JENS NEUHALFEN

DATABASE

DATABASE

APPLICATION

APPLICATION

TLS

TLS

GOOD CRYPTOGRAPHY

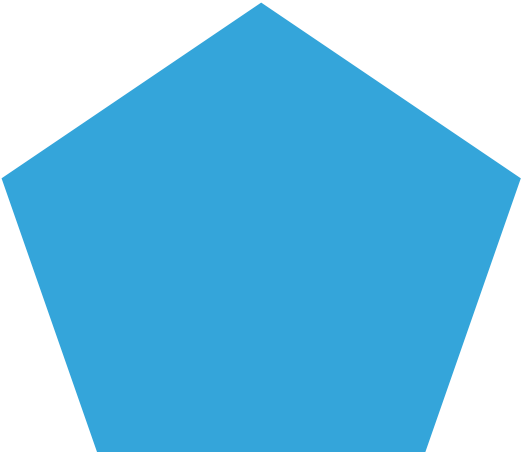
YOUR FATHERS CRYPTO (*)

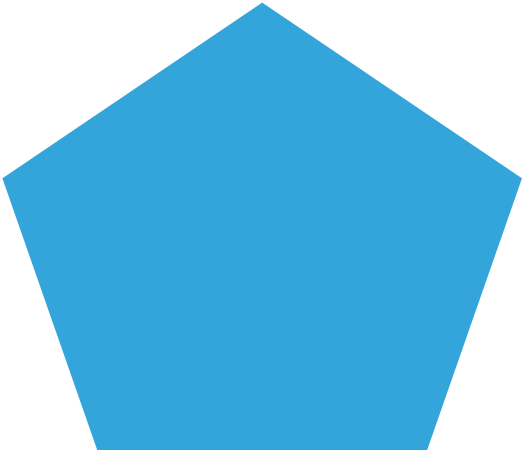
- CLIENT sends request
- APPLICATION applies logic
- DATABASE stores result
- Transport encrypted via TLS

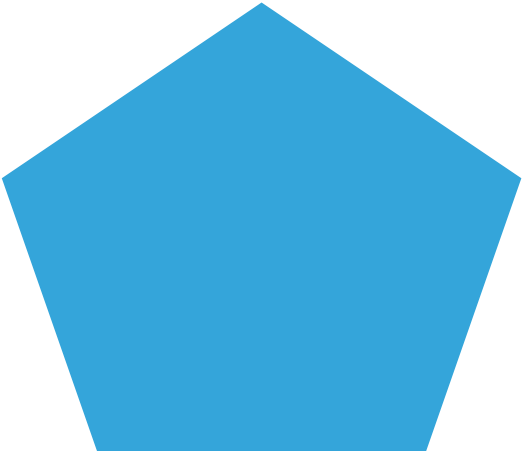
CLIENT

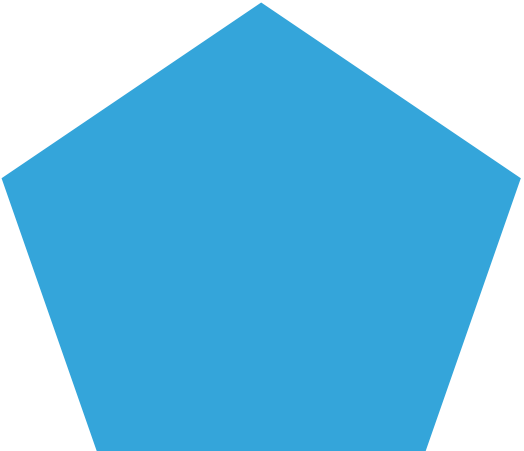
REQUEST

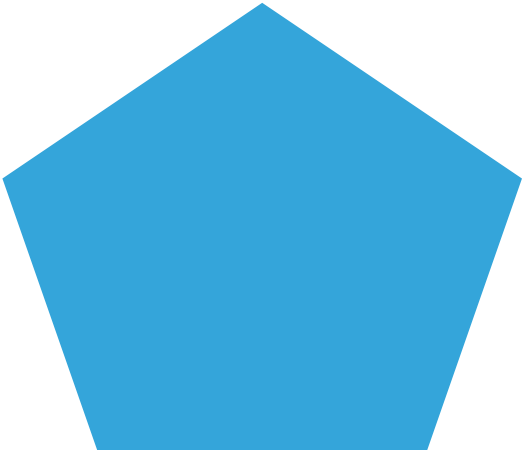

DATA

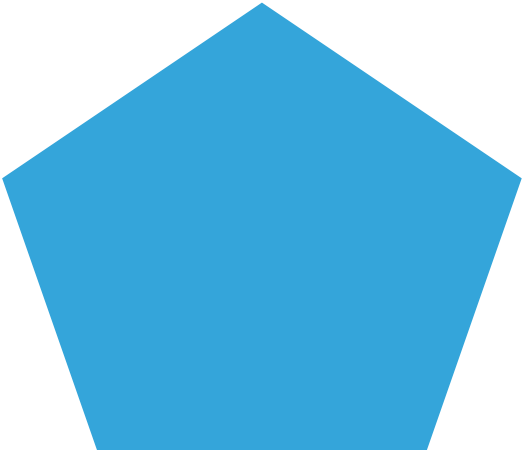


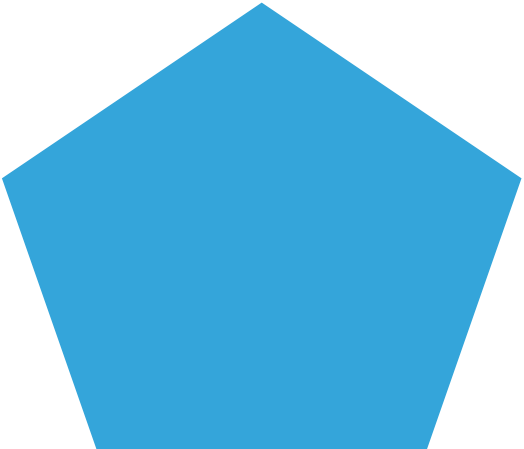


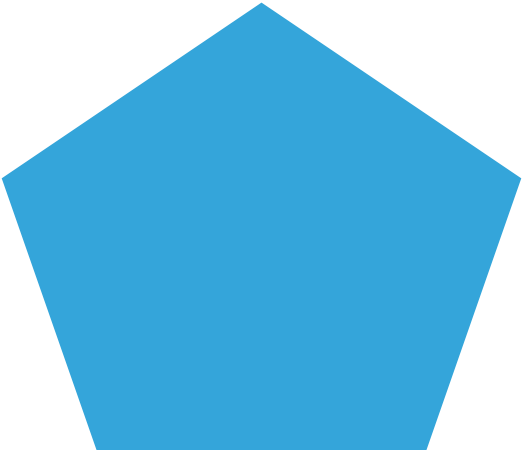


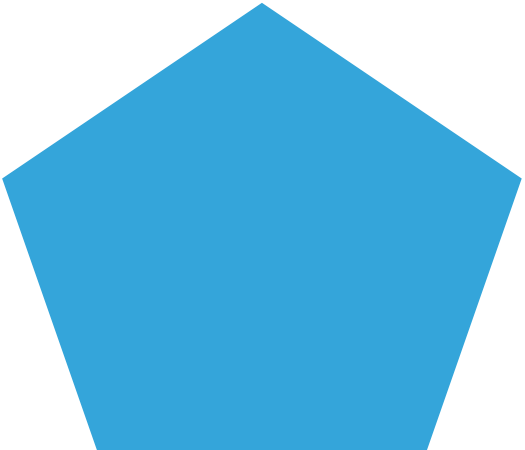


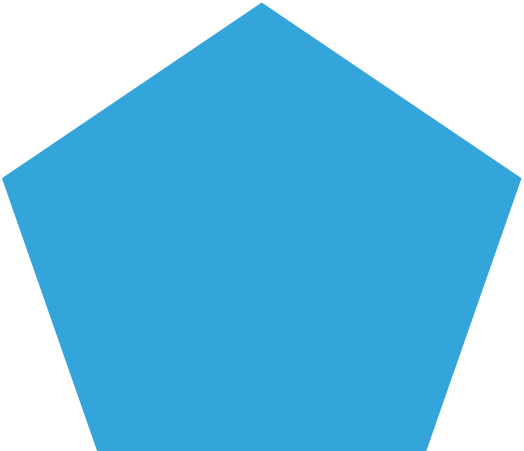


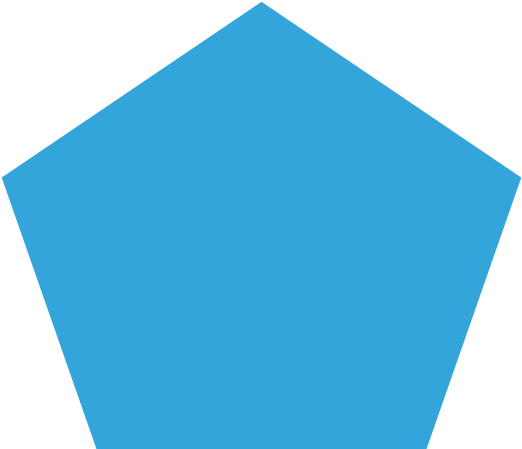












TLS

TLS

(*) I’m going to gloss over the whole cryptography nomenclature in these first slides. Bear with me.

9

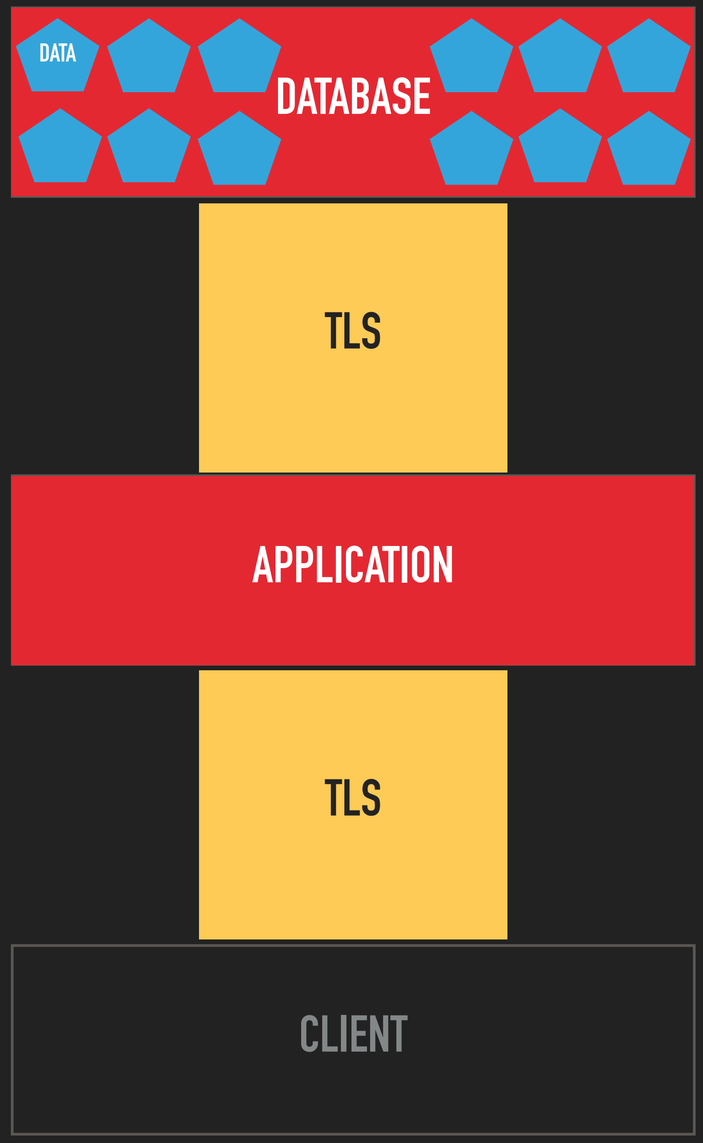
SO, EVERYTHING IS SAFE?


DATA

YOUR FATHERS CRYPTO (*)

- CLIENT sends request
- APPLICATION applies logic
- DATABASE stores result
- Transport encrypted via TLS 🔒

SO, EVERYTHING IS SAFE?



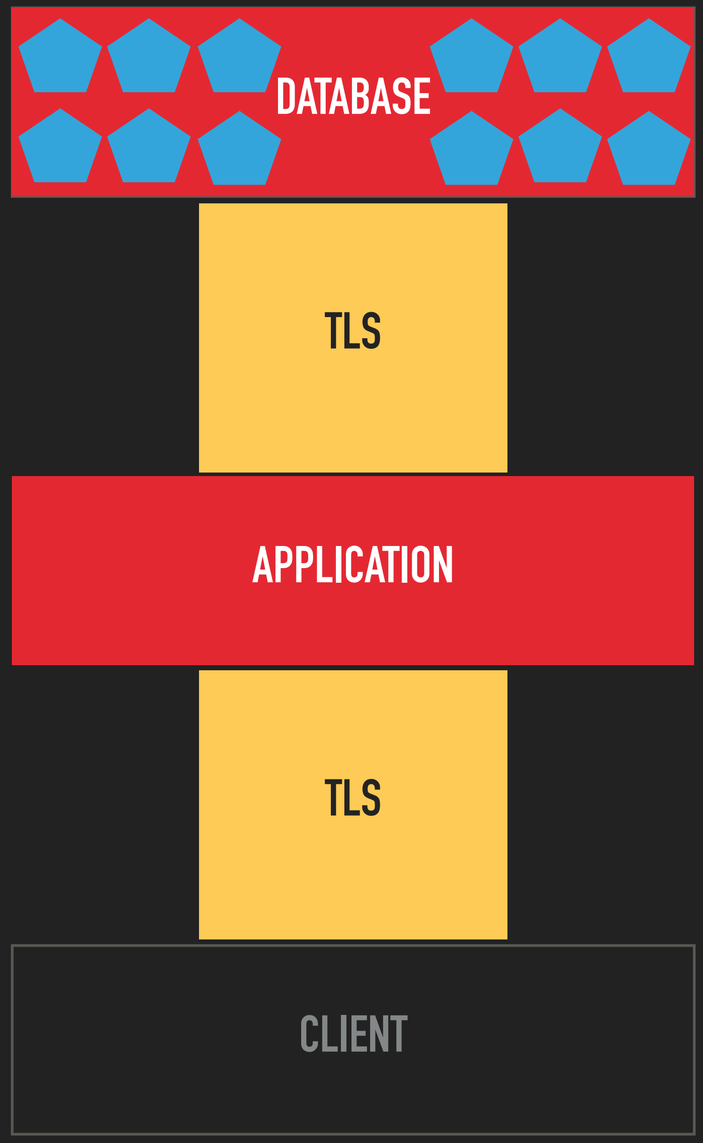
(*) I'm going to gloss over the whole cryptography nomenclature in these first slides. Bear with me.

WHAT ABOUT TLS?

- Data is at rest for ~99.99998% of the time (*)
- Also: Heartbleed, POODLE, DROWN, Lucky13, Logjam, FREAK, …
- Also: Backups!

WHAT IS THIS ABOUT?

- Protect** data ‘itself’
- E.g. encrypted** data at rest
- Even: Protected** data while working with it



(*) 10s transit / 2 years storage (**) Cryptographically protected - details later!