Intelligens kártyák biztonsági modelljei

Bruce Schneier
Counterpane Systems
schneier@counterpane.com

Adam Shostack
Netect, Inc.
adam@netect.com

1999. október 19.

Kivonat

A smart card rendszerek abban különböznek a hagyományos számítógépes rendszerektől, hogy az egyes összetevők nincsenek egy megbízható egységen belül. A processzor, az I/O, az adatok, a programok és a hálózat különböző, ellenséges csoportok ellenőrzése alatt állhatnak. A következőkben ezeknek a megbízhatósági határoknak a hatását vizsgáljuk a biztonság szempontjából. Látni fogjuk, hogy ezek ismerete alapvető fontosságú a Smart Card rendszerek biztonságának megértéséhez.

Magyar fordítás

A fordítást Bruce Schneier és Adam Shostack *„Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards"* című cikke alapján Lécz Pál (zeewolf@inf.elte.hu) készítette. A fordítást Kincses Zoltán (kincses@ludens.elte.hu) lektorálta.

Az eredeti cikk a http://www.counterpane.com/smart-card-threats.html címen olvasható.

1. Bevezetés

A smart card egy hitelkártya méretű eszköz, amelybe egy chip-et ágyaznak (ez tartalmaz egy processzort, RAM-ot és ROM-ot). A biztonságtechnikában sokan varázsszernek tekintik, és a legkülönbözőbb helyekre javasolják és alkalmazzák őket (beléptető rendszerek, elektronikus kereskedelem, azonosító rendszerek, stb.) Ugyanakkor kevesen vizsgálják ezeknek az eszközöknek az alkalmazásával járó biztonsági kockázatokat, és azokat a speciális fenyegetéseket amelyekkel ezeknek a rendszereknek számolniuk kell.

Ebben a cikkben az adott alkalmazástól függetlenül vizsgáljuk a smart card rendszerek biztonságát. Kitérünk a kártyák egyik legfontosabb tulajdonságára - ez egy olyan processzorral és memóriával rendelkező egység amelynek nincs módja kommunikálni a környezetével - és rámutatunk arra, hogy ezek a tulajdonságok miért tesznek egy smart card rendszert kockázatosabbá egy hasonló, független számítógépeket alkalmazó rendszernél. Példa erre egy olyan személy akinek a számítógépe valaki más irányítása alatt áll. Ez egy számítógép esetén nem

hétköznapi eset, de a smart card-ok esetében gyakori. Megmutatjuk, hogy sok alkalmazás esetén a kártyák biztonságos felhasználásához nem úgy kell tekinteni őket, mint egy megbízható számítási környezetet, hanem mint adathordozókat, amleyek korlátozott számítási kapacitással is rendelkeznek.

1.1. A számítógépektől az intelligens kártyákig

Az intelligens kártyákat fenyegető veszélyeket úgy a legkönnyebb megérteni, ha először a hagyományos asztali gépekre leselkedő veszélyekkel kezdjük. A legfontosabb biztonsági szempont amelyet a kártyákkal, mint valamilyen protokoll résztvevőivel szemben vizsgálnunk kell az, hogy miben különböznek a többi számítási kapacitással rendelkező eszközöktől. Egy számítógépet alapul véve és fokozatosan lebontva olyan részekre amelyek megfelelnek egy kártyának és annak a környezetnek amelyben a kártyának működnie kell, megvizsgálhatjuk az egyes változtatásokat és ezek hatását a biztonságra. A felbontás minden egyes lépése újabb és újabb lehetőségeket kínál a támadásra. Vegyük például azt az esetet, amikor a kártyát birtokló személynek nincs joga hozzáférni a kártyán lévő adatokhoz. Ez kiteszi a kártyát a kartyát birtokló személy által a kártyán elhelyezett adatok ellen intézett támadásoknak. Ilyesmiről nem lehet szó, ha a kártya birtokosa rendelkezhet a kártyán lévő adatok felett.

A mi általános számítógép-modellünk rendelkezik egy processzorral, valamilyen adattárral, I/O egységekkel, és tápegységgel. A processzor feladata a számítások elvégzése. Egy hagyományos számítógép esetén a CPU szoros kapcsolatban áll a tárral (ez lehet RAM, disk vagy akár szalag), a kimeneti és a bemeneti kapcsolatot biztosító egységekkel (billentyűzet, egér, terminál, printer vagy más kommunikációt lehetővé tevő kapcsolat, például soros port vagy Ethernet kártya). Ebben az esetben a számítógépet egy egységnek tekinthetjük a legtöbb fenyegetéssel szemben.

Kezdjük a gép miniatűrizálásával. Ezután szükségünk lesz valamilyen használható megjelenítő eszközre. Vegyünk például egy REX elekronikus noteszt. Ez egy PC-CARD amin van egy kis képernyő, egy PC-CARD interface, hogy kommunikálhasson egy másik számítógéppel, és néhány gomb az adatok bevitelére. Csináljunk a REX-ből több lépésben smart card-ot, és nézzük meg, hogyan válik az egyes lépések után egyre könnyebben támadhatóvá.

Cseréljük ki az I/O portot egy lassú soros porttal. A rendszer, amelyhez az egység csatlakozik, csak korlátozott mértékben képes azt támadni, mivel valószínűleg csak a tulajdonos saját számítógépéhez lesz csatlakoztatva, esetleg egy másik hasonló egységhez információcsere céljából. Ezalatt a berendezés információkat küldhet és fogadhat a képernyőjén és a billentyűzetén keresztül. Nem lenne nehéz egy REX-hez hasonló dologot biztonságos elektronikus csekkfüzetté alakítani. Lennének persze más tervezési nehézségek, de egyszerűbb lenne, mintha smart card-ra építenénk a rendszert.

Folytassuk a beviteli egység leválasztásával. Ezek után az adatok beviteléhez egy külső billentyűzetet kell csatlakoztatni. Nyilvánvaló, hogy a billentyűzet rögzítheti pl. a PIN kódot vagy más információkat amelyeket egy támadó később felhasználhat. Végül távolítsuk el a képernyőt, így az egység már csak valamilyen külső képernyőt használhat az adatok megjelenítésére amelyről viszont nem tudjuk, hogy mennyire hűen jeleníti meg azokat.

Az intelligens kártyák legfontosabb jellemzője, hogy „hátrányos helyzetűek" abból a szempontból, hogy képtelenek a külvilággal valamilyen külső egység segítsége nélkül kommunikálni. Ez az intelligens kártyák egyik alapvető jellemzője,

ebben különböznek az olyan hordozható számítógépektől, mint pl. a Palm Pilot. Ez a tulajdonság határozza meg a biztonsági modelljét annak a környeyetnek, amelyben a kártyának működnie kell. Más funkcionális megszorítás is elképzelhető, de a legfontosabb ez az I/O korlátozás.

A kártyák működése más szempontból is lehet korlátozva. Lehet, hogy a kártyabirtokos semmilyen ellenőrzéssel nem rendelkezik a kartyán futó programok felett. A multifunkciós kártyák esetén az is elképzelhető, hogy a kártya kibocsátója sem. Az is lehetséges, hogy a kártyán tárolt információk tulajdonosa nem azonos a kártyabirtokossal, és az adat tulajdonosa előírhatja, hogy a kártyabirtokos ne tudja az adatokat módosítani, vagy akár kiolvasni se.

A következő fejezetekben megvizsgáljuk a fenti, és más hasonló, a smart card rendszerekben gyakori korlátozások következményeit. A modellünkben gyakran öt vagy hat résztvevő is szerepel. Részletesen tárgyaljuk, hogy a szerepek részekre bontása során hogyan keletkeznek újabb és újabb támadási felületek, és ezt kihasználva hogyan támadhatnak egymásra a szereplők. Azt is vizsgáljuk, mi motiválhatja arra a résztvevőket, hogy a szerepek szétválása után megpróbálják kijátszani egymást. Végül a különböző védelmi módszerek kerülnek sorra.

2. Intelligens kártyák biztonsági modellje

Egy smart card alapú rendszerben a működés során sok szereplő kerül egymással kapcsolatba. Általában legalább öt vagy hat, köztük a kártyabirtokos, a kártyakibocsátó, a kártya előállítója, az adatok tulajdonosa, a programfejlesztő, és valamilyen terminál.

- A **kártyabirtokos** az a személy akinél nap mint nap ott van a kártya. A zsebében tarthatja, eldöntheti hogy mikor használja, vagy hogy használja-e egyátalán. Ha a kártya elektronikus igazolványként működik, akkor ő az, akinek az igazolványt kiállították. A rendszertől függően esetleg rendelkezhet a kártyán lévő adatok felett, de nem valószínű, hogy befolyásolhatta azokat a protokollokkal, szoftverekkel, hardverrel kapcsolatos döntéseket amelyeket a rendszer tervezésekor hoztak. Ezzel ellentétben a legtöbb számítógépes rendszer esetén a tulajdonos és a felhasználó dönthet a rendszerrel kapcsolatos kérdések egy részében.

- Az **adattulajdonos** az, aki a kártyán lévő adatok felett rendelkezhet. Ha például a kártyát digitális bizonylatok (certificate) hordozójaként alkalmazzák, akkor a kártyabirtokos egyben az adatok tulajdonosa is. Ha a kártya egy elektronikus pénztárca, akkor a kártya kibocsátója az adattulajdonos, és ez a különbség lehetőséget és okot ad a támadásra.

- A **terminál** egy olyan eszköz, amelynek segítségével kapcsolat jöhet létre a kártya és a külvilág között. A terminál vezérel minden a kártyáról kiinduló vagy a kártya felé irányuló adatforgalmat. A billentyűzetet, amellyel adatokat lehet bevinni a kártyába, és a képernyőt, amely a kártya által küldött adatokat megjeleníti. Telefonkártya esetén ez a telefonkészülék tulajdonosa, bankkártya esetén az ATM üzemeltetője (illetve az ő irányításuk alatt áll a

terminál). Ha egy TV-csatorna előfizetői kártyájáról van szó, akkor a terminál a set-top box.[1]

- A kártya **kibocsátója** az aki kiadja a kártyát. Ő rendelkezik a kártyán lévő operációs rendszer és a kártyára kezdetben felkerülő adatok felett. Ha telefonkártyáról van szó, akkor a telefontársaság a kibocsátó. Egy alkalmazottak számára kiadott azonosítókártya esetén ez az alkalmazó cég. Egyes esetekben a kibocsátó csak a kártya kiadásával vesz részt a rendszer működésében, máskor végig jelen van a rendszer egészében. Néhány multifunkciós kártya esetén a kibocsátónak semmi köze a kártyán futó alkalmazásokhoz, csak az operációs rendszerhez. Más multifunkciós kártyáknál a kibocsátó rendelkezhet a kártyán futó összes alkalmazásról.

A biztonsági elemzés szempotjából gyakran az a legegyszerűbb, ha a kártya kibocsátóját, a gyártót és a programozókat egy szereplőnek tekintjuk, ez az eset azonban meglehetősen ritkán fordul elő.

- A kártya **gyártója** az aki előállítja magát a kártyát. Valójában ez is egy egyszerűsítés, hiszen nem feltétlenül a kártya gyártója a tulajdonosa annak a gyárnak ahol a chip-eket előállítják; lehet, hogy a tervezés során alvállalkozók végeztek bizonyos munkákat, vagy az előállítás során használnak máshonnan származó eszközöket. Ennek ellenére mindezt egy szereplővel, a kártyagyátóval modellezzük. Sok helyen és sokak számára nyílik lehetőség a gyártási folyamatba történő beavatkozásra.
- A **programozó** az aki a kártyára kerülő szoftvereket előállítja. Ez ismét egy egyszerűsítse a fordító- és egyéb segédprogramok, stb. készítőiből álló valószínűleg bonyolult hálózatnak. Itt is ugyanazok a megbízhatósággal kapcsolatos kérdések [Tho84] merülnek fel, mint a kártya gyártásakor.

3. A bizalom megoszlása a smart card rendszerekben

A következőkben néhány jellemző smart card alapú rendszert mutatunk be abból a szempontból, hogy a rendszer egyes összetevői kinek az ellenőrzése alatt állnak. A lista nem teljes, találhatunk más példákat az itt felsorolt megosztásokra, és léteznek olyan megosztások amelyek itt nem szerepelnek.

- **Digitális pénztárca (Digital Stored Value Card)** Ezeknek a kártyáknak a célja a készpénz helyettesítése, vagyis fizetni lehet velük. Ilyen például a Mondex vagy a VisaCash. A kártyabirtokos a vásárló. A terminál a kereskedőnél van. Az adatok tulajdonosa és egyben a kártya kibocsátója az a pénzintézet amelyik a rendszert üzemelteti.

[1] A két utóbbi példa - a bankkártya és a TV előfizetői kártya - példa arra az esetre, amikor a terminál több szereplőre bontható. A bankkártya esetében gyakori, hogy a művelet során egy másik bank ATM-jét és hálózatát kell igénybe venni, ami azt jelenti, hogy a kártyát kibocsátó bank nem tekintheti ezeket a rendszer megbízható komponenseinek. A TV kártya esetén a terminált hosszabb ideig az előfizető birtokolja, ezzel lehetősége nyílik arra, hogy az otthona biztonságában és kényelmében intézzen támadást a terminál ellen. Azokban az esetekben amikor a terminál tulajdosa, programozója, birtokosa (vagy bárki aki a terminál valamilyen funkciója fölött ellenőrzést gyakorolhat) nem egy személy, akkor részletesen elemezni kell, hogy ez a különbség miként befolyásolja a biztonságot.

- **Digitális csekkfüzet (Digital Check Card)** Ezek megegyeznek az előző típussal, kivéve, hogy a kártyabirtokos az adatok tulajdonosa.
- **Előre fizetett telefonkártya (Prepaid Phone Card)** Ezek az első típusba tartozó speciális kártyák. A kártyabirtokos a vásárló. A terminál tulajdonosa, az adattulajdonos és a kártyakibocsátó pedig a telefontársaság.
- **Számla alapú telefonkártya (Accout-based Phone Card)** Ebben a rendszerben a kártya nem tárolja a számlaegyenleget, csak egy számlaszámot amellyel azonosítani lehet a számlát a háttérben lévő adatbázisban. A kártyabirtokos és az adatok tulajdonosa a vásárló, míg a terminál tulajdonos és a kibocsátó a telefontársaság.
- **Hozzáférési kulcs (Access Token)** Ennél az alkalmazásnál a kártya egy kulcsot tartalmaz, amelyet valamilyen login vagy authentikációs protokollhoz használnak. Egy cég esetén a kártyabirtokos az alkalmazott, az adatok és a terminál a vállalat tulajdonában vannak, és ő a kártyakibocsátó is. Többfelhasználású kulcs esetén a kartyabirtokos és az adattulajdonos lehet ugyanaz a a személy, míg a terminál lehet egy kereskedő tulajdona és az adattulajdonos pedig valamilyen pénzintézet.
- **Web-böngésző kártya (Web Browsing Card)** A kártyát a birtokosa a saját számítógépében az Interneten történő vásárlásainak kifizetésére használhatja. Ez is az elektronikus pénztárca egy típusa. A különbseg az, hogy a kártya birtokosa és a terminál tulajdonosa ugyanaz a személy (a számítógép gazdája). Az adatok tulajdonosa és a kártya kibocsátója a pénzintézet.
- **Digitális bizonylat-kártya (Digital Credential Device)** Ezeken a kártyákon digitális bizonylatokat (certificate) vagy másféle tanúsítványokat tárolnak, hogy azokat a kártyabirtokos bemutathassa egy másik félnek. Itt az adattulajdonos és a kártyabirtokos ugyanaz a személy. A terminál tulajdonosa lehet a másik fél, akinek a bizonylatot bemutatják vagy a kártyabirtokos. A kártyakibocsátó az a hitelesítő szervezet amely kibocsátotta a bizonylatokat, vagy az aki osszegyűjtötte őket.
- **Kulcstároló kártya (Key Storage Card)** Ebben az esetben különböző (lehetőleg ellenőrzött) nyilvános kulcsokat helyeznek a kártyán biztonságba, így elkerülve a kevésbé biztonságos PC-n történő tárolást. A kártyabirtokos, az adattulajdonos és a terminál tulajdonosa ugyanaz a személy.
- **Multifunkciós kártya (Multi-function Card)** Ez a legbonyolultabb kártyatípus. A kártya gyártója, kibocsátója és az alkalmazásfejlesztő mind különböző szereplők. Egyes adatok a kártyabirtokos tulajdonában lehetnek, míg más adatok tulajdonosai egyéb szereplők. A kártyán lévő alkalmazásoktól függően több terminál tulajdonos is lehetséges.

4. A kártyákat fenyegető veszélyek modelljei

A támadást úgy definiálhatjuk, mint csalást, amelyet a kártyás tranzakció egy vagy több szereplője próbál meg elkövetni. A támadók két típusát különböztethetjük meg, az egyik a rendszer szereplője, a másik külső beavatkozó. Rendszeren

belüli támadás esetén például elképzelhető, hogy a kártyabirtokos próbálja meg becsapni a terminháltulajdonost, a kártya kibocsátója a kártyabirtokost, stb. A külső támadó lehet egy ideiglenesen kártyát birtokló személy aki ellopja a kártyát a jogos tulajdonostól, kicseréli a terminált vagy az azt működtető szoftvert. A külső támadások gyakran hasonlóak a hagyományos számítógépek protokolljai ellen irányuló támadásokhoz, de itt a támadók kihasználhatják a rendszer azon tulajdonságait, amelyek a szerepek szétválasztása miatt jelennek meg a rendszerben.

A támadási okok néhány nagyobb csoportba oszthatók [Sch97]. Az első és egyben a legnyilvánvalóbb ok az anyagi haszon, ide tartozik a pénz vagy a hitelkeret ellopása, vagy a nyilvános szolgáltatások fizetés nélküli igénybevétele például telefonkártyákkal történő csalások esetén. A következő csoportba a személyazonossággal kapcsolatos támadások tartoznak, amikor maga a kártya csak egy közbülső célpont, a támadó célja pedig az, hogy hozzáférést szerezzen valamilyen számítógépes rendszerhez vagy más korlátozott hozzáférésű szolgáltatáshoz. Ezek az esetek abban különböznek az első típustól, hogy a támadó legálisan nem is tudná megvásárolni a szolgáltatást. Például használhat valaki lopott kártyát, hogy bejusson egy számítógéprendszerbe; általában a rendszerekhez történő hozzáférés elérhető, de a támdó célpontja egy bizonyos rendszer. Léteznek a titkos adatok megszerzésére irányuló támadások, amikor egy szereplő több adatot akar megszerezni, mint amennyit az adott protokoll lehetővé tesz. Az utolsó csoportba tartoznak azok a támadások amikor a támadó célja nem az anyagi haszon, hanem a nyilvánosság figyelmét akarja magára irányítani, valamiféle hírnévre szeretne szert tenni.

5. A támadások osztályozása

A kártyás rendszerek sok szereplője miatt sokféle támadási lehetőséget kell figyelembe venni. A mi célunk, hogy a támadásokat a funkciók megoszlása alapján osztályozzuk, ezért sorra vesszük a támadásokat, amelyeket a rendszer résztvevői egymás ellen intézhetnek. Ezek legtöbbje egy szokásos számítógépes rendszerben nem lehetséges, mivel a hagyományos gépek biztonsági határain belül kellene őket végrehajtani. A smart card világban azonban lehetségesek.

5.1. A terminháltulajdonos támadásai a kártyabirtokos vagy az adattulajdonos ellen

Ezeket a támadásokat a legkönnyebb megérteni. Amikor a kártya felhasználója behelyezi a kártyát egy terminálba, akkor bízik abban, hogy a terminál a pontosan továbbítja a kártya felől illetve a kártya felé irányuló adatokat. Például ha egy elektronikus pénztárca birtokosa 1 dollár értékben vásárol egy automatából, akkor arra számít, hogy az automata az ,,1 dollár levonás" parancsot küldi a kártya felé, és nem a ,,10 dollár levonás" parancsot. Ugyanígy, amikor a kártya az ,,Egyenleg: 1 dollár" üzenetet próbálja meg a birtokosa felé továbbítani (a terminálon keresztül), arra számít, hogy a terminál pontosan ezt is jeleníti meg. Ebben a környezetben egy csaló terminál nagy valószínűséggel képes kárt okozni, ráadásul a kártyabirtokops sem tudja érzékelni a csalást amíg csak ezzel az egy terminállal áll kapcsolatban. Hamis ATM-ek felhasználásával már előfordult ilyen típusú csalás.

A legtöbb rendszerben a megelőzési módszerek azon alapulnak, hogy a terminál csak rövid ideig fér hozzá a kártyához. A kártya szoftvere korlátot szabhat

a csaló terminálok által okozható kárnak. Egy elektronikus pénztárca esetében az egy tranzakcióval levonható összeget maximálhatja 1 dollárban, a tranzakciók számát pedig percenként 1-re korlátozhatja [KS99]. Más védelmi módszerek a kártyabirtokos tulajdonába adják a terminált, például valamilyen számítógéphez kapcsolható perifériaként. Az igazi vedelmi mechanizmusoknak azonban semmi közük a kártya-terminál kapcsolathoz, ezek háttérfeldolgozó rendszerek amelyek a terminálokat és a kártyákat figyelve jelzik a gyanús viselkedést.

5.2. A kártyabirtokos támadásai a terminál ellen

A kártyabirtokos terminál elleni támadásai ennél kifinomultabbak. Ezeknél hamis vagy módosított kártyákat használnak olyan szoftverrel, amellyel megpróbálnak a kártya és a terminál közötti protokollba beavatkozni. Erre [McC96]-ban találhatunk néhány példát.

Egy jól megtervezett protokollal csökkenthető az ilyen támadásokkal járó kockázat. Még nehezebbé tehetik a támadó dolgát a kártya nehezen hamisítható fizikai jellegzetességei (például a Visa és a MasterCard kártyáin található hologram) amelyeket a terminál tulajdonosa saját kezűleg ellenőrizhet. Fontos, hogy a szoftver digitális aláírása itt nem segít, mivel a csaló kártya adhat hamis aláírást, és a terminálnak nincs arra lehetősége, hogy belenézzen a kártya belsejébe. Az ezen támadások elleni védekezéshez egy újabb funkciómegosztásra van szükség: a kártyabirtokosnak nem szabad megengedni, hogy módosíthassa a kártyán tárolt adatokat.

5.3. A kártyabirtokos támadásai az adattulajdonos ellen

Sok smart card alapú üzleti rendszerben szükség van arra, hogy a kártyán tárolt adatokat megvédjük a kártya tulajdonosával szemben. Bizonyos esetekben a kártya birtokosa nem ismerheti az adatokat, például egy épület beléptető rendszere esetén a kártya tárolhat valamilyen titkos kódot, amelynek ismeretében a kártya birtokosa újabb kártyákat készíthetne. Elektronikus kereskedelmi rendszerekben a kártyán tárolt titkos kulcs ismerete tisztességtelen tranzakciókat tenne lehetővé. Más esetekben a kártya birtokosa megismerheti a tárolt adatokat, de nem módosíthatja őket. Ha egy elektronikus pénztárca tulajdonosa módosíthatná a kártyán tárolt összeget, akkor gyakorlatilag pénzt állíthatna elő.

Az ide sorolható támadásokkal kapcsolatban két fontos jellemzőt kell kiemelni. Először is a kártyának olyan biztonságos tárolóként kell működnie, ami meggátolja a birtokosát az adatokhoz való hozzáférésben. Ebben a tekintetben a kártyának nagy biztonsággal érzékelnie kell az ilyen támadásokat, és ezekre megfelelő választ kell adnia. Másodszor, a támadó a számára legelőnyösebb körülmények között próbálkozhat. Magával viheti a kártyát egy jól felszerelt laborba, ahol tetszése szerint kísérletezhet vele, akár tönkre is teheti annak érdekében, hogy megtudja, hogyan működik.

Sok sikeres, a kártyán tárolt adatok ellen intézett támadás ismert. Ezek között van visszafejtés, a fizikai integritás védelmének hatástalanítása [AK96], hibaelemzés [BS97, BDL97], a teljesítményfelvétel és az időzítések elemzése [Koc96, Koc98b, KSWH98b, DLK+99].

Ezek a támadások különösen hatásosak voltak az előfizetéses TV-kártyák esetében [McC96, Row97], és gyakran használták őket mobiltelefonok kártyái el-

len is [BGW98]. Az elektronikus pénztárcák és más kereskedelmi kártyák területén most kezdenek megjelenni [Row97].

5.4. A kártyabirtokos támadásai a kártya kibocsátója ellen

Sok üzleti célú támadás esetén úgy tűnhet, hogy a célpont a kártya kibocsátója, de gyakran ez csak a látszat. A támadás valójában a kártyán tárolt adatok vagy szoftverek integritása illetve hitelessége ellen irányul. Az ilyen támadások úgy válnak lehetővé, hogy a kártyakibocsátó úgy dönt, hogy saját vagy harmadik fél tulajdonát képező adatokat tárol a kártyán. Vegyünk például egy telefonkártya-rendszert. Ha olyan számlaalapú rendszert használunk, ahol egy kártya egy számlaszámot tartalmaz amelyet a telefontársaság arra használ, hogy azonosítson vele egy háttérben nyilvántartott számlát, akkor megjelennek a számlaszámokon alapuló támadások (a számlaszámok ellopása vagy kitalálása). Egy ilyen rendszer kiegészíthető egy challenge/response eljárással vagy egy inverz hash függvénnyel, így visszajátszás ellen védett jelszavak küldése is lehetséges. Az eredmény egy erősen kártyaközpontú rendszer a háttérben egy irodai irányítású védelmi rendszerrel ami a csalásokat hivatott megakadályozni. Ha a kártyakibocsátó úgy dönt, hogy a rendszer felhasználóit azonosító adatokat a kártyán helyezi el, nem csodálkozhat, ha ezeket az adatokat megpróbálják megszerezni. Ezek az adatok lehetnek azonosító számlaszámok, de ide tartoznak azok a rendszerek is, ahol a kártyára egy kulcsot rejtenek abban bízva, hogy ezt nem lehet kiolvasni és a protokollnak megfelelő kommunikáció annak a jele, hogy a kártyát nem módosították. Ezen rendszerek biztonsága azon az erősen megkérdőjelezhető feltevésen alapszik, hogy a kártyát fizikailag védő biztonsági megoldások elegendőek.

5.5. A kártyabirtokos támadásai a szoftvergyártó ellen

Általában azokban a rendszerekben ahol a kártyát egy potenciálisan akár ellenséges felhasználó kezébe adják, azzal a feltételezéssel élnek, hogy a kártyára nem kerül új szoftver. A kártya kibocsátása előtti gyártási fázisokban alkalmazott egyirányú transzformációkkal próbálják meg biztosítani, hogy a szoftvert ne lehessen módosítani. A háttérben feltételezik, hogy a kártya birtokosa és a szoftver fejlesztője között nem lehet olyan kapcsolat amely támadási lehetőséget teremt. Ugyanakkor a tapasztalat azt mutatja, hogy a támadók képesek elérni, hogy (gyakran akár ingyen is) megkapják azokat a hardvereszközöket, amelyekre a támadáshoz szükségük van.

5.6. A terminháltulajdonos kártyakibocsátó elleni támadásai

A kívülállók számára zárt rendszerekben, mint a telefonkártyák esetén, a terminál tulajdonosa egyben a kártya kibocsátója (ez esetben a telefontársaság). Más, nyitottabb rendszerek esetén, mint például a Mondex a terminháltulajdonos egy kereskedő, a kártyakibocsátó pedig a Mondex. Ez a szerepmegosztás egyben új támadási felületet is jelent.

A terminál felelős a kártya és a kártyakibocsátó (illetve a háttérben lévő rendszer) közötti összes kommunikációért. Ebben a rendszerben a terminál bármikor előállíthat hamis tranzakciókat, vagy ,,elfelejtheti" a valós tranzakciók rögzítését. Ezen kívül kihagyhatja a tranzakció egyes lépéseit így segítve valamilyen csalást, vagy csak azért, hogy ezzel nehézségeket okozzon a kibocsátó számára a szolgáltatás

teljesítésében. Becsaphatja a kibocsátót azzal, hogy nem terheli meg a kártyát a szolgáltatás árával, vagy például egy telefonkártya esetén komoly problémákat okozhat azzal, hogy elvégzi a megterhelő tranzakciót, de nem teljesíti a szolgáltatást.

Ezen támadások esetén nincs jelentősége annak, hogy a rendszerben smart card-ot alkalmazunk, ezek ugyanis a kibocsátó és a terminál közötti kapcsolat ellen irányulnak. Egyes rendszerek úgy próbálnak ez ellen védekezni, hogy a terminálon keresztül egy biztonságos kapcsolatot építenek ki a kártya és a háttérben működő számítógépes rendszer között. A háttérben lévő gépen gyakran monitoring szolgáltatás is futtatnak, hogy minél kisebb esélye legyen az ilyen típusú támadásoknak a sikerre.

5.7. A kártyakibocsátó támadásai a kártyabirtokos ellen

Általában a legtöbb rendszer esetén feltesszük, hogy a kártyakibocsátók a kártyabirtokosok érdekeit tartják a legfontosabbnak. Ez nem feltétlenül igaz, és egy rosszindulatú kártyakibocsátó számára több lehetőség is adódik, ha meg akarja támadni a kártyabirtokosokat.

Ezeknek a támadásoknak a célja legtöbbször valamilyen bizalmas információ megszerzése. A készpénzt helyetesítő kártyákat nagyon körültekintően kell megtervezni abból a szempontból, hogy megőrizzük a készpénzre jellemző anonimitást és visszakövethetetlenséget. A támadások és a tervezési hibák jelentősen lecsökkenthetik a rendszer biztonságát. Másrészt az is előfordulhat, hogy egy olyan rendszert próbálnak eladni, amely jóval kisebb biztonságot nyújt, mint ahogy azt állítják róla, és lehetővé teszi a kibocsátó számára, hogy titokban adatokat gyűjtsön a kártyáit használókról.

A rendszer fejlődése során bevezetésre kerülő új lehetőségek módosíthatják a rendszer kezdeti jellemzőit és jelentős hatásuk lehet a biztonságra is. Ezek a kibocsátó által indított támadásnak is tekinthetők, mivel a kártyabirtokos a legritkább esetben tájékozódhat a kibocsátó által bevezetett változtatás biztonságot érintő hatásairól. Ezek a változtatások legtöbbször nem csak opcionálisak a vásárló számára: az egyetlen alternatíva a elfogadásukkal szemben a rendszerből történő kilépés. Ilyen típusú támadásokat nem csak a kártyakibocsátó, hanem a hardver vagy a szoftver tervezője is végrehajthat a terminháltulajdonosok közreműködésével, a kibocsátó tudta nélkül.

5.8. A gyártó támadásai az adatok tulajdonosa ellen

A gyártók által alkalmazott bizonyos megoldások jelentős hátrányt okozhatnak a rendszerben szereplő adatok tulajdonosai számára. Egy biztonságos többfelhasználós számítógép megtervezése nem könnyű feladat, és nem megoldott az a probléma sem, hogyan kell olyan kernelt tervezni ami képes a futó folyamatokat megvédeni egymástól. Egy olyan operációs rendszer létrehozása ami megengedi esetleg kifejezetten támogatja, hogy több felhasználó futtathasson programokat ugyanazon a kártyán, több új biztonsági kérdést is felvet.

Az első és egyben a legnyilvánvalóbb az operációs rendszerbe és ezen keresztül a többi alkalmazásba történő beavatkozás kérdése. Ez az a terület, ahol a nagy, ismert operációs rendszerek gyártói képtelenek voltak jó megoldásokkal előállni az utóbbi 30 évben. Ugyanígy a smart card operációs rendszerek készítői sem dicsekedhetnek irigylésre méltó eredményekkel. Mindenesetre még ha a kártya operációs

rendszerét sikerülne is biztonságossá tenni, a felhasználói felülettel kapcsolatos biztonsági kérdések továbbra is megoldatlanok a kártyák hiányosságai miatt. Honnan tudhatja a felhasználó (vagy a tervező), hogy milyen program fut amikor a kártyát egy terminálba helyezik? Hogyan győződhet meg a program arról, hogy egy valódi terminállal kommunikál, és nem egy másik programmal? Ha egy program azt érzékeli, hogy módosították, hogyan tud biztonságosan leállni, és hogyan jelezheti kifelé a leállást és annak okát? Meg kell-e egyátalán próbálnia? Milyen érdekes támadási módokat tesz lehetővé, ha a kártya valamilyen jelzést ad közvetlenül azt megelőzően, hogy megsemmisíti magát? Honnan tudhatja a kártya, hogy egy ilyen jelzés továbbítása után a memória törlése valóban megtörtént, ha a tápellátást a támadó biztosítja számára?

Kevésbé nyilvánvalóak a szándékosan rossz véletlenszám-generátorral [KSWH98a] vagy más kriptográfiai szempontból fontos részek implementációjával kapcsolatos kérdések, mivel ezek hatásainak a felmérése és tesztelése is nehéz feladat [Sch97, Sch98a, Koc98a, Sch98a]. Az ún. kleptográfiai* támadások végrehajtásának szempontjából a gyártó irigylésre méltó helyzetben van [YY96, YY97a, YY97a]. A nagy kártyagyártók közül egy sem tud felmutatni olyan operációs rendszert amelyben ne lennének kihasználható hibák. Ezen kívül a legkülönbözőbb protokollok implementálása során is olyan helyzetben vannak, hogy különféle rejtett csatornákon keresztül kiszivárogtathatják az alkalmazások által használt kulcsokat [KSW96].

Végül egy alkalmazás tönkretehet egy másik, ugyanazon a kártyán futó alkalmazást. Megmutatták, hogy lehetséges egy megbízható protokollhoz készíteni egy másik, szintén megbízható protokollt úgy, hogy a második protokoll segítségével az első feltörhetővé válik, ha ugyanazt az eszközön futnak és ugyanazokat a kulcsokat használják.

6. Szerepcserés támadások

A támadásoknak ez az osztálya azon alapul, hogy a rendszer szereplőit fizikailag elválasztják egymástól, vagy megváltoztatják a résztvevők a szerepét. Például a kártyabirtokos kicserélése a kártya ellopásával hozzáférhetővé teszi a kártyabirtokos által tárolt adatokat, vagy ActiveX komponensek segítségével a támadó gyakorlatilag a terminál tulajdonosává válhat, így lehetővé válnak számára azok a támadási módok amelyeket a terminál tulajdonosa alkalmazhat.

Ezeknek a támadásoknak a lényege az, hogy valamelyik szereplő megváltozik, és a tevékenységét ezután olyan okok motiválják, amelyeket ettől a szereplőtől nem vártunk. Amikor egy kártyát ellopnak a kártya új birtokosa (a tolvaj) már nem érdekelt a számla biztonságának vagy akár a kártya fizikai integritásának megőrzésében. Amikor a támadó beavatkozik egy terminál működésébe akkor a terminál a rendszerben való szabályos részvétel helyett arra törekszik, hogy megzavarja a kommunikációs protokollt (mi másért szerezné meg valaki a terminált?). Így minden esetben amikor a rendszerben azzal a feltételezéssel élnek, hogy a kártyán tárolt adatok biztonságban vannak, mivel a kibocsátó és a kártyabirtokos érdekei egybeesnek, a kártya ellopásakor egy biztonsági rés keletkezik.

Vagy vegyünk egy olyan rendszert ahol a kártyaolvasót egy PC-hez kapcsolják, a PC pedig a terminál részeként működik. A terminálról feltehető, hogy a tulajdonosa érdekeinek megfelően működik, aki például Web-es tanúsítványokat szállít otthonról a munkahelyére. Sajnos a terminál viselkedése könnyen megváltoztatható

* ld. [YY97a]: ,,Kleptográfia: A kriptográfia felhasználása a kriptográfia ellen" (a ford. megj.)

egy ActiveX komponenssel ami lecseréli az olvasó szoftvert. Ez a támadás megváltoztatja a terminál viselkedését, az nem olyan lesz, mint amilyenre a rendszer számít. Ez a protokoll megbízhatóságára is hatással van. A viselkedésbeli változtatás lehet aktív, amikor például megváltoznak a terminál által kért vagy megjelenített adatok, vagy passzív, amikor a támadó csak megfigyeli az adatforgalmat. A megfigyeléses támadások célja lehet a kártya által végrehajtott tranzakciók lehallgatása vagy a PIN és más hasonló bizalmas adatok megszerzése. Az utóbbi valószínűsíthetően egy aktív támadás előzménye, amelyre nem feltétlenül a kártyaprotokoll területén kell számítani, hiszen a PIN-t gyakran nem csak egy rendszer használja, és az aktív támadásnak sem feltétlenül a kártyarendszer lesz a célpontja.

6.1. Kívülállók támadásai lopott kártyával

Ezek a támadások két dologban különböznek azoktól, amelyekkel a kártyabirtokos próbálkozhat. Az első különbség, hogy a tolvaj nem rendelkezik azokkal a titkos információkkal, amelyek a kártya aktiválásához szükségesek. Másodszor a támadó számára rendelkezésére álló idő korlátozott, csak addig próbálkozhat, amíg a kártya tulajdonosa észre nem veszi, hogy a kártyáját ellopták.

Ennélfogva az összes, a kártyabirtokos számára lehetséges támadás előfordulhat a következő kiegészítéssel: a tolvaj nem törődik a kártyabirtokost hátrányosan érintő hosszútávú következményekkel. Például egy kis összegek tárolására alkalmas elektronikus pénztárca esetén elképzelhető a kártyabirtokos által elkövetett csalások kivédésére egy olyan megoldás, amikor naplózzák a tranzakciókat, és pénz- vagy más büntetéssel torolják meg a szabálytalanságokat. Ha valaki lopott kártyát használ, akkor egy ilyen óvintézkedés nem fogja visszatartani.

A kártya és a kibocsátó szintjén egyaránt lehetséges valamilyen védelmi intézkedés bevezetése a rendszerbe. A kártyaszinten beépíthető védelmek a korlátvédelem és a rendellenességek figyelése. Az előbbi azt jelenti, hogy a több egymást követő rossz PIN bevitelét a kártya támadásként értékelheti. Ugyanakor ez lehetővé teszi egy rosszindulatú terminál számára, hogy elérje a szolgáltatás megtagadását (Denial of Service támadás). A rendellenességek figyelésekor a kártya információkat tart nyilván a korábbi műveletekről, és képes érzékelni, ha megváltoznak a felhasználó szokásai. Ez egy erős követelmény, de azokban az esetekben amikor a kártya offline használatára is lehetőség van érdemes valamilyen jelzést alkalmazni amelynek hatására a kártya további használatához kapcsolatba kell lépni a kibocsátóval. Így a rendszer lehetőséget kap arra, hogy gondosan mérlegelje a döntést vagy csak egyszerűen arra, hogy védekezzen a kártyaklónozás ellen.

6.2. Eve és Mallet*

Tegyük fel, hogy a kártya használatának célja az, hogy valamilyen protokoll szerint lehetővé tegye az együttműködést két olyan fél között, akik kölcsönösen bizalmat-

* Eve es Mallet a kriptográfiai algoritmusok működésének szemléltetésére használt „mesék" szereplői. Ezekben Alice és Bob a két biztonságos csatornán kommunikálni kívánó fél, Eve és Mallet pedig a támadók. Eve célja, hogy a csatorna lehallgatásával (eavesdropping) jogosulatlanul szerezzen információkat. Mallet a rosszinulatú támadó (malicious attacker), aki be is avatkozik a csatornán folyó kommuniukációba. Az ő célja (az információk megszerzésén kívül) kifejezetten a károkozás, például a kommunikáció megakadályozása, vagy hitelesnek tűnő hamis információk továbbítása. (a ford. megj.)

lanok egymással szemben, vagy legalábbis az érdekeik eltérnek. Ilyenkor a protokollnak ugyazokra a támadástípusokra kell számítania (és ezeknek ellenállnia), mint a hagyományos számítógépekkel kiépített rendszerek esetén. Így a lehallgatáson, vagy a protokoll rosszindulatú manipulálásán alkapuló támadások nagy része modellezhető úgy, mint az egyik szereplő másik ellen irányuló támadása. Ha a protokoll jól van megtervezve, akkor ugyanolyan jól képes ellenállni ezeknek a támadásoknak akár külső akár belső támadó próbálkozik velük.

6.3. Kooperatív támadások

Ha a rendszer tervezői arra számítanak, hogy az egyes szereplők közötti érdekellentét által fenntartott korlátok kizárnak közöttük mindenféle együttműködést, igencsak meglepődhetnek amikor a szerintük jól elválasztott szereplők egymásra találnak. A TV-kártya és a set-top box, amelyek alapvetően más érdekeket képviselnek együttműködhetnek annak érdekében, hogy a TV tulajdonosa jogosulatlanul vegyen igénybe szolgáltatásokat. Hasonlóképp a terminál tulajdonosa is meglepődve tapasztlahatja, hogy a kártya és a terminál, amelyeket ugyanaz a gyártó állított elő és programozott be, különböző nem dokumentált jellemzőkkel rendelkeznek. A lehetséges együttműködések és érdekes támadási modellek száma együtt nő a rendszer szereplőinek számával. Ha valaki elfeledkezik arról, hogy a legtöbb támadást bennfentesek indítják, akkor ezt valószínűleg hamar eszébe juttatják (feltéve, hogy a rendszere elég jó ahhoz, hogy érzékelje a csalásokat.)

7. Védelmi modellek

Alapjában véve kétféleképp lehet védekezni a smart card rendszereket érő támadások ellen. Az első csoportba azok a módszerek tartoznak amelyek egy bzionyos támadást próbálnak megnehezíteni: erős titkosítási algoritmusokkal, a kártya fizikai integritásának fokozott védelmével, stb. Ezekkel nem foglalkozunk részletesen, mivel az a véleményünk, hogy kevésbé hatékonyak és sokkal érzékenyebbek a tervezési és implementációs hibákra, mint a második csoportba tartozó módszerek, amelyek a lehetséges támadások egy teljes csoportja ellen próbálnak meg védeni. Ezt a gyakorlatban a szereplők számának csökkentésével lehet elérni, illetve az egyes résztvevők szerepét kell olyan mértékben átláthatóvá tenni, hogy a támadás kivitelezése már jelentős nehézséget okozzon. A szereplők számának csökkentésére a legegyszerűbb mód a szerepek összevonása. Például ha a kártyabirtokos és az adattulajdonos ugyanaz a személy akkor minden olyan támadás értelmetlenné válik amelyet a kártyabirtokos indíthatna az adatok tulajdonosa ellen. Ha a terminál tulajdonosa egyben a kártyakibocsátó akkor a terminháltulajdonos csak szerepcsere esetén indít támadást a kibocsátó ellen, vagyis csak abban az esetben ha egy támadó átvette az ellenőrzést terminál felett.

7.1. Kevesebb megosztás

Minden alkalommal, amikor a rendszer tervezése során összevonunk két vagy több szereplőt, azok a támadási lehetőségek, amelyek az összevont szereplők között álltak fenn egyszerűen eltűnnek. Ha például összevonjuk a kártyabirtokost és a megbízható terminált úgy, hogy egy képernyőt és valamilyen adatbeviteli eszközt

kapcsolunk a kártyához, a terminál billentyűzetének lehallgatásával és a megjelenítés megbízhatóságával kapcsolatos problémák megszűnnek.

Ezzel ellentétben az új résztvevők megjelenése új támadási lehetőségeket is teremt, amelyeket figyelembe kell venni. A terminál és a kártya szétválasztása egy olyan kapcsolódási pontot hoz létre amelynél jobbat nehezen lehetne tervezni ha man-in-the-middle támadásokat szeretnénk lehetővé tenni. A kártya fizikailag zárt, a hálózati adatforgalmat és a felhasználóval történő kommunikációt a terminál vezérli, így a legtöbb ismert ilyen jellegű támadás lehetséges, hacsak a protokollt nem készítik fel az ellenük való védekezésre. A tapasztalat azt mutatja, hogy a piacra kerülő biztonsági termékek legnagyobb részénél nem is gondolnak a man-in-the-middle támadásra vagy az adatforgalom esetleges visszajátszására vagy visszatükrözésére [Sho96, Sho97]. Még ha figyelembe veszik is ezeknek a támadásoknak a lehetőségét, az új szereplők megjelenése megnehezíti a kulcsok, sorozatszámok kezelését de az összes többi védelmi eljárást is.

Ha figyelembe vesszük, hogy egy smart card képtelen önállóan kommunikálni a külvilággal akkor a legegyszerűbb (és egyben a legolcsóbb) lehetőség a szerepek összevonására, ha biztosítani tudjuk, hogy a kártryabirtokos és az adattulajdonos személye megegyezzen. Ezzel megszabadulunk a legtöbb jelenlegi rendszert terhelő problémától, a kártyabirtokos adatok megszerzésére irányuló támadásaitól. A másik rendkívül hatékony megoldás, amikor kijelzővel és beviteli eszközökkel látjuk el a kártyát jelentősen növeli a költségeket.

7.2. Jobb átláthatóság

A biztonsági szakemberek legtöbbje egyetért abban, hogy a legjobb módja annak, hogy egy rendszer megbízhatóságáról meggyőződjünk az, ha széles körben lehetővé tesszük annak nyilvános vizsgálatát. Többször bebizonyosodott, hogy ha valakinek érdekében áll megtámadni a rendszert, akkor előbb-utóbb megszerzi a specifikációt, vagy akár azok hiányában is megkísérli a támadást [Sho96, Bla94]. Ezzel szemben a nyilvános publikációval értékes vizsgálatokat, elemzéseket nyerünk. (Példa erre az IPSec, a PGP vagy a S/MIME.) Az egyszerűség és a nyilvánosság kombinációja jelentősen egyszerűsíti azoknak az elemzőknek a munkáját, akik vizsgálni kívánják a rendszert. Így a rendszerben megjelenő szereplők számának csökkentésével nem csak a lehetséges támadások egy részét szüntetjük meg, de a rendszer elemzésének feladatát is egyszerűbbé tesszük. Az elemzés egyszerűsödése révén egyrészt gyorsabban befejeződhet az elemzés, másrészt a sikeres elemzés valószínűsége is nő.

Az átláthatóság megköveteli a szerepek világos elválasztását a rendszerben, így még nehezebbé válik a támadások végrehajtása. Például a Mondex rendszerében többféle olyan terminált (köztük hordozhatóakat is) találunk, amelyek segítségével a kártyabirtokos a kereskedőtől függetlenül ellenőrizheti a kártya bizonyos paramétereit. Így a kártyabirtokos hamarabb észreveheti az ellene intézett támadásokat. A Mondex által tárolt paraméterek (vagyis az adattulajdonos adatainak) teljes elérhetővé tétele valószínűleg még megbízhatóbbá tenné a rendszert azáltal, hogy növelné az átláthatóságot. Ugyanígy a támadó szoftvergyártó dolgát is megnehezítik a világos, átgondolt specifikációk és/vagy a nyílt forráskódú implementáció.

7.3. Biztonságos tervezés

Ez a védelmi modell arra öszpontosít, hogy a rendszer tervezése során kezdettől fogva figyelembe kell venni a megbízatóságot [SSS+98]. Bebizonyosodott, hogy egy rendszert a tervezés után, utólag biztonságossá tenni nehéz, költséges és nagy a hibák elkövetésének valószínűsége. Ezért mi egy olyan modellt javaslunk amely feleslegessé teszi a biztonsági intézkedések utólagos beépítésének bonyolult és költséges feladatát. A redukcionista modell nem csak egyszerűsíti a tervezést és az implementációt, de a hibás megvalósítás lehetőségét is csökkenti. Sok esetben láthattuk, hogy egy kriptográfiai rendszer gyakorlati kudarcának elsődleges oka a rossz implementáció [And94, Sch97, Sch98a, Koc98a, Sch98a].

Szintén az átláthatóság szempontjából fontos, hogy kerüljük a bonyolult és kockázatos multifunkciós kártyák alkalmazását. Ezzel nem csak a rendszer résztvevőinek számát csökkentjük, de egy egyszerűbb operációs rendszert is kapunk amelyben így kisebb valószínűséggel fordulnak majd elő hibák. Ha lecsökkentjük a kártyát használó szereplők számát (N-ről 2-re) akkor az operációs rendszert célzó és az alkalmazások egymás ellen irányuló támadásainak lehetőségét is kiküszöböljük.

8. Következtetések

Megmutattuk, hogy a biztonsági határok meghúzása nehéz feladat. Különösen kockázatos az adattulajdonos számára, ha egy olyan felhasználó hordoz helyette egy számítógépet, aki esetleg meg akarja őt támadni. Láttuk, hogy a kártya legnagyobb hátránya az, hogy nem képes önálló kommunikációra, így különösen sebezhető a terminál támadásaival szemben. Ezek a hátrányok a smart card rendszerek sajátosságai, amelyek leküzdése jelentős erőfeszítést igényel.

Körvonalaztunk néhány alapvető védelmi eljárást a kártyás rendszerekhez, ismertettünk egy rendszerszintű modellt amelynek segítségével a tervezők értékelhetik a rendszerüket. Ez a modell arra ösztönöz, hogy a biztonsági szempontokat már a tervezés legkorábbi fázisában vegyék figyelembe. A legfontosabb fejlesztési iránynak azt tarjuk, hogy a felhasználói interface irányítását a felhsználó kezébe kell adni. Azok a rendszerek amelyek tervezése során a szerepeket kombinálva kevesebb résztvevővel működnek, hatékonyabbak lesznek és a ráfordítások eredményeként a gyenge pontok száma is csökken.

Hivatkozások

[And94] R. Anderson, "Why Cryptosystems Fail," *Communications of the ACM*, v. 37, n. 11, Nov 1994, pp. 32–40.

[AK96] R. Anderson and M. Kuhn, "Tamper Resistance - A Cautionary Note,"*Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, 1996, pp. 1–11.

[BDL97] D. Boneh, R.A. Demillo, R.J. Lip- ton, "On the Importance of Checking Cryptographic Protocols for Faults," *Advances in Cryptology — EUROCRYPT '97 Proceedings*, Springer-Verlag, 1997, pp. 37–51.

[BGW98] M. Briceno, I. Goldberg, D. Wagner, "Attacks on GSM Security," work in progress.

[BS97] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," *Advances in Cryptology — CRYPTO '97 Proceedings*, Springer-Verlag, 1997, pp. 513–525.

[Bla94] M. Blaze, "Protocol Failure in the Escrowed Encryption Standard", *Proceedings of Second ACM Conference on Computer and Communications Security*, ACM Press, 1994.

[DLK+99] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, and J.-L. Willerns, "A Practical Implementation of the Timing Attack," *CARDIS '98 Proceedings*, Springer-Verlag, 1999, to appear.

[Jon93] K. Johnson, "One Less Thing to Believe in: High-Tech Fraud at an ATM," *The New York Times, 13 May 93*, pp. 1,B9.

[Koc96] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," *Advances in Cryptology — CRYPTO '96 Proceedings*, Springer-Verlag, 1996, pp. 104–113.

[Koc98a] P. Kocher, "Hidden Flaws: Avoiding Unexpected Weaknesses," *The 1998 RSA Data Security Conference Proceedings*, RSA Data Security, Inc., 1998.

[Koc98b] P. Kocher, Differential Power Analysis," available online from `http://www.cryptography.com/dpa/`.

[KS99] J. Kelsey and B. Schneier, "Authenticating Secure Tokens Using Slow Memory Access," in preparation.

[KSW96] J. Kelsey, B. Schneier, and D. Wagner, "Protocol Interactions and the Chosen Protocol Attack," *Security Protocols, International Workshop April 1997 Proceedings*, Springer-Verlag, 1998, pp. 91–104.

[KSWH98a] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," *Fast Software Encryption, 5th International Workshop Proceedings*, Springer-Verlag, 1998, pp. 168–188.

[KSWH98b] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," *ESORICS '98 Proceedings*, Springer-Verlag, 1998, pp. pp 97–110.

[McC96] J. McCormac, *European Scrambling Systems*, Waterford University Press, 1996.

[Row97] T. Rowley, "How to Break a Smart Card," *The 1997 RSA Data Security Conference Proceedings*, RSA Data Security, Inc., 1997.

[Sch97] B. Schneier, "Why Cryptography is Harder than it Looks," *Information Security Bulletin*, v. 2, n. 2, March 1997, pp. 31–36.

[Sch98a] B. Schneier, "Security Pitfalls in Cryptography," *CardTech/SecureTech Conference Proceedings, Volume 1: Technology*, CardTech/SecureTech, Inc., 1998, pp. 621–626.

[Sch98a] B. Schneier, "Cryptographic Design Vulnerabilities," *IEEE Computer*, v. 31, n. 9, September 1998, pp. 29–33.

[Sho96] A. Shostack, "Observed Weaknesses in the Security Dynamics Client/Server Protocol", *Network Threats Workshop, Dec 2-4 1996*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 38, R.N. Wright and P.G. Neumann, eds., American Mathematical Society, 1996.

[Sho97] A. Shostack, "Low Hanging Fruit: A Replay Attack on the TIS FWTK," presentation at the CRYPTO '97 rump session.

[SSS+98] C. Salter, O. Saydjari, B. Schneier, and J. Wallner, "Toward a Secure System Engineering Methodology," *New Security Paradigms Workshop 1998 Proceedings*, IEEE Computer Society Press, to appear.

[Sim84] G.J. Simmons, "The Prisoner's Problem and the Sublimianal Channel, *Advances in Cryptology: Proceedings of CRYPTO '83*, Plenum Press, 1984, pp. 364–378.

[Sim85] G.J. Simmons, "The Subliminal Channel and Digital Signatures," *Advances in Cryptology: Proceedings of EUROCRYPT 84*, Springer-Verlag, 1985, pp. 364–378.

[Sim86] G.J. Simmons, "A Secure Sublinimal Channel (?)" *Advances in Cryptology: Proceedings of CRYPTO 85*, Springer-Verlag, 1986, pp. 33–41.

[Sim94] G.J. Simmons, "Subliminal Channels: Past and Present," *European Transactions on Telecommunications*, v. 4, n. 4, 1994, pp. 459–473.

[Tho84] Ken Thompson, "Reflections on Trusting Trust," *Communications of the ACM* Vol. 27, No 8, August 1984, pp. 761–763.

[YY96] A. Young and M. Yung, "The Dark Side of Black Box Cryptography," *Advances in Cryptology — CRYPTO '96 Proceedings*, Springer-Verlag, 1996, pp. 89–103.

[YY97a] A. Young and M. Yung, "Kleptography: Using Cryptography against Cryptography," *Advances in Cryptology — EUROCRYPT '97 Proceedings*, Springer-Verlag, 1997, pp. 62–74.

[YY97a] A. Young and M. Yung, "The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems," *Advances in Cryptology — CRYPTO '97 Proceedings*, Springer-Verlag, 1997, pp. 264–276.