Tanúsítványokról

Dr. Keszthelyi András

Óbudai Egyetem, Keleti Károly Gazdasági Kar

Szervezési és Vezetési Intézet

keszthelyi.andras@kgk.uni-obuda.hu

Absztrakt: Korunkat szokás az információs társadalom korának (is) nevezni. Talán helyesebb lenne a kiberbűnözés, sőt kiberháborúk korának hívni. A számítógépes környezetben tárolt és kezelt adatoknak nemcsak a mennyisége növekszik napról napra, de egyre erősödik az azoktól való függésünk is. Ilyen helyzetben fokozott jelentősége van adataink megvédésének, ezen belül is az egymástól távol eső gépek közötti adatforgalom védelmének. Ennek egyik eszköze a széles körben alkalmazott https protokoll (facebook, gmail, Neptun, netbank stb.). Ennek alapja a kétkulcsos titkosításra épülő tanúsítványok rendszere. Mivel a tanúsítványok rendszere nem egyszer s mindenkorra kőbe vésett, színre lép az emberi tényező is: vannak olyan, a tanúsítványok kezelésével kapcsolatos műveletek, amelyek megszüntetik a rendszer biztonságát. Kövesse el ezen műveleteket a felhasználó személyesen, tévedésből vagy megtévesztés áldozataként személyesen, vagy bármilyen rosszindulatú program. Mivel a vélt biztonság rosszabb, mint a biztonság tudott hiánya, fontos, hogy tisztában legyünk evvel a problémával, s a védekezés lehetséges módjaival is.

1 Bevezetés és célkitűzések

Korunkat szokás az „információs társadalom” korának nevezni. Talán helyesebb volna a kiberbűnözés és kiberháborúk koráról beszélni. A „kibervadnyugaton” élünk.

A Stuxnet vírus iráni atomcentrifugákat tett tönkre, kínai netcowboyok magas színvonalú ipari kémkedés formájában szerzik a csúcstechnológiához szükséges tudást egyenesen Amerikából, a BME Adat- és Rendszerbiztonság Laboratórium (CrySyS) olyan célzott informatikai támadássorozatot leplezett le, amelyben hazai kormányszervek is célpontok lehettek. Az Anonymous csoport képes volt lehallgatni az FBI és a Scotland Yard telefonjait, miközben Amerika a teljesség igényével nemcsak lehallgatja, hanem tárolja is polgárai elektronikus üzenetváltásait, beleértve a telefonbeszélgetéseket is.

Az okostelefonok (tulajdonosai) számára hegyekben állnak a rosszindulatú programok, egyes esetekben már a gyárban telepítettek ilyeneket, manipulálhatók

nemcsak a gépkocsik, de akár egy repülőgépet is el lehet téríteni egy androidos alkalmazással.

Eközben a hétköznapi kibercowboyok a Facebookon keresztül tájékozódnak – felhasználva a Google Maps és StreetView szolgáltatásokat is –, hogy hova menjenek betörni, bankszámlánk, villámlevél-ládánk, okostelefonunk – s így mi magunk is – állandó veszélynek van kitéve.

A kocsi és az adat között az az alapvető különbség, hogy ha kocsimat ellopják, akkor az eltűnt onnan, ahol hagytam. Ráadásul legalább annyi támpontunk van, hogy a tettes a lopás időpontjában személyesen megjelent a kocsinál. Virtuális útonálláskor a tettesnek sehol és semmikor nem szükségszerű ott lennie. Ilyen körülmények között nem könnyű a fizikai biztonságunkat virtuális világban megvédelmezni.

Van alkalmas technika, kiváló eszközök állnak rendelkezésünkre, sajnos az ellenség rendelkezésére is. Ráadásul tudjuk, hogy hibátlan program nincs, csak felületesen tesztelt. Mivel hiába akár a legjobb technika – a leggyöngébb láncszem sokszor a jámbor és naiv felhasználó, ezért nem ritkán a sikeres támadásokat nem elsősorban technikai bravúrok, hanem az emberi gyöngeség, felületesség, nem kellő tudás és tudatosság kihasználása teszi lehetővé.

Az alábbiakban a böngészők által használt tanúsítványok, pontosabban azok kezelésének egy problémás vonatkozását vesszük szemügyre.

2 Alapvetés

2.1 Az emberi tényező szerepe

Mondhatnánk azt, hogy mi „kis halak” vagyunk ahhoz, hogy bárki is bennünket akarna (virtuálisan) támadni. Ez önmagunk becsapása lenne, egyrészt azért, mert a netrabló nemcsak közvetlenül a pénzünkre törhet, hanem adatokat is gyűjthet tőlünk, rólunk, ellenünk. Számos esetben a virtuális ellenség számára teljesen mindegy, hogy kinek a gépét kaparintja meg („csak” virtuálisan persze), a lényeg nem a személy, hanem a minél több gép.

Mi minden állhat a háttérben? Szakmai kivagyiság, dicsekvés. Botnet építés spamküldéshez, elosztott túlterheléses támadáshoz, fizetős hirdetésekre való álkattintgatásokhoz. Esetleg csak ugródeszkára van szüksége a tettesnek, saját nyomai eltüntetése céljából.

Az emberi hanyagság és felületesség, lustaság mellett a véletlen szerepét sem hagyhatjuk figyelmen kívül. Míg Obama twitter-fiókjának és számos celeb különféle fiókjainak feltörését a gyönge jelszavak tették lehetővé, addig a francia

központi bank hitelezési rendszerébe 2008-ban úgy jutott be egy férfi, hogy véletlenül bukkant rá a betárcsázós csatlakozásra, s elsőre kitalálta az egyébként nagyon gyönge jelszót (123456).

A kibervadnyugati körülmények közötti – virtuális – túlélés érdekében a lehető legjobb befektetés az, ha tanulunk, képezzük magunkat.

2.2 Kétkulcsos titkosítás

A titkosítások története egyidős az emberiség történetével. Gyöngébb, jobb, egyre jobb módszereket, eljárásokat találtak ki idők folyamán, s váltakozó sikerrel folyt az örök küzdelem a titkosítók s a titkos üzeneteket megfejteni próbálók között. 1976-ban aztán Rivest, Shamir és Adleman kifejlesztettek egy olyan eljárást (RSA-algoritmus), amely a tudomány ma nyilvánosan ismert állása szerint bár elméletileg megfejthető, de gyakorlatilag ezt mégsem lehet kivitelezni. Legnagyobb előnye, hogy nem kell biztonságos csatorna – személyes találkozás pl. – az előzetes kulcscseréhez.

Az első alkalmazást erre az eljárásra, a PGP-t 1991-ben Philipp Zimmermann készítette el.

2.2.1 Alapelve

Minden résztvevő generál magának két kulcsot, amelyek összetartozó párost alkotnak, s egyikből a másik nem számítható ki. Az egyiket nevezzük nyilvános kulcsnak (N), és a lehető legszélesebb körben terjesztjük. A másikat pedig nevezzük titkos kulcsnak (T), és kizárólag a gazdája birtokában lehet.

Maga az eljárás úgy működik, hogy ha egy tetszőleges szöveget a kulcspár egyik tagjával kódolunk, azt annak párjával lehet dekódolni.

```
kódolás[kódolás(szöveg,N),P]=szöveg
```

illetve

```
kódolás[kódolás(szöveg,P),N]=szöveg
```

Így tehát, ha – mondjuk – Aladár titkosított üzenetet szeretne küldeni Bélának, Béla nyilvános kulcsával kell azt titkosítania. Ennek párja, Béla titkos kulcsa a definíció szerint Béla kizárólagos tulajdonában lehet, tehát kizárólag Béla lesz képes a titkos üzenetet dekódolni, még Aladár sem tudja azt megtenni.

Ha azonban Aladár azt is szeretné, hogy Béla biztos lehessen abban, hogy az üzenet tőle származik, akkor saját titkos kulcsával is titkosítja azt. Ekkor Béla a feladó, azaz Aladár nyilvános kulcsával tudja fejteni a küldeményt. Ez azt jelenti, hogy azt valóban Aladár titkos kulcsával titkosították, ami viszont kizárólag

Aladár birtokában lehet, s így a feladó hitelessége bizonyított. Ez vezet el a digitális aláíráshoz.

2.2.2 Alapvető biztonsági szabályok

Az eljárásnak két alapvető fontosságú biztonsági szabálya van. Az egyik, hogy a titkos kulcsnak titokban, gazdája kizárólagos birtokában kell maradnia, a másik pedig, hogy a nyilvános kulcsok hitelességéről mindig meg kell győződni valahogyan.

A titkos kulcs titkosságának követelménye nyilvánvaló, hiszen ha valaki azt el tudja lopni Aladártól, akkor nemcsak az Aladárnak szóló titkos üzeneteket tudja megfejteni, hanem – ami a kellemetlenebb – Aladár nevében hitelesnek látszó küldeményeket is tud küldeni.

2.2.3 Digitális aláírás

A digitális aláírásnak, hasonlóan a hagyományoshoz, két dolgot kell bizonyítania. Az egyik, hogy valóban az aláírótól származik, másrészt pedig, hogy tartalma nem változott meg időközben.

Tekintettel arra, hogy pusztán a feladó hitelességének bizonyítására nem érdemes egy dokumentumot egészében az aláíró titkos kulcsával titkosítani, hiszen az fölöslegesen nehezíti meg annak olvashatóságát (dekódolni kell, de azt bárki megteheti az aláíró nyilvános kulcsának birtokában), egyszerűbb eljárást alkalmazunk. Az aláíró az aláírni szándékozott dokumentumnak (bármilyen fájl, amely legalább 1 bájtot tartalmaz) kiszámolja egy fix hosszúságú ellenőrző összegét egy alkalmas számítási módszerrel (hash függvény). Ezt az ellenőrző összeget titkosítja saját titkos kulcsával, és mellékeli a dokumentumhoz.

Ezen digitális aláírás ellenőrzése két lépésből áll.

Egyikben a (vélt) aláíró nyilvános kulcsával dekódolni kell a titkosított ellenőrző összeget. Ha ez a nyilvános kulcs valóban az ellenőrző összeg titkosításához használt titkos kulcs párja, akkor ebben a lépésben visszakapott ellenőrző összeg pontosan megegyezik avval, amelyet még az aláíró számolt ki az aláírás során.

A második lépésben ki kell számolni a dokumentum ellenőrző összegét ugyanavval az eljárással (ugyanazon hash függvénnyel). Ha a dokumentum tartalma időközben nem változott meg, akkor az ellenőrzés során kiszámolt ellenőrző összeg nyilván megegyezik az aláíráskori ellenőrző összeggel.

Ha tehát az ellenőrzés során kétféleképpen megkapott ellenőrző összeg azonos, akkor mind az aláíró, mind a dokumentum tartalma hiteles. Ha nem egyeznek meg, akkor vagy a dokumentum tartalma változott meg, vagy pedig másvalakitől származik.

A történelmileg hagyományos, papírra kézírással elkövetett aláírás biometrikus jellemző, ellenben a digitális aláírás tisztán birtoklás alapú, azaz aki a titkos kulcs birtokában van, az tudja létrehozni. A hagyományos aláírás hamisítását írásszakértő kimutathatja, a digitális aláírásnál ilyen lehetőség nincs. Ezért kell nagyon vigyázni arra, hogy a titkos kulcs gazdájának kizárólagos birtokában maradjon.

2.2.4 Közbeékelődéses támadás

A nyilvános kulcs hitelességét ellenőrizni kell – így szól az egyik biztonsági rendszabály. Miért? Hogy kivédjük a közbeékelődéses támadás (man-in-the-middle-attack, MITM) lehetőségét.

Tegyük fel ugyanis, hogy Béla elküldi saját nyilvános kulcsát Aladárnak emilben. Megteheti, a kulcs nyilvános, akárkinek a birtokában lehet. Tegyük fel továbbá, hogy Cilla ezt az elküldött nyilvános kulcsot útközben el tudja fogni, mint területileg illetékes rendszergazda, vagy ügyes netkalóz, vagy titkosszolgálat stb. Kicserélheti egy általa generált kulcspár nyilvános felére, majd azt küldi tovább Aladárnak. Aladár így valójában Cilla nyilvános kulcsát fogja használni Béláé helyett, ami azt eredményezi, hogy az általa titkosított üzenetet Cilla tudja fejteni (majd megváltoztatni, újra titkosítani az általa elfogott igazi bélai kulccsal, majd továbbküldeni Bélának).

Olyan ez, mint amikor a mexikói határvidéken a seriff megfogja a spanyol anyanyelvű rablóvezért, és tolmács útján kénytelen vallatni. Seriff a tolmácsnak: „Kérdezd meg tőle, hol a zsákmány!" A tolmács fordít: „Arra kíváncsi, hova dugtad el a zsetont". Rablóvezér: „Nem árulom el!" A tolmács fordít: „Nem hajlandó megmondani". A seriff előveszi a pisztolyát, és azt mondja: „Ha azonnal nem mondja meg, szétlövöm a fejét!" A tolmács fordít: „Ha nem árulod el, kiloccsantja az agyadat!" A rablóvezér: „Jó, a templomkertben ástam el a vadkörtefa tövében". A tolmács ferdít: „Azt mondja, nem fél a haláltól".

2.2.5 Bizalmi lánc és háló

Hogyan lehet egy nyilvános kulcs hitelességét ellenőrizni, más szavakkal: hogyan lehet meggyőződni arról, hogy valóban azé a személyé, akiének véljük azt?

Ennek legegyszerűbb esete, ha személyesen az illetőtől kapjuk, illetve neki személyesen adjuk. Csakhogy pont ez az, amire a legtöbb esetben nincs lehetőség, és épp ez volt a fő előnye a kétkulcsos eljárásnak, hogy nem szükséges a kulcs cseréjéhez személyesen találkozni.

Aladár megteheti, miután megkapta Bélától emilben a nyilvános kulcsot, hogy fölhívja telefonon Bélát, és egyeztetik azt. Ha azonban Aladár és Béla nem régi jó ismerősök, akkor abban sem lehet bizonyos Aladár, hogy a telefonvonal túlsó végén valóban Béla van...

Ha Béla nemcsak emilben, de sms-ben, telefaxon és papír alapú levélben is elküldi a nyilvános kulcsát Aladárnak, és mindegyik csatornán ugyanaz érkezik meg Aladárhoz, akkor a manipuláció lehetősége nagyon csekély, gyakorlatilag nulla lesz.

Egy másik lehetőség a bizalmi lánc, illetve bizalmi háló építése. Tegyük fel, hogy Aladárnak és Bélának módja van a személyes kulcscserére. Ez esetben mindketten birtokolják egymás nyilvános kulcsát, s a legmagasabb fokú bizonyosságuk van annak hitelességéről. A későbbiek folyamán Cecil, akit Béla jól ismer, elmehet Bélához, s megkérheti, hogy írjon alá számára egy olyan dokumentumot, amely tartalmazza a nevét, fontosabb személyi adatait, telefonszámát, arcképét s végül nyilvános kulcsát. Mivel Béla jól ismeri Cecilt, azaz tudja, hogy ő valóban Cecil, aláírja ezt a dokumentumot. Cecil utána ezt elküldheti akár Aladárnak is, aki ezután elfogadja Cecil nyilvános kulcsát hitelesnek, mert Béla aláírta azt, Béla aláírását pedig tudja ellenőrizni, hiszen Béla nyilvános kulcsából abszolút hiteles példánya van.

Később esetleg Dezső felkeresi jó barátját, Cecilt, és hasonlóan járnak el.

Így épül fokonként a bizalmi lánc, Aladártól Bélán és Cecilen át Zénóig. Ha az egyes nyilvános kulcsokat és az azok gazdáit leíró dokumentumokat nemcsak egy-egy ember írja alá, hanem sokat aláírnak sokaknak, akkor bizalmi hálóról beszélhetünk bizalmi lánc helyett. Minél több ember vesz részt benne, annál könnyebben tudunk egy-egy újabb nyilvános kulcsot hitelesség szempontjából ellenőrizni. Egy nyilvános kulcs hitelessége annál erősebb, minél többen írták alá azt olyan személyek, akiktől hiteles nyilvános kulcsunk van.

Vegyük észre, hogy ez egy olyan rendszer, amelynek semmilyen központi eleme, kiszolgálója nincs, teljesen magánúton, személytől személyig épül és erősödik.

2.2.6 Tanúsítványok mint ellenőrzött nyilvános kulcsok

Ezt a folyamatot lehet intézményesíteni is. Elképzelhető, hogy abból a célból alapítunk egy vállalkozást, hogy szervezetten és üzletszerűen végezzünk ilyen aláírásokat a személyes ismerősök helyett. Ennek során nyilván igen gondosan kell eljárni a személyazonosság ellenőrzése során, az adott körülmények között elvárható legnagyobb gondossággal. Ezen túlmenően – ugyancsak nyilván – akkor fog bárki is fizetni cégünknek az aláírásért, ha cégünk nyilvános kulcsa, amely aláírásunk ellenőrzéséhez szükséges, a világ bármely pontján könnyen elérhető, és hitelessége általánosan elfogadott. Ezt nem könnyű biztosítani.

Ha szabványosítjuk a nyilvános kulcsot és gazdájának leírását tartalmazó dokumentum szerkezetét és formáját, akkor annak felhasználhatóságát automatikussá, különféle programok számára közvetlenül felhasználhatóvá tesszük.

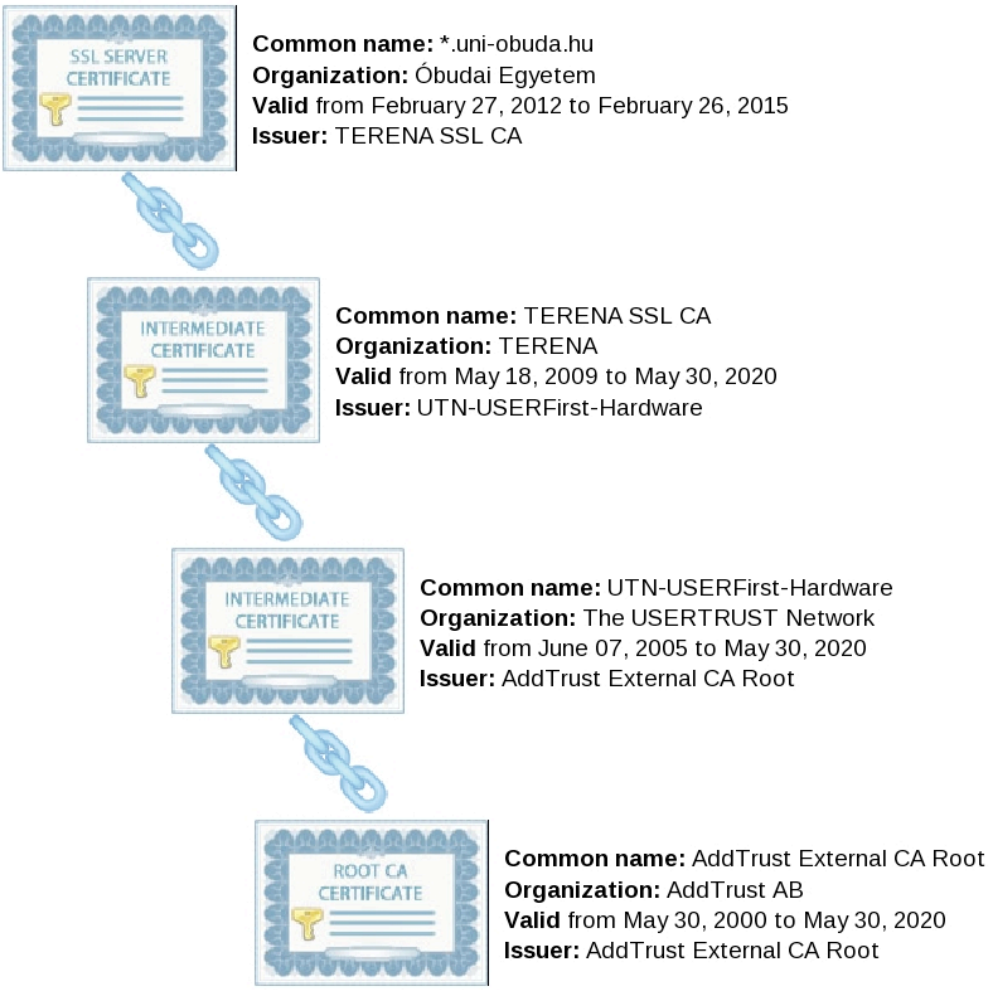
Így jutunk el a tanúsítvány (CERT, certificate) és a CA (certificate authority) fogalmához illetve intézményéhez.

2.2.7 A HTTPS protokoll

Valójában nem önálló protokoll, hanem a http protokoll használata kétkulcsos titkosítás közbeiktatásával. Lényegi tulajdonsága, hogy nemcsak az adatforgalom titkosított, hanem a felhasználó abban is biztos lehet, hogy valóban avval a kiszolgálóval áll kapcsolatban, amelyhez kapcsolódni szándékozott. Példának okáért, ha netbankolni akar, akkor nemcsak hogy esetleges lehallgatók nem fogják tudni megszerezni a banki jelszavát és egyéb adatait, de attól sem kell tartania, hogy a hálózati adatok ügyes elterelésével egy ál-szerverre csalták volna az igazi bank igazi kiszolgálója helyett.

Ezt a kétkulcsos titkosítás, illetve az azon alapuló digitális aláírás teszi lehetővé. A nagy, nemzetközi tanúsítványkibocsátó cégek (CA-k) nyilvános kulcsait gyárilag tartalmazzák a böngészők. Így tehát, ha egy böngészővel pl. neptunozni szeretnénk, akkor a böngészőbe azt írjuk be, hogy https://neptun.uni-obuda.hu.

Ekkor a böngésző megkapja a neptun kiszolgáló tanúsítványát, megnézi annak kibocsátóját (aláíróját), majd bekéri annak a saját tanúsítványát, s így tovább. Ha véges sok lépés után eljut egy olyan tanúsítványig, amelyet azon nagy, nemzetközi tanúsítványkibocsátó cégek (CA-k) valamelyike írt alá, amelyek saját tanúsítványait saját „gyári” tanúsítványtára tartalmazza, akkor indulhat a folyamat, betöltődik a Neptun nyitóoldala. Ellenkező esetben hibaüzenetet kapunk, amelyből kiderül, hogy milyen okból volt sikertelen a tanúsítvány ellenőrzése, pl. lejárt az érvényességi ideje, nem arra a gépre szól, ismeretlen az aláíró stb.



1. ábra

A neptun.uni-obuda.hu tanúsítványlánca

Ezen esetekben az történik – az ügyfél szemszögéből nézve –, hogy a kiszolgáló (esetünkben a neptun.uni-obuda.hu) önmagával való azonosságának ellenőrzését másra bíztuk (a Terena SSL CA-ra). Lemondok ezen ellenőrzés jogáról és egyben felelősségéről, mert megbízom abban, hogy a tanúsító cég elég gondosan járt el. Hogy vannak-e olyan esetek, amelyekben ezt esetleg nem célszerű megtenni, mindenki gondolja végig saját maga.

3 „Tudok egy rövidebb utat az erdőn keresztül”

3.1 MITM – pl. ARP mérgezéssel

A hálózati adatforgalom lehallgatása, sőt elterelése nem feltétlenül nehéz művelet technikai értelemben. Közbeékelődéses támadást például kitűnően meg lehet valósítani ún. ARP mérgezéssel. Ennek során a helyi alhálózati szegmensre csatlakozó gépeket előbb megtévesztjük az alapértelmezett átjáró címét illetően, majd hamis választ lehet adni a neptun kiszolgáló IP-címét firtató DNS-kérdésre, ami azt eredményezi, hogy az adatforgalom az igazi kiszolgáló helyett egy alkalmasan beállított kalóz gépre jut el.

Csakhogy a böngésző figyelmeztetni fogja a felhasználót, hogy nem jó helyen jár. Ugyanis egyetlen tanúsító cég sem lesz hajlandó egy netkalóznak a neptun.uni-obuda.hu gépre szóló tanúsítványt adni, hanem csak az egyetem gondosan ellenőrzött, felhatalmazott képviselőjének. A netkalóz tehát csak saját maga által aláírt tanúsítványt tud a kalózkiszolgálóra elhelyezni, amelyet a böngésző – értelemszerűen – nem fog tudni visszavezetni egyetlen beépített, fölső szintű tanúsítványra sem.

3.2 A tanúsítványok manipulálhatók

Sajnos nem lehet kizárni az ügyféloldali tanúsítványok manipulálhatóságát. Programhibák, biztonsági rések, süket duma (social engineering) vagy bármilyen trükk, amely a felhasználót ráveszi arra, hogy elvégezze a támadó számára szükséges módosításokat – ehhez esetleg egyetlen egérkattintás is elegendő lehet, l. a Kurnyikova-vírus példáját.

A böngészők különféle módon és helyen tárolják a beépített legfölső szintű tanúsítványokat, azonban alapvető műveleteket a felhasználó saját jogán végezhet. Ilyen műveletek a tanúsítványok importálása, a kivételek fölvétele, a megbízhatósági jellemzők szerkesztése. A tanúsítványok kezelését a felhasználókra bízni teljesen indokolt, hiszen az ezekkel kapcsolatos döntéseket a felhasználó hozza meg, neki kell meghoznia a körülmények mérlegelése alapján. Ez azonban feltételezi, hogy a felhasználó a megfelelő háttérismeretek, -tudás birtokában van, és gondosan mérlegeli cselekedetei lehetséges következményeit. Ez utóbbi feltétel azonban sokszor nem teljesül maradéktalanul.

Mivel a tanúsítványokkal kapcsolatos műveleteket felhasználói jogon lehet végezni, egy esetleges támadónak nem szükséges rendszergazdai jogosultságot szereznie a felhasználó gépén, elegendő annak korlátozott jogosultságával végrehajtani egyes utasításokat, futtatni egyszerűbb programokat. Ez a korlátozott

jogú programfuttatás elegendő ahhoz, hogy a böngésző tanúsítványtárában el lehessen végezni a szükséges műveleteket.

Mivel a felhasználók tudása és tudatossága sokszor hagy kívánnivalókat maga után, jó eséllyel magát a felhasználót is rá lehet venni arra, hogy a kívánt műveletet, pl. egy általnúsítvány importját elvégezze.

További lehetőség lehet adott esetben annak kihasználása, ha a böngésző újabb változatát http protokollon keresztül tölthetjük le – semmi technikai akadálya nincs annak, hogy a letöltés adatfolyamát manipulálja egy támadó, és módosított tanúsítványtárral felszerelt csomagot juttasson el a felhasználónak.

Ha pedig sikerült bejuttatni a felhasználó személyes tanúsítványtárába bejuttatni egy kivételt, vagy esetleg importál(tat)ni egy legfölső szintű tanúsítványt, semmi akadálya nincsen a célzott közbeékelődéses támadásnak, akár ARP mérgezéses módszerrel, akár más célravezető eljárással.

3.3 Egy lehetséges megoldás

Vállalati környezetben mindenképpen szükséges az informatikai biztonsági szabályzatba belevenni, hogy a felhasználói jogosultsági rendszert úgy kell kialakítani, hogy a felhasználók a tanúsítványokkal kapcsolatos semmilyen változtatást ne tudjanak végrehajtani. Ha ilyen igény fölmerül, az illetékes rendszergazda a kellő tudás birtokában, a szükséges ellenőrzéseket végrehajtva majd megoldja. Így kiküszöbölhetjük a felhasználó tévedésének vagy figyelmetlenségének következményeként föllépő tanúsítványmanipuláció lehetőségét. Mivel ez esetben felhasználói jogon nem lehetséges a tanúsítványokkal kapcsolatos műveletek elvégzése, ezért ezt rosszindulatú programeszközök bevetésével sem lehet elérni, csak rendszergazdai jogosultság eredményes megszerzésével, ami már lényegesen nehezebb feladat.

Magánhasználatú, saját gépen a helyzet ennél összetettebb. Alapvető fontosságú szabály, hogy saját gépünket sem használjuk a mindennapokban rendszergazdai jogosultságokkal. Ezt a szabályt betartani végül is nem nehéz feladat, viszonylag ritkán kerülünk olyan helyzetbe, amelynek megoldásához indokoltan rendszergazdai jogosultságra van szükség. A nagyobb probléma az, hogy itt fel kell tételeznünk, hogy a felhasználó birtokában van annak a tudásnak, amelynek birtokában megalapozott döntést tud hozni egyes tevékenységek szükséges vagy megengedhető voltáról. Ez pedig erősen fölértékeli az oktatás szerepét.

4 A tanulás és tanítás szerepe

Kibervadnyugati korunkban az informatikai biztonságnak kiemelt jelentősége van. Gyakorló tanárként arra kell fölhívnom a figyelmet, hogy a föntebb vázlatosan bemutatott probléma nem csupán számítástechnikai, IT-biztonsági probléma, hanem oktatási is. Ráadásul az oktatási probléma is legalább két síkon jelenik meg. Egyrészt az oktatásban is használatos a https protokoll – Neptun, általánossá vált e-naplók –, másrészt pedig a tinédzser diákok különféle veszélyeknek lehetnek kitéve, ha nincsenek tisztában a legfontosabb tudnivalókkal. Ezeket nem lehet néhány gyakorlatias szabályra leegyszerűsíteni (bár azokra is szükség van), feltétlenül szükséges foglalkozni ezek elméleti hátterével és magyarázatával is, mert a https protokoll használata mindennapi életük része (csak a leggyakoribbakat említve: Facebook, Gmail).

A diákok számítástechnikai tárgyi tudását és készségeit, jártasságukat megvizsgálva akár Magyarországon, akár Közép-Európában, riasztó helyzetet találunk. Személy szerint nem gondolom, hogy a helyzet Európa, vagy akár a világ más részein lényegesen jobb lenne. Van dolgunk tehát elegendő.

Irodalom

[1] Adhikari Richard: Remote Airplane Hijack Threat Demoed: Simon Says 'Crash!'. TechNewsWorld.com, 2013.04.11., http://www.technewsworld.com/story/77776.html

[2] Ben Weitzenkorn: Bank of France's Accidental Hacker Acquitted. TechNewsDaily, 2012.09.21. http://www.technewsdaily.com/8140-accidental-hacker-bank-france.html

[3] Bodnár Ádám: Több éve zajló támadást leplezett le a BME CrySyS. hwsw.hu, 2013.03.21.

[4] Greenwald Glenn: Are all telephone calls recorded and accessible to the US government? A former FBI counterterrorism agent claims on CNN that this is the case. The Guardian, guardian.co.uk, 2013.05.04.

[5] Hungarian National Security Authority (NSA HUN) and CrySyS Lab Malware Intelligence Team: TeamSpy – Obshie manevri. Ispolzovat' tolko s razreshenija S-a. Budapest University of Technology and Economics, Department of Networked Systems and Services, 2013. március

[6] Kiss G.: Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course / TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4. ISSN: 2146 – 7242, pp. 222-235.

[7] Kiss G.: Comparison of the Programming Knowledge of Slovakian and Hungarian Students / Procedia of Social and Behavioral Science Journal különszám, ISSN: 1877-0428, p. 10.

[8] Koscher Karl et al.: Experimental Security Analysis of a Modern Automobile. 2010 IEEE Symposium on Security and Privacy. http://www.autosec.org/

[9] Ködmön József: Kriptográfia. Computerbooks, Budapest, 2002.

[10] Nemetz Tibor: Kriptográfiai mondanivaló újonnan beinduló adatvédelmi rendszerek szervezői számára. "Adatvédelem Magyarországon" c. konferencia, Mátraháza, 1995. L. pl. http://193.225.224.240/gazdinfo/gyak_KEA/Nemetz.html

[11] Robinson, Sarah: Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. SIAM News, Volume 36, Number 5, June 2003.

[12] Schneier, Bruce: Applied cryptography: Protocols, algorithms, and source code in C. Wiley & Sons, New York, 1996. (2nd ed.)

[13] Schneier, Bruce: Schneier a biztonságról. HVG könyvek, Budapest, 2010.

[14] The Free Software Definition. http://www.fsf.org/licensing/essays/free-sw.html

[15] Zetter Kim: Anonymous Eavesdrops on FBI Anti-Anonymous Strategy Meeting. Wired.com, 2012.03.02., http://www.wired.com/threatlevel/2012/02/anonymous-scotland-yard/

[16] Zimmermann, Philip: The official PGP user's guide. MIT Press (Cambridge, Mass), 1996. ISBN 0262740176. Originally part of the PGP program package: ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf