INTELLIGENS KÁRTYÁK VÉLETLENSZÁM-GENERÁTORÁNAK EMPIRIKUS VIZSGÁLATA

Bencsáth Boldizsár, Berta István Zsolt
Budapesti Műszaki és Gazdaságtudományi Egyetem,
Híradástechnikai Tanszék
Email: boldi@ebizlab.hit.bme.hu, isti@ebizlab.hit.bme.hu

Az intelligens kártyák biztonságos mikroszámítógépek, a bennük tárolt adatokat illetéktelenek nehezen tudják kinyerni. Ha garantáljuk, hogy egy *k* kulcs soha nem hagyja el a *C* kártyát, a *k* kulccsal rejtjelezett szöveg nem fejthető meg *C* hozzájárulása nélkül. [3] Ha *k* teljes életciklusa (generálás, tárolás, használat, megsemmisülés) a kártyán megy végbe, a fenti feltétel biztosítható. Jelen előadásunkban a kártyán történő kulcsgenerálás problémakörét vizsgáljuk meg részletesebben.

Kriptográfiai értelemben jó kulcs előállításához megfelelő véletlen forrás szükséges. (Ha a kulcs nem véletlenszerű, akkor a véletlenszám-generáló algoritmus alapján egy támadó is rájöhet a kulcsra.) A véletlenszám-generátorok valamely fizikai folyamatból nyert valódi véletlen jelenséget használnak fel véletlenszám-generálásra. Az ún. álvéletlenszám-generátorok egy folyamatosan változó belső állapot (seed) alapján állítják elő az álvéletlenszámokat.

Biztonságtechnikai szempontból létfontosságú, hogy a kulcsgenerálásra használt véletlenszám-generátor kimenete megjósolhatatlan legyen, különben a támadó is hozzáférhetne a kulcshoz. A megfelelő termék kiválasztásához szükség van arra, hogy az előállított véletlen számok minőségét ellenőrizni lehessen.

Sajnos, a véletlenszámokat nem tudjuk konkrét eredményhez hasonlítani, csupán a kapott adatfolyam statisztikai paramétereire tudunk elvárásokat megfogalmazni. A véletlenszám-generátorok tesztelésének eredménye mindig kétséges. Ha megállapítjuk, hogy a véletlenszám-generátor hibás, az egyértelmű. Ellenben, ha egy teszt szerint az előállított adat véletlenszerű, az nem jelenti azt, hogy a véletlenszám-generátor jó, csak azt, hogy nem sikerült hibát találnunk.

Laboratóriumunkban megvizsgáltuk néhány nagyobb gyártó intelligens kártyájának (Bull – Odyssey, Schlumberger – Cyberflex, Oberthur – Simphonic, Dallas Semiconductor – iButton) véletlenszám-generátorát. A fenti eszközökkel a mérések elvégzéséhez elég nagy mennyiségű (kb. 100-200 kilobyte) véletlen adatot állítottunk elő, majd ezen adatfolyamot statisztikai teszteknek vetettük alá. Ezek között szerepelt az egyenletes eloszlásra való illeszkedést vizsgáló chi-négyzet próba, az entrópiavizsgálat, az értékek átlaga, valamint a véletlen forrás segítségével előállított Pi érték vizsgálata. A tesztek között szerepelt a véletlenszám-generátorok egyik legjobb tesztje, a Maurer teszt ([4]), valamint a FIPS 140-1 szabványnak megfelelő tesztsorozat ([5]) is. Részletes eredményeinket [1] tartalmazza.

Méréseink a Bull Odyssey I smartcard véletlenszám-generátorában hibát mutattak ki. A bájtonkénti entrópia ennél a generátornál mintegy 7.98, a Chi-négyzet próba rossz eredményt ad, és az mért adatok átlaga is jelentős differenciát tartalmaz a várt értéktől. A Maurer teszt a Bull kártyára egyértelmű hibát jelez, és a FIPS teszt a különböző 20 kilobites blokkokra nézve sok esetben szintén hibát mutatott ki. (Többnyire a poker és monobit tesztekre, néha a „runs” tesztre is.)

A chipkártyák véletlenszám-generátorának működése nem nyilvános, belső felépítésükről a gyártók nem szívesen adnak információt. Ma viszonylag kevés kártya van a piacon, amely valódi véletlenszám-generátorral rendelkezik, többségük – feltehetően – egy rejtjelező segítségével megvalósított álvéletlenszám-generátort tartalmaz.

Sajnos egy chipkártya véletlenszám-generátorának hibája a függetlennek látszó tranzakciók biztonságát is veszélyezteti. Ha a támadó egy biztonsági szempontból nem kritikus tranzakció kulcsához hozzájut, kikövetkeztetheti – a véletlenszám-generátor hibájának ismeretében – az elkövetkező összes tranzakció kulcsait.

Mivel a chipkártyák felépítése nem nyilvános, javasoljuk a terminál bevonását a véletlenszám-generálás folyamatába. Modellünkben az intelligens kártyát fogadó terminál is rendelkezik saját véletlenszám-generátorral, melynek segítségével generál egy $r_{terminal}$ véletlen számot. Ezt elküldi a kártyának, ami a terminálától kapott számot mod2 hozzáadja a saját r_{card} véletlenszámához, s így hozza létre a $k = r_{terminal} \oplus r_{card}$ kulcsot. Bizonyítható, hogy k entrópiája nem lesz kisebb, mint r_{card} entrópiája.

Szintén igazolható, hogy ha a terminál nem juthat k-ról több információhoz $k = r_{terminal} \oplus r_{card}$ esetben, mint $k = r_{card}$ esetben, vagyis a módszer alkalmazható nem megbízható terminálok esetén is, bár ekkor a véletlenszám minőségét a terminál nem javítja.

Ha a terminál nem rendelkezik saját megbízható véletlenszám-generátorral, a hálózati késleltetések gyűjtőhálózati architektúrával történő méréséből származó adatokat használhatjuk a véletlen adatok javítása érdekében. Ennek a módszernek részletes statisztikai analízisét korábbi publikációnk, [2] tartalmazza.

Irodalomjegyzék

[1] B. Bencsáth, I. Zs. Berta, A. Bognár, I. Verók, „Smart cardok véletlenszám-generátorának empirikus vizsgálata” 2001,
http://ebizlab.hit.bme.hu/~isti/publications/scrandom/scrandom-kz.pdf

[2] B. Bencsáth, I. Vajda, „Collecting randomness from the net”, In Proceedings of the IFIP TC6 and TC11 Joint Working Conference on Communications and Multimedia Security 2001, Darmstadt, Germany, May 2001, Kluwer,
http://ebizlab.hit.bme.hu/~boldi/publications/collrnd.pdf

[3] Berta, I. Zs., Mann, Z. Á., „Programozható chipkártyák és azok biztonsága”, Magyar Távközlés, Budapest, 2000.

[4] Maurer, Ueli M., „A universal statistical test for random number generators”, Journal of Cryptology, vol.5, no. 2., 1992, pp. 89-105.

[5] „Security Requirements for Cryptographic Modules”, Federal Information Processing Standards Publication 140-1, 1994, http://csrc.ncsl.nist.gov/fips, Implementation: Neal Bridges, 2000.