Takács Péter – Vályi Sándor

Többcsatornás kriptográfiai protokollok vizsgálata a bővített CSN-logika eszközeivel

1. Bevezetés

Napjainkban a kommunikáló partnerek sok esetben több eszközt, és ezzel párhuzamosan több információs csatornát is képesek használni. A dolgozat célja a többcsatornás rendszerek matematikai logikai eszközökkel történő vizsgálatának bemutatása. Munkánk során a Coffey-Saidha-Newe-féle (a továbbiakban: CSN) logikai rendszert bővítettük a kommunikációs csatornák leírásának és kezelésének lehetőségeivel. Az új rendszert már ismert és gyakorlatban is alkalmazott többcsatornás kriptográfiai protokollok biztonsági elemzésére használtuk fel. Jelen írásban részletesebben a MANA III protokoll elemzését mutatjuk be. A helyszűke miatt csak vázlatosan ismertethetjük a logikai rendszert, de az érdeklődők a következő forrásokban megtalálják a pontosabb részleteket.

A CSN-logikai rendszer két cikkben jelent meg. Először 1997-ben T. Coffey és P. Saidha tette közzé az alaprendszert. [1] Ebben a cikkben a nyilvános kulcsú titkosítást használó protokollok számára kidolgozott elmélet látott napvilágot. Ezt követően 2003-ban jelent meg a Newe és T. Coffey írása, amely kibővíttette az eredeti modellt a titkos kulcsú titkosításta alkalmazó rendszerek körére. [2] A két rendszer összefoglalva [2] és [3] cikkekben érhető el. A bővített CSN logika alkalmazásaként tanulmányozott MANA III protokollról [4]-ben olvashatunk.

További kapcsolódási pontként kell megemlítenünk Wong F-L. és Stajano F. 2005-ben megjelent cikkét, amely a többcsatornás kriptográfiai protokollok körében a MANA protokollcsaládot vizsgálja. [5] Írásukban a MANA I, II és III protokollok kerülnek elemzésre, valószínűségszámítási eszközök felhasználásával. A cikk végén jelzik a szerzők, hogy aktuális feladatként jelentkezik egy olyan rendszer kidolgozása, amely lehetővé tenné a többcsatornás protokollok logikai alapú vizsgálatát. Munkánk során ezen az úton indultunk el, és alkalmaztuk eredményeinket a már említett MANA protokollcsalád egyes elemeire.

Hasznos összefoglalását találja az érdeklődő még a többcsatornás kriptográfiai protokollok körének Wong és Stajano 2007-ben megjelent cikkében[6], amely a tudományterület aktuális helyzetét foglalja össze.

2. A kriptográfiai protokollok és a többcsatornás protokollok

A kriptográfiai protokollok olyan kommunikációs protokollok, amelyek célja a partnerek biztonságos, védett és ellenőrzött kommunikációjának biztosítása. A protokollok elmélete a támadások detektálásától kezdve a protokollok különböző eszközökkel történő vizsgálatára vállalkozik. Napjainkban erősödött meg az az irányzat, amely külön vizsgálja a protokollokban szereplő csatornák szerepét és jelentőségét. Ez a vonulat kapcsolódik a *„mindenütt jelen lévő, láthatatlan számítástа!!!!!chnika”* (~~ubicomp~~ ubiquitous computing, vagy pervasive computing [7]) fogalmához. Az újonnan megjelenő számítástechnikai és informatikai eszközök már az egymáshoz kapcsolódás képességével, a vezetékes, vagy vezeték nélküli kommunikációval vannak felruházva. Kialakult a PAN (Personal Area Network – Személyes hálózat [8]) fogalomköre és technológiája, amelynek kommunikációs protokolljai eltérnek az Internet és a mobilhálózatok eddig felépített protokolljaitól. [9][10]

Részletesen és behatóan tanulmányozva a tradicionális (titkos kulcsú) kriptográfiai rendszereket, könnyen megtaláljuk többcsatornás protokollok alapjait. Például a protokollokban szereplő titkos kulcsú kommunikáció kulcsát egy védett csatornán kell eljutatni a parnerhez, ami jelentheti egy futár alakalmazását, vagy személyes találkozáskor lebonyolított kulcscserét. Hasonló megoldások találhatók különböző elektronikus pénzkezelési megoldásokban, eBank rendszerekben, stb.
Elmondhatjuk tehát, hogy több csatorna használata nem jelent lényegesen új eszközt a kritptográfiában, viszont az ilyen megoldások megalapozott tudományos vizsgálata még csak napjainkban zajlik. Ahhoz, hogy részletesebben ismertessük elért eredményeinket, be kell mutatnunk a protokollok formális vizsgálatának lépéseit.

3. A kriptográfiai protokollok formális vizsgálata

A kriptográfiai kutatások napjainkra két fő irányzatot alakítottak ki. Az egyik a *számításelméleti megközelítés* (főleg valószínűségelméleti és komplexitáselméleti eszközök alkalmazása), a másik pedig a *formális megközelítés* (főleg modális logikai eszközök). [11] A formális módszerek kriptográfiai protokollok tervezésének és ellenőrzésének különböző szakaszaiban használhatók. A leginkább kutatott az ellenőrzés (verifikáció) szakasza. A bővített CSN logika a modális logika alkalmazását jelenti a verifikáció során.

A modális logika alkalmazásának sémája a kriptográfiai protokollok ellenőrzése során a következő:

1. lépésben a vizsgált protokollt kell formalizálni.
2. lépés a kezdeti feltételek meghatározása.
3. lépésként a protokoll céljait kell megfogalmazni.
4. lépés a logikai posztulátumok alkalmazását jelenti.
5. lépés a 4. lépés esedményeinek és a protokoll céljainak (3. lépés) összevetését jelenti.

4. A CSN-logika és bővítése

A CSN logika teljes és szabatos leírása terjedelmi okokból itt nem szerepelhet, de a következő vázlat elegendő útmutatást adhat az eredmények leírásához.

A logikai rendszer magában foglal formális jeleket az egyedek és az állapotok leírására, tartalmaz függvényeket és operátorokat. A rendszer alkalmazza a klasszikus logikai jeleket: konjunkció, duszjunkció, negálás, implikáció, stb. Használjuk az univerzális és az egzsiztenciális kvantorokat, és más ismert matamatikai jelölésmódokat. A rendszer hét következtetési szabályt sorol fel, amelyek megegyeznek a hagyományos logikai rendszerek következtetési szabályaival (modus ponens, általánosítási szabály, stb.).
Az axiómák két típusba sorolhatók: az első a logikai axiómák köre (4 axióma, *A1-A4*); a másik típusú axiómák a nemlogikai axiómák (10 axióma, *A5-A15*), amelyek a nyilvános- és a titkos kulcsú kommunikáció körét foglalják magukba. Ezek az axiómák kapcsolódnak az üzenetek kibocsátásához és fogadásához, a üzenet-titkosítás és a -visszafejtés folyamatához.
Az eredeti Coffey-Saidha rendszer (*A1-A10*) a nyilvános kulcsú kriptográfiai protokollok analízise során alkalmazható, az axiómák második része (*A11-A15*) pedig a szimmetrikus kulcsú protokollok leírására.

A rendszer nem tartalmazta a többcsatornás protokollok körébe eső vizsgálatok lehetőségét, ami módot teremtett számunkra a bővítés visgálatára.

A bővítés során a következő alapcélokat tűztük magunk elé:

1. Az eredeti rendszer kiterjesztése a csatornákat megkülönböztető jelölésmóddal.
2. A különböző kommunikációs csatornák eltérő tulajdonságainak leírási lehetőségének biztosítása.

A célok megvalósítását a következő módon értük el:

- Jelöljük a protokollban alkalmazott csatornák számát *c*-vel.
- Jelöljük magukat a csatornákat a következőképpen: $ch_1, ch_2, \ldots, ch_c$.
- Az eredeti rendszerben *ENT* jelöli a protokollban résztvevő egyedek körét. Jelöljük ENT_{chi}-vel azon egyedeket, akik a ch_i csatornát tudják használni.
- Jelöljük $CH(ch_i, sec)$-el azt a tényt, hogy a ch_i csatorna védett, és ehhez hasonlóan $CH(ch_i, pub)$ jelölje azt, hogy ch_i nem védett csatorna.
- Amennyiben egy csatorna védett, meg tudjuk adni azoknak a felhasználóknak a halmazát, akik használják a csatornát. Ezt a halmazt jelöljük ENT_{chi}-vel, amennyiben $CH(ch_i, sec)$ teljesül.

A 2. cél elérésére a következőket alkalmaztuk: A csatornák eltérő tulajdonságait a protokollok formalizálása során a kezdeti feltételeknél célszerű megadni.
Ezeket a feltételeket figyelembe véve már lehetőségünk van úgy kibővíteni az eredeti CSN logikai rendszert, hogy az alkalmas legyen a többcsatornás protokollok alapvizsgálataira.
A következő lépésünk a bővítés során a csatorna-jelölés alkalmazása volt a logikai rendszerben. Ennek során az *R* fogadó és *S* küldő operátort kellett megváltoztatnunk, hogy bennük alkalmazhassuk a csatornajelölést. Így az új $R(ch_i, A, t, x)$ operátor jelentése: az *A* egyed a *t* időpillanatban az *x* üzenetet fogadja a ch_i csatornán. Az új $S(ch_i, A, t, x)$ operátor ejlentése: az *A* egyed a *t* időpillanatban az *x* üzenetet küldi el a ch_i csatornán.
Az axiómákat átvizsgálva, az A5, A6, A8, A12 és A15 axiómákat kell átfogalmaznunk a csatornajelek segítségével.

Ahhoz, hogy a többcsatornás protokollokat elemezni tudjuk, egy új A16 jelü axiómát vezettünk be, amely azt rögzíti, hogy: ha a ch_b csatorna védett és a ch_b csatornát *i* és *j* egyedek képesek használni és az *i* egyed a *t* időpontban az *x* üzenetet küldte a ch_b csatornán és a *j* egyed egy *y* üzenetet fogadott a *t′* időpontban a ch_b csatornán és *j* nem fogadott más üzenetet a ch_b csatonán a *t* és *t′* időpontok között, akkor az *x* és *y* üzenetek megegyeznek.
Fromálisan:

$$[CH(ch_b, sec) \land ENT_{chb}=\{i,j\} \land S(ch_b, i, t, x) \land R(ch_b, j, t', y)$$
$$\land\, t'' (t<t''<t' \land \lnot\exists u\, R(ch_b, j, t'', u)] \rightarrow x=y.$$

Tudjuk, számos más feltételt !!!!! rögzíteni lehetne az axiómarendszerben (a különböző támadási lehetőségekből kiindulva finomítani lehet a csatorna-jelölési rendszert), de a bővítést ezen a ponton lezártuk, hogy a kilalakított !!!!! rendszer életképességét gyakorlati szinten is bizonyíthassuk többcsatonás protokollok vizsgálata során.

5. A bővített CSN-logika alkalmazása – A MANA protokollcsalád

A MANuális Authentikáció (MANA) főleg vezetéknélküli (wireless) eszközök hitelesítésére lett kialakítva. Ez a hitelesítés egy nem biztonságos vezetéknélküli csatornát egészít ki manuális

adatátvitellel (mint második csatorna), így biztosítva a megfelelő szintű védelmet. Hasonló megoldásokat használunk e-bank szolgáltatások, Bluetooth eszközök esetén.

Négy protokoll tartozik jelenleg a MANA protokollcsaládba. Ezek között az alapvető különbség a protokoll során felhasznált eszközök tulajdonságaiban van (alkalmazható az eszközön billentyűzet, LED, kijelző képernyő, beviteli gomb, nyomógomb, stb.). A nyilvános csatorna általában gyors és szélessávú; míg a nem nyilvános csatorna általában a manuális csatorna kis kapacitással – a felhasználók olvassák és/vagy írják a csatornajeleket. [5]

A továbbiakban csak a MANA III protokollal foglalkozunk. A MANA I és II protokollok vizsgálatának eredményei elhangzottak a ICAI'07 és Tatracrypt'07 konferenciákon. [12][13]

A MANA III protokoll vizsgálatának eredményei

Ebben a protokollban két eszköz (A és B) és az eszközöket kezelő felhasználó (U - user) vesz részt. Mindkét eszköz rendelkezik egy input egységgel, ami ez esetben egy billentyűzet és egy output egységgel, ami egy egyszerű LED (vagy világít, vagy nem világít). A protokoll célja az, hogy mindkét eszköz bizonyítottan rendelkezzen ugyanazzal az kezdeti paraméterrel (D_A), amelyet a későbbi védett kommunikáció során használhat fel.

A protokoll lépései a következők:

1. Az *A* eszköz generál egy D_A számot. Ezt és azonosítóját (I_A) átküldi a *B* eszköznek a ch_1 csatornán. *B* egy D_B számot és I'_A azonosítót kap a ch_1 csatonán (a ch_1 csatorna nem védett, így feltételezzük, hogy egy támadó képes megváltoztatni az üzenet tartalmát, ezt jelöljük ezen a módon).
2. *B* eszköz a ch_1 csatornán elküldi az I_B azonosítóját. Az *A* eszköz I'_B számot fogad a ch_1 csatornán.
3. Az *U* user egy *R* véletlenszámot generál és ezt a védett ch_2 és ch_3 csatornákon eljuttatja az *A* és a *B* félhez.
4. Az *A* eszköz egy K_1 véletlenszámot generál és kiszámítja az $M_1=m_{K1}(I_A||D_A||R)$ számot (itt || konkatenációt jelent, *m* egy megfelelő hash függvény).
5. Az *A* elküldi M_1-t *B*-nek a ch_1 csatornán. *B* M'_1-t kap üzenetként.
6. *B* egy K_2 véletlenszámot generál és kiszámítja az $M_2=m_{K2}(I_B||D_B||R)$ számot.
7. *B* elküldi M_2-t *A*-nak a ch_1 csatornán. *A* M'_2-t kap üzenetként.
8. Miután *A* fogadja M'_2-t *B*-től (és nem előbb), *A* átküldi K_1 számot *B*-nek a ch_1 csatornán (*B* K'_1-et kap).
9. Amikor *B* megkapja az M'_1 értéket *A*-tól (és nem előbb), *B* átküldi a K_2 számot *A*-nak a ch_1 csatornán (*A* K'_2-t kap).
10. *A* újraszámítja M_2-t. Amennyiben ez megegyezik a *B*-től kapott M'_2 értékkel, úgy *A* erről egy jelet küld (világító LED) *U*-nak a ch_2 csatornán.
11. *B* újraszámítja M_1-t. Amennyiben ez megegyezik az *A*-tól kapott M'_1 értékkel, úgy *B* erről egy jelet küld (világító LED) *U*-nak a ch_3 csatornán.
12. Amennyiben mindkét eszköz sikeres számítást jelez (és csak ekkor), *U* visszajelzi ezt mindkét eszköznek.

Az előbbi protokoll formalizált alakja a következő (t_1, …, t_{24} időpontokat jelöl):

1. $S(ch_1, A, t_1, (D_A, I_A)); R(ch_1, B, t_2, (D_B, I'_A))$
2. $S(ch_1, B, t_3, I_B); R(ch_1, A, t_4, I'_B)$
3. $S(ch_2, U, t_5, R); R(ch_2, A, t_6, R)$
4. $S(ch_3, U, t_7, R); R(ch_3, B, t_8, R)$
5. $S(ch_1, A, t_9, M_1); R(ch_1, B, t_{10}, M'_1)$
6. $S(ch_1, B, t_{11}, M_2); R(ch_1, A, t_{12}, M'_2)$
7. $S(ch_1, A, t_{13}, K_1); R(ch_1, B, t_{14}, K'_1)$
8. $S(ch_1, B, t_{15}, K_2); R(ch_1, A, t_{16}, K'_2)$
9. $S(ch_2, A, t_{17}, x); R(ch_2, U, t_{18}, x)$
10. $S(ch_3, B, t_{19}, y); R(ch_3, U, t_{20}, y)$
11. $S(ch_2, U, t_{21}, z); R(ch_2, A, t_{22}, z)$
12. $S(ch_3, U, t_{23}, z); R(ch_3, B, t_{24}, z)$

A MANA III protokoll vizsgálatánál alkalmazott kezdeti feltételek:

I31. $ENT = \{ A, B, U, \ldots\}; ENT_{ch2}=\{A, U\}; ENT_{ch3}=\{B, U\}.$

I32. $CH(ch_1, pub); CH(ch_2, sec); CH(ch_3, sec).$

I33. A protokollban alkalmazott *m* függvény egy hash függvény. Egyik tulajdonsága: $\forall x,y$ $(m_K(x)=m_K(y) \Rightarrow x=y).$

I34. Az egyedek a paraméterek ismeretében tudják használni *m*-t:
$L_{\{S, t\}}x \Rightarrow L_{\{S, t\}}K \Rightarrow L_{\{S, t\}}m_K x.$

I35. A felhasználók képesek dönteni paraméterek egyenlőségéről:
$L_{\{S, t\}}x \Rightarrow L_{\{S, t\}}y \Rightarrow K_{\{S, t\}}(x=y) \vee K_{\{S, t\}}(x \neq y).$

I36. Kétszer nem küldenek a felhasználók el egy üzenetet:
$\forall t, x\ S(ch_j, i, t, x) \Rightarrow \neg\exists (t', t'>t\ S(ch_j, i, t', x)).$

I37. A protokoll megfelelő időpontjai (t_{14} és t_{16}) után kapott *'1'* üzenetek a helyes működést jelentik az egyedek számára:
$\forall t', t' > t_{16}\ R(ch_2, A, t', '1') \Rightarrow K_{A,t'}(D_A=D_B).$
$\forall t'', t''> t_{14}\ R(ch_3, B, t'', '1') \Rightarrow K_{B,t''}(D_A=D_B).$

I38. Egy időben egy felhasználó egy csatornán csak egy üzenetet küld:
$\forall t, x_1, x_2\ [R(ch_j, S, t, x_1) \Rightarrow R(ch_j, S, t, x_2)] \Rightarrow x_1=x_2.$

1. Tétel:
Tegyük fel, hogy a D_A és D_B paraméterek nem egyenlők a protokoll végrehajtása során (egy illetéktelen felhasználó módosítja a kommunikációt). Ekkor a MANA III protokoll lefutásának a végén az A és B partnerek (eszközök) mindketten tudják azt, hogy $D_A \neq D_B$. Formálisan:

$$D_A \neq D_B \Rightarrow K_{A,t22}(D_A \neq D_B) \wedge K_{B,t24}(D_A \neq D_B).$$

Bizonyítás vázlata:
A bizonyításnál használt axiómajelölések a korábban felsorolt forrásokban találhatók. A tétel

bizonyításának vázlata hasonlít a MANA II protokoll hasonló tételének bizonyításához. A $D_A \neq D_B$ feltételből következően az A5'(a) és A6'(a) axiómák segítségével belátható, hogy a megfelelő M1, M'1 és M2, M'2 függvényértékeket A és B egyedek ki tudják számítani. Mivel a DA és DB értékek paraméterként jelennek meg, így M1 és M'1 valamint M2 és M'2 értékek nem fognak megegyezni, aminek következtében az A16, A3(b) axiómák és az I37 kezdeti feltétel felhasználásával adódik a tétel állítása.

2. Tétel:
Tegyük fel, hogy a D_A és D_B paraméterek egyenlők a protokoll végrehajtása során. Ekkor a MANA III protokoll nem garantálja, hogy lefutásának a végén az A és B partnerek (eszközök) mindketten tudják azt, hogy $D_A = D_B$.

Bizonyítás vázlata:
A bizonyításnál használt axiómajelölések a korábban felsorolt forrásokban találhatók. A tétel bizonyításának vázlata hasonlít a MANA II protokoll hasonló tételének bizonyításához. Belátható, hogy amennyiben $D_A = D_B$, de $K_1 \neq K'_1$ (hasonlóan adódik $K_2 \neq K'_2$), úgy az egyedek számítási módszeréből következik, hogy az összehasonlítások eredménytelenek lesznek. Ez a tény már a tétel állítását adja.

Megjegyzés: Ebben az esetben a felek hiába rendelkeznek a helyes D_A értékkel, annak közös elfogadhatóságát a protokoll nem tudja garantálni. Mivel a K_1 és K_2 kulcsok nyilvános csatornán kerülnek továbbításra, így egy zavaró fél módosítani tudja értéküket, megzavarva a protokollt. Ismételt kulcsküldés már a protokoll hatáskörén kívül esik. Az újra és újra lejátszott eredménytelen protokollismétlések pedig a felhasználók bizalmának elvesztését jelenthetik. Hasonló eset alakulhat ki, mint amikor biztonsági rendszereket kapcsolnak ki a generált téves riasztások elkerülésére.

6. Összegzés

A munkánk során kibővített logikai rendszer alkalmas arra, hogy vizsgáljuk vele a többcsatornás kriptográfiai protokollokat. Ezen eszközök felhasználása bizonyos korlátok figyelembevételével történhet meg csak. [14] A modális logikán alapuló megközelítés csak egyik módja az ilyen rendszerek vizsgálatának. Sok más módszert is ismert annak tanulmányozására, hogy a kommunkációs protokollok milyen erősebb, gyengébb hitelesítési, azonosítási, stb. tulajdonságokkal bírnak. [15] Ezen vizsgálatok gyakorlati alkalmazásai mindenképpen szükségesek, hiszen egyre több olyan eszközt használunk, amelyek egymással kommunkálva segítik életünket. Például a mobiltelefonok vezeték nélkül kapcsolódnak egymáshoz, személyi számítógépekhez, a hálózaton keresztül pedig más kommunikációra képes eszközökhöz. Megjelennek ezek a berendezések a üzleti kommunikációban, a szórakoztatóiparban, de a gyógyítás és rehabilitáció területén is. [16] A több csatorna alkalmazása tehát nem a jövő, hanem már a ma technikája, amit védenünk kell mert sokszor személyes adataik !!!!!! is megjelennek rajtuk.

Irodalom

1. Coffey, T., Saidha, P.: Logic for verifying public-key cryptographic protocols.
IEE Proc. Computers and Digital Techniques, Vol.\ 144. No. 1., 28--32., 1997.

2. Newe, T., Coffey, T.: Formal verification logic for hybrid security protocols.
Comput. Syst. Sci. and Eng., Vol.\ 1., 17--25., 2003.
3. Takács, P.: The Additional Examination of the Kudo-Mathuria Time-Release Protocol. Journal of Universal Computer Science, vol 12, no.9 (2006), 1373-1384.
4. Gehrmann, C., Mitchell, C. J., Nyberg K.: Manual authentication for wireless devices.
Cryptobytes, 7(1) 29--37, 2004.
5. Wong F. L., Stajano F.: Multi-channel protocols.
Proceedings of Security Protocols Workshop, LNCS, Springer-Verlag, 2005.
6. Wong F. L., Stajano F.: Multichannel Security Protocols, IEEE Pervasive Computing. Special Issue on Security and Privacy, 6(4):31-39, Oct-Dec 2007.
7. Wikipedia: Pervasive Computing, Ubiquitous computing.
http://en.wikipedia.org/wiki/Pervasive_Computing
8. Wikipedia: PAN, Personal Area Network.
http://en.wikipedia.org/wiki/Personal_area_network
9. Goeman, S. (ed.): Specification of Prototypes - D11. IST – 2000, 25350 - SHAMAN
Public Report, (2002), 26-29.
10. Windirsch, P. (ed.),: Security for mobile systems beyond 3G.
Presentations and Posters of the IST - 2000 - 25350 - SHAMAN WorShop ,(2002).
11. Gergely, Á.: Biztonságos útvonalválasztás ad hoc hálózatokban. Diplomamunka, Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar, Híradástechnikai Tanszék, Budapest , 2005.
12. Takács, P.: The Extension of CSN-logics: On Examine of Multi-channel Protocols. ICAI - Eger. 2007.01.28-31.
13. Takács, P., Vályi S.: On Verification of the MANA Protocol Family.
7th Central European Conference on Cryptology, Smolenice, June 22-24, 2007.
14. Vajda I., Buttyán L.: Kriptográfia és alkalmazásai. Typotex Kiadó, Budapest, 2004.
15. Buttyán, L.: Formal methods in the design of cyptographyprotocols
(State of the Art). EPFL SSC Technical Report, No.SSC/1999/038. (1999).
16. Borriello G., Stanford V., Narayanaswami C., Menning W.: Guest Editors' Introduction: Pervasive Computing in Healthcare.
IEEE Pervasive Computing, January-March 2007 (Vol. 6, No. 1), pp. 17-19.