Mission Accomplished? HTTPS Security after DigiNotar

Johanna Amann*	ICSI / Corelight / LBL
Oliver Gasser*	Technical University of Munich
Quirin Scheitle*	Technical University of Munich
Lexi Brent	The University of Sydney
Georg Carle	Technical University of Munich
Ralph Holz	The University of Sydney

* Joint First Authorship

Internet Measurement Conference (IMC) 2017

TLS/HTTPS Security Extensions

- Certificate Transparency
- HSTS (HTTP Strict Transport Security)
- HPKP (HTTP Public Key Pinning)
- SCSV (TLS Fallback Signaling Cipher Suite Value)
- CAA (Certificate Authority Authorization)
- DANE-TLSA (DNS Based Authentication of Named Entities)

Methodology

- Active & passive scans
  - Shared pipeline where possible
- Active measurements from 2 continents
  - Largest Domain-based TLS scan so far
  - More than 192 Million domains
- Passive measurements on 3 continents
  - More than 2.4 Billion observed TLS connections

Certificate Transparency

CA

Issues Certificates

CT Log

Provides publicly auditable, append-only Log of certificates

Also provides proof of inclusion

Browser

Verifies Proof of Inclusion

Certificate Transparency

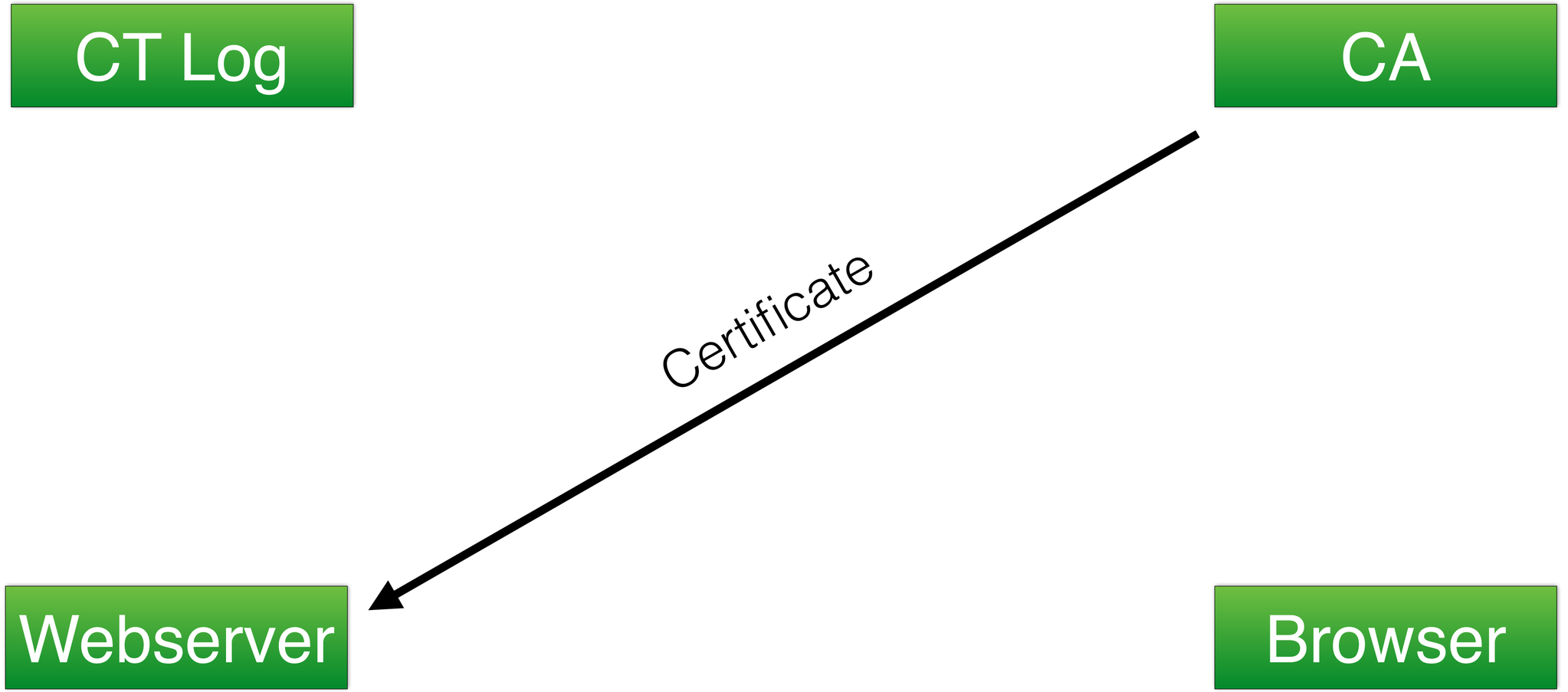
CT Log

CA

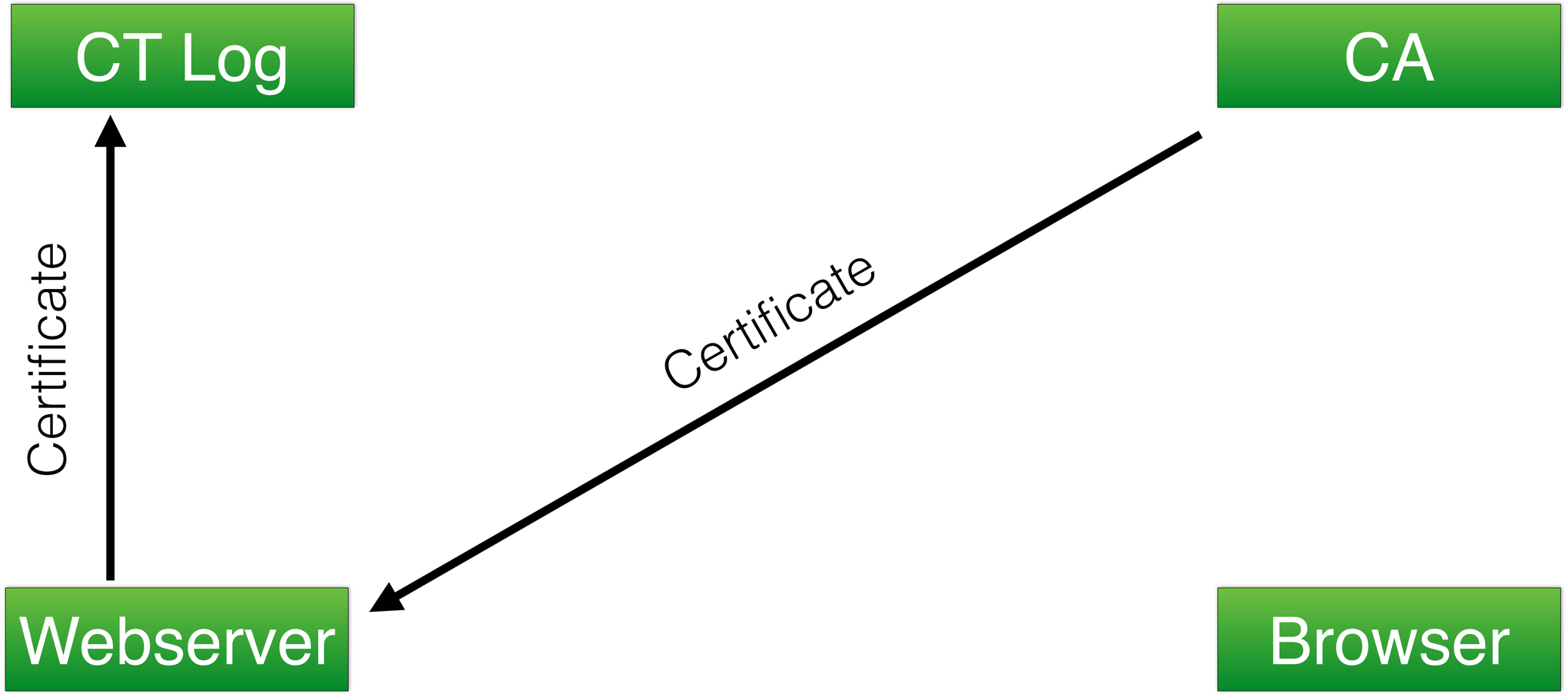
Webserver

Browser

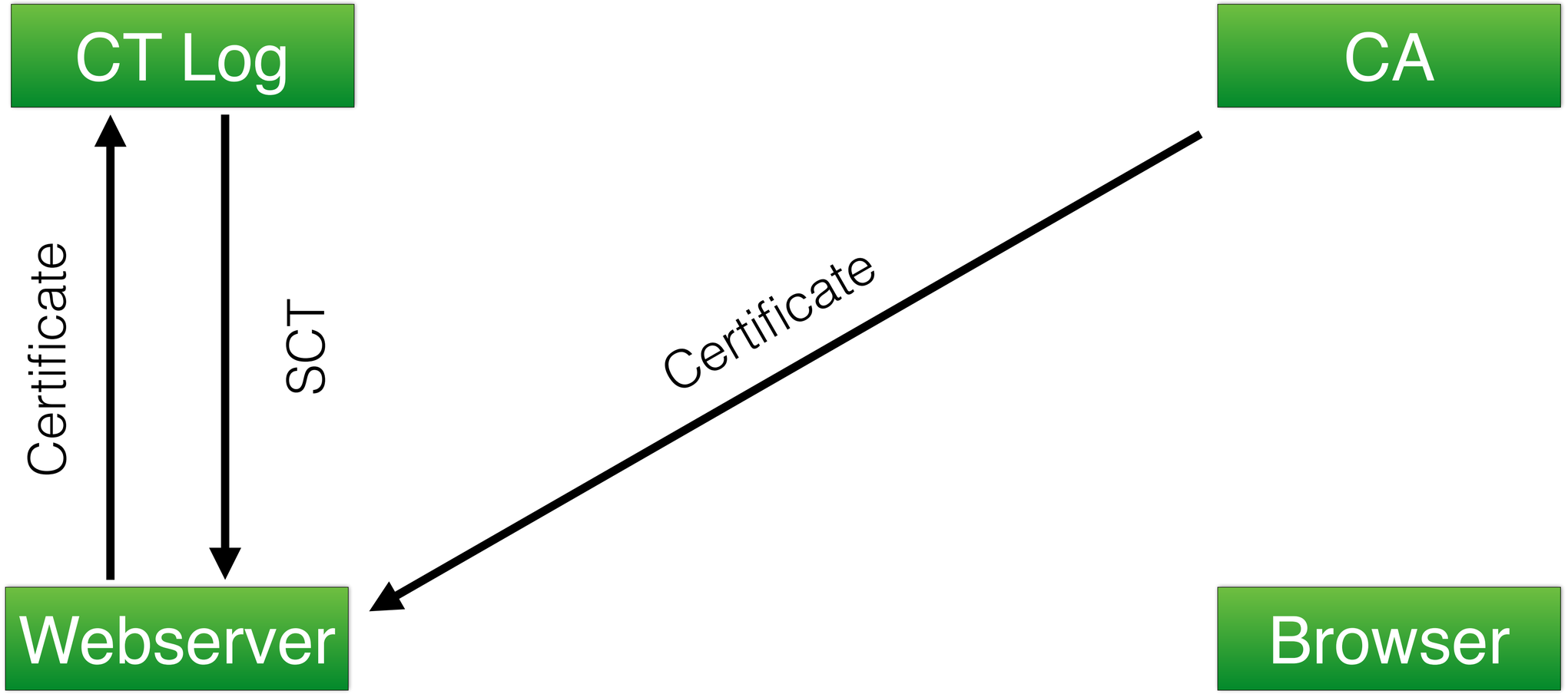
Certificate Transparency



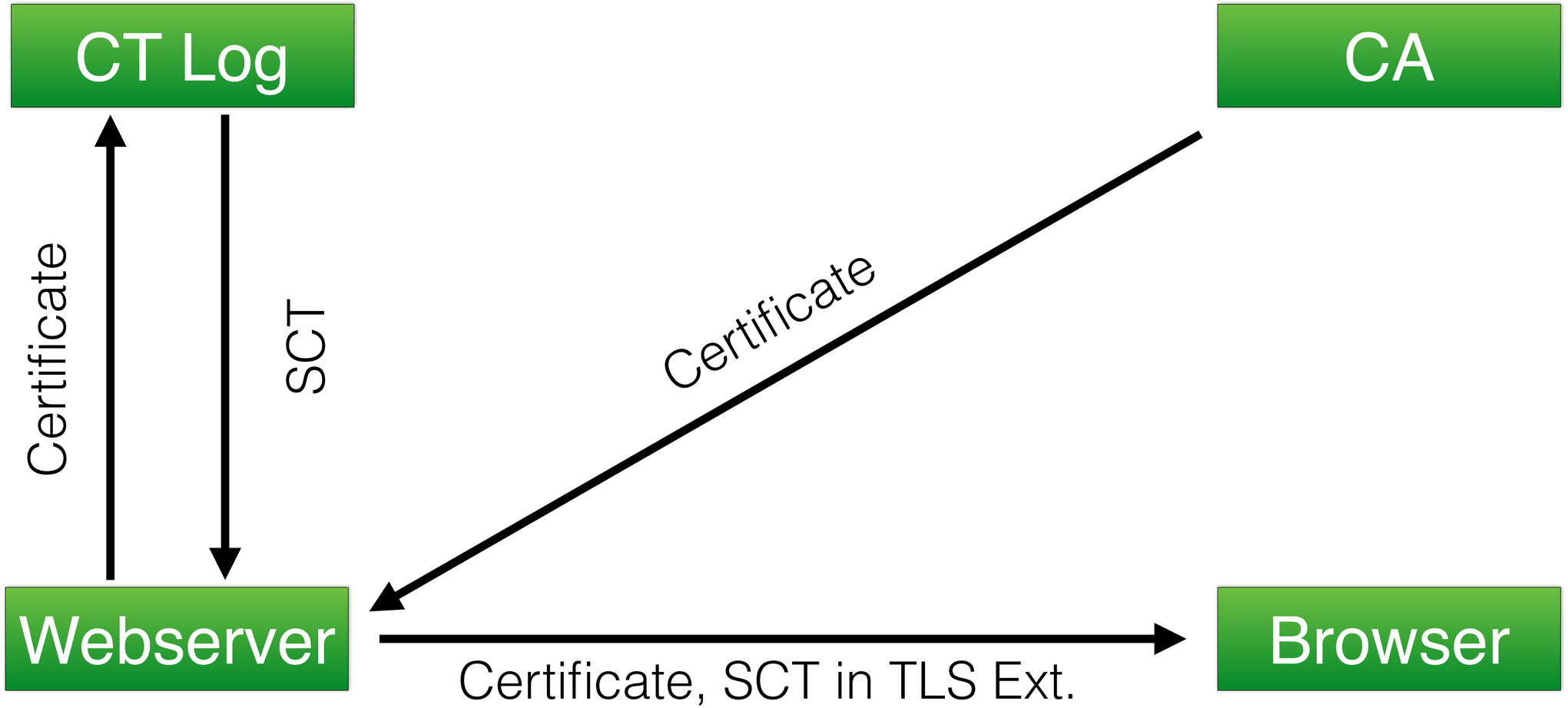
Certificate Transparency



Certificate Transparency



Certificate Transparency



Certificate Transparency

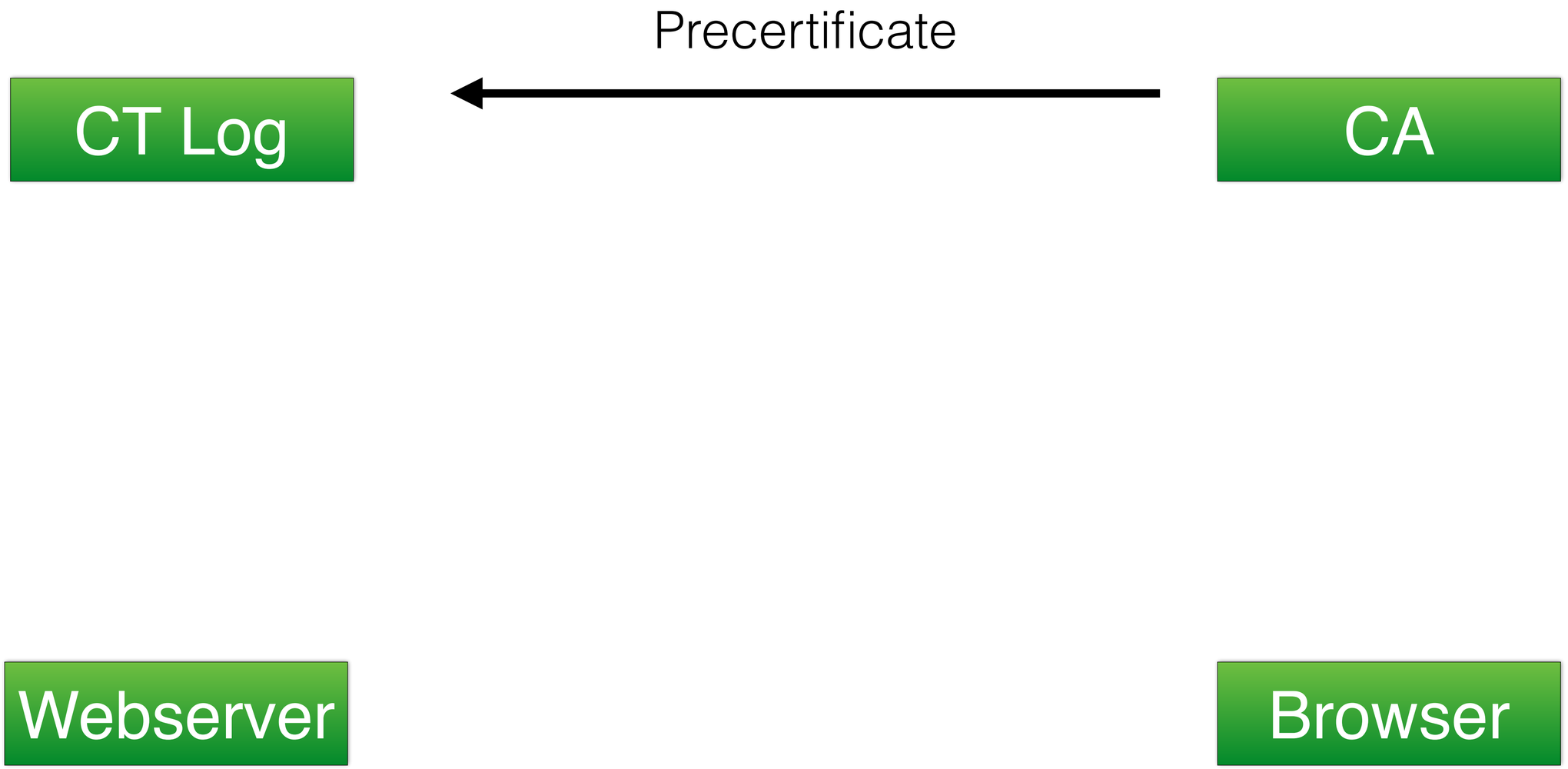
CT Log

CA

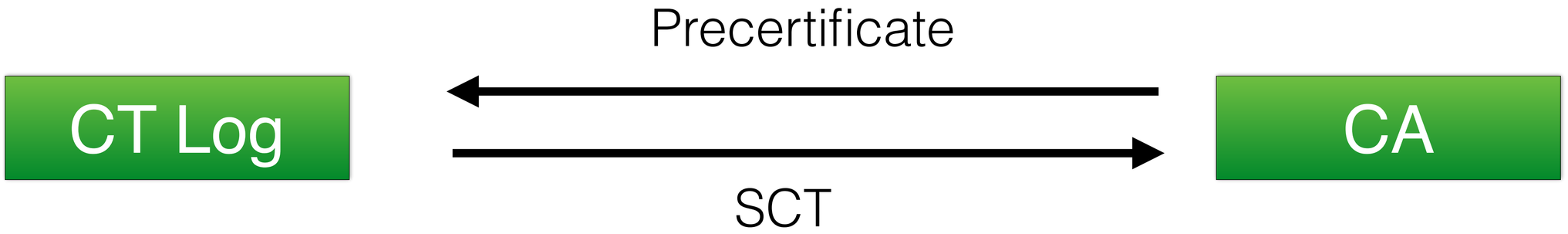
Webserver

Browser

Certificate Transparency



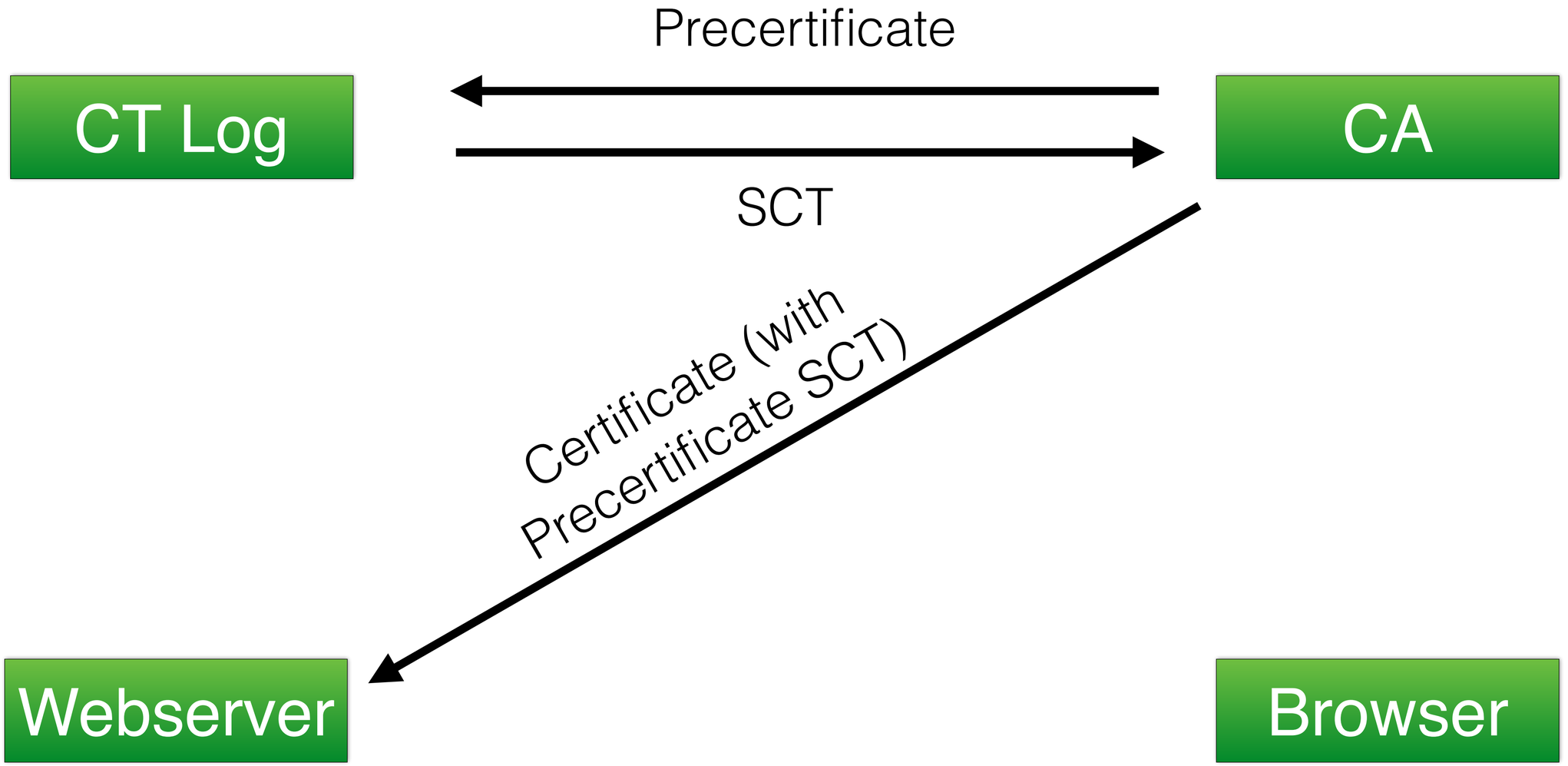
Certificate Transparency



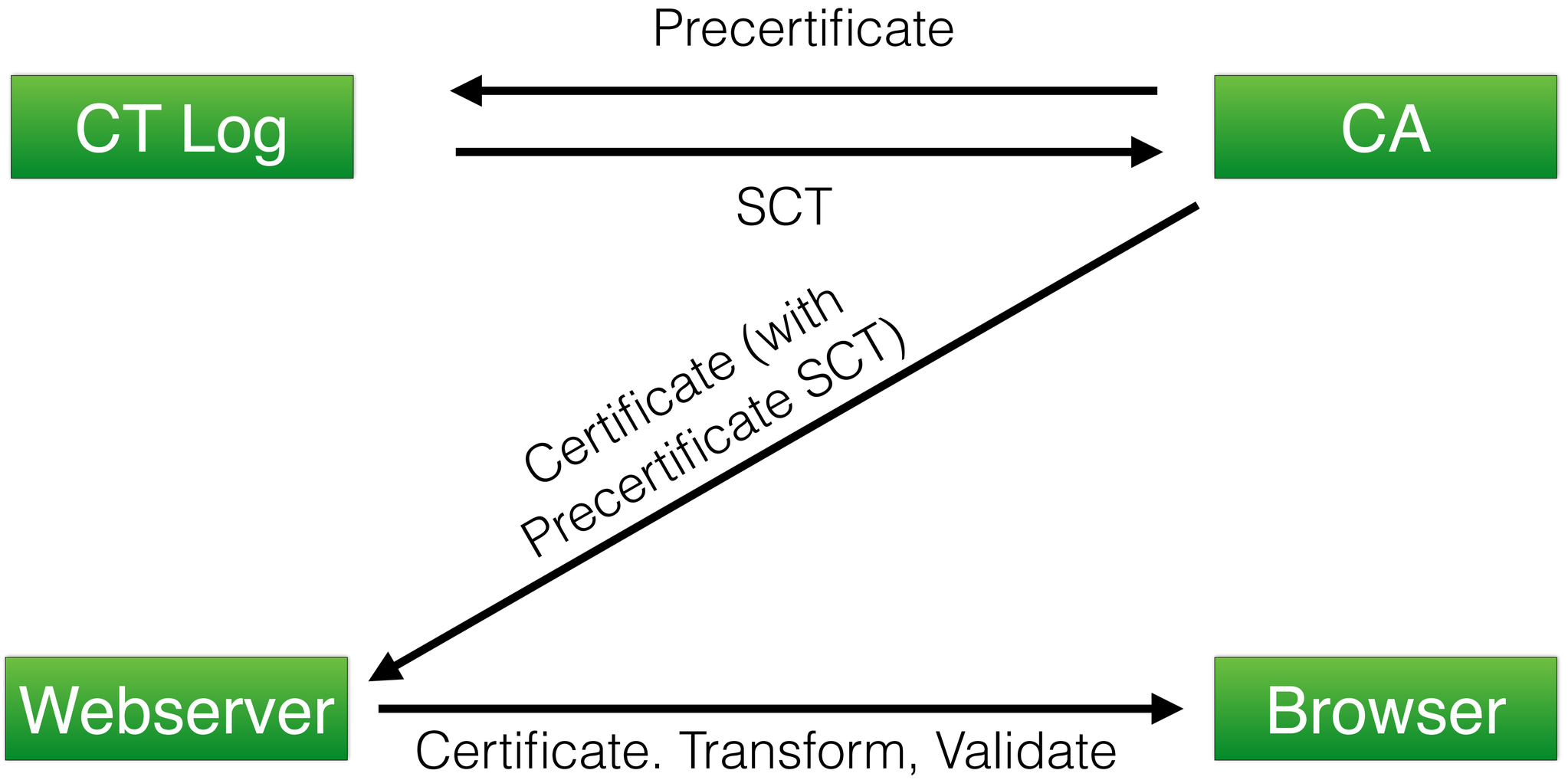
Webserver

Browser

Certificate Transparency



Certificate Transparency



Certificate Transparency

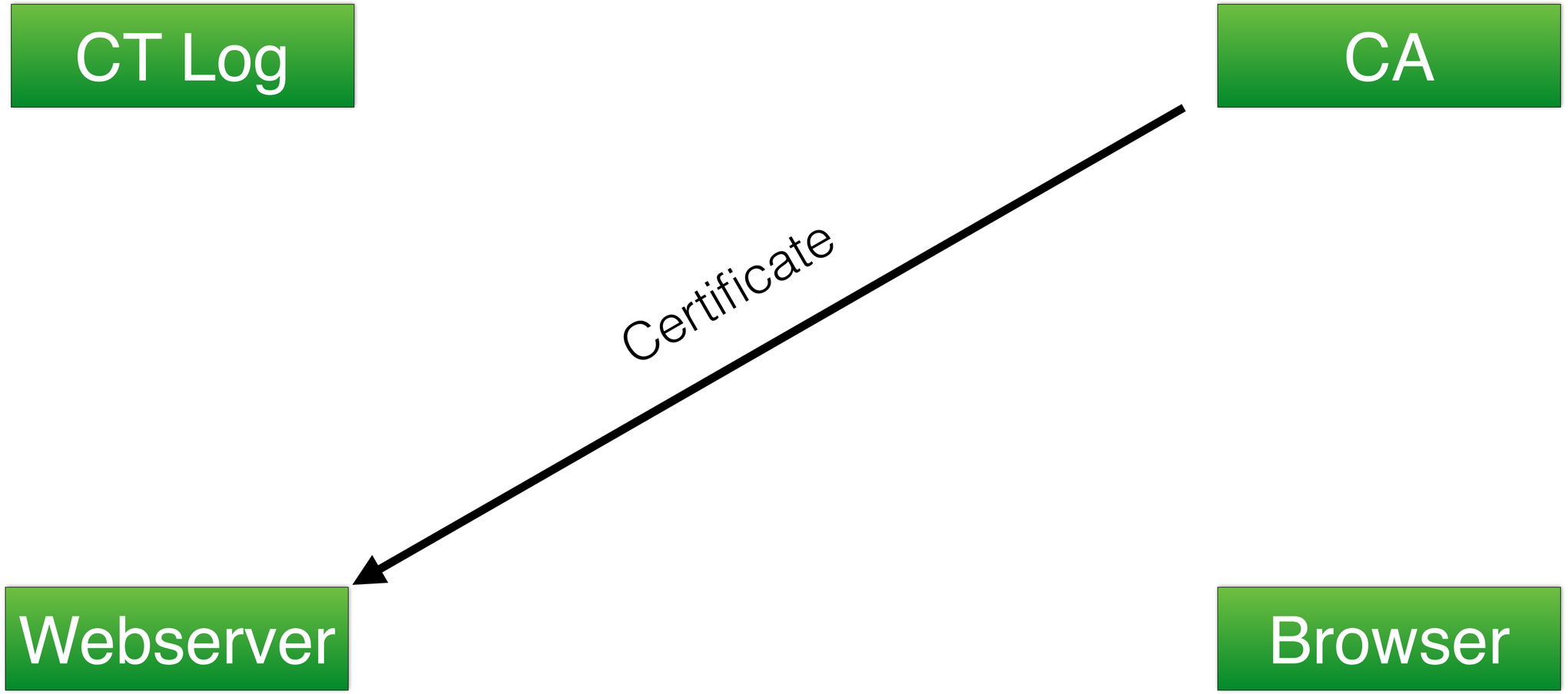
CT Log

CA

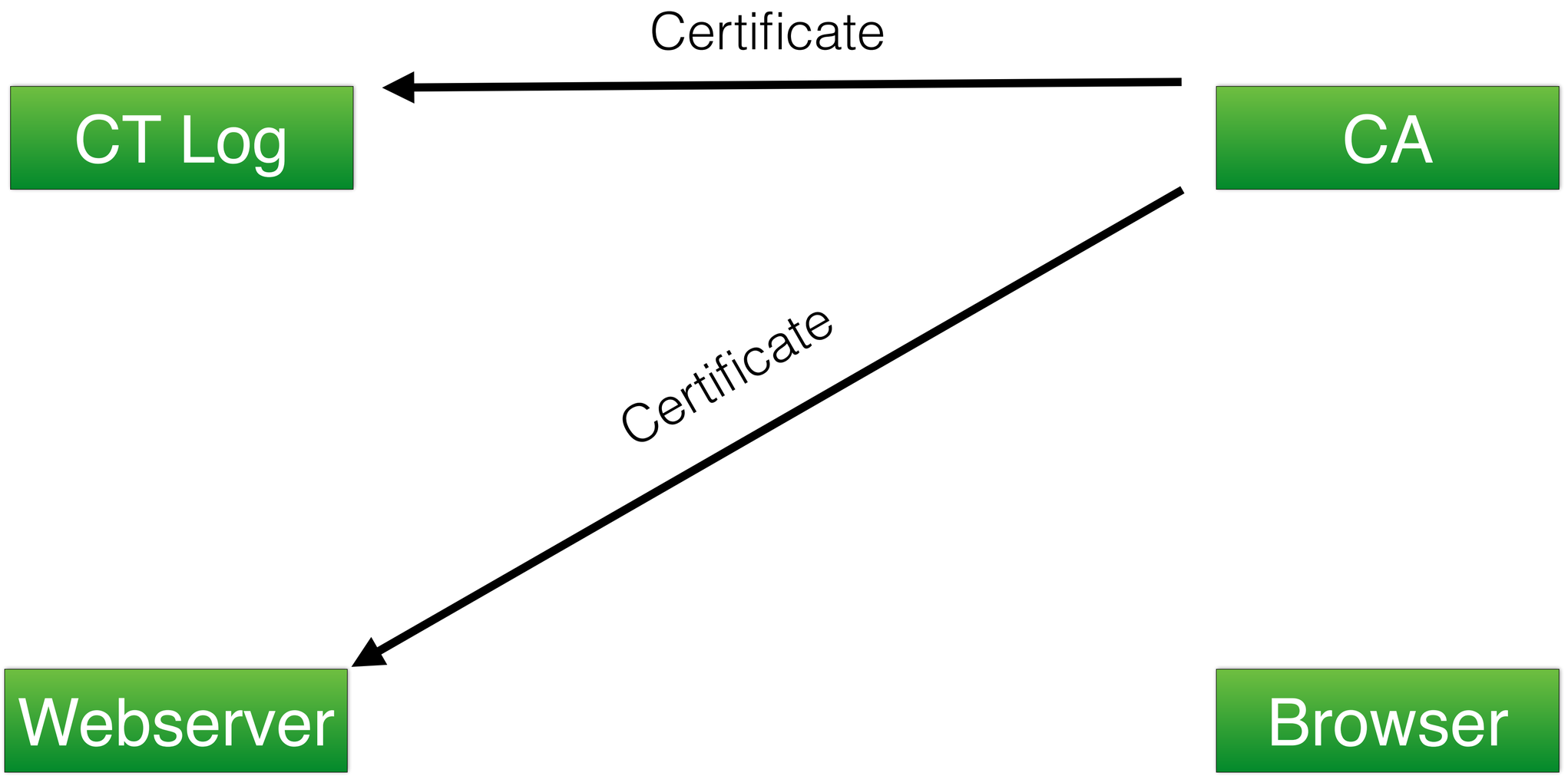
Webserver

Browser

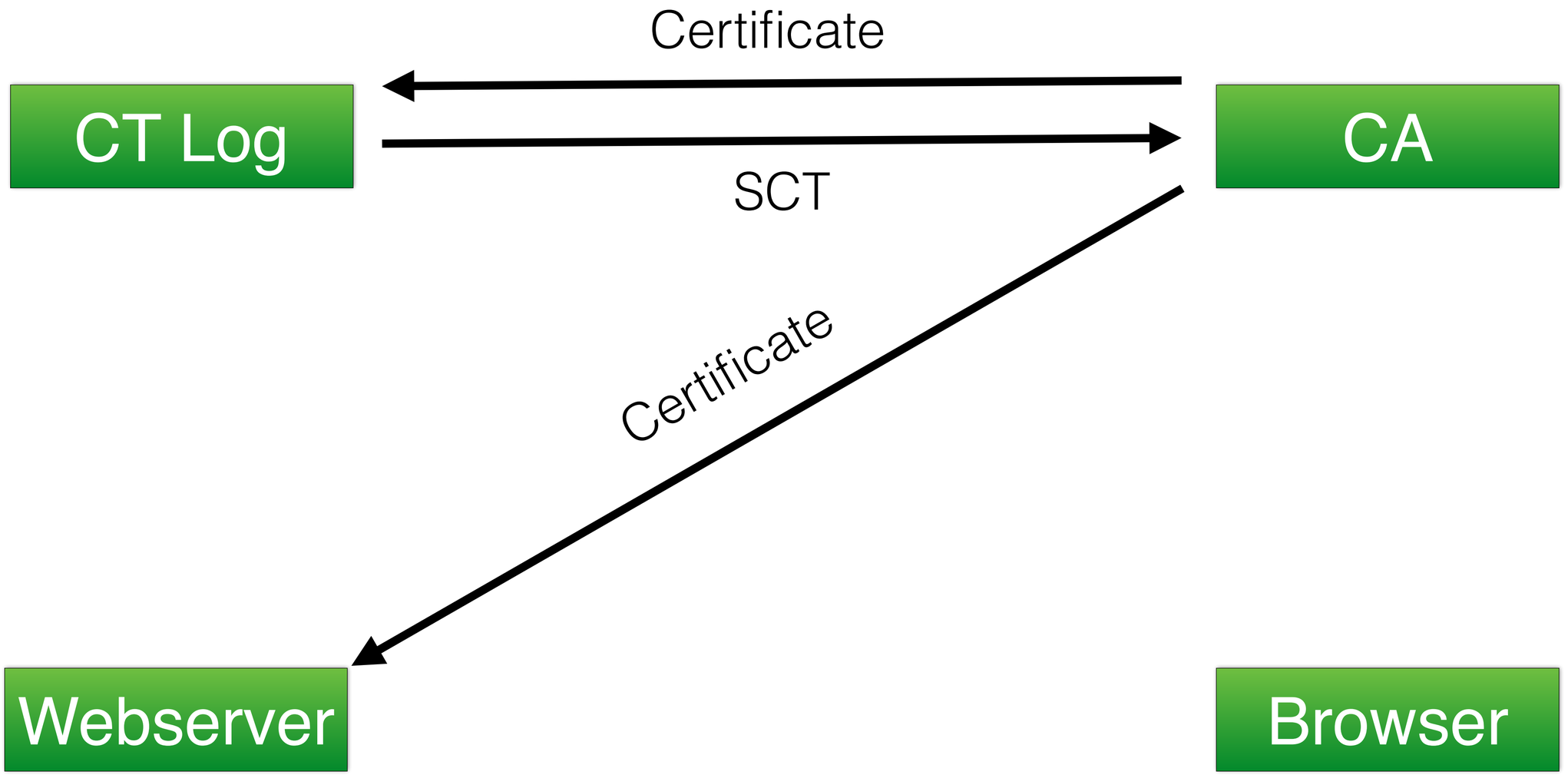
Certificate Transparency



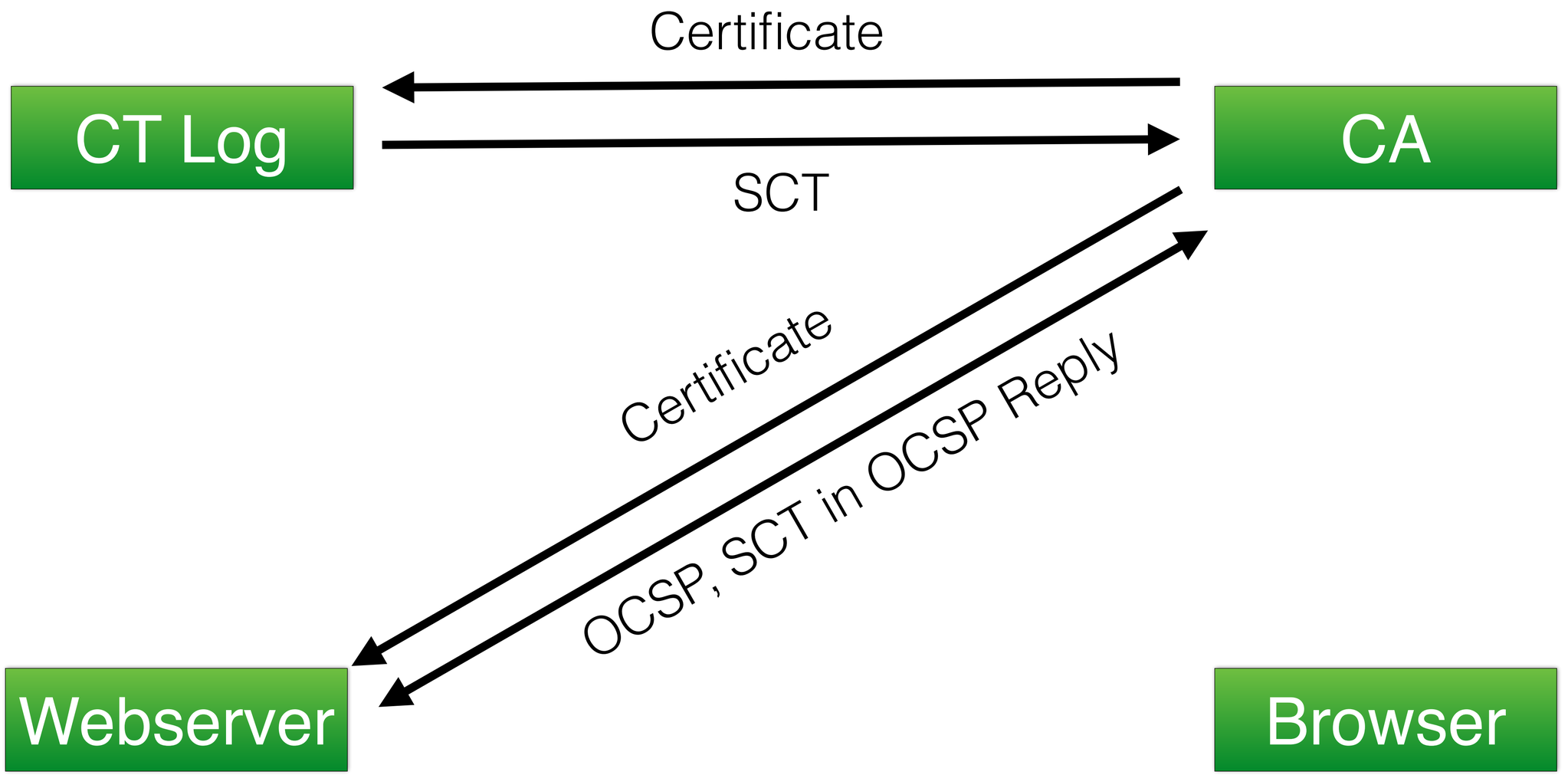
Certificate Transparency



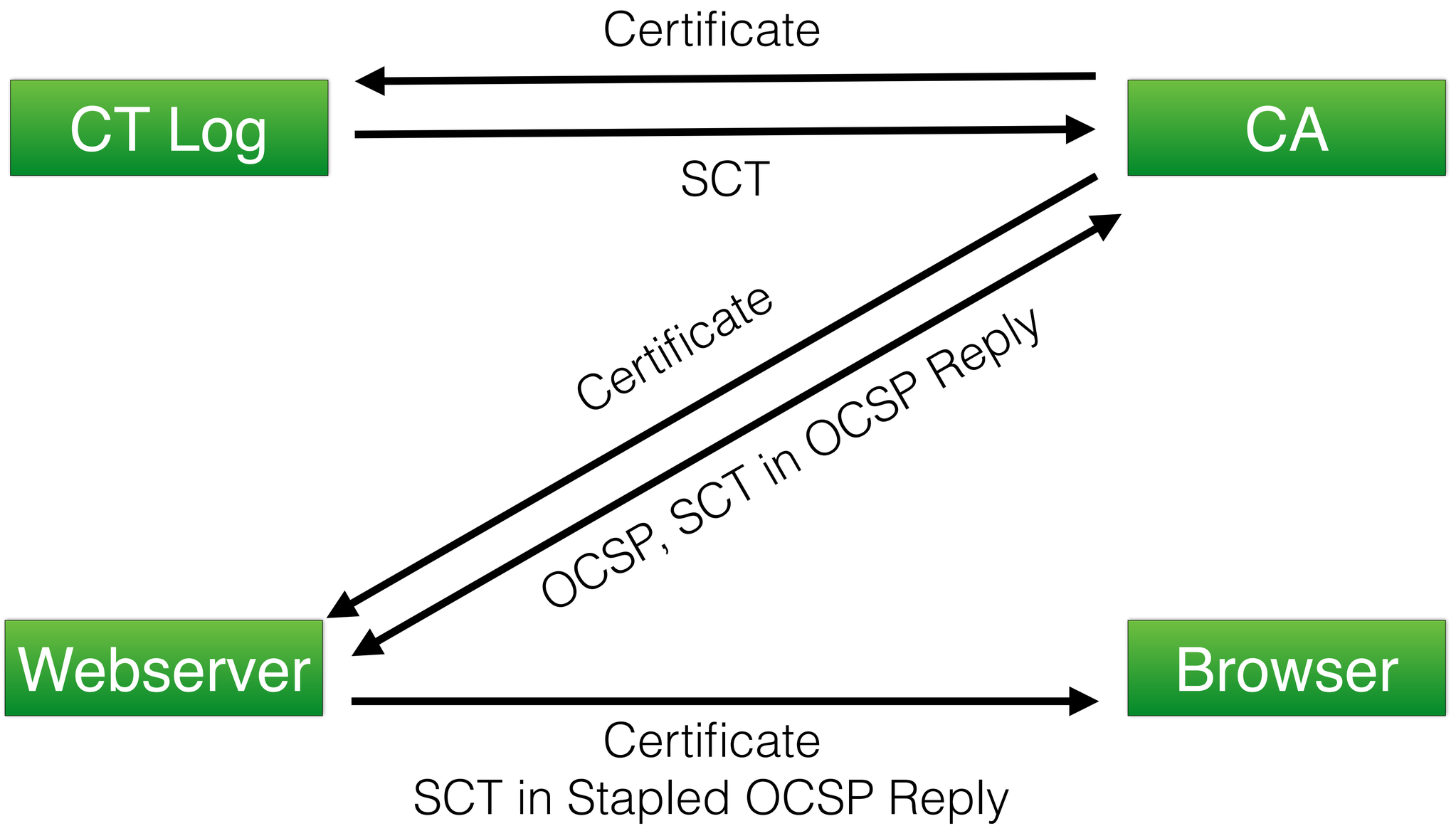
Certificate Transparency



Certificate Transparency



Certificate Transparency

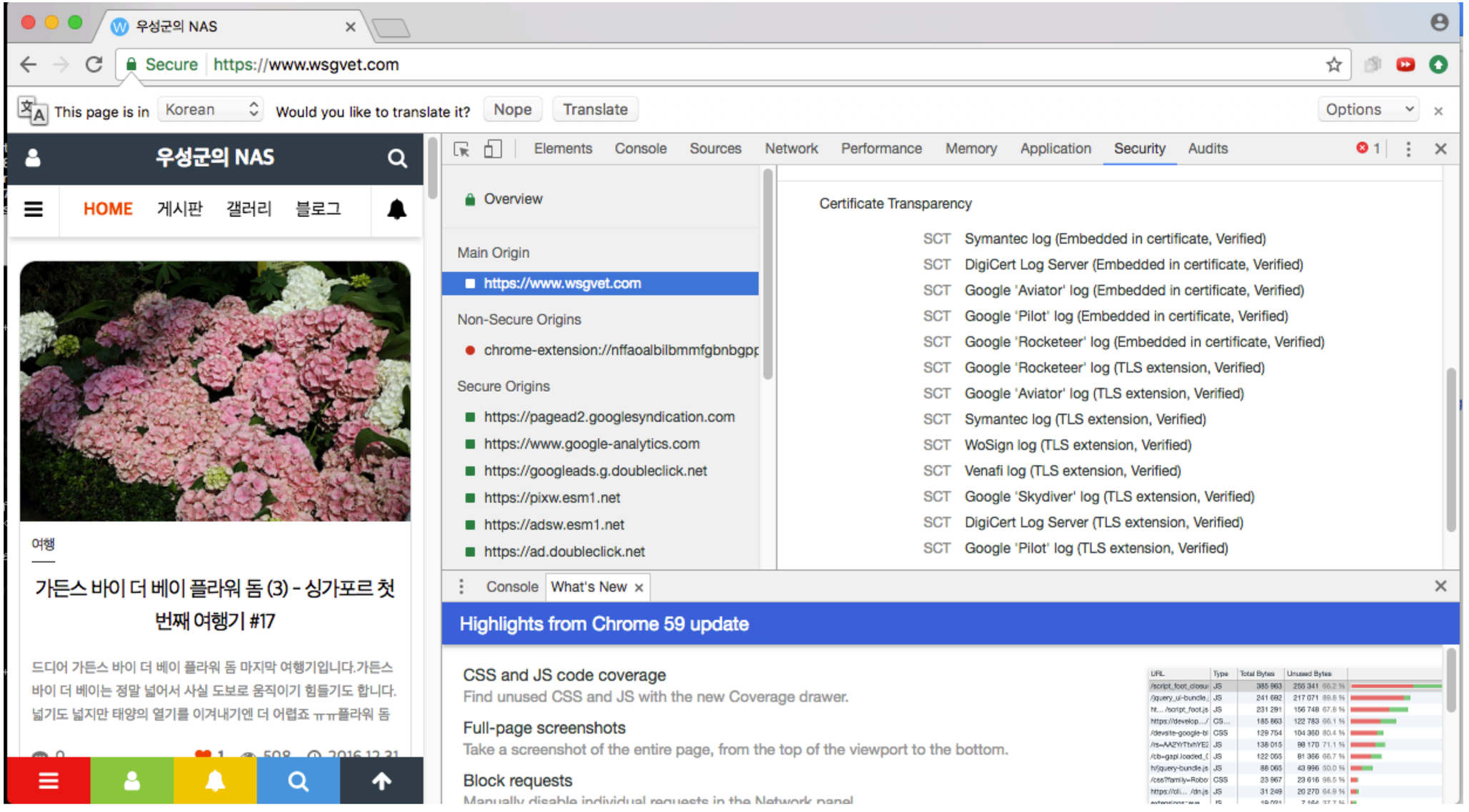


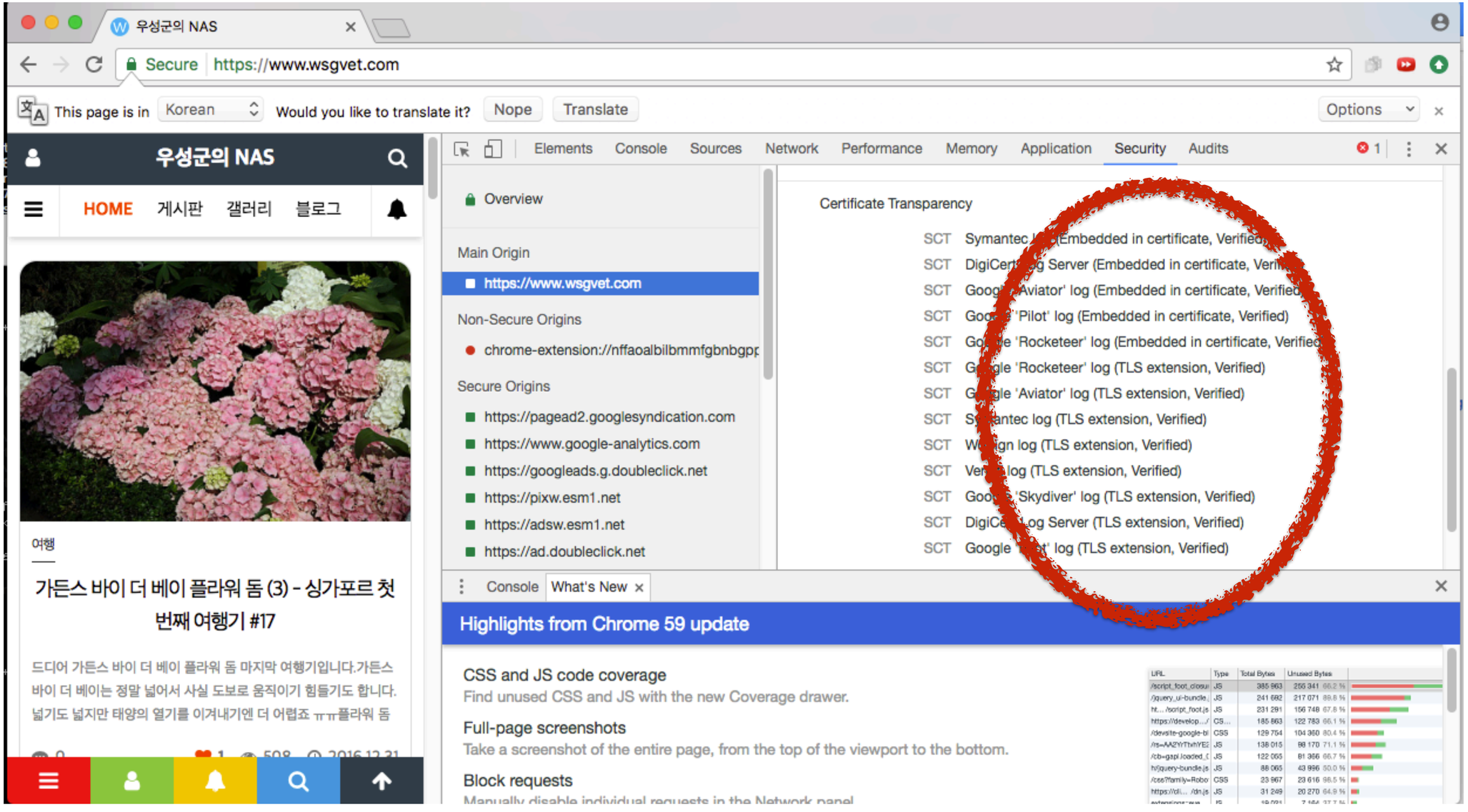
SCT Statistics - Active

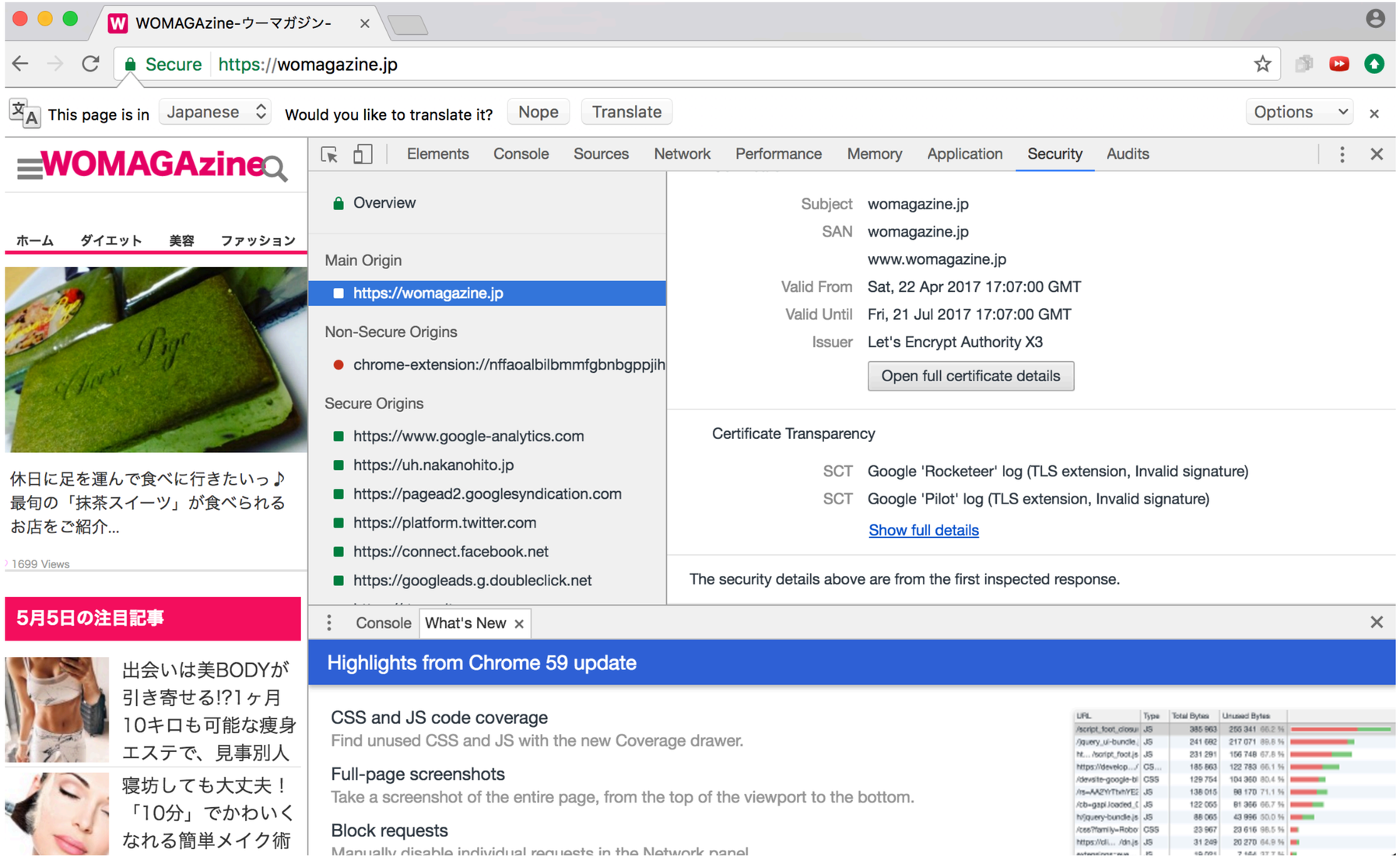
	Sydney v4	Munich v4	Munich v6
Domains we could connect to	55.7M	58.0M	5.1M
Domains with SCT	6.8M	6.8M	357K
… via X509	6.7M	6.8M	344K
… via TLS Ext.	27.6K	27.2K	12.9K
… via OCSP	180	188	3
Certificates (Total)	10.62M	9.66M	549.98K
Certificates with SCT Ext.	799.9K	834.5K	193.9K

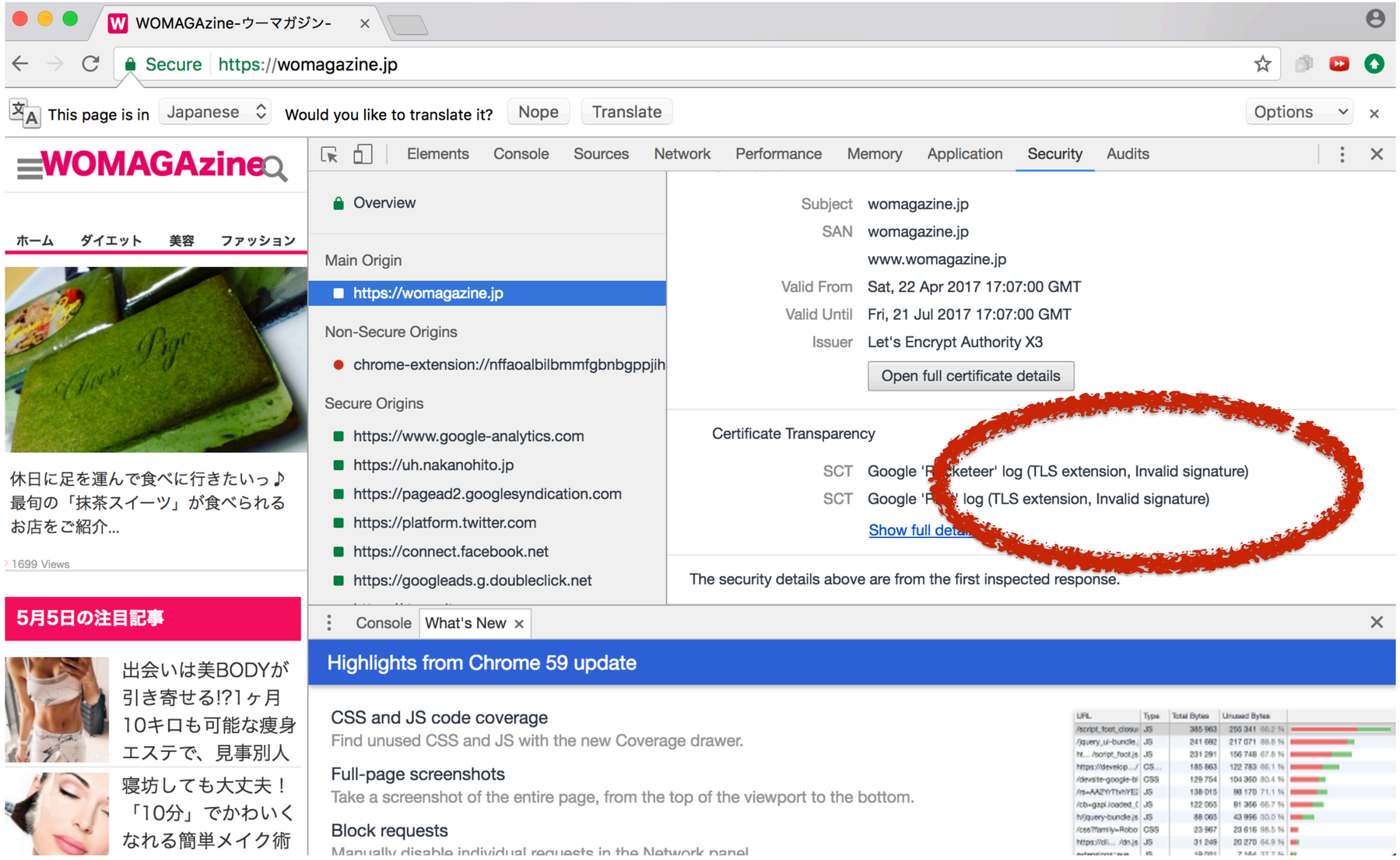
SCT Statistics - Passive

	California	Munich	Sydney
Time	4/4-5/2	5/12-5/16	5/12-5/16
Conns	2.6B	287M	196M
Conns with SCT	779M	73M	58M
… in Cert	520M	58M	44M
… in TLS	248.1M	14.4M	13.6M
… in OCSP	155.8K	37.6K	31.1K
# v4 IPs	737K	344K	226K
# SCT v4 IPs	222K	102K	66K

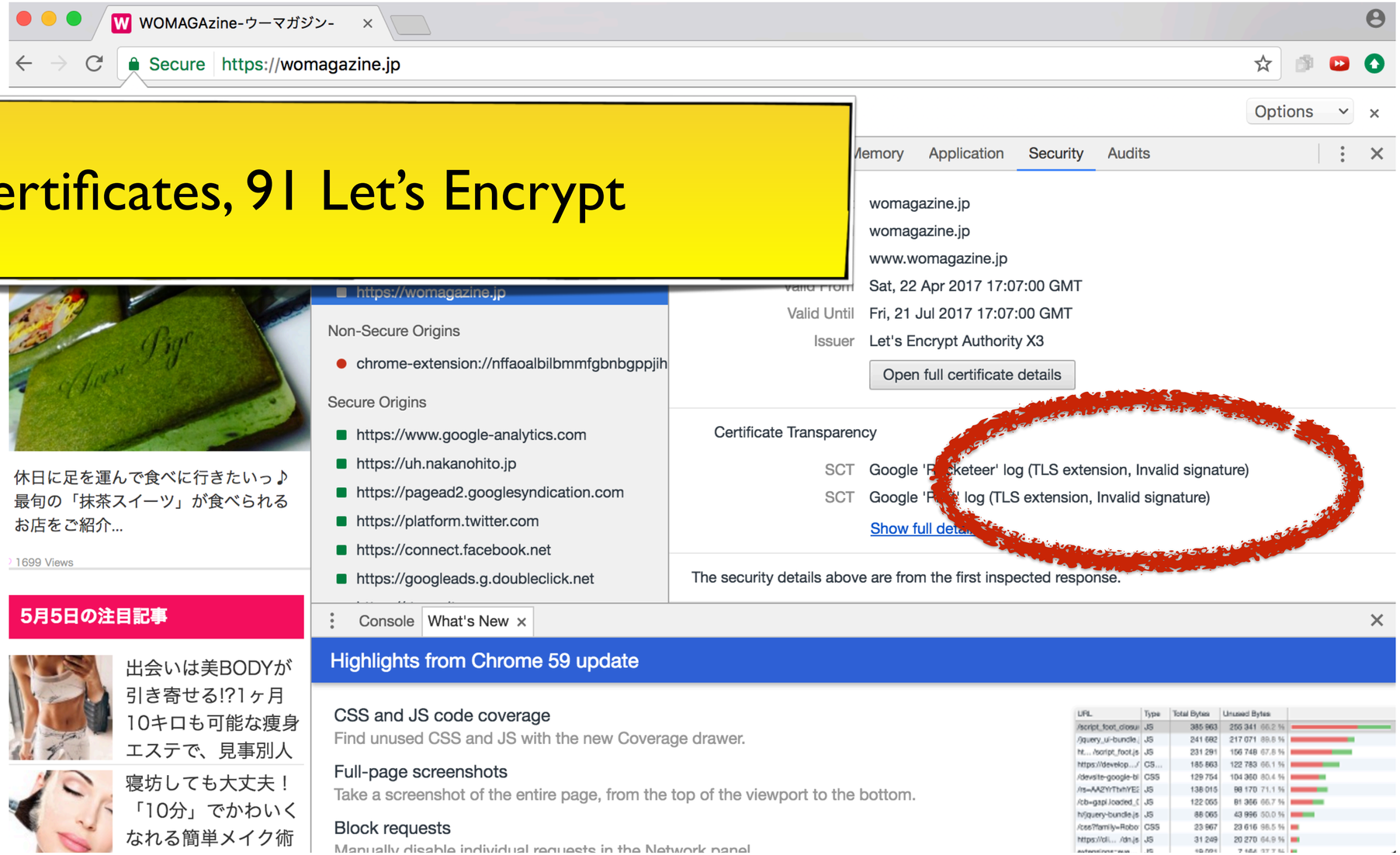

우성군의 NAS
Secure https://www.wsgvet.com
This page is in Korean Would you like to translate it? Nope Translate Options
우성군의 NAS
HOME 게시판 갤러리 블로그
여행
가든스 바이 더 베이 플라워 돔 (3) - 싱가포르 첫 번째 여행기 #17
드디어 가든스 바이 더 베이 플라워 돔 마지막 여행기입니다.가든스 바이 더 베이는 정말 넓어서 사실 도보로 움직이기 힘들기도 합니다. 넓기도 넓지만 태양의 열기를 이겨내기엔 더 어렵죠 ㅠㅠ플라워 돔
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.wsgvet.com
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgpp
Secure Origins
https://pagead2.googlesyndication.com
https://www.google-analytics.com
https://googleads.g.doubleclick.net
https://pixw.esm1.net
https://adsw.esm1.net
https://ad.doubleclick.net
Certificate Transparency
SCT Symantec log (Embedded in certificate, Verified)
SCT DigiCert Log Server (Embedded in certificate, Verified)
SCT Google 'Aviator' log (Embedded in certificate, Verified)
SCT Google 'Pilot' log (Embedded in certificate, Verified)
SCT Google 'Rocketeer' log (Embedded in certificate, Verified)
SCT Google 'Rocketeer' log (TLS extension, Verified)
SCT Google 'Aviator' log (TLS extension, Verified)
SCT Symantec log (TLS extension, Verified)
SCT WoSign log (TLS extension, Verified)
SCT Venafi log (TLS extension, Verified)
SCT Google 'Skydiver' log (TLS extension, Verified)
SCT DigiCert Log Server (TLS extension, Verified)
SCT Google 'Pilot' log (TLS extension, Verified)
Console What's New
Highlights from Chrome 59 update
CSS and JS code coverage
Find unused CSS and JS with the new Coverage drawer.
Full-page screenshots
Take a screenshot of the entire page, from the top of the viewport to the bottom.
Block requests

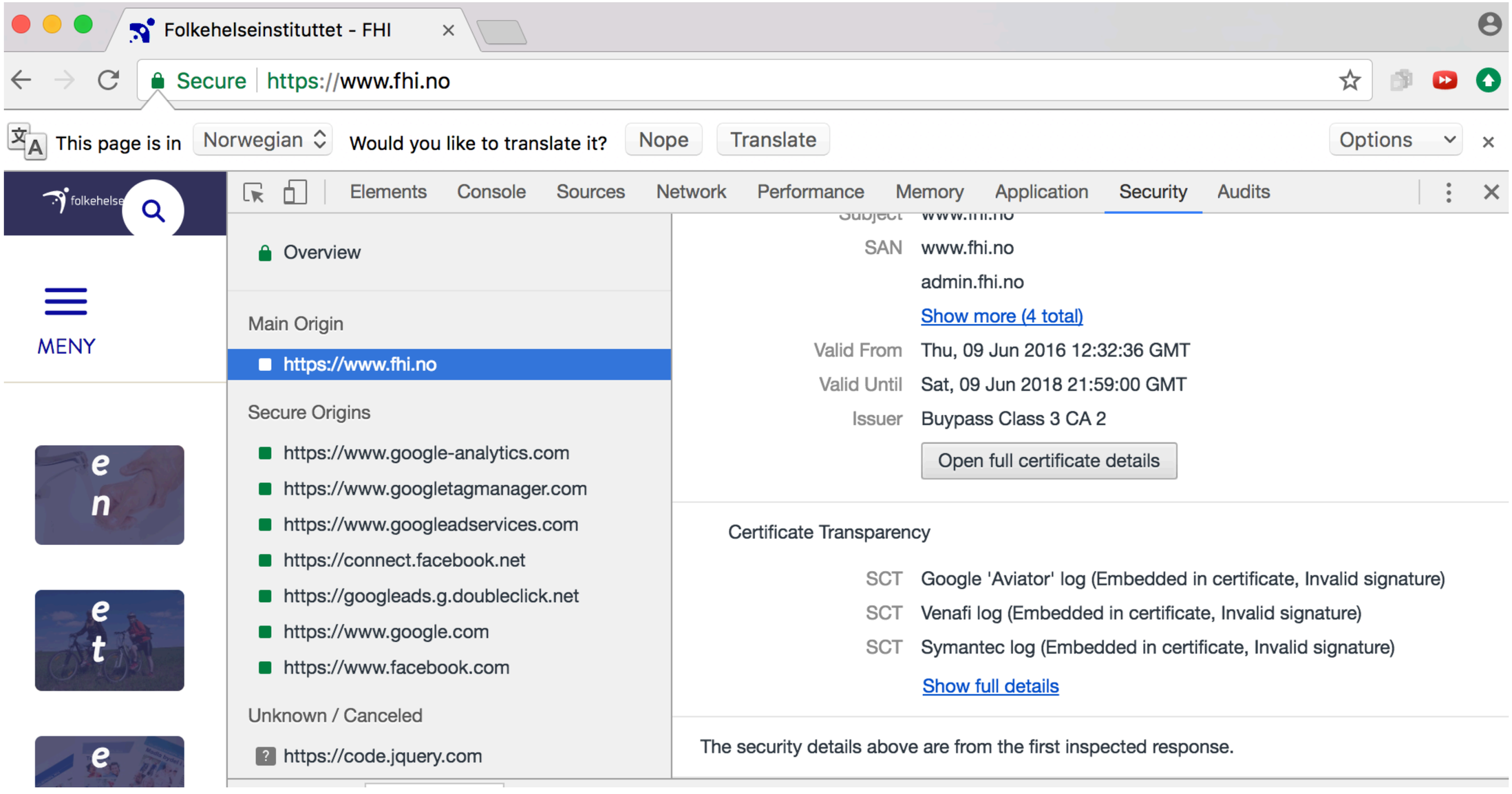

우성군의 NAS
Secure https://www.wsgvet.com
This page is in Korean Would you like to translate it? Nope Translate Options
우성군의 NAS
HOME 게시판 갤러리 블로그
여행
가든스 바이 더 베이 플라워 돔 (3) - 싱가포르 첫 번째 여행기 #17
드디어 가든스 바이 더 베이 플라워 돔 마지막 여행기입니다.가든스 바이 더 베이는 정말 넓어서 사실 도보로 움직이기 힘들기도 합니다. 넓기도 넓지만 태양의 열기를 이겨내기엔 더 어렵죠 ㅠㅠ플라워 돔
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.wsgvet.com
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgpp
Secure Origins
https://pagead2.googlesyndication.com
https://www.google-analytics.com
https://googleads.g.doubleclick.net
https://pixw.esm1.net
https://adsw.esm1.net
https://ad.doubleclick.net
Certificate Transparency
SCT Symantec (Embedded in certificate, Verified)
SCT DigiCert Log Server (Embedded in certificate, Verified)
SCT Google 'Aviator' log (Embedded in certificate, Verified)
SCT Google 'Pilot' log (Embedded in certificate, Verified)
SCT Google 'Rocketeer' log (Embedded in certificate, Verified)
SCT Google 'Rocketeer' log (TLS extension, Verified)
SCT Google 'Aviator' log (TLS extension, Verified)
SCT Symantec log (TLS extension, Verified)
SCT WoSign log (TLS extension, Verified)
SCT Venafi log (TLS extension, Verified)
SCT Google 'Skydiver' log (TLS extension, Verified)
SCT DigiCert Log Server (TLS extension, Verified)
SCT Google 'Icarus' log (TLS extension, Verified)
Console What's New
Highlights from Chrome 59 update
CSS and JS code coverage
Find unused CSS and JS with the new Coverage drawer.
Full-page screenshots
Take a screenshot of the entire page, from the top of the viewport to the bottom.
Block requests
Manually disable individual requests in the Network panel

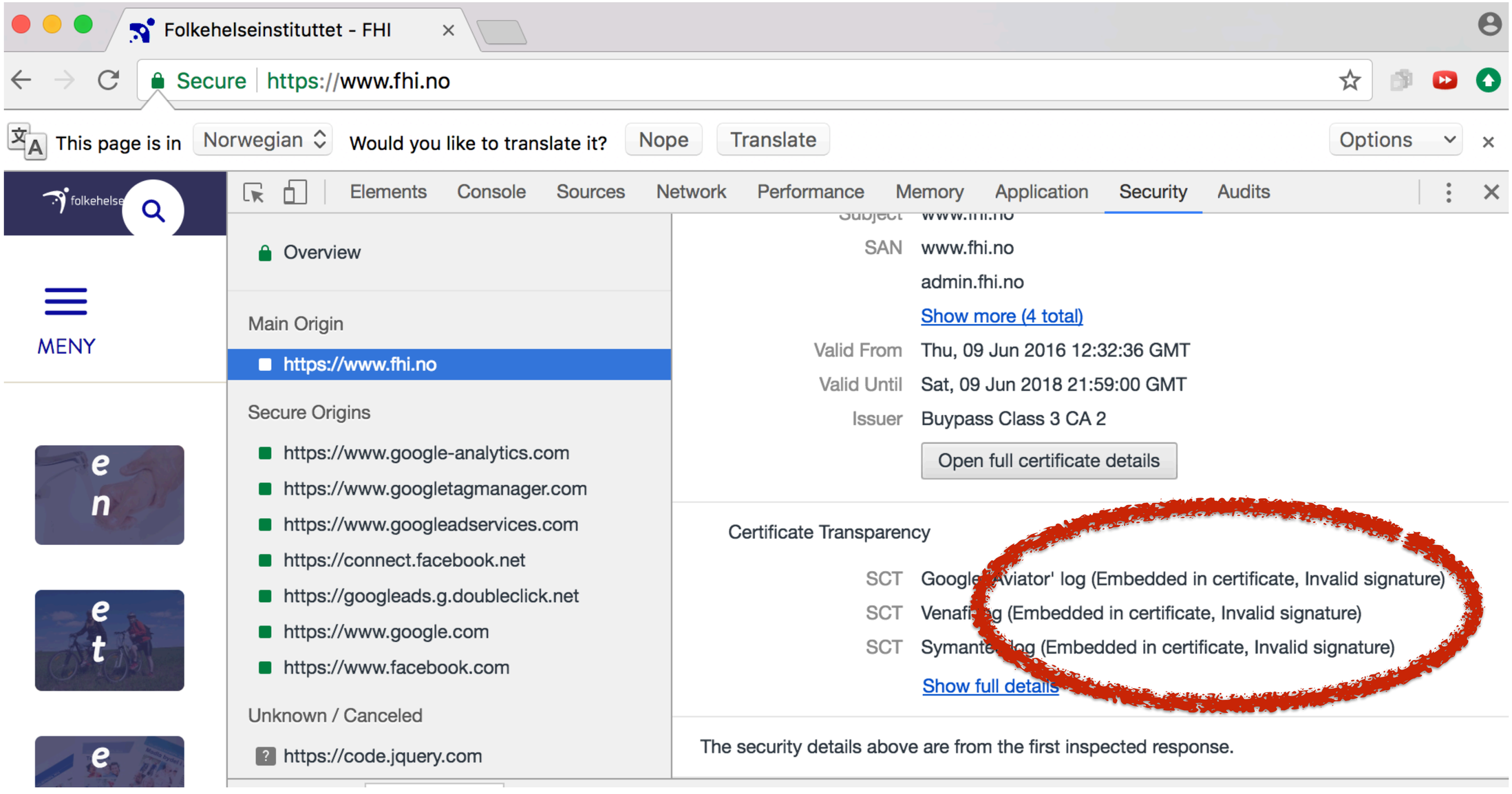

WOMAGAzine-ウーマガジン-
Secure https://womagazine.jp
This page is in Japanese Would you like to translate it? Nope Translate Options
WOMAGAzine
ホーム ダイエット 美容 ファッション
休日に足を運んで食べに行きたいっ♪
最旬の「抹茶スイーツ」が食べられる
お店をご紹介...
1699 Views
5月5日の注目記事
出会いは美BODYが
引き寄せる!?1ヶ月
10キロも可能な痩身
エステで、見事別人
寝坊しても大丈夫！
「10分」でかわいく
なれる簡単メイク術
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://womagazine.jp
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgppjih
Secure Origins
https://www.google-analytics.com
https://uh.nakanohito.jp
https://pagead2.googlesyndication.com
https://platform.twitter.com
https://connect.facebook.net
https://googleads.g.doubleclick.net
Subject womagazine.jp
SAN womagazine.jp
www.womagazine.jp
Valid From Sat, 22 Apr 2017 17:07:00 GMT
Valid Until Fri, 21 Jul 2017 17:07:00 GMT
Issuer Let's Encrypt Authority X3
Open full certificate details
Certificate Transparency
SCT Google 'Rocketeer' log (TLS extension, Invalid signature)
SCT Google 'Pilot' log (TLS extension, Invalid signature)
Show full details
The security details above are from the first inspected response.
Console What's New
Highlights from Chrome 59 update
CSS and JS code coverage
Find unused CSS and JS with the new Coverage drawer.
Full-page screenshots
Take a screenshot of the entire page, from the top of the viewport to the bottom.
Block requests


WOMAGAzine-ウーマガジン-
Secure https://womagazine.jp
This page is in Japanese Would you like to translate it? Nope Translate Options
WOMAGAzine
ホーム ダイエット 美容 ファッション
休日に足を運んで食べに行きたいっ♪ 最旬の「抹茶スイーツ」が食べられるお店をご紹介...
1699 Views
5月5日の注目記事
出会いは美BODYが引き寄せる!?1ヶ月10キロも可能な痩身エステで、見事別人
寝坊しても大丈夫！「10分」でかわいくなれる簡単メイク術
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://womagazine.jp
Non-Secure Origins
chrome-extension://nffaoalbilbmmfgbnbgppjih
Secure Origins
https://www.google-analytics.com
https://uh.nakanohito.jp
https://pagead2.googlesyndication.com
https://platform.twitter.com
https://connect.facebook.net
https://googleads.g.doubleclick.net
Subject womagazine.jp
SAN womagazine.jp
www.womagazine.jp
Valid From Sat, 22 Apr 2017 17:07:00 GMT
Valid Until Fri, 21 Jul 2017 17:07:00 GMT
Issuer Let's Encrypt Authority X3
Open full certificate details
Certificate Transparency
SCT Google 'R keteer' log (TLS extension, Invalid signature)
SCT Google 'P log (TLS extension, Invalid signature)
Show full deta
The security details above are from the first inspected response.
Console What's New
Highlights from Chrome 59 update
CSS and JS code coverage
Find unused CSS and JS with the new Coverage drawer.
Full-page screenshots
Take a screenshot of the entire page, from the top of the viewport to the bottom.
Block requests

105 Certificates, 91 Let's Encrypt



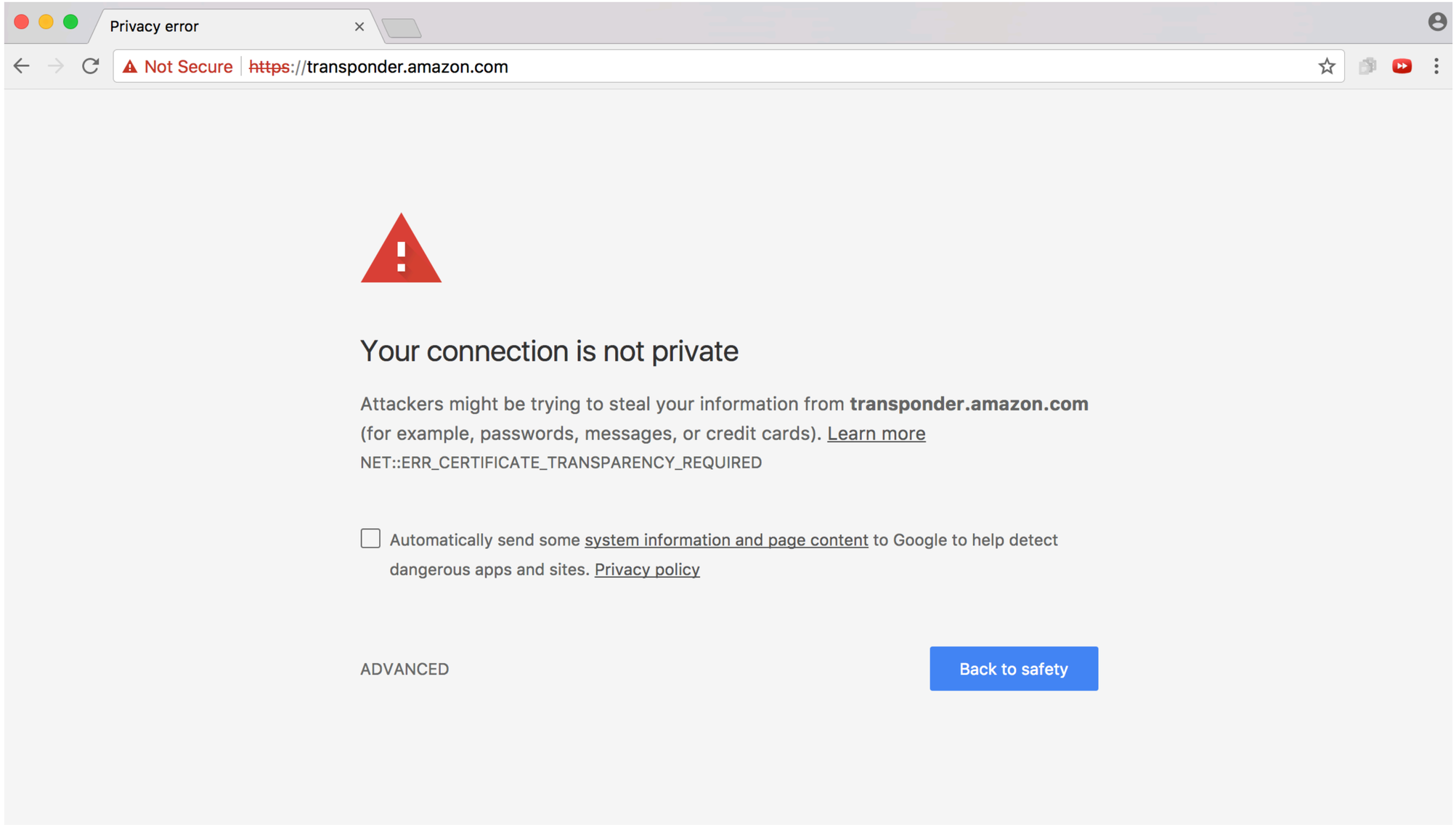

Folkehelseinstituttet - FHI
Secure https://www.fhi.no
This page is in Norwegian Would you like to translate it? Nope Translate Options
folkehelse
MENY
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.fhi.no
Secure Origins
https://www.google-analytics.com
https://www.googletagmanager.com
https://www.googleadservices.com
https://connect.facebook.net
https://googleads.g.doubleclick.net
https://www.google.com
https://www.facebook.com
Unknown / Canceled
https://code.jquery.com
SAN www.fhi.no
admin.fhi.no
Show more (4 total)
Valid From Thu, 09 Jun 2016 12:32:36 GMT
Valid Until Sat, 09 Jun 2018 21:59:00 GMT
Issuer Buypass Class 3 CA 2
Open full certificate details
Certificate Transparency
SCT Google 'Aviator' log (Embedded in certificate, Invalid signature)
SCT Venafi log (Embedded in certificate, Invalid signature)
SCT Symantec log (Embedded in certificate, Invalid signature)
Show full details
The security details above are from the first inspected response.


Folkehelseinstituttet - FHI
Secure https://www.fhi.no
This page is in Norwegian Would you like to translate it? Nope Translate Options
folkehelse
MENY
Elements Console Sources Network Performance Memory Application Security Audits
Overview
Main Origin
https://www.fhi.no
Secure Origins
https://www.google-analytics.com
https://www.googletagmanager.com
https://www.googleadservices.com
https://connect.facebook.net
https://googleads.g.doubleclick.net
https://www.google.com
https://www.facebook.com
Unknown / Canceled
https://code.jquery.com
SAN www.fhi.no
admin.fhi.no
Show more (4 total)
Valid From Thu, 09 Jun 2016 12:32:36 GMT
Valid Until Sat, 09 Jun 2018 21:59:00 GMT
Issuer Buypass Class 3 CA 2
Open full certificate details
Certificate Transparency
SCT (Embedded in certificate, Invalid signature)
SCT (Embedded in certificate, Invalid signature)
SCT (Embedded in certificate, Invalid signature)
Show full details
The security details above are from the first inspected response.

Log Operators

Active	Passive
Symantec log (81.26%)	Symantec log (62.78%)
Google ’Pilot’ log (79.9%)	Google ’Rocketeer’ log (58.6%)
Google ’Rocketeer’ log (31.72%)	Google ’Pilot’ log (58.48%)
DigiCert Log Server (26.96%)	Google ’Icarus’ log (14.37%)
Google ’Aviator’ log (25.67%)	Google ’Aviator’ log (9.39%)
Google ’Skydiver’ log (8.32%)	Vena log (7.47%)
Symantec VEGA log (3.98%)	WoSign ctlog (4.64%)
StartCom CT log (1.49%)	DigiCert Log Server (4.07%)
WoSign ctlog (0.67%)	Google ’Skydiver’ log (1.7%)

Log Operators



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
        Validity
            Not Before: May 30 00:00:00 2016 GMT
            Not After : May 30 00:00:00 2018 GMT
        Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=*.cloudfront.net
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:cloudfront.net, DNS:*.cloudfront.net
            X509v3 Basic Constraints:
                CA:FALSE
            Authority Information Access:
                OCSP - URI:http://ss.symcd.com
                CA Issuers - URI:http://ss.symcb.com/ss.crt

            CT Precertificate SCTs:
                ..Random string goes here
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
        Validity
            Not Before: May 30 00:00:00 2016 GMT
            Not After : May 30 00:00:00 2018 GMT
        Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=*.cloudfront.net
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:cloudfront.net, DNS:*.cloudfront.net
            X509v3 Basic Constraints:
                CA:FALSE
            Authority Information Access:
                OCSP - URI:http://ss.symcd.com
                CA Issuers - URI:http://ss.symcb.com/ss.crt

            CT Precertificate SCTs:
                ..Random string goes here
```

```
 853:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 CRL Distribution Points
 858:d=5  hl=2 l=  36 prim: OCTET STRING      [HEX DUMP]:30223020A01EA01C861A687474703A2F2F73732E73796D63622E636F6D2F73732E63726C
 896:d=4  hl=2 l=  87 cons: SEQUENCE
 898:d=5  hl=2 l=   8 prim: OBJECT            :Authority Information Access
 908:d=5  hl=2 l=  75 prim: OCTET STRING      [HEX DUMP]:3049301F06082B06010505073001861368747470 3A2F2F73732E73796D63642E636F6D30260
D63622E636F6D2F73732E637274
 985:d=4  hl=2 l=  39 cons: SEQUENCE
 987:d=5  hl=2 l=  10 prim: OBJECT            :CT Precertificate SCTs
 999:d=5  hl=2 l=  25 prim: OCTET STRING      [HEX DUMP]:0C1752616E646F6D20737472696E6720676F65732068657265
```

```
 853:d=5  hl=2 l=   3 prim: OBJECT            :X509v3 CRL Distribution Points
 858:d=5  hl=2 l=  36 prim: OCTET STRING      [HEX DUMP]:30223020A01EA01C861A687474703A2F2F73732E73796D63622E636F6D2F73732E63726C
 896:d=4  hl=2 l=  87 cons: SEQUENCE
 898:d=5  hl=2 l=   8 prim: OBJECT            :Authority Information Access
 908:d=5  hl=2 l=  75 prim: OCTET STRING      [HEX DUMP]:3049301F06082B06010505073001861368747470 3A2F2F73732E73796D63642E636F6D30260
D63622E636F6D2F73732E637274
 985:d=4  hl=2 l=  39 cons: SEQUENCE
 987:d=5  hl=2 l=  10 prim: OBJECT            :CT Precertificate SCTs
 999:d=5  hl=2 l=  25 prim: OCTET STRING      [HEX DUMP]:0C1752616E646F6D20737472696E6720676F65732068657265
```

```
$ openssl asn1parse -in invalidsct.crt -inform der -strparse 999
    0:d=0  hl=2 l=  23 prim: UTF8STRING        :Random string goes here
```

Normal SCT

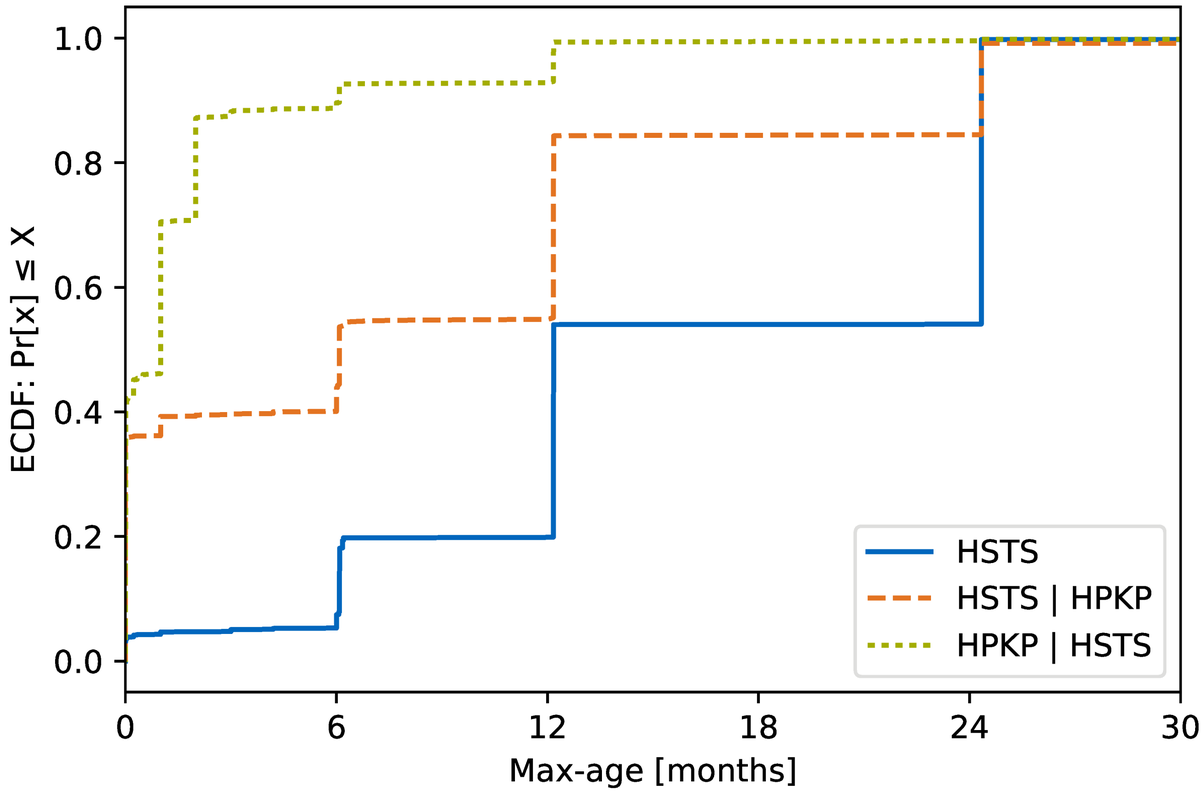
```
CT Precertificate SCTs:
    Signed Certificate Timestamp:
        Version   : v1(0)
        Log ID    : DD:EB:1D:2B:7A:0D:4F:A6:20:8B:81:AD:81:68:70:7E:
                    2E:8E:9D:01:D5:5C:88:8D:3D:11:C4:CD:B6:EC:BE:CC
        Timestamp : Aug 17 17:25:11.747 2016 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:46:02:21:00:B9:6C:2B:9A:D5:C8:70:EC:CD:2E:17:
                    E6:69:5E:C0:51:47:24:D5:DE:37:CF:10:54:84:A7:D6:
                    FD:6B:A4:A6:31:02:21:00:ED:0C:E0:49:63:60:D7:26:
                    DD:DD:06:B4:80:D6:42:FC:F4:C5:74:70:C5:4F:4D:8D:
                    9F:41:61:91:BB:B1:73:86
    Signed Certificate Timestamp:
        Version   : v1(0)
        Log ID    : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
                    3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
        Timestamp : Aug 17 17:25:11.810 2016 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:45:02:21:00:C4:A9:7D:4B:93:C1:57:BB:AF:39:01:
                    D9:5B:CB:01:35:44:97:7A:9B:E9:FD:A2:F7:15:CA:F2:
                    16:4B:88:5E:AC:02:20:10:9D:1E:54:8D:3A:C1:20:65:
                    A9:25:BE:8F:00:8E:26:26:2D:D8:E7:BA:AE:48:84:19:
                    35:86:0D:B8:EC:B3:D4
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:9a:c7:3d:67:06:3a:a2:75:83:0d:fc:66:84:1c:1e
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
        Validity
            Not Before: May 30 00:00:00 2016 GMT
            Not After : May 30 00:00:00 2018 GMT
        Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=*.cloudfront.net
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:cloudfront.net, DNS:*.cloudfront.net
            X509v3 Basic Constraints:
                CA:FALSE
            Authority Information Access:
                OCSP - URI:http://ss.symcd.com
                CA Issuers - URI:http://ss.symcb.com/ss.crt

            CT Precertificate SCTs:
                ..Random string goes here
```

HSTS, HPKP

- HSTS: ~3.5% of domains
  - 0.2% send incorrect headers (misspellings, wrong attributes, …)
- HPKP: ~0.02% of domains (6,181)
  - 41 invalid



SCSV

Automatically deployed when servers/libraries update

> 96% deployment

Deployment

Mechanism	Standard-ized	Deployment Overall	Deployment Top 10K↓	Effort	Availability Risk
SCSV	2015	49.2M	6789	**none**	low
CT-x509	2013	7.0M	1788	**none**[2]	**none**
HSTS	2012	0.9M	349	low	low
CT-TLS	2013	27,759	171	high	**none**
HPKP	2015	6616	156	high	high
HPKP PL.	2012[1]	479	150	high	high
HSTS PL.	2012[1]	23,539	144	medium	medium
CAA	2013	3057	20	medium	low
TLSA	2012	973	3	high	medium
CT-OCSP	2013	191	0	low	**none**

1: Preloading list first added to Chrome in 2012

2: Requires deployment effort on CA side and a new site certificate.

Intent To Deprecate And Remove: Public Key Pinning

31 posts by 14 authors

Chris Palmer Oct 27

Primary eng (and PM) emails

palmer@chromium.org, rsleevi@chromium.org, estark@chromium.org, agl@chromium.org

Summary

Deprecate support for public key pinning (PKP) in Chrome, and then remove it entirely.

This will first remove support for HTTP-based PKP ("dynamic pins"), in which the user-agent learns of pin-sets for hosts by HTTP headers. We would like to do this in Chrome 67, which is estimated to be released to Stable on 29 May 2018.

Finally, remove support for built-in PKP ("static pins") at a point in the future when Chrome requires Certificate Transparency for all publicly-trusted certificates (not just newly-issued publicly-trusted certificates). (We don't yet know when this will be.)

Community Contributions

- PCAPs of active scans
- Active scan results, CT database dumps
- Analysis Scripts (primarily Jupyter notebooks)
- Datasets: https://mediatum.ub.tum.de/1377982
- Software:
  - goscanner (HTTPS scanner): https://github.com/tumi8/goscanner
  - extended Bro TLS support (in 2.6): https://bro.org

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

Quirin Scheitle (TUM), Oliver Gasser (TUM), Theodor Nolte (HAW Hamburg),
Johanna Amann (ICSI/Corelight/LBNL), Lexi Brent (The University of Sydney),
Georg Carle (TUM), Ralph Holz (The University of Sydney),
Thomas C. Schmidt (HAW Hamburg), Matthias Wählisch (FU Berlin)

Internet Measurement Conference (IMC) 2018

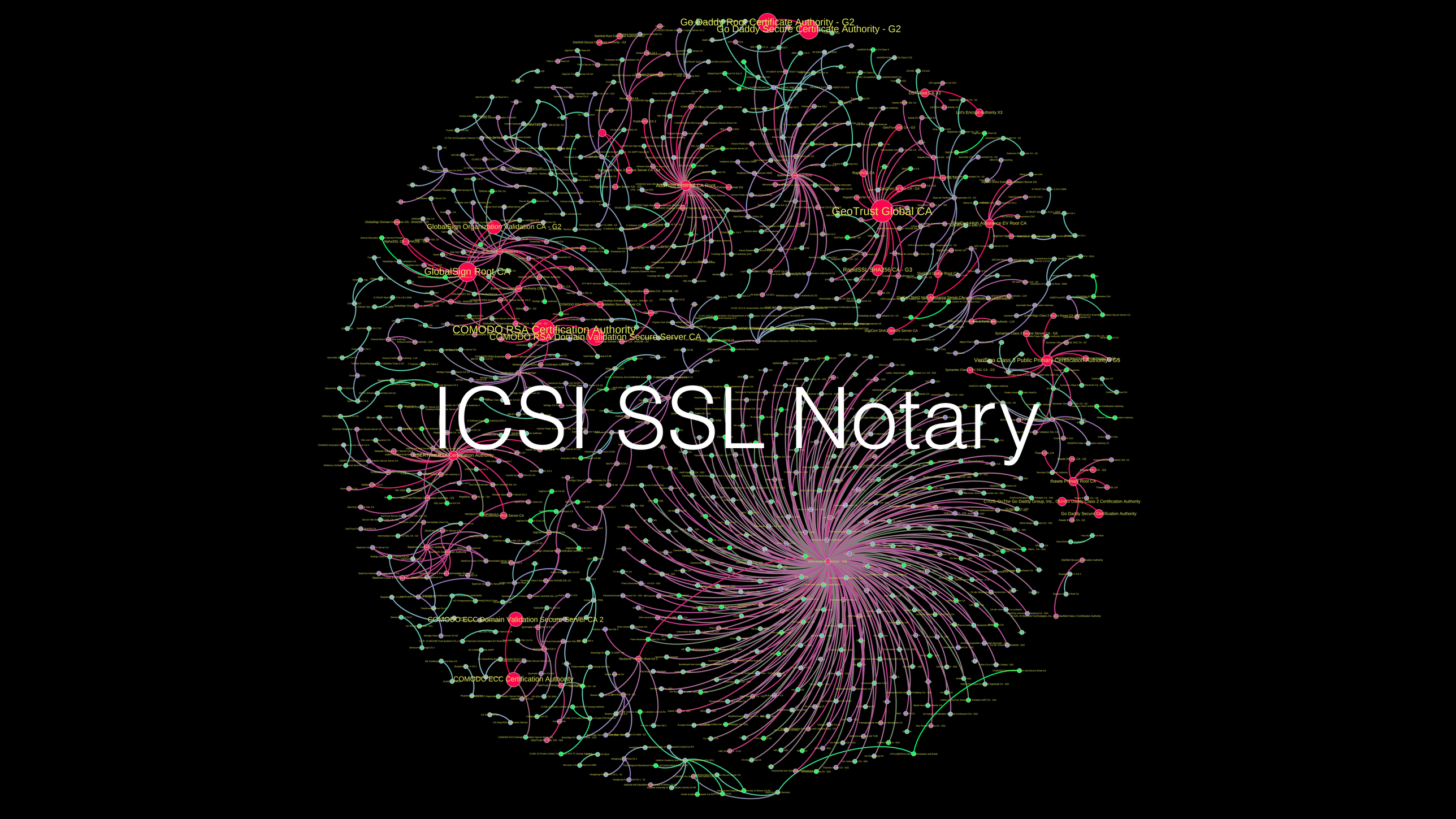
CT Honeypot

DNS Queries after 73s to 3m

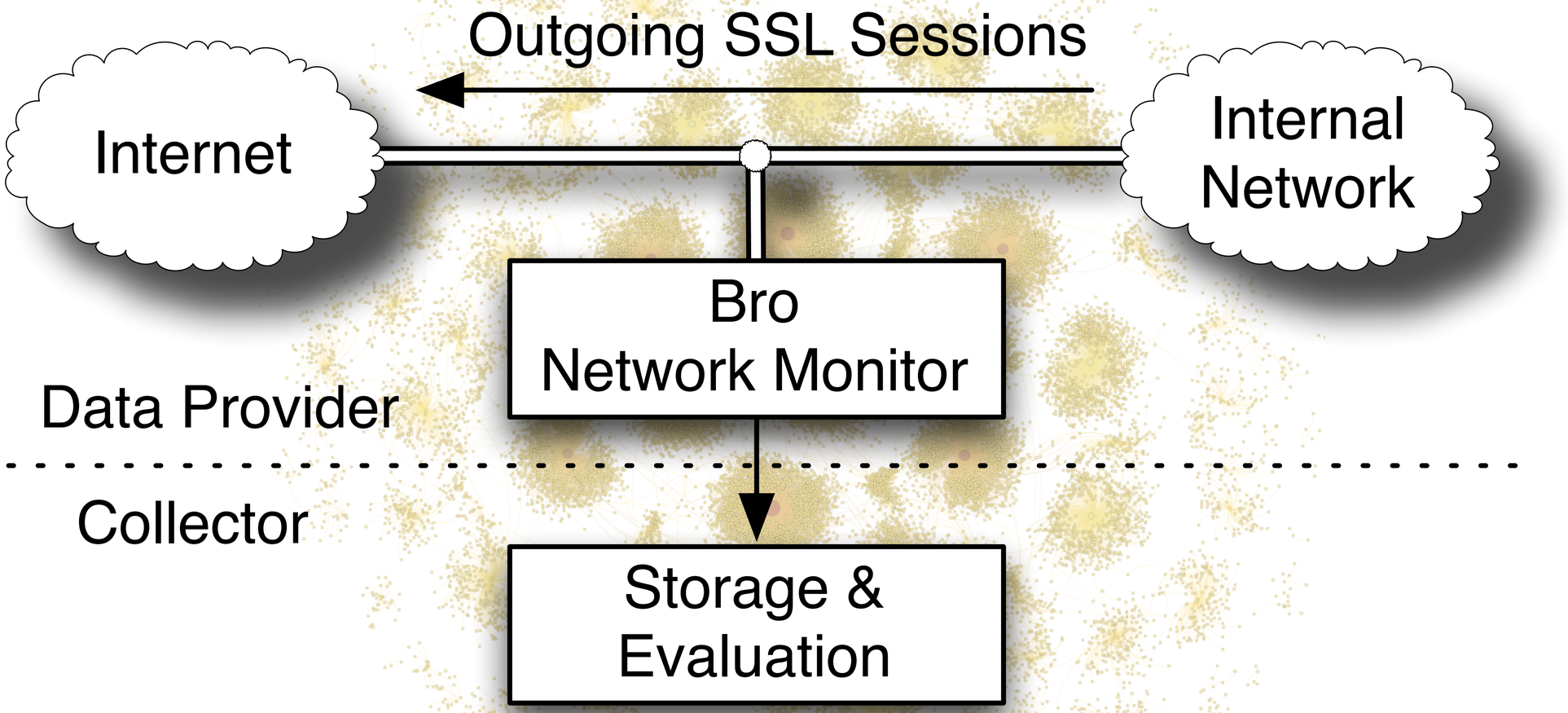
Requests from 82 ASes

Phishing Domains

e.g. 63k Domains trying to mimic Apple

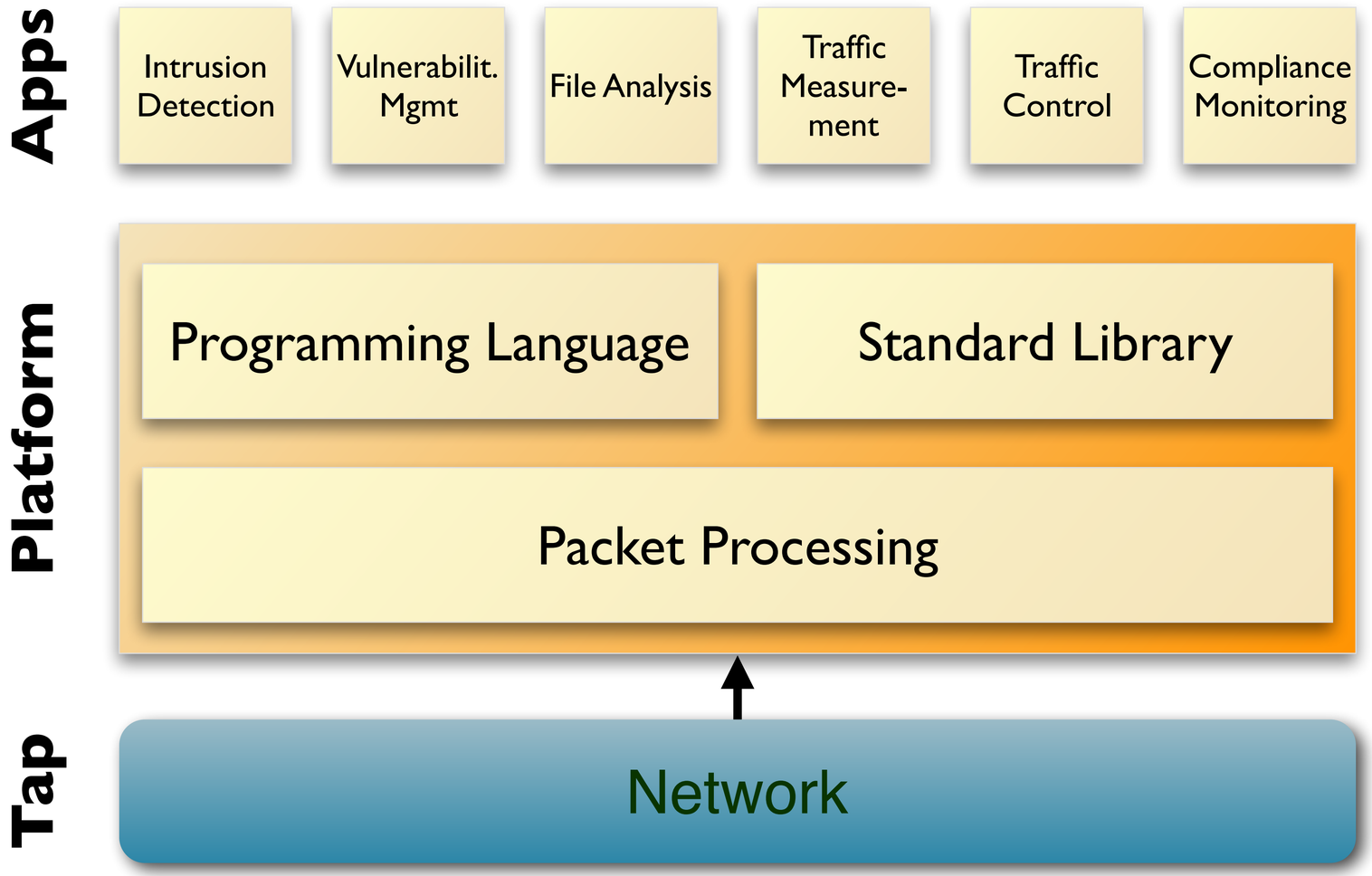

ICSI SSL Notary
Go Daddy Root Certificate Authority - G2
Go Daddy Secure Certificate Authority - G2
AddTrust External CA Root
GeoTrust Global CA
GlobalSign Root CA
GlobalSign Organization Validation CA - G2
COMODO RSA Certification Authority
COMODO RSA Domain Validation Secure Server CA
VeriSign Class 3 Public Primary Certification Authority - G5
thawte Primary Root CA
COMODO ECC Domain Validation Secure Server CA 2
COMODO ECC Certification Authority

ICSI Notary

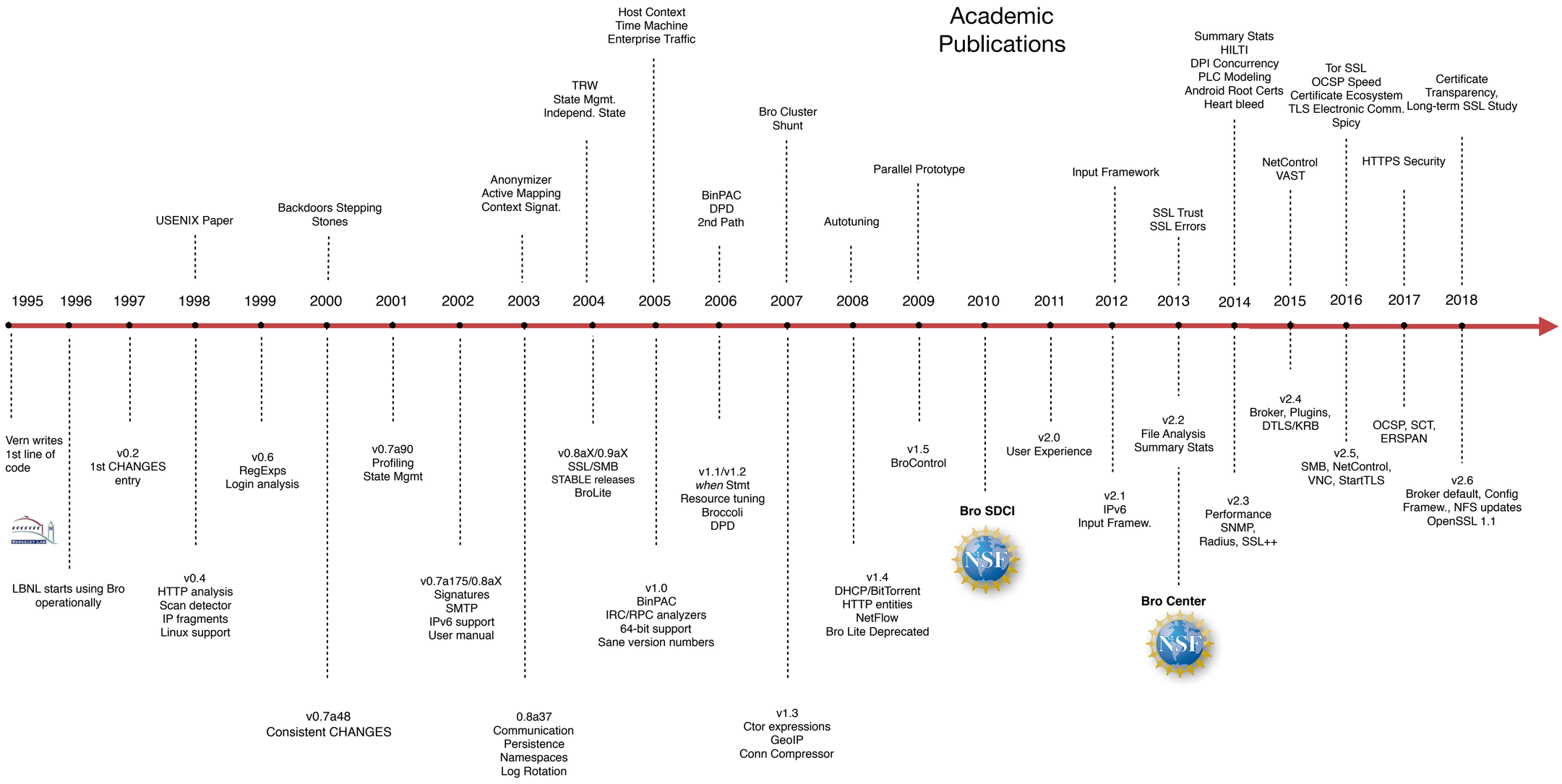

Outgoing SSL Sessions
Internet
Internal Network
Bro Network Monitor
Data Provider
Collector
Storage & Evaluation

The Zeek (Bro) Platform

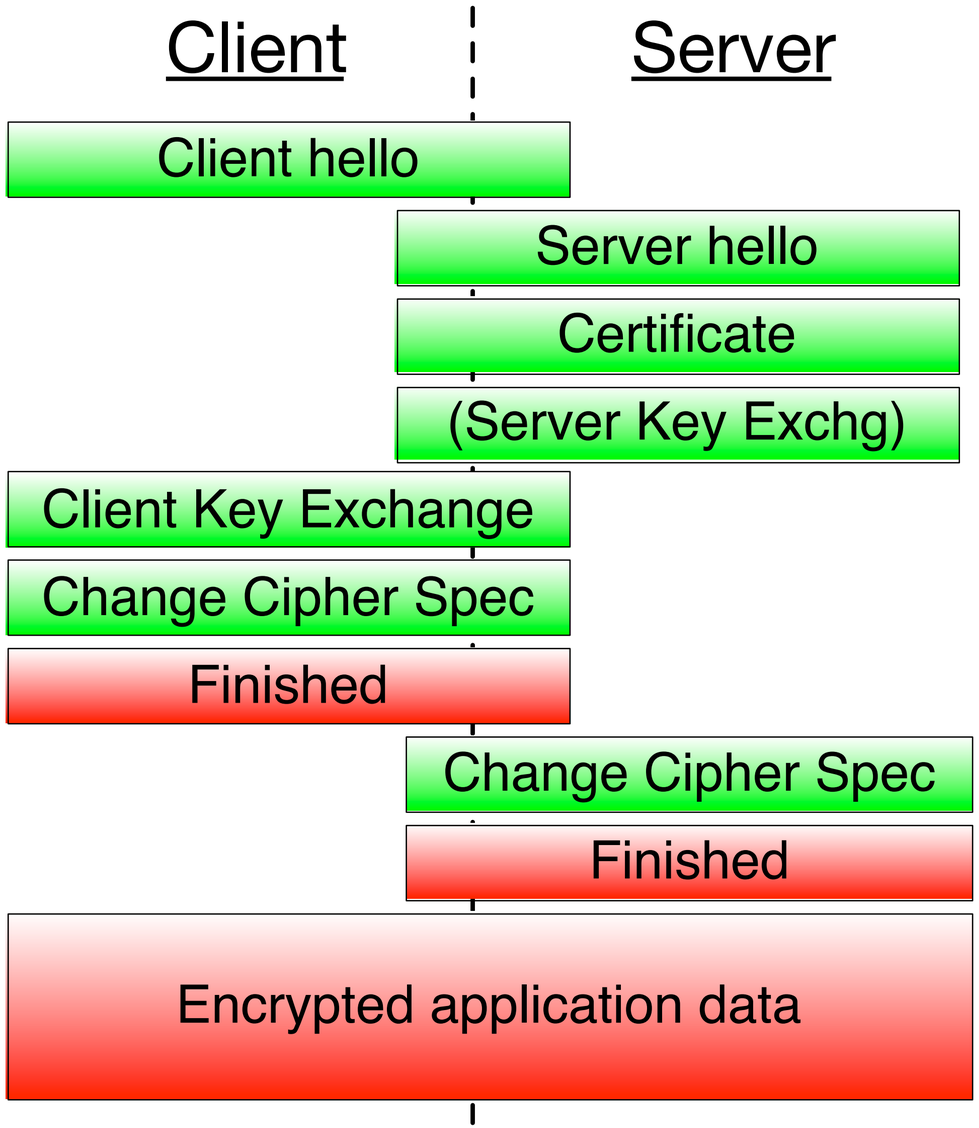
Open Source
BSD License



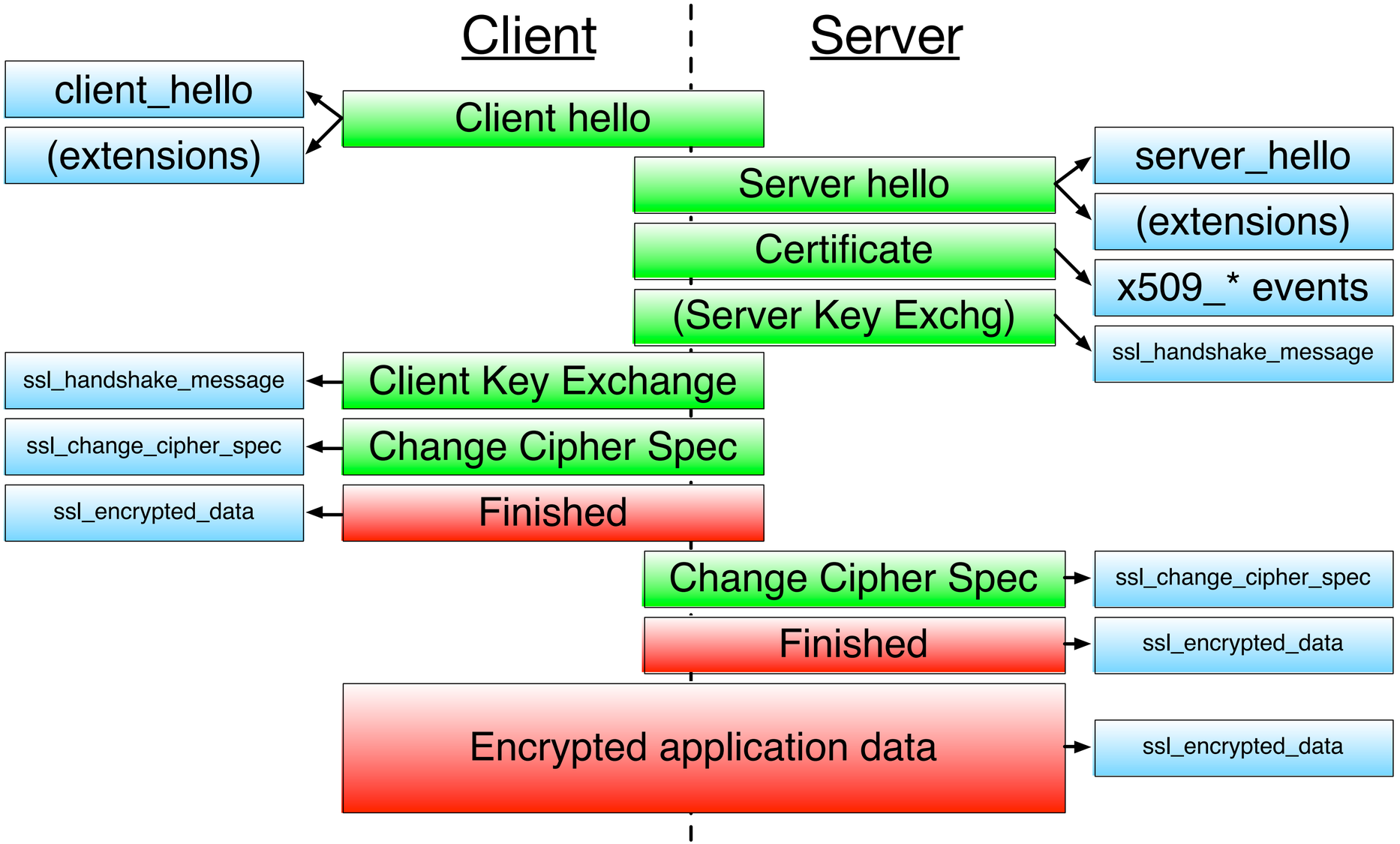
Zeek History



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

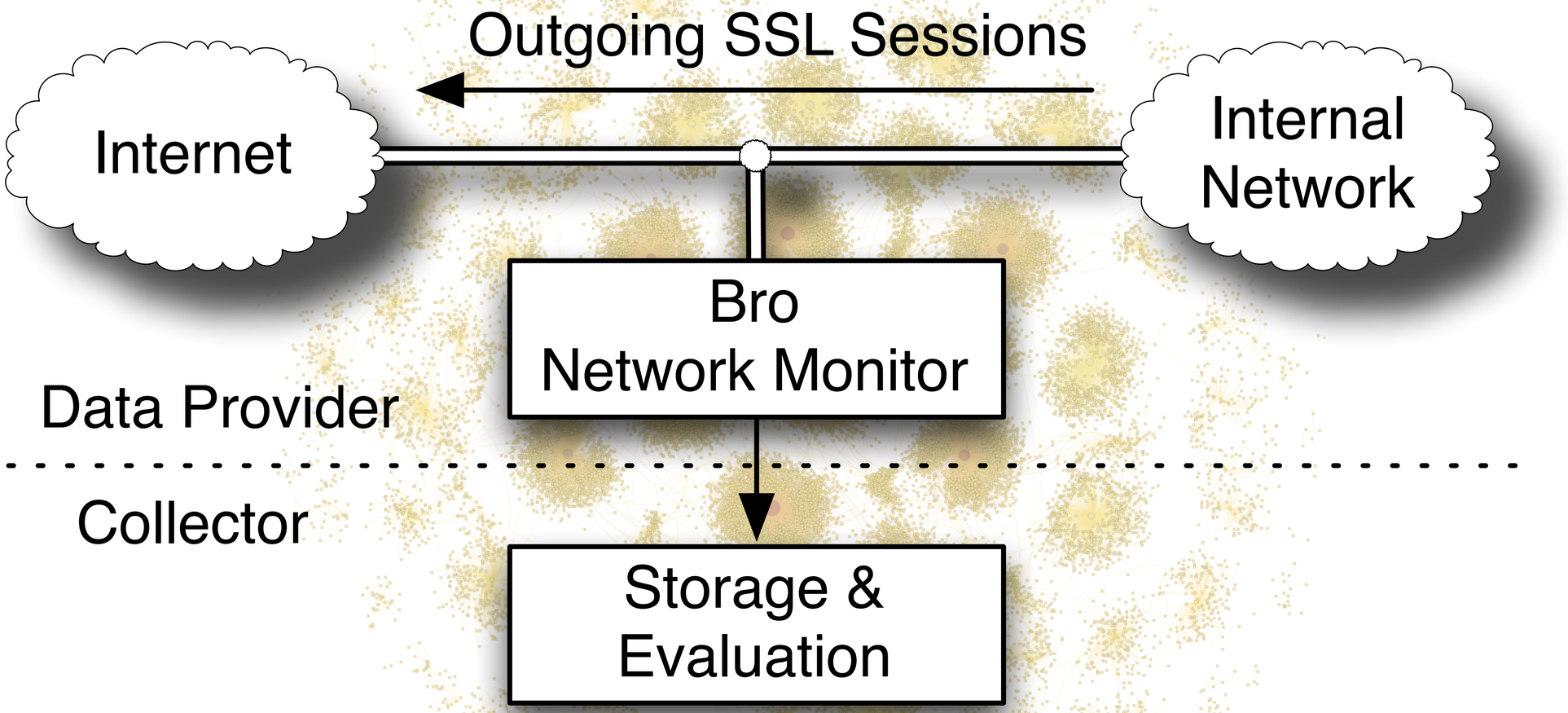
SSL


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

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

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)

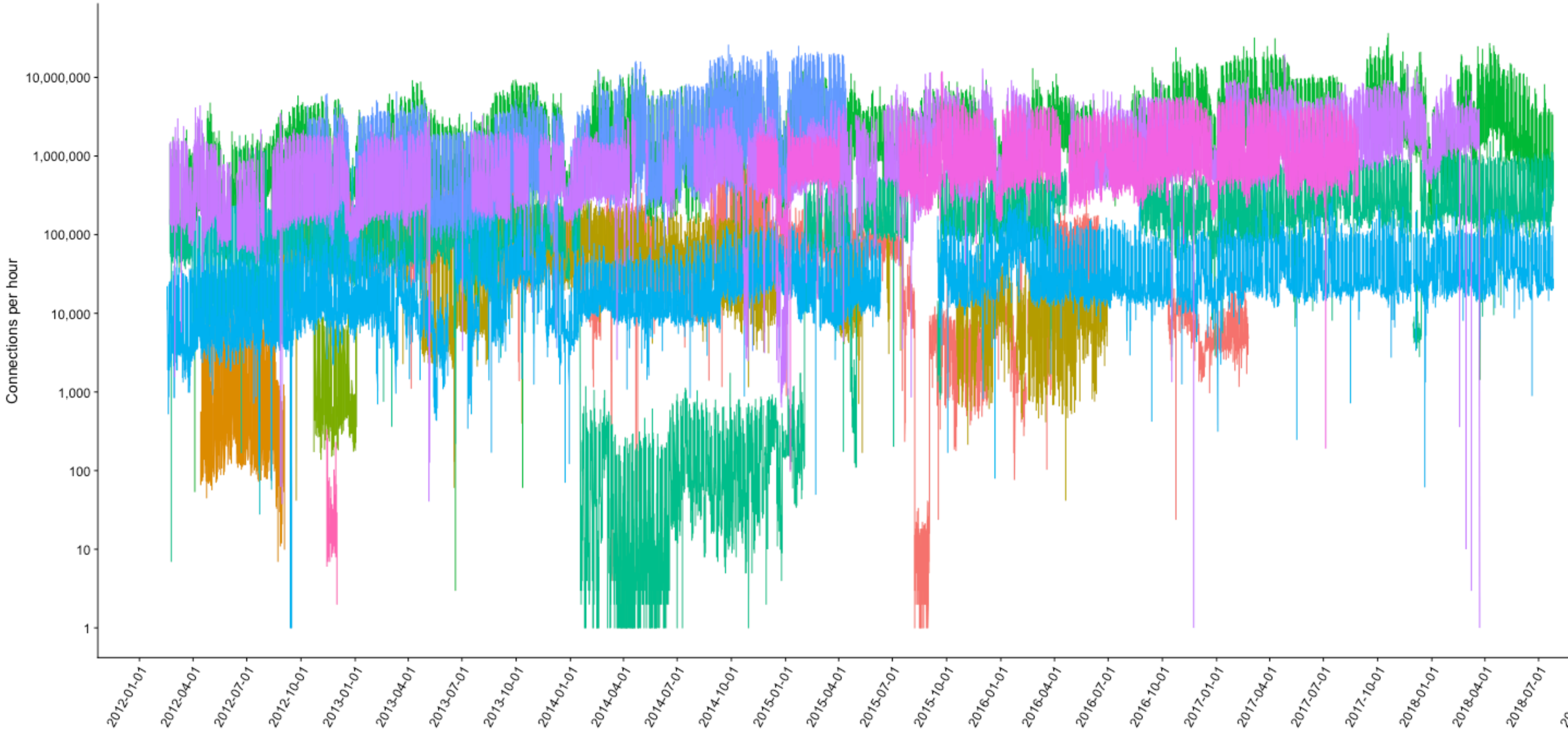
Ticket lifetime hint

Client EC curve

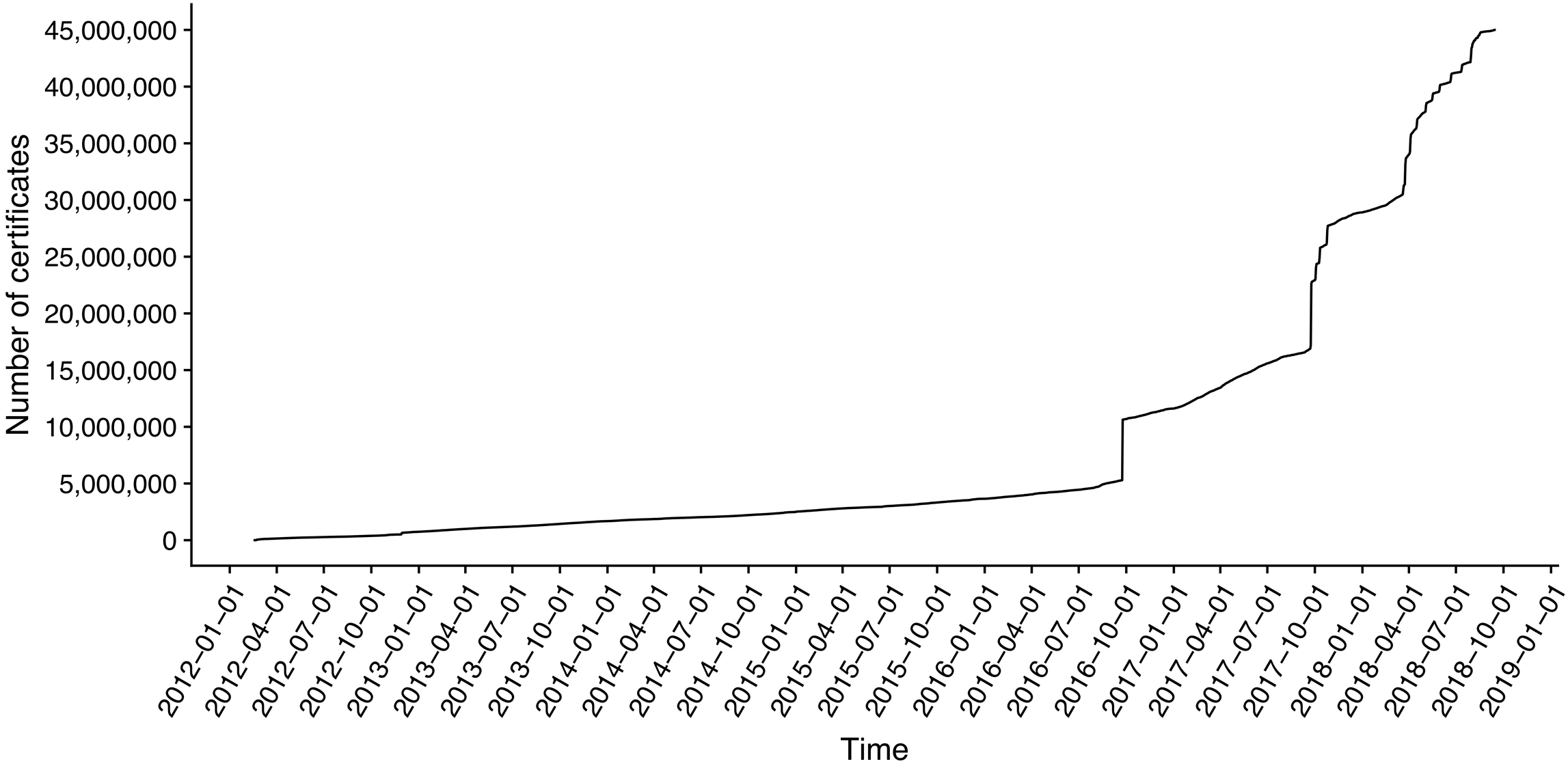
Number Client Certs

TLS Alerts

Notary - Connections



Notary - Certificates



Coming of Age:
A Longitudinal Study of TLS Deployment

Platon Kotzias	IMDEA Software Institute
Abbas Razaghpanah	Stony Brook University
Johanna Amann	ICSI
Kenneth G. Patterson	Royal Holloway University of London
Narseo Vallina-Rodriguez	ICSI/IMDEA Networks Institute
Juan Caballero	IMDEA Software Institute

Internet Measurement Conference (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

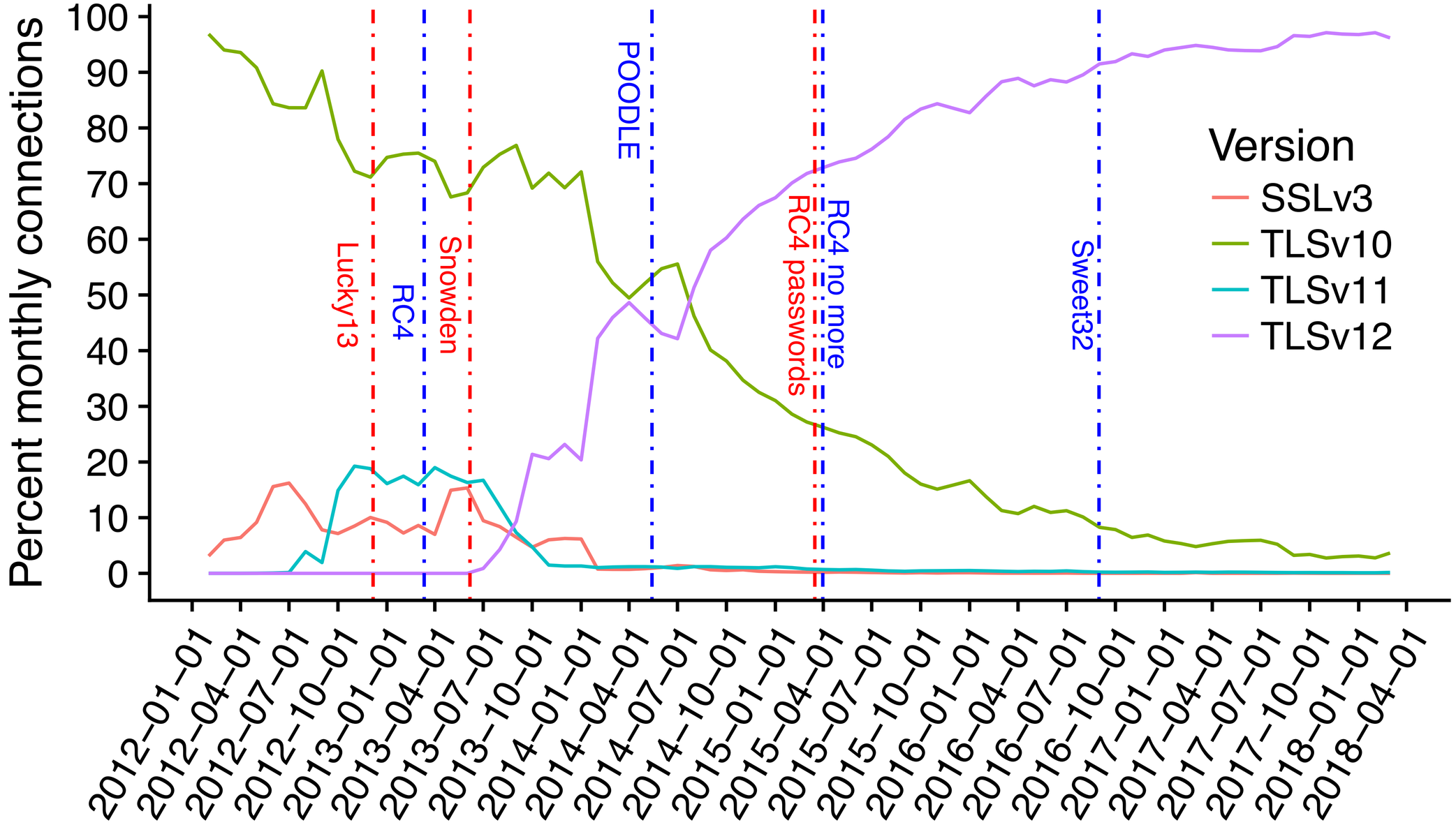
Allows an MITM attacker to attack connections if the server supports DHE_EXPORT and the client requests a DHE cipher suite.

2016

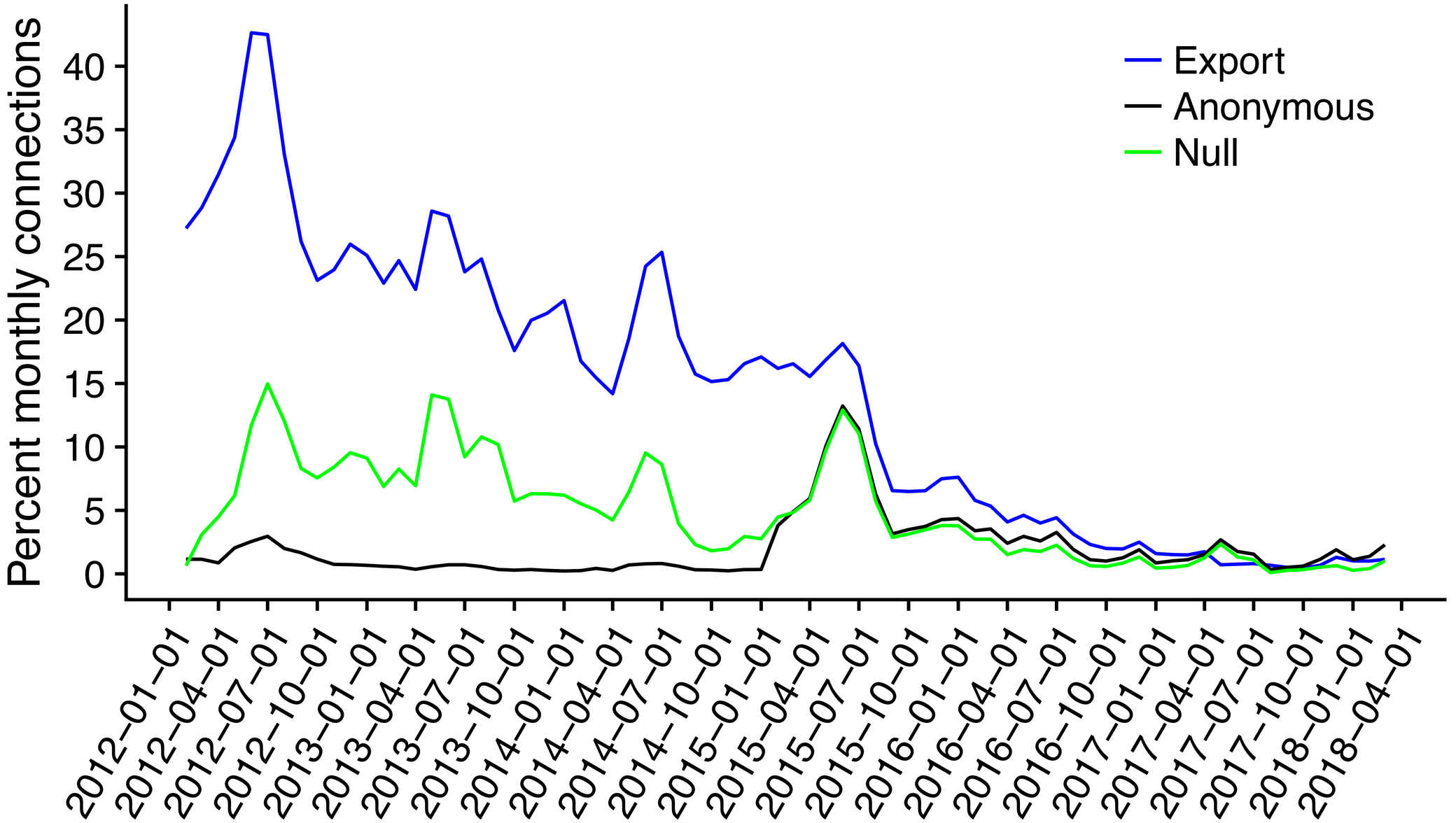
Sweet 32

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.

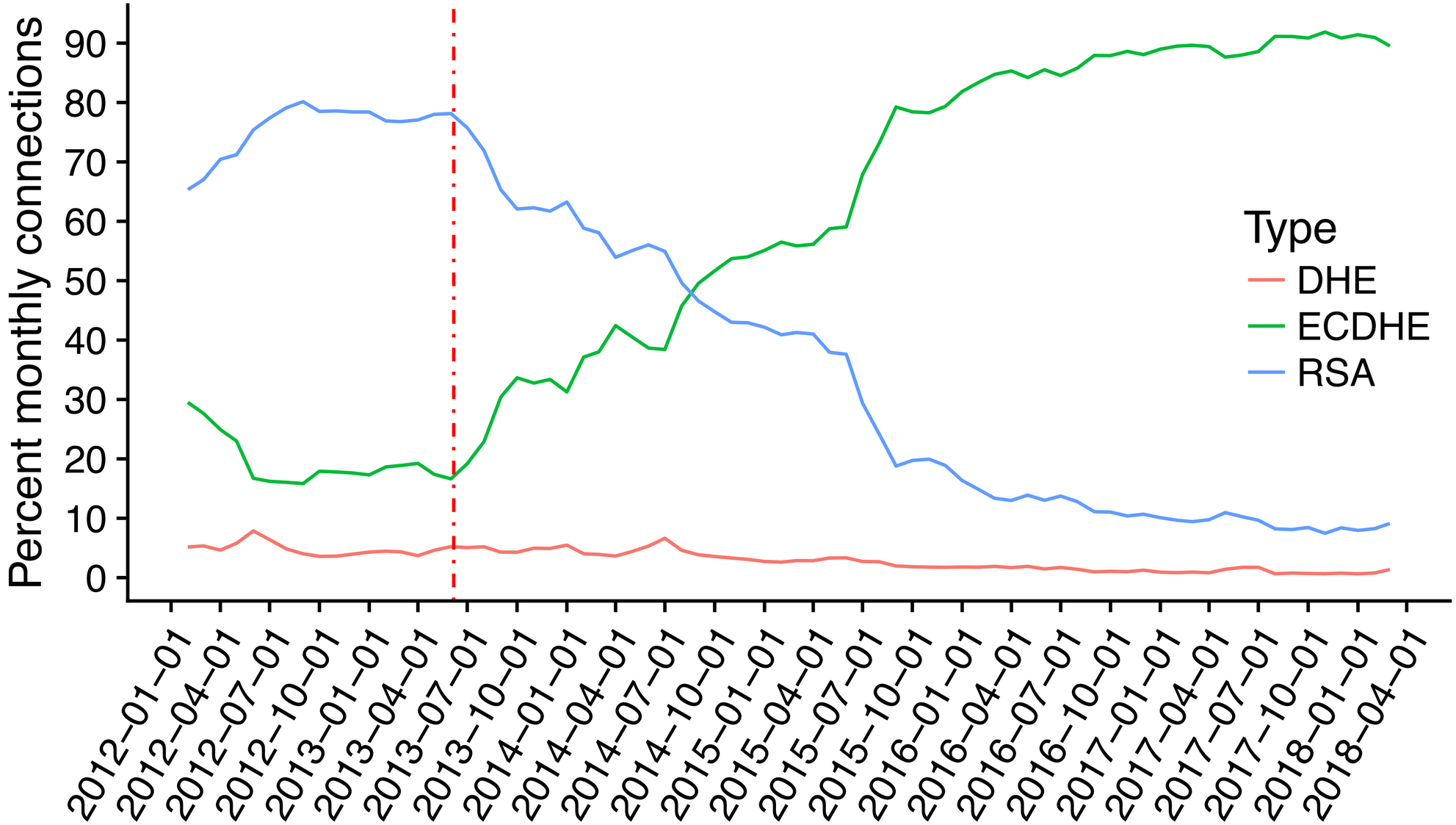
SSL Versions (negotiated)



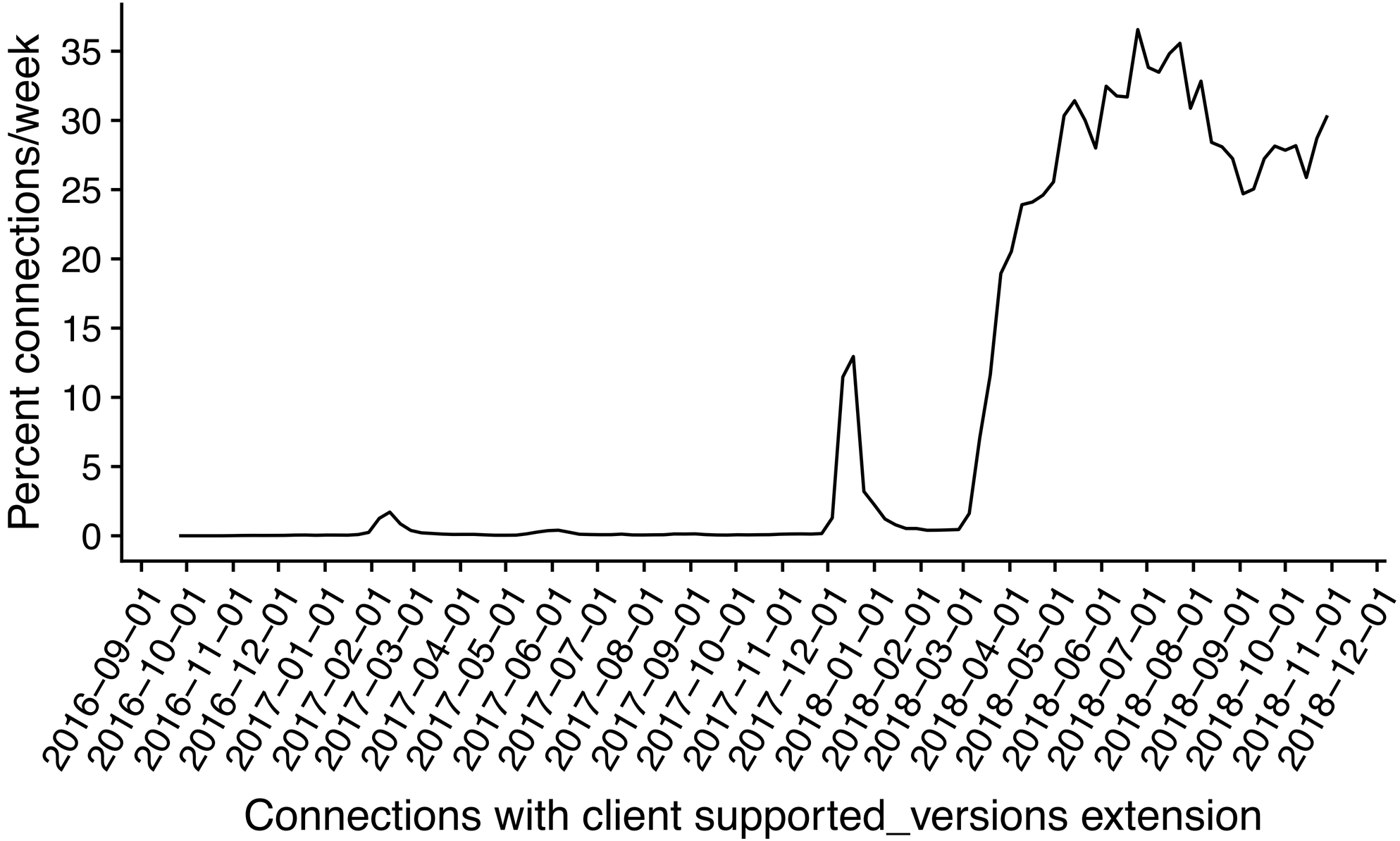
Export/Anon/NULL advertised

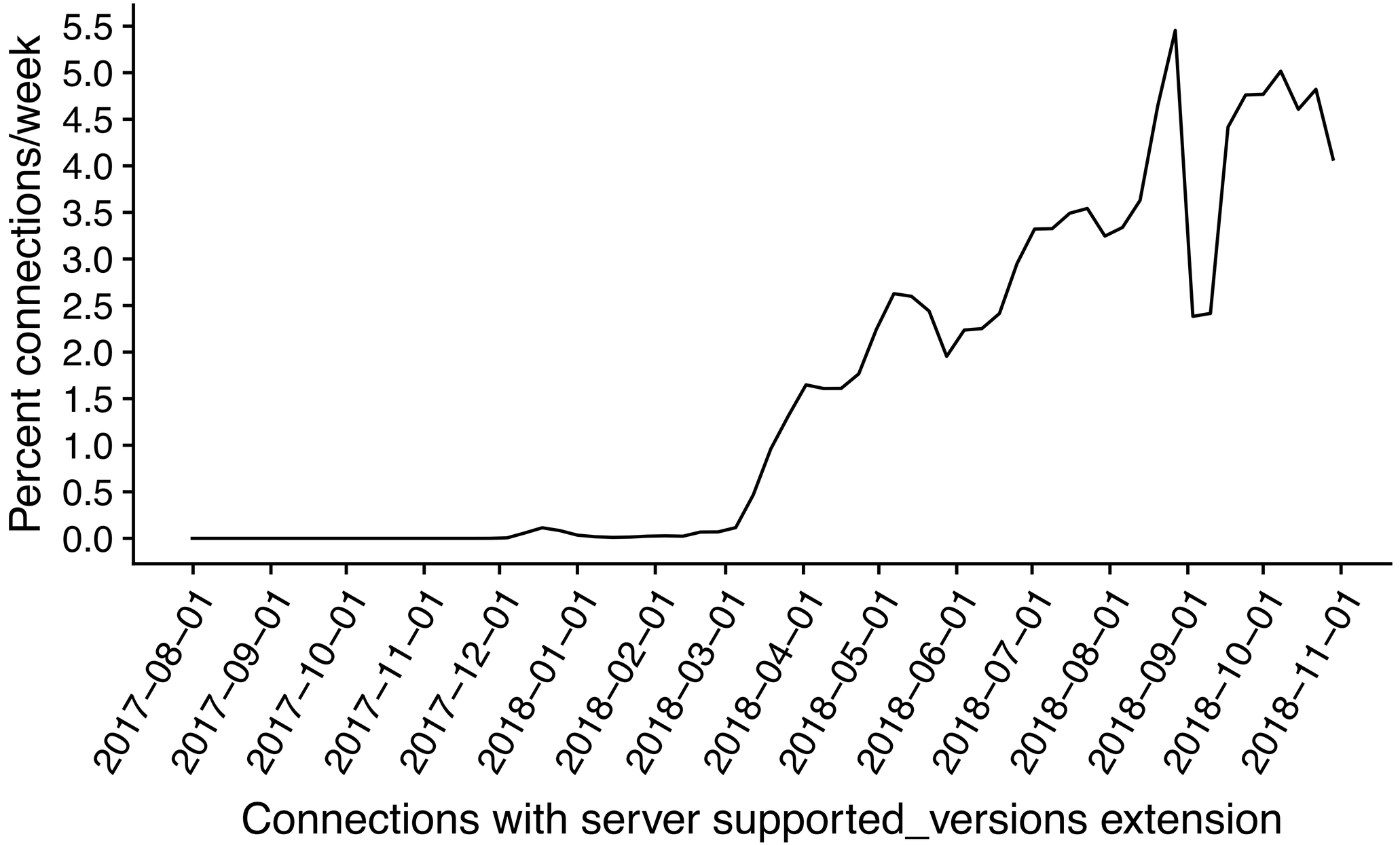


Negotiated RSA vs forward secret



TLS 1.3


Percent connections/week
0
5
10
15
20
25
30
35
2016–09–01
2016–10–01
2016–11–01
2016–12–01
2017–01–01
2017–02–01
2017–03–01
2017–04–01
2017–05–01
2017–06–01
2017–07–01
2017–08–01
2017–09–01
2017–10–01
2017–11–01
2017–12–01
2018–01–01
2018–02–01
2018–03–01
2018–04–01
2018–05–01
2018–06–01
2018–07–01
2018–08–01
2018–09–01
2018–10–01
2018–11–01
2018–12–01
Connections with client supported_versions extension


Percent connections/week
5.5
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
2017–08–01
2017–09–01
2017–10–01
2017–11–01
2017–12–01
2018–01–01
2018–02–01
2018–03–01
2018–04–01
2018–05–01
2018–06–01
2018–07–01
2018–08–01
2018–09–01
2018–10–01
2018–11–01
Connections with server supported_versions extension

Summary

- Deployment status correlates with:
  - Configuration effort
  - Risk
  - Default deployment / settings work best
- Measurements from several sites have very similar results
  - One measurement location probably good enough in most cases

Contact: johanna@icir.org