Office Hours 11/16

Wednesday, November 16, 2022 8:18 PM

HTTPS does not protect you against comprised clients

Keyloggers

Point of sending vulnerability

Packet-level man in the middle

Code is executing in thread, anything else can read the process the moment you exit

Multiple types of encryption

Assymetrical

Public key encryption

Not recommended

Symmetrical

Secret value used in encryption and decryption

1 single key

Trying to make sensitive information masked

How to send key in secure way, not as plaintext

Client should be able to unscramble the key

Integration Test for Registration

- Still using the code we wrote to test encryption
- Test saving part separately
- One object for all of cryptography
- One object for validation
- One object for account creation

Arrange: original value, encrypted value (mock input)

Client requirements

- Handling an email if its below 8 characters
- Possibly want to use an external value that's uniquely identifying
    - Email, phone number
- Password:
    - We can restrict it more if we want it to

OTP

- Turn it in as its own thing to maximize code reuse

BRD Revision

- Don’t need to send the whole thing, but focus on a section at a time
    - Iterative feedback

Registration is not considered an artifact for milestone 3