Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

10. Exercise sheet
Hand in solutions until Monday, 06 July 2009.

Any claim needs a proof or argument. Answer in complete sentences and your own words. A verbatim quote is never a complete answer.

Exercise 10.1 (Advanced Security Mechanisms). (12 points)

Read the BSI Technical Guideline TR-03110 "Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.01" (You may skip the appendices). A link is available on the course's website.

(i) What is the purpose of the Chip Authentication Protocol? Under which assumptions can Version 1 be considered secure? Describe the security model and explain how an attacker with the power to compute discrete logarithms can break the scheme. $\boxed{4}$

(ii) What is the purpose of the Terminal Authentication Protocol? Under which assumptions can Version 1 be considered secure? Describe the security model. Can an attacker with the power to factor quickly break the scheme. $\boxed{4}$

(iii) What is the purpose of the Restricted Identification Protocol? Describe the process to revoke an MRTD chip. $\boxed{2}$

(iv) What is the purpose of the PACE Protocol? The Security Discussion explicitly forbids "more than one execution of PACE within the same session". Why? $\boxed{2}$

Exercise 10.2 (AtE and died: confidentially poisoned). (10+2 points)

Horton's principle says that one should always prove the integrity of the *plain text*. One solution to ensure the integrity is to first authenticate and then encrypt (AtE). Though this paradigm is clearly correct and the conclusion grants integrity as desired, we overlooked a different issue here. This exercise shall prove it.

Suppose we use some encryption function ENC_{K_e} and any message authentication function MAC_{K_a}. For a message m we compute $a := \mathrm{MAC}_{K_a}(m)$ and send $c := \mathrm{ENC}_{K_e}(m|a)$. (Here, the vertical line '|' denotes concatenation.)

Assume both are as secure as you like. In particular, the encryption function shall guarantee that even to a *c*hosen *p*laintext *a*ttacker the encryptions of two known plain texts are *ind*istinguishable. In other words, there is no (ie. no probabilistic polynomial time) so-called IND-CPA attacker: the attacker may ask for encryptions of chosen plain texts and he fixes two further plain texts m_0, m_1 for which he never inquired the encryption. Finally, the attacker is given the encryption of m_0 or of m_1 and shall tell which of the two plain texts was used. One possible encryption function under these constraints is the one-time pad (assuming that the encryption procedure keeps track of the already used parts of the key).

Now, suppose additionally that the encryption XORs something on the cipher text (like a one-time-pad), and define a variant $\mathrm{ENC}^*_{K_e}$ of this encryption function as follows: first replace every 0-bit by two bits 00 and every 1-bit by two bits 01 or 10, choose randomly each time, next encrypt with ENC_{K_e}. For the decryption we translate 00 back to 0, 01 and 10 to 1, and 11 is considered as a transmission error. So we send $\mathrm{ENC}^*_{K_e}(m|\,\mathrm{MAC}_{K_a}(m))$.

2+2 (i) Prove (at least, argue) that $\mathrm{ENC}^*_{K_e}$ is still secure in the previous sense.

4 (ii) Suppose that a ruthless person, called Raul, has overheard the messages of your login to some server which was done by sending the password. Of course, your password was authenticated and encrypted, as all messages. Now, Raul takes the transmission of your password and resends it with a bit pair in the cipher text inverted.

(a) How does the recipient react if the original bit was 0?

(b) How does the recipient react if the original bit was 1?

Conclude that Raul learns the bit from the reaction of the server (and thus your passwords after enough trials).

2 (iii) Estimate the effect of this observation.

2 (iv) In SSH we transmit $\mathrm{ENC}_{K_e}(m)|\,\mathrm{MAC}_{K_a}(m)$, so we authenticate and encrypt (rather than first authenticating and second encrypting). Is that better? [Try to use $\mathrm{ENC}^*_{K_e}$ here.]

Exercise 10.3 (Final discussion of MRTD security features). (12+10 points)

2 (i) What prevents chip cloning?

2 (ii) Why is step 2 before step 3 in the Advanced Inspection Procedure?

2 (iii) The BSI suggests to combine Chip Authentification and Passive Authentication. Consider a man-in-the-middle attack on this combination.

2 (iv) What grants confidentiality of the conversation between chip and reader?

4 (v) Can an attacker – with or without knowledge of the MRZ – identify a certain passport, say to trigger a bomb?

(vi) Formulate and discuss further questions. +10