HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

EAP protokol

CCERT–PUBDOC–2008–01–216

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.

Sadržaj

1. Uvod

Proširivi autentikacijski protokol EAP (eng. *Extensible Authentication Protocol*) omogućuje autentikaciju korištenjem neke od podržanih metoda, kojih trenutačno na raspolaganju ima četrdesetak, a najčešće se koristi kod bežičnih računalnih mreža. Definiran je RFC 3748 (eng. *Request for Comment*) dokumentom IETF (eng. *Internet Engineering Task Force*) standardizacijske organizacije dok su u dokumentu RFC 4017 navedeni zahtjevi postavljeni na EAP metode namijenjene bežičnim mrežama.

EAP protokol se koristi na podatkovnom mrežnom sloju OSI (eng. *Open System Interconnection*) referentnog modela. Na raspolaganju su implementacije protokola namijenjene mrežama s usmjerivačima (eng. *router*) te prospojnim (eng. *switched*) mrežama. Kod bežičnih mreža implementira se u pristupnim točkama i preklopnicima (eng. *switch*). Prednost ovog autentikacijskog protokola laži u njegovoj proširivost, koja se očituje u mogućnosti izbora autentikacijske metode te jednostavnog dodavanja novih metoda bez potrebe za izmjenama cjelokupne implementacije protokola.

U ovom dokumentu prikazani su struktura i osnovne funkcionalnosti EAP protokola, opisana je EAP komunikacija, povezivanje s AAA (eng. *Authentication, Authorization and Accounting*) protokolima te format EAP podatkovnih paketa. Također je dan pregled popularnih EAP metoda i sigurnosnih prijetnji.

2. Osnove proširivog autentikacijskog protokola

EAP protokol nastao je kao nadogradnja PPP (eng. *Point-to-Point Protocol*) protokola kako bi se prilikom pokušaja spajanja na mrežu omogućila autentikacija proizvoljnom metodom. Kod do tada podržanih PPP autentikacijskih protokola, kao što su CHAP (eng. *Challenge Handshake Authentication Protocol*), MS-CHAP (eng. *Microsoft CHAP*) i MS-CHAP v2 (eng. *MS-CHAP version 2*), tijekom faze uspostavljanja veze odabire se specifičan autentikacijski mehanizam. Za vrijeme autentikacijske faze usuglašeni autentikacijski protokol omogućuje razmjenu podataka o klijentu koji se pokušava povezati. Ovaj postupak provodi se razmjenom točno određenih poruka koje se šalju specifičnim redoslijedom.

Kod EAP protokola se za vrijeme faze uspostavljanja veze ne usuglašava autentikacijski mehanizam, već se sudionici komunikacije dogovaraju o korištenju EAP protokola tijekom autentikacijske faze. Na početku ove faze usuglašuje se način EAP autentikacije, tzv. EAP metoda.

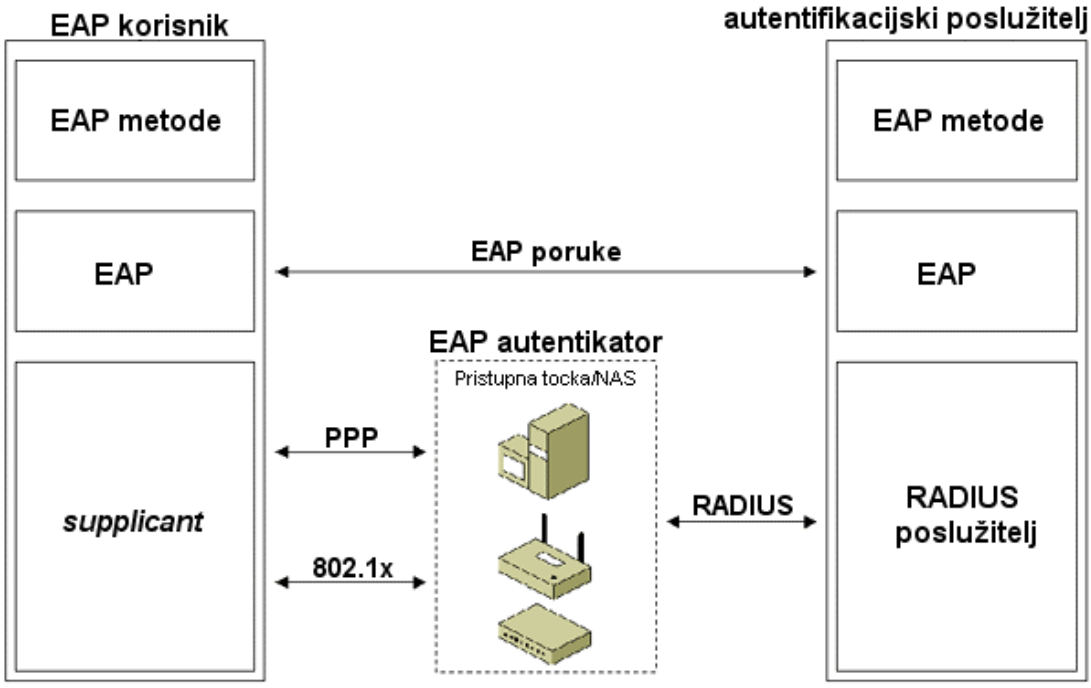
Nakon što je dogovorena EAP metoda, između klijentskog računala i poslužitelja započinje razmjena autentikacijskih poruka čiji tijek nije strogo određen već može ovisiti o parametrima veze. Razmjenjuju se zahtjevi za autentikacijskim podacima i odgovori na njih. Duljina pojedine poruke i ostali detalji određeni su odabranom EAP metodom.

EAP autentikacijska struktura sastoji se od:

- **EAP klijent** (eng. *peer*) predstavlja računalo koje se pokušava povezati na mrežu.
- **EAP autentikator** je mrežna pristupna točka ili pristupni poslužitelj (eng. *Network Access Server - NAS*) koji prije omogućavanja pristupa mreži od klijenta zahtjeva EAP autentikaciju.
- **Autentikacijski poslužitelj** s klijentom dogovara korištenje određene EAP metode, ocjenjuje njegove autentikacijske podatke te mu dopušta ili uskraćuje pristup mreži. Ulogu autentikacijskog poslužitelja često kod EAP autentikacije igra RADIUS (eng. *Remote Authentication Dial-In User Service*) poslužitelj.

EAP autentikator i poslužitelj mogu biti implementirani na jednom uređaju ili odvojeni u dva zasebna uređaja.

Proširivost EAP protokola proizlazi iz mogućnosti njegove nadogradnje novim metodama u obliku dodataka (eng. *plug-in*). Kako bi se omogućilo korištenje nove metode potrebno je nadograditi inačice protokola na klijentskom računalu i na poslužitelju odgovarajućom programskom bibliotekom.



Slika 1: EAP autentikacijska struktura

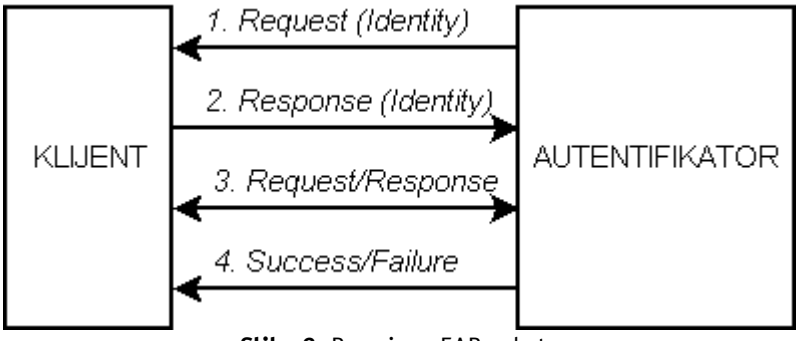
EAP korisnik i autentikator poruke šalju pomoću tzv. *supplicant* programske komponente i nekog protokola iz sloja podatkovne veze (eng. *data link layer*) OSI mrežnog modela, kakvi su PPP ili IEEE 802.1X (eng. *Institute of Electrical and Electronics Engineers*) protokoli. Autentikator i poslužitelj međusobno komuniciraju RADIUS protokolom ili nekim srodnim protokolom. Pri tome EAP autentikator djeluje kako posrednik prenoseći poruke između klijenta i poslužitelja te na njemu nije potrebna podrška za pojedine EAP metode. Opisna struktura prikazana je slikom *Slika 1*.
Pomoću EAP protokola moguće je implementirati različite autentikacijske metode, kao što su GTC (eng. *Generic Token Card*), OTP (eng. *One Time Password*), MD5-*Challenge* (eng. *Message Digest 5*) i TLS (eng. *Transport Layer Security*) autentikacija, različite autentikacijske metode temeljene na digitalnim certifikatima idr.
Pored PPP protokola, EAP autentikacija podržana je i od strane IEEE 802 skupine protokola, unutar sloja podatkovne veze. IEEE 802.1X standardom definirano je EAP autentikacija IEEE 802 uređaja, kao što su IEEE 802.11 bežične pristupne točke i mrežni preklopnici. EAP implementacija kod IEEE 802.1X protokola se od PPP implementacije razlikuje po tome što podržava isključivo EAP metode.

3. EAP komunikacija

EAP komunikacija provodi se u sljedećim koracima:

1. Autentikator započinje autentikaciju slanjem zahtjeva klijentu u obliku EAP paketa tipa *Request*. Vrijednost *Type* polja ovog paketa određuje na što se točno odnosi zahtjev. Primjeri ovakvih zahtjeva su *Identitiy* i *MD5-Challenge* paketi. Uobičajeno je da autentikacija započinje *Identity* zahtjevom, ali on može biti i izostavljen ako je identitet klijenta utvrđen na neki drugi način. Identitet je, na primjer, moguće utvrditi na temelju porta na kojega se klijent spojio, iz njegove MAC (eng. *Media Access Control*) adrese ili može biti sadržan u *Name* polju odgovora na MD5-*Challange* zahtjev.
2. Korisnik na ispravno oblikovan zahtjev autentikatora odgovara EAP paketom tipa *Response*. Odgovor u *Type* polju sadrži vrijednost koja odgovara vrijednosti *Type* polja primljenog zahtjeva.
3. Nakon primitka odgovora na prvi zahtjev, autentikator šalje dodatne *Request* pakete, na koje korisnik odgovara odgovarajućim *Response* paketima. Takva razmjena nije ograničena ni vremenski niti brojem poslanih ili primljenih paketa. EAP spada u skupinu tzv. „*lock step*" protokola, što znači da autentikator, nakon slanja početnog zahtjeva, ne šalje nove *Request* pakete ukoliko nije primio ispravan odgovor na prethodni zahtjev. U slučaju izostanka odgovora na neki od zahtjeva autentikator provodi odgovarajuću proceduru njegova ponovnog slanja. Ako ni nakon određenog broja ponovnih slanja zahtjeva klijent ne pošalje ispravan odgovor, autentikator prekida EAP autentikaciju. Pri tome se korisniku ne šalje ni *Success* niti *Failure* paket.
4. Razmjena poruka između klijenta i autentikatora nastavlja se do utvrđivanja nemogućnosti autentikacije klijenta, npr. uslijed neprihvatljivog odgovora na jedan ili više zahtjeva, pri čemu se postupak završava slanjem obavijesti o neuspjeloj autentikaciji klijentu *Failure* EAP paketom. Ako je postupak autentikacije uspješno proveden autentikator klijenta o tome obavješćuje slanjem *Success* paketa.

Opisana razmjena EAP paketa između klijenta i autentikatora prikazana je slikom Slika 2.



Slika 2: Razmjena EAP paketa

4. Autentikacija, autorizacija i obračun

AAA protokoli koriste se za upravljanje pristupom mrežnim resursima i sadrže tri komponente:

- **Autentikacija** se odnosi na potvrđivanje identiteta korisnika koji je zatražio određenu mrežnu uslugu te na utvrđivanje prava pristupa korisnika zatraženoj usluzi. Provodi se iskazivanjem identiteta, npr. korisničkog imena, i predočavanjem vjerodajnice (eng. *credential*), npr. zaporke.
- **Autorizacija** predstavlja odobravanje određenih vrsta usluga, uključujući tzv. *no service* uslugu, korisniku na temelju rezultata prethodno provedene autentikacije, zatražene usluge i trenutnog stanja poslužitelja. Autorizaciju je, na primjer, moguće provoditi:
  - vremenskim ograničenjima, npr. onemogućavanjem određenih usluga pojedinim korisnicima tijekom određenih vremenskih perioda,
  - ograničavanjem pristupa korisnicima s određenih fizičkih lokacija,
  - onemogućavanjem višestrukog prijavljivanja istog korisnika.
- **Obračun** se odnosi na praćenje potrošnje mrežnih resursa od strane pojedinih korisnika s ciljem upravljanja mrežom, planiranja održavanja i nadogradnje, naplaćivanja usluga idr.

U okviru EAP autentikacije, AAA protokol se izvodi na pozadinskom poslužitelju, ukoliko je on odvojen od autentikatora, ili na samom autentikatoru. EAP protokol podržava AAA protokole RADIUS i Diameter.

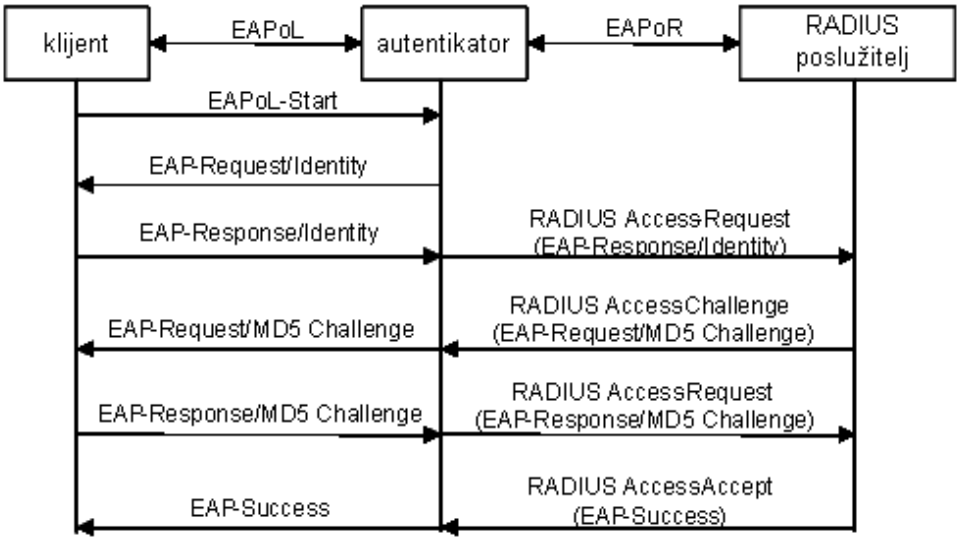
4.1. RADIUS

RADIUS je centralizirani AAA protokol prvotno namijenjen modemskom (eng. *dial-up*) pristupu udaljenim mrežama koji danas podržava bežične pristupne točke, eternet preklopnike, VPN (eng. *Virtual Private Network*) poslužitelje, DSL (eng. *Digital Subscriber Line*) poslužitelje te druge pristupne poslužitelje.

Infrastruktura RADIUS sustava sastoji se od:

- **Pristupni klijent** zahtjeva pristup mreži.
- **RADIUS klijent (EAP autentikator)** je uređaj koji omogućuje pristup računalnoj mreži ili njenom segmentu, kao što su bežične pristupne točke, preklopnici ili NAS poslužitelji.
- **RADIUS poslužitelj (autentikacijski poslužitelj)** je uređaj koji prima zahtjeve za uspostavljanjem veze i podatke o klijentima. Na temelju skupa pravila, RADIUS atributa primljenog zahtjeva i podataka iz baze podataka korisničkih računa poslužitelj odlučuje o uspješnoj autentikaciji i dozvoljava pristup mreži slanjem *Access-Accept* poruke ili ga uskraćuje *Access-Reject* porukom. *Access-Accept* poruka može sadržavati ograničenja na dozvoljenu vezu.
- **Baza podataka korisničkih računa** omogućuje RADIUS poslužitelju provjeru korisničkih vjerodostojnica.
- **RADIUS *proxy* poslužitelj** prosljeđuje i usmjerava zahtjeve i odgovore između RADIUS klijenata i poslužitelja.

EAP poruke razmjenjivane između EAP klijenta i autentikatora oblikuje se kao *EAP-Message* RADIUS atribut i šalju unutar RADIUS poruka između autentikatora i autentikacijskog poslužitelja. Tako se EAP komunikacija odvija posredstvom autentikatora, djelomično prema EAP, a dijelom prema RADIUS protokolu, kao što je prikazano na slici *Slika 3*. Autentikator je postavljen tako da koristi EAP protokol za autentikaciju te RADIUS poslužitelj kao pozadinski autentikacijski poslužitelj. Klijent autentikatoru šalje EAP poruku koju on ugrađuje u RADIUS poruku i prosljeđuje ju poslužitelju. Nakon obrade poruke, poslužitelj autentikatoru odgovara EAP porukom unutar RADIUS paketa. Autentikator klijentu prosljeđuje primljenu EAP poruku.

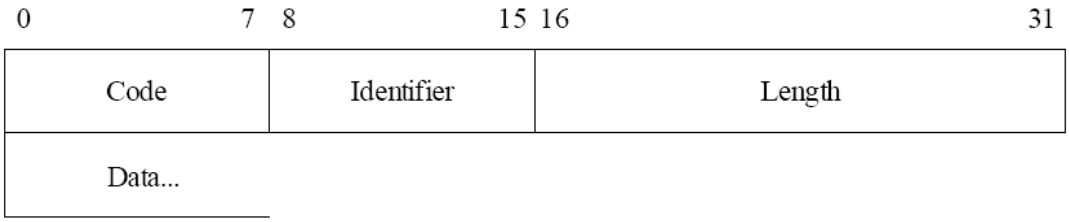


Slika 3: Komunikacija EAP klijenta s RADIUS poslužiteljem

5. Format EAP paketa

5.1. Format osnovnog EAP paketa

Format osnovnog EAP paketa prikazan je na slici *Slika 4*.



Slika 4: Osnovni format EAP paketa

Prvi oktet EAP paketa zauzima polje *Code*, koje sadrži tip (eng. *Type*) EAP paketa. Moguće vrijednosti ovog polja dane su u tablici *Tablica 1*. EAP protokol podržava samo navedene vrijednosti *Code* polja, te svi paketi s drugačijim vrijednostima bivaju odbačeni.

Vrijednost	Opis
1	zahtjev (eng. *Request*)
2	odgovor (eng. *Response*)
3	uspjeh (eng. *Success*)
4	neuspjeh (eng. *Failure*)

Tablica 1: Vrijednosti *Code* polja EAP paketa

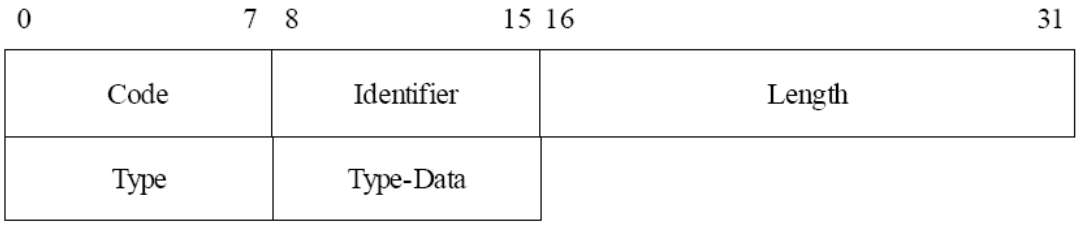
Sljedeći oktet zauzima *Identifier* polje, čiji sadržaj omogućuje povezivanje odgovora sa zahtjevima.
Polje *Length* sadrži vrijednost koja označava duljinu EAP paketa u oktetima. Duljina EAP paketa uključuje polja *Code*, *Identifier*, *Length* i *Data*. Svi okteti koji prelaze vrijednost navedenu u polju *Length* se po primitku smatraju popunom (eng. *padding*) te se zanemaruju.
Nakon prva 4 okteta slijede podaci u polju *Data*. Duljina tog polja varira i može poprimiti vrijednosti 0 ili nekoliko okteta. Tip podataka EAP paketa ovisi o vrijednosti u polju *Code*, odnosno o tipu EAP paketa.
EAP paketi se mogu podijeliti u dvije skupine:

- *Request/Response* skupina paketa sastoji se od
  - *Request* paketa koje šalje autentikator, a predstavljaju upite klijentu, te

- *Response* paketa koji predstavljaju odgovore klijenta autentikatoru.
- *Success/Failure* skupina također sadrži dva tipa paketa:
  - *Success* paketom autentikator klijenta obavještava o uspješno provedenoj autentikaciji dok
  - *Failure* paket predstavlja obavijest o neuspješnoj autentikaciji.

5.2. Format *Request/Response* tipa paketa

Na slici *Slika 5* je prikazan format *Request/Response* vrste paketa. U odnosu na općeniti format EAP paketa, razlikuje samo u polju *Type*. Ono je duljine jednog okteta te sadrži heksadecimalnu vrijednost koja označava različite tipove *Request/Response* paketa.



Slika 5: Format *Request/Response* paketa

Neke vrijednosti polja *Type* prikazane su u tablici *Tablica 2*.

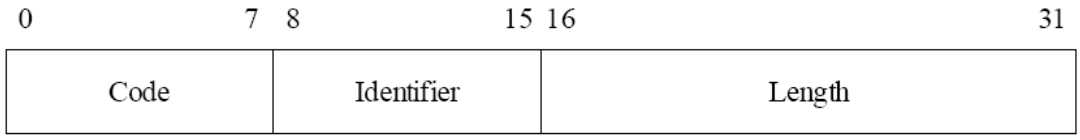
Vrijednost	Tip paketa
1	*Identity*
2	*Notification*
3	*Nak* (smo za *Response* pakete)
4	*MD5-Challenge*
5	OTP (eng. *One Time Password*)
6	GTC (eng. *Generic Token Card*)
13	TLS
26	EAP MSCHAPv2
254	*Expanded*
255	*Experimental*

Tablica 2: Vrijednosti *Type* polja za različite tipove EAP paketa

Sve implementacije EAP protokola moraju podržavati tipove 1 do 4 , a trebale bi podržavati i tip 254. Nakon polja *Type* slijedi polje *Type-Data* koje sadrži podatke specifične za određenu vrstu paketa.

5.3. Format *Request/Response* tipa paketa

Format paketa iz Success/Failure skupine paketa prikazan je na slici *Slika 6*. Ovi paketi sadrže samo tri polja čija uloga je jednaka kao kod osnovnog EAP paketa. *Success* paket u polju *Code* ima vrijednost 3, dok *Failure* paket u istom polju ima vrijednost 4.



Slika 6: Format *Success/Failure* paketa

6. Prednosti i nedostaci EAP protokola

Osnovne prednosti EAP protokola su:

- EAP protokol podržava višestruke načine autentikacije, bez potrebe za prethodnim usuglašavanjem korištenog autentikacijskog mehanizma.
- Pristupni poslužitelji, kao što su preklopnici i pristupne točke, ne moraju podržavati pojedine autentikacijske metode već mogu djelovati kao posrednik u komunikaciji klijenta s pozadinskim autentikacijskim poslužiteljem. Na primjer, autentikatora je moguće postaviti tako da provodi autentikaciju lokalnih klijenata dok za udaljene klijente i klijente koji se autenticiraju metodama koje autentikator ne podržava djeluje kao posrednik.
- Odvajanjem autentikatora od autentikacijskog poslužitelja pojednostavljuje upravljanje vjerodajnicama i olakšava donošenje odluka vezanih uz sigurnosnu politiku.

Glavni nedostaci EAP protokola su:

- Za korištenje EAP protokola unutar PPP protokola potrebno je PPP LCP (eng. *Link Control Protocol*) protokol nadograditi dodatnim autentikacijskim tipom, odnosno nužna je izmjena implementacije PPP protokola. Također, EAP odstupa od izvornog PPP autentikacijskog modela kod kojega se način autentikacije usuglašava tijekom LCP faze.
- Kako bi koristile EAP protokol implementacije pristupnih točaka i preklopnika moraju podržavati IEEE 802.1X standard.
- U slučaju odvajanja autentikatora od pozadinskog autentikacijskog poslužitelja otežana je analiza sigurnosti sustava te raspodjela ključeva.

7. EAP metode

U nastavku su opisane neke češće korištene EAP metode.

7.1. LEAP

LEAP (eng. *Lightweight EAP*) je EAP metoda kod koje ulogu autentikacijskog poslužitelja igra RADIUS poslužitelj. Koristi za autentikaciju bežičnih klijenta, kao što su prijenosna računala ili računala s bežičnom karticom, te definira komunikaciju između pristupne točke (tj. autentikatora) i RADIUS poslužitelja u sljedećim koracima:

1. Protokol započinje porukom pristupne točke RADIUS poslužitelju s imenom korisnika koji je zatražio autentikaciju.
2. Poslužitelj odgovara *RadiusChallenge* porukom, koja sadrži nasumičnu *MSCHAP PC* (eng. *Peer Challenge*) vrijednost.
3. Treću poruku šalje pristupna točka poslužitelju s odgovorom na PC vrijednost poslanu prethodnom porukom.
4. Ako je autentikacija uspjela, RADIUS poslužitelj odgovara *Access-Accept* porukom.
5. Zatim pristupna točka šalje RADIUS *Request* poruku koja sadrži APC (eng. *Access Point Challenge*).
6. Poslužitelj na to odgovara porukom koja sadrži ključ sjednice u obliku Radius atributa: *leap:session-key=nnnn*.

Sve poruke su EAP oblika, polje *Type* ima vrijednost 17, a polje *Type-Data* je podijeljeno na sljedeće dijelove:

- jedan oktet s brojem verzije LEAP protokola,
- jedan oktet postavljen na vrijednost 0x00,
- oktet s duljinom polja koje slijedi (*Binary-Data*),
- *m* okteta polja *Binary-Data*,
- *n* okteta s imenom korisnika koji je zatražio autentikaciju.

LEAP je još poznat i pod nazivom EAP-CISCO, jer se koristi u usmjerivačima tvrtke *Cisco Systems*.

7.2. EAP-TLS

EAP-TLS je metoda za obostranu autentikaciju koja omogućava zaštitu integriteta i razmjenu ključeva između dvije krajnje točke. Ova metoda provodi se u sljedećim koracima:

1. EAP-TLS metoda započinje razmjenom *Identity Request/Response* poruka.
2. Nakon utvrđivanja identiteta partnera, EAP poslužitelj šalje *EAP-TLS Start* paket. Time započinje TLS komunikacija koja se provodi porukama s vrijednošću 13 u EAP polju *Type*.

3. Zatim slijedi *client_hello_handshake* poruka (unutar EAP *Response* paketa, također s poljem *Type* postavljenim na EAP-TLS), koja sadrži inačicu TLS metode, nasumičan broj te oznaku skupa kriptografskih metoda podržanih od strane klijenta.
4. Poslužitelj odgovara *server_hello_handshake* paketom koji sadrži TLS zapise: TLS certifikat, ključ poslužitelja, zahtjev za certifikatom, idr.
5. Poslužitelj nakon toga šalje zahtjev za certifikatom kako bi usporedio identitet partnera kojeg je primio u prvoj poruci (*Identity*) s identitetom sadržanim u certifikatu.
6. Klijent također šalje zahtjev za certifikatom, s istom svrhom.
7. Ako je postupak autentikacije uspješno završen autentikator šalje odgovor kojim završava komunikacija *handshake* porukama. Klijent tada šalje TLS paket bez podataka u polju *Data*, a EAP poslužitelj na to odgovara *Success* porukom. U slučaju neuspješne autentikacije, poslani odgovor sadrži i razloge zbog kojih autentikacija nije uspjela.

EAP-TLS paketi, u odnosu na osnovni EAP paket, sadrže i jedno dodatno polje. To je 8-bitno polje *Flags*, kojim se postavljaju zastavice (LMSRRRRR) i rezervirani bitovi (RRRRR), ovisno o tome je li u paketu uključeno polje *Length* (L), dodatni fragmenti (M), radi li se o EAP_Start paketu (S).

7.3. EAP-MD5

EAP-MD5 metoda omogućuje provjeru autentičnosti primljenih poruka pomoću 128-bitne *hash* vrijednosti dobivene MD5 algoritmom. Nedostaci ove metode su ranjivost MD5 jednosmjerne funkcije na tzv. rječničke napade (eng. *dictionary attack*) te nemogućnost uzajamne autentikacije. Naime, za razliku od ostalih EAP metoda, EAP-MD5 omogućuje samo autentikaciju klijenta poslužitelju, ali ne i obrnuto, što ju čini ranjivom na MITM (eng. *Man-In-The-Middle*) napade.

7.4. EAP-PSK

EAP-PSK (eng. *PreShared Key*) metoda temelji se na simetričnoj kriptografskoj metodi AES-128 (eng. *Advanced Encryption Standard*). PSK predstavlja 128-bitni ključ, kojeg znaju samo EAP poslužitelj i klijent, te služi za računanje AK (eng. *Authentification Key*) i KDK (eng. *Key Derivation Key*) ključeva. Iz KDK ključa se dalje računaju drugi potrebni ključevi. Uz PSK, metoda koristi i identifikacijske oznake poslužitelja (*ID_S*) i klijenta (*ID_P*). Autentikacija ovom metodom se zasniva na AKEP2 (eng. *Authentication Key Exchange Protocol*) protokolu.

U slučaju uspješne autentikacije EAP-PSK metoda stvara tzv. *PCHANNEL* zaštićeni komunikacijski kanal korištenjem EAX postupka kriptirane autentikacije. EAP-PSK autentikacija provodi se u četiri poruke:

1. Prvu poruku šalje poslužitelj. Ona, uz uobičajena polja EAP paketa, ima dva dodatna polja: *RAND_S* polje koje sadrži nasumičan broj i *ID_S* polje s identifikacijskom oznakom poslužitelja.
2. Drugu poruku šalje klijent, a njena dodatna polja su: *RAND_S* i *RAND_P* polja s nasumičnim brojevima, *MAC_P* polje s MAC adresom klijenta te *ID_P* polje s identifikacijskom oznakom klijenta.
3. Treću poruku šalje poslužitelj, a sadrži dodatna polja: *RAND_S*, *MAC_S* polje s MAC adresom poslužitelja te *PCHANNEL* polje. *PCHANNEL* polje se sastoji od polja:
   - *Nonce N* je 4-bitno polje s cjelobrojnom vrijednošću koja se inkrementira sa svakom EAP-PSK porukom unutar jednog autentikacijskog postupka,
   - *Tag* polje sadrži MAC (eng. *Message Authentication Code*) vrijednost čija namjena ja zaštita podatkovnog sadržaja poruke,
   - *zastavica R* kojom se označuje uspjeh, odnosno neuspjeh, autentikacije,
   - *zastavica E* kao oznaka dodatka (eng. *Extension*),
   - *Reserved* polje u kojem se prilikom slanja pišu nule, a po primitku se ignorira.
4. Četvrtu poruku šalje klijent. Ona sadrži RAND_S te PCHANNEL polja.

7.5. EAP-TTLS

EAP-TTLS (eng. *Tunnelled TLS*) metoda predstavlja nadogradnju EAP-TLS metode. Kod ove metode klijent se ne mora poslužitelju autenticirati pomoću certifikata potpisanog od strane CA (eng.

Certified Authority) ovlaštenog tijela, već je dovoljna takva autentikacija poslužitelja klijentu. Ovime se uvelike pojednostavljuje postavljanje sustava jer nije potrebno instalirati certifikat na pojedinim klijentima.
Nakon autentikacije poslužitelja on prema klijentu stvara sigurnu vezu, takozvani tunel, posredstvom koje se provodi autentikacija klijenta. Pri tome je moguće koristiti uobičajene autentikacijske protokole i infrastrukture jer tunel pruža zaštitu od prisluškivanja i MITM napada. Također, korisničko ime se šalje samo u kriptiranom obliku čime se osigurava zaštita privatnosti.

7.6. EAP-IKEv2

EAP-IKEv2 metoda temelji se na IKEv2 (eng. *Internet Key Exchange Protocol version 2*) te omogućuje uzajamnu autentikaciju EAP klijenta i poslužitelja te uspostavljanje sjedničkih ključeva. Metoda podržava autentikacijske tehnike temeljene na sljedećim tipovima vjerodostojnica:

- asimetrični par ključeva - javni ključ ugrađen u digitalni certifikat i odgovarajući privatni ključ koji je poznat samo vlasniku,
- zaporke - znakovni nizovi niske entropije poznati klijentu i poslužitelju,
- simetrični ključevi - znakovni nizovi visoke entropije poznati klijentu i poslužitelju.

Moguće je korištenje različitih autentikacijskih vjerodajnica, a prema tome i različitih tehnika, za pojedini smjer autentikacije. Na primjer, moguća je autentikacija EAP poslužitelja pomoću asimetričnog para ključeva dok se klijent autenticira pomoću simetričnih ključeva. Dozvoljene kombinacije navedene su u tablici

EAP poslužitelj	EAP klijent
asimetrični par ključeva	asimetrični par ključeva
asimetrični par ključeva	simetrični par ključeva
asimetrični par ključeva	zaporka
simetrični par ključeva	simetrični par ključeva

Tablica 3: Kombinacije autentikacijskih vjerodajnica podržane od strane EAP-IKEv2 metode

7.7. PEAP

PEAP (eng. *Protected EAP*) je EAP metoda slična EAP-TTLS metodi, a primjenjuje se kod bežičnih mreža. Ova metoda je podijeljena u dvije faze. U prvoj fazi autentikacije uspostavlja se sigurnosni tunel između autentikatora i poslužitelja, korištenjem EAP-TLS za autentikaciju poslužitelja dok se u drugoj fazi autenticira klijent, koristeći bilo koju EAP metodu.
U prvoj fazi EAP poslužitelj se autenticira korištenjem odgovarajućeg certifikata. Zatim klijent uspostavlja vezu s autentikatorom, a autentikator uspostavlja sigurnosni kanal prema poslužitelju. Nakon toga slijede uobičajene EAP *Request/Response* poruke između klijenta i autentikatora te autentikatora i poslužitelja, poslije kojih se provodi razmjena EAP-TLS poruka. S krajem EAP-TLS metode uspostavljen je sigurnosni kanal te završava prva faza autentikacije.
Druga faza započinje razmjenom *Identity* poruka, a zatim slijedi autentikacija klijenta nekom od EAP metoda. Autentikacija se odvija sigurnosnim kanalom uspostavljenim u prvoj PEAP fazi. Nakon toga klijent i poslužitelj računaju ključeve te ih šalju autentikatoru, kao i rezultate autentikacije. Time se završava autentikacija: klijent i pristupna točka mogu sigurno razmjenjivati poruke.

8. Sigurnosne prijetnje

Zlonamjerni korisnik s pristupom komunikacijskom kanalu preko kojega se provodi EAP autentikacija može pokušati izvesti niz napada:

- Prisluškivanjem autentikacijskog postupka napadač može pokušati otkriti identitet korisnika.
- Napadač može pokušati izmijeniti ili krivotvoriti EAP pakete.
- Zlonamjerankorisnik može pokušati izvesti napad uskraćivanja usluga (eng. *Denial of Service - DoS*) stvaranjem posebno oblikovanih EAP paketa.
- Moguće je razotkriti korisničku zaporku izvođenjem rječničkog napada.
- Klijenta je moguće navesti na povezivanje na nesigurnu mrežu izvođenjem MITM napada.

- Napadač može ometanjem postupka autentikacije postići odabir nesigurnije EAP metode.
- Zlonamjeran korisnik može pokušati steći kriptografske ključeve iskorištavanjem slabosti algoritama za njihovo računanje.
- Napadač može igrati ulogu autentikatora te EAP klijentu i/ili poslužitelju slati neispravne podatke.

8.1. Zaštita identiteta

Obavještavanje o identitetu korisnika kod EAP protokola moguće je potpuno izostaviti ili koristiti neku od tehnika karakterističnih za pojedine EAP metode, a koje se provode nakon uspostavljanja sigurnog komunikacijskog kanala.
U slučaju zaštite identiteta klijenta, moguća je razlika identiteta iznesenog u prvotnom *Identity* odgovoru u odnosu na autenticirani identitet. Pri tome EAP protokol u daljnjem radu kao ispravan koristi autenticirani identitet.

8.2. MITM napadi

Ako se EAP protokol tunelira nekim drugim protokolom, koji ne zahtjeva autentikaciju, postoji mogućnost pojave ranjivosti na MITM napade. Napadač kod takvog napada tunelira EAP pakete vjerodostojnog EAP klijenta preko svog računala prema autentikatoru i tako neovlašteno stječe pristup ranjivoj mreži.
MITM napade moguće je spriječiti:

- zahtijevanjem obostrane autentikacije unutar mehanizma za tuneliranje,
- zahtijevanjem kriptografskog povezivanja tunelirajućeg protokola i EAP metode koju se tunelira,
- ograničavanjem korištenja nezaštićenih EAP metoda,
- izbjegavanjem korištenja tuneliranja ako je dostupna sigurna EAP metoda.

8.3. Izmjena EAP paketa

Na EAP sloju nije podržana provjera porijekla pojedinih paketa, njihova integriteta niti zaštita od ponovnog slanja, iako je takve zaštite moguće implementirati unutar EAP metoda. Zbog toga je moguće umetanje poruka u postupak EAP autentikacije te mijenjanje zaglavlja izvornih paketa, ukoliko korištena metoda ne pruža njihovu zaštitu.
Kako bi se onemogućile zlonamjerne manipulacije paketima preporučeno je implementirati zaštićeno usuglašavanje korištene kriptografske metode, obostranu autentikaciju, korištenje kriptografskih ključeva, zaštitu integriteta paketa te zaštitu od ponovnog slanja paketa.

8.4. Rječnički napadi

Autentikacijski algoritmi zaštićeni zaporkama, kao što su EAP-MD5, MS-CHAPv1 i Kerberos V ranjivi su na rječničke napade. Ranjive metode moguće je dodatno zaštititi tuneliranjem, ali tako se uvodi ranjivost na MITM napade pa je preporučeno korištenje EAP metoda koje nisu ranjive na rječničke napade.

8.5. Povezivanje na nesigurnu mrežu

Kod metoda koje podržavaju samo jednosmjernu autentikaciju, kao što je EAP-MD5 metoda, autentikator se ne autenticira klijentu. Zlonamjeran korisnik može takve sustave napasti stvaranjem zlonamjerno oblikovanog autentikatora pomoću kojega može klijente navesti na spajanje na nesigurnu mrežu pa se savjetuje korištenje metoda koje podržavaju obostranu autentikaciju.

9. Zaključak

EAP protokol omogućuje autentikaciju korištenjem neke od brojnih podržanih EAP metoda. Svaka od tih metoda je posebna, po formatu paketa koji se u procesu autentikacije razmjenjuju, ali i po samom načinu provođenja autentikacije. Upravo raznolikost EAP metoda te mogućnost proširivanja protokola novim metodama čine glavne prednosti ovog protokola. Također, EAP protokol od pristupnih točaka i usmjerivača ne zahtjeva podržavanje svih EAP metoda, već oni mogu poslužiti kao posrednici u komunikaciji klijenta i autentikacijskog poslužitelja. Spomenuti poslužitelj pri tome podržava dostupne EAP metode i na njemu se provodi proces autentikacije.

Različite autentikacijske metode donose i različite ranjivosti, pa su tako mogući napadi na EAP protokol koji rezultiraju otkrivanjem identiteta korisnika, uskraćivanjem usluga, izmjenama EAP podatkovnih paketa, otkrivanjem potencijalno osjetljivih informacija, zavaravanjem klijenta i njegovim navođenjem na povezivanje na nesigurnu mrežu. Ipak, pažljivim odabirom odgovarajuće EAP metode moguće je u bitnom umanjiti rizik uspješne zlouporabe postojećih ranjivosti, a za specifične i posebno osjetljive primjene uvijek je moguće stvoriti potpuno novu autentikacijsku metodu.

10. Reference

[1] *Extensible Authentication Protocol*, http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol, siječanj 2008.

[2] AAA protocol, http://en.wikipedia.org/wiki/AAA_protocol, siječanj 2008.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlso, H. Levkowetz: *Extensible Authentication Protocol (EAP)*, http://tools.ietf.org/html/rfc3748, siječanj 2007.

[4] Extensible Authentication Protocol Overview, https://thesource.ofallevil.com/technet/network/eap/eap.mspx, siječanj 2008.

[5] Wireless Deployment Technology and Component Overview, http://technet.microsoft.com/en-us/library/bb457015.aspx#EEAA, siječanj 2008.