Adatbiztonság és adatvédelem a mindent átható számítógépes technológia világában

OTKA T046664 – zárójelentés

Dr. Vajda István
BME Híradástechnikai tanszék
vajda@crysys.hu

2008. február 20.

1. Összefoglaló

Az elmúlt évtizedben a számítógépes technológia hatalmas fejlődésen ment keresztül. Ez nemcsak a hagyományos számítógépek teljesítményének növekedésével járt, hanem megteremtette olyan új számítógépes eszközök és alkalmazások létrehozásának technikai feltételeit, melyek jelentős mértékben megváltoztatják az informatika és a távközlés ma ismert arculatát. Ezt a trendet foglalja magában *a mindent átható számítógépes technológia* (ubiquitous computing) fogalma. A számos hasznos alkalmazás lehetősége mellett ugyanakkor felmerülnek adatbiztonsággal és adatvédelemmel kapcsolatos problémák, melyek megnyugtató megoldása a mindent átható számítógépes technológia elterjedésének fontos feltétele.

Ebben a kontextusban kutatócsoportunk az alábbi témakörök vizsgálatát tűzte ki célul a T046664 OTKA projekt keretében: (1) több ugrásos vezeték nélküli hálózatok (pl. szenzor hálózatok és mobil ad hoc hálózatok) biztonsága, (2) személyes biztonsági tokenek, (3) RFID hálózatok biztonsági és adatvédelmi kérdései, és (4) formális biztonsági modellek.

Ezen témakörökhöz kapcsolódóan az alábbi konkrét eredményeket értük el:

1. Több ugrásos vezeték nélküli hálózatok biztonsága:
   - Ad hoc és szenzorhálózatokban használt útvonalválasztó protokollok biztonágának analízise, új biztonságos útvonalválasztó protokollok tervezése (enairA, Secure tinyLUNAR), a biztonság bizonyítása
   - Támadás-ellenálló adataggregáció problémájának vizsgálata szenzorhálózatokban, új támadás-ellenálló adataggregációs algoritmusok tervezése (RANBAR, CORA), analízise
   - Spontán kooperáció kialakulása feltételeinek vizsgálata ad hoc és szenzorhálózatokban, kooperáció ösztönzése késleltetéstűrő ad hoc hálózatokban (Barter)
2. Személyes biztonsági tokenek:
   - A nem-megbízható terminál probléma vizsgálata, feltételes aláírásra épülő megoldás tervezése és analízise
3. RFID biztonsági és adatvédelmi kérdések:

- Kulcsfa alapú azonosító-rejtő hitelesítő protokollok analízise, az elért privacy szintjének meghatározása, optimális kulcsfa tervezése, új elvekre épülő azonosító-rejtő hitelesítő protokoll tervezése és összehasonlítása a kulcsfa alapú módszerrel

4. Formális biztonsági modellek:

   - Szimulációs paradigmára épülő biztonsági modell útvonalválasztó protokollok analízisére, a biztonság bizonyítására
   - Támadó-modellek és analízis módszer támadás-ellenálló adataggregációs algoritmusok teljesítményének vizsgálatára
   - Formális modell kidolgozása a nem-megbízható terminál probléma vizsgálatára és a korlátozott számítási képességekkel rendelkező humán felhasználó leírására
   - Metrika kidolgozása azonosító-rejtő hitekesítő protokollok által nyújtott biztonság (privacy szint) karakterizálására
   - Játékelméleti modellek a spontán koopráció vizsgálatára ad hoc és szenzor hálózatokban, valamint spam és DoS elleni védelmi mechanizmusok analízisére

A továbbiakban tömör áttekintést adunk az egyes részterületeken elért fontosabb eredményeinkről és publikációinkról.

2. Biztonságos útvonalválasztás ad hoc és szenzor hálózatokban

Az útvonalválasztás egy alapvető hálózatrétegbeli szolgáltatás. Ismert, hogy egy kis erőforrással rendelkező támadó is könnyen működésképtelenné teheti az egész hálózatot az útvonalválasztó protokoll megtámadása által. Elég csupán néhány üzenet módosítása vagy új, fabrikált üzenet beszúrása ahhoz, hogy a támadó sikeresen megzavarja a hálózat normál működését. Ennél fogva a biztonságos útvonalválasztás kérdése nagyon fontos bármely hálózatban.

Ugyan biztonságos útvonalválasztó protokollokat javasoltak már többugrásos vezetéknélküli hálózatokra, azok biztonságát csak informális eszközökkel vizsgálták. Ugyanakkor ismert, hogy ezek a módszerek sok hibalehetőséget is rejtenek magukban. A formális, precíz módszerek hiánya magyarázható a biztonságos útvonalválasztás pontos definíciójának hiányával.

A mi célunk a vezetéknélküli ad-hoc és szenzorhálózatok útvonalválasztó protokolljainak formális analízise, a főbb tervezési elvek meghatározása, valamint ezen elvek felhasználásval új bizonyított biztonságú útvonaválasztó protokollok tervezése volt.

A kutatás keretében kifejlesztettünk egy olyan matematikai keretrendszert, amelyben definiálható a biztonságos útvonalválasztás fogalma, valamint precízen elemezhető a többugrásos vezetéknélküli hálózatokra javasolt útvonalválasztó protokollok biztonsága A keretrendszer a szimulációs paradigmára épül, mely egy eddig sikeresen és széleskörben használt módszer a különböző kriptográfiai protokollok biztonságának elemzésére. A mi modellünk elég általánosnak bizonyult ahhoz, hogy a különböző útvonalválasztó protokollok biztonságát elemezni tudjuk vezetékélküli ad-hoc és szenzorhálózatokban.

A kutatás első részében a vezetéknélküli ad hoc hálózatokra javasolt útvonalválasztó protokollok biztonságát vizsgáltuk. Az általános modellünket adaptáltuk ad hoc útvonalválasztó protokollokra, azon belül is először a forrás alapú útvonalválasztó protokollok biztonságát vizsgáltuk. Ezt a modellt felhasználva elemeztük az SRP és Ariadne biztonságos forrás alapú útvonalválasztó protokollokat, amelyek nem bizonyultak biztonságosnak a modellünkben, mivel sikeresen találtunk ellenük

eddig még ismeretlen támadásokat. Ez a tény motiválta egy új bizonyíthatóan biztonságos protokoll tervezését vezetéknélküli ad hoc környezetben. Az új protokoll neve endairA, amely az Ariadnehez hasonlóan működik, de azzal szemben nem a kérés hanem a válaszüzeneteket írják alá az egyes csomópontok. Az új protokoll amellett, hogy bizonyíthatóan biztonságos, még bizonyos szempontból hatékonyabb is az Ariadne-nál.

A kutatás következő részében a vezetéknélküli ad hoc hálózatok távolság vektor alapú útvonalválasztásának biztonságát vizsgáltuk. A modellünket sikeresen adaptáltuk távolság vektor alapú protokollokra. Ezt a modellt felhasználva elemeztük az ismert SAODV és ARAN biztonságos útvonalválasztó protokollokat. Ezek közül az SAODV nem bizonyult biztonságosnak a modellünkben. Ezzel szemben az ARAN biztonságát sikerült bizonyítanunk. Ez igazolta a modellünk használhatóságát, hiszen már létező protokollok között sikerült különbséget tennünk biztonsági szempontból.

Ezt követően elemeztük a vezetéknélküli szenzorhálózatokra javasolt útvonalválasztó protokollok biztonságát. Először áttekintettük a főbb létező vezetéknélküli szenzor hálózatokra javasolt útvonalválasztó protokollokat. Ezt követően a korábban javasolt formális modellünket adaptáltuk szenzorhálózatokra, mely elsősorban a hálózati csomópontok energiafogyasztásának figyelembevételét jelentette. Először a link-state alapú protokollok biztonságát vizsgáltuk. Ennek keretében bebizonyítottuk, hogy az INSENS útvonalválasztó protokoll egy valóban biztonságos link-state alapú útvonalválasztó protokoll a modellünkben. Foglalkoztunk továbbá a pozíció alapú útvonalválasztás biztonságával, valamint a label-switching alapú útvonalválasztás biztonságával. Ennek keretében egy létező de nem biztonságos label-switching alapú protokollt felhasználva (TinyLUNAR terveztünk egy új bizonyíthatóan biztonságos útvonaválasztó protokollt (Secure TinyLUNAR).

Kapcsolódó publikációk:

- L. Buttyán, I. Vajda. Towards Provable Security for Ad Hoc Routing Protocols. In *Proceedings of the 2nd ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN)*, 2004.
- G. Ács, L. Buttyán. Ad hoc útvonalválasztó protokollok bizonyított biztonsága. *Híradástechnika*, March 2005.
- G. Ács, L. Buttyán. Provable Security for Ad Hoc Routing Protocols. *Híradástechnika*, June 2005. (angol nyelvű szám)
- G. Ács, L. Buttyán, I. Vajda. Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks. In *Proceedings of the Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, 2005.
- G. Ács, L. Buttyán, I. Vajda. Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, Vol. 5, No. 11, 2006.
- G. Ács, L. Buttyán, I. Vajda. Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks. In *Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2006.
- G. Ács, L. Buttyán. Útvonalválasztó protokollok vezeték nélküli szenzorhálózatokban. *Híradástechnika*, November 2006. (Pollák-Virág díj, 2007)
- G. Ács, L. Buttyán. A taxonomy of routing protocols for wireless sensor networks. *Híradástechnika*, January 2007. (angol nyelvű szám)

- G. Ács, L. Buttyán, I. Vajda. The Security Proof of a Link-state Routing Protocol for Wireless Sensor Networks. In *Proceedings of the 3rd IEEE Workshop on Wireless and Sensor Networks Security (WSNS)*, 2007.
- G. Ács, L. Buttyán. Secure Routing in Wireless Sensor Networks. In J. Lopez and J. Zhou (eds.), *Wireless Sensor Network Security*, IOS Press, 2008.

3. Támadás-ellenálló adataggregáció szenzorhálózatokban

Egy biztonsági probléma amely fokozott mértékben jelentkezik a vezeték nélküli ad hoc és szenzor hálózatokban a szenzorok fizikai védelmének hiánya, ami azt vonja maga után, hogy a szenzorok viszonylag könnyen kompromittálódhatnak. A kompromittált szenzorok a többi szenzor számára továbbra is legális, hiteles szenzoroknak látszanak, ám működésük eltérhet a specifikált működéstől. Egy kompromittált szenzor például egy kompromittált kulccsal digitálisan aláírt üzenetet küldhet a bázisállomásnak, melyet a bázisállomás hitelesnek fog tekinteni, ám az üzenet tartalmát (aláírás előtt) a szenzor tetszőlegesen választhatja meg, így például nem feltétlenül a ténylegesen mért értéket továbbítja a bázis felé. Nyilvánvaló, hogy a kompromittált szenzorok nem kívánatos hatással lehetnek a rendszer egészére, hiszen a felsorolt statisztikák egyike sem tekinthető ellenállónak kompromittálódott mérésekkel szemben (vagyis nem tekinthető támadás-ellenállónak), hiszen egyetlen kompromittált (támadott) érték képes a statisztika félrevezetésére. Hasonlóképpen, a legtöbb ismert statisztika sem tekinthető támadás-ellenállónak ezen definíció szerint.

Kutatásainkban azt vizsgáljuk, hogy hogyan lehetne ezeket az eredendően nem támadás-ellenálló statisztikákat támadás-ellenállóvá tenni.

Az egyik megoldásunkban egy olyan modellt javasoltunk, melyben a szenzoroktól érkező adatok nem kerülnek rögtön aggregálásra, hanem először egy támadásdetektáló eljáráson mennek keresztül. Ez az eljárás a szenzorok méréseit valószínűségi változóknak tekintve statisztikai alapon próbálja detektálni az esetleges támadásokat. Két támadásdetektáló eljárást is javasoltunk. Az elsőnél független, azonos eloszlású mintaelemeket tekintve a mintafelezés és a két mintafél statisztikai összevetése jelenti az ellenőrzést. A másodiknál figyelembe vettük a mintaelemeket közötti korrelációt és ismertnek tekintett sűrűségfüggvények alapján végeztük az ellenőrzést. Mindkét javasolt algoritmus hatékonyságát analítikusan elemeztük.

A másik megoldás eljárásunkban nem próbálunk támadást detektálni, hanem megpróbáljuk a szenzorok által mért eredményekből, mint mintából kiszűrni a statisztikailag kilógó (outlier) elemeket. Az alapötletet itt a RANSAC elv adta, amelyet mi a támadás-ellenálló adataggregáció követelményeinek megfelelően adaptáltunk. A megoldásban először a kapott kompromittált minta alapján próbálunk egy adatmodellt létrehozni, majd a minta elemeit ehhez hasonlítani, és a kilógó elemeket eldobni. Túl sok elem eldobása esetén az algoritmus újrapróbálkozik egy másik modell létrehozásával. Végül, ha sikerül olyan modellt találni, amelyik az adott mintát jól lefedi, akkor a bentmaradó elemek alapján lehet aggregálni, akár olyan statisztikák felhasználásával is, amelyeket eddig nem tekintettünk támadás-ellenállónak. Ezen algoritmus hatékonyságát szimulációs módszerekkel elemeztük.

Kapcsolódó publikációk:

- L. Buttyán, P. Schaffer, I. Vajda. Resilient Aggregation: Statistical Approaches. In N. P. Mahalik (ed.), *Sensor Networks and Configuration*, Springer, 2006.
- L. Buttyán, P. Schaffer, I. Vajda. Resilient Aggregation with Attack Detection in Sensor Networks. In *Proceedings of the 2nd IEEE International Workshop on Sensor Networks and Sys-*

tems for Pervasive Computing (PerSeNS), IEEE Computer Society Press, 2006.

- L. Buttyán, P. Schaffer, I. Vajda. RANBAR: RANSAC-Based Resilient Aggregation in Sensor Networks. In *Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, ACM Press, 2006.

- P. Schaffer, I. Vajda. CORA: Correlation-based Resilient Aggregation in Sensor Networks. In *Proceedings of the 10th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*, ACM Press, 2007.

4. Spontán kooperáció feltételeinek vizsgálata ad hoc és szenzorhálózatokban

Önszerveződő ad hoc hálózatokban a hálózat működése nagymértékben függ a csomópontok kooperációs készségétől. A kooperáció elősegítése érdekében különböző stimulációs mechanizmusokat javasoltak az irodalomban, ám azt nem vizsgálták, hogy nem alakulhat-e ki a kooperáció spontán módon, illetve, hogy mik a spontán kooperáció kialakulásának feltételei. Ezt a problémakört először az ad hoc hálózatokban történő kooperatív csomagtovábbítás kontextusában vizsgáltuk meg. Játékelméleti módszereket alkalmazva meghatároztuk, hogy mik a Nash egyensúly kialakulásának feltételei, majd szimulációval vizsgáltuk a feltételek teljesülésének valószínűségét statikus és dinamikus (mobil) ad hoc hálózatokban. Arra a következtetésre jutottunk, hogy statikus hálózatokban a spontán kooperáció elvileg lehetséges, de a szükséges feltételek teljesülésének valószínűsége igen csekély, ezért a kooperáció kialakulásához stimulációs mechanizmusokra van szükség. Dinamikus ad hoc hálózatokban, a spontán kooperáció létrjöttének esélyei nagyobbak, mert a hálózati topológia változása miatt a csomópontok kiszolgáló és kiszolgált szerepe dinamikusan változik.

A spontán kooperáció kialakulásának problémáját több operátor által működtetett szenzorhálózatok kontextusában is megvizsgáltuk. A szenzorhálózatok egyik legfontosabb tervezési kritériuma a szenzorok élettartamának maximalizálása, hiszen a legtöbb alkalmazásban a szenzorok akkumulátorának újratöltése vagy cseréje praktikusan vagy egyáltalán nem lehetséges. Az utóbbi években a kutatók számos protokollt javasoltak a szenzorhálózatokban történő energiahatékony kommunikációra. Ezen munkák azzal az alapfeltevéssel éltek, hogy az összes szenzort egy hatóság tartja ellenőrzése alatt. Várható azonban, hogy a gyakorlatban különböző fennhatóság alatt álló és különböző célt szolgáló szenzorhálózatok megjelenhetnek és működhetnek egyazon földrajzi helyen. Még ha a szenzorok különböző irányítás alatt is állnak és különböző feladatokat látnak is el, a közöttük lévő kommunikációs csatlakozási felület lehet szabványos, és ez lehetőséget ad kooperáció kialakulására.

Munkánk során megvizsgáltuk, hogy létrejöhet-e spontán módon – minden külső kényszerítő körülmény nélkül – kooperáció különböző fennhatóság alá tartozó szenzorhálózatok között. A modellünkben nem tételeztünk fel semmilyen külső serkentést, a kooperáció kialakulását a szenzorok racionális viselkedésére alapoztuk. Megvizsgáltunk a két szenzorból és két bázisállomásból álló hálózatokat, majd a biztató eredmények hatására a vizsgálatot kiterjesztettük mind térben, mind a résztvevők számát tekintve. Térben eljutottunk a két dimenziós véletlen elhelyezkedésig, számban a száz szenzorból álló, tíz bázisállomást tartalmazó hálózatokig. Megvizsgáltunk egy közös, több közös és több saját bázisállomást tartalmazó hálózatokat. Szimulációink szerint jellemzően létrejön spontán kooperáció, de különböző hálózatokban különböző mértékben. A különböző hálózatokban a kooperáció mértékét a hálózat paraméterei határozzák meg, különös tekintettel a sűrűségre, amit az egy bázisállomásra jutó szenzorok száma befolyásol a lefedett terület mellett.

Kapcsolódó publikációk:

- M. Félegyházi, J.-P. Hubaux, and L. Buttyán. Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks – the Dynamic Case. In *Proceedings of the Second International Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, 2004.
- L. Buttyán, T. Holczer, and P. Schaffer. Spontaneous Cooperation in Multi-Domain Sensor Networks. In *Proceedings of the Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, Springer, 2005.
- M. Félegyházi, J.-P. Hubaux, and L. Buttyán. Cooperative Packet Forwarding in Multi-Domain Sensor Networks. In *Proceedings of the First International Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS)*, 2005.
- N. Ben Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. Node Cooperation in Hybrid Ad hoc Networks. *IEEE Transactions on Mobile Computing*, Vol. 5, No. 4, April 2006.
- M. Félegyházi, J.-P. Hubaux, and L. Buttyán. Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, Vol. 5, No. 5, May 2006.

5. Kooperáció ösztönzése késleltetéstűrő ad hoc hálózatokban

A késleltetés tűrő hálózatok (delay-tolerant network – DTN) a vezetéknélküli ad-hoc hálózatok egy speciális fajtája, ahol az üzenettovábbítás a *tárol-hord-és-továbbít* elv alapján hajtják végre. Ez azt jelenti, hogy a résztvevő csomópontok tárolják az üzeneteket, és akkor továbbítják, amikor egy másik csomóponthoz csatlakoznak (pl. amikor egymás rádiósugarába lépnek). Kutatásaink során a DTN hálózatok személyi használatú változatát vizsgáltuk, melyek könnyedén megvalósíthatók akár a mai mobil eszközök segítségével is. Ilyen hálózatok elősegítik közösségen belüli üzenetek terjedését azzal, hogy az üzenetek mozgása összefüggésben áll az üzenetterjesztő eszköz hordozójának mozgásával. Ennek megfelelően a DTN hálózat nem konkurál a már létező vezetéknélküli rendszerekkel (pl. a GSM hálózat), hanem kiegészíti azokat.

Megvizsgálva a DTN hálózatokban javasolt néhány üzenet továbbító protokollt, arra jutottunk, hogy még biztonsági szempontból gyenge protokollok sem támadhatók hatékonyan köszönhetően a rendszer elosztottságának és az állandóan változó szomszédsági kapcsolatoknak. Ugyanakkor potenciális probléma, hogy a DTN hálózatokban az üzenet továbbítás minősége nagy mértékben függ a résztvevő csomópontok tárolási és továbbítási hajlandóságától, önzetlenségétől. Amennyiben egy csomópont önző, úgy letölt és továbbít olyan üzeneteket, ami őt érdekli, ugyanakkor a mások számára hasznos üzenetek terjesztését nem vállalja. Az önző viselkedést az serkenti, hogy a mobil eszközök általában korlátolt processzor és memória kapacitással rendelkeznek, miközben a tápellátást akkumulátorral oldják meg. A felhasználók, hogy erőforrásaikat óvják, olyan alkalmazásokat telepíthetnek az eszközeikre, melyek az önző magatartásnak felel meg. Csakhogy, ahogy más kutatócsoportok kimutatták több üzenettovábbító protokollt vizsgálva, az önző csomópontok növekedésével a célbaért üzenetek száma jelentősen csökken.

Kutatásaink első felében azt vizsgáltuk, hogy mely paraméterek mellett szükséges, és mely paraméterek mellett nem a kooperáció ösztönzése. Ehhez megalkottuk a megfelelő modellt és szimulációval megállapítottuk, hogy ösztönzés nélkül olyan üzenetek terjednek nagymértékben, melyek amúgy is sokakat érdekelnek.

Ennek megfelelően kutatásaink során egy olyan mechanizmust fejlesztettünk ki, amely ösztönzi a csomópontokat, hogy mások üzeneteit is hordják és továbbítsák. A javasolt protokoll a barter kereskedelem elvén alapszik: egy csomópont csak akkor tud egy üzenetet megszerezni, ha ő is képes cserébe új üzenetet biztosítani. Ettől azt vártuk, hogy a csomópontoknak olyan üzeneteket is érdemes gyűjteni és továbbítani, ami közvetlenül őket nem érdekli, viszont remélhetőleg később becserélhetik olyanokra, ami már őket érdekli.

A javasolt megoldást játékelméleti módszerrel elemeztük. Az üzenet továbbítást, mint játékot vizsgáltuk, melyben a csomópontok minél több és minél frissebb, őket érdeklő üzenetet akarnak megszerezni. A játékelméleti módszer alkalmazását ugyanakkor az indokolta, hogy az üzenet terjedését befolyásolja a csomópontok egyéni önző, de racionális döntése is. A modellünkben a játék szimmetrikus, azaz a csomópontok döntési (stratégia) tere azonos és azonos körülmények mellett a nyereség is azonos. Ebben a játékban kerestünk szimmetrikus stratégiájú Nash egyensúlyt. Szimulációval megmutattuk, hogy a csomópontoknak valóban megéri olyan üzenetek is hordozni, ami közvetlenül nem érdekli őket, azaz ha önzővé válnak, kevesebb üzenetet tudnak megszerezni. Ennek megfelelően a célba ért üzenetek száma nőtt. Ráadásul, a barter mechanizmus akkor sem rontotta az üzenet terjedést, amikor azok az ösztönzés nélküli rendszerben is jól terjedtek.

Kapcsolódó publikációk:

- L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter-based cooperation in delay-tolerant personal wireless networks. In *Proceedings of the IEEE Workshop on Autonomic and Opportunistic Communications (AOC)*, 2007.

6. RFID biztonsági és adatvédelmi kérdések

Az RFID (Radio Frequency IDentification, Rádió Frekvenciás Azonosítás) célja egy eszköz vagy személy egyértelmű azonosítása rádiós kommunikáció felhasználásával. A rendszer előnye a már elterjedt más nem rádiófrekvenciás azonosítási módokhoz képest a nagy átbocsátó képessége (nem szükséges semmilyen közvetlen kapcsolat az azonosított tárgyhoz, de még közvetlen rálátás sem szükséges mint a vonalkódoknál).

Egy RFID rendszer három fő komponensből áll. Ezek az *RFID adó* (RFID Tag), az *RFID olvasó* (RFID Reader) és a *háttéradatbázis* (Backend Database). Az adó feladata egy egyértelmű azonosító számot eljuttatni az olvasóhoz, amit az továbbküld feldolgozásra az adatbázisnak. Mivel az adó nagy példányszámban készül, ezért annak minél olcsóbbnak és egyszerűbbnek kell lennie.

Az RFID rendszerek előnyös kényelmi szolgáltatásai mellett sajnos vannak hátrányos hatásai is, főleg az adatvédelem témájában. A két fő adatvédelmi probléma a következő:

Követhetőség (Tracking): Minden ember, aki magánál hord valamilyen RFID adó(ka)t könnyen követhetővé válik, ha egy támadó elhelyez olvasó eszközöket a környezetben. Ezáltal automatikusan tudni lehet, hogy egy adott célszemély mikor és hol jár pár olcsó olvasó telepítése árán.

Leltározás (Inventorying): Egy olvasó segítségével meg lehet állapítani, hogy egy adott személy milyen ruhát hord, milyen gyógyszereket szed, sőt esetleg a nála lévő készpénz mennyisége is megállapítható (a nagyobb értékű Euro bankjegyekben van RFID adó).

Az ilyen jellegű támadásokat elkerülendő több megoldási javaslat is született. Ezek a bonyolultság szempontjából az egyszerű megsemmisítéstől kezdve a szelektív olvasó blokkoláson át a kriptográfiát

is felhasználó módszerekig terjednek. Mi a sor bonyolultabb végén elhelyezkedő szimmetrikus kulcsú kriptográfián alapuló, az azonosító titkosításán alapuló megoldásokat kutattuk.

A projekt folyamán született nemzetközi publikációban két módszert dolgoztunk ki, amelyek gyors azonosítást kínálnak, de meggátolják mind a követést mind a leltározást.

A megoldások a felhasználók rendezésén alapulnak. Az időrendileg első megoldásban egy fába vannak rendezve a felhasználók. Az azonosítás folyamán az olvasó a fában szintről szintre lépve határozza meg az éppen vele kommunikáló eszköz azonosítóját. Természetesn ugyanarra az azonosítási feladatra többféle fa is megoldást nyújthat. Hogy melyik fa a legjobb, azt egy nemlineáris programozási feladat megoldása határozza meg. Ezért kidolgoztunk egy algoritmust, ami megoldja a feladatot, ezáltal meghatározva a bizonyos értelemben vett optimális fa paramétereit. Az így kapott megoldást elemeztük egy aktív támadó feltételezésével, és megmutattuk, hogy hogyan változik a felhasználók anonimitása a támadó erejének függvényében.

Az időrendileg második publikációban a felhasználókat halmazokba rendeztük. Az olvasó az azonosítás folyamán először meghatározza, hogy a vele kommunikáló eszköz melyik halmazba esik, majd a halmazon belül megtalálja az eszközt. Ugyanazokat a feltételeket figyelembe véve megmutattuk, hogy ezzel a megoldással még nagyobb anonimitás érhető el mint az előző megoldással úgy, hogy az olvasó feladata nem nehezedik, sőt az adó feladata jelentősen könnyebbé válik.

Kapcsolódó publikációk:

- L. Buttyán, T. Holczer and I. Vajda. Optimal Key-Trees for Tree-Based Private Authentication. In *Proceedings in the International Workshop on Privacy Enhancing Technologies (PET)*, 2006.
- L. Buttyán, T. Holczer, and I. Vajda. Providing Location Privacy in Automated Fare Collection Systems. In *Proceedings of the 15th IST Mobile and Wireless Communication Summit*, 2006.
- G. Avoine, L. Buttyán, T. Holczer, and I. Vajda. Group-Based Private Authentication. In *Proceedings of the IEEE Workshop on Trust, Security, and Privacy for Ubiquitous Computing (TSPUC)*, 2007.

7. Nem-megbízható terminál probléma

Az intelligens kártya (smart card) lényegében egy mikro-számítógépnek tekinthető, amely rendelkezik CPU-val és memóriával, és képes különböző számítások elvégzésére. Az intelligens kártyák nagy előnye, hogy könnyen hordozhatók. Bontás-ellenálló tulajdonságaik miatt az intelligens kártyákat gyakran használják biztonsági alkalmazásokban is (pl. digitális aláíró kulcsok tárolására és digitális aláírás generálására). Az intelligens kártyák már ma is sokféle alkalmazásban megtalálhatók (pl. bankkártyák, GSM SIM kártyák, tömegközlekedési kártyák, stb), s ez a kör a jövőben bővülni látszik.

Egy kapcsolódó biztonsági probléma a nem-megbízható terminál problémája, mely abból ered, hogy az intelligens kártyának nincsen felhasználói interfésze, s így a felhasználónak mindenképpen szüksége van egy terminálra, amelyen keresztül a kártya funkcióit elérheti. Egy rosszindulatú terminál azonban egy "man-in-the-middle" támadást hajthat végre, és félrevezetheti a felhasználót. Egy digitális aláírás alkalmazásban pl. a terminál tetszőleges dokumentumot aláírathat a kártyával miután a felhasználótól bekérte a funkció aktiválásához szükséges PIN kódot.

A probléma enyhítésére javasoltunk egy keretrendszert, mely lehetőséget biztosít a nem-szándékolt (azaz a terminál által csalárd módon megszerzett) digitális aláírások érvénytelenítésére. Módszerünk egy új koncepcióra, a feltételes aláírás fogalmára épül. Az ötlet lényege a következő. A felhasználó kártyája naplózza az aláírás generálásának tényét, majd egy olyan aláírást generál, melynek

érvényessége két feltételhez van kötve. Egyrészt adott egy jövőbeli időpont, s az aláírás biztosan nem érvényes ezen időpont előtt. Másrészt a kártya tulajdonosának ezen jövőbeli időpontig konfirmálnia kell az aláírást, vagy effektíve vissza kell azt vonnia, amit egy megbízható terminálnál tehet meg, miután végignézte a kártya által naplózott tranzakciókat, és azonosította azokat, melyeket nem szándékozott végrehajtani. Így az adott körülmények között a felhasználó egy nem-megbízható terminálnál is tud aláírást generálni, feltéve, hogy később hozzáfér egy megbízható terminálhoz, ahol a kártya tranzakcióit ellenőrizni tudja.

Munkánk során több protokollt is terveztünk, melyek a fenti koncepcióra épülnek. Ezen protokollokat implementáltuk is a laborunkban megtalálható Java-kártya platformon.

Kapcsolódó publikációk:

- I. Zs. Berta, L. Buttyán, I. Vajda. Mitigating the Untrusted Terminal Problem Using Conditional Signatures, In *Proceedings of IEEE International Conference on Information Technology (ITCC)* 2004.
- I. Zs. Berta, L. Buttyán, I. Vajda. Privacy Protecting Protocols for Revokable Digital Signatures, In *Proceedings of Cardis 2004*, Kluwer, 2004.
- I. Zs. Berta, B. Bencsáth. Sending authentic messages from malicious terminals, In *Proceedings of the Networkshop 2004 Conference*, NIIF, Hungary, 2004.
- I. Zs. Berta, I. Vajda. Limitations of humans when using malicious terminals *Tatra Mountains Mathematical Publications*, vol. 29, 2004.
- I. Zs. Berta. Why are not digital signatures spreading as quickly as it was expected? MBA dissertation, Buckinghamshire Chilterns University College, Buckinghamshire Business School, Számalk Open Business School, 2004.
- I. Zs. Berta, L. Buttyán, I. Vajda. A framework for the revocation of unintended digital signatures initiated by malicious terminals. *IEEE Transactions on Secure and Dependable Computing*, Vol. 2, No. 3, July-September 2005.
- I. Zs. Berta. Mitigating the attacks of malicious terminals. PhD Theses, BME, 2005.

8. Spam és DoS elleni védelem

A szolgáltatás-megtagadásos támadások, azaz Denial-of-Service (DoS) támadások régóta ismertek. Az évek során számos típusát és esetét ismertük meg, a legegyszerűbb és legelterjedtebb típusai a programok hibáit kihasználó egyszerű támadások (pl. ping of death) vagy a sávszélességet teljesen felemésztő támadások. A szolgáltatás-megtagadásos támadások elleni védekezés csak igen szűk körben fejlődött. Ez azért van így, mert az általános szolgáltatás-megtagadásos támadások elleni legjobb védekezés a megfelelő architektúra, a jelenlegi környezet pedig nem úgy jött létre, hogy komolyan figyelembe vette volna ezt a problémát. A DoS probléma elleni küzdelem nehézségeinek hangsúlyozására megemlíthetjük, hogy még a detekció is nehéz feladat. A kéretlen reklámlevelek, a spamek is tudnak akár szolgáltatásmegtagadásos helyzetet létrehozni. A hálózati e-mail forgalom nagyobbik hányada ma már kéretlen levél. Ezeket speciális célszoftverekkel szűrjük ki, mely szoftverek nagy erőforrásigényűek. Ha sok e-mail érkezik, úgy a rendszerben nagyobb az erőforrásigény, ami egyre könnyebben okoz szolgáltatás-megtagadásos jellegű problémát. A spam problémát nem egy

forrás okozza és az egyes forrásoknak nem is támadás a célja. A sok elküldött levél eredménye viszont egy összeomlás, ezen összeomlást viszont nehéz vizsgálni a szokásos eszközökkel, mivel a küldött levelek nem valós kiszolgáláshoz kötődnek, hanem főként reklámtevékenységhez. A szokásos megbízhatósági- és teljesítménytervezés azonban főként a valós szolgáltatási igényekkel foglalkozik, nem olyan ettől jelentősen eltérő problémával, mint a spam kérdése.

A DoS és spam problématerületen számos különböző megoldás ismert, mi a területet új módszereket közelítettük meg.

Mérések segítségével megmutattuk, hogy sikeres Denial-of-Service támadás hajtható végre SMTP szerverek ellen alacsony sávszélesség felhasználása mellett, és a támadási lehetőség még valósabb, ha a szerveren tartalomszűrés is aktív. Méréseink a támadhatóság mértékét konkrét számokkal is alátámasztják.

Új védelmi módszert terveztünk a DoS elleni védekezésre, amely hálózati forgalmi analízisen alapul. Egy ún. front-end bemeneti modul érzékeli a támadásokat és végzi el a támadók kiszűrését. A várható hamis pozitív és hamis negatív hibavalószínűségek kiszámításának módját is bemutatjuk.A javasolt módszer nem teszi szükségessé a megtámadott szervereken kívüli hálózati elemek módosítását és minimalizálja a hibásan kiszűrt legális felhasználók számát. Felső becslést adtunk a detekciós algoritmus hibavalószínűségére és a hibás azonosítás valószínűségére. Ezek a számítások lehetővé teszik az algoritmus valós körülmények közötti alkalmazásának paraméterezését. Szimulációk is megerősítették az analitikus eredményeket és információval szolgálnak a paraméterekre való érzékenység tekintetében. Architektúrát terveztünk, hogy a javasolt valós körülmények között is beágyazható legyen egy STMP környezetbe. A tervezett architektúrára alapozva prototípus formában is megvalósítottuk a rendszert.

Analizáltuk az ún. Directory Harvest Attack (DHA) e-mail címkigyűjtő támadásokat. A DHA tipikus célja e-mail címek összegyűjtésére, de maga a DHA támadás akár DoS helyzet kialakulását is okozhatja. Megterveztük a DHA támadás egy optimális formáját, emely az e-mail címek felhasználóneveinek, az ún. local partok valószínűségi eloszlását és a célrendszerben feltételezett felhasználószámot használja ki az optimalizáláshoz.

Képletet adtunk meg a sikeresen detektálható címek számának várható értékének kiszámításához. Bizonyítottuk, hogy modellben a támadás optimális, azaz a sikeresen összegyűjtött e-mail címek száma adott erőforrásfelhasználás mellett maximális. Szimulációval is bemutattuk, hogy az optimális támadás hatékonyabb a megfigyelt támadási formáknál. A szimuláció valós adatokon alapul. Megterveztük egy központosított, RBL (real-time blacklist) alapú architektúrát a DHA támadások elleni védekezésre. A tervezett rendszert prototípus szinten is megvalósítottuk.

Kapcsolódó publikációk:

- B. Bencsáth, M. A. Rónai Empirical Analysis of Denial of Service Attack Against SMTP Servers, In *Proceedings of The 2007 International Symposium on Collaborative Technologies and Systems*, IEEE, 2007, pp. 72-79.

- B. Bencsáth, I. Vajda, Protection Against DDoS Attacks Based On Traffic Level Measurements, In *Proceedings of the 2004 International Symposium on Collaborative Technologies and Systems, The Society for Modeling and Simulation International*, 2004, Waleed W. Smari, William McQuay, pp. 22-28., San Diego, CA, USA, January, Simulation series vol 36. no. 1., ISBN 1-56555-272-5.

- B. Bencsáth, I. Vajda, Efficient Directory Harvest Attacks, In *Proceedings of the 2005 International Symposium on Collaborative Technologies and Systems*, pp. 62-68., IEEE Computer

Society, July 2005.

- Géza Szabó, B. Bencsáth, Statistical analysis of the results of the DHA protection system (in hungarian), In *Proceedings of Networkshop 2006 conference*, NIIF, 2006, NIIF.
- B. Bencsáth, I. Vajda, Efficient Directory Harvest Attacks and Countermeasures, *International Journal of Network Security*, vol 5. no 3. pp. 264-273. 2007.