Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

10. Exercise sheet
Hand in solutions until Sunday, 19 June 2011, 23:59

Exercise 10.1 (Needham-Schroeder protocol). (8+4 points)

(i) Read DOROTHY E. DENNING & GIOVANNI MARIA SACCO (1981). Timestamps in key distribution protocols. *Commun. ACM* **24**, 533–536. ISSN 0001-0782. URL `http://doi.acm.org/10.1145/358722.358740`.

(ii) Describe the Needham-Schroeder symmetric key protocol ("Distribution of Communication Keys"). [3]

(iii) Under which circumstances is a replay attack possible if no timestamps are included? [2]

(iv) How do timestamps prevent this attack? [2]

(v) Kerberos is based on the Needham-Schroeder protocol. Are timestamps included in the up to date version of Kerberos (RFC4120)? [1]

(vi) Can one prevent this kind of replay attack without timestamps, eg. if there is no clock available? [+4]

Exercise 10.2 (IPsec/IKE repetition). (9 points)

In any of your answers to this exercise you may restrict to IPsec with ESP in tunnel mode with authentication and optional encryption.

(i) How does IPsec provide authenticity of messages? [2]

(ii) How does IPsec prevent replay attacks? [1]

(iii) Which keys uses IPsec and how are they agreed upon? (In other words: which is the underlying protocol?) [1]

(iv) The Diffie Hellman key exchange allows to agree on a key that an eavesdropper cannot derive from the conversation. But it can be broken by a woman in the middle attack. Explain how. 3

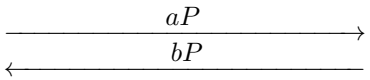
(v) Explain how a woman in the middle attack can be prevented. 2

Exercise 10.3 (Key exchange threats). (12+4 points)

We have considered the Diffie-Hellman key exchange: Given a group G generated by P of order d such that the discrete log problem is difficult, ie. given $A \in G$ there is no efficient (ie. randomized polynomial time) algorithm to determine a with $A = aP$. To fix a shared secret key, Alice sends aP and Bob sends bP. Then both can compute the shared key abP.

Protocol DH. Diffie-Hellman key exchange.

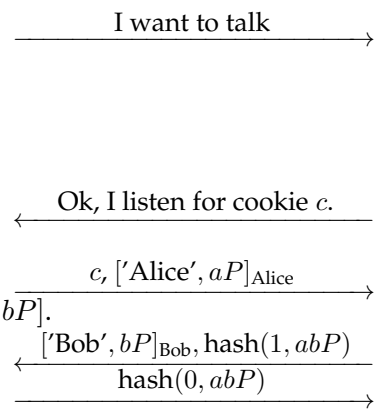
1. Alice chooses $a \in \mathbb{N}_{<d}$ and computes aP.
2. Bob chooses $b \in \mathbb{N}_{<d}$ and computes bP.
3. Alice computes $(a(bP) = abP$.
4. Bob computes $(b(aP) = abP$.



Now both can use abP to derive common secrets for the subsequent message exchanges. What if Wilma puts herself in the middle? Neither Bob nor Alice will notice anything apart possibly from a slightly slower connection. 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. To be polite we should start with a "Hello".

Protocol DH+cookie+ack. Polite Diffie-Hellman key exchange with a cookie and acknowledgement.

1. Alice wants to talk.
2. Bob agrees and chooses a cookie c, which is a suitably random number, for example, the hash value of Alice's IP address and some fixed secret of Bob. (It's nice if the number is deterministically determined!)
3. Alice chooses $a \in \mathbb{N}_{<d}$, computes aP and signs $['\text{Alice}', aP]$.
4. Bob chooses $b \in \mathbb{N}_{<d}$, computes bP and signs $['\text{Bob}', bP]$.
5. Bob computes $b(aP) = abP$ and a hash.
6. Alice computes $a(bP) = abP$ and a hash.



Here is a further variant.

Protocol DH+enc-ack. Polite Diffie-Hellman key exchange with encrypted acknowledgement.

1. Alice chooses $a \in \mathbb{N}_{<d}$, computes aP.
2. Bob chooses $b \in \mathbb{N}_{<d}$, computes bP.
3. Alice computes $a(bP) = abP$ and uses it to encrypt her name and a signature to her share aP.
4. Bob computes $b(aP) = abP$ and uses it to encrypt his name and a signature to his share bP.

$$\xrightarrow{\text{I want to talk, } aP.}$$
$$\xleftarrow{\text{Ok, } bP.}$$
$$\xrightarrow{E_{abP}(\text{'Alice'}, [aP]_{\text{Alice}})}$$
$$\xleftarrow{E_{abP}(\text{'Bob'}, [bP]_{\text{Bob}})}$$

Consider each of the two modified DH 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? [2]

(ii) *Mutual authentication*: Examine which of the given protocols ensure that Alice' partner is Bob. [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? [2]

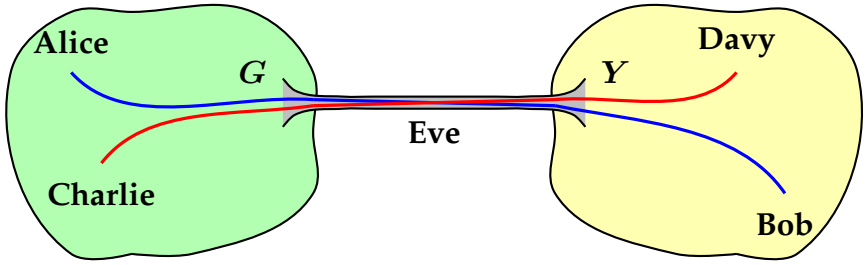
(iv) *Denial of Service*: Daniel is a weird person that only wants to prevent say Bobs' computer to do good work. So he floods Bob with tons of requests. For each of these requests Bob's computer is forced to compute and send an answer. Consider vaguely the effort which Daniel and Bob have to spend for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

(vi) *Live Partner Reassurance*: Romeo likes repetitions 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. [2]

(vii) Devise a protocol that Romeo cannot trick. (Do not forget to argue!) [+4]

Exercise 10.4 (Splicing Attack). (6+2 points)



Suppose that the gateways G and Y link the green and the yellow LAN by an encrypted but not authenticated IPsec tunnel using a fixed SA. Assume that the encryption is done by some symmetric cipher in CBC mode. We want to show that Eve and her boss Davy can read all the traffic between Alice and Bob.

2 (i) How does the beginning of a packet from Charlie to Davy look like?

2 (ii) Replace the beginning of a packet from Alice to Bob or from Bob to Alice with the start of an eavesdropped packet from Charlie to Davy. What happens?

+2 (iii) How can Davy find out the part just after the replaced beginning? [Consider retransmitting…]

2 (iv) Draw conclusions. [Formulate a proposal, explain, argue.]

(v) Go beyond.