Tutorial 4

Aims

To illustrate the limitations of identification methods

To demonstrate the applicability of authentication methods in various cases

Questions

1. Identification
   (a) Explain how a human would establish the identity of
   - someone sitting in front of the local computer
   - someone who connects to the local computer via remote access
   - a remote computer connecting to the local computer

   (b) How could a computer establish the above three identities?

2. Assume that you are only allowed to use the 26 letters of the alphabet to construct passwords of length *n*. In one system passwords are case-sensitive, in another system they are not.
   (i) In the worst-case scenario, how many attempts are needed for a successful brute-force attack in each system?
   (ii) How long will take that attack if each password can be checked in
   (a) one-tenth of a second (100 milliseconds) and
   (b) if it takes 10^{-6} second(1 microsecond)?
   Calculate the values for n=5 and 10.

3. Authentication tries to determine the eligibility of using a particular computer or service. Different authentication factors represent different ways of establishing eligibility.
   (a) Do all authentication factors offer the same level of security? Discuss.
   (b) Will the use of more than one authentication method necessarily improve reliability? Can you find examples when it does and when it doesn’t?
   (c) Passwords have been used for authentication since the early days of computing. What are the main problems with password authentication?

4. Give some examples of certificates in real life. Explain where they are used and how their reliability is ensured. Compare their use to electronic certificates.