

Támadások egy és többprotokollos környezetekben

GENGE Béla¹, dr. HALLER Piroska²
^{1,2}“Petru Maior” Egyetem, Marosvásárhely, ROMÁNIA
{¹bgenge, ²phaller}@upm.ro

Abstract. We examine several security protocol specification methods discussing the possible advantages and disadvantages these introduce. By using the mentioned specifications we present different type of attacks in single and multi-protocol environment. We also propose an extension of a specification model that allows a formal analysis of multi-protocols.

1. BEVEZETŐ

Adatbiztonsági protokolloknak nevezzük azokat a kommunikáció protokollokat, amelyekben a kódolás arra a célra van felhasználva, hogy az adatokat kizárólag a protokoll résztvevői érhessek el. Az adatbiztonság protokollokat a kutatók több évtizede elemzik, de az általános leírási modell hiánya többféle elemzési módszer kialakulásához vezetett az évek során [1, 2].

Az említett elemzési módszerek többsége használja a Dolev-Yao támadó modellt [3], amelyben a támadó teljes hatalmat gyakorol a hálózatra. Elemezve külön mindegyik protokollt a Dolev-Yao támadó jelenlétében, az irodalom többféle támadást is megemlít [4]. Gyakorlatban, több protokoll is futhat ugyanazon a hálózaton, így a támadónak új lehetőségei nyílnak, mivel az üzeneteket át lehet küldeni egyik protokollból a másikba. Ezeket a támadásokat *többprotokollos támadásoknak* nevezzük [4].

Ebben a dolgozatban bemutatunk több leírási módszert és vizsgáljuk hogy lehet azokat felhasználni a támadások elemzésében. Bizonyítva hogy a létező leírási módszerek nem biztosítják a többprotokollos támadások felderítését, javasoltuk a létező leírások kiterjesztését új tulajdonságokkal.

2. ADATBIZTONSÁGI PROTOKOLLOK LEIRÁSA

Mielőtt bemutatnánk az adatbiztonsági protokollok legismertebb támadásait, meg kell ismernünk a jelen dolgozatban használt protokoll leírási módszereket:

- *Reguláris leírás* – a leggyakrabban használt az irodalomban;
- *Üzenet szekvencia diagramok* – hasznosok mikor a protokoll szereplőit vizuálisan ki akarjuk emelni.

A megnevezett leírási módszerek nem biztosítanak egy formális nyelvet, amely segítségével ellenőrizni lehet a protokollt. Több formális leírást is kidolgoztak, melyek lehetővé teszik a leírások elemzését. A protokollok biztonságának elemzésére a *strand-tér* modell alapú leírást javasolja a szakirodalom [1, 5, 6].

2.1 Adatbiztonsági protokollok leírási nyelve

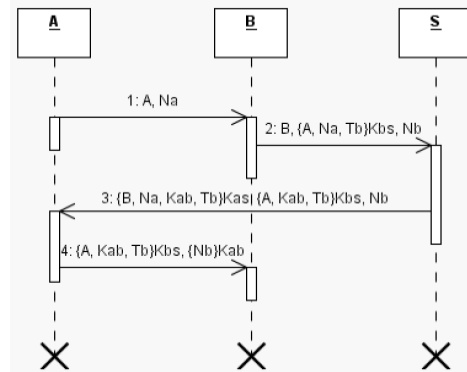
A legtöbb protokoll leíró nyelv használja a reguláris leírásban található szimbólumokat. A nagybetűk képviselik a protokoll szereplőit (pl. A, B, C, S, I). A véletlen számok vagy egyedi üzenetszámok (*nonce* “number once used”) egyszer elküldött adatok és N_x szimbólummal jelöljük, ahol x a generáló szereplő nevét képviseli (pl. N_a , N_b).

A kulcsokat K_x szimbólumokkal jelöljük, például K_{ab} , K_a , K_b . A kódolt adatokat kapcsos zárójelbe írjuk és a kódolási függvény nevét a zárójel után tüntetjük fel. Például: sk szimmetrikus kódolást jelent; pk aszimmetrikus kódolást (nyilvános kulccsal); pvk

aszimmetrikus kódolást (személyes kulccsal); h hasító függvényt jelent. Ahhoz, hogy a leírás kevésbé bonyolult legyen, ha szimmetrikus kódolást használunk a függvény neve elhagyható.

A reguláris leírás (1.a. ábra), az egyszerű formátuma és informatív tulajdonsága miatt, a legismertebb ezen a területen. A megemlített leírás nem tartalmaz implementáció-specifikus adatokat, illetve az üzenetek feldolgozására vonatkozó információt.

A, B, S: résztvevők neve
 Na, Nb: véletlen számok
 Kbs: hosszú tavu kulcs
 Kab: rövid tavu kulcs
 $A \rightarrow B: A, B, \{A, Na, Kab\} Kbs$
 $B \rightarrow S: \{Na, Nb\} pk(S)$
 $S \rightarrow B: \{\{Nb\} h\} pvk(S)$

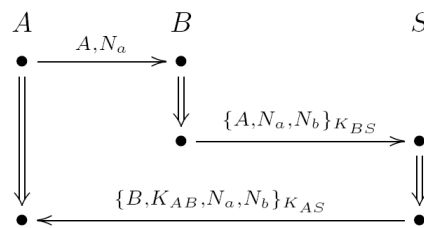


a) Normal protokoll leírás

b) Üzenet szekvencia diagram protokoll leírás

1. ábra Adatbiztonság protokollok leírása

Egy vizuálisabb protokoll leírás az üzenet szekvencia diagramokon alapszik (1.b. ábra). Használata előnyös, ha szükséges kiemelni a protokoll résztvevői közti üzenetküldési szekvenciákat, lehetővé téve a támadások ábrázolását is.



2. ábra Strand protokoll leírás

2.2 Az esemény-tér modell

Az említett leírásokból hiányzik egy formális eszköz, amely megengedné a protokollok automatikus ellenőrzését. Több esemény-tér modell alapú formális leírás létezik ilyen, például strand-tér modell [1].

Egy *strand* egy esemény sorozat, melyet a protokoll egy résztvevője küld illetve fogad. Ha az adott szereplő több protokollt futtat egyszerre, minden protokollban más strand jellemzi. Egy strand halmazt nevezünk *strand térnek*. A strand tér tartalmazza a protokoll résztvevőinek és a támadóknak a strand-ját.

Az említett modell (2. ábra) nem csak egy grafikus ábrázolási módszer, hanem egy formális nyelv is. Lehetővé teszi az ellenőrzéshez szükséges feltételek formális leírását is. Például, ellenőrizhető hogy egy adott üzenet rész Na attól érkezett akitől várták (A):

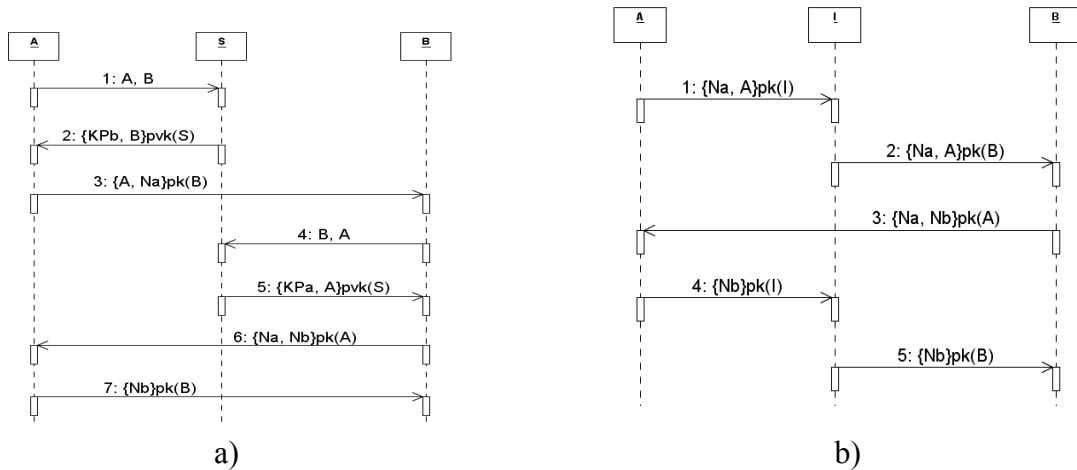
$$\exists n \in \mathcal{N} : sign(n) = + \wedge role(strand(n)) = A \wedge Na \subseteq term(n)$$

3. ADATBIZTONSÁGI PROTOKOLL TÁMADÁSOK

Mielőtt bemutatnánk hogyan épülnek fel a többszörös protokoll támadások, szükséges áttekinteni az egyes protokoll támadások felépítését.

3.1 Protokoll támadások

Az egyik leggyakrabban említett támadás a szakirodalomban a közbeékelődéses támadás (3. ábra). A támadó elindít egy új autentifikálási szekvenciát az A szereplővel. A válaszol mert nem ismeri fel a támadót. Ugyanakkor, párhuzamosan a támadó elindít egy kulcszcere protokollt B-vel ki azt gondolja, hogy A-val kommunikál.



3. ábra a) – Needham-Schroeder protokoll; b) – közbeékelődéses támadás a Needham-Schroeder protokoll-ra

Más támadások elemzése is hasonló módon történik, mint például visszatükrözéses támadás, visszajátszásos támadás. Helyhiány miatt, a megnevezett támadásokat nem mutatjuk be a dolgozatban, bővebben áttekintés a [3, 4, 7] dolgozatokban.

3.2 Többszörös-protokoll támadások

Ezek a támadások olyan környezetekben fordulnak elő, hol több mint egy protokoll fut egyszerre ugyanazon a csomóponton. Ilyen esetekben, a támadónak a rendelkezésére állnak üzenetek más protokollokból is, így támadásokat tud létrehozni olyan protokollon is amely helyesnek bizonyult egyszerűbb környezetben (4.ábra).

A → B: A, Na

B → S : { A, Na, Nb } K_{bs}

S → A : { B, Kab, Na, Nb } K_{as}

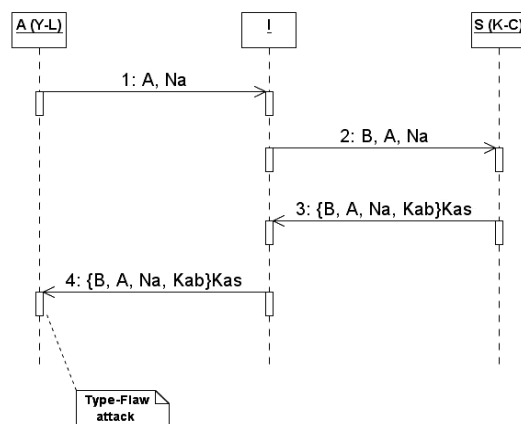
a) Yahalom-Lowe protokoll

A → S: A, B, N'a

S → B: { A, B, N'a, K'ab } K_{as},
 { A, B, N'a, K'ab } K_{bs}

B → A: { A, B, N'a, K'ab } K_{as}

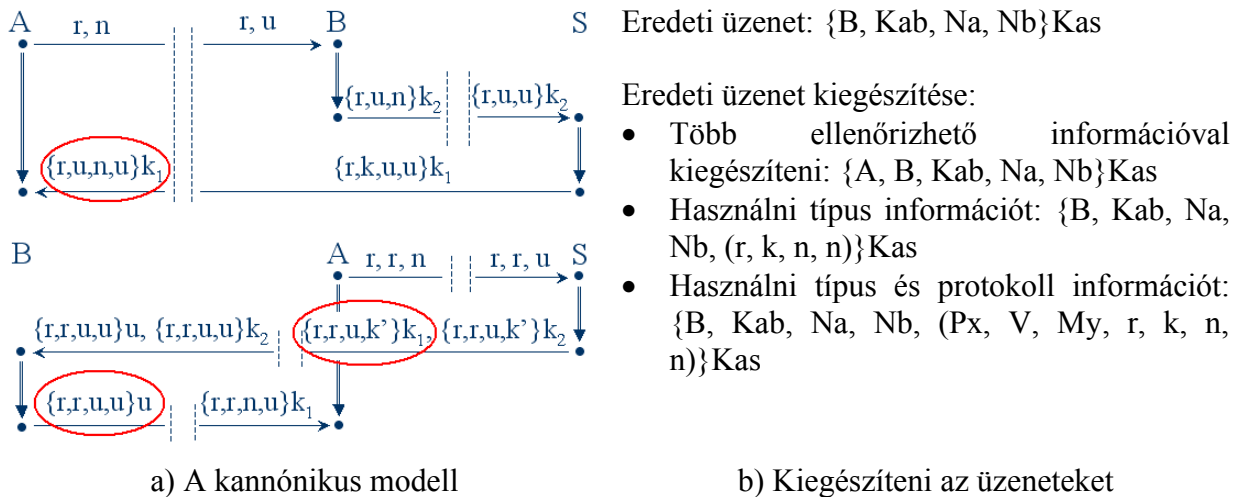
b) Kao-Chow protokoll



2. ábra Típus tévesztés támadás többszörös protokoll környezetben

3.3 Ellenőrizni a protokollok önállóságát

Ahhoz, hogy le tudjuk ellenőrizni két protokoll biztonságos használatát ugyanabban a környezetben, javasoltuk a strand tér kiterjesztését. Minden üzenethez hozzárendeljük még küldéskor a forrás azonosítóját, minden mező típusát, illetve a protokoll típusát és verzióját, létrehozva egy kannonikus modellt [7]. Az üzenet fogadásakor minden mezőre ellenőrizzük annak típusát. A továbbiakban bemutatjuk ennek alkalmazását a Yahalom-Lowe és Kao-Chow protokollok leírására (5a. ábra). Itt tisztán látható, hogy egy támadás létrejöhet mivel az üzenetek túlságosan kevés információt tartalmaznak a résztvevők számára. Ahhoz, hogy a támadás ne történjen meg és a protokollok önállóak legyenek, ki kell terjeszteni az üzeneteket több információval (5b. ábra).



5. ábra Egy kannonikus modell protokoll ellenőrzésre

4. ÖSSZEFOGLALÁS

Ebben a dolgozatban bemutattunk többféle adatbiztonság protokoll leírást és több támadást ami az említett protokollokat illeti. Ugyanakkor, mindenik leírás esetében megemlítettük az előnyöket és hátrányokat a támadások felderítésének szempontjából. és a többszörös protokoll támadások esetében bemutattunk egy kannonikus modellt mely egyszerűsít az elemzés automatizálásán. Szintaktikusan elemezve a Yahalom-Lowe és Kao-Chow protokollokat kimutatható egy támadási lehetőség de a típusinformációval kiegészített a protokollok esetében a támadás többet nem jöhet létre.

IRODALOM

- [1] F.J.T. Fabrega, J.C. Herzog, J.D. Guttman, "Strand Spaces: Proving security protocols correct", Journal of Computer Science, Vol. 7, 1999, pp. 191-230.
- [2] C. Weidenbach, "Towards an automatic analysis of security protocols", In the Proc. of the 16th International Conference on Automated Deduction, 1999, pp. 378-382.
- [3] D. Dolev, A. Yao, "On the security of public-key protocols", IEEE Transactions on Information Theory, Vol. 29, 1983, pp. 198-208.
- [4] C.J.F. Cremers, "Feasibility of Multi-Protocol Attacks", In the Proc. of the first ARAS conference, 2006.
- [5] Hyun-Jin Choi, "Security protocol design by composition", Cambridge University, UK, Technical report Nr. 657, UCAM-CL-TR-657, ISSN 1476-2986, 2006.
- [6] A.D. Gordon, A. Jeffrey, "Authenticity by Typing for Security Protocols", Journal of Computer Security, Vol. 4, 2003, pp. 451-520.
- [7] B. Genge, I. Ignat, "Verifying the independence of security protocols", In the Proc. of the 3rd IEEE International Conference ICCP, 2007, pp. 155-163.