FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SUSTAVI ZA PRAĆENJE I VOĐENJE PROCESA

EAP/PEAP - security over 802.11 wireless

Tonković Franjo
0036371303

Zagreb, 08.06.2004.

Sadržaj:

1. IEEE 802.1X

IEEE 802.1X standard, Port Based Network Access Control, definira mehanizme za portno orijentiranu kontrolu mrežnom pristupu te korištenje fizičkog pristupa karakteristikama IEEE 802 LAN infrasrukture. On omogućava sredstva za autentifikaciju i autorizaciju uređaja spojenih na LAN port koji ima karakteristike point-to-point veze. On također onemogućava pristup u slučaju u kojem autentifikacija i autorizacija nisu uspješno provedene.
Ovaj standard je prvotno razvijen za ožičene ethernet mreže, ali je kasnije prilagođen za korištenje na 802.11 bežičnim mrežama (WLAN). Ovo uključuje mogućnost da pristupna točka WLAN-a distribuira ili dobije global key information za/od priključenih stanica pomoću EAPOL- poruke s ključem.

IEEE 802.1X definira sljedeće pojmove:

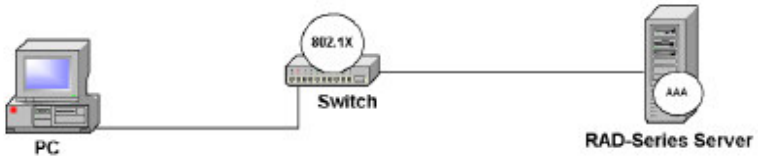
- Entitet za portni pristup (Port access entity)
- Autentifikator
- Pristupnik (Supplicant)
- Autentifikacijski server

1.1. Entitet za portni pristup

Port access entitiy (PAE), također znan i kao LAN port, je logički entitet koji podržava IEEE 802.1X protokol koji je pridružen portu. LAN port može preuzeti ulogu autentifikatora, pristupnika ili oboje. Svaki od portova komunicira jedan na jedan sa portom na stanici.

1.2. Autentifikator

Autentifikator je LAN port koji prisiljava na izvođenje autentifikacije prije dopuštanja pristupa uslugama kojima se pristupa preko porta. Autentifikator je odgovoran za komunikaciju sa pristupnikom te za prosljeđivanje informacija dobivenih od pristupnika odgovarajućem autentifikacijskom serveru. Ovo omogućava verifikaciju pristupnikovih prava te određivanje stanja porta. Važno je primijetiti da funkcionalnost autentifikatora ne ovisi o autentifikacijskoj metodi. On funkcionira kao prolaz za izmjenu autentifikacija. Za bežične mreže, autentifikator je logički LAN port na bežičnoj pristupnoj točki (access point - AP) kroz koju klijenti sa bežičnim pristupom djeluju za dobivanje pristupa ožičenoj mreži.



Slika 1. 802.1X

1.3. Pristupnik

Pristupnik je LAN port koji zahtjeva pristup uslugama kojima se pristupa preko autentifikatora. Pristupnik je odgovoran za odgovaranje na zahtjeve autentifikatora kojima traži informacije za potvrđivanje autentičnosti Kod bežičnih mreža pristupnik je logički LAN port na bežičnom mrežnom adapteru koji zahtjeva pristup mreži. To radi prvo povezivanjem a autetifikatorom, a zatim i autentifikacijom.
Bez obzira koristimo li ožičene ili bežične mreže, pristupnik i autentifikator su logički ili fizički spojeni kao point-to-point LAN segment.

1.4. Autentifikacijski server

Da bi potvrdili autentičnost pristupnika, autentifikator koristi autentifikacijski server. Autentifikacijski server provjerava pristupnikova prava na pristup i odgovara autentifikatoru. Autentifikacijski server može biti:

- komponenta pristupne točke (Access Point - AP). AP mora biti konfiguriran setom korisnikovih kredibiliteta koji odgovaraju klijentima koji se pokušavaju spojiti na mrežu. Tipično, ovo se ne implementira kod bežičnih AP.
- posebni entitet. AP prosljeđuje kredibilitet od pokušaja pristupa posebnom autentifikacjskom serveru. Tipično, bežični AP koristi Remote Authentication Dial-In User Server (RADIUS) protokol za slanje parametara pokušaja pristupa RADIUS-u.

1.5. RADIUS

RADIUS je standardni način omogućavanja Autentification, Authorization and Accounting (AAA) usluga mreži. Iako je RADIUS protokol omogućen kao izbor kod IEEE 802.1X, očekuje se da će mnogi IEEE 802.1X autentifikatori raditi kao RADIUS klijenti. U stvari, aneks D kod IEEE 802.1X standarda opisuje smjernice za korištenje 802.1X RADIUS-a, a i mnoge pristupne točke koje podržavaju 802.1X rade to pomoću RADIUS-a.

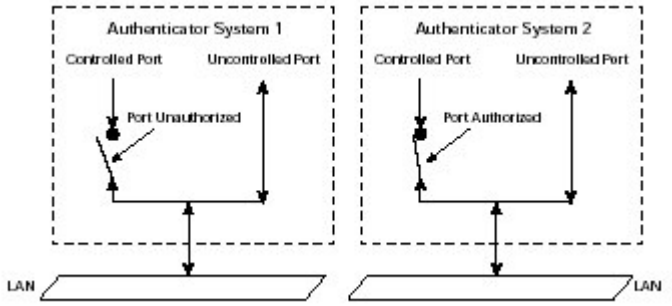
1.6. Kontrolirani i nekontrolirani portovi

Autentifikatorova portno orijetirana kontrola pristupa definira slijedeće tipove logičkih portova, koji pristupaju žičanom LAN-u preko jednog fizičkog porta:

- nekontrolirani port
- kontrolirani port

Nekontrolirani port

Nekontrolirani port dozvoljava nekontroliranu razmjenu podataka između autentifikatora (bežična AP) i drugog mrežnog uređaja na ožičenoj mreži, bez obzira na stanje autorizacije bežičnog klijenta. Dobar primjer ovakve razmjene su RADIUS poruke između AP i RADIUS servera na ožičenoj mreži, koja omogućava autorizaciju bežičnih veza. Okviri koji su poslani od strane bežičnog klijenta nikad nisu proslijeđeni iz AP preko nekontroliranog porta.



Slika 2. 802.1X portovi

Kontrolirani port

Kontrolirani port dozvoljava da se šalju podaci između bežičnog klijenta i ožičene mreže, ali jedino ako je bežični klijent autenificiran. Prije autentifikacije, preklopnik je otvoren i okviri nisu prosljeđivani između bežičnog klijenta i ožičene mreže.. Nakon, što je bežični klijent uspješno autentificiran korištenjem IEEE 802.1X, preklopnik se zatvara i okviri se prosljeđuju između bežičnog klijenta i čvorova na ožičenoj mreži.

Na autentificiranom ethernet switchu, ožičeni ethernet klijent može slati ethernet okvire prema ožičenoj mreži čim završi proces autentifikacije. Switch prepoznaje promet specificiranog ožičenog ethernet klijenta korištenjem fizičkog porta na koji je klijent spojen. Tipično, samo je jedan ethernet klijent spojen na fizički port ethernet switcha.

Zbog toga što više bežičnih klijenata koristi isti kanal za pristup, potreban je dodatak osnovnom IEEE 802.1X protokolu koji dopušta bežičnoj AP da identificira osigurani promet pojedinog bežičnog klijenta. Ovo se čini preko obostranog određivanja jedinstvenog ključa po klijentu pri određenoj vezi od strane bežičnog klijenta i bežičnog AP. Jedino autentificirani bežični klijenti imaju ispravno određen ključ. Bez ispravnog ključa, okviri koji su poslani od strane neautentificiranog bežičnog klijenta se zanemaruju.

2. EAP

Extensible Authentication Protocol (EAP) je način provođenja autentifikacije između korisnika i autentifikacijskog servera. Među uređaji poput AP-a ili proxy servera ne sudjeluju u komunikaciji. Njihova je uloga prenošenje EAP poruka između strana koje obavljaju autentifikaciju. 802.1X koristi EAP kako autentifikacijski framework.

EAPOL

Extensible Autentication Protocol Over Lan (EAPOL)
802.1X definira standard za enkapsulaciju EAP poruka tako da one mogu biti upravljane direktno sa LAN MAC servisima. Enkapsulacijska forma EAP-a je poznata kao i EAPOL. Dodatno prenošenju EAP paketa, EAPOL također omogućava kontrolne funkcije poput starta, logoff i distribuciju ključa.
Najčešće korišteni EAP autentifikacijski tipovi su EAP-TLS, EAP-SIM i PEAP.

3. EAP-TLS

EAP omogućava standardne mehanizme za podršku dodatnih autentifiikacijskih metoda. Kroz korištenje EAP-a moguće je dodati razne autentifikacijske načine, uključujući smartcards, public key, one time password itd.
Međutim, ponekad je poželjno podržavati obostranu autentifikaciju i pošto razne metode podrazumijevaju korištenje ključa, korisno je imati mehanizme za uspostavljanje ključa. Pošto je stvaranje novih protokola koji koriste ključeve zahtjevan posao, potrebno je zaobići stvaranje novih mehanizama za to.

EAP-TLS komunikacija tipično započinje dogovaranjem autentifikatora i pristupnika oko EAP-a. Zatim, autentifikator tipično šalje paket sa EAP zahtjevom za identitetom, a pristupnik odgovara na traženi zahtjev. Odgovor sadrži korisnikov ID. Od ove točke nadalje, dok se nominalno komunikacija odvija između pristupnika i autentifikatora, autentifikator može raditi kao proslijeđivač. EAP paketi koji su primljeni se enakpsuliraju za transmisiju prema RADIUS-u. Kad jednom primi pristupnkovu identifikaciju, server mora odgovoriti i to sa EAP-TLS/Start paketom, koji se dobije kao EAP-zahtjev paket i EAP-tip=EAP-TLS, start bit postavljen i bez podataka.

3.1. EAP Transport Layer Security

EAP-TLS je baziran na TLS protokolu (RFC2246). TLS je sadašnja verzija Secure Socket Layera korištenog u većini web browsera. TLS se dokazao kao siguran autentifikacijski mehanizam i sada je dostupan i kao 802.1X EAP autentifikacijski tip.

TLS je dizajniran da omogući sigurnu autentifikaciju i enkripciju kod TCP/IP veza.

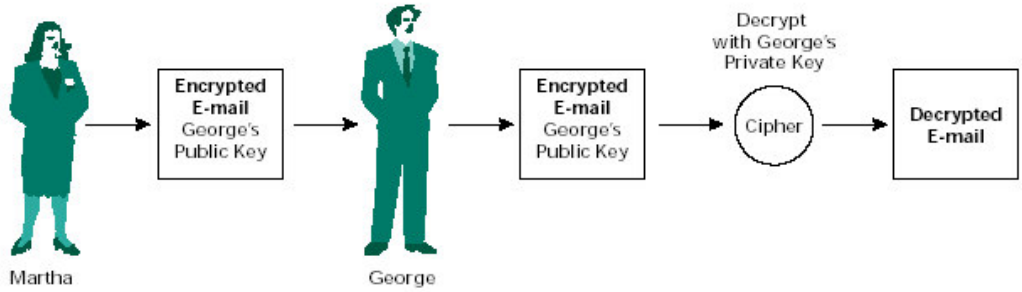
Da bi se to postigl, TLS se sastoji od tri protokola:

- handshake protokol - on dogovara parametre za SSL sesiju. SSL klijent dogovaraju verziju protokola, enkripcijski algoritam, autentificiraju jedan drugoga i izračunaju enkripcijske ključeve
- Record protokol – olakšava enkriptiranu razmjenu između SSL klijenta i servera. Dogovoreni enkripcijski mehanizam i enkripcijski ključ se koriste za osiguravanje sigurnog tunela za aplikacijske podatke između krajnjih točaka SSL-a
- Alert protokol – to je mehanizam korišten za obavještavanje SSL klijenta o greškama kao i prekidu veze

TLS autentifikacija je generalno podijeljena u dvije grupe: autentifikacija sa serverske strane i sa klijentove strane. Serverska autentifikacija koristi javni ključ (PKI). Klijentova autentifikacija može koristiti PKI certifikate. EAP-TLS koristi cerifikate sa klijentove strane

3.2. PKI i digitalni certifikati

PKI enkripcija se temelji na asimetričnim enkripcijskim ključevima. PKI korisnik ima dva ključa, javni i privatni ključ. Bilo koji podatci enkriptirani sa javnim ključem mogu biti dekriptirani jedino sa privatnim ključem. Npr: Gorge daje Marthi svoj javni ključ. Martha zatim šalje Georgeu e-mail enkriptiran njegovim javnim ključem. Da bi George pročitao poruku, mora je dekriptirati svojim privatnim ključem Pošto je George jedina osoba koja ima pristup privatnom ključu, jedino on može pročitati originalnu poruku.



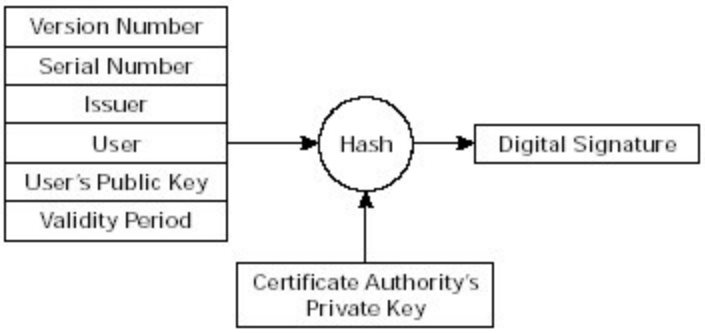
Slika 3. Enkripcija javnim ključem

Digitalni certifikati su strukture podataka distribuirane od nadležne ustanove koja pridjeljuje javne ključeve korisnicima. Digitalni certifikati se tipično sastoje od sljedećih informacija:

- Verzije certifikata
- Serijskog broja
- Izdanje certifikata
- Korisnik

- Korisnikov javni ključ
- Vrijeme korištenja
- Dodatci
- Algoritam potpisa
- Potpis

Digitalni certifikat se dobije kombinacijom verzije certifikata, serijskog broja, izdanja , korisnika i korisnikova javnog ključa te vrijeme trajanja te provlačenjem istih kroz hash funkciju. Nadležna ustanova zaključava hash sa svojim privatnim ključem.



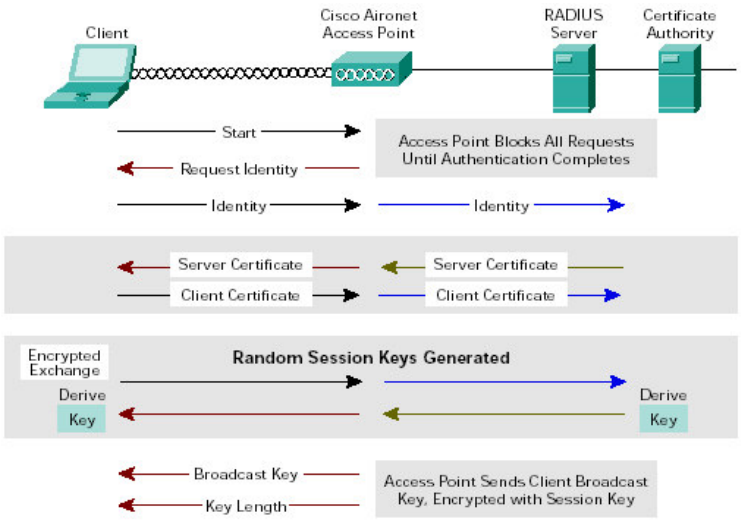
.

Slika 4. Digitalni potpis

3.3. EAP-TLS Autentifikacija

Proces EAP-TLS autentifikacije slijedi:

1. Klijent šalje EAP Start poruku prema pristupnoj točki
2. AP dogovara porukom sa EAP zahtjevom za identitetom
3. Klijent šalje svoju mrežnu pristupnu identifikaciju (Network Access Identiifier - NAI), koja je njegovo korisničko ime, pristupnoj točki u EAP odgovor poruci
4. AP prosljeđuje NAI prema RADIUS serveru, enkapsuliranu u poruku sa zahtjevom za pristup RADIUS
5. RADIUS server će odgovoriti svojim digitalnim certifikatom
6. Klijent će ocijeniti taj digiitalni certifikat
7. Klijent će odgovoriti RADIUS-u sa svojim digitalnim certifikatom
8. RADIUS će ocijeniti klijentova prava u odnosu n acertifikat
9. Klijent i RADIUS izračunavaju enkripcijske ključeve
10. RADIUS šalje pristupnoj točki RADIUS prihvaćajuću poruku, koja uključuje i klijentov WEP ključ, čime se pokazuje uspješna autentifikacija
11. AP klijentu šalje EAP prihvaćajuću poruku
12. AP šalje broadcast ključ i duljinu ključa klijentu, enkriptirano pomoću klijentova WEP ključa



Slika 5. Poces autentifikacije kod EAP-TLS

4. EAP SIM Arhitektura

EAP pretplatnički idenitski modul (Subscriber Identity Module- SIM) autentifikacijski algoritam je dizajniran da omogući po-korrisniku/po-sesiji obostranu autentifikaciju između bežičnog klijenta i AAA servera. On također definira metodu za generiranje glavnog ključa korištenog od strane klijenta i AAA servera za izračunavanje WEP ključa.

EAP SIM autentifikacija se temelji na autentifikacijskim i enkripcijskim algoritmima pohranjenim u globalnom sistemu za mobilne komunikacije (GSM) SIM, koji ima dizajniranu smartcard prema specifičnim zahtjevima po GSM standardima.

4.1. Proces EAP SIM Autentifikacije

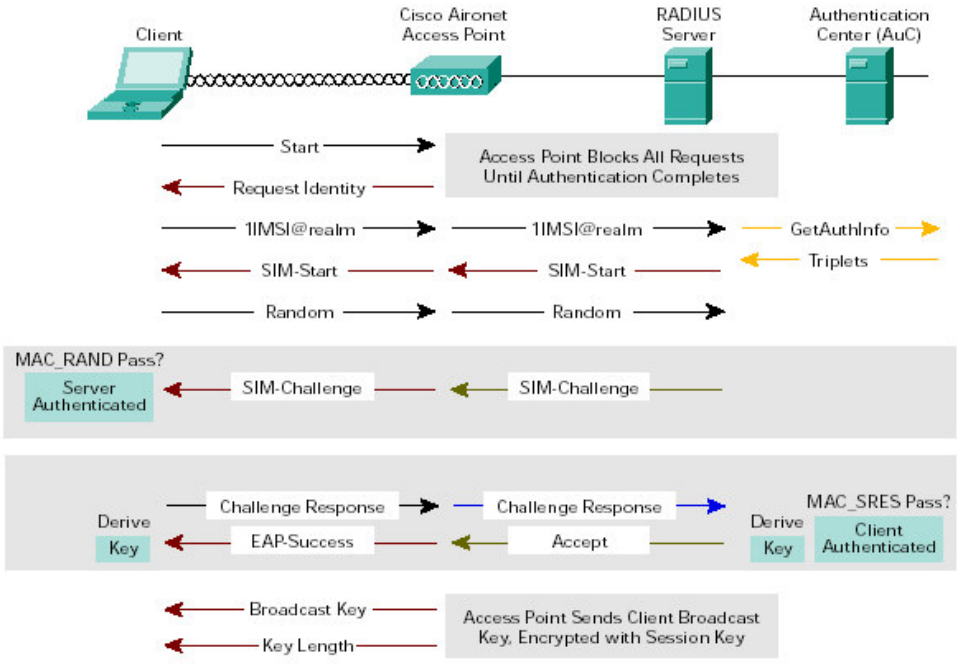
EAP SIM autentifikacija omogućava hardverski baziranu autentifikacijsku metodu dovoljno sigurnu za implementaciju i u potencijalno neprijateljskim javnim upotrebama bežične mreže. Ona dopušta GSM mobilnim operaterima da još jednom iskoriste njihovu postojeću infrastrukturu za pristup bežičnim mrežama. EAP SIM kombinira podatke iz nekoliko GSM 'trojki' (RAND, SRES, Kc) dobivenih od autentifikacijskog centra, za stvaranje sigurnijeg enkripcijskog ključa.
EAP SIM također unapređuje GSM autentifikacijski mehanizam osiguravajući obostranu autentifikaciju između klijenta i AAA servera.
Na klijentovoj strani, EAP SIM protokol, kao i kod potreban za pristup smart-kartici su implemetirani kod EAP SIM pristupnika. Pristupnikov kod je povezan sa

EAP od operativnog sistem koji trenutno za Windows XP i 2000. EAP radi sa porukama od EAP protokola i komunikacijom između pristupnika i AAA servera.

802.1X autentifikacija uz pomoć EAP SIM

1. EAPOL startna poruka započinje autentifikacijski protokoli indicira pristupnoj točki da se klijent želi autentificirati pomoću EAP-a
2. Kao odgovor, pristupna točka šalje EAP zahtjev za identifikacjom klijenta. U ovom trenutku, klijentu još nije dodijeljena IP adresa i AP blokira sve poruke od klijenta osim onih koje su potrebne za autentifikaciju.
3. Klijent odgovara na zahtjev pristupne točke EAP identificirajućom porukom koja sadrži njegov mrežni identitet, koji je određen od strane davatelja usluge. Taj identitet je pročitan sa SIM kartice koja je pridodana klijentu.
4. Pristupna točka prosljeđuje EAP identificirajuću poruku prema AAA serveru uz pomoć RADIUS protokola.
5. AAA server ustanovljuje da pristupnik namjerava koristiti EAP SIM autentifikaciju čime se stvara EAP SIM proširenu kod. Taj kod pak pokreće EAP SIM prošireni protokol slanjem EAP SIM start zahtjeva nazad klijentu. On također generira poruku za dobivanje autentifikacije od autentifikacijskog centra, zahtjeva odgovarajuće GSM trojke.
6. Poruka za dobivanje autentifikacije se prosljeđuje na pretvaranje u GSM standarde.
7. Nakon primanja EAP SIM startnog zahtjeva, klijent čita 128-bitni slučajni broj generiran na SIM kartici i prosljeđuje ga nazad AAA serveru kao odgovor na EAP SIM start poruku.
8. Jednom kada AAA server primi klijentov odgovor na EAP SIM startnu poruku, kao i odgovor od autentifikacijskog centra koji sadrži dovoljan broj GSM 'trojki', on tada stvara EAP SIM ispitnu poruku koja sadrži slučajni broj primljen od autentifikacijskog centra i 160-bitne poruke autentifikacijskog koda (MAC_RAND)
9. Klijent prosljeđuje ispitni zahtjev prema SIM kartici, koja prvo izračuna svoj MAC_RND. AAA server je odgovarajući ako rezultat odgovara MAC_RND primljenom kodu od servera Jedino u tom slučaju SIM izračunava GSM rezultat (SRES) i enkripcijski ključ za svaki primljeni RAN, kako 160-bitnu poruku autentifikacijskog koda (MAC_SRES) temeljenu na rezultatu i korisnikovu identitetu. Jedino se MAC_SRES vraća AAA serveru u odgovoru na ispitnu EAP SIM poruku. SIM također izračunava enkripcijske ključeve, korištenjem sigurne hash funkcije.
10. Kada AAA server primi klijentov odgovor na EAP SIM ispitnu poruku, on izračunava MAC_SRES i uspoređuje ga sa onim primljenim od klijenta. Ako oba odgovaraju, klijent je autentificiran i AAA server također izračunava enkripcijske ključeve. On tada šalje RADIUS prihvaćajuću poruku prema pristupnoj točki koja sadrži enkapsuliranu EAP prihvaćajuću poruku i klijentov ključ za ovu sesiju.

11. Pristupna točka instalira ključ za ovu sesiju i pridružuje ga klijentovom identitetu. Zatim prosljeđuje EAP prihvaćajuću poruku klijentu. Zatim šalje broadcast ključ kriptiran sa klijentoim ključem za sesiju. Također deblokira pristupne portove, tako da može početi promet podacima.
12. Kod primanja EAP prihvaćajuće poruke, EAP SIM pristupnik vraća enkripcijski ključ izračunat pomoću SIM-a EAP-frameworku, koji ga instalira na klijentovu WLAN karticu.
13. Klijent sada može sigurno primati i slati podatke



Slika 6. EAP SIM Autentifikacija

Klijentov sesijski ključ nikad nije poslan preko radio linka, pa nikad nije mogao biti otkriven od napadača koji osluškuju mrežni promet.

Hash funkcija je algoritam koji jednosmjerno enkriptira podatke tako da ne mogu biti dekriptirani da se izračunaju originalni ulazni podatci.

5. PEAP

PEAP – Protected Extensible Authentication Protocol.
PEAP je EAP tip koji dozvoljava hibridnu autentifikaciju. PEAP koristi na serverovoj strani PKI autentifikacju. Na klijentovoj strani, PEAP može koristiti bilo koji drugi EAP autentifikacijski tip. Zbog toga što PEAP uspostavlja sigurni tunel preko serverove strane, ne obostrani tipovi autentifikacije se mogu koristiti na klijentovoj strani,. Tipovi poput EAP generičkih token kartica (GTC), lozinke za jednokratnu upotrebu i EAP MD5 za autentifikaciju pomoću lozinki.

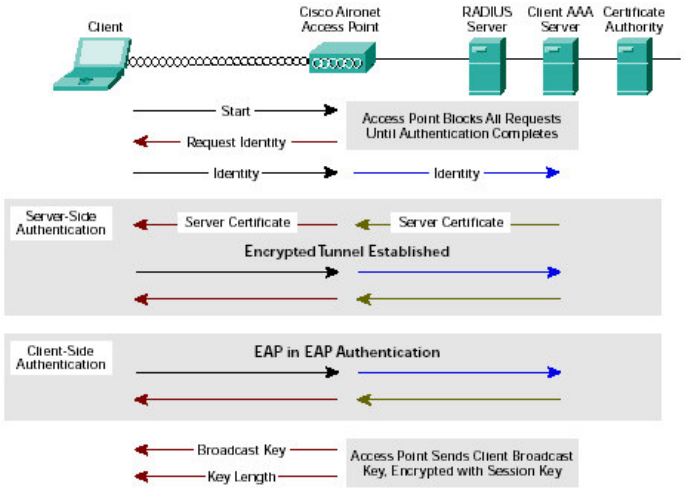
PEAP se temelji na EAP-TLS-u na serverskoj strani i time se rješava većina sigurnosnih problema. Organizacije mogu izbjeći instalacije digitalnih certifikata na sva računala kako to zahtjeva EAP-TLS i mogu izabrati način autentifikacije koji njima najviše odgovara.

PEAP Autentifikacijski proces

1. Klijent šalje EAP start poruku pristupnoj točki
2. AP odgovara sa EAP zahtjevom za autentifikacijom
3. Klijent šalje svoju mrežnu pristupnu identifikaciju (NAI), koja se sastoji od korisničkog imena , prema AP u obliku EAP identificirajućom porukom
4. AP prosljeđuje NAI prema RADIUS serveru enkapsulirano u RADIUS poruku sa zahtjevom pristupa
5. RADIUS server će odgovoriti klijenti njegovim digitalnim certifikatom
6. Klijent procjenjuje RADIUS-ov digitalni certifikat

Odavde nadalje , autentifikacija se razlikuje od EAP-TLS-a:

7. Klijent i server se dogovaraju o otvaranju kriptiranog tunela
8. Taj tunel omogućava sigurnu izmjenu podataka prilikom klijentove autentifikacije
9. Koristeći TLS Record protokol, nova EAP autentifikacija započinje od strane RADIUS servera
10. Razmjena uključuje specifičnosti EAP tipa korištenog za klijentovu autentifikaciju
11. RADIUS server šalje AP RADIUS prihvaćajuću poruku, koja uključuje klijentov WEP ključ, koji indicira uspješnu autentifikaciju.



Slika 7. PEAP Autentifikacija

6. Literatura:

InterLink Networks: Introduction to 802.1X for Wireless Local Area Networks

Cisco: A comprehensive Review of 802.11 wireless LAN security and Cisco wireless security suite

L. Blunk, J. Vollbrecht: RFC2284

B. Aboba, D. Simon : RFC2716