

# Assignment 1: Authentication

Information and Communications  
Security (SS 2008)

Prof. Dr. Kai Rannenber

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

Authentication Mode

Choose the authentication mode.

Windows Authentication Mode

Mixed Mode (Windows Authentication and SQL Server Authentication)

Add password for the sa login:

Enter password:

Confirm password:

Blank Password (not recommended)

Help < Back Next > Cancel

- Name one defense 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.
  - -: inhomogenous: different policies employed by different sites, confusing users

- At login: Limited login attempts
  - +: Strengthen passwords, makes brute force attacks take longer due to greater strength of used passwords
  - -: May lock user out when password is forgotten/mistyped
    - ->False negatives.
  - -: no effect against offline attacks

- 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

- 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?
- $(26 \cdot 2 + 10)^n = (62)^n$
- $(62)^4 = 14776336$
- $(62)^6 = 56800235584$
- $(62)^8 = 218340105584896$

- 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 to 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.

- 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.





{yes, no}



