Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Monday, 27 May 2013, 08:00

Exercise 6.1 (IKEv2 parameter). (10 points)

(i) Read RFC 5996.

(ii) If a Security Association (SA) expires, how can a new (valid) SA be negotiated? [2]

(iii) After rekeying, may the new SA have cryptographic schemes being different from the old one? [1]

(iv) What is a "Nonce"? How is it used in IKEv2? How long must a nonce be? May it be chosen deterministically? [3]

(v) Which block cipher algorithms can be used in IPsec/IKEv2? Give an up to date list. [1]

(vi) Describe the groups for the Diffie-Hellman key exchange that can be used in IKEv2. In particular, are elliptic curves among them? [3]

Exercise 6.2 (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.

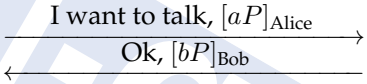
$$\xrightarrow{['\text{Hello, I am Alice.}']_{\text{Alice}}}$$
$$\xleftarrow{['\text{Hello, I am Bob.}']_{\text{Bob}}}$$
$$\xrightarrow{aP}$$
$$\xleftarrow{bP}$$

5. Alice computes $(a(bP) = abP$.
6. Bob computes $(b(aP) = abP$.

Here is a further variant.

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.

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

2 (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?

Exercise 6.3 (Project, part 1). (8+12 points)

Choose either TLS/SSL or SSH for this exercise. Make your choice public via `http://doodle.com/ye22etgxbrxxpueg`. Restriction: the number of persons choosing TLS and the number of persons choosing SSH may differ by at most two after your choice.

Find sources that describe the chosen protocol and study them. These sources should include the relevant up-to-date RFCs. Supply a list of all used sources! Give a short description of the protocol (in your own words!), enough to answer the following questions.

2 (i) Summarize the protocol briefly.

2 (ii) Where is the chosen protocol located in the OSI-model? What are pros and cons of this placement?

4 (iii) How is the start of a communication specified and how is the key exchange done in the chosen protocol? Is a man-in-the-middle attack possible?

+12 (iv) Discuss!