Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Heiko Niedermayer
Dipl.-Inf. Ali Fessi

Exercises for lecture „Netzsicherheit“
Assignment 3, WS09/10

Hand-out:	Thursday November 26th 2009
Deadline:	Thursday December 10th 2009
Exercise course:	Thursday December 17th 2009

Task 1: Cryptographic Hash Functions - Basics

a) How many bits does an ideal hash function need for as output, so that the effort to find a collision is comparable to breaking a symmetric block cipher with a vrute force attack? The bitlength of the symmetric cipher is 100 bits.
b) What is the danger when one uses SHA-1 for digital signitures?
c) The computation of a SHA-1 hash value with 512 bits needs 80 steps (rounds). How many steps are necessary, so that every bit of the input was used?
d) In SHA-1, what is the value W_{19} and how is it computed?

Task 2: Authentication Protocols; the Needham-Schroeder Protocol

a) In the lecture we introduced a replay attack on the Needham-Schroeder Protocol (symmetric variant). What are the prerequesits that allow this attack, in particular with respect to the session key $K_{A,B}$?
b) The Kerberos protocol prevents this attack. Extend the Needham-Schroeder Protocol, so that this replay attack is not possible.

Task 3: Authentication Protocols; Kerberos

a) Change the Kerberos Protocol so that it does not need timestamps and therefore also no synchronized clocks.
b) Argue why the Kerberos Protocol does not achieve the property of „Forward Secrecy“.
c) Extend the Kerberos Protocols so that the communication between Alice and the service S1 is „forward secure“(property Forward Secrecy for Alice and S1).
d) What did Kerberos V5 do to reduce the impact of dictionary attacks in comparison to Kerberos V4? How much does this reduce the threat?

Task 4: Attacks on (in)secure Channels

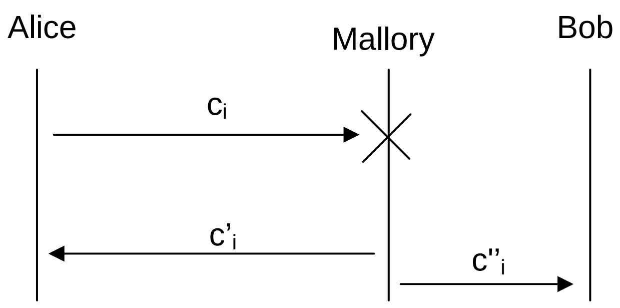
A protocol to secure the communication between 2 communication partners is to be developped. Let us assume that the following design decisions were taken:

- A cryptographic hash function is used for data integrity. The designers selected SHA-1 and the output of the hash function is reduced to its first 96 bits. Each message then consists of the message and these first 96 bits from the hash function:

  (m , first-96-bits(H(m)))
- This combination of message and hash value is then encrypted with a shared predefined key *K* of 256 bits of length..
- For the encryption AES in CTR mode is used, primarily to benefit from the performance advantages of CTR mode. The key *K* is used to compute the necessary key streams. To avoid the complexity and overhead of key management, the same key *K* is used in both directions of the communication channel.
- For a message with sequence number *i* the principal generate the corresponding key streams k_i.. The key stream is generated from the sequence number *i* and the counter for the blocks of the message *j*. To be more precise the concatenation of ($i \| j$) is encrypted with key *K* using the 256 bit AES block cipher. The sequence number *i* is initialized with 0 and each sender increases the count by 1 for each message it sends. *j* is initialized with 0 in each message and increased by 1 for each block.

  k_i = E(i||0, K) || E(i||1, K) || E(i||2, K) || ….

a) Let us now assume that „Alice“ and „Bob“ use the protocol as described above for their communication. An attacker called „Mallory“ intercepts the encrypted messages c_i from Alice and ensures that they do not reach Bob. Let us further assume that Mallory can guess the plaintext m_i for some messages. Argue why then the following is the case:
   - Mallory can send her own messages c'_i to Alice so that Alice is not able to detect that the message that is decrypted to *m'* is not from Bob.
   - Mallory can even send her own messages c''_i to Bob, so that Bob cannot decide whether the messages are from Alice or Mallory..



b) Argue why this protocol design has some flaws and propose improvments to make the protocol more secure.