VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
ELEKTRONIKOS FAKULTETAS
KOMPIUTERIJOS IR RYŠIŲ TECHNOLOGIJŲ KATEDRA

RADIUS PROTOKOLO APŽVALGA

Namų darbas darbas

Atliko: TETfm-18 grup. stud. Lukas Stankovičius

Vilnius, 2018

ĮVADAS

1.1. Temos problema

Šiandieniniame pasaulyje vis svarbesnė tampa saugumo tema, dėl išaugusių kibernetinių nusikaltimų skaičiaus nukenčia tiek įmonės, tiek namų vartotojai. Belaidžiuose tinkluose įsibrovimas yra dažnas reiškinys. Dažna situacija, kuomet interneto kavinėse yra paliekamas atviras kenkėjų prieigos taškas. Žmonės susigundę nemokamu belaidžiu ryšiu prisijungia prie prieigos taško net nepagalvodami, kas gali valdyti prieigos tašką ir per kontroliuoti per jį einančius duomenis. Tokiu būdu sužinomos klientų prisijungimo slaptažodžiai, atskleidžiama privati informacija. Belaidžiuose tinkluose įmonės tampa vis dažnesniu taikiniu įsibrovėliams, todėl auga poreikis saugumui. Taikiniais tampa netik atviri tinklai, bet ir apsaugoti šifravimo protokolais tinklai. Šiuolaikinės įmonės skiria daugiau pastangų darbuotojų kompiuteriniam raštingumui kelti bei skiria papildomas investicijas į informacijos perdavimą, saugojimą ir šifravimą.

1.2. Temos aktualumas

Belaidžiuose „Wi-Fi“ tinkluose prieigos taškai dažnai būna apsaugoti šifravimo protokolais, tokie kaip WEP, WPA ar WPA2, tačiau artėjama prie situacijos, kuomet reikalingas kitas sprendimo būdas. Taip ir todėl, ne vienas iš populiariausių prieigos taško šifravimo protokolų WPA2-PSK tampa vis labiau pažeidžiamas. Pagrindinė esmė, jog WPA2-PSK protokolas tampa vis mažiau atsparus įsibrovėlių atakoms. Galima situacija: įsibrovėliams reikalingas prieigos taško SSID, kad galėtų dekoduoti 256 bitų PMK (angl. Pairwise Master Key), aišku, tai užtruktų, bet yra įmanoma. PMK raktas yra naudojamas šifruoti duomenis keliaujančius per prieigos tašką CCMP/AES ar TKIP protokolais. Šis PMK raktas yra toks pat tarp visų prieigos taško klientų. Iš eterio galima gauti daug duomenų su tokiu pačiu PMK raktu. Įsibrovimo realus pavyzdys yra KRACK (angl. Key Reinstallation Attacks) atakos galinčios, pasinaudojant WPA2-PSK 4 lygiu saugumo spraga, sužinoti PSK (angl. Pre-Shared Key) ir dešifruoti prisijungusio kliento duomenis. PSK yra tiesiog užšifruotas prieigos taško prisijungimo slaptažodis. Grėsmė atsiranda, jog įsibrovėlis gali periodiškai siųsti 3 rankos [3] paspaudimo etapą iš kito įrenginio siekiant manipuliuoti ar atstatyti šifravimo raktą. Kiekvienas rakto atstatymas verčia duomenims būti šifruojamu tokiu pačiu raktu, todėl su tokiais pačiais duomenų blokai gali būti suvienodinami ir randami skirtumai tol, kol sužinomas visas raktas. Tokiu būdu įsibrovėlis gali sužinoti visą nustatytos aukos sesijos srautą. Tiesa WPA2-Enterpise protokolas neapsaugo vartotojo nuo galimos KRACK atakos, tačiau sudaro papildomus autenfikacijos žingsnius.

Belaidžių tinkų pažeidžiamumas yra aktuali tema. Vienas iš įmonių apsisaugojimo būdu naudoti RADIUS serverį, kuris veikia kartu su WPA2-Enterprise protokolu. Esmė, jog vartotojo duomenų

autentifikacija vykdoma ne prieigos taške, o nutolusiame serveryje. Kada RADIUS serveris autentifikuoja klientą prieigos taškui grąžinamas atsitiktinis PSK raktas duomenų šifravimui, kiekvienas vartotojas turi po atskirą raktą. Tai yra vienas iš daugelio RADIUS serverio panaudojimo būdų. Kitame skyriuje yra apžvelgiama RADIUS protokolo architektūra, valdymas, pranešimai ir veikimo būdas.

2. RADIUS PROTOKOLO APŽVALGA

Šiame skyriuje aptariama RADIUS protokolo esmė, veikimas, paketo formatas, panaudojimo būdas. Apžvelgiama struktūra, naudojamos kodo vertės ir kokio rezultato tikimasi naudojant protokolą.

2.1. RADIUS protokolo esmė

Remiantis šaltiniu [4] RADIUS (angl. Remote Authentication Dial In User Service) – tinklo protokolas, sukurtas Livigston Enterprises kompanijos, vėliau buvo nupirktas IETF ir standartizuotas. Protokolas leidžia centralizuoti AAA (autenfikacijos, autorizacijos ir apskaitos) valdymą. RADIUS naudoja klientas/serveris architektūrą, kurioje programinė įranga leidžia nuotoliniu būdu patvirtinti vartotojus prieiga prie vidinio tinklo ar paslaugos. Dažnai RADIUS serveriai naudojami kompanijų dėl patogaus darbuotojų profilio palaikymo centrinėje duomenų bazėje kurią kiti nuotoliniai serveriai gali pasiekti.

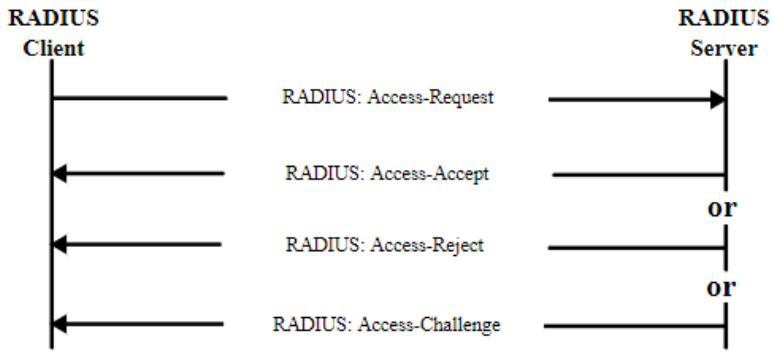
2.2. RADIUS pranešimų tvarka

Vartotojų prieigos autentifikacija vykdoma, kai vartotojas arba prietaisas išsiunčia prašymą (angl. request) į NAS (angl. Network Access Server) su atitinkamais duomenimis, gauti prieigą prie paslaugos ar vidinio tinklo. Duomenys yra perduodami PPP (angl. Point-to-Point) protokolu ar HTTPS (angl. Hypertext Transfer Protocol Secure) per interneto svetainės sąsają. RADIUS kliento ir RADIUS serverio tarpusavio pranešimų sąveika geriausiai atvaizduojama nagrinėjant WPA2-Enterprise autenfikacijos procesą. RADIUS kliento ir serverio pranešimų eiga atvaizduojama 1 paveiksle.

Prašymo paketą sudaro prieigos įgaliojimai (angl. credentials), kurie paprastai būna vartotojo vardas ir slaptažodis arba vartotojui skirtas sertifikatas. RADIUS serveris patikrina gautus duomenis su turimais duomenų bazėje naudodamas autenfikacijos schemas kaip: PAP, CHAP, EAP. Dažniausiai įmonėse naudojamas EAP (angl. Extensible Authentication Protocol) protokolas. Iš esmės standartas nusakantis kaip klientas bendrauja su serveriu, pagrindinis darbas perduoti šifruotus pranešimus, todėl yra įvairios versijos kaip EAP-TTLS, EAP-PSK, EAP-PEAP suteikiančios papildomo saugumo parametrų. Galimi trys serverio atsakymo variantai: Access Accept, Access Challenge, Access Reject.

1) Access Accept pranešimas siunčiamas iš serverio tada, kai vartotojui yra suteikiama prieigą prie tinklo paslaugos. RADIUS serveris periodiškai tikrina ar vartotojas turi prieigą prie tinklo paslaugos.
2) Access Challenge pranešimas siunčiamas, kai reikalinga papildoma vartotojo informacija tapatybei patvirtinti. Tokia informacija gali būti kaip papildomas slaptažodis, PIN kodas, darbuotojo numeris. Taip pat šis pranešimas siunčiamas, kai vykdomas saugesnė autentifikacija, t.y prašoma daugiau informacijos susijusiu su vartotoju. Taip sukuriamas tunelis tarp vartotojo ir RADIUS serverio, tuomet NAS įrenginys neturi jokios informacijos apie vartotojo perduodamus duomenis.

3) Access Reject pranešimas siunčiamas, kai vartotojui nesuteikiama prieiga prie tinklo paslaugos, kaip galimos klaidos priežastys gali būti tapatybės duomenų klaida ar išjungtas vartotojas duomenų bazėje.

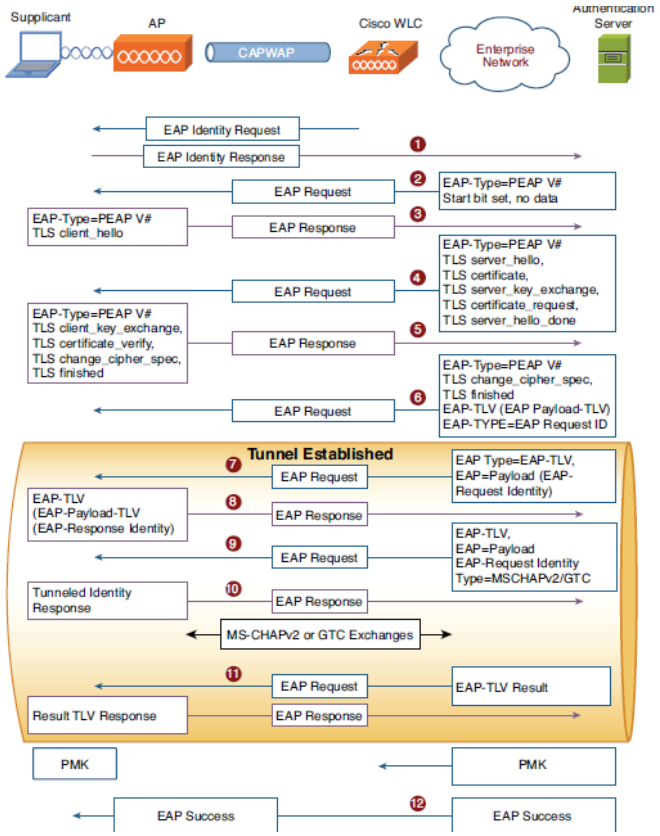


1 pav. RADIUS kliento ir serverio tarpusavio pranešimų apsikeitimas [4]

Paprastai autenfikacijos procesą galima suskirstyti į punktus:

1) Autentifikacija pradedama, kai vartotojas prisijungia belaidžiu ar laidiniu būdu prie NAS serverio, kas dažnai būna tiesiog prieigos taškas, ir nurodo vartotojo vardą ir slaptažodį.
2) Tada NAS įrenginys (prieigos taškas) aptinka prisijungimą ir pradeda autenfikacijos procesą.
3) Prieigos taškas sugeneruoja RADIUS Access-Request paketą su vartotojo vardu ir slaptažodžiu kartu nurodydamas papildomus AVP informaciją.
4) RADIUS serveris gavęs paketą suformuoja vieną iš galimų atsakymų: Access-Accept, Access-Request, Access-Challenge.
5) RADIUS serveriui patvirtinus vartotojo informacija, siunčiami Access-Chanllenge paketai, kuriuose vykdomi „Client Hello“, „Server Hello“, „Server Key Exchange“, „Server Hello Done“, „Change Cipher Sec“, „Encrypted Handshake Message“ pranešimai.
6) Sukuriamas EAP-PEAP tunnelis, kuriame apsikeičiama GTC (Generic Token Card) arba MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) priklausomai nuo prie NAS prisijungusio įrenginio.
7) Access-Challenge ir Access-Request pranešimai siunčiami tol, kol įvykdoma visa 4 lygių rankų paspaudimas.
8) Autenfikacijos pabaigoje vartotojui sugeneruojamas atsitiktinis 256 bitų PMK raktas šifruoti duomenis.

Visa RADIUS ir EAP-PEAP protokolų pranešimų eiga tarp kliento ir aptarnaujančio serverio parodyta 2 paveiksle.

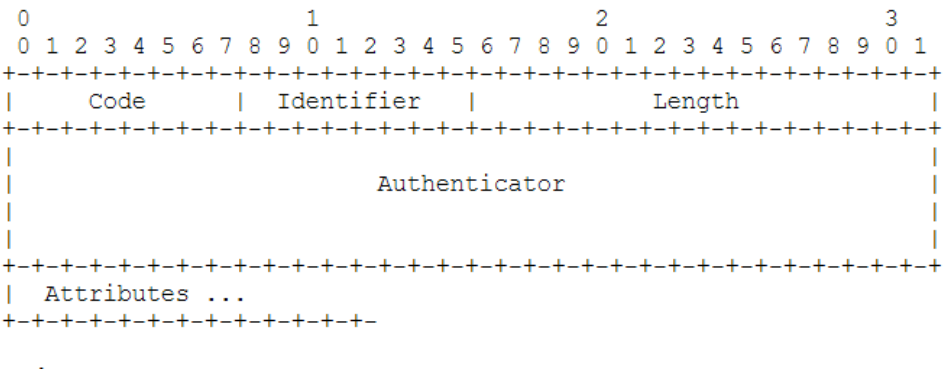


2 pav. RADIUS serverio EAP-PEAP pranešimų seka [2]

EAP-PEAP esmė, jog sukuriamas TLS tunelis tarp RADIUS serverio ir kliento, tada RADIUS serveris pateikia sertifikatą klientui kaip patvirtinimą, jog yra saugus. Jeigu klientas atpažįsta serverio sertifikatą savoje duomenų bazėje autorizacijos procesas tęsiamas toliau. Jeigu ne klientas gauna perspėjimą.

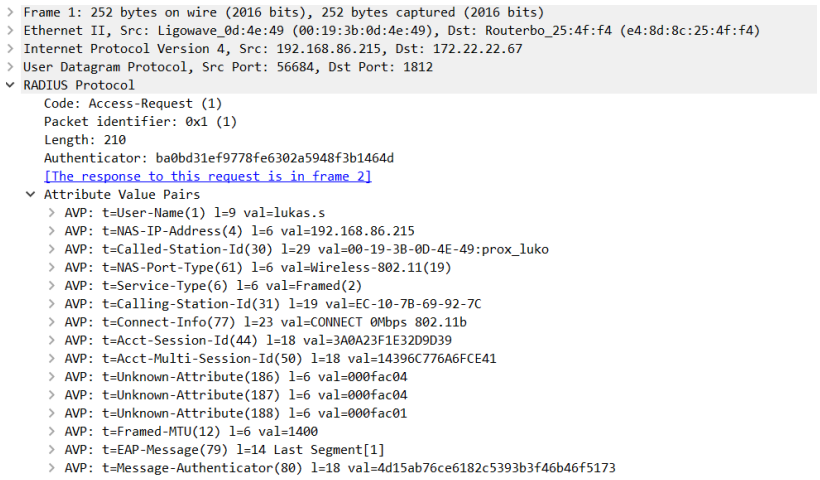
2.3. RADIUS paketo formatas

RADIUS paketas yra inkapsuliuojamas į UDP protokolo duomenų lauką, kur UDP gavėjo sąsaja nurodama 1812. Kuomet yra sugeneruojamas atsako pranešimas šaltinio ir gavėjo sąsajos apsikeičia. Perduodamo paketo struktūra pavaizduota 3 paveiksle.



3 pav. RADIUS protokolo paketo struktūra [4]

1) Kodo antraštę sudaro 8 bitai, todėl galimos iš viso 255 reikšmės, kurios reiškia tam tikrą pranešimą. Dažniausiai naudojami kodai: 1, 2, 3, 4, 5, 11, analogiškai Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, Access-Challenge.
2) Paketų indentifikavimo atrašė sudaro 8 bitai. Šis laukas padeda paketų atpažinimo procese. Kiekvienam pranešimui yra priskiriamas ID, pagal kurį eina atsakai arba prašymai.
3) Ilgio antraštė nurodo visą RADIUS paketo ilgį, kuris yra inkapsuliuojamas į UDP segmentą. Antraštės ilgis yra 16 bitų.
4) Autentifikatoriaus antraštė skirta vartotojo slaptažodžio šifravimui ir perdavimui. Šio lauko ilgis yra 16 baitų.
5) AVPs (angl. Attribute value pairs) perneša duomenis susijusius su autentifikacija, prieigos kontrolę. Paketo ilgis nusako AVP antraštės ilgį. AVP pernešamų duomenų analizė „WireShark“ programinėje įrangoje pateikiama 4 paveiksle.



4 pav. RADIUS paketas „WireShark“ programinėje įrangoje [6]

APIBENDRINIMAS

Rašto darbe apžvelgta saugumo tema ir jos keliamos problemos šiuolaikiniame pasaulyje. Ypač pažeidžiami tampa belaidžiai tinklai, kuriuose įsibrovėliai gali šnipinėti vartotojų srautą.

Temos aktualume trumpai aptarti belaidžiuose tinkluose esantys WPA saugumo protokolai ir jų veikimo būdai. Išsiaiškinta, jog šiuo metu geriausias variantas yra naudoti, tiek įmonėms, tiek galimai ir namų vartotojams, WPA2-Enterprise protokolą, kuris veikia pasitelkdamas RADIUS serverį.

RADIUS serveris yra tinklo protokolas, skirtas centralizuoti vartotojų autenfikaciją, pagal esančią duomenų bazę. RADIUS serveris naudoja klientas/serveris architektūra. RADIUS serveriai naudojami kompanijų dėl patogaus darbuotojų profilio palaikymo centrinėje duomenų bazėje kurią kiti nuotoliniai serveriai gali pasiekti.

Apžvelgta RADIUS pranešimų perdavimo būdas: RADIUS klientas su RADIUS serveriu bendrauja per NAS įrenginį, kas dažnai būna prieigos taškas. Išsiaiškinta kaip ir kokie pranešimai siunčiami esant ryšiui. Yra trys su autenfikaciją gaunami pranešimai iš serverio: Access-Challenge, Access-Reject ir Access-Accept. Klientas siunčia Access-Response pranešimus.

Aptartas vienas iš RADIUS įgyvendinimo būdu – WPA2-Entprise autenfikacijos procesas. Išsiaiškina, jog RADIUS pranešimai yra perduodami EAP protokolu, kuris gali turėti daug versijų. Apžvelgta EAP-PEAP versija, kuomet RADIUS serveriui autorizavus vartotojo vardą ir slaptažodį ir yra sukuriamas transporto sluoksnio saugumo sluoksnis, kuriame įvykdomi 4 lygiu rankos paspaudimo etapai, siekiant sugeneruoti PMK kodą klientui.

Galiausiai aptarto RADIUS protokolo paketo struktūra, kuriame apžvelgti antraščių dydžiai ir nešama informacija. Informacija palyginama su realiu nuskaitytų srautu gautu iš „WireShark“ programinės įrangos.

INFORMACIJOS ŠALTINIAI

1. *Cisco RADIUS serverio dokumentacija* [interaktyvus, žiūrėta 2019-03-16]. Prieiga per internetą: <https://www.cisco.com/c/en/us/td/docs/net_mgmt/access_registrar/17/concepts/guide/radius.html>
2. *EAP-PEAP protokolo darbo eiga* [interaktyvus, žiūrėta 2019-03-16]. Prieiga per internetą: <https://mrncciew.files.wordpress.com/2013/03/peap-1.png>
3. *New KRACK Attack Breaks WPA2 WiFi Protocol, Catalin Cimpanu* [interaktyvus, žiūrėta 2019-03-16]. Prieiga per internetą: <https://www.bleepingcomputer.com/news/security/new-krack-attack-breaks-wpa2-wifi-protocol/>
4. *RFC2865 standarto dokumentacija* [interaktyvus, žiūrėta 2019-03-16]. Prieiga per internetą: <https://tools.ietf.org/html/rfc2865>
5. *Why Use Enterprise Wi-Fi Security, Eric Geier* [interaktyvus, žiūrėta 2019-03-16]. Prieiga per internetą: <http://techgenix.com/why-use-enterprise-wi-fi-security>
6. *WireShark programinės įrangos naudojimosi knyga* [interaktyvus, žiūrėta 2019-03-16]. Prieiga per internetą: <https://www.wireshark.org/download/docs/user-guide.pdf>