Dima Oana-Teodora 341

Examen Securitatea Sistemelor Informatice
Ianuarie 2022

Subiecte netratate: 3(a), 3(b), 3(c), 3(d)

Exercițiul 1

a. fals

Decriptarea, folosind OTP, a textului criptat 0x253505ba folosind cheia 0x717056ee este mesajul clar **TEST.**

b. adevărat
c. adevărat
d. adevărat
e. fals

Este recomandat sa se folosească **AES + RSA** pentru transmiterea fișierelor în mod criptat.

f. fals

Pentru a asigura integritatea unor fisiere personale, este suficient să stocați pe calculatorul propriu fișierele și valoarea SHA256 corespunzătoare fiecăruia sub forma (file1,SHA256(file1)), (file2,SHA256(file2))....**pe un mediu de stocare extern**.

g. fals

SHA256(PAROLA) =
0x**467b4a3eca61a4e62447400d93fc35d4295c08ffa2b04ae942f4de03fa62f464**

h. adevărat
i. adevărat
j. adevărat

Exercițiul 2

a. Principiului *security by default* este satisfăcut.

Utilizatorul are dreptul să își schimbe parola la cerere, iar link-ul pentru schimbarea parolei este valabil doar o oră. Se respectă principiul deoarece la început are drepturi minimale și doar pentru a-și îndeplini o nevoie primește un drept temporal în plus.

b. Principiul *defence în depth* **nu** este satisfăcut.

Un risc de securitate foarte mare provine din lipsa validării și al sanitizării câmpurilor pentru introducerea datelor utilizatorului. Toate intrările utilizatorului ar trebui să fie considerate nesigure. Pot apărea vulnerabilități de injectare, cum ar fi injecția SQL, dar și vulnerabilităților care ar permite unui atacator să ocolească autentificarea sau să solicite un fișier pe care nu ar trebui să-l vadă.

c. Confidențialitatea și integritatea aplicației

Confidențialitatea datelor este îndeplinită deoarece datele confidențiale ale utilizatorilor sunt criptate prin funcția hash(parola), respectiv de criptare(fișierele).

Integritatea mesajelor nu este îndeplinită, deoarece CRC(m) oferă un prag minim de securitate al fișierelor, mesajele putând fi foarte usor alterate de către un atacator.

d. Atac activ care permite logarea prin impersonarea unui alt utilizator

Logarea prin impersonare presupune ca atacatorul să intre în posesia datelor de conectare (username și parola) ale unui utilizator al aplicației. Link-ul pentru resetarea parolei poate fi ușor de prezis. Atacatorul cere întâi resetarea parolei din care obține PRNG-ul. Iar apoi folosește ca seed username-ul și ziua curentă pentru a obține link-ul de resetare al parolei al userului.

Exercițiul 4

Pentru orice mesaj *m*, evaluarea expresiei *m AND NOT(m)* o să aibă mereu ca rezultat un șir lung de 0(ceva cu ceva negat dă mereu 0).

Mac(k, *m* AND NOT(*m*)) = Mac(k, 0……..0) = *t*, oricare ar fi *m* mesaj
0 de |*m*| ori

Presupunem că un adversar trimite către MAC mesajele m_0 si m_1(două șiruri diferite de aceeași lungime) . MAC întoarce tagurile asociate acelor mesaje.

Relația 1: Mac(k, m_0 AND NOT(m_0)) = Mac(k, 0..……0) = t_0
0 de |m_0| ori

Relația 2: Mac(k, m_1 AND NOT(m_1)) = Mac(k, 0……...0) = t_1
0 de |m_1| ori

Relația 3 din ipoteză: Mac'(k, *m*) = Mac(k, *m* AND NOT(*m*)) = *t*

Relația 1 + Relația 2 + Relația 3 ⇒ Mac'(k, m_0) = Mac'(k, m_1) = t_0 = t_1= *t* (tagul este același pentru cele 2 mesaje) ⇒ se poate trimite mesajul nou m_2 cu tagul *t* spre verificare către MAC.

Vrfy algoritm de verificare care întoarce un bit (1 valid, 0 invalid).
Adversarul nu ar trebui să poată să găsească un tag pentru niciun mesaj nou care nu a fost deja trimis.

Vrfy'(k, m_2, t) = Vrfy(k, m_2 AND NOT(m_2), t) = Vrfy(k, 0……0, t) = 1 ⇒ MAC-ul **nu** este sigur
În concluzie, un atacator poate foarte ușor să genereze un tag de securitate pentru orice mesaj de o anumită lungime.