Biztonságos szolgáltatások kihelyezése mobil eszközök számára

SZENTGYÖRGYI ATTILA, SZÜTS PÉTER LÓRÁNT

Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék
{szgyi, szuts}@alpha.tmit.bme.hu

Lektorált

Kulcsszavak: WLAN, mobil eszközök, PDA, Security Proxy, titkosítás, adatbiztonság

Napjainkban egyre többen használnak kézi számítógépet (Personal Digital Assistant, PDA) és okostelefont (Smartphone). A hordozhatóságból származó előnyt azonban beárnyékolja az eszközök számára rendelkezésre álló limitált erőforrások mennyisége: a processzor teljesítménye és a memóriaterület mérete. Az erőforráshiány következtében a biztonságos hálózati szolgáltatások igénybevételénél adatátviteli sebesség csökkenést tapasztalhatunk. Emellett számos olyan biztonságos kommunikációt használó szolgáltatással is találkozhatunk, amelyek a mobil eszközök számára mindeddig nem álltak rendelkezésre. A problémák megoldásához egy olyan eljárást kerestünk, amely a biztonságos kommunikáció megtartása mellett nem csökkenti az adatátvitel sebességét, és lehetővé teszi új, a mobil eszközök számára eddig elérhetetlen szolgáltatások igénybevételét. Vizsgálódásaink eredményeként megszületett egy erre a célra alkalmas megoldás; a Security Proxy (SP).

1. A Security Proxy működése

A Security Proxy [9] a mobil eszközök megbízásából (Proxy) biztonságos kapcsolatot épít ki az Internet egy távoli szerverével, és így a készülék felől érkező titkosítatlan adatokat titkosítva továbbítja (Security).

A Security Proxy az adatok titkosítását két szinten végezheti. Egyrészt létrehozhat a távoli szerverhez egy titkosított csatornát (tunnel), amelyen a mobil eszköz csomagjait titkosítva, ám változtatás nélkül küldheti tovább. Ezt a működést hívjuk *tunnel* üzemmódnak. A tunnel mód egy tipikus alkalmazása a virtuális magánhálózatokhoz [2] (Virtual Private Network, VPN) történő csatlakozás.

Amikor tunnel üzemmódban egy mobil eszköz a Security Proxyt igénybe véve csatlakozni kíván egy virtuális magánhálózathoz, akkor ezt jeleznie kell a Security Proxynak, ami ezek után VPN kliensként működve kapcsolódni fog a távoli VPN szerverhez. Miután létrejött a kapcsolat, és erről értesítette a mobil eszközt, a készülék megkezdheti a kommunikációt a távoli számítógépen keresztül elérhető hálózattal. Ezt a folyamatot mutatja be az *1. ábra*.

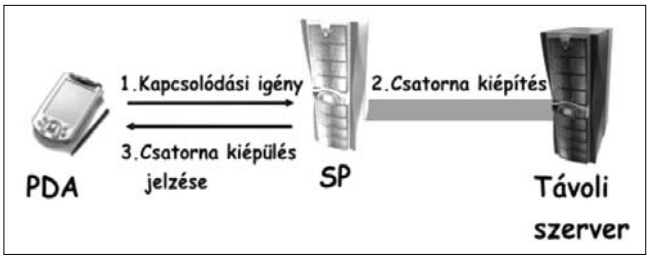
A Security Proxy alkalmazási szinten is működhet, ezt az üzemmódot hívjuk *proxy* módnak. Proxy mód esetében, amikor egy mobil eszköz csatlakozni szeretne egy titkosítást igénylő távoli alkalmazáshoz, akkor egy jóval gyengébb, vagy titkosítást egyáltalán nem használó programmal (pl. Telnet [5]) a Security Proxyhoz fordul, ami egy biztonságosabb szoftver (például SSH [4]) segítségével továbbítja az adatokat a távoli számítógéphez. Ezt a folyamatot szemlélteti a *2. ábra* a Telnet-SSH átalakítás esetében.

A két működési mód közötti alapvető különbség, hogy a tunnel üzemmód esetén a mobil eszköz az alkalmazásszintű protokolltól függetlenül a teljes hálózati forgalmát átküldheti a titkosított csatornán, míg proxy módban minden alkalmazásszintű protokoll támogatását egyenként kell megvalósítani.

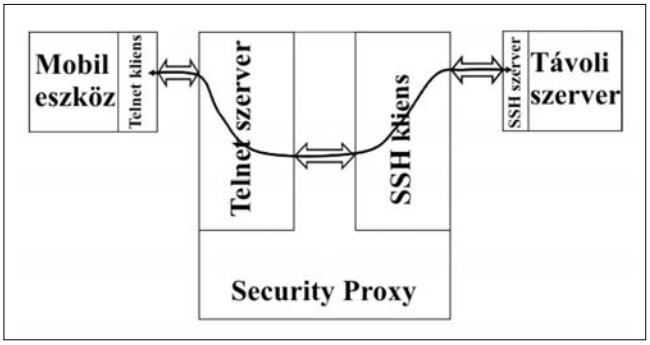
A Security Proxy transzparens módon látja el a feladatát. A mobil eszközön futó alkalmazás nem tudja, hogy a csomagjai a Security Proxyn haladnak keresztül, és a távoli szerver sincs tisztában azzal, hogy a kapott csomagok közvetlen forrása nem a mobil eszköz. Ez azért előnyös, mert a Security Proxy szolgáltatásainak igénybevételéhez nem szükséges módosítani sem a távoli szerveren futó alkalmazásokat, sem a mobil eszközön meglévő szoftvereket.

Biztonságos hálózati alkalmazásoknál előfordulhat, hogy egy mobil eszköz a Security Proxyn keresztül egy távoli hálózatot vagy alkalmazást szeretne elérni, de a

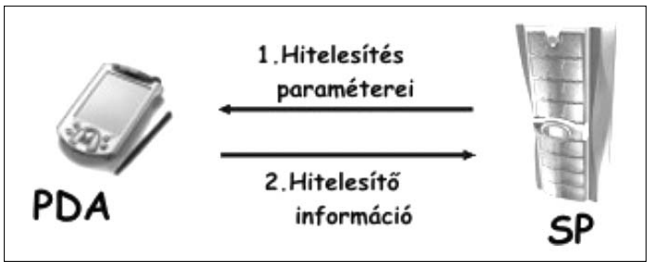
1. ábra Security Proxy tunnel módja VPN kapcsolattal



2. ábra A proxy mód



Security Proxy nem rendelkezik a hitelesítéshez szükséges titokkal – ami lehet egy jelszó, vagy egy privát kulcs. Ebben az esetben a titkosított csatornát a Security Proxy nem tudja kiépíteni a jogosultság hiánya miatt. A jogosultság megszerzéséhez hozzá kell jutnia a készülék által őrzött információhoz.



3. ábra A kihelyezett hitelesítési eljárás

Mivel a felhasználótól a titkának kiadását nem várhatjuk el, de a Security Proxy számára biztosítani kell a titokhoz való közvetett hozzáférést, ezért a Security Proxynak egy üzenetet kell küldenie a mobil eszköznek, amely tartalmazza azokat a paramétereket, amelyek a titok hozzáadásával hitelesítik a felhasználót a távoli hálózatban. Miután a készülék megkapta a hitelesítéshez szükséges adatokat, a titok hozzáadásával előállítja a hitelesítő információt, majd ezt visszaküldi a Security Proxynak *(3. ábra)*. A Security Proxy ezt felhasználva a mobil eszköz nevében már ki tudja építeni a távoli szerverrel a biztonságos kapcsolatot.

Profilokat használhatunk annak érdekében, hogy a mobil eszköz beállításait ne kelljen minden egyes alkalommal megadni, és a szolgáltatásokat több Security Proxynál is egyszerűen igénybe lehessen venni. A profilokat egy böngészőn keresztül lehet módosítani, amit azután le kell tölteni a mobil eszközre. A szolgáltatások igényléséhez a profilt tartalmazó fájlt csak fel kell tölteni a Security Proxyra, ami ezt követően kiépíti a fájlban megadott szolgáltatásokat.

3. Security Proxy illesztése meglévő hálózatokhoz

A Security Proxyt meglévő hálózatok kiegészítő szolgáltatásaként terveztük, ezért a hozzá tartozó adatforgalmat el kell különíteni a hálózat többi forgalmától. A hálózatban így szükség van a mobil eszköz és a Security Proxy között egy átjáróra (*Gateway,* GW), amely képes a készülék bizonyos csomagjait a Security Proxy felé irányítani.

Vezetéknélküli hálózatok esetében az átjáró lehet például a mobil eszköz vezetéknélküli hozzáférési pontja is. Az átjárónak így információt kell cserélnie a Security Proxyval, és ez alapján kell módosítania a készülék csomagjainak útvonalát. Ezt szemlélteti a *4. ábra*.

Amikor egy mobil eszköz tunnel módot szeretne használni, akkor ezt jelzi a Security Proxynak. A Security Proxy ekkor üzenetet küld az átjárónak, hogy azokat a csomagokat, amelyeknek forráscíme a mobil eszköz IP címe, a célcíme pedig a Security Proxytól induló csatorna végén lévő alhálózat valamely IP címe, a Security Proxy felé irányítsa. Ebben az esetben tehát az útvonalválasztó a csomagok forrás- és célcíme alapján választja ki a helyes irányt. Proxy mód használata esetén a mobil eszköztől származó csomagok célcíme csak a távoli kiszolgáló IP címe lehet, így nincs szükség egy teljes címtartomány figyelésére. Mindemellett figyelni kell a mobil eszköz IP címét is, vagyis a csomagok forráscímét.

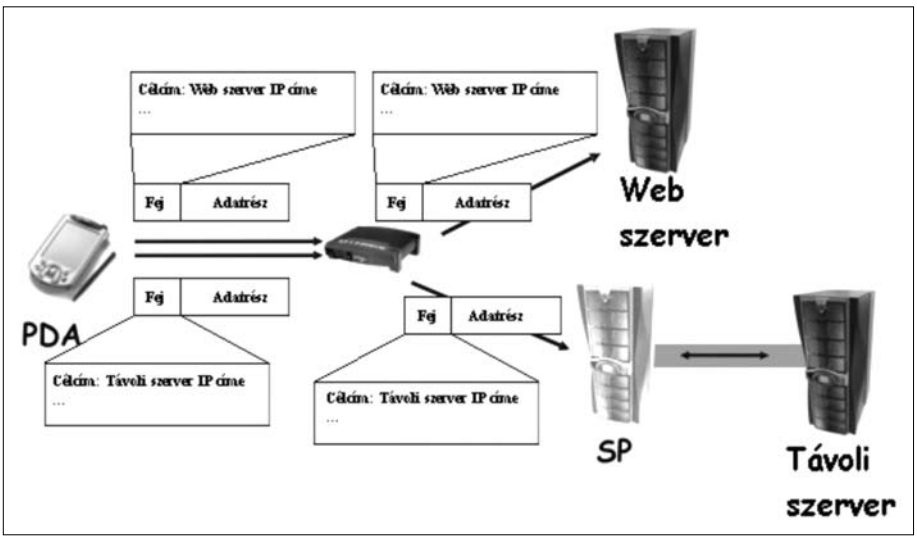
4. A Security Proxy Control Protocol

Az SPCP egy általunk készített protokoll, melynek célja a Security Proxy és a hálózati elemek közötti kommunikáció biztosítása. Ez a kommunikáció magában foglalja a kapcsolatfelépítést és -bontást a mobil eszköz és a Security Proxy között, a kihelyezett hitelesítési eljárás használatát, illetve a Security Proxy és az átjáró kommunikációját. Ez a kommunikáció kérdés-válasz alapú.

Mobil eszköz és Security Proxy kommunikáció

A mobil eszköz a kapcsolatot egy kapcsolatfelépítés (CONNECT) üzenet elküldésével veheti fel a Security Proxyval. Ha a kapcsolat felépült és a készülék egy új szolgáltatást kíván igénybe venni (set), vagy egy korábbi megrendelését szeretné törölni (del), akkor egy módosító (MODIFY) üzenetben jelezheti mindezt. Amikor a mobil eszköz egy ilyen üzenetet küld, akkor a Security Proxy kiépíti a távoli szerverrel a titkos csatornát, majd jelzi a készülék átjárójának, hogy hozza létre a megfelelő bejegyzéseket a routing táblájában, a sikeres létrehozás visszaigazolása után pedig a Security Proxy nyugtázza a mobil eszköz felé a szolgáltatás kiépítését. Kihelyezett hitelesítés használata során a mó-

4. ábra Security Proxy által vezérelt átjáró



dosító (MODIFY) üzenet után a Security Proxy egy státusz (STATUS) üzenetben elküldi a hitelesítéshez szükséges paramétereket. A készülék ezt feldolgozza, majd megismétli az előző módosító (MODIFY) üzenetét kiegészítve a hitelesítő információkkal.

A feltöltés (UPLOAD) üzenettel a mobil eszköz adatokat tölthet fel a Security Proxyra. Ilyen adat lehet a szolgáltatások paramétereit tartalmazó profil, illetve a hitelesítéshez szükséges tanúsítvány [6].

A kapcsolat lebontását a kapcsolatbontás (DISCONNECT) üzenettel lehet kezdeményezni. A kapcsolatbontás (DISCONNECT) üzenet hatására a lefoglalt erőforrások azonnal felszabadíthatók, és az átjáró konfigurációja visszaállítható anélkül, hogy meg kellene várni, amíg a készülék és a Security Proxy közötti kapcsolat időtúllépés miatt megszűnik.

A parancsok feldolgozásának sikerességét, illetve az esetleg fellépő hibákat a státusz (STATUS) üzenet segítségével jelezzük.

Átjáró és Security Proxy kommunikáció

A Security Proxy és az átjáró között routing (ROUTE) üzenetek haladnak. Ezekkel az üzenetekkel lehetővé válik a csomagok szeparációja attól függően, hogy a készülék éppen a Security Proxy valamely szolgáltatása számára küldi a csomagot, vagy a csomag független a Security Proxytól. Ha a Security Proxy egy routing (ROUTE) üzenetet küld az átjárónak, akkor az egy válaszüzenetben jelzi, hogy sikerült-e megfelelően kitölteni (set) vagy törölni (del) a routing-táblájának a szolgáltatáshoz tartozó bejegyzéseit.

Az *5. ábra* egy egyszerű kapcsolatfelépítési eljárást mutat proxy üzemmód esetén.

5. A Security Proxy és a biztonság

A Security Proxy Control Protocol alapesetben nem nyújt biztonságot a támadásokkal és az üzenetmódosításokkal szemben, így az adatforgalom biztonságát és hitelességét hálózati szinten kell biztosítani.

A mobil eszköztől érkező csomagok a készülék és a hozzáférési pont között egy WPA TKIP [8] által titkosított csatornán mennek át, a hozzáférési pont és a Security Proxy között pedig egy kiépített biztonságos alagúton (pl. IPSec [2]) haladnak *(6. ábra)*.

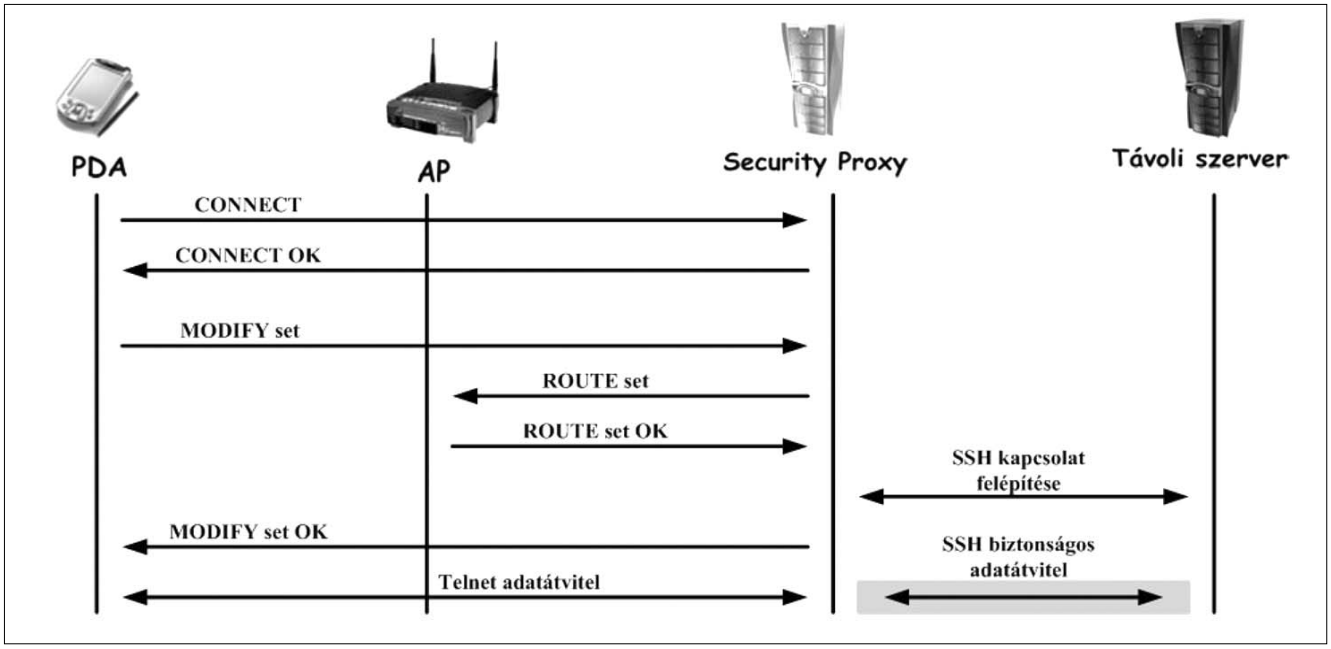
A mobil eszköz a hozzáférési pontot könnyen hitelesítheti például egy tanúsítvány segítségével. Mivel azonban a WPA TKIP titkosítás megszűnik a hozzáférési pontnál, ezért az hozzáférhet a mobil eszköz csomagjaihoz: láthatja és értelmezheti az IP fejlécet, de akár módosíthatja is a csomag tartalmát. Ez egyrészt előnyös, hiszen képessé válik a forgalom irányának befolyásolására, másrészt viszont megszemélyesítéses támadásra *(man-in-the-middle/evil twin attack)* adhat okot.

Ez a támadás azonban nem hajtható végre a hálózatban, ugyanis a hitelesítéshez szükséges közös titkot csak a hálózat hitelesítő szervere (pl. RADIUS [7]) és a mobil eszköz ismeri, és a titkot egyikük sem adja ki a támadónak, így tehát a hálózat biztonságos lesz.

6. Teszthálózat és elért eredmények

A Security Proxyt az Infopark teszthálózatába [1] illesztettük be, amelyben található egy vezetéknélküli hozzáférési pont, egy RADIUS hitelesítő szerver, egy VPN szerver és az Internet és a belső hálózat között elhelyezkedő tűzfal. A Security Proxy közvetlenül a tűzfalhoz kapcsolódik, és a tűzfalon keresztül kommunikál a mobil eszköz átjárójaként szolgáló vezetéknélküli hozzáférési ponttal. A tűzfalat úgy állítottuk be, hogy a Security Proxy által az Internet felé kezdeményezett kapcsolatokat engedélyezze.

5. ábra
Kapcsolatfelépítés proxy üzemmódban (Telnet / SSH)



6. ábra
Titkosítás a mobil eszköz és a Security Proxy között

A méréseket ebben a hálózatban végeztük el. A mérések során két főbb esetet vizsgáltunk. Először a mobil eszköz egy IPSec szolgáltatást vett igénybe. Ekkor megmértük az adatátviteli sebességet Security Proxy használatával és anélkül. Az eredmény a *7/a. ábrán* látható.

Ha a hálózatban nem használtunk titkosítást, akkor az adatátviteli sebesség jóval nagyobb, mint amikor a kézi számítógép IPSec titkosítást használt. Amikor azonban a titkosító funkciót áthelyeztük a Security Proxyhoz, akkor láthatóan nem történt adatátviteli sebesség csökkenés.

A másik esetben egy olyan biztonsági szolgáltatást tettünk elérhetővé a kézi számítógép számára, amelyet eddig nem vehetett igénybe. A *7/b. ábrán* látható, hogy ha a Security Proxy végzi az openVPN [3] biztonságos csatornához szükséges titkosítást, akkor – az IPSec esetéhez hasonlóan – nem tapasztalható adatátviteli sebességcsökkenés.

Megállapítható tehát, hogy mindkét esetben, amikor a mobil eszköz igénybe vette a Security Proxy szolgáltatásait, adatsebesség csökkenés nélkül tudta használni a biztonságos szolgáltatásokat.

7. Összefoglalás

Cikkünkben bemutattuk a Security Proxy működésének elméletét és a hozzá kapcsolódó kihelyezett hitelesítési eljárást. Ezzel kapcsolatban találkoztunk a Security Proxy és a hálózati elemek információcseréjéhez létfontosságú SPCP-vel, és bemutattuk a Security Proxy vezetéknélküli hálózatokba történő biztonságos integrációját és az így született mérési eredményeket. Látható tehát, hogy a Security Proxy egy olyan komplex, bővíthető megoldás, mely bármely vezetéknélküli hálózatban lehetővé teszi a kisteljesítményű mobil eszközök számára a biztonságos szolgáltatások igénybevételét.

Köszönetnyilvánítás

Köszönetet mondunk a Budapesti Műszaki és Gazdaságtudományi Egyetem Távközlési és Média-Informatikai Tanszékének, hogy támogatta TDK dolgozatunk elméletének és prototípusának megvalósítását, valamint a cikk létrejöttét, továbbá külön szeretnénk köszönetet mondani a rengeteg segítségért konzulenseinknek, Dr. Fehér Gábornak és Korn Andrásnak.

Irodalom

[1] DR. FEHÉR GÁBOR (SZERK): Biztonságos vezetéknélküli szuperhálózat elosztott környezetben, 2004. http://qosip.tmit.bme.hu/cgi-bin/twiki/view/SECLab/ResultS/Rendszerterv_final.pdf
[2] NAGANAND DORASWAMY, DAN HARKINS: IPSec: The new Security Standard for the Internet, Intranets, and Virtual Private Networks, Second Edition, Prentice Hall PTR, 2003.
[3] CHARLIE HOSNER: OpenVPN and the SSL VPN Revolution 2004, http://www.sans.org/rr/whitepapers/vpns/1459.php
[4] T. YLONEN, C. LONVICK: SSH Protocol Architecture, Internet-Draft, 2005.
[5] J. POSTEL AND J. REYNOLDS: Telnet Protocol Specification, RFC 854, 1983.
[6] R. HOUSLEY, W. FORD, W. POLK, D. SOLO: Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 2459, 1999.
[7] JONATHAN HASSEL: „RADIUS", O'Reilly, 2002.
[8] JON EDNEY, WILLIAM A. ARBAUGH: „Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Addison-Wesley, 2003.
[9] Security Proxy weboldala: http://alpha.tmit.bme.hu/~szgyi/sp.html

7. ábra
a) Mérések IPSec-el, b) Mérések openVPN-el