Request mTLS

Jonathan Hoyland
Distinguishing Bots is Hard

- Many bots come from public clouds
- Bots distinguish themselves by setting a special user agent
Distinguishing Bots is Hard

- Both these signals are easy to forge
CertificateRequest lets us Identify Bots

- Mutual TLS needs to be initiated by the server
- Post-handshake auth and Exported Authenticators add an extra RTT
But Humans might be confused

- If we incorrectly send a CertificateRequest to a human they probably won’t know what to do
Request mTLS Flags

- Configure the client to send a hint when a client certificate is available
- TLS Flags is perfect for this
Questions?

- Do people think this is useful?
- Is there interest in working on this?