CYBER SECURITY

5. forduló

Continental The Future in Motion

A kategória támogatója: Continental Automotive Hungary Kft.

Ismertető a feladathoz

A kriptográfiai kulcsok kezelésekor külön figyelmet kell fordítanunk a megfelelően biztonságos tárolásra. Ennek oka, hogy az autóiparban is megjelentek a szabványos célhardverek, hardver-kiegészítések, melyeknek feladata a kulcsok biztonságos tárolása.

Ebben a fordulóban egy beágyazott rendszer memóriájából kell egy kulcsot kinyerni, és a kulcs segítségével titkosított adatot visszafejteni.

A forduló megoldásához erősen ajánlott egy kriptográfiai eszköztár használata (pl. Python környezet PyCryptodome libraryvel).

Felhasznált idő: 00:00/25:00 **Elért pontszám:** 0/15

Indítás utáni csatolmányok

1. feladat 0/15 pont

Egy AES-128-as kulcsot egy változóként rögzítettünk a rendszer memóriájában. Azt itt tárolt adatok hexadecimálisak. A feladatunk a kulcs megtalálása, majd AES ECB módszerrel vissza kell fejteni a következő titkosított szöveget (padding mechanizmusként a PKCS7-es standard lett használva):

```
7a4aa3819f3d5d14fa82dea63648a614a5dd75ee624edb7c849a29a31cea5283 (hex)
```

A megoldás a padding nélküli szövegrész!

Az eredményt szövegesen szeretnénk kérni.

Válasz

A helyes válasz:

The future in motion

Magyarázat

Két megoldás kínálkozik a feladat megoldására:

- Brute force módszer,

- vizuálisan megtalálni a kulcsot.

Brute force módszer esetén minden 16 bájtnyi adatot ki kell próbálnunk, mintha az lenne a kulcsunk. Amennyiben valamelyik 16 bájtnyi adattal sikerül a decryptálás, a feladatot megoldottuk. Egy példa a brute force megoldás kivetelezésére:

```
from Crypto.Util.Padding import unpad
from Crypto.Cipher import AES

def decrypt(ciphertext, key):
    cipher = AES.new(key, AES.MODE_ECB)
    return unpad(cipher.decrypt(ciphertext), 16, style='pkcs7')

with open('eeprom_dump', 'r') as f:
    for line in f.readlines():
        line = line.split('|')[1].strip().replace(' ','')
        rawbytes = bytearray.fromhex(line)
        try:
            print(decrypt(bytearray.fromhex('7a4aa3819f3d5d14fa82dea63648a614a5dd75ee624edb7c849a29a31cea5283'), rawbytes))
            print(f'Decrypted from: {line}\n')
        except Exception as e:
            pass
```

A másik megoldás a vizuális keresés. Itt észre kell vennünk, hogy a 615. és 617. sorok teljes FF-eket tartalmaznak. Köztük 16 bájtnyi adatsor található, ami a kulcs.

Ezt követően a kulcsot a megfelelő formátumra kell hoznunk, majd vissza kell fejtenünk a fenti titkosított üzenetet. Legvégül a padding során bekerült extra karaktereket kell eltávolítanunk.

Lehetséges megoldás Python programnyelven:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad


key =  bytes.fromhex("70367F904803SB1F36C7015CE6FA7FD4") #-> 66. sor
cipher = AES.new(key, AES.MODE_ECB)


plaintext_pad = cipher.decrypt(bytes.fromhex("d496fe98e35288d8c6d5bfc1f0be412f2615270ef1bc35571893247ae012238e"))

plaintext = unpad(plaintext_pad, 16, style='pkcs7')
print(plaintext)
```