Langattoman vierailijaverkon toteutus kampuksille

Tiivistelmä

Työtä ja opiskelua tehdään entistä useammin muualla kuin omalla työpisteellä tai tietokoneluokassa, joten langattomien verkkojen merkitys on korostunut. Yliopistojen, ammattikorkeakoulujen ja tutkimuslaitosten vierailijoille onkin syytä taata toimiva, helppokäyttöinen ja tietoturvallinen ratkaisu verkkoon pääsemiseksi, jotta vierailijoiden työskentely tai opiskelu myös vierailtaessa on helppoa ja sujuvaa.

WLAN-tekniikalla toteutetulle vierailijaverkolle on neljä erilaista toteutustapaa. Niiden hyvät ja huonot puolet sekä kustannusarvio on esitetty taulukossa 1. Täysin avoin WLAN-verkko on kaikkien käytettävissä verkon kuuluvuusalueella. Web-autentikointiin perustuvaan verkkoon tarvitaan etukäteen luotu käyttäjätunnus ja salasana, jotka syötetään webbisivulle verkkoon liittymisen jälkeen. Henkilökohtainen jaettu avain on menetelmä, jossa syötetään liittymisen yhteydessä etukäteen luotu avain, jota käytetään autentikointiin ja kryptaukseen. Käytettäessä 802.1x autentikointia ja WPA2/AES-salausta, käyttäjät tunnistetaan ennen kuin liikennöinti on mahdollista. Liikenne on kryptattua ja kryptausavainta vaihdetaan usein. Liittyminen verkkoon tapahtuu suplikantin avulla.

Taulukko 1. Eri tekniikoilla toteutetut WLAN-vierailijaverkot, niiden hyvät ja huonot puolet sekä kustannusarvio.

Tekniikka	Hyvät puolet	Huonot puolet	Kustannukset
Avoin verkko	Helppokäyttöinen Vierailijatunnuksia ei tarvitse luoda	Ei voida mitenkään määritellä kuka saa käyttää verkkoa Salaamaton yhteys, verkon tietoturva huono (tietoturva käyttäjän vastuulla)	Ei erityisiä investointi- tai operointikustannuksia (halpa)
Web-autentikointiin perustuva verkko	Helppokäyttöinen ja toimintavarma Osittainen mahdollisuus määritellä kuka saa käyttää verkkoa	Salaamaton yhteys, verkon tietoturva huono (tietoturva käyttäjän vastuulla) On määriteltävä prosessi, jolla luodaan vierailijatunnuksia yksittäiselle vierailijalle ja tapahtumille.	Vaatii RADIUS-palvelimen, sisäänkirjautumissivun ja käyttäjähallintaa (keskihintainen)
Henkilökohtainen jaettu avain	Mahdollistaa hyvän tietoturvan olemalla myös helppokäyttöinen ja helposti toteutettavissa	Ei tuettuna kaikissa tukiasemissa	Riippuu valmistajien hinnoittelupolitiikasta. Vaatii käyttäjähallintaa (luultavasti keskihintainen)
802.1x autentikointi ja WPA2/AES-salaus (eduroam)	Erittäin tietoturvallinen Automaattinen liittyminen verkkoon ensimmäisen liittymisen jälkeen.	Konfigurointiongelmia esiintyy Rajattu käyttäjäkunta (eduroam-vierailijaverkkopalvelu on vain yliopistoille, ammattikorkeakouluille ja tutkimuslaitoksille)	Vaatii RADIUS-palvelimen ja käyttäjien opastusta (keskihintainen)

IT-hallinnon näkökulmasta täysin avoimeen verkkoon liittyy se riski, että väärinkäytöstapauksissa vain laite voidaan selvittää MAC-osoitteen perusteella – ei käyttäjää. Web-autentikointiin perustuva verkko on IT-hallinnon kannalta hieman suojatumpi koska kuka tahansa ei päästetä verkkoon. Käyttäjän kannalta riski on kuitenkin suurempi käytettäessä kyseisiä menetelmiä. Käyttäjän tekemisiä avoimessa tai web-autentikointiin perustuvassa verkossa voidaan helposti salakuunnella tai manipuloida, eikä käyttäjä välttämättä tiedä, miten suojautuminen erilaisilta verkkouhilta pitäisi tapahtua. Eli käyttäjän kannalta olisi hyvin tärkeätä tarjota tietoturvallista eduroam-vierailijaverkkoa, joka perustuu 802.1x autentikointiin ja WPA2/AES-salaukseen. Henkilökohtainen jaettu salaisuus tarjoaa myös hyviä mahdollisuuksia vierailijaverkoksi, mutta tällä hetkellä vain muutama laitevalmistaja tukee menetelmää.

Halvin ratkaisu lienee avoin verkko, muut ratkaisut edellyttävät investointeja kuten esim. RADIUS-palvelimen hankinnan. Myös opertointikustannuksia verrattaessa avoin verkko on halvin, muut ratkaisuehdotukset vaativat jonkin verran käyttäjähallintaa ja käyttötukea.

Johdanto

Työtä ja opiskelua tehdään entistä useammin muualla kuin omalla työpisteellä kiinteän verkon kautta, joten langattomien verkkojen merkitys on korostunut. Myös yrityksissä ja kampuksilla vierailevat henkilöt ovat yhä enemmän riippuvaisia muiden tarjoamasta langattomasta verkosta. Vierailijoille onkin syytä taata toimiva, helppokäyttöinen ja tietoturvallinen ratkaisu verkkoon pääsemiseksi, jotta vierailijoiden työskentely myös vierailtaessa on helppoa, sujuvaa ja tietoturvallista.

Tässä dokumentissa esitetään asioita, jotka on otettava huomioon suunniteltaessa langatonta vierailijaverkkoa kampukselle tai muuhun toimipisteeseen. Ensin kartoitetaan avoimen-, web-autentikointiin perustuvan-, jaetun salaisuuteen perustuvan- sekä 802.1x autentikointiin ja WPA2/AES-salauksen perustuvan verkon hyvät ja huonot puolet. Myös muita WLAN-verkkoihin liittyviä asioita tarkastellaan, mutta WLAN-verkon suunnittelua, rakentamista ja valvontaa ei käsitellä.

Ratkaisujen suurimmat erot liittyvät tietoturvaan. Etenkin käyttäjän näkökulmasta erot ovat suuret – avoimessa ja web-autentikointiin perustuvissa verkoissa liikenne on salaamaton ja uhat ovat suuret. Henkilökohtainen jaettu salaisuus lisää huomattavasti tietoturvaa, mutta paras mahdollinen tietoturva saavutetaan 802.1x autentikoinnilla ja WPA2/AES salauksella, kuten eduroamissa. eduroamin käyttäjäkunta on kuitenkin suhteellisen rajattu, eivätkä kaikki vierailijat pääse sitä käyttämään. IT-hallinnon kannalta ratkaisut eroavat etenkin siinä, että halutaanko määritellä kuka saa käyttää verkkoa tai onko verkko avoin kaikille sen kuuluvuusalueella oleville.

WLAN-verkon rakenne ja ylläpito

Kontrolleripohjaiseen WLAN-verkkoon voidaan helposti lisätä ja poistaa verkkoja (eli verkkonimiä ts. SSID:tä). Kontrolleri määrittää mitkä verkot tarjotaan siihen liittyneiden tukiasemien kautta. Jos WLAN-verkko koostuu itsenäisistä tukiasemista, verkkonimi (SSID:n) on määriteltävä jokaiseen tukiasemaan erikseen. Myös langattoman vierailijaverkon ylläpito on selvästi helpompi kontrolleripohjaisessa WLAN-verkossa, eikä itsenäisistä tukiasemista koostuvaa verkkoa enää suositella. Myös kevyitä kontrolleripohjaisia ratkaisuja on nykyään saatavilla [1].

Uusi verkko kontrolleripohjaiseen WLAN-verkkoon määritellään luomalla sille verkkonimi (SSID). Tämän jälkeen määritellään verkolle asetukset – eli onko verkko avoin ja jos ei, miten pääsyä verkkoon rajataan. Seuraavaksi määritellään, miten vierailijaverkon liikennettä hoidetaan, eli mihin virtuaaliverkkoon (VLAN-verkkoon) liikenne sijoitetaan ja mitkä palvelut tarjotaan verkossa, eli mitkä portit avataan palomuurissa.

On myös huomioitava, että WLAN-verkkoa tulisi paitsi valvoa, myös auditoida säännöllisesti. Auditoinnissa havaitaan radioverkon kuuluvuusongelmat, konfiguraatioiden oikeellisuus, puutteelliset tai vanhentuneet tunnistus- ja tietoturvamenetelmät sekä luvattomat tukiasemat.

Verkon IP-osoitteiden ja lokituksen suhteen pätevät samat säännöt kuin lähiverkkoa suunniteltaessa. Jos päätetään WLAN-verkossa käyttää RFC1918-standardissa määiteltyjä privaattiosoitteita, edellyttää se käytännössä Network Address and Port Translation (NAPT) – lokien keräämistä, jotta abuse-tapauksissa löytyy oikea käyttäjä [2]. Jos ei ole tarpeeksi julkisia IPv4-osoitteita WLAN-verkolle, on IPv6-osoitteiden käyttöä suositeltavaa ainakin jäljitettävyyden osalta.

WLAN-verkkoa tarkistaessa keskitytään tukiaseman ja päätelaiteen väliseen ilmarajapintaan ja tähän liittyvään tietoturvaan. Kokonaisuuden kannalta on huomioitava paitsi lokitus myös muut infrastruktuuriin liittyvät asiat, esim. ilmarajapinnan kryptaus ei ole turvallisempi jos käyttäjät kuitenkin IP-tasolla pystyvät samassa verkossa juttelemaan ilman rajoituksia.

Vierailijaverkon vaihtoehdot

Avoin verkko

+ Helppokäyttöinen

+ Vierailijatunnuksia ei tarvitse luoda

- Ei voida etukäteen määritellä kuka saa käyttää verkkoa

- Salaamaton yhteys, verkon tietoturva huono (tietoturva käyttäjän vastuulla)

Helppo tapa järjestää langaton vierailijaverkko on määritellä vierailijaverkko täysin avoimeksi. Verkkonimi voi olla esimerkiksi yliopisto-visitor tai amk-open. Näin kuka tahansa, ei pelkästään organisaation vieraat, pystyvät verkkoa käyttämään. IT-hallinnon työn ajatellaan usein helpottuvan, koska käyttäjien hallintaa ei avoimessa verkossa tehdä. Kuitenkin mahdolliset ongelmat ja niiden selvittely voivat olla aikaa ja resursseja vievää. Avoimiin verkkoratkaisuihin ohjaudutaan yleensä loppukäyttäjien kirjautumisen helpottamiseksi ja käyttömukavuuden parantamiseksi. Verkon ylläpito on kuitenkin hieman ongelmallista puuttuvan tietoturvallisuuden takia. IT-hallinto ei pysty määrittelemään ketkä päästetään verkkoon ja ongelmia aiheuttavan käyttäjän tapauksen selvittämiseen saattaa viedä huomattavia resursseja IT-hallinnolta.

Käyttäjien kannalta ongelmaksi muodostuu, että heidän tekemisiä täysin avoimessa verkossa voidaan salakuunnella. Lisäksi heihin voidaan kohdistaa erilaisia hyökkäyksiä. Tavallisimmat uhat ovat:

- Snooping/sniffing/sidejacking [2] [3] [4]: Käyttäjän lähettämän ja hänelle saapuvan liikenteen salakuuntelu, koska liikennettä ei kryptata. Myös käyttäjätunnuksia ja salasanoja voidaan tällöin varastaa.
- Evil twin/man-in-the-middle hyökkäyksiä [2] [3] [4]: Hyökkääjä pystyttää tukiaseman, joka teeskentelee olevansa yliopistoon kuuluva tukiasema ja täten houkuttelee päätelaitteita liittymään siihen. Valmiita työkaluja löytyy tähän tarkoituksen, kuten WiFi Pineapple [5]. Liittymisen jälkeen käyttäjän liikenne kulkee hyökkääjän tukiaseman läpi ja liikenne voidaan kaapata, muuttaa tai uudelleenohjata. Hyökkääjä voi myös pystyttää huijaussivun, jossa annetaan ymmärtää, että WLAN-verkon käytöstä on maksettava luottokortilla. Täten hyökkääjä pystyy varastamaan käyttäjän luottokorttitietoja.

Aalto-yliopistolla on käytössä täysin avoin vierailijaverkko ja heidän järjestelmäasiantuntijan Ville Pursiaisen mukaan joitain verkon väärinkäytöstapauksia on ollut. Yleensä on ollut kyse peer-to-peer liikenteestä, mutta tallennettujen MAC-osoitteiden avulla tapaukset on ratkaistu. Tällä hetkellä peer-to-peer

liikennöintiä ei sallita Aallon avoimessa vierailijaverkossa. Käytännössä se on hidastettu käyttökelvottomaksi. Aalto-yliopistolla ei olla tietoisia tapauksista, joissa vierailija olisi joutunut vaikeuksiin käyttäessään heidän avointa verkkoa. Toisaalta vakavammista rikoksista esim. luottokorttitietojen varastamisesta, käyttäjät ilmoittavat suoraan poliisille. Ville Pursiainen painottaa myös, että Aalto-yliopisto on saanut paljon kiitosta avoimesta langattomasta verkostaan. Käyttäjät ovat olleet tyytyväisiä siihen, että verkko ei missään vaiheessa kysele käyttäjiltä mitään tai pakota liittymisen jälkeen kirjautumissivulle.

Avoimen vierailijaverkon tarjoaminen Suomessa etukäteen rajoitetulle käyttäjäpiirille on lakiteknisesti hyväksyttävää. Nykylainsäädännön mukaan avoimen langattoman verkon esimerkiksi kerrostalonaapurin verkon käyttö on myös laillista [6]. Koska käyttöön ei liity riskiä syyllistyä rikokseen, voidaan katsoa, että avointen langattomien verkkojen tarjoaminen on mahdollista myös kampuksilla.

Jos Internet-yhteyttä tarjotaan WLAN-verkon kautta etukäteen rajaamattomalle käyttäjäpiirille, on kyse yleisestä teletoiminnasta. Tästä seuraa ilmoitusvelvollisuus Viestintävirastolle ja yleisiin viestintäverkkoihin asetettuja velvoitteita on seurattava. Funet-yhteisönä nähdään kuitenkin, että myös avoimen kampusverkon käyttäjäpiiri on peittoalueen rajallisen ulottuvuuden takia etukäteen rajattu, eikä ole kyse yleisestä teletoiminnasta. Asiasta lisätietoja WLAN-verkot ja lainsäädäntö Parhaat käytännöt-dokumentissa [7]. Kampuksen verkon peittoalue on kuitenkin aina hieman suurempi kuin itse kampus, eli vieressä olevat yritykset ja asuintalot voivat IT-hallintoa tietämättä käyttää avointa verkkoa.

Funetin sisarorganisaatiot Englannissa, Hollannissa ja Italiassa ovat kieltäneet avointen WLAN-verkkojen liittämistä kansalliseen tutkimusverkkoinfrastruktuuriin. Käytännössä näiden maiden yliopistot ja ammattikorkeakoulut joutuvat hankkimaan erillisen yhteyden kaupalliselta operaattorilta, jos he haluavat tarjota avoimen WLAN-verkon. Näissä tapauksissa yliopistot ja ammattikorkeakoulut tarjoavat ja ylläpitävät omia tukiasemia, kontrollereita ja kytkimiä tiettyyn pisteeseen, josta liikenne siirtyy kaupallisen operaattorin vastuulle. Yksi ratkaisun seuraus on, että abuse-viestien ja viranomaispyyntöjen käsittely siirtyy ensisijaisesti kaupalliselle operaattorille.

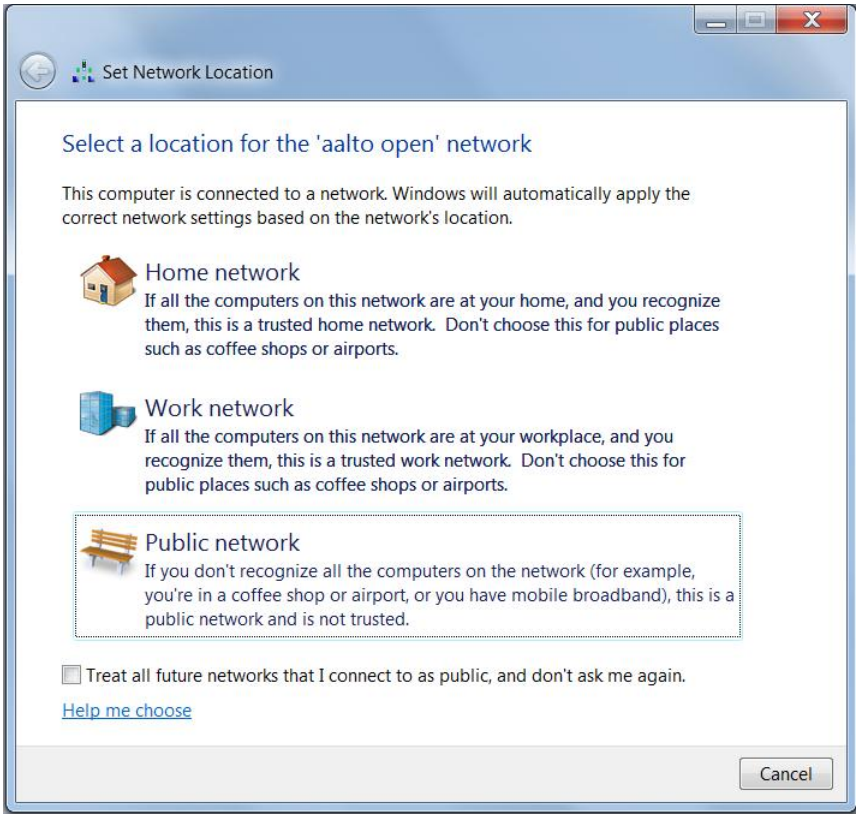
IT-hallinnon kannalta avoin WLAN-verkko tulisi ainakin erottaa loogisesti tai fyysisesti ns. tuotantoverkosta, jotta tuotantoliikenne ei häiriinny avoimen verkon käytöstä. Looginen erotus tarkoittaisi avoimelle WLAN-verkolle omaa erillistä VLAN:ia, jossa on esimerkiksi kaistankäyttörajoituksia ja erilainen politiikka avoimissa porteissa (katso lisää kappaleesta Vierailijaverkossa tarjottavat palvelut). Lisäksi IT-hallinnon tulisi jollain tasolla seurata kuka käyttää verkkoa, esim. MAC-osoitteiden perusteella.

On huomauttavaa, että käyttäjiä on varoitettava siitä, että heille tarjottu verkkoyhteys on salaamaton. Asia on käsitelty WLAN-verkot ja lainsäädäntö Parhaat käytännöt-dokumentissa [7]. Varoitus voidaan lisätä ohjesivulle, joka aukeaa selaimessa verkkoon liittymisen jälkeen tai ohjeistusta voidaan laittaa näkyville rakennusten sisäänkäyntien luo. Vähintään organisaation kotisivuilta on löydyttävä tietoa salaamattomasta WLAN-verkosta, mutta on epävarmaa riittääkö tämä lakiteknisesti.

Hyvin toteutettu ohjesivu, joka aukeaa käyttäjälle liittymisen jälkeen selaimeen, on hyvä tapa varoittaa, että kyseessä on todella avoin ja suojaamaton verkko. Hyvin tehty ohjesivu tai aloitussivu vaikeuttaa vierailijaverkon väärentämistä. Sivulle voidaan laitaa ruutu, jonka rastittamalla käyttäjä hyväksyy avoimen verkon ehdot esim.: laittoman materiaalin jako ja muu luvaton käyttö on kielletty; verkon käyttö on käyttäjän omalla vastuulla.

Avoimessa verkossa käyttäjiä voidaan myös opastaa tietoturva-asioissa mm. käyttämällä http:n sijasta https-salattuja webbisivuja. Tämä ei ole kuitenkaan riittävä varokeino liikenteen kulkiessa hyökkääjän asettaman tukiaseman läpi [2] [3]. Pääsyä käyttäjän päätelaitteeseen avoimen verkon yli voidaan rajoittaa käyttämällä palomuuria ja arvioimalla päätelaitteesta verkkoon näkyviä palveluita esim. estämällä tiedostojenjako Windowsissa (katso kuva 1). Suojaamattomaan liikennöimiseen keinot eivät kutenkaan

vaikuta. Paras suojaustapa on aina käyttää VPN-yhteyttä avoimessa verkossa [2] [3]. VPN saattaa kuitenkin hidastaa verkkoyhteyttä. Vaikka VPN on yleinen palvelu työsuhdetietokoneilla, sitä ei yleensä ole työsuhdematkapuhelimissa. VPN ei myöskään kytkeydy välittömästi päälle verkkoon liittymisen yhteydessä. Tällöin epätoivottu salaamaton liikennöinti voi tapahtua jo ennen VPN:än päälle kytkeytymistä [8].



Kuva 1. Käyttäjän kannalta avoin verkko on luokiteltava oikein, jotta mm. tiedostojenjako estetään Windowsissa.

Avoimen WLAN-verkon tarjoaminen kampuksella sisältänee enemmän uhkia käyttäjille, eli vierailijoille, kuin IT-hallinnolle. Organisaation maine saattaa kuitenkin kärsiä, jos vierailija joutuu vaikeuksiin vieraillessaan kampuksella. Viestintävirasto ei suosittele avoimia WLAN-verkkoja edes kotikäyttöön [9]. Kaiken kaikkiaan radioliikenteen salaaminen ratkaisee useimmat WLAN-verkon turvallisuusuhat.

Verkko vierailijatunnuksilla - web-autentikointi

+ Helppokäyttöinen ja toimintavarma

+ Parempi mahdollisuus määritellä kuka saa käyttää verkkoa kuin avoimessa verkossa

- Yhteys on salaamaton, joten verkon tietoturva on heikko ja tietoturva jää käyttäjän vastuulle

- On määriteltävä prosessi, jolla luodaan vierailijatunnuksia yksittäiselle vierailijalle ja tapahtumille

Web-autentikoinnissa käyttäjä ohjataan aina sisäänkirjautumissivulle verkkoon liittymisen ja selaimen avaamisen yhteydessä. Kirjautumissivulle on syötettävä käyttäjätunnus ja salasana. Monet vierailijaverkot toimivat tätä periaatetta noudattaen, eli vierailijalle luodaan tunnus käyttäjätietokantaan. Kyseistä tunnusta ja salasanaa käytetään liittyessä kampuksen vierailijaverkkoon. Esim. Helsingin yliopiston HUPnet on web-autentikointia käytettävä vierailijaverkko. Heidän tietotekniikka-asiantuntijan Mikko Laihon mukaan ratkaisuun ollaan tyytyväisiä eikä konkreettisia muutossuunnitelmia ole. HUPnetista on pääosin saatu positiivista palautetta ja suurimmat ongelmat ovat liittyneet sisäänkirjautumissivun ohjaukseen. Jos

käyttäjän selain auetessa yrittää ladata https-sivua, sisäänkirjautumissivulle ohjaaminen epäonnistuu. Oletussivun käyttäessä http:tä ongelmia ei ole.

Autentikoinnin onnistuttua liikennöinti tapahtuu samalla tavalla kuin avoimessa verkossa, Web-autentikointia koskevat siis myös samat uhat kuin avoimessa verkossa. Käyttäjän tekemisiä verkossa voidaan tarkistaa (snooping/sniffing/sidejacking). Hyökkääjä voi myös tässä tapauksessa pystyttää tukiaseman ja päästä käyttäjän verkkoon ilman sisäänkirjautumissivua tai esittämällä käyttäjälle väärennetyn sisäänkirjautumissivun (evil twin/man-in-the-middle). IT-hallinnolle web-autentikointiin perustuva verkko tarjoaa kuitenkin avointa verkkoa parempaa mahdollisuutta käyttäjien hallintaan. Käyttäjien kirjautumisen tietoturvaa voidaan parantaa HTTP Strict Transport Security-mekanismilla.

Käyttäjän kannalta myös samat vastatoimet kuin avoimen verkon tapauksessa pätevät. Eli paras suoja saadaan VPN:n avulla. On kuitenkin muistettava, että käyttäjäkokemus saattaa kärsiä, koska ennen kuin VPN:ää voidaan käyttää, on vierailijan avattava selain ja syötettävä käyttäjätunnus ja salasana. Vasta sen jälkeen VPN-tunneli muodostetaan. Organisaation omat käyttäjät voidaan sallia viestittämään organisaation VPN-palvelimen kanssa ilman web-autentikointia, jos he käyttävät samaa SSID:tä kuin vierailijat.

Prosessi

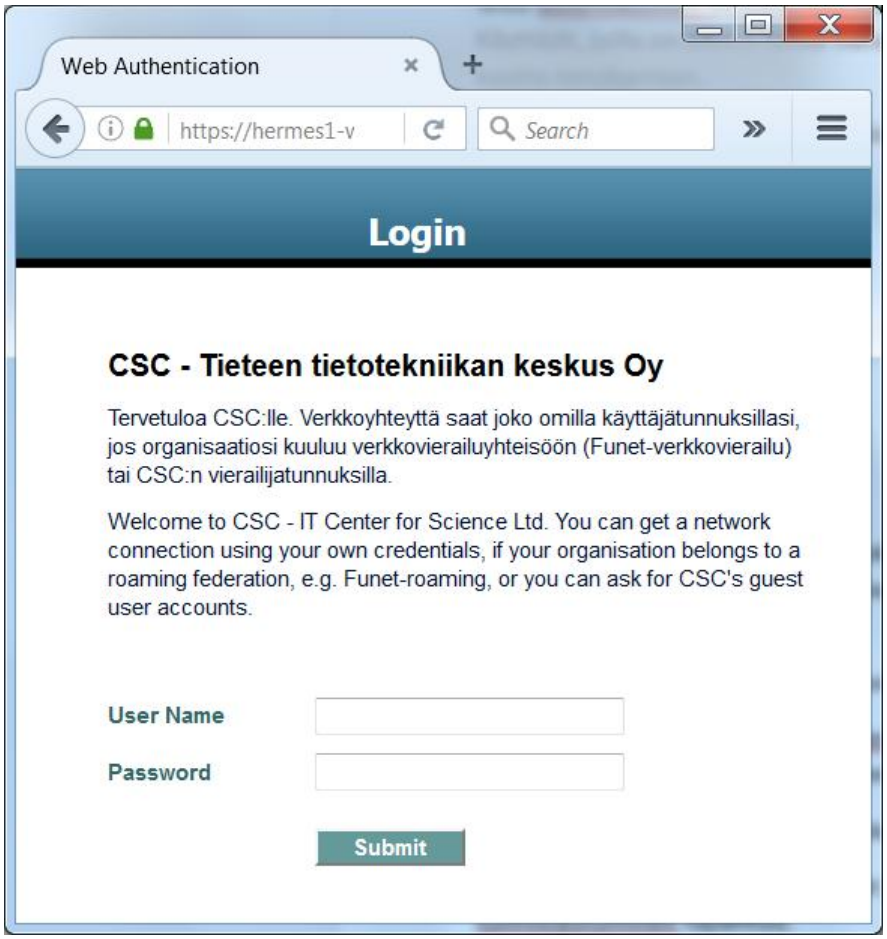
Ennen vierailijaverkon käyttöönottoa on mietittävä, miten tunnukset luodaan ja jaetaan sekä miten pitkään ne ovat voimassa. Tunnuksen voi luoda vain helpdesk/aulapalvelut tai organisaatiossa työskentelevät. Helsingin yliopistolla kaikki työntekijät voivat luoda tunnuksia ja ne ovat voimassa yhden päivän tai yhden viikon ensimmäisestä käyttökerrasta eteenpäin [10]. Tunnus voidaan luoda etukäteen ja sillä saa verkkoyhteyden sekä pääsyn kirjastotietokantoihin. Mikko Laihon mukaan käytäntö on toimiva eikä muutoksia ole pohdittu. Etenkin se, että tunnuksia voivat luoda kaikki työntekijät, on osoittanut toimivaksi järjestelyksi. CSC:lläkin on web-autentikointiin perustuva vierailijaverkko, johon vain tietohallinto ja aulapalvelut voivat luoda tunnuksia. Koulutustapahtumien yhteydessä vierailijatunnus printataan nimilapun yhteyteen. Tunnusten luominen on kuitenkin koettu jossain organisaatiossa aikaa vieväksi varsinkin muiden toimien ohessa.

Teknisesti vierailijatunnuksen hankkiminen tekstiviestin avulla on myös mahdollista. Voidaan luoda prosessi, jossa käyttäjä rekisteröi itse itsensä ja saa käyttäjätunnuksensa ja salasanansa tekstiviestillä. Ainakin Aruban Clearpass mahdollistaa tällaisen prosessin luomisen.

Tekninen ratkaisu ja vierailijatietokanta

Web-autentikointiin perustuvalle verkolle tarvitaan käyttäjätietokanta, jonne vierailijatunnukset luodaan. Käyttäjät, joilla on oikeus luoda vierailijatunnuksia, luovat tunnukset yleensä graafisen käyttöliittymän kautta tietokantaan.

Lisäksi tarvitaan RADIUS-palvelin, joka välittää autentikointipyynnöt tukiasemilta WLAN-kontrollerin kautta käyttäjätietokantaan. RADIUS-palvelin voi olla sama kuin esim. eduroamissa käytetty RADIUS-palvelin. Tämän lisäksi tarvitaan myös sisäänkirjautumissivu, josta on esimerkki kuvassa 2.



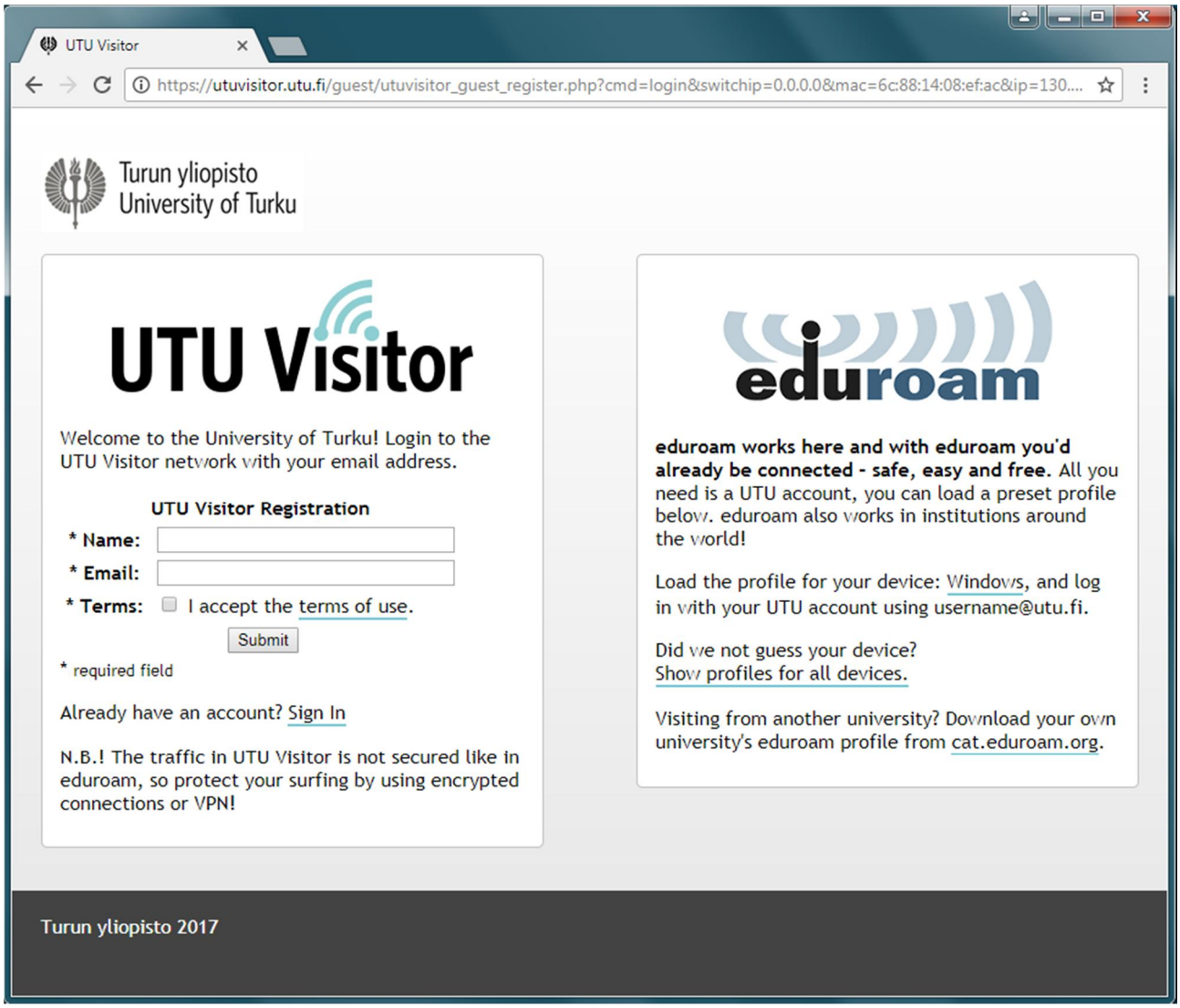
Kuva 2. Esimerkki web-autentikointiin perustuvan verkon sisäänkirjautumissivusta.

Kevyempi web-autentikointi

Turun yliopistolla on UTU Visitor – niminen vierailijaverkko, joka on avoimen ja web-autentikointiin perustuvan verkon välimuoto eli käytetään sisäänkirjautumissivua, missä käyttäjältä pyydetään nimi ja sähköpostiosoite, mutta antamia tietoja ei mitenkään tarkisteta. Luottamukseen perustuva itserekisteröinti on poistanut kokonaan yhden työsaran asiakaspalvelulta ja muilta yliopistolaisilta, kun verkkoon pääsee helpommin, eikä esim. tapahtumia varten tarvitse luoda vierailijatunnuksia. Turun yliopiston järjestelmäarkitehdin Tuukka Vainion mukaan menetelmä on ollut toimiva. Käyttäjien verifikointia, esim. salasanan toimitus tekstiviestillä, selvitettiin uudistuksessa ja siihen palataan tarvittaessa.

Tuukka Vainio painottaa, että UTU Visitor on tarkoitettu vain vierailijoille, joten verkkoon ei kirjauduta yliopiston tunnuksilla. Tämä auttaa jossain määrin pienentämään riskiä yliopiston tunnuksien kaappaamisesta evil twin -hyökkäyksellä, mikäli käyttäjät ymmärtävät yliopiston tunnusten kyselyn olevan poikkeuksellista.

UTU Visitorin kirjautumissivulla käyttäjille tiedotetaan avoimen verkon tietoturvasta ja kehotetaan salaamaan liikenteensä tai käyttämään VPN-yhteyksiä, katso kuva 3. Samalla sivulla tarjotaan myös Turun yliopiston käyttäjille eduroam-verkon konfigurointiapua, koska eduroam on web-autentikointia tietoturvallisempi ja sitä suositellaan käytettäväksi aina kun mahdollista, katso lukua 802.1x autentikointi ja WPA2/AES-salaus (eduroam).

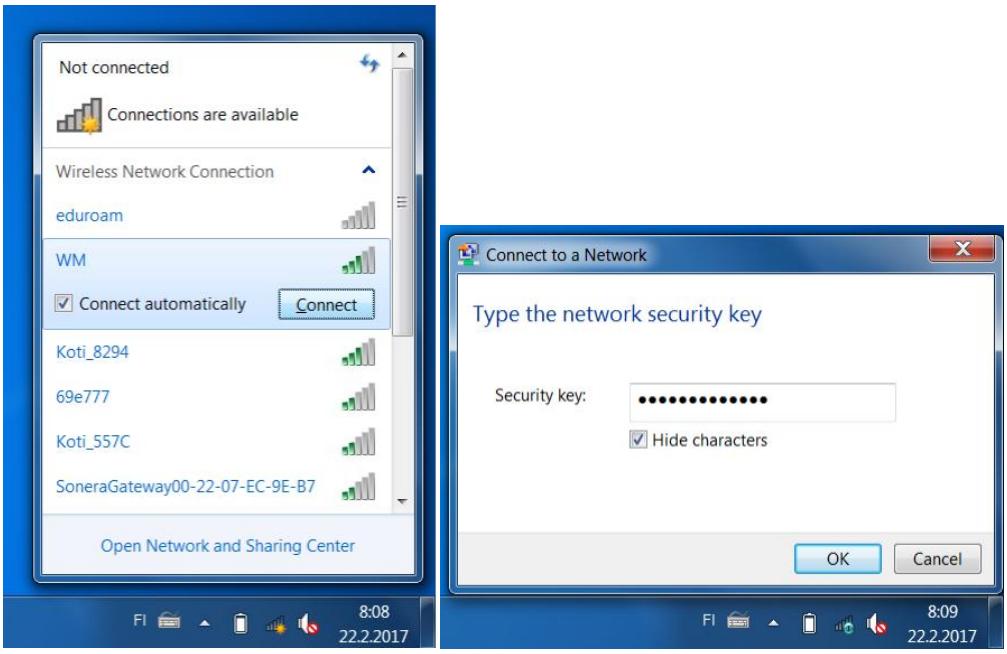


Kuva 3. Turun yliopiston vierailijaverkon sisäänkirjautumissivu, missä tiedotetaan tietoturvasta ja mistä tarjotaan yliopiston omille käyttäjille eduroam-konfigurointiapua.

Henkilökohtainen jaettu salaisuus - Private Pre Shared Key

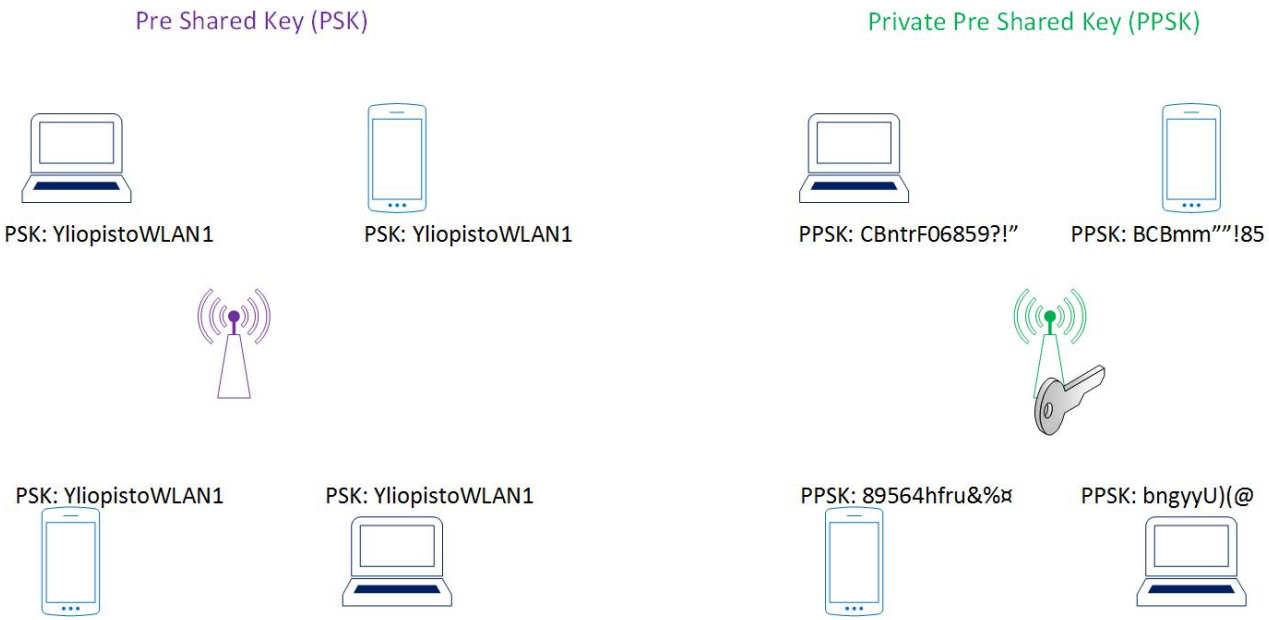
+ Tarjoaa hyvää tietoturvaa olemalla samalla helppokäyttöinen ja helposti toteutettavissa
- Ei tuettuna kaikissa tukiasemamalleissa

Kotikäytössä oleva WLAN-verkko suojataan yleensä jaetulla salaisuudella, eli Pre Shared Key (PSK)-menetelmällä. Verkkoon liitytään syöttämällä päätelaitteeseen jaettu avain, joka on sama kaikilla käyttäjillä, katso kuva 4. Menetelmä on tietoturvan kannalta heikko, koska liikenteen suojauksessa käytetään samaa avainta kaikille käyttäjille. Myös pääsynhallinta on hankala, koska käyttömahdollisuuden poistaminen yhdeltä käyttäjältä edellyttää jaetun avaimen muuttamista kaikille käyttäjille.



Kuva 4. Jaetun salaisuuden syöttäminen päätelaitteeseen.

Menetelmästä on olemassa myös kehittyneempi versio nimeltään Private Pre Shared Key (PPSK), jossa jokaiselle käyttäjälle jaetaan henkilökohtainen avain, jolla hän liittyy verkkoon [11] kuten kuvassa 5. Käyttäjän radioliikennettä siis suojataan henkilökohtaisen avaimen avulla. Tietoturva on hyvä, vaikka 802.1x autentikointi ja WPA2/AES-salaus tarjoaakin vielä paremman tietoturvan, koska jälkimmäisessä tapauksessa avaimet luodaan autentikoinnin yhteydessä ja vaihdetaan usein [12]. IT-hallinnolle menetelmä tarjoaa hyvää pääsynhallintaa ilman RADIUS-palvelinta tai suplikanttien konfigurointia. IT-hallinto voi haluttaessaan liittää henkilökohtaisen avaimen käyttäjän identiteettiin tai käytettyyn MAC-osoitteeseen ja määritellä käyttäjien liikenteen tietylle VLANille. Lisäksi yksittäinen käyttäjä voidaan poistaa verkosta poistamalla vain hänen avaimensa liikennöintimahdollisuus, eikö tällöin tarvitse koskea muiden käyttäjien avaimiin.



Kuva 5. Pre Shared Key (PSK) ja Private Pre Shared Key (PPSK) .

Vierailijaverkkoon PPSK soveltuu erinomaisesti, koska se tarjoaa helposti järjestettävän ja ylläpidettävän, tietoturvallisen WLAN-verkon, joka on käyttäjän kannalta jopa helppokäyttöisempi kuin web-autentikointi. Tällä hetkellä vain Aerohive, Ruckus ja Xirrus tarjoavat PPSK-menetelmää laitteissaan. Cisco:lla on beta-versio menetelmästä, mutta HP ja Aruba eivät ole vielä tehneet päätöksiä PPSK:n suhteen.

Myös esineiden internettiin (Internet of Things, IoT) PPSK tarjoaa potentiaalisia mahdollisuuksia, koska 802.1x-autentikointi on tähän tarkoitukseen hyvin raskas. IoT laitteet voisivat autentikoitua PPSK:lla.

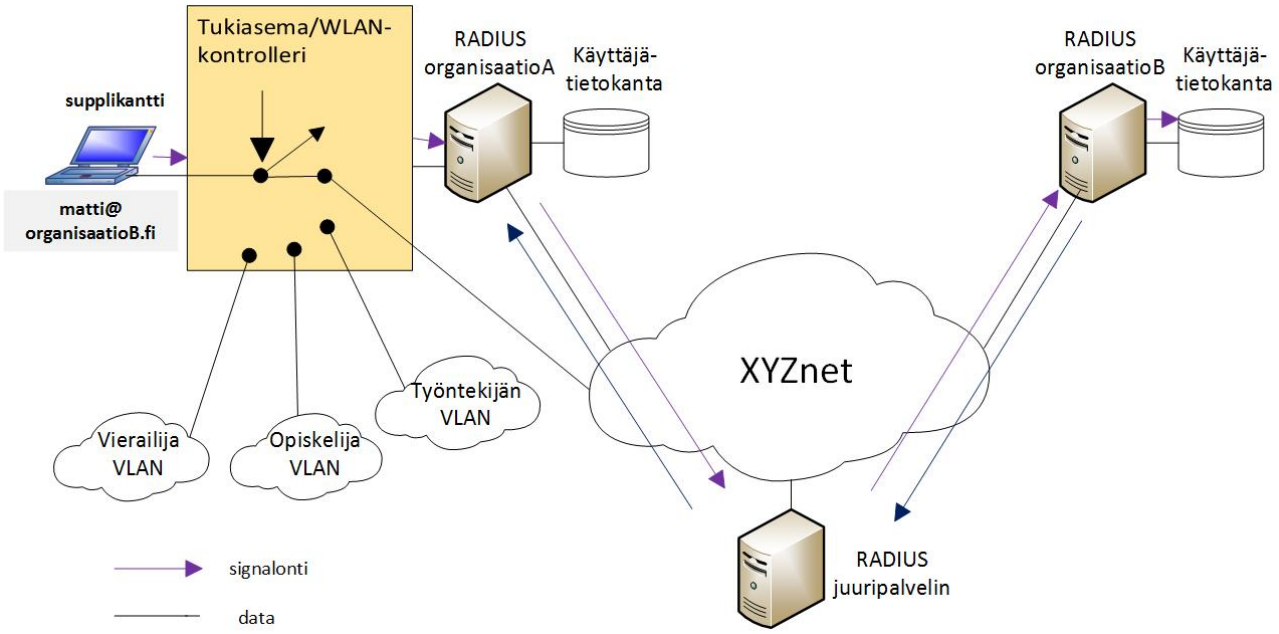
802.1x autentikointi ja WPA2/AES-salaus (eduroam)

+ Erittäin tietoturvallinen
+ Käyttäjien automaattinen liittyminen verkkoon ensimmäisen liittymisen jälkeen

- Konfigurointiongelmia esiintyy varsinkin, jos ei hyödynnetä suplikantin/päätelaiteen automaattista provisiointityökalua (esim. CAT eduroamissa)
- rajattu käyttäjäkunta (eduroam-vierailijaverkkopalvelu on vain yliopistojen, ammattikorkeakoulujen ja tutkimuslaitosten henkilöstölle)

Tietoturvallisin WLAN-verkko saadaan aikaan käyttämällä 802.1x autentikointia ja WPA2/AES-salausta. Yhteys on kryptattu, jolloin liikenteen salakuuntelu ei ole mahdollista. Verkkoon liitytään päätelaiteessa olevan ohjelman ts. suplikantin avulla.

eduroam on WLAN-verkkovierailupalvelu, jossa käyttäjät voivat kirjautua omilla tutuilla käyttäjätunnuksillaan WLAN-vierailijaverkkoon vieraillessaan minkä tahansa eduroam-yhteisöön liittyneen organisaation kuuluvuusalueella [13]. eduroamiin liitetyn WLAN-verkon SSID:n on oltava nimeltään eduroam. Tämän lisäksi WLAN-verkon on käytettävä 802.1x autentikointia ja WPA2/AES-salausta. Käyttäjän autentikointi eduroamissa esitetään kuvassa 6. eduroam tarjoaa suplikantin konfiguroimiseen apua provisiointityökalun CAT:in (Configuration Automation Tool) [14] avulla. IT-hallinto syöttää työkaluun organisaatiokohtaiset tiedot, kuten autentikointipalvelimen nimi ja varmenne, ja käyttäjä lataa itselleen exe-tiedoston, jonka ajamalla suplikantti konfiguroidaan oikein.



Kuva 6. Autentikointi eduroamissa 802.1x-tekniikkaa soveltaen. Autentikointipyyntö lähetetään RADIUS-hierarkiassa käyttäjän kotiorganisaatioon, jossa käyttäjätunnus ja salasana verrataan tietokantaan tallennettuihin tietoihin.

Yliopistot ja ammattikorkeakoulut ympäri Suomea ja maailmaa ovat pitkään tarjonneet eduroamia sekä omille käyttäjilleen kotikampuksella, että muualta korkeakoulumaailmalta saapuneille vierailijoilleen. Käyttötukea tarjotaan vain oman organisaation käyttäjille. Käyttäjät pystyvät kirjautumaan automattisesti eduroam-verkkoon myös kotiorganisaation ulkopuolella (esim. vierailtaessa toisen paikkakunnan kampuksella), kunhan ovat ensin kertaalleen kirjautuneet eduroam-verkkoon omassa organisaatiossa. Mahdollisissa ongelmatilanteissa käyttäjä on aina ensin yhteydessä kotiorganisaatioonsa eikä esim. vierailtavan organisaation palvelupisteeseen.

IT-hallinnon on hyvä tietää, että kaikki verkon käyttäjät tunnistetaan ennen kuin he päästetään verkkoon. Kunhan käyttäjän päätelaitteeseen on määritelty kotiorganisaation autentikointipalvelin varmennetietoineen, autentikointipyyntö ei lähetetä, vaikka olisi pystytetty liikenteen häiritsemiseksi tarkoitettu tukiasema eduroam-SSID:llä. Kun verkossa käytetään 802.1x autentikointia ja WPA2/AES-salausta, poistuu mm. Avoin verkko-kappaleessa esitetyt tietoturvauhat. Tietoturva eduroam-verkossa edellyttää kuitenkin sen, että suplikantti on konfiguroitu oikein. Siihen on määriteltävä oikea varmennemyöntäjä sekä kotiorganisaation palvelimen nimi [15].

IT-hallinto on autettava omia käyttäjiään konfiguroimaan suplikanttinsa oikein. Sitä voidaan tehdä ohjaamalla käyttäjät CAT-sivulle [15] tai kuten Turun yliopistossa tarjoamalla tarvittavat exe-tiedostot vierailijaverkon kirjautumissivulla, katso kuva 3. Käyttäjäagentti tunnistaa käyttöjärjestelmän ja IT-hallinnon CAT:in avulla luotu sopiva exe-tiedosto on käyttäjän ladattavissa. Tiedosto poistaa tunnettujen verkkojen listalta vierailijaverkon SSID:n ajon jälkeen, jotta käyttäjä rupeaisi käyttää tietoturvallista eduroamia.

eduroamissa käyttäjäkunta on etukäteen rajattu eduroamin politiikan mukaan [15] koskemaan yliopisto- ja tutkimusmaailmaa, joka on tietyissä tapauksissa koettu ongelmaksi. Kampuksilla kuitenkin vierailee myös muita tahoja kuten yritysten edustajia ja koulutukseen osallistujia, joille eduroamia ei tällä hetkellä tarjota.

Funetin hollantilainen sisarorganisaatio SURFnet on ratkaissut ongelman palvelullaan eduroam Visitor Access (eduroam-yhteys vierailijoille), jonka avulla organisaatio voi luoda väliaikaisia eduroam-tunnuksia vierailijoilleen. Kampus, joka haluaa tarjota kaikille vierailijoilleen tietoturvallista eduroam-verkkoa, voi luoda erilliseen käyttäjätietokantaan määräaikaisia vierailijatunnuksia, jotka välitetään vierailijoille paperilla, sähköpostitse tai SMS-viestinä. Vierailija liittyy eduroamiin samalla tavalla kuin omat käyttäjät. Vierailijan eduroam-tunnus toimii ainoastaan myönnetyn organisaation eduroam-verkossa eli sillä ei pysty roamaamaan. On muistettava, että tunnus on väliaikainen ja tapauksia, jossa vierailijan päätelaite yrittää autentikoitua vanhentuneella tunnuksella, ovat mahdollisia. eduroam Visitor Access-palvelun avulla pärjättäisiin yhdellä ja ainoalla SSID:llä – eduroam – ,jonka kautta kaikki käyttäjät autentikoitaisiin suojattuun yhteyteen. eduroam Visitor Access-palvelua ei vielä tarjota Funetissa, mutta sen käyttöönottoa pohditaan tulevaisuudessa riittävän suuren asiakaskiinnostusten löytyessä.

Useampi vierailijaverkko

Kontrolleripohjaiselle verkolle on helppo määrittää useampi SSID ja voitaisiin haluttaessa määritellä kontrollerin tukema maksimimäärä SSID:tä omille käyttäjille ja vierailijoille. Esimeksiksi voitaisiin haluta tarjota eduroamin lisäksi ”staff” ja ”student”-verkkoja. On kuitenkin huomioitava, että jokainen SSID aiheuttaa verkossa ylimääräistä liikennöintiä ja itse käyttäjien tiedonsiirtoon jää vähemmän resursseja [16]. SSID:tä mainostetaan merkkikehyksissä (beacon frame), jotka lähetetään oletusarvoisesti noin 10 kertaa sekunnissa. Jos lisätään verkkoon toinen SSID tarkoittaa se, että merkkikehyksiä lähetetään noin 20 kertaa sekunnissa. Jokainen SSID mainostuu eri merkkikehyksessä ja tästä syystä SSID:tä on lisättävä verkkoon vain perustelluista syystä. Onkin suositeltavaa, ettei WLAN-verkossa käytettäisi useita SSID:tä. Monesti enemmän kuin kolme SSID:tä on käytön kannalta turhaa [17] [18].

Vierailijaverkon palvelut

Kun pääsy vierailijoille tarkoitetulle WLAN-verkolle on määritelty, on päätettävä, miten vierailijoiden liikenne hoidetaan tukiasemista eteenpäin. Vierailijoille tarkoitetun WLAN-verkon liikenne voidaan haluttaessa erottaa lähiverkossa muusta liikenteestä asettamalla se eri aliverkolle, Virtual Local Area Network: ille (VLAN). Tälle VLANille voidaan määritellä, mitkä palvelut vierailijoille tarjotaan.

Vierailijaverkon palvelutarjontaa on pohdittu eduroam-yhteisön piirissä ja sen politiikka-dokumentissa [15] on määritelty vaatimuksia vierailijaverkolle. Vaikka vaatimukset koskevat vain eduroam-verkkoa, niitä on syytä hyödyntää kaikissa Funet-organisaatioiden vierailijaverkoissa. Kyseisen politiikan mukaisesti liikenteelle on avattava taulukossa 2 esitetyt portit.

Taulukko 2. eduroam-politiikan mukaan vierailijoille avattavat portit.

Palvelu	Protokolla/Portti	Suunta
Standard IPSec VPN	IP protocol 50 (ESP) IP protocol 51 (AH) UDP port 500 (IKE)	saapuva ja lähtevä saapuva ja lähtevä lähtevä
OpenVPN 2.0	UDP port 1194	saapuva ja lähtevä
IPv6 Tunnel broker service	IP protocol 41	saapuva ja lähtevä
IPSec NAT - Traversal	UDP/4500	saapuva ja lähtevä
Cisco IPSec VPN over TCP	TCP/10000	lähtevä
PPTP VPN	IP protocol 47 (GRE) TCP port 1723	saapuva ja lähtevä lähtevä
SSH	TCP port 22	lähtevä
HTTP	TCP port 80 TCP port 443 TCP port 3128 TCP port 8080	lähtevä lähtevä lähtevä lähtevä
Sähköpostin lähettäminen	TCP port 465 TCP port 587	lähtevä lähtevä
Sähköpostin saapuminen	TCP port 143 TCP port 993 TCP port 110 TCP port 995	lähtevä lähtevä lähtevä lähtevä
FTP (passiivinen)	TCP port 21	lähtevä

Taulukossa on esitetty lähtevälle liikenteelle minimivaatimukset. Politiikan mukaan kaikki lähtevä verkkoliikenne olisi hyvä sallia, mutta jos sitä rajataan, rajattujen protokollien määrä on oltava niin pieni kuin mahdollista.

Turun yliopiston UTU Visitor – nimisessä vierailijaverkossa käyttäjiltä sallittu liikenne ulospäin on rajattu muutamaan peruspalveluun: Web-selailuun (käytännössä taulukon http-portit), salattuun sähköpostiin (IMAPS, POP3S, SMTP Submission portilla 587 ja vanha SMTPS portilla 465) ja SSH-protokollaan. Kaista on rajattu murto-osaan tukiaseman kapasiteetista, jotta mahdolliset ongelmat vierailijaverkossa eivät haittaisi juurikaan muita SSID:itä. Menetelmä rajoittanee mahdollisia ongelmia eikä Turun yliopistolle ole tullut abuse-ilmoituksia juurikaan, Tuukka Vainion mukaan.

Turun yliopiston WLAN-verkossa olevat laitteet saavat julkisen IPv4-osoitteen. UTU Visitor-vierailijaverkon käyttäjät sekä ulkopuoliset eduroam-käyttäjät erotetaan omiin aliverkkoihinsa. Yliopiston omat käyttäjät eduroam-verkossa tunnistetaan autentikointivaiheessa käyttäjätunnuksessa olevan domain-osan

perusteella (@utu.fi) ja he pääsevät käyttämään aliverkkoa missä on eri palomuuraussääntöjä ja IP-pohjaisia käyttörajoituksia. Samoin henkilökunnan käyttämä UTU Staff – SSID:llä oleva WLAN-verkko käsitellään erikseen.

Vierailijaverkkojen nykytila Funet-yhteisössä

Funet toteutti avoimiin kysymyksiin perustuvan sähköpostikyselyn MobileFunet -yhteisölle vierailijaverkkoihin liittyen marraskuussa 2015. Kyselyssä kartoitettiin nykytilaa sekä selvitettiin tulevaisuuden näkymiä keskittyen pelkästään langattomiin vierailijaverkkoihin. Jokainen kyselyyn vastannut organisaatio mainosti eduroamin lisäksi myös muita langattomia vierailijaverkkoja. Näiden ratkaisujen toteutustavat ja tekniset ratkaisut vaihtelivat organisaatioittain täysin avoimesta kirjautumista vaativaan ratkaisuun. Joissain organisaatioissa oli havaittu painetta täysin avoimiin WLAN-vierailijaverkkoihin kirjautumista vaativien sijaan. Suurin osa vastaajista oli kiinnostunut yhteisestä kansallisesta/kansainvälisestä langattomasta vierailijaverkosta ei-eduroam vierailijoille.

Yhteenveto ja ehdotukset

Haasteena vierailijaverkon rakentamiselle on, että helppokäyttöisyys ja tietoturvallisuus eivät nykytekniikoilla ole helposti yhdistettävissä. Kun halutaan helppoa käytettävyyttä, joudutaan usein karsimaan tietoturvasta. Tietoturvan lisääminen taas aiheuttaa mahdollisesti käytettävyyden heikkenemistä joko loppukäyttäjälle tai lisätyötä IT-hallinnolle.

Jos organisaatio haluaa tarjota avointa verkkoa vierailijoille, on oltava tietoinen niihin liittyvistä vaaroista. Salakuuntelu, sekä liikenteen kaappaaminen, muuttaminen tai uudelleenohjaaminen on mahdollista. Web-autentikointiin perustuvassa verkossa tiedetään, kuka on päästetty verkkoon, mutta tietoturvauhat ovat samat kuin avoimessa verkossa. 802.1x-autentikointia ja WPA2/AES-salausta käytettävissä verkoissa, kuten eduroamissa käyttäjien hallinta on kunnossa ja liikenne on salattua eikä täten aiemmin mainittuja tietoturvauhkia pääse muodostumaan. Myös henkilökohtainen jaettu salaisuus tarjoaa WLAN-verkossa suhteellisen hyvän tietoturvan.

IT-hallinnon näkökulmasta täysin avoimeen verkkoon liittyy se riski, että väärinkäytöstapauksissa vain laite voidaan selvittää MAC-osoitteen perusteella – ei käyttäjää. Web-autentikointiin perustuva verkko on IT-hallinnon kannalta hieman suojatumpi koska kuka tahansa ei päästetä verkkoon.

Käyttäjän kannalta riski on taas suurempi. Käyttäjä ei välttämättä tiedä, miten hänen pitäisi suojautua erilaisilta verkkouhilta avoimissa tai web-autentikointiin perustuvissa verkoissa. Eli käyttäjän kannalta eduroam tai vastaava ratkaisu on tietoturvaltaan paras ratkaisu. Tulevaisuudessa kaikille vierailijoille voitaisiin tarjota samanlaista tietoturvaa ja käytettävyyttä eduroam Visitor Access-palvelun avulla. Henkilökohtainen jaettu salaisuus tarjoaa myös hyviä mahdollisuuksia vierailijaverkoksi. Tällä hetkellä menetelmän haasteeksi muodostuu, ettei se ole kovin hyvin tuettu laitevalmistajien keskuudessa.

Viiteluettelo

[1] ”https://www.ubnt.com/,” [Online].

[2] ”http://www.privatewifi.com/wp-content/uploads/2015/01/PWF_whitepaper_v6.pdf,” [Online].

[3] ”http://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-e

[4] ”http://www.digitaltrends.com/mobile/how-dangerous-is-public-wi-fi/,” [Online].

[5] ”https://www.wifipineapple.com/,” [Online].

[6] ”https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409171602.html,” [Online].

[7] ” https://wiki.eduuni.fi/pages/viewpage.action?pageId=23691386,” [Online].

[8] ”http://arstechnica.com/security/2015/06/even-with-a-vpn-open-wi-fi-exposes-users/,” [Online].

[9] ”https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahive
” [Online].

[10] ”https://helpdesk.it.helsinki.fi/ohjeet/kirjautuminen-ja-yhteydet/kayttajatunnus/hupnet-tunnus-vierailijoille,” [On

[11] ”http://www.aerohive.com/solutions/technology/ppsk.html,” [Online].

[12] ”http://www.aerohiveworks.com/Authentication.asp,” [Online].

[13] ”https://monitor.eduroam.org/map_service_loc.php,” [Online].

[14] ”https://cat.eduroam.org/,” [Online].

[15] ”https://www.eduroam.org/wp-content/uploads/2016/05/GN3-12-192_eduroam-policy-service-definition_ver28_

[16] ”http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html,” [Online].

[17] ”https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Multi-SSID_Deployment_Consideration

[18] ”http://www.computerworld.com/article/2467807/network-hardware-solutions/3-dumb-mistakes-network-admin
part-1-.html,” [Online].