Security

Securing the computer
1. O.S./software
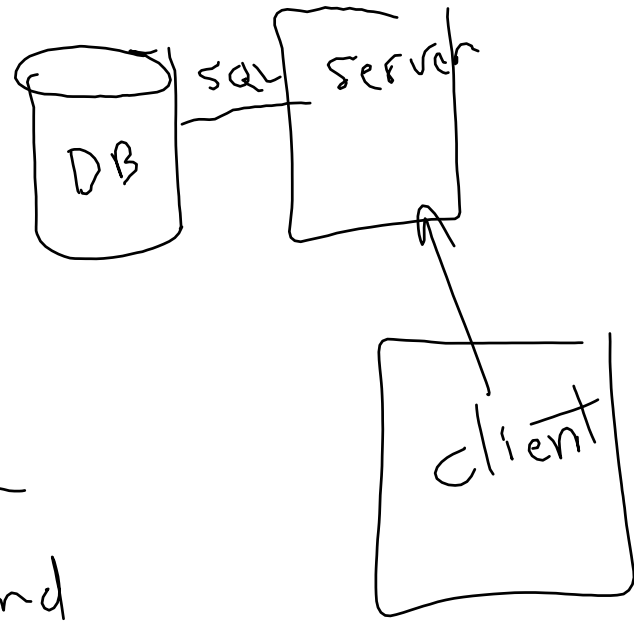
2. Physical

3. User

4. Network

Attacks

- DDoS
- Phishing
- SQL injection

user= 'aname', and
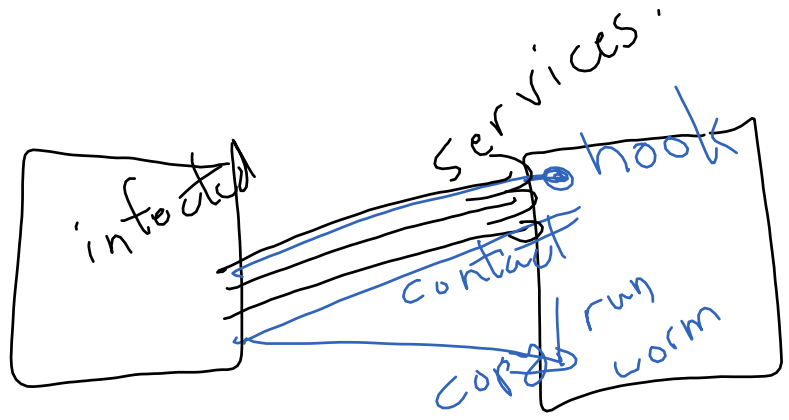pwd=' _____

pwd=

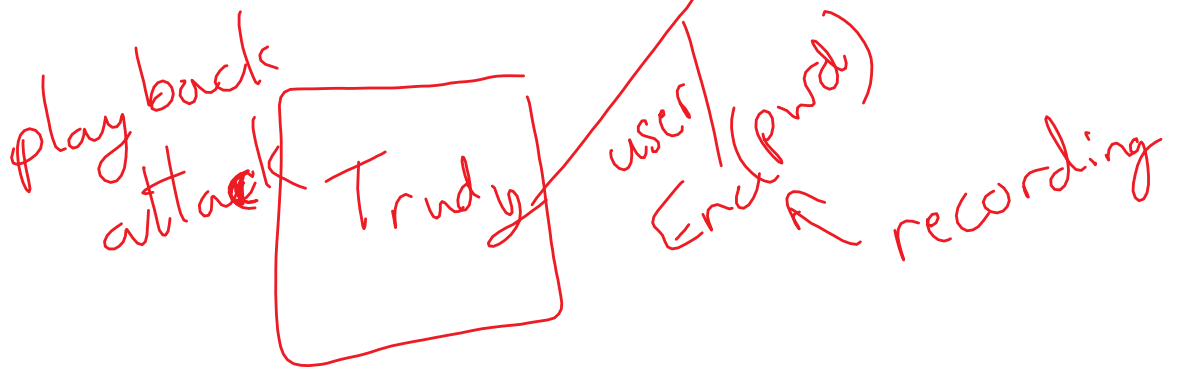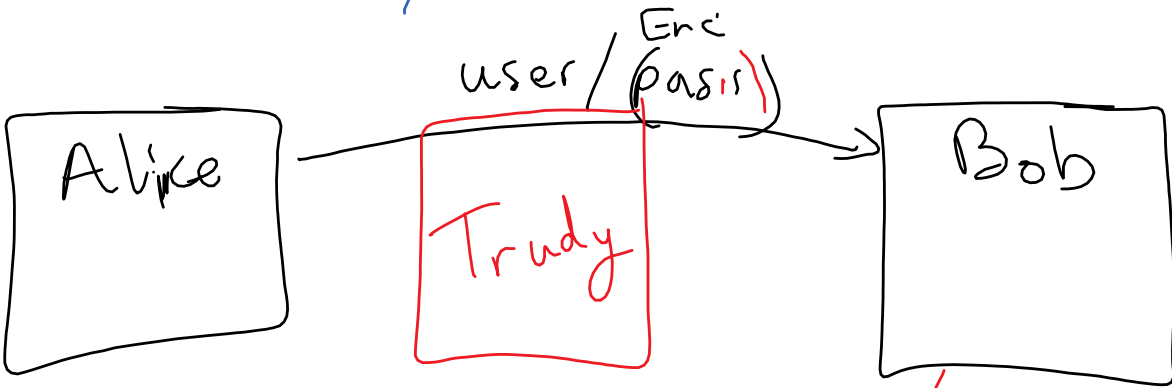\' OR TRUE; --   comment

prepared statement

- cross site scripting
- trojan horses

...vices?

- virus

- worms

infected   services: hook

contact

cord/run   worm

Network/ Communication

Alice

Trudy

Bob

user / Enc(pass)

playback attack

Trudy

user/ Enc(pwd)

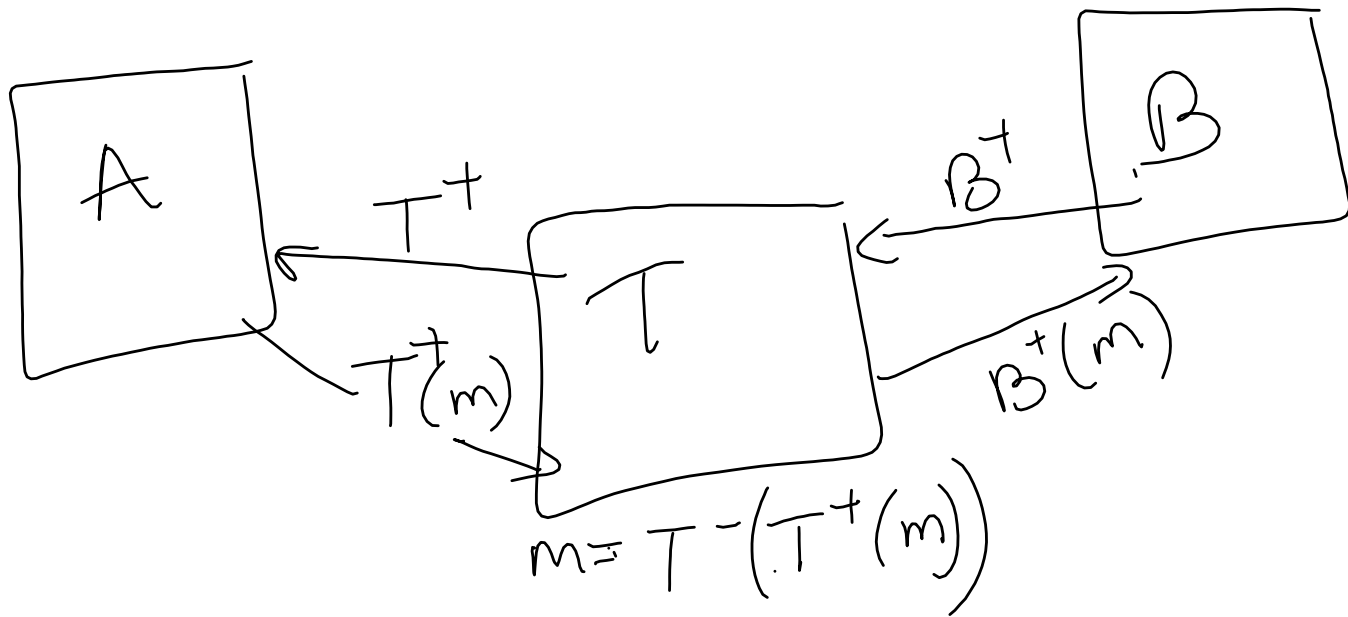recording

Cryptography

- symetric key (shared)
- asymmetric key
                public key

Alice
A^+ - public key
A^- - private key

Bob
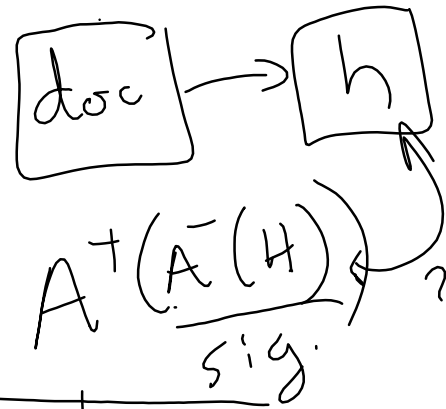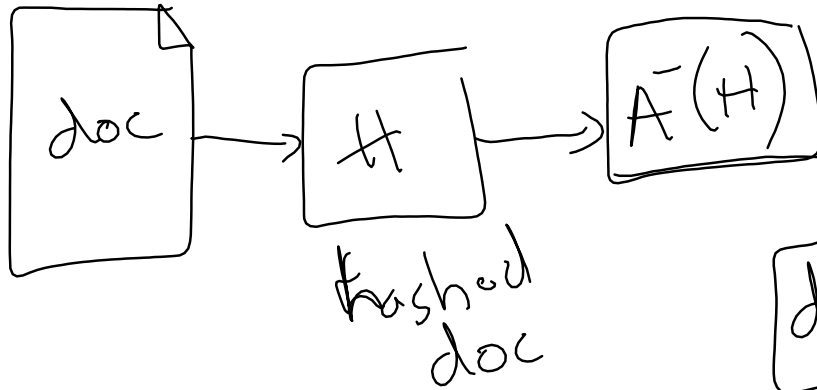B^+, B^-

send msg, m $\xrightarrow{\quad B^+(m) \quad}$ rcv. msg

$m = B^-(B^+(m))$

A

T

B

T^+

$T^+(m)$

B^+

$B^+(m)$

$$m = T^-(T^+(m))$$

Digital Signatures

A:

doc $\longrightarrow$ H (hashed doc) $\longrightarrow$ $A^-(H)$

doc $\longrightarrow$ h

$A^+(A^-(H))$
sig.   ?

Certificate Authorities