Authentication by Passwords: Introduction and Storage Techniques

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 12-1

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
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

User ID

Stored Password

Password Verification

User ID

Plaintext Password

User ID

Stored Password

= ?

Loss of stored passwords = Catastrophic failure
Password Storage and Verification

Password Storage

User ID

Plaintext Password

Hashing Process

User ID

Stored Hash

Password Verification

User ID

Plaintext Password

Hashing Process

User ID

Computed Hash

= ?

Loss of stored hashes = Attack by single dictionary
Password Storage and Verification

Password Storage

User ID
Plaintext Password
Hashing Process
User ID
Stored Hash

Password Verification

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

Loss of stored hashes = Attack by single dictionary
Password Storage and Verification

Password Storage

User ID  Random Salt  Plaintext Password

User ID  Stored Salt  Stored Hash

Hashing Process

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

Password Verification

User ID  Plaintext Password

Hashing Process

Computed Hash

User ID  Stored Salt  Stored Hash

=}?