Authentication by Passwords

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 16

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

Authentication

Something you know
- password
- "secret" questions

Something you have
- smartphone
- registered device

Something you are
- fingerprint
- iris
- keyboard dynamics
- signature dynamics
Authentication Techniques

Authentication

Something you know
- password
- “secret” questions

Something you have
- smartphone
- registered device

Something you are
- fingerprint
- iris
- keyboard dynamics
- signature dynamics

single factor  multi factor
Phishing

Personalized image to authenticate webserver to user
Phishing Man in the Middle

Personalized image passed through
Password Attacks

Online
- Lock out
- Throttling

Offline (Dictionary Attack)
- Complex passwords
- Salting
Password Storage and Verification

Password Storage

User ID

Plaintext Password

Stored Password

Password Verification

User ID

Plaintext Password

User ID

Plaintext Password

= ?

Loss of stored passwords = Catastrophic failure
Password Storage and Verification

Password Storage

- User ID
- Plaintext Password
- Hashing Process
- Stored Hash

Loss of stored hashes = Attack by single dictionary

Password Verification

- User ID
- Plaintext Password
- Hashing Process
- Computed Hash
- Stored Hash

Computed Hash = ?
Password Storage and Verification

Password Storage

Password Verification

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