SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering, Master in Embedded Computing Systems

05 February 2016

❖: all **◆: all but LMECS** **■: only LMECS**

EXERCISE NO. 1 (❖) #MARKS: 10

With reference to the Shannon's theory,

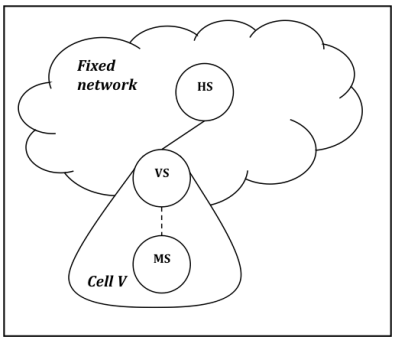
1. Give the definition of perfect cipher;
2. Give the physical interpretation of the definition;
3. Prove the Shannon's theorem.

EXERCISE NO. 2 (❖) #MARKS: 10

Let K_A be the public key of Alice, $S_P(x)$ be the digital signature of principal P on item x, CA be a Certification Authority (trusted by all principals of the system), and finally $H()$ a secure hash function. Validity period apart, which of the following certificates are useful to establish a secure channel with Alice? Argue why.

(A) "Alice" || $S_{CA}(H(\text{"Alice"} || K_A))$
(B) "Alice" || K_A || $S_A(H(\text{"Alice"} || K_A))$
(C) "Alice" || K_A || S_{CA} ("Alice")
(D) "Alice" || K_A || $S_{CA}(\text{"Alice"} || H(K_A))$
(E) "Alice" || K_A || $S_{CA}(H(\text{"Alice"} || K_A))$
(F) "Alice" || K_A || S_{CA} (K_A)
(G) "Alice" || K_A || $S_B(\text{"Alice"} || H(K_A) || \text{"issuer: Bob"}) || S_{CA}(\text{"Bob"} || K_B)$
(H) "Alice" || K_A || $S_B(\text{"Alice"} || H(K_A) || \text{"issuer: Bob"}) || S_{CA}(\text{"Bob"} || \text{"CA=Yes"} || K_B)$

EXERCISE NO. 3 (◆) #MARKS: 10



In a roaming system, a mobile station MS, whose home server is HS, is visiting a cell V served by server VS. MS and HS share the key k_{mh}. Furthermore, HS and VS belong to the fixed infrastructure and share the key k_{vh}. Design a key establishment protocol that fulfils the following requirements:

1. Establish of *secret* shared key k_{mv} between MS and VS;
2. Mutual authentication between VS and MS;
3. Resistance against replay attacks.

Assume that MS, HS e VS use the same cipher E() and that their clocks synchronized. Analyse the protocol by means of the BAN logic and argue that it fulfils requirements 1–3. What if the clocks are not synchronized?

EXERCISE NO. 4 (■) #MARKS: 10

With reference to the CBC encryption mode,

4. Draw the encryption and decryption scheme;
5. State the CBC equations;
6. Briefly discuss pros and cons w.r.t. ECB.

SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering, Master in Embedded Computing Systems

05 February 2016

SOLUTION

EXERCISE N.1

See theory.

EXERCISE N.2

A. "Alice" || $S_{CA}(H(\text{"Alice"} || K_A))$. Not valid because it doesn't carry a ley.
B. "Alice" || K_A || $S_A(H(\text{"Alice"} || K_A))$. Not valid because it is self-signed and Alice is not trusted.
C. "Alice" || K_A || S_{CA} ("Alice"). Not valid because key and name are not linked together.
D. "Alice" || K_A || $S_{CA}(\text{"Alice"} || H(K_A))$. Valid.
E. "Alice" || K_A || $S_{CA}(H(\text{"Alice"} || K_A))$. Valid.
F. "Alice" || K_A || S_{CA} (K_A). Not valid because key and name are not linked together.
G. "Alice" || K_A || $S_B(\text{"Alice"} || H(K_A) || \text{"issuer: Bob"}) || S_{CA}(\text{"Bob"} || K_B)$. Not valid because the certificate is issued by Bob who is not trusted to do so.
H. "Alice" || K_A || $S_B(\text{"Alice"} || H(K_A) || \text{"issuer: Bob"}) || S_{CA}(\text{"Bob"} || \text{"CA=Yes"} || K_B)$. Valid because the certificate is issued by Bob who has been delegated by the CA to do so.

EXERCISE N. 3

Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 12 settembre 2009

The protocol

PROTOCOL (real)

1) $MS \rightarrow VS$: MS, VS, t_m

2) $VS \rightarrow HS$: MS, VS, t_m, t_v

3) $HS \rightarrow VS$: $\{ MS, VS, t_m, t_v, k_{vh} \}_{k_{hm}}$,

$\{ VS, MS, t_v, t_m, k_{vh} \}_{k_{hv}}$

4) $VS \rightarrow MS$: $\{ MS, VS, t_m, t_v, k_{vh} \}_{k_{hm}}$,

$\{ VS, MS, t_m \}_{k_{vm}}$

5) $MS \rightarrow VS$: $\{ MS, VS, t_v \}_{k_{vm}}$

Assumptions

ASSUMPTIONS (only the most important ones)

1. $VS \models HS \Rightarrow (MS \overset{k_{mv}}{\longleftrightarrow} VS)$
2. $MS \models HS \Rightarrow (MS \overset{k_{mv}}{\longleftrightarrow} VS)$
3. $HS \models (MS \overset{k_{mv}}{\longleftrightarrow} VS)$
4. $VS \models \#(t_v)$
5. $MS \models \#(t_m)$

Proof

PROOF (sketch)

AFTER M3

$VS \Subset MS \overset{k_{vm}}{\longleftrightarrow} VS$ (A1)

AFTER M4

$MS \Subset MS \overset{k_{vm}}{\longleftrightarrow} VS$ (A2)

$MS \Subset VS \Subset MS \overset{k_{vm}}{\longleftrightarrow} VS$ (A5)

AFTER M5

$VS \Subset MS \Subset MS \overset{k_{vm}}{\longleftrightarrow} VS$ (A4)