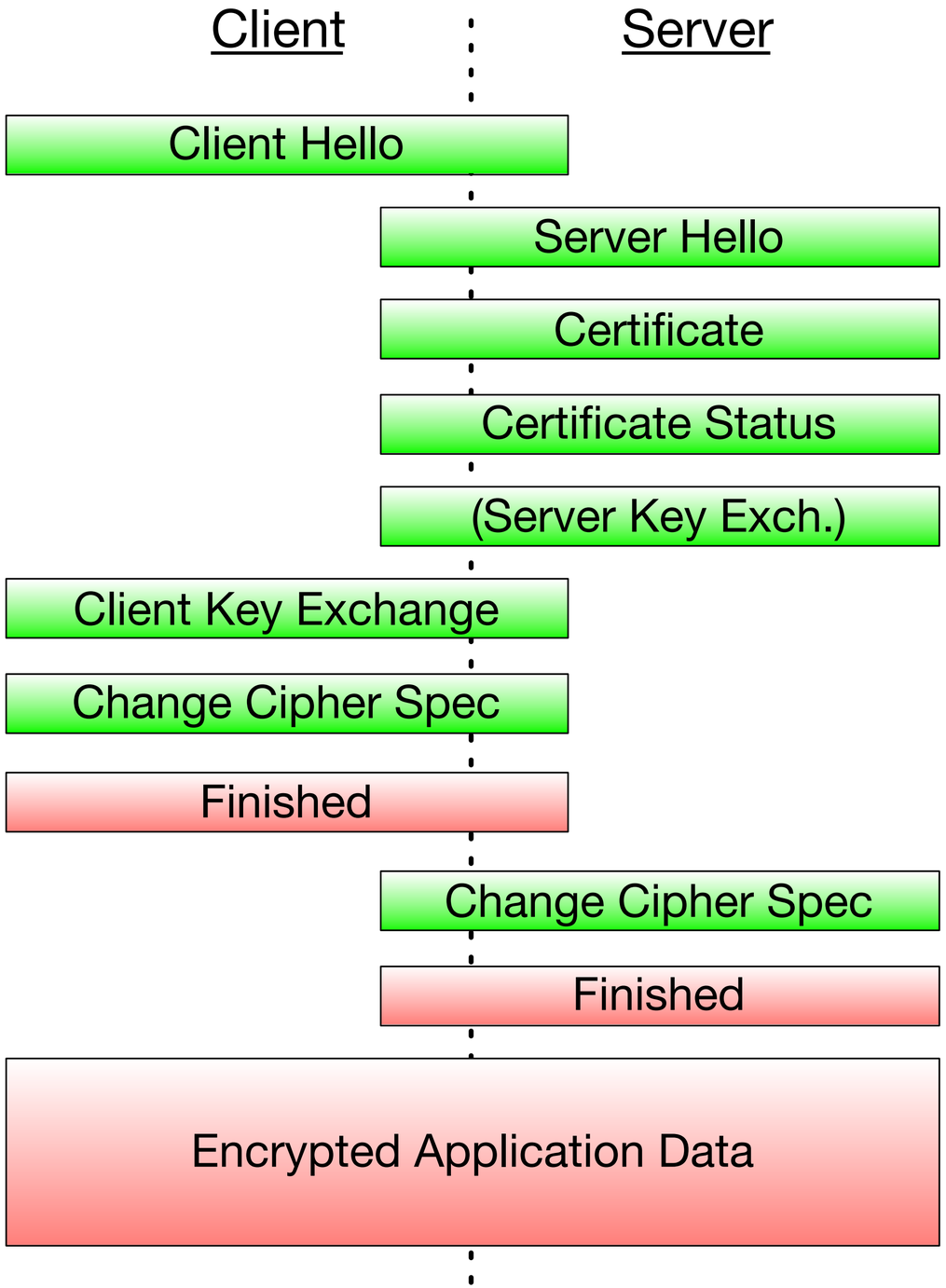
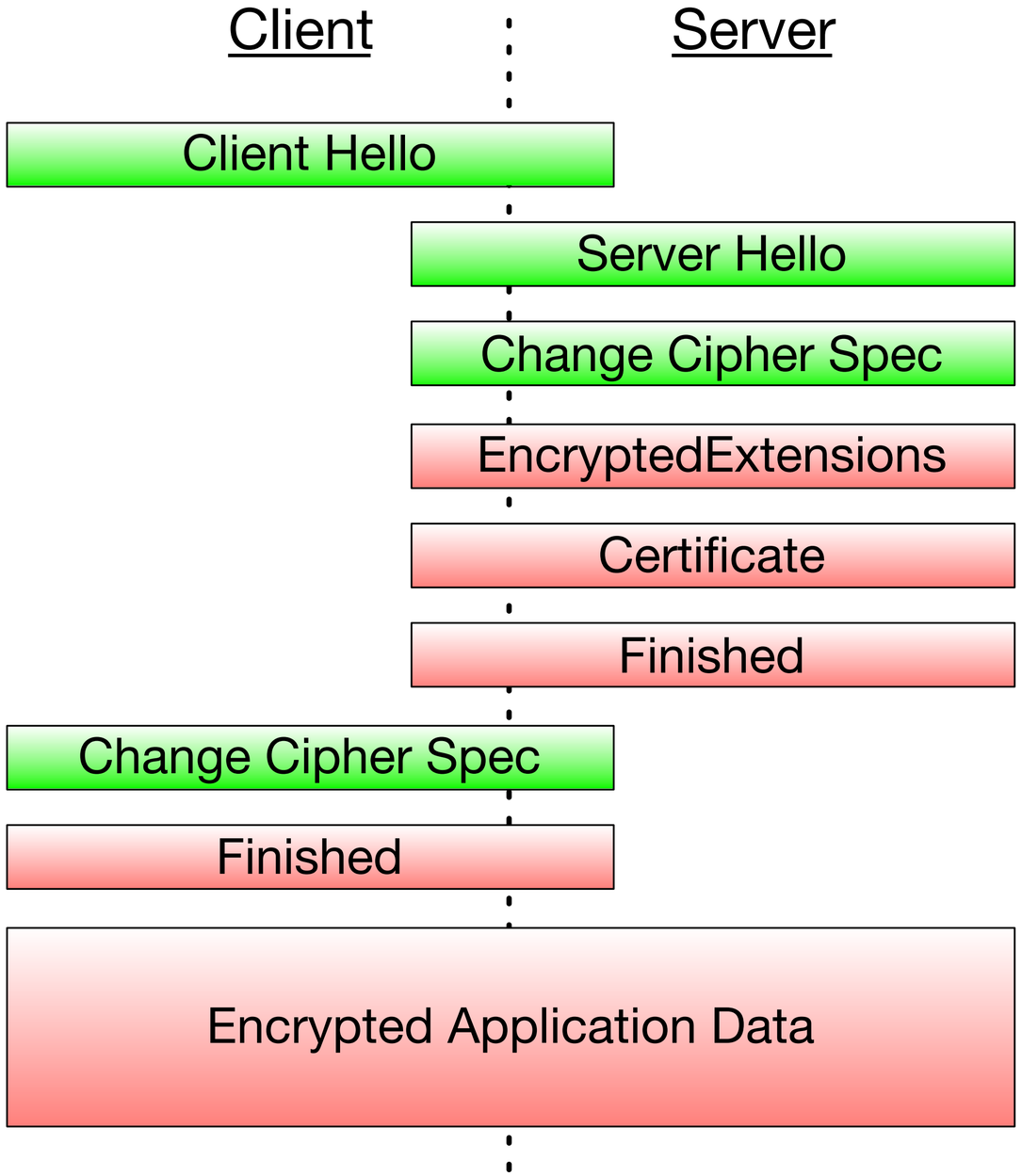

Client
Server
Client Hello
Server Hello
Certificate
Certificate Status
(Server Key Exch.)
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished
Encrypted Application Data

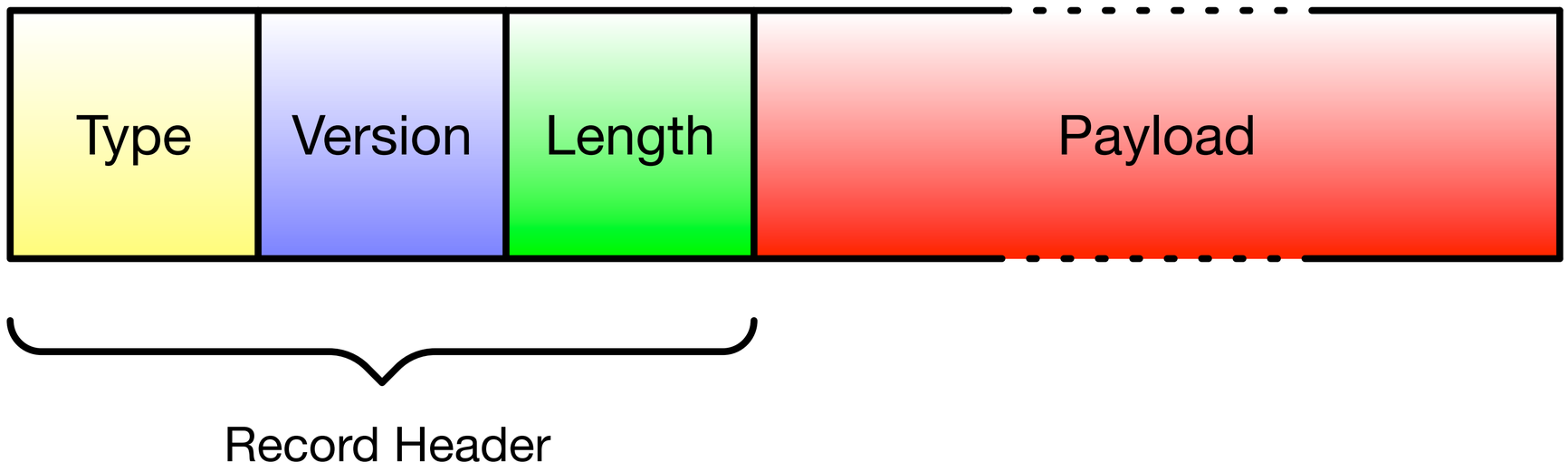
Photo by Markus Spiske on Unsplash


Client
Server
Client Hello
Server Hello
Certificate
Certificate Status
(Server Key Exch.)
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished
Encrypted Application Data

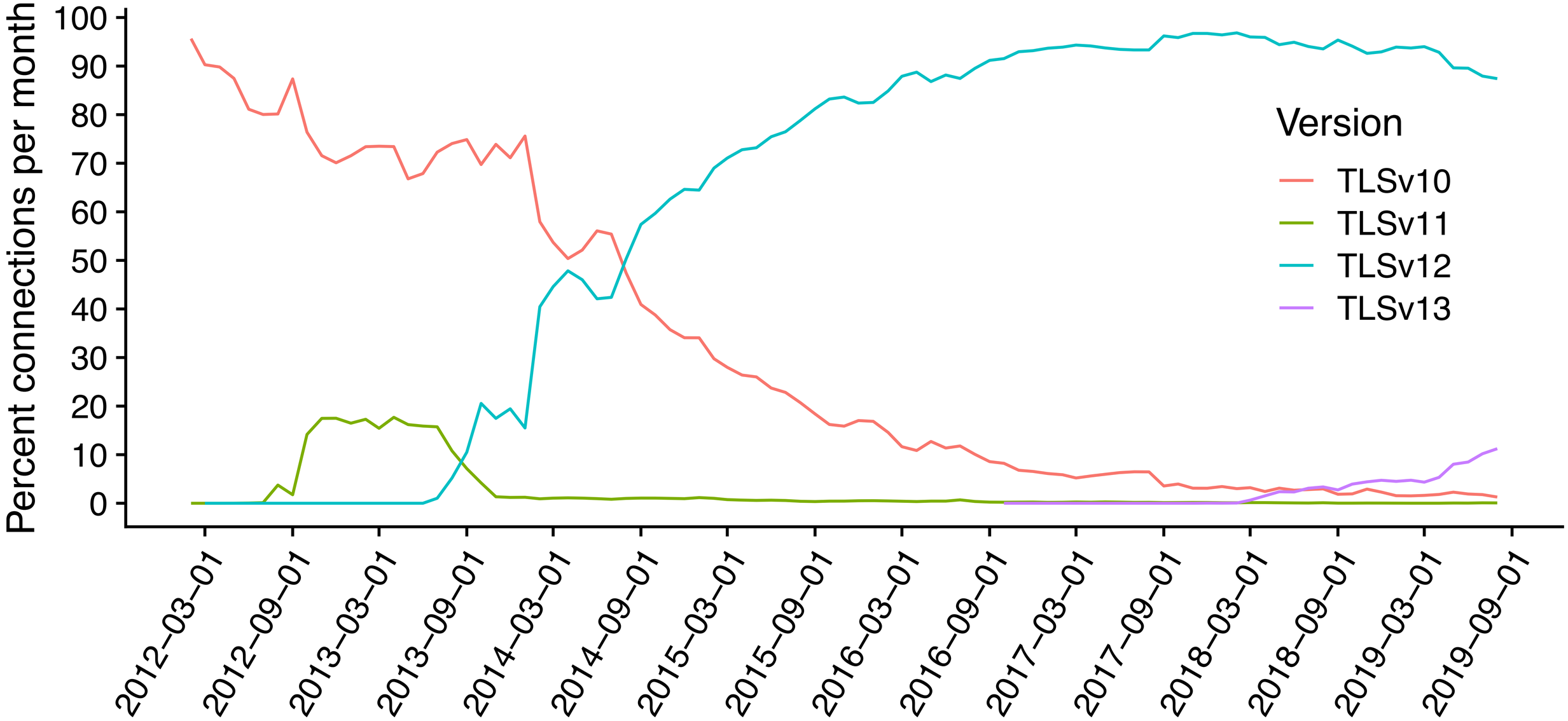

Client
Server
Client Hello
Server Hello
Certificate
Certificate Status
(Server Key Exch.)
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished
Encrypted Application Data


Client
Server
Client Hello
Server Hello
Change Cipher Spec
EncryptedExtensions
Certificate
Finished
Change Cipher Spec
Finished
Encrypted Application Data

SSL/TLS Protocol

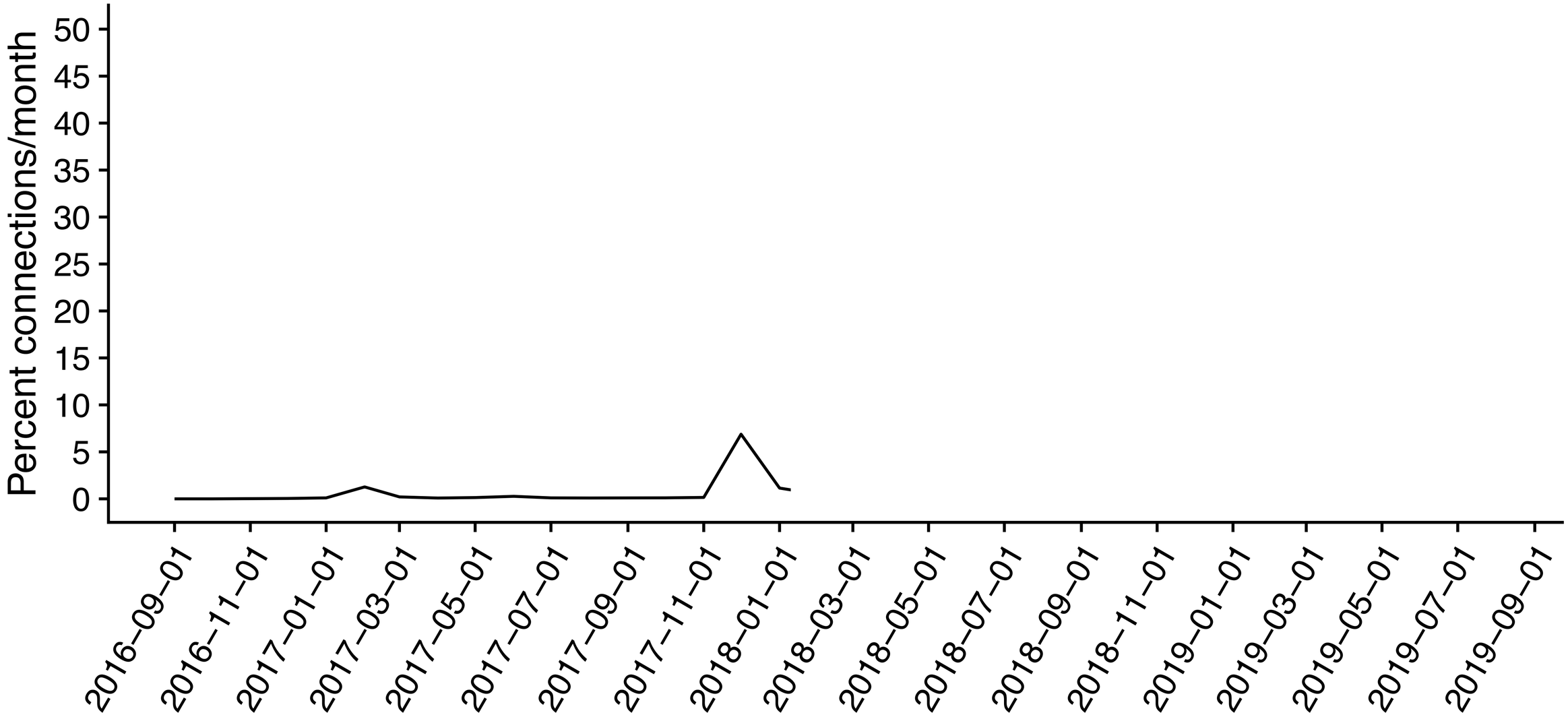


Negotiated Versions



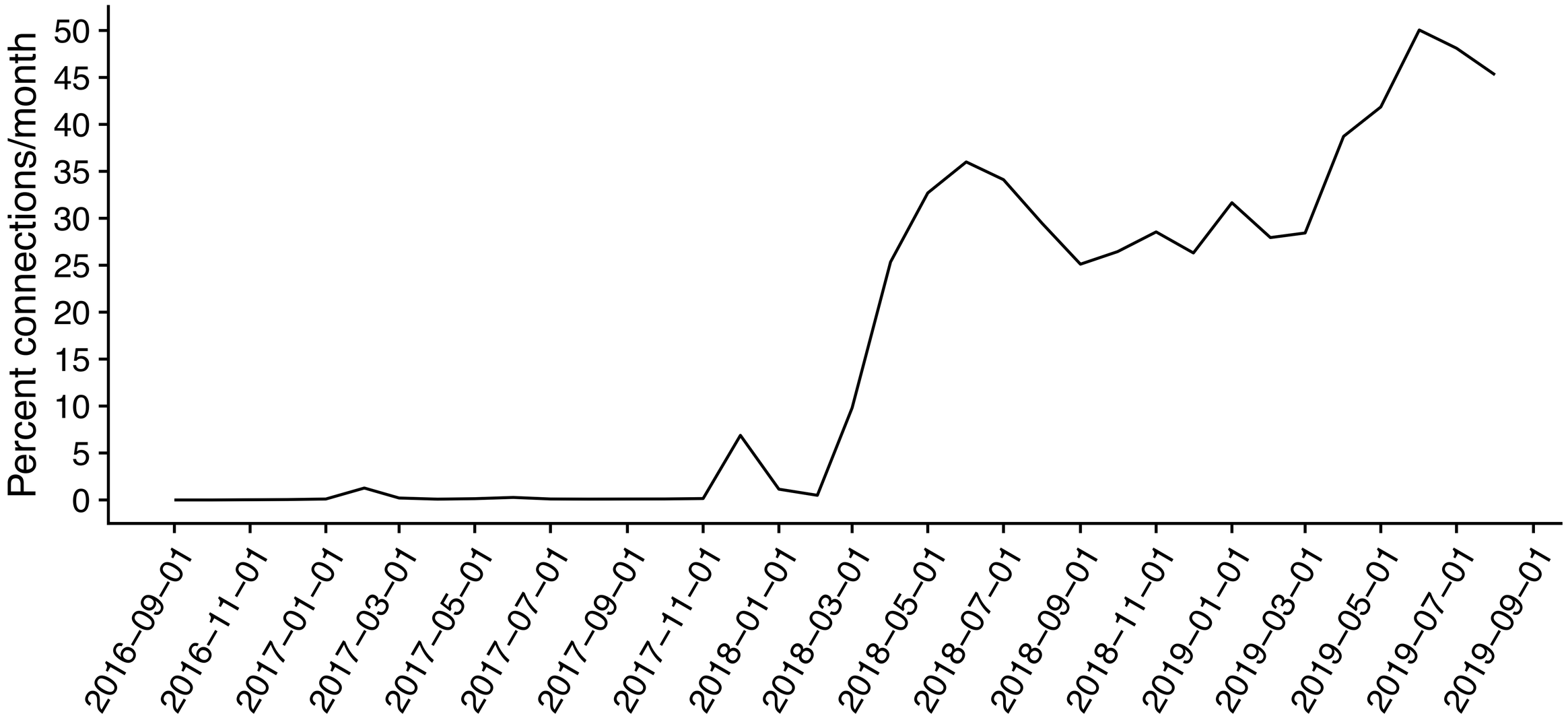
https://arxiv.org/abs/1907.12762

Client offered



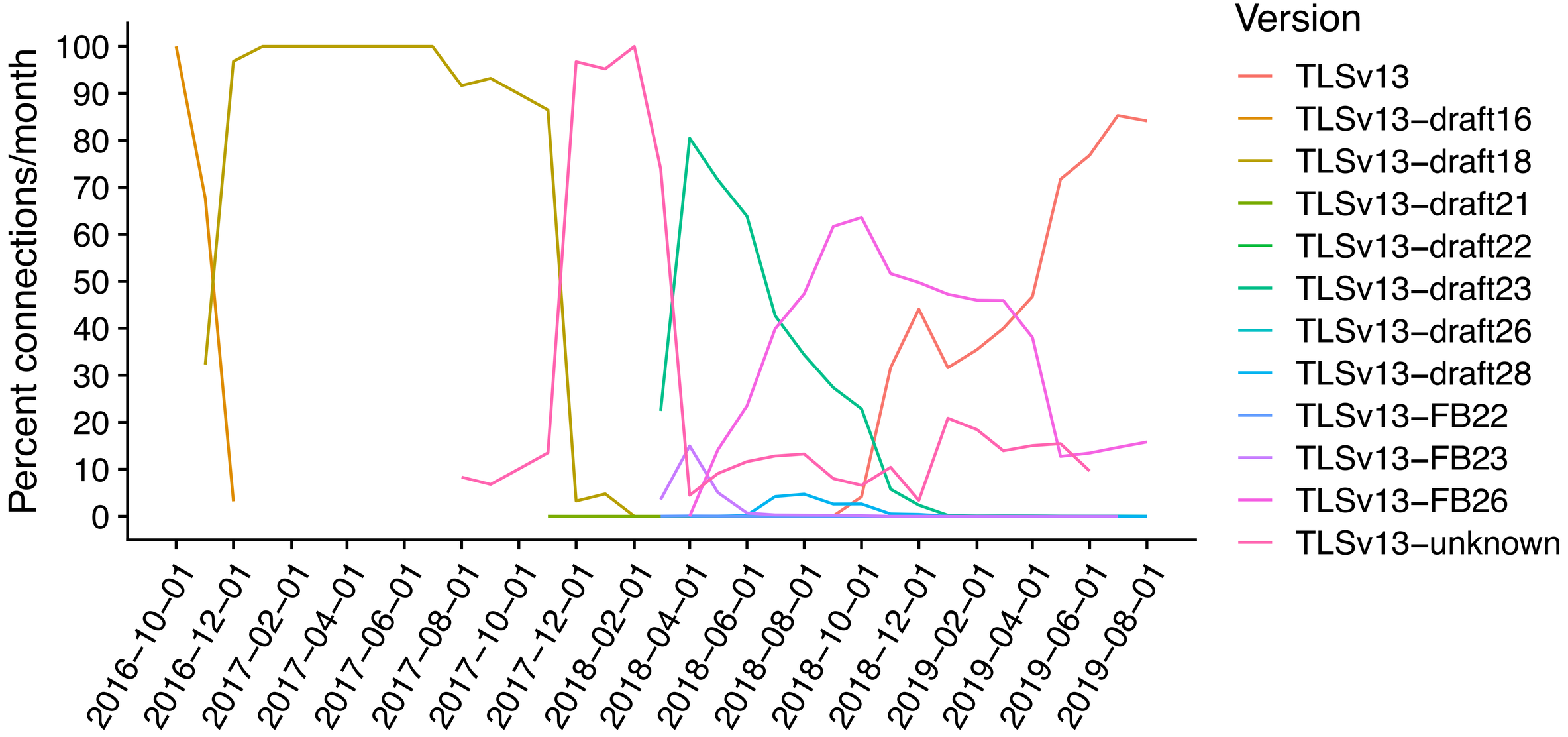
https://arxiv.org/abs/1907.12762

Client offered



https://arxiv.org/abs/1907.12762

Client offered



Offered/negotiated versions

Version	*Server Conn.*	*Client Conn.*
TLS 10	1.28%	44.07%
TLS 11	0.07%	42.96%
TLS 12	**87.42%**	**97.06%**
TLS 13	9.45%	**44.93%**
TLS 13-7E01	none	< 0.01%
TLS 13-7E02	none	< 0.01%
TLS 13-draft18	none	0.02%
TLS 13-draft22	none	< 0.01%
TLS 13-draft23	< 0.01%	0.25%
TLS 13-draft26	< 0.01%	< 0.01%
TLS 13-draft27	none	< 0.01%
TLS 13-draft28	< 0.01%	0.03%
TLS 13-FB23	none	< 0.01%
TLS 13-FB26	1.78%	1.78%

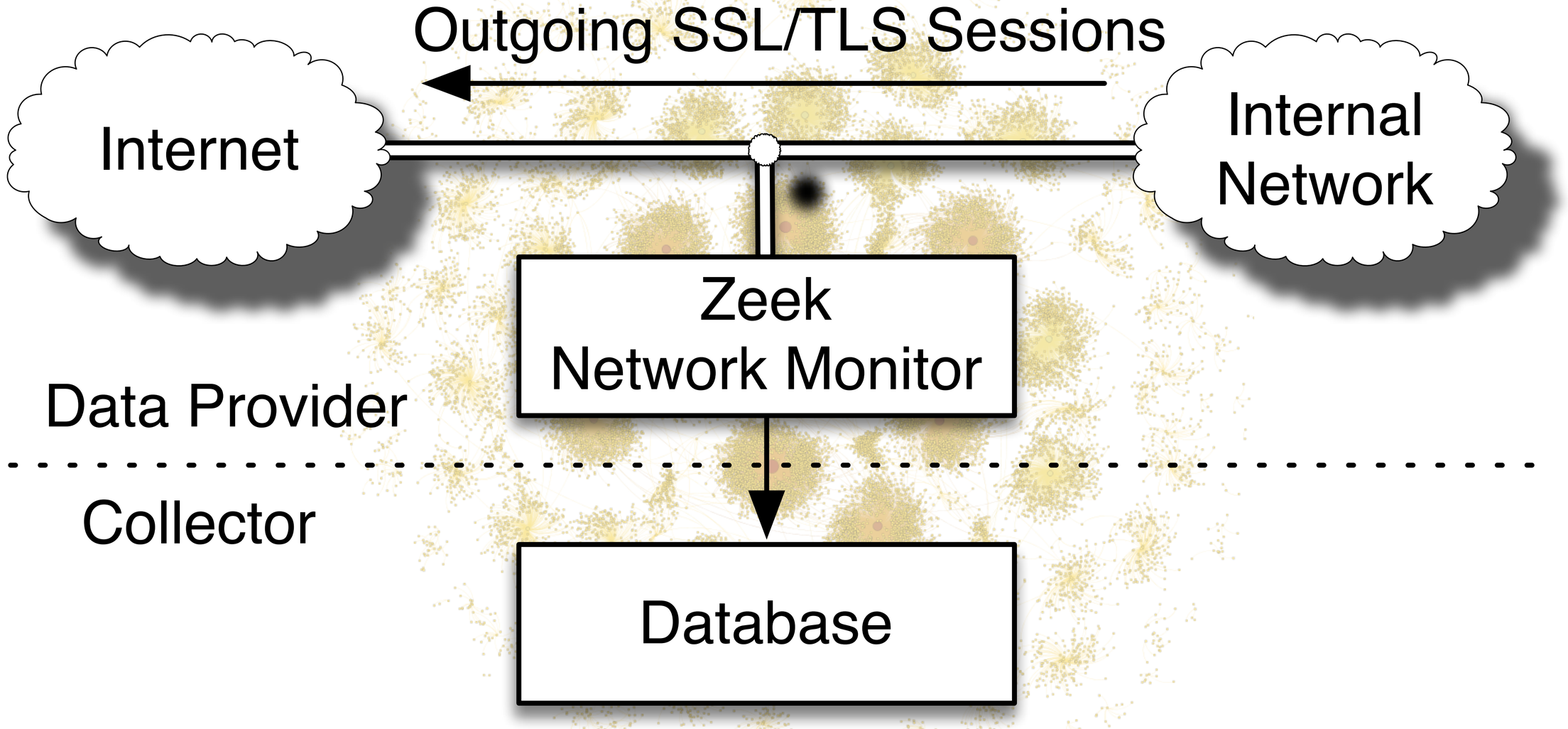
https://arxiv.org/abs/1907.12762

Connections to different providers

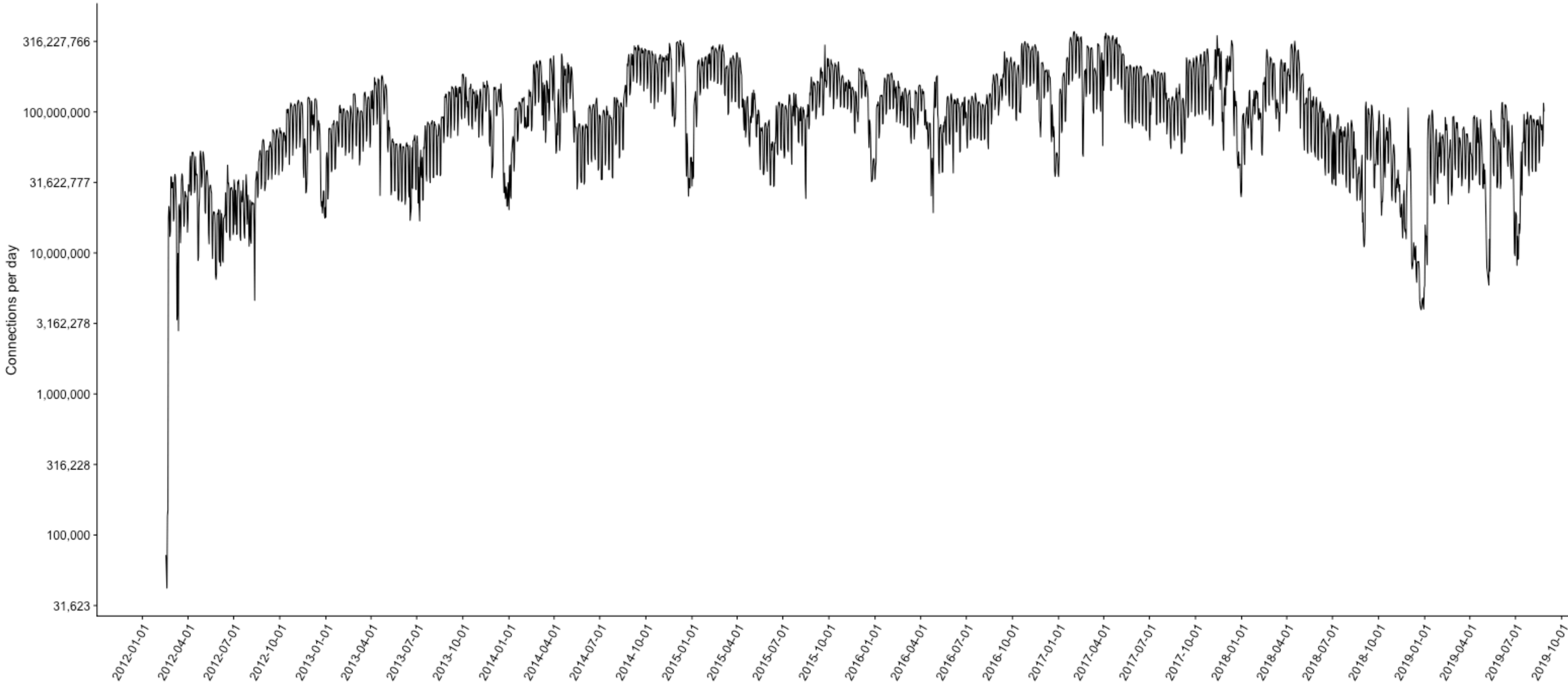
	% Connections		% IPs	
	TLS1.3	$\leq$ *TLS1.2*	*TLS1.3*	$\leq$ *TLS1.2*
Facebook	**60.78** (1)	1.02 (7)	3.22 (4)	0.12 (10)
Cloudflare	9.66 (3)	1.39 (6)	**70.45** (1)	4.86 (4)
Google	8.33 (4)	12.87 (3)	4.91 (3)	1.47 (5)
Amazon	0.42 (5)	**33.64** (2)	2.32 (5)	**68.02** (1)
Akamai	0.41 (6)	7.2 (5)	0.86 (6)	6.13 (3)
Digitalocean	0.05 (7)	0.16 (9)	0.65 (7)	0.69 (6)
Squarespace	0.04 (8)	<0.01 (12)	0.01 (11)	<0.01 (12)
Alibaba	0.02 (9)	0.04 (11)	0.04 (10)	0.04 (11)
Ovh	0.02 (10)	0.2 (8)	0.24 (8)	0.43 (8)
Azure	<0.01 (11)	8.88 (4)	0.07 (9)	0.45 (7)
Godaddy	<0.01 (12)	0.06 (10)	0.01 (12)	0.37 (9)
Others	20.26 (2)	34.54 (1)	17.2 (2)	17.42 (2)

https://arxiv.org/abs/1907.12762

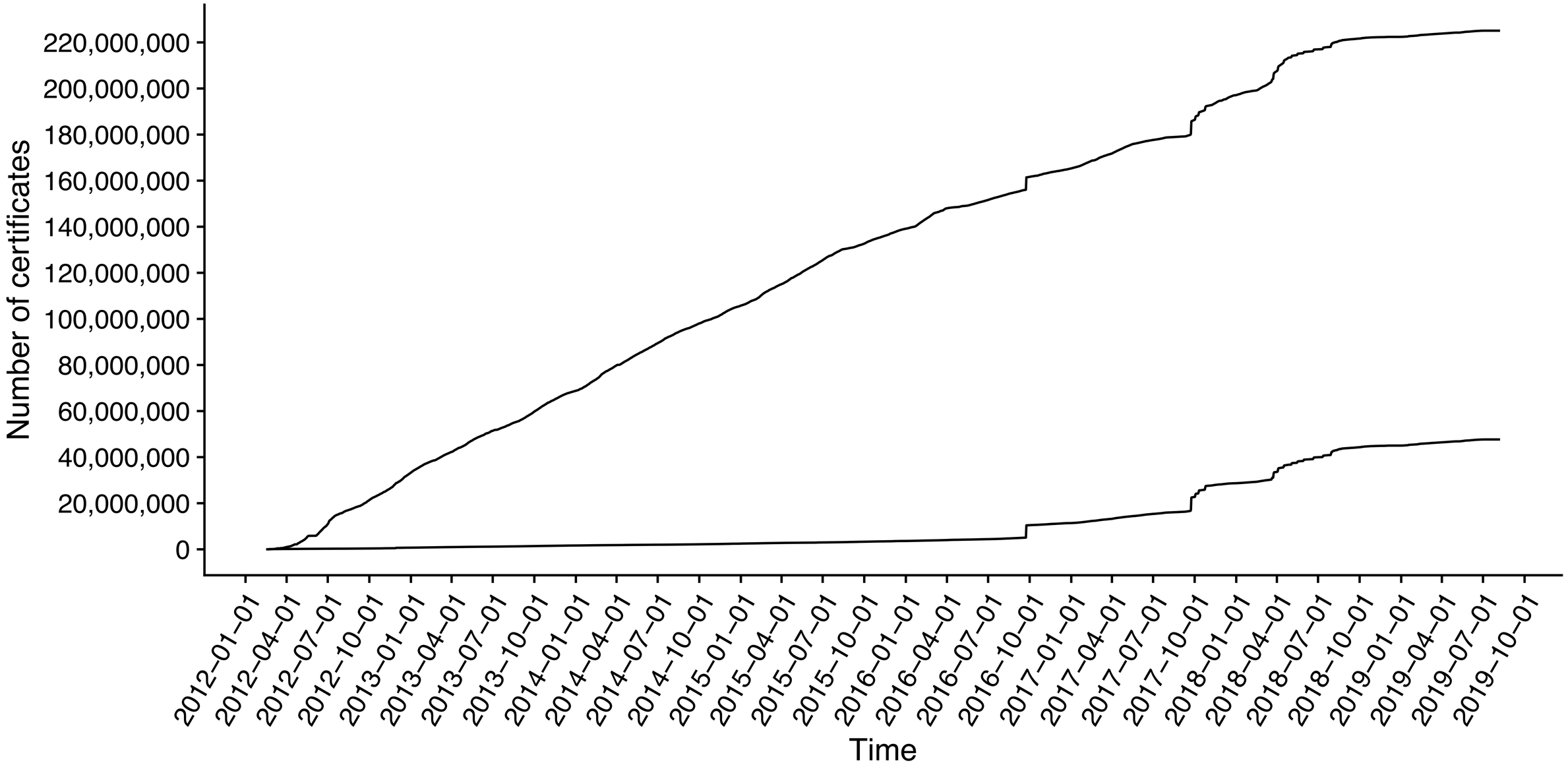
ICSI Notary


Outgoing SSL/TLS Sessions
Internet
Internal Network
Zeek Network Monitor
Data Provider
Collector
Database

Notary - Connections



Notary - Certificates



Notary - Collected features

Available ciphers

Analyzer Error

Client & Server TLS extensions

Content length

Connection history

Duration

Client EC point formats

Send & received bytes

Timestamp

Packet loss

Selected cipher

Server certificates

Server IP

Server Name Indication

DH parameter size

Client & Server ALPN

Version

Hash(client session ID)

Hash(client IP, server IP)

Hash(server session ID)

Ticket lifetime hint

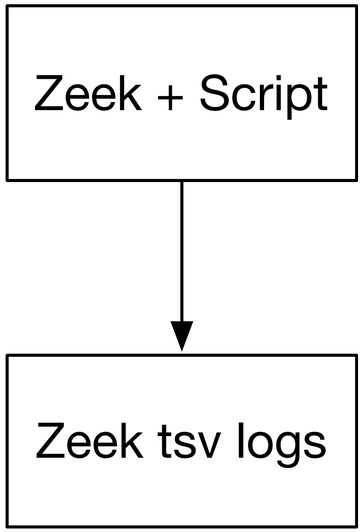
Client EC curve

Number Client Certs

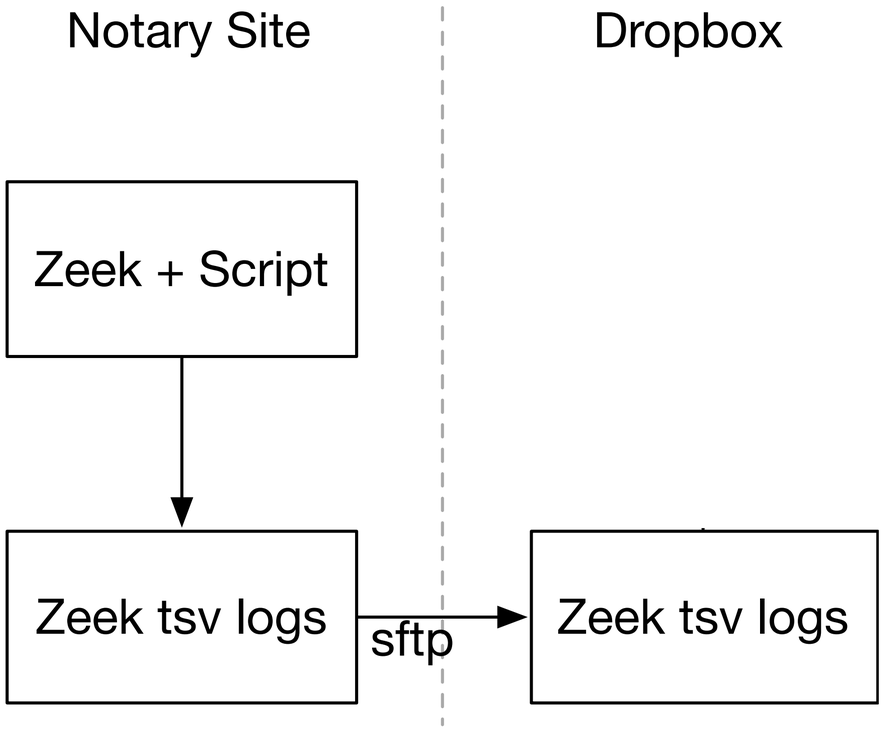
TLS Alerts

Dataflow

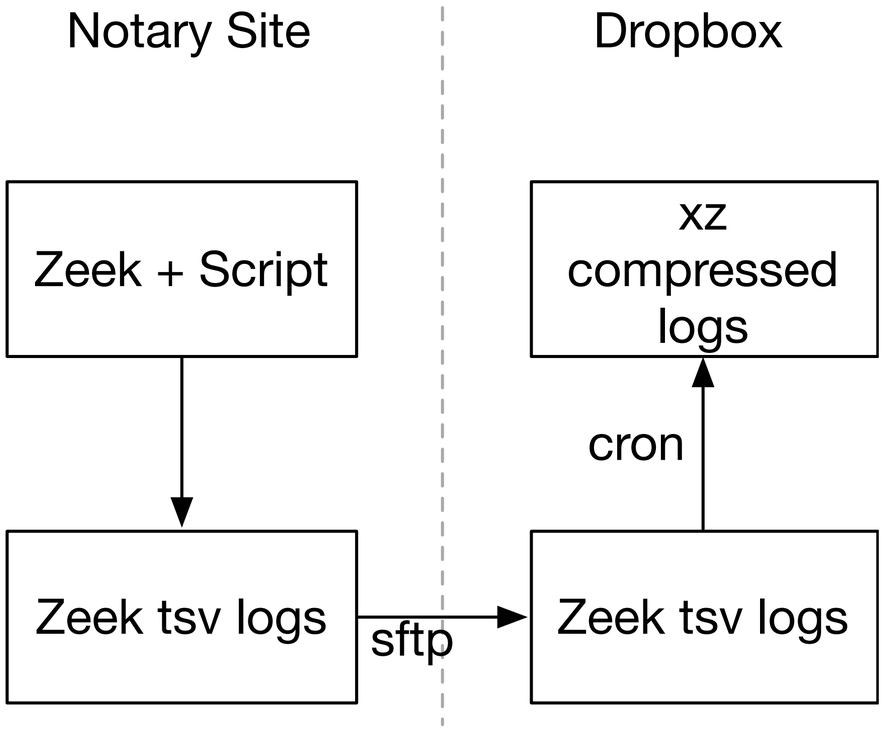
Notary Site



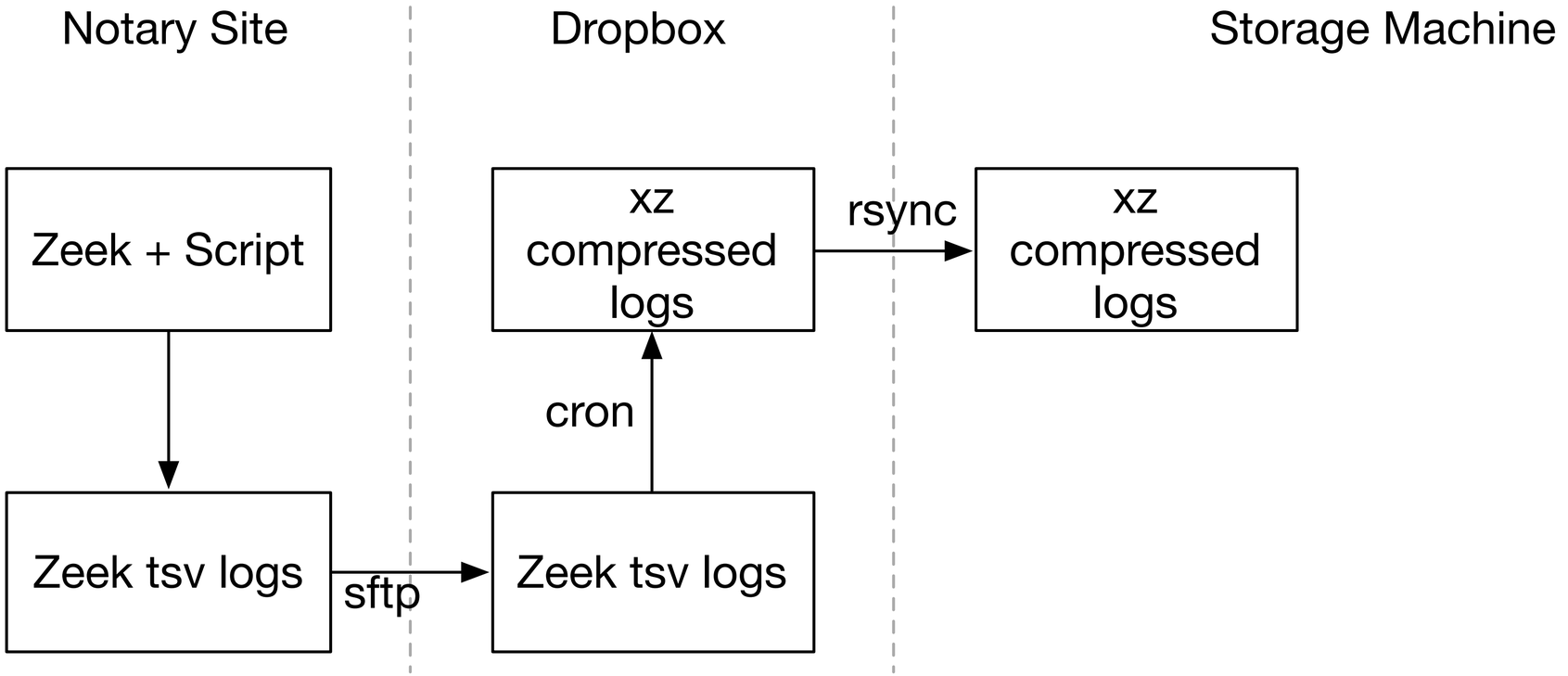
Dataflow


Notary Site
Dropbox
Zeek + Script
Zeek tsv logs
sftp
Zeek tsv logs

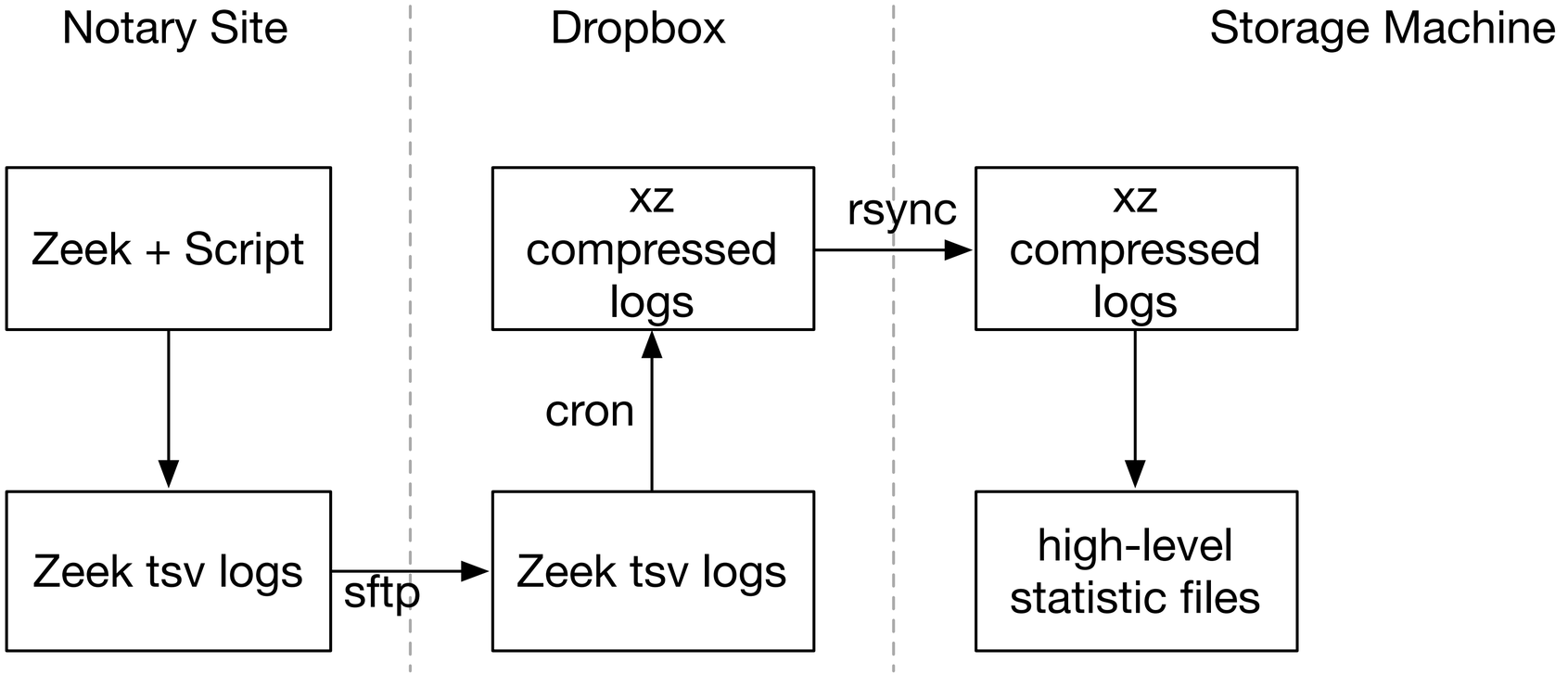
Dataflow


Notary Site
Dropbox
Zeek + Script
xz compressed logs
cron
Zeek tsv logs
sftp
Zeek tsv logs

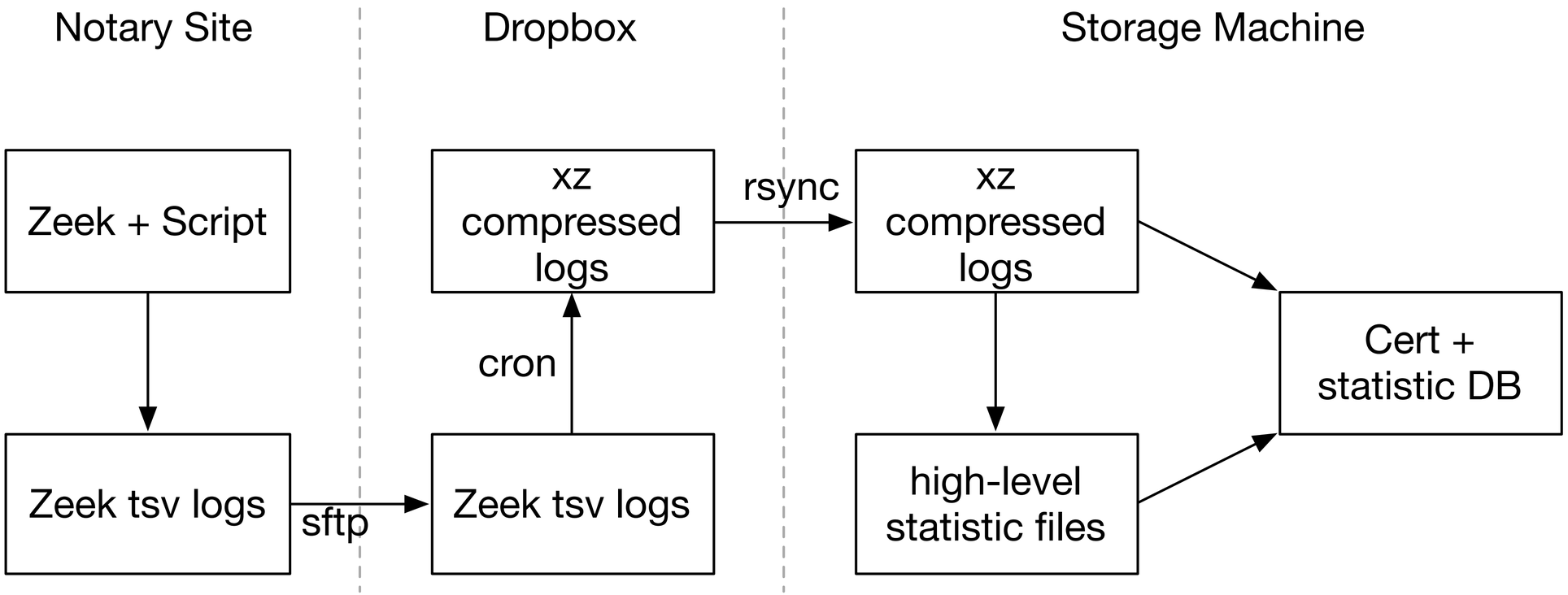
Dataflow


Notary Site
Dropbox
Storage Machine
Zeek + Script
Zeek tsv logs
sftp
Zeek tsv logs
cron
xz
compressed
logs
rsync
xz
compressed
logs

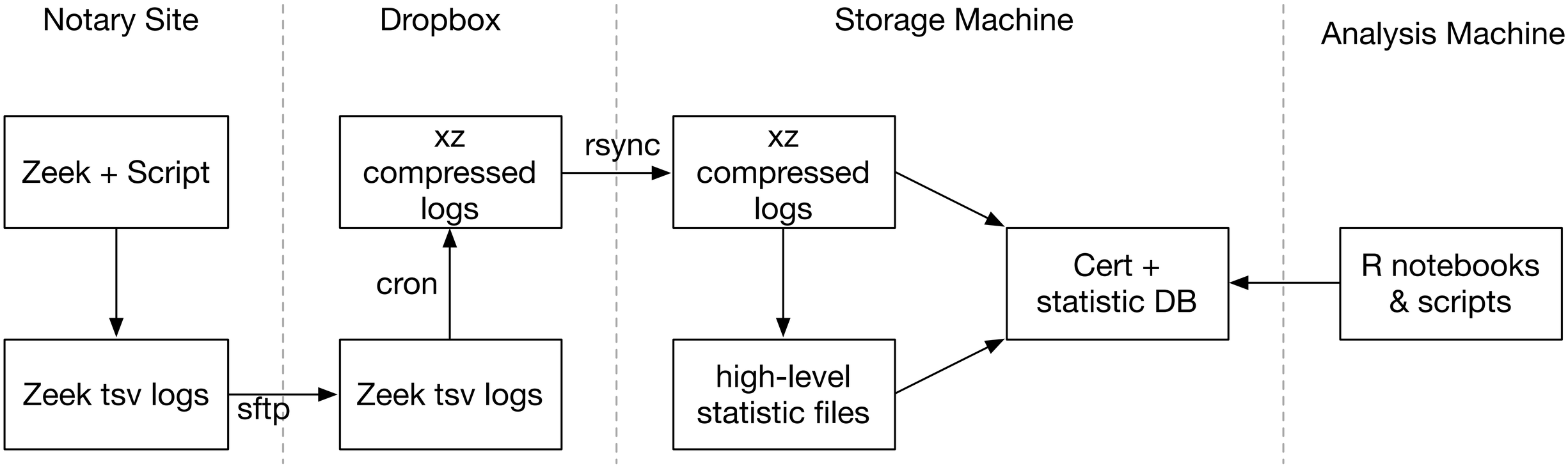
Dataflow


Notary Site
Dropbox
Storage Machine
Zeek + Script
Zeek tsv logs
sftp
Zeek tsv logs
cron
xz
compressed
logs
rsync
xz
compressed
logs
high-level
statistic files

Dataflow


Notary Site
Dropbox
Storage Machine
Zeek + Script
Zeek tsv logs
sftp
Zeek tsv logs
cron
xz compressed logs
rsync
xz compressed logs
high-level statistic files
Cert + statistic DB

Dataflow


Notary Site
Dropbox
Storage Machine
Analysis Machine
Zeek + Script
Zeek tsv logs
sftp
Zeek tsv logs
cron
xz compressed logs
rsync
xz compressed logs
high-level statistic files
Cert + statistic DB
R notebooks & scripts

Certificate Log

Timestamp	1414444290.810620
SHA1	3c757505c22c4e1cf325368280ef2a0dd2bb2bde
Certificate	3082052e30820416a003020102020308c40c300d06092a864886f70d01010505003c 310b3009060355040613025553311730150603550 40a130e47656f54727573742c2049 6e632e311430120603550403130b52617069645534c204341301e170d313231303131
Host	89.238.65.180
Host_p	443
Host_cert	T

Connection Log

Timestamp	1520820013.6215
server	52.32.149.186
server_p	443
version_num	771
client_version	771
client_ciphers	39578,4865,4866,4867,49195,49199,49196,49200,52393,52392,49171,49172,156,157,47,5
cipher_num	4865
sni	tls13.crypto.mozilla.org
ticket_lifetime_hint	-
ssl_client_exts	19018,65281,0,23,35,13,5,18,16,30032,11,51,45,43,10,24,31354,21
ssl_server_exts	51,43
server_certs	-
packet_loss	F
dh_param_size	-

Connection Log

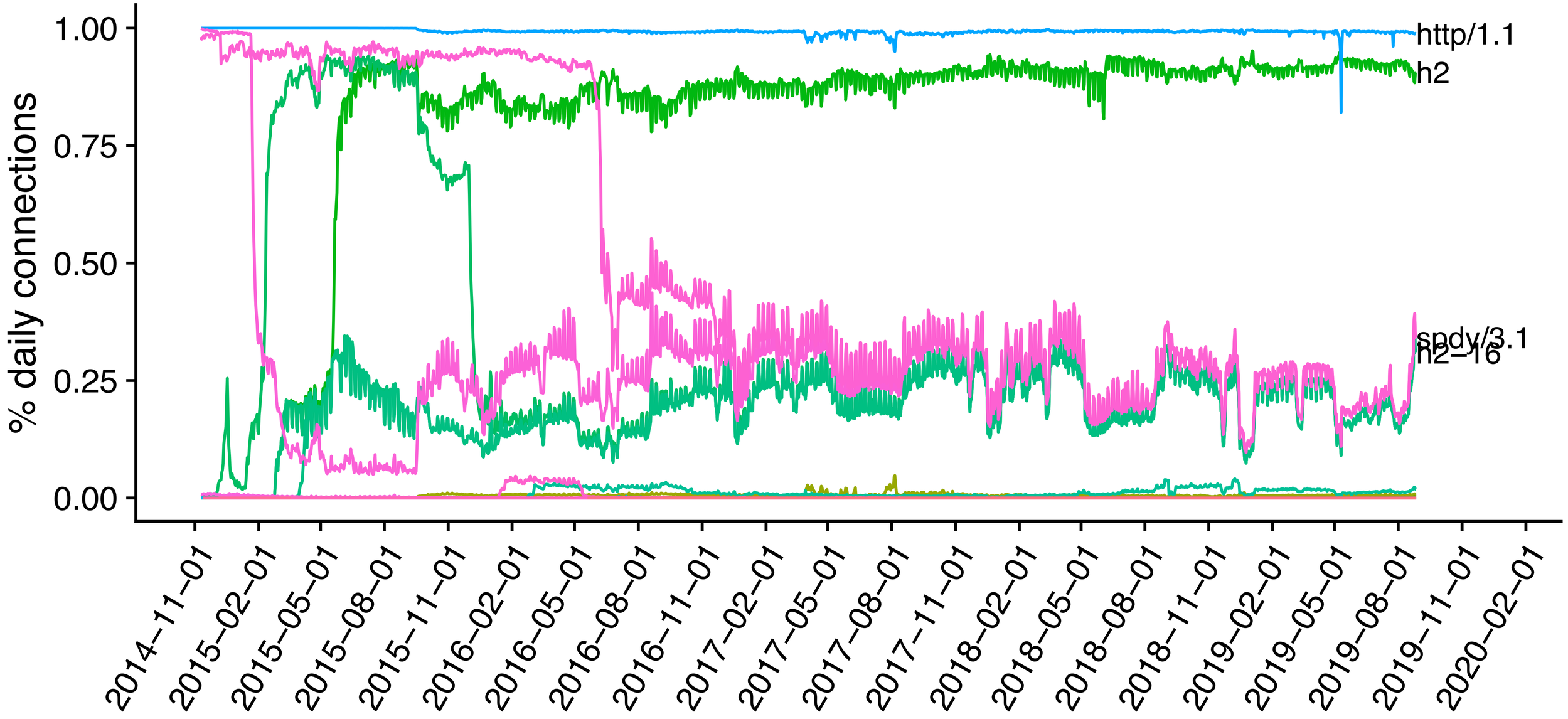
Timesta	
serve	
server	
version_	
client_ve	
client_ci	57,47,5
cipher_	
sni	
ticket_lifeti	
ssl_clien	
ssl_serve	
server_c	
packet_	
dh_param_size	-

{"ts":
1398362902.971438,"sha1":"7359755c6df9a0abc3060bce369564c8ec4542a3","cert":"3082037d308202e6a0030201
02020312bbe6300d06092a864886f70d0101050500304e310b3009060355040613025553110300e060355040a130
74571756966617831 2d302b060355040b13244571756966617820536563757265204365727469666963617465204 1
7574686f72697479301e170d3032303532313034303030305a170d3138303832313034303030305a3042310b300906
035504061302555331163014060355040a130d47656f547275737420496e632e311b3019060355040313124765 6f54
7275737420476c6f62616c20434130820122300d06092a864886f70d0101010500038201 0f003082010a0282010100d
acc186330fdf417231a567e5bdf3c6c38e471b77891d4bca1d84cf8a843b603e94d21070888da582f663929bd05788b
9d38e805b76a7e71a4e6c460a6b0ef80e489280f9e25d6ed83f3ada691c798c9421835149dad9846922e4fcaf18743c
11695572d50ef892d807a57adf2ee5f6bd2008db914f8141535d9c046a37b72c891bfc9552bcdd0973e9c2664ccdfce
831971ca4ee6d4d57ba919cd55dec8ecd25e3853e55c4f8c2dfe502336fc66e6cb8ea4391900b7950239910b0efe38
2ed11d059af64d3e6f0f071daf2c1e8f6039e2fa36531339d45e262bdb3da814bd32eb180328520471e5ab333de138b
b073684629c79ea1630f45fc02be8716be4f90203010001a381f03081ed301f0603551d23041830168014 48e668f92bd
2b295d747d82320104f3398909fd4301d0603551d0e04160414c07a98688d89fbab05640c117daa7d65b8cacc4e300
f0603551d130101ff040530030101ff300e0603551d0f0101ff0404030201 06303a0603551d1f04333031302fa02da02b8
629687474703a2f2f63726c2e67656f74727573742e636f6d2f63726c732f73656375726563612e63726c304e0603551
d2004473045304306045 51d2000303b303906082b06010505070201162d68747470733a2f2f7777772e67656f74727
573742e636f6d2f7265736f75726365732f7265706f7369746f7279300d06092a864886f70d0101050500038181 0076e1
126e4e4b1612863006b28108cff008c7c7717e66eec2edd43b1ffff0f0c84ed64338b0b9307d18d05583a26acb36119c
e84866a36d7fb813d447fe8b5a5c73fcaed91b321938ab973414aa96d2eba31c140849b6bbe591ef8336eb1d566fca
dabc736390e47f7b3e22cb3d07ed5f38749ce303504ea1af98ee61f2843f12","host":"74.125.239.152","host_p":
443,"host_cert":false}

Connection Log

Timestamp	1520820013.6215
server	52.32.149.186
server_p	443
version_num	771
client_version	771
client_ciphers	39578,4865,4866,4867,49195,49199,49196,49200,52393,52392,49171,49172,156,157,47,5
cipher_num	4865
sni	tls13.crypto.mozilla.org
ticket_lifetime_hint	-
ssl_client_exts	19018,65281,0,23,35,13,5,18,16,30032,11,51,45,43,10,24,31354,21
ssl_server_exts	51,43
server_certs	-
packet_loss	F
dh_param_size	-

Client ALPNs




zkg install 0xxon/tls-log-alternative