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

11 September 2013

NAME____ SERIAL NO. ____________________

EXERCISE NO. 1 — #MARKS: 10

(A) State the Shannon's definition of Perfect Security.
(B) State the assumptions under which One Time Pad (OTP) is a perfectly secure cipher.
(C) In order for OTP to be perfectly secure, which of the following do we need to assume about the adversary?
   a. The adversary has limited computing power.
   b. The adversary does not know anything about the key.
   c. The adversary cannot modify the message.

EXERCISE NO. 2 — #MARKS: 10

The figure shows an identification protocol that allows a mobile station (MS) to identify itself w.r.t. an access point (AP) where c is a 128-bit random *challenge*, r is the corresponding *response*, and v is 24-bit random *initialization vector*.

M1	$MS \to AP:$	REQ
M2	$AP \to MS:$	c
M3	$MS \to AP:$	v, r
M4	$AP \to MS:$	$YES \mid NO$

Upon receiving message M2 carrying a challenge c from AP, MS generates an initialization vector v at random, computes the response r by encrypting c, $r = \text{SPRG}\left(k \| v\right)\Big|_{128} \oplus c$, where $\text{SPRG}\left(k \| v\right)\Big|_{128}$ is a 128-bit sequence generated by a secure pseudo-random generator SPRG. The generator is seeded by $k \| v$, where k is a long-term cryptographic key secretely shared by AP and MS. Upon receiving the response r from MS in message M3, AP computes $r' = \text{SPRG}\left(k \| v\right)\Big|_{128} \oplus c$, and returns $r' == r$ to the user.

A. Does this protocol guarantee identification? Can a passive adversary impersonate a mobile station?

Let us suppose now that AP sends MS the initialization vector v together with the challenge c in message M2 which becomes $\langle c, v \rangle$ (v in M3 is not necessary anymore)

B. Define a *dictionary attack* against this variant of the protocol and evaluate the size in bytes of the dictionary.[1]

EXERCISE NO. 3 — #marks: 10

We consider the basic version of Kerberos insufficient and feel the need to introduce the Ticket Granting Ticket. Explain why.

[1] Hint: the initialization vector space is small and thus vectors can be reused with high likelihood.

1 July 2013

SOLUTION

EXERCISE #1

A. See the theory.
B. See the theory.
C. The correct answer is B). Option A) is wrong because, a perfectly secure cipher is secure regardless the adversary's computing power. Option C) is wrong because OTP is malleable.

EXERCISE #2.

A. An adversary can eavesdrop the channel, and obtains v, r an c. So it is able to determine $z = r \oplus c$, where $z = \text{SPRG}(k||v)$. By using the pair (v, z) then the adversary is able to identify as MS w.r.t. to AP as many times he likes.
B. As in step A, the adversary can eavesdrop the channel, and obtains v, r an c. However, now, the choice of v is not under its control. So he has to build a dictionary (v, z). Whenever AP reuses v, the adversary is able to reuse z. The dictionary has a number of entries n_e that is equal to the number of initializations vectors, namely $n_e = 2^{24}$. Each entry must accommodate the pseudo-random sequence of bits corresponding to v. So, its size s_e is 16 bytes. It follows that the dictionary size s_d is $s_d = n_e \times s_e = 2^{28}$ bytes = 256 Mbytes.

EXERCISE #3.

See the theory.