Examen securitatea sistemelor informatice

Subiecte netratate : 3, 4

Exercitiul 1:

a) Fals – Decriptarea, folosind OTP, a textului criptat 0x253505ba folosind cheia 0x717056ee este mesajul clar **TEST**.
b) Adevarat
c) Adevarat
d) Adevarat
e) Fals – Este recomandat sa se foloseasca RSA pentru transmiterea **cheilor** ın mod criptat
f) Adevarat
g) Fals – SHA256(PAROLA) = **467b4a3eca61a4e62447400d93fc35d4295c08ffa2b04ae942f4de03fa62f464**
h) Scopul principal al unui adversar ımpotriva schimbului de chei Diffie-Hellman este **sa sparga cheia in timpul comunicarii**.
i) Adevarat
j) Adevarat

Exercitiul 2:

a) Conform celui de-al doilea punct, se satisfice principiul separarii cheilor pentru ca se folosesc 4 chei diferite, 2 pentru confidentialitate si 2 pentru integritate. Aceste chei difera pentru sensul de comunicatie.
b) Principiul securitatii “de design” este incalcat conform celui de-al 5-lea punct deoarece exista in aplicatie campuri de input care sunt nesanitizate si nevalidate, permitand injectarea de coduri daunatoare aplicatiei sau bazei de date (exemplu sql injection).
c) Integritatea end-to-end a mesajelor este garantata de functia CRC pentru deteriorarea neintentionata, dar nu si pentru cea intentionata, ce poate fi

cauzata de un atacator. Integritatea poate fi incalcata si conform punctului b). Confidentialitatea poate fi incalcata in momentul in care un atacator descopera modalitatea slaba de securizare a generarii link-ului pentru schimbarea parolei, acesta poate obtine link-ul pentru un alt user folosind username-ul acestuia si data curenta si ii poate schimba parola, avand prin urmare acces la toate informatiile de pe contul acestuia. Confidentialitatea poate fi incalcata si din faptul ca facturile sunt criptate folosind un algoritm determinist.

d) Un astfel de atac poate fi realizat prin exploatarea link-ului de generare pentru schimbarea parolei. Un atacator poate observa pattern-ul predictibil prin criptanaliza(PRNG-ul este public) dupa care link-urile se genereaza si poate schimba parola altui utilizator declansand generarea link-ului, folosind username-ul si data curenta pentru a-si genera singur link-ul victimei, schimbandu-i parola si accesand astfel contul acestuia.