Kutxabank Praktika

Haitz Aldaraborda, Jon Mugica eta Iker Zaldua

2024.eko urriaren 18

1 Sarrera

Kutxabank banku batean lapurreta bat egin eta gero, sisteman dagoen informazio bakarra zifratutako fitxategi bat da. Honetan lapurretarekin erlazionatutako informazioa egon daiteke, eta hau deszifratu behar da.

Arazo honekin laguntzeko fitxategia zifratu duen exekutagarria eskuratu da, baina hau zifratua dago. Hau aztertuz fitxategia deszifratzea espero da.

2 Exekutagarriaren azterketa

Exekutagarria *hexdump -C* komandoaren bitartez aztertuta, hurrengo informazioa aurkitu dugu:

- AES zifratze algoritmoa erabil da.
- AES blokekako zifratze moduetan hiru aukeretati CBC da. Zifratutako mezuak beti luzeera berdina duelako (padding-a dauka), ondorioz CTR ez izanez, eta zifratuko den mezuaren lehen blokea modifikatuz bigarren blokearen zifratzea aldatu egiten delako, ECB moduan ez bezala.
- Gakoa bilatuz "privatekeyaescypherkutxabank" hitz segida aurkitu da, honek "key" hitza duelako gakoa izatea supodatu daiteke.
- Gako honen luzeera kontuan hartuta (28 byte) AES-256 da zifratze algoritmo aukera bakarra. Hau programaren funtzionamenduarekin frogatu daiteke, fitxagtegi bat zifratzerakoan honek teklatuko sarrera bat eskatzen duelako, eta bakarrik lehen lau byteak hartzen dituealako kontuan. Honela lortutako gakoa + 4 byte = 32 byte dira, AES-256 algoritmoaren gako luzeera.
- *Kutxabank* entitateko fitxategi guztiek ur-marka bat dutela suposatu dezakegu hau zifratze algoritmoan aurkitutako "ownedbykutxabank" izanda.

3 Gakoa lortzea

AES-256 CBC enkriptazio baten aurrean egonda gakoa *brute force attack* baten bidez lortzea zentzugabekeri bat da.

Baina, gakoa berreskuratzean laguntzeko gakoaren zati handi bat eskuratu dugu, baita gako oso zuzenarekin enkriptatutako fitxategiaren lehen blokea ("owned-bykutxabank). Honela gako osoaren balio guztiak aztertu ordez bakarrik azkeneko 4 byteak aztertuko dira.

Honetarako, azken 4 bytearen aukera guztiak frogatuko dituen programa motz bat egin da. Honek, gakoaren aukera posible guztiak probatuko ditu "owned-bykutxabank" cypher textua desencriptatuz, fitxategi deszifratuaren lehen bloke berdina lortu arte.

Bilaketa hau motzagoa egiteko, bi modifikazio egin dira. Lehenik, CPU-ak AES kriptografia azkarrago egiteko dakarteen hardware berezia erabiltzea lortu da, bilaketa laburtua egiteko. Gainera zifratzerako orduan lau byte eskatu egiten direlako, eta banku baten arloan eman delako, lau byte hauek zenbakiak izatea suposatu da, honela 256 ASCII balioen artean bilatu ordez bakarrik 48-57 (9 balio) balioen artean bilatuz.

4 Exekuzioa

Aurreko algoritmoa aplikatuta, programa osatu eta exekuzioa hasi da.

Lehenengo kasua, **AES estandarra** erabiliz. Exekuzioaren denborak lortu dira eta emaitza ondorengoa izan da:

AES estandarraren exekuzio denbora
0.049910 segundu

Bigarren kasua, **AESNI** erabiliz. Exekuzioaren denborak lortu dira eta emaitza ondorengoa izan da:

AESNI-ren exekuzio denbora
0.003506 segundu

Datuak ikusita, antzeman daiteke, azeleragailuak exekuzio denbora asko jeisten duela, x14 aldiz azkarragoa baita.

5 Ondorioak

Programa exekutatu ondoren, Key-aren azkeneko 4 byteak lortu dira,
50 48 51 52 zenbaki hexadezimalak lortuz. Zenbaki hauen ASCII balioa lortzen badugu, 2034 zenbakia lortzen da.
Hau ikusita, esan daiteke, deszifraketa betetzeko azkeneko 4 zenbakiak horiek izan direla, beraz, "decryptfile" exekutagarria erabiliz, ondorengo .odt fitxategia lortu da:

Fitxategia

NOTA PERSONAL:
Otra vez no me han subido el sueldo. Estoy cansada de este trabajo. Hoy he descubierto una vulnerabilidad en el sistema de cuentas que podría permitir hacer transacciones. Me va a llevar tiempo saber como aprovecharla pero lo voy a hacer.
Libe