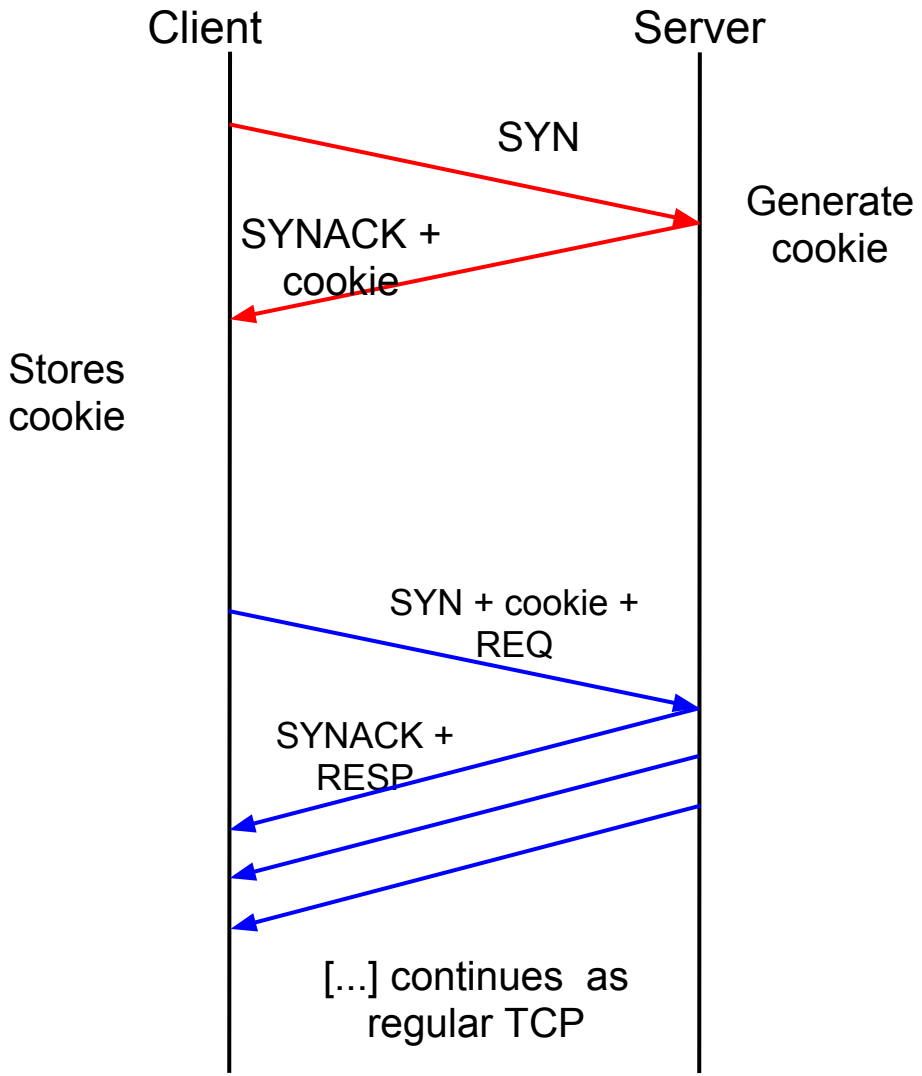
draft-ietf-tcpm-fastopen-04.txt updates

Presenter: Jerry Chu

Yuchung Cheng, Sivasankar Radhakrishnan, Arvind Jain

TCP Fast Open (TFO) fast recap



Server grants nonce

Clients replays nonce with SYN/data

Nonce

- AES_encrypt(cli_IP, secret)
- TCP option (32 - 64bits)

Defend simple SYN-data flood attacks

Warnings of semantic change on the syn-data replay issue

Abstract

… However TFO deviates from the standard TCP semantics in that the data in the SYN could be replayed to an application in some rare circumstances. *Applications should not use TFO unless they can tolerate this issue, which is detailed in the Applicability section.*

2. Data in SYN

… TCP implementations MUST NOT use TFO by default, but only use TFO if requested explicitly by the application on a per service port basis. *Applications need to evaluate TFO applicability described in Section 6 before using TFO.*

6.3.1. HTTP Request Replay

While TFO is motivated by Web applications, the browser should not use TFO to send requests in SYNs if those requests cannot tolerate replays. One example is POST requests without application-layer transaction protection.

New Appendix:
socket API appendix

1. Client: MSG_FASTOPEN flag for sendto() or sendmsg()

2. Server: TCP_FASTOPEN setsockopt() Socket Option

Design rationale: Any better alternative?

E.g., keep connect()/sendmsg() sequence but make connect() return immediately...

Pro: no API changes

Con: incompatible error return

New section:
Open areas for experimentation

1. Performance impact due to firewalls / NAT
   a. Drop of SYN data
   b. Client using different public IP on new connection behind (carrier-grade) NAT

2. Cookie-less Fast Open
   a. Cookie not needed on some services

New subsection: browser pre-connect in related work

Speculative connect to achieve same goal as Fast Open

1. Default on Chrome, Firefox, and IE
2. Simple hack to achieve same goal as Fast Open
3. Force servers and NAT to drop idle connections faster due to load increase
   a. Browsers timeout if NAT drops silently
4. Not a good network / transport solution

Next Step

Comments?

WGLC?