

## Assignment 1

# Authentication

Information and Communications  
Security (WS 2010/11)

Prof. Dr. Kai Rannenber  
Dr. Ioannis Krontiris

T-Mobile Chair for  
Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.  
[www.m-chair.net](http://www.m-chair.net)

The screenshot shows a dialog box titled "Authentication Mode" with a close button (X) in the top right corner. The dialog contains the following elements:

- Text: "Choose the authentication mode."
- Radio button: "Windows Authentication Mode" (unselected)
- Radio button: "Mixed Mode (Windows Authentication and SQL Server Authentication)" (selected)
- Text: "Add password for the sa login:"
- Text: "Enter password:" followed by a text input field.
- Text: "Confirm password:" followed by a text input field.
- Text: "Blank Password (not recommended)" with an unchecked checkbox.
- Buttons at the bottom: "Help", "< Back", "Next >", and "Cancel".

- Name one defence mechanism for password authentication systems that is enacted after the user chooses a password, and one mechanism that is enacted after each login. Describe advantages and potential problems of both methods.

- When choosing: Password policies
  - + Strengthen passwords, makes brute force attacks take longer due to greater strength of used passwords
  - May force user to choose new password
    - -> Users may forget hastily constructed passwords.
  - Inhomogeneous: different policies employed by different sites, confusing users

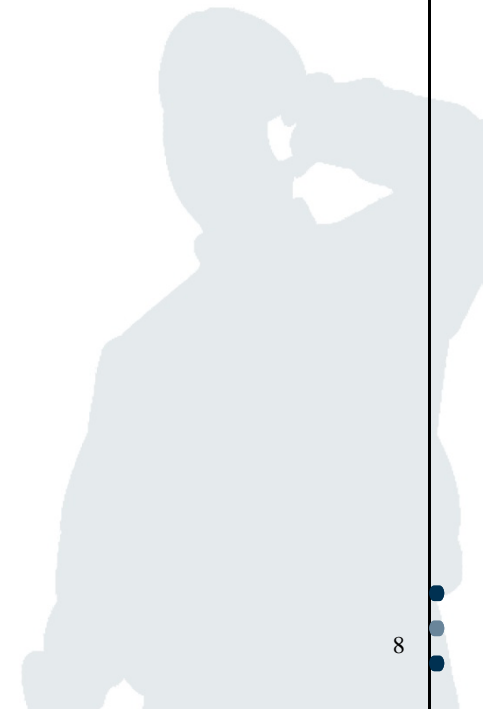
- At login: Limited login attempts
  - + Makes brute force attacks less risky as the number of trials is limited
  - May lock out users when password is forgotten/mistyped
    - ->False negatives.
  - No effect against attacks on software that attackers can always reinstall after they used up “their” limited number of trials

- Classify the following proposed passwords as good choices or poor choices, and justify your reasoning.
  - Bayern
    - Very bad, county, sports team, dictionary word
  - go2work
    - Better, but may still be obvious. Only 2 character types (lowercase & numbers).
  - cat&dog
    - Special character not really helpful compared to number, about as strong as “go2work”. Depends on how obvious it is (does user have a cat & dog?)
  - 3.1piNUMB
    - longest
    - Individual words harder to make out
    - All character classes (lower-, uppercase, numbers, special)
    - Probably harder to guess

- Phpbb website was hacked in 2009
- Hacker published 20,000 passwords
- Phpbb had no restrictions to passwords
- Most passwords were dictionary words. 65% match (for a simple English dictionary) and 94% (for "hacker" dictionaries)
- [http://www.darkreading.com/blog/archives/2009/02/phpbb\\_password.html](http://www.darkreading.com/blog/archives/2009/02/phpbb_password.html)

- 16% of passwords matched a person's first name
- 14% of passwords were patterns on the keyboard, like "1234," "qwerty," or "asdf", "159357".
- 4% are variations of the word "password," such as "passw0rd," "password1," or "passwd."
- 5% of passwords are pop-culture references from TV, movies, and music. "hannah," "pokemon," "tigger", "klinton," "starwars," "matrix," "legolas," "ironman"
- 4% of passwords appear to reference things nearby. "samsung", "dell," "packard," "apple," "pavilion," "presario," "compaq," and so on.
- 3% of passwords are "emo" words.
- 3% are "don't care" words: "abc123", "blahblah", "whatever," "whocares," or "nothing."

- How many different passwords are possible if a password is exactly  $n$  characters long (for  $n = 4, 6, 8$ ) and there is no distinction between upper case and lower case characters?
- $(26+10)^n = (36)^n$
- $(36)^4 = 1679616$
- $(36)^6 = 2176782336$
- $(36)^8 = 2821109907456$



- How many different passwords are possible if a password is exactly  $n$  characters long (for  $n = 4, 6, 8$ ) and there is a distinction between upper case and lower case characters?
- $(26*2+10)^n = (62)^n$
- $(62)^4 = 14776336$
- $(62)^6 = 56800235584$
- $(62)^8 = 218340105584896$

<http://howsecureismypassword.net/>

- There are several methods for authenticating users based on different classes of attributes they may supply to the service.
  - Name the different forms of authentication.
    - Something you know, you have, you are or someplace you are
- It is also possible to combine several authentication methods. Name an authentication method you would not use without combining it with other factors (Why?).
  - Tokens should be combined with other forms of authentication to ward off e.g. pickpockets. Also, biometrics are often combined with a simple surveillance, to make manipulations of the sensor harder for an attacker.



Hardware Token

- A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions.
- The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.
- The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends a “yes” or “no” to the system indicating whether or not the user has been authenticated.
- The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends the raw biometric data read to the system, which decides whether or not the user can be authenticated.

# mobile business





← {yes, no}



