

TCP Fast Open

Sivasankar Radhakrishnan ^{★§}, Yuchung Cheng[★],
Jerry Chu[★], Arvind Jain[★], Barath Raghavan[⊙]

★ Google Inc. § UC San Diego ⊙ ICSI

Web Page Load Performance

Web object

Avg $\approx$ 7.3KB

Median $\approx$ 2.4KB

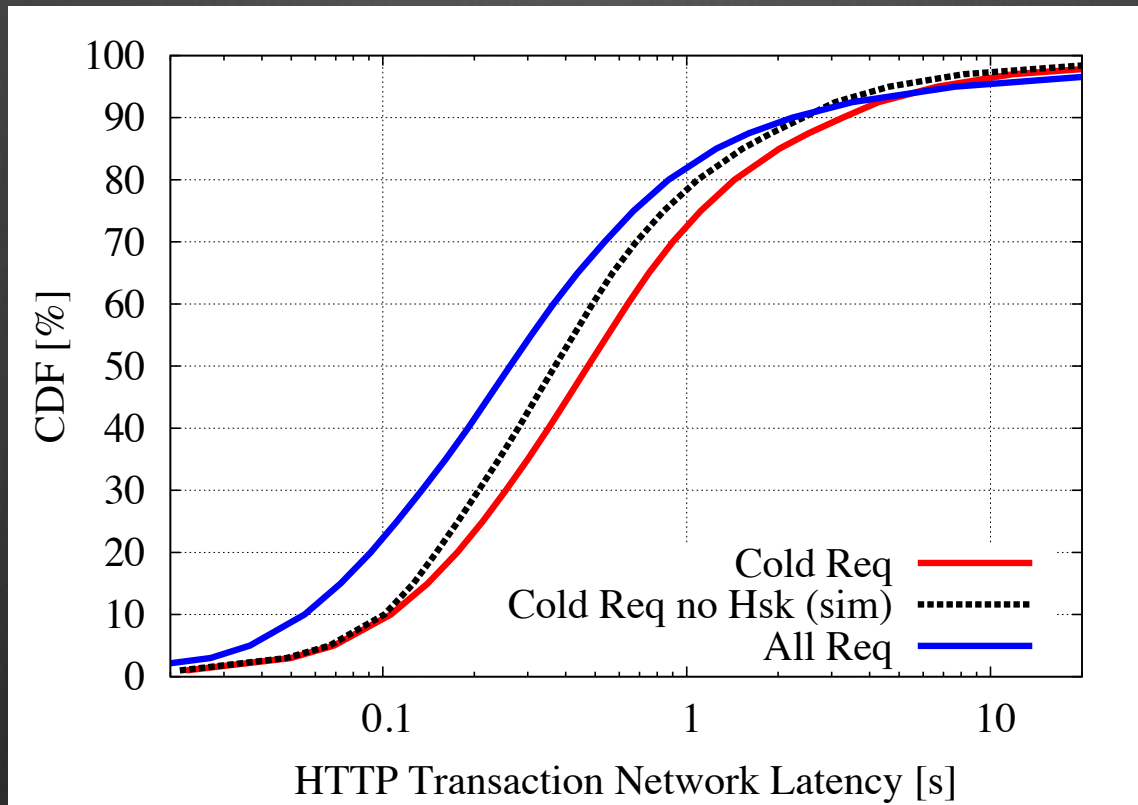
Web transfer latency

- ⊗ HTTP response transfer $\approx$ 1-3 RTTs
- ⊗ TCP connection setup – 1 RTT overhead

- ⊗ HTTP Persistent Connections
 - ⊗ Reuses TCP connections for multiple transactions
 - ⊗ Widely deployed (92% connections support it)
- ⊗ > 33% of requests still use new connections (cold requests)
 - ⊗ [Chrome, Yahoo CDN] statistics

TCP Handshake Cost

Chrome Browser Logs – 1 month, billions of requests, opt in users

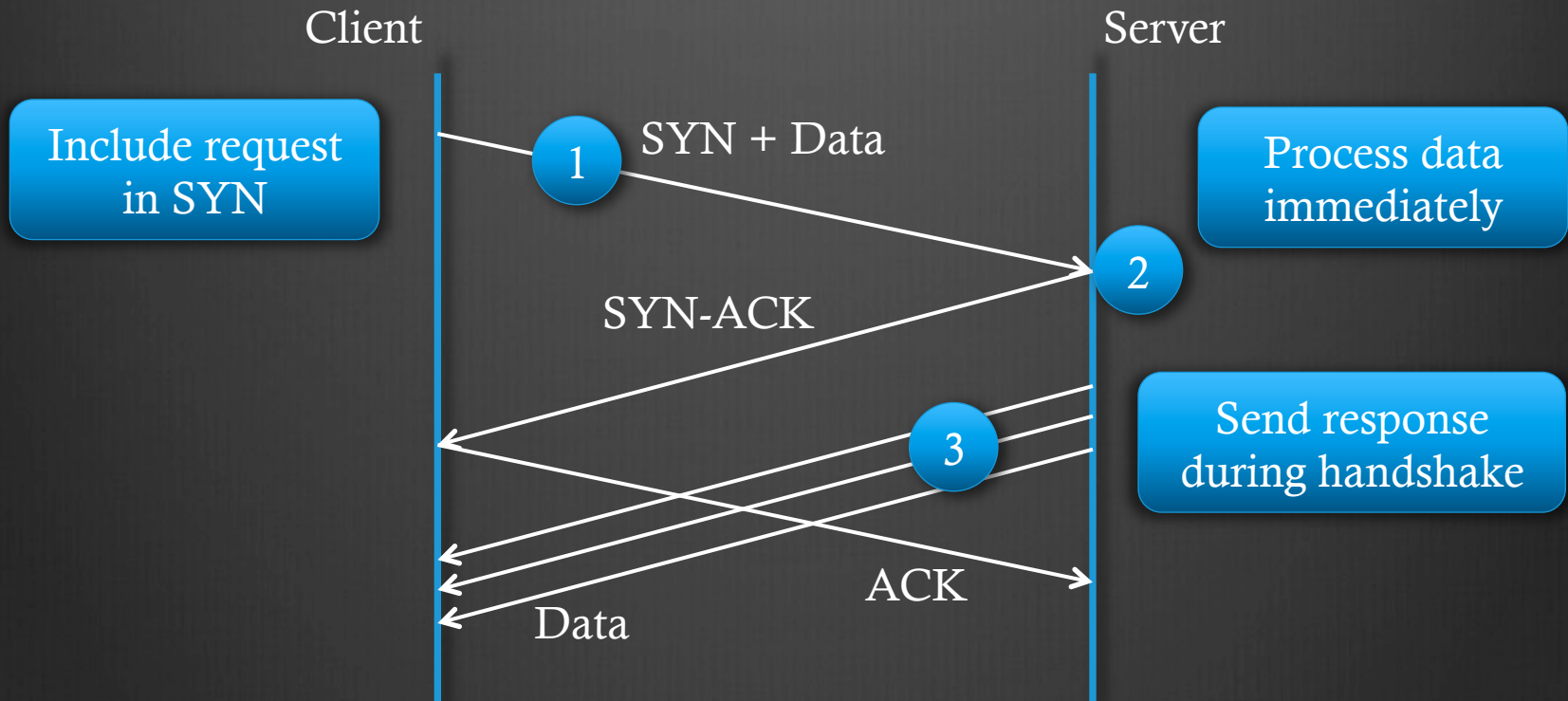


Up to 25% of latency of cold requests

TCP Fast Open

Allows data exchange during TCP handshake

In An Ideal World



- ⊗ RFC 793 – TCP specification
 - ⊗ Allows including data in SYN packets
 - ⊗ Forbids processing data until handshake completes

Duplicate SYN Packets

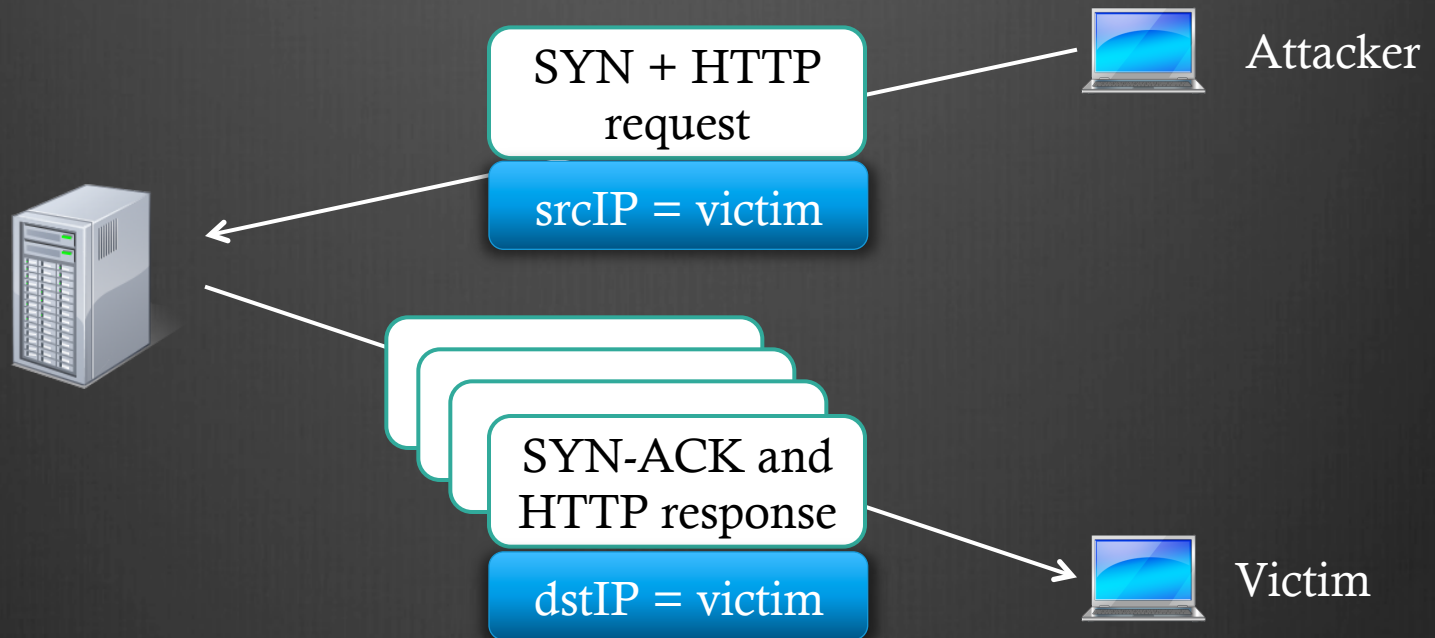
- ⊗ Network duplicates a SYN packet w/ data
- ⊗ Packet gets replayed at the server if previous connection state is not retained
- ⊗ Acceptable for idempotent requests
 - ⊗ Large number of applications can use the feature
 - ⊗ Application level measures for additional safety
 - ⊗ Already required today – users refresh slow pages causing duplicate requests

Server Resource Exhaustion



- ❶ Bogus requests consume CPU and memory at the server
- ❷ Threshold pending TCP Fast Open connections at server
- ❸ Fallback to regular TCP if threshold is exceeded

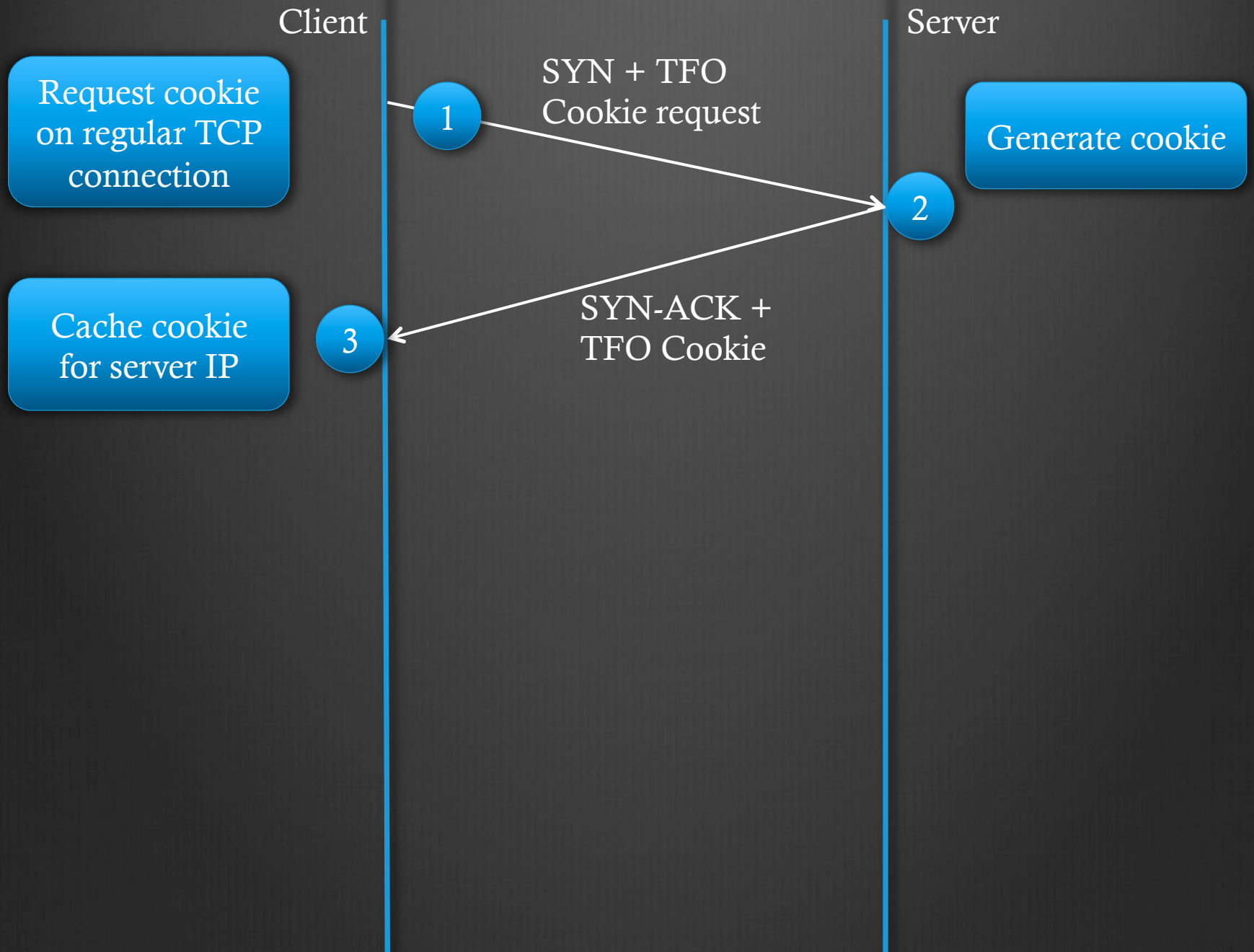
Amplified Reflection Attack



- ⦿ Small SYN packet triggers N response packets to victim

TCP Fast Open Cookie

- ⊗ 8 – 16 byte token
- ⊗ Granted and validated by servers
 - ⊗ Permission to send request in SYN packet to the server
- ⊗ Validates IP ownership of client
- ⊗ Encrypts IP address of client using a server secret key
- ⊗ Expires after a timeout set by server
- ⊗ Transmitted via TCP options



Client

Server

Request cookie
on regular TCP
connection

1 SYN + TFO
Cookie request

2 Generate cookie

3 Cache cookie
for server IP

3 SYN-ACK +
TFO Cookie

TFO connection

4 SYN + TFO
cookie + Data

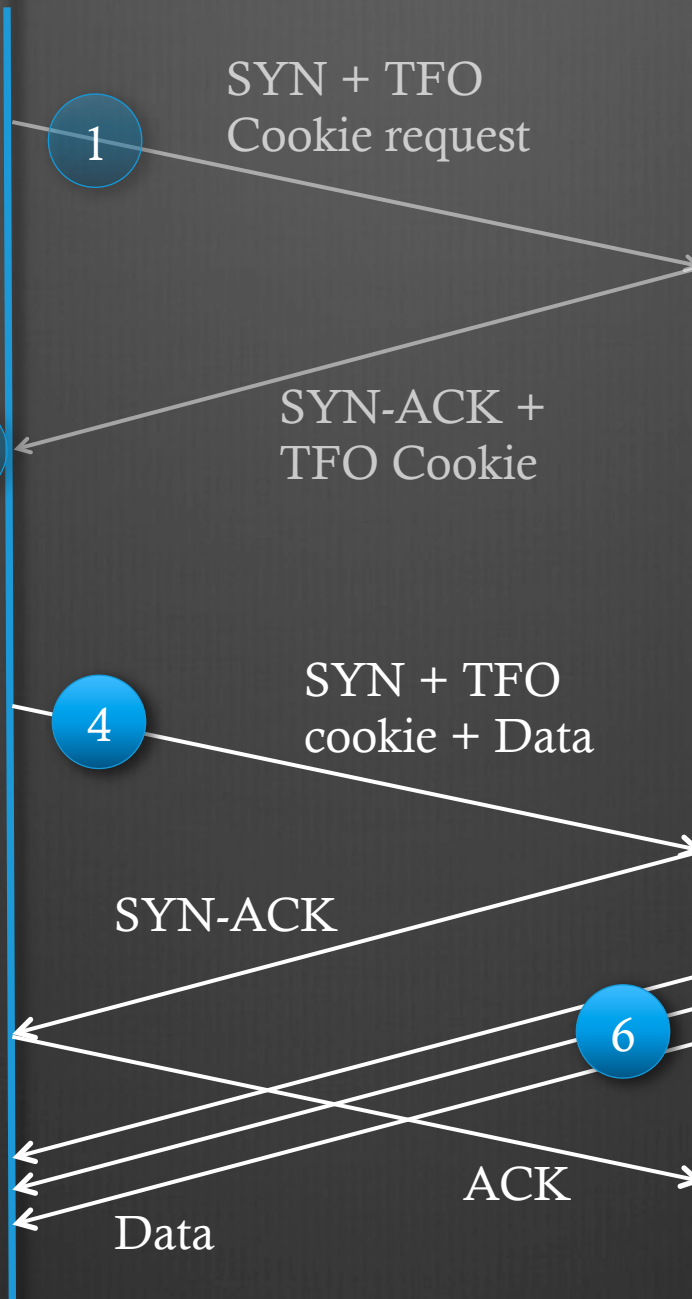
5 Validate cookie
Process data

5 SYN-ACK

6 Send response
during handshake

6 ACK

Data



Amplified Reflection Attack

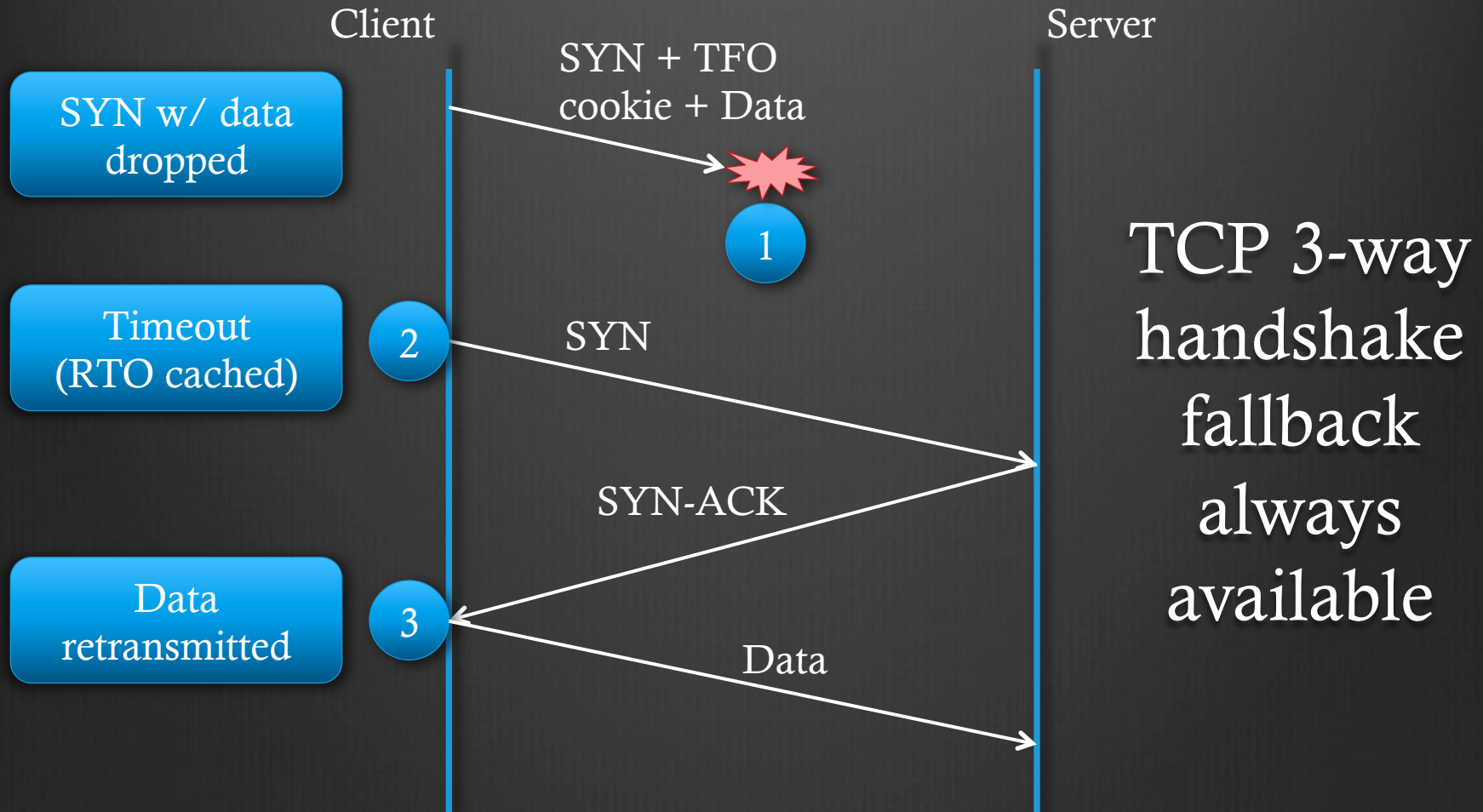
- ⊗ TFO Cookie validates client IP address
- ⊗ Attacker first has to compromise the host to access cookie

Straw man solution (does not require TFO cookies):

- ⊗ Defer sending server response until 3WHS completes
- ⊗ Server may still process request on receipt of SYN w/ data

Middlebox Concerns

Behavior with new TCP options or SYN w/ data



Implementation

- ❁ Kernel – Linux 2.6.34
 - ❁ 2000 lines of modifications to TCP stack
 - ❁ Congestion control not directly affected, only connection setup is changed
 - ❁ AES functions from CryptoAPI for cookie operations
- ❁ Applications
 - ❁ Client – Chrome browser
 - ❁ `sendto()` and `sendmsg()` system calls with new `MSG_TFO` flag
 - ❁ Chrome supports TCP Fast Open since mid 2010
 - ❁ Server – Apache
 - ❁ Socket option to enable TCP Fast Open on listen socket

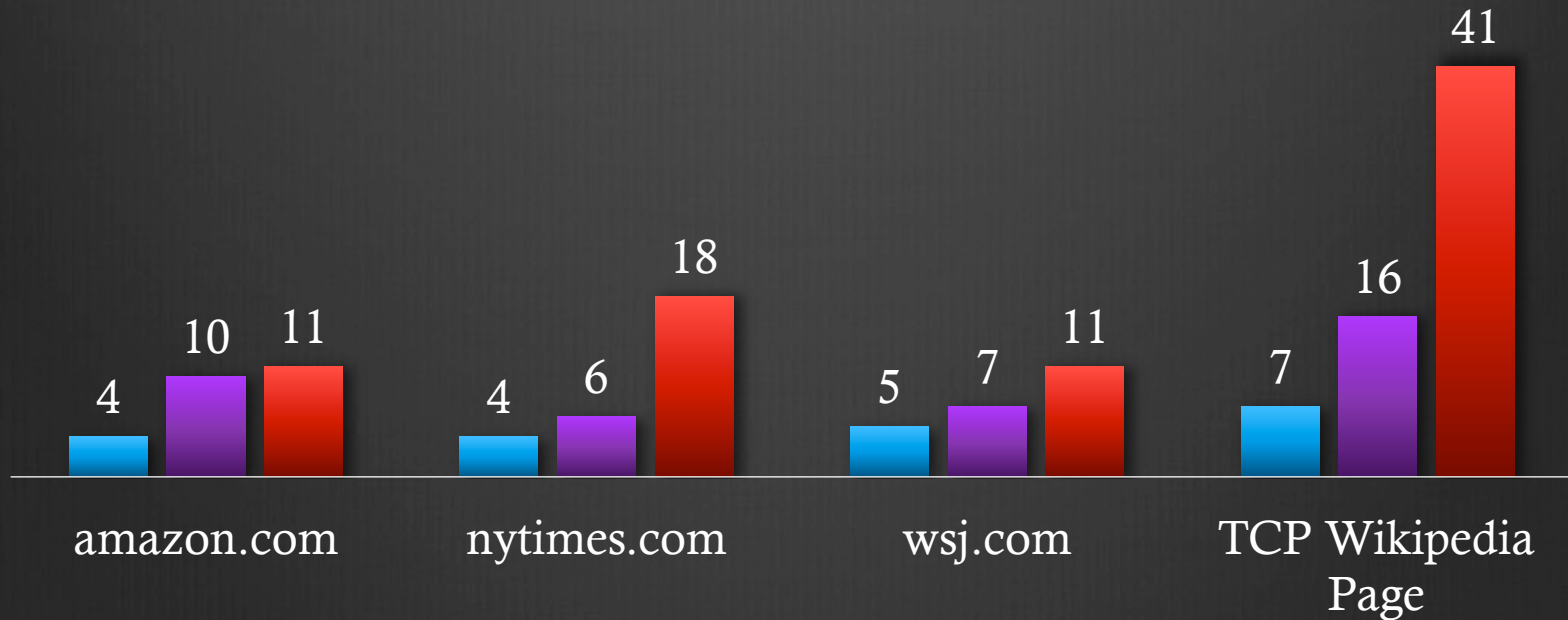
Evaluation

- ⊗ Metric – Page Load Time (PLT)
- ⊗ Web page replay tool – 2 modes
 - ⊗ Record – saves DNS and web pages accessed
 - ⊗ Replay – serves as proxy and serves requests locally
- ⊗ Testbed: 1 x Intel Core 2 Quad CPU 2.4GHz, 8 GB RAM
- ⊗ Dummynet
 - ⊗ Emulate different RTTs – 20ms, 100ms, 200ms
 - ⊗ 4Mbps downlink, 256Kbps uplink, 128KB buffer
- ⊗ Persistent HTTP connections – enabled

Page Load Time

Up to 41 % improvement in PLT

■ RTT = 20ms ■ RTT = 100ms ■ RTT = 200ms



Related Work

	T/TCP	TCPCT – Rapid Restart	ASAP
Motivating application	Transactional RPC	DNSSEC & Web	Web
Additional State	Per client counter	Per client TCB on server	None
Pros/Cons	Insecure; Incompatible with server farms	Per client state; so incompatible with server farms	More generality; computational overhead

Conclusion

- ⊗ TCP Fast Open enables safe data exchange during TCP handshake
- ⊗ Incrementally deployable, backwards compatible, middlebox friendly
- ⊗ 5 – 40% improvement in page load time

Ongoing work

- ⊗ Published IETF draft
 - ⊗ <http://tools.ietf.org/html/draft-cheng-tcpm-fastopen-01>
- ⊗ In the process of deploying at Google
- ⊗ Patch for Linux kernel (soon to be published)

Thank You