



JENNER

DATABASE

DATABASE

APPLICATION

APPLICATION

TLS

TLS



YOUR FATHERS CRYPTO (*)

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

CLIENT

REQUEST

A solid blue pentagon with the word "DATA" centered inside in white, bold, uppercase letters.

DATA









TLS

TLS

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

1

0



SO, EVERYTHING IS SAFE?

A solid blue pentagon with the word "DATA" centered inside in white, bold, uppercase letters.

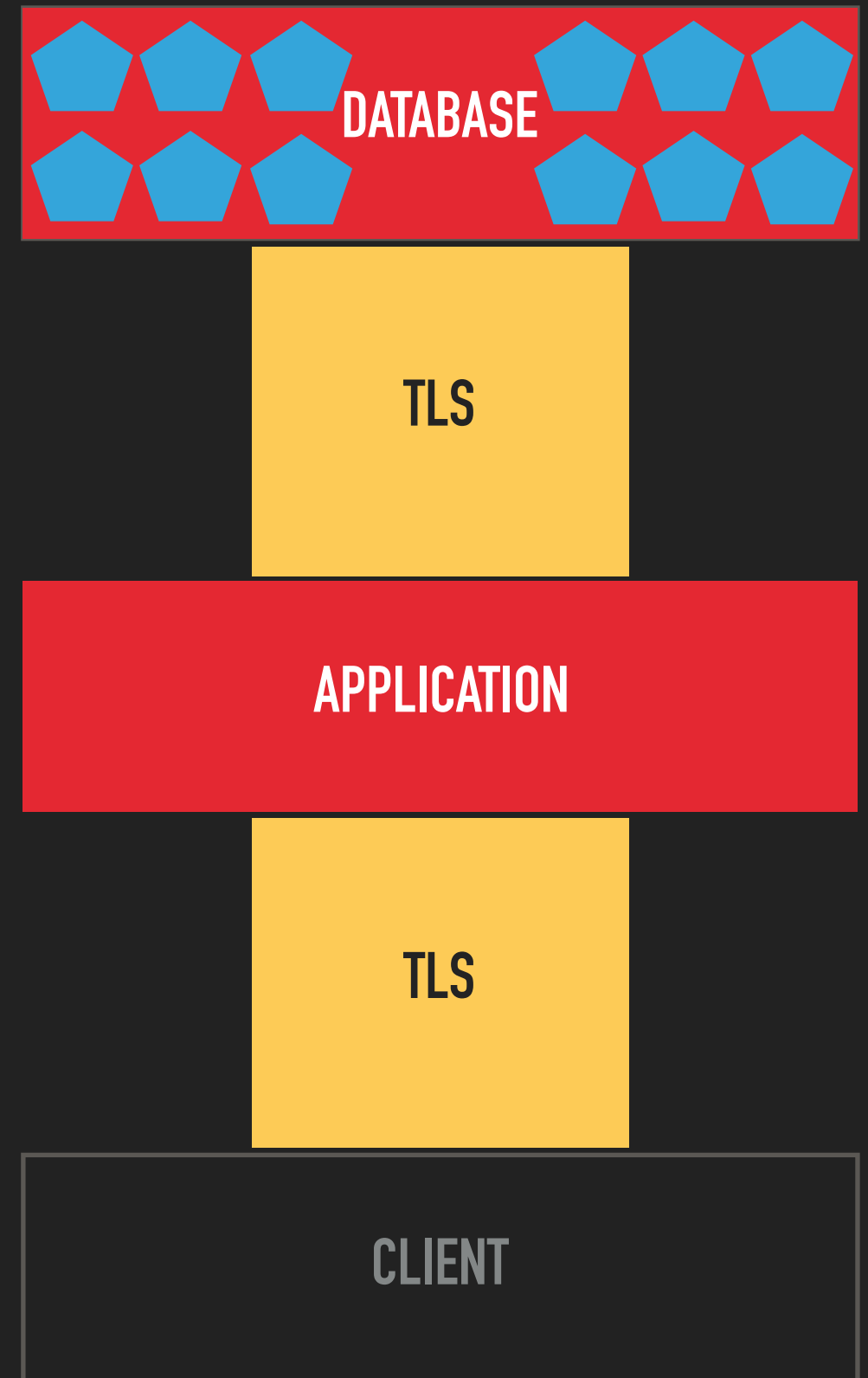
DATA

WHAT ABOUT TLS?

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

WHAT IS CONTENT ENCRYPTION?

- ▶ Encrypt** data 'itself'
- ▶ E.g. encrypted** data at rest
- ▶ Even: Protected** data while working with it



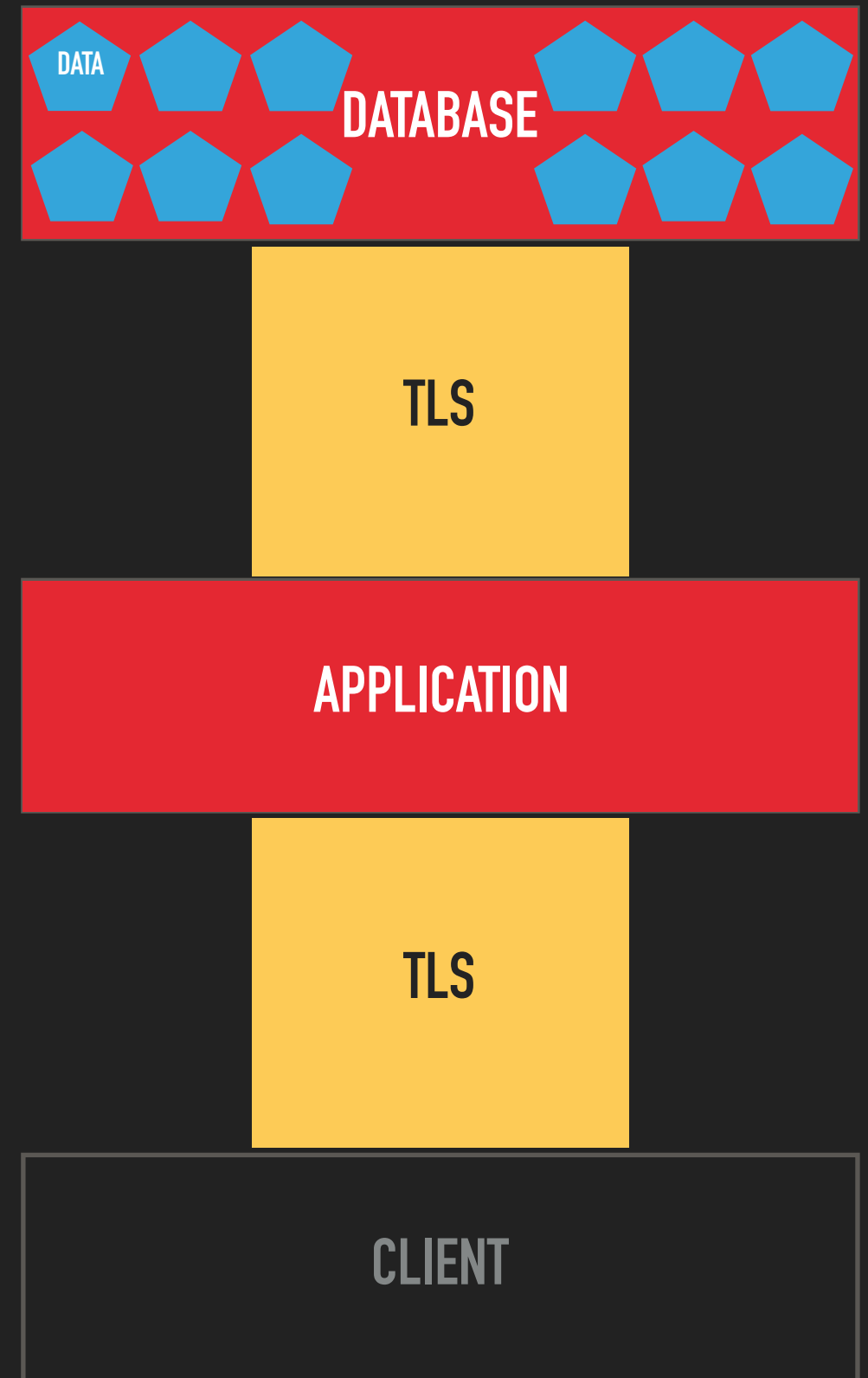
(*) 10s transit / 2 years storage

(**) Cryptographically protected - details later!

YOUR FATHERS CRYPTO (*)

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

SO, EVERYTHING IS SAFE?



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