Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti
Cybersecurity

Remote exam *of 13rd January 2022, a.y. 2021-22. Time: 2 hours*

Q1: **Before you start**

Please insert starting from top line:

A. position (regular, not Infostud registered, Infostud registered but blocked, etc.)
B. degree course (master in something, or other)
C. number of homeworks (≥ 0) validly (within the proper deadline, or, if on late, explicitly authorized by the prof.) delivered
D. comment (whatever you want to say to prof.)

best wishes now…

Q2: **Data integrity**

Q2.1 [3/30] Describe what we mean by data integrity and discuss the use of keyed HMACs for guaranteeing the integrity of a file being transmitted over the network (no other guarantees requested).

Q2.2 [3/30] Suppose you are requested to ensure the integrity of a file but you are only allowed to use AES (and a symmetric key): what can it be done?

Q3: **Diffie-Hellman**

Q3.1 [3/30] Describe in detail how two parties can establish a secret key by using the Diffie-Hellman scheme and discuss the vulnerability of the approach.

Q3.2 [3/30] Generalize Diffie-Hellman so that three parties can establish a shared secret key.

Q3.3 [3/30] Describe a scheme for mutual authentication that is strong with respect to dictionary attack and that uses Diffie-Hellman for defining a session key. Do vulnerabilities discussed in Q3.1 still hold?

Q4: **Leader selection**

A leader should be selected by randomly choosing one of three parties *A*, *B* and *C*. The parties use the following protocol

$A \rightarrow B$: N_A	{ *A* chooses nonce N_A }
$B \rightarrow C$: ($N_{AB} = N_A \text{ ^ } N_B$)	{ B chooses nonce N_B and sends $N_{AB} = N_A \text{ ^ } N_B$, where ^ is the ex-or operation}
$C \rightarrow A$: ($N_{ABC} = N_{AB} \text{ ^ } N_C$)	{ C chooses nonce N_C and sends $N_{ABC} = N_{AB} \text{ ^ } N_C$ }
{ Now both *A* and *C* know N_{ABC} }	
$A \rightarrow B$: N_{ABC}	{ Now *B* knows N_{ABC}, too }
{ Each of the three parties can now compute $p = N_{ABC} \bmod 3$, where p = 0 denotes *A*, p = 1 denotes *B*, and p = 2 denotes *C* }	

Q4.1 [1/30] Discuss the security of the protocol with respect to possible fraudulent behaviors of *A*, *B* and/or *C*. In particular, is it possible for some of the parties to deterministically choose the leader, while the others are not aware of the fraud?

Q4.2 [3/30] Fix the protocol.

Q5: **Shamir**

Q5.1 [3/30] Describe the Shamir scheme (k, n) for sharing a secret.

Q5.2 [3/30] Make a numerical example for the case (2, 4), for sharing the secret number 6. Show how the 4 fragments are computed.

Q6: **Access control**

Q6.1 [2/30] Illustrate the DAC model (from Harrison-Ruzzo-Ullman, or HRU), define the concept of safety of the protection system and discuss what practical problems arise within the model.

Q6.2 [2/30] Why is the DAC model vulnerable to Trojans? What type of access control model can prevent them from illegally accessing private data? Discuss.

Q7: **Miscellaneous**

Provide short answers (2 lines max per question) to the following questions.

Q7.1 [1/30] RSA: if $p = 13$ and $q = 17$, what is the range for exponent e?

Q7.2 [1/30] Can iptables block incoming datagrams that are IPSec-tunneled packets going to port 25?

Q7.3 [1/30] What is port forwarding and what protocol implements it?