**Design Document**

**Threat Model:**

1. Compromised database files, physical access to server (but not client)
2. Dolev-yao attacker

**Database Design:**

users = username : {password, pwd\_salt, key\_salt}

data = username : encrypted\_fields

**Protocols:**

REGISTER

C: h = sha256(pwd), K\_c = pbkdf2(pwd + key\_salt)

C -> S: (username, h, key\_salt)

S: check if username exists, gen pwd\_salt, x = hash\_&\_salt(h), store (username, x, pwd\_salt, key\_salt)

S -> C: 200/401

LOGIN

C: h = sha256(pwd)

C -> S: (username, h)

S: verify(username, h), auth\_cookie = hmac(username, h, timestamp; K\_s) , timestamp

S -> C: 200, key\_salt + auth\_cookie OR 401

C: K\_c = pbkdf2(pwd + key\_salt)

VERIFY(username, h)

S: get pwd\_salt from db, x = sha256(h + pwd\_salt), return stored pwd == x

AUTHENTICATION

C -> S: post\_data + auth\_cookie

S: check hmac(username, h, timestamp; K\_s) auth\_cookie, check timestamp expiration

continue handling post data…