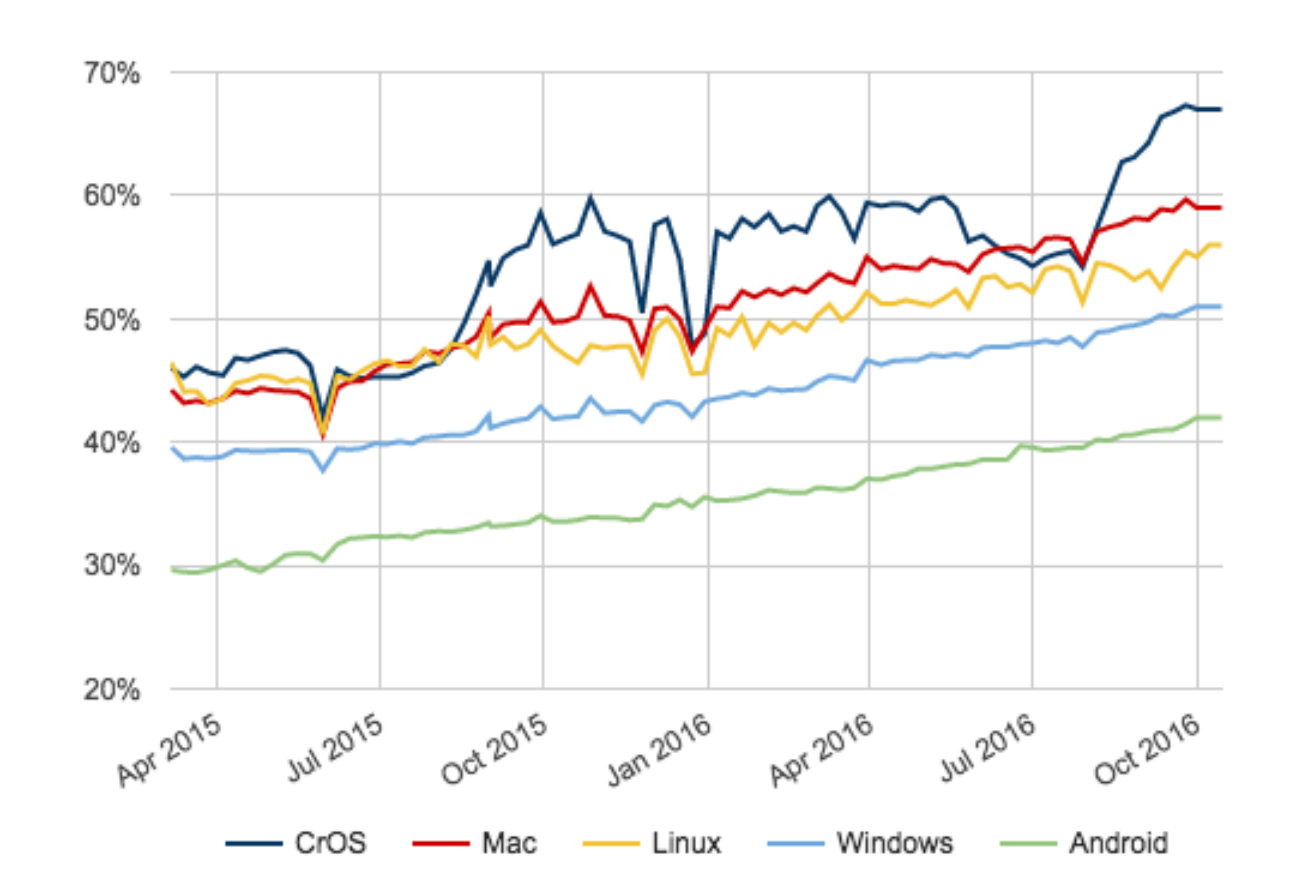
Measuring the Security Harm of TLS Crypto Shortcuts

Drew Springall, Zakir Durumeric, and J. Alex Halderman
University of Michigan

TLS on the Internet



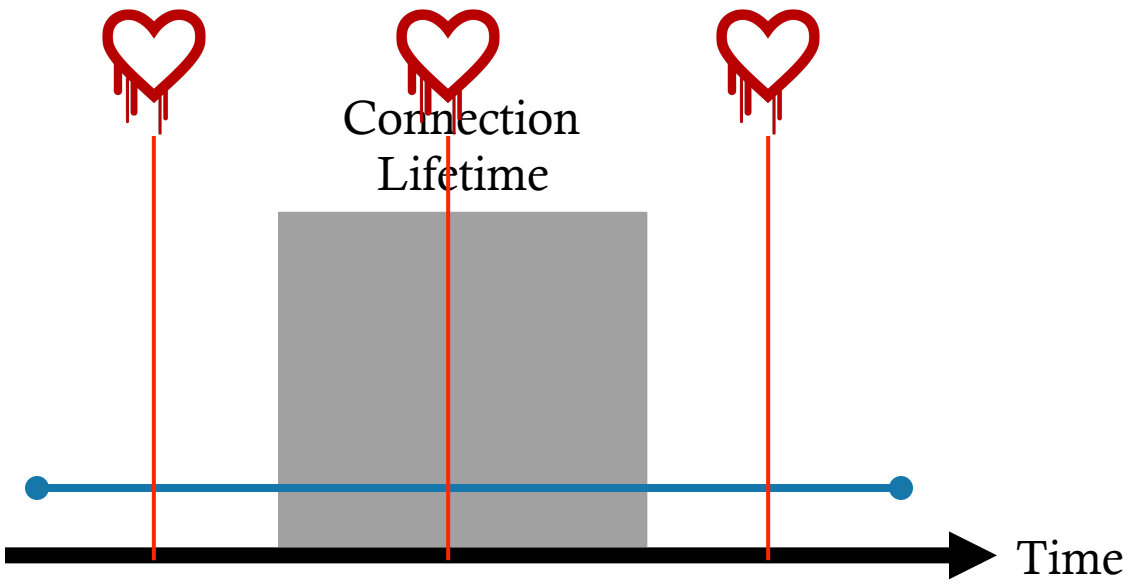
Recent TLS Vulnerabilities

- FREAK
- Logjam/WeakDH
- DROWN
- CRIME/BREACH
- BEAST
- POODLE

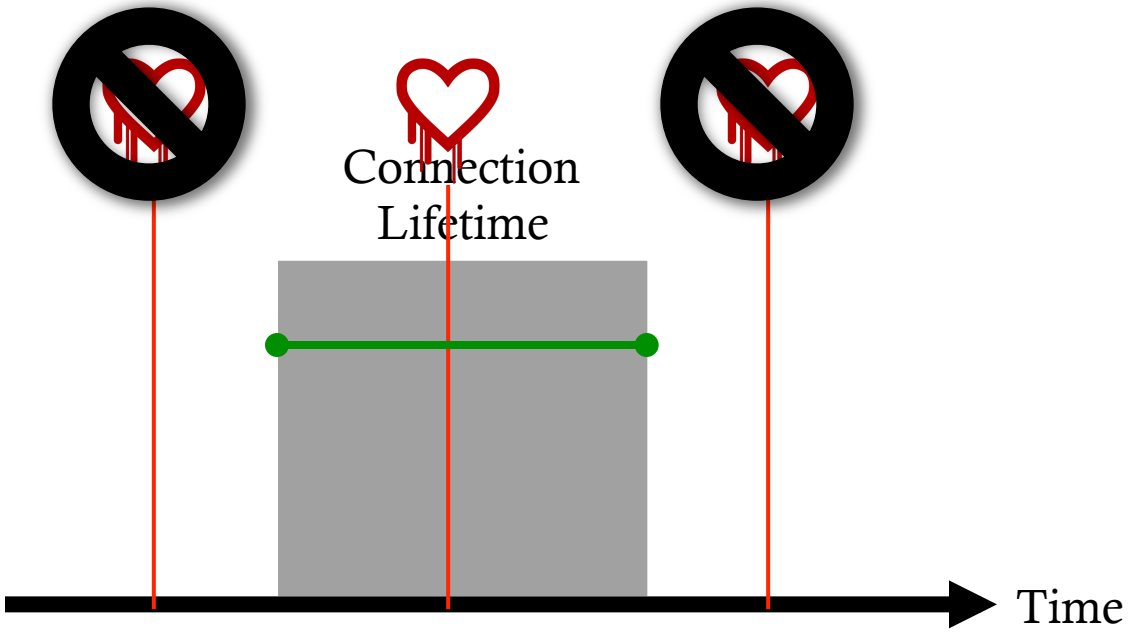
Heartbleed

- Allowed 64k memory disclosure
  - Including SSL private key
- Allowed Man-in-the-Middle attack
- Allowed retrospective decryption attacks

Exposure Window (Non-Forward Secret)



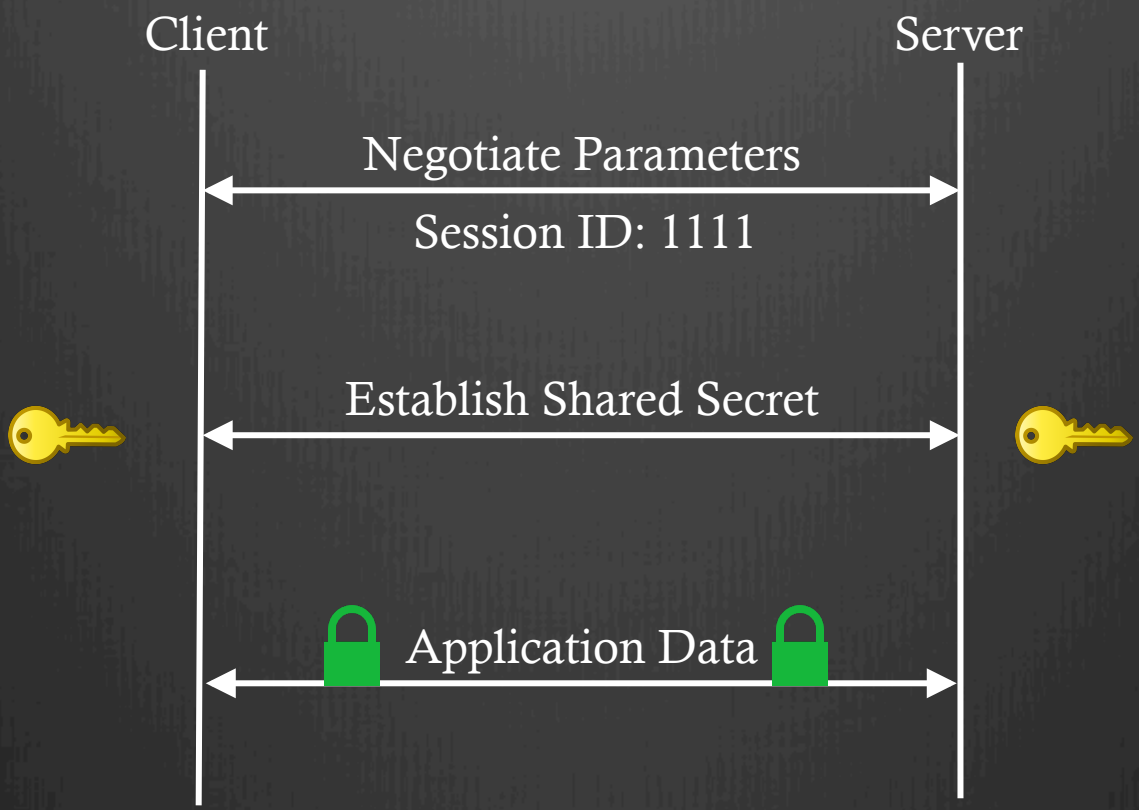
Exposure Window (Forward Secret)



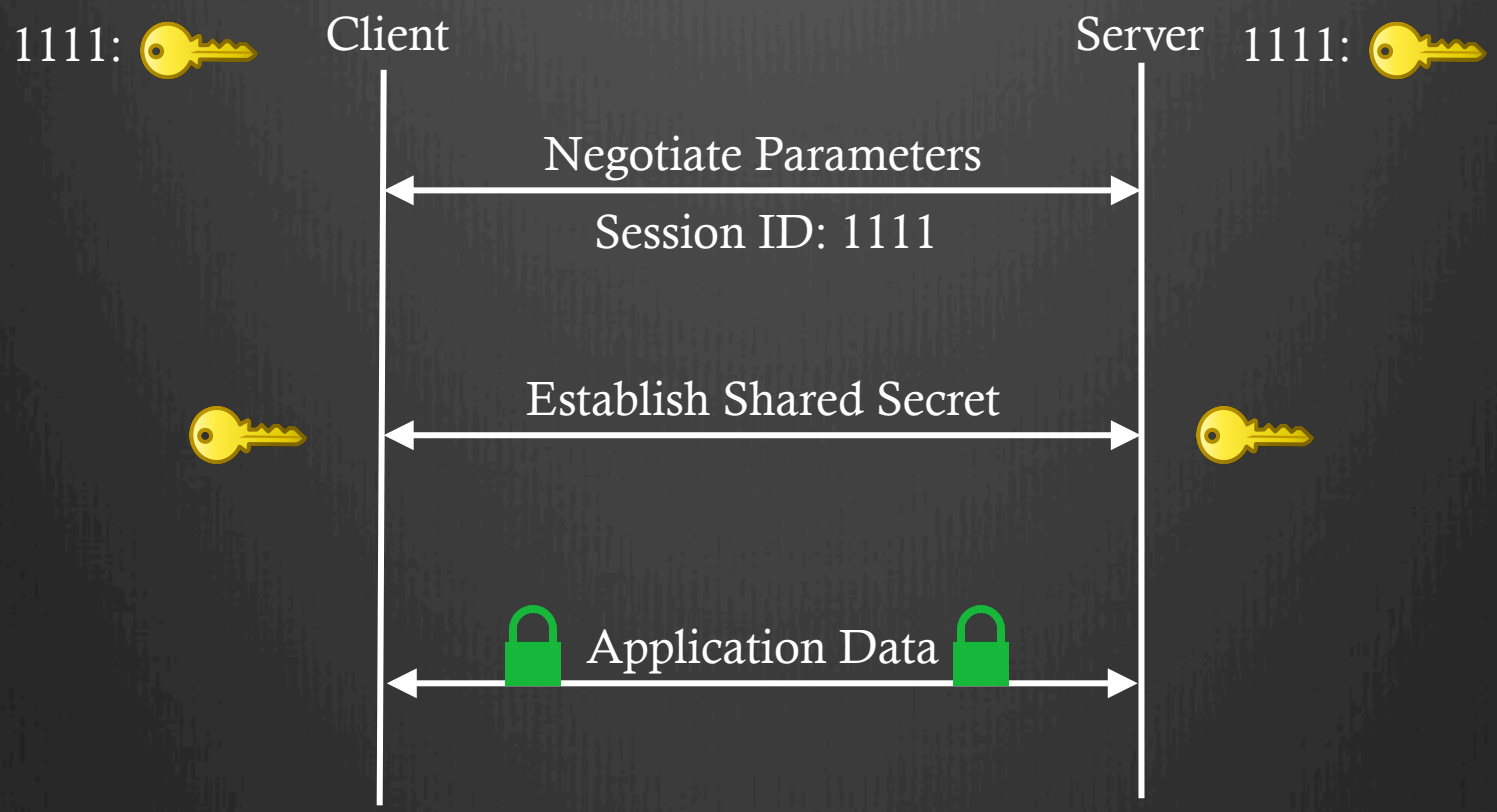
Crypto Shortcuts

- Session ID Resumption
- Session Ticket Resumption
- (EC)DHE Value Reuse

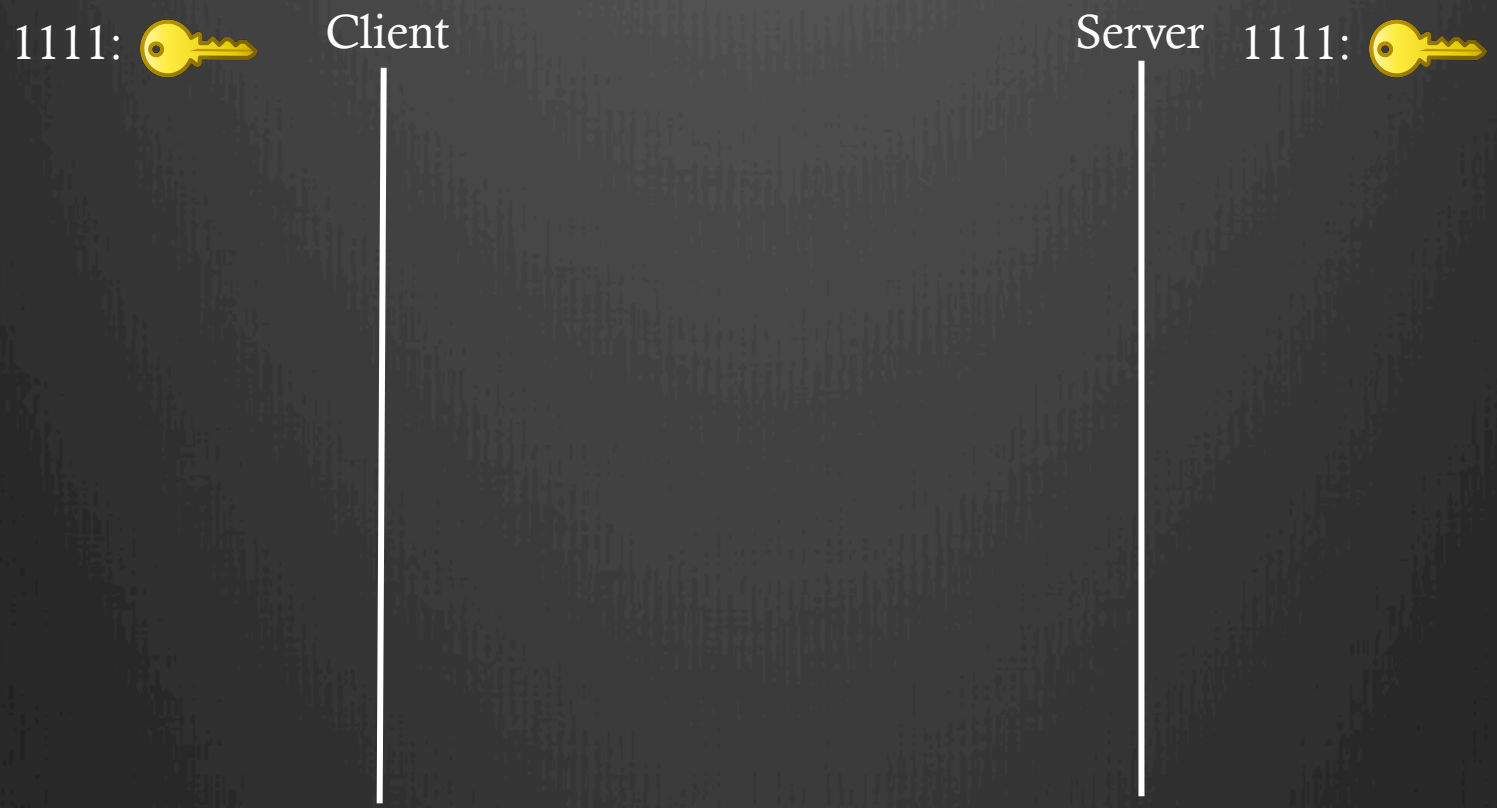
Session ID Resumption (Initial Connection)



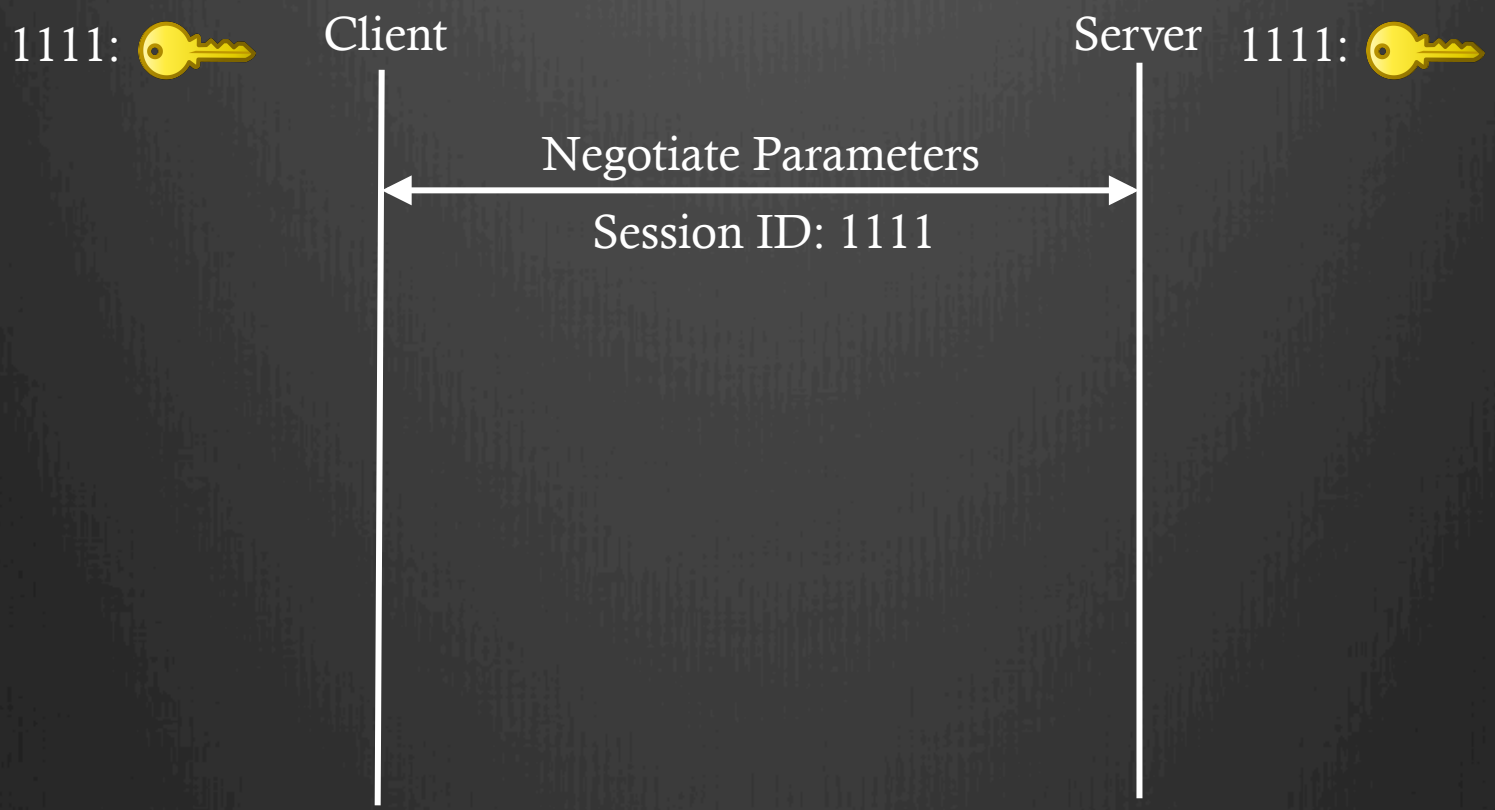
Session ID Resumption (Initial Connection)



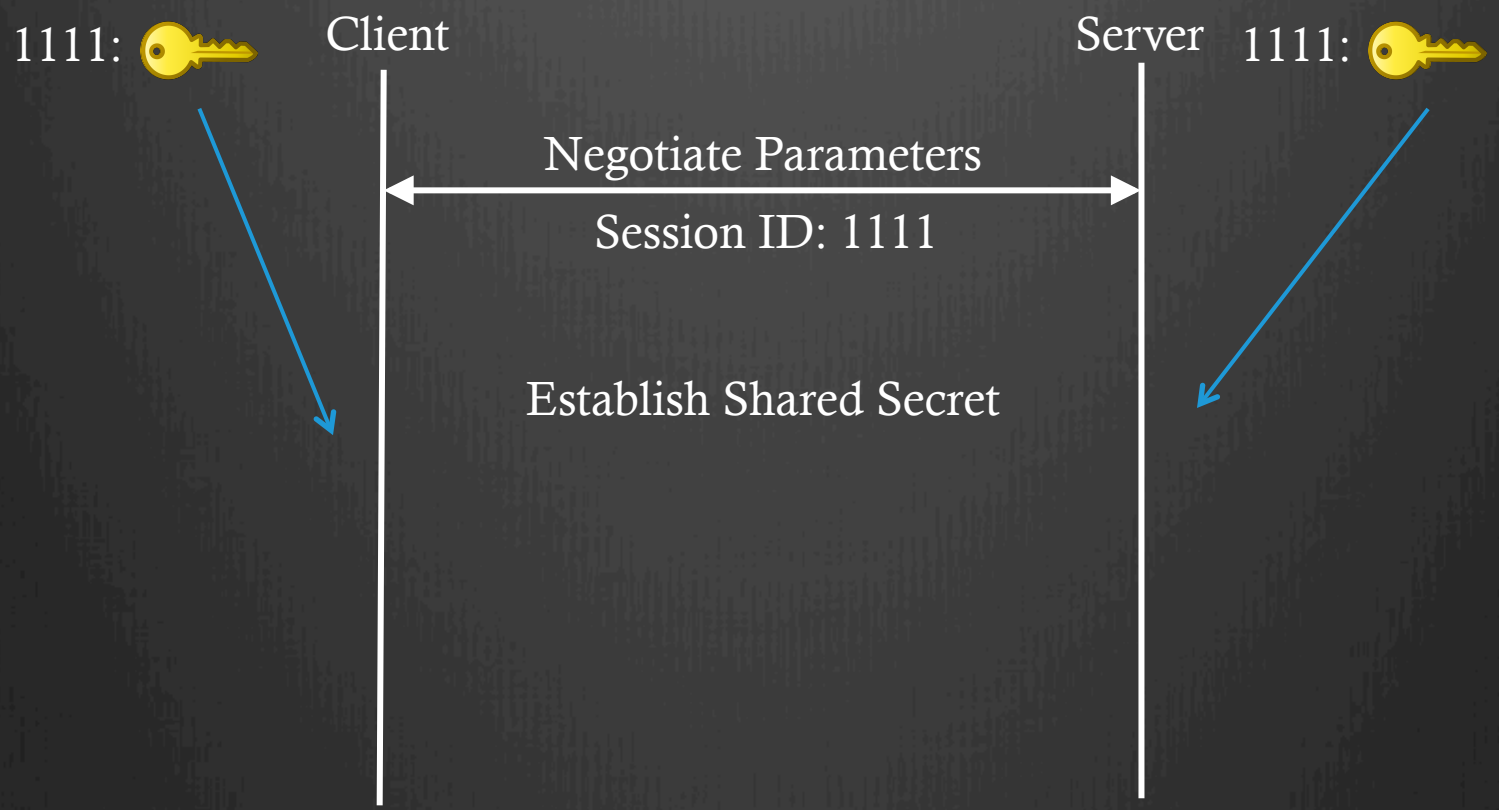
Session ID Resumption (Subsequent Connection)



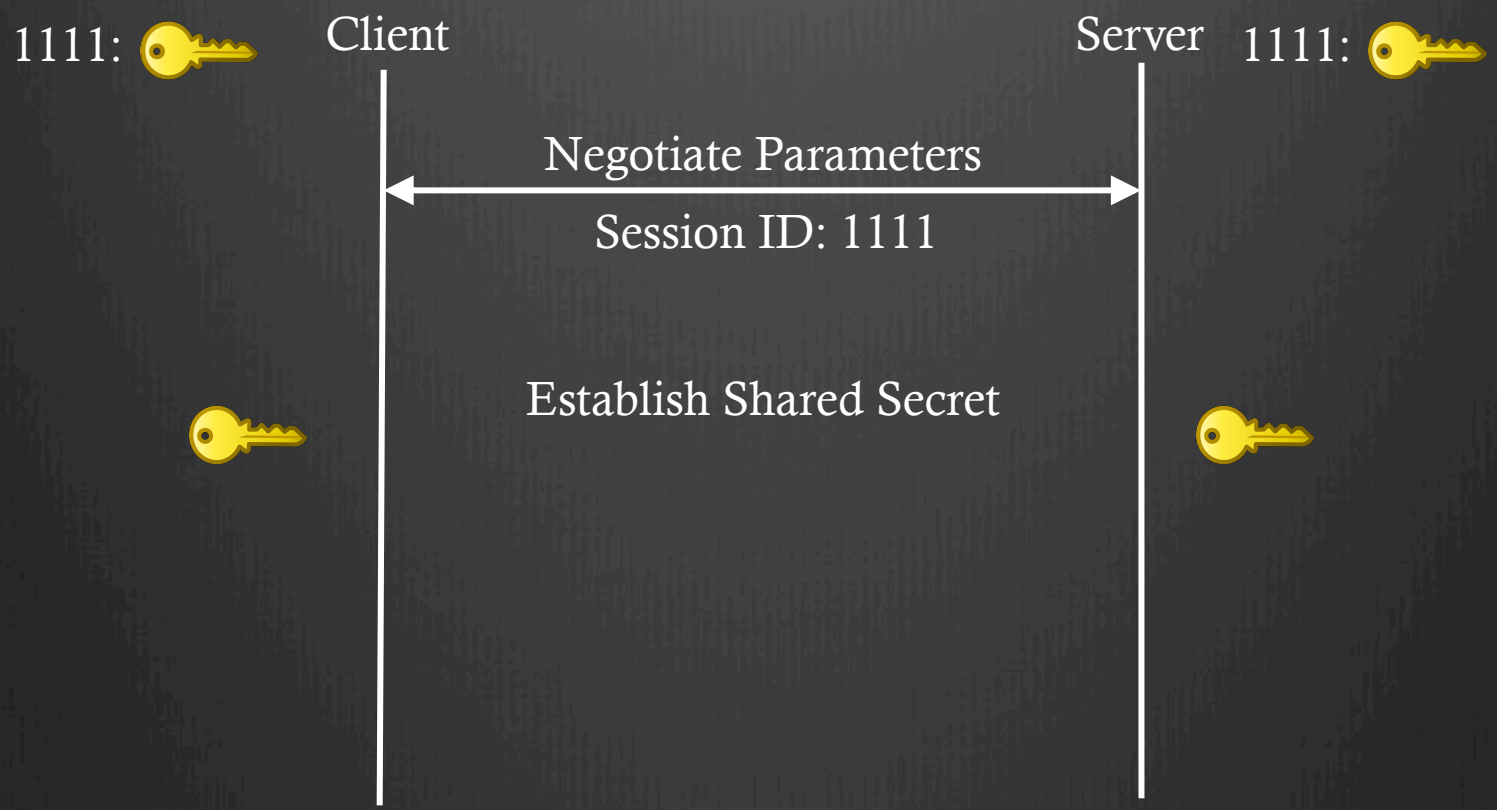
Session ID Resumption (Subsequent Connection)



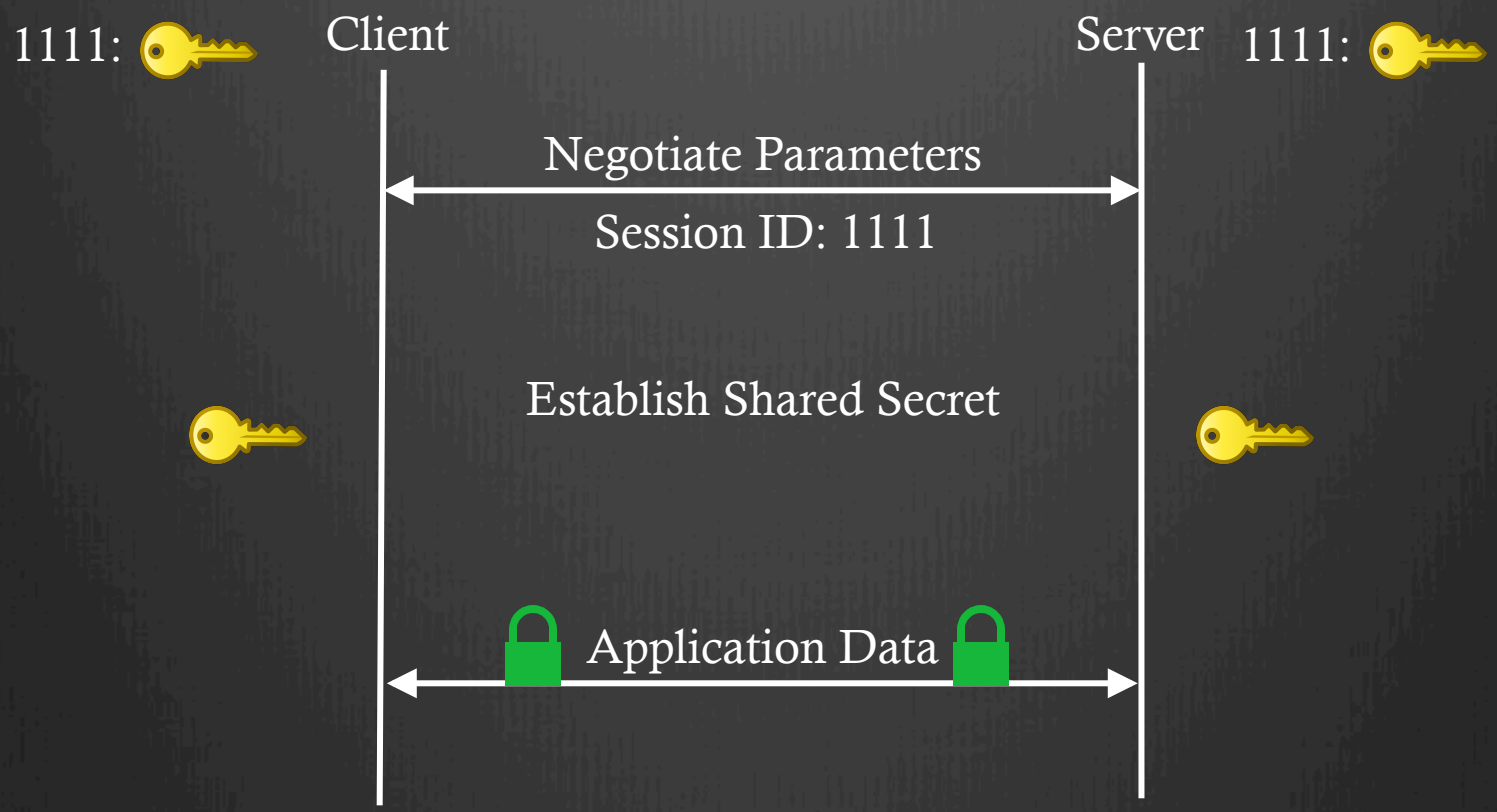
Session ID Resumption (Subsequent Connection)



Session ID Resumption (Subsequent Connection)



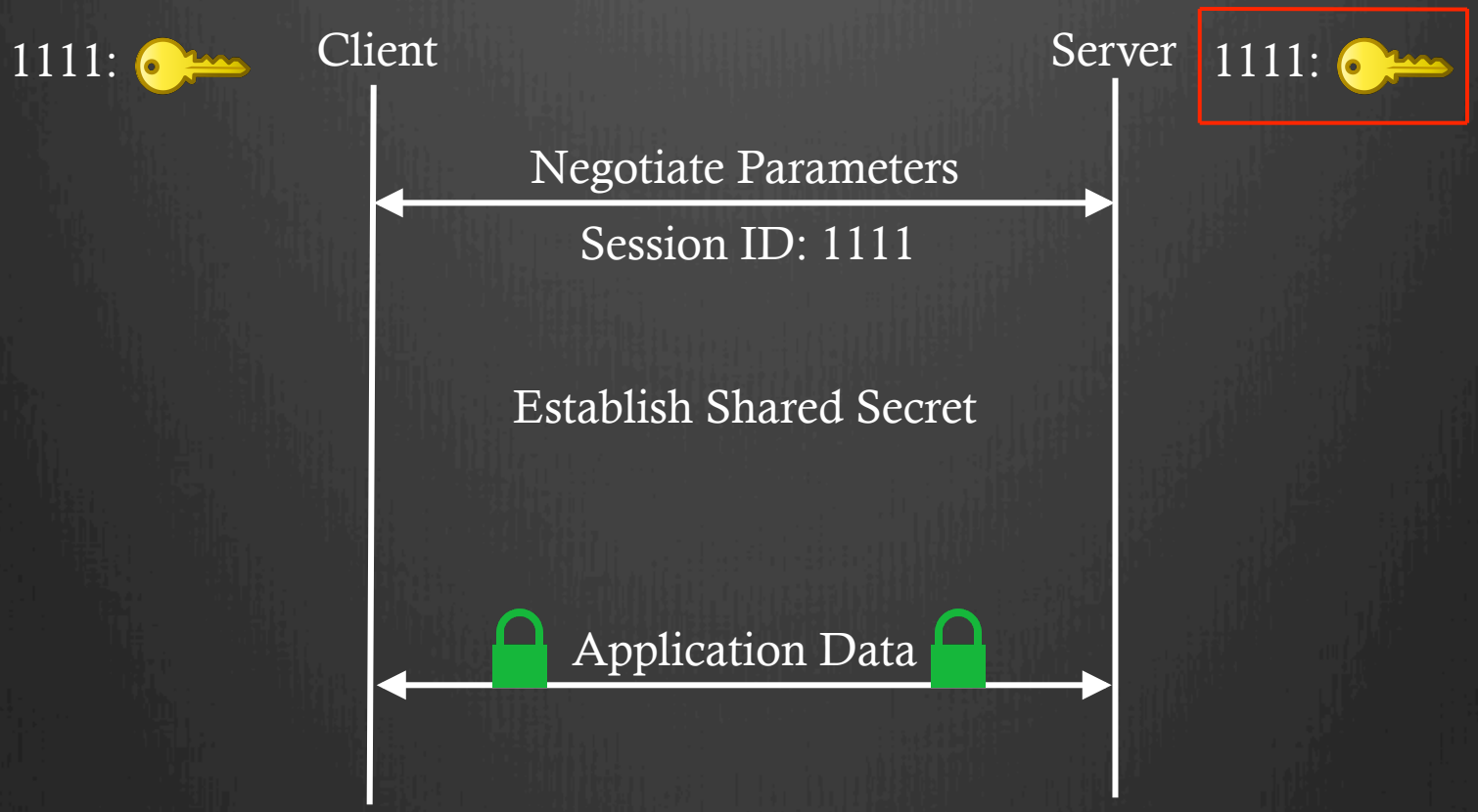
Session ID Resumption (Subsequent Connection)



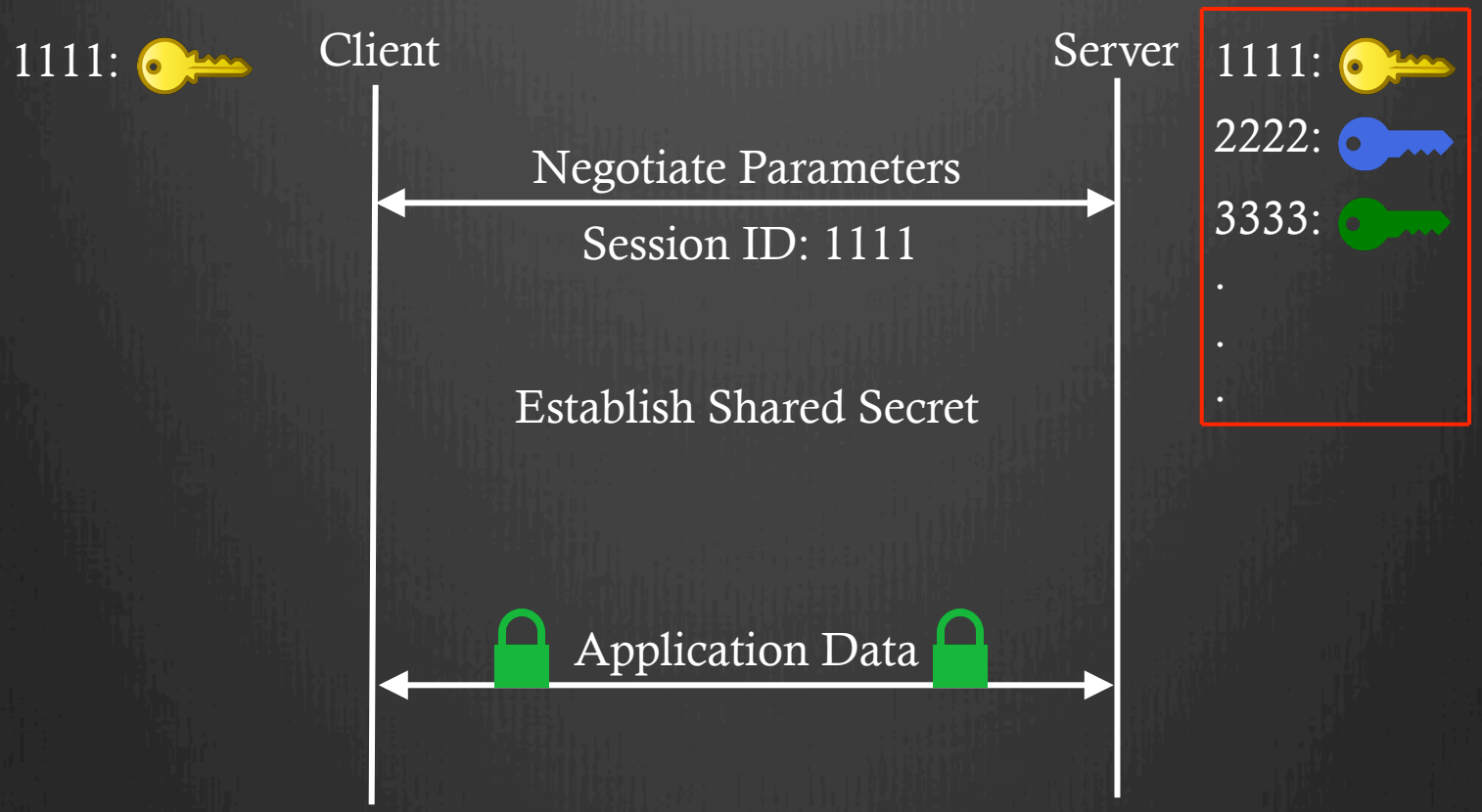
Session ID Resumption

- Session ID: database key for the server's cache
- Client and Server store Data
  - Session ID → Session State (Cipher, Session keys)
- Server blindly determines the cache lifetime

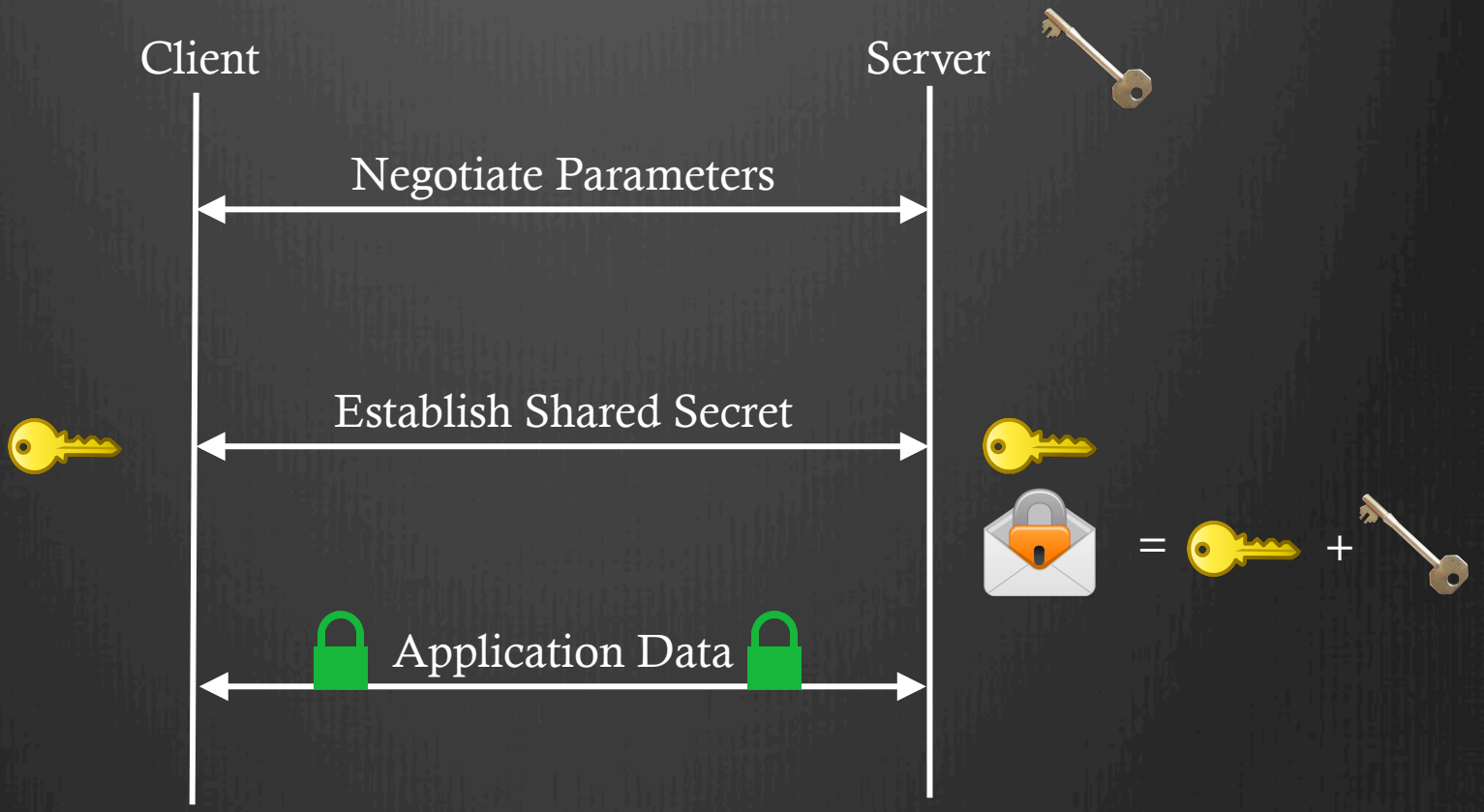
Session ID Resumption



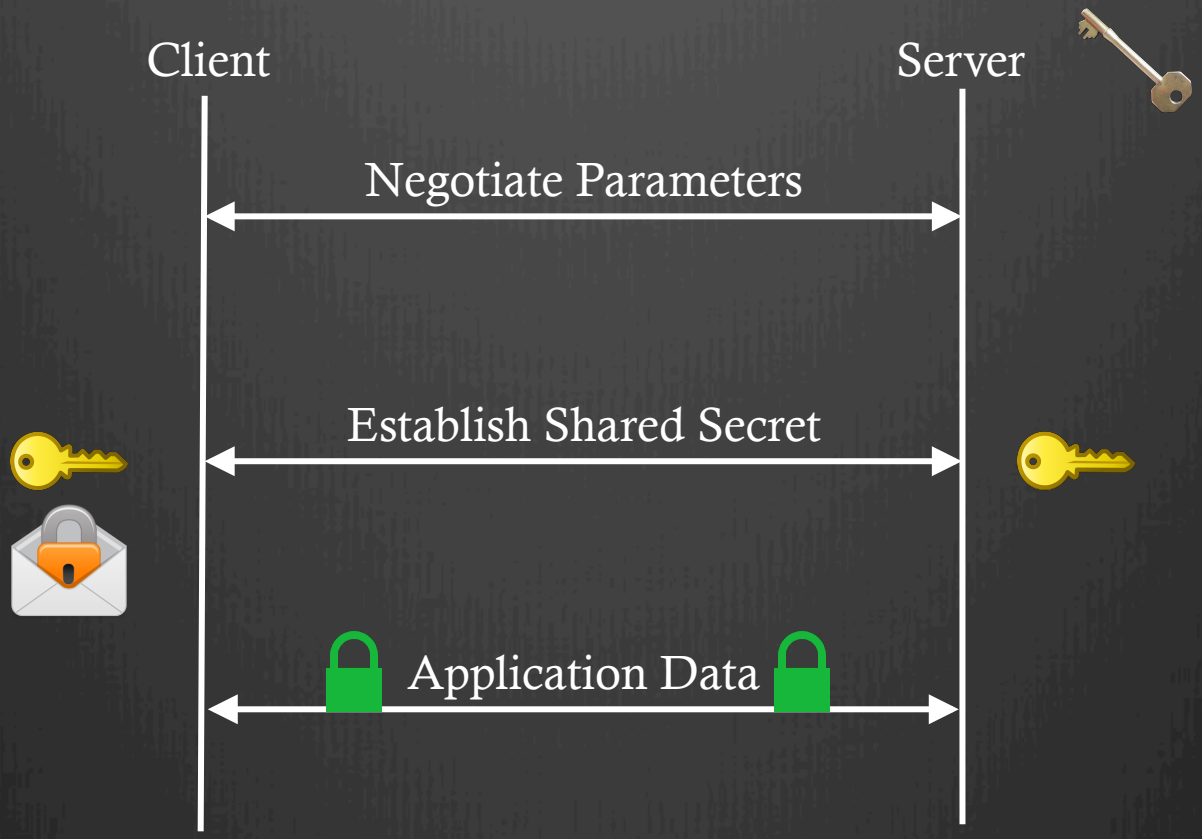
Session ID Resumption



Session Ticket Resumption (Initial Connection)



Session Ticket Resumption (Initial Connection)

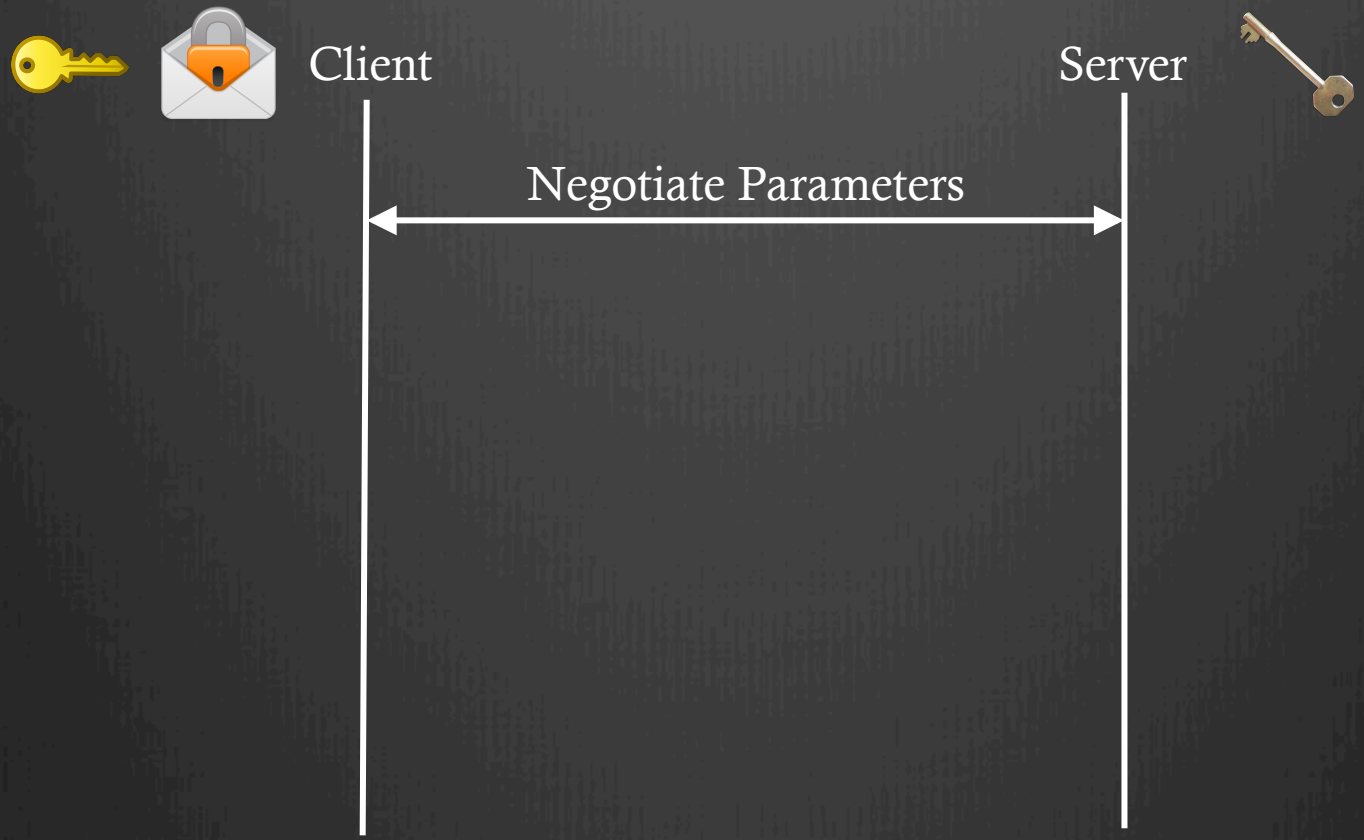


Session Ticket Resumption (Subsequent Connection)

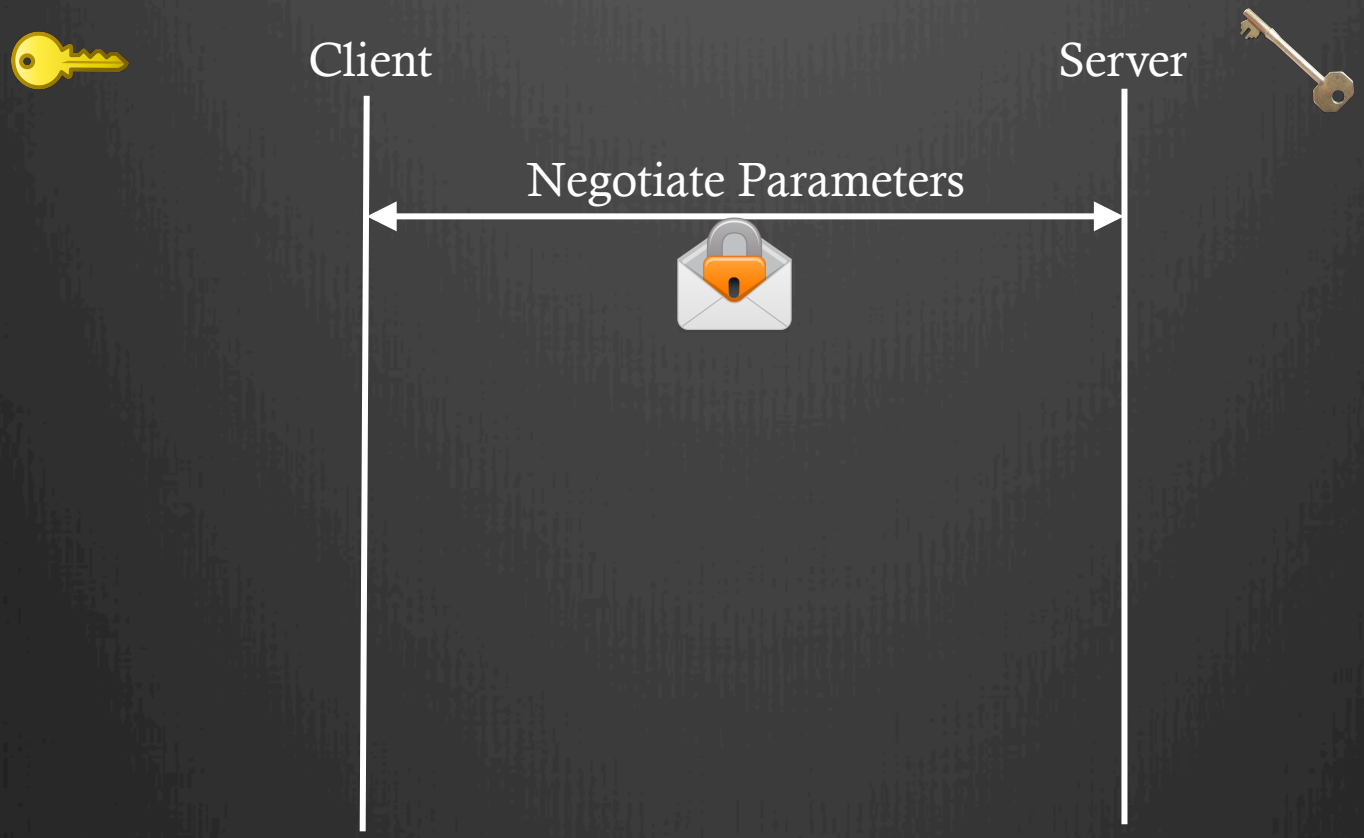
Client

Server

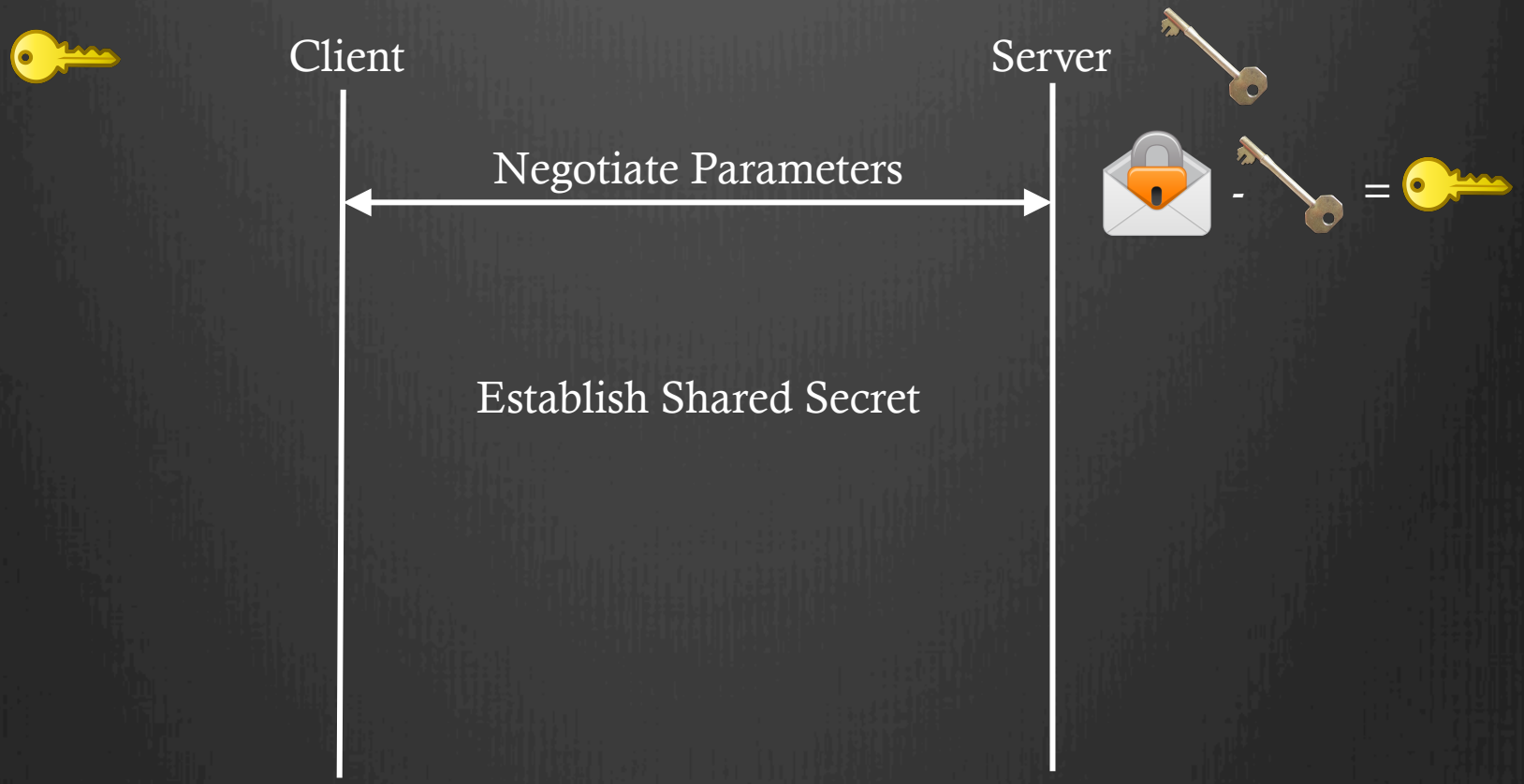
Session Ticket Resumption (Subsequent Connection)



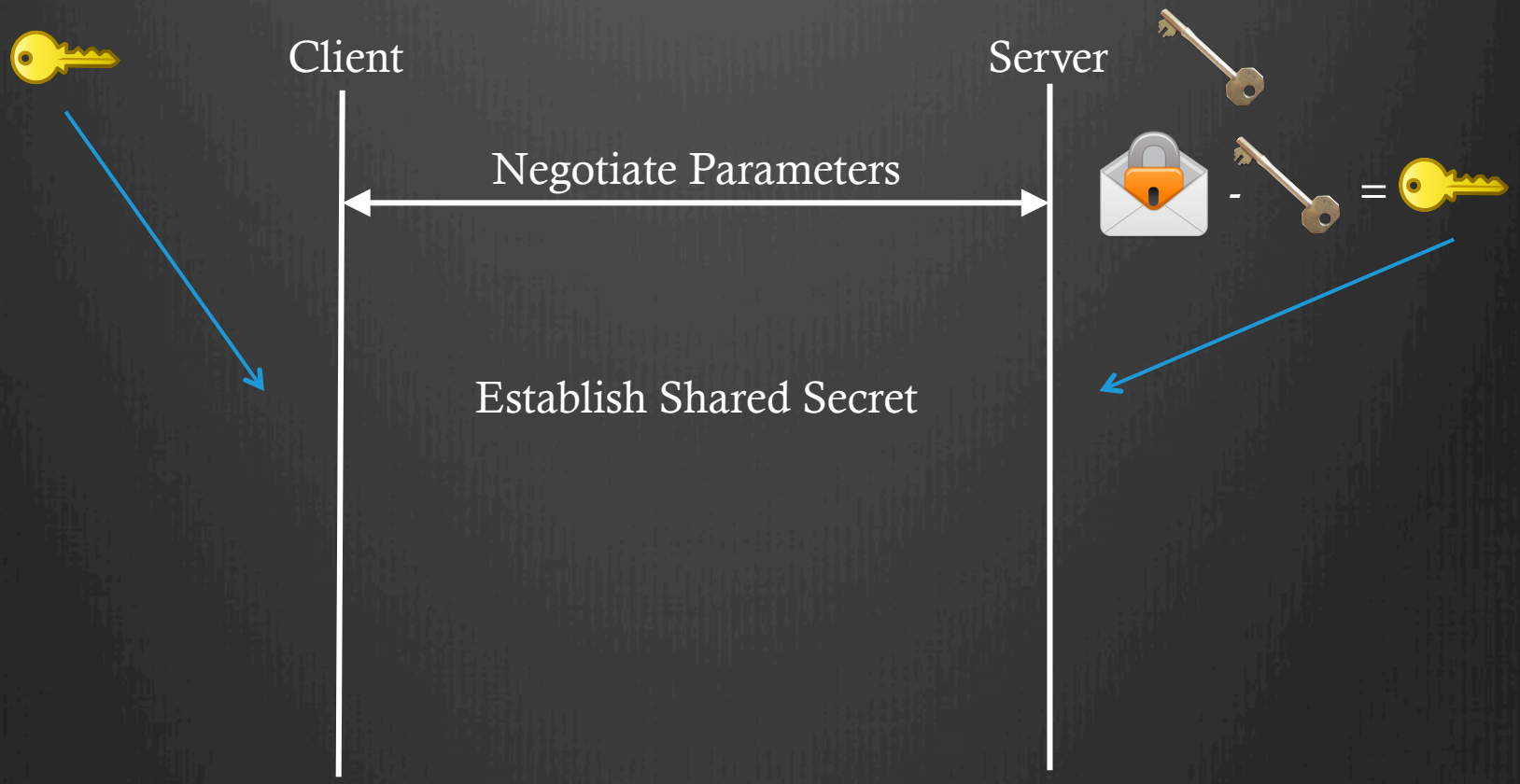
Session Ticket Resumption (Subsequent Connection)



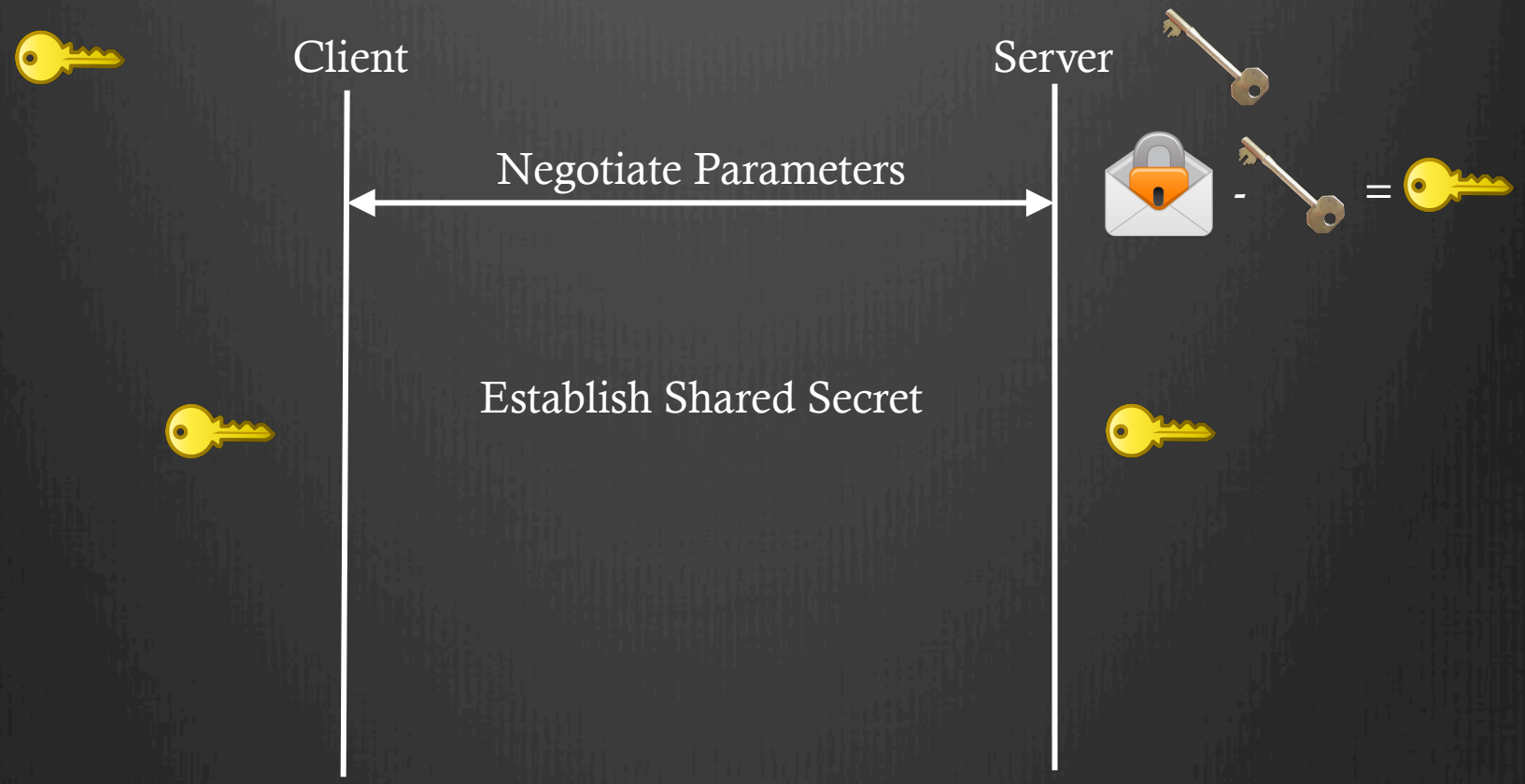
Session Ticket Resumption (Subsequent Connection)



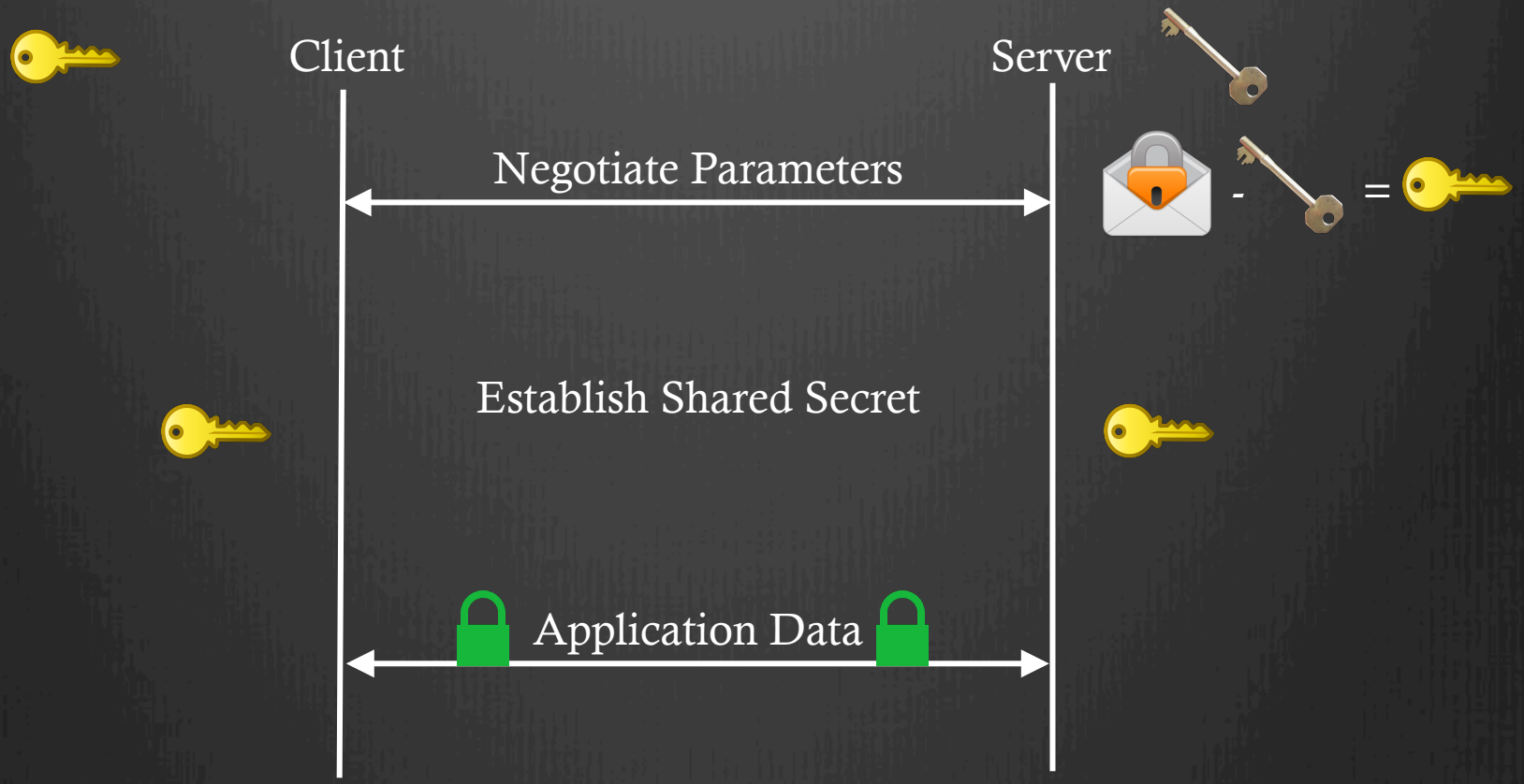
Session Ticket Resumption (Subsequent Connection)



Session Ticket Resumption (Subsequent Connection)



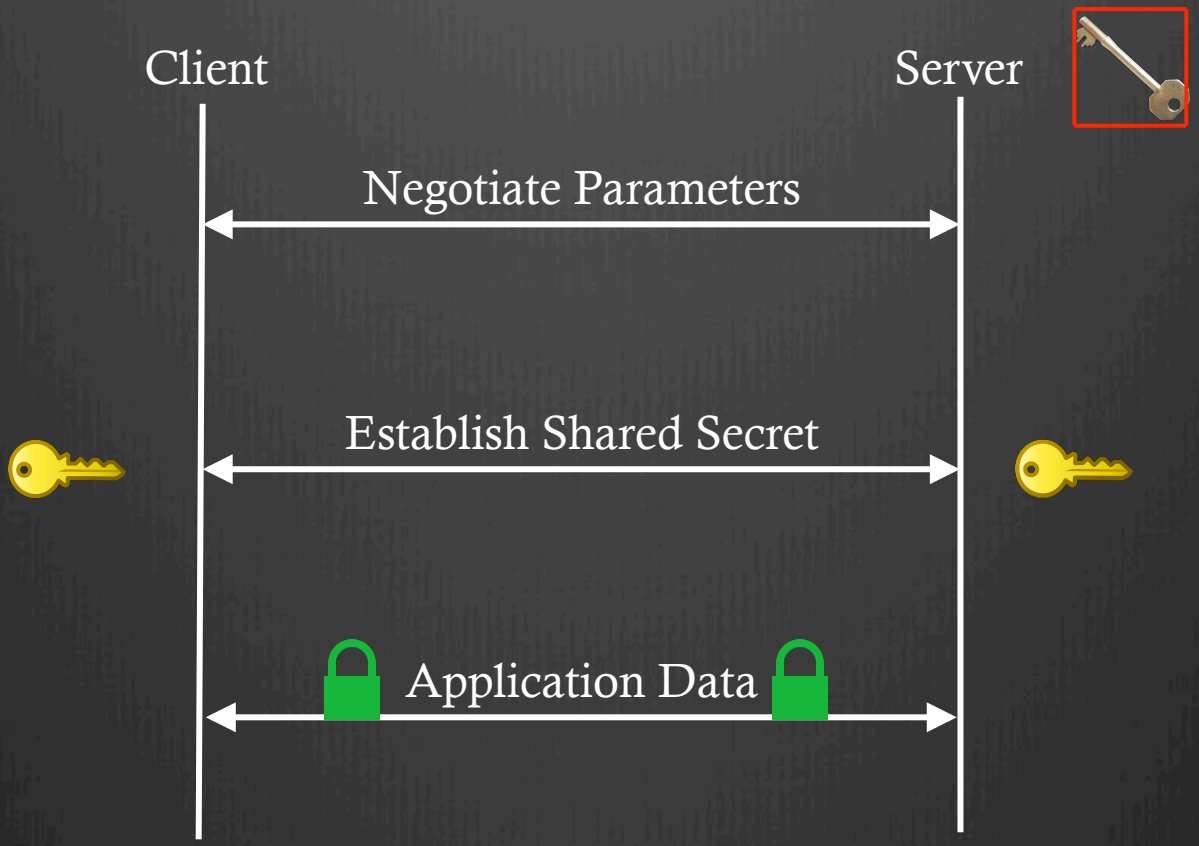
Session Ticket Resumption (Subsequent Connection)



Session Ticket Resumption

- Ticket is encrypted/authenticated session state
- Client stores Domain→Session State + Session Ticket
- Server stores Session Ticket Encryption Key (STEK)

Session Ticket Resumption



(EC)DHE Value Reuse

Client #1

Client #2

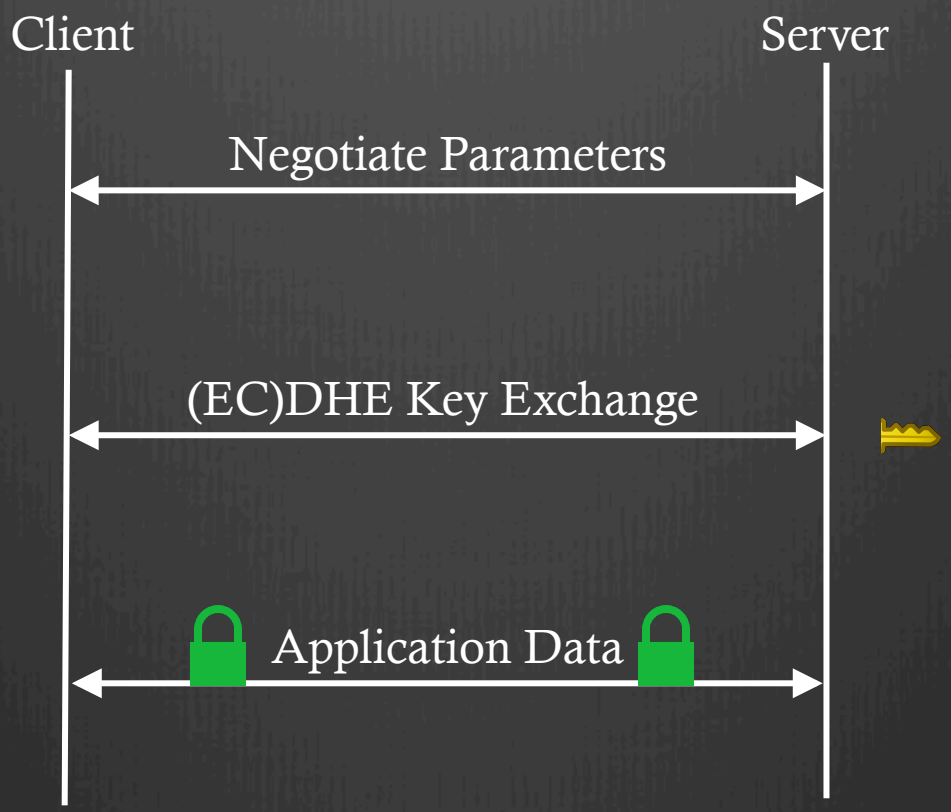
Client #3

.

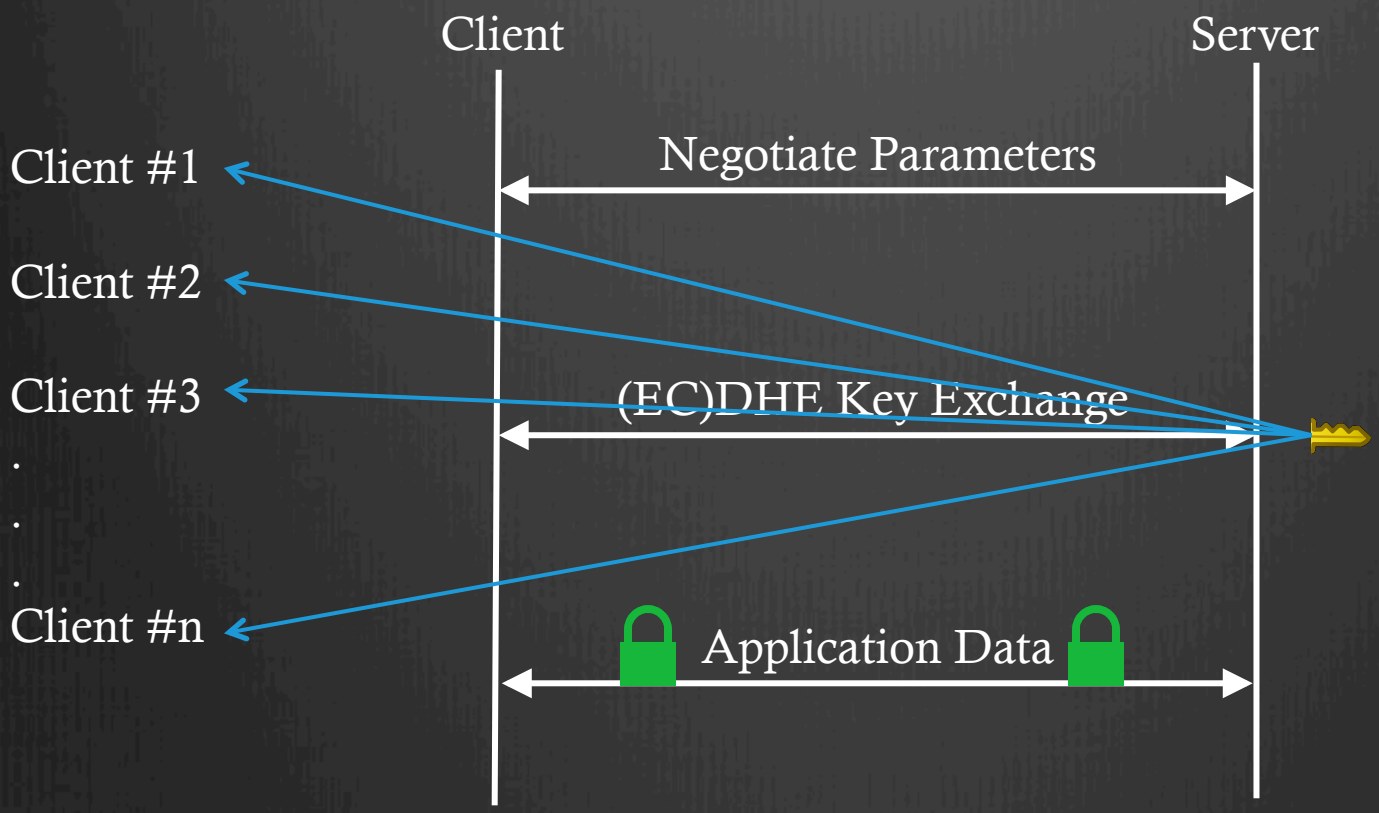
.

.

Client #n



(EC)DHE Value Reuse



(EC)DHE Value Reuse

Client #1

Client #2

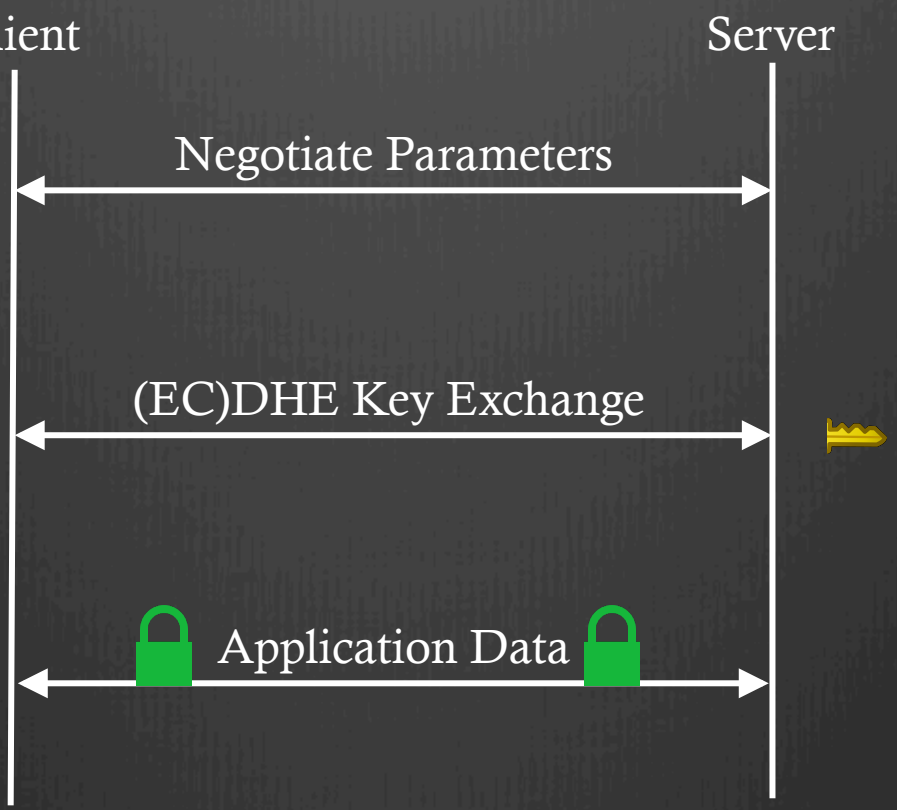
Client #3

.

.

.

Client #n



(EC)DHE Value Reuse

- Not a resumption technique
- Saves computing g^a or D_aG for each connection

(EC)DHE Value Reuse

Client #1

Client #2

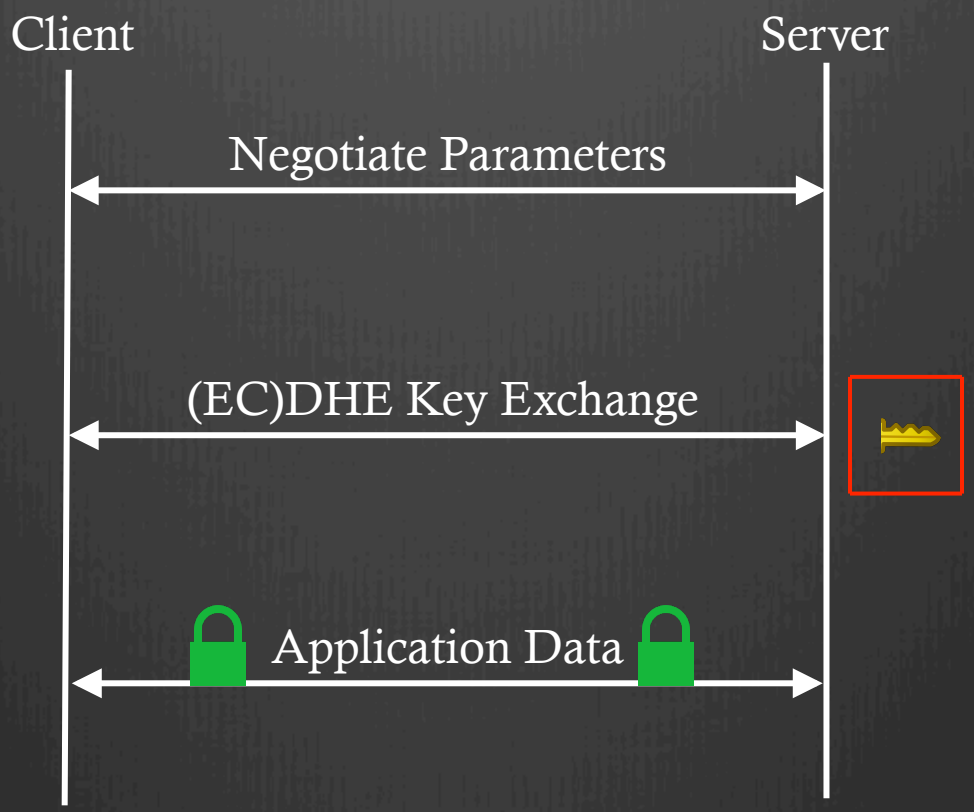
Client #3

.

.

.

Client #n



- TLS on the Internet
- Background
- **Methodology**
- Longevity Study
- Sharing Study
- Nation-State Perspective
- Conclusions

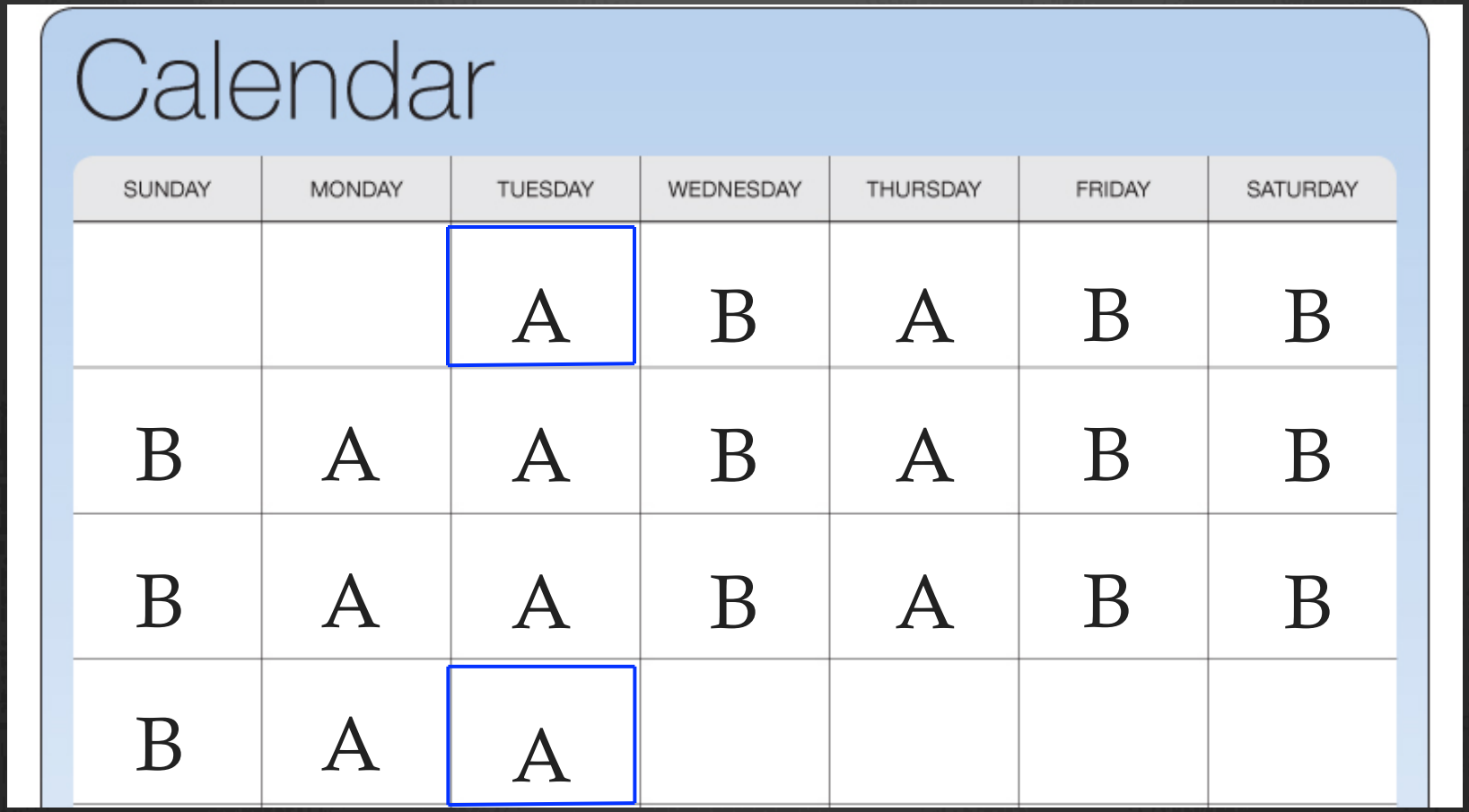
Methodology

- 9-week time period in Spring 2016
- Used modified ZMap/ZGrab toolchain
- Re-used scans from Censys project whenever available
- Focused on Alexa Top Million domains

Alexa Top Million

- 1,527,644 unique domains over 9-weeks
- 539,546 remained in Top Million for entire period
- 369,034 ever supported HTTPS
- 291,643 presented a browser trusted SSL certificate
- 288,252 issued a session ticket, completed an (EC)DHE KEX, or resumed a session

Measuring Longevity

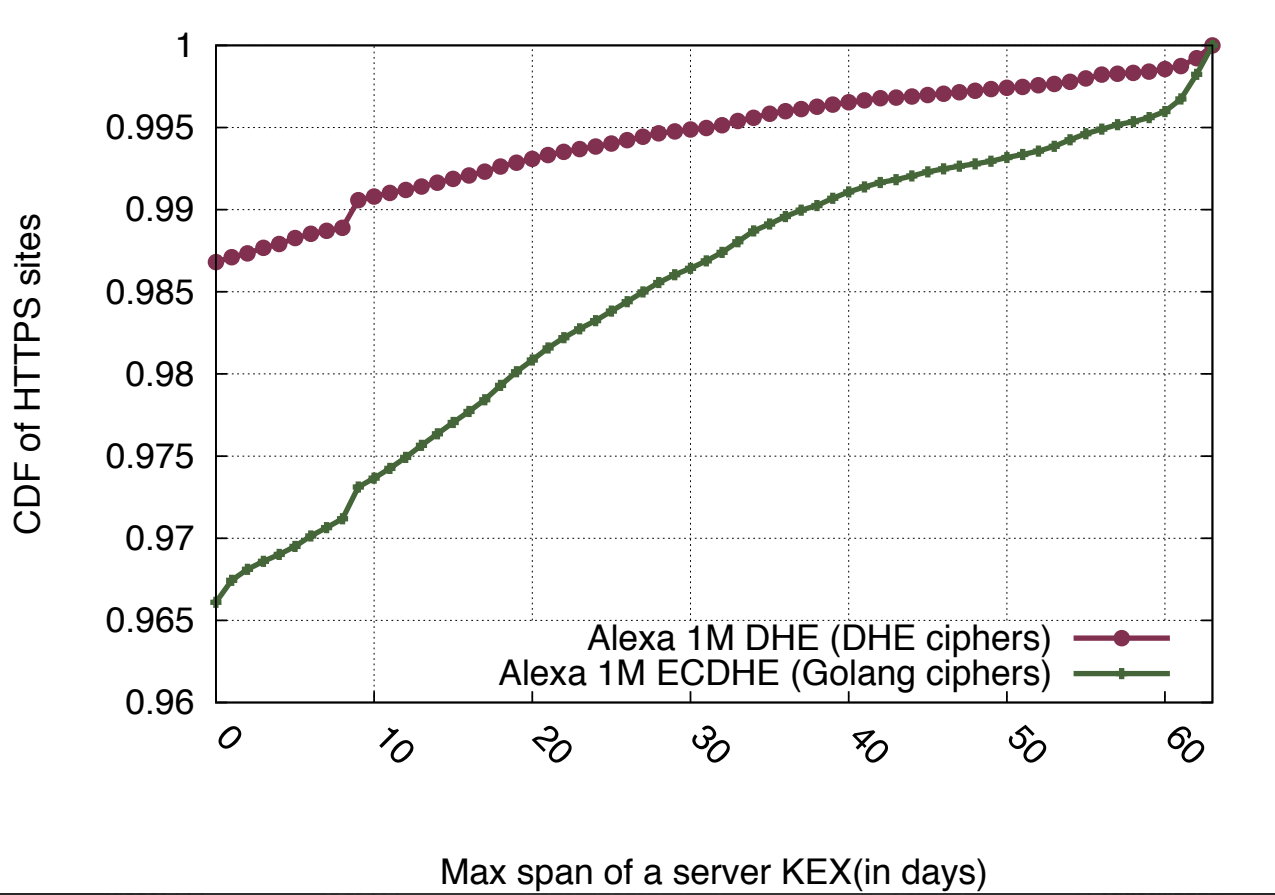


- TLS on the Internet
- Background
- Methodology
- **Longevity Study**
- Sharing Study
- Nation-State Perspective
- Conclusions

(EC)DHE Value Longevity

- Daily scans of Alexa Top Million
  - DHE-only ciphers
  - Golang ciphers (ECDHE preferred)
- Use the DH public value to determine when DH private value changes

(EC)DHE Value Longevity



(EC)DHE Value Longevity

DHE

Rank	Domain	# Days
31	netflix.com	59
53	fc2.com	18
392	ebay.in	7
456	ebay.it	8
528	bleacherreport.com	24
580	kayak.com	13
592	cbssports.com	60
626	gamefaqs.com	12
633	overstock.com	17
730	cookpad.com	63

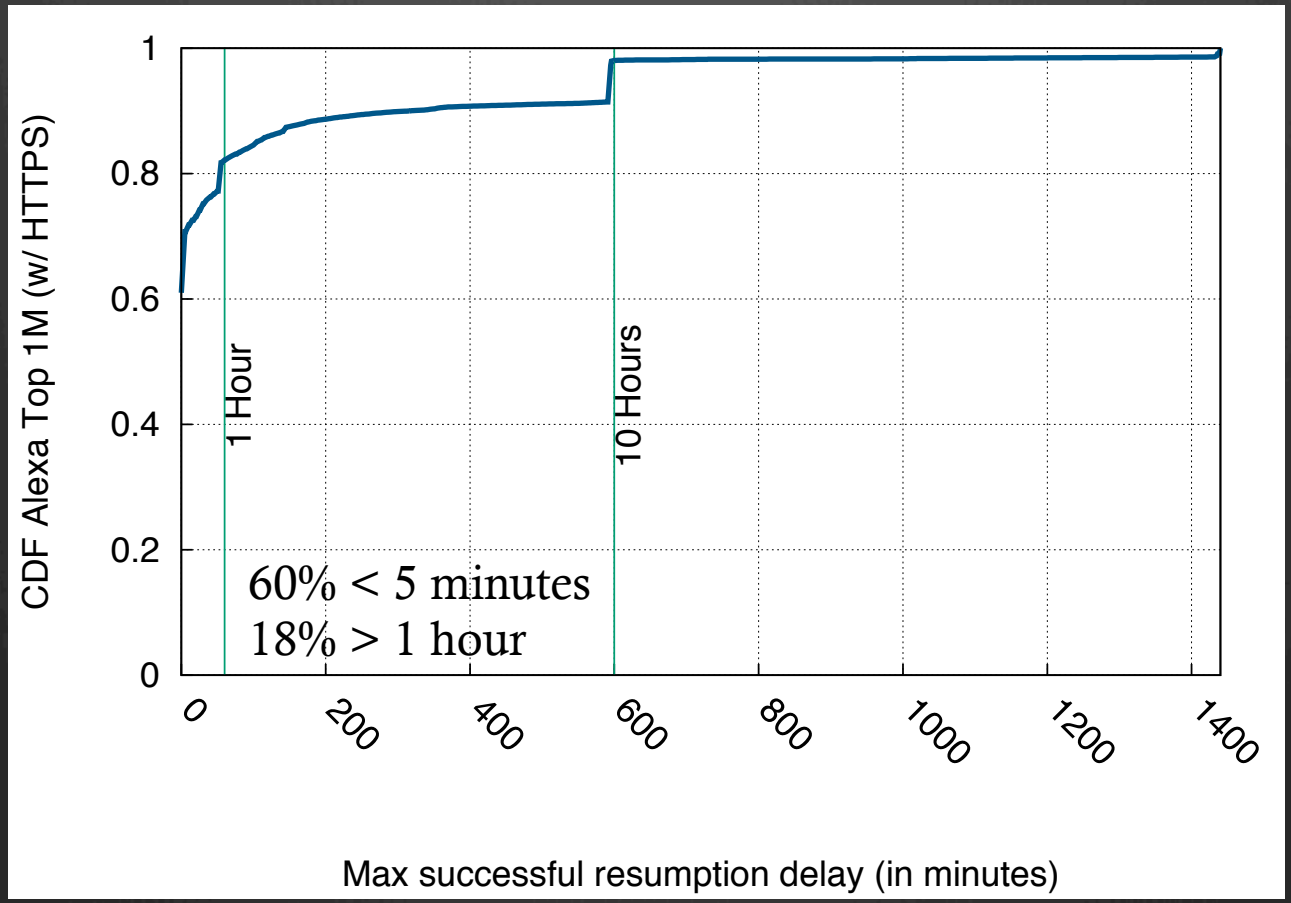
ECDHE

Rank	Domain	# Days
31	netflix.com	59
74	whatsapp.com	62
158	vice.com	26
221	9gag.com	31
322	liputan6.com	28
353	paytm.com	27
464	playstation.com	11
527	woot.com	62
528	bleacherreport.com	24
615	leagueoflegends.com	27

Session Cache Longevity

- Connect to domain
- Store Session ID → Session State
- Attempt to resume session 1-second later (check validity)
- Attempt to resume session every 5-minutes
- Continue until domain fails to resume or 24-hour passes

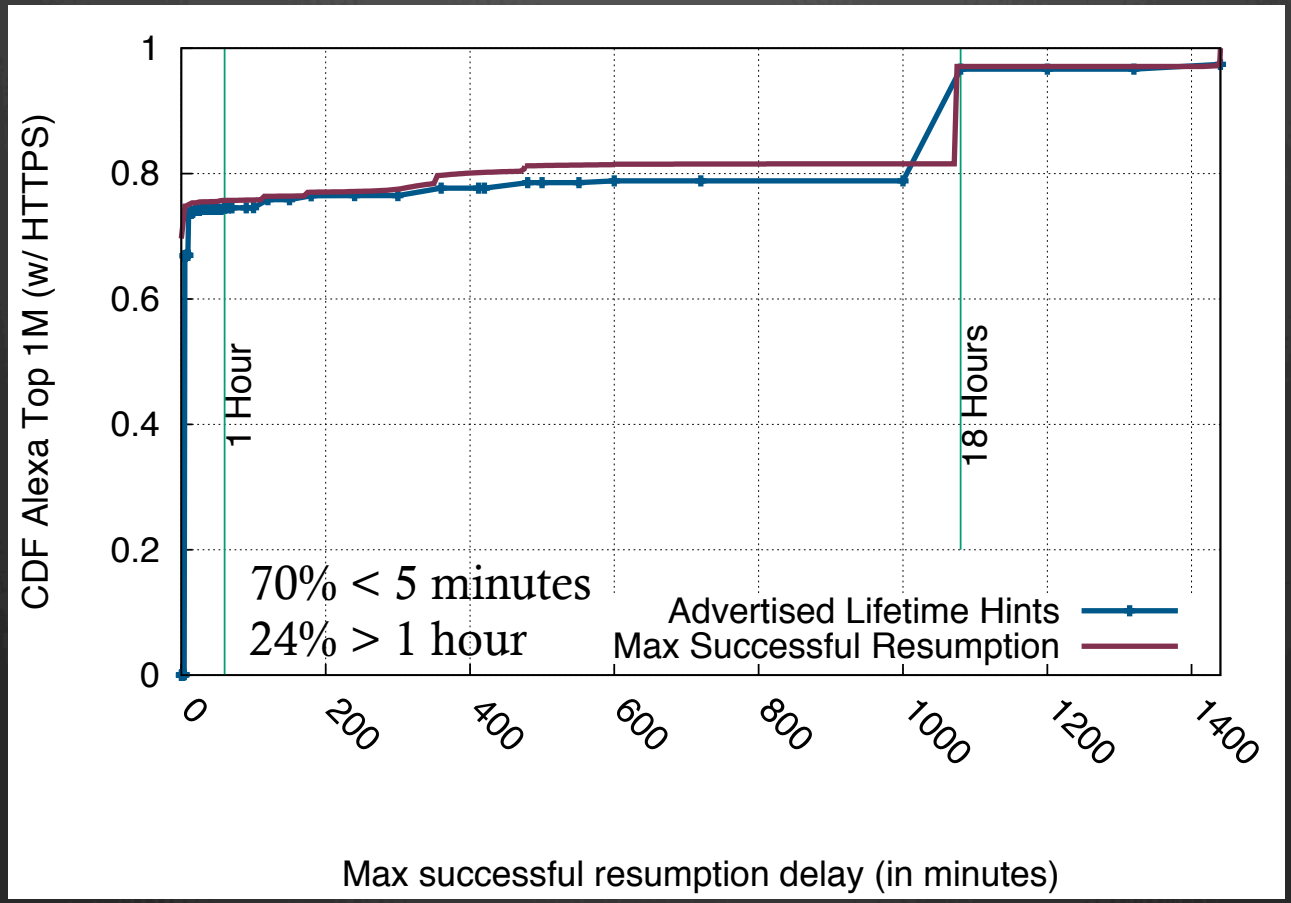
Session Cache Longevity



Session Ticket Longevity

- Connect to domain with Session Ticket extension
- Store Session Ticket → Session State
- Attempt to resume session 1-second later (check validity)
- Attempt to resume session every 5-minutes
- Continue until domain fails to resume or 24-hour passes

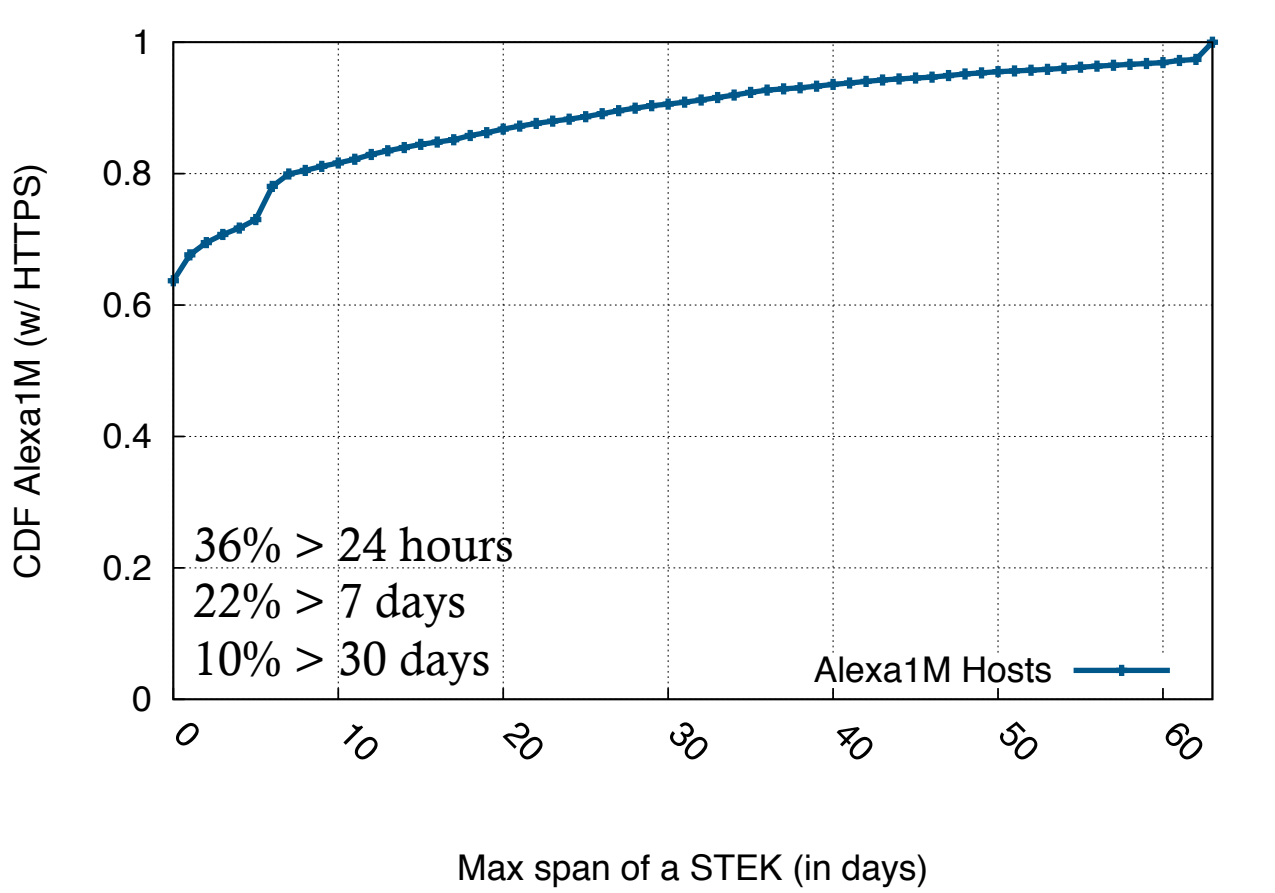
Session Ticket Longevity



STEK Longevity

- Daily scans of Alexa Top Million
- Parse the ticket to extract the Key Identifier
- Maintain `{domain:{key_id:[dates seen]}}`

STEK Longevity

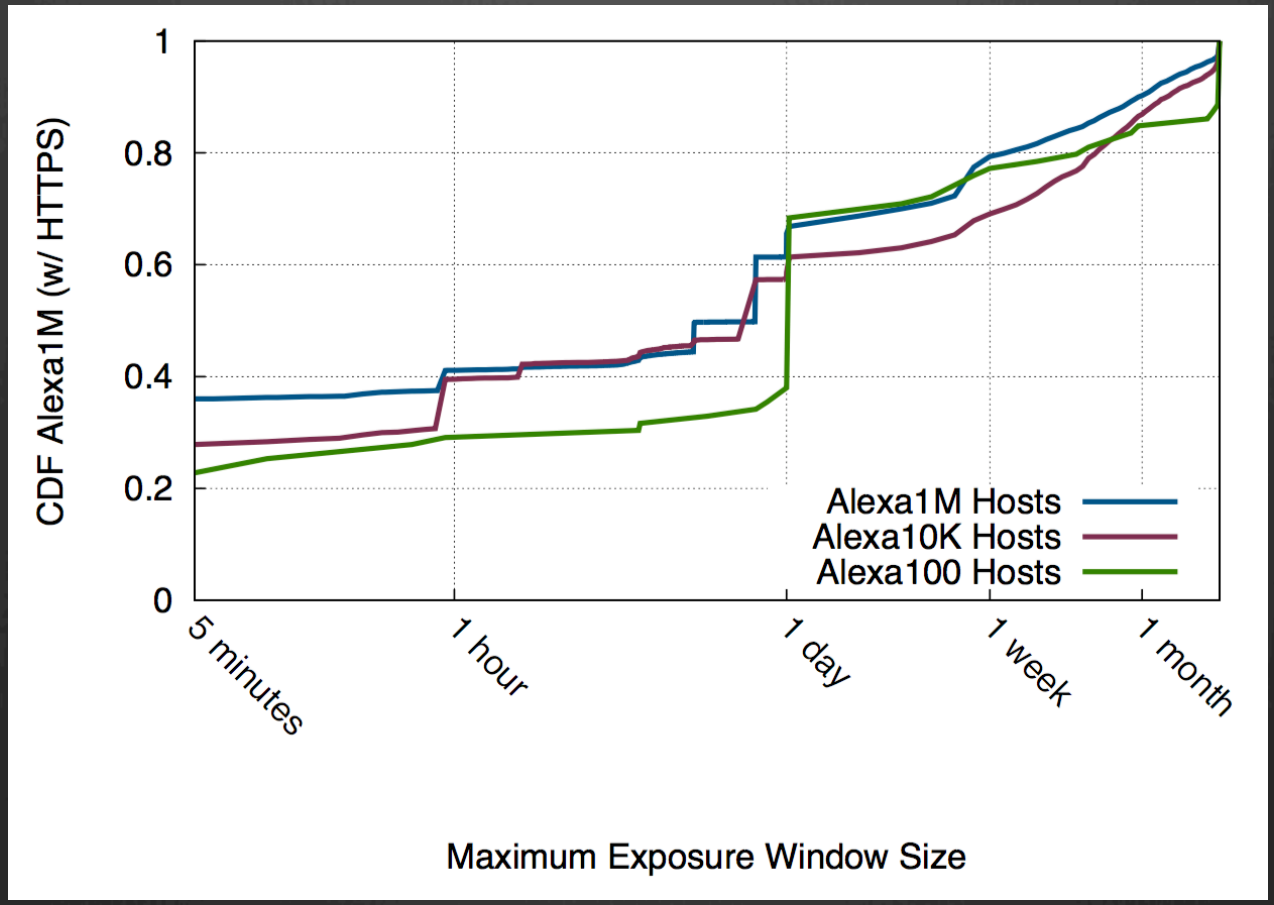


STEK Lifetime

Rank	Domain	# Days	Rank	Domain	# Days
5	yahoo.com	63	31	netflix.com	54
19	qq.com	56	35	imgur.com	63
20	taobao.com	63	41	tmall.com	63
21	pinterest.com	63	53	fc2.com	18
28	yandex.ru	63	55	pornhub.com	29

* 63 days means used the same STEK on the first and last day of our study

Overall Exposure Window



- TLS on the Internet
- Background
- Methodology
- Longevity Study
- **Sharing Study**
- Nation-State Perspective
- Conclusions

(EC)DHE Value Sharing

- 10 connections to each Alexa Top Million domain
- Group all domains that share at least one (EC)DHE value into a “service group”

(EC)DHE Value Sharing

Operator	# domains	Operator	# domains
SquareSpace	1,627	Atypon	167
LiveJournal	1,330	Affinity Internet	146
Jimdo #1	179	Line Corp.	114
Jimdo #2	178	Digital Insight	98
Distil Networks	174	EdgeCast CDN	75

Table 7: **Largest Diffie-Hellman Service Groups**

STEK Sharing

- 10 connections to each Alexa Top Million domain
- Group all domains that share at least one STEK ID value into a “service group”

STEK Sharing

Operator	# domains	Operator	# domains
CloudFlare	62,176	GoDaddy	1,875
Google	8,973	Amazon	1,495
Automattic	4,182	Tumblr #1	975
TMall	3,305	Tumblr #2	959
Shopify	3,247	Tumblr #3	956

Table 6: **Largest STEK Service Groups**

Session Cache Sharing

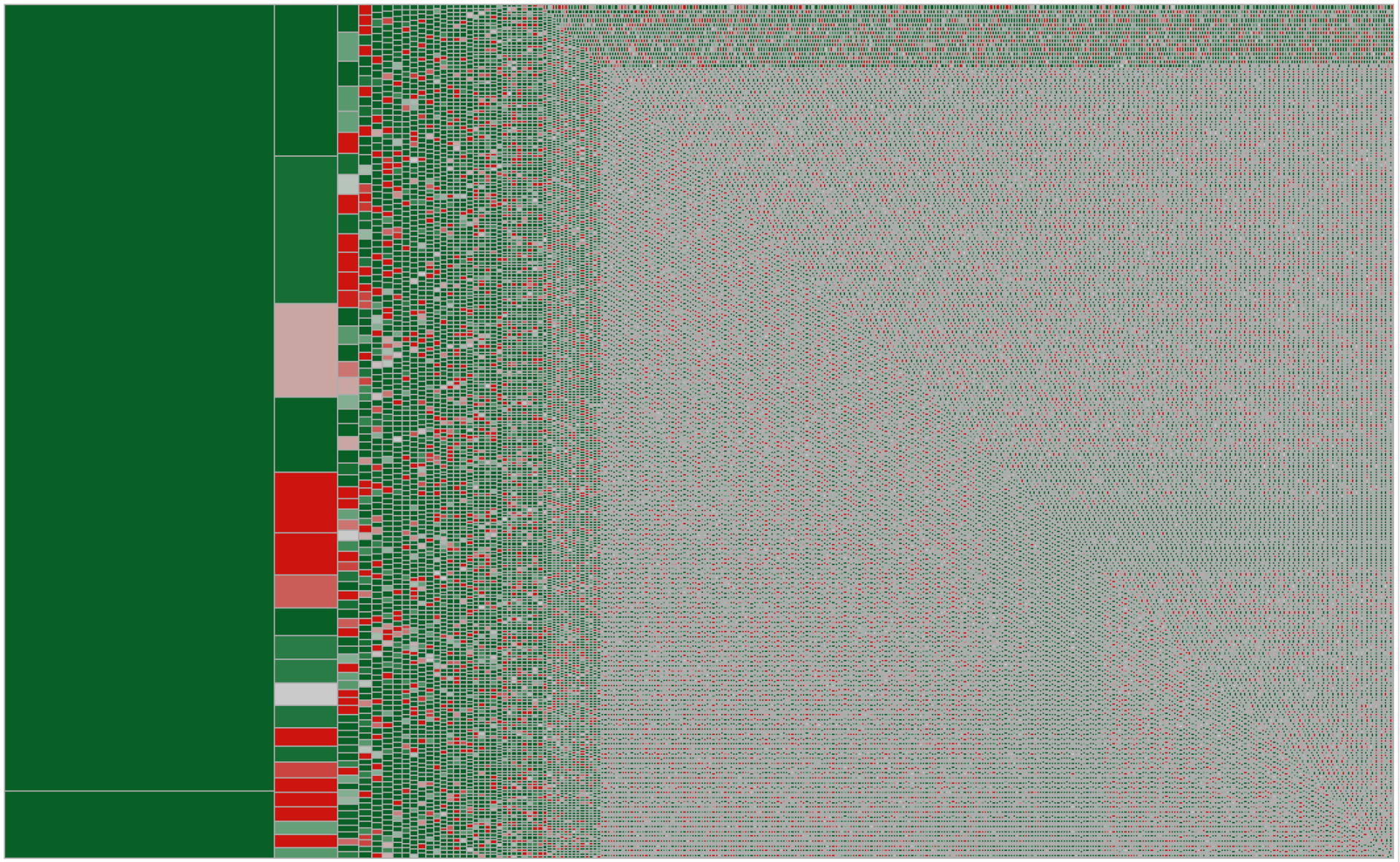
- No information available to client to determine directly
- Complete probing is intractable (n^2 connections)
- Probe up to 5 domains on same AS and 5 on same IP
  - Acquire session S_a from domain D_a
  - Attempt to resume S_a on D_b
  - Successful resumption indicates cache is shared
- Grow the service group transitively
  - If S_a is valid on D_b and S_b is valid on D_c, conclude that S_a would be valid on D_c

Session Cache Sharing

Operator	# domains	Operator	# domains
CloudFlare #1	30,163	Blogspot #2	743
CloudFlare #2	15,241	Blogspot #3	732
Automattic #1	2,247	Blogspot #4	648
Automattic #2	1,552	Shopify	593
Blogspot #1	849	Blogspot #5	561

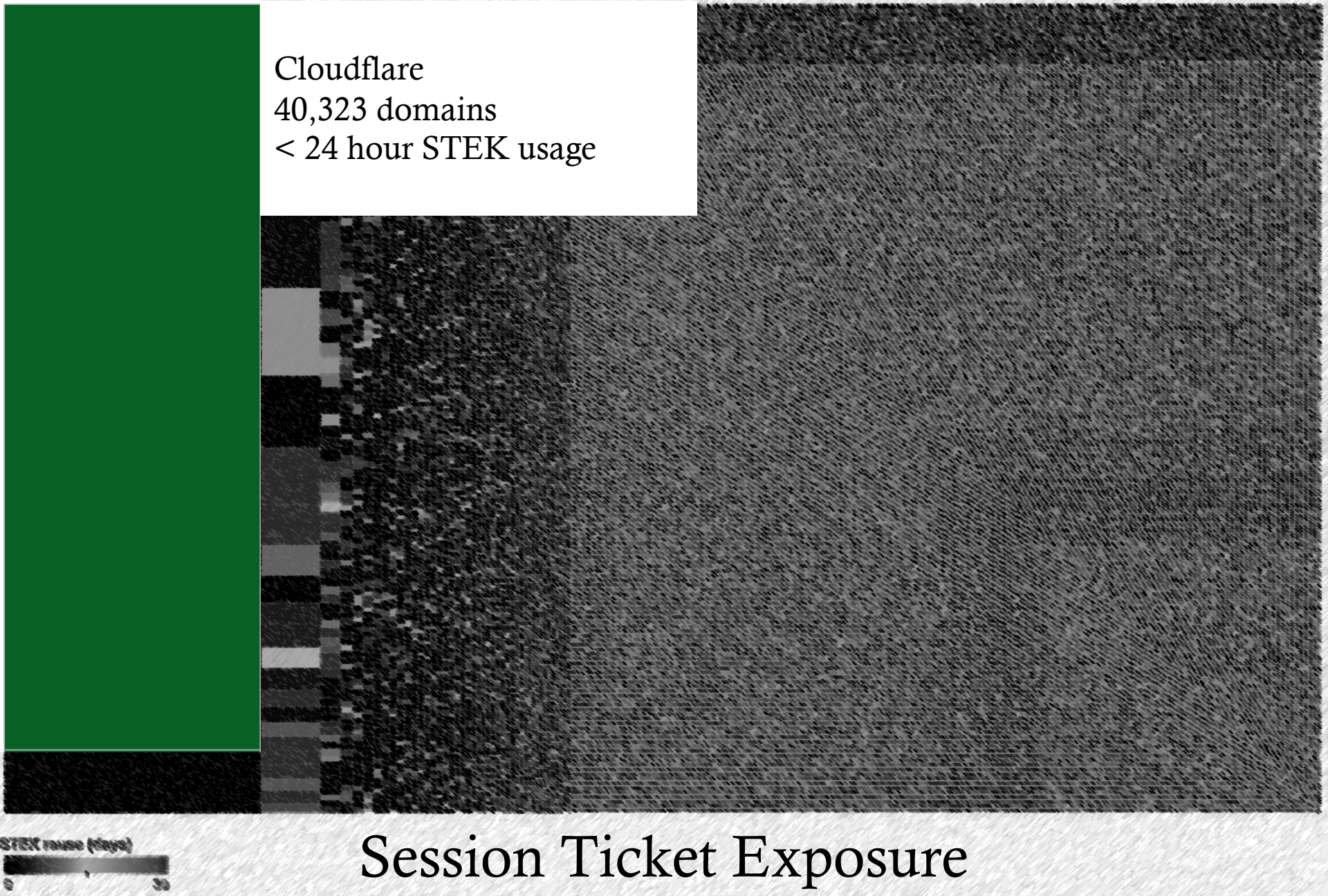
Table 5: **Largest Session Cache Service Groups**

- TLS on the Internet
- Background
- Methodology
- Longevity Study
- Sharing Study
- **Nation-State Perspective**
- Conclusions

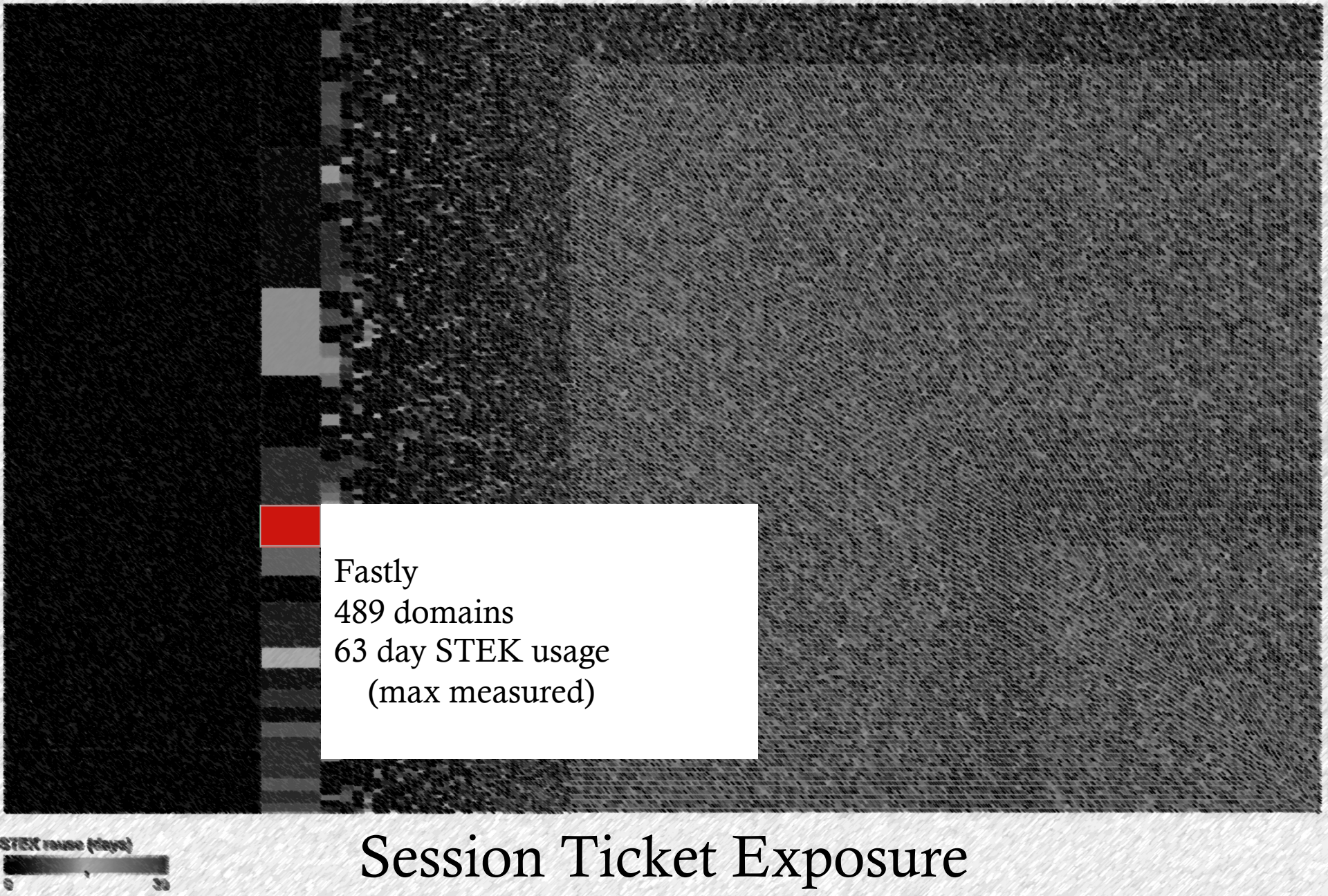


Session Ticket Exposure

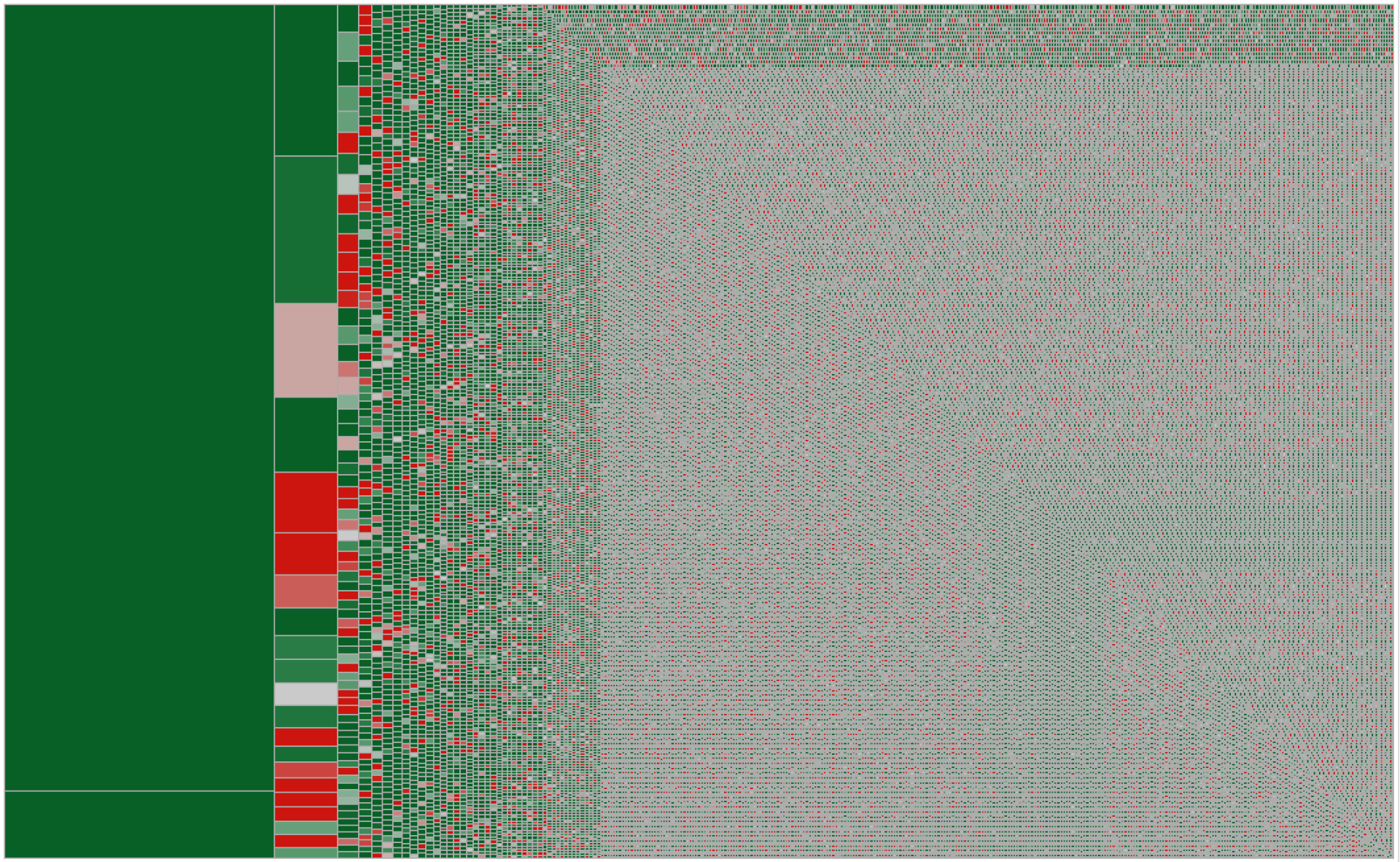
Cloudflare
40,323 domains
< 24 hour STEK usage



Session Ticket Exposure



Session Ticket Exposure



Session Ticket Exposure

Appealing to Nation States

- Asymmetric Attack
  - Fewer resources expended than a per-connection attack

Appealing to Nation States

- Asymmetric Attack
  - Fewer resources expended than a per-connection attack
- Leverage in-place passive collections systems and processes

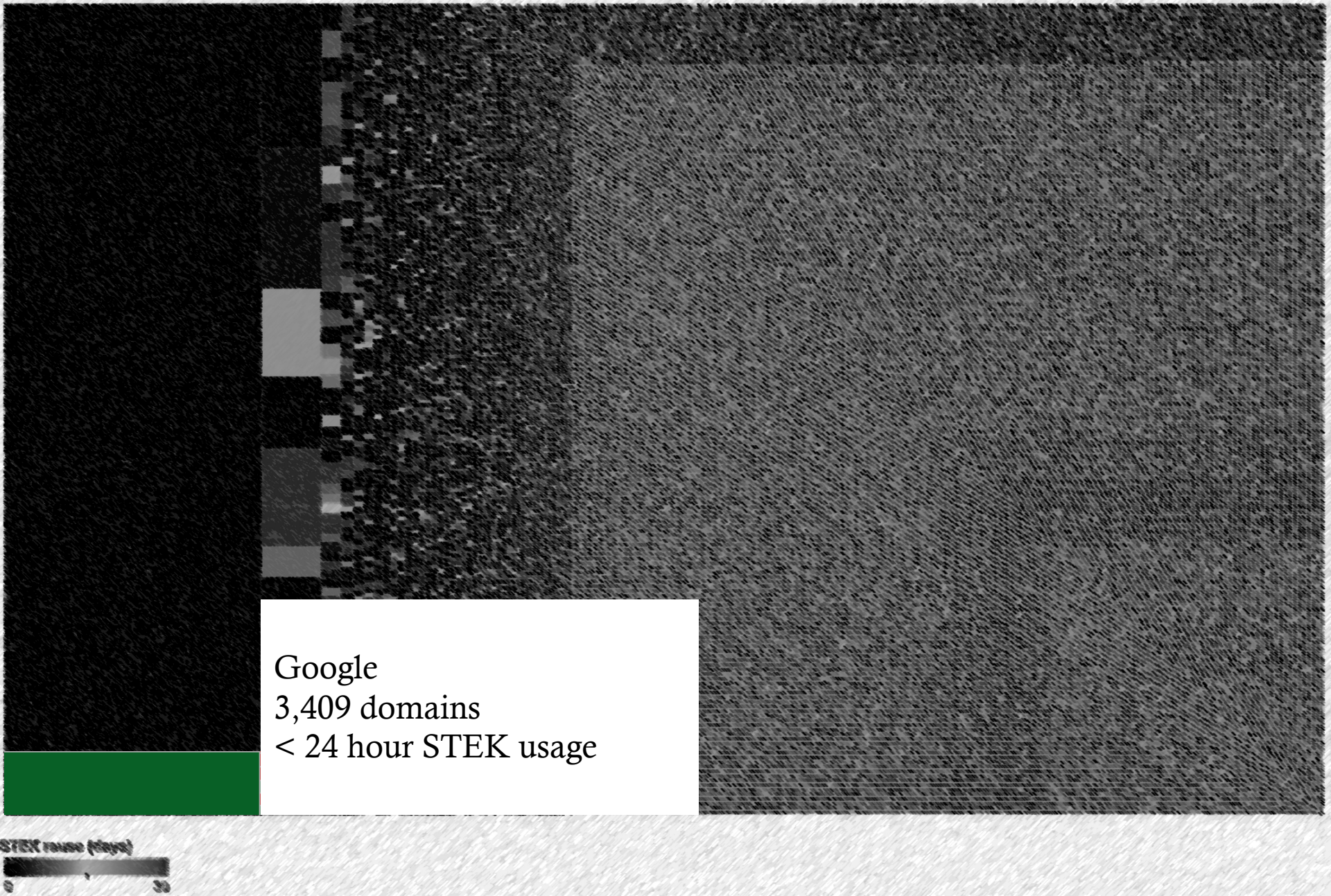
Appealing to Nation States

- Asymmetric Attack
  - Fewer resources expended than a per-connection attack
- Leverage in-place passive collections systems and processes
- Can gain via legal compulsion
  - LavaBit

Appealing to Nation States

- Asymmetric Attack
  - Fewer resources expended than a per-connection attack
- Leverage in-place passive collections systems and processes
- Can gain via legal compulsion
  - LavaBit
- Attack a 3rd party
  - Gemalto, Belgacom, Juniper show willingness

Target Analysis



Google
3,409 domains
< 24 hour STEK usage

Usefulness of Google's STEK

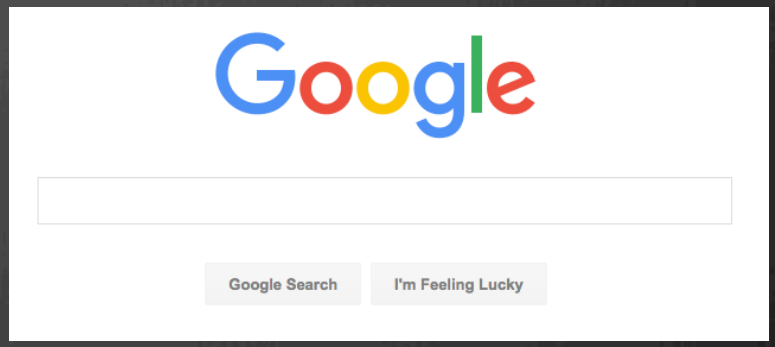
Allows Decryption of:

Usefulness of Google's STEK

Allows Decryption of:

- Search and Results

Search and Results

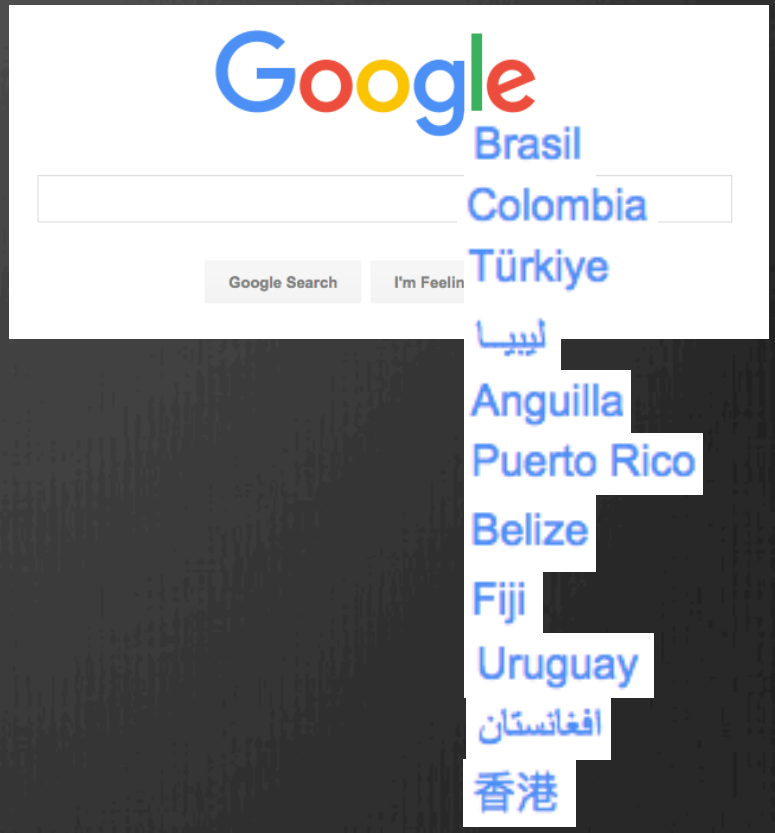


Usefulness of Google's STEK

Allows Decryption of:

- Search and Results
- Many TLDs

Many TLDs



Usefulness of Google's STEK

Allows Decryption of:

- Search and Results
- Many TLDs
- Webapp Traffic

Webapp Traffic

Usefulness of Google's STEK

Allows Decryption of:

- Search and Results
- Many TLDs
- Webapp Traffic
- Non-HTTPS Traffic

Non-HTTPS Traffic

- SMTP + STARTTLS
- SMTPS
- IMAPS
- POP3S

Usefulness of Google's STEK

Allows Decryption of:

- Search and Results
- Many TLDs
- Webapp Traffic
- Non-HTTPS Traffic
- Google for Work

Google for Work

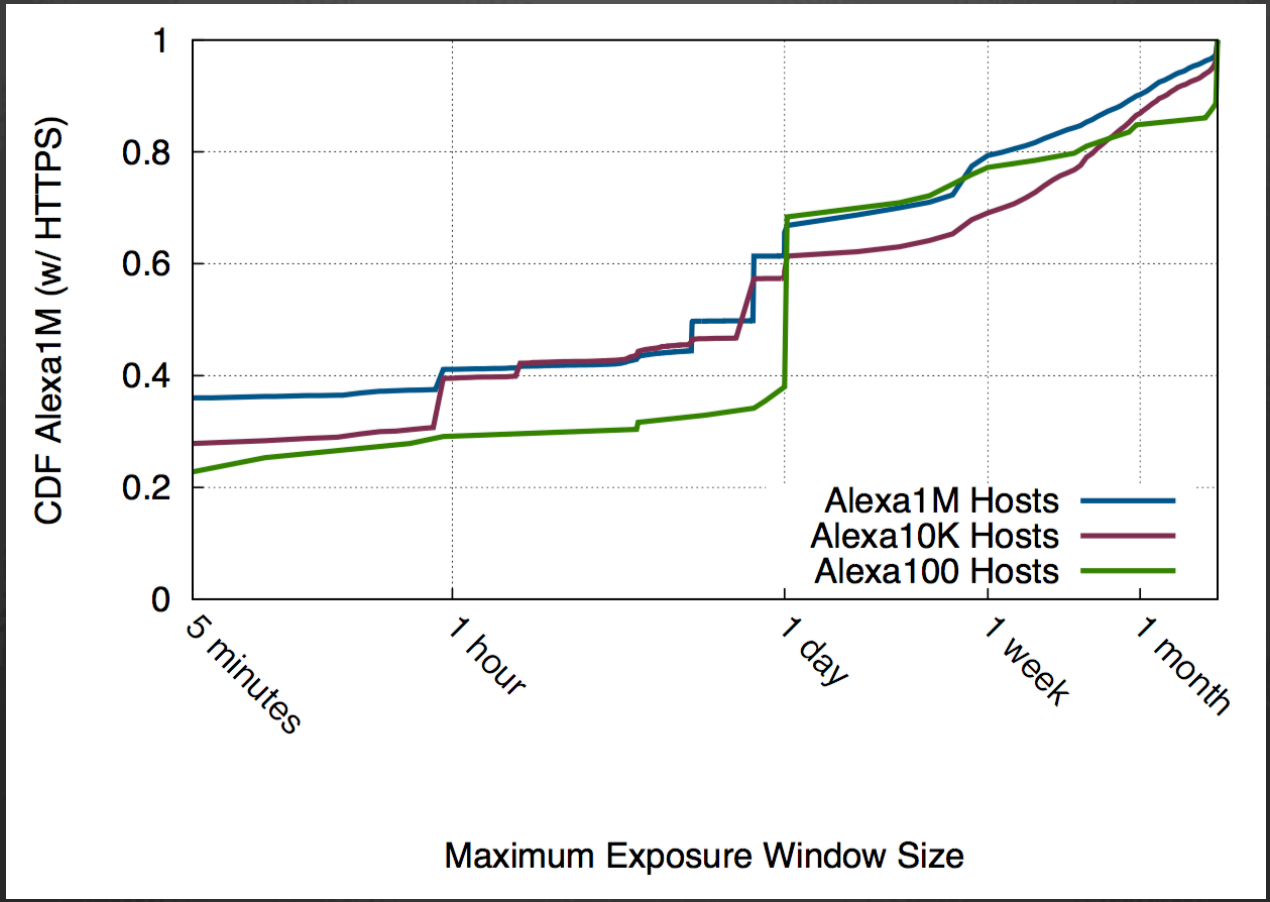
- Millions of companies who use Google's Infrastructure
- E-Mail, webapp, etc

Hypothetical Attack

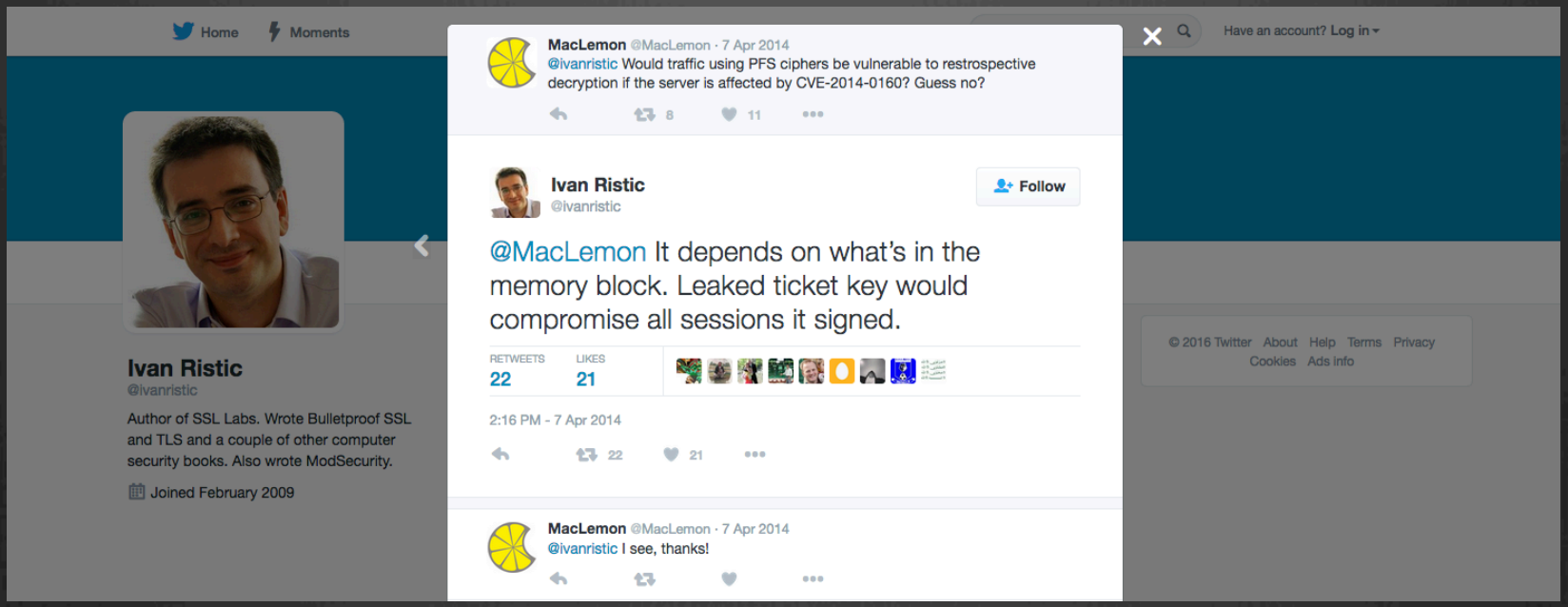
- Obtain STEK (via technical or legal means)
  - 28 hour lifetime (issues for 14 hours)
- Use passive collection systems to collect connections
- Use STEK + connection to decrypt content
  - All Google & Google For Work domains

- TLS on the Internet
- Background
- Methodology
- Longevity Study
- Sharing Study
- Nation-State Perspective
- **Conclusions**

Conclusions



Conclusions



Conclusions

Security Community

- TLS caveats exist and are important to understand
- Caveats should be more clearly communicated to others

Server Administrators

- Use HTTP/2
- Rotate STEKs frequently
- Store, distribute, and erase secrets securely

Measuring the Security Harm of TLS Crypto Shortcuts

Drew Springall, Zakir Durumeric, and J. Alex Halderman
University of Michigan