Version negotiation

A strawman

By Watson Ladd, Cloudflare

What do we need?

- No downgrade: an attacker cannot produce a weaker version choice
  - In general impossible: if a version is too weak, so attacker can rewrite transcript, explodes
- “Best” possible outcome
  - Server and client dependent
- Not all versions have compatible initial packets
- Not all initial packets work with versions client is willing to speak
- Latency cost of getting it wrong
- Size of first flight matters

What does incompatible mean?

- Can we require all servers can extract the list of supported versions from any initial packet?
- Or do we need to require that initial version number, if unsupported, is only part server looks at?

TLS style

- Client lists its supported versions
- Server picks and sends in response
- Part of transcript
- This is enough: attacker cannot modify versions or selection

Problem: compatibility

- Easy: Client may speak versions X and Y, but have sent a first flight compatible only with X
- Harder: Client may speak X and Y, have sent a first flight compatible with X and Y, but server disagrees with that assessment
- Hardest: Client speaks X and Y, has sent first flight compatible with X, but server thinks it’s compatible with X and Y

Tentative solution

- Easy case is easy
- Harder case: server selects X
- Hardest case: don’t do it
  - Version Y must define what flights are compatible with it in way that is easy to implement correctly

Psych and Brown Sticker

- Latency induced when server doesn’t like any version compatible with opening
- Tradeoffs when server would like a version that is supported but not offered, but got something they are ok with in offer
- Pysch: advertise desired versions in HTTPSVC and remember preferences
- Brown sticker: let client know that you would actually like something different, have them initiate another connection for ensuing requests

Simplifying the problem

- Everything is easy if most is done in extensions
- Few versions with commonly understood ordering

Any Questions?