AZ ELEKTRONIKUS ALÁÍRÁS HASZNÁLATÁNAK BIZTONSÁGI PROBLÉMÁI

Dr. Leitold Ferenc
Veszprog Kft., Veszprémi Egyetem Információs Rendszerek Tsz.
fleitold@veszprog.hu

BEVEZETÉS

Az elektronikus aláírásról szóló törvény elfogadása mérföldkő az információs társadalom magyarországi életében. A törvény azonban jogi oldalról közelíti meg az elektronikus aláírás problémakörét, nem vagy csak minimális mértékben foglalkozik biztonsági kérdésekkel. Sajnos a gyakorlatban számos olyan elterjedt eszköz és eljárás létezik, melyeknek az elektronikus aláírásra történő használata súlyos biztonsági problémákat vet fel. Minden elektronikusan aláírónak, aláírást elfogadónak elemi érdeke, hogy a rendszer használata során keletkező biztonsági réseket csökkentsük, illetve a rendszer felállításával ne teremtsünk újabbakat. Az előadás megpróbálja összegezni az elektronikus aláírás használatából eredő, illetve a törvényi előírásokból következő támadási pontokat.

AZ ELEKTRONIKUS ALÁÍRÁS MŰKÖDÉSI HÁTTERE

Az elektronikus aláírás létrehozása, illetve a létező elektronikus aláírás ellenőrzése/elfogadása az alábbi lépésekben történik:

1. Első lépésben a küldő eszközén előáll az aláírandó dokumentum.
2. Az aláírandó dokumentum bináris kódsorozatából elkészül a dokumentumra egyedileg jellemző ujjlenyomat. Ez az eljárás Hash algoritmusok segítségével valósítható meg, melyek lényege, hogy az ujjlenyomatból csak nagyon "nehezen" lehet előállítani az eredeti dokumentumot.
3. Az ujjlenyomatot valamely nyilvános kulcsú algoritmus kulcspárjának titkos részével titkosítjuk. Az így előálló kódsorozat a dokumentumhoz rendelt **digitális vagy elektronikus aláírás**.
4. A küldő ezt követően a dokumentumot és a hozzá rendelt digitális aláírást továbbítja.
5. A fogadó megkapja a dokumentumot és a digitális aláírást.

6. A dokumentumból ugyanazzal a Hash algoritmussal, mint a küldő előállítja a dokumentumhoz rendelt ujjlenyomatot.
7. Előállítja továbbá a digitális aláírásból a küldő nyilvános kulcsának felhasználásával a digitális aláíráshoz rendelt ujjlenyomatot.
8. Abban az esetben, ha ez a két ujjlenyomat megegyezik, a fogadó biztos lehet abban, hogy az elektronikus aláírás az ellenőrzéshez felhasznált nyilvános kulcs titkos párjával készült.

A módszer matematikai elmélete önmagában NEM biztosítja tehát azt, hogy az elektronikus aláírást az aláíró személyéhez rendeli. Ezt az elektronikus aláírásról szóló törvény oldja meg.

Jelen előadás NEM foglalkozik azokkal a veszélyekkel, melyeket az alábbiak jelentenek:

- **A nyilvános kulcsú algoritmus okozta támadási lehetőség**: megfelelően nagy számítási kapacitással a leggyakrabban használt RSA algoritmus is visszafejthető.
- **Az ujjlenyomatot készítő Hash algoritmus okozta támadási lehetőség**: megfelelően nagy számítási kapacitással elképzelhető, hogy generálható olyan dokumentum, amely egy létező ujjlenyomathoz tartozik.
- **Az elektronikus aláírásról szóló törvény által megvalósított hitelesítési eljárás okozta támadási lehetőség:** a törvény által megszabott eljárás az, amely garantálja, hogy a nyilvános kulcsú algoritmus titkos kulcsa valóban az aláírónak vélt személy birtokában van.

AZ ELEKTRONIKUS ÉS A PAPÍR ALAPÚ ALÁÍRÁS ÖSSZEHASONLÍTÁSA

Az aláírás létrehozásakor két alapvető fontosságú dolgot kell figyelembe venni:

1. Az aláírónak pontosan tudnia kell, hogy mit ír alá, meg kell azt értenie, és el kell döntenie, hogy valóban azt szeretné-e aláírni.
2. Az aláírónak biztosnak kell lennie abban, hogy azt és csakis azt írja alá, amit szeretne.

Nézzük, hogyan teljesülnek a felvetett szempontok a papír alapú, illetve az elektronikus aláírás esetében.
Ha egy papír alapú szerződést szeretnénk az aláírásunkkal ellátni, pontosan tudjuk, hogy mit írunk alá:

- CSAK A SZEMÜNKNEK KELL ELHINNI, HOGY MIT LÁTUNK!
- Nyilvánvaló továbbá, hogy azt is csak a szemünknek kell elhinnünk, hogy mit írunk alá, milyen papírra helyezzük el aláírásunkat.

Amennyiben viszont elektronikusan szeretnénk az aláírást a dokumentumon elhelyezni, akkor

- El kell hinnünk a szemünknek, hogy azt látjuk és értjük, ami a monitoron vagy nyomtatásban megjelenik.
- El kell hinnünk továbbá, hogy ami megjelent, annak pontosan az az értelme, amit a háttértár egy állományának bitsorozata jelképez.
- Végül el kell hinnünk, hogy az aláírás létrehozásával csak és kizárólag az általunk aláírni szándékozott állomány bitsorozatához képződik az aláírás.

A szemének általában minden értelmes ember elhiszi, hogy mit lát, így a továbbiakban csak az utóbbi két problémával foglalkozunk.

BITSOROZAT MEGJELENÍTÉSE

Alapvető elvárás (lenne), hogy az aláírandó dokumentum minden információt tartalmazzon annak értelmezéséhez, illetve megjelenítéséhez. Amennyiben ugyanis az értelmezéshez bármilyen máshonnan vett információ szükséges, úgy befolyásolni lehet a dokumentum megjelenített képét. Tipikusan ilyen információ például a karakterek képe. Egy Word dokumentum nem tartalmazza azokat a betűtípusokat, amelyek szükségesek ahhoz, hogy a dokumentum képét megjelenítsük. Így a betűtípusok változtatásával elérhető, hogy ugyanazon dokumentum megjelenített képe más és más legyen. Sajnos ugyanez a helyzet az ASCII szövegállományokkal is. Jóllehet, itt nincsenek betűtípusok, de a megjelenítéshez szükséges a karakterek képének az ismerete. Ez pedig a dokumentumon (a szöveg bitsorozatán) kívüli információ, melyet az ASCII szabvány rögzít, azonban a megjelenítést a számítógépek szoftverei végzik. Ahhoz tehát, hogy biztosítsuk a dokumentum és a megjelenített képe közti egyértelműséget elengedhetetlen, hogy a dokumentum **önmagában** tartalmazza a karakterek bináris képét.

Felvetődik a kérdés, hogy milyen lehetőségei vannak egy támadónak, hogy ezen biztonsági hézagot kiaknázza:

1. Megteheti, hogy ha hozzáfér a másik számítógéphez, akkor egy kis alkalmazással felcserélje a betűk képét valamely betűtípusban.
2. A betűk felcserélését elérheti egy kis programmal is.
3. Ezt a kis programot akár bejuttathatja egy e-mail elküldésével is. Erre rengeteg lehetőséget kínálnak az utóbbi időben egyre "népszerűbb" e-mail vírusok példái.

Megállapíthatjuk tehát, hogy egy rosszindulatú támadó könnyedén megteheti azt (különösen ha például a partnere nem ért az informatikai biztonsághoz), hogy a laikus partner számítógépébe bejuttat valamilyen programot, ami aztán gondoskodik arról, hogy az aláíró ne azt lássa a képernyőn, amit aláír. Megteheti azt is, hogy az aláírást követően (például egy meghatározott időben) teljesen kiirtja magát a laikus számítógépéről. Ezt követően a laikus felhasználó hiába bizonyítaná igazát az elektronikus aláírás a törvény szerint a bíróság előtt bizonyító erejű…

BITSOROZAT ALÁÍRÁSA

Amennyiben pontosan tudjuk azt, hogy mit szeretnénk aláírni (vagy legalábbis elhisszük azt) elláthatjuk a dokumentumot elektronikus aláírásunkkal. Ahhoz, hogy ezt megtegyük *aláírás-létrehozó eszközre* van szükségünk. Az aláírás-létrehozó eszköz mindenképpen tartalmaz szoftver elemeket és tartalmazhat hardver elemeket is. Lényege, hogy amikor úgy döntünk, hogy egy dokumentumot szeretnénk aláírni, akkor minden feltétel adott a számítógépben, hogy ezt megtegyük. Manuálisan nem vagyunk képesek arra, hogy ellenőrizzük azt, hogy valóban azt a bizonyos bitsorozatot látjuk el aláírással, amit szeretnénk és abban sem lehetünk bizonyosak, hogy más bitsorozathoz nem készül aláírás.

Tipikus támadási lehetőség lehet például az alábbi módszer: egy kis program (amit az előző fejezetben leírt módszerek bármelyikével bejuttathatunk a számítógépbe) figyel egy olyan interaktív tevékenységet, amit a felhasználónak kell megtennie az után, hogy az aláíráshoz szükséges valamennyi feltételt előállított (pl. behelyezte a chipkártyáját az olvasóba). Az esemény hatására érzékeli, hogy a felhasználói program milyen információkat küld aláírásra pl. a kártyaolvasónak. Ezt elküldi az olvasónak és megvárja a választ, de nem továbbítja a felhasználói programnak, hanem miután megkapta elküld egy másik bitsorozatot olvasónak aláírásra. Ha ez megtörtént, csak azután küldi vissza az elsőként megkapott aláírt választ a felhasználói programnak. Az egész természetesen olyan gyorsan történhet, hogy a felhasználó

semmit sem vesz észre. Sőt! Még azt is megteheti a “kis program”, hogy az e-mail vírusok többségéhez hasonlóan, a saját SMTP rutinjával visszaküldi az aláírt bitsorozatot a támadónak!

ALÁÍRT DOKUMENTUM TOVÁBBÍTÁSA

Amennyiben rendelkezünk egy elektronikusan aláírt dokumentummal, akkor ezt szeretnénk továbbítani partnerünk felé. Megtehetjük ezt például úgy, hogy floppy lemezre másoljuk és elvisszük az illetőnek. Ebben az esetben azonban semmivel sem könnyebb az életünk, mintha papíron írnánk alá a szerződést. Az igazi könnyebbséget az jelenti, ha anélkül, hogy felállnánk a székünkből, az információs “szupersztrádán” továbbítjuk az aláírt dokumentumot. Azonban tisztában kell lennünk azzal, hogy egy egyszerű e-mail elküldése az kb. olyan biztonságú, mintha egy képeslapot adnánk fel a postán. Tekintettel arra, hogy szerződéseinket, nyilatkozattételeinket, adóbevallásunkat általában szeretjük bizalmasan kezelni, így alapvető elvárás, hogy minimum egy zárt borítéknak megfelelő biztonsági szinttel továbbíthassuk az aláírt üzenetet. Ehhez kiváló megoldást nyújt a nyilvános kulcsú kriptográfia, melyet nem csak az elektronikus aláírásra, hanem titkosításra is használhatunk. Azonban ezt a felhasználási módot, az aláíráshoz használt kulcspár tekintetében a törvény egyértelműen kizárja. Törvényes keretek között az egyedüli megoldás, ha egy másik kulcspárt használunk titkosítási célra. Titkosítás esetén alapvető követelmény, hogy a titkosított üzenetet csak és kizárólag a címzett tudja kicsomagolni. Nézzünk erre egy egyszerű példát: Tegyük fel, hogy két cégvezető szerződést szeretne kötni egymással, és elektronikusan szeretnék azt aláírni. Tegyük fel továbbá, hogy egyikük (vagy esetleg mindegyikük) Windows operációs rendszer alatt Outlook-kal levelezik. Mindkét cégnek – az internetes támadásoktól félve – hatékony tűzfalrendszere van. Ahhoz, hogy a szerződéskötést e-mail-en keresztül, titkosítva le tudják bonyolítani, mindenképpen szükséges, hogy a tűzfalrendszer átengedjen olyan e-mail-eket, amelyek titkosítva vannak és a tűzfal nem képes azt megvizsgálni. Ha viszont ez így van az Outlook-ot használó cégvezető(k) számítógépe a tűzfalon kívül, titkosított üzenetekkel könnyen támadható. A támadónak nem kell mást tennie, mint e-mailben, titkosítva elküldeni támadó programját a cégvezetőnek. Például a Badtrans vírushoz hasonlóan az Outlook alatt nem szükséges a cégvezetőnek bármit tennie ahhoz, hogy a programkód elinduljon és elvégezze azt, amit a támadó szeretne.

ÖSSZEFOGLALÁS

Az előadás két problémakört igyekezett körüljárni:

- Amennyiben az aláírás-létrehozó eszköz egy más célra is használt PC, akkor ez egy hatalmas biztonsági hézagot vet fel. Semmi probléma olyan esetben, ha egy zárt rendszerben célgépek csak meghatározott feladatot látnak el (például bankautomaták.) A fokozott biztonságú elektronikus aláírás, a törvényi definíció alapján, olyan elektronikus aláírás, amely többek között rendelkezik azzal a feltétellel, hogy "olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll". Ezek alapján megállapíthatjuk, hogy semmilyen Windows alapú operációs rendszer nem lehet az alapja az aláírás-létrehozó eszköznek.
- Az aláírt dokumentum biztonságos továbbításának lehetősége a tűzfalrendszerek védelmi képességeit teszi próbára. Különösen gondot jelent a probléma, ha valamely államigazgatási szerv esetén kötelezővé válik az elektronikus aláírás elfogadása. Kérdés, hogy az APEH hogyan oldja meg azt, hogy titkosított üzeneteket fogadjon anélkül, hogy biztonsági tűzfalrendszerén csorba essék.

A 90-es évek elején (lehet, hogy még manapság is) gyakran előfordult, hogy a nagykörúton haladó 4-es, illetve 6-os villamos vezetője figyelmeztette az utasokat: "Figyelem! A villamoson zsebtolvajok vannak, kérjük kedves utasainkat, vigyázzanak értékeikre!" Ki kérdőjelezné meg a villamosvezető figyelmeztetésének jogosságát ? Pedig minden támadásra felhívó nyilvános üzenetnek két hatása van: Egyrészt az emberek szorosabban fogják táskáikat, belső zsebbe teszik át irataikat, azaz jobban vigyáznak az értékeikre (a törvénytisztelők számára ez a természetes). Másrészt viszont a potenciális, újabb zsebtolvajoknak az üzenet felhívja a figyelmét arra, hogy ez egy jó lehetőség, amit ki lehet használni, akkor, vagy később, egy másik alkalommal. Jelen előadás megpróbálta az elektronikus aláírás használatával kapcsolatosan, a lehetséges támadási pontokat bemutatni. Nyílván eme figyelmeztetésnek is két hatása lehet. Azonban minden digitálisan aláírónak, aláírást elfogadónak érdeke, hogy a rendszer használata során jelentkező veszélyekkel tisztában legyen, illetve megtegyen mindent annak érdekében, hogy ezeket a réseket csökkentse. Ha felszáll valaki a villamosra, szeretne tisztában lenni a rá leselkedő fenyegetésekkel, támadási lehetőségekkel.