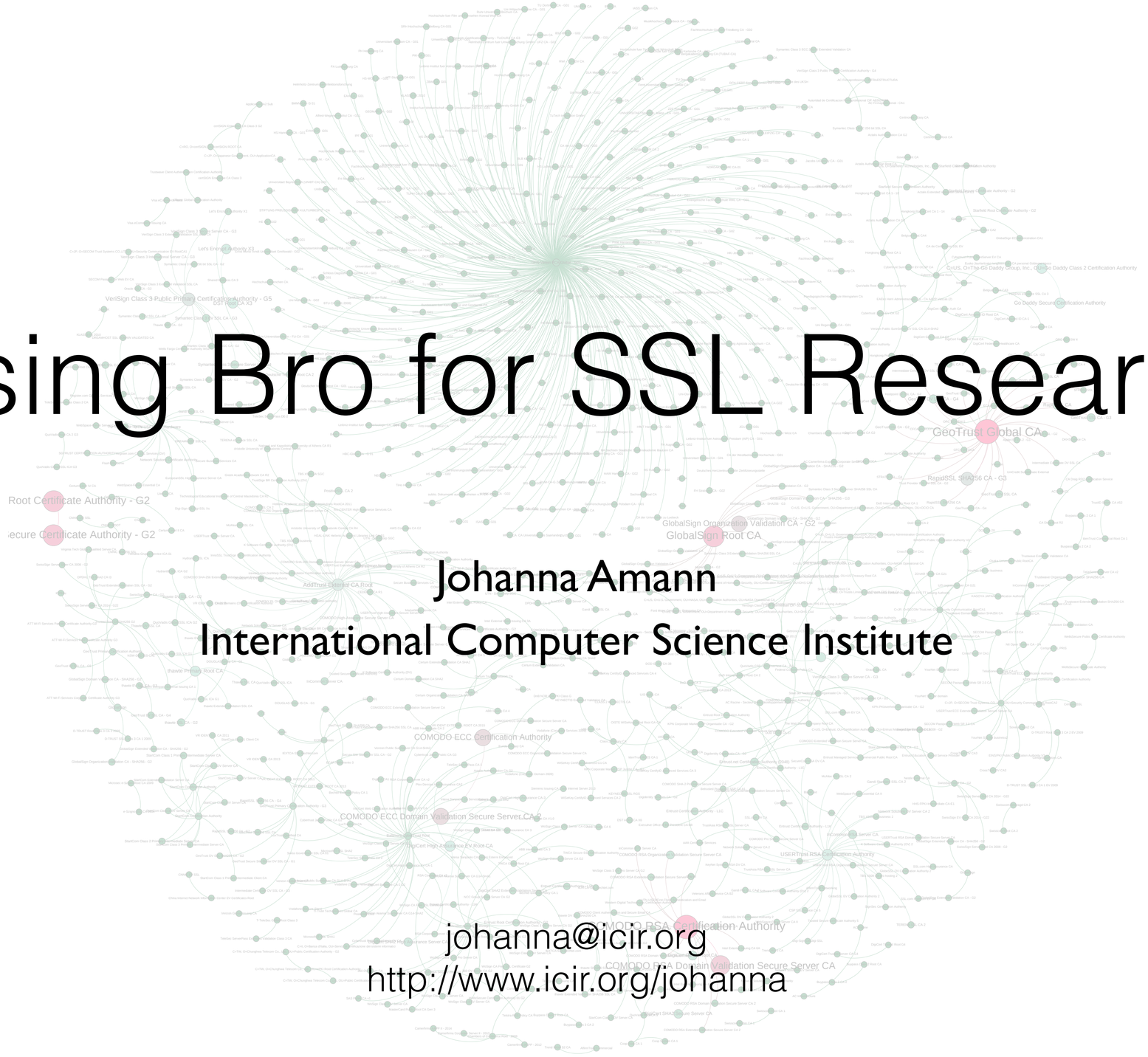
Using Bro for SSL Research



Johanna Amann

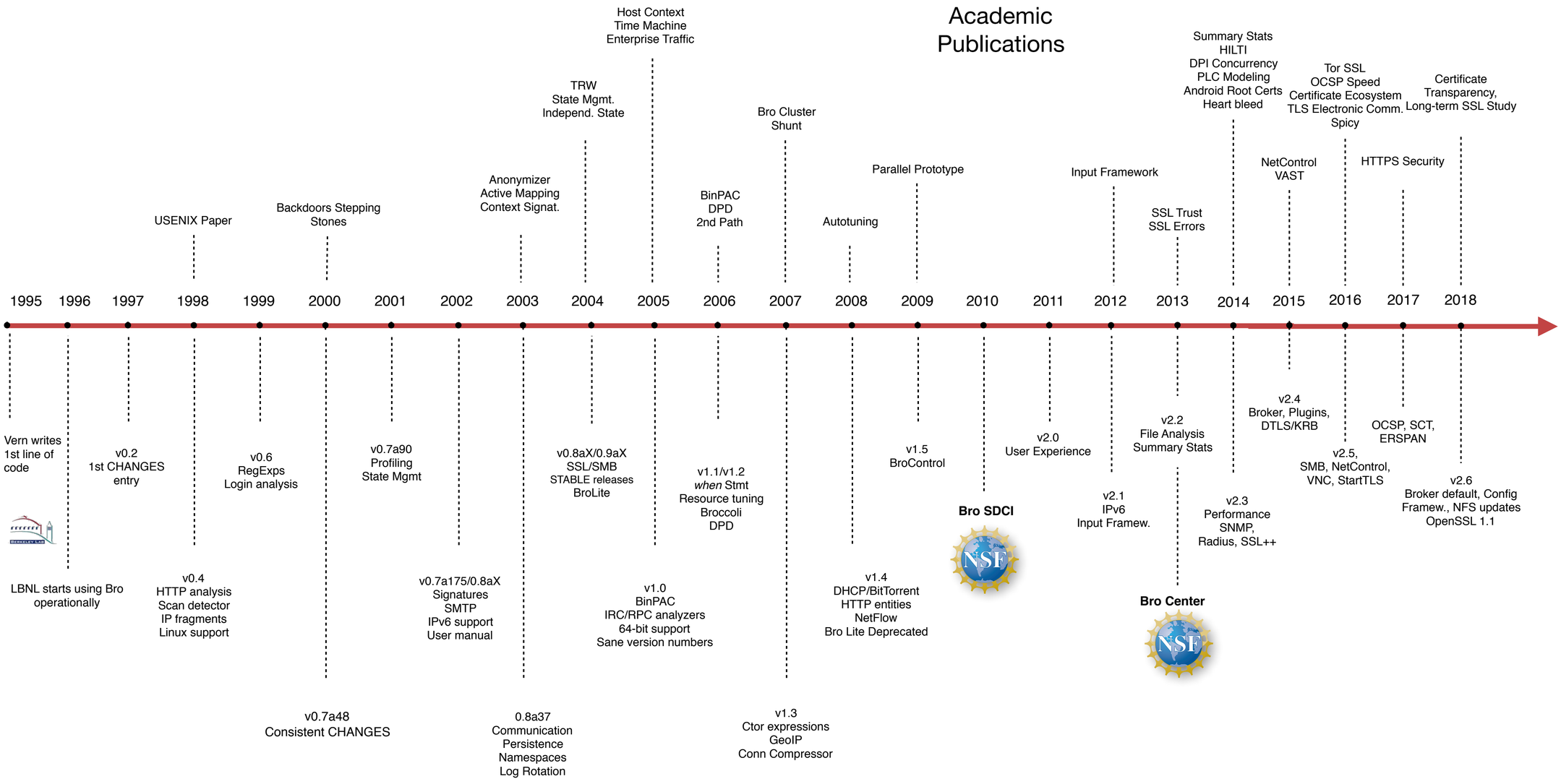
International Computer Science Institute

johanna@icir.org

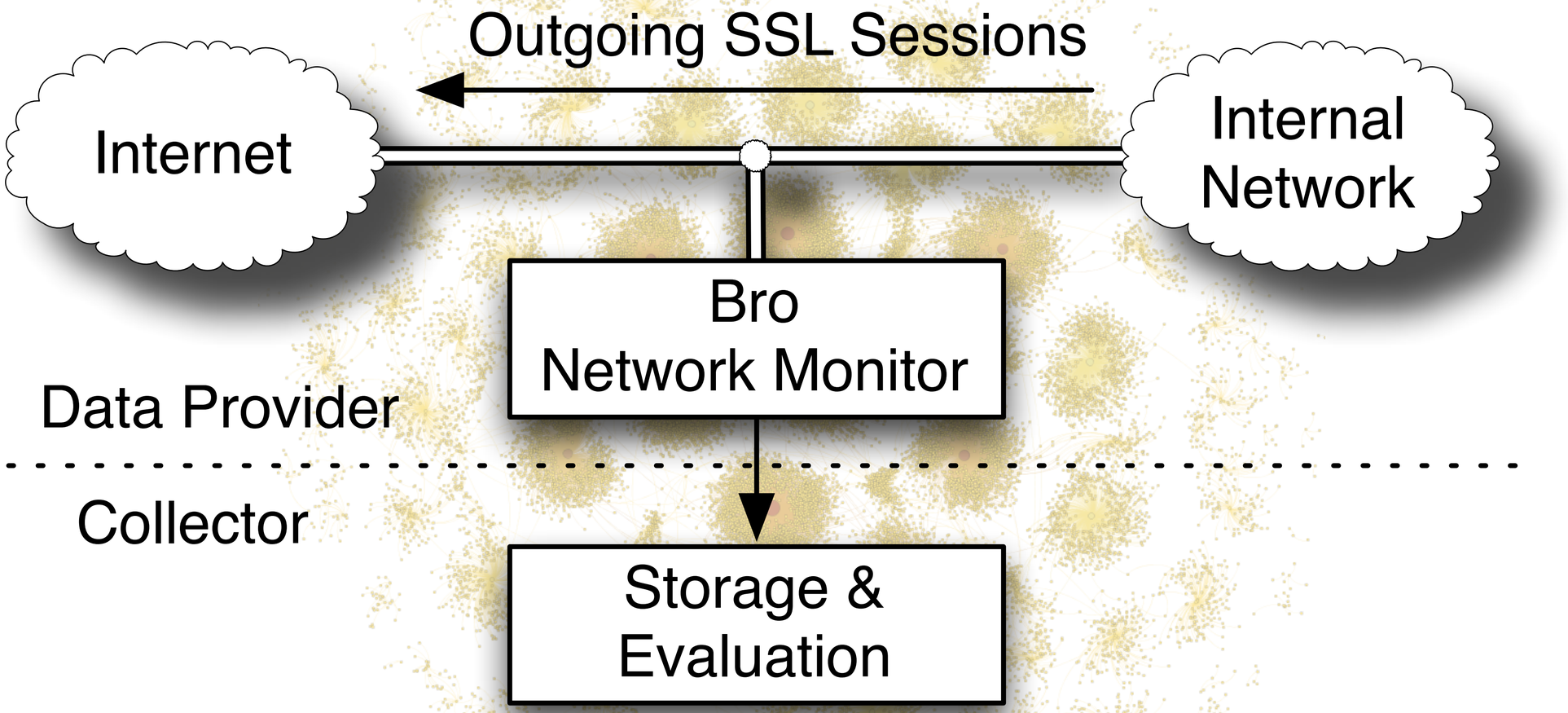
http://www.icir.org/johanna

ICSI
INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Bro History

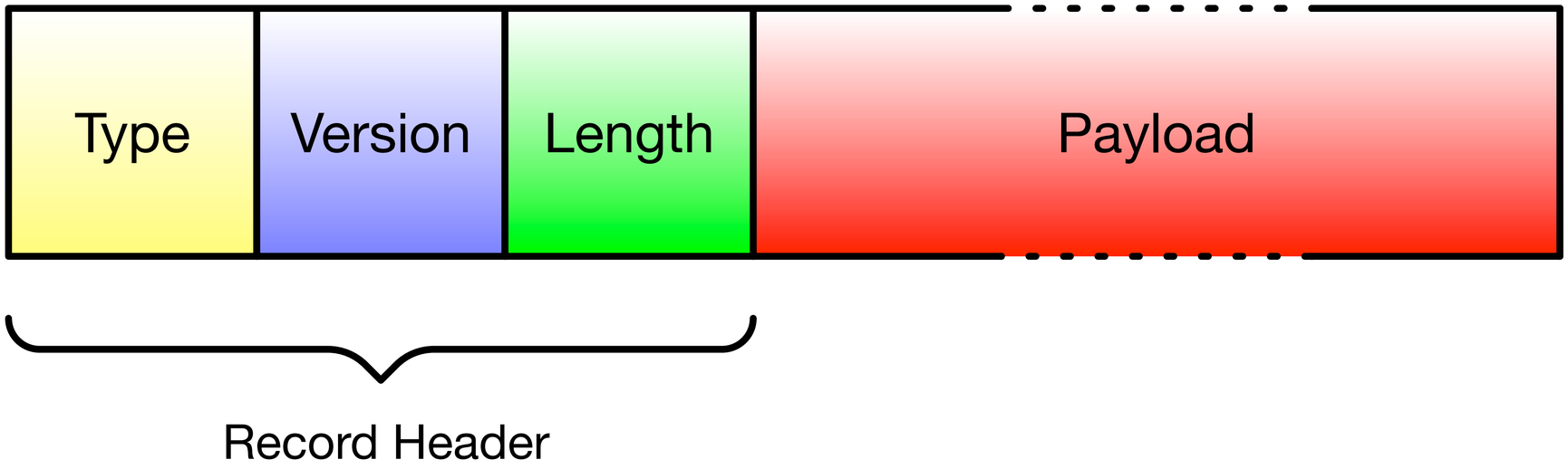

Academic Publications
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Vern writes 1st line of code
LBNL starts using Bro operationally
USENIX Paper
v0.2 1st CHANGES entry
v0.4 HTTP analysis Scan detector IP fragments Linux support
Backdoors Stepping Stones
v0.6 RegExps Login analysis
v0.7a48 Consistent CHANGES
v0.7a90 Profiling State Mgmt
Anonymizer Active Mapping Context Signat.
v0.7a175/0.8aX Signatures SMTP IPv6 support User manual
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
0.8a37 Communication Persistence Namespaces Log Rotation
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
HTTPS Security
OCSP, SCT, ERSPAN
Certificate Transparency, Long-term SSL Study
v2.6 Broker default, Config Framew., NFS updates OpenSSL 1.1

ICSI Notary


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

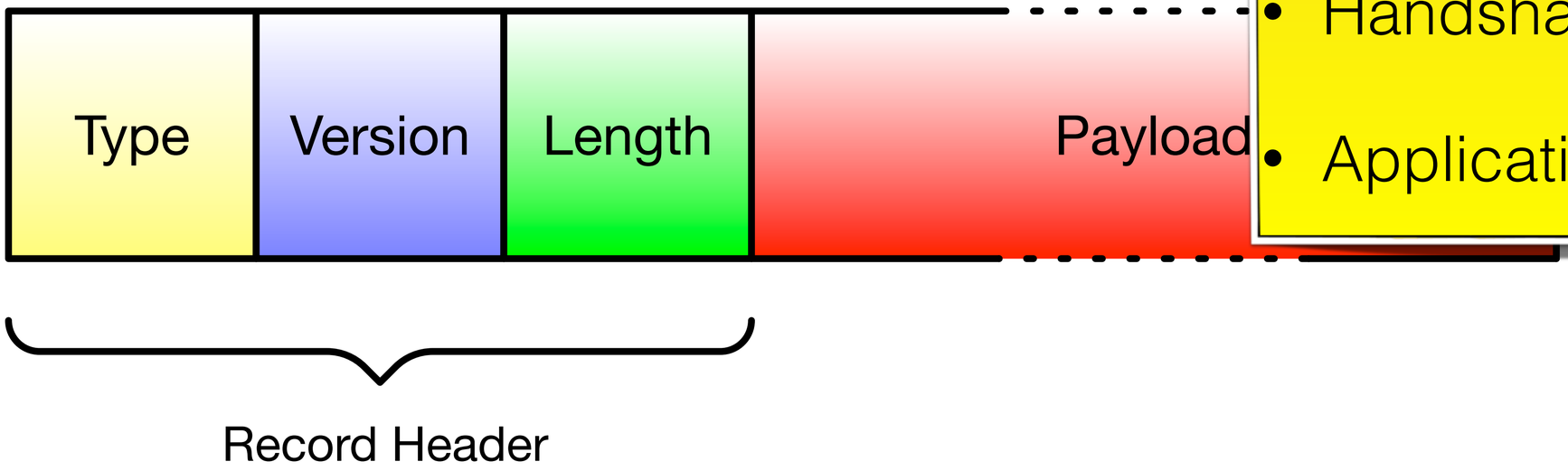
SSL/TLS Protocol

- 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)

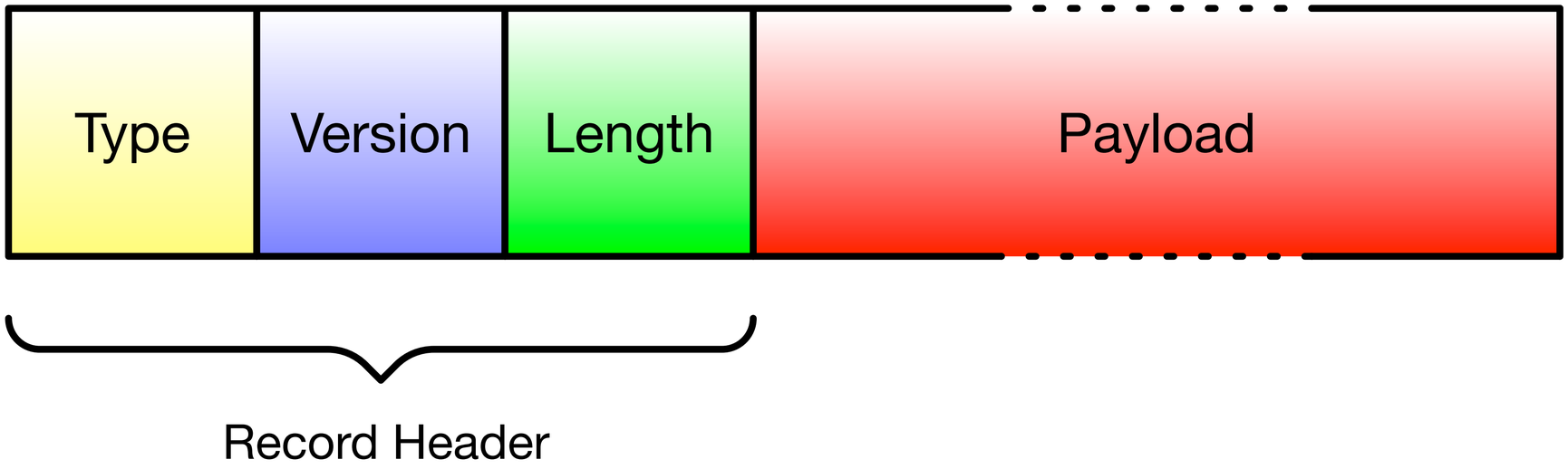


Common record types:

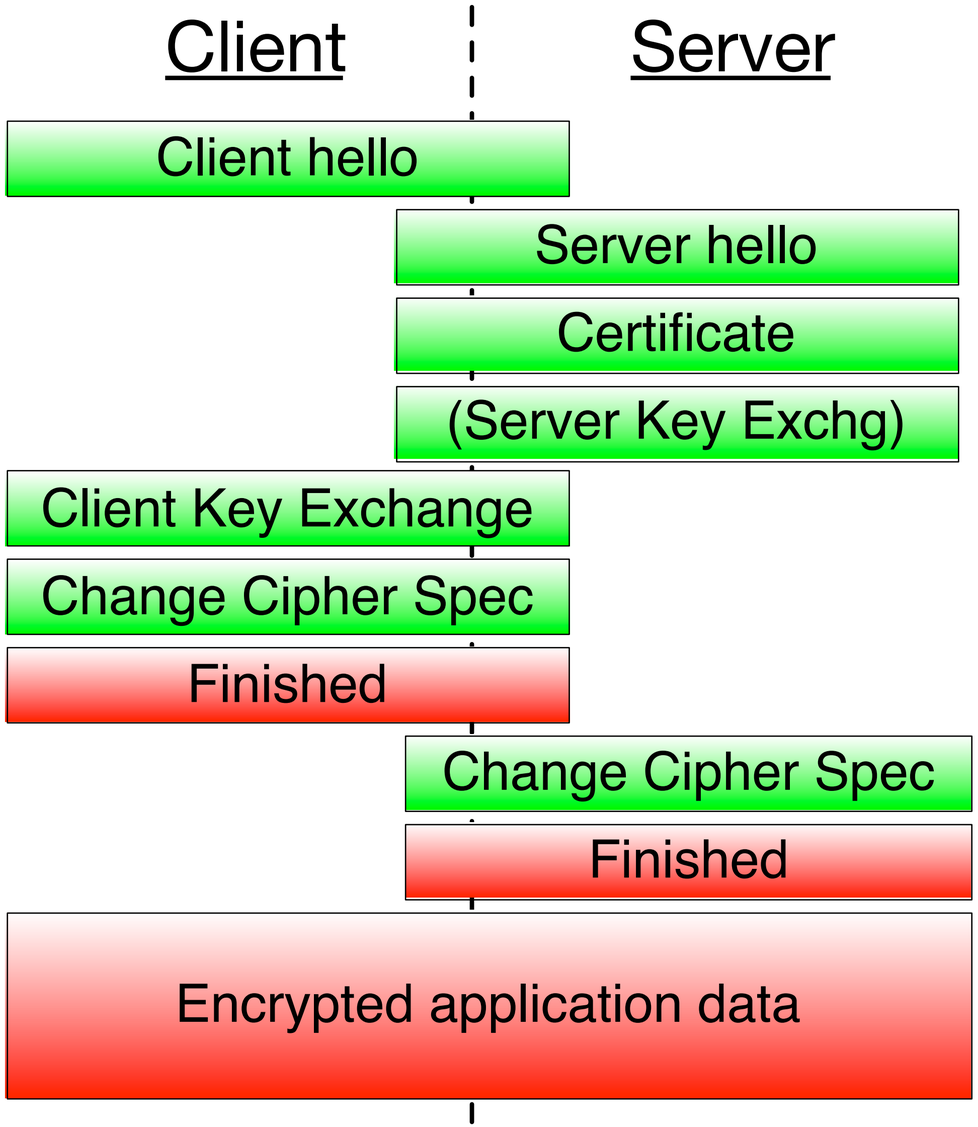
- Change Cipher Spec
- Alert
- Handshake
- Application Data

SSL/TLS Protocol

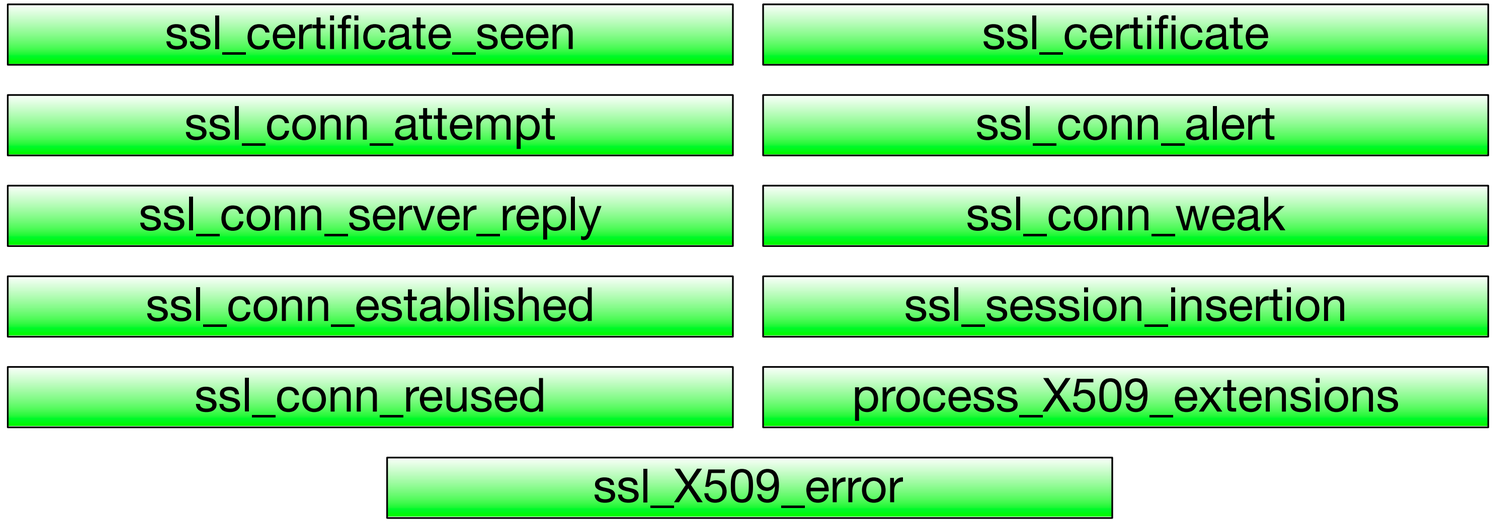
- Record based protocol
- Record header is never encrypted, only payload is (after the handshake is done)



SSL

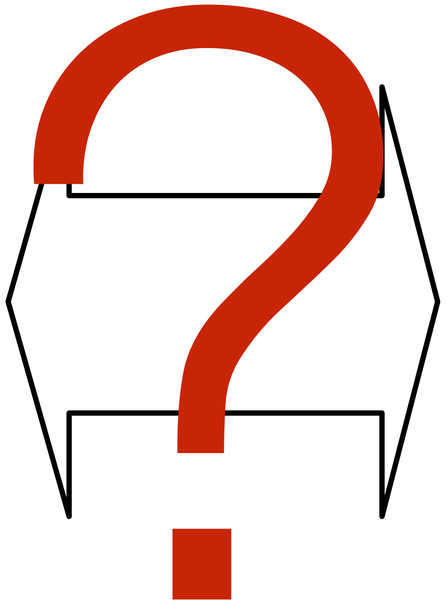

Client
Server
Client hello
Server hello
Certificate
(Server Key Exchg)
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished
Encrypted application data

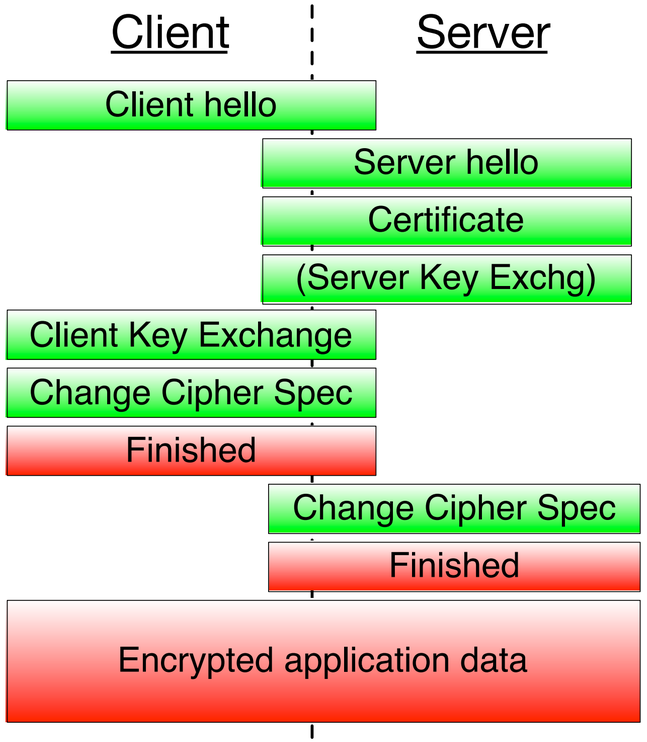
Bro SSL - v1.5.3


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

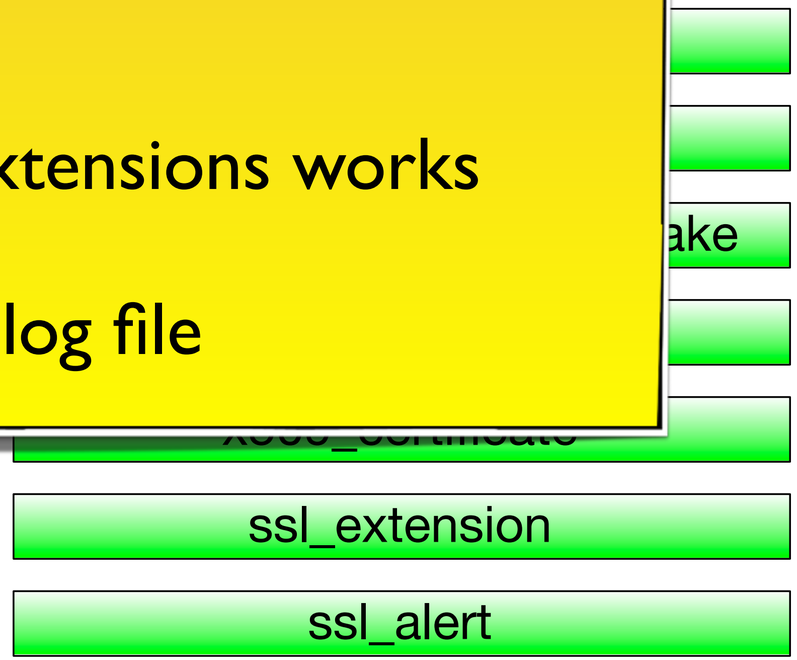
ssl_alert

Bro SSL - v2.1

Several bug fixes

Parsing TLS server extensions works

More information in log file



Bro SSL - v2.2

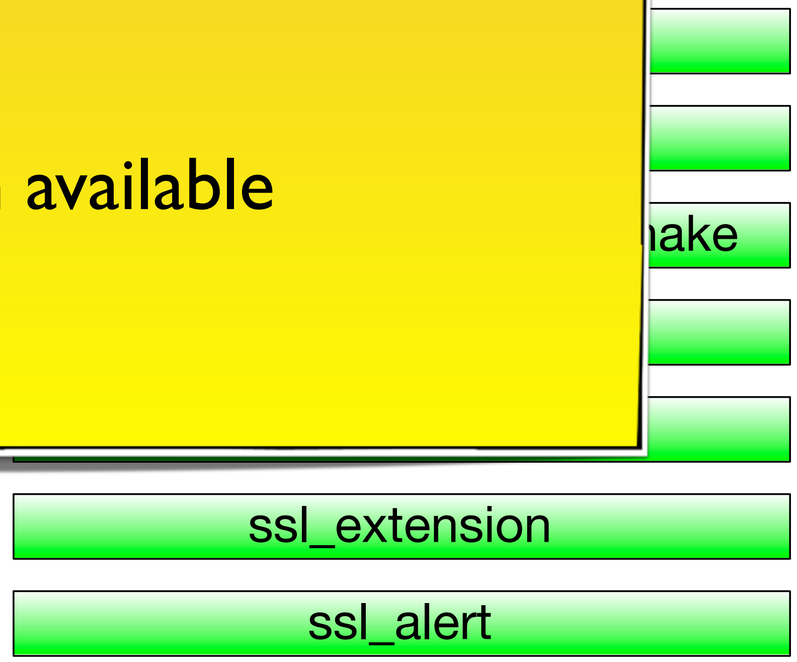

client_hello
server_hello
ssl_session_ticket_handshake
ssl_established
x509_certificate
ssl_extension
ssl_alert

Bro SSL - v2.2

Several bug fixes

Client/server random available

Support TLS 1.2



Bro SSL Events - v2.3

Bro SSL Events - 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

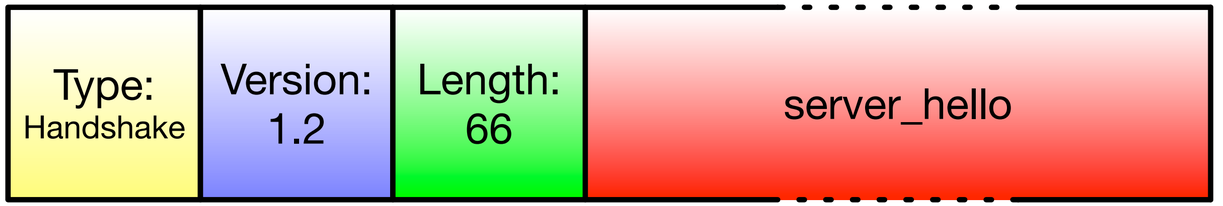
x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

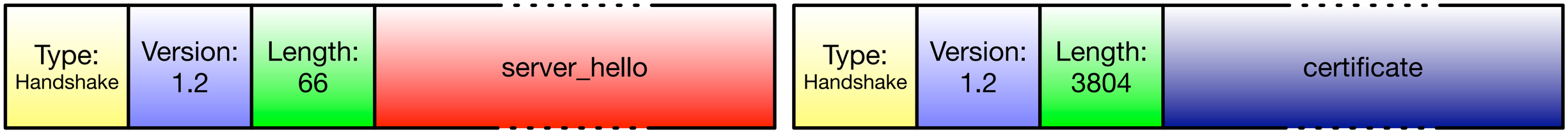
ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

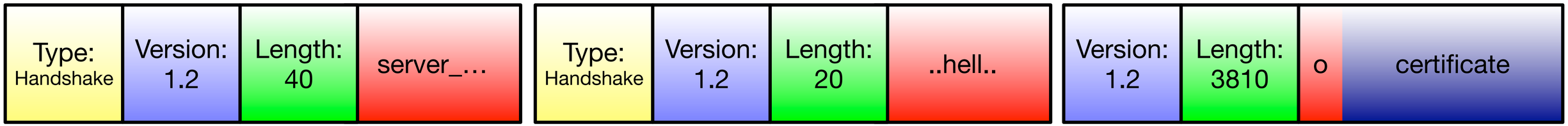
Fragmentation



Fragmentation



Fragmentation



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 - v2.5

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_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_change_cipher_spec

x509_extension

x509_ext_basic_constraints

x509_ext_subject_alternative_name

ssl_extension_elliptic_curves

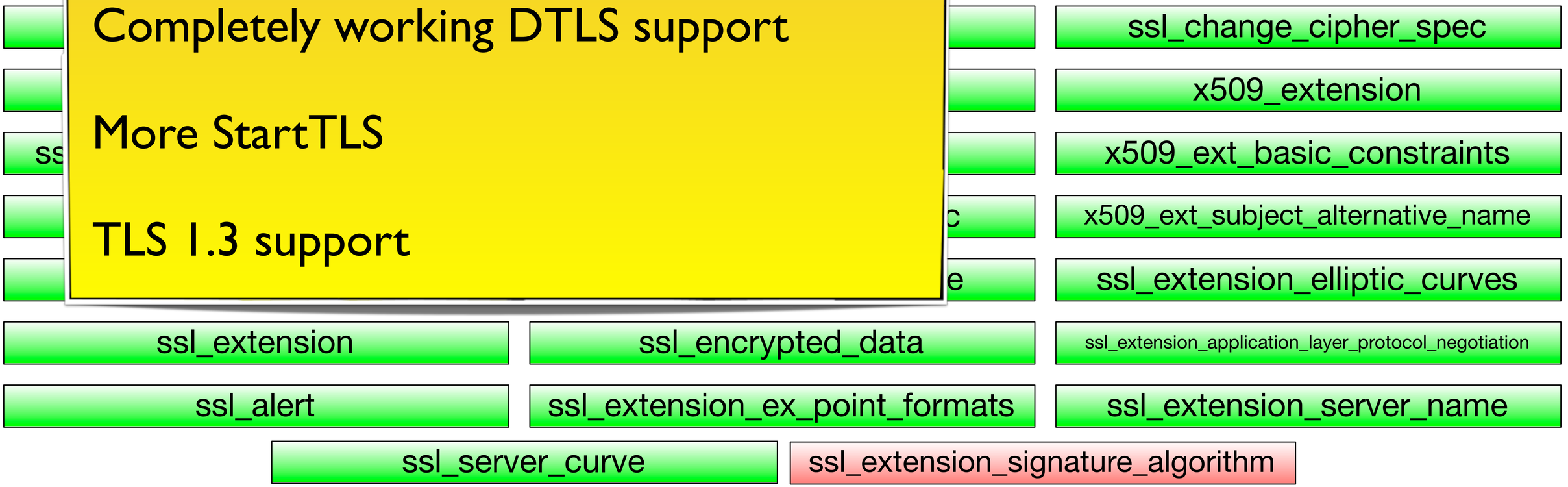
ssl_extension_application_layer_protocol_negotiation

ssl_extension_server_name

ssl_server_curve

ssl_extension_signature_algorithm

Bro SSL Events - v2.5



Bro SSL Events - v2.6

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 - v2.6

client_hello	ssl_stapled_ocsp	ssl_change_cipher_spec
server_hello	ssl_encrypted_data	x509_extension
ssl_session_ticket_handshake	ssl_dh_server_params	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	x509_ocsp_ext_signed_certificate_timestamp
ssl_extension_supported_versions	ssl_extension_psk_key_exchange_modes	ssl_extension_signed_certificate_timestamp
ocsp_request	ocsp_request_certificate	ocsp_response_status
ocsp_response_bytes	ocsp_response_certificate	ocsp_extension

Bro SSL Events - v2.6

client_hello

server_hello

ssl_server_curve

ssl_extension_supported_versions

ocsp_request

ocsp_response_bytes

ssl_stapled_ocsp

ssl_encrypted_data

ssl_extension_signature_algorithm

ssl_extension_psk_key_exchange_modes

ocsp_request_certificate

ocsp_response_certificate

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

x509_ocsp_ext_signed_certificate_timestamp

ssl_extension_signed_certificate_timestamp

ocsp_response_status

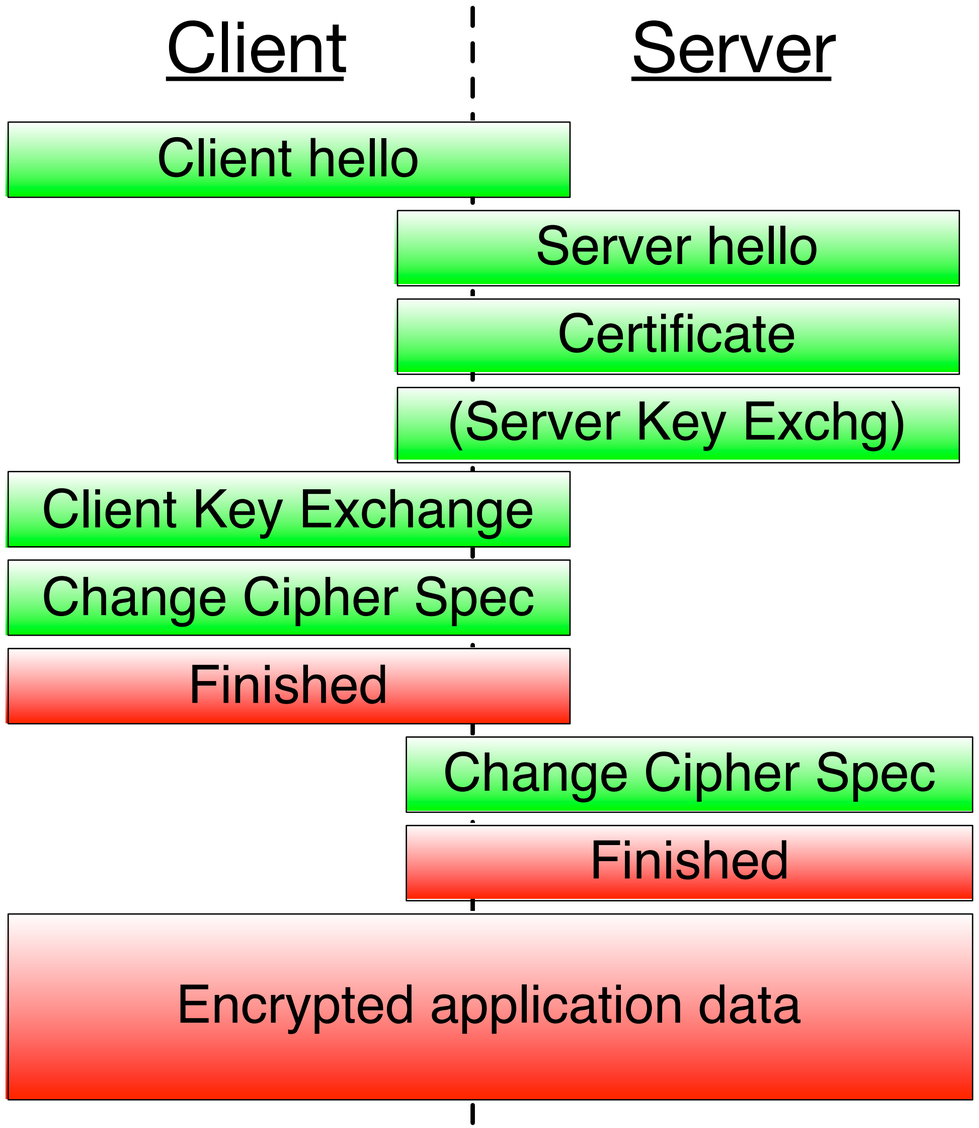
ocsp_extension

OCSP support

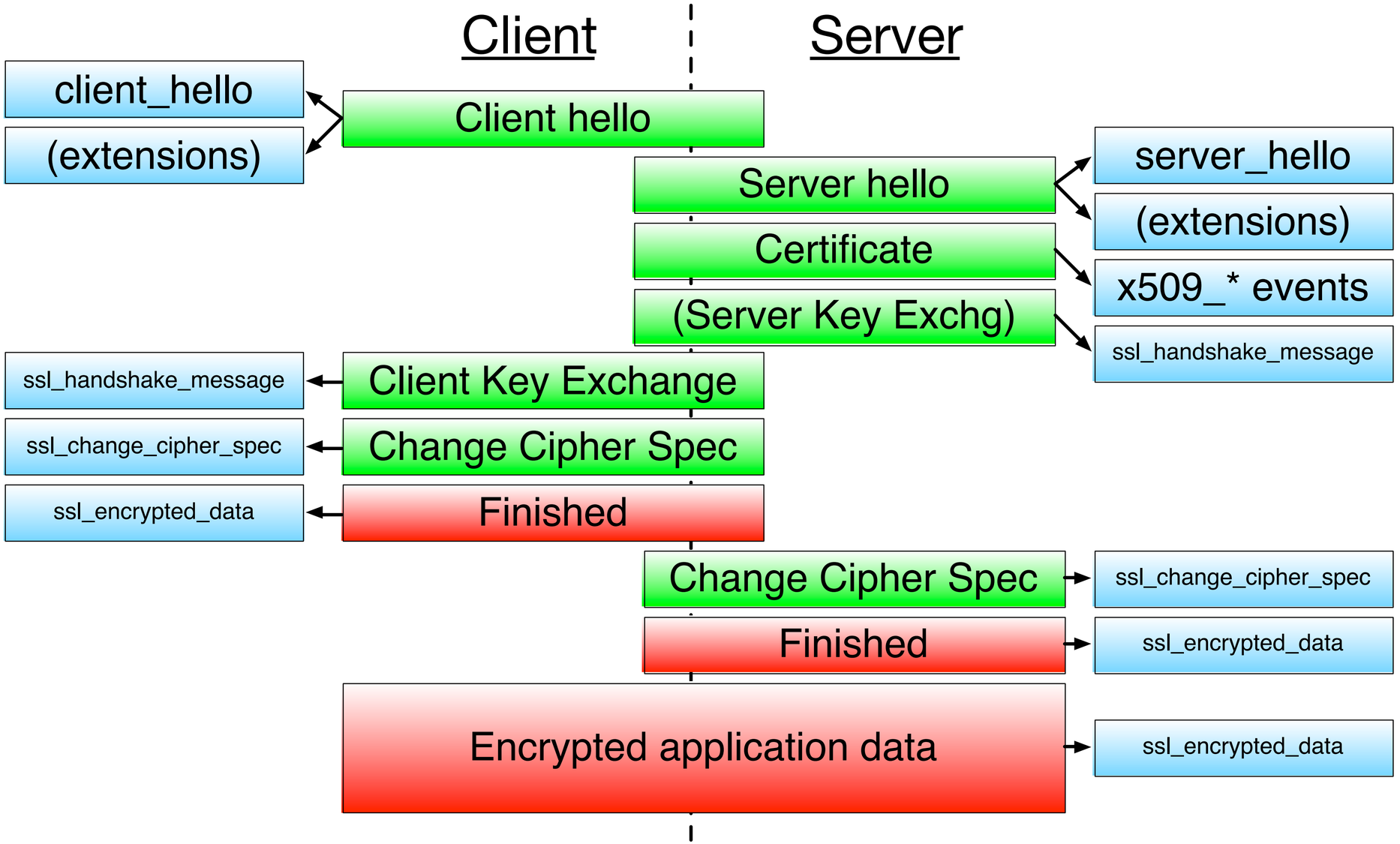
SCT Support (Certificate Transparency)

TLS 1.3 extensions

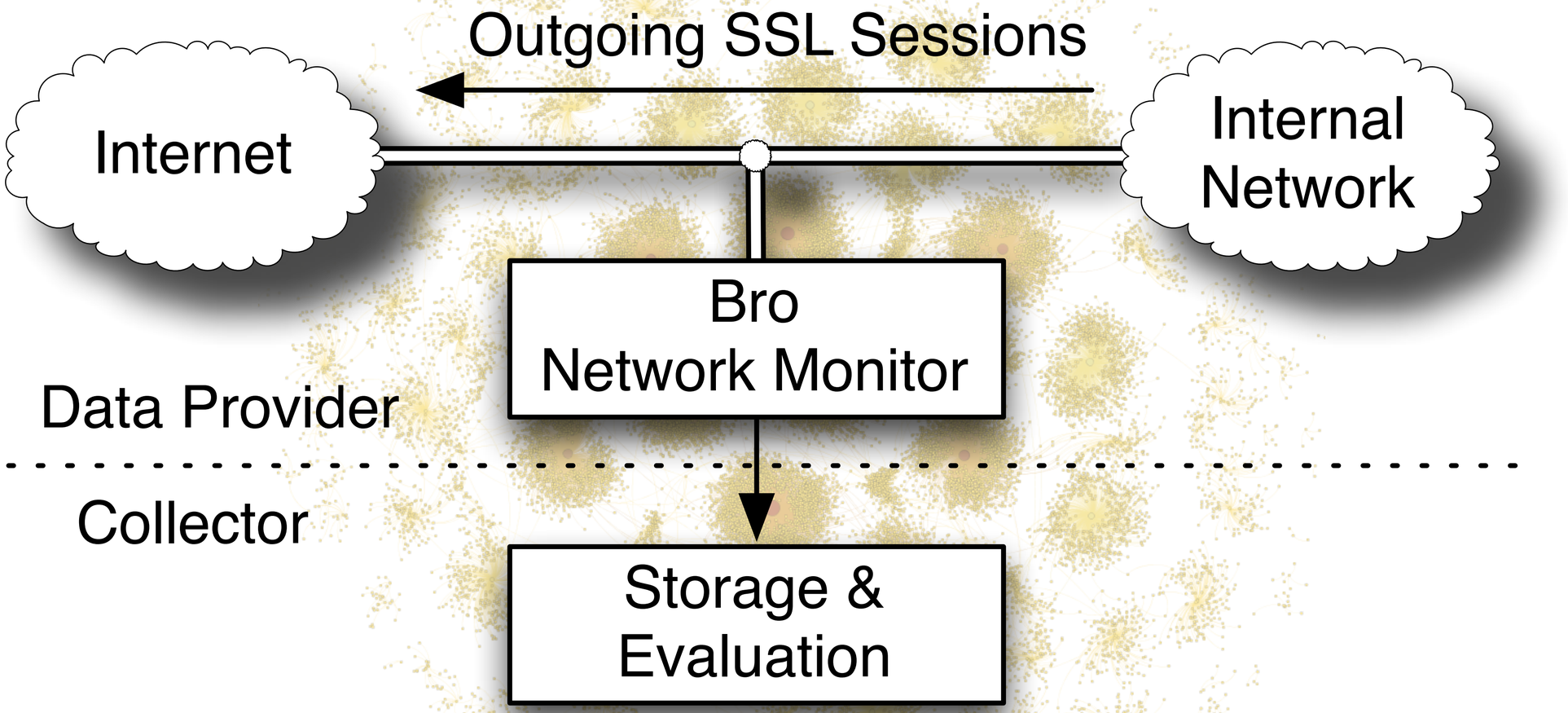
SSL


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

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)

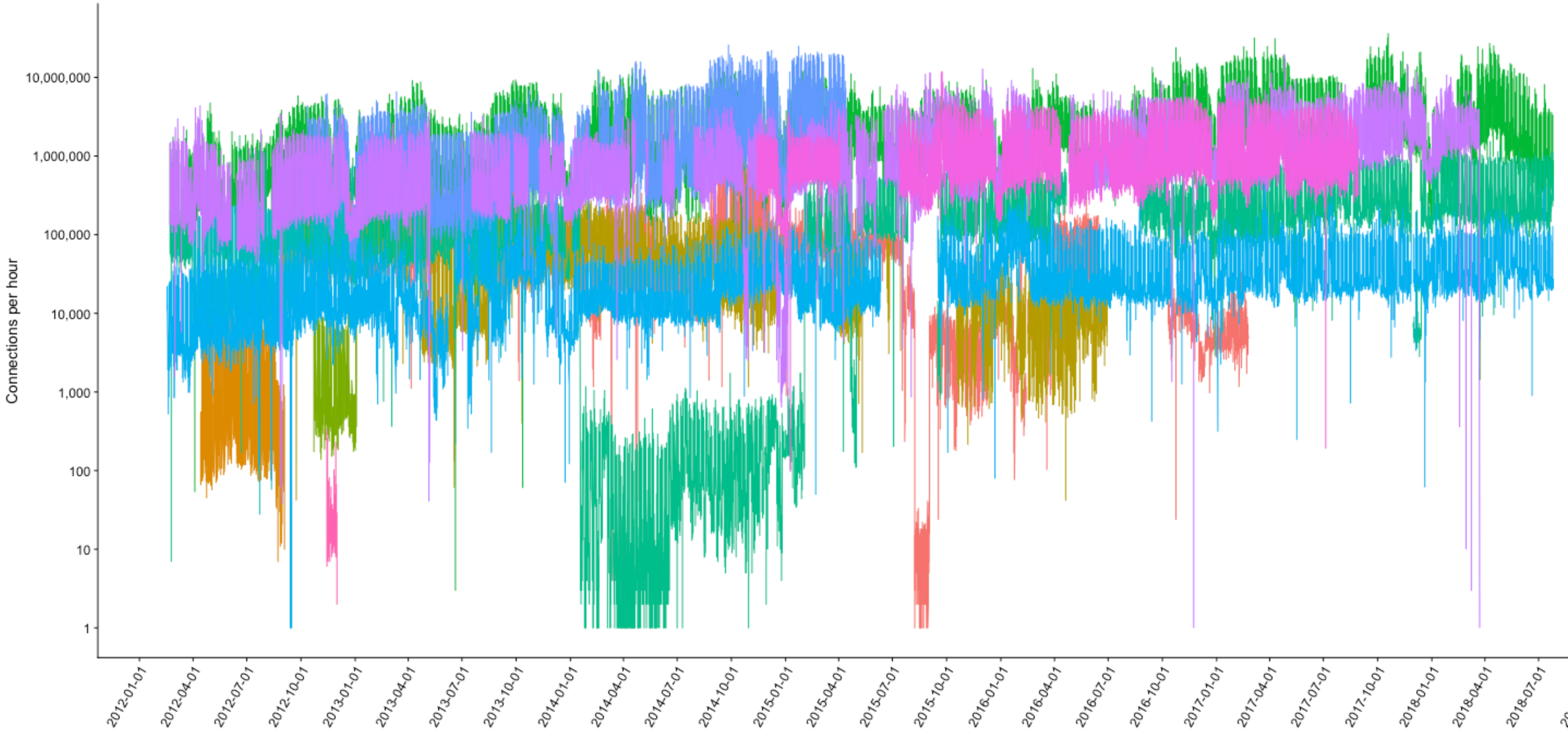
Ticket lifetime hint

Client EC curve

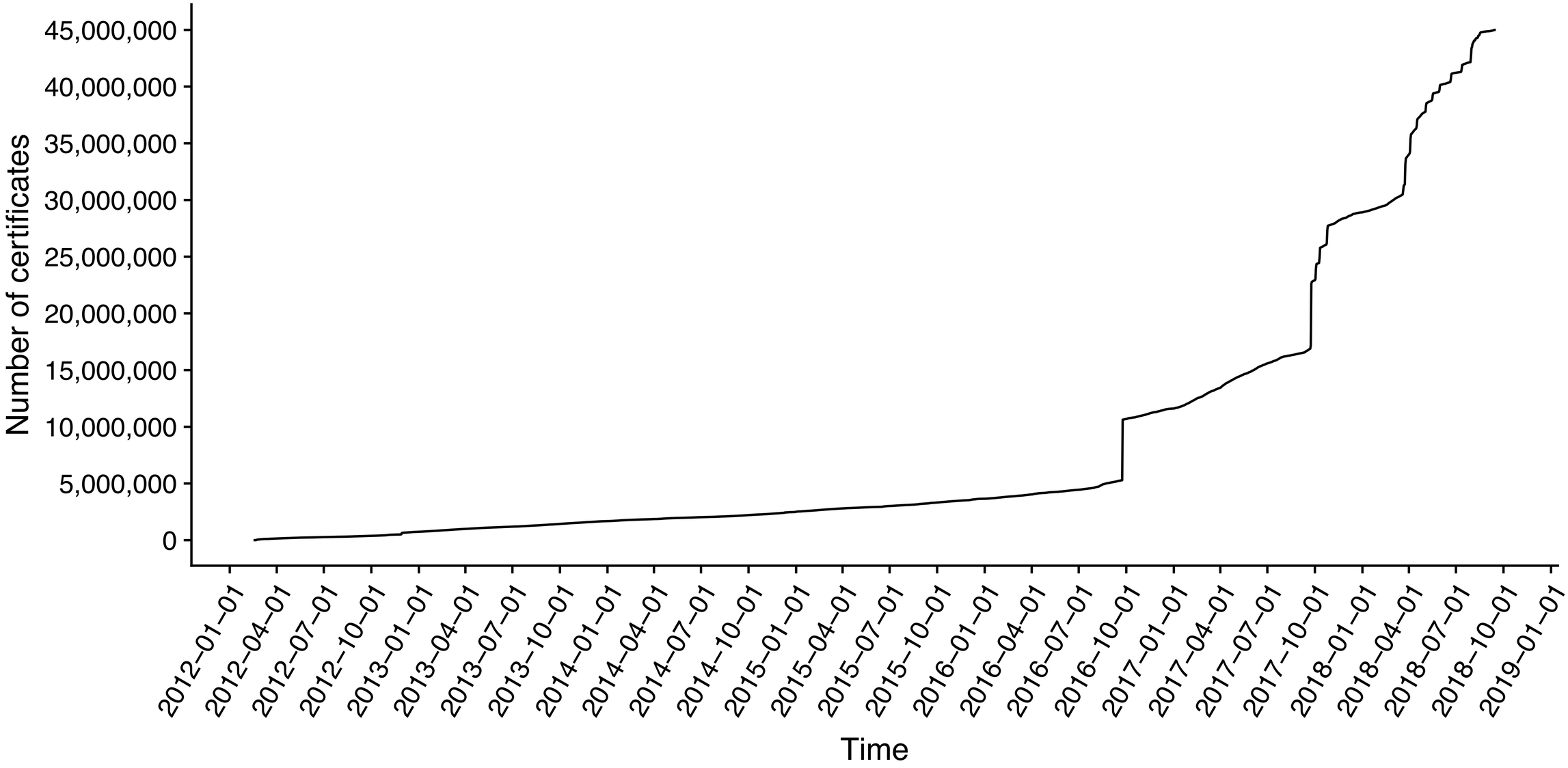
Number Client Certs

TLS Alerts

Notary - Connections



Notary - Certificates



Coming of Age: A Longitudinal Study of TLS Deployment

P. Kotzias, A. Razaghpanah, J. Amann, K. Paterson, N. Vallina-Rodriguez, J. Caballero, *IMC 2018*

The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem

Q. Scheitle, O. Gasser, T. Nolte, J. Amann, L. Brent, G. Carle, R. Holz, T. Schmidt, M. Wählisch, *IMC 2018*

Mission Accomplished? HTTPS Security after DigiNotar

J. Amann, O. Gasser, Q. Scheitle, L. Brent, G. Carle, R. Holz, *IMC 2017*

Coming of Age

Longitudinal Study of TLS Deployment

Coming of Age: A Longitudinal Study of TLS Deployment
P. Kotzias, A. Razaghpanah, J. Amann, K. Paterson, N. Vallina-Rodriguez, J. Caballero, IMC 2018

Major SSL attacks in the last years

BEAST

MITM attack against CBC cipher suites in TLS 1.0 and earlier. The attack exploits the reliance on predictable IVs. Mitigated in TLS 1.1 and client-side; use of RC4 encouraged.

2011

2012

Lucky 13

Cryptographic timing attack against TLS implementations using CBC mode. All CBC ciphers are potentially vulnerable; best counter-measure is to switch to AEAD and TLS 1.2 which was ill-supported at the time.

RC4 attacks

Attacks exploit biases in the output of the RC4 stream cipher to recover plain-texts that are sent repeatedly, e.g. cookies or passwords.

2013

Heartbleed

Heartbleed is an OpenSSL bug allowing attackers to obtain sensistive information from process memory via packets that trigger a buffer over-read.

Poodle

Poodle is a cryptographic exploits taking advantage of the willingness of clients to fall back to SSLv3 and the CBC mode padding in SSLv3.

2014

Freak

Freak allows a MITM attacker to downgrade TLS connections to export-grade cryptography. It is possible when a server supports RSA_EXPORT and the client requests an RSA cipher suite.

2015

Logjam

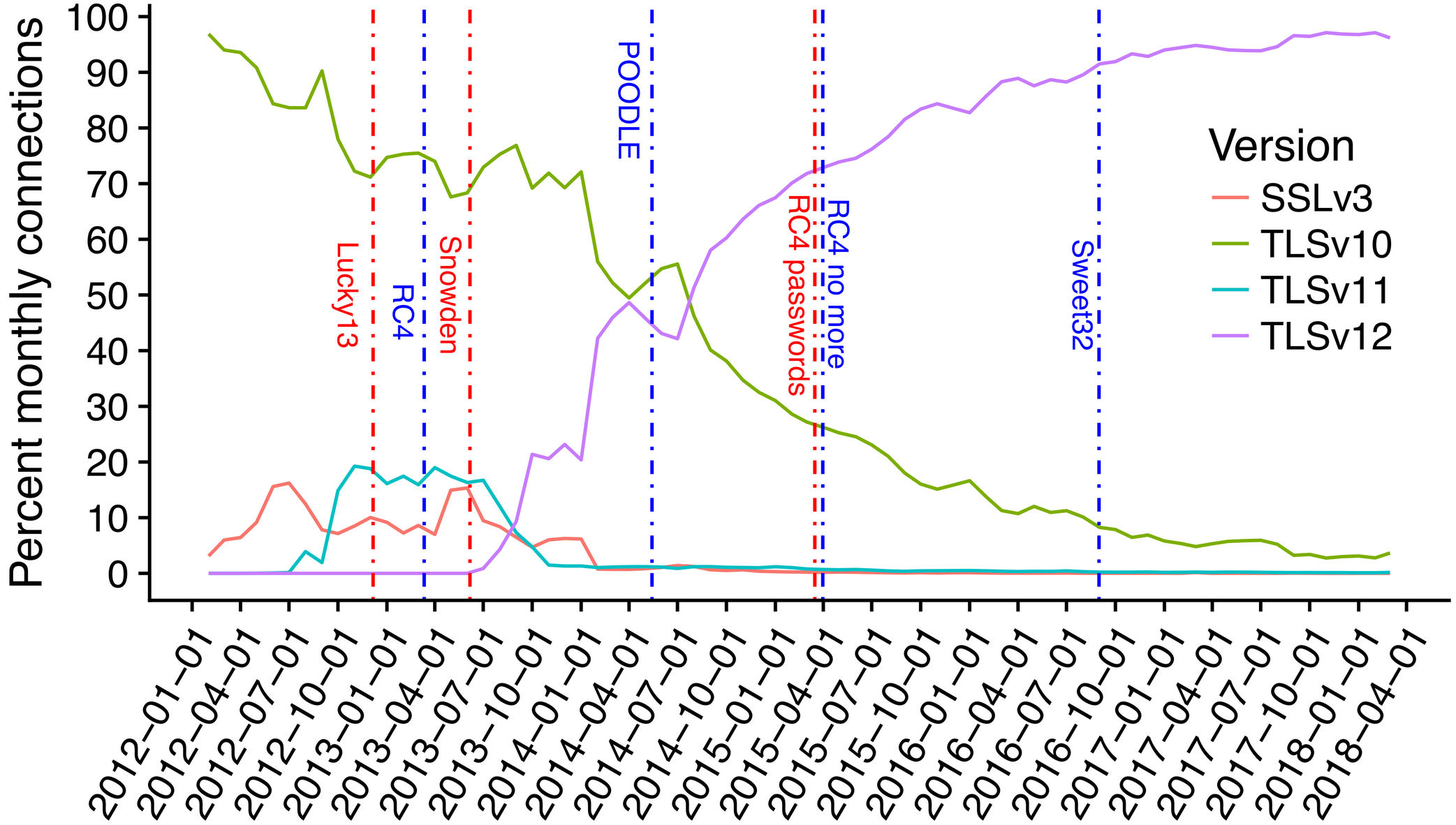
Allows an MITM attacker to attack connections if the server supports DHE_EXPORT and the client requests a DHE cipher suite.

2016

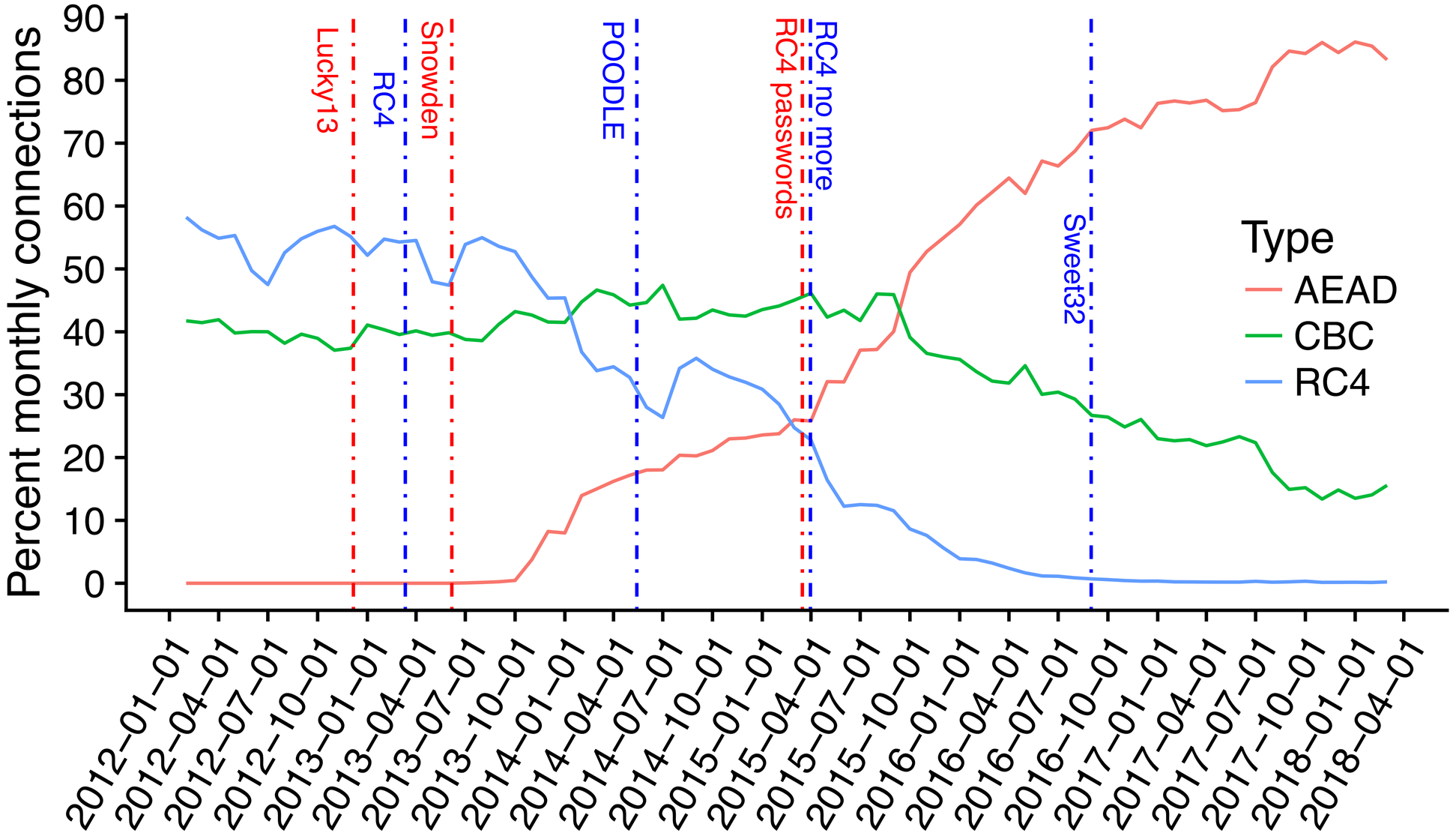
Sweet 32

DES and 3DES are vulnerable to a birthday-bound attack on CBC mode, which makes it possible for a MITM attacker to recover plaintext from long-duration connections.

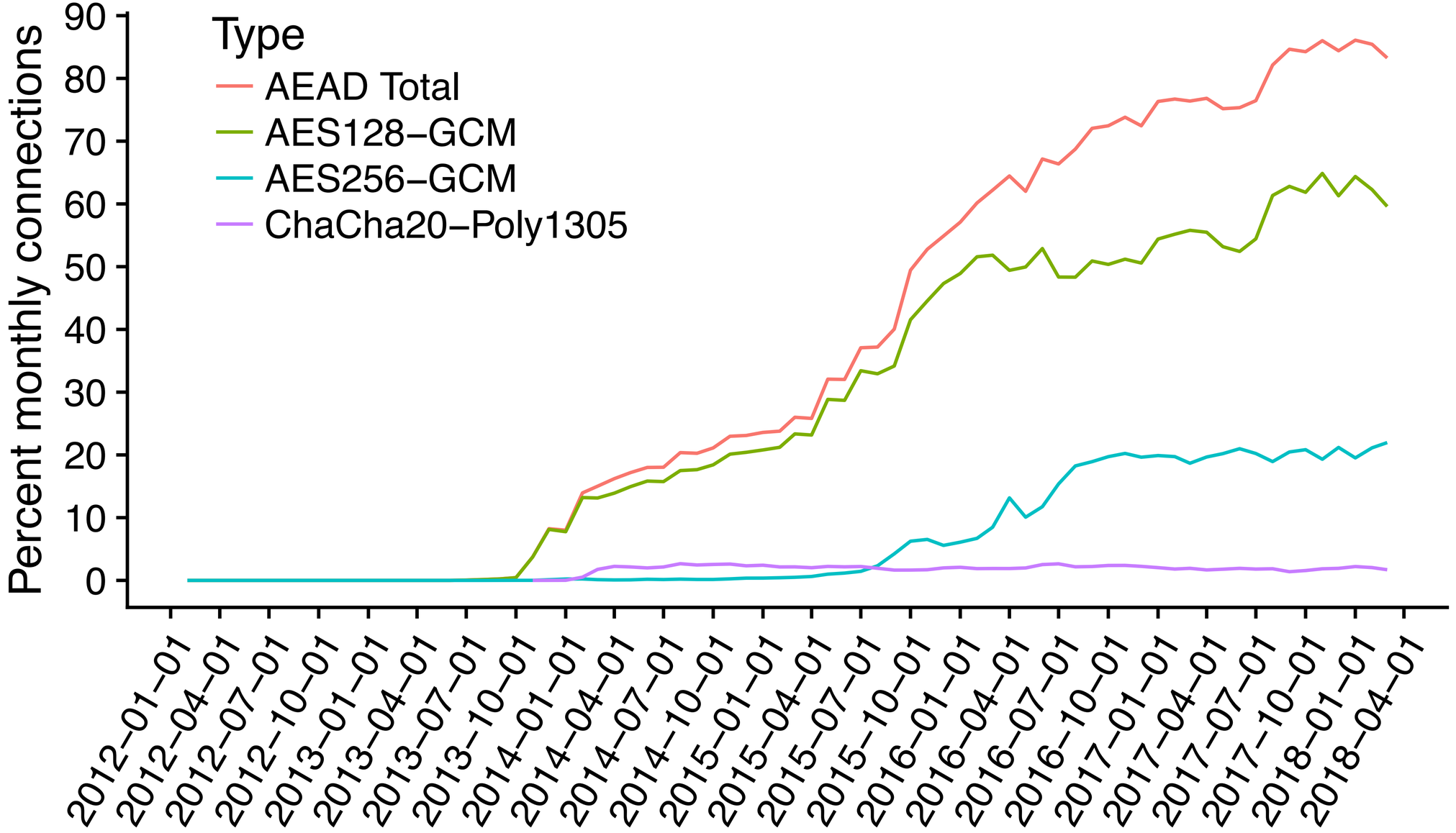
SSL Versions (negotiated)



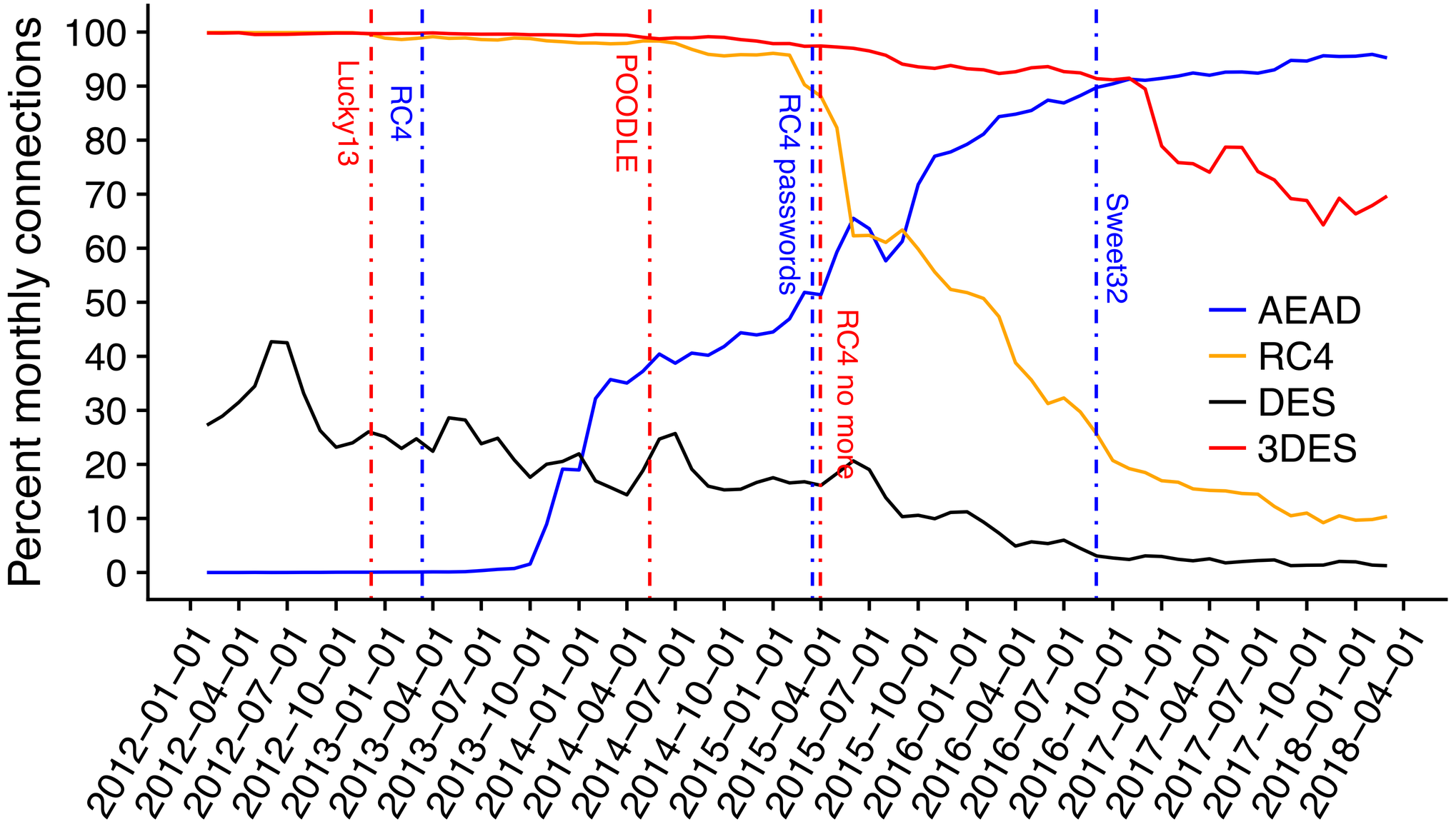
RC4, CBC or AEAD (negotiated)



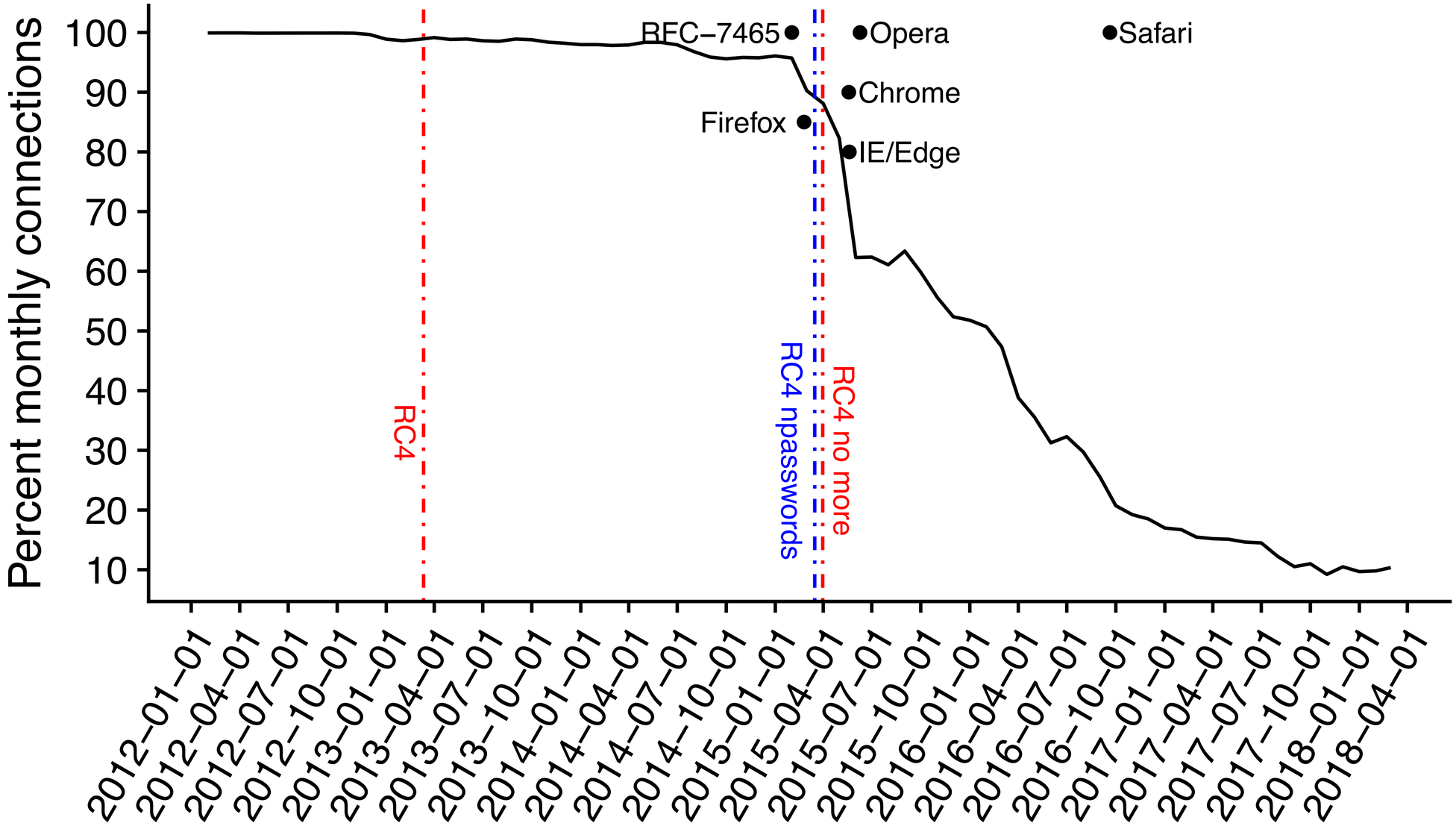
AEAD connection types



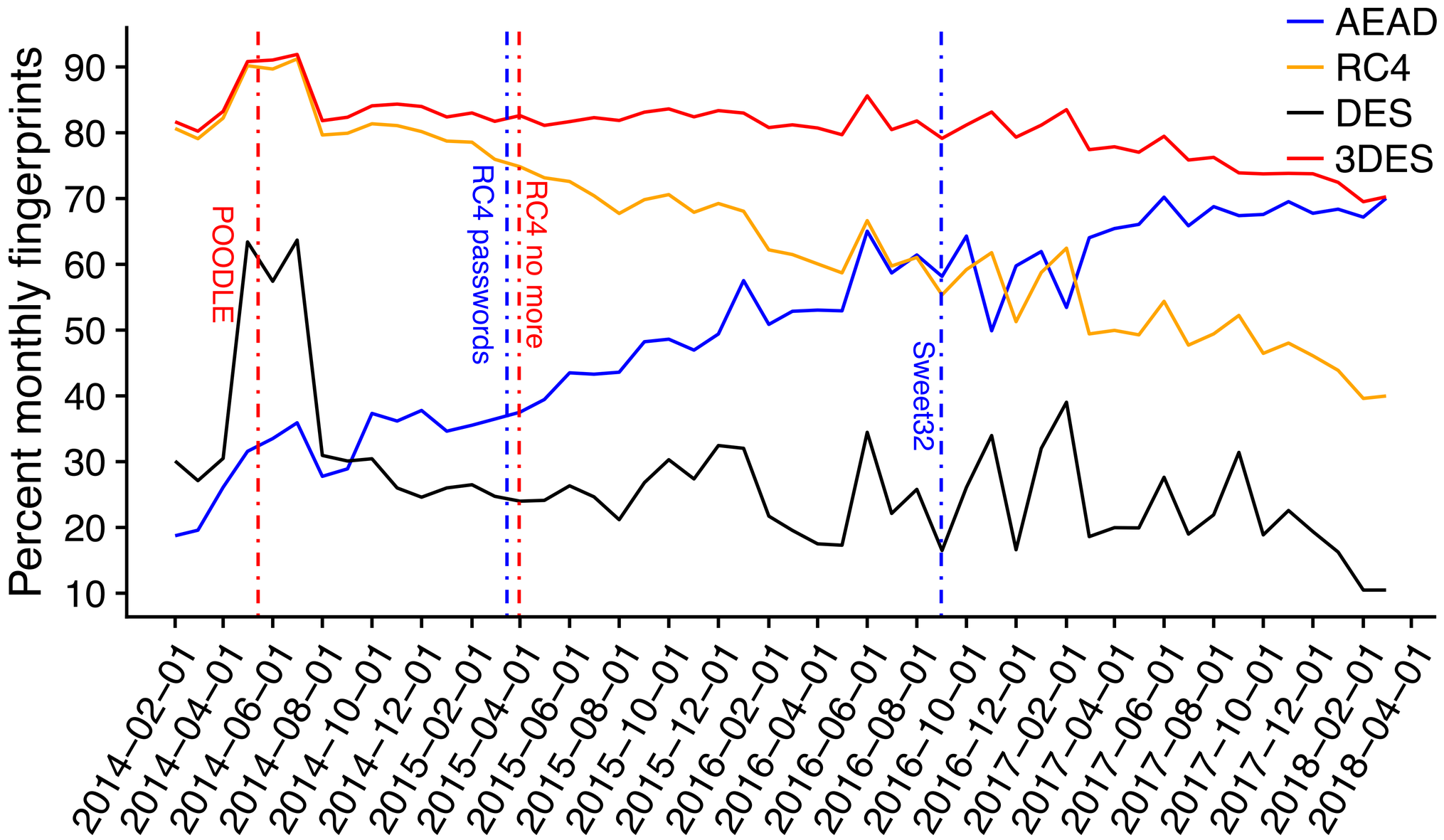
RC4, (3)DES, AEAD (advertised)



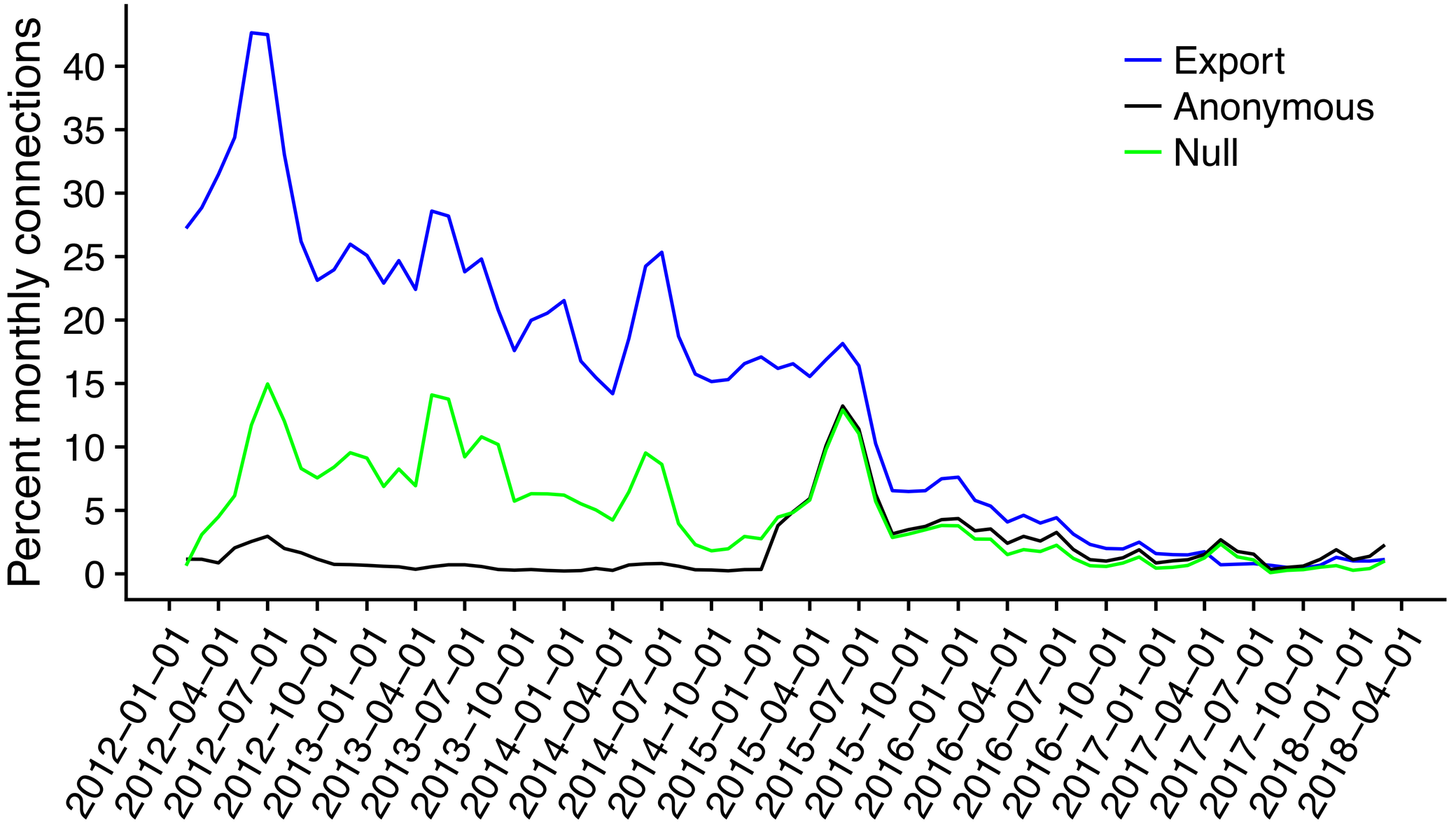
Conns. advertising RC4



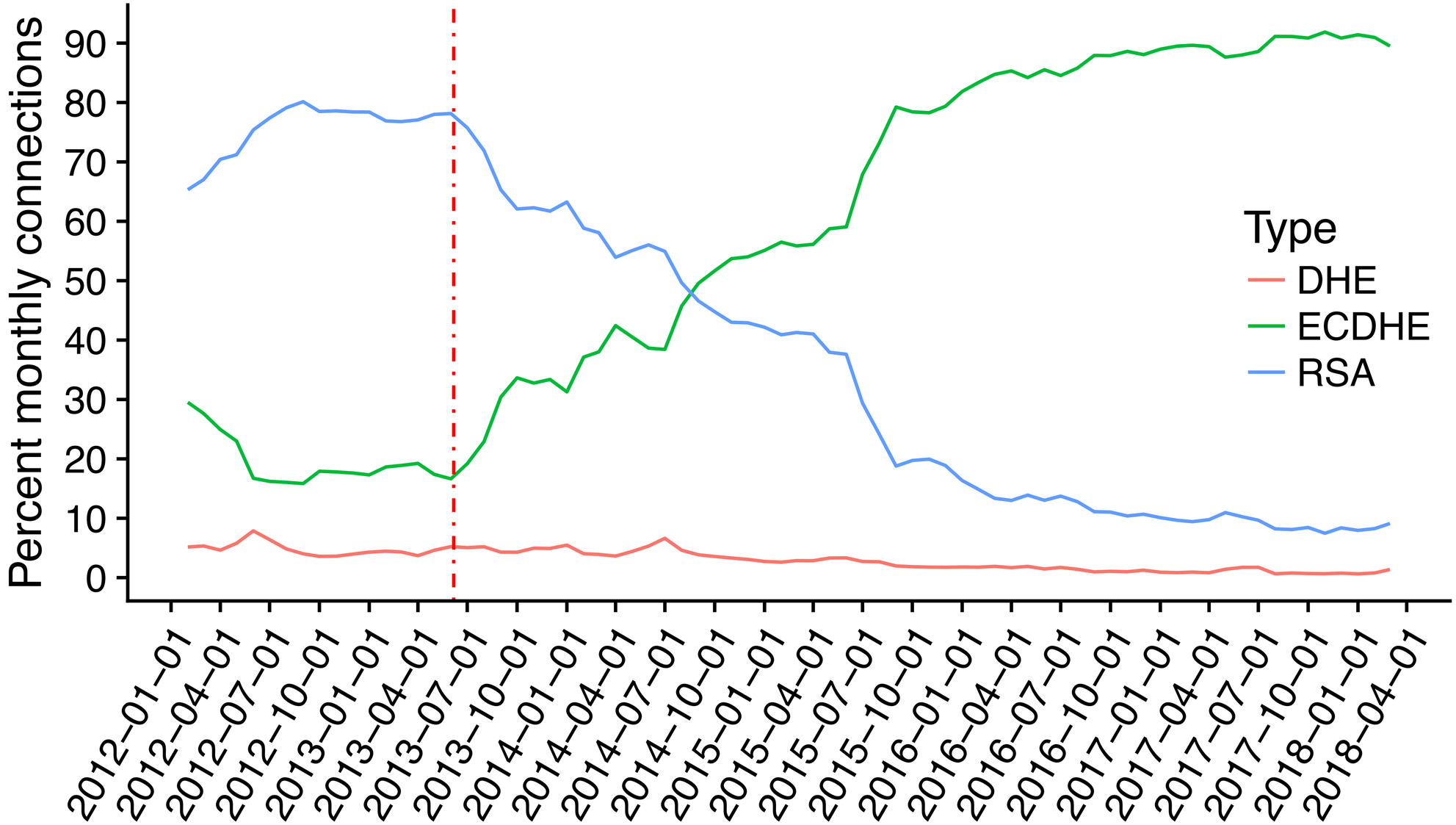
TLS Fingerprints AEAD/RC4/(3)DES

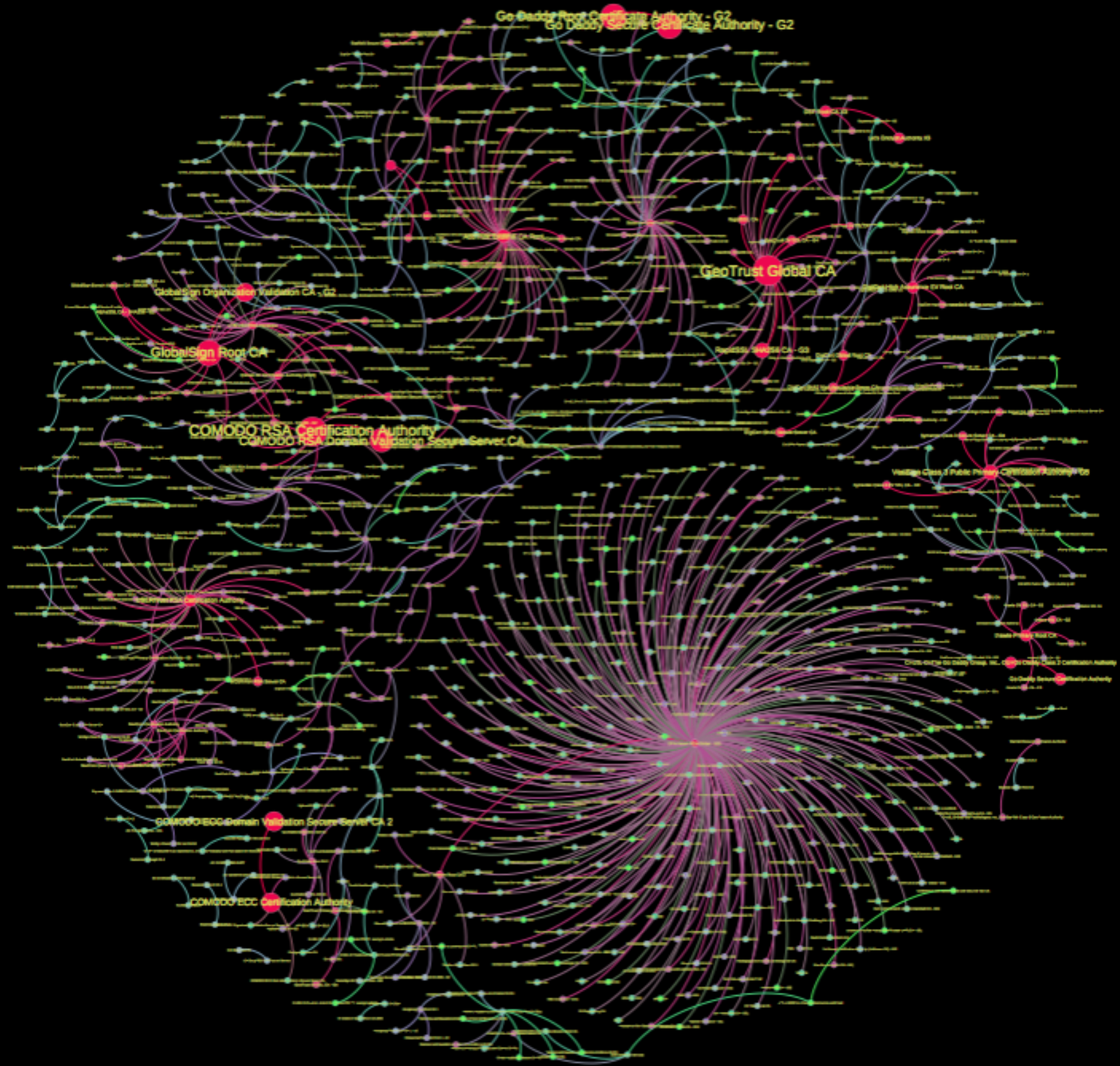


Export/Anon/NULL advertised



Negotiated RSA vs forward secret




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