Tampereen ammattikorkeakoulu

Langattoman verkon tietoturva yrityksessä

Jere-Pekka Pajuranta

OPINNÄYTETYÖ
Toukokuu 2019

Tieto- ja viestintätekniikan koulutus
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan koulutus
Tietoliikennetekniikka ja tietoverkot

PAJURANTA, JERE-PEKKA:
Langattoman verkon tietoturva yrityksessä

Opinnäytetyö 31 sivua, joista liitteitä 1 sivu
Toukokuu 2019

Opinnäytetyön tarkoituksena oli kerätä informaatiota langattoman verkon tietoturvasta erityisesti yrityksen näkökulmasta. Tavoitteena oli kerätä tietoa siten, että sitä voidaan hyödyntää mahdollisimman turvallisen yritysverkon toteuttamisessa.

Langattoman verkon tietoturvan parantamiseksi on olemassa erilaisia salausmenetelmiä ja työkaluja. Ensimmäisenä salausmenetelmänä kehitettiin WEP (Wired Equivalent Privacy), jonka päätavoitteita olivat luottamuksellisuus, pääsyn hallinta ja datan eheys. Vuonna 2001 WEP onnistuttiin kuitenkin murtamaan, minkä vuoksi julkaistiin uusi salausmenetelmä WPA (Wi-Fi Protected Access). Tavoitteena oli korjata WEP-salauksessa havaitut haavoittuvuudet. Uusia ominaisuuksia olivat vahvemmat salausavaimet, eri avaimen luonti kaikille käyttäjille ja uusi paranneltu tarkistussumma. Tämän jälkeen WPA-salauksesta on kehitetty myös paranneltu versio WPA2. WPA ja WPA2 on havaittu myös haavoittuvaisiksi. Tästä syystä WPA3 on jo julkaistu, mutta se ei ole vielä käytössä kovinkaan yleisesti.

Fortiauthenticator on työkalu, joka tarjoaa erilaisia autentikointiin liittyviä ominaisuuksia. Kyseisellä työkalulla voidaan toteuttaa yritykselle vierailijaverkko siten, että vierailijalla on useita eri kirjautumistapoja verkkoon. Fortiauthenticatorin avulla voidaan myös toteuttaa käyttäjille kaksivaiheinen autentikointi verkossa, jolloin kirjautuminen ei ole yhden salasanan varassa. Lisäksi Fortiauthenticator tarjoaa käyttäjätietokannan, jonka avulla pystytään hallitsemaan verkon käyttäjiä. Fortiauthenticator mahdollistaa myös SSO:n (Single Sign-On) käytön, jolloin verkon käyttäjän ei tarvitse syöttää kirjautumistietoja useita kertoja.

Langattomaan lähiverkkoon kohdistuvia hyökkäysmenetelmiä on yleisesti tiedossa useita. Yhtenä hyökkäysmenetelmänä on luvaton tukiasema. Luvaton tukiasema on lähiverkossa oleva langatonta verkkoa jakava laite, joka ei ole verkon ylläpitäjän hallittavissa. Hyökkääjä voi päästä käsiksi lähiverkkoon käyttäen kyseistä tukiasemaa. Toisena yleisenä hyökkäysmuotona on palvelunestohyökkäys. Palvelunestohyökkäyksen ideana on toteuttaa hyökkäys verkkoa kohtaan siten, että verkossa kommunikointi on mahdotonta. Verkkoa vastaan voidaan toteuttaa myös Man-in-the-middle-hyökkäys, jossa hyökkääjä asettuu laitteiden väliin. Tällöin hyökkääjä pystyy muokkaamaan tai kaappaamaan laitteiden välistä liikennettä.

Asiasanat: tietoturva, langaton verkko, salausmenetelmä, fortiauthenticator

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

PAJURANTA, JERE-PEKKA:
Wireless Network Security in Company Network

Bachelor's thesis 31 pages, appendices 1 page
May 2019

The purpose of this thesis was to gather information about wireless network security, especially from a business perspective. Information was collected from literature and articles. Information was also obtained from a project carried out by ICT Elmo Oy. The goal was to implement a secure business network.

There are various encryption methods for a wireless network. WEP was the first to be developed and it is the most basic encryption method. WPA and WPA2 was developed after the weaknesses of the WEP was discovered in 2001. WPA3 was also developed to improve WPA and WPA2.

Fortiauthenticator is a tool that offers various authentication features. The tool can implement a visitor network in which the user has several ways to log in. Fortiauthenticator can also be used to enable two-factor authentication for network users. In addition, Fortiauthenticator provides a user database to manage network users.

There are several different ways to attack a wireless local area network. One way is to use rogue access point. Rogue access point is a device on the network that the administrator can not control. The attacker can take advantage of this device and access the local area network. The attack can also be implemented by running down the network. That kind of attack is called denial of service attack. During this attack, communication on the network does not work. An attacker can also settle between two devices, which is called Man-in-the-middle attack. In this case, the attacker can collect or edit traffic between the devices.

The result of the project shows that company has several security threads. The network administrator must take care to update the encryption methods. The administrator must also know as more about network users. Poor security can lead to leakage of corporate secret information.

Key words: security, wireless network, fortiauthenticator, encryption methods

SISÄLLYS

ERITYISSANASTO

CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, salausprotokolla
DNS	Domain Name System, nimipalvelujärjestelmä
EAP	Extensible Authentication Protocol, käyttäjien tunnistusprotokolla
GTK	Group Temporal Key, väliaikainen avain. Käytetään tukiaseman ja työaseminen broadcast-liikenteen salaamiseen
HTTP	Hypertext Transfer Protocol, hypertekstin siirtoprotokolla
ICMP	Internet Control Message Protocol, TCP/IP-pinon kontrolliprotokolla
ICV	Integrity Check Value, tarkistussumma
IP	Internet Protocol, TCP/IP-verkkokerroksen protokolla. Käytetään verkkosovittimien yksilöimiseen Internetissä
IV	Initialization Vector, WEP-salauksessa käytettävä alustusvektori
KSA	Key-Scheduling Algorithm, WEP-salauksessa käytettävä avainten muodostus -algroritmi
MAC	Media Access Control, ethernet-verkossa verkkosovittimen yksilöivä osoite
MIC	Message Integrity Code, tarkistussumma. Käytetään datan eheyden tarkistamiseen
PMK	Pairwise Master Key, salausavain
PSK	Pre-Shared Key, ennalta määritelty salasana WLAN-verkkoon kirjauduttaessa
PTK	Pairwise Transient Key, tukiaseman ja käyttäjän välisen liikenteen salaamiseen ja purkamiseen käytetty avain
RC4	Ron’s Code 4, salausalgoritmi
SSID	Service Set Identifier, langattoman lähiverkon verkkotunnus

SSO	Single Sign-On, kertakirjautuminen
TCP	Transmission Control Protocol, erilaisten tietoliikenne-protokollien yhdistelmä
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla
WEP	Wired Equivalent Privacy, salausmenetelmä
Wi-Fi	Wi-Fi Alliancen jäsenten käyttämä määritellyn laatutason symboli WLAN-tuotteissa
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, salausprotokolla

1 JOHDANTO

Langattomien verkkojen käyttö yritysten verkoissa on kasvanut langallisten verkkojen epäkäytännöllisyyden vuoksi. Langattoman verkon käytössä on kuitenkin useita tekijöitä, joista verkon ylläpitäjän pitää olla tietoinen, mikäli verkko halutaan pitää turvallisena.

Tässä opinnäytetyössä käsitellään erilaisia langattoman verkon salausmenetelmiä ja niiden ominaisuuksia, Fortiauthenticator-työkalun käyttöä osana verkkoa ja tutustutaan erilaisiin hyökkäystapoihin, joita verkkoon voi kohdistua.

ICT Elmo Oy:lle toteutettiin projekti, jonka yhteydessä otettiin käyttöön Fortiauthenticator. Se sisältää erilaisia käyttäjän tunnistukseen liittyviä ominaisuuksia, kuten vierailijaverkon käyttäjien tunnistus, monivaiheinen tunnistautuminen ja verkon käyttäjien hallinta.

Työn tärkeimpänä tavoitteena on saada lisää tietoa langattoman verkon tietoturvasta erityisesti yritysten näkökulmasta. Kattava tietoisuus langattoman verkon uhkatekijöistä on tärkeää yritykselle, mikäli yrityksen arkaluontoinen informaatio halutaan pitää turvassa.

2 SALAUSMENETELMÄT

Langattoman verkon liikenteen salaamiseen on kehitetty erilaisia salausmenetelmiä, kuten esimerkiksi WEP (Wired Equivalent Privacy). WEP:n haavoittuvuuksien havaitsemisen jälkeen kehitettiin WPA (Wi-Fi Protected Access) ja WPA2, joiden oli tarkoitus paikata WEP:ssä havaitut tietoturva-aukot.

2.1 WEP-salausmenetelmä

WEP (Wired Equivalent Privacy) on salausmenetelmä, joka käyttää RC4-salausalgoritmia. Aluksi 802.11-standardi oli määritelty ainoastaan 64-bittiselle WEP-salaukselle, mutta 128-bittiselle WEP-salaukselle saatiin myös hyvin nopeasti tuki standardissa. (Coleman & Westcott 2014, 466.)

WEP-salausta kehiteltäessä päätavoitteita oli yhteensä kolme: luottamuksellisuus, pääsyn hallinta ja datan eheys. Luottamuksellisuudella tarkoitettiin yksityisyyden säilyttämistä datassa salaamalla data ennen kuljetusta. Pääsyn hallinnalla tarkoitetaan käyttäjän tunnistusta siten, että pääsyä ei sallita käyttäjälle, jonka avain ei ole yhteensopiva. Datan eheydellä pyritään estämään datan muokkaamista siirron aikana. Datan muokkaamista pyritään estämään tarkistussummalla ICV (Integrity Check Value), jonka avulla vastaanottopäässä pystytään varmistamaan datan eheys. (Coleman ym. 2014, 466.)

2.1.1 Käyttäjän tunnistus

Suojatussa WEP-verkossa käytetään jaettua salausavainta (Shared Key), jonka avulla verkon käyttäjät pystyvät tunnistautumaan verkkoon. Tässä tunnistautumismenetelmässä on neljä vaihetta. Ensimmäiseksi päätelaite lähettää tunnistautumispyynnön vastaanottajalle, mikä tavallisesti on tukiasema. Se vastaa päätelaitteelle selkokielisellä haasteella. Tämän jälkeen päätelaite käyttää RC4-algoritmia viestin salaukseen ja lähettää salatun viestin takaisin tukiasemalle. Lopuksi tukiasema purkaa salatun viestin ja vertaa vastaanotettua viestiä aikaisemmin

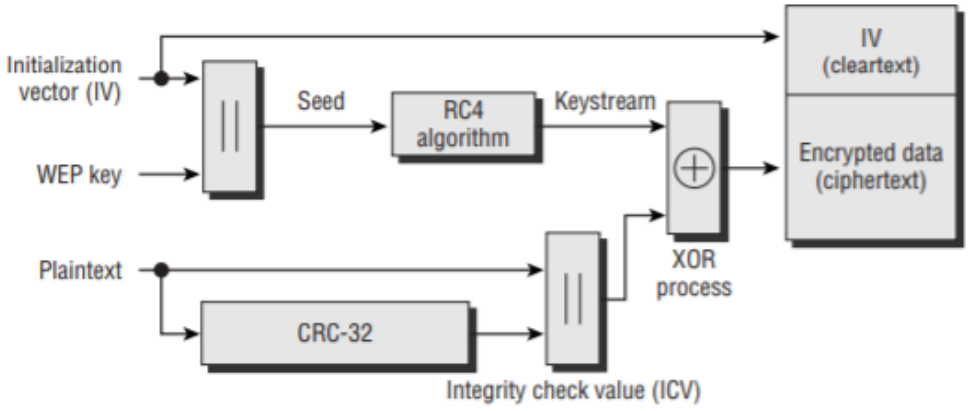
lähettämäänsä haasteeseen. Mikäli viestit vastaavat toisiaan, tukiasema myöntää päätelaitteelle pääsyn verkkoon. (Jacobs 2008)

Tunnistautumisprosessin jälkeen päätelaite ja tukiasema voivat lähettää dataa käyttäen RC4-salausalgoritmia ja avainta, jota käytettiin autentikointiprosessissa. (Jacobs 2008)

2.1.2 Salausmenetelmä

WEP-salauksen ensimmäisessä vaiheessa viestille lasketaan virheentarkistussumma CRC (Cyclic Redundancy Check). Tämän jälkeen viestin perään liitetään tarkistussumma ICV (Integrity Check Value). Seuraavaksi luodaan selkokielinen alustusvektori IV (Initialization Vector), joka yhdistetään staattiseen salausavaimeen (WEP key). (Coleman ym. 2014, 467.)

Tämän jälkeen staattisen avaimen ja alustusvektorin (IV) bitit satunnaistetaan RC4-algoritmilla. Satunnaistettuja bittejä kutsutaan nimellä keystream ja bittejä on yhtä monta kuin datassa, jota ollaan salaamassa. Tämän jälkeen RC4-algoritmin avulla luotuihin bitteihin ja selkokieliseen dataan käytetään XOR-operaatiota. Tästä saadaan tulokseksi salattu data. Lopuksi salattuun dataan liitetään vielä alustusvektori IV. Kuvasta 1 nähdään WEP-salausmenetelmä selvitettynä lohkokaavion avulla. Kuvassa kaksi pystyviivaa sisältävät lohkot kuvaavat bittijonojen yhdistämistä. (Coleman ym. 2014, 468.)



Kuva 1 WEP-salausmenetelmän lohkokaavio (Coleman ym. 2014, 468.)

2.1.3 Haavoittuvuus

WEP-salausmenetelmällä on kuitenkin haavoittuvuuksia. Yleisimpinä hyökkäyksinä voidaan pitää neljää erilaista hyökkäystapaa: IV Collisions Attack, Weak Key Attack, Reinjection Attack ja Bit-Flipping Attack. (Coleman ym. 2014, 468.)

Alustusvektori (IV) pitäisi olla joka kehyksessä erilainen. Erilaisia alustusvektoreita on rajoitettu määrä (n. 16 miljoonaa), joten WEP-salausta käyttävässä verkossa IV saattaa toistua samanlaisena. Tällöin hyökkääjä pystyy käyttämään kyseisen vektorin toistumista hyökkäykseen ja saada tätä kautta salausavaimen käsiinsä. Tällaista hyökkäystä kutsutaan nimellä IV Collisions Attack. (Coleman ym. 2014, 468.)

RC4-algoritmin yhtenä osana on KSA-algoritmi (Key-Scheduling Algorithm), jonka vuoksi generoituu heikkoja IV-avaimia. Hyökkääjä pystyy käyttämään tunnettuja heikkoja avaimia ja tätä kautta saamaan haltuunsa salausavaimen. Tätä hyökkäystapaa kutsutaan nimellä Weak Key Attack. Hyökkääjällä voi myös olla käytössä erilaisia työkaluja, joilla pystytään nopeasti keräämään heikkoja IV-avaimia myös verkoista, joissa on vähän liikennettä. Tällaisia työkaluja käytettäessä hyökkäystä kutsutaan nimellä Reinjection Attack. (Coleman ym. 2014, 468.)

Salauksen tarkistussumma ICV on myös todettu haavoittuvaiseksi. Hyökkääjä pystyy siis muokkaamaan dataa siirron aikana. Tätä hyökkäysmenetelmää kutsutaan nimellä Bit-Flipping Attack. (Coleman ym. 2014, 468.)

Erilaisia työkaluja WEP:n murtamiseen on ollut käytössä jo kauan. Työkalut käyttävät useita mm. tässä kappaleessa mainittuja hyökkäystapoja yhdistettynä siten, että hyökkääjä voi murtaa salauksen hetkessä. Tästä syystä WEP-salausta ei tule käyttää enää missään tilanteessa. (Coleman ym. 2014, 468)

2.2 Salausmenetelmät WPA ja WPA2

Vuonna 2001 onnistuneet hyökkäykset WEP-salausta vastaan pakottivat kehittelemään vahvemman salausmenetelmän, minkä vuoksi vuonna 2003 luotiin uusi

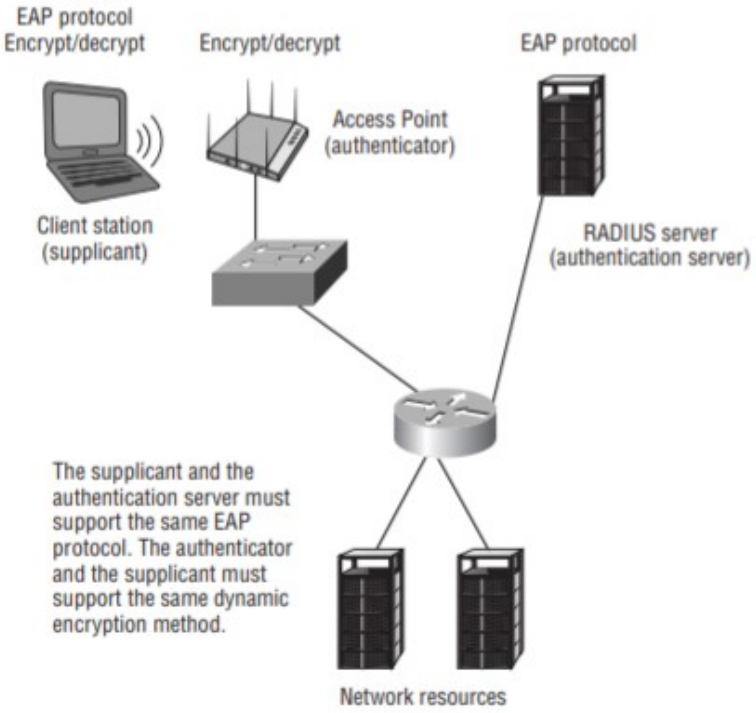
802.11i-standardi, joka tuki uutta WPA-salausmenetelmää (Wi-Fi Protected Access). (Jacobs 2008)

WPA kehitettiin siten, että laitteistolle ei tarvitsisi tehdä päivityksiä kuin ainoastaan ohjelmistotasolla. RC4-algoritmia käytettiin jo WEP:n yhteydessä, koska se ei vaatinut tehokasta prosessoria. Tämän vuoksi RC4-algoritmia käytetään myös WPA:n yhteydessä. WPA-salauksessa RC4-algoritmille on kuitenkin tehty muutamia turvallisuutta parantavia muutoksia. Ensinnäkin käyttäjät pystytään tunnistamaan yksilöllisesti käyttäen esimerkiksi Radius-palvelinta. Alustusvektorin IV pituutta on myös nostettu 48 bittiin ja master key on 128 bittiä pitkä. RC4-algoritmissa on myös uusi TKIP-protokolla (Temporal Key Integrity Protocol), jolla pystytään luomaan eri avaimet kaikille käyttäjille. Lisäksi tarkistussummana toimii uusi MIC-tarkistussumma (Message Integrity Code), jolla pystytään varmistamaan, että viestiä ei ole muokattu siirron aikana. (Jacobs 2008)

WPA:sta on kaksi eri versiota: Personal ja Enterprise. WPA-Personal tarkoittaa, että käyttäjille luodaan avaimet manuaalisesti saman tapaisella periaatteella kuin WEP:ssä. Tällöin kaikilla käyttäjillä on sama master key. WPA-Enterprise luo jokaiselle käyttäjälle PMK-avaimet (Pair-wice Master Key) erikseen käyttäen EAP:ta (Extensible Authentication Protocol). Tämän jälkeen tukiasema varmistaa käyttäjän identiteetin palvelimelta. Tukiasema hyväksyy tai estää jokaisen käyttäjän erikseen palvelimen tietojen perusteella käyttäen jokaisella käyttäjälle yksilöllistä avainta. (Jacobs 2008)

WPA-salauksesta on luotu myös paranneltu versio WPA2 (Wi-Fi Protected Access 2). Wi-Fi-allianssi vaatii vuodesta 2006 lähtien laitteelta WPA2-salauksen tuen, jotta se on oikeutettu käyttämään leimaa ”Wi-Fi-Certified”. Suurimpana erona WPA-salaukseen verrattuna on CCMP:n (Counter Mode with Cipher-Block Chaining Message Authentication Protocol) käyttö autentikoinnissa ja datan salauksessa. CCMP on turvallisempi verrattuna RC4:n ja TKIP:n yhdistelmään. WPA2-salauksesta on myös kaksi versiota: Personal ja Enterprise. WPA2-Personal luo PMK:n SSID:n (Service Set Identifier) ja PSK:n (Pre-Shared Key) perusteella. Tällöin siis kaikilla käyttäjillä on sama PMK. Tämän jälkeen käyttäjä ja tukiasema lähettävät toisilleen pyynnön, jonka perusteella luodaan PTK (Pairwise

Transient Key). PTK:ta käytetään tukiaseman ja käyttäjän välisen liikenteen salaamiseen ja purkamiseen. WPA2-Enterprise-versiossa käyttäjä ja tukiasema vastaanottaa viestin palvelimelta, jonka perusteella luodaan PMK. PMK on siis jokaisella käyttäjällä yksilöllinen. Tämän jälkeen käyttäjä ja tukiasema sopivat PTK:n luomisesta, jota käytetään datan salaamiseen ja purkamiseen. (Jacobs 2008)



Kuva 2 WPA/WPA2-Enterprise-verkko (Coleman ym. 2014, 483.)

Kuvassa 2 nähdään esimerkki verkosta, jossa on käytetty WPA/WPA2-Enterprise salausmenetelmää.

2.2.1 TKIP-salausprotokolla

WPA-salauksen yhteydessä esitelty TKIP parantaa tietoturvaa ja ottaa huomioon WEP-salauksessa havaitut heikkoudet. TKIP käyttää RC4-algoritmia, mutta parantaa sen ominaisuuksia. (Coleman ym. 2014, 482.)

Protokollassa on muutamia parannuksia RC4-algoritmiin liittyen. Ensinnäkin TKIP käyttää Per-Packet Key Mixing -prosessia. Prosessissa yhdistetään 128-

bittinen väliaikainen avain, vastaanottajan MAC-osoite ja lähettäjän MAC-osoite monimutkaisessa prosessissa. Tällä tavalla pystytään estämään WEP:ssä esiintyneitä IV collision- ja weak key -hyökkäyksiä. Lisäksi TKIP käyttää kehysten sekvensointimenetelmää, jolla pystytään estämään ns. reinjection-hyökkäys. TKIP:ssa on myös paranneltu tarkistussumma MIC, jonka avulla pystytään parantamaan datan eheyttä ja estämään bit-flipping-hyökkäys. (Coleman ym. 2014, 482.)

2.2.2 CCMP-salausprotokolla

CCMP on salausprotokolla, jota käytetään WPA2-salauksessa. Kyseinen protokolla korvaa RC4-protokollan ja TKIP:n. CCMP käsittelee dataa lohkoittain toisin kuin RC4-protokolla, joka käsittelee datan bitti kerrallaan. CCMP käyttää AES-salausprotokollaa, jossa data salataan 128 bitin lohkoissa. Tämän vuoksi CCMP on tunnettu myös nimikkeellä CCMP/AES. (Capano 2015)

CCMP voidaan jakaa kahteen eri osaan. Counter mode on CCMP:n osa, jota käytetään datan tietosuojaan, kun taas toista osaa (cipher-block chaining message authentication) käytetään autentikointiin ja datan eheyden varmistamiseen. CCMP käyttää yhtä väliaikaista avainta kaikissa salausprosesseissa. Tämä voi olla joko PTK (Pairwise Temporal Key) tai GTK (Group Temporal Key). Salausprosessi on esitetty tarkemmin liitteessä 1. (Capano 2015)

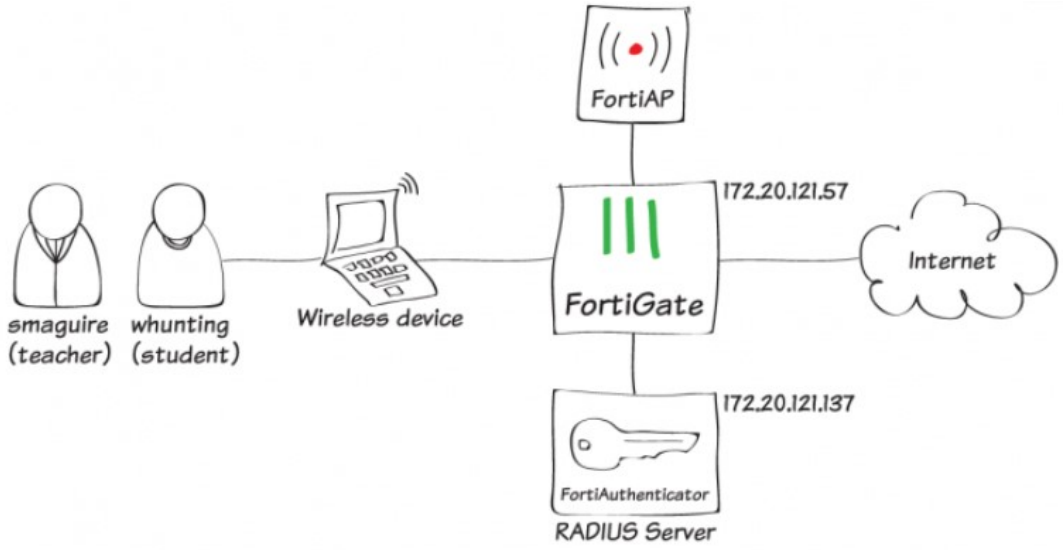
2.2.3 Haavoittuvuus

WPA- ja WPA2-salausmenetelmissä on havaittu myös haavoittuvuuksia. Hyökkäys pystytään toteuttamaan käytännössä esimerkiksi odottamalla käyttäjän yhdistämistä verkkoon ja kopioimalla tunnistautumisprosessi. Tämän jälkeen salasana yritetään saada selville niin sanotulla väsytyshyökkäyksellä eli kokeilemalla järjestelmällisesti eri salasanoja. Haavoittuvuuksien korjaamiseksi on julkaistu WPA3 (Wi-Fi Protected Access 3), joka ei kuitenkaan ole vielä kovinkaan laajalti käytössä. (Bayern 2018)

3 FORTIAUTHENTICATOR-TYÖKALU

Fortiauthenticator on Fortinetin tarjoama työkalu. Fortiauthenticator tarjoaa useita erilaisia käyttäjän tunnistukseen liittyviä ominaisuuksia, joilla pystytään parantamaan tietoturvaa esimerkiksi yritysverkoissa. Tietoturvaa parantavia ominaisuuksia ovat muun muassa vierailijaverkon käyttäjien tunnistus, monivaiheinen tunnistautuminen ja käyttäjien hallinta verkossa. (Fortinet)

Kuvassa 3 on pelkistetty kuva, jossa Fortiauthenticator on liitetty verkkoon. Kuvassa Fortiauthenticator on yhdistetty palomuuriin Fortigate. Lisäksi kuvassa Fortigaten yläpuolella on FortiAP, joka on langattoman verkon tukiasema. Fortigaten vasemmalla puolella näkyy verkon käyttäjiä.



Kuva 3 Fortiauthenticator osana verkkoa (Fortinet 2016)

3.1 Vierailijaverkko

Yrityksessä vierailevat henkilöt tarvitsevat mahdollisesti pääsyn langattomaan vierailijaverkkoon. Vierailijoiden tunnistus verkossa on tässä tapauksessa tärkeää, jotta saadaan tarvittavaa informaatiota verkon käyttäjistä, jotka pystytään tunnistamaan Fortiauthenticatorin avulla. Fortiauthenticator tarjoaa muutaman eri

tavan käyttäjien tunnistukseen. Käyttäjä voi tunnistautua olemassa olevilla kirjautumistunnuksilla, kolmannen osapuolen kirjautumistunnuksilla, kävijätietolomakkeen täyttämisellä tai MAC-osoitteen perusteella. (Fortinet 2017)

Käyttäjä voidaan tunnistaa vierailijaverkkoon olemassa olevilla käyttäjätunnuksilla. Tässä tapauksessa käyttäjä uudelleenohjataan portaaliin (Captive Portal), jossa olemassa olevien käyttäjätunnuksen ja salasanan syöttäminen on mahdollista. Mikäli syötetyillä tunnuksilla on oikeus verkon käyttöön, käyttäjä uudelleenohjataan haluamaansa verkon palveluun. Tavoitteena on mutkaton verkkoon pääsy vierailijoille, joilla on jo olemassa olevat tunnukset. (Fortinet 2017)

Uusi käyttäjä voi tunnistautua vierailijaverkkoon myös käyttäen kolmannen osapuolen tunnuksia. Fortiauthenticatorin tukemia kolmannen osapuolen tunnuksia ovat Google +, Facebook, LinkedIn ja Twitter. Kolmannen osapuolen tunnuksilla kirjautuessa ideana on se, että verkon ylläpitäjä ei missään vaiheessa saa haltuunsa kyseisiä tunnuksia. Tämä on monesti toteutettu käyttäen OAUTH-protokollaa. Kolmannen osapuolen tunnuksilla kirjautumisessa tavoitteena on, että käyttäjiin saadaan jonkinlaista jäljitettävyyttä ilman erillistä mahdollisesti työlästä vierastilin luomista. (Fortinet 2017)

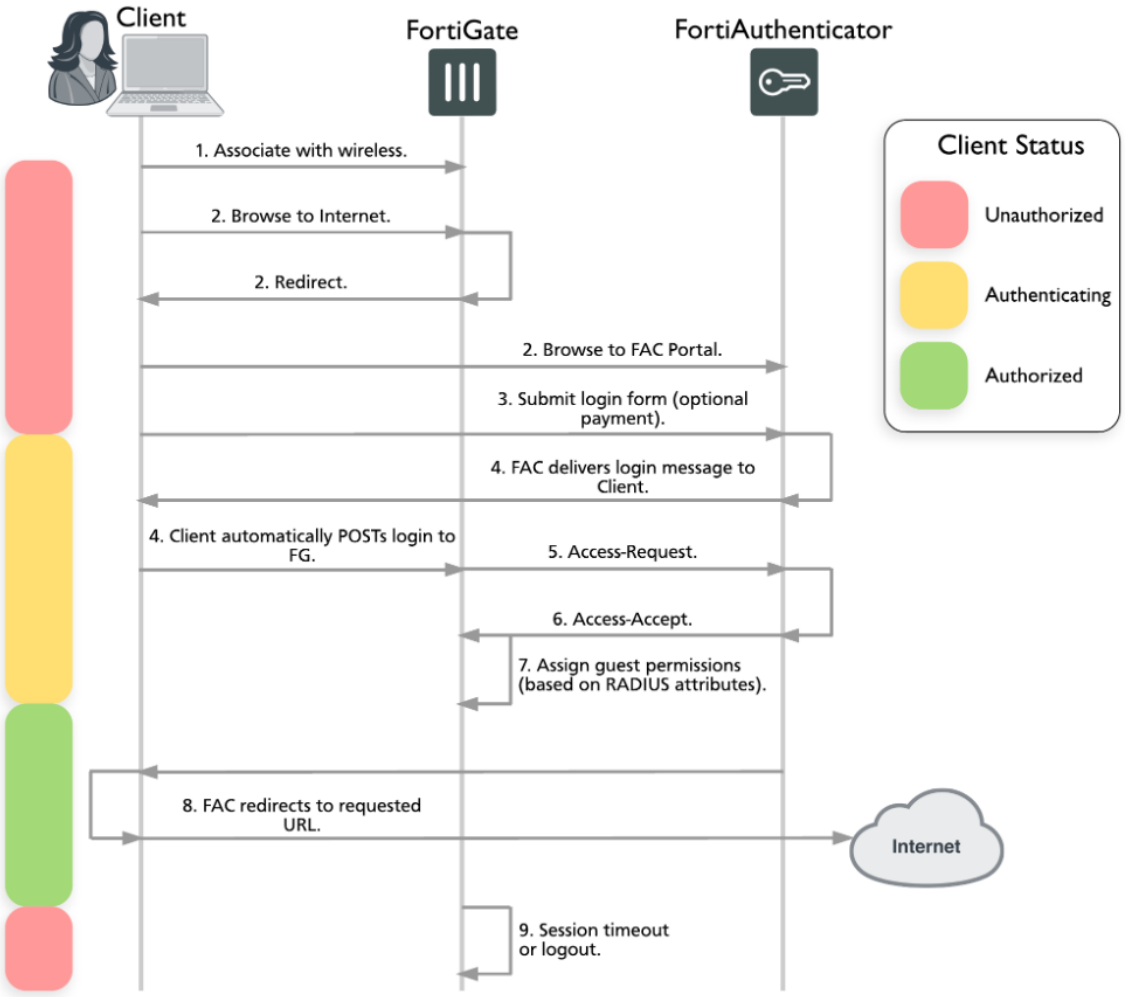
Käyttäjän tunnistukseen voidaan käyttää myös lomakepohjaista tunnistautumista (Form-based authentication). Käyttäjä ohjataan vierailijaverkkoon kirjautuessaan erilliselle rekisteröitymissivulle (Self-registration page). Tämän jälkeen käyttäjä voi syöttää lomakkeelle vaadittavat tiedot, kuten puhelinnumeron tai sähköpostiosoitteen. Lopuksi käyttäjä saa kirjautumistiedot syöttämäänsä sähköpostiosoitteeseen tai puhelinnumeroon. Lomakepohjaisella tunnistautumisella saadaan usein melko epäluotettavaa tietoa käyttäjästä, jonka vuoksi kyseinen tapa on käytössä usein yleisillä paikoilla kuten esimerkiksi lentokenttien ja kahviloiden vierasverkoissa käytännöllisyyden vuoksi. (Fortinet 2017)

Käyttäjän näkökulmasta MAC-osoitteen käyttö on mahdollisesti helpoin tapa tunnistautua vierailijaverkkoon. Tämä ei vaadi käyttäjältä toimenpiteitä, koska Fortiauthenticator tallentaa päätelaitteen MAC-osoitteen automaattisesti, jonka jälkeen päästää käyttäjän verkkoon. Tämä tunnistautumistapa ei kuitenkaan anna

juuri lainkaan tietoa käyttäjästä, jonka vuoksi se on helppokäyttöisyydestään huolimatta useille tietoturvauhille altis tapa tunnistaa käyttäjiä. (Fortinet 2017)

3.1.1 Tunnistautumisen eteneminen

Kuvassa 4 nähdään prosessin eteneminen käyttäjän yhdistäessä vierailijaverkkoon.



Kuva 4 Käyttäjän tunnistautumisprosessi vierailijaverkkoon (Fortinet 2017)

Ensimmäiseksi käyttäjä liittyy vierailijaverkkoon SSID:n perusteella. Käyttäjän avatessa selaimen, Fortigate-palomuuri estää käyttäjän HTTP-liikenteen. Tämän jälkeen Fortigate uudelleenohjaa käyttäjän Fortiauthenticatorin kirjautumissivulle, joka on määritelty Fortigatelle. Kirjautumissivulla käyttäjä syöttää olemassa ole-

vat käyttäjätunnukset tai käyttää mahdollisesti toista käytössä olevaa tunnistautumistapaa. Seuraavaksi Fortiauthenticator lähettää käyttäjän verkkoselaimelle kirjautumisviestin, jonka perusteella selain lähettää käyttäjän kirjautumistiedot suoraan Fortigatelle. Tämän jälkeen Fortigate lähettää Access-Request-pyynnön Fortiauthenticatorille. Fortiauthenticator vahvistaa pyynnön käyttäen käyttäjätietokantaansa ja vastaa palomuurille Access-Accept- tai Access-Reject-viestillä. Viesti on muotoa Access-Accept, mikäli käyttäjä on Fortiauthenticatorin käyttäjätietokannan perusteella oikeutettu verkkoon pääsyyn. Tällöin viesti sisältää muutakin tietoa käyttäjän istunnosta, kuten istunnon keston, maksimisiirtonopeuden ja käyttöoikeudet. Kyseiset attribuutit on konfiguroitu Fortiauthenticatorille. Seuraavaksi käyttäjä uudelleenohjataan haluamalleen sivustolle, mikäli oikeus verkkoon pääsyyn on myönnetty. Tämän jälkeen Fortigate alkaa laskea mahdollista määriteltyä aikaa, jolloin käyttäjän istunto aikakatkaistaan. (Fortinet 2017)

3.2 Monivaiheinen tunnistautuminen

Monivaiheinen tunnistautuminen tarkoittaa systeemiä, joka vaatii käyttäjältä enemmän kuin yhden kirjautumistiedon tunnistautumisen yhteydessä. Monivaiheisessa tunnistautumisessa tavoitteena on parantaa tietoturvaa siten, että käyttäjälle ei riitä pelkästään yksi salasana järjestelmään kirjautuakseen. (Rouse 2015)

Varmastikin yleisin käyttäjältä kysyttävä kirjautumistieto on jotain, jonka käyttäjä tietää. Tällöin kyseessä on todennäköisesti salasana. Käyttäjä voi kuitenkin tunnistautua järjestelmään myös muulla tavalla. Käyttäjältä voidaan vaatia esimerkiksi jotain, joka käyttäjällä on hallussaan. Tällöin kyseessä on monesti vaihtuva salasana (token), joka on jokaisella kirjautumiskerralla eri. Kolmas yleisesti käytössä oleva tunnistetieto on biometrinen kirjautuminen. Tällöin käyttäjältä kysytään esimerkiksi sormenjälkeä. (Rouse 2015)

3.2.1 Kaksivaiheinen tunnistautuminen Fortiauthenticatorilla

Kaksivaiheinen autentikointi pystytään toteuttamaan verkkoon Fortiauthenticatorilla. Tällöin käyttäjältä kysytään kirjautumisen yhteydessä salasanan lisäksi vaihtuva salasana (token) tai sertifikaatti, joka on tallennettuna käyttäjän tietokoneelle. (Martin 2014)

Vaihtuvaa salasanaa käytettäessä käyttäjältä kysytään salasanan lisäksi asetetuin väliajoin vaihtuva salasana (one-time password). Vaihtuvasta salasanasta käytetään Fortinetin laitteiden yhteydessä nimitystä FortiToken. Kaksivaiheinen tunnistautuminen voidaan liittää haluttuun käyttäjään Fortiauthenticatorin hallinnan kautta. Lisäksi voidaan määrittää verkon palvelut, joissa kyseistä tunnistautumistapaa vaaditaan. Näitä voivat olla esimerkiksi verkkolaitteisiin kirjautuminen tai VPN-yhteyden luominen. FortiToken voidaan toimittaa käyttäjälle tekstiviestillä, sähköpostilla, erillisellä Fortinetin FortiToken laitteella tai Fortinetin omalla sovelluksella. Kuvassa 5 näkyy Fortinetin sovellus, joka on asennettuna käyttäjän puhelimeen. (Martin 2014)

Kuva 5 FortiToken Mobile (Martin 2014)

3.3 Käyttäjien hallinta

Fortiauthenticator sisältää tietokannan verkon käyttäjistä, josta pystyy näkemään erilaista informaatiota käyttäjästä. Käyttäjän tiedoista voidaan nähdä esimerkiksi

ylläpito-oikeuden omaavat käyttäjät, käyttäjän henkilötiedot ja käyttäjän autentikointitapa. (Fortinet 2017)

Käyttäjät luokitellaan erilaisiin ryhmiin sen perusteella, miten Fortiauthenticator saa käyttäjätiedot haltuunsa. Ylläpitäjä voi luoda paikalliset käyttäjät (Local Users) Fortiauthenticatorin hallinnan kautta, jolloin käyttäjätiedot sijaitsevat ainoastaan Fortiauthenticatorilla. Etäkäyttäjät (Remote Users) voidaan synkronoida jostakin yrityksellä olevasta erillisestä käyttäjätietokannasta, kuten Windows Active Directorysta. Näiden lisäksi ovat vielä vieraskäyttäjät (Guest Users) ja kolmannen osapuolen kirjautumistavalla kirjautuneet käyttäjät (Social Login Users). Guest users on käytännössä sama asia kuin paikalliset käyttäjät, mutta näillä käyttäjillä on usein joitakin rajoituksia, kuten ajallisesti rajattu käyttöaika verkkoon. Social login users tarkoittaa käyttäjiä, jotka ovat autentikoituneet verkkoon käyttäen vierasverkon Captive Portalia ja kolmannen osapuolen tunnuksia. (Fortinet 2017)

3.3.1 Fortinet Single Sign-On

Käyttäjällä voi olla pääsy useisiin verkon palveluihin yhdellä kirjautumiskerralla siten, että käyttäjältä ei kysytä kirjautumistietoja uudelleen. Tällöin on kyseessä Fortinet Single Sign-On (FSSO). Fortiauthenticator säilyttää tarvittavia käyttäjätietoja ja lähettää ne palomuurille. Tällöin Fortigate tietää käyttäjänimen, IP-osoitteen ja ryhmän, johon käyttäjä kuuluu. Mikäli käyttäjä kuuluu sallittuun ryhmään, Fortigate sallii liikenteen. Kirjautumistietoja ei tässä tapauksessa tarvitse kysyä käyttäjältä uudelleen. (Fortinet 2019)

4 LANGATTOMAN VERKON UHAT

WLAN:in tärkein tarkoitus on käytännössä tarjota käyttäjälle pääsy verkkoon langattomasti. Langattomasti siirtyvä informaatio on altis kaappauksille, minkä vuoksi langattomassa lähiverkossa on oltava käytössä vahva suojausmenetelmä, jotta mahdolliset hyökkäykset voidaan torjua.

Erilaisia verkkoon kohdistettavia hyökkäysmenetelmiä on useita. Hyökkääjä voi päästä käsiksi lähiverkkoon esimerkiksi työntekijän asentaman tukiaseman kautta, jossa on heikko suojaus. Hyökkääjä voi myös toteuttaa palvelunestohyökkäyksen, jolloin verkko saattaa olla pois käytöstä pitkiäkin aikoja. Yhtenä hyökkäystapana on myös toteuttaa Man-in-the-middle-hyökkäys, jolloin hyökkääjä voi saada haltuunsa verkossa liikkuvaa informaatiota.

4.1 Luvaton tukiasema

Luvattomat tukiasemat (Rogue Access Point) ovat yksi suurimmista tietoturvauhista langattomiin verkkoihin liittyen. Luvattomalla tukiasemalla tarkoitetaan mitä tahansa langatonta verkkoa jakavaa laitetta, jota verkon ylläpitäjä ei pysty hallitsemaan. (Coleman ym. 2014, 501.)

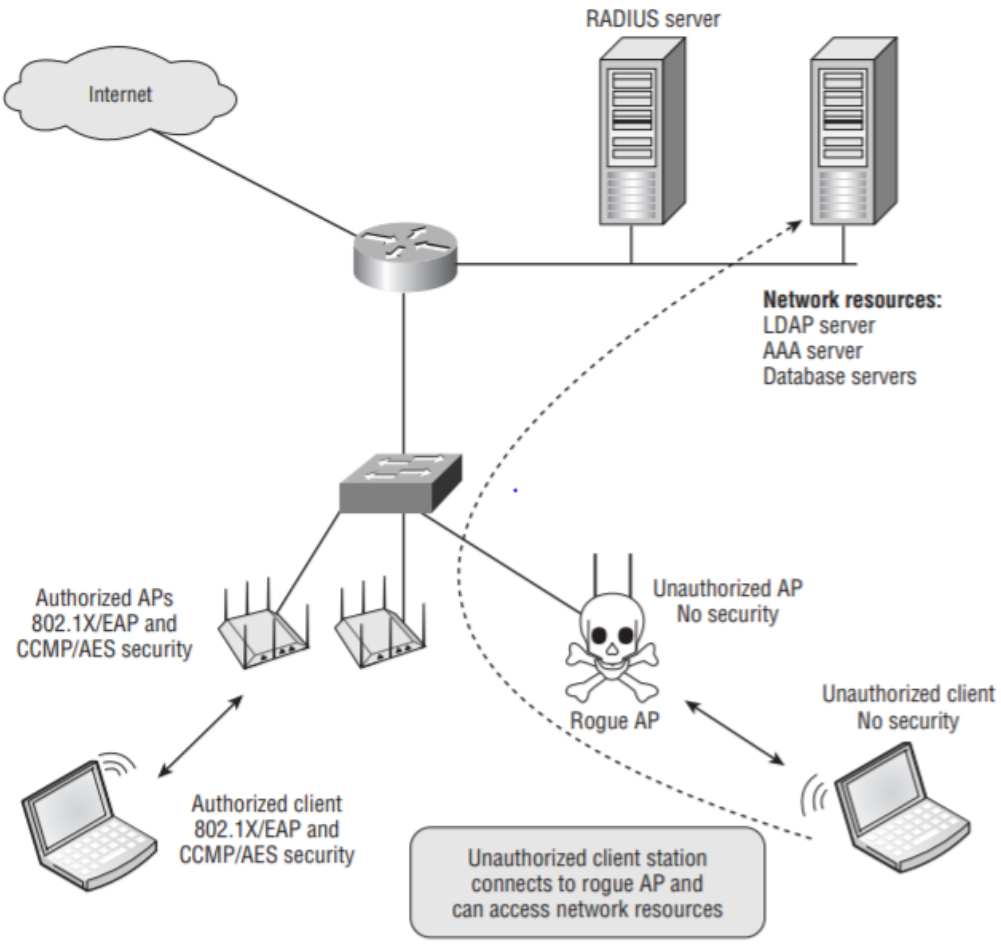
4.1.1 Luvattoman tukiaseman asennus

Monesti luvattoman tukiaseman käyttöönottajana ei toimi itse verkkoon murtautuja, vaan esimerkiksi yrityksen työntekijä. Tässä tapauksessa työntekijä asentaa oman langattoman laitteensa tukiasemaksi yrityksen verkkoon. Ongelmana tässä on se, että työntekijän asentama laite ei mahdollisesti ole suojattu tarpeeksi hyvin, jolloin se antaa murtautujalle pääsyn yrityksen lähiverkkoon. (Coleman ym. 2014, 501.) Toisena vaihtoehtona on, että murtautuja asentaa itse luvattoman tukiaseman yrityksen sisäverkkoon. Tällöin hyökkääjä tarvitsee kuitenkin pääsyn yrityksen tiloihin.

4.1.2 Luvattoman tukiaseman haitat

Luvaton tukiasema on suuri tietoturvauhka, koska mahdollinen hyökkääjä pääsee käsiksi yrityksen lähiverkkoon langattomasti. Päästessään yrityksen lähiverkkoon, hyökkääjällä on useita tapoja aiheuttaa haittaa. (Juniper Networks 2016) Kuvassa 6 luvaton tukiasema on merkitty pääkallolla. Haitallinen tukiasema on kytketty suoraan kytkimelle, jonka jälkeen hyökkääjällä on pääsy muun muassa uhrin lähiverkossa sijaitseville palvelimille.

FIGURE 14.1 Rogue access point



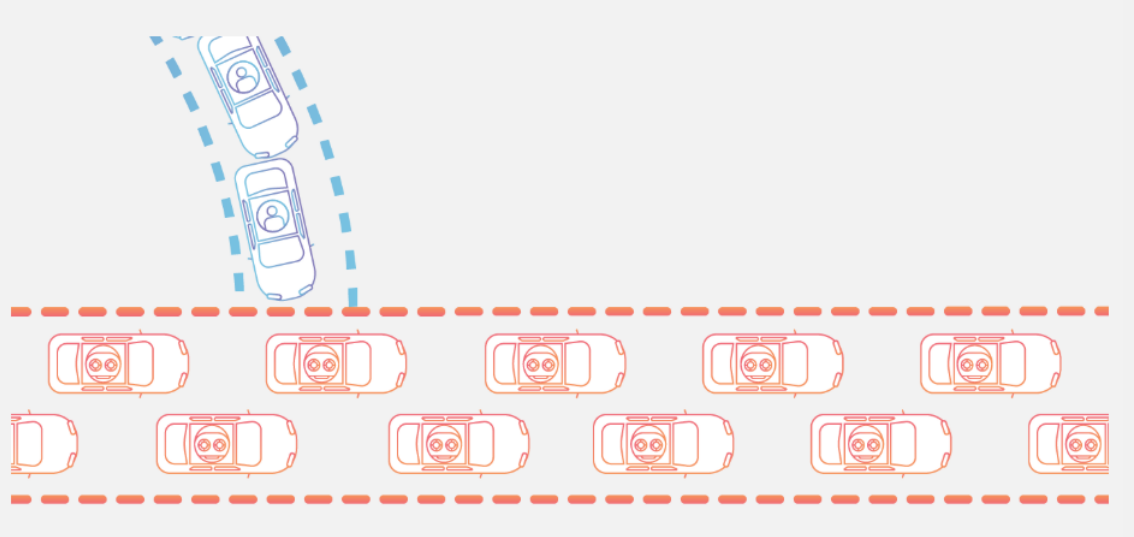
Kuva 6 Verkkoon liitetty luvaton tukiasema (Coleman ym. 2014, 502)

Päästessään yrityksen lähiverkkoon, hyökkääjällä on mahdollisesti pääsy yrityksen salaiseen informaatioon, joka voi sijaita esimerkiksi verkkolevyllä. Lisäksi

hyökkääjä voi aloittaa esimerkiksi Man-in-the-middle-hyökkäyksen tai palvelunestohyökkäyksen. (Juniper Networks 2016)

4.2 Palvelunestohyökkäys

Palvelunestohyökkäyksellä tarkoitetaan hyökkäystä, joka kohdistetaan laitteeseen tai verkkoon siten, että sen kommunikointi käyttäjien kanssa on mahdotonta hyökkäyksen aikana (Paloalto Networks). Kuva 7 havainnollistaa palvelunestohyökkäystä. Kuvassa punaiset autot kuvaavat hyökkääjän tuottamaa turhaa liikennettä ja siniset autot kuvaavat verkon oikeaa liikennettä. Palvelunestohyökkäyksen aiheuttama turha liikenne ruuhkauttaa verkon, jolloin verkon oikea liikenne ei pääse liikkumaan.



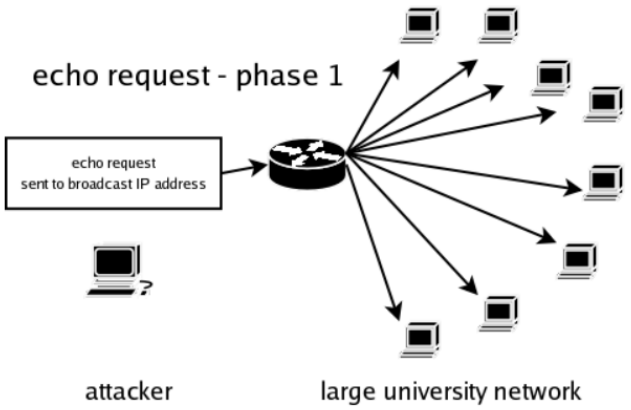
Kuva 7 Havainnollistava kuva palvelunestohyökkäyksestä (Cloudflare)

Toisena vaihtoehtona on lähettää kohteelle tietyn tyyppistä informaatiota, joka aiheuttaa kohteen kaatumisen. Useissa tapauksissa palvelunestohyökkäyksen kohteena on isoja yrityksiä kuten esimerkiksi pankkeja, mediatoimistoja, kauppoja tai valtion palveluja. (Paloalto Networks)

4.2.1 Verkon ruuhkauttaminen

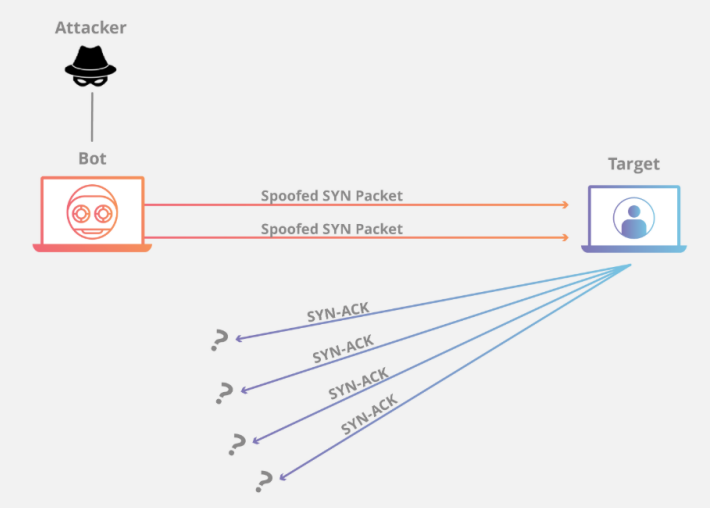
Ruuhkauttamalla aiheutetusta palvelunestohyökkäyksestä käytetään nimeä Flood attack. Järjestelmän kapasiteetin ylitystä kutsutaan myös nimellä Buffer overflow attack. (Paloalto Networks)

Toisena tapana liikenteen ruuhkauttamiselle on niin sanottu ICMP Flood. Tässä hyökkäyksessä hyödynnetään virheellisesti konfiguroituja verkkolaitteita. Verkkolaitteelle lähetetään paketteja, jotka aiheuttavat ping-pyyntöjen lähettämisen jokaiselle verkon laitteelle. Tämä ping-pyyntöjen aiheuttama ICMP-pakettien tulva ruuhkauttaa verkon liikennettä. Esimerkkinä kuvassa 8 on yliopiston verkossa oleva reititin, joka lähettää turhia ping-kyselyjä kaikille verkon tietokoneille, jolloin yliopiston verkko ruuhkautuu. (Paloalto Networks)



Kuva 8 Verkon ruuhkauttaminen turhilla ping-kyselyillä (Tomicki 2012)

Yhtenä yleisenä tapana ruuhkauttaa verkon liikennettä on aloittaa niin sanottu SYN Flood -hyökkäys. Tässä hyökkäyksessä uhrille lähetetään suuri määrä TCP-paketteja, jotka käytännössä pyytävät yhteyden muodostusta. Tämän jälkeen uhri vastaa jokaiseen yhteyspyyntöön ja jää odottamaan TCP-kättelyn viimeistä vaihetta. Hyökkääjä ei kuitenkaan suorita viimeistä vaihetta, jolloin verkkoon syntyy ruuhkaa. Kuvassa 9 esiintyy hyökkääjä, joka lähettää ensin SYN-paketteja, joihin uhri vastaa. Kuvassa on merkitty punaisella hyökkääjän tietokone ja sinisellä hyökkäyksen uhrin tietokone. Viimeistä vaihetta TCP-kättelystä ei kuitenkaan tapahdu. (Cloudflare)



Kuva 9 SYN Flood -hyökkäyksen eteneminen (Cloudflare)

4.2.2 Hajautettu palvelunestohyökkäys

Palvelunestohyökkäys voidaan toteuttaa myös useasta järjestelmästä samanaikaisesti. Tällöin hyökkäystä kutsutaan hajautetuksi palvelunestohyökkäykseksi. Hajautetussa palvelunestohyökkäyksessä hyökkäyksen aiheuttajaa on vaikeampi selvittää, koska hyökkääviä järjestelmiä voi olla useita ympäri maailmaa. Hyökkääjän etuna on myös se, että useita hyökkääviä tietokoneita on vaikeampi sammuttaa. Lisäksi todellisia hyökkääjiä on vaikea havaita, koska ne voivat olla naamioitu erilaisten järjestelmien taakse. (Paloalto Networks)

4.2.3 Langattoman verkon palvelunestohyökkäys

Sopivilla työkaluilla lähes kuka tahansa pystyy kaatamaan langattoman verkon siten, että käyttäjät eivät pysty käyttämään sitä. Tällöin palvelunestohyökkäys kohdistetaan pelkkään WLAN-verkkoon. (Coleman ym. 2014, 514.)

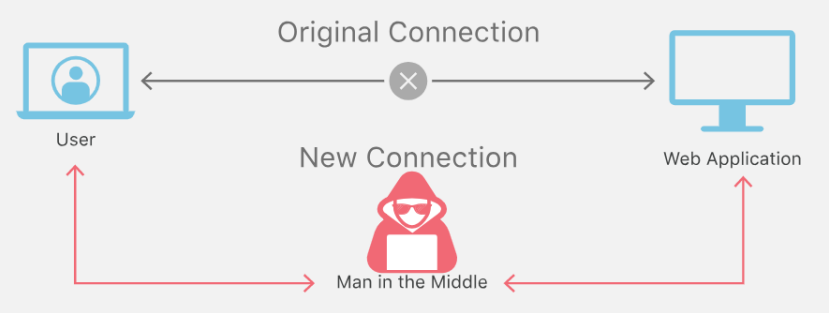
Langattoman verkon palvelunestohyökkäys voidaan toteuttaa häiritsemällä radiosignaalia. Tällöin häirintä tapahtuu käyttämällä esimerkiksi signaaligeneraattoria. Tällaista hyökkäystä kutsutaan myös tahalliseksi häirinnäksi. Häirintä voi olla myös tahatonta, jolloin sitä voi aiheuttaa muut radiotaajuuksia käyttävät laitteet. Spektrianalysaattorin avulla voidaan paikallistaa häiriötä aiheuttavat laitteet

seuraamalla analysaattorin mittaamaa tehoa kohdetta lähestyttäessä. (Coleman ym. 2014, 514.)

Yleisempänä palvelunestohyökkäyksenä langatonta verkkoa kohtaan voidaan pitää kuitenkin hyökkäystä, jossa muokataan tahallisesti WLAN-verkon kehyksiä. Hyökkääjä voi muokata kehyksestä MAC-osoitteita siten, että tukiasema luulee kehyksen tulevan esimerkiksi toiselta tukiasemalta. Tällaisella kehysten muokkaamisella hyökkääjä pystyy pahimmassa tapauksessa kaatamaan langattoman verkon. Kyseisiä hyökkäyksiä pystytään torjumaan esimerkiksi käyttämällä analysaattoria, joka analysoi protokollaa, jolloin kehyksiin tehdyt muokkaukset pystytään mahdollisesti havaitsemaan. Lisäksi WLAN-standardeissa on myös kehitetty havaitsemisjärjestelmiä, jotka tunnistavat kyseiset hyökkäykset paremmin. (Coleman ym. 2014, 514.)

4.3 Man-in-the-middle-hyökkäys

Man-in-the-middle-hyökkäyksessä hyökkääjä asettuu kahden laitteen väliin, jolloin se voi esimerkiksi muokata tai kaapata liikennettä, joka liikkuu laitteiden välillä. Useimmissa tapauksissa hyökkääjä asettuu web-selaimen ja web-palvelimen välille, jolloin hyökkääjällä on mahdollisuus kerätä informaatiota käyttäjästä. (Cloudflare)



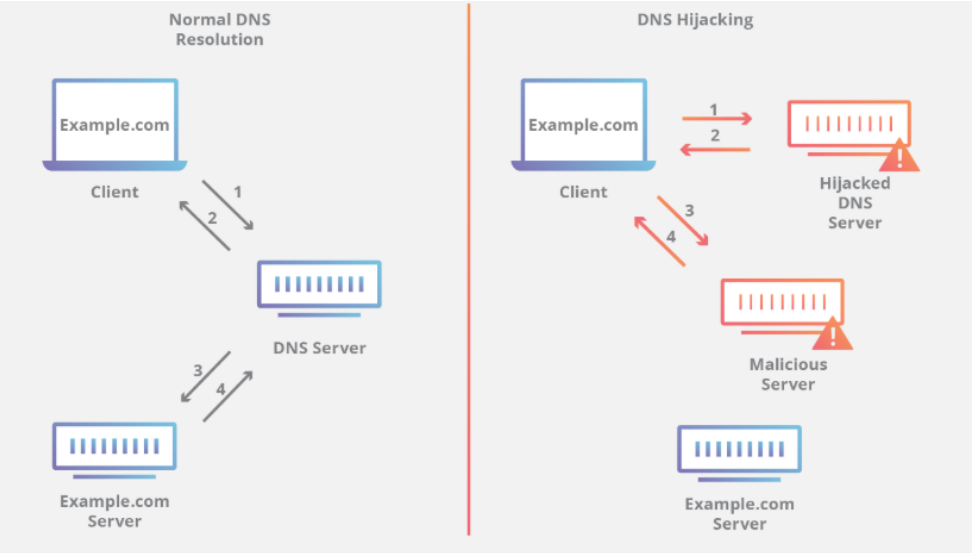
Kuva 10 Man-in-the-middle hyökkäys (Cloudflare)

Kuvassa 10 nähdään Man-in-the-middle -hyökkäys, jossa hyökkääjä on kaapannut käyttäjän ja web-sovelluksen välisen yhteyden.

4.3.1 Hyökkäystapoja

Man-in-the-middle-hyökkäyksen kohteena voi olla esimerkiksi käyttäjän ja verkkosivun välillä oleva HTTP-yhteys. Tällöin hyökkääjä esiintyy välityspalvelimena siten, että se pystyy kaappaamaan ja muokkaamaan informaatiota, jota lähetetään käyttäjän ja verkkosivuston välillä. Tämän seurauksena hyökkääjä voi saada haltuunsa käyttäjän laitteelle tallentuvia evästetietoja, joiden avulla pystyy esiintymään itse käyttäjänä. (Cloudflare)

Toinen hyökkäystapa on kohdistaa hyökkäys DNS-palvelimelle, joka kääntää verkkoselaimelle käyttäjän asettaman domain-nimen IP-osoitteeksi, jolloin käyttäjän haluama verkkosivu pystytään avaamaan. Tässä hyökkäystavassa hyökkääjä esiintyy DNS-palvelimena, jolloin se pystyy ohjaamaan käyttäjän väärälle verkkosivulle. Väärä verkkosivu voi olla jokin henkilökohtaista informaatiota keräävä sivusto tai haittaohjelman sisältävä sivusto. (Cloudflare)



Kuva 11 Man-in-the-middle-hyökkäys DNS-palvelimelle (Cloudflare)

Kuvassa 11 nähdään vasemmalla puolella normaali tilanne selaimen ja DNS-palvelimen välillä. Oikealla puolella nähdään tilanne, jossa Man-in-the-middle-hyökkäys on käynnissä (Cloudflare).

Hyökkääjä voi toteuttaa hyökkäyksen myös asettumalla sähköpostipalvelimen ja ulkoverkon väliin. Tällöin hyökkääjä pystyy seuraamaan sähköpostiliikennettä ja käyttää sitä erilaisiin tarkoituksiin. Esimerkkinä voidaan pitää tilannetta, jossa

käyttäjää on pyydetty sähköpostilla lähettämään rahaa tilinumeron perusteella. Tässä tapauksessa hyökkääjä pystyy näkemään sähköpostin ja lähettämään käyttäjälle uuden sähköpostin esittäen sähköpostin lähettäjää. Uudessa sähköpostissa hyökkääjä voi esimerkiksi ilmoittaa tilinumeron vaihtuneen, jolloin käyttäjä lähettää rahat suoraan hyökkääjän tilille. (Cloudflare)

Julkisia WLAN-verkkoja käyttävällä on myös suuri riski joutua Man-in-the-middle-hyökkäyksen kohteeksi. Hyökkääjä voi luoda langattoman verkon, jonka nimi vaikuttaa vaarattomalta tai kloonata jo olemassa olevan julkisen verkon. Käyttäjän yhdistäessä hyökkääjän luomaan verkkoon hyökkääjä pystyy seuraamaan käyttäjän liikennettä ja tätä kautta aiheuttamaan haittaa. (Cloudflare)

4.3.2 Hyökkäykseltä suojautuminen

Käyttäjä pystyy pienentämään riskiä Man-in-the-middle-hyökkäyksen kohteeksi joutumiselle useilla eri tavoilla. HTTP-yhteyden tulee olla salattu verkkosivuilla vierailtaessa. Tämän tunnistaa verkkoselaimessa olevasta HTTPS-tunnuksesta URL-kentässä. Käyttäjän tulee olla myös tietoinen mahdollisista sähköpostilla toimitettavista kalasteluviesteistä, jotka mahdollisesti pyytävät esimerkiksi päivittämään salasanan. Sähköposteissa olevat linkit tulisi kirjoittaa itse selaimen URL-kenttään manuaalisesti. Lisäksi julkisiin Wi-Fi-verkkoihin ei tulisi liittyä koskaan, mikäli mahdollista. Mikäli julkisiin Wi-Fi-verkkoihin on välttämätöntä liittyä, tulee ehdottomasti käyttää virtuaalista erillisverkkoa, joka salaa liikenteen. Man-in-the-middle-hyökkäyksessä saatetaan käyttää myös haittaohjelmia, minkä vuoksi käyttäjän laitteella tulisi aina olla päivitetty virustentorjuntaohjelma asennettuna. Näiden lisäksi kaikkien verkossa olevien verkkolaitteiden tulee olla päivitettyjä ja niissä olevat salasanat pitää olla vahvoja. (Norton)

5 POHDINTA

Lähiverkko halutaan tavallisesti toteuttaa langattomasti kätevyyden vuoksi. Yrityksissä kannettavat laitteet ovat yleisiä, koska oma päätelaite pitää pystyä ottamaan mukaan esimerkiksi neuvotteluhuoneeseen.

Kätevyyden varjopuolena ovat kuitenkin lukuisat tietoturvauhat, joita langattoman verkon käyttö aiheuttaa. Informaation kulkiessa langattomasti kaapeleiden sijaan, tietoturvauhat lisääntyvät huomattavasti. Langattoman verkon tietoturvauhista on saatavana paljon tietoa, minkä vuoksi lähes kuka tahansa pystyy halutessaan toteuttamaan hyökkäyksen langatonta verkkoa vastaan.

Jatkuvasti kasvavien tietoturvauhkien vuoksi varsinkin yritysten tulisi ottaa uhat entistä vakavammin. Käyttäjän monivaiheinen tunnistautuminen pienentää käyttäjän kirjautumistietojen väärinkäytön mahdollisuutta, minkä vuoksi sitä tulisi käyttää, vaikka käytettävyys hieman kärsisikin. Lisäksi yrityksen verkkolaitteet tulisi aina konfiguroida käyttäjäkohtaisilla tunnuksilla, jotta mahdolliset väärinkäytöt pystytään havaitsemaan. Vierailijaverkon käyttäjillä pitäisi myös olla yksilölliset tunnukset, jotta verkon ylläpitäjä on tietoinen käyttäjien identiteetistä. Nämä kaikki on mahdollista toteuttaa esimerkiksi Fortiauthenticatorilla tai muilla vastaavilla työkaluilla, joita yritysten tulisi käyttää.

Varsinkin yrityksillä tulisi olla hyvä tietämys salausmenetelmistä ja niiden heikkouksista. WPA2-salausmenetelmässä on myös havaittu haavoittuvuuksia, jonka vuoksi uusi WPA3-salausmenetelmä on jo julkaistu. WPA3 ei kuitenkaan ole käytössä vielä kovinkaan laajasti. Tietoturvan kannalta erittäin tärkeää on verkon ylläpitäjän huolehtiminen salausmenetelmien päivityksestä. Verkon ylläpitäjän välinpitämättömyys voi pahimmassa tapauksessa aiheuttaa esimerkiksi yrityksen salaisten tietojen vuotamisen ulkopuolisille.

LÄHTEET

Bayern, M. 2018. New method makes cracking WPA/WPA2 WiFi network easier and faster. Luettu 19.5.2019.
https://www.techrepublic.com/article/new-method-makes-cracking-wpawpa2-wi-fi-network-passwords-easier-and-faster/

Capano, D. 2015. Wireless security: IEEE 802.11 and CCMP/AES. Luettu 4.5.2019.
https://www.controleng.com/articles/wireless-security-ieee-802-11-and-ccmp-aes/

Cloudflare. Man-In-The-Middle Attack. Luettu 27.4.2019.
https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/

Cloudflare. What is a DDoS Attack?. Luettu 27.4.2019.
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Coleman, D., Westcott, A. 2014. CWNA: Certified Wireless Network Administrator Official Study Guide. 4. painos. Indiana: John Wiley & Sons, Inc.

Fortinet. 2016. WiFi with WSSO using FortiAuthenticator RADIUS and Attributes. Luettu 19.5.2019.
https://cookbook.fortinet.com/wifi-wsso-using-fortiauthenticator-radius-attributes-54/

Fortinet. 2017. User Management. Luettu 19.5.2019.
https://help.fortinet.com/fauth/5-1/Content/Admin%20Guides/5_1%20Admin%20Guide/400/403_User_management.htm#Social

Fortinet. 2017.Captive Portals. Luettu 19.5.2019.
https://help.fortinet.com/fauth/5-1/Content/Admin%20Guides/5_1%20Admin%20Guide/400/406_Captive_portal.htm#CredentialsAuth

Fortinet. 2019. Introduction to authentication. Luettu 19.5.2019.
https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-authentication/Auth_Intro.htm#Single_sign-on_authentication_for_users

Fortinet. Fortiauthenticator. Luettu 19.5.2019.
https://cookbook.fortinet.com/fortiauthenticator/

Jacobs, D. 2008. Wireless security – How WEP encryption works. Luettu 4.5.2019.
https://searchnetworking.techtarget.com/tip/Wireless-security-How-WEP-encryption-works

Jacobs, D. 2008. Wireless security protocols – How WPA and WPA2 work. Luettu 4.5.2019.
https://searchnetworking.techtarget.com/tip/Wireless-security-protocols-How-WPA-and-WPA2-work

Juniper Nerworks. 2016. Understanding Rogue Access Points. Luettu 27.4.2019. https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

Martin, V. 2014. Two-factor authentication with FortiToken Mobile. Luettu 19.5.2019. https://cookbook.fortinet.com/two-factor-authentication-fortitoken-mobile/

Norton. What is a man-in-the-middle attack?. Luettu 27.4.2019. https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Paloalto Networks. What is a denial of service attack (DoS)?. Luettu 27.4.2019. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

Rouse, M. 2015. multifactor authentication (MFA). Luettu 19.5.2019. https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

Tomicki, L. 2012. Ping Flooding. Luettu 27.4.2019. https://www.tomicki.net/ping.flooding.php

LIITTEET

Liite 1. CCMP-salausprosessi (Capano 2015)