A Graphical Password Authentication System

Ahmad Almulhem

KFUPM, SAUDI ARABIA

WorldCIS-2011 – London, UK
February 21-23, 2011

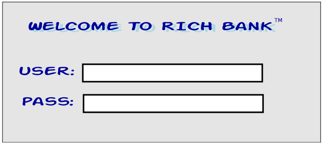
Outline

1. User Authentication
    - Overview
    - Alphanumerical Passwords
    - Graphical Passwords
2. Proposed System
    - Overview
    - Enrollment Step
    - Login Step
3. Conclusion

User Authentication

- **User Authentication** refers to the process of verifying an identity claimed by a system entity (user/process) (Stallings & Brown)
    - Two steps: (1) enrollment/registration, (2) login/authentication
- fundamental security building block and primary line of defense
- based one something an individual
    - knows - e.g. password, PIN, answer to secret question
    - has - e.g. smartcard, hotel keycards, (referred to as tokens)
    - is (static biometrics) - e.g. fingerprint, retina scan
    - does (dynamic biometrics) - e.g. voice, signature
    - any combination of the above (multi-factor)

User Authentication: Alphanumerical Passwords



WELCOME TO RICH BANK™

USER:

PASS:

- based on something an individual knows (remembers)
- by far most widely used authentication type
- easy to implement and use
- dilemma: password must be easily remembered by user; hard to guess by attacker
- studies show users tend to use short and easy to guess passwords
- enforcing a strong password policy; does it really work?

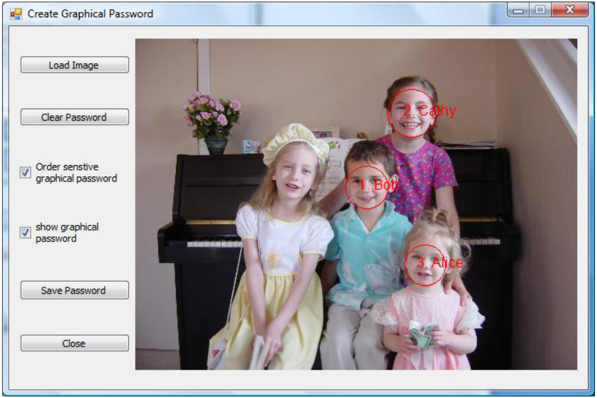
User Authentication: Graphical Passwords

- use graphics (images) instead of alphanumerical passwords
- why?
    - A picture is worth a thousand words
    - humans remember pictures better than words
    - more resistant to brute-force attacks; search space is practically infinite
- two main approaches
    - recognition-based (recognize something user picked at registration)
    - recall-based (re-produce something user created at registration)

Proposed System: Overview

- At the time of registration, a user creates a graphical password by first uploading a picture of her/his choice
- The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius)
- For every POI, the user types a word or phrase that would be associated with that POI
- If the user does not type any text after selecting a POI, then that POI is associated with an empty string
- The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant

Proposed System: Creating A Graphical Password

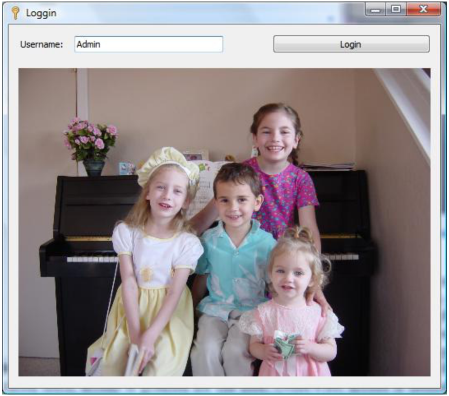


☑ Order senstive graphical password

☑ show graphical password

- Load a picture of your choice (e.g family picture)
- Click on POI (e.g. kids faces)
- Type some word (e.g. names/nicknames)
- Order may be enforced (stronger password)

Proposed System: Logging In



Username: Admin

Discussion and Conclusion

- Search space (system parameters):
  - picture
  - POIs (number and order)
  - words associated with POIs
- Together, the above parameters define a very large password space (infinite?)
- multi-factor authentication (graphical, text, POI-order, POI-number) in a friendly intuitive system

Questions?

Ahmad Almulhem

http://www.ccse.kfupm.edu.sa/~ahmadsm/