Lec5_Password Security

- rainbow tables

hash = h(salt || password) - random salt but not secret

bcrypt - Password-specific hash functions

entropy

- random password

- H = log2(N^L)

password strength meter & Database breaches

Passphrase

complexity: (word list size) ^ words

OTP

HOTP: HOTP(K,C)=HMAC-K(C)

- pre-share K between user and server

TOTP: C = lower bound(T/Tx)

T = current timestamp

Tx = length of one time duration

Disadvantage

- plaintext code displayed
- phishing

- vulnerable to attack if phished
- shared secret may stored plaintext on server

FIDO2(U2F)

FIDO2 = web authentication standard + FIDO client to authenticator protocol

- Relies on a cryptographic authenticator
- resistant to phishing attempts, replay attacks, and server breaches.