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

15 July 2015

EXERCISE NO. 1 #MARKS: 10

In RSA, encryption/decryption performance depends on the key's binary representation.

1. Argue the above sentence.
2. Argue why the public exponent $e = 3$ or $e = 2^{16}+1$ are a good choice.
3. Argue whether a private exponent d with only two 1's in its binary representation is a good choice or not.
4. Is a public exponent with only one 1 in its binary representation a viable solution?

EXERCISE NO. 2 #MARKS: 12

Alice a Bob share a password (or PIN) P. For identification, they run the following challenge-response protocol:

M1 A→B: CHL
M2 B →A: RSP

Indicate which one of the following implementations of CHL and RSP is secure w.r.t. to an off-line password-guessing attack.

1. CHL = r_a and RSP = $\{r_a\}_K$;
2. CHL = r_a and RSP = $H_K(r_a)$;
3. CHL = r_a and RSP = $\{r_a, r_b\}_K$;
4. CHL = r_a and RSP = $H_K(r_a \| r_b)$;
5. CHL = r_a and RSP = $\{H_K(r_a)\}_{\Pi_A}$;
6. CHL = r_a and RSP = $\{H_K(r_a), r_b\}_{\Pi_A}$.

where: **i)** $\{\cdot\}_\kappa$ denotes encryption by means of key κ (whether symmetric or asymmetric depends on the context), **ii)** $H_k(\cdot)$ denotes a secure MAC; **iii)** r_X is a random number generated by X; **iv)** K is a symmetric key, with $K = f(P)$ and $f(\cdot)$ a deterministic function; and, finally, **v)** Π_A is A's public key, known to B.

EXERCISE NO. 3 #marks: 8

Indicate which of the following certificates is correct.

1. A, Π_A, L, $S_{CA}(H(A\|\Pi_A\|L))$
2. A, Π_A, L, $S_{CA}(H(\Pi_A\|L))$
3. A, Π_A, L, $S_{CA}(H(A\|\Pi_A))$
4. A, Π_A, L, $S_{CA}(A\|\Pi_A\|L)$

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

15 July 2015

SOLUTION

Exercise n.1

For the relationship between performance and key-bit configuration see theory. From that relationship, it follows that the number of multiplications depends on the number of bits equal to 1.

We choose those values for e because they contain only two 1's in their binary representation.

Selecting d so that it has only two 1's in its binary representation would reduce the private key space and make it vulnerable to exhaustive key search.

If e contains only one 1 in its binary representation, then its value is either 1 or even. In both case, it does not fulfill the constraint specified by the RSA key generation algorithm.

Exercise n.2

Case 1 is insecure. The adversary guesses a password, computes a key and decrypts RSP. Then (s)he compares the resulting plaintext with r_a.It follows the complexity of the attack is equal to the password-guessing attack.

Case 2 is insecure. The adversary guesses a password and computes a key. Then (s)he computes the MAC of r_a and checks whether it is equal to RSP. It follows the complexity of the attack is equal to the password-guessing attack.

Case 3 is insecure. The adversary guesses a password, computes a key and decrypts RSP. Then (s)he compares the resulting plaintext with the first field of the resulting plaintext. It follows the complexity of the attack is equal to the password-guessing attack.

Case 4 is insecure. A is not able to verify RSP because (s)he does not know r_b.

Case 5 is insecure. The adversary guesses a password and computes a key. Then (s)he computes the MAC of r_a, encrypts it by means of Π_A, and checks whether it is equal to RSP. It follows the complexity of the attack is equal to the password-guessing attack.

Case 6 is secure, because r_b randomizes RSP.

Exercise n. 3

Case 1 and **4** are secure.

Case 2 is insecure because it doesn't link the user identifier to his/her key.

Case 3 is insecure because it doesn't link the period of validity to the user's key and user's identifier

15 July 2015

martedì 23 maggio 2017 14:43

sncs-150701

Exercise number 1

1. Square-and-multiply algorithm
2. See notes
3. No. Altrimenti si ridurrebbe lo spazio delle chiavi.
4. Uno non cifra niente, e un numero pari non serve a niente.
   e dev'essere co-primo rispetto a phi = (p -1)(q -1).

Exercise number 2

3. I falsi positivi (di K) possono essere eliminati analizzando altre coppie di r_a ed r_b.
4. L'avversario per fare l'attacco dovrebbe provare tutti i possibili r_b per ogni password da provare.
   L'attacco è difficile, ma A non conosce r_b.
5. La chiave pubblica ce l'ha anche l'avversario, perciò la sfrutta sempre.
   Prova un K (generato da una P), fa l'hash e la cripta con la chiave pubblica di A.
   Siccome l'avversario parte dalla password, l'attacco è molto semplice.
6. Lo stesso attacco nel 5, ma per ogni chiave K generata, occorre provare tutti i valori di r_b.
   r_b di solito ha la stessa dimensione delle chiavi, perciò si tratta di tanti valori da provare.

Exercise number 3

1. Certificato giusto, con l'Hash che lega le tre entità.
   È una versione più efficiente da calcolare.
2. Non c'è legame tra
3. .
4. Certificato classico, versione meno efficiente della digital signature.