Köztesréteg adatbiztonsági protokollok megvalósítására

GENGE Béla[1], dr. HALLER Piroska[2]
[1,2] "Petru Maior" Egyetem, Marosvásárhely, ROMÁNIA
{[1]bgenge, [2]phaller}@upm.ro

Abstract

This paper presents a Web service based middleware, which ensures secure access to distributed system resources. The client application frequently runs multiple security protocols simultaneously to communicate with different resources. The proposed formal description and implemented middleware guarantee the automatic discovery, interrogation, composition and execution of the required security protocol, thus performing the dynamic creation of secure connections.

Abstract
Scopul lucrării este crearea unei platforme intermediare bazată pe servicii Web, care asigură accesul securizat la resursele unui sistem distribuit. În majoritatea cazurilor aplicațiile client rulează simultan mai multe protocoale de securitate pentru a comunica cu diferite resurse. Platforma şi descrierile formale propuse oferă posibilitatea interogării şi executării automate a protocoalelor de securitate, adică construirea dinamică a sistemelor sigure.

Összefoglaló
A dolgozat célja egy webszolgáltatásokra épülő köztesréteg kidolgozása mely lehetővé teszi az erőforrások biztonságos elérését nagy osztott rendszerek esetén. Sok esetben a kliens alkalmazás egyidőben többféle adatbiztonsági protokollt futtat, különböző erőforrások elérése érdekében. A javasolt formális leírás és köztesréteg biztosítja a leírások biztonságos lekérdezését, értelmezését és a protokollok automatikus kezelését.

1. BEVEZETŐ

Adatbiztonsági protokolloknak nevezzük azokat a kommunikációs protokollokat, amelyek célja, hogy az adatokat kizárólag a protokoll részvevői érhetik el. Jelenleg számos adatbiztonsági protokoll létezik egyidejűleg a web-en. A protokollok formális leírása nem csak ezek ellenőrzését teszi lehetővé, hanem a lebontását is egyszerűbb függvényekre. A kompozíció [1, 2, 3] az a folyamat amelyben bonyolult adatbiztonsági protokollt építünk fel létező protokollok szekvenciális összerakásából. A létező módszerek a kompozíciót úgynevezett „off-line" mechanizmusként kezelik. Egy alkalmazás csak akkor használhat egy adatbiztonsági protokollt ha az adott csomópont azt implementálta. Kevés erőforrással rendelkező eszköz esetén több protokoll egyidejű megvalósítása nem lehetséges. Ebben az esetben szükséges egy dinamikus „on-line" rendszerben alkalmazható kompozíció[4]. Ugyanakkor a kompozíció során generált protokollt a rendszerben levő csomópontok képesek kell legyenek végrehajtani.

Ebben a dolgozatban bemutatunk egy köztesréteget, mely biztosítja a leírások biztonságos lekérdezését, értelmezését és automatikus kezelését. A köztesréteg komponensei webszolgáltatások, melyek biztosítják az adatbiztonsági protokollok meghirdetését, megtalálását, létrehozását, komponálását, végrehajtását. A webszolgáltatások[5] adott ontológián értelmezett szemantikus adatokkal való ellátása lehetővé teszi e feladatok automatizálhatóságát.

Minden szolgáltatás biztosít egy interfészt amelyen keresztül más szolgáltatás is hozzáférhet. A webszolgáltatások leírására a WSDL-S [6] és OWL [7] nyelveket használtuk.

2. A KÖZTESRÉTEG ARCHITEKTÚRÁJA

2.1 Szolgáltatás orientált architektúra

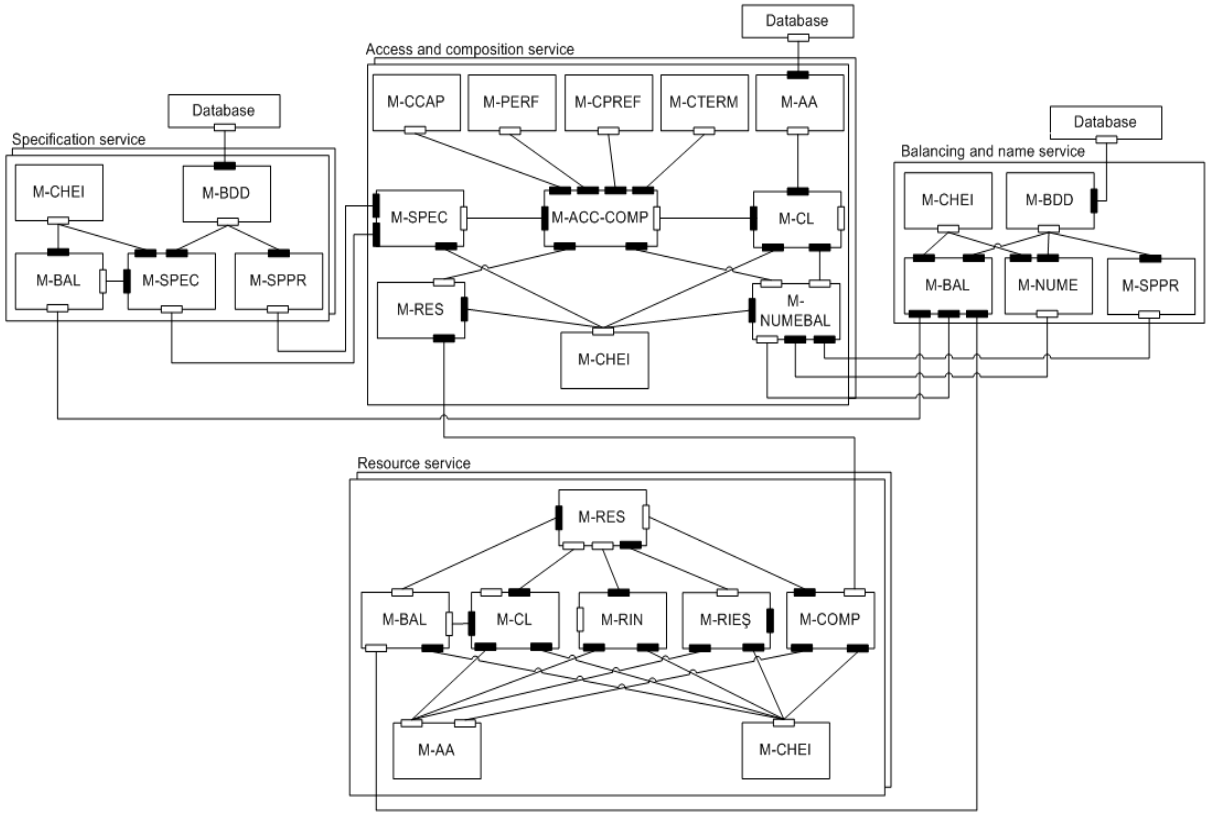
A javasolt köztesréteg [1. ábra] négy szolgáltatást foglal magába: névszolgáltatás, leírás tároló szolgátatás, kompozició szolgáltatás, erőforrás tároló szolgáltatás, az utóbbi háromból több is jelen van egyidőben a rendszerben.

A platformhoz a hozzáférés a névszolgáltatáson keresztül történik, mely biztosítja a szolgátatások regisztrálását, keresését, kiválasztását. Mint egyedi belépési pont, ez a szolgáltatás lehetővé teszi a terhelés kiegyenlítését is a rendszerben. Az adatokat egy adatbázisban tároljuk és lekérdezésükre HTTP-GET protokollt használunk.

A leírás tároló szolgátatás hozzáférhetővé teszi az eddig létrehozott adatbiztonsági protokoll leírásokat beleértve a leírások alapjául szolgáló ontológiákat is. Minden leírás digitális aláírással védett.

Az erőforrás tároló szolgáltatás a kliens által elérhető erőforrások halmaza, a hozzájuk rendelt biztonsági követelményekkel illetve az általuk elfogadott biztonsági protokollal. Ezek típusa igen változatos lehet: multimédia szolgáltatások, elektrónikus fizetési szolgáltatások, kereső szolgáltatások.

A belépési és kompozició szolgáltatás biztosítja a kliens hozzáférését a kért erőforrásokhoz. A kompozició szolgáltatás felhasználja a leírásokat, a kliens által kért források képességeit és összeállít egy új leírást illetve elvégzi az üzenetek kompozicióját. A szolgáltatás figyelembe veszi a protokollok előfeltételeit és utófeltételeit az új leírás létrehozásánál.

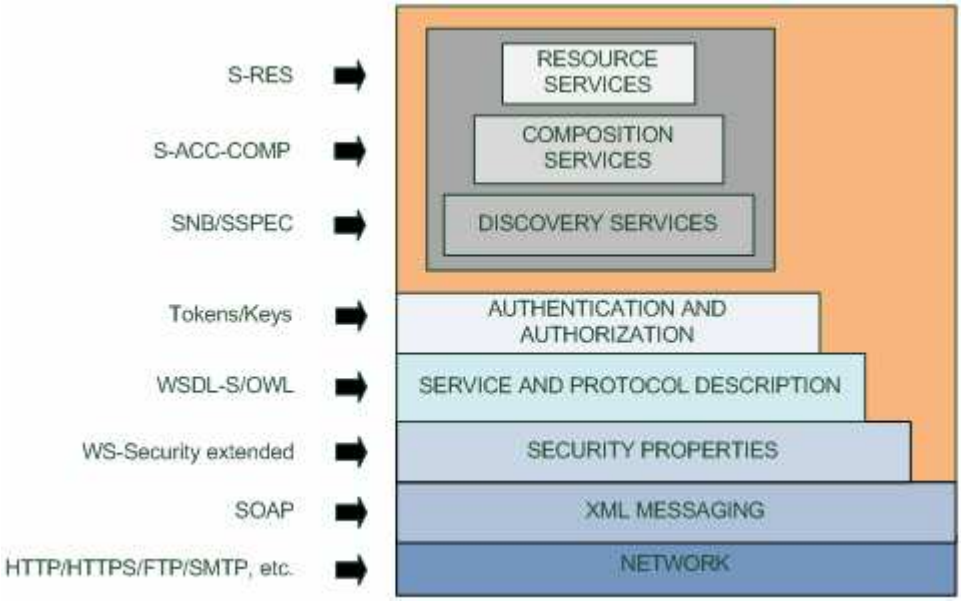


1. ábra A platform szolgáltatás-orientált arhitektúrája

2.2 Szoftver architektúra

A köztesréteg adat kommunikációja XML üzeneteken keresztül történik és a következő szint adatbiztonsági tulajdonságokat csatol az XML üzenetekhez. Ez lehetővé teszi a szolgáltatások leírásának biztonságos lekérdezését. A szolgáltatások közötti zsetonalapú hozzáférhetőségi rendszer biztosítja a kliens azonosítását a belépési szolgáltatáson keresztül.

A belépési és kompozició szolgáltatás megkeresi a felhasználó által kért erőforrásokat és a szemantikus leírásokat felhasználva automatikusan végrehajtja az adott protokollokat.



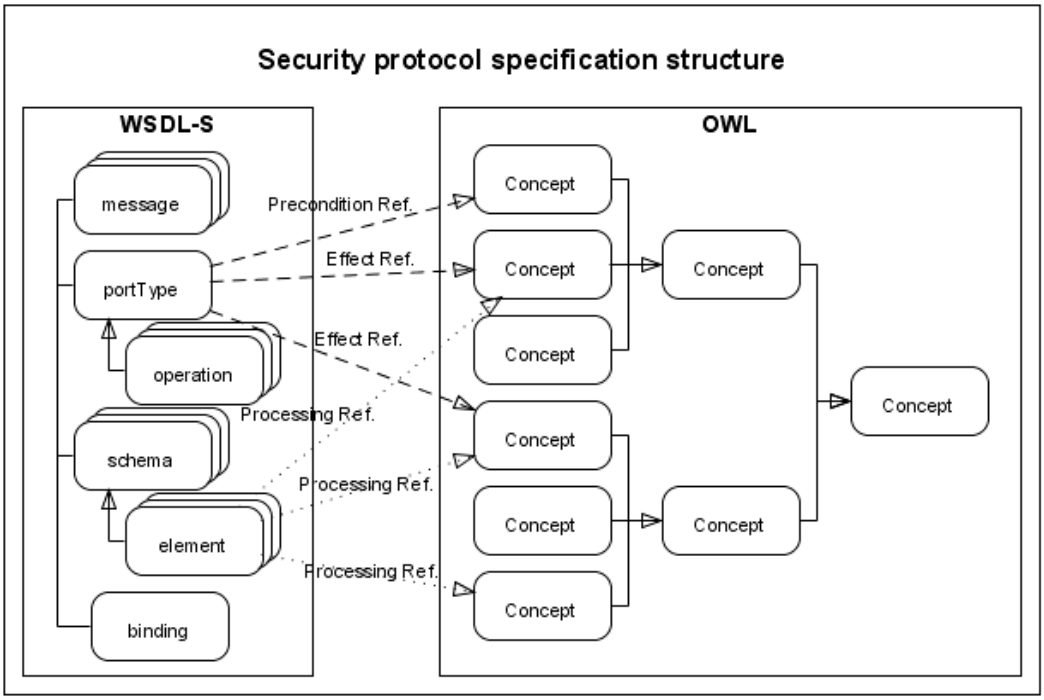
2. ábra A platform szofver architectúrája

3. A LEÍRÁSOK STRUKTURÁLIS FELÉPÍTÉSE

Az adatbiztonsági protokollok leírása az alábbi követelményeknek kell eleget tegyen:

- tartalmazza az üzenet minden komponensének a típusát
- megnevezi a protokoll részvevőit
- leírja a használt kriptográfiai algoritmusokat
- leírja az üzenet felépítését
- megadja a részvevők elérhetőségét és a használt adatátviteli protokollt
- tartalmazza az előfeltételeket és a végrehajtás hatását

Annak érdekében, hogy a protokollok automatikusan végrehajthatóak legyenek javasoltunk egy két részből álló leírást. A szekvenciális leírás az üzenet szekvenciák megnevezését tartalmazza, melyekhez csatlakoznak szemantikus címkék.



3. ábra A leírások strukturális felépítése

Egy végrehajtható adatbiztonsági protokoll leírásához a protokoll informális leírásából indulunk ki. Ez tartalmazza a protokoll részvevőit, az üzenet komponenseit és irányát, a használt kriptográfiai algoritmusokat.

$$A \rightarrow \mathrm{B}: A, N_a$$
$$B \rightarrow \mathrm{A}: \{N_a, K, B\}_{K_{AB}}$$
$$A \rightarrow \mathrm{B}: \{N_a\}_K$$
$$B \rightarrow \mathrm{A}: N_b$$

4. ábra A „BAN Concrete Secure RPC” protokoll informális leírása

Ez a leírás azonban nem elég mert nem tartalmaz információt az üzenetek felépítéséről, feldolgozásáról ellenőrzéséről illetve a részvevők elérhetőségéről.

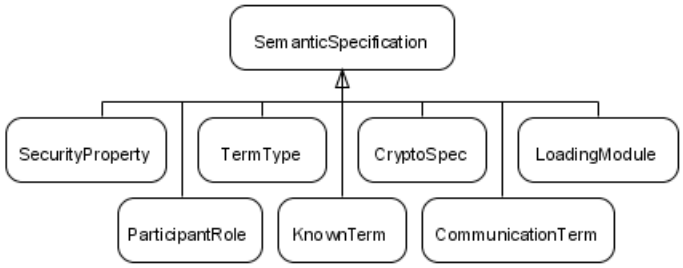
A szekvenciális leíráshoz a WSDL-S használtuk mely lehetővé teszi a paraméterek hozzárendelését az ontológia elemekhez, az elő és utófeltételek megadását. A szekvenciális komponens leírásának egyik része látható a 5. ábrán. Az egyik feltüntetett előfeltétel a kezdeményező szerepe melyet XML formátumban *Initiator_role* címkével jelöltünk. A protokoll végrehajtásának a hatása egy kulcscsere a protokoll résztvevői között, lásd a *Session_key_exchange* címkét.

5. ábra Egy része a szekvenciális leírásoknak

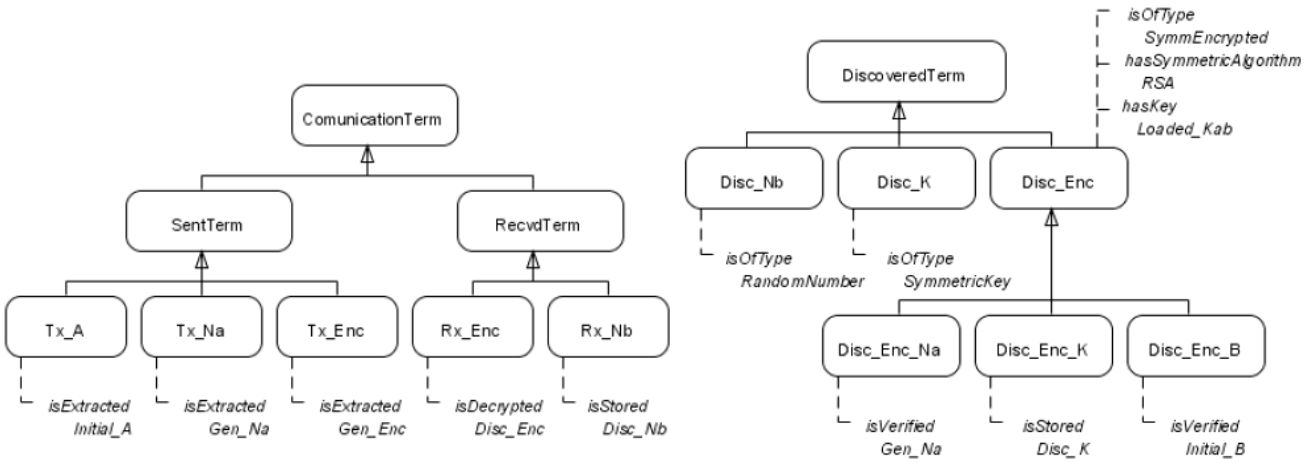
```
<wsdl:portType name="Encrypted communication">
  <wsdl:operation name="Msg1">
    <wsdl:output message="tns:Msg1Request"/>
  </wsdl:operation>
  ...
  <wssem:precondition name="Initiator"
    wssem:modelReference=".../SecProt.owl#
                          Initiator_role"/>
  <wssem:effect name="SessionKeyExchange"
    wssem:modelReference=".../SecProt.owl#
                          Session_key_exchange"/>
</wsdl:portType>
```

A szekvenciális leírás minden eleméhez (előfeltétel, küldött vagy fogadott tag, hatás...) tartozik egy ontológia.

A szemantikus komponensek közül az alábbiakban láthatóak az adatbiztonsági protokollok általános ontológia fogalmai illetve a különböző üzenetekhez rendelt fogalmak és tulajdonságok.



6. ábra Általános fogalmak



7. ábra Kommunikációs fogalmak

Végül a megadott ontológiák segítségével leírjuk a generálási illetve ellenőrzési szabályokat.

4. Következtetések

A köztesréteg tesztelésére 13 adatbiztonsági protokollt írtunk le formálisan és rendeltünk hozzá erőforrás szolgáltatásokhoz. A kliens minden esetben több erőforráshoz akart csatlakozni. A kompozició szolgáltatás letöltötte a megfelelő leírásokat, felépítette az összetett protokollt. A tesztek bizonyították hogy a leírások elég információt tartalmaznak a protokollok sikeres végrehajtásához és a végrehajtás eredményeként az erőforrások eléréséhez. Újabb protokollok hozzáadása nem változtat a köztesréteg felépítésén csak az egyes szolgáltatások tudásbázisát kell bővíteni. A rendszer tovább bővíthető az algoritmusok dinamikus megvásztásával abban az esetben ha a két fél több lehetőséget is kínál.

IRODALOM

[1] Hyun-Jin Choi, “Security protocol design by composition”, Cambridge University, UK, Technical report Nr. 657, UCAM-CL-TR-657, ISSN 1476-2986, 2006.

[2] Cas J. F. Cremers, Compositionality of Security Protocols: A Research Agenda, Electr. Notes Theor. Comput. Sci., 142, pp. 99-110, 2006.

[3] S. Andova, Cas J.F. Cremers, K. Gjosteen, S. Mauw, S. Mjolsnes, and S. Radomirovic, A framework for compositional verification of security protocols, to appear, 2007.

[4] Genge Bela, Iosif Ignat, Verifying the Independence of Security Protocols, 3rd IEEE International Conference on Intelligent Computer Communication and Processing, Cluj-Napoca, Romania, pp. 155-163, September 2007.

[5] K. Gottschalk, S. Graham, H. Kreger, J. Snell, Introduction to Web services architecture, IBM Systems Journal, Vol. 41, No. 2, pp. 170-177, 2002.

[6] R. Akkiraju, J. Farrell, J.Miller, M. Nagarajan, M. Schmidt, A. Sheth, K. Verma, Web Service Semantics - WSDL-S, A joint UGA-IBM Technical Note, version 1.0, April 18, 2005.

[7] World Wide Web Consortium, OWL Web Ontology Language Reference, W3C Recommendation 10 February 2004.