Zagotavljanje varnosti v lokalnih omrežjih

Grega Modrijan
Fakulteta za elektrotehniko, Univerza v Ljubljani

Ključne besede:

802.1x, NAC, NAP, RADIUS, EAP, PEAP, TLS, MSCHAPv2, OTP, overjanje, odjemalec (supplicant), overitelj, avtentikacijski strežnik, avtorizacija, obračunavanje, certifikat, LAN, WLAN, VLAN.

Termini

communication security (COMSEC) - komunikacijska varnost
computer security (COMPUSEC) - računalniška varnost
information security - informacijska varnost
network security - varnost omrežja
network security architecture - varnostna arhitektura omrežja
network security management - upravljanje varnosti omrežja
network admission control (NAC) - krmiljenje dostopa do omrežja
safety – netveganost
threat – grožnja
vulnerability – ranljivost
supplicant – odjemalec
extensible authentication protocol over LAN (EAPOL) - razširljivi overilni protokol v omrežju LAN
tunneled transport layer security (TTLS) -varnost tuneliranega transportnega sloja
mutual authentication - medsebojna overitev
publickey infrastructure (PKI) - infrastruktura javnih ključev
dictionary attack - napad z uporabo slovarja
public key infrastructure (PKI) - infrastruktura javnih ključev
rogue access point - sleparska dostopovna točka

1 Povzetek

V dokumentu so opisani mehanizmi, ki pripomorejo k večji varnosti v lokalnih ethernet omrežjih. Poudarek je na overjanju uporabnikov in naprav v lokalnem ethernet omrežju ter krmiljenju dostopa do omrežja (NAC[1]). Opisane so tehnologije 802.1x, EAP, NAC in NAP[2], ki zagotavljajo na ravni vrat zasnovan avtoriziran dostop uporabnikov in naprav v lokalno ethernet omrežje.
Rešitev zagotavljanja varnosti v lokalnih ethernet omrežjih sestavljajo: odjemalec (angl. supplicant), t.j. ustrezna programska oprema nameščena na uporabnikovem računalniku, overitelj (stikalo, usmerjevalnik ali brezžična dostopovna točka) in avtentikacijski strežnik (AAA/RADIUS). Avtentikacijski strežnik poleg overjanja omogoča še avtorizacijo in obračunavanje. Overjanje poteka po protokolu EAP, ki zagotavlja podporo različnim metodam overjanja. Protokol 802.1x je namenjen transportu EAP avtentikacijskih sporočil preko medija IEEE 802 (ethernet, brezžični ethernet) med odjemalcem in overiteljem, RADIUS pa poskrbi za prenos EAP avtentikacijskih sporočil med overiteljem in avtentikacijskim strežnikom. Sam proces overjanja poteka med odjemalcem in avtentikacijskim strežnikom, overitelj je pri tem le posrednik pri izmenjavi EAP avtentikacijskih sporočil.
Podane so zahteve strojne in programske opreme pri izvedbi rešitve 8021x/EAP in NAC. Prikazane so omejitve in težave, ki pri tem nastopajo.

2 Uvod

Zagotavljanje ustrezne varnosti omrežja ni več v domeni zgolj velikih podjetij in organizacij, temveč se z rizikom pomankljive varnosti omrežja soočajo tudi manjša podjetja in nenazadnje rezidenčni uporabniki. V preteklosti je bila varnost omrežja pojmovana zgolj kot požarna pregrada, ki je varovala notranje omrežje (LAN) pred vdori iz zunanjega omrežja (WAN). Z vedno bolj kompleksnejšim povezovanjem informacijskih sistemov in vedno večjo odvisnostjo poslovanja podjetij in organizacij od informacijske infrastrukture, je zagotavljanje varnosti omrežja prešlo izpod okrilja posamezne požarne pregrade. Prav tako je pomembno poudariti, da predstavlja varnost omrežja le del v zagotavljanju celovite varnosti informacijskega sistema.

3 Varnost omrežja

V mnogih pogledih je varnost informacijskega sistema (angl. Information security) ugotavljanje ter nadzorovanje groženj in ranljivosti informacijskega sistema nekega podjetja ali organizacije. Varnost informacijskega sistema sama po sebi ne zagotavlja netveganosti pred nepooblaščenim razkritjem informacij ali uporabo informacijskega sistema neke organizacije oziroma podjetja. Prav tako varnost informacijskega sistema ne more zagotoviti zaščite informacij. Torej kaj točno pojmujemo pod varnost informacijskega sistema? Pri varnosti informacijskega sistema gre predvsem za

[1] NAC – Network Admission Control (krmiljenje dostopa do omrežja)
[2] NAP - Network Access Protection

vzpostavitev nekih preventivnih korakov, ki pripomorejo k varovanju informacij in zakrivanju zmožnosti/ranljivosti informacijskega sistema pred grožnjami [1].
Z dobo interneta je povezovanje informacijskih sistemov preko telekomunikacijskih omrežij postala stalnica. Prav slednje pa narekuje slojevit pristop k zagotavljanju varnosti informacijskih sistemov in obsega praktično vse nivoje OSI referenčnega modela. Tako lahko govorimo o zagotavljanju fizične varnosti, komunikacijske varnosti (COMSEC), varnosti omrežja in računalniške varnosti (COMPUSEC).

V notranjem omrežju tipično ne uporabljamo nikakršnih varnostnih mehanizmov. Glavni razlog je najti v tem, da notranje omrežje smatramo kot varno in ga zato ni potrebno zaščititi. Vedno bolj pa vemo, da to ni res. Prepričanje, da nevarnosti lokalnega omrežja prežijo zgolj zunaj omrežja (internet) je zmotno. Ravno zlorabe omrežja od »znotraj« so najpogostejši način izvajanja napadov. Kako pa lahko sploh nekdo to naredi? Na žalost v mnogih primerih zelo enostavno. Glavni vzrok oz. načini so naslednji.

- Zlorabo lahko povzroči nezadovoljni ali pa nelojalni zaposleni, ki ima določene pravice v sistemu.
- Zaradi napačno postavljenih varnostnih sistemov lahko pridemo v notranje omrežje mimo obstoječih varnostnih sistemov (npr. klicni usmerjevalniki, povezave z oddaljenimi lokacijami ipd.).
- Slaba fizična varnost prostorov omogoča nepooblaščen fizičen dostop do notranjega omrežja.

Kaj torej lahko naredimo? Postavimo lahko varnostni sistem tudi v notranje omrežje. Katerega pa? Mogoče požarno pregrado, ali pa implementacija določenih filtrirnih mehanizmov na aktivni opremi lokalnega omrežja. Vsekakor takšni varnostni mehanizmi v notranjosti omrežja pripomorejo k večji varnosti. Praviloma pa osnovnega problema ne rešijo. Požarne pregrade in filtrirni mehanizmi praviloma delujejo do 4. nivoja OSI referenčnega modela. Lahko torej le onemogočijo uporabo določenih aplikacij, ne morejo pa dostope do sicer dovoljenih aplikacij vsebinsko nadzorovati. In prav to bi v notranjosti omrežja potrebovali. Uporabniki, ki se nahajajo v notranjem omrežju praviloma potrebujejo dostop do pomembnih aplikacij, tega niti ne želimo, niti ne moremo preprečiti. Radi pa bi dosegli nadzor nad uporabo teh aplikacij, ki ga požarne pregrade torej ne morejo nuditi.

Arhitektura večine današnjih žičnih lokalnih omrežij (LAN) omogoča priključitev in dodelitev notranjih virov informacijskega sistema uporabnikom brez predhodnega overjanja le-teh. Vzrok temu je najti v prepričanju, da je prenosni medij v žičnih lokalnih omrežjih zaseben in da lahko do tega dostopajo samo zaupanja vredni uporabniki. Taka arhitektura omrežja zagotavlja posledično vsakomur, ki se lahko fizično priključi na LAN stikalo dostop do notranjih virov informacijskega sistema.
Danes se vedno pogosteje srečujemo z brezžičnimi lokalnimi omrežji (WLAN). Z varnostnega vidika morajo biti brezžična lokalna omrežja deležna dodatne pozornosti. Pri brezžičnih lokalnih omrežjih prenosni medij ni zaseben. Za razliko od žičnih lokalnih omrežij, kjer mora uporabnik imeti fizičen dostop do omrežnega priključka na LAN stikalu, se lahko uporabnik v brezžično lokalno omrežje zaradi same narave radijskih signalov, povezuje iz drugega prostora ali celo stavbe preko ulice. Tako se lahko praktično vsakdo, ki se nahaja v območju dosega radijskega signala brezžične dostopovne točke, z dovolj usmerjeno anteno ter občutljivim radijskim sprejemnikom poveže v brezžično lokalno omrežje. Zaradi tega je v

brezžičnih lokalnih omrežjih poleg samega overjanja potrebno zagotoviti tudi šifriranje in celovitost podatkov.

Brezpogojno spoštovanje varnostne politike in nadzor nad priključitvijo in uporabo virov informacijskega sistema je zato kritičnega pomena. Kakršnokoli odstopanje od tega predstavlja velik rizik za podjetje, organizacijo.

Vse zgoraj našteto je vplivalo na nastanek nove arhitekture lokalnih omrežij, ki zagotavlja predhodno overjanje uporabnikov in naprav v lokalnem omrežju. Tehnologije 802.1X, EAP, NAP, NAC in AAA/RADIUS so sestavni elementi novodobnih lokalnih omrežij.
.

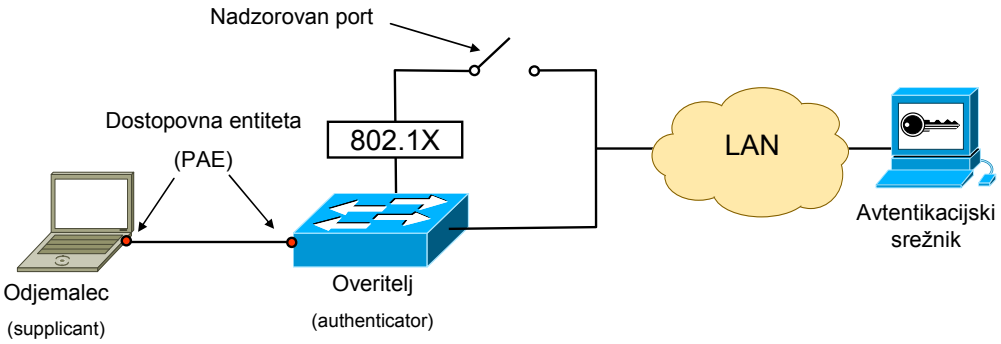
Tako je zelo pomembno zagotoviti zaščito pred vdori v notranje omrežje neke organizacije, po drugi strani pa notranjim uporabnikom, glede na pravice, ko jih imajo omogočiti dostop le do tistih virov informacijskega sistema, ki jih za delovanje potrebujejo in prav nič več kot to.

4 Mehanizmi overjanja v lokalnih ethernet omrežjih

4.1 IEEE 802.1X

IEEE 802.1X je protokol 2. plasti OSI referenčnega modela in določa nadzorovan dostop do omrežja zasnovan na ravni vrat. Dejanska uveljavitev protokola 802.1X je bila dosežena z nadzorovanim dostopom do omrežja na ravni vrat, ki temelji na mehanizmu nadzorovanega porta ter na filtriranju MAC naslovov.
Poudariti je potrebno, da sam protokol 802.1X ne zagotavlja overjanja. Overjanje uporabnikov in naprav se izvaja s protokolom EAP. Protokol 802.1X pri tem poskrbi za prenos EAP avtentikacijskih sporočil med odjemalcem in overiteljem v omrežjih IEEE 802 (ethernet, brezžični ethernet, obroč z žetonom itd.). Tako moramo na protokola 802.1X in EAP gledati kot celoto, saj se med seboj dopolnjujeta. Standard IEEE 802.1X določa naslednje gradnike:

- dostopovno entiteto PAE[3]
- overitelja (authenticator)
- odjemalca (supplicant)
- avtentikacijski strežnik
- nadzorovan/nenadzorovan port



Slika 4-1: Gradniki protokola IEEE 802.1x

Dostopovna entiteta *(PAE)* je logična entiteta protokola 802.1X na overitelju in odjemalcu. Nanaša se na posamezen LAN port.

Overitelj (Authenticator) je LAN port, ki uporabnikom in napravam, ki želijo dostopati do omrežnih resursov preko tega porta vsiljuje predhodno overjanje. V brezžičnem ethernet omrežju je overitelj logičen LAN port na 802.1X brezžični dostopovni točki, v žičnem ethernet omrežju pa je to fizičen port na 802.1X podprtem stikalu.

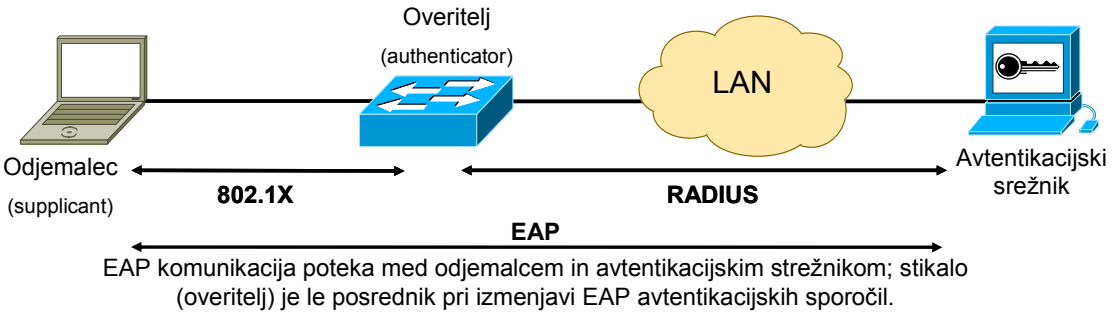
[3] PAE – Port Access Entity

Odjemalec (supplicant) je logičen LAN port na omrežni kartici, ki zahteva dostop do storitev dostopnih preko overitelja. Glede na način povezave (brezžična ali žična) sta odjemalec in overitelj med seboj povezana z logičnim ali fizičnim točka-točka LAN segmentom.

Avtentikacijski strežnik overja poverilnice odjemalca, ki jih posreduje overitelj in nato odgovori overitelju ali ima odjemalec pooblastilo za dostop do overiteljskih storitev. Avtentikacijski strežnik se lahko nahaja na samem overitelju (brezžična dostopovna točka, stikalo) ali pa je ločena enota (samostojni AAA/RADIUS avtentikacijski strežnik). V slednjem primeru overitelj posreduje odjemalčevo zahtevo po overjanju do avtentikacijskega strežnika.

Nadzorovan/nenadzorovan port: na vsakem 802.1X portu overitelja ustvari overitelj dve navidezni vstopni točki – nadzorovan in nenadzorovan port. Nenadzorovan port zagotavlja prenos le EAPOL okvirjev. Prenos ostalega prometa med overiteljem in ostalimi napravami v lokalnem omrežju preko nenadzorovanega porta ni mogoč. Nadzorovan port omogoča prenos podatkov med odjemalcem in LAN omrežjem le, če je odjemalec pooblaščen (avtoriziran) za dostop v LAN omrežje.
Pred overjanjem je navidezno stikalo odprto in noben okvir se ne prenaša med odjemalcem in LAN omrežjem. Po uspešni overitvi odjemalca se navidezno stikalo sklene in prenos okvirjev med odjemalcem in LAN omrežjem se prične.

Overitelj je zgolj posrednik v komunikaciji med odjemalcem in avtentikacijskim strežnikom, saj EAP avtentikacijskih sporočil ne interpretira ampak le posreduje do njiju. Prenos EAP avtentikacijskih sporočil preko omrežij IEEE 802 med odjemalcem in overiteljem zagotavlja protokol 802.1X. IEEE 802.1X določa standardizirano metodo ovijanja EAP avtentikacijskih sporočil v ethernet okvirje- EAPOL[4]. Prenos EAP avtentikacijskih sporočil med overiteljem in avtentikacijskim strežnikom (RADIUS[5]) poteka preko protokola RADIUS (RFC 3579).



Slika 4-2: EAP komunikacija med odjemalcem in avtentikacijskim strežnikom

[4] EAPOL – EAP Over LAN
[5] RADIUS - Remote Authentication Dial-In User Service - uporabniška storitev z oddaljeno overitvijo

EAP avtentikacijska sporočila se prenašajo med odjemalcem in overiteljem v obliki koristne vsebine okvirja 802.1X.

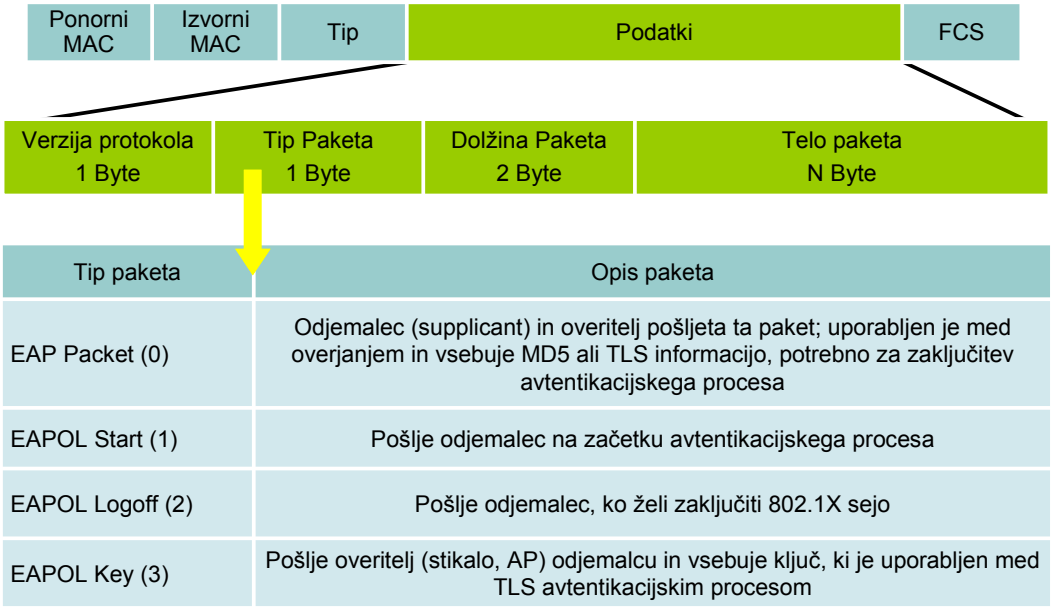
Slika 4-3: Prenos EAP avtentikacijskih sporočil v okvirju 802.1X - EAPOL

RADIUS protokolna sporočila lahko poleg EAP koristne vsebine prenašajo tudi parametre politike dostopa v obliki atributov - A V (RFC 3580).

Slika 4-4: RADIUS format sporočila definiran v RFC 3579 in RFC 3580

Standard 802.1X definira naslednje tipe EAPOL okvirjev:

- EAP-Packet
- EAPOL-Start
- EAPOL-Logoff
- EAPOL-Key



Tip paketa	Opis paketa
EAP Packet (0)	Odjemalec (supplicant) in overitelj pošljeta ta paket; uporabljen je med overjanjem in vsebuje MD5 ali TLS informacijo, potrebno za zaključitev avtentikacijskega procesa
EAPOL Start (1)	Pošlje odjemalec na začetku avtentikacijskega procesa
EAPOL Logoff (2)	Pošlje odjemalec, ko želi zaključiti 802.1X sejo
EAPOL Key (3)	Pošlje overitelj (stikalo, AP) odjemalcu in vsebuje ključ, ki je uporabljen med TLS avtentikacijskim procesom

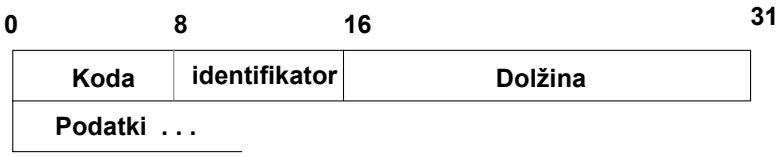
Slika 4-5: Format EAPOL okvirja

4.2 EAP – razširljivi avtentikacijski protokol

Extensible Authentication Protocol (EAP) je standardiziran razširljiv avtentikacijski protokol, ki je bil sprva namenjen razširjenemu overjanju v protokolu PPP[6]. Ob vedno večji potrebi po overjanju naprav in uporabnikov v lokalnih ethernet omrežjih je EAP bil izbran za avtentikacijski mehanizem protokola 802.1X. Vzrok temu se skriva v njegovi prožnosti, ki se kaže v prenosu poljubnih avtentikacijskih informacij. EAP tako ni omejen zgolj na današnje metode overjanja (gesla, certifikati, žetonske kartice, biomtrika itd.) ampak se lahko zlahka prilagodi prihodnjim potrebam.
EAP protokol se ovija v spodaj ležeče protokole: PPP, 802.1X, RADIUS.
Ločimo naslednje tipe EAP avtentikacijskih sporočil: Identity, Notification, Nak, MD5-Challenge, One-Time Password in Generic Token Card.

EAP avtentikacijsko sporočilo sestavljajo naslednja polja :

- Koda: *Request, Response, Exchange, Success, Failure*
- Identifikator: namenjen razločevanju med odgovori (responses) posameznih zahtev (requests)
- Podatki: format podatkovnega polja določa koda EAP sporočila



Slika 4-6: Format EAP sporočila

Sam protokol EAP zagotavlja le standardiziran format za prenos EAP avtentikacijskih sporočil. Pri razširjenem avtentikacijskem protokolu EAP je zato potrebno izbrati tudi metodo EAP overjanja. EAP metode overjanja lahko zaobjamemo v naslednje skupine:

- **Metode overjanja na podlagi »pozivov-odzivov« (challenge-response):**
  - *EAP-MD5*[7]: metoda overjanja na podlagi MD5 šifriranih pozivov-odzivov (challenge-response)
  - *LEAP*[8]: metoda overjanja na podlagi uporabniških imen in gesel
  - *EAP-MSCHAPv2*[9]: metoda overjanja na podlagi uporabniških imen in gesel

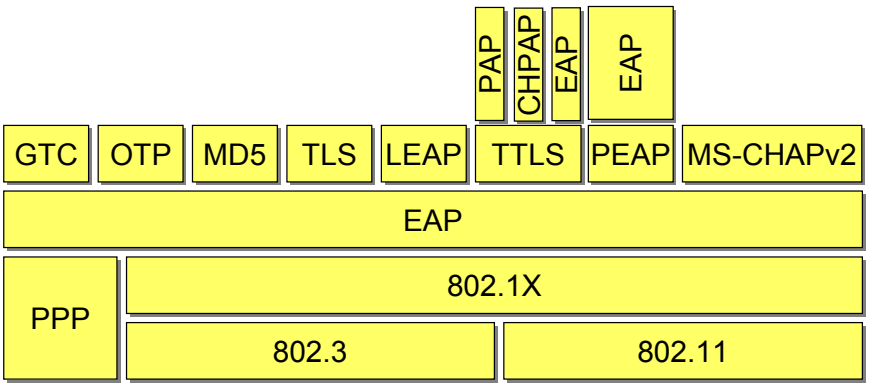
- **Metode overjanja na podlagi digitalnih certifikatov:**
  - *EAP-TLS*[10]: metoda overjanja z digitalnimi certifikati; metoda uporablja x.509v3 certifikate in TLS mehanizem za overjanje

[6] PPP – Point-to-Point Protocol: protokol točka-točka
[7] EAP-MD5: EAP-Message Digest5
[8] LEAP: Lightweight Extensible Authentication Protocol
[9] EAP-MSCHAPv2: EAP-Microsoft Challenge Handshake Authentication Protocolv2
[10] EAP- TLS: EAP-Transport Layer Security

- **Metode tuneliranja EAP avtentikacijskih sporočil:**
  - *PEAP*[11]: zaščiten EAP; prenaša EAP avtentikacijska sporočila različnih EAP metod znotraj šifriranega tunela; ena izmed priljubljenih različic EAP je PEAP/EAP-MSCHAPv2
  - *EAP-TTLS*[12]: zagotavlja izvedbo drugih EAP metod overjanja znotraj šifriranega tunela EAP-TLS

- **Druge metode:**
  - *EAP-OTP*[13]: metoda overjanja na podlagi enkratnih gesel
  - *EAP-GTC*[14]: metoda overjanja na podlagi žetonskih kartic

Standardizirane so tri metode EAP overjanja:
- EAP-MD5 - MD5 kodirana uporabniška imena/gesla
- EAP-OTP - uporablja enkratna gesla
- EAP-TLS - temelji na močnih kriptografskih mehanizmih z overjanjem s certifikati

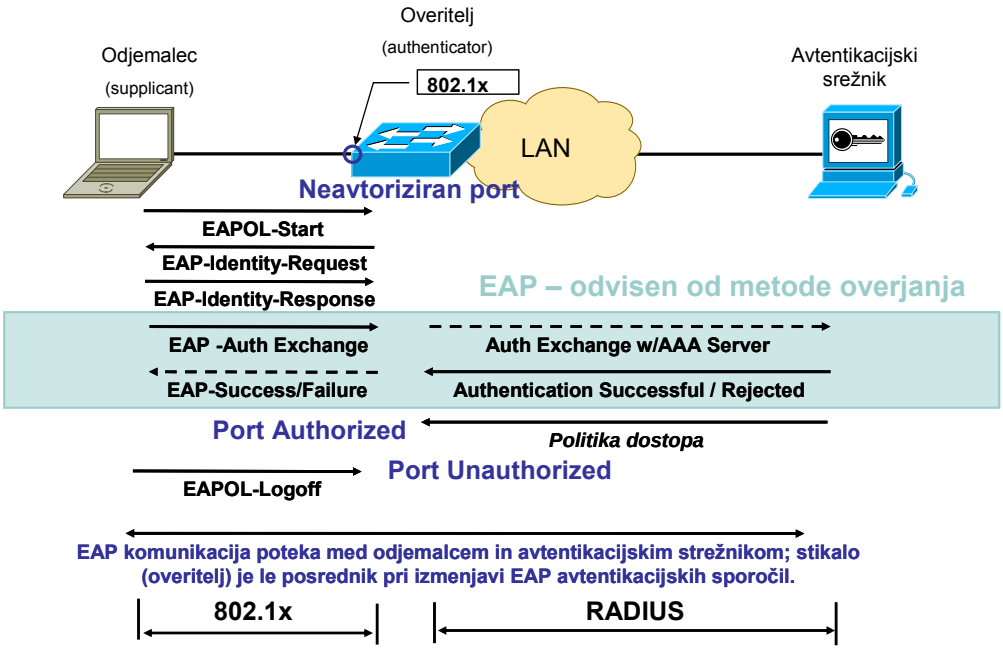


Slika 4-7: Metode EAP overjanja

Bistvena odlika protokola EAP je prav njegova prožnost, ki zagotavlja podporo raznolikim metodam overjanja in možnost uporabe prihodnjih metod. Danes je zaradi svoje relativno preproste izvedbe in močne zaščite priljubljena metoda overjanja PEAP/EAP-MSCHAPv2.

Za razliko od protokola PPP, kjer se metoda overjanja (PAP ali CHAP) določi v fazi vzpostavitve povezave, se v primeru EAP izbere metodo overjanja v fazi avtentikacije. Pogajanje za EAP metodo overjanja poteka med končnima entitetama v EAP procesu overjanja – med odjemalcem in avtentikacijskim strežnikom. Potem, ko je dogovorjena EAP metoda overjanja, se med odjemalcem in avtentikacijskim strežnikom odpre komunikacijski kanal preko katerega si izmenjujeta EAP avtentikacijska sporočila. Dolžina in vsebina EAP komunikacije je odvisna od izbrane EAP metode overjanja.

[11] PEAP: Protected Lightweight Extensible Authentication Protocol
[12] EAP-TTLS: EAP- Tunneled Transport Layer Security;
[13] EAP-OTP: EAP- One Time Password
[14] EAP-GTP: EAP- Generic Token Card



Slika 4-8: Izmenjava EAP sporočil v procesu overjanja

4.2.1 EAP-MD5

EAP-MD5 je avtentikacijska metoda, ki temelji na geslih. V brezžičnih omrežjih ta metoda ni zaželena zaradi odkritih varnostnih pomanjkljivosti. To metodo uspešno zamenjuje metoda overjanja PEAP-MSCHAPv2.

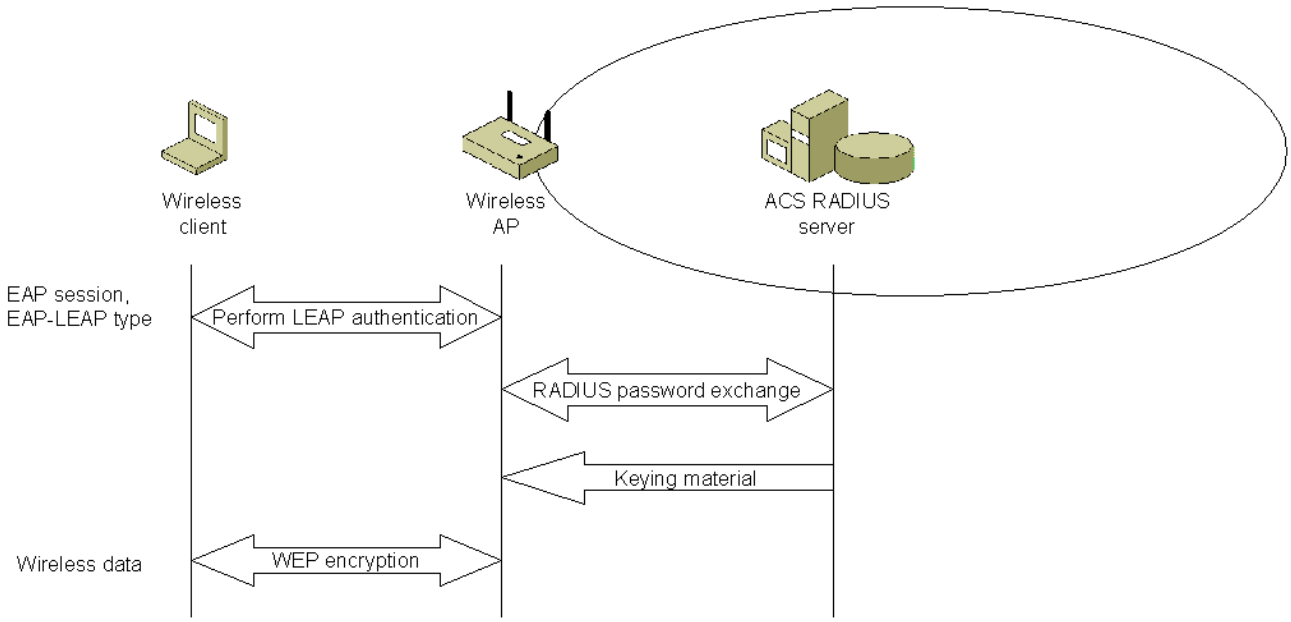
Bistveni pomanjkljivosti metode EAP-MD5 sta naslednji:

- overjanje na podlagi gesel; ker overjanje poteka preko nešifriranega kanala je ta metoda ranljiva na napade z uporabo slovarja (dictionary attack),
- ne zagotavlja medsebojne overitve (mutal authentication), kar pomeni, da se lahko odjemalec poveže v sleparsko omrežje (rogue network).

4.2.2 LEAP

V pomanjkanju primernih standardiziranih pristopov, ki bi olajšali težave v zvezi z varnostjo v omrežjih 802.11, je Cisco predstavil LEAP (Lightweight Extended Authentication Protocol). LEAP ne podpira TLS sheme. Namesto tega ponuja močno avtentikacijo (močnejšo od EAP-MD5), vendar ji še vedno primanjkuje TLS podpora za zaščito med koncema. To pomeni, da so avtentikacijske poverilnice podvržene napadom z uporabo slovarja. Poleg tega LEAP odjemalec ne overi avtentikacijskega strežnika, kar ima lahko za posledico prijavljanje na sleparko brezžično dostopovno točko oz. sleparsko omrežje.

Na spodnji sliki je prikazan primer LEAP avtentikacije v brezžičnih omrežjih. V prvi fazi se izvede avtentikacija, ki ji sledi druga faza v kateri se izmenja šifrirni material za generiranje šifrirnih ključev.



Slika 4-9: LEAP avtentikacijska metoda

Avtentikacijska metoda LEAP ni standardizirana, kar je ena njenih večjih pomanjkljivosti. Njeno delovanje je podprto večinoma le v produktih proizvajalca Cisco.

4.2.3 EAP-TLS

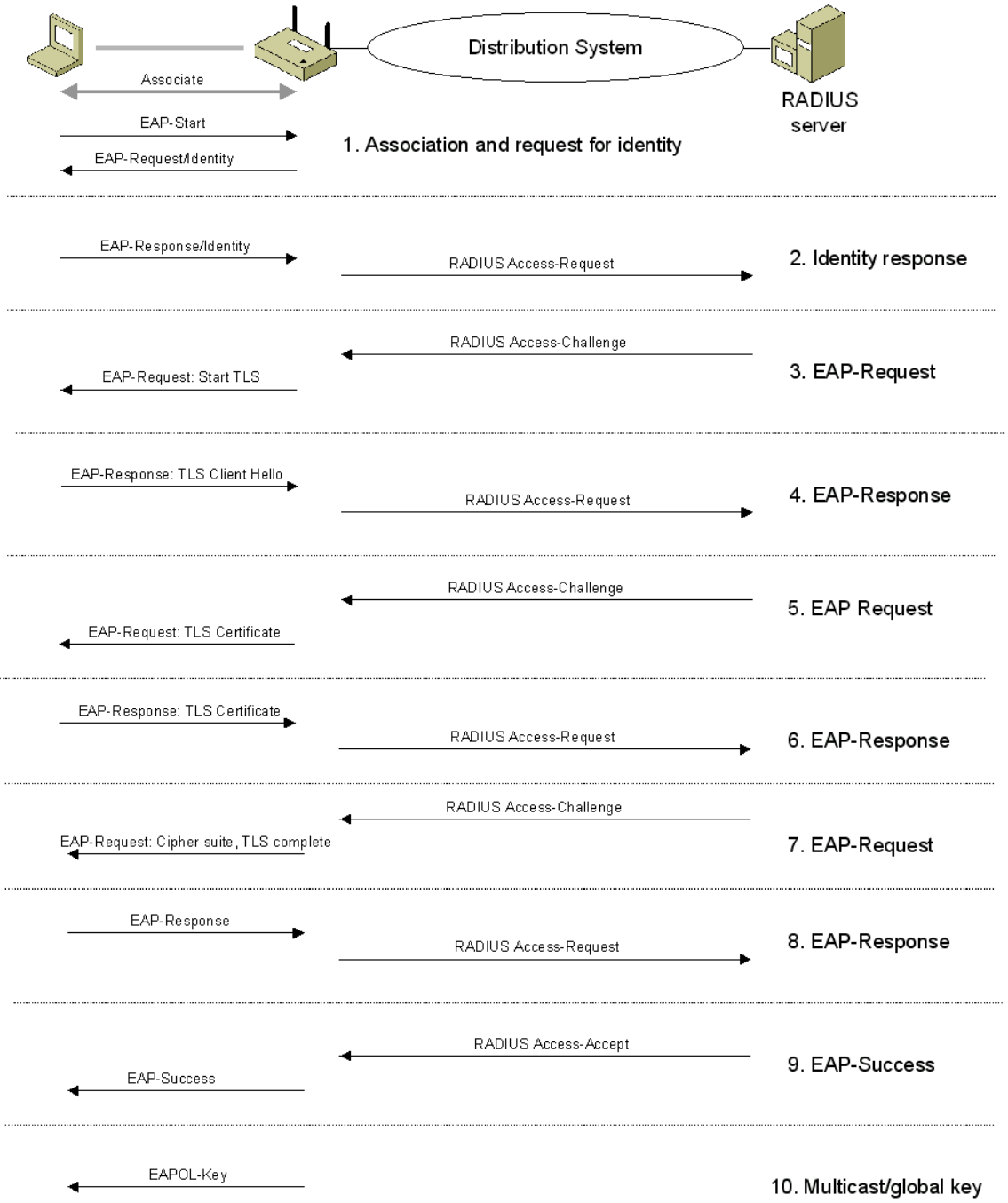
Metoda overjanja EAP-TLS temelji na overjanju z digitalnimi certifikati. Izmenjava avtentikacijskih sporočil na podlagi protokola EAP-TLS zagotavlja medsebojno overjanje (mutual authentication), celovitost prenesenih sporočil in varno izmenjavo zasebnih ključev. EAP-TLS omogoča najmočnejšo metodo overjanja. Protokol je opisan v dokumentu RFC 2716.

V praksi se najpogosteje uporablja različico protokola EAP-TLS, ki za overjanje uporablja uporabniške in računalniške digitalne certifikate shranjene v registru računalnika (registry-based). Prednosti takega načina overjanja so naslednje:

- izognemo se vpisovanju uporabniških gesel,
- overjanje uporabnikov in naprav poteka avtomatično in je praktično nevidno za uporabnike,

- uporaba digitalnih certifikatov velja za trenutno izredno močno avtentikacijsko shemo,
- EAP-TLS temelji na kriptografiji javnega ključa in ni ranljiv na napade z uporabo slovarja (dictionary attacks),
- V EAP-TLS avtentikacijskem procesu se medsebojno določi potreben material za generiranje ključev potrebnih za šifriranje podatkov in digitalno podpisovanje.

Postopek overjanja pri protokolu 802.1xEAP-TLS je opisan v nadaljevanju.



Slika 4-10: Avtentikacijski proces 802.1x:EAP-TLS

1. **asociacija in zahteva po identifikaciji**

Kadar se odjemalec (računalnik, IP telefon ipd.) povezuje v omrežje preko stikala (žično), prične s postopkom overjanja stikalo samo. Postopek prične s predhodnim pošiljanjem paketa »EAP-Request/Identity« odjemalcu. Ta paket vsebuje zahtevo za identifikacijo odjemalca.
Začetek overjanja pa se malo razlikuje v primeru, ko se odjemalec priključuje preko brezžične dostopovne točke. V kolikor je odjemalec že asociran z brezžično dostopovno točko (povezan preko radijskega medija), prične proces overjanja uporabnik sam s pošiljanjem paketa »EAP-Start« brezžični dostopovni točki.

2. **EAP-Response/Identy**

V kolikor na odjemalca ni prijavljen noben uporabnik, odjemalec pošlje paket »EAP Response/Identity«, v katerem je vsebovana identiteta same fizične naprave (računalnika) preko katere se uporabnik povezuje v omrežje.

3. **RADIUS pošlje »EAP-Request« (pričetek TLS komunikacije)**

RADIUS strežnik pošlje RADIUS sporočilo »Access-challenge«, ki vsebuje avtentikacijsko sporočilo »RADIUS EAP-Request« s tipom EAP (EAP-Type) nastavljenim na EAP-TLS. To sporočilo aktivira avtentikacijski proces TLS.

4. **Odjemalec pošlje »EAP-Response« (TLS Client Hello)**

Odjemalec odda sporočilo »EAP-Response« s tipom EAP nastavljenim na EAP-TLS. To sporočilo je odjemalčev pozdrav avtentikacijskemu strežniku. Overitelj (stikalo, brezžična dostopovna točka) posreduje EAP sporočilo do RADIUS strežnika v obliki sporočila »RADIUS Access-Request«.

5. **RADIUS pošlje »EAP-Request« (Certifikat RADIUS strežnika)**

RADIUS strežnik odda RADIUS sporočilo »Access-Challenge«, ki vsebuje sporočilo »EAP-Request« s tipom EAP nastavljenim na EAP-TLS ter digitalni certifikat RADIUS strežnika. Overitelj (stikalo, brezžična dostopovna točka) nato posreduje to sporočilo do odjemalca (PC, brezžična dostopovna točka, stikalo ipd.).

6. **Odjemalec pošlje »EAP-Response« (Certifikat odjemalca)**

Odjemalec odda sporočilo »EAP-Response« s tipom EAP nastavljenim na EAP-TLS ter svoj digitalni certifikat. Overitelj posreduje to sporočilo do RADIUS strežnika v obliki sporočila »RADIUS Access-Request«.

7. **RADIUS pošlje »EAP-Request« (šifrirni material, zaključek TLS)**

RADIUS strežnik odda sporočilo »EAP-Request« z EAP tipom nastavljenim na EAP-TLS ter šifrirni material. S tem sporočilom RADIUS strežnik sporoči odjemalcu, da je izmenjava TLS avtentikacijskih sporočil zaključena.

8. **Odjemalec odgovori z »EAP-Response«**

Odjemalec pošlje RADIUS strežniku »EAP-Response« z EAP tipom nastavljenim na EAP-TLS. Overitelj nato posreduje to sporočilo do RADIUS strežnika v obliki sporočila »RADIUS Access-Request«.

9. **RADIUS pošlje »EAP-Success«**

Kadar se odjemalec priključuje v preko brezžične dostopovne točke, mora v tem koraku RADIUS strežnik izračunati še šifrirne ključe za odjemalca. Šifrirne ključe izračuna iz šifrirnega materiala, ki ga je pridobil v fazi overjanja.

4.2.4 PEAP

PEAP (Protected Enhanced Authentication Protocol) je ena izmed različic razširljivega avtentikacijskega protokola EAP. Njegov razvoj je bil v domeni treh podjetij, Cisco, Microsoft in RSA. Značilnost protokola PEAP je vnaprejšnja vzpostavitev varnega kanala, ki zagotavlja šifriranje in celovitost podatkov med odjemalcem (supplicant) ter avtentikacijskim strežnikom. Varen kanal je vzpostavljen po protokolu EAP-TLS.
V mnogih pogledih je PEAP bolj prožen od EAP-TLS, saj ne zahteva vzpostavitve drage infrastrukture javnega ključa (PKI[15]). Vzpostavitev varnega kanala temelji na predhodnem overjanju avtentikacijskega strežnika s strani odjemalca. Avtentikacijski strežnik se odjemalcu overi z digitalnim certifikatom. Po vzpostavitvi varnega TLS kanala pa je možno uporabiti katerokoli standardizirano EAP avtentikacijsko metodo.

PEAP-MSCHAPv2 je ena izmed uveljavljenih metod overjanja, saj vsebuje pravšnjo kombinacijo varnosti, medsebojne obratovalnosti, prožnosti in preprostosti izvedbe.

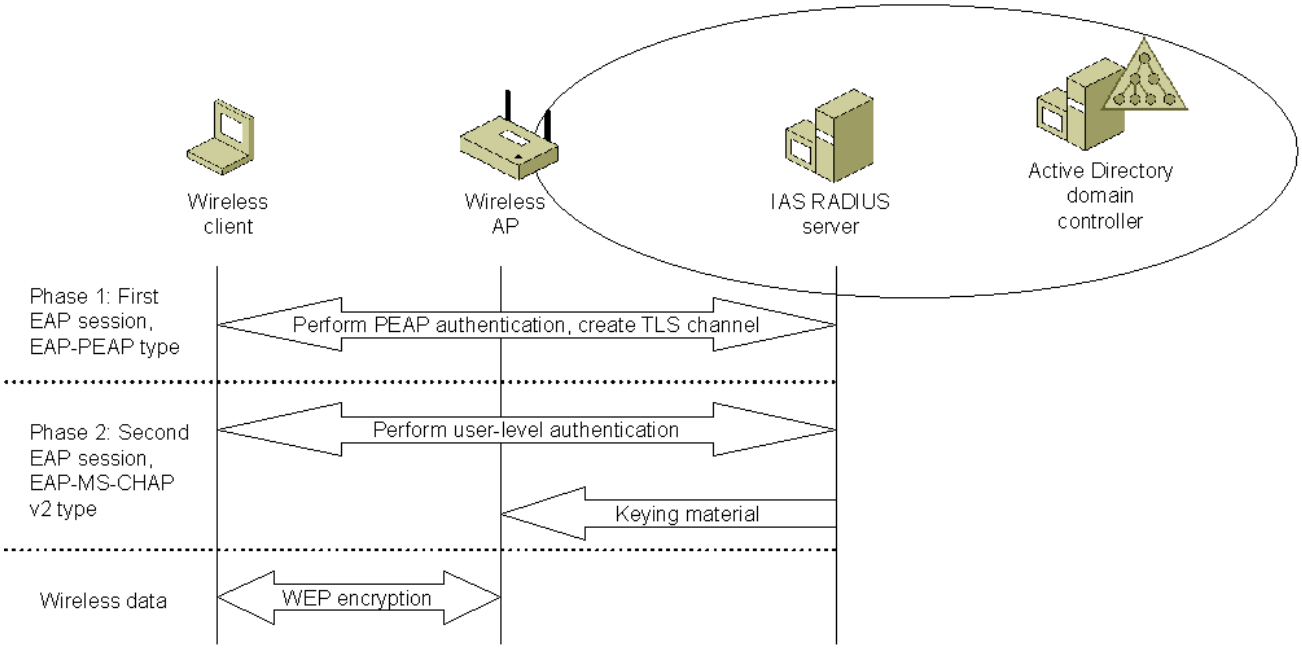
PEAP proces avtentikacije je sestavljata dve fazi:

Faza1: odjemalec najprej overi avtentikacijski strežnik; s tem se izogne povezovanju v t.i. sleparska omrežja (rogue networks). TLS vzpostavi robusten in šifriran kanal med odjemalcem in avtentikacijskim strežnikom.

Faza2: TLS kanal ščiti izmenjavo avtentikacijskih sporočil med odjemalcem in avtentikacijskim strežnikom.

Na spodnji sliki je prikazan postopek overjanja brezžičnega odjemalca. Kadar je odjemalec uspešno overjen, posreduje avtentikacijski strežnik do brezžične dostopovne točke šifrirni material. Iz tega šifrirnega materiala brezžična dostopovna točka ustvari nove šifrirne ključe.

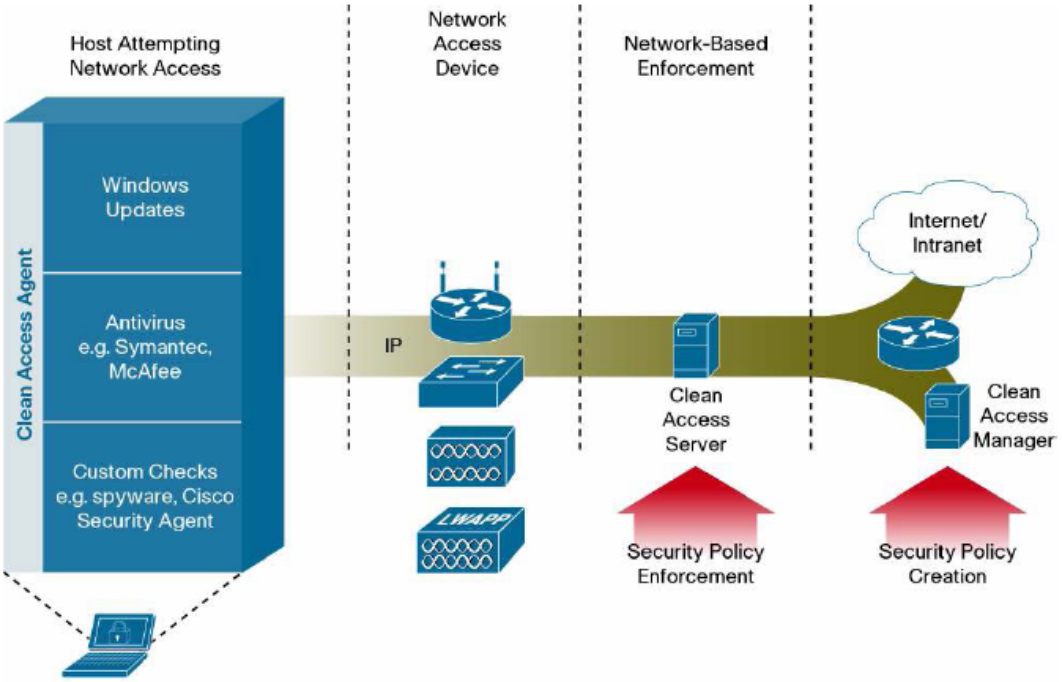
[15] PKI - public key infrastructure - infrastruktura javnih ključev



Slika 4-11: 802.1x/PEAP avtentikacija v brezžičnem omrežju

5 Krmiljenje dostopa do omrežja

Overjanje uporabnikov in naprav je seveda pomembna komponenta v rešitvi zagotavljanja varnosti omrežja, kljub temu pa ta predstavlja le del celotne rešitve. Uporabnikom in napravam je namreč omogočen dostop zgolj na podlagi overjanja njihovih poverilnic, ne pa tudi na preverjanju skladnosti samih naprav z varnostno politiko omrežja. Tako se vse pogosteje dogaja, da se uporabnik z okuženim računalnikom ali pa z operacijskim sistemom brez varnostnih popravkov, ne da bi se tega seveda zavedal, poveže v lokalno omrežje in s tem povzroči širjenje virusov, črvov in ostale škodljive kode v samo produkcijsko omrežje.
Krmiljenje dostopa do omrežja ali NAC (Network Admission Control) pri tem zagotavlja predhodno preverjanje stanja (posture) naprav, ki se povezujejo v notranje omrežje podjetja oziroma organizacije.



Slika 5-1: Arhitektura krmiljenega dostopa do omrežja (NAC)

Krmiljenje dostopa do omrežja (NAC) je tehnologija proizvajalca Cisco in jo sestavljajo ustrezna programska oprema na strani odjemalca, podporni strežniki, kjer se preverja stanje naprav, ter omrežna oprema (stikala, usmerjevalniki, brezžična dostopovna točka) z ustrezno funkcionalnostjo.

6 Avtorizacija in obračunavanje

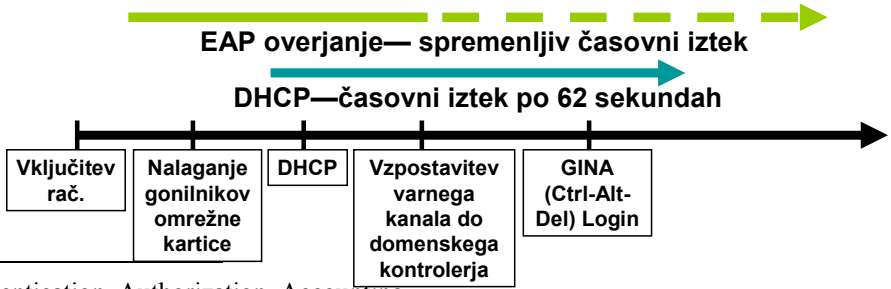
Samo overjanje brez avtorizacije nima pravega pomena. Po overitvi odjemalca AAA/RADIUS strežnik preko atributov v AAA/RADIUS paketih posreduje overitelju politiko dostopa. Avtorizacijo odjemalcev izvaja overitelj na podlagi atributov v AAAA/RADIUS paketih. Najpreprostejša oblika avtorizacije je dovolitev oz. prepoved dostopa v lokalno omrežje na povezavnem nivoju OSI referenčnega modela. Politika dostopa lahko vključuje tudi omejitve na višjih nivojih OSI modela. Tako lahko na primer v RADIUS paketih prenašamo atribute o dodelitvi uporabnikov/naprav v navidezno lokalno omrežje (VLAN) in pristopnih listah (ACL) za posameznega uporabnika/napravo. Avtorizacija lahko tako kot overjanje poteka na skupnem strežniku RADIUS, oziroma se lahko izvaja ločeno na AAA[16] strežnikih.
Izrednega pomena je tudi obračunavanje, ki zagotavlja beleženje aktivnosti posameznih uporabnikov in naprav na AAA oz. RADIUS strežniku.

7 Zahteve programske in strojne opreme

Standard 802.1X zahteva posebno programsko opremo nameščeno na strani odjemalca, t.i. *supplicant*. Supplicant mora poleg protokola 802.1X podpirati tudi EAP metode overjanja. EAP metode overjanja morajo biti podprte na vseh končnih točkah EAP komunikacije – na odjemalcu in avtentikacijskem strežniku. Overitelj mora podpirati le protokol 802.1X. Slednje je izredno dobrodošlo, saj ob uvedbi nove EAP metode overjanja ni potrebno na novo nameščati strojno-programske opreme na overitelju, temveč je potrebna le nadgradnja supplicant-a na odjemalcu ter namestitev programske opreme z dodatkom nove funkcionalnosti na centralnem AAA/RADUS strežniku.

8 Omejitve in težave

Znane so predvsem omejitve, ki izhajajo iz Windows okolja. Te so posledica neuglašenih časovnikov med procesoma DHCP[17] in EAP. DHCP je protokol, ki dinamično dodeljuje IP naslove ter ostale parametre odjemalcem in je od procesa EAP povsem neodvisen. DHCP proces se pri žičnem omrežnem vmesniku sproži z zaznavo linijskega signala (takrat gre vmesnik v stanje »up«) in traja 62 sekund. Težava nastopi, ko se odjemalec v procesu EAP ne overi v tem časovnem intervalu. Takrat odjemalec ne prejme ustreznih nastavitev DHCP strežnika.



[16] AAA – Authentication, Authorization ,Accounting
[17] DHCP - Dynamic Host Configuration Protocol: DHCPprotokol za dinamično konfiguriranje gostiteljev

Slika 8-1: Zagonski cikel v Windows okolju ter prikaz časovnih iztekov EAP in DHCP procesa

Omenjeno težavo lahko zaobidemo, če pred overjanjem uporabnikov overimo napravo. Overjanje naprave se izvede na začetku zagonskega cikla Windowsov in se zaključi pred časovnim iztekom procesa DHCP. Omenjeno težavo je naslovil tudi Micrsoft v popravku za Windows.

9 Zaključek

Pojmovanje varnosti v omrežjih je prešlo okvir posamezne požarne pregrada. Slednja sicer lahko do neke mere ščiti notranje omrežje pred napadi od »zunaj«, t.j. javnega omrežja, vendar ne zagotavlja zaščite pred nepooblaščenim dostopom uporabnikov v notranje omrežje podjetja »od znotraj«, t.j. iz lokalnega omrežja. Z sistemi za zaznavo in preprečevanje vdorov (IDS/IPS) bi v neki meri sicer bilo možno omejiti tudi tovrsten nepooblaščen dostop do omrežja (dostop do notranjega omrežja od znotraj), vendar bi taka rešitev lahko bila prekomplicirana in posledično predraga.

Za vsako podjetje, organizacijo je pomembno, da jasno definirana pravila dostopa ter uporabe virov svojega informacijskega sistema, ki so natančno opredeljena z varnostno politiko podjetja oziroma organizacije. Zanašati se na to, da bodo uporabniki dosledno upoštevali in se ravnali po pravilih definiranih v varnostni politiki je zmotno. Vse pogosteje se dogaja, da notranji uporabniki iskoč lažjih in predvsem hitrejših načinov dostopa do notranjih virov informacijskega sistema zaobidejo pravila definirana v varnostni politiki in s tem ogrozijo varnost celotnega sistema. V varnosti velja, da je ta dobra toliko, kot je dober njen najšibkejši člen.

Tako se danes zastavlja dve ključni vprašanji:
Kako zagotoviti nadzor nad nepooblaščenim priključevanjem naprav in uporabnikov v lokalno omrežje od »znotraj«, t.j. preko notranjega omrežja?
Kako zagotoviti, da naprave s katerimi se uporabniki priključujejo v notranje omrežje nekega podjetja oziroma organizacije ustrezajo varnostni politiki tiste organizacije?

Odgovor na ti dve vprašanji lahko poiščemo v tehnologijah, ki prihajajo in obetajo veliko: 802.1x/EAP in krmiljenje omrežnega dostopa (NAC, NAP). Prva omogoča overjanje uporabnikov in naprav v lokalnem omrežju, druga pa preverjanje stanja naprav (posture), ki se povezujejo v lokalno omrežje.
NAC (Network Admission Control) je tehnologija proizvajalca Cisco. V tej rešitvi poleg podpornih strežnikov nastopajo tudi omrežne naprave, kot so stikala, usmerjevalniki in brezžične točke. NAP (Network Access Protection) pa je tehnologija proizvajalca Microsoft. Slednja prav tak zagotavlja pregled stanja naprav preden je le-tem omogočen dostop v notranje omrežje podjetja oziroma organizacije. Vendar pa slednja rešitev ne zagotavlja podporo v omrežnih elementih (stikala, usmerjevalniki, brezžična dostopovna točka) kot je to značilno za rešitev proizvajalca Cisco, ampak je podprta zgolj na končnih strežnikih.

Obe tehnologiji (NAC in NAP) sta dokaj novi in ju v praksi še ne srečujemo, medtem ko se tehnologijo 802.1X/EAP že implementira v večjih omrežjih.

10 Literatura

[1] Mainwald E.:*Network Security,* McGraw-Hill/Osborne, 2001
[2] Peikari C., Fogie S.: *Maximum Wireless Security*, Sams, 2003
[3] Burton Group: *Directory and Security Strategies: User Authentication,* 2004
[4] Meta Group: *Evolving the Network Edge*, White Paper, 2004
[5]CSI: *ComputernSecurity Issues&trends,* Vol. 8, No.1, 2002
[6] Cisco: www.cisco.com
[7] Juniper: www.juniper.net
[8] NortelNetworks: www.nortelnetworks.com
[9] Microsoft: www.microsoft.com
[10] Slovar informatike: http://www.islovar.org/iskanje_enostavno.asp
[11] Slovar ITkT: http://www.ltfe.org