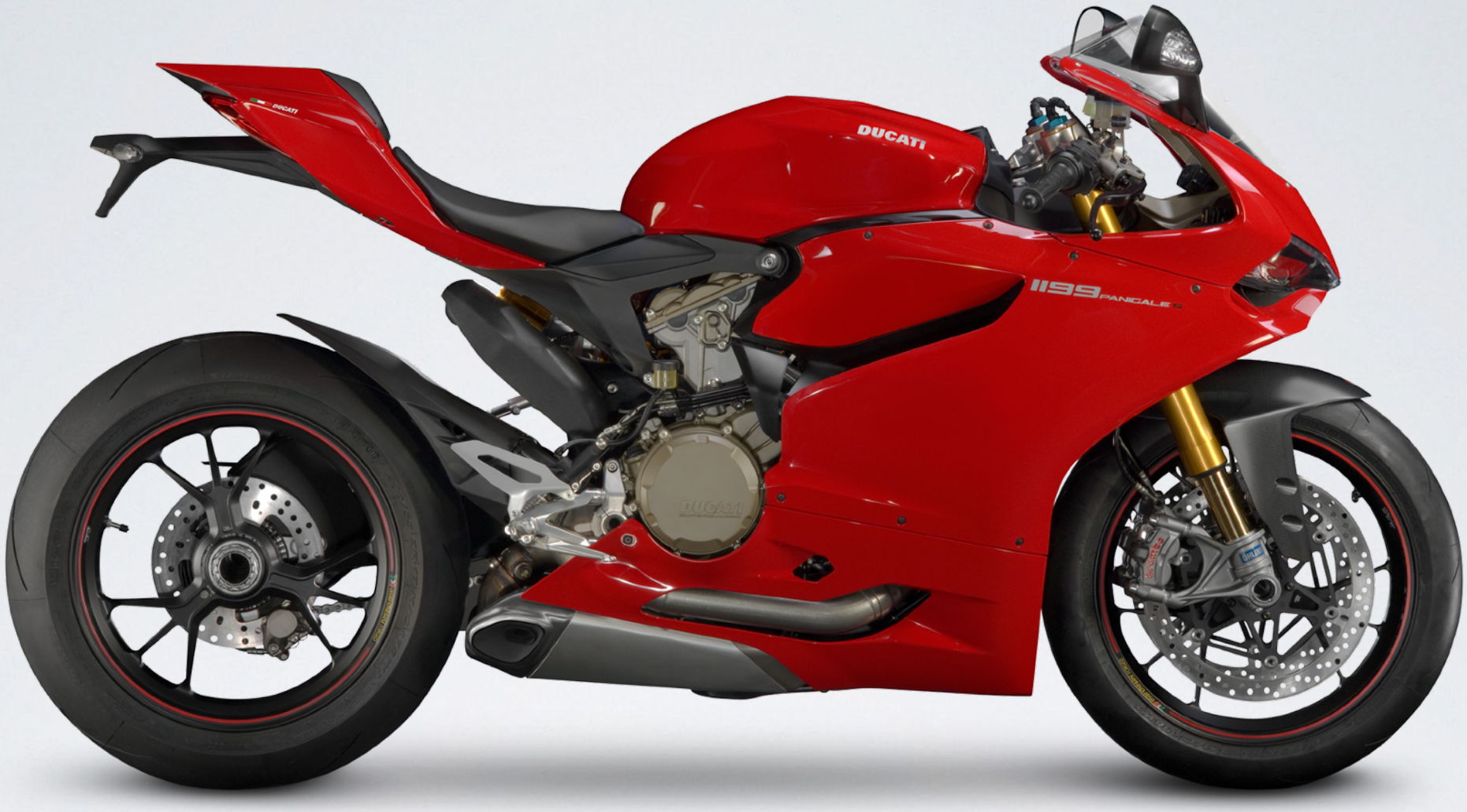
IETF 100

HACKATHON

TLS 1.3

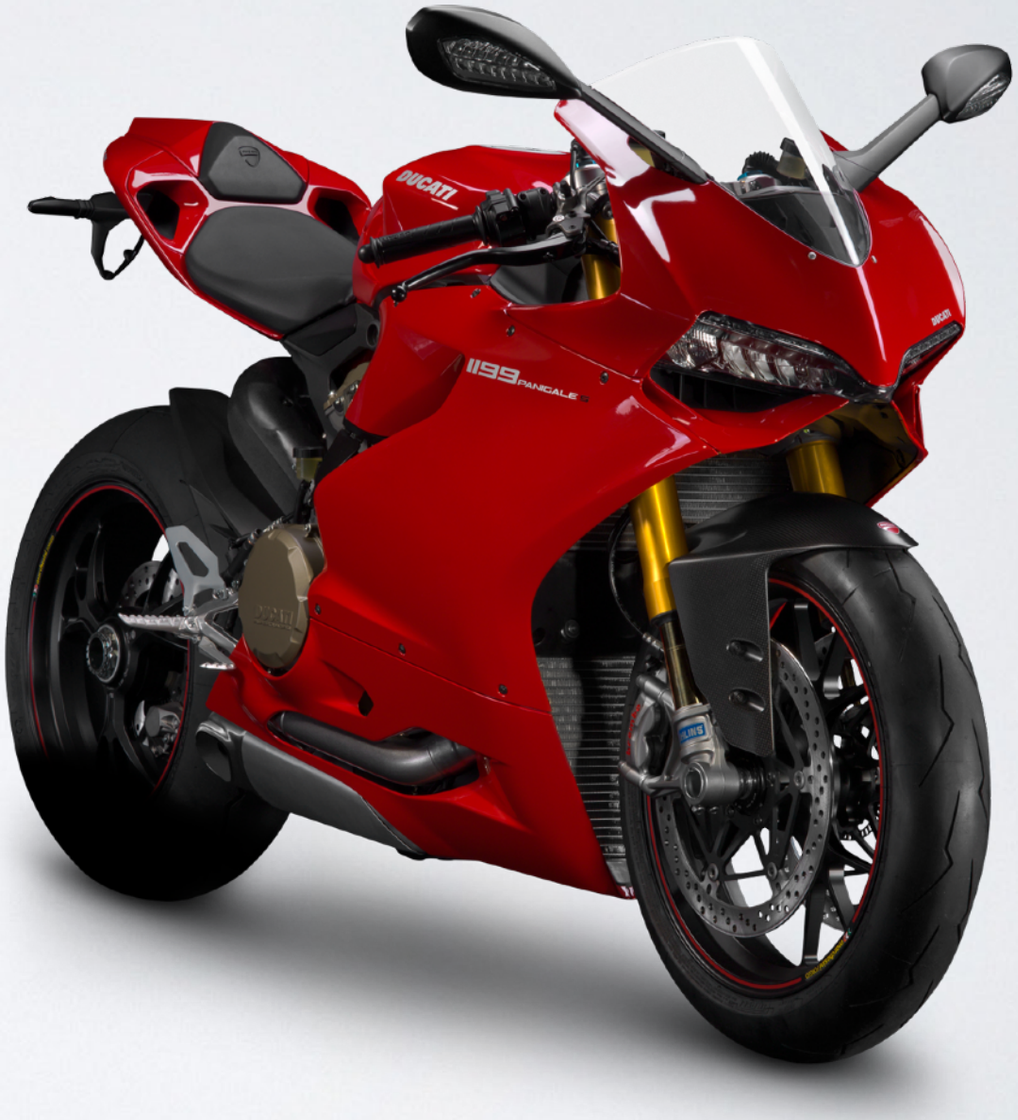


THE FINAL LAP

Deploying TLS 1.3

GOALS

- Interoperability
  - TLS 1.3 Draft 21 plus middlebox compatibility patch (#1091 on Github)
- Application integration
  - Proxies, debugging tools, development tools



TEAM

- 16 in Singpore
- 8 remote participants
- Japan, London, Mauritius (hackers.mu)

APPLICATIONS

- Wireshark, stunnel, wget, curl (w/ WolfSSL D18)
- Monit, Stunnel, Hitch, Aria2c, Nagios-plugins, Ftimes (D21)
- Envoy (D21+)

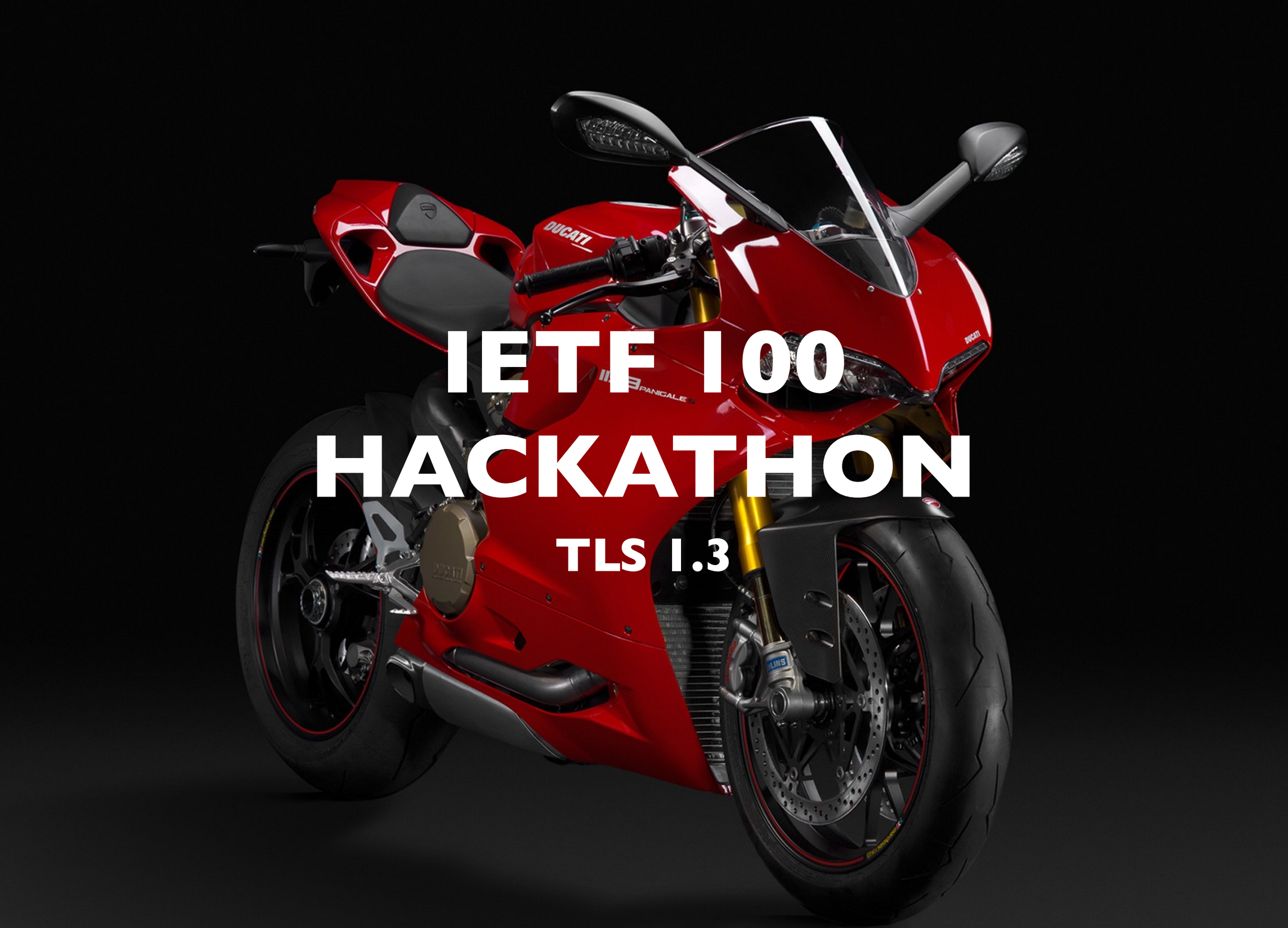
TLS INTEROP

F = Full Handshake, R = Resumption, H = HRR, Z = 0RTT, “-“ = 21 only

Client\Server	NSS	BoringSSL	OpenSSL	TLS-tris	Envoy	Fizz	Haskell 1.3	picotls	mint	mbedTLS
NSS		F								FH-
BoringSSL		FRHZ	FRHZ		FRHZ	FRHZ	FRZ	FRHZ		
OpenSSL		FRHZ	FRH(Z)			FRHZ		FRHZ		
TLS-tris		F-		F-				F-		
Fizz										
Haskell 1.3		FRZ						FRHZ		
picotls		FRHZ			FRHZ	FRZ	FRHZ	FRHZ		F-
mint				F-						F-
mbedTLS	F-							F-	F-	

TAKEAWAYS

- TLS 1.3 is closer than ever to releasing
- Ready for more experiments with middleboxes
- Integration into a wider variety of applications
- A strong network of implementers



IETF 100 HACKATHON

TLS 1.3