BIZTONSÁGOS ELEKTRONIKUS ALÁÍRÁS MEGBIZHATATLAN KÖRNYEZETBEN

Dr. Leitold Ferenc
Veszprémi Egyetem, Információs rendszerek Tanszék
fleitold@veszprog.hu

BEVEZETÉS

Aki gyakran ül autóba, tisztában van vele, hogy milyen dolgokra kell odafigyelnie, hogy az utazás során a biztonságát maximalizálja. Általában mindenki el szokta vinni autóját a rendszeres átvizsgálásokra, ha észrevesszük, hogy nem fog a fék, szerelőhöz fordulunk. De vajon hasonló gondossággal járunk-e el, ha a számítógépünkről van szó? Alkalmazunk-e olyan szoftvereket, amelyek biztonságunkat szolgálják? Frissítjük-e megfelelő gyakorisággal vírusvédelmünket, tűzfalunkat? Figyeljük-e folyamatosan operációs rendszerünk javításait, melyek az újabb és újabb biztonsági réseket foltozzák be? ... és még sorolhatnánk a megválaszolandó kérdéseket.

A fentiek alapján felmerül a kérdés, hogy megbízhatunk-e számítógépünkben. Használhatjuk-e számítógépünket - megfelelő biztonsággal – például egy 50 milliós szerződés elektronikus aláírására? Megbízhatunk-e ennyire a számítógépben és a rajta futó szoftverekben?

Mit tehetünk annak érdekében, hogy az elektronikus aláírás használatának kockázatát csökkentsük, és mit tehet egy laikus számítógép használó, aki nem kíván a számítógépes biztonság rejtelmeiben elveszni, de mindennapi életében szívesen használna a technika új vívmányait?

AZ ELEKTRONIKUS ALÁÍRÁS HASZNÁLATÁNAK BIZTONSÁGA

Az elektronikus aláírás gyakorlati alkalmazásának biztonságát az alábbiak garantálják:

- Nyilvános kulcsú algoritmusok (pl. RSA), mely matematikai hátterével gondoskodik róla, hogy belátható időn belül ne lehessen az elektronikus aláírást a titkos kulcs nélkül előállítani, a titkosított üzenetet ne lehessen visszaállítani.

- Az elektronikus aláírásról szóló törvény biztosítja a titkos kulcs felhasználóhoz rendelését, illetve azt is, hogy ellenőrizhető legyen, hogy az aláírás érvényes volt az aláírás létrehozásakor.

- Az elektronikus aláírásról szóló törvény alapján a kijelölt tanúsító szervezetek minősítik az aláírás létrehozó eszközöket.

Az alábbiakban az első és az utolsó biztonsággal foglalkozunk.

AZ RSA ÁLTAL NYÚJTOTT BIZTONSÁG

Az RSA Laboratories rendszeresen hirdeti meg nagy számok faktorizálási versenyét (RSA Factoring Challenge). Az alábbi táblázat a verseny aktuális állását mutatja:

Challenge Number	Prize ($US)	Status	Submission Date	Submitter(s)
RSA-576	$10,000	Factored	December 3, 2003	J. Franke et al.
RSA-640	$20,000	Not Factored		
RSA-704	$30,000	Not Factored		
RSA-768	$50,000	Not Factored		
RSA-896	$75,000	Not Factored		
RSA-1024	$100,000	Not Factored		
RSA-1536	$150,000	Not Factored		
RSA-2048	$200,000	Not Factored		

Az RSA Laboratories szerint a mai nap ismert – RSA feltörésére szolgáló - algoritmusok az alábbi erőforrásigénnyel rendelkeznek, ha feltételezzük, hogy a faktorizálást egy év alatt kell elvégezni:

Number Length (bits)	**Machines**	**Memory**
430	1	trivial
760	215,000	4 Gb
1020	342,000,000	170 Gb
1620	1.6×10^{15}	120 Tb

A 2004-es év elején sorra jelentek meg az olyan, nagyon gyorsan terjedő féregvírusok, melyek képesek arra, hogy a támadónak hátsóajtót nyissanak. Az ilyen vírusok esetén egy támadó kezében rendkívüli számítási kapacitás összpontosulhat, amely minden eddiginél számításigényesebb feladatok elvégzésére is használható.
E cikk írásáig a MyDoom-nak nyolc, a Netsky féregnek hat változata került az internetre és a Beagle is tíz variánssal büszkélkedhet, pedig mindegyik vírus idén bukkant fel először. Ezen vírusok által fertőzött számítógépek száma – óvatos becslések szerint is – milliókban, tízmilliókban mérhető. Ez nagy kihívás a vírusvédelemmel foglalkozó gyártóknak is, hiszen nekik egyre gyorsabban kell kifejleszteniük, tesztelniük majd eljuttatniuk a felhasználókhoz a legújabb fenyegetésektől megvédő ellenszert.

A BellResearch elektronikus biztonsági tanulmánya szerint az internet-hozzáféréssel rendelkező hazai vállalatok kétharmada a vezetők saját bevallása szerint sem készült fel kellőképp a világháló felől érkező veszélyekkel szemben, és minden harmadik cég rendszere nyitva áll a vírusok és a behatolási kísérletek előtt.

AZ ALÁÍRÁS LÉTREHOZÓ ESZKÖZÖK BIZTONSÁGA

Vizsgáljuk meg, hogy milyen lehetőségei vannak egy támadónak, hogy az aláírás létrehozó eszköz manipulálásával végezze el a támadást:

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.
4. Egy újonnan készített vagy régebbi vírus segítségével hatol be az áldozat számítógépébe.

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, mint ahogy azt egyes vírusok meg is teszik. Ezt követően a laikus felhasználó hiába bizonyítaná igazát az elektronikus aláírás a törvény szerint a bíróság előtt bizonyító erejű…

ÖSSZEFOGLALÁS

A cikk az elektronikus aláírás két biztonsági kérdésével foglalkozott. Megállapíthatjuk, hogy az újonnan megjelent féregvírusok tapasztalatai tovább fokozzák az elektronikus aláírás fenyegetettségét. Az egyedüli megoldás – különösen a kritikus rendszerek esetén – a komplex vírusvédelmi és tűzfalrendszerek használata. Emellett a rendszer üzemeltetőjének fel kell mérnie az egyes szoftverelemek használatának kockázatát is.

FELHASZNÁLT IRODALOM

1. 2001. évi XXXV. törvény az elektronikus aláírásról
2. Virasztó Tamás: Kriptográfia és szteganográfia – avagy rövid bevezetés a rejtjelezés és az adatrejtés világába; www.wacher.hu; 2001.
3. Ködmön József: Kriptográfia; Computerbooks Kft.; 1999.
4. F. Ható Katalin: Adatbiztonság, adatvédelem; SZÁMALK Kiadó; 2000.
5. Denis Zenkin (Kaspersky Labs): The Invulnerable Penguin; SC Magazine; West Coast Publishing
6. SaveAs Kft.: Esettanulmány egy felfedezett poloska programról; www.saveas.hu; 1999.
7. www.index.hu/tech/biztonság
8. www.virushirado.hu
9. www.rsasecurity.com/rsalabs/challenges/