Tutorial 4

Aims

To illustrate the limitations of identification methods

To demonstrate the applicability of authentication methods in various cases

Questions

1. Identification
   - Explain how a human would establish the identity of
     - someone sitting in front of the local computer

       Check his photo ID;
     - someone who connects to the local computer via remote access

       Make a phone call to the number where the user is supposed to be.
     - a remote computer connecting to the local computer

       Check any certificate the remote computer may have, make a phone call to the number where the computer is supposed to be?
   - How could a computer establish the above three identities?
     - Via face recognition or other biometric method
     - Using a biometric device at the remote end
     - Checking its electronic (e.g. X.509) certificate

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.

(i)	(ii)	(a)	(b)
26^n	26^5	$1.188*10^6$ sec ~ 13.75 days	11.88 sec
	26^{10}	$1.411*10^{13}$ sec ~ $4*10^5$ years	$1.411*10^8$ sec ~ 4 years
52^n	52^5	$3.8*10^7$ sec ~ 12 years	3800 sec ~ 1.05 hour
	52^{10}	$1.45*10^{16}$ sec ~ $4.58*10^8$ years	$1.45*10^{11}$ sec ~ $4.58*10^3$ years

3. Authentication tries to determine the eligibility of using a particular computer or service. Different authentication factors represent different ways of establishing eligibility.
    - Do all authentication factors offer the same level of security? Discuss.

Factor	Advantages	Weaknesses	Example
Proof by knowledge	• Easy to implement • Portable	• Cannot detect sniffing attacks • Passwords are easy to guess or hard to remember	Password, PIN
Proof by possession	• Hardest to abuse	• Device can be expensive • Can be lost or stolen • Risk of hardware failure	Smart card, bank card, USB key, token device
Proof by property	• Easy to authenticate with • Portable	• Expensive • Privacy risks • Characteristics cannot be changed • Works for human users only	Fingerprint, iris, palm, hand geometry, hand vein pattern

    - Will the use of more than one authentication method necessarily improve reliability? Can you find examples when it does and when it doesn't?

    In general it will, as an impostor needs more information and more work for an attack, e.g. withdrawing money from an ATM.
    However, in case of a remote session, a replay attack can spoof several factors' information.

    - Passwords have been used for authentication since the early days of computing. What are the main problems with password authentication?

    Passwords are forgotten, written down, shared between different systems, vulnerability to re-play attacks

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.

    Certificates in real life:

    University degree, certificate for a specific training/test/certification course (CompTIA Security+, MCSE--Microsoft Certified Systems Engineer, CCNA…), certificate of a product (stating the authenticity, e.g.: genuine official World Cup 2010 jersey)

    Electronic certificates: PKI (X.509)

    Where they are used:

    Job application, an application for admission to school, scholarship application, included with unit (certificate of product)

    How their reliability is ensured:

    Detailed information about the subject is presented, certificate can be verified via the issuing authority — e.g. record number or database reference number, bar code or the subject's personal information

    Issued by a Certificate authority (CA) in both cases

Usage

- Purpose (of electronic and hard copy certificates) is the same
- Form is totally different: electronic ones can be copied, hard copy ones are more difficult to copy and still maintain veracity
- Binding to the subject uses different methods. Hard copy uses biometric or similar information (e.g. photo). Electronic ones use proof by knowledge (private encryption key)
- Verification:
    - Hard copy: performed mostly by humans
    - Electronic: performed by computers, certificate chains are common