

adventures in paranoia with `sinatra` and `sequel`

Eleanor McHugh
@feyeleanor
<http://github.com/feyeleanor>

disclaimer

- I am not a certified security professional
- and it's unlikely you are either
- what follows is definitely above our pay grade
- so if privacy matters to you - and it should!
- hire a certified security professional
- and allow six months for them to do their job

trust

- how can we believe our are visitors who they claim to be?
- how can visitors believe our claims to store data securely on their behalf?

identity

- the basic foundation of trust

security

- authenticate
- authorise
- store identifying data securely
- maintain private communications
- separate concerns

- how to obfuscate data using OpenSSL
 - symmetric and public key cryptography
 - hashing algorithms

- designing databases for privacy
- Sequel & encrypted keys in the relational model
- meta-programming for ease & consistency
- searching encrypted data

- the transport layer
 - Sinatra
 - Rack middleware
 - HSTS
 - cookies
 - SSL & certs