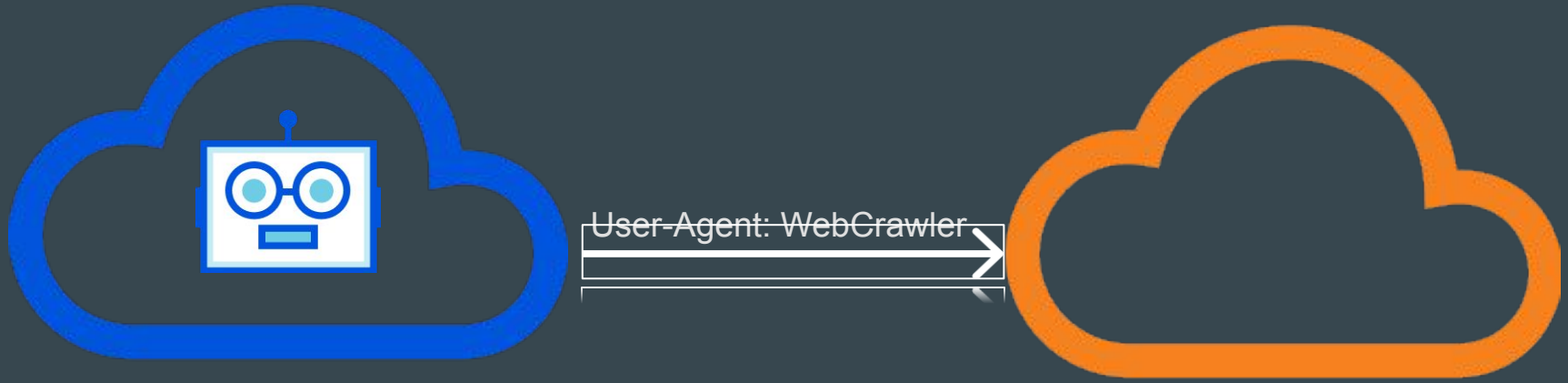
Request mTLS

Jonathan Hoyland

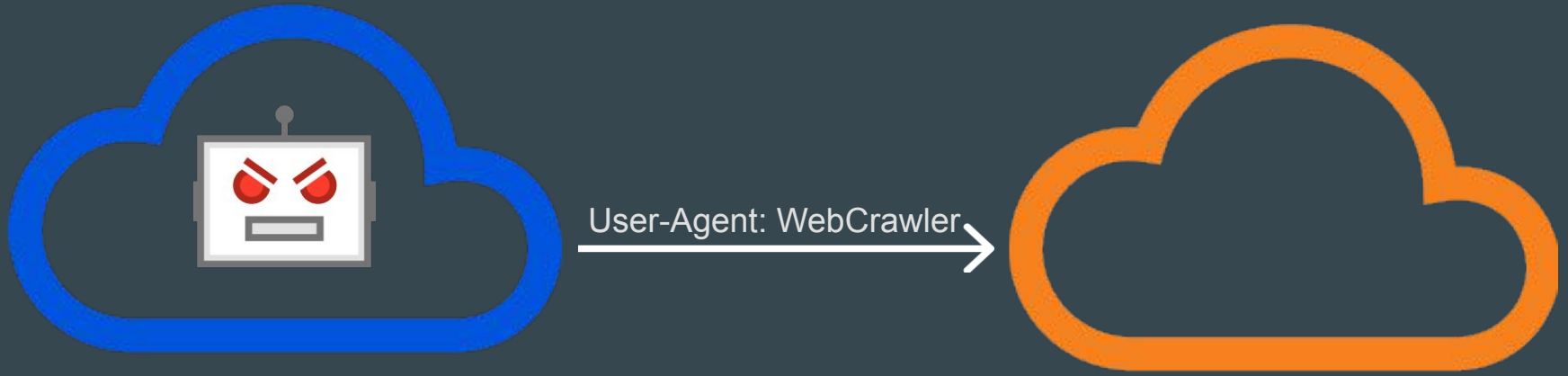
Distinguishing Bots is Hard

- 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

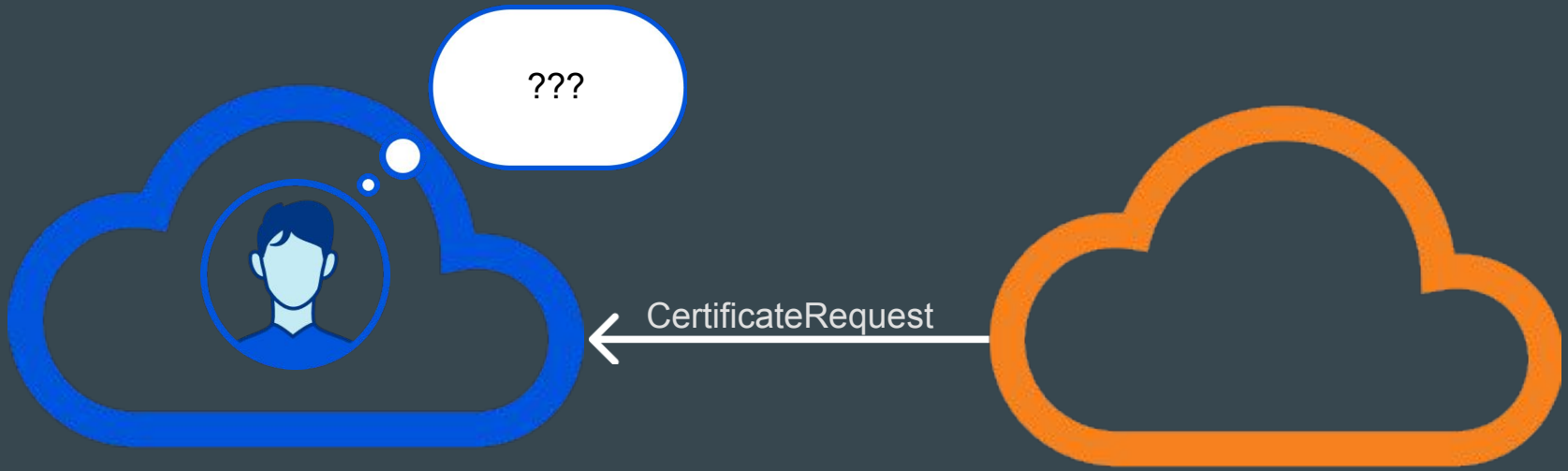


CertificateRequest lets us Identify Bots

- 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

Why Adopt Here?

- Feedback that the exact semantics of the flag are unclear
- Discussion on use cases
- Drive TLS Flags by providing a use case
- Point allocation dependant on expected frequency

Questions?

...

We have three working interoperable implementations (C, Go, and Python)
Demo server running at https://tls-flags.research.cloudflare.com/
If you send the TLS Flags extension with flag 80 (0x50) set it will ask you for a certificate
Adoption call?