SSL Research with Bro

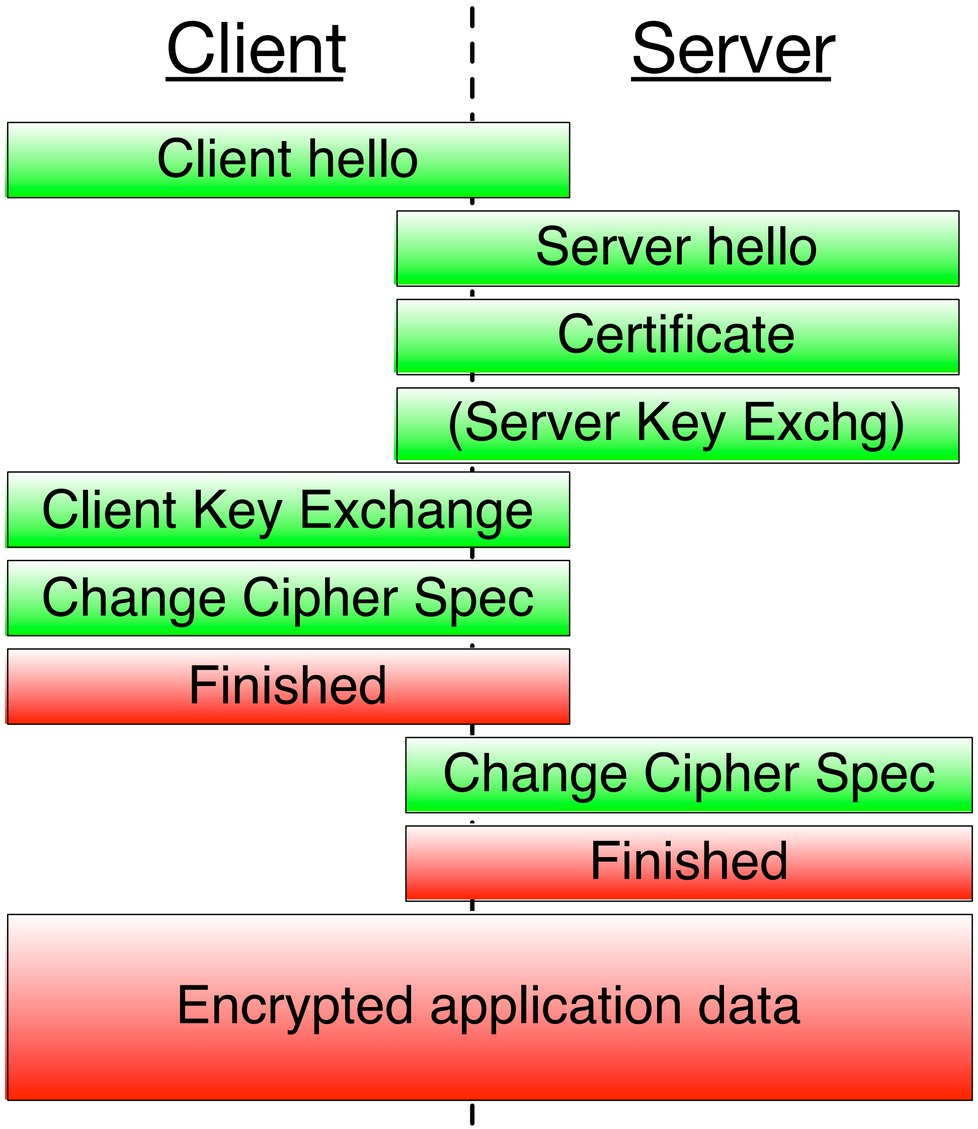
Johanna Amann

International Computer Science Institute

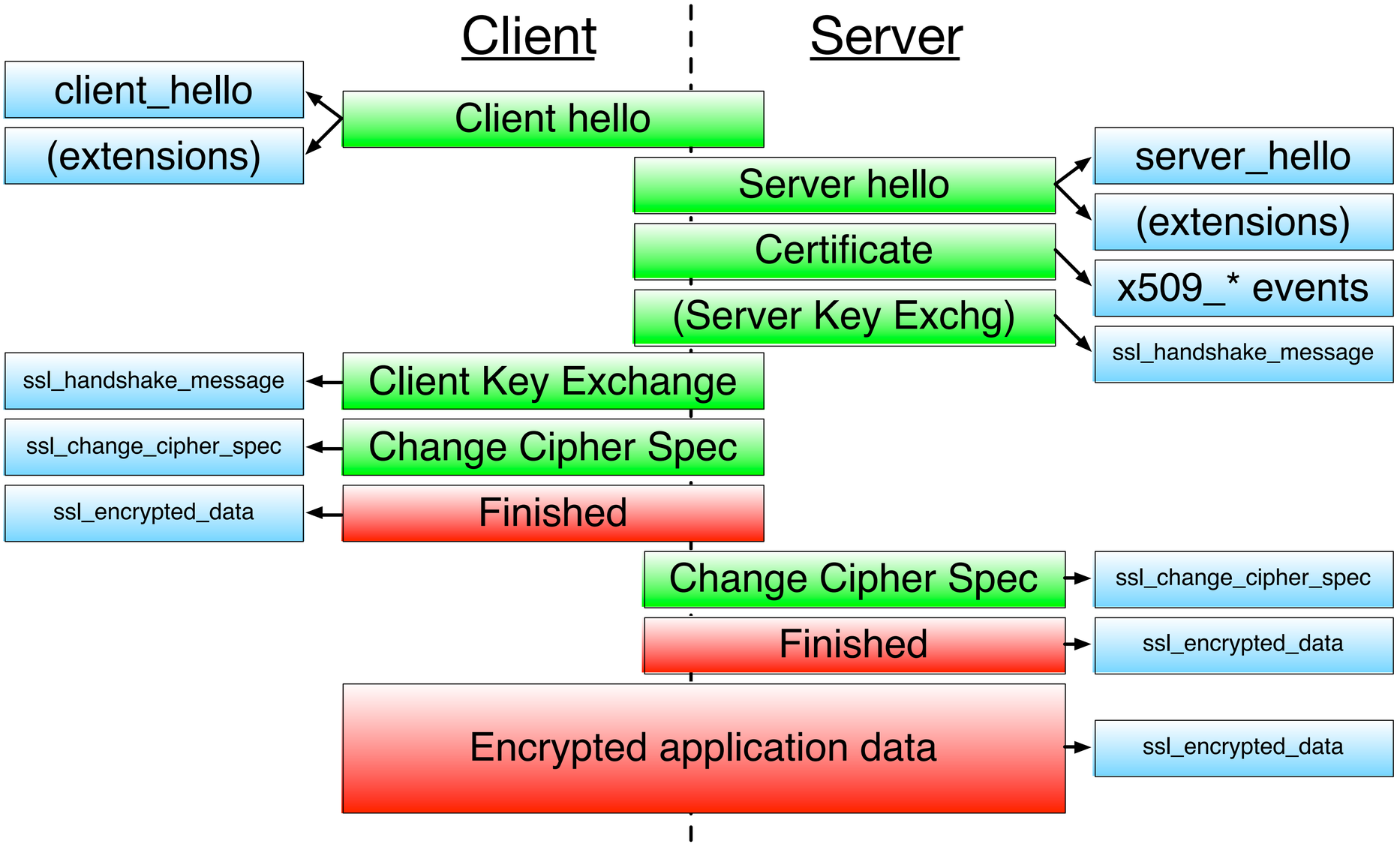
johanna@icir.org

http://www.icir.org/johanna

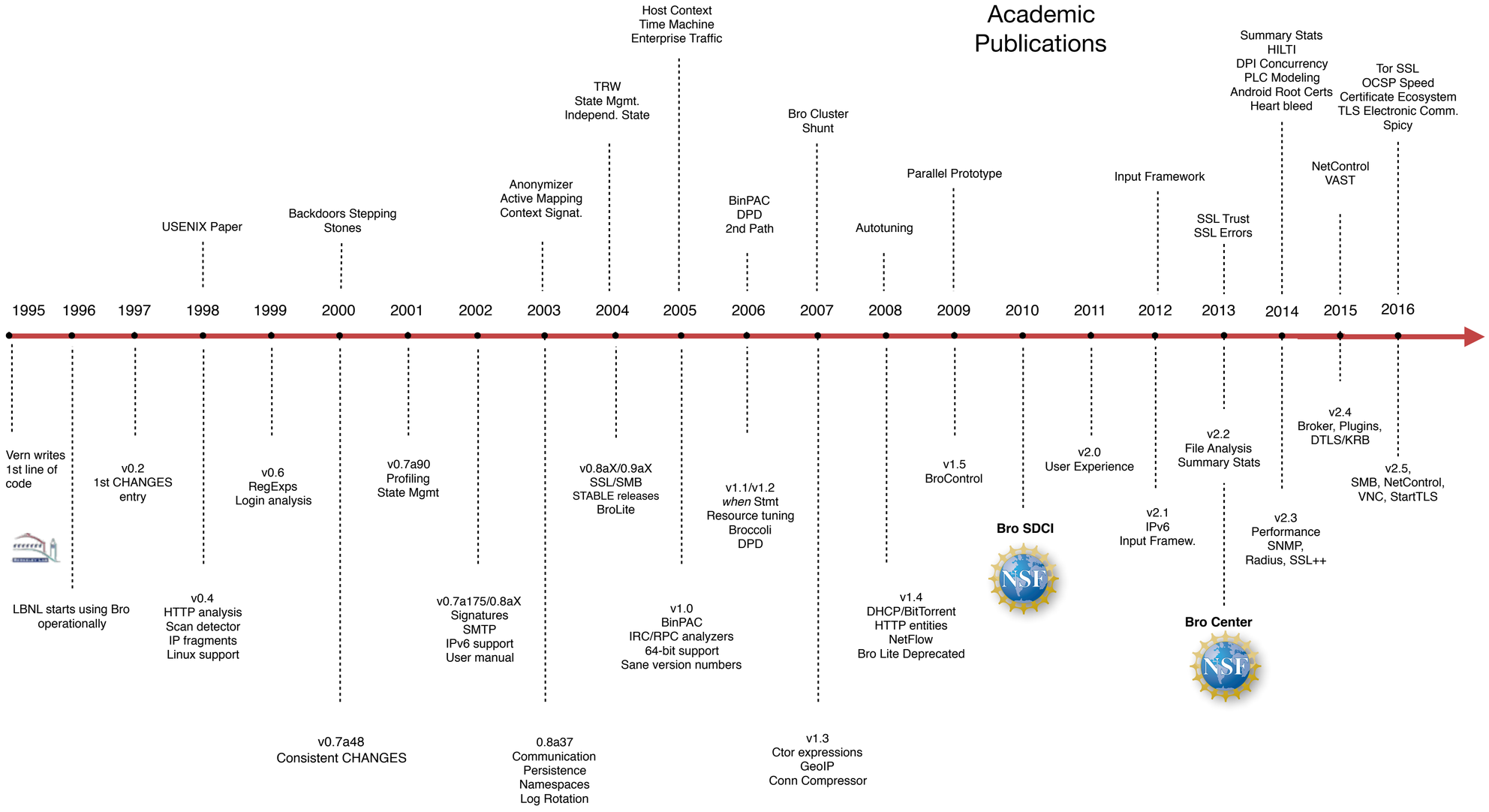
SSL


Client
Server
Client hello
Server hello
Certificate
(Server Key Exchg)
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished
Encrypted application data

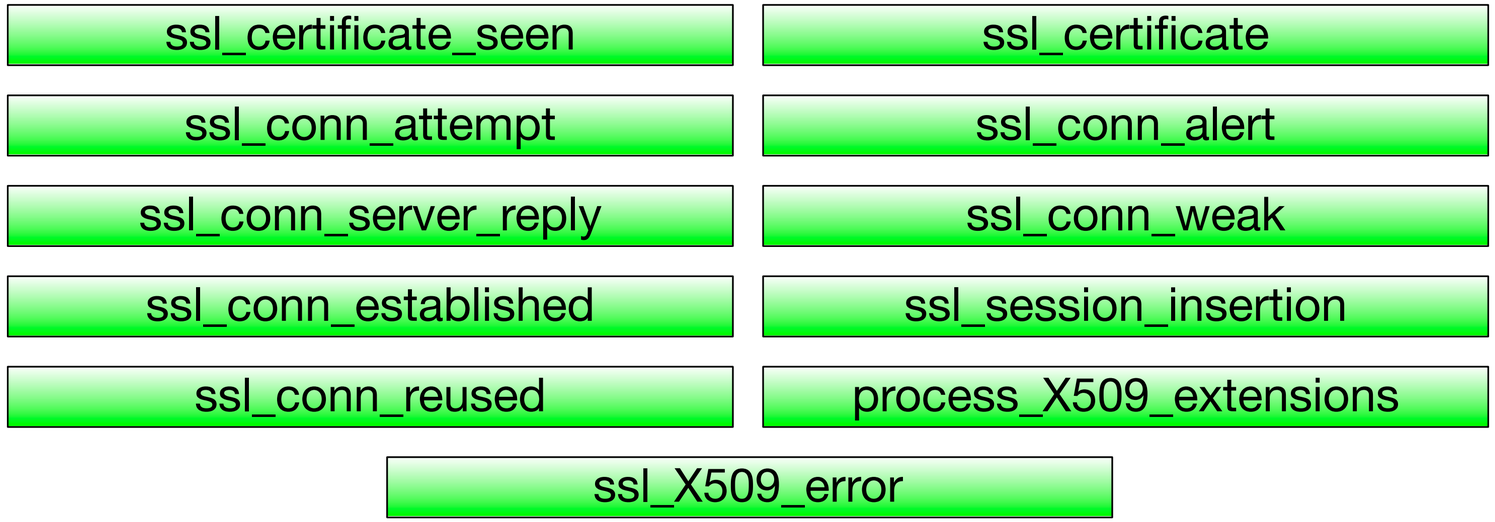
SSL


Client
Server
client_hello
(extensions)
Client hello
Server hello
server_hello
(extensions)
Certificate
x509_* events
(Server Key Exchg)
ssl_handshake_message
ssl_handshake_message
Client Key Exchange
ssl_change_cipher_spec
Change Cipher Spec
ssl_encrypted_data
Finished
Change Cipher Spec
ssl_change_cipher_spec
Finished
ssl_encrypted_data
Encrypted application data
ssl_encrypted_data

Bro History

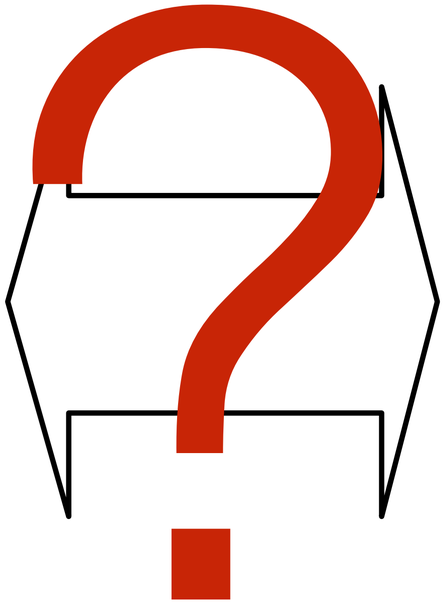

Academic Publications
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
Vern writes 1st line of code
LBNL starts using Bro operationally
v0.2 1st CHANGES entry
v0.4 HTTP analysis Scan detector IP fragments Linux support
USENIX Paper
v0.6 RegExps Login analysis
Backdoors Stepping Stones
v0.7a48 Consistent CHANGES
v0.7a90 Profiling State Mgmt
v0.7a175/0.8aX Signatures SMTP IPv6 support User manual
Anonymizer Active Mapping Context Signat.
0.8a37 Communication Persistence Namespaces Log Rotation
TRW State Mgmt. Independ. State
v0.8aX/0.9aX SSL/SMB STABLE releases BroLite
Host Context Time Machine Enterprise Traffic
v1.0 BinPAC IRC/RPC analyzers 64-bit support Sane version numbers
BinPAC DPD 2nd Path
v1.1/v1.2 when Stmt Resource tuning Broccoli DPD
Bro Cluster Shunt
v1.3 Ctor expressions GeoIP Conn Compressor
Autotuning
v1.4 DHCP/BitTorrent HTTP entities NetFlow Bro Lite Deprecated
Parallel Prototype
v1.5 BroControl
Bro SDCI
NSF
v2.0 User Experience
Input Framework
v2.1 IPv6 Input Framew.
SSL Trust SSL Errors
v2.2 File Analysis Summary Stats
Bro Center
NSF
Summary Stats HILTI DPI Concurrency PLC Modeling Android Root Certs Heart bleed
v2.3 Performance SNMP, Radius, SSL++
NetControl VAST
v2.4 Broker, Plugins, DTLS/KRB
Tor SSL OCSP Speed Certificate Ecosystem TLS Electronic Comm. Spicy
v2.5, SMB, NetControl, VNC, StartTLS

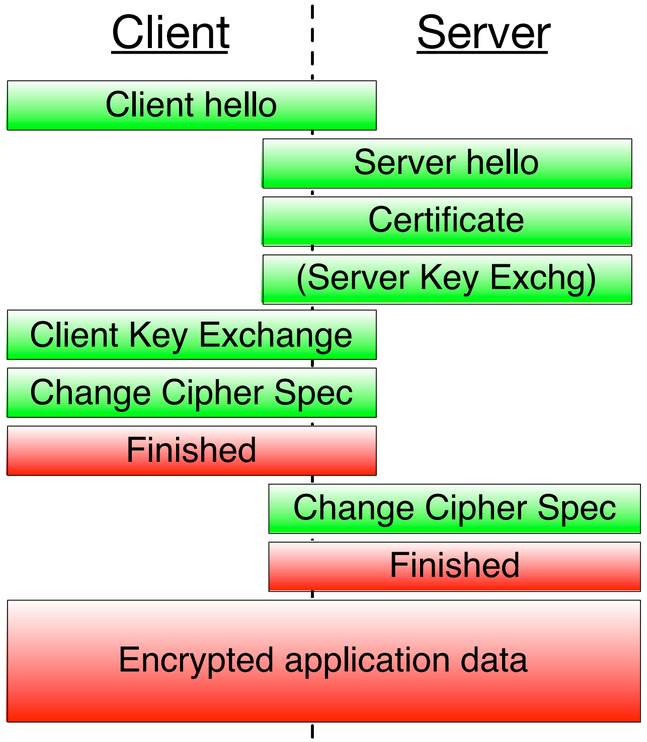
Bro SSL - v1.5.3


ssl_certificate_seen
ssl_certificate
ssl_conn_attempt
ssl_conn_alert
ssl_conn_server_reply
ssl_conn_weak
ssl_conn_established
ssl_session_insertion
ssl_conn_reused
process_X509_extensions
ssl_X509_error

Bro SSL - v1.5.3

- ssl_certificate_seen
- ssl_certificate
- ssl_conn_attempt
- ssl_conn_alert
- ssl_conn_server_reply
- ssl_conn_weak
- ssl_conn_established
- ssl_session_insertion
- ssl_conn_reused
- process_X509_extensions
- ssl_X509_error





Bro SSL - v2.0


client_hello
server_hello
ssl_session_ticket_handshake
ssl_established
x509_certificate
ssl_extension
ssl_alert

Bro SSL - v2.1

client_hello

server_hello

ssl_session_ticket_handshake

ssl_established

x509_certificate

ssl_extension

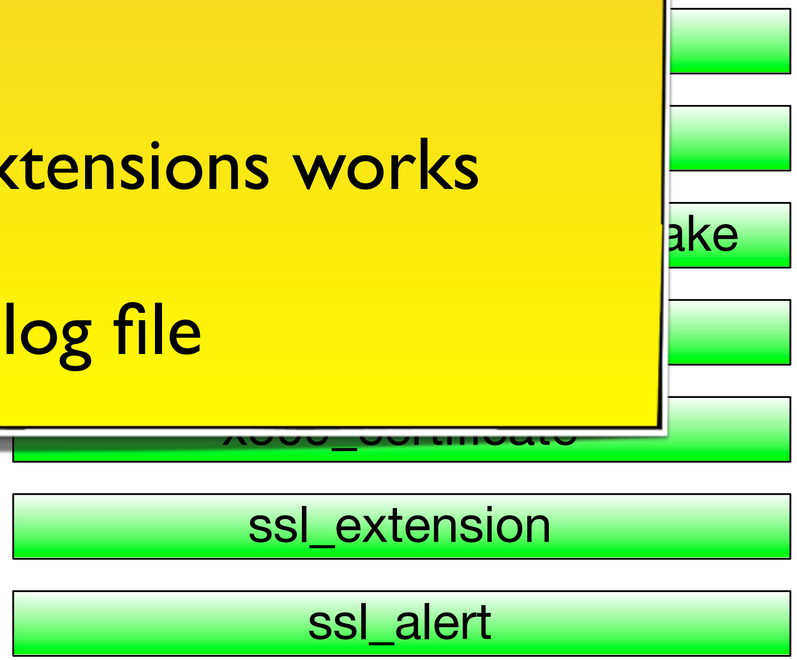
ssl_alert

Bro SSL - v2.1

Several bug fixes

Parsing TLS server extensions works

More information in log file



Bro SSL - v2.2

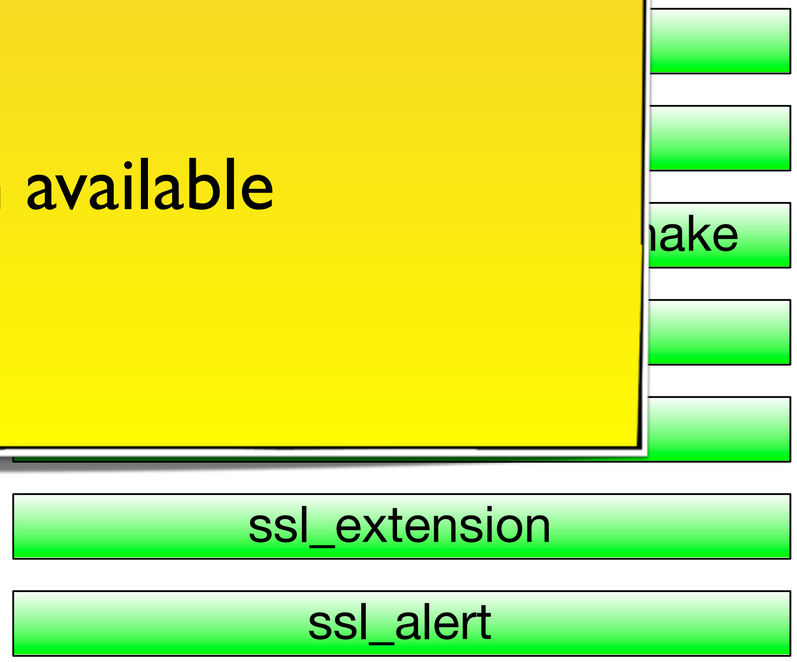

client_hello
server_hello
ssl_session_ticket_handshake
ssl_established
x509_certificate
ssl_extension
ssl_alert

Bro SSL - v2.2

Several bug fixes

Client/server random available

Support TLS 1.2



Bro SSL - v2.3


client_hello
server_hello
ssl_session_ticket_handshake
ssl_established
x509_certificate
ssl_extension
ssl_alert

Bro SSL - v2.3

client_hello

server_hello

ssl_session_ticket_handshake

ssl_established

x509_certificate

ssl_extension

ssl_alert

ssl_stapled_ocsp

ssl_encrypted_data

ssl_dh_server_params

ssl_change_cipher_spec

ssl_handshake_message

ssl_encrypted_data

ssl_extension_ex_point_formats

ssl_server_curve

ssl_change_cipher_spec

x509_extension

x509_ext_basic_constraints

x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

Bro SSL events - v2.4

client_hello

server_hello

ssl_session_ticket_handshake

ssl_established

x509_certificate

ssl_extension

ssl_alert

ssl_stapled_ocsp

ssl_encrypted_data

ssl_dh_server_params

ssl_change_cipher_spec

ssl_handshake_message

ssl_encrypted_data

ssl_extension_ex_point_formats

ssl_server_curve

ssl_change_cipher_spec

x509_extension

x509_ext_basic_constraints

x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

Bro SSL events - v2.4

First DTLS support

TLS record layer fragmentation

ssl_established

x509_certificate

ssl_extension

ssl_alert

ssl_change_cipher_spec

ssl_handshake_message

ssl_encrypted_data

ssl_extension_ex_point_formats

ssl_server_curve

ssl_change_cipher_spec

x509_extension

x509_ext_basic_constraints

x509_ext_subject_alternative_name

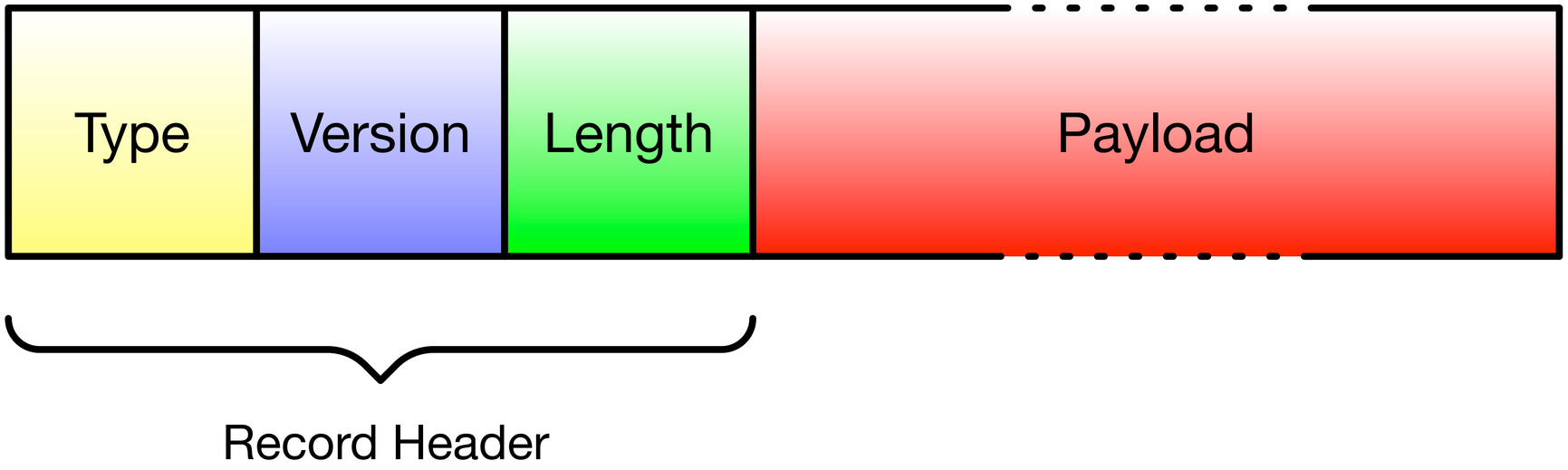
ssl_extension_elliptic_curves

ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

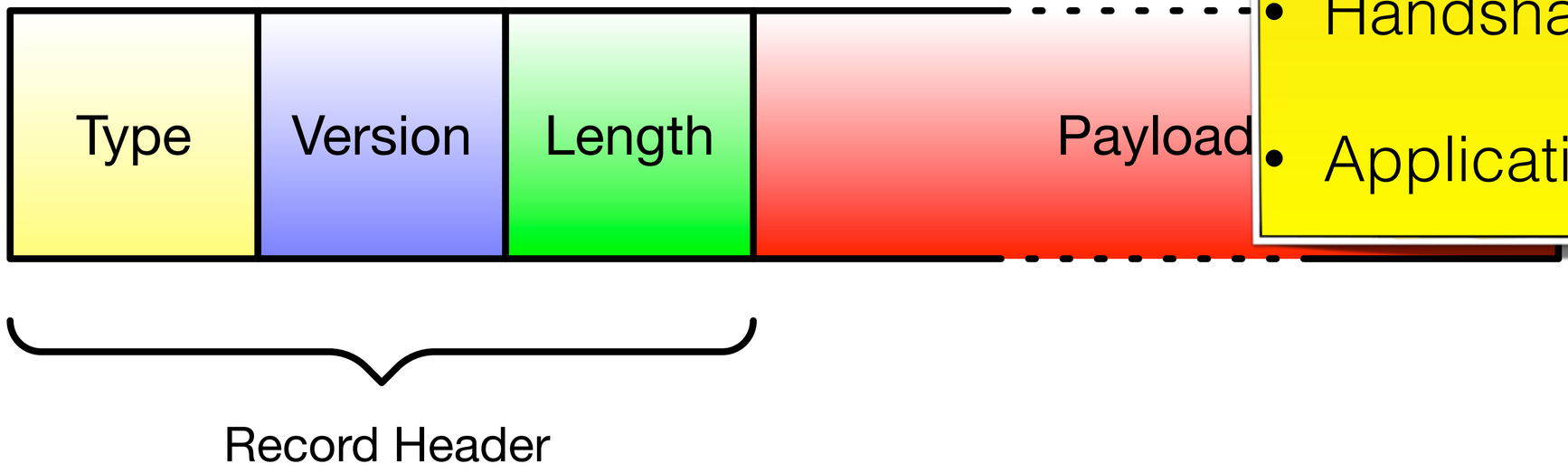
SSL Protocol Basics

- Record based protocol
- Records do not have to map to TCP packets
- Record header is never encrypted, only payload is (after the handshake is done)



SSL Protocol Basics

- Record based protocol
- Records do not have to map to TCP packets
- Record header is never encrypted, only payload (after the handshake is done)

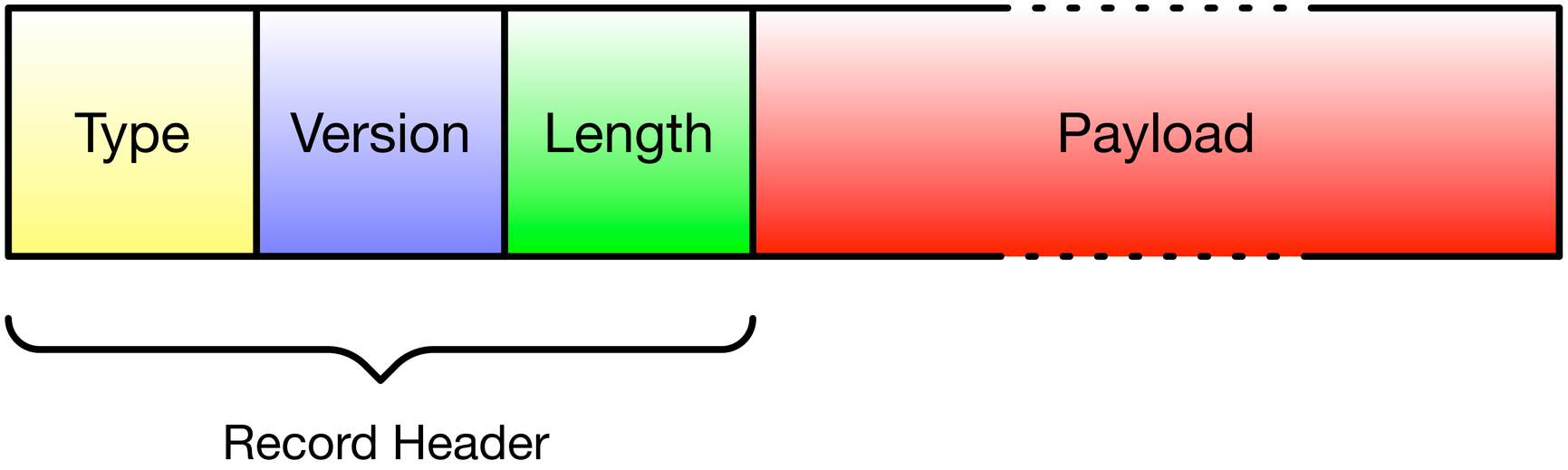


Common record types:

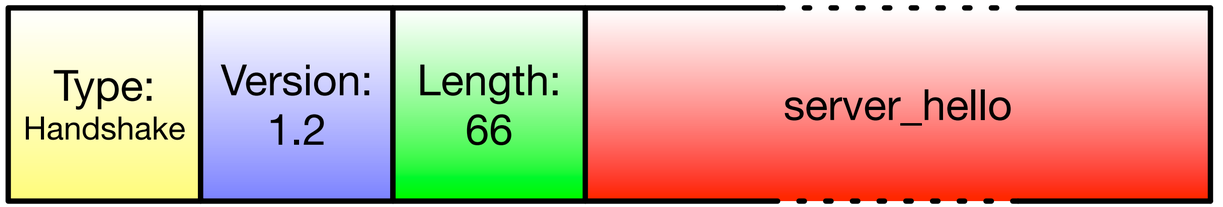
- Change Cipher Spec
- Alert
- Handshake
- Application Data

SSL Protocol Basics

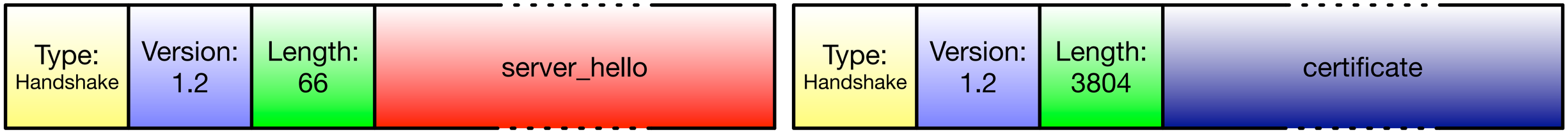
- Record based protocol
- Records do not have to map to TCP packets
- Record header is never encrypted, only payload is (after the handshake is done)



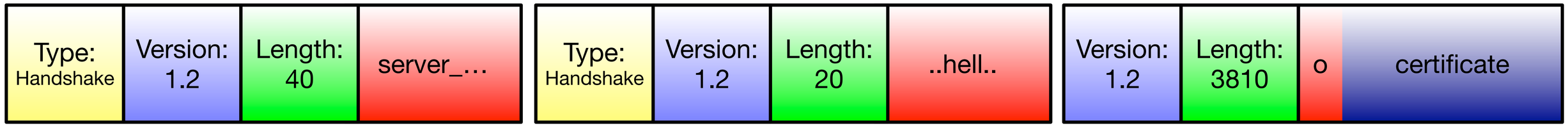
Fragmentation



Fragmentation



Fragmentation



Bro SSL events - v2.5

client_hello

server_hello

ssl_session_ticket_handshake

ssl_established

x509_certificate

ssl_extension

ssl_alert

ssl_stapled_ocsp

ssl_encrypted_data

ssl_dh_server_params

ssl_change_cipher_spec

ssl_handshake_message

ssl_encrypted_data

ssl_extension_ex_point_formats

ssl_server_curve

ssl_change_cipher_spec

x509_extension

x509_ext_basic_constraints

x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

Bro SSL events - v2.5

client_hello

server_hello

ssl_session_ticket_handshake

ssl_established

x509_certificate

ssl_extension

ssl_alert

ssl_server_curve

ssl_stapled_ocsp

ssl_encrypted_data

ssl_dh_server_params

ssl_change_cipher_spec

ssl_handshake_message

ssl_encrypted_data

ssl_extension_ex_point_formats

ssl_extension_signature_algorithm

ssl_change_cipher_spec

x509_extension

x509_ext_basic_constraints

x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

Bro SSL events - v2.5

Completely working DTLS support

More StartTLS

ssl_change_cipher_spec

x509_extension

ss

x509_ext_basic_constraints

ssl_established

ssl_change_cipher_spec

x509_ext_subject_alternative_name

x509_certificate

ssl_handshake_message

ssl_extension_elliptic_curves

ssl_extension

ssl_encrypted_data

ssl_extension_application_layer_protocol_negotiation

ssl_alert

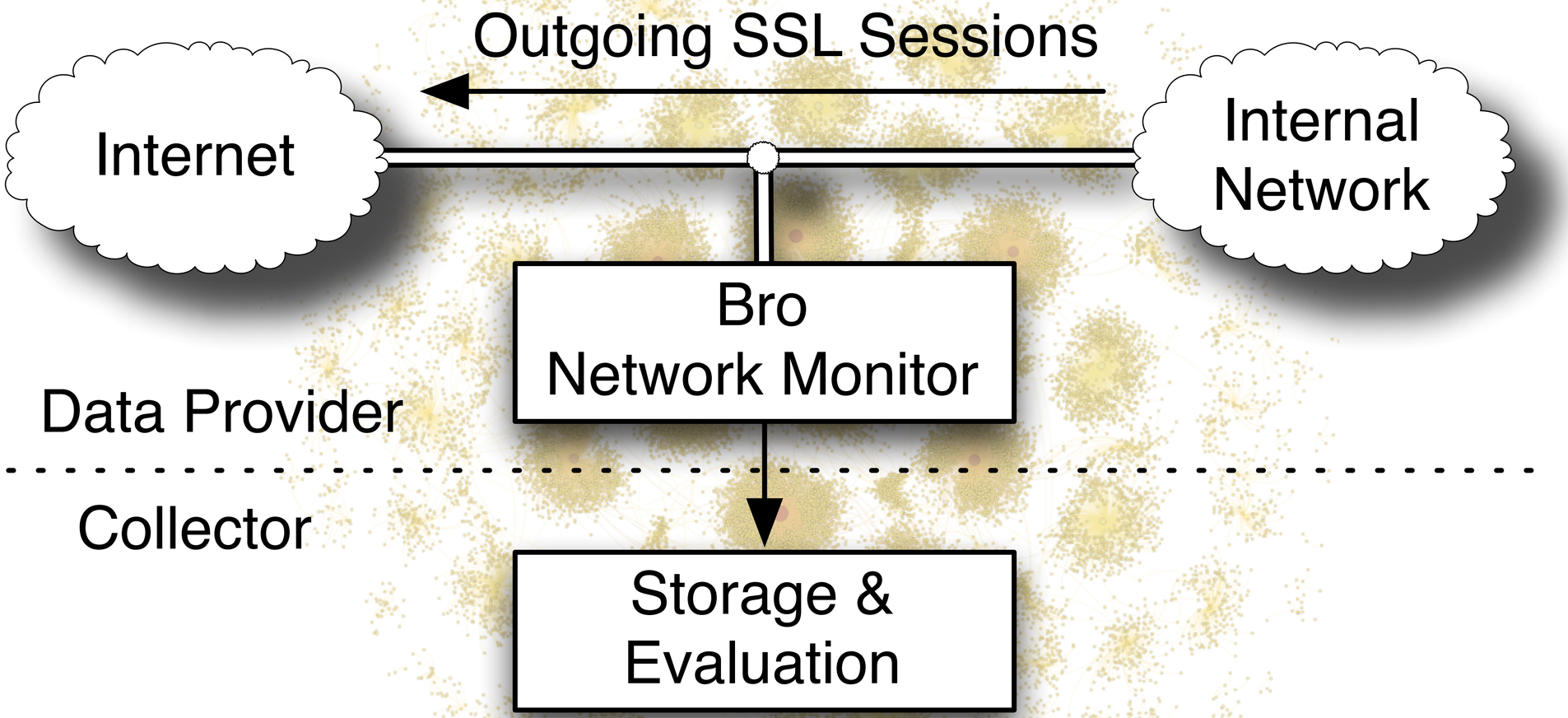
ssl_extension_ex_point_formats

ssl_extension_server_name

ssl_server_curve

ssl_extension_signature_algorithm

ICSI Notary


Outgoing SSL Sessions
Internet
Internal Network
Bro Network Monitor
Data Provider
Collector
Storage & Evaluation

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)

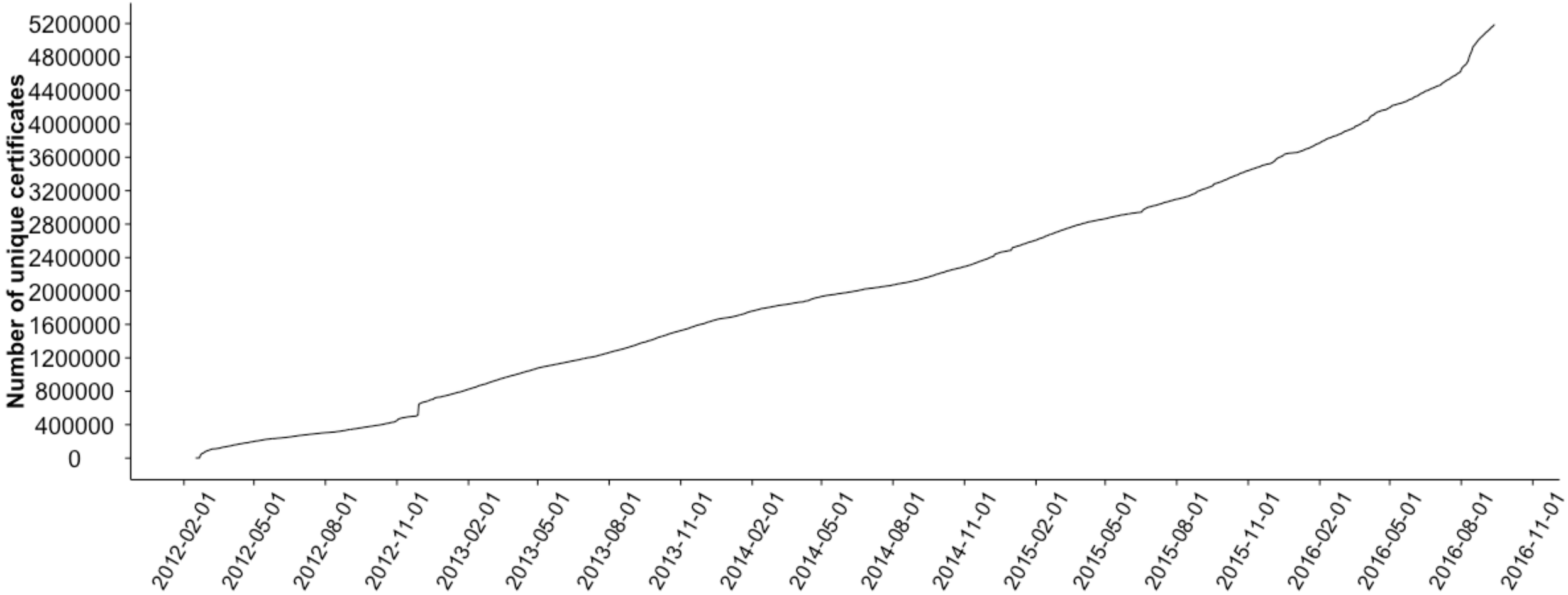
Ticket lifetime hint

Client EC curve

Number Client Certs

TLS Alerts

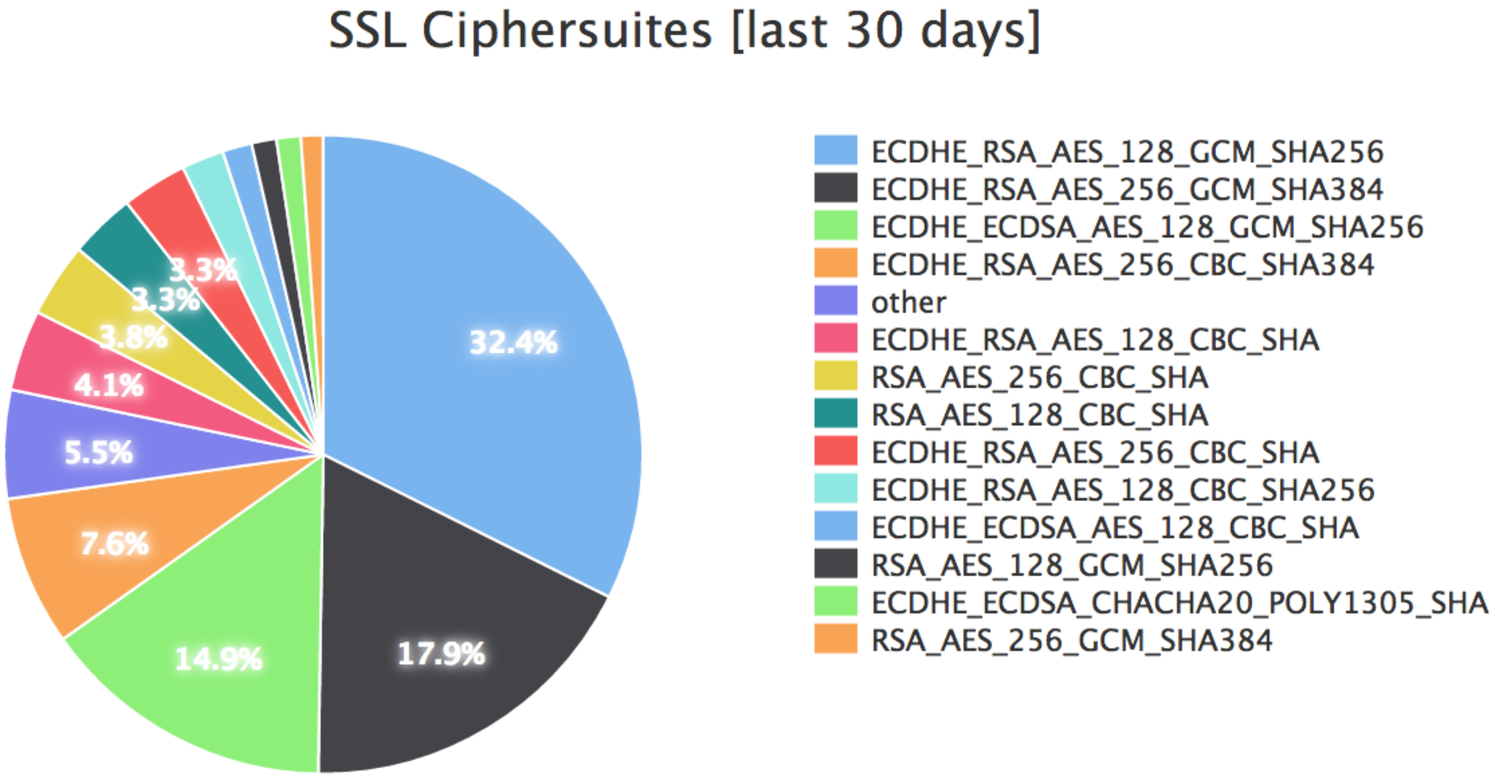
Notary - Certificates



http://notary.icsi.berkeley.edu

Connection Cipher Details

The following graph shows the most-used cipher-suites that we saw being used in all connections in the last 30 days.



SSL Research 2016

Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement

J. Amann, R. Sommer, *PAM 2016*

Measuring the Latency and Pervasiveness of TLS Certificate Revocation

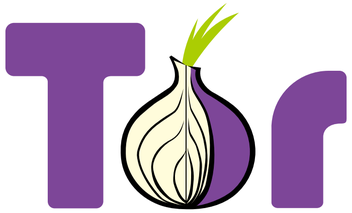
L. Zhu, J. Amann, J. Heidemann, *PAM 2016*

TLS in the wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication

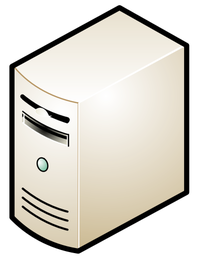
R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, *NDSS 2016*

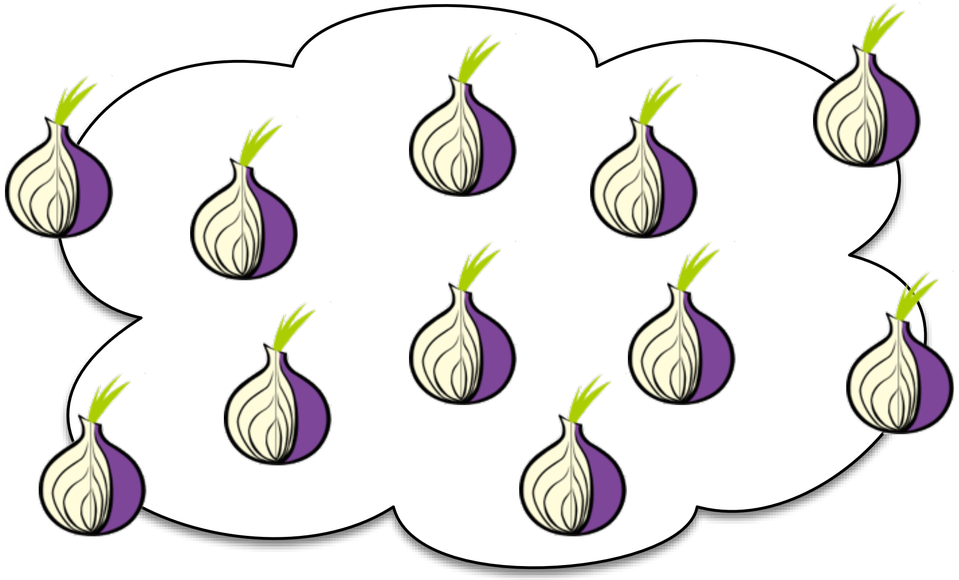
Towards a Complete View of the Certificate Ecosystem

B, VanderSloot, J. Amann, M. Bernhard, Z. Durumeric, M. Bailey, J. A. Halderman, *IMC 2016*



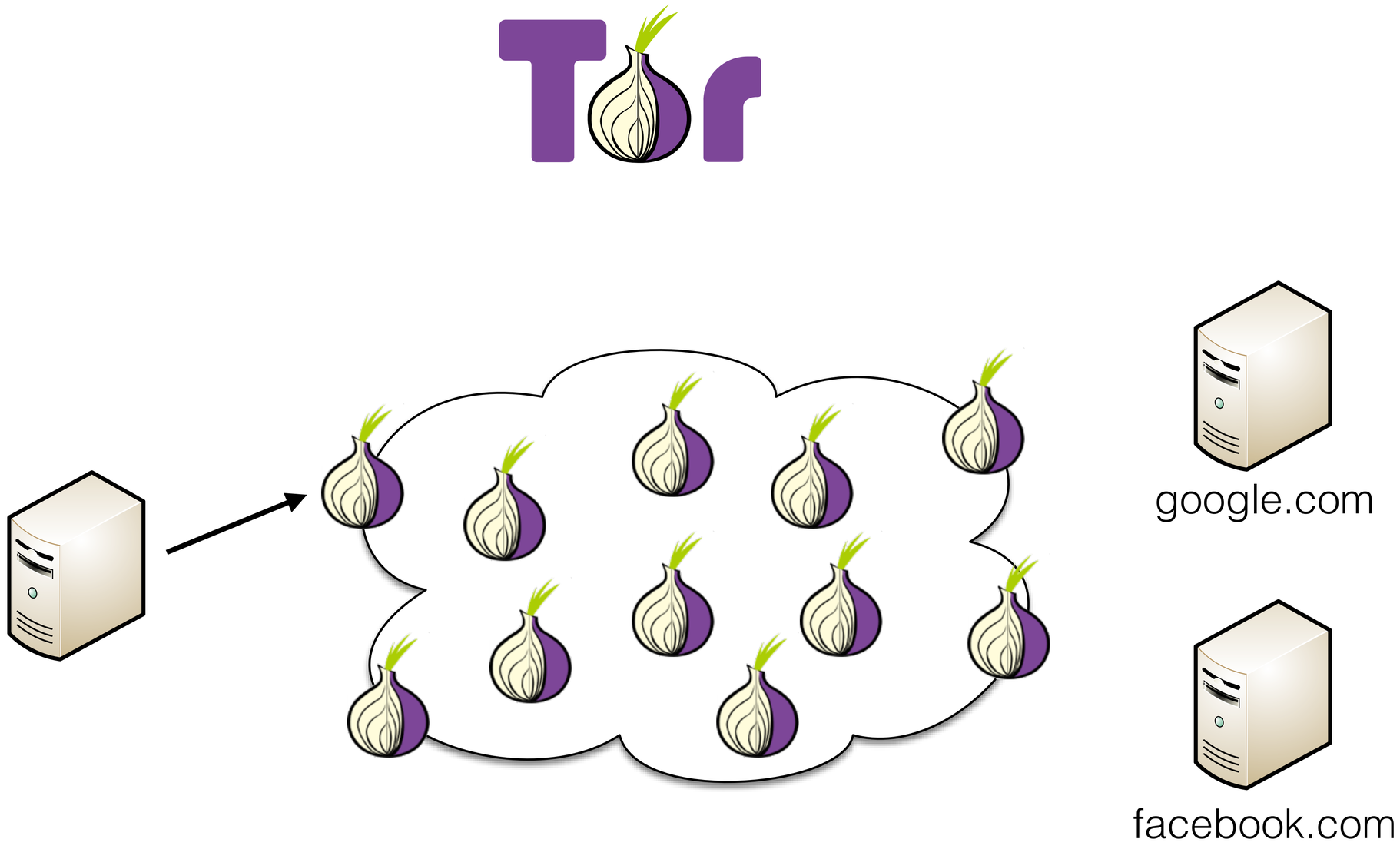
- Popular network for anonymous Internet access
- First release in 2002
- Today more than 2,000,000 simultaneous clients
- Uses TLS as its underlying communication protocol

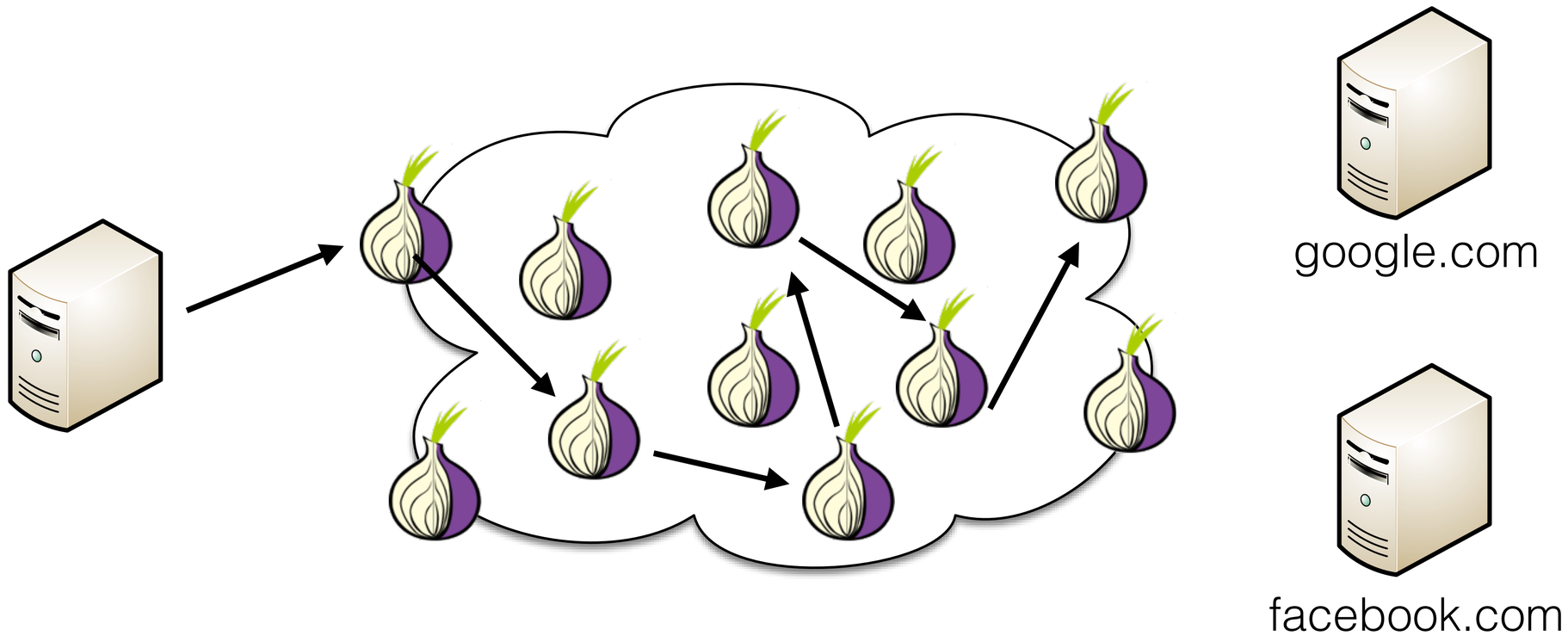


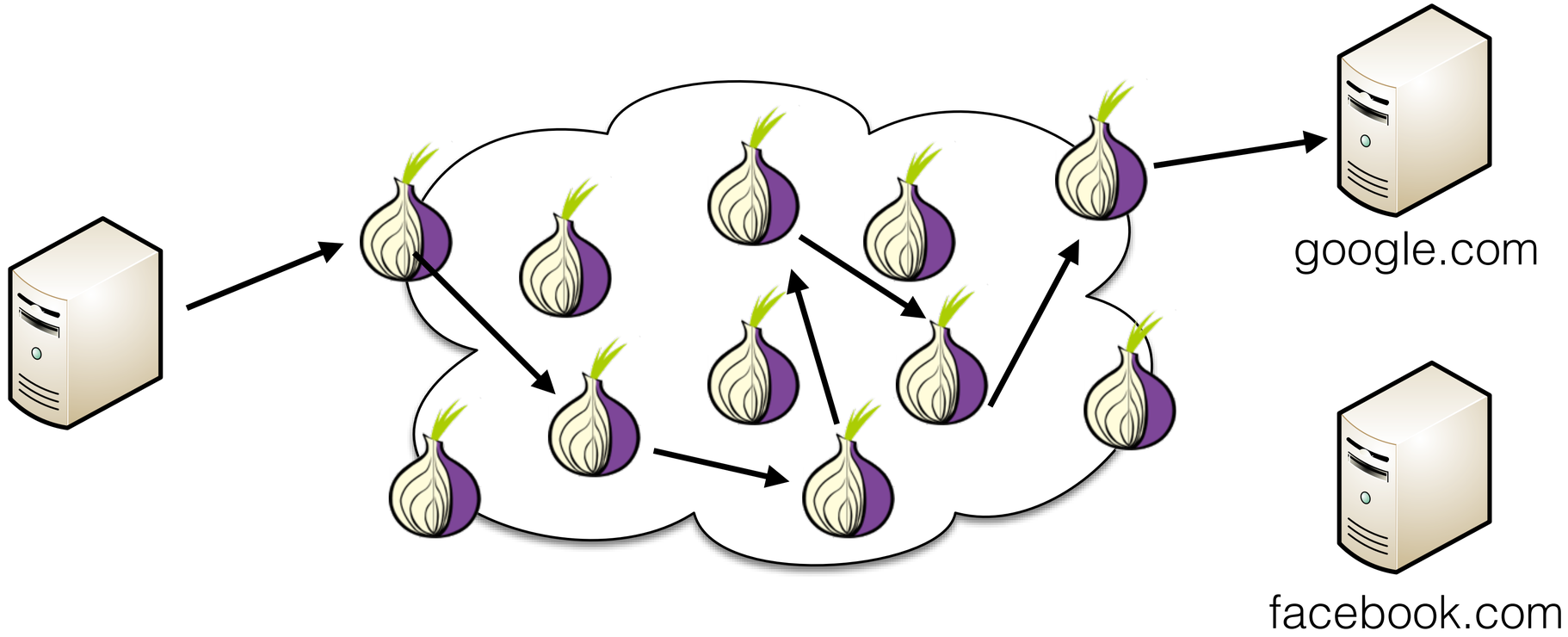


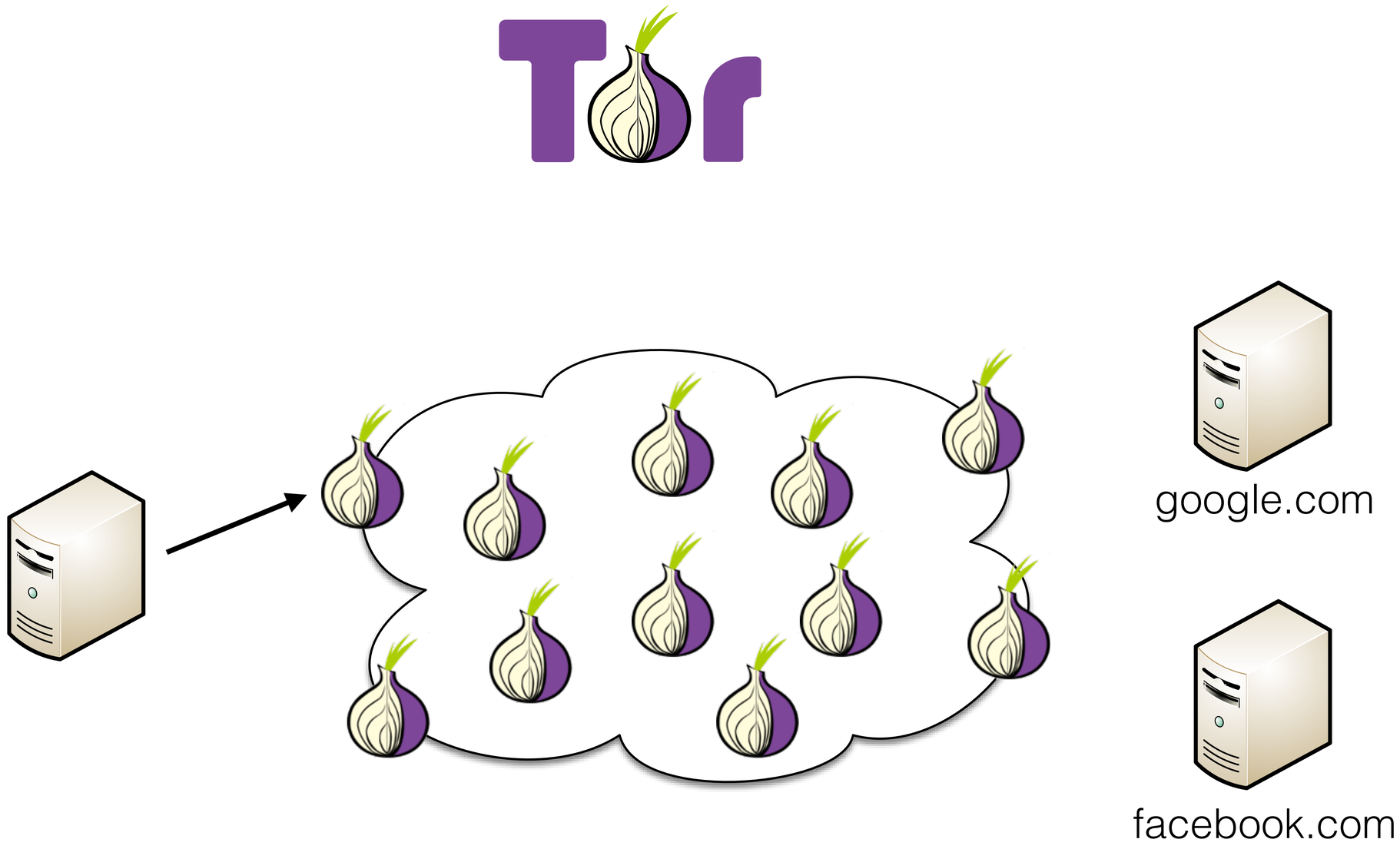
google.com

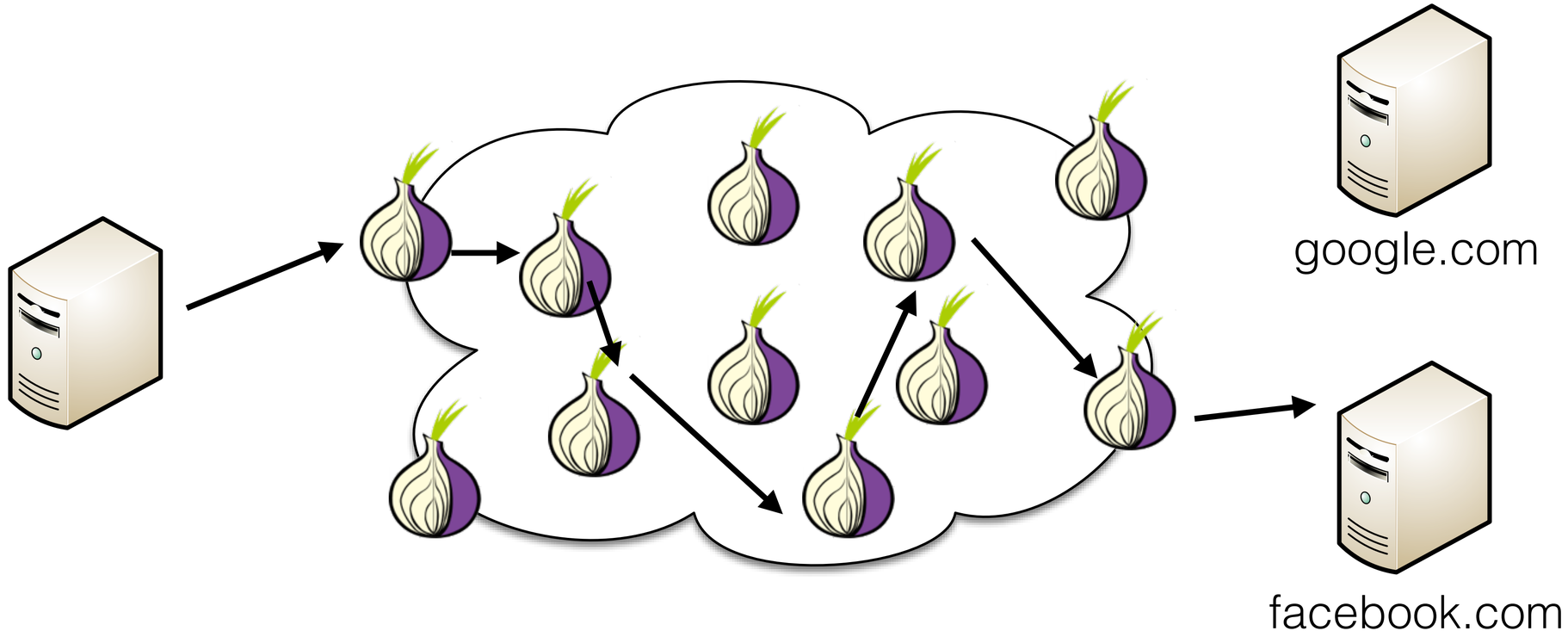
facebook.com

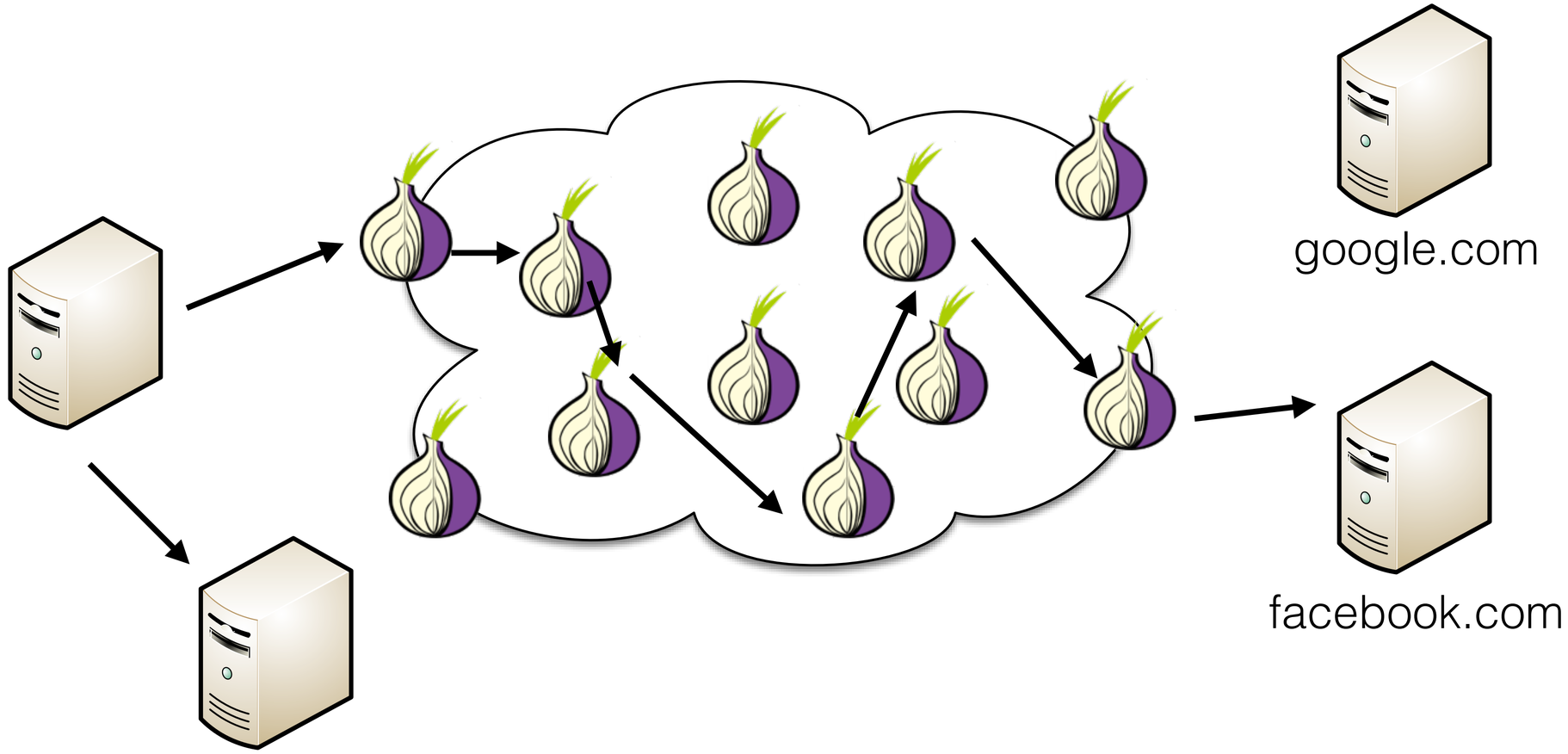

Tor
google.com
facebook.com


google.com
facebook.com


google.com
facebook.com


Tor
google.com
facebook.com


google.com
facebook.com


google.com
facebook.com
Directory Server

Tor Certificates

Version	3
Issuer	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Domain Validation CA - SHA256 - G2
Subject	OU=Domain Control Validated, CN=*.bro.org
Not-Before	Aug 25 16:55:00 2015 GMT
Not-After	Nov 28 21:21:16 2016 GMT

Tor Certificates

Version	3
Issuer	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Domain Validation CA - SHA256 - G2
Subject	OU=Domain Control Validated, CN=*.bro.org
Not-Before	Aug 25 16:55:00 2015 GMT
Not-After	Nov 28 21:21:16 2016 GMT

Version	3
Issuer	CN=www.hjo5uvxa5cdg3gjgf.com
Subject	CN=www.pongobhog2f6p.net
Not-Before	Dec 17 10:34:58 2013 GMT
Not-After	Dec 17 10:34:58 2014 GMT

Tor Certificates

Version	3
Issuer	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Domain Validation CA - SHA256 - G2
Subject	OU=Domain Control Validated, CN=*.bro.org
Not-Before	Aug 25 16:55:00 2015 GMT
Not-After	Nov 28 21:21:16 2016 GMT

Version	3
Issuer	CN=www.hjo5uvxa5cdg3gjgf.com
Subject	CN=www.pongobhog2f6p.net
Not-Before	Dec 17 10:34:58 2013 GMT
Not-After	Dec 17 10:34:58 2014 GMT

Tor Certificates

```
  tor_tls_init();
  nickname = crypto_random_hostname(8, 20, "www.", ".net");
#ifdef DISABLE_V3_LINKPROTO_SERVERSIDE
  nn2 = crypto_random_hostname(8, 20, "www.", ".net");
#else
  nn2 = crypto_random_hostname(8, 20, "www.", ".com");
#endif
```

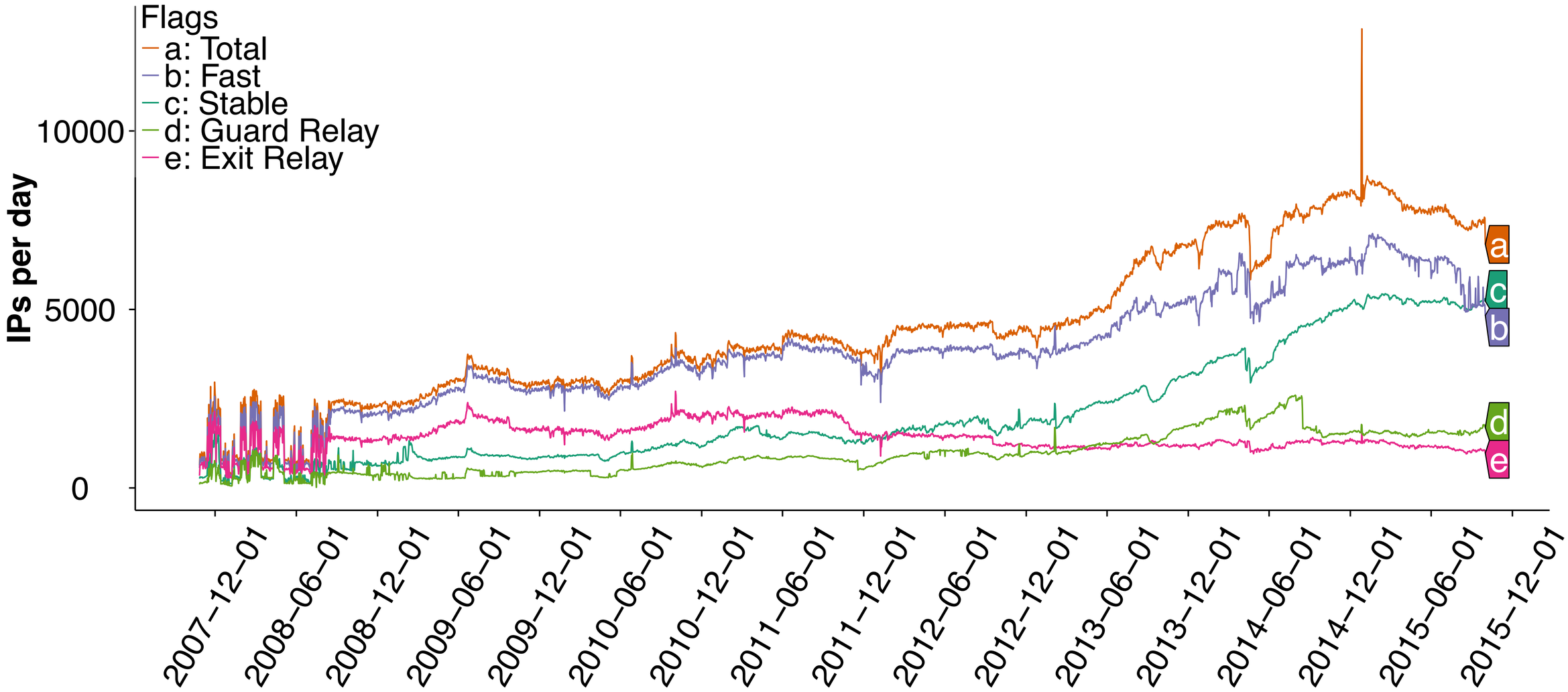
Source: Tor src/common/tortls.c

Tor Certificates

```
/** Generate and return a new random hostname starting with <b>prefix</b>,
 * ending with <b>suffix</b>, and containing no fewer than
 * <b>min_rand_len</b> and no more than <b>max_rand_len</b> random base32
 * characters. Does not check for failure.
 *
 * Clip <b>max_rand_len</b> to MAX_DNS_LABEL_SIZE.
 **/
char *
crypto_random_hostname(int min_rand_len, int max_rand_len, const char *prefix,
                       const char *suffix)
{
  char *result, *rand_bytes;
  int randlen, rand_bytes_len;
  size_t resultlen, prefixlen;
```

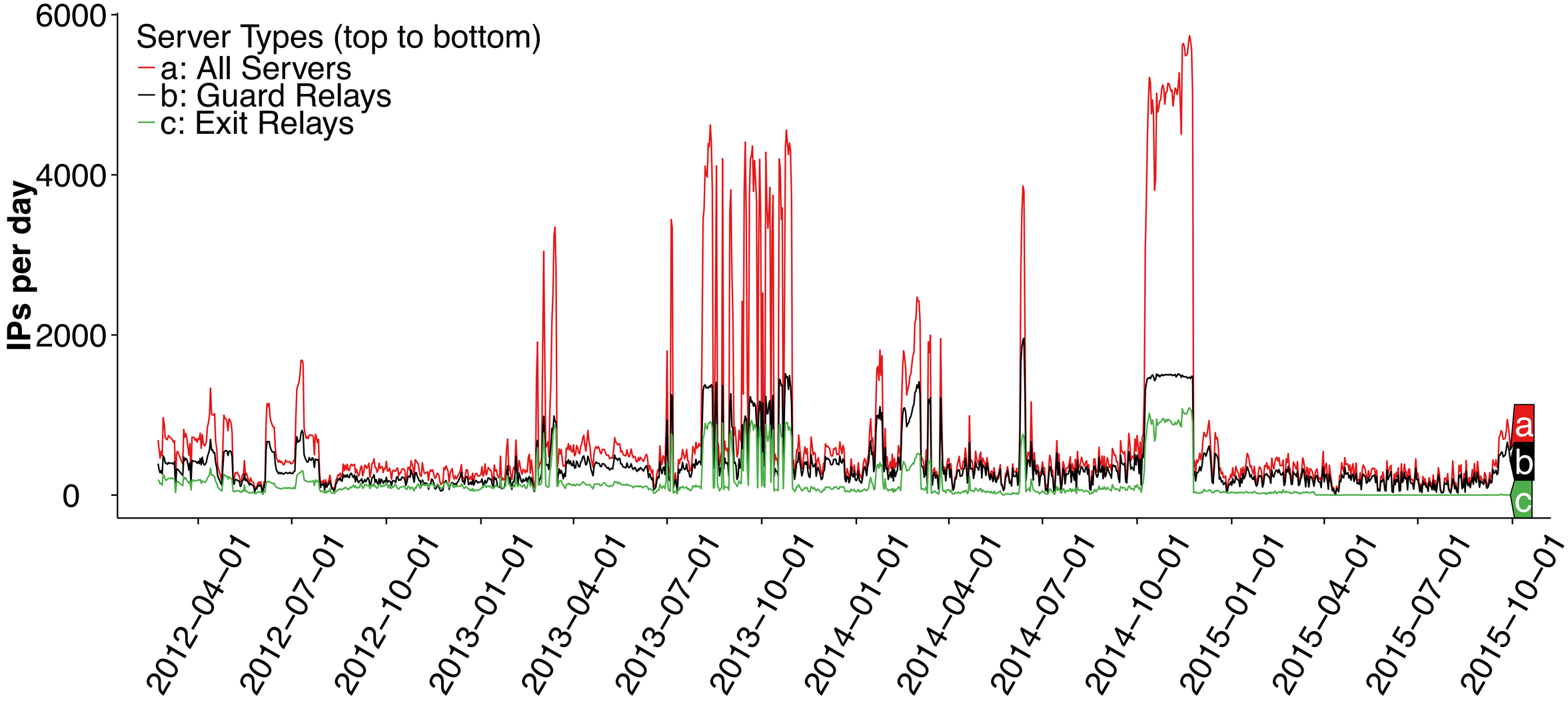
Source: Tor src/common/crypto.c

Relays by Day



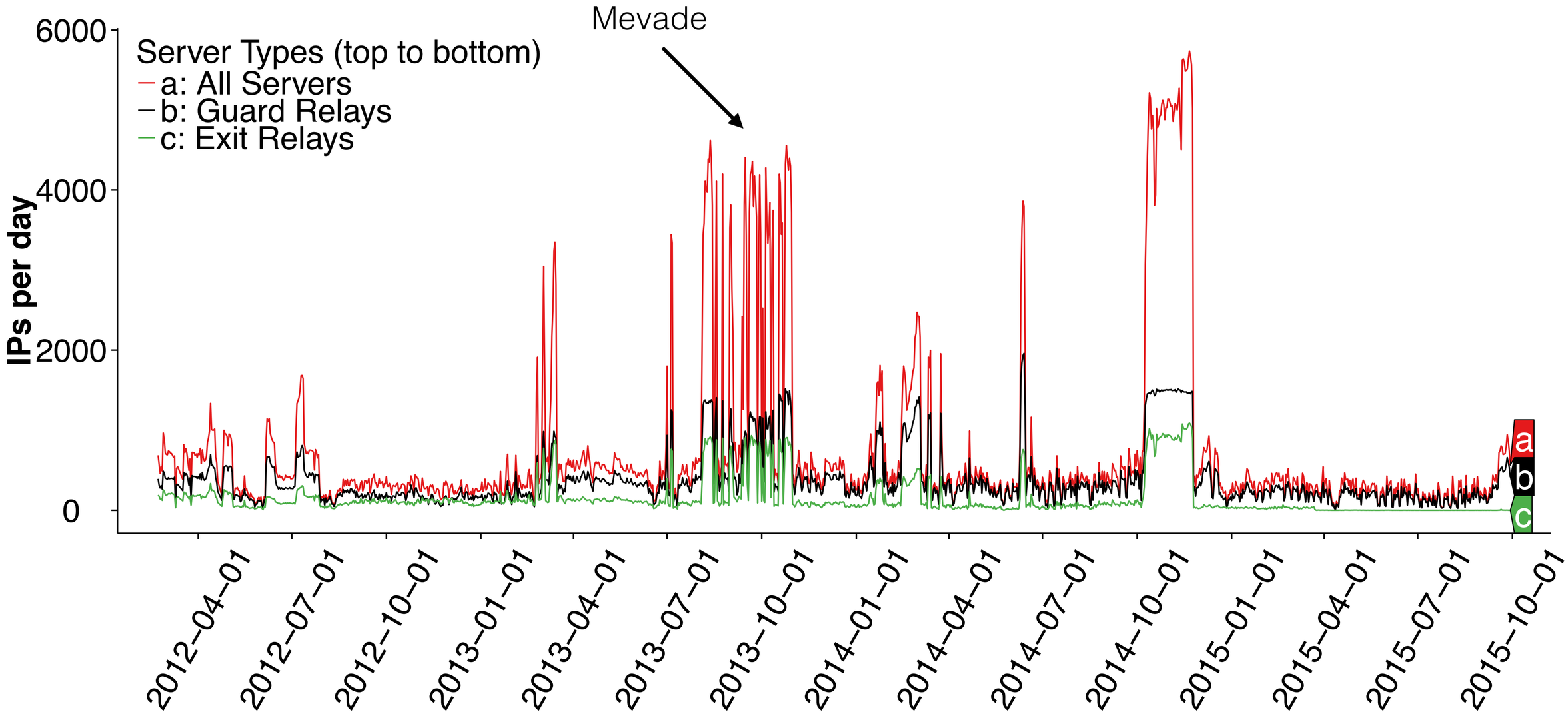
Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

Relays by Day



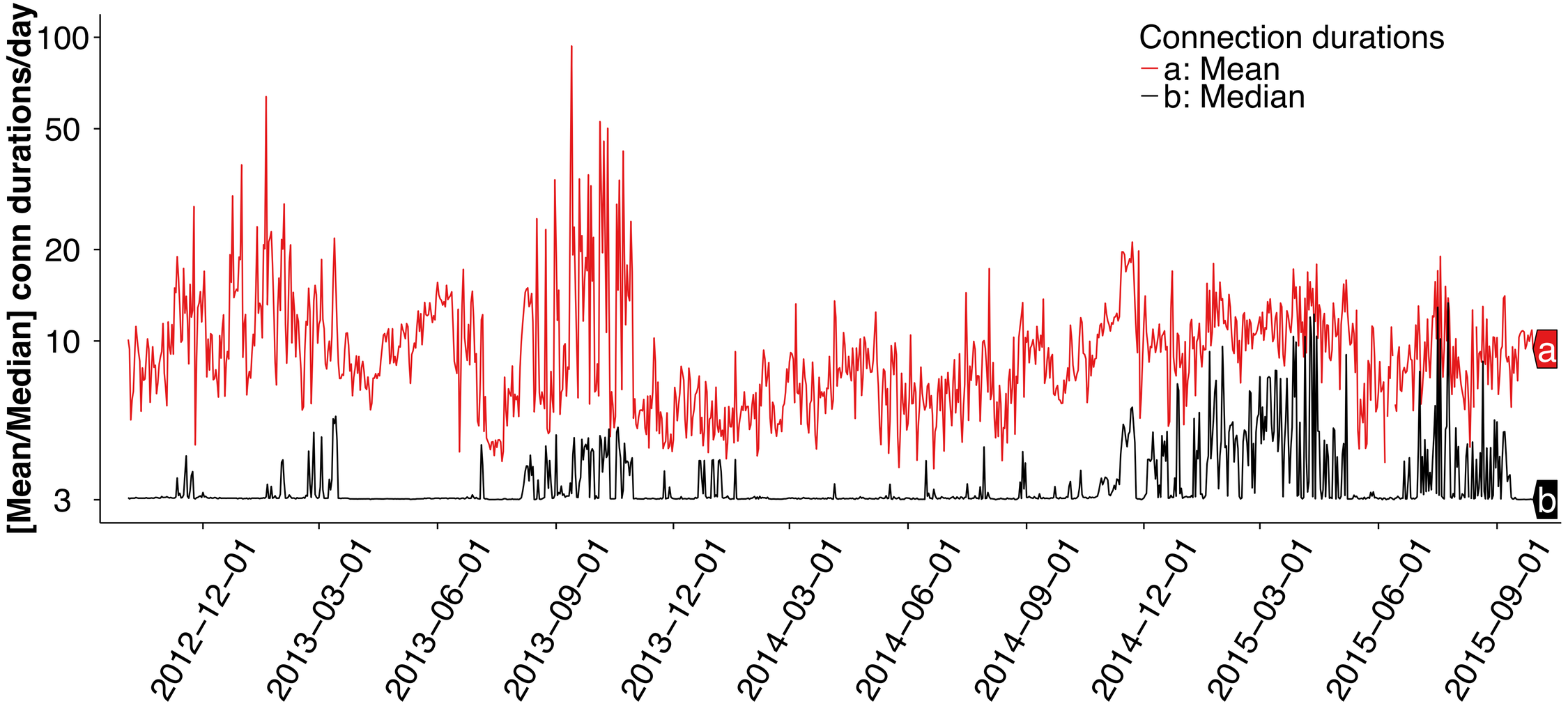
Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

Relays by Day



Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

Median & Mean Conn. Durations



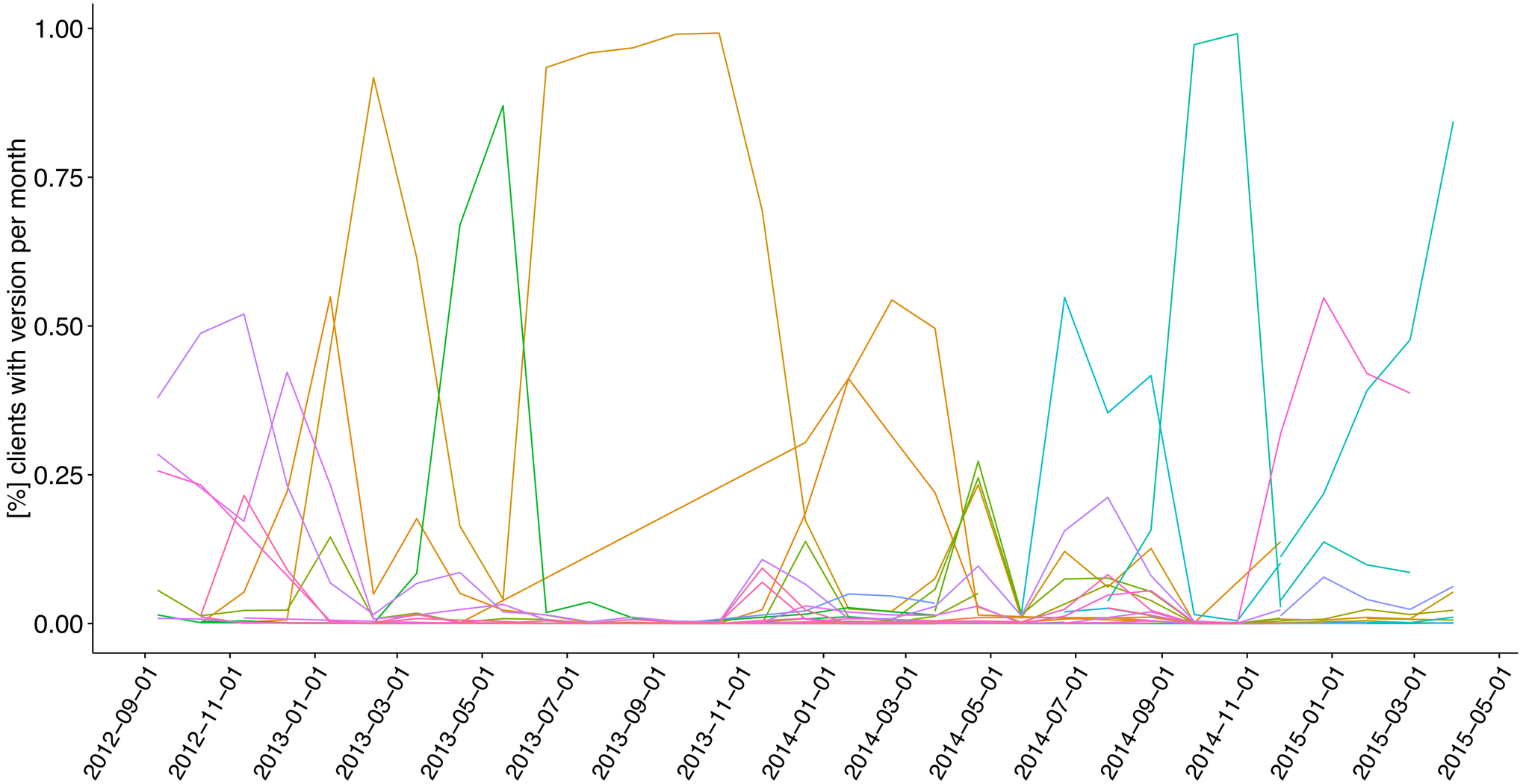
Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

Tor connection Durations

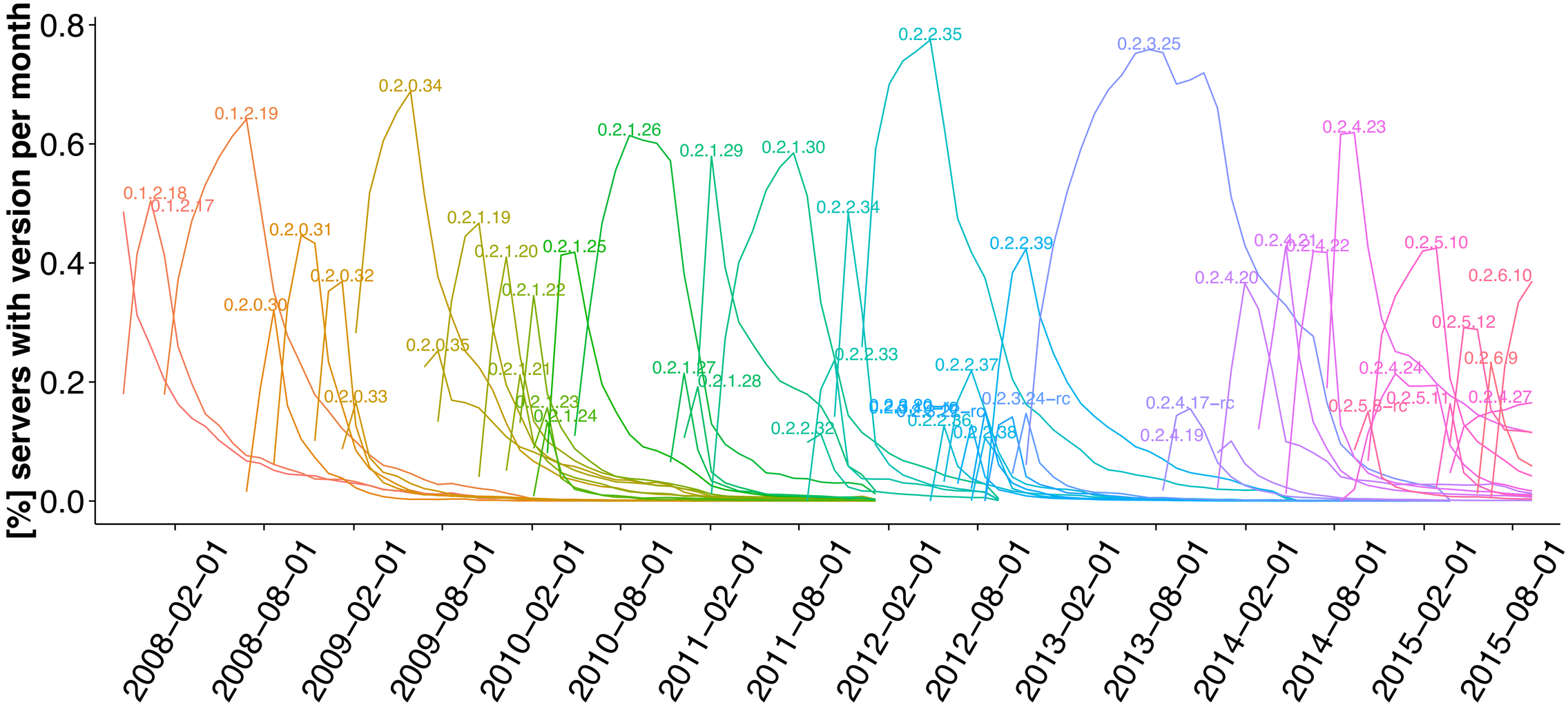
Site	1st Qu.	Median	Mean	3rd Qu.	Max
N1	3.0	3.0	9.6	10.1	9,839
N2	3.0	6.3	19.5	16.8	22,280
N3	1.5	3.0	7.3	3.2	16,370
X1	3.0	3.0	8.3	3.3	10,120

Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

Client Fingerprints

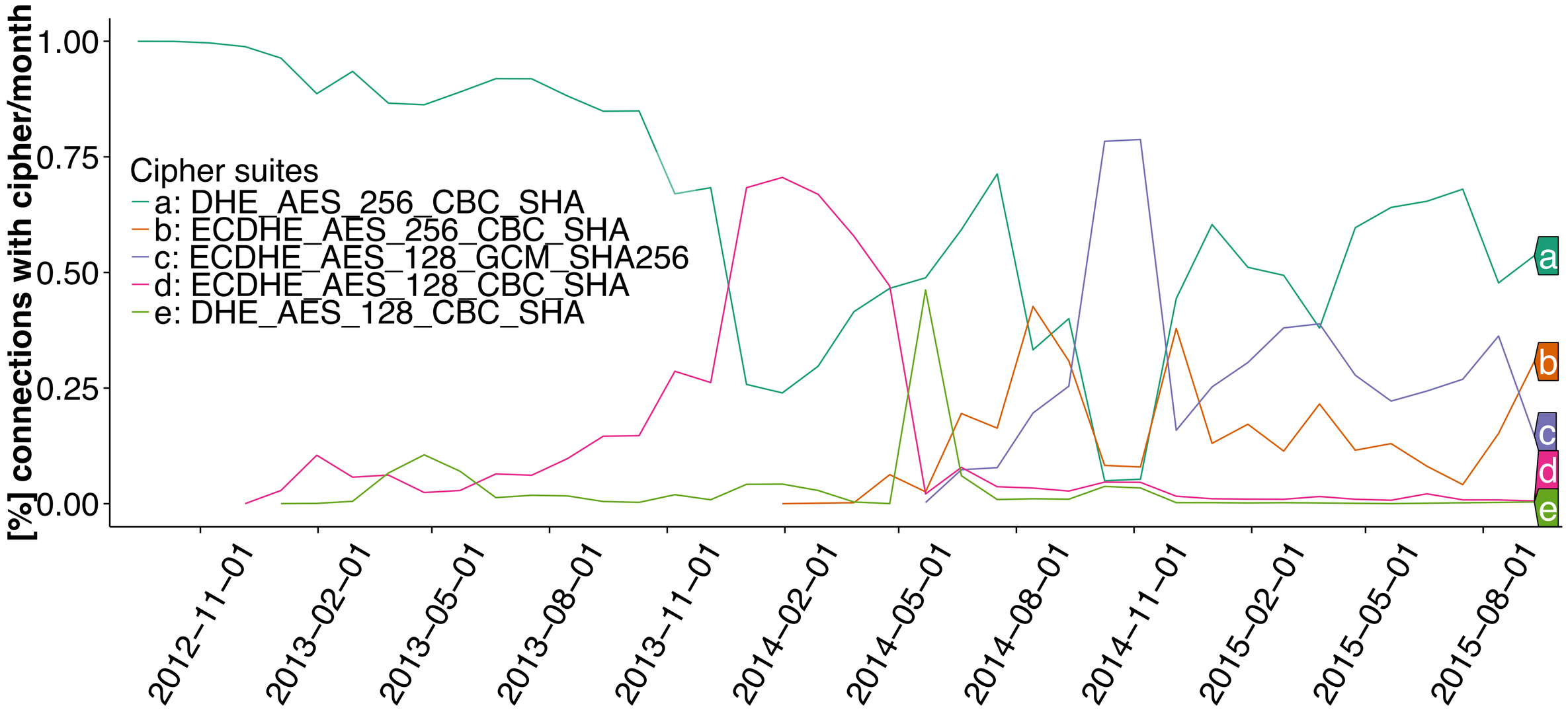


Tor Server Versions



Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

Chosen Ciphersuites



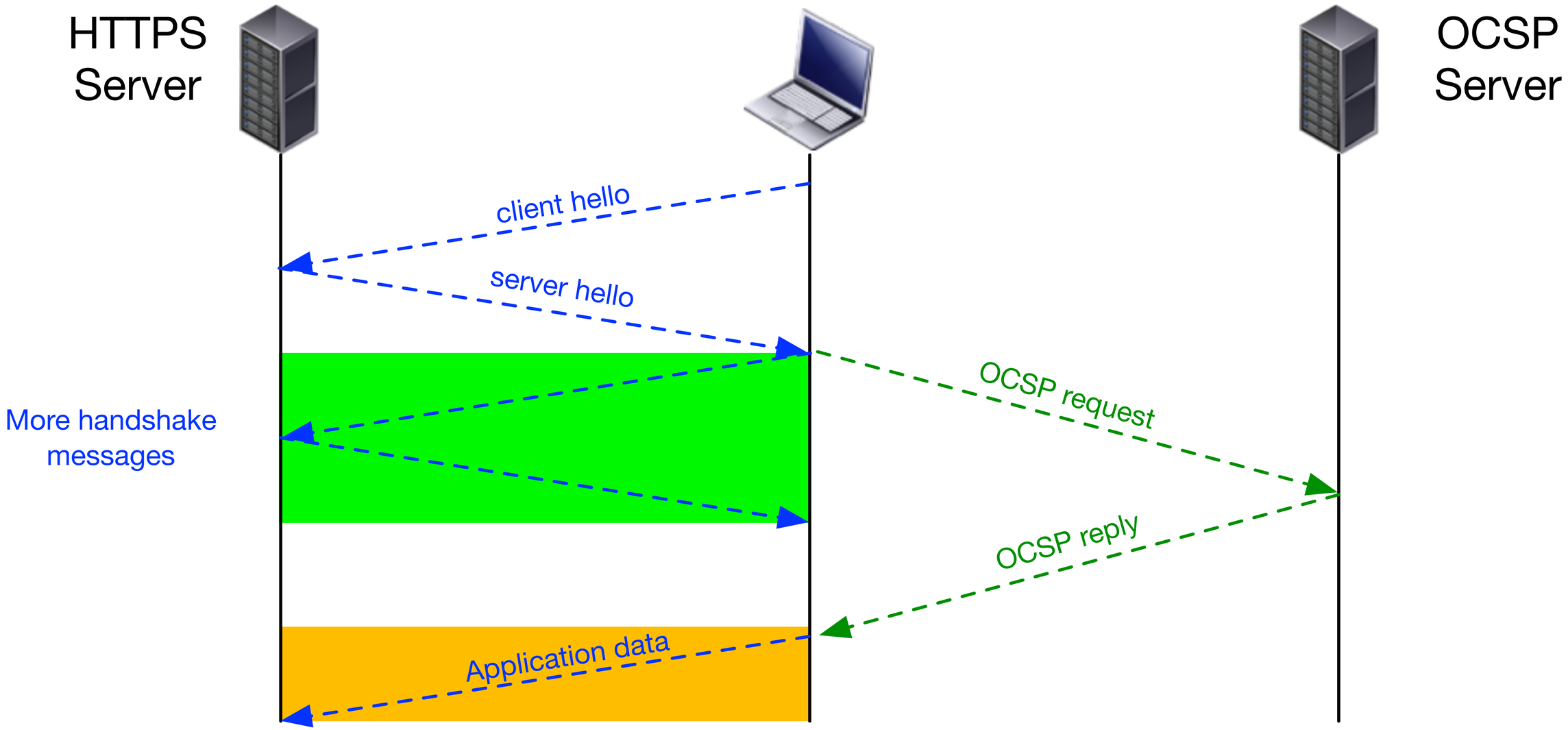
Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement
J. Amann, R. Sommer, PAM 2016

OCSP

Is revocation checking really not feasible?

Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP



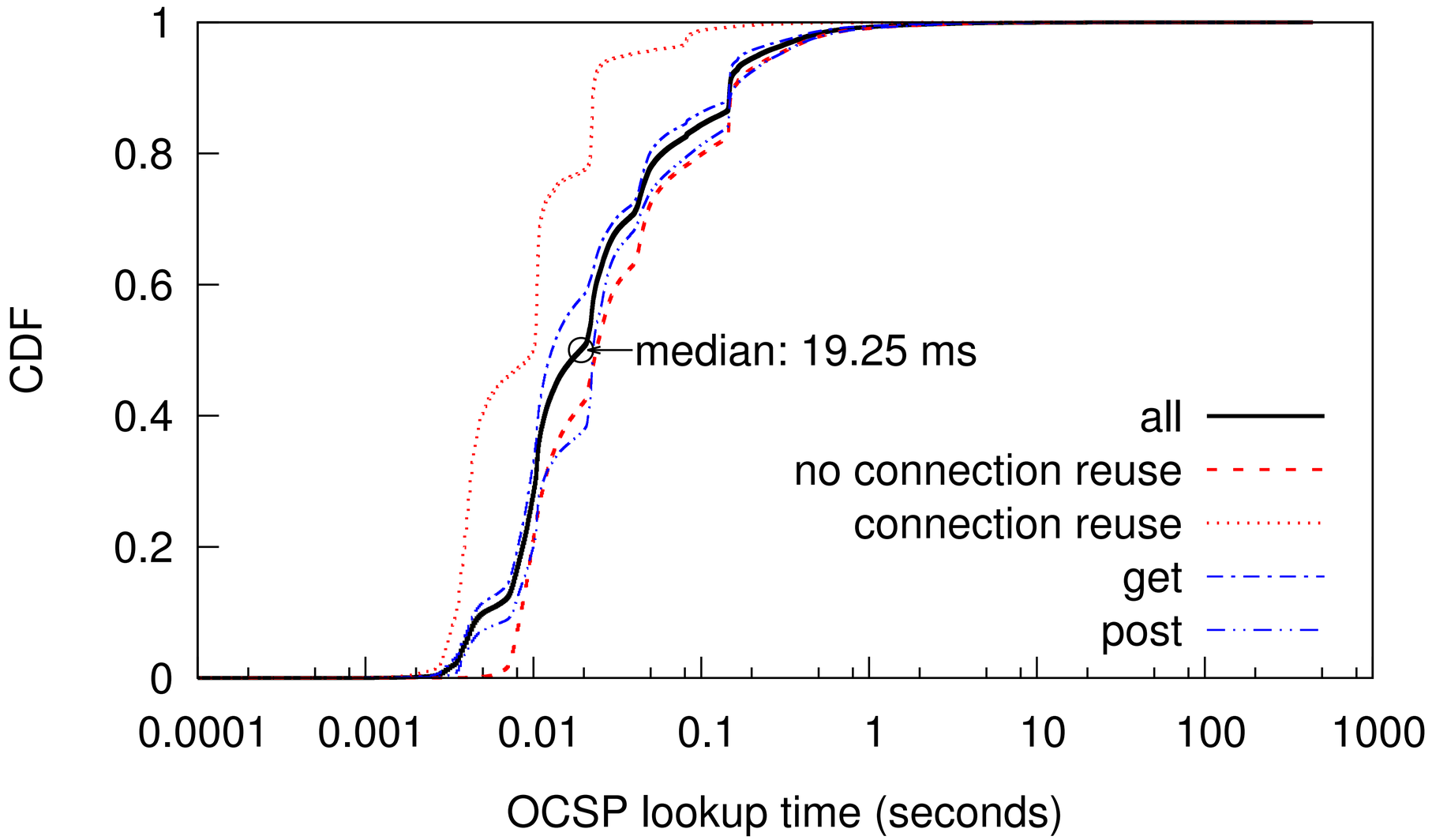
Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP Clients

category		**application**	**percent**
Web browsers	32.10%	Firefox	31.63%
		Chrome	.21%
		Pale moon	.06%
		Opera	.06%
		Rekonq, Bolt, Midori, Iceweasel, Seamonkey, Safari Sonkeror, IE, Camino, Epiphany, Konqueror	<.15%
Library or daemon used by applications	66.87%	ocspd	37.15%
		Microsoft-CryptoAPI	23.74%
		securityd	4.74%
		java	1.24%
		cfnetwork	<.0001%
Email client	.32%	Thunderbird	.30%
		Postbox, Gomeza, Zdesktop, Eudora, Icedove	.02%
Other applications	.33%	Lightning	.31%
		Zotero	.01%
		Celtx, ppkhandler, Komodo, Dalvik, slimerjs, Unity Phoenix, Sunbird, Slurp, miniupnpc, googlebot Entrust entelligence security provider	<.0074%
Unknown	.38%	Unknown	.38%

Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP - Speed



Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP Servers

	Query Traffic		**OCSP Servers**	
CDN	39313464	94%	120	39%
other	2526338	6%	184	61%
total	41839802	100%	304	100%

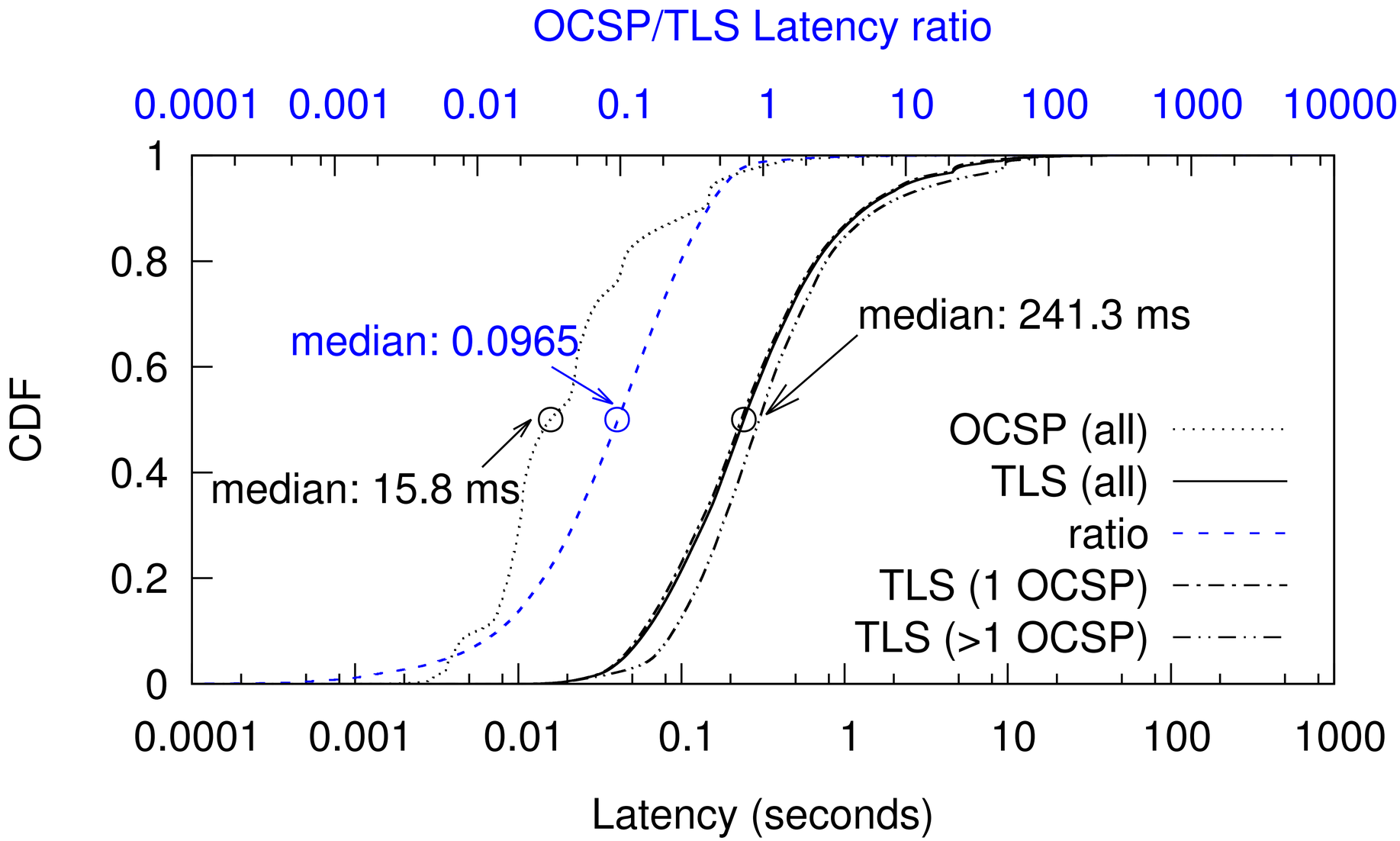
Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP Servers

server	**observed CDN**	**lookup**	
ocsp.digicert.com	phicdn.net	6,205,125	14.83%
clients1.google.com	self-hosted	4,859,409	11.61%
sr.symcd.com	akamaiedge	3,778,672	9.03%
ocsp.entrust.net	akamaiedge	2,421,420	5.79%
ocsp.godaddy.com	self-hosted (using akadns)	2,399,931	5.74%
ocsp.usertrust.com	self-hosted	2,248,577	5.37%
vassg141.ocsp.omniroot.com	akamai	1,915,287	4.58%
ss.symcd.com	akamaiedge	1,663,053	3.97%
ocsp.comodoca.com	self-hosted	1,478,911	3.53%
ocsp.verisign.com	akamaiedge	1,345,724	3.22%
all 294 others		13,523,693	32.32%
total		41,839,802	100%

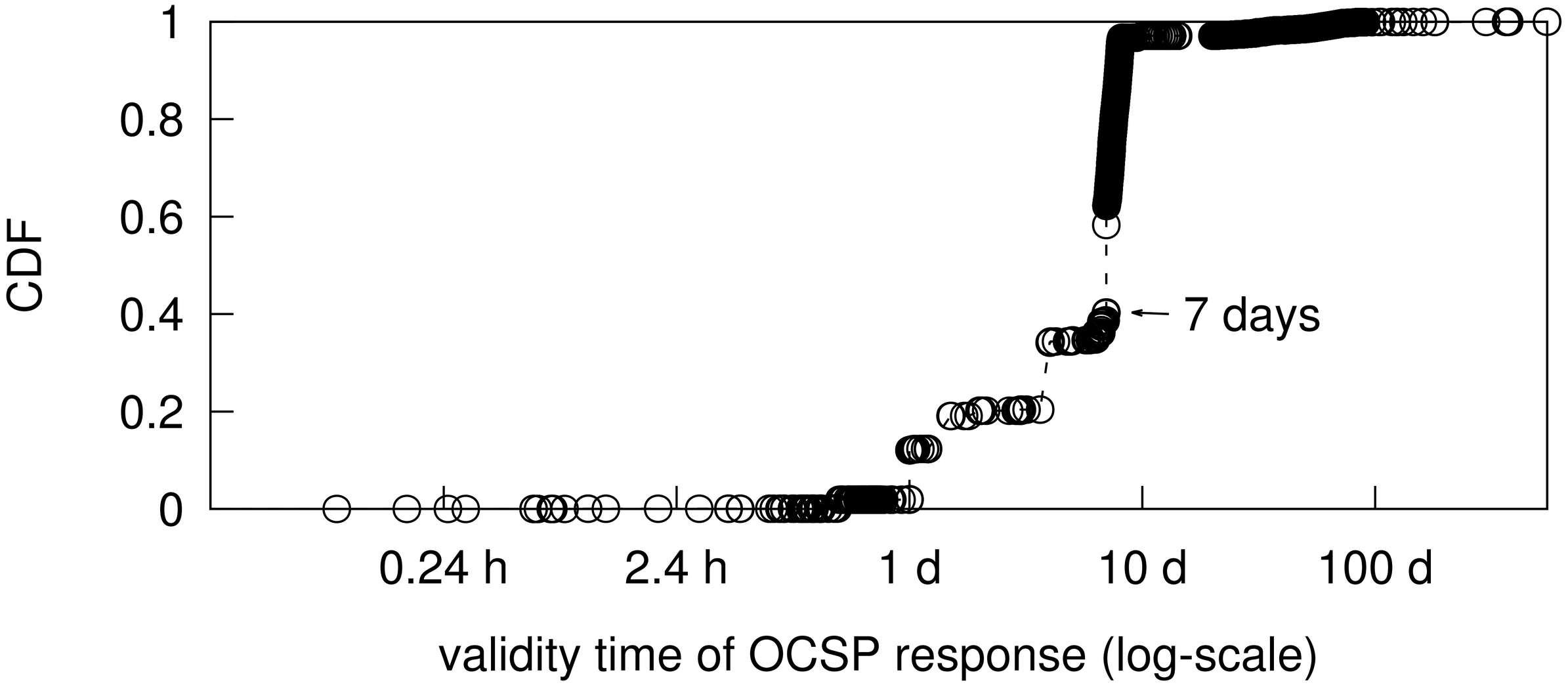
Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP - Speed



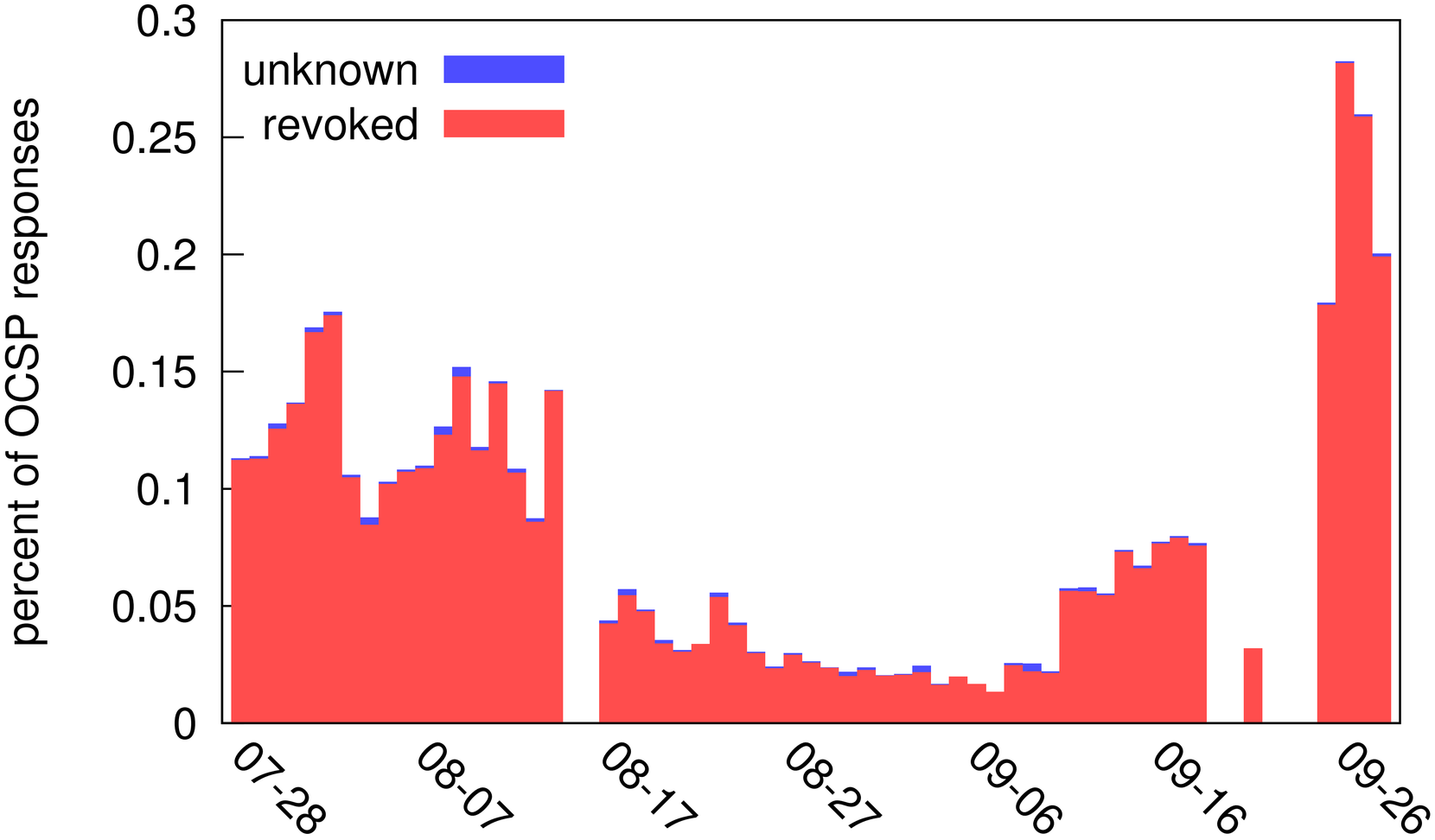
Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP - Caching time



Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

OCSP - Revoked Certificates



Measuring the Latency and Pervasiveness of TLS Certificate Revocation
L. Zhu, J. Amann, J. Heidemann, PAM 2016

Electronic Communication

How secure is SSL for SMTP, IMAP, XMPP, …

TLS in the wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication
R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, NDSS 2016

Dataset

Protocol	Port	Connections	Servers
SMTP†	25	3,870,542	8626
SMTPS	465	37,306	266
SUBMISSION†	587	7,849,434	373
IMAP†	143	25,900	239
IMAPS	993	4,620,043	1196
POP3†	110	18,774	110
POP3S	995	159,702	341
IRC†	6667	53	2
IRCS	6697	18,238	15
XMPP, C2S†	5222	13,517	229
XMPPS, C2S	5223	911,411	2163
XMPP, S2S†	5269	175	2
XMPPS, S2S	5270	0	0

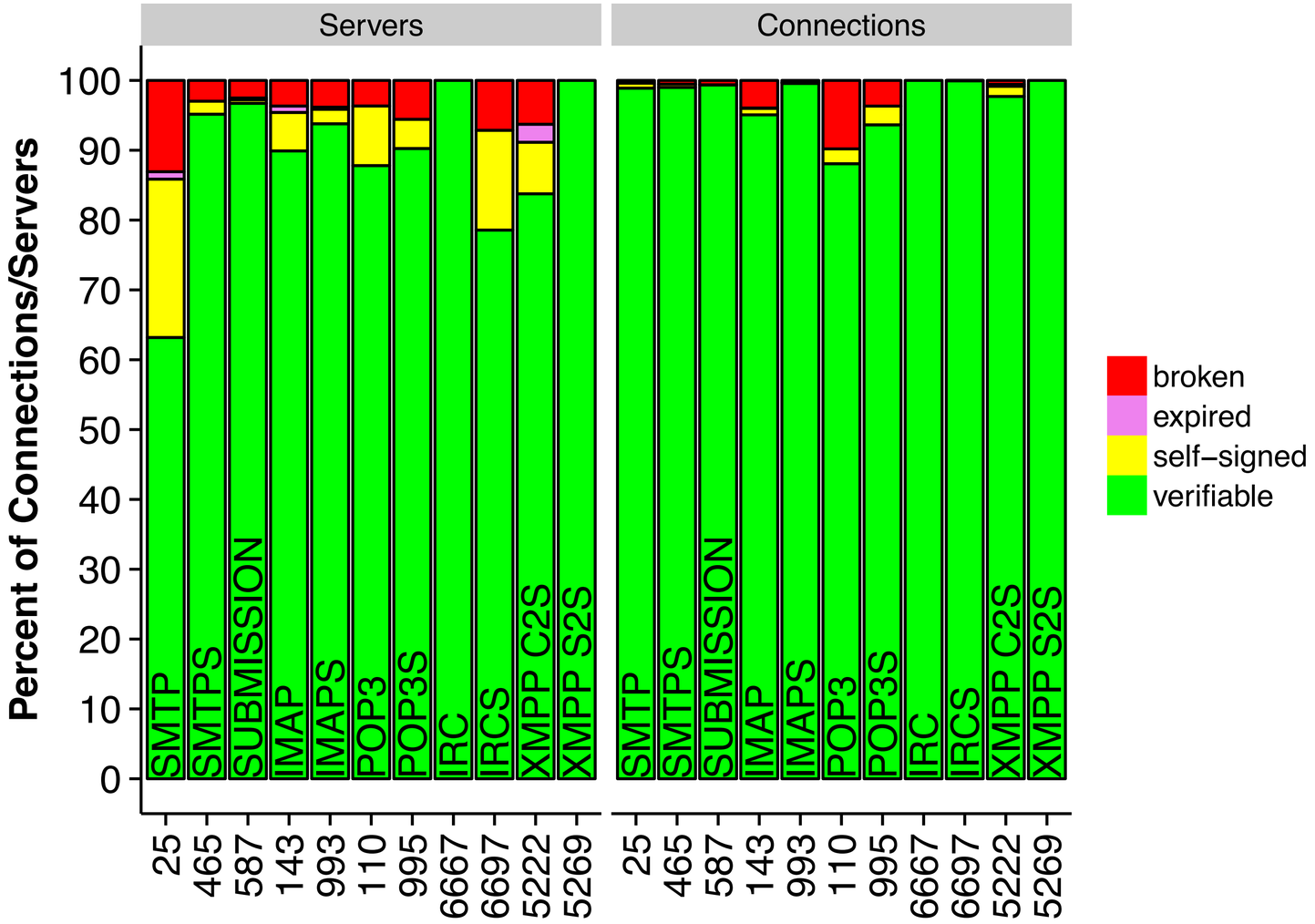
TLS in the wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication
R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, NDSS 2016

StartTLS - upgraded

	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%
IRC	0.14%	–	–	–
XMPP, C2S	2.44%	–	–	–
XMPP, S2S	0.39%	–	–	–

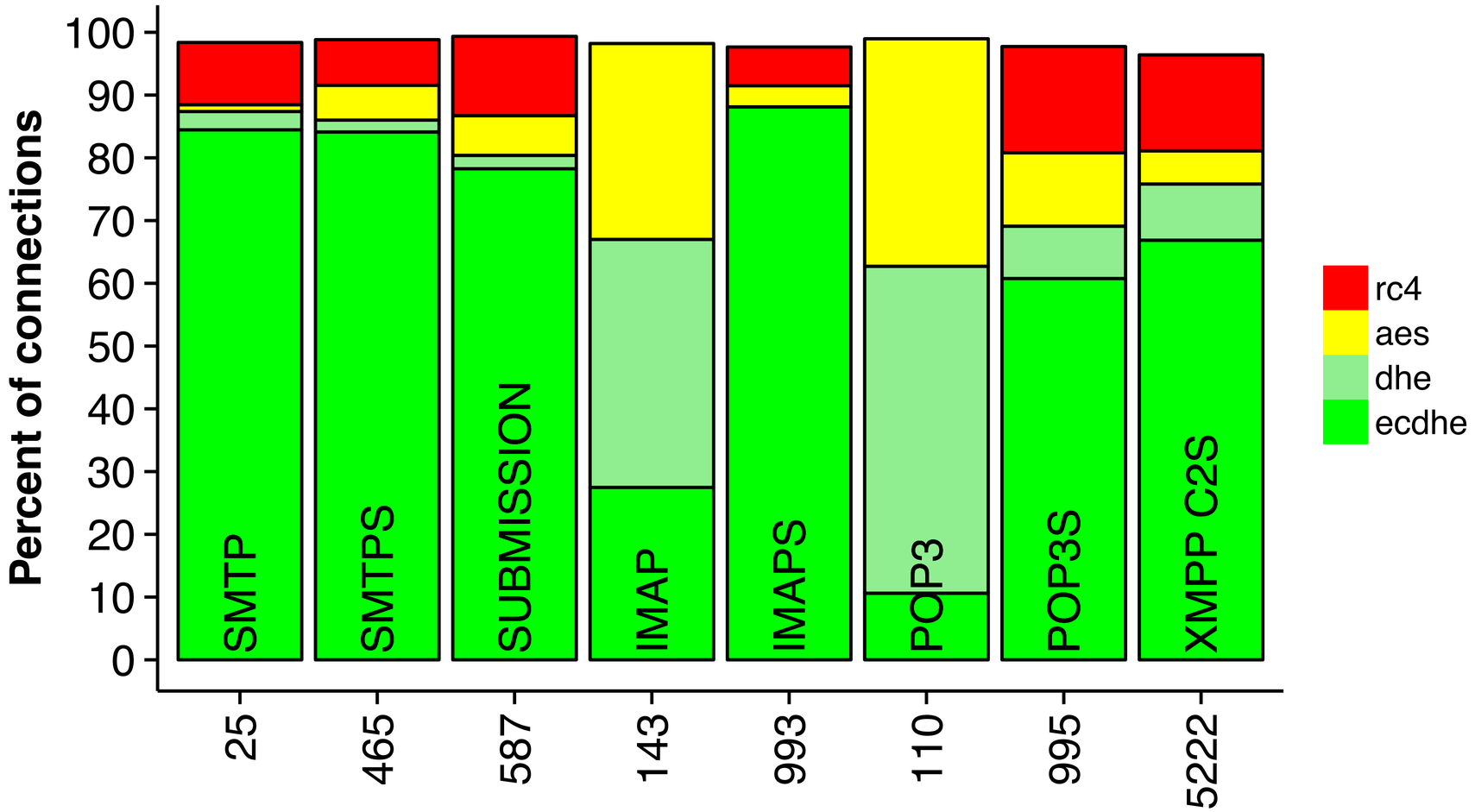
TLS in the wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication
R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, NDSS 2016

Valid certificates

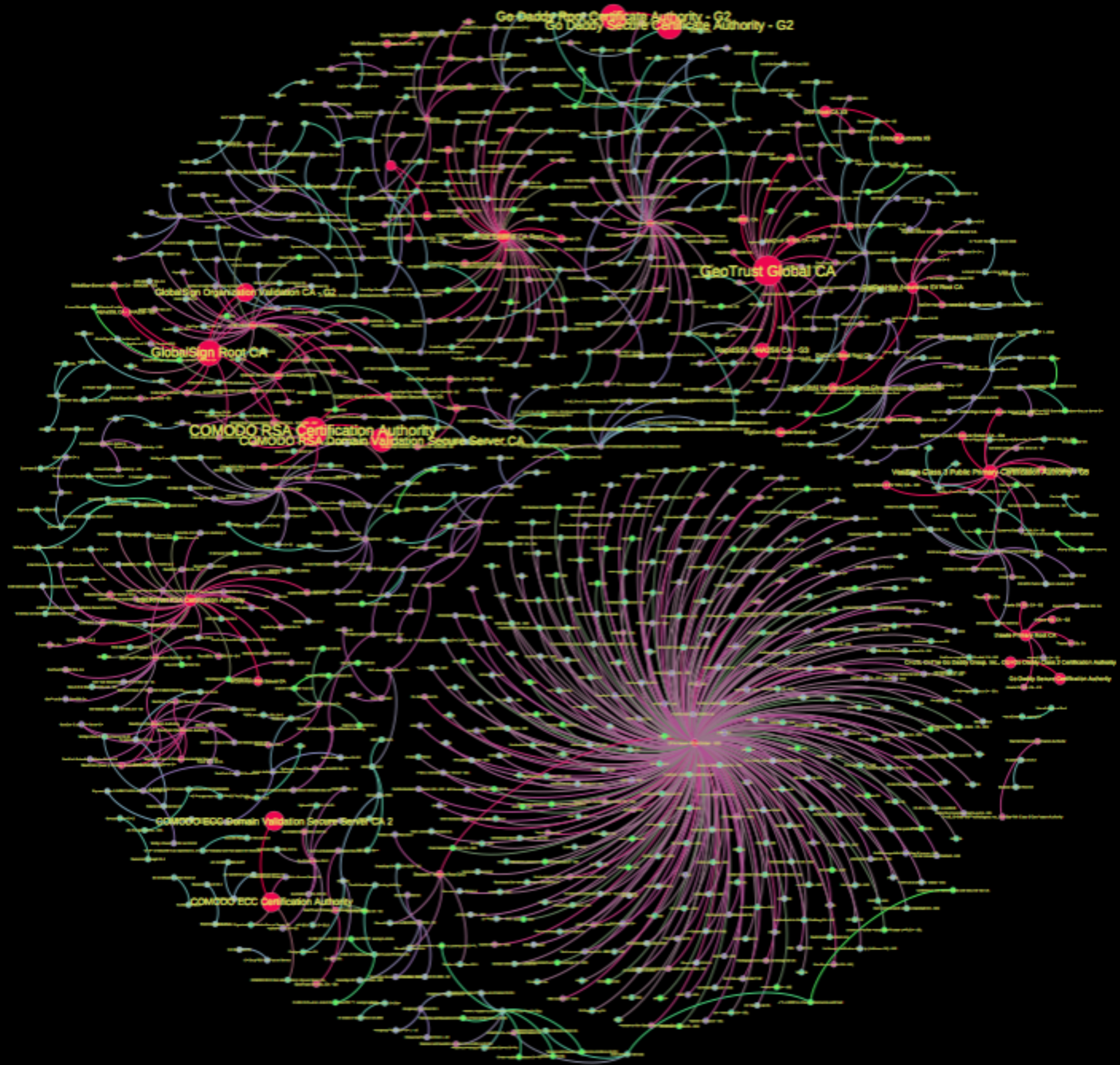


TLS in the wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication
R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, NDSS 2016

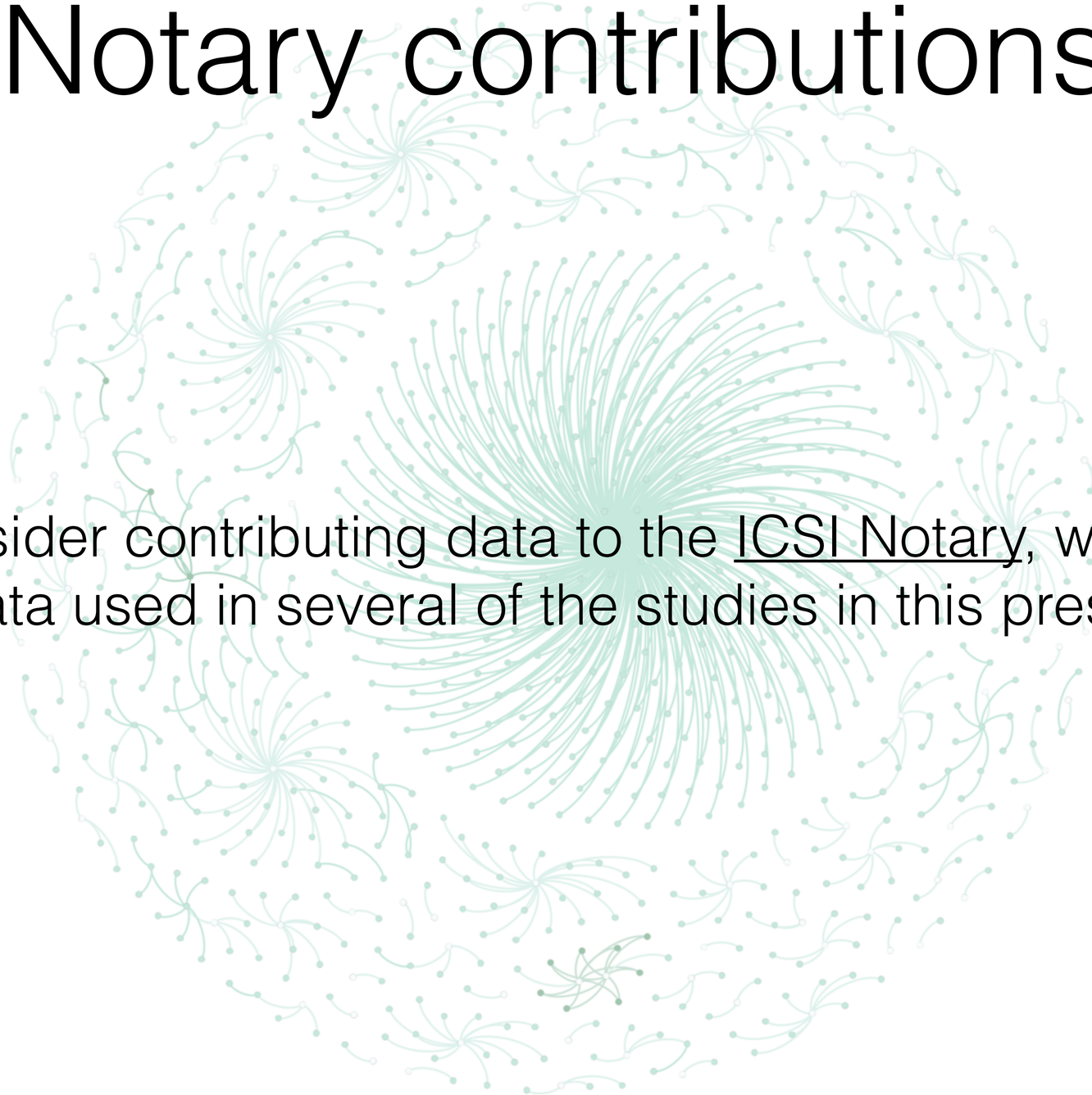
Used ciphers



TLS in the wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication
R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, NDSS 2016


Go Daddy Secure Certification Authority - G2
GeoTrust Global CA
GlobalSign Organization Validation CA - G2
GlobalSign Root CA
COMODO RSA Certification Authority
COMODO RSA Domain Validation Secure Server CA
COMODO ECC Domain Validation Secure Server CA 2
COMODO ECC Certification Authority

Notary contributions



Please consider contributing data to the ICSI Notary, which provided data used in several of the studies in this presentation.