Hardver és szoftver biztonság I.

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, titkosítás, hitelesítés.

1. Bevezetés

A villamos energia termelése, szállítása, elosztása és felhasználása területén az elmúlt években soha nem látott fejlődésnek lehettünk tanúi. Ez a változás az elektrotechnika eszközeinek, berendezéseinek és rendszereinek fejlődését jelentette. Ugyanakkor az informatika és a telekommunikáció (telematika) robbanásszerű előretörése, a legkülönbözőbb területeken való elterjedése, és alapvető fontossága miatt a villamos energetika is döntően megváltozott. A minőségi és biztonságos energiaszolgáltatás a hagyományos erősáramú problémák korszerű megoldása mellett az informatikai biztonsági feladatok megoldásán is múlik. Ma már sok esetben a hardver, illetve a szoftver biztonság nem választható el egymástól, hiszen a csúcstechnológiát képviselő rendszereinkben (a korszerű energetikai rendszerek egyértelműen ide tartoznak!) az sem mindig dönthető el, hogy egy adott feladatot a hardver, vagy a szoftver oldja meg. Cikkünk célja az új típusú gondolkodásnak, az egymástól látszólag távol eső szakmai területek összefonódásának bemutatása.

2. Biztonság

A biztonság szónak a különböző területeken más és más jelentése lehet. Érthetünk alatta biztonságos működést, a villamosság biztonságtechnikáját, baleset- vagy betörésvédelmet, villám-, túlfeszültség- vagy zavarvédelmet, de akár rejtjelezést vagy adatvédelmet is. Számos veszély leselkedik ránk, készülékeinkre, berendezéseinkre és rendszereinkre, de adatainkra is, ezek mindegyike bizonyos kockázatot jelent. Minden biztonsági szemlélet egyfajta tudatos szembeállást jelent ezen kockázatokkal, illetve eszközöket kínál ezek – a rendszer tervezője által megadott feltételrendszer (támadás jellege, támadó célja, támadó ismeretei) szerinti – mérséklésére. Tökéletes biztonság a gyakorlatban nincsen, legfeljebb arról beszélhetünk, hogy a kockázat elég kicsi.

Minden biztonsági rendszer valamely érték védelmére irányul. Attól félünk, hogy értékünk megsemmisül, vagy illetéktelen személy megszerzi azt. Felmerül a kérdés, mennyit érdemes értékeink védelmére fordítanunk? Össze kell vetnünk a védelem költségeit a kár várható értékével. Egyetlen káresemény értékének, a káresemények gyakoriságának, valamint az adott készülék vagy berendezés várható élettartamának ismeretében becsülni tudjuk a kár várható értékét. Ezt kell összehasonlítanunk a védelem kiépítésének azonnali biztos költségével és a védelem fenntartásának az adott időtartamra számított folyamatos biztos költségével. A gazdasági számítások elvégzésénél természetesen figyelembe kell vennünk, hogy az egyes költségek eltérő időpontokban jelentkeznek (diszkontálás). Amennyiben szándékos támadás, emberi rosszindulat ellen védekezünk, meg kell becsülnünk, mennyit ér a támadónak értékünk megszerzése vagy megsemmisítése. Akkor mondhatunk egy rendszert biztonságosnak, ha a megtámadásához szükséges erőforrások költsége meghaladja a rendszert támadónál bekövetkező nyereséget.

Megkülönböztethetünk fizikai és logikai biztonságot, mindkettőnek léteznek műszaki, jogi és szabályzati vonatkozásai. Cikkünkben adatbiztonsággal, logikai biztonsággal foglalkozunk, különös tekintettel annak műszaki, informatikai kérdéseire. Az adatbiztonság célja az adatok védelme. Adatokban három szempontból keletkezhet kár:

- **Elérhetőség** (availability): Akkor sérül az adatok elérhetősége, ha az illetékes felhasználók nem férnek hozzá a munkájukhoz szükséges adatokhoz.
- **Bizalmasság** (confidentiality): Akkor sérül az adatok bizalmassága, ha azokat illetéktelenek megszerzik vagy lemásolják.
- **Sértetlenség** (integrity): Akkor sérül az adatok integritása, ha azok hiba vagy emberi rosszindulat következtében törlődnek vagy módosulnak.

Míg az adatok elérhetősége a rendszer megbízható működését jelenti, a bizalmasságuk és sértetlenségük garantálása inkább a rendszer működésének bizonyos korlátozását jelenti rosszindulatú támadások kivédése céljából. Cikkünkben elsősorban ez utóbbi két szempont

kérdéskörét tárgyaljuk üzenetek titkossága illetve hitelessége kapcsán.

3. TITKOSSÁG ÉS HITELESSÉG

Egy üzenetet a feladója akkor tekinthet titkosnak (bizalmasnak), ha biztos abban, hogy azt a vevőn (címzetten) kívül más nem olvashatja el. Ennek elérésére alkalmazhatunk fizikai és logikai megoldásokat. Fizikai megoldás például, ha az üzenetet megbízható futár szállítja lezárt táskában, vagy ha azt védett csatornán továbbítjuk, amelyet illetéktelenek nem képesek lehallgatni. Tipikus logikai megoldás, ha az üzenetet rejtjelezve továbbítjuk. Egy üzenetet vevője akkor tekinthet hitelesnek, ha az üzenet sértetlen és a feladó azonosítható, azaz a vevő biztos abban, hogy azt valóban annak feladója küldte, és hogy az üzenetet útközben senki nem módosította. Klasszikus fizikai módszerek a hitelesség biztosítására a pecsét vagy az aláírás. E két eszköz az adathordozót (esetünkben a papírt) jelöli meg egyedi – az üzenet feladójára jellemző – módon. Feltételezzük továbbá, hogy a pecsét vagy aláírás elválaszthatatlanok az adathordozótól – akárcsak maga az üzenet. A logikai hitelesítő módszerek (például a digitális aláírás) nem foglalkoznak az adathordozóval, hanem az üzenethez (mint adathoz) illesztenek olyan speciális blokkot, amelyet csakis a feladó képes előállítani az üzenet, és valamilyen titkos információ alapján.

A titkosság és a hitelesség az adatbiztonság két alapvető fogalma, célunk gyakran ezek egyikének vagy akár mindkettőnek a megvalósítása. Előfordulhat, hogy ennél többet, vagy kevesebbet szeretnénk elérni. Ha egy üzenet letagadhatatlan, vevője megbizonyosodhat arról, hogy az valóban a rajta feltüntetett feladótól jött, és valóban a feladó által küldött információt tartalmazza. Mindemellett a vevő igazolni is képes ezt harmadik fél (pl. bíróság) előtt. Elektronikus szerződések esetén a letagadhatatlanság elengedhetetlen feltétel. Előfordul, hogy célunk éppen ennek ellenkezője. A feladóra nemcsak, hogy ne lehessen rábizonyítani az üzenet elküldését, de meg se lehessen állapítani, hogy ki a feladó. A felhasználók anonimitása és személyiségi adatainak védelme az elektronikus társadalom egyik legfontosabb és legösszetettebb kérése. Míg egy betörés esetén szeretnénk kideríteni, hogy ki volt a tettes, nem szeretnénk, hogy elektronikus kereskedők a beleegyezésünk nélkül nyilvántarthassák, ki mit vásárolt náluk. Másik példa, ahol az anonimitás létfontosságú, az elektronikus szavazások esete.

Az irodalomban számos, a fentiekhez hasonló követelmény ismert [7]. Cikkünk további részében elsősorban a titkosságról és hitelességről, valamint azok kriptográfiai (a titkosítással foglalkozó tudomány szerinti) megvalósításáról lesz szó.

3.1 Kriptográfiai kulcs fogalma

A feladó (*A*) üzenetet kíván küldeni a vevőnek (*B*). Mivel az *x* üzenet érzékeny információt tartalmaz, védeni kell azt a támadó (*C*) ellen. A védelem esetünkben kriptográfiai kódolást jelent, amely titokra kell, hogy épüljön. Mivel ezt a titkot gyakran cserélni kell, nem jó, ha maga a kódolási módszer (algoritmus) a titok. Egyrészt kevés „erős” kódoló algoritmust ismerünk, másrészt igen nehéz annak megállapítása, hogy egy kódoló algoritmus mekkora biztonságot nyújt. A tapasztalat azt mutatja, hogy a nyilvánosságra nem hozott, tudományos fórumokon meg nem vitatott módszerek sorra megbuknak. A kriptográfiában az a bevett gyakorlat, hogy a kódoló algoritmus minden részlete publikált és nyilvános, egyedül annak egy paramétere, az ún. kulcs a titkos. (Ez az ún. Kerckhoff feltétel. [5]) Egy jó algoritmus ilyen feltétel mellett is képes megfelelő védelmet nyújtani, ezért szegénységi bizonyítványt jelent, ha egy algoritmust a tervezője nem mer nyilvánosságra hozni.

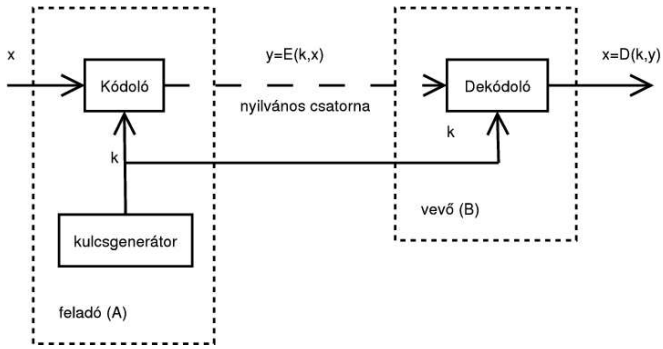
A kulcs általában kicsi és rövid, így könnyű generálni vagy a hálózaton továbbítani. Lényeges, hogy a kulcs kellően nagy kulcstérből kerüljön ki, különben a támadó könnyen megfejtheti az üzeneteket az összes lehetséges kulcs végigpróbálgatásával. Az is fontos, hogy a kulcsot véletlenszerűen válasszuk ki a kulcstérből, különben a támadó (ismerve kulcsválasztásunk elvét) kitalálhatná a kulcsot. Célunk az, hogy a támadót olyan helyzetbe hozzuk, hogy kénytelen legyen az összes lehetséges kulcsot végigpróbálni. Ha a kulcstér elegendően nagy, ez a feladat reménytelen. Például, *128* bit hosszú véletlenül választott kulcs esetén a kulcstér kimerítő kereséssel való végignézése 2^{128}, vagyis több mint 10^{36} kulcs kipróbálását jelentené, ami a gyakorlatban kivitelezhetetlen. Minden rendszerben létfontosságú a kulcsgondozás, vagyis a kulcsok generálásának, továbbításának és tárolásának módszere.

Ábráinkon (1. ábra és 2. ábra) a szaggatott vonallal jelölt csatorna modellezi azt az utat, amelyen a kódolt üzenet eljut a feladótól a vevőhöz. Ez a csatorna nem biztonságos, az üzenet számos olyan berendezésen (telefonvonal, Internet, lokális hálózat) halad keresztül, melyet sem a feladó, sem pedig a vevő nem képes megvédeni. A cikkünkben használt, általánosan elfogadott modell szerint, a támadó csakis e nyilvános csatornán támadhatja (lehallgathatja, módosíthatja) az üzenetet, a biztonságos (az ábrákon folytonos vonallal jelölt) csatornákhoz nem fér hozzá.

3.2 Titkos kulcsú rendszerek

A hagyományos titkos kulcsú rendszereket szimmetrikus kulcsú rendszereknek is nevezik, hiszen a kódoláshoz és dekódoláshoz használt kulcs megegyezik, vagyis mindkét félnek (a feladónak és a vevőnek is) rendelkeznie kell a *k* kulccsal. (1. ábra) Létfontosságú, hogy *k* titokban maradjon,

hiszen ha a *C* támadó megtudná a *k* kulcsot, megfejthetné a *k*-val rejtjelezett üzeneteket. Jelölje $y=E(k,x)$ azt a rejtett üzenetet, amelyet *x* üzenet *k* kulccsal történő kódolásával (encryption) kapunk. Ennek megfelelően a dekódolás (decryption) jelölése: $x=D(k,y)$.

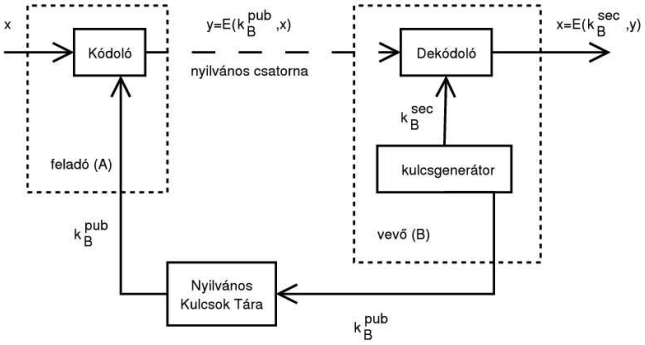


1. ábra. Titkos kulcsú rendszer

A *k* kulcsot jellemzően az egyik fél (vagy egy kulcsközpont) generálja, és biztonságos csatornán juttatja el a másik félnek. Ezt követően *A* és *B* képesek a *k* kulcs segítségével titkosan kommunikálni egymással. A titkos kulcsú rendszerek előnye, hogy igen gyors titkos kulcsú kódoló és dekódoló algoritmusokat ismerünk, valamint a *k* kulcs mérete kicsi lehet. (Ahogy a számítógépek sebessége növekszik, a támadó egyre nagyobb és nagyobb kulcsokat képes feltörni. Ma a legalább *128* bit hosszú kulcsokat már elég biztonságosnak tekintjük szimmetrikus kulcsú rendszerekben.) Ezen rendszerek legfőbb problémája, hogy a *k* kulcsnak – amelyet ábránkon *A* generál – biztonságosan kell eljutnia *B*-hez, hiszen *k* kiszivárgása végzetes lehet. Szimmetrikus kulcsú titkosítással csak akkor kommunikálhat *A* és *B*, ha előzőleg megállapodtak egy közös titkos kulcsban. Feloldást jelenthet e problémára egy kulcsszerver (*S*), amelyben mind *A*, mind *B* egyaránt megbízik, és már mindketten megállapodtak *S*-sel egy-egy közös k_{AS} illetve k_{BS} kulcsban. Ekkor *S* segítségével *A* és *B* megállapodhat egy közös titkos k_{AB} kulcsban. Híres titkos kulcsú rejtjelező algoritmusok például DES, 3DES, Blowfish, Idea, AES, [7], [2].

3.3 Nyilvános kulcsú rendszerek

A nyilvános kulcsú titkosítás (más néven aszimmetrikus kulcsú titkosítás) megoldja a szimmetrikus kulcsú rendszerek fő problémáját: *A* és *B* úgy képesek egymással titkosan és hitelesen kommunikálni, hogy nem rendelkeznek közös titokkal. A nyilvános kulcsú rendszerben minden szereplőnek két kulcsa van: egy titkos kulcsa és egy nyilvános kulcsa. (Így például A kulcsai: k_A^{sec} és k_A^{pub} lesznek.) Amit *A* nyilvános kulcsával kódolunk, azt *A* a titkos kulcsával dekódolhatja, és fordítva: amit *A* a titkos kulcsával kódol, azt mi *A* nyilvános kulcsával dekódolhatjuk (2. ábra). A titkos kulcsát minden szereplő titokban tartja, a nyilvános kulcsát viszont nyilvánosságra hozza, hogy mindenki hozzáférhessen. A nyilvános kulcsok közzétételéről ábránkon a Nyilvános Kulcsok Tára gondoskodik, ahonnan mindenki (akár a támadó is) hitelesen megkaphatja bárkinek a nyilvános kulcsát. Ha *A* üzenetet akar küldeni *B*-nek, elkéri *B* nyilvános kulcsát, majd ennek segítségével kódolja az *x* üzenetet. ($y=E(k_B^{pub},x)$) Az *y* üzenet így csak *B* titkos kulcsa segítségével dekódolható ($x=D(k_B^{sec},y)$). Ezt csupán *B* teheti meg, hiszen *B* titkos kulcsával csupán *B* rendelkezik.



2. ábra. Nyilvános kulcsú rendszer

A azt is megteheti, hogy nem *B* nyilvános kulcsával, hanem saját titkos kulcsával kódolja az üzenetét. Ekkor az $s=D(k_A^{sec},x)$ adat nem lesz titkos, hiszen ezt *A* nyilvános kulcsával bárki visszafejtheti: $x=E(k_A^{pub},s)$. Az viszont megállapítható az s üzenetről, hogy *A*-tól származik, hiszen *A* titkos kulcsa segítségével kódolták, az pedig csak *A* birtokában lehet. Egy üzenetet a címzett nyilvános kulcsa segítségével titkosíthatunk, a saját nyilvános kulcsunkkal kódolva pedig hitelesíthetünk. Amellett, hogy az *A* titkos kulcsával kódolt üzenet hiteles, letagadhatatlan is egyben, mivel a hitelesség ellenőrzése nem igényli a titkos kulcsot. *B* pusztán nyilvános információkra támaszkodva is képes bizonyítani, hogy az *s* üzenet valóban *A*-tól származik [7], [4].

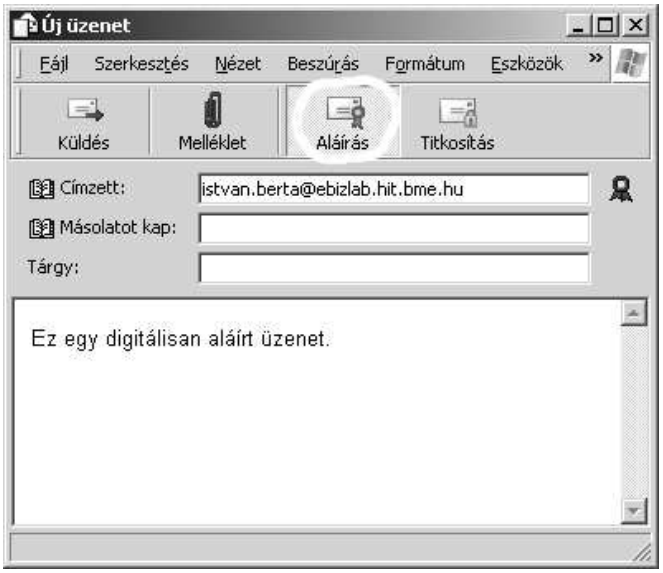
Üzenetet hitelesíteni lehet szimmetrikus kulcsú módszerekkel is. Ekkor a vevőnek rendelkeznie kell a titkos *k* kulccsal ahhoz, hogy ellenőrizhessen egy *k* kulccsal hitelesített üzenetet. Így azonban maga is képes a *k* kulccsal üzeneteket hitelesíteni. Tehát a vevő szimmetrikus kulcsú rendszerben nem bizonyíthatja harmadik fél számára, hogy ezt az üzenetet kapta a feladótól.

A nyilvános kulcsú rendszerek hátránya, hogy az ismert algoritmusok lassabbak, és csak hosszabb kulcsokkal nyújtanak azonos biztonságot, mint a titkos (szimmetrikus) kulcsúak. (Például, a kriptográfia mai állása szerint az RSA nyilvános kulcsú algoritmus csak *1024* vagy *2048* bit hosszú kulcsokkal tekinthető biztonságosnak.) A nyilvános kulcsú rendszerek előnye viszont, hogy segítségükkel két fél úgy is kommunikálhat egymással titkosan és hitelesen, hogy nem kell, hogy előtte találkozzanak, előzőleg nem állapodtak meg

egymással biztonságos körülmények között közös titkos kulcsban. Gyakori megoldás, hogy *A* és *B* nyilvános kulcsú algoritmussal állapodik meg egymással egy közös *k* kulcsban, és a későbbiekben titkos kulcsú algoritmussal kommunikálnak e *k* kulcs segítségével. Így működik például az SSH és az SSL protokoll [7].

A legismertebb, és a gyakorlatban legelterjedtebb nyilvános kulcsú algoritmus az RSA [6], de léteznek egyéb nyilvános kulcsú algoritmusok is (pl. ECC és NTRU), [1], [3], [4].

3.4 Digitális aláírás



3. ábra. Digitális aláírás Microsoft Outlook segítségével

A nyilvános kulcsú rendszer segítségével végzett hitelesítés - a digitális aláírás - kriptográfiai kódolás eredményeképpen jön létre úgy, hogy az üzenetet (gyakran annak csak egy tömörítvényét ún. hash leképezését [6]) a feladó kódolja a saját titkos kulcsával. Az x dokumentum aláírva az A felhasználó által *(x;s)*, ahol $s=D(k_A^{sec},hash(x))$. Az így kapott kódolt blokkot a feladó A (elküldés előtt még titkosíthatja, majd) továbbítja a *B* címzettnek, aki a feladó nyilvános kulcsa segítségével ellenőrizheti azt. Dekódolja az aláírást, majd megvizsgálja, hogy az így kapott eredmény megegyezik-e az *x* üzenettel. A digitális aláírás létrehozásához a felhasználónak egy bonyolult matematikai műveletet kell végrehajtani a titkos kulcsa és a kódolandó dokumentum között. Az aláírás ellenőrzése hasonló bonyolultságú folyamat. Ezek számításigénye meghaladja az ember képességeit, így feltétlenül gépi segítséget kell igénybe vennünk. A legtöbb ma használt levelezőprogram támogatja a digitális aláírást, így egy üzenet digitális aláírással való ellátása általában csak egy kattintást igényel. (3. ábra) A bejövő üzenetek aláírásának ellenőrzése is gépi feladat. Ha a levelezőprogram digitális aláírást talál a megjelenő levélen, ellenőrzi azt, és jelzi a felhasználónak, ha az aláírás érvénytelen. Magyarországon a digitális aláírás hitelességét a törvény is elismeri. A 2001. évi XXXV. törvényünk vonatkozik digitális aláírásokra.

4. Összefoglalás

Nyilvános kulcsú rendszerekben életbevágó, hogy a titkos kulcs valóban titokban maradjon, a nyilvános kulcs pedig hitelesen kerüljön nyilvánosságra. Ha *C* sikeresen becsempészi saját nyilvános kulcsát *B* nyilvános kulcsának helyére, az összes *B*-nek szóló üzenetet meg tudja fejteni. Cikkünk második részében bemutatjuk, hogy nyilvános kulcsú kriptográfiára épülő rendszerek milyen lehetőségeket nyújtanak a nyilvános kulcs biztonságos, hiteles lekérdezésére. Összefoglaljuk továbbá a BME-n e témákban folyó kutatómunka néhány legújabb eredményét.

5. IRODALOMJEGYZÉK

[1] Berta I. Zs. – Mann Z. Á.: Evaluating Elliptic Curve Cryptography on PC and Smart Card, Periodica Polytechnica 2001. (megjelenés alatt)
[2] Daemen, J. – Rijmen, V.: The Block Cipher Rijndael, Smart Card Research and Applications, LNCS 1820, Springer, 2000.
[3] Endrődi Cs. – Hornák Z. – Selényi E.: „Egy új nyilvános kulcsú rendszer: NTRU”, Networkshop2003, Pécs, 2003.
[4] Győrfi L. – Győri S. – Vajda I.: Információ- és kódelmélet, Typotex, 2000.
[5] Kerckhoff, A.: La Cryptographie Militaire, Journal des Sciences Militaires, 1883, Jan.
[6] Rivest, R. – Shamir, A. – Adlemann, L. M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, MIT/LCS/TM-82, 1978.
[7] Schneier, B.: Applied Cryptography, John Wiley & Sons, 1996.

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. A MEE tagja.

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

Hardware and Software Security I - II

Abstract – Safety and quality of the supplied energy are not only depending on the traditional electrotechnical background, but are strongly determined by the security conditions of informatics, too. The formation and the operation of the energy market (like any other electronic commerce application) have to be based on secure communication between the partners. The secret and authentic communication can be ensured using public key infrastructure. The most important goal of the authors was to present the connection, the joint role of the two, originally separated fields, namely power engineering and cryptography. Some of the new results of the research work carried out at Budapest University of Technology and Economics are also presented in the paper.