Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

8. Exercise sheet
Hand in solutions until Monday, 33 May 2014, 13:00

Exercise 8.1 (Key exchange threats). (12 points)

Consider the following protocols for establishing shared keys. Assume 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.

Protocol 3.

1. Alice wants to talk.	$\xrightarrow{\text{I want to talk}}$
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!)	$\xleftarrow{\text{Ok, I listen for cookie } c\text{.}}$
3. Alice computes RSA keys (e, N) and (d, N).	$\xrightarrow{c,\ (e, N)}$
4. Bob chooses a 128-bit number K, encrypts K with Alice's RSA key (e, N) with a secure padding scheme.	$\xleftarrow{\text{enc}_{(e,N)}(\text{pad}(K))}$

Let h be a collision resistant hash function and $G = \langle P \rangle$ be a cyclic group of order d such that the discrete log problem is difficult. Assume Alice has a secret passphrase a. She computes $A = h(a|s)P$, where s is a random number (the "salt"), and lets Bob know A in a secure way. In the following $\{m\}_K$ means the message m is send authenticated and encrypted by K.

Protocol 4.

1. Alice wants to talk.	$\xrightarrow{\text{Hello, I am Alice.}}$
2. Bob chooses $b \in \mathbb{N}_{<d}$ and computes $B = bP$, $K = bA$, and $h(K)$.	$\xleftarrow{\text{Ok, } B,\ \{h(0\|K)\}_K}$
3. Alice computes $K = h(a\|s)B$, decrypts the last message and checks wether she computes the same values $h(0\|K)$.	$\xrightarrow{\{h(1\|K)\}_K}$
4. Bob checks wether he computes the same value $h(1\|K)$.	

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

2 (i) *Man in the middle*: Michael puts himself in the middle. What happens?

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

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*: Raoul likes repetitions and so after listening to a conversation, he calls Bob (or is called by Alice) with replayed messages from the overheard talk making him (her) think he (she) is Alice (Bob). Examine the given protocols under this attack.

Exercise 8.2 (Authenticated encryption). (9 points)

(i) Read Rogaway & Wagner (2003).

1 (ii) What is authenticated encryption?

3 (iii) Briefly describe the CCM mode.

4 (iv) Summarize the criticism made in the paper.

References

P. ROGAWAY & D. WAGNER (2003). A Critique of CCM. Technical Report 070. URL `http://eprint.iacr.org/2003/070`.