HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Autentikacija u bežičnim mrežama

CCERT-PUBDOC-2006-10-170

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

Autentikacija je proces potvrde identiteta korisnika. Najčešće se taj proces sastoji od unosa zaporke koju sustav provjerava prema danom korisničkom identitetu. U većini situacija ovakva autentikacija pruža dovoljnu razinu zaštite, ali se u slučaju bežične komunikacije pokazala neprikladnom. Zbog toga se u mrežama poput bežičnih računalnih mreža (eng. WLAN – *Wireless Local Area Networks*) primjenjuju različite metode autentikacije koje su prilagođene specifičnim uvjetima prisutnim u bežičnim mrežama i koje garantiraju veću razinu sigurnosti u tim uvjetima.

Autentikacija kod WLAN bežičnih mreža se temelji na 802.11 standardu i pripadnim komunikacijskim protokolima. 802.11 interno koristi EAP (eng. *Extensible Authentication Protocol*) autentikacijski protokol koji je izveden povrh transportnog *Ethernet* protokola. EAP osigurava univerzalnu infrastrukturu za autentikaciju na način da kod klijenta i poslužitelja osigurava sve potrebne preduvjete za dogovaranje pogodne metode autentikacije, a zatim obavlja autentikaciju dogovorenom metodom.

Cilj ovog dokumenta je opisati metode autentikacije u bežičnim mrežama i način kojim EAP osigurava uvjete za njihovu provedbu.

2. Autentikacija u bežičnim mrežama

Postoji nekoliko zahtjeva koji moraju biti zadovoljeni kako bi se stvorili uvjeti za sigurnu autentikaciju zaporkom:

- korisnik mora biti siguran da autentikaciju provodi za to odgovoran entitet,
- komunikacijski kanal između korisnika i autentikacijskog entiteta mora biti siguran (i korisnik i autentikacijski entitet moraju biti sigurni da nitko ne prisluškuje),
- pogađanje prave zaporke mora biti vrlo teško – obično se mogućnost pogotka smanjuje ograničenjem dozvoljenog broja pokušaja, i
- ako je korisnik čovjek (može biti i neka aplikacija) zaporka mora biti dovoljno jednostavna da se može zapamtiti, ali ujedno i toliko složena da se ne može lako pogoditi.

Kod bežičnih mreža navedeni zahtjevi nisu zadovoljeni. Problem se javlja već kod prvog zahtjeva – korisnik prilikom pristupa WLAN mreži ne može znati je li pristupna točka putem koje se prijavljuje autentični dio mreže kojoj želi pristupiti. Naime, moguća je situacija u kojoj napadač postavlja zasebnu pristupnu točku, a korisnik koji nije svjestan opasnosti pokušava se putem nje prijaviti na ciljnu računalnu mrežu te samim pokušajem prijave napadaču dostavlja svoje autentikacijske podatke. Drugi problem predstavljaju svojstva komunikacijskog kanala. U ovom slučaju to je radio kanal, koji svatko može neometano prisluškivati i na taj način prikupljati podatke o pokušajima autentikacije. Opisani nedostatak može se djelomično riješiti korištenjem tehnike izazova i odgovora, pri čemu autentikator šalje izazov, a klijent odgovara odgovorom koji sadrži samo sažetak zaporke i izazova. Iako se zaporka nikad ne šalje komunikacijskim kanalom, sigurnost nije potpuno zajamčena. Budući da napadač ima uvid i u izazov i u sažetak, napadač može metodom uzastopnih pokušaja pronaći prikladnu zaporku (napad rječnikom) koja će primjenom algoritma za izračunavanje sažetka davati isti sažetak kao i prava zaporka.

Iz navedenog je vidljivo da, barem kod bežičnih mreža, ne postoje uvjeti za sigurnu autentikaciju zaporkom. Zahtjevi koji moraju biti zadovoljeni kako bi autentikacija u bežičnim komunikaciji bila sigurna moraju biti znatno stroži od prethodno navedenih, a mogu se podijeliti u tri skupine:

- obvezni zahtjevi,
- dodatni zahtjevi i
- poželjni zahtjevi.

2.1. Obvezni zahtjevi na sigurnost autentikacije u bežičnim mrežama

Autentikacija nužno mora zadovoljavati slijedeće zahtjeve da bi se u okruženju bežičnih mreža smatrala sigurnom:

- Obostranost – autentikacija mora biti obostrana, tj. autentikator mora autenticirati korisnika i korisnik mora autenticirati autentikatora. Ovo svojstvo je važno zbog izbjegavanja klopki nastalih postavljanjem lažnih pristupnih točaka. Postoje dvije vrste lažnih pristupnih točaka koje se koriste za napade – one koje nisu povezane na ciljnu bežičnu mrežu i one koje jesu. U prvom slučaju napadač želi samo zavarati korisnika kako bi dobio njegove autentikacijske podatke. U drugom slučaju napadač ignorira korisnikove autentikacijske podatke, odobrava mu pristup mreži kroz lažnu pristupnu točku i time dobiva uvid u sav njegov naknadni promet.
- Samozaštita – autentikacijski proces mora osigurati zaštitu i za vrijeme autentikacije jer prijenosni medij koji se koristi nije siguran od prisluškivanja. Zaštita mora biti takva da napadač iz podataka koji se razmjenjuju ne može naučiti ništa što bi mogao iskoristiti za razbijanje zaštite.
- Imunost na napade rječnikom – autentikacija mora biti otporna na *on-line* i *off-line* napade rječnikom. *On-line* napadi su napadi uzastopnim pokušajima autentikacije na samom autentikatoru i mogu se izbjeći ograničenim brojem pokušaja. Kod *off-line* napada napadač zaštitu ne probija uzastopnim pokušajima na pravom autentikatoru, već to čini na vlastitom računalu na kome simulira rad autentikatora. Jednostavni oblici izazov/odgovor autentikacija nisu otporni na takav napad jer korisnik dobiva uvid u izazov i odgovor i može sam na svom računalu tražiti zaporku koja odgovara danom izazovu i odgovoru.

- Generiranje ključeva sjednice – autentikacijski proces mora generirati ključeve sjednice koji se mogu koristiti za osiguravanje naknadne autentikacije te za zaštitu povjerljivosti i integriteta podataka koji će se razmjenjivati tijekom naknadne korisničke sjednice.

2.2. Dodatni zahtjevi na sigurnost autentikacije u bežičnim mrežama

Dodatni zahtjevi na sigurnost autentikacije su oni zahtjevi koje metoda autentikacije nije obavezna zadovoljiti, ali ako ih zadovoljava, time značajno doprinosi povećanju sigurnosti procesa autentikacije.
Takvi zahtjevi su sljedeći:

- Autentikacija korisnika – autentikacija bi se trebala odnositi na korisnika, a ne na njegov uređaj. Time se povećava otpornost sustava na napade putem korisnikovog uređaja. Uobičajeno se ovaj zahtjev zadovoljava uporabom jednostavne tajne koju korisnik može lako zapamtiti. Sustav u procesu autentikacije korisnikov identitet potvrđuje samo ako korisnik zna odgovarajuću tajnu. Ukoliko je tajna složenija, za njenu pohranu se koristi pametna kartica, a korisnik u tom slučaju svoj identitet potvrđuje posjedovanjem odgovarajuće kartice.
- Tajnost unaprijed (eng. *Forward Secrecy*) – autentikacija bi trebala unaprijed osigurati buduću komunikaciju nakon autentikacije. To znači da korisnikova tajna (zaporka, tajni ključ) ne smije naknadno biti kompromitirana. Napadač, koji je dobio uvid u podatke korisnikove sjednice zaštićene ključem dobivenim autentikacijom, ne bi trebao moći dekriptirati podatake sjednice čak ni uz poznavanje korisnikove tajne. Jednom kad je sjednica osigurana, ona mora takva i ostati.
- Pristupne točke – autentikacija bi trebala raditi sa svim pristupnim točkama koje podržavaju 802.1x protokol s EAP autentikacijom.
- Brzina i efikasnost – autentikacija bi se trebala izvršiti u minimalnom broju interakcija uz minimalne procesorske zahtjeve za potrebne izračune.
- Mali troškovi održavanja – autentikacija bi trebala biti jednostavna za administriranje. Metoda koja, primjerice, zahtjeva instalaciju certifikata na svaki korisnički uređaj nije jednostavna za administraciju, a administracija liste opozvanih certifikata može predstavljati značajan posao za administratora.
- Jednostavnost korištenja – autentikacija korisnicima ne bi trebala predstavljati teret. Na primjer, autentikacija certifikatom pohranjenim na korisnikovom računalu može zahtijevati veći administratorski trud, ali je zato za korisnika gotovo neprimjetna. S druge strane pametne kartice, iako nezgodne za korisnike, jednostavne su za administriranje. Korisnicima neće biti naporno upisivanje kratkih, jednostavnih zaporki, ali će im zasigurno biti nezgodno upisivati duge nizove heksadecimalnih znakova.

2.3. Poželjni zahtjevi na sigurnost autentikacije u bežičnim mrežama

Za dodatno poboljšanje autentikacije poželjno je zadovoljiti sljedeće zahtjeve:

- Poboljšanje postojeće autentikacije – metoda autentikacije koja zadržava postojeću metodu i pritom je dodatno osigurava sukladno specifičnim zahtjevima bežičnih mreža smatra se vrlo pogodnim rješenjem pogotovo za sustave gdje je postojeću autentikaciju teško izbaciti ili potpuno zamijeniti.
- Brza ponovljena autentikacija – ukoliko je moguće autentikacija bi trebala osigurati mehanizam ponovne autentikacije koji je manje zahtjevan od inicijalne autentikacije. To je posebno značajno za mobilne korisnike gdje je potrebno obaviti brz prijenos korisnika iz nadležnosti jedne pristupne točke u nadležnost druge. Budući da su ti prijenosi vremenski vrlo ograničeni, ponovna autentikacija bi trebala biti ostvarena u što manjem broju interakcija. Taj broj se dodatno smanjuje ako se ponovljena autentikacija ostvaruje samo uz pomoć poslužitelja koji je dio mreže davatelja usluge i bez sudjelovanja matične korisnikove domene.

2.4. 802.1x standard

Iz prethodno opisanih zahtjeva proizašao je standard 802.1x. On definira proces autentikacije koji je nastao prilagodbom EAP standarda za uporabu u WLAN okruženju. Naime, EAP definira proces autentikacije za komunikaciju povrh PPP (eng. *Point-To-Point Protocol*) komunikacijskog protokola, tj. definira kako se EAP poruke pakiraju i prenose unutar PPP paketa.
Budući da se u WLAN mrežama ne koristi PPP protokol, već se umjesto njega koristi *Ethernet* protokol, 802.1x standard definira pakiranje i prijenos EAP poruka unutar *Ethernet* paketa. Sam način rada protokola definiranog u 802.1x standardu ostao je nepromijenjen u odnosu na EAP standard, uz manje razlike u korištenoj terminologiji.
EAP standard i njime definirane metode autentikacije opisani su u nastavku dokumenta.

3. EAP protokol

EAP (eng. *Extensible Authentication Protocol*) nastao je uslijed potrebe za autentikacijom povrh PPP komunikacijskog protokola. Prvotna inačica EAP protokola definirana je 1998. godine standardom RFC2284 [1]. Naknadno je protokol doživio izmjene koje su opisane standardom RFC 3748 [2].
PPP je najčešće korišteni protokol za ostvarenje *dial-up* veze na Internet, ali se također koristi i za ostvarenje autentikacije kod DSL (eng. *Digital Subscriber Line*) ili kabelskog pristupa Internetu. Osim funkcije udaljenog pristupa, jedan njegov dio definira i autentikacijski mehanizam koji se temelji na zaporci i korisničkom imenu.
Budući da su zahtjevi na sigurnost s vremenom povećavani, potreba za novom metodom autentikacije je postajala sve izraženija pa je kao posljedica te težnje nastao EAP protokol. On se nadograđuje na PPP protokol i osigurava podlogu za implementaciju različitih autentikacijskih metoda. Kada se on kod udaljenog pristupa koristi kao autentikacijski protokol, udaljeni autentikacijski poslužitelj ne mora poznavati metodu i parametre autentikacije na lokalnom računalu. Sve potrebne podatke može dobiti kroz izmjenu EAP poruka i kroz intepretiraciju njihova sadržaja. Ovo svojstvo bitno umanjuje posao administratora pri konfiguraciji, jer podatke o postavkama lokalnih računala nije potrebno zapisivati na poslužitelj.
EAP protokol omogućava implementaciju različitih metoda autentikacije. Čak štoviše, EAP standardom su definirane i različite metode autentikacije koje udovoljavaju specifičnim zahtjevima bežičnih mreža. Podijeljene su u dvije grupe:

- Metode autentikacije temeljene na digitalnim certifikatima i TLS (eng. *Transport Layer Security*) protokolu:
  - EAP-TLS,
  - EAP-TTLS (eng. *EAP Tunnelled Transport Layer Security*) i
  - PEAP (eng. *Protected Extensible Authentication Protocol*).
- Metode autentikacije temeljene na metodi jake zaporke ZKPP (eng. *Zero Knowledge Password Proof*)
  - SPEKE (eng. *Strong Password Exponential Key Exchange*) i
  - LEAP (eng. *Lightweight Extensible Authentication Protocol*).

Način rada EAP protokola, kao i opis metoda autentikacije koje se na njemu temelje opisani su u nastavku dokumenta.

3.1. Način rada EAP protokola

EAP je protokol namijenjen prijenosu autentikacijskih podataka, a u svom radu ne zahtijeva uporabu određenog transportnog protokola. Razmjena EAP poruka u uobičajenom procesu autentikacije događa se ovim slijedom:

- Čim utvrdi prisutnost klijenta Autentikator šalje zahtjev za identifikaciju i autentikaciju. Zahtjev sadrži podatak o vrsti autentikacije koja se traži (npr. identitet, MD5-izazov,...).
- Klijent, nakon uspješnog primitka zahtjeva, šalje tražene podatke unutar odgovora koji dodatno sadrži i podatak o tipu autentikacije klijenta. On treba biti jednak tipu autentikacije dobivenom u zahtjevu Autentikatora.
- Autentikator prosljeđuje primljene podatke autentikacijskom protokolu, nakon čega slijedi izmjena autentikacijskih poruka. Izmjenu uvijek započinje Autentikator slanjem zahtjeva, a

završava ju klijent slanjem odgovora na primljeni zahtjev. EAP ne dozvoljava izmjenu opisane sekvence te ne može poslati drugi zahtjev dok na prethodni nije primio odgovor. Ukoliko je potrebno, Autentikator može ponoviti slanje pojedinih poruka zbog grešaka u prijenosu.

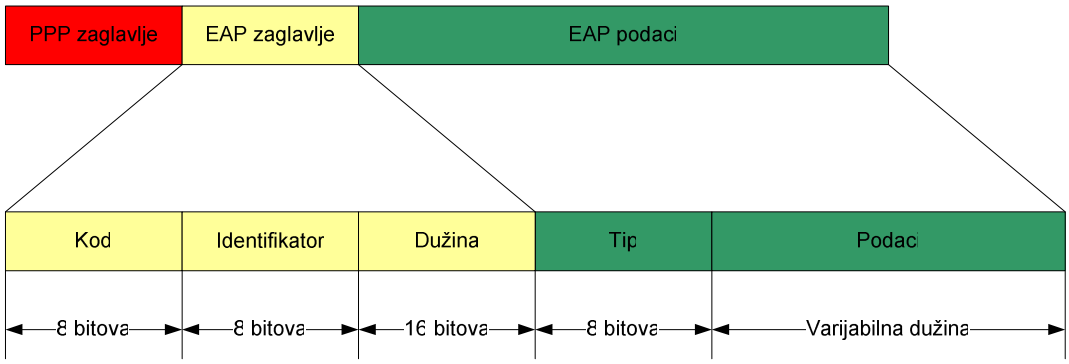
- Ako je autentikacija provedena uspješno, Autentikator šalje klijentu *„EAP Success“* poruku (kod 3), a ako nije šalje *„EAP Failure“* poruku (kod 4). Nijedna od ove dvije poruke ne smije biti poslana u nekoj drugoj situaciji (npr. u slučaju greške u prijenosu).
- Nakon uspješne provedbe autentikacije, Autentikator dozvoljava klijentu pristup mrežnim resursima prema prethodno određenim pravilima.

EAP protokol vodi računa o nekim greškama u prijenosu i implementira mehanizam ponavljanja poruke, ali ne može ukloniti pogrešku uzrokovanu krivim redoslijedom poruka pa od transportnog sloja zahtjeva očuvanje redoslijeda poslanih i primljenih poruka. Također, EAP podržava slanje samo jednog paketa, tj. ne podržava fragmentaciju i defragmentaciju podataka, pa autentikacijske metode koje zahtijevaju prijenos podataka čija je veličina veća od one podržane EAP standardom moraju same osigurati pravilnu fragmentaciju i defragmentaciju.

EAP autentikacija je inicirana od strane poslužitelja (Autentikatora) što je razlika u odnosu na većinu autentikacijskih metoda kod kojih autentikaciju inicira klijent. Za implementaciju takvih autentikacijskih metoda posredstvom EAP protokola potrebno ih je proširiti dodatnim porukama (jednom ili najviše dvije).

Ukoliko se EAP-om ostvaruje autentikacija temeljena na certifikatima, broj interakcija, tj. EAP poruka može biti povećan zbog potrebe fragmentacije. To može dovesti do problema u slučaju implementacije EAP-a povrh transportnog protokola koji zahtijeva ponavljanje slanja poruka jer će u tom slučaju broj poruka biti značajno povećan.

Struktura EAP poruke prikazana je na sljedećoj slici:



Slika 1: Struktura EAP poruke

Značenje pojedinih polja unutar EAP zaglavlja je sljedeće:

- Kod – koriste se samo prva 4 bita koja označavaju kod (tip) poruke:
  - 1 – Zahtjev (eng. *Request*),
  - 2 – Odgovor (eng. *Response*),
  - 3 – Uspjeh (eng. *Success*) i
  - 4 – Neuspjeh (eng. *Failure*).
- Identifikator – jedinstveni identifikator poruke prema kojem se uparuju zahtjev i odgovor.
- Dužina – informacija o dužini podatkovnog dijela poruke.

Podatkovni dio EAP poruke podijeljen je na 2 dijela:

- Tip – tip autentikacijskog protokola koji se prenosi EAP protokolom i
- Podaci – podaci autentikacijskog protokola.

Tip autentikacijskog protokola označava se prema shemi prikazanoj sljedećom tablicom:

Tip	Opis
0	Rezervirano
1	Identitet
2	Obavijest
3	Nak (samo odgovor)
4	MD5-izazov
5	OTP - jednokratna zaporka (eng. *One Time Password*)
6	GTC - generički token / kartica (eng. *Generic Token Card*)
7	
8	
9	RSA PKI autentikacija (eng. *RSA Public Key Infrastructure*)
10	DSS obostrani (eng. *Digital Signature Standard*)
11	KEA (eng. *Key Exchange Algorithm*)
12	KEA validacija
13	EAP-TLS
14	Obrambeni Token (AXENT)
15	RSA Security SecurID EAP
16	Arcot Systems EAP
17	EAP-Cisco Wireless
18	EAP-SIM (eng. *GSM Subscriber Identity Modules*)
19	SRP-SHA1 Part 1 (eng. *Secure Remote Password Protocol - Secure Hash Algorithm*)
20	
21	EAP-TTLS
22	RAS (eng. *Remote Access Service*)
23	EAP-AKA, EAP metoda za 3G autentikaciju i upravljanje ključevima
24	EAP-3Com Wireless
25	PEAP
26	MS-EAP autentikacija
27	MAKE (eng. *Mutual Authentication w/Key Exchange*)
28	CRYPTOCard
29	EAP-MSCHAP-V2
30	DynamID
31	Rob EAP
32	EAP-POTP (eng. *Protected One-Time Password*)
33	MS-Authentication-TLV
34	SentriNET
35	EAP-Actiontec Wireless
36	Cogent Systems Biometrics Authentication EAP
37	AirFortress EAP
38	EAP-HTTP Digest
39	SecureSuite EAP
40	DeviceConnect EAP
41	EAP-SPEKE
42	EAP-MOBAC
43	EAP-FAST (eng. *EAP Flexible Authentication via Secure Tunneling*)
44	ZLXEAP (eng. *ZoneLabs EAP*)

45	EAP-Link
46	EAP-PAX (eng. *EAP Password Authenticated eXchange*)
47	EAP-PSK (eng. EAP *Phase-Shift Keying*)
48	Dostupno uz reviziju ovlaštenog stručnjaka
…	
191	
192	Rezervirano za buduće potrebe standarda
…	
253	
254	Prošireni tip
255	Eksperimentalna upotreba

Tablica 1: Popis mogućih tipova autentikacijskih protokola

Iz prikazane tablice vidljivo je postojanje velikog broja autentikacijskih metoda implementiranih povrh EAP protokola.

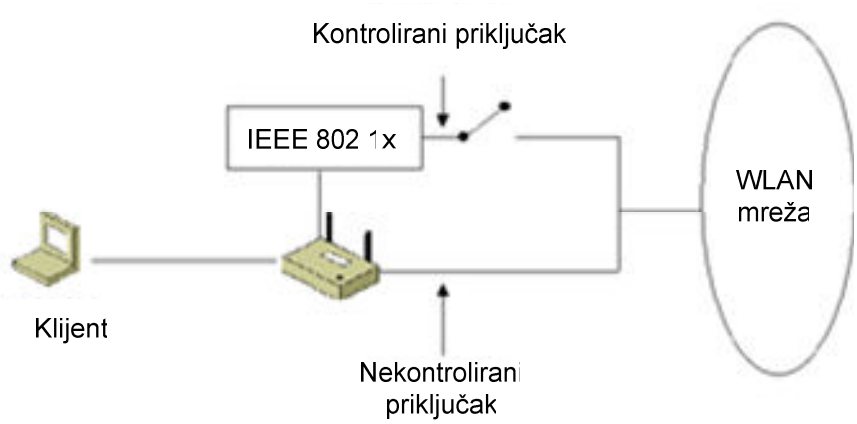
U dosadašnjem razmatranju EAP je kao potporu u prijenosu podataka koristio PPP protokol, ali to nije nužan preduvjet njegovog rada. Zbog svojih karakteristika EAP se može implementirati povrh proizvoljnog transportnog protokola. Ovo svojstvo iskorišteno je za ostvarenje EAP-a u žičnim ili bežičnim LAN mrežama, gdje se komunikacija ostvaruje povrh *Ethernet* protokola. Standard koji opisuje ovakvu realizaciju nosi oznaku 802.1x, a budući se odnosi na EAP u LAN mrežama, još se naziva i EAP *Over* LAN (EAPOL).

3.2. EAPOL (802.1x)

EAPOL je drugo ime za protokol definiran 802.1x standardom. Taj standard definira primjenu EAP protokola u slučaju kad se kao prijenosni protokol koristi *Ethernet*.

802.1x unosi neke izmjene u terminologiju definiranu EAP standardom pa se tako korisnik/klijent koji se želi autenticirati naziva „*Supplicant*“, poslužitelj koji obavlja autentikaciju je autentikacijski poslužitelj, a autentikator je uređaj između klijenta i poslužitelja koji implementira EAP. U slučaju bežičnih WLAN mreža autentikator je bežična pristupna točka, a kao autentikacijski poslužitelj se obično koristi RADIUS (eng. *Remote Authentication Dial In User Service*) poslužitelj. Budući da EAP protokol na strani autentikatora ne zahtijeva veliku računalnu snagu, idealan je za ugradnju u bežične pristupne točke koje obično raspolažu vrlo ograničenim računalnim resursima.

Uobičajeno ostvarenje 802.1x protokola u WLAN bežičnoj mreži realizirano je uz podjelu ulaznih priključaka kao što je prikazano na sljedećoj slici.



Slika 2: Uobičajena realizacija 802.1x protokola

U prikazanoj situaciji ulazni priključci se dijele na:

- kontrolirane priključke – promet kroz njih odvija se između klijenta i bežične pristupne točke i ne dolazi u doticaj s WLAN mrežom,

- nekontrolirane priključke – promet kroz te priključke prolazi preko bežične pristupne točke prema WLAN mreži, ali zahtjeva prethodnu autentikaciju klijenta.

4. EAP metode autentikacije

EAP podržava velik broj različitih metoda autentikacije. Neke od njih definirane su RFC standardima (EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-SIM i EAP-AKA), dok su druge razvijene od strane komercijalnih proizvođača. EAP metode prikladne za upotrebu u bežičnim mrežama su: EAP-TLS, PEAP, LEAP, SPEKE i EAP-TTLS.

EAP-SIM (eng. *EAP-Subscriber Identity Module*), definiran RFC4186 standardom, je EAP autentikacijska metoda razvijena za upotrebu u GSM telefoniji gdje se koristi za autentikaciju korisnika i razmjenu ključeva sjednice pomoću SIM kartice. EAP-AKA (eng. *EAP-Authentication and Key Agreement*), definiran RFC4187 standardom, je autentikacijska metoda koja se koristi za autentikaciju i razmjenu ključeva u UMTS mrežama pomoću USIM kartice. EAP-SIM i EAP-AKA ne koriste se u WLAN mrežama pa nisu detaljnije opisani u nastavku dokumenta.

4.1. EAP-TLS

EAP-TLS metoda autentikacije (eng. *EAP Transport Layer Security*) definirana je RFC2716 standardom [3] i podržana je od većine proizvođača opreme za bežične WLAN mreže. Ona pruža visoku razinu sigurnosti i smatra se nasljednikom SSL (eng. *Secure Socket Layer*) standarda jer koristi PKI (eng. *Public Key Infrastructure*) infrastrukturu za osiguranje komunikacije prema RADIUS autentikacijskom poslužitelju. Budući da EAP-TLS podrazumijeva korištenje PKI infrastrukture i dodjelu digitalnih certifikata klijentu i poslužitelju, administracija sustava je nešto zahtjevnija i to se smatra glavnim nedostatkom ove autentikacijske metode. Funkcionalnosti koje EAP-TLS autentikacijska metoda pruža su sljedeće:

- međusobna autentikacija (klijenta poslužitelju i obratno),
- razmjena ključeva (za uspostavu dinamičkih WEP-*Wired Equivalent Privacy*, ili TKIP-*Temporal Key Integrity Protocol* ključeva),
- fragmentacija i defragmentacija dugih EAP poruka (zbog dužine digitalnih certifikata) te
- brza obnova autentikacije (kroz mehanizam TLS obnove).

EAP-TLS se smatra jednom od najsigurnijih EAP metoda autentikacije, ali se unatoč tome ne primjenjuje često baš zbog potrebe za administracijom velikog broja klijentskih digitalnih certifikata. Upotreba certifikata daje dodatnu sigurnost jer, čak i u slučaju razotkrivanja korisničke zaporke, napadač bez odgovarajućeg certifikata ne može pristupiti sustavu. Ako se certifikati korisnika pohranjuju na pametne kartice, napadač nužno mora ukrasti karticu kako bi došao do certifikata. Budući da je krađu kartice relativno lako otkriti, certifikat s ukradene kartice može se opozvati, čime je opasnost brzo i efikasno uklonjena.

Do 2005. godine EAP-TLS je bila jedina EAP metoda koju je bilo potrebno podržati za dobivanje WPA (eng. *Wi-Fi Protected Access*) ili WPA2 certifikata sigurnosti bežičnih mreža. Ova metoda podržana je klijentskim i poslužiteljskim implementacijama poznatih proizvođača poput Microsoft, Cisco i Apple organizacija te Linux zajednice, a dolazi i kao standardna komponenta slijedećih operacijskih sustava:

- MAC OS 10.3 i noviji,
- Windows 2000 SP4,
- Windows XP,
- Windows Mobile 2003 i noviji, te
- Windows CE 4.2.

4.2. EAP-TTLS

EAP-TTLS (eng. *EAP-Tunnelled Transport Layer Security*) autentikacijska metoda nastala je kao nadogradnja EAP-TLS metode kojom se nastojalo smanjiti zahtjeve na potrebnu infrastrukturu, kao i zahtjeve vezane uz administraciju klijenata. Ona se temelji na uspostavi zaštićenog tunela između klijenta i autentikacijskog poslužitelja kojim se naknadno prenose autentikacijski podaci. Tunel se osigurava uporabom digitalnog certifikata poslužitelja, a od klijenti se ne zahtjeva posjedovanje certifikata. Opisani mehanizam znatno pojednostavljuje administraciju sustava, a nije potrebno

osiguravati ni PKI infrastrukturu, čime se postižu znatne uštede. Rezultat je razina zaštite jednaka razini zaštite web stranica kojima se obavlja sigurno plaćanje.
Sama EAP-TTLS autentikacija obavlja se u dva koraka:

- TTLS rukovanje (eng. *handshake*) – autentikacija poslužitelja klijentu i uspostava sigurnog TLS tunela (budući da klijent ne posjeduje certifikat, obavlja se samo jednostrana autentikacija).
- Autentikacija klijenta – obavlja se izmjenom preddefiniranih parova atribut-vrijednost. Njima se prenose autentikacijski podaci, a sigurnost je zajamčena jer se podaci prenose uspostavljenim TTLS tunelom.

Opcionalno se unutar drugog koraka mogu izmijeniti i enkripcijski ključevi za zaštitu naknadne komunikacije. Bitna je značajka sustava siguran prijenos svakog autentikacijskog podatka razmijenjenog nakon TTLS rukovanja.
EAP-TTLS autentikacijsku metodu razvile su tvrtke Funk Software i Certicom te ju podržavaju one i njihovi partneri. Microsoft ju ne podržava i umjesto nje preferira PEAP metodu, iako je ova u usporedbi s EAP-TTLS inferiornija.

4.3. PEAP

PEAP (eng. *Protected Extensible Authentication Protocol*) autentikacijska metoda je gotovo identična EAP-TTLS metodi. Također se sastoji od dva koraka od kojih je prvi autentikacija poslužitelja i uspostavljanje TLS tunela, a drugi autentikacija klijenta koja od klijenta također ne zahtijeva posjedovanje digitalnog certifikata. Za razliku od EAP-TTLS metode, kod PEAP autentikacije svi autentikacijski podaci nisu zaštićeni. Primjer je korisničko ime koje se šalje prije uspostave sigurnog tunela u nepromijenjenom tekstualnom obliku. Time ono postaje dostupno napadačima koji prisluškuju bežični promet. Iako ovaj nedostatak ne predstavlja značajan rizik, ipak jest nedostatak.
Nakon uspostave sigurnosnog TLS tunela, PEAP autentikacija podržava izmjenu dviju vrsta autentikacijskih podataka, prema čemu se PEAP implementacije dijele u dvije skupine:

- PEAPv0/EAP-MSCHAPv2 autentikacija klijenta obavlja se MSCHAPv2 protokolom. Ovu implementaciju PEAP metode izradio je Microsoft, pa je podržana na većini njegovih proizvoda i platformi. Zbog široke podržanosti često se PEAP metodom smatra upravo ova implementacija.
- PEAPv1/EAP-GTC autentikacija klijenta obavlja se EAP-GTC (eng. *Generic Token Card*) protokolom. Ovu implementaciju načinila je tvrtka Cisco Systems, a opisana je RFC 3748 standardom. Protokol podrazumijeva razmjenu tekstualnog izazova koga generira poslužitelj i odgovora koga generira klijent uz pomoć sigurnosnog tokena. Iako je Microsoft koautor PEAP standarda, PEAPv1 nije podržan od strane proizvoda i platformi izdanih od strane Microsoft organizacije. Uzevši u obzir to, ali i preferiranje LEAP autentikacijske metode od strane Cisco Systems organizacije, lako je objasniti vrlo slabu zastupljenost PEAPv1 autentikacije.

PEAP standard je zajednički proizvod Cisco Systems, Microsoft i RSA Security organizacija i baš zbog te široke podrške istiskuje s tržišta ranije razvijenu i kvalitetniju EAP-TTLS autentikacijsku metodu. Iako je PEAP standard razvijen partnerstvom Microsoft i Cisco organizacijaa, vrlo brzo nakon preuzimanja većine tržišta Microsoft je prestao podržavati PEAPv1/EAP-GTC metodu pa je partnerski odnos raskinut. Danas Cisco većinom podržava PEAPv0/EAP-MSCHAPv2 metodu, a Microsoft ne podržava PEAPv1/EAP-GTC metodu.

4.4. LEAP

LEAP (eng. *Lightweight Extensible Authentication Protocol*) je autentikacijski protokol temeljen na upotrebi zaporke, a razvijen je od strane Cisco Systems organizacije. Od njegovih važnijih karakteristika bitno je naglasiti međusobnu autentikaciju klijenta i bežične pristupne točke prije odobravanja pristupa samoj mreži i to pomoću dijeljene tajne. Osim toga, bežična sjednica se zaštićuje sigurnosnim ključevima, a sama autentikacija se temelji na korisničkom imenu i zaporci. Budući da se zaštitni ključevi mijenjaju u svakoj sjednici, komunikacija bi trebala biti prilično sigurna. Unatoč tome, otkriveno je nekoliko sigurnosnih ranjivosti od kojih je najznačajnija neotpornost na napad rječnikom.

Usprkos otkrivenim i dokazanim sigurnosnim propustima, Cisco Systems tvrdi da je LEAP protokol dovoljno siguran ako se koristi u kombinaciji s dovoljno kompleksnim zaporkama. Međutim, pokazalo se da se kompleksne zaporke ipak najčešće ne koriste zbog njihove nepraktičnosti.
LEAP protokol podržan je u svim Cisco Systems proizvodima i proizvodima partnera Cisco organizacije, ali nije podržan u proizvodima ostalih proizvođača, pa tako za LEAP nema podrške ni u Windows operacijskim sustavima. Obzirom na veću razinu sigurnosti ostalih autentikacijskih metoda, većina proizvođača odabire podršku za EAP-TLS ili EAP-TTLS. LEAP se tako danas koristi gotovo isključivo na Cisco Systems bežičnim pristupnim točkama.

4.5. SPEKE

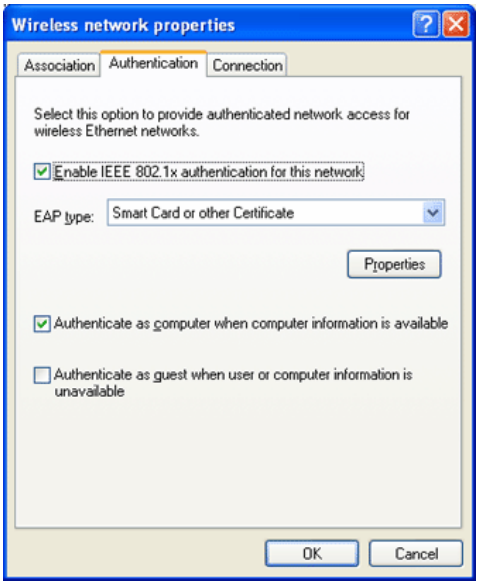
SPEKE (eng. *Strong Password Exponential Key Exchange*) je autentikacijska metoda temeljena na zaporci i korisničkom imenu (kao i LEAP), ali se smatra znatno sigurnijom jer je gotovo nemoguće otkriti zaporku iz poruka koje se razmjenjuju između klijenta i poslužitelja. SPEKE metoda sastoji se od razmjene serija poruka koje izgledaju kao niz slučajnih brojeva. SPEKE moduli na strani klijenta i poslužitelja provode obradu tih poruka i na osnovu rezultata obrade određuju je li zaporka korištena na drugoj strani ispravna. Ako je tako, SPEKE moduli izdaju dijeljene ključeve za daljnju komunikaciju.
Mogućem napadaču SPEKE poruke izgledaju kao niz slučajnih brojeva i napadač na temelju tih poruka ne može ni pokušati pogoditi izgled zaporke. Osim toga, dodatna snaga SPEKE metode je korištenje javnih ključeva koji se ne distribuiraju niti ne administriraju na strani klijenata. Jedino što je potrebno administrirati su zaporke, a njihova zaštita ostvarena je korištenjem ZKPP (eng. *Zero Knowledge Password Proof*) metode za siguran prijenos zaporke. Ova metoda klijentu omogućava dokazivanje poznavanja zaporke bez otkrivanja bilo kojeg dijela njenog sadržaja.
SPEKE metoda koristi se u postupcima za poboljšanje sigurnosti autentikacije zaporkom pa se, kao i njoj slične, naziva autentikacijom jakom zaporkom. Kod takve autentikacije čak i male i jednostavne zaporke dobro su zaštićene od napada.
Karakteristike SPEKE autentikacije su:

- mogućnost korištenja jakih i neograničeno dugih ključeva,
- zaštita od *off-line* napada rječnikom (bolja od zaštite koju pruža metoda izazov/odgovor),
- klijent i poslužitelj se autenticiraju istovremeno,
- nije potrebna nikakva dodatna infrastruktura (za implementaciju SPEKE metode potrebno je samo jednom instalirati SPEKE upravljački program na klijent i bežičnu pristupnu točku),
- nisu potrebni klijentski ili poslužiteljski certifikati,
- pruža sve dobrobiti suvremene kriptografije korištenjem obične zaporke, itd…

Treba napomenuti da je SPEKE moguće koristiti s bilo kojom bežičnom pristupnom točkom koja podržava 802.1x standard te da SPEKE standardno nudi podršku za administraciju zaporki.

5. EAP i Windows operacijski sustav

Windows XP operacijski sustav podržava 802.1x standard i EAP-TLS autentikacijsku metodu. Konfiguracija te autentikacije obavlja se postavljanjem autentikacijskih parametara unutar postavki parametara bežične mreže.



Slika 3: Prikaz postavki autentikacije u Windows XP operativnom sustavu

Unutar autentikacijskih postavki moguće je uključiti ili isključiti 802.1x autentikaciju te odabrati željenu metodu autentikacije. Dostupne su slijedeće metode:

- EAP-TLS metoda – autentikacija pametnom karticom ili certifikatom (standardno podešena) i
- PEAP metoda – Microsoft PEAP autentikacija.

Dodatno se mogu postavljati parametri EAP-TLS metode odabirom opcije *Properties*. Tako se može odabrati da se autentikacija obavlja pomoću pametne kartice ili certifikata pohranjenog na računalu, a mogu se postaviti i druge sigurnosne opcije poput ocjene ispravnosti certifikata, popisa provjerenih autentikacijskih poslužitelja i korisničkog imena za autentikaciju.

Vidljivo je da je korištenje EAP-TLS i PEAP metode autentikacije unutar EAP protokola za Windows korisnike vrlo jednostavno. Stoga je razumljiva i popularnost spomenutih metoda autentikacije kod proizvođača opreme za WLAN mreže.

6. Zaključak

Sigurnost bežičnih mreža neupitno pruža značajne prednosti. Neke od njih su, primjerice, ušteda zbog spriječenih napada i zaštićenih podataka, povećana produktivnost i komparativna prednost na tržištu. Prema tome, uopće nije upitno da li su potrebne sigurne bežične mreže, već je jedino pravo pitanje koju vrstu zaštite koristiti.

Slijedeća tablica prikazuje usporedbu dostupnih EAP autentikacijskih metoda predstavljenih ovim dokumentom. Podijeljene su prema temelju svoga rada na tri skupine: certifikati, zaporke i jake zaporke. Usporedba je načinjena prema zahtjevima koje bi autentikacija u bežičnim mrežama trebala zadovoljiti.

Zahtjev	Certifikat (EAP-TLS, EAP-TTLS, PEAP)	Zaporka (LEAP)	Jaka zaporka (EAP-SPEKE)
Obavezni			
Obostranost	DA	DA	DA
Samozaštita	DA	DA	DA
Imunost na napade rječnikom	DA	NE	DA
Generiranje ključeva	DA	DA	DA
Potrebni			
Autentikacija korisnika	NE ako su certifikati pohranjeni na disku	DA	DA
Tajnost unaprijed	NE uz standardne enkripcijske metode	DA	DA
Brzina i efikasnost	NE	DA	DA
Mali troškovi održavanja	NE	DA	DA
Jednostavnost korištenja	Samo ako su certifikati pohranjeni na disku	DA	DA
Pristupne točke (podržanost)	DA	NE	DA
Poželjni			
Poboljšanje postojeće autentikacije	DA	NE	NE
Brza ponovljena autentikacija	DA	NE	NE – obavezno vraćanje na vlastitu domenu

Tablica 2: Usporedba EAP metoda autentikacije

Metode temeljene na certifikatima i na jakoj zaporci zadovoljavaju sve obavezne uvjete dok LEAP nije imun na napade rječnikom. Metode temeljene na certifikatima zadovoljavaju i poželjne uvjete kao što je mogućnost poboljšanja postojećih metoda autentikacija, ali nisu dovoljno pogodne za administraciju. Baš je jednostavnost administracije područje u kojem SPEKE autentikacija dominira. Zbog toga i zbog zadovoljavajuće razine sigurnosti koju pruža, SPEKE autentikacija je pogodna za primjenu u javnim bežičnim pristupnim točkama jer je jednostavna za korištenje svim korisnicima, a istovremeno ne predstavlja veliki trošak vlasniku mreže. Osim navedenog, SPEKE metodu podržavaju gotovo sve bežične pristupne točke što je čini pogodnom za upotrebu u heterogenim mrežama.

7. Reference

[1] PPP Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc2284.txt
[2] Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc3748.txt
[3] PPP EAP TLS Authentication Protocol, http://www.ietf.org/rfc/rfc2716.txt
[4] EAP Methods for 802.11 Wireless LAN Security, http://www.iec.org/online/tutorials/eap_methods/topic01.html, listopad 2006.
[5] IEEE 802.1X: EAP over LAN (EAPOL) for LAN/WLAN Authentication & Key Management, http://www.javvin.com/protocol8021X.html, listopad 2006.
[6] EAP - Extensible Authentication Protocol, http://www.networksorcery.com/enp/protocol/eap.htm, listopad 2006.
[7] The EAP heap: wireless authentication protocols, http://www.techworld.com/mobility/features/index.cfm?featureID=404&pagtype=all, listopad 2006.
[8] IEEE 802.1X Authentication for Wireless Connections, http://www.microsoft.com/technet/community/columns/cableguy/cg0402.mspx, listopad 2006.