Fritz-chip

Trusted Computing' Frequently Asked Questions - TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA Version 1.1 (August 2003)

*

Az emberek többsége talán úgy véli, hogy a drágán megvásárolt számítógép olyan eszköz, amely a meg- felelő -es szabadon kiválasztott -szoftverek segít- ségével képes bizonyos számításokat elvégezni. A felhasználó bizonyara saját maga szeretne eldönteni, hogy a PC milyen feladatokat végezzen el, es a le- hetősegek skálája igen szeles: a pénzügyi elemzé- sektől kezdve az internetezésen keresztül a zenehallgatásig barmi szoba jöhet. A legnagyobb szórakoztatóipari es számítástechnikai vállalatok azonban szeretnék kalodába zárni a felhasználókat, hogy mindenki csak az általuk 'megbízhatónak' ítélt hardvereket, szoftvereket es fájlokat használhassa. Az orwelli terv technikai megvalósításának már nevet is adtak, ez a Trusted Computing Platform Al- liance (TCPA). A szövetség 1999 októberében jött létre a Compaq, a HP, az IBM, az Intel es a Micro- soft kezdeményezésére, de azóta több, mint 150 vál- lalat csatlakozott hozzájuk. E cégek közös célja az, hogy egy fejlett hardverelemekre és szoftverekre épülő, biztonságos és megbízható szamítógépes platformot hozzanak létre. Elképzeléseik szerint a jövőben az összes hardver igazodni fog a TCPA elő- írasaihoz, míg a szoftverek terén a Microsoft által kifejlesztett Palladium (újabb nevén NGSCB, azaz Next Generation Secure Computing Base) fog gon- doskodni a megbízhatóságról.

Ki lesz nagyobb biztonságban? A TCPA rendsze- rekben elsősorban azok a szoftverfejlesztők, kiadok, vállalatok és kormányok lesznek nagyobb bizton- ságban, amelyek dönthetnek majd a fájlok megbíz- hatóságáról. A felhasználok, az egyszerű alkalmazottak, a zenehallgatók -azaz a többség -meg kiszolgáltatottabbak lesznek.

Galántai Zoltán egyetemi docens, a Privacy International jogvédő szervezet vezetőségének tagja arra mutatott rá, hogy a szerzői joggal foglalkozó törvények világszerte egyre inkább azt tartják szem előtt, hogy mi a jó a tartalomtulajdonosoknak (es a fogyasztok, felhasználok érdekeire ügyet sem vetnek). Az 1998-as CTEA (Copyright Term Extension Act) például további 20 evvel terjesztette ki az USA- ban a copyright-védelmet, és a jogvédők most attól tartanak, hogy ha ez 2018-ban lejár, akkor újra ki fog- jak terjeszteni (es így tovább a végtelenségig). A TCPA ugyanennek a felfogásnak a műszaki tükör- képe: itt nem a jog, hanem a technika az, ami kizá- rólag a "hatalmon belül lévők" érdekeit védi. Galántai kérdésünkre elmondta, reális veszélyt lat a TCPA-ban, hiszen "azok az emberek, akik benyeltek a Windowst, ezt is könnyen benyelhetik". Mindenre figyel a Fritz-chip A TCPA beépített felügyelő-és je- lentőrendszerrel látja el a jövő asztali számítógépeit, egy alaplapra forrasztott hardverkulcs képében. A PC bootolasa közben az úgynevezett "Fritz-chip" el- lenőrzi, hogy a szamítógépben megtalálható hardve- relemek a TCPA által elfogadottak-e, a szoftverek hitelesítettek-e es hogy a komponensek mindegyiké- nek érvényes-e a sorozatszáma. Az iranyítást innen- től az operációs rendszer rendfenntartó szoftvere veszi át -a Windows esetében a Palladium.

A Fritz-chip képes egy harmadik felnek igazolást adni arról, hogy az adott PC alkalmas egy bizonyos DVD fogadására. Ezután a chip a kiadótól letölt egy kulcsot, amellyel az arra jogosult szoftverek képe- sek lejátszani a DVD-t, de a másolás szóba sem jöhet. (A megfigyelő chipet Fritz Holling dél-Karo- linai szenátorról nevezték el, aki fáradhatatlanul dol- gozik a TCPA népszerűsítésén.)
A fájlcserének annyi. A szoftverfejlesztők, a film-és zenekiadók évek óta azt hangoztatják, hogy túlságosan elburjánzott az interneten az "illegális" fájlcsere, es (meg több) pénzt szeretnének kapni a termékeikért. A TCPA tökéletesen alkalmas a digi- tális jogkezelésre (DRM, Digital Rights Manage- ment): olyan DVD-ket, szoftvereket, letöltéseket forgalmazhatnak, amelyeket nem lehet lemásolni. Ha valaki mégis "biztonsági másolatot" készít, akkor az interneten keresztül barmikor működésképte- lenné tehetők a jogtalanul használt fájlok.
Az alkalmazásra lesz bízva, hogy milyen sza- bályok érvényesek az általa lejátszott fájlokra, a sza- bályokat pedig egy központi szerverről, a kiadótól tölti majd le a program. Ha egy vállalat úgy dönt, hogy egy CD meghallgatását csak tízszer engedé- lyezi, akkor azt egy gombnyomással elintézheti. Ross Anderson, a

Cambridge Egyetem számítás- technikai laboratóriumának kutatója szerint az is el- képzelhető, hogy a jövőben egy alkalomra szóló CD-t is lehet majd vásárolni, amelyet csak egy bi- zonyos napon -például valakinek a születésnapján - lehet lejátszani.

A korrupció es a bűnözés melegágya. A vál- lalatoktól és a kormányoktól kiszivárogtatott infor- mációkkal az újságírók semmit sem tudnak majd kezdeni, a számítógépük ugyanis nem fogja betöl- teni a titkosított dokumentumokat. A korrupt hiva- talnokok így szinte barmit megtehetnek, nem kell félniük a lebukástól.

Az alkalmazottak is kényes helyzetbe kerül- hetnek, ha egy rossz főnöki döntés miatt hibát kö- vetnek el. Egy munkaügyi perben úgysem tudjak majd bebizonyítani igazukat, ugyanis vagy nem fér- nek, majd hozza a korábbi utasításhoz, vagy az idő- zárral ellátott dokumentum már rég letörölte önmagát.

Néhány funkciót a bűnözők is hasznosíthat- nak: megoldhatjak, hogy a kábítószer- szállítmá- nyokról szóló táblázatokat csak a felhatalmazott számítógépeken lehessen olvasni, és az adatok min- den hónap végén megsemmisüljenek. Ez megnehe- zíti a bűnüldöző szervezetek dolgát, bár a Microsoft tárgyal a kormányzatokkal arról, hogy a rendőrök és a kémek kapjanak-e hozzáférést a főkulcsokhoz. Aki a Fritz-chip kulcsait kontrollalja, az Anderson szerint szörnyű hatalomra tehet szert. "Ez a köz- pontosított kontroll olyan, mintha mindenkinek ugyanahhoz a bankhoz kellene járnia, mindenkinek ugyanaz lehetne csak a könyvelője és az ügyvédje" - írta Anderson.

Erősödnek a monopóliumok. A szoftverfej- lesztő cégek megnehezíthetik a rivális cégek eletet, mert olyan kulccsal titkosíthatják dokumentumai- kat, amelyhez más szoftver nem fér hozza. Így el- képzelhető, hogy egy Microsoft Word dokumentumot más, konkurens szövegszerkesztő- vel nem lehet majd megnyitni. A legnagyobb hasz- not az IT piacon mar most is azok a cégek szerzik, amelyek sikeresen elterjesztettek egy platformot (mint például a Windows vagy a Word), es uraljak az azokkal való kompatibilitást, így el tudjak tenni a láb alól a konkurenciát.

Richard Stallman, a GNU szabadszoftver- kezdemenyezés alapítója a TCPA rendszert nem "megbízhatónak", hanem "árulónak" tartja, hiszen a tervek szerint a szamítógépek szisztematikusan nem fognak engedelmeskedni a felhasználó utasításainak. Szerinte ez a rendszer a Microsoft Windows kon- kurenciáját jelentő

nyílt forráskódú operációs rend- szerek létét veszélyezteti, mert előfordulhat, hogy nem is futtathatjuk majd őket.
Keveset tehetünk ellene Ha a rendszergazda nem konfigurálta a TCPA-t kötelezőnek, akkor ad- minisztrátori jogokkal "nem megbízható" alkalma- zásokat is lehet futtatni. A Fritz-chip azonban a kalózmásolatokat így is figyelni fogja. Az első Fritz- chipeket valószínűleg néhányan fel tudjak majd törni, de a második generációs lapkák már a pro- cesszorokba kerülnek.
A TCPA leírását 2000-ben tették közzé, és az Atmel vállalat már forgalmaz Fritz-lapkát. A lapka 2002 májusától az IBM Thinkpad noteszgé- pekben is megtalálható, valamint az X-box es a Win- dows XP is tartalmazott TCPA funkciókat (hardvercserénél újabb regisztráció szükséges, az eszközmeghajtókat hitelesíteni kell).

*

Világméretű megfigyelőhálózat épül Az emberek többsége talán úgy véli, hogy a drágán megvásárolt számítógép olyan eszköz, amely a megfelelő - és szabadon kiválasztott - szoftverek segítségével képes bizonyos számításokat elvégezni. A felhasználó bizonyára saját maga szeretné eldönteni, hogy a PC milyen feladatokat végezzen el, és a lehetőségek skálája igen széles: a pénzügyi elemzésektől kezdve az internetezésen keresztül a zenehallgatásig bármi szóba jöhet. A legnagyobb szórakoztatóipari és számítástechnikai vállalatok azonban szeretnék kalodába zárni a felhasználókat, hogy mindenki csak az általuk 'megbízhatónak' ítélt hardvereket, szoftvereket és fájlokat használhassa.

Az orwelli terv technikai megvalósításának már nevet is adtak, ez a Trusted Computing Platform Alliance (TCPA). A szövetség 1999 októberében jött létre a Compaq, a HP, az IBM, az Intel és a Microsoft kezdeményezésére, de azóta több mint 150 vállalat csatlakozott hozzájuk. E cégek közös célja az, hogy egy fejlett harverelemekre és szoftverekre épülő, biztonságos és megbízható számítógépes platformot hozzanak létre. Elképzeléseik szerint a jövőben az összes hardver igazodni fog a TCPA előírásaihoz, míg a szoftverek terén a Microsoft által

kifejlesztett Palladium (újabb nevén NGSCB, azaz Next Generation Secure Computing Base) fog gondoskodni a megbízhatóságról. Ki lesz nagyobb biztonságban? A TCPA rendszerében elsősorban azok a szoftverfejlesztők, kiadók, vállalatok és kormányok lesznek nagyobb biztonságban, amelyek dönthetnek majd a fájlok megbízhatóságáról. A felhasználók, az egyszerű alkalmazottak, a zenehallgatók - azaz a többség - még kiszolgáltatottabbak lesznek. Galántai Zoltán egyetemi docens, a Privacy International jogvédő szervezet vezetőségének tagja arra mutatott rá, hogy a szerzői joggal foglalkozó törvények világszerte egyre inkább azt tartják szem előtt, hogy mi a jó a tartalomtulajdonosoknak (és a fogyasztók, felhasználók érdekeire ügyet sem vetnek). Az 1998-as CTEA (Copyright Term Extension Act) például további 20 évvel terjesztette ki az USA-ban a copyrightvédelmet, és a jogvédők most attól tartanak, hogy ha ez 2018-ban lejár, akkor újra ki fogják terjeszteni (és így tovább a végtelenségig). A TCPA ugyanennek a felfogásnak a műszaki tükörképe: itt nem a jog, hanem a technika az, ami kizárólag a "hatalmon belül lévők" érdekeit védi. Galántai kérdésünkre elmondta, reális veszélyt lát a TCPA-ban, hiszen "azok az emberek, akik benyelték a Windowst, ezt is könnyen benyelhetik". Mindenre figyel a Fritz-chip A TCPA beépített felügyelő- és jelentőrendszerrel látja el a jövő asztali számítógépeit, egy alaplapra forrasztott hardverkulcs képében. A PC bootolása közben az úgynevezett "Fritz-chip" ellenőrzi, hogy a számítógépben megtalálható hardverelemek a TCPA által elfogadottak-e, a szoftverek hitelesítettek-e és hogy a komponensek mindegyikének érvényes-e a sorozatszáma. Az irányítást innentől az operációs rendszer rendfenntartó szoftvere veszi át - a Windows esetében a Palladium. A Fritz-chip képes egy harmadik félnek igazolást adni arról, hogy az adott PC alkalmas egy bizonyos DVD fogadására. Ezután a chip a kiadótól letölt egy kulcsot, amellyel az arra jogosult szoftverek képesek lejátszani a DVD-t, de a másolás szóba sem jöhet. (A megfigyelő chipet Fritz Holling dél-karolinai szenátorról nevezték el, aki fáradhatatlanul dolgozik a TCPA népszerűsítésén.) A fájlcserének annyi A szoftverfejlesztők, a film- és zenekiadók évek óta azt hangoztatják, hogy túlságosan elburjánzott az interneten az "illegális" fájlcsere, és (még több) pénzt szeretnének kapni a termékeikért. A TCPA tökéletesen alkalmas a digitális jogkezelésre (DRM, Digital Rights Management): olyan DVD-ket, szoftvereket, letöltéseket forgalmazhatnak, amelyeket nem lehet lemásolni. Ha valaki mégis "biztonsági másolatot" készít, akkor az interneten keresztül bármikor működésképtelenné tehetők a jogtalanul használt fájlok. Az alkalmazásra lesz

bízva, hogy milyen szabályok érvényesek az általa lejátszott fájlokra, a szabályokat pedig egy központi szerverről, a kiadótól tölti majd le a program. Ha egy vállalat úgy dönt, hogy egy CD meghallgatását csak tízszer engedélyezi, akkor azt egy gombnyomással elintézheti. Ross Anderson, a Cambridge Egyetem számítástechnikai laboratóriumának kutatója szerint az is elképzelhető, hogy a jövőben egy alkalomra szóló CD-t is lehet majd vásárolni, amelyet csak egy bizonyos napon - például valakinek a születésnapján - lehet lejátszani. A korrupció és a bűnözés melegágya A vállalatoktól és a kormányoktól kiszivárogtatott információkkal az újságírók semmit sem tudnak majd kezdeni, a számítógépük ugyanis nem fogja betölteni a titkosított dokumentumokat. A korrupt hivatalnokok így szinte bármit megtehetnek, nem kell félniük a lebukástól. Az alkalmazottak is kényes helyzetbe kerülhetnek, ha egy rossz főnöki döntés miatt hibát követnek el. Egy munkaügyi perben úgysem tudják majd bebizonyítani igazukat, ugyanis vagy nem férnek majd hozzá a korábbi utasításhoz, vagy az időzárral ellátott dokumentum már rég letörölte önmagát. Néhány funkciót a bűnözők is hasznosíthatnak: megoldhatják, hogy a kábítószer-szállítmányokról szóló táblázatokat csak a felhatalmazott számítógépeken lehessen olvasni, és az adatok minden hónap végén megsemmisüljenek. Ez megnehezíti a bűnüldöző szervezetek dolgát, bár a Microsoft tárgyal a kormányzatokkal arról, hogy a rendőrök és a kémek kapjanak-e hozzáférést a főkulcsokhoz. Aki a Fritz-chip kulcsait kontrollálja, az Anderson szerint szörnyű hatalomra tehet szert. "Ez a központosított kontroll olyan, mintha mindenkinek ugyanahhoz a bankhoz kellene járna, mindenkinek ugyanaz lehetne csak a könyvelője és az ügyvédje" - írta Anderson. Erősödnek a monopóliumok A szoftverfejlesztő cégek megnehezíthetik a rivális cégek életét, mert olyan kulccsal titkosíthatják dokumentumaikat, amelyhez más szoftver nem fér hozzá. Így elképzelhető, hogy egy Microsoft Word dokumentumot más, konkurens szövegszerkesztővel nem lehet majd megnyitni. A legnagyobb hasznot az IT piacon már most is azok a cégek szerzik, amelyek sikeresen elterjesztettek egy platformot (mint például a Windows vagy a Word), és uralják az azokkal való kompatibilitást, így el tudják tenni a láb alól a konkurenciát. Richard Stallman, a GNU szabadszoftver-kezdeményezés alapítója a TCPA rendszerét nem "megbízhatónak", hanem "árulónak" tartja, hiszen a tervek szerint a számítógépek szisztematikusan nem fognak engedelmeskedni a felhasználó utasításainak. Szerinte ez a rendszer a Microsoft Windows konkurenciáját jelentő nyílt forráskódú operációs rendszerek létét veszélyezteti, mert előfordulhat, hogy

nem is futtathatjuk majd őket. Keveset tehetünk ellene Ha a rendszergazda nem konfigurálta a TCPA-t kötelezőnek, akkor adminisztrátori jogokkal "nem megbízható" alkalmazásokat is lehet futtatni. A Fritz-chip azonban a kalózmásolatokat így is figyelni fogja. Az első Frizt-chipeket valószínűleg néhányan fel tudják majd törni, de a második generációs lapkák már a processzorokba kerülnek. A TCPA leírását 2000-ben tették közzé, és az Atmel vállalat már forgalmaz Fritz-lapkát. A lapka 2002 májusától az IBM Thinkpad noteszgépekben is megtalálható, valamint az X-box és a Windows XP is tartalmazott TCPA funkciókat (hardvercserénél újabb regisztráció szükséges, az eszközmeghajtókat hitelesíteni kell).