Egyetemi doktori (PhD) értekezés tézisei

Kriptográfiai protokollok formális vizsgálata a CSN logikai rendszer bővítésével

Formal examination of cryptographic protocols with the extended CSN-logic

Takács Péter

Témavezető: Prof. Dr. Pethő Attila

Debreceni Egyetem
Természettudományi Doktori Tanács
Informatikai Tudományok Doktori Iskola

Debrecen, 2009

Tartalomjegyzék

Összefoglaló

Értekezésünk tárgya a kriptográfiai protokollok formális alapú vizsgálata. Az első fejezet áttekinti a témát, bemutatja a kutatási munka irányát.

A második fejezet fő célja a kriptográfia alapvető fogalmainak ismertetése és tisztázása. Ez a rész azokat a meghatározó elemeket hangsúlyozza, amelyek a kriptográfiai protokollok elemzéséhez elengedhetetlenül szükségesek.

Ki kell emelnünk a fejezet jelölési módokra vonatkozó részét. A későbbiekben több jelölési rendszert is alkalmazunk. Ennek egyik oka a szakirodalomban kialakult hagyományok követése. A másik ok az alkalmazott logikai rendszer (CSN-logika) viszonylag összetett leírási módja. A hagyományos jelölést a fogalmak tisztázása során használjuk. Az összetettebb jelölési rendszert az általunk elvégzett logikai vizsgálatok során alkalmazzuk.

Hosszabb részt foglal el a fejezetben az alapvető protokollok bemutatása. Ennek oka a protokollok sokrétűségének hangsúlyozása. Az áttekintés bemutatja, hogy az egyes protokollok egymásra épülnek. Az egyik protokoll hiányosságait egy következő javítja. Jellemző a protokollokra az is, hogy igen apró eltérések is zavarokat, támadhatóságot okozhatnak. Ebben a fejezetben bemutatásra kerültek különböző támadási módok (lehallgatás, beékelődő támadás, szótáralapú támadás, stb.). Mindezek a 4. és 5. fejezet tematikáját és eredményeit készítik elő.

A dolgozat harmadik részének célja a kriptográfiai protokollok vizsgálati eszközeinek bemutatása. Ennek során két nagy terület különíthető el. Az egyik a számításelméleti megközelítés, a másik pedig a formális vizsgálat. A kétféle nézőpont napjainkban összefonódni látszik. Ez nyilván a vizsgálati módszerek közös céljából eredeztethető: megbízható, biztonságos, a kitűzött céloknak megfelelő protokollok megalkotása.

A formális módszerek bemutatása során kétféle megközelítést alkalmazunk. A másodikként szereplő osztályozás napjaink felfogását tükrözi.

Vizsgálódásaink eredményeként megfogalmazhatjuk azt az állítást, amely szerint az 1990-es évek végéig végzett kutatások elkülöníthetők a

későbbiektől. Tekinthetjük ezeket az időszakokat I. és II. generációs vizsgálati szakaszoknak. További alapvető változást jelent a protokollok fejlődésében a vezeték nélküli kommunikáció általánossá válása. Ez új eszközrendszert, új protokollokat és új vizsgálati modelleket jelent. Itt kellett szóvá tennünk a protokollok összekapcsolását, a többszereplős és sok esetben nyílt végű protokollokat. Az, hogy az így elkülönített szakaszok tényleges fejlődési fázisokat jelentenek csak hosszabb időtávlatban igazolható. A megközelítés egy új szemléletét jelentheti a tudományterületnek, de a végső törvényszerűségek kibontása további vizsgálatokat igényel.

A CSN logika

Kriptográfiai protokollok vizsgálatának általános sémája modális logikai eszközökkel a következő. Először formalizáljuk a protokollt (vagyis a protokoll-lépéseket leírjuk a formális logika eszközeivel). A második lépés: rögzítjük a kezdeti feltételeket. Harmadik lépésben meghatározzuk a protokoll céljait. Negyedik lépés: alkalmazzuk a logikai posztulátumokat. Az ötödik lépés során összehasonlítjuk az eredményeinket a célokkal. A fő törekvés a protokoll célok származtatása a formális protokollból és a kezdeti feltételekből.

A 3.2.2. fejezetben a formális vizsgálatok első jelentősnek tekintett rendszerét, a BAN-logikát [2] mutattuk be részletesen. A 7.1. fejezet részletesen is tartalmazza a BAN-logika leírását. Ennek oka a 3.2.3. fejezetben leírt CSN-logika összevethetősége a BAN-logikával. A CSN-logika első leírása 1997-ben jelent meg, majd 2003-ban tettek közzé egy jelentős bővítést a logika alkotói (T. Coffey, P. Saidha és T. Newe). [4][10]

Mivel az eredeti források nem tükrözik a matematikai logika elvárt precizitását, saját átdolgozott rendszerünket mutatjuk be. Munkánk során pontosítjuk az alkalmazott logikai nyelvet, a jelölésrendszert, a következtetési szabályokat. Kisebb módosításokat eszközlünk az axiómák körében is.

A negyedik és ötödik fejezet tartalmazza az általunk elvégzett és közleményekben publikált kutatások összefoglalását. A tételek pontos matematikai logikai formáját itt zárójelben közöljük. A jelölésrendszer értelmezése és a teljes logikai rendszer a disszertáció 61-76 és 111-117 oldalain találhatók.

A Kudo-Mathuria-féle időfeloldó protokoll vizsgálata

A negyedik fejezetben kerül bemutatásra az időfeloldó (*time-release*) problémakör története és a K-M-P1 protokoll, amelyet M. Kudo és A. Mathuria dolgozott ki, és elemzett a CSN-logikával. [7] Munkánkban ezt a protokollt vizsgáljuk tovább.

Az időfeloldó titkosítás (time release cryptography) kérdését először Timothy C. May vetette fel 1993-ban. [8] Ennek a protokollnak a célja úgy titkosítani egy üzenetet, hogy azt ne tudja visszafejteni a küldőn kívül senki egy előre meghatározott időpontig (idő-kapszula). Ennek a protokollnak számos alkalmazási lehetősége van: zárt aukciós árajánlatok, hosszú időre titkosított dokumentumok, hosszú-távú tranzakciók, stb.

Ronald L. Rivest, Adi Shamir és David A. Wagner 1996-ban két megoldási módot összegzett, amelyek napjainkban is iránymutatók. [11] Az első megoldás a kiszámíthatóság-elméletre épít. Ekkor egy matematikai rejtvénnyel van dolgunk (time-lock puzzle), amely nem oldható meg csak egy bizonyos idő alatt. A második megoldás egy megbízható T fél bevonását igényli, aki egy meghatározott időpontig titokban tart bizonyos információkat.

Sok kutató foglalkozott 1996 óta mindkét kutatási iránnyal. Michiharu Kudo és Anish Mathuria 1999-ben publikálta azt a kriptográfiai protokollt, amely a második megoldási irányt követi, és amelyet a szerzők matematikai logikai eszközökkel is analizáltak. Kudo és Mathuria a következő tételeket mondják ki és bizonyítják.

G1. Tétel Az A küldő félen és a T szerveren kívül senki nem tudja visszafejteni az időbizalmas adatokat a megadott időpontig.
$(\forall t < t_8 \forall \Sigma \in ENT \backslash \{T, A\} \neg L_{\Sigma,t} d(m, k_{t_8}^{-1}))$

G2. Tétel A B fél vissza tudja fejteni az időbizalmas adatokat a megadott időpontban. $(L_{B,t_9} d(m, k_{t_8}^{-1}))$

G3. Tétel B ismeri az időbizalmas adatok eredetét és átviteli folyamatát az adott protokollban.
$(\forall t < t_6 \; K_{B,t_6} S(\Sigma, t, d(\{n, n_b\}, k_\Sigma^{-1})),\; n = \{e(\{m, r_a, \Sigma\}, k_{t_8}), \Sigma, B, t_8, k_{t_8}\})$

A negyedik fejezetben a $G2$. tételre új bizonyítás mutatunk be.

A 4.3. fejezet bemutatja, hogy a protokoll futása során a passzív támadó

képes lehallgatni a résztvevők közötti kommunikációt. A $G4$. és $G5$. tételek szerint:

G4. Tétel Az E támadó - aki lehallgatja az üzeneteket - ugyanolyan információkkal rendelkezik, mint B a t_9 időpontban, a t_8 időpont után. Vagyis E szintén képes visszafejteni az idő-bizalmas üzenetet.
$(\forall t > t_8 \;\; L_{E,t}d(n, k_{t_8}^{-1}) \; , ahol \; n = e(\{m, r_A, A\}, k_{t_8}))$

G5. Tétel Az abszolút megbízható T fél képes visszafejteni az időbizalmas üzenetet a protokoll befejezése előtt.
$L_{T,t_6}(d(n, k_{t_8}^{-1})) \; , ahol \; n = e(\{m, r_A, A\}, k_{t_8})$.

Ezek nem az eredeti protokoll hibái, az nem köti ki az ilyen irányú védettséget. Kutatásaink során megvizsgájuk a kommunikáció ilyen irányú védelmének lehetőségeit. Két új protokollt alakítunk ki a felmerülő hibák javítására. A kidolgozott K-M-P2 és K-M-P3 protokollokról a $G6$., $G7$. és $G8$. tételekben igazoljuk, hogy már megfelelnek az általunk kitűzött céloknak.

G6. Tétel - A K-M-P2 protokoll esete. Az E támadó (lehallgató) nem képes visszafejteni a titkosított üzenetet a K-M-P2 protokoll használatakor - még akkor sem, ha E ismeri a protokoll teljes üzenetforgalmát.
$(\forall t > t_8 \;\; \neg L_{E,t}d(n, k_{t_8}^{-1}) \; , ahol \; n = e(\{m, r_A, A\}, k_{t_8}))$

A K-M-P2 protokoll $G6$. tétele T egyed esetén nem bizonyítható, mivel T generálja a k_{t_8}, $k_{t_8}^{-1}$ kulcspárt, így ismeri és fel is tudja használni azokat.

G7. Tétel - A K-M-P3 protokoll, T felhasználó esete. Az abszolút megbízható T fél nem képes visszafejteni a titkosított üzenetet a K-M-P3 protokoll használatakor - még akkor sem, ha T a partnerek minden üzenetváltását ismeri. $(\forall t > t_8 \;\; \neg L_{T,t}m)$

Az E egyedre hasonló tételt bizonyíthatunk.

G8. Tétel - A K-M-P3 protokoll, E felhasználó esete. Az üzeneteket lehallgató E fél nem képes visszafejteni a titkosított üzenetet a K-M-P3 protokoll használatakor - még akkor sem, ha E a partnerek minden üzenetváltását ismeri. $(\forall t > t_8 \;\; \neg L_{E,t}m)$

Összefoglalva elmondhatjuk, hogy a passzív támadók (E és T lehallgatói szerepben) a K-M-P1 protokollban közvetített idő-bizalmas üzeneteket képesek megismerni. E a protokoll lefutása után, T pedig már előtte is képes

erre. A javított protokollok esetén K-M-P2 az E támadásának, K-M-P3 pedig E és T támadásának is ellenáll. Ekkor T szerepe a kulcsok generálására és a megfelelő időben történő közlésére korlátozódik. A és B biztos lehet abban, hogy sem E, a lehallgató, sem T, az abszolút megbízhatónak tekintett szerver sem ismeri a titkosított üzenet tartalmát. Ez a tény T számára is előnyös, hiszen az eljárás védi T-t a lehallgatás vádja alól.

A K-M protokoll AVISPA vizsgálata

Ezt követően a 4.4. fejezetben az aktív támadás lehetőségeit vizsgáljuk a K-M-P1, K-M-P2, K-M-P3 protokollokban. A vizsgálatot az AVISPA rendszer segítségével végezzük el. Az AVISPA rendszer (*Automated Validation of Internet Security Protocols and Applications*) egy grafikus felületű (fél-automata) eszköz biztonsági protokollok és alkalmazások automatikus ellenőrzésére. Egy moduláris és rugalmas formális nyelvi eszközt (HLPSL) biztosít a protokollok leírására. Négy különböző elemzési lehetőséget kínál (OFMC, CL-AtSe, SATMC, TA4SP), amelyek különböző szintű analizálási technikák alkalmazását teszik lehetővé. A SPAN alkalmazás kiegészíti az AVISPA rendszert, grafikus felületet nyújtva a fejlesztőknek. [1]

A protokollok leírását és a futási eredményeket a 7.2. fejezet tartalmazza. Összefoglalva elmondhatjuk, hogy a K-M-P1 protokoll támadható, a módosított K-M-P2 és K-M-P3 protokollok esetén viszont már nem mutathatók ki hasonló támadások. Ezek az eredmények a [12][14] közleményekben jelentek meg.

A CSN-logika bővítése többcsatornás protokollok körére

Az ötödik fejezetben tovább bővítjük a CSN-logika alkalmazási körét. A vezeték nélküli kommunikációs megoldások fejlődésével előtérbe kerültek a többcsatornás protokollok. Amennyiben megvizsgáljuk a hagyományos titkos kulcsú kriptográfiai rendszereket, rábukkanhatunk a többcsatornás rendszerek alapjaira. Egy titkos kulcsot védett csatornán tudunk eljuttatni a partnerekhez, utána pedig titkosított üzeneteket tudunk küldeni a nyilvános csatornán. Egynél több csatorna alkalmazása tehát nem új ötlet. Napjainkban a felhasználók sok kommunikációs eszközt tudnak alkalmazni (például: mobil-telefon kamerával, internet, e-mail, fax, stb.). Az alkalmazások több csatorna használatát jelenthetik. Mindezek vizsgálatára egy új kutatási terület látszik formálódni. [18]

A kriptográfiai alkalmazások nagyon gyakran egy kapcsolat-kulcsot (session key) alkalmaznak a kommunikációs folyamatokban a védett kommunikáció támogatására. Habár az ilyen kulcsok használata bonyolultabbá teszi a kriptográfiai rendszereket, alkalmazásuk ugyanakkor jelentősen visszaszorít bizonyos támadásokat. Például nem rögzített kiépítésű hálózatok esetén is (ilyenek a vezeték nélküli hálózatok, amelyek népszerűsége napjainkban nő) szükséges kapcsolat-kulcsok alkalmazása. Ugyanakkor a kulcs-kezelő infrastruktúra kisebb hálózatok esetén (például személyi hálózatok - PAN) nem megoldott.

Egy lehetőség biztonságos kapcsolat- és kulcs-kezelés kiépítésére az emberi beavatkozást alkalmazó hitelesítés. Ez az eljárás nem teljesen automatikus, hanem emberi beavatkozást igényel a protokoll futása során. Például a Bluetooth technológia rövid személyi azonosító-számot alkalmaz az eszközök kapcsolódása során.

Ezekben a protokollokban az emberi közreműködés egy kiegészítő csatonát jelent. Ez lehet egy információ darabnak a begépelése mindkét eszközre, outputok összehasonlítása, adatok átvitele egyik eszközről a másikra. Az ilyen protokollok tipikusan többcsatornás protokollok, általában emberi beavatkozást igénylő kapcsolódási protokolloknak (human assisted pairing protocol) nevezik őket.

Fő eredményünk ebben a körben az, hogy a CSN-logikát sikerült úgy bővítenünk, hogy az alkalmassá vált a többcsatornás protokollok formális vizsgálatára. Munkánk során bővítetjük a CSN-logikát egy új típussal (csatorna típus) és a kapcsolódó axiómákkal, amivel elértük a kívánt célt. Ez a bővítés az 5.3. fejezetben került bemutatásra. Az alkalmazhatóság igazolására a MANA protokollcsalád három protokollját elemezzük.

A kriptográfiai eszközök inicializálása egy olyan eljárás, amelynek során megfelelő kezdeti paramétereket állítunk be. Ezt az eljárást *imprinting* folyamatnak is nevezik. A MANual Authentication protokollok (MANA) más protokollok inicializáló részei. [5][6] Ezekkel az egyszerű protokollokkal a partnerek ellenőrizni tudják, hogy a két eszköz pontosan ugyanazokkal a kiinduló adatokkal rendelkezik.

Négy protokoll (és néhány variáns) tartozik jelenleg ebbe a családba (MANA I-IV, MA-DH, stb.). A protokollok közötti különbség a rendelkezésre álló eszközökben (billentyűzet, LED, képernyő, kijelző, nyomógomb, stb.) és természetesen a protokoll-lépésekben van. A MANA protokoll-család esetén a nyilvános csatorna általában gyors és széles sávú. A nem publikus (védett) csatorna tipikusan manuális csatorna - a felhasználó olvassa és írja a csatornajeleket.

A MANA I protokoll esetén az A és B eszközök próbálnak meg egy közös karaktersorozatban megegyezni. Ez a sorozat lehet például a két eszköz nyilvános kulcsának konkatenációja, vagy más inicializáló paraméterek. Az A eszköz egy kijelzővel és egy egyszerű input gombbal - bináris kapcsolóval - rendelkezik. A B eszköznek egy billentyűzete és egy egyszerű output LED-je van. Mindketten használják a ch_1 nyilvános csatornát (például vezeték nélküli csatorna). Az U felhasználó az eszközök működését és felügyeletét látja el. U két védett (manuális) ch_2, ch_3 csatornát is kezel.

Vizsgálataink során belátjuk, hogy a MANA I protokoll helyesen működik.

5.4.1. Tétel A MANA I protokoll befejezése után mind A és mind B tudja, hogy $n_A = n_B$ teljesül vagy nem.
$(n_A = n_B \rightarrow K_{A,t_{10}}(n_A = n_B) \wedge K_{B,t_{10}}(n_A = n_B)$
$(n_A \neq n_B \rightarrow K_{A,t_{10}}(n_A \neq n_B) \wedge K_{B,t_{10}}(n_A \neq n_B))$

A MANA II protokoll a MANA I protokoll egyszerű változata. Mindkét eszköz rendelkezik egy kijelzővel, és egy egyszerű input kapcsolóval. Az elemzés során olyan támadási pontokat mutatunk be a MANA II (és MANA III) protokollok esetén, amelyek megzavarhatják a protokollok működését.

5.4.2. Tétel Tegyük fel, hogy az (n_A, n_B) paraméterek nem egyenlők. Ekkor a MANA II protokoll befejezése után A is és B is tudja, hogy $n_A \neq n_B$.
$(n_A \neq n_B \rightarrow K_{A,t_{12}}(n_A \neq n_B) \wedge K_{B,t_{12}}(n_A \neq n_B))$

5.4.3. Tétel $n_A = n_B$ nem garantálja, hogy a MANA II protokoll végén A és B tudja, hogy $n_A = n_B$.
$(n_A = n_B \rightarrow \neg K_{A,t_{12}}(n_A = n_B) \wedge \neg K_{B,t_{12}}(n_A = n_B))$

Így kijelenthetjük, hogy a MANA II protokoll csak részben teljesíti a kitűzött célokat. A protokollt módosíthatjuk úgy, hogy kulcsolt hash értékek helyett *„hagyományos"* hash függvényeket (MD sorozat, SHA sorozat, HAVAL, RIPEM sorozat, stb.) [3][9]) használunk. Ekkor feleslegessé válik a kulcsok alkalmazása és a kulcsok átküldése. Erre alapozva új protokollt (MANA II') mutatunk be.

5.4.4. Tétel A MANA II' protokollban a helyesen átküldött n_A paraméter garantálja, hogy a protokoll lezárásakor A és B is tudja, hogy $n_A = n_B$. $n_A \neq n_B$ esetén a MANA II' protokoll lefutása után mind A és mind B tudja, hogy $n_A \neq n_B$.

$(n_A = n_B \rightarrow K_{A,t_8}(n_A = n_B) \wedge K_{B,t_{10}}(n_A = n_B))$
$(n_A \neq n_B \rightarrow K_{A,t_8}(n_A \neq n_B) \wedge K_{B,t_{10}}(n_A \neq n_B))$

A módosított protokoll kialakítása során természetesen figyelembe kell venni a szakirodalom ajánlásait. [9]

A MANA III protokoll esetén az A és B egység próbál egy közös karaktersorozatot kialakítani. Mindkét egységnek billentyűzete és egy egyszerű outputja (LED) van. Mindketten használják a ch_1 nyilvános csatornát. Az U felhasználó az eszközök működését és felügyeletét látja el. U két védett (manuális) ch_2, ch_3 csatornát is kezel. A következő tételeket bizonyítjuk.

5.4.5. Tétel Tegyük fel, hogy az n_A és n_B paraméterek nem egyenlők a protokoll végrehajtása során (egy illetéktelen felhasználó módosítja a kommunikációt). Ekkor a MANA III protokoll lefutásának végén az A és B partnerek (eszközök) mindketten tudják azt, hogy $n_A \neq n_B$.
$(n_A \neq n_B \rightarrow K_{A,t_{22}}(n_A \neq n_B) \wedge K_{B,t_{24}}(n_A \neq n_B))$

5.4.6. Tétel $n_A = n_B$ nem garantálja, hogy a MANA III protokoll befejezésekor A és B tudja,azt, hogy $n_A = n_B$.
$(n_A = n_B \rightarrow \neg K_{A,t_{22}}(n_A \neq n_B) \wedge \neg K_{B,t_{24}}(n_A \neq n_B))$

Így kijelenthetjük, hogy a MANA III protokoll is csak részben teljesíti a kitűzött célokat. Sajnos nem tudjuk a MANA III protokoll olyan módon javítani, ahogy a MANA II javítása lehetséges. Ennek a hibának a javítása egy új protokoll kidolgozását igényli. Ezek az eredmények a [13][15][17][16] közleményekben jelentek meg.

A protokoll-vizsgálat további lehetőségei

A dolgozat hatodik fejezete a protokollok vizsgálatának további lehetőségeit mérlegeli. A gondolatsor legfőbb eleme a protokollok egyre általánosabb használata, a protokollszerű megközelítési mód *terjedése*. Véleményünk szerint hasonló fejlődési szakaszok mutathatók ki a számítógépes hálózatok, a kriptográfiai protokollok és az orvos-szakmai irányelvek területén. A gazdasági- és biztosítási döntéshozatalnál eljárásrendeket, döntési-fákat igyekeznek kidolgozni. Kirajzolódni látszik egy általánosabb protokoll-elméleti megközelítés. Ezeket a tendenciákat, a belőlük levont sejtéseket nem állt módunkban igazolni, további vizsgálatok szükségesek igazolásukhoz, csupán gondolatébresztő szándékkal közöltük őket.

Summary

The theme of this dissertation is to examine cryptographic protocols based on formal methods. In chapter one we survey the direction of our research work.

The aim of the second chapter is to review and clear the basic notions of cryptographic protocols. This part of the dissertation emphasizes crucial elements which are necessary to analyze cryptographic protocols.

We have to highlight the notation part of the chapter. We apply more notations in this chapter. One of the reasons is to follow the traditions of this scientific area. The other reason is the complexity of the applied logical system (CSN-logic). We apply the classical notation to describe basic notations. The more complex notation is used to describe our logical examinations.

The description of the basic protocols is a longer part of the dissertation. The reason of this is to enhance the variety of protocols. The outline presents that the protocols are based on each other. The faults of one protocol are corrected by another. It is also typical of protocols that tiny variances may cause vulnerable points and disorders. Different attack methods (interception, Man in the Middle attack, dictionary attack, etc.) are presented in this chapter. These prepare the programme and results of chapter four and five.

In chapter three the aim is to introduce the examination tools of the cryptographic protocols. Two main parts can be divided. The first one is the computability theory and the second one is the formal examination. The two methods seem to interlock these days. The process of this connection dates back to the common objects and aims of the methods: to construct trusty, secure, adequate protocols.

We apply two methods in the course of the introduction of formal examination. The second classification reflects the approach of our days.

As a result we can state that researches done all at the end of 1990s can be separated from later ones. We can consider these periods I and II generation examination periods. Further basic change in the evolution of protocols is that wireless communication has become general. This situation has created new tools, protocols and examination methods. Here we should

mention the interlocking of protocols, the multi-user and open-ended protocols. The fact that the separated periods are factual evolutionary phases can only be confirmed in longer time perspective. This approach may be a new concept in this area of science but finding the final regularities demands further researches.

The CSN-logic

The general shceme for analyzing cryptographic protocols with modal logic tools are the following. At first: we formalize the protocol (namely we describe steps of the protocol with formal logic). Secondly: we specify the initial assumptions. Thirdly: we specify the goals of the protocol. At the fourth step: we apply the logical postulates. The fifth step is: comparing the results with the goals. The main aim is to deduce the protocol goals from formal protocol and from initial assumptions.

In chapter 3.2.2. we present the BAN-logic [2] as the first significant system of the formal examinations of cryptographic protocols. Chapter 7.1. (Appendix 7.1.) contains the description of the BAN-logic in details. The reason is the contrastability of the BAN-logic and the CSN-logic in chapter 3.2.3. The first description of the CSN-logic was published in 1997 and the creators of the logic (T. Coffey, P. Saidha amd T. Newe) extended it in 2003. [4][10]

As the original sources do not reflect the expected exactitude of the mathematical logic, we present our remodelled CSN-logic. We specify the applied logic language, the notation system and the rules of inferences in our work. We modify the axiom system in lesser degree.

Chapters four and five contain the summary of our researches which we published in scientific papers. We announce the accurate mathematical logic forms of the theorems in brackets. The interpretation of the notation system and the entire logical system can be found on pages 61-76 and 111-117.

The examination of the Kudo-Mathuria time-release protocol

We present the history of the time-release problem and the K-M-P1 protocol in chapter four.

This protocol was worked out and analyzed with the CSN-logic by M. Kudo and A. Mathuria. [7] Henceforth we analyzed this protocol in our research.

The question of time-release cryptography was suggested by Timothy C. May in 1993 for first time. [8] The aim of this protocol is to encrypt a message that cannot be decrypted by anyone (not even by the sender), until a predetermined time (time capsule). This protocol has many applications: closed sales bids in an auction, encrypt documents for long time, long-dated transactions, etc.

Ronald L. Rivest, Adi Shamir and David A. Wagner summarized two solutions in 1996 - which are still acceptable nowadays. [11] The first solution is based on computability. This is a mathematical puzzle (time-clock puzzle) that cannot be solved for at least a certain amount of time. The second one is based on involving a trusted agent - Trent (T) - who promise not to reveal certain information until a specific time.

Many researchers have been dealing with both recommended solutions since 1996. Michiharu Kudo and Anish Mathuria published a cryptographic protocol in 1999, which not only covered the second solution, but it was also analyzed by tools of mathematical logic. Kudo and Mathuria predicate and prove the next theorems.

Theorem G1. Nobody (except A the sender, and T the server) can decrypt the time-confidential data until a specific time.
$(\forall t < t_8 \forall \Sigma \in ENT \backslash \{T, A\} \neg L_{\Sigma,t} d(m, k_{t_8}^{-1}))$

Theorem G2. B can decrypt the time confidential data at a specific time.
$(L_{B,t_9} d(m, k_{t_8}^{-1}))$

Theorem G3. B knows the origin of the time-confidential data and its transmission in the current protocol execution.
$(\forall t < t_6 \; K_{B,t_6} S(\Sigma, t, d(\{n, n_b\}, k_\Sigma^{-1})),\; n = \{e(\{m, r_a, \Sigma\}, k_{t_8}), \Sigma, B, t_8, k_{t_8}\})$

We give a new proof for the Theorem $G2$. in chapter four.

Chapter 4.3. presents that the passive attackers are able to intercept the communication between partners.

Theorem G4. Attacker E - who eavesdrops messages - has the same information as B at time t_9 after the milestone t_8. Namely, E is able to decrypt the time-confidential messages too.
$(\forall t > t_8 \;\; L_{E,t} d(n, k_{t_8}^{-1}) \;,\; n = e(\{m, r_A, A\}, k_{t_8}))$

Theorem G5. The absolute reliable partner T is able to decrypt the time-

release messages before the end of the protocol.
$L_{T,t_6}(d(n, k_{t_8}^{-1}))\ ,\ n = e(\{m, r_A, A\}, k_{t_8})$.

These are not the mistakes of the original protocol because it does not specify this kind of secrecy. We examine this kind of direction of the protection of the communication in our research. We form two new protocols (K-M-P2 and K-M-P3) to revise the occurrent failures. The protocols K-M-P2 and K-M-P3 elaborated by us meet our original requirements as we proved it in the theorem G6, G7 and G8.

Theorem G6. - Case K-M-P2 The attacker E (who eavesdrops all messages) is not able to decrypt the time-confidential message when we use the K-M-P2 protocol. $(\forall t > t_8\ \ \neg L_{E,t} d(n, k_{t_8}^{-1})\ ,\ n = e(\{m, r_A, A\}, k_{t_8}))$

We cannot prove theorem for user T like $G6$. As T generates the k_{t_8} and $k_{t_8}^{-1}$ key-pairs, T knows and can use them.

Theorem G7. - Case K-M-P3 user T T (the absolute reliable partner) is not able to decrypt the time-confidential message when we use the K-M-P3 protocol. $(\forall t > t_8\ \ \neg L_{T,t} m)$

We can prove theorem for user E like $G7$.

Theorem G8. - Case K-M-P3 user E E (who eavesrops all messages) is not able to decrypt the time-confidential message when we use the K-M-P3 protocol. $(\forall t > t_8\ \ \neg L_{E,t} m)$

Our main result is that we establish the passive attackers E and T are able to decrypt the time-confidential message when we use the K-M-P1 protocol. E knows the decrypted message at the end of the protocol and T knows it before the end of the protocol. The K-M-P2 protocol stands against the attack of E and the K-M-P3 stands against the attack of E and T. In this case the role of T is generate keys and provide them in accurate time. A and B are well assured that neither eavesdropper E nor absolute reliable partner T knows the contents of the messages. This fact is advantageous for T because this procedure protects T from charge of eavesdrop.

The AVISPA examination of the K-M protocol

Next we examine the possibilities of the active attack in protocols K-M-P1, K-M-P2, K-M-P3. The examination is achieved with the AVISPA system.

The AVISPA system (*Automated Validation of Internet Security Protocols and Applications*) is a push-button (semi-automated) tool for the automated validation of security protocols and applications. It provides a modular and expressive formal language (HLPSL) for specifying protocols and their security properties. It integrates four different back-end processes (OFMC, CL-AtSe, SATMC, TA4SP) that implement a variety of state-of-the-art automatic analysis techniques. The SPAN application complements the AVISPA system. SPAN gives graphical interface to the developers. [1]

The description of the protocols and the results of running the AVISPA code are in chapter 7.2. (Appendix). To sum up, we state that the protocol K-M-P1 can be attacked but we cannot detect similar attacks in the modified protocols K-M-P2 and K-M-P3. The two examination methods (formal analysis and the semi-automated validation) give the same results. These results were published in [12][14].

The extension of CSN-logic for multi-channel protocols

In chapter five we extend the application range of the CSN-logic further. Multi-channel protocols come to the front by the development of wireless communication solutions. If we examine the traditional secret-key cryptographic systems, we can find the principle of multi-channels. We can share a security key across a protected channel to the partners, afterwards we can send encrypted messages across a public channel. Using more than one channel in a security protocol is not a new idea. Nowadays a user can use many comunication devices (for example: mobile phone with camera, internet pages, e-mail, fax, and so on). These examples mean using more than one channel in the course of communication, too. A new research area is formed to examine the possibilities. [18]

Cryptographic applications very often use session keys in the communication processes to support secure connections. Although session keys complicate the cryptographic systems, at the same time they significantly reduce the possibility of certain attacks. For example, in ad-hoc networks - which have a growing popularity nowadays - it is necessary to apply session keys. At the same time key management infrastructure is not solved in smaller ad-hoc networks (for example in personal area networks - PANs).

One recommended solution to build secure connections and to solve key management problems is human assisted authentication. This authentication procedure is not totally automatic, human assistance is required when the protocols run. For example, the Bluetooth technology uses short personal identification numbers to create associations between devices.

In these protocols, the human assistant is used as an auxiliary channel. This assistance can be, for example, key in the same information to both of the devices or comparing the outputs of the devices or key in data from one device to another device. These protocols are typically multi-channel protocols. These protocols are usually called human assisted pairing protocols.

Our main results is that we can extend the CSN-logic to be able to carry out formal examinations of multi-channel protocols. We extend the CSN-logic with a new type (channel type) and related axioms, so we achieve the wanted goal. It is presented in chapter 5.3. We apply the extended logic to verify validity of three protocols in the MANA protocol family.

The initialisation of cryptographic devices is a procedure of equipping the components with suitable cryptographic parameters. This process sometimes is called *imprinting*. The MANual Authentication Protocols (MANA) are an initialization part of many other protocols (see [5],[6]). With these simple protocols, the partners can verify that the two equipments share the same data exactly.

There are four protocols (and some sub-variants) in this family at present (MANA I-IV, MA-DH etc.). Differences between the protocols are in the availability of devices (device with keypad, LED, screen, display, input button, etc.) and the steps of protocols - evidently. In the MANA protocol family the public channel is generally fast and wideband. The unpublic and secure channel is typically a lowband manual channel - the user reads or writes the channel signs.

In MANA I protocol, device A and device B try to agree on a data strings $n_A = n_B$. For example, this could be the concatenation of the two public keys of two devices or other cryptographic initialization parameters. Device A has a display and a simple input - a binary switch. The other device B has a keypad and a simple output - a LED. They use the public (for example wireless) channel ch_1, and user U helps and supervises them. User U handles two secure channels ch_2, ch_3.

We have established that protocol MANA I is correct.

Theorem 5.4.1 At the end of protocol MANA I, both A and B know whether $n_A = n_B$ or not.
$(n_A = n_B \rightarrow K_{A,t_{10}}(n_A = n_B) \wedge K_{B,t_{10}}(n_A = n_B)$
$(n_A \neq n_B \rightarrow K_{A,t_{10}}(n_A \neq n_B) \wedge K_{B,t_{10}}(n_A \neq n_B))$

The MANA II protocol is a simple variant of MANA I. Both devices (A and B) have a display and simple input switch. We have disclosed such attack points in the protocol MANA II and MANA III with which the process of the protocols can be disturbed.

Theorem 5.4.2. Suppose the parameters (n_A, n_B) are not equal. Then at the end of the protocol MANA II both A and B know that $n_A \neq n_B$.
$(n_A \neq n_B \rightarrow K_{A,t_{12}}(n_A \neq n_B) \wedge K_{B,t_{12}}(n_A \neq n_B))$

Theorem 5.4.3. $n_A = n_B$ does not guarantee that at the end of the protocol MANA II A and B know that $n_A = n_B$.
$(n_A = n_B \rightarrow \neg K_{A,t_{12}}(n_A = n_B) \wedge \neg K_{B,t_{12}}(n_A = n_B))$

So we stress that protocol MANA II satisfies its goals only partially. We can modify the MANA II protocol. We can use conventional hash functions (MD series, SHA series, HAVAL, RIPEM series, etc.)[3][9] instead of keyed hash functions. The use and send of keys will be unnecessary. We develop a new protocol MANA II' based on this case. We can prove the next theorems.

Theorem 5.4.4. $n_A = n_B$ guarantees that at the end of the protocol MANA II' A and B know that $n_A = n_B$. Suppose the parameters (n_A, n_B) are not equal. Then at the end of the protocol MANA II' both A and B know that $n_A \neq n_B$.
$(n_A = n_B \rightarrow K_{A,t_8}(n_A = n_B) \wedge K_{B,t_{10}}(n_A = n_B))$
$(n_A \neq n_B \rightarrow K_{A,t_8}(n_A \neq n_B) \wedge K_{B,t_{10}}(n_A \neq n_B))$

We should followthe literature and practice when we form the changed protocol.[9]

In MANA III protocol, device A and device B try to agree on data strings. Both devices have a keyboard and a simple output (LED). They use the public (for example wireless) channel ch_1, and user U helps and supervises the devices. User U handles two secure channels ch_2, ch_3. We prove the next theorems.

Theorem 5.4.5. Suppose the parameters (n_A, n_B) are not equal (for example

an unauthorized user changed the messages). Then at the end of the protocol MANA III both A and B know that $n_A \neq n_B$.
$(n_A \neq n_B \rightarrow K_{A,t_{22}}(n_A \neq n_B) \wedge K_{B,t_{24}}(n_A \neq n_B))$

Theorem 5.4.6. $n_A = n_B$ does not guarantee that at the end of the protocol MANA III A and B know that $n_A = n_B$.
$(n_A = n_B \rightarrow \neg K_{A,t_{22}}(n_A \neq n_B) \wedge \neg K_{B,t_{24}}(n_A \neq n_B))$

So we stress that protocol MANA III satisfies its goals only partially too. Unfortunately we can not revise the MANA III protocol like MANA II. The correction of this fault require development of a new protocol. These results were published in [13][15][17][16].

Additional possibilities of protocol examinations

We study additional possibilities of protocol examination in chapter six. The main component of the chain of ideas that a new 'protocol aspect thinking' become general. In our opinion similar development phases can be detect in the areas of computer networks, cryptographic protocols and medical guidelines. Similar processes and decision-trees are being worked out in economic and insurance decision-making. A general protocol theory approach seems to outline. We cannot verify these tendencies and conjectures from them. We need more examinations to verify them, so our intension is only thought-provoking.

Irodalomjegyzék

[1] Team AVISPA. AVISPA v1.1 User manual. http://avispa-project.org/package/user-manual.pdf, June 2006.

[2] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactins on Computer Systems*, 8(1):18–36, February 1990.

[3] L. Buttyán and I. Vajda. *Kriptográfia és alkalmazásai*. TypoTex, 2004.

[4] T. Coffey and P. Saidha. Logic for verifying public-key cryptographic protocols. *IEEE Proceedings Computers and Digital Techniques*, 144(1):28–32, 1997.

[5] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *Cryptobytes*, 7(1):29–37, 2004.

[6] S. Goeman. Specification of prototypes - D11, IST - 2000 - 25350 - SHAMAN, Public Report. http://www.isrc.rhul.ac.uk/shaman/docs, March 2003. D11v2.pdf.

[7] M. Kudo and A. Mathuria. An extended logic for analyzing timed-release public-key protocols. In *Proceedings Information and Communication Security, Second International Conference, ICICS'99, Sysdney*, pages 9–11, November 1999.

[8] T. May. Timed-release crypto. In Manuscript; http://www.hks.net/ cpunks/cpunks-0/ 1460.html; Visited: 2009.02.18., 1993.

[9] I. Mironov. Hash functions: Theory, attacks, and applications. Technical Report MSR-TR-2005-187, Microsoft Research, November 2005.

[10] T. Newe and T. Coffey. Formal verification logic for hybrid security protocols. *International Journal of Computer Systems Science & Engineeing*, pages 17–25, 2003.

[11] R. Rivest, A. L. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical Report 684, MIT Laboratory for Computer Science, 1996.

[12] P. Takács. The additional examination of the Kudo-Mathuria time-release protocol. *Journal of Universal Computer Science*, 12(9):1373–1384, 2006. Submitted: 31/12/05, accepted: 12/05/06, appeared: 28/09/06.

[13] P. Takács. The extension of CSN-logic for multi-channel protocols. In *Proceedings of the 7th ICAI Conference, Eger*, pages 147–154, 2007. Reviewed by Zentralblatt für Mathematik.

[14] P. Takács. A Kudo-Mathuria protokoll vizsgálata az AVISPA protokollellenőrző rendszerben. In *II. Nyíregyházi Doktorandusz Konferencia*. Nyíregyházi Főiskola, Nyíregyházi Főiskola, November 2008. Megjelenés alatt. Lektorálta: dr. Ködmön József és Vályi Sándor.

[15] P. Takács and S. Vályi. Többcsatornás kriptográfiai protokollok vizsgálata a bővített CSN-logika eszközeivel. In *I. Nyíregyházi Doktorandusz Konferencia, DE-EK*, December 2007. Megjelenés alatt.

[16] P. Takács and S. Vályi. An extension of protocol verification modal logic to multi-channel protocols. *Tatra Mountains Mathematical Publications*, 41:153–166, 2008.

[17] P. Takács and S. Vályi. Javaslat a MANA II kriptográfiai protokoll korrekciójára. In *Informatika a felsőoktatásban 2008*, Augusztus 2008.

[18] F-L. Wong and F. Stajano. Multi-channel protocols. In *Proceeding of Security Protocols, 13th International Workshop, Cambridge, UK*, volume 4631 of *Lecture Notes in Computer Science*. Springer-Verlag, April,20-22 2005.

List of papers/ Publikációs lista

1. P. Takács *The Additional Examination of the Kudo-Mathuria Time-Release Protocol*, Journal of Universal Computer Science, vol 12, no.9 (2006), 1373-1384. Submitted: 31/12/05, accepted: 12/05/06, appeared: 28/09/06.

2. P. Takács, *The extension of CNS-logic for multi-channel protocols*. Proceedings of the 7th ICAI Conference, Eger, 2007, 147-154.

3. P. Takács, Zs. Kristóf, *The investigation of the development of programming languages*, Proceedings of the 7th ICAI Conference, Eger, 2007, 327-332.

4. P. Takács, S. Vályi, *An extension of protocol verification modal logic to multi-channel-protocols*, Tatra Mountains Mathematical Publications - TATRACRYPT 2007. Editors: O. Grosek, K. Nemoga, M. Vojvoda. Vol. 41. (2008), 153-166.

5. Takács P. *A Windows NT biztonsági jellemzői*, Informatika a Felsőoktatásban'99 Konferencia kiadvány, Debrecen, 1999.

6. Takács P. *Bevezetés az Internet használatába*, Fejezet a Bevezetés az alkalmazott kutatásmódszertanba című tankönyvben, Pro Educatione Alapítvány, Nyíregyháza, 2001. ISBN 963 00 7697 7

7. Takács P. *A kriptográfia időtényezőiről*. Informatika a felsőoktatásban'05 Konferencia kiadvány, Debrecen 2005.

8. Takács P., *Hálózati alapismeretek I., II.* Távoktatási jegyzetek. HEFOP-3.5.1-K-2004-10-0001/2.0 országos pályázat keretében, a Nyíregyházi Regionális Képző Központ vezetésével, 2006. Nyelvi lektor: Takács Ferencné; Szakmai lektorok: Molnár Gábor (Györgyi Gyula, Szemcsák Imre - NYRKK belső lektorok).

9. Takács P., *Adatbázis-kezelés I., II.* Távoktatási jegyzetek. HEFOP-3.5.1-K-2004-10-0001/2.0 országos pályázat keretében, a Nyíregyházi

Regionális Képző Központ vezetésével, 2006. Nyelvi lektor: Takács Ferencné; Szakmai lektorok: Máté István (Györgyi Gyula, Szemcsák Imre - NYRKK belső lektorok).

10. Takács P., Vályi S. *Javaslat a MANA II kriptográfiai protokoll korrekciójára*, Informatika a felsőoktatásban'08, Konferenciakiadvány, Debrecen 2008.

List of talks/ Előadások

1. Takács P., Ködmön J., *Egészségügyi informatika a DOTE Egészségügyi Főiskolai Karán*, Informatika a Felsőoktatásban '96 - Networkshop '96, Debrecen, 1996.

2. Ködmön J., Takács P., *Hálózatbiztonsági technikák az egészségügyben*, Informatika a Felsőoktatásban '96 - Networkshop '96, Debrecen, 1996.

3. Takács P., *Adatvédelem és egészségügy*, XX. Neumann Kollokvium, A számítástechnika orvosi és biológiai alkalmazásai, Veszprém, 1996.

4. Komoróczy T., Takács P., *DOM - Digitális OrvosMúzeum* Networkshop '97, 6. Országos konferencia és kiállítás, Keszthely, 1997.

5. Takács P., *A Windows NT biztonsági jellemzői.* Informatika a Felsőoktatásban '99, Debrecen, 1999.

6. Dr. Iszlai É., Dr. Ágoston S., Dr. Rácz F., Dr. Kapin M., Takács P., Dr. Szerafin L., *Szabolcs-Szatmár-Bereg megyei Helicobacter pylori (H.p.) seroepidemiológiai szűrésen részt vettek további vizsgálata (gastroscopia, szövettan, anti-CagA ea.)*, Magyar Gasztroenterológiai Társaság Endoszkópos Szekciójának ülése, Gödöllő, 2001. aug. 31. - szept. 01.

7. Kántor I., Gaál Zs., Takács P., Dicső F., Valenta B., *Halmozottan előforduló diabetes egy családon belül - MODY?*, Gyermekdiabetalogiai Kongresszus, Dobogókő, 2002.11.25-26.

8. Kántor I., Gaál Zs., A.T. Hattersley, Stenszky V., Takács P. *'MODY 2' betegek utánkövetéses vizsgálata*, Gyermekdiabetologiai Kongresszus, Szeged, 2003.

9. Kántor I., Gaál Zs., A. T. Hattersley, Stenszky V., Takács P., *'MODY 2' betegek utánkövetéses vizsgálata (esetismertetés)* Sz.-

Sz.-B. Megyei Önkormányzat Jósa András Kórház Tudományos Bizottságának Tudományos Ülése - 2003. Évi "Jósa András Pályázat" díjnyertes pályamű. Nyíregyháza, 2004.

10. Takács P., *A kriptográfia időtényezőiről*, Informatika a felsőoktatásban'05, Debrecen 2005.

11. Takács P., Ködmön J., *Az egészségügyi szervező képzés Nyíregyházán*, Informatika a felsőoktatásban'05, Debrecen 2005.

12. P. Takács, *On time-dependent cryptographic protocols and it's allpications*, ISBIS'05 Győr - International Syposium on Business Information Systems, 2005.

13. P. Takács, *On examine of Multi-channel Protocols*, NyírCrypt - 6th Central European Conference on Cryptography. Nyíregyháza, 2006.

14. P. Takács, *The Extension of CSN-logics: On Examine of Multichannel Protocols* ICAI'07 - Eger. 2007.

15. P. Takács, S. Vályi, *On Verification of the MANA Protocol Family*, 7th Central European Conference on Cryptology, Smolenice, 2007.

16. S. Vályi, P. Takács, J. Ködmön, *Algorithmic aspecs of some protocol verification logics*, 7th Central European Conference on Cryptology, Smolenice, 2007.

17. Takács P., Vályi S. *Többcsatornás kriptográfiai protokollok vizsgálata a bővített CSN-logika eszközeivel*, I. Nyíregyházi Doktorandusz Konferencia, DE-EK, 2007.

18. Takács P., Vályi S. *Javaslat a MANA II kriptográfiai protokoll korrekciójára*, Informatika a felsőoktatásban '08, Debrecen, 2008.

19. Kristóf Zs., Csajbók Z., Takács P., Bodnár K., Ködmön J. *Azonosítón alapuló kriptográfiai rendszerek alkalmazása eLearning környezetben*, Multimédia a felsőoktatásban '08 konferencia, Budapest, 2008.

20. Takács P. *A Kudo-Mathuria protokoll vizsgálata az AVISPA protokollellenőrző rendszerben.*, II. Nyíregyházi Doktorandusz Konferencia, Nyíregyházi Főiskola, 2008.