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

29 January 2014

NAME____ SERIAL NO.________________________

EXERCISE NO. 1 #MARKS: 10

Argue whether a truly random block cipher is practically feasible or not.

EXERCISE NO. 2 #MARKS: 10

A client *C* and a server *S* share a password Π. Furthermore, client *C* knows the public key P_S of server *S*. Client and server are equipped with computationally secure hash functions as well as symmetric and asymmetric ciphers. Finally client and server clocks are not synchronized. Under these assumptions, client and server attempt to establish a symmetric session key k_{cs} by means of the following protocol.

M1 $C \rightarrow S: \ E_{P_S}\left(C, S, n_c, \Pi, k_{cs}\right)$

M2 $S \rightarrow C: \ E_{k_{cs}}\left(S, C, n_c, n_s\right)$

M3 $C \rightarrow S: \ n_s$

The encryption key indirectly defines the scheme that is used at a given step.

1. Determine whether the protocol satisfies the confidentiality of the Π password in the case of ciphertext-only attack.
2. Assume the adversary gets hold of a session key $\bar{k}_{cs}$ and records the protocol instance $\{\bar{M}1, \bar{M}2, \bar{M}3\}$ that led to that key establishment.
   a. Determine whether the confidentiality of password Π is still guaranteed under this assumption (hint: considers an off-line guessing attack).
   b. Determine whether the protocol suffers from a replay attack.
   c. If the protocol suffers from any of these attacks, modify it in order to prevent them and satisfy the key authentication and key confirmation requirements under the same set of assumptions.

EXERCISE NO. 3 #marks: 10

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 || $S_{CA}(K_A)$
(B) "Alice" || K_A || S_A("Alice" || K_A)
(C) "Alice" || K_A || S_{CA}("Alice" || K_A)
(D) "Alice" || K_A || S_{Bob} (K_A)
(E) "Alice" || K_A || "issuer: Bob" || S_{Bob}("Alice" || K_A || "issuer: Bob") || S_{CA}("Bob, CA: yes", K_B).

[1] Neglect any issue related to time.

SICUREZZA NELLE RETI
Laurea Specialistica in Ingegneria Informatica

SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)
Laurea Magistrale in Ingegneria Informatica

SECURITY IN NETWORKED COMPUTING SYSTEMS
Computer Engineering

29 January 2014

SOLUTION

EXERCISE #1

See theory

EXERCISE #2.

Question 1. The protocol guarantees confidentiality of the password because it is transmitted in its encrypted form. Furthermore M1 is randomized so that an exhaustive data search is not feasible.

Question 2a. Confidentiality is not guaranteed anymore because the adversary can obtain nc from M2 and thus can mount an off-line password guessing attack exploiting M1. The adversary knows fields C, S, n_c and k_{cs} of this message.

Question 2b. The protocol is subject to replay attack because S has no proof of the freshness of message M1. Therefore, if an adversary M has obtained a key $\overline{k}_{cs}$ and the related messages $\{\bar{M}1,\bar{M}2,\bar{M}3\}$, then M can mount a replay attack by replaying message $\bar{M}1$ and then completing the protocol using the key.

Question 2c.

$$
\begin{aligned}
&\text{M1} \quad S \to C: \quad n_s \\
&\text{M2} \quad C \to S: \quad E_{P_S}\left(C,S,\Pi,k_{cs},n_c,n_s\right) \\
&\text{M3} \quad S \to C: \quad E_{k_{cs}}\left(S,C,h\left(n_c\right)\right)
\end{aligned}
$$

Quantity n_s proves S the freshness of message M2.

Quantity $h(n_c)$ proves C that S knows n_c without revealing n_c. Thus the adversary cannot exploit this knowledge in a off-line guessing attack of the password based on M2. Notice that the adversary knows n_s which is transmitted in the clear.

EXERCISE #3.

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