KÖZPONTOSÍTOTT EAP ALAPÚ HITELESÍTÉS VEZTÉK NÉLKÜLI HÁLÓZATOKBAN

CENTRALIZED EAP BASED AUTHENTICATION FOR WIRELESS NETWORKS

Orosz Péter, oroszp@unideb.hu
Debreceni Egyetem, DISZK

Sztrik János, jsztrik@inf.unideb.hu
Debreceni Egyetem, Informatikai Kar

Kim Che Soong, dowoo@sangji.ac.kr
Sangji University, Korea

Bevezetés

Vezeték nélküli helyi hálózatok esetén kiemelten fontos biztonsági kérdés a hálózati erőforrásokhoz való hozzáférés szabályozása. Erre az IEEE 802.1X keretszabvány nyújt megoldást, mely a hitelesítési üzenetek formátumaként EAP protokollt alkalmaz. Az EAP-on alapuló autentikációs protokollok és eljárások biztosítják a vezeték nélküli kliensek hitelesítését, szabályozzák a közeg-hozzáférést. A nagyobb gyártók kifejlesztették saját EAP alapú hitelesítési protokolljaikat, amely megnehezítheti a különböző platformok együttműködését. Nagy méretű, heterogén hálózat és nagy számú bázisállomás esetén felmerül az igény központosított hozzáférés-szabályozás kialakítására. Lehetséges-e az EAP mechanizmuson alapuló különböző hitelesítési eljárások együttes kezelése centralizált hozzáférés-szabályozással? A gyakorlatban felállított tesztkörnyezetben végzett vizsgálatok erre próbálnak választ adni.

A 802.1X keretszabvány

1. Amikor egy vezeték nélküli csomópont hozzáférést kér a hálózati erőforrásokhoz, a bázisállomás azonosítást kér tőle. A vezeték nélküli kliens számára hitelesítés előtt kizárólag EAP üzenetek forgalmazása engedélyezett.

2. Miután a kliens elküldte az azonosító üzenetet, megkezdődik a hitelesítési folyamat. Ebben a folyamatban a kérvényező (vezeték nélküli kliens) és a hitelesítő egymás között EAP vagy még pontosabban EAPOL (EAP over LAN) protokollal kommunikálnak. A Hitelesítő átcsomagolja az EAP üzenetet RADIUS formátumra, majd továbbítja a Hitelesítő szervernek. A hitelesítés alatt az Autentikátor csak továbbítja az üzeneteket a Kérvényező és a Hitelesítő szerver között. Miután befejeződött az autentikációs folyamat, a Hitelesítő szerver üzenetet küld az Autentikátor számára a hitelesítés eredményéről, melynek sikeressége esetén a Hitelesítő kinyitja az adott port-ot a Kérelmező számára.

3. Sikeres hitelesítés után a Kérelmező megkapja a jogosultságot a hálózati erőforrások használatára.

Az EAP protokoll

Az EAP protokoll csupán egy hitelesítésre optimalizált, szállító protokoll, nem egy teljes hitelesítési módszer. Valójában egy hitelesítési keret, amely többféle autentikációs eljárást támogat. Alapvetően az EAP közvetlenül az adatkapcsolati rétegekben működik (pl. PPP, IEEE 802), IP protokoll használata nélkül.

Mivel az IEEE 802.1X hitelesítésre EAP-ot használ, többféle összetett autentikációs séma használható, mint például a Smart-kártya, Kerberos, publikus kulcs, egyszeri jelszó, stb. Az alábbi táblázatban a leggyakrabban alkalmazott EAP hitelesítési eljárások olvashatóak.

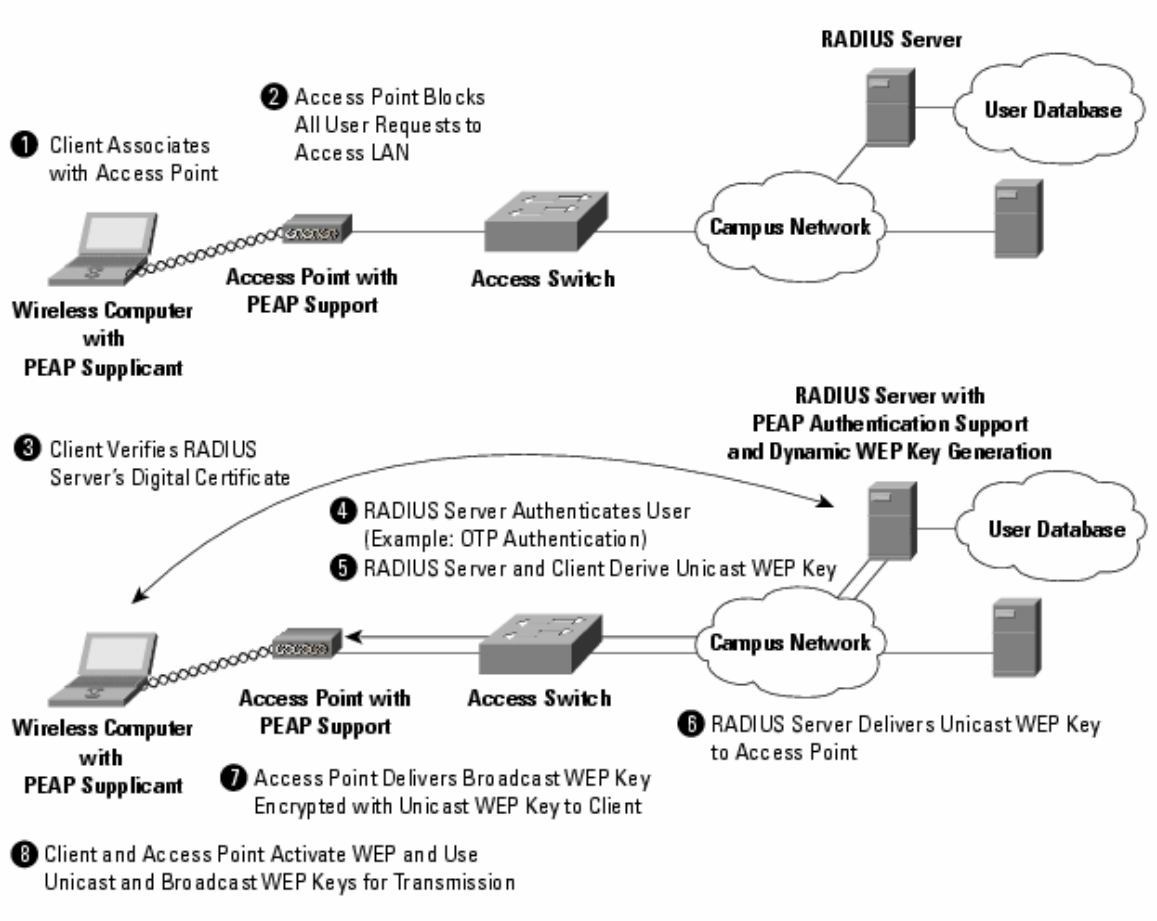
1. táblázat

EAP típus	Leírás
EAP-MD5	Az MD5-Challenge hitelesítéshez felhasználói név és jelszó szükséges. Nincs tanúsítvány. Gyakorlatilag megegyezik a PPP CHAP (RFC 1994) protokollal.
Lightweight EAP (LEAP)	Felhasználói név/jelszó pár küldése szükséges a Hitelesítő szerverhez (RADIUS). Nem tekinthető biztonságos hitelesítési eljárásnak. Cisco fejlesztés.
EAP-TLS	TLS session-t állít fel EAP-on belül a Kérelmező és a Hitelesítő-szerver között. Mind a kliens, mind a szerver tanúsítvánnyal kell, hogy rendelkezzen, tehát egy publikus kulcs infrastruktúráról (PKI) van szó. A eljárás kétirányú autentikációt biztosít. (RFC 2716)
EAP-TTLS	Titkosított TLS-csatornát hoz létre a hitelesítési adatok biztonságos továbbítására. A TLS-csatornán belül bármilyen más autentikációs módszer használható. Jelenleg IETF draft/tervezet formában létezik.
Protected EAP (PEAP)	Hasonlóan az EAP-TTLS-hez, titkosított TLS-csatornát használ. Kérelmezői oldalon a tanúsítvány opcionális, de szerver oldalon kötelező. Microsoft/Cisco fejlesztés, IETF tervezet.
EAP-MSCHAPv2	Felhasználói név/jelszó pár szükséges. Lényegében az MS-CHAPv2 becsomagolása EAP-ba. Gyakran használatos PEAP TLS-csatornában. Microsoft fejlesztés, jelenleg IETF tervezetként létezik..

Hitelesítő szerver – RADIUS (Remote Authentication of Dial-In User Service)

A RADIUS szervert eredetileg Internet Szolgáltatók használták ügyfeleik jelszavas hitelesítésére, a szolgáltató hálózatába történő belépés előtt. A 802.1X keretszabvány nem írja elő a háttérben működő hitelesítő szerver típusát, de a RADIUS tekinthető alapértelmezett autentikációs szervernek 802.1X környezetben.

Az 1. ábrán az autentikációs folyamat sémája látható:



1.ábra

Tesztkörnyezet és konfiguráció

A fentebb ismertetett EAP alapú hitelesítési eljárások működőképességének vizsgálata heterogén tesztkörnyezetben történt. Összeállítottunk egy teszt vezeték nélküli helyi hálózatot, amely két bázisállomásból, két vezeték nélküli kliensből, valamint egy RADIUS alapú hitelesítő szerverből állt, opcionálisan a hitelesítő szerver központi névtár (LDAP) szerverhez kapcsolódik, a felhasználói azonosítók és jogosultságok ellenőrzése céljából.

Megvizsgáltuk mely EAP implementáció alkalmas leginkább az egyetemi heterogén WLAN környezet felhasználóinak biztonságos, központosított hitelesítésére. Az egyetemen működő vezeték nélküli hálózatokban, mind a bázisállomások, mind a vezeték nélküli kliensek esetén megjelenik a heterogenitás. A különböző típusú bázisállomások mellett a kliensek hálózati adapterei, szoftveres jellemzői, és a klienseken futó operációs rendszerek is széles skálán mozognak. A teszteket az alábbi környezetben végeztük:

A RADIUS szerver az alábbi szoftver-konfigurációval rendelkezett:
Operációs rendszer: Linux (Debian 3.1 Sarge), kernel verzió: 2.6.8-2.smp
RADIUS szerver: FreeRadius 1.0.2/1.0.3
SSL: OpenSSL 0.9.8-stable
Tanúsítvány: Self-signed Certificated

1. kliens gép konfigurációja:
Vezeték nélküli hálózati adapter: Cisco Aironet 352, 11Mbps wireless adapter
Operációs rendszer: Debian Linux,
Vezeték nélküli hitelesítés: XSupplicant
SSL: OpenSSL 0.9.8-stable
Tanúsítvány: Self-signed Certificate

2. kliens gép konfigurációja:
Vezeték nélküli hálózati adapter: Cisco Aironet 352,11Mbps wireless adapter
Operációs rendszer: Windows XP, Service Pack 2
Vezeték nélküli hitelesítés: A Windows beépített vezeték nélküli kapcsolat-menedzser
Tanúsítvány: Self-signed Certificate

Bázisállomás:
Gyártó/típus: Cisco Aironet 1120B
IOS verzió: 12.3.(2)JA2
Kliens hitelesítés: Open + EAP (RADIUS szerver)

A bázisállomás és a Hitelesítő (RADIUS) szerver között hármas szinten (L3), IP csomagban továbbítódik az EAP üzenet, így a szerver elhelyezése nincs hálózathoz kötve, viszont az AP és a szerver között biztosítani kell az UDP csomagok forgalmazását, szerver oldalon a 1812-1814-es UDP portokra, míg a bázisállomáson alapértelmezésben a 1645-1647-es UDP portokra. A titkosított csatornán keresztül történő EAP autentikáció alkalmazásakor a hitelesítő szervernek tanúsítvánnyal kell rendelkeznie saját maga hitelesítésére a kliens felé. A kliens oldali tanúsítvány bizonyos EAP típusok esetén kötelező (TLS, TTLS), másoknál opcionális (PEAP), vagy nem támogatott (MD5, LEAP). Mint ahogy a korábbi (1.) táblázatból kiderült, az egyes EAP típusok más-más biztonsági szintet valósítanak meg. A hatékony adminisztráció érdekében, egyetemi környezetben azok az EAP eljárások alkalmazhatóak eredményesen, melyek szerver oldalon kötelezően megkövetelik a tanúsítvány használatát, kliens oldalon viszont felhasználói név/jelszó formában kérik az azonosítást, és csak opcionális lehetőségként jelenik meg a kliens-tanúsítvány használata.

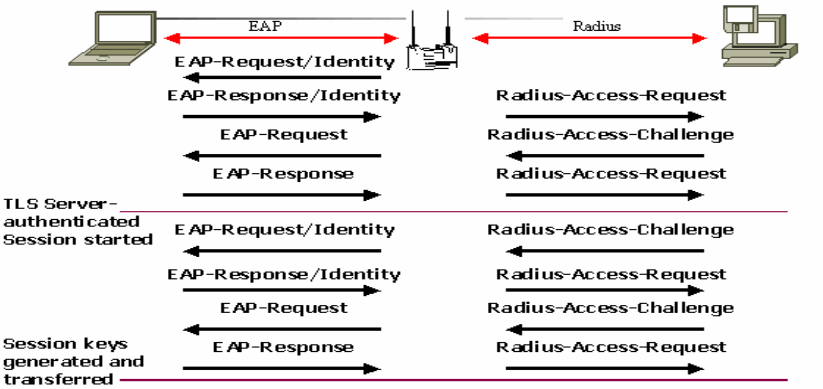
A tesztkörnyezetben üzemelő RADIUS szerveren a FreeRadius 1.0.2-es verziója futott, mely a különböző hitelesítés mechanizmusok széles skáláját támogatja, beleértve a legjelentősebb EAP típusokat is, ezen felül az azonosításhoz adatbázis (MySQL, PosgreSQL), illetve LDAP kapcsolódás is lehetséges. A szerver hitelesítéséhez használt tanúsítványt OpenSSL segítségével generáltunk. A bázisállomáson nyitott (open) autentikációt alkalmaztunk EAP hitelesítéssel. Az EAP típusát az üzenetben található azonosító alapján automatikusan érzékeli a Hitelesítő szerver.

A vizsgálat eredményei, tapasztalatok

Tapasztalataink szerint a különböző FreeRadius és OpenSSL változatok együttműködése erősen verziófüggő, így számos nehézséggel kellett szembenézni a rendszer konfigurálásakor. Biztonsági, illetve támogatottsági szempontból a PEAP bizonyult a leghatékonyabbnak, mivel ezt az EAP típust alkalmazni tudtuk mind a Linux-os, mind a Windows XP kliens autentikációjára. Külön kiemelendő, hogy a PEAP titkosított csatornán (TLS) alapuló mechanizmus, így alkalmazásával biztonságosan továbbíthatóak a felhasználó adatai a

hitelesítési folyamat alatt. Az EAP-MD5 szintén támogatott mindkét rendszerben, viszont biztonsági szempontból jelentős mértékben elmarad a PEAP mellett. Minkét módszer felhasználói név/jelszó párost használ a kliens azonosítására, így könnyen összekapcsolható a vezeték nélküli hálózat hitelesítése a központi névtár-szolgáltatással, miáltal magas fokú biztonság mellet valósítható meg a központosított, egyetem-szintű hozzáférés menedzsment. Az egyéb EAP mechanizmusokat a gyártók önálló kliens-programjaikba építették be, így ezek csak az adott típusú adapter esetén alkalmazhatóak.

A PEAP opcionálisan lehetővé teszi a kliens oldali tanúsítványok használatát, mellyel magas biztonsági szintet igénylő hálózati szolgáltatásokat, alkalmazásokat tehetünk elérhetővé az arra jogosultak számára. Bár alapértelmezésben érdemes a szokásos jelszavas védelmet alkalmazni az egyszerűbb adminisztráció érdekében.



A hitelesítés két fázisban megy végbe:

1. A titkosított TLS csatorna kiépítése az EAP kliens (Kérvényező) és az EAP (Radius hitelesítő) szerver között.
2. Kiépített csatornában kerülnek átvitelre a kliens azonosítására szolgáló információk.

A közeljövőt tekintve további előnyt jelent, hogy a módszer gyors újrahitelesítést szolgáltat mobil környezetben (roaming esetén), amikor is a kliens mozgása közben átkerül egy másik rádiós cellába (tehát új bázisállomáshoz kapcsolódik), ami ismételt hitelesítést igényel.

Összefoglalás

A közepes és nagy kiterjedésű vezeték nélküli hálózatokban a hitelesítési folyamatok központosítása lényeges tényező a megfelelő biztonsági szint eléréséhez. Számos hitelesítési módszert fejlesztettek a közelmúltban, ugyanakkor ezek jelentős része gyártó-specifikus. A vezeték nélküli hálózatkora a legkülönfélébb gyártmányú és tulajdonságú adapterek csatlakozhatnak, és az operációs rendszer környezet sem homogén, így célszerű olyan autentikációs módszert választani, amelyet a desktop operációs rendszerek, és a hálózati adapterek lehető legszélesebb skálája támogat, emellett kellő biztonságot nyújt a kliens hitelesítési adatainak védelmére. Felhasználói oldalon felmerül az igény az egyszerű alkalmazhatóságára, például hitelesítés név/jelszó pár használatával, ami adminisztratív szempontból is kényelmes megoldást jelent. Ebből a tapasztalatból kiindulva, kliens-oldali tanúsítványokat csak olyan hálózatokban érdemes alkalmazni, ahol alapkövetelmény a magas biztonság szintet megvalósító hozzáférés-szabályozás.

További, a témához kapcsolódó vizsgálati lehetőség a vezeték nélküli adatforgalom titkosítási mechanizmusainak (WPA, WPA2, WEP) elemzése, valamint ezek együttműködése a különböző EAP alapú autentikációs eljárásokkal. Az IPv6 elterjedésével a mobil vezeték nélküli technológiák széleskörű térhódítása várható, miáltal szükségessé válik a gyors és egyben biztonságos hitelesítés és újrahitelesítés. A legújabb, csatorna-alapú EAP fejlesztések ebbe az irányba mutatnak, köztük a PEAP és az EAP-Fast.

Irodalom

1. Extensible Authentication Protocol (EAP) reference:
   http://www.ietf.org/rfc/rfc2284.txt
2. EAP-TLS reference:
   http://www.ietf.org/rfc/rfc2716.html
3. Lightweight EAP (LEAP):
   http://www.cisco.com/warp/public/784/packet/exclusive/apr02.html
4. 802.1X Authentication and Extensible Authentication Protocol (EAP):
   http://www.foundrynet.com/solutions/appNotes/PDFs/EAPWhitePaper.pdf
5. Cisco Aironet 1200 Series: SAFE Wireless LAN security

A kutatásokhoz a KOSEF-HAS, 2004, koreai-magyar tudományos együttműködési pályázat részleges anyagi támogatást nyújtott