



Authentication by Passwords

Prof. Ravi Sandhu Executive Director and Endowed Chair

Lecture 16

ravi.utsa@gmail.com www.profsandhu.com



Authentication Techniques





Something you know

Something you have

Something you are

password "secret" questions

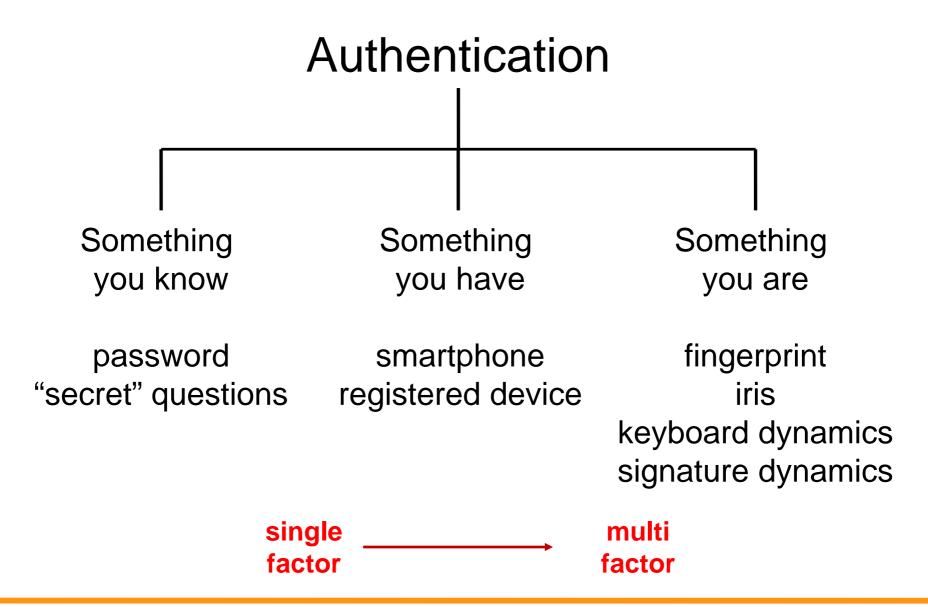
smartphone registered device

fingerprint
iris
keyboard dynamics
signature dynamics



Authentication Techniques











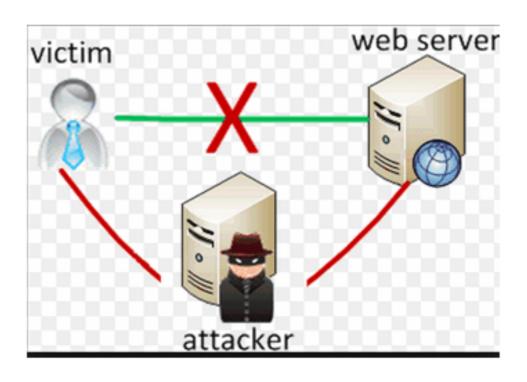


Personalized image to authenticate webserver to user



Phishing Man in the Middle



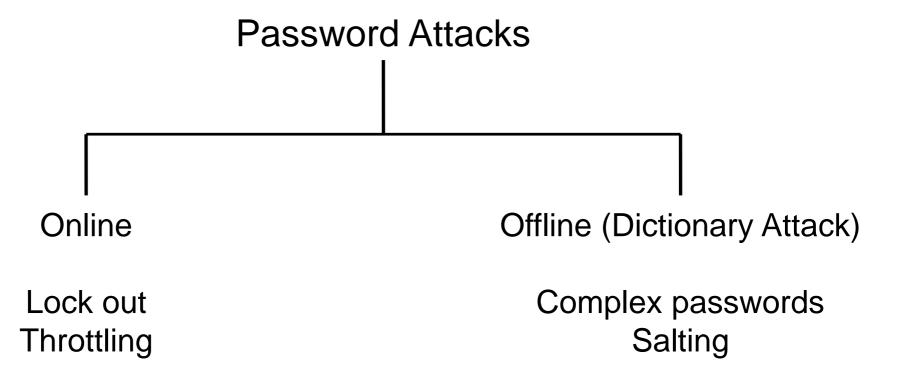


Personalized image passed through



Password Attacks

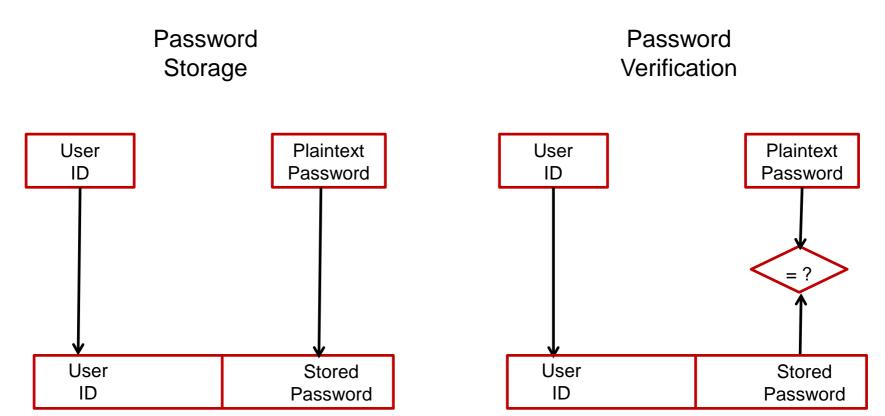






Password Storage and Verification



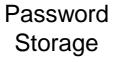


Loss of stored passwords = Catastrophic failure

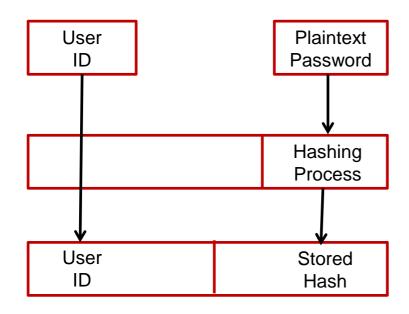


Password Storage and Verification

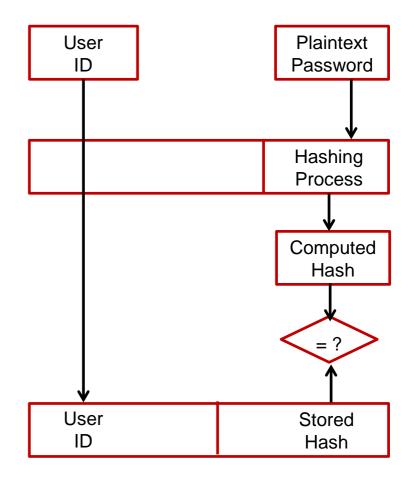




Password Verification



Loss of stored hashes = Attack by single dictionary



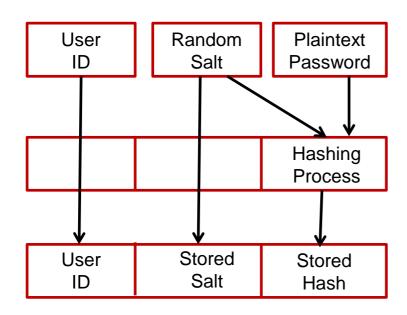


Password Storage and Verification



Password Storage

Password Verification



Loss of stored hashes =
Attack by different dictionary
for each salt value

