Hardver és Szoftver Biztonság II

Berta István Zsolt – Dr. Berta István

Összefoglalás – A villamos energia ellátás megbízhatósága, a szolgáltatott energia minősége a hagyományos elektrotechnikai feltételek mellett ma már döntő mértékben függ az informatikai biztonság kérdéseitől is. Az árampiac kiépítésének és működtetésének alapfeltétele, hogy (más elektronikus kereskedelmi formákhoz hasonlóan) a felek közötti kommunikáció biztonságos legyen. A nyilvános kulcsú infrastruktúra lehetőséget biztosít partnerek titkos és hiteles kommunikációjára. A szerzők célja, hogy megmutassák az elektrotechnika és a kriptográfia – két látszólag egymástól távol eső szakterület – összefonódását, együttes, egymást kölcsönösen segítő megjelenését. A cikk második része összefoglalja a BME-n e témákban folyó kutató munka néhány legújabb eredményét.

Kulcsszavak: digitális aláírás, kriptográfia, nyilvános kulcsú infrastruktúra, titkosítás, hitelesítés.

1. BEVEZETÉS

Cikkünk előző részében bevezettük a nyilvános kulcsú titkosítás fogalmát. Nyilvános kulcsú rendszerben minden szereplőnek két kulcsa van: titkos kulcsa, amelyet titkokban tart és nyilvános kulcsa, amelyet nyilvánosságra hoz. Amit a nyilvános kulccsal kódolunk, azt csakis a hozzá tartozó titkos kulcs segítségével lehet visszafejteni. Ha a titkos kulccsal kódolunk egy üzenetet, azt nem lesz titkos, viszont hiteles lesz. A nyilvános kulcshoz bárki hozzáfér, segítségével visszafejtheti az üzenetet, és megállapíthatja, hogy az üzenetet a titkos kulcs segítségével kódolták. Nyilvános kulcsú rendszerben a titkos kulcs segítségével való hitelesítést nevezzük digitális aláírásnak.

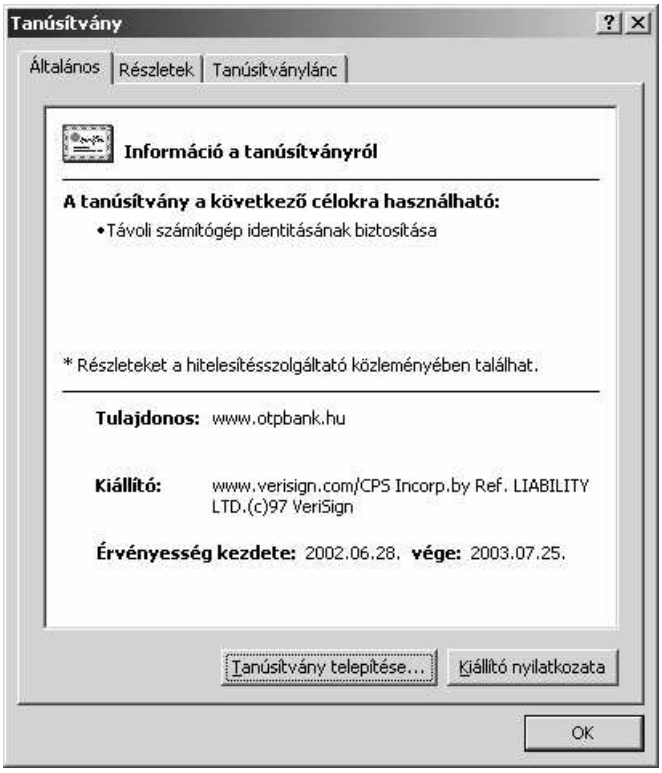
2. NYILVÁNOS KULCSÚ INFRASTRUKTÚRA (PKI)

A PKI-ról általában

Nyilvános kulcsú rendszerben létfontosságú, hogy a titkos kulcsot a tulajdonosán kívül senki ne ismerhesse. Ha ugyanis a titkos kulcs kiszivárog (kompromittálódik), segítségével bárki képes a tulajdonosa nevében digitálisan aláírni, és ezzel a rendszer alkalmatlanná válik a hitelesítésre. Épp ennyire fontos, hogy az *A* felhasználó nyilvános kulcsát mindenki megismerhesse, méghozzá hitelesen. Ha *C* sikeresen elhiteti *A*-val, hogy *B* nyilvános kulcsa nem k_B^{pub}, hanem k_C^{pub}, akkor *C* képes lesz elolvasni *A* *B*-nek szóló "titkosított" (a k_C^{pub} kulccsal rejtjelezett) üzeneteit. Sőt, a fenti esetben, ha *C* a saját k_C^{sec} titkos kulcsával ír alá egy üzenetet, arról *A* azt fogja hinni, hogy azt *B* írta alá.

A kulcsok generálására és felhasználókhoz való hozzárendelésére, valamint a nyilvános kulcsok hiteles közzétételére és a titkos kulcsok biztonságos őrzésére szolgáló rendszert nevezzük nyilvános kulcsú infrastruktúrának (public key infrastructure - PKI).

Tanúsítványok

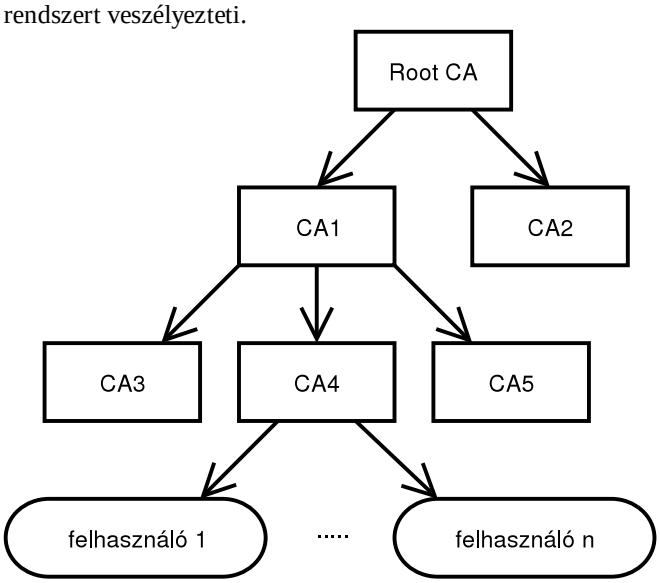


1. ábra. Tanúsítvány

Tegyük fel, hogy *A* és *B* nem ismerik egymást, de üzletet szeretnének kötni egymással. Amíg *A* és *B* nem ismerik egymás nyilvános kulcsát, nem képesek egymással hitelesen kommunikálni, ugyanis enélkül nem lehetséges a másik digitális aláírásának ellenőrzése. Mindketten ismerik viszont *T*-t, és *T* nyilvános kulcsát. Ha *T* digitálisan aláírva elküldi *A*-nak *B* nyilvános kulcsát ($T \rightarrow A$: $D(k_T^{sec}, k_B^{pub})$), és *B*-nek *A* nyilvános kulcsát, ($T \rightarrow B$: $D(k_T^{sec}, k_A^{pub})$), akkor mindketten birtokában lesznek a másik nyilvános kulcsának. Az ehhez hasonló "igazolást", amelyet megbízható harmadik fél állít ki, nevezik tanúsítványnak (certificate), a megbízható harmadik felet pedig tanúsító szervezetnek (CA - certification authority). A gyakorlatban a tanúsítvány (1. ábra) nemcsak a nyilvános kulcsot tartalmazza, hanem többek közt tulajdonosának, valamint a kiállító CA-nak a nevét és egy lejárati határidőt is. Minden felhasználó, kap a CA-tól egy tanúsítványt, amellyel igazolhatja saját nyilvános kulcsát. Ha nyilvánosságra hozza a tanúsítványát, amelyet a CA aláírása hitelesít, mindenki küldhet neki titkos üzeneteket, és

mindenki képes fogadni és ellenőrizni az ő digitálisan aláírt üzeneteit.

A gyakorlatban a helyzet persze nem ilyen egyszerű. Komoly probléma például, hogy sok CA van a világon, és nem biztos, hogy *A* és *B* ugyanahhoz a CA-hoz tartozik. Így lehetséges, hogy *A* hiába rendelkezik *B* tanúsítványával (amely igazolja CA_1 aláírásával, hogy *B* nyilvános kulcsa k_B^{pub}), mert *A* nem ismeri CA_1 nyilvános kulcsát, így nem képes ellenőrizni *B* tanúsítványát. A probléma egyik megoldása, hogy a CA-k fastruktúrába szerveződnek, és a fa felsőbb szintjén lévő CA-k tanúsítványokat adnak ki az alájuk tartozó CA-k számára. (2. ábra) E fát visszafejtve található olyan CA, amely alá mind *A*, mind *B* tartozik. Különösen kritikus helyzetben van a fa gyökerében lévő CA (ún. Root CA) kulcsa, hiszen ennek kompromittálódása az egész rendszert veszélyezteti.



2. ábra. A CA-k fastruktúrába szerveződnek

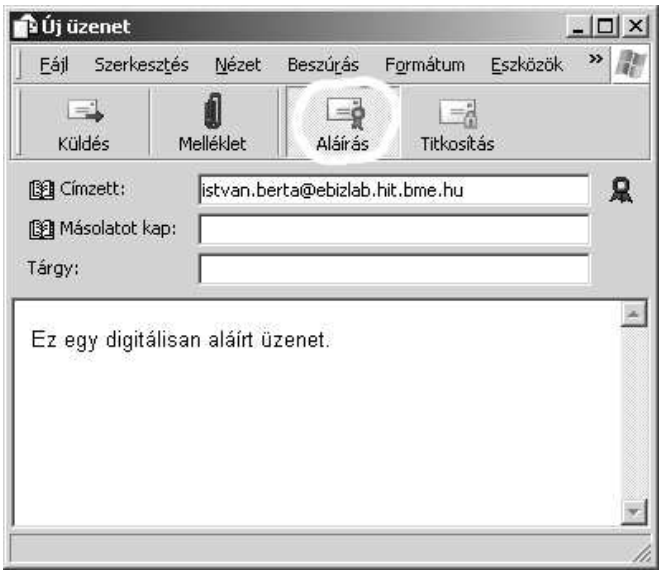
Szintén probléma annak a szabályozása, hogy mi történik akkor, ha *A* titkos kulcsát ellopják. Ha *A* észreveszi a lopást, jelentenie kell azt a CA-nál, amely *A* nyilvános kulcsát hitelesítette. A CA ekkor ún. visszavonási listára (CRL – certificate revocation list) teszi a tanúsítványt. Mielőtt *A* nyilvános kulcsát használjuk, ellenőriznünk kell, hogy *A* tanúsítványa érvényes-e, nem szerepel-e a visszavonási listán. Sőt, a láncban érintett minden CA visszavonási listáját ellenőriznünk kell, így egy tanúsítvány ellenőrzése igen komplex feladattá válhat. Lényeges, hogy az általunk használt PKI szoftver valóban elvégzi-e az összes ellenőrzést, amely a tanúsítvány elfogadásához szükséges.

Chipkártyák

Míg a tanúsítványok arra szolgálnak, hogy nyilvános kulcsunk hitelesen jusson el partnerünkhöz, a chipkártyák – többek közt – abban nyújtanak segítséget, hogy a titkos kulcsunk valóban titokban maradjon. A chipkártyák bankkártya méretű műanyag kártyák, melyeken mikrochip helyezkedik el (3 ábra).

3. ábra. Chipkártya

Ez a chip csakis akkor enged hozzáférést a benne tárolt adatokhoz, ha megfelelően azonosította a felhasználót. A kártyán az adatok file-ba, a file-ok pedig filerendszerbe szerveződnek, ahol minden file-hoz definiálhatjuk, az egyes felhasználók milyen jelszó vagy titkos kulcs birtokában férhessenek hozzá [12], [14]. A kártyákat úgy alakítják ki, hogy a chip tartalmához semmilyen más módszerrel, még a kártya szétszerelésével, felboncolásával se lehessen hozzáférni. (tamper resistance) A modern chipkártyák már biztonságos mikroszámítógépek. Azon túl, hogy tárolják a kriptográfiai kulcsokat, képesek velük kódolni is. Megoldható, hogy a titkos kulcsot tároló kártya senkinek, még a kártya birtokosának sem adja ki a kulcsot. Ugyanakkor, aki a kártyabirtokos jelszavát ismeri, az utasíthatja a kártyát, hogy kódoljon a titkos kulccsal. Így használhatjuk a kulcsot anélkül, hogy az egy pillanatra is elhagyná a biztonságos chipkártyát. Egyes kártyák képesek kulcsokat generálni is, így a kulcs teljes életciklusa (generálás, tárolás, használat, megsemmisülés) a kártyán zajlik le. Tipikus eset, hogy a felhasználó chipkártyán kapja meg a kulcspárját (nyilvános és titkos kulcsát) a CA-tól.



4. ábra. Digitális aláírás Microsoft Outlook segítségével

Ha a felhasználó használni szeretné a titkos kulcsát, be kell helyeznie a kártyáját a számítógépéhez csatlakoztatott kártyaolvasóba. Miután megírta az üzenetét, levelező-programjában rákattint az aláírás gombra (4. ábra). A felhasználó azonosítását követően, a számítógép elküldi a

kártyának az üzenetet, az pedig – a titkos kulcs segítségével – előállítja a felhasználó digitális aláírását. Mivel a titkos kulcs soha nem hagyja el a kártyát, a felhasználó nevében digitálisan aláírni a kártya (és annak jelszava, PIN kódja) nélkül nem lehet [4], [5].

Kitekintés

Magyarországon a digitális aláírás hitelességét a törvény is elismeri. A 2001. évi XXXV. törvény vonatkozik digitális aláírásokra. A törvény három különböző digitális aláírást különböztet meg: egyszerű digitális aláírást, fokozott biztonságú digitális aláírást és minősített digitális aláírást. Ezek közül egyszerű digitális aláírás (ilyen például, ha a felhasználó a nevét odaírja az emailje végére) kriptográfiai szempontból nem hitelesítés (az *A* felhasználó nevét elvileg bári odaírhatta), e cikk digitális aláírásnak a fokozott biztonságú, illetve a minősített digitális aláírást nevezi. E kettő között elsősorban az jelent különbséget, hogy a rendszerben szereplő szolgáltatók és eszközök (CA, chipkártya stb.) milyen biztonsági minősítéseken estek át. A digitális aláírásról szóló törvény, valamint a magyar – fokozott biztonságú és minősített – CA-k listája megtalálható a Hírközlési Főfelügyelet honlapján (http://www.hif.hu).

A nyilvános kulcsú rendszerek matematikai, kriptográfiai alapjai rendelkezésre állnak; több erős nyilvános kulcsú kriptográfiai algoritmus ismert. Ugyanakkor, a PKI szabványok nem kellőképpen egységesek, valamint a különböző cégek termékei (PKI implementációi) egyelőre nem képesek zökkenőmentes együttműködésre. Így, míg egyes cégek rendelkeznek PKI rendszerrel, egyelőre közel sem beszélhetünk az egész világot átfogó, egységes infrastruktúráról.

3. KUTATÁSOK A BME-N

A következőkben a szerzők által a BME laboratóriumaiban művelt néhány főbb kapcsolódó kutatási területről számolunk be, a teljesség igénye nélkül.

A chipkártyán futó alkalmazás helyessége

A kártyák biztonságos mikroszámítógépek. Azt szeretnénk, ha érzékeny adatainkat, kulcsainkat ők védenék. Ugyanakkor, mivel számítógépek, a rajtuk futó szoftverek alig különböznek a PC-n futó szoftverektől, így a hibás programok PC-n előforduló problémái (pl.: "lefagyás") elvileg chipkártyán is előfordulhatnak.

Sajnos, éppen a chipkártya védelmi rendszerei miatt, a kártyán futó szoftver működésébe sokkal kevesebb lehetőség van később beavatkozni, ráadásul az adatok érzékenysége (például banki adataink) miatt a keletkező károk is jelentősek lehetnek. Ezért létfontosságú, hogy a kártyán futó alkalmazás pontosan szándékaink szerint működjön, vagyis szeretnénk megbizonyosodni arról, hogy tervezése vagy megvalósítása közben nem történt hiba. Szintén érdekes dolog annak ellenőrzése, hogy az alkalmazás fejlesztője nem csempészett-e be olyan kiskaput, melyet kihasználva később megkárosíthat bennünket.

A szoftverhelyesség-bizonyítás olyan tudományág, amely számos módszert kínál, a fentiek ellenőrzésére. Ezt nemcsak teszteléssel végezhetjük el, hanem matematikai eszközökkel is bizonyíthatjuk, hogy egy alkalmazás megfelel bizonyos terveknek, specifikációknak. A chipkártyákon futó alkalmazások elég kicsik, külvilággal való kapcsolatuk pedig elég jól definiált ahhoz, hogy ezen formális módszereket esetükben alkalmazhassuk [13].

Appletek interakciója

Gyakori, hogy egy kártyán nem csak egy, hanem több alkalmazás van. Sőt, a modernebb kártyák arra is lehetőséget biztosítanak, hogy a kártya élete során újabb alkalmazásokat telepíthessünk. Egy biztonságos kártya megtervezése akkor is nagy kihívást jelent, ha ezen alkalmazásokat elkülönítjük egymástól, de a piac egyre nagyobb igényt mutat arra, hogy különböző cégek alkalmazásai egymással együtt-működhessenek. Jó példa erre az, amikor több cég közös kártyát bocsájt ki, melyen vásárlóik hűségpontokat gyűjthetnek. A cégek kölcsönösen elismerhetik egymás hűségpontjait, így például a benzinkút-hálózattól kapott pontokat a vásárló beválthatja egy áruházban vagy egy gyorsétteremben is. Ma több ilyen rendszer is működik Magyarországon.

Egyazon kártyán több – akár egymással ellenérdekelt – fél alkalmazásai futhatnak. Ilyenkor a tervező feladata annak biztosítása, hogy ezen felek együttműködhessenek, viszont illetéktelenül ne férhessenek hozzá egymás érzékeny adataihoz, és a felhasználó személyiségi jogai se sérüljenek. A modern chipkártya-szabványok (pl.: Visa Open Platform, Java Card) számos eszközt kínálnak e kettősség feloldására. Ugyanakkor, a helytelen tervezés még az erős biztonsági megoldásokat is romba döntheti.

Chipkártyák EMC problémái

Sajátságos problémát jelentenek a villamos, mágneses és elektromágneses erőterek okozta – természetes vagy mesterséges eredetű, véletlen vagy szándékos – zavarok (EMC = ElectroMagnetic Compatibility), illetve működési bizonytalanságok. Ezek a hatások esetenként roncsolhatják a chipkártyákat, de befolyásolhatják a működésüket, megváltoztathatják a tárolt adatokat, programokat. Ilyen módon az EMC a biztonság egyik alapvető kérdésévé lépett elő. A kisfrekvenciás mágneses erőterek, a közeli villámcsapások okozta vezetett, vagy indukált túlfeszültségek, az elektrosztatikus szikrák és a nagyfrekvenciás zavarok elleni védekezés a BME több tanszékének közös kutatási területe [3], [10].

Nem biztonságos terminálok

Ha titkos kulcsunkat chipkártyán tároljuk, megvédhetjük attól, hogy illetéktelenek kezébe jusson, miközben kódolunk vele. A chipkártyák – mivel nem rendelkeznek saját felhasználói felülettel – a felhasználóval csak egy ún.

terminálon keresztül képesek kommunikálni. A terminál lehet számítógép, bankautomata, de akár mobiltelefon is. Sajnos, ha a terminál nem biztonságos (például, mert vírusos lett, vagy egy támadó manipulálta), képes lehet megkerülni a chipkártya által nyújtott védelmet.

Tegyük fel, hogy kártyánkat digitális aláírásra akarjuk használni egy rosszindulatú terminálon! A terminálba begépeljük az üzenetet, az továbbküldi chipkártyánknak, a kártyánk pedig digitális aláírással látja el. A digitálisan aláírt dokumentum már letagadhatatlan, tartalmáért jogilag felelősek vagyunk. Csakhogy, ha a terminál rosszindulatú, lehet, hogy nem a tőlünk származó üzenetet küldi el a chipkártyának, hanem valami olyasmit, amit mi egyáltalán nem szándékozunk aláírni. Hiába használunk erős digitális aláírást, ha nem tudjuk befolyásolni, mit írunk alá. Hiába azonosít a chipkártya bennünket (PIN kód, jelszó vagy akár ujjlenyomatunk alapján), mindez nem garantálja, hogy a támadó az üzenet tartalmát nem változtatja meg.

A chipkártyák használata nem biztonságos terminálokon erősen ingoványos terület, komoly gondot jelent, hogy ez esetben nincsen biztonságos csatorna a felhasználó és a kártyája között. Sajnos igen sok terminált sorolhatunk a "nem biztonságos" kategóriába. Ha bankkártyánkat ismeretlen automatánál akarjuk használni, nehéz megállapítani, hogy azt valóban a bank tette-e oda, vagy pedig egy támadó szeretné ellopni a PIN kódunkat. Ha Internet-kávézóból csatlakozunk a hálózatra, nem tudhatjuk, hogy nem manipulált szoftverek futnak-e az idegen gépen, emellett komoly veszélyforrást jelent, ha a terminálon marad (például a böngészőprogram gyorsítótárában) valamely érzékeny információnk. Otthoni számítógépünkben sem bízhatunk meg feltétel nélkül, hiszen ha behatolt rá egy vírus, az könnyűszerrel manipulálhatja a chipkártya felé küldött adatainkat. A nem biztonságos terminálok egyik legfőbb problémája az, hogy rájuk vagyunk utalva.

A világon számos helyen ([1], [2], [8]) – így a budapesti Műegyetemen ([6], [7]) is – kutatják a nem biztonságos terminálok biztonságos használatának lehetőségeit. Egy lehetséges irány, hogy a felhasználó maga végezze el a hitelesítést úgy, hogy a terminál ne legyen képes azt manipulálni. Ha nem áll rendelkezésére megbízható számító eszköz, ez a feladat nagyon nehéz. Ugyanakkor, lehetőség van a felhasználó biometriai azonosítására (pl. ujjlenyomat- vagy hangazonosítás). Másik lehetőség, hogy a chipkártyát látjuk el olyan perifériákkal (például nyomógombokkal vagy LED-del), hogy képes legyen közvetlen kommunikációra a felhasználóval. Ez a megoldás biztonsági szempontból jelentős előrelépés lenne, ugyanakkor megnövelné a kártyák költségét.

4. Összefoglalás

A jövőben a BME-n folyó kutatásokat két fő területen erősítjük. Egyrészt tovább vizsgáljuk a nem biztonságos terminálok elméletének kérdéseit, másrészt laboratóriumi mérésekkel határozzuk meg a chipkártyák és a hozzájuk kapcsolódó eszközöknek és berendezéseknek a villamos, mágneses és elektromágneses erőterekre való érzékenységét. A szokásos szabványos EMC vizsgálatok mellett speciális biztonsági mérések kidolgozását tervezzük.

5. IRODALOMJEGYZÉK

[1] Abadi, M. – Burrows, M. – Kaufman, C. – Lampson, B.: Authentication and Delegation with Smart-card, Proc. of TACS'91, Springer, 1992.

[2] Asokan, N. – Debar, H. – Steiner, M. – Waidner, M.: Authenticating Public Terminals, Computer Networks, 1999.

[3] Balog E. – Berta I.: Fuzzy Solutions in Electrostatics, Journal of Electrostatics 51 & 52 (2001), pp 409-415.

[4] Berta I. Zs. – Mann Z. Á: Smart Cards – Present and Future, Híradástechnika, Journal on C^5, 2000/12.

[5] Berta I. Zs. – Mann Z. Á: Programozható chipkártyák – elmélet és gyakorlati tapasztalatok, Magyar Távközlés, 2000/4.

[6] Berta I. Zs – Vajda, I.: Documents from malicious terminals, SPIE Microtechnologies for the New Millenium 2003, Bioengineered and Bioinspired Systems, Maspalomas, 2003.

[7] Berta I. Zs. – Vajda, I.: Limitations of Humans when using Malicious Terminals, TATRACRYPT'03, 2003.

[8] Clarke, D. – Gassend, B. – Kotwal, T. – Burnside, M. – van Dijk, M. Devadas, S – Rivest, R.: The Untrusted Computer Problem and Camera-Based Authentication, 2002.

[9] Ellison, C. – Schneier, B.: Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure

[10] Horváth T. – Berta I.: Level and expected frequency of LEMP caused by near and far lightning strokes, 26th International Conference on Lightning Protection, Proc. of ICLP 2002, pp. 574-578

[11] Schneier, B.: Applied Cryptography, John Wiley & Sons, 1996.

[12] Rankl, W. – Effing, W.: Smart Card Handbook, John Wiley & Sons, 1997.

[13] Verok I.: Formális módszerek a JavaCard alkalmazások biztonsági tulajdonságainak formális verifikációja, HTE-BME 2002 Korszerű távközlési és informatikai rendszerek és hálózatok konferencia, Budapest, 2002.

[14] Zoreda, J. L. – Oton, J. M.: Smart Cards, Artech House, 1994.

6. ÉLETRAJZ

Berta István Zsolt Debrecenben, 1978-ban született. 2001-ben diplomázott mérnök-informatikusként a BME Híradástechnikai Tanszékén. Jelenleg doktorandusz a BME Híradástechnikai Tanszékén, a CrySyS Adatbiztonság Laboratóriumban. Kutatási területe a chipkártyák (smart card) biztonsága, ezen belül a chipkártyák használatának veszélyei nem biztonságos terminálon.

e-mail: istvan.berta@crysys.hit.bme.hu

Dr. Berta István Debrecenben, 1949-ben született. Okleveles villamosmérnök, a műszaki tudomány doktora, Dr. Habil. A BME egyetemi tanára, Gábor Dénes díjas. Szakterülete az ipari elektrosztatika, EMC, elektromágneses környezetvédelem, villám-, túlfeszültség- és zavarvédelem. A MEE elnöke, a MTESZ alelnöke. e-mail: berta@ntb.bme.hu