Esecurity: secure internet & evoting, summer 2010

Michael Nüsken, Konstantin Ziegler

5. Exercise sheet
Hand in solutions until Sunday, 30 May 2010, 23.59 h

Exercise 5.1 (Key exchange threats). (15 points)

We have considered the Diffie-Hellman key exchange: Given a group G (additively written) consisting of multiples of a generator P of order ℓ, so $G = \{0, P, 2P, \dots, (\ell - 1)P\}$ such that the discrete log problem is difficult, ie. given $Q \in G$ there is no efficient (ie. randomized polynomial time) algorithm to determine η with $Q = \eta P$. To fix a shared secret key, Alice sends αP and Bob sends βP. Then both can compute the shared key $\alpha\beta P$.

Protocol DH. Diffie-Hellman key exchange.

1. Alice chooses $\alpha \in \mathbb{N}_{<\ell}$ and computes αP.
2. Bob chooses $\beta \in \mathbb{N}_{<\ell}$ and computes βP.
3. Alice computes $\alpha(\beta P) = \alpha\beta P$.
4. Bob computes $\beta(\alpha P) = \alpha\beta P$.

$$\xrightarrow{\qquad\qquad \alpha P \qquad\qquad}$$
$$\xleftarrow{\qquad\qquad \beta P \qquad\qquad}$$

Now both can use $\alpha\beta P$ to derive common secrets for the subsequent message exchanges. What if Wilma puts herself in the middle? She will have a common secret $\alpha\omega P$ with Alice and a common secret $\omega'\beta P$ with Bob, and as long as she continues to pass all messages on, neither Bob nor Alice will notice anyhting apart possibly from a slighlty slower connection. So we modify this.

Protocol DH+sign+ack. Signed and acknowledged Diffie-Hellman key exchange.

1. Alice chooses $\alpha \in \mathbb{N}_{<\ell}$, computes αP and signs $[\text{'Alice'}, \alpha P]$.
2. Bob chooses $\beta \in \mathbb{N}_{<\ell}$, computes βP and signs $[\text{'Bob'}, \beta P]$.
3. Alice computes $\alpha(\beta P) = \alpha\beta P$ and a hash.
4. Bob computes $\beta(\alpha P) = \alpha\beta P$ and a hash.

$$\xrightarrow{\qquad [\text{'Alice'}, \alpha P]_{\text{Alice}} \qquad}$$
$$\xleftarrow{\qquad [\text{'Bob'}, \beta P]_{\text{Bob}} \qquad}$$
$$\xrightarrow{\qquad \text{hash}(0, \alpha\beta P) \qquad}$$
$$\xleftarrow{\qquad \text{hash}(1, \alpha\beta P) \qquad}$$

Consider the above protocols in the following questions. (Be brief, but don't forget the essential arguments.)

(i) *Woman in the middle*: Try to put Wilma in the middle. What happens? $\boxed{2}$

(ii) *Mutual authentication*: Examine which of the given protocols ensure that Alice' partner is Bob. $\boxed{2}$

$\boxed{2}$ (iii) *Perfect Forward Security*: Next, suppose that the Beagle Boys intercepted the conversation between Alice and Bob. Then after the conversation is terminated the Beagle Boys take over Alice' and Bob's entire equipment including their secret keys. Will they be able to read what Alice and Bob told each other?

$\boxed{2}$ (iv) *Denial of Service*: Daniel is a weird person that only wants to prevent say Bobs' computer to do good work. So he floods Bob with tons of requests. For each of these requests Bob's computer is forced to compute and send an answer. Consider vaguely the effort which Daniel and Bob have to spend for their first messages and vote for the 'best' protocol.

$\boxed{2}$ (v) *Endpoint Identifier Hiding*: Eve does not want to be spotted, so she only listens on the conversation. If she can detect who the partners are, this is already valuable information for her. Which protocols hide the identity of Alice and/or Bob?

$\boxed{2}$ (vi) *Live Partner Reassurance*: Romeo likes repetions and so after listening to a conversation, he calls Bob with replayed messages from the overheared talk making him think he is Alice. (Imagine this could be successfully done when you log in to your home banking account!) Examine the given protocols under this attack.

$\boxed{3}$ (vii) Devise a protocol that Romeo cannot trick. (Do not forget to argue!)

$\boxed{+0}$ (viii*) Devise a protocol that is not vulnerable to any of these attacks.

Exercise 5.2 (Project). (12+12 points)

$\boxed{12+12}$

Choose whether you consider SSL or SSH for this exercise.

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 security questions.

Discuss the security of the chosen protocol under the same security aspects as we did for IPsec:

(i) Session key agreement.

(ii) Perfect forward security.

(iii) Denial of Service.

(iv) Endpoint identifier hiding.

(v) Live partner reassurance.

(vi) Plausible deniability.

(vii) Stream Protection.

(viii) Negotiating parameters.

We will summarize your results in the course and tutorial on 1 June.