Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

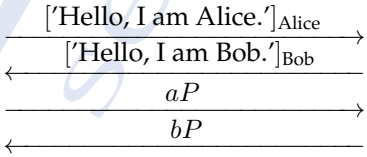
8. Exercise sheet
Hand in solutions until Wednesday, 15 January 2014, 23:59

Exercise 8.1 (Signed key exchange). (6 points)

We have considered the Diffie-Hellman key exchange: Given a group G (additively written) generated by P of order d such that the discrete log problem is difficult. To fix a shared secret key, Alice sends aP and Bob sends bP. Then both can compute the shared key abP. This procedure is vulnerable to man-in-the-middle attacks. So we modify the Diffie-Hellman key exchange and assume that there is an infrastructure such that Alice and Bob can sign their messages in a secure way. Thereby $[m]_{\text{Alice}}$ should denote the pair consisting of the message m and a valid signature of m produced by Alice. To be polite we should start with a "Hello".

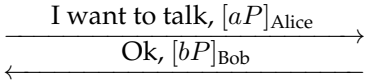
Protocol 1. Signed and polite Diffie-Hellman key exchange.

1. Alice wants to talk.
2. Bob agrees.
3. Alice chooses $a \in \mathbb{N}_{<d}$, computes aP.
4. Bob chooses $b \in \mathbb{N}_{<d}$, computes bP.
5. Alice computes $a(bP) = abP$.
6. Bob computes $b(aP) = abP$.



Protocol 2. Signed Diffie-Hellman key exchange.

1. Alice chooses $a \in \mathbb{N}_{<d}$, computes aP.
2. Bob chooses $b \in \mathbb{N}_{<d}$, computes bP.
3. Alice computes $a(bP) = abP$.
4. Bob computes $b(aP) = abP$.



Answer the following questions and prove your claims.

(i) Which of the two protocols are vulnerable against man-in-the-middle attacks, and which are not? 4

(ii) How could the vulnerable protocol(s) be modified by adding further communication (not changing the present steps) to prevent man-in-the-middle attacks? 2

Exercise 8.2 (Vulnerability of TLS). (13+5 points)

(i) Read `http://www.isg.rhul.ac.uk/tls/TLStiming.pdf`.

2 (ii) Give a short overview of the described attack.

3 (iii) Which powers/sources does an attacker need?

4 (iv) Describe each step of the attack along with a judgment of feasibility.

1+3 (v) Why is the attack called Lucky Thirteen?

3 (vi) Quickly describe the idea behind the suggested countermeasures. Is the attack still feasible in the latest version of TLS?

+2 (vii) Read up on the so called "BEAST" attack and summarize (see for instance `https://bugzilla.mozilla.org/show_bug.cgi?id=665814`).

Exercise 8.3 (IPsec and IKEv1 criticism). (8 points)

4 (i) At `http://www.schneier.com/paper-ipsec.html` you find the IPsec and IKEv1 criticism of Niels Ferguson and Bruce Schneier. Read and summarize it. (What are their recommendations? What are their major reasons? Do they say whether IPsec/IKE is secure or how to make it secure?)

4 (ii) Reconsider their arguments in the presence of IKE version 2 (that we discussed in the course).