draft-ietf-tcpm-fastopen

Updates from -01 and IETF84
Yuchung Cheng

IETF 85. Nov 6, 2012

Clarification of dup SYN-data issue

Data in SYN may be replayed

1. The server receives the duplicate and the original before and after reboot
2. The server receives the duplicate after the connection has been closed by the client (no 2MSL protection)

But network duplicate or client reusing same port and ISN is rare. Also TCP never guarantees once-only semantics

Sec 6.3: reflection attacks behind NAT

Attacker (sharing the src IP) can obtain valid cookies to launch reflection attacks

- But shared path == shared fate
- Or he can just request tons of junk

Idea (Briscoe): adds TS into cookie validation so server can tell good guys from bad guys

- But an attacker can just get more new cookies

In the server needs to rate-throttle based on IP

Misc

Null cookie: server can optionally return a null cookie to signal TFO support

Interim option number: 254 /magic 0xF989 (draft-tcpm-experimental-options.txt)

Stuff after -02

Concerns on congestion

- TFO does NOT change congestion control

- But the initial send in handshake can not react to SYN-ACK loss (but subsequent sends do)
  - Linux never changes IW on (first) SYN-ACK loss
  - Syn-cookie also won't

- But we'll mention this

Negative caching in Linux 3.7

TFO biggest risk is middlebox drops SYN with data and/or new options

- Stripping data or option is totally OK
- Such drop can detected precisely b/c TFO retries with pure SYN
- On recurring losses disable TFO for (1sec << losses)

Path change so cached MSS is invalid?

- ICMP need-frag and you retry with new MSS

WGLC

Ready?

Please try TFO out by downloading Linux 3.7!

Soon Google.com will happenly process your data in the SYN packets :)