

Browser

Server

encrypted
comm.ask for
email
page

login page

send
login

password page

send
password

account info

A - encr. msg

attacker
is listening
record theseEncryption1. Verify
w/ CA2. Set up
symm. encryption

3. key exchange

Replay
Attack

-different keys

-2FA

email page?
login

A

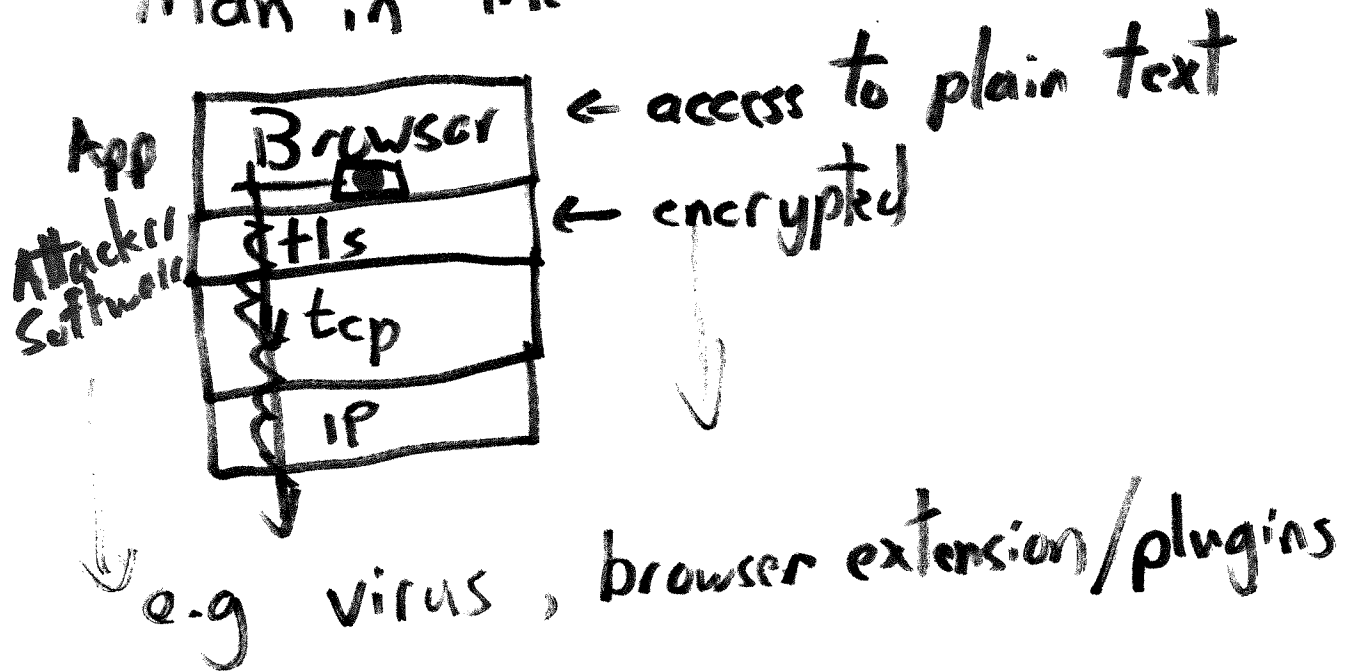
pwd
page

B

account
info

2. Man in the Middle (MitM)
- take over network hardware
e.g. router/switch
 - preassigned admin password
(must be changed!)

Man in the Browser (MitB)



Anti-virus scan
cve.org (look up)

- ③ Denial of Service (DoS)
- prevent access (availability)
 - break the server
 - overload a device
(make it busy)

Distributed DoS (dDoS)

- multiple attacks