PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 6, for key exchange

1. In order to increase confidentiality of data sent via email, some people put sensitive data into a file, encrypt it (symmetrically), and attach the ciphertext instead of sensitive data in plaintext. The question is which key to use? The key should be shared by the sender and the receiver.

   One of the solutions (unfortunately) used is to take PESEL number of the recipient as the encryption key. Why this is a particularly bad choice?

2. Frequently, key exchange comes together with password authentication (so called Password Authenticated Key Exchange - PAKE): the session key is established iff both partners use the same password. The password should be memorable (so not a 80-character random string!).

   Below there is a description of a quite stupid PAKE protocol. Find out why it is stupid.

   Alice and Bob share a password π.

   (a) Alice chooses s at random and calculates $c := \mathrm{Enc}_\pi(s)$,

   (b) Alice sends c to Bob,

   (c) Bob sets $s := \mathrm{Dec}_\pi(c)$,

   (d) Alice and Bob use s as a session key.

3. Personal ID cards (PIC) issued in the EU must implement PAKE (the password is the so called CAN number – find it on your *dowod osobisty*, if it comes with a chip). The protocol, called PACE, is executed by a PIC and a reader device:

   (a) password π is entered to the reader by the holder of a PIC,

   (b) PIC chooses an s at random and sends $\mathrm{Enc}_{\mathrm{Hash}(\pi)}(s)$ to the reader,

   (c) PIC and the reader execute Diffie-Hellman key exchange, the result is h,

   (d) both PIC and the reader calculate $\hat{g} = h \cdot g^s$,

   (e) PIC and the reader run Diffie-Hellman key exchange, but this time for the generator $\hat{g}$,

   (f) the resulting key K is used for deriving the session keys,

   (g) some tags are exchanged to prove that both sides hold the same keys,

   (h) data exchange starts, it is secured with session keys.

   Check, whether an adversary monitoring the communication between a PIC and a reader can check afterwards which password has been used (offline attack).

4. Browse Internet to check what is the mechanism for establishing a session key during execution of the TLS protocol. be aware that there are version of this standard and that they may differ significantly!

/-/ Mirosław Kutyłowski