SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

18 September 2014

NAME _____ **SERIAL NO.** _____

♥: MCE, SSI, SnR; ♠: DSS

EXERCISE NO. 1 (♥,♠) #MARKS: 10

With reference to hash functions,

1. Provide the definition of the *pre-image resistance*, *second-preimage resistance* and *collision resistance* properties;
2. Argue about the relevance of these properties w.r.t. to a digital signature scheme;
3. Argue about the security of hash functions with respect to black box attacks.

EXERCISE NO. 2 (♥,♠) #MARKS: 12

Let us consider the following *secret sharing scheme* that allows us to share a secret x between two non-colluding people so that each person alone is not able to reconstruct the secret.

1. Let x be a secret bit-string t-bit long;
2. Generate a t-bit truly random key k;
3. Compute a *share* s, s.t., $s_i = x_i \oplus k_i$, $0 \le i \le t-1$;
4. Give the key k to Alice and the share s to Bob.

The candidate answers the following questions.

- Question A. Under the assumption that Alice and Bob do not collude, is the scheme perfectly secure? In other words, can Alice or Bob alone derive any information about the secret x?
- Question B. What about if Alice and Bob collude?
- Question C. Generalize the scheme in order to share a secret among n users.
- How many key bits do we need to share a t-bit secret among n users?

EXERCISE NO. 3 (♥) #marks: 8

How the problem of delegation is solved in Kerberos?
Describe the protocols for proxiable and forwardable tickets.

EXERCISE NO.4 (♠) #MARKS: 8

Let (S, D) be a secure digital signature scheme with appendix. Let S and D be the signature and verification algorithm, respectively. Furthermore, let K_P be principal P's public key, and CA a Certification Authority that is trusted by all principals of the system. Finally let H be a secure hash function. Which of the following *certificates* are useful to establish a secure channel with Alice? Argue why.[1]

(A) "Alice" || K_A || S_{CA}(*Alice*)
(B) "Alice" || K_A || S_{CA}(K_A)
(C) "Alice" || K_A || S_A(H("Alice" || K_A))
(D) "Alice" || K_A || S_{CA}("Alice" || H(K_A))
(E) "Alice" || K_A || S_{CA}(H("Alice" || K_A))
(F) "Alice" || K_A || S_{Bob} ("Alice" || K_A) || "Bob" || K_B || S_{CA}("Bob" || K_B)
(G) "Alice" || K_A || S_{Bob}("Alice" || K_A) || "Bob, CA: yes" || K_B || S_{CA}("Bob, CA: yes" || K_B).

[1] Neglect any issue related to time.

SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**
Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS
Master in Computer Engineering

18 September 2014

NAME _____ **SERIAL NO.** _____

SOLUTION

Exercise n.1

See theory

Exercise n.2

Question A. Under the assumption that users do not collude, the scheme is perfectly secure because the key is perfectly random and the share is the result of one-time pad.

Question B. If Alice and Bob collude, they can compute the secret.

Question C. Define $(n - 1)$ keys, k_1, k_2,…, k_{n-1}, and compute a share $s = x \oplus k_1 \oplus k_1 \oplus \cdots \oplus k_{n-1}$. Then distribute share and keys to n different, non-colluding users. Notice that we need the presence (or collusion) of n users in order to reconstruct the secret.

A possible different approach is to 1) generate a single key k; 2) compute a share $s = x \oplus k$, and finally 3) split k into $(n - 1)$ pieces, $P = \{p_1, p_2, \ldots, p_n\}$. Each piece requires $v = t / (n - 1)$ bits. This solution is less secure than the previous one because $(n - 2)$ users may be sufficient to reconstruct the secret. Let us suppose that $(n - 2)$ users are present (or colluding) and that one user, say user u_i is missing. Then, reconstructing the secret through a brute force attack is a matter of attempting all possible sequences of v bits in order to guess the missing key piece. Its complexity is $O(2^v) = O\left(2^{\frac{t}{n-1}}\right) = O\left(\sqrt[n-1]{2^t}\right)$. This computation complexity could be affordable for an adversary also for a small value of n.

Question D. The number of key bits is $(n - 1) \times t$.

Exercise n. 3

See theory

Exercise n.4

A. Certificate A does not link KA to Alice
B. Certificate A does not link KA to Alice
C. Certificate B is self-signed and Alice is not a trusted authority
D. Certificate C is fine.
E. Certificate C is fine.
F. Bob, who is not a trusted authority, signed certificate D.
G. Certificate E is fine: CA delegates B to sign certificates.

SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**

Laurea Specialistica in Ingegneria Informatica ***Laurea Magistrale in Ingegneria Informatica***

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

18 September 2014