Rasmus Virtanen

Julkisen verkon tietoturvauhat

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

16.4.2015

Metropolia

Tekijä Otsikko Sivumäärä Aika	Rasmus Virtanen Julkisen verkon tietoturvauhat 46 sivua + 1 liitettä 16.4.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	projekti-insinööri Heikki Rahkonen

Insinöörintyössä pyritään tarjoamaan lukijalle tietoa tietoturvauhkista julkisissa verkoissa ja kuinka suojautua niitä vastaan. Tämä saavutetaan esittelemällä Internetin toimintaa, kertomalla haittaohjelmista ja hyökkäystekniikoista sekä esittelemällä käytännössä, miten hyökkäykset toimivat. Työn tavoitteena on kokonaisuutena toimia oppaana henkilökohtaisen tietoturvan parantamiseen.

Insinöörityön tavoite saavutetaan esittelemällä Internetin toimintaa, tietoturvauhkia ja niiltä suojautumista. Teorian lisäksi demonstroidaan kahta hyökkäystekniikkaa ja niiltä suojautumista. Hyökkäykset suoritettiin koulun tietoverkko-laboratoriossa käyttäen reititintä, tietokoneita ja Android-puhelinta. Laboratoriossa suoritettiin evästeiden kaappaus Droidsheep-ohjelmalla ja yritettiin kaapata HTTPS-suojattua liikennettä käyttäen väliintulohyökkäystä.

Testit osoittivat, että hyökkäystekniikat julkisessa verkossa ovat toimivia pienin varauksin. Evästeiden kaappaus toimi ongelmitta, mutta väliintulohyökkäys osoittautui haastavammaksi. Varmentein suojatusta liikenteestä tiedon kaappaaminen onnistuu, mutta ei ilman varoituksia kohdekoneeella. Varoituksistakin on mahdollista päästä eroon, mutta se vaatii fyysistä pääsyä kohdekoneelle. Tällöin voi asentaa väärennetyn varmenteen ja poistaa selainten esittämät varoitukset.

Testien perusteella julkisen langattoman verkon käytössä on syytä noudattaa varovaisuutta tai suojata liikenteensä VPN-yhteydellä.

Avainsanat	Julkinen langaton verkko, tietotuva, väliintulohyökkäys

Author(s) Title Number of Pages Date	Rasmus Virtanen Public Wi-Fi's information security threats 46 pages + 1 appendices 16 April 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Information Networks
Instructor(s)	Heikki Rahkonen, Project Engineer

The objective of the thesis is to provide information to the reader about information security threats in public Wi-Fi and how to protect against these. This is achieved by explaining how the Internet works, providing information about malware and attacking techniques and also demonstrating the techniques in practice. The purpose of the thesis as a whole is to be a guide to personal security improvement.

To give a reader better understanding of the threats, attacking techniques were tested in an information network laboratory using a router, computers and an Android phone. In the laboratory cookie capturing was tested using a program called Droidsheep and attempts were made to capture HTTPS encrypted data using a man-in-the-middle attack.

The tests showed that the attack techniques in public Wi-Fi were working although with small reservations. Cookie capturing went without problems but the man-in-the-middle attack was more problematic. In general, it is possible to capture data from certificate protected communications but not without warnings on the target machine although it is possible to get rid of the warnings if one has physical access to the target machine. If that is the case then this is done by installing false certificates.

In conclusion, the performed tests indicate that there is cause for caution while using public Wi-Fi and it is preferable to encrypt connection using VPN.

Keywords	Public Wi-Fi, information security, man-in-the-middle attack

Sisällys

Lyhenteet

3G	Third Generation. Matkapuhelinteknologia.
4G	Fourth Generation. Matkapuhelinteknologia.
ARP	Address Resolution Protocol. Internet-protokolla.
ASLR	Address Space Layout Randomization. Mekanismi puskurin ylivuoto hyökkäyksiä vastaan.
Bit	Tiedon pienin yksikkö. 8 bittiä = 1 tavu, 1024 tavua = 1 kilotavu.
Botnet	Bottiverkko. Useiden keskenään toimimaan määritetyn botin järjestelmä.
DEP	Data Execution Prevention. Tietojen suorittamisen estäminen.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteita verkkoon kytkeytyville laitteille.
EMET	Enhanced Mitigation Experience Toolkit tietoturvasovellus.
ETSI	European Telecommunications Standards Institute. Riippumaton, voittoa tavoittelematon eurooppalainen telealan standardisoimisjärjestö.
FTP	File Transfer Protocol. Internet-protokolla.
GSM	Global System for Mobile Communications. Matkapuhelinjärjestelmä.
GPS	Global Position System. Paikannusteknologia.
HIPERLAN	HIgh PERformance radio local area network. ETSI:n langaton lähiverkko standardi.
HTTP(S)	HyperText Transfer Protocol (Secure). Internet-protokolla.

HTST	HTTP Strict Transport Security. Tietoturva mekanismi joka pakottaa selaimen käyttämään HTTPS-protokollaa yhteyden muodostamiseen.
IANA	Internet Assigned Numbers Authority. Maailmanlaajuinen Internetin hallinnointiin osallistuva järjestö.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
ICMP	Internet Control Message Protocol. Internet-protokolla.
IGMP	Internet Group Management Protocol. Internet-protokolla.
IP	Internet Protocol, TCP/IP-viitemallin verkko-kerroksen protokolla.
IPS	Intrusion Prevention Systems. Tunkeutumisenestojärjestelmä.
IPv4	Internet Protocol version 4. Neljäs versio IP-protokollasta.
IPv6	Internet Protocol version 6. Kuudes versio IP-protokollasta. Versio 4:n korvaaja tulevaisuudessa.
MAC	Media Access Control. Verkkosovittimen yksilöivä osoite.
Mbps	Megabittiä sekunnissa.
NAT	Network Address Translation. Osoitteenmuunnosverkkotekniikka.
NMT	Nordisk Mobiletelefon. Yhteispohjoismainen radiopuhelinverkko.
PAT	Port Address Translation. Porttimuunnos.
PKI	Public Key Infrastructure, julkisten avainten hallintajärjestelmä. Käytetään SSL /TLS-protokollassa.
PPP	Point to Point Protocol. Internet-protokolla.

RPD	Remote Desktop Protocol. Internet-protokolla.
SNMP	Simple Network management Protocol. Internet-protokolla.
SSID	Service set identifier. Langattoman lähiverkon verkkotunnus.
TCP	Transmission Control Protocol tietoliikenneprotokolla.
Tera	SI-järjestelmän kerrannaisyksikön etuliite, tarkoittaa miljardikertaista (10^9).
UDP	User Data Protocol. Internet-protokolla.
VoIP	Voice over Internet Protocol. Tekniikka, jonka avulla voidaan siirtää ääntä IP-protokollaa käyttävän verkon välityksellä.
VPN	Virtual Private Network virtuaalinen erillisverkko.
Wi-Fi	WLAN-tuotteiden kaupallinen nimi.
WLAN	Wireless local area network. Langaton lähiverkko.
WPA2	Wi-Fi Protected Access 2. Langattoman verkon tietoturvastandardi.

1 Johdanto

Insinöörityön innoitteena oli viime vuosien aikana tapahtunut nopea muutos Internetin käyttötavoissa jokapäiväisessä elämässä. Erityisesti sosiaalisen median suosion jatkuva kasvu on tuonut Internetin käytön paikasta ja ajasta riippumattomaksi tekemiseksi. Ennen älypuhelimien, tablettikoneiden ja pienten kannettavien yleistymistä Internetiä käytettiin joko töissä tai kotona. Nykyisin Internetiä käytetään yhä useammin kaikkialla yleistyvissä julkisissa langattomissa verkoissa (eng. Public Wi-Fi).

Sen missä verkkoa käyttää pitäisi vaikuttaa myös asioihin, joita verkossa tekee, mutta vain harva muuttaa Internetin käyttöään. Asiaa tuntemattomalle vaikuttaa siltä, että koti-, työ- ja julkisella verkolla ei ole eroja, nehän kaikki mahdollistavat Internetin käytön. Tietoturvan kannalta asia ei näin ole. Työpaikan sisäverkko on yleensä paremmin suojattu kuin kotiverkko, joka taas tarjoaa jo riittävän suojan tavalliselle käyttäjälle. Julkinen langaton verkko, jollainen löytyy esimerkiksi kahviloista, kirjastoista ja hotelleista edustaa toista ääripäätä, eli käytössä ei ole välttämättä mitään tietoturvaa parantavia ominaisuuksia.

Pyrkimyksenä on antaa tavalliselle peruskäyttäjälle ymmärtämys Internetin toiminnan mahdollistavasta tekniikasta ja erilaisista tietoturvauhkista, joihin riittämätön suojaus voi käyttäjän altistaa. Huomion painopiste on julkisissa verkoissa, koska niissä tietoturva on täysin käyttäjän itsensä vastuulla. Julkisen verkon hyökkäyskeinoista kerrotaan ja niiden toimintaa esitellään myös käytännössä, jotta lukija saisi konkreettisen kuvan vaaroista.

Tietoturva on ongelmallinen asia tavalliselle käyttäjälle. Harvalla on tietoa mahdollisista vaaroista, olivatpa ne hyökkäyksiä tai haittaohjelmia. Lisäksi tavalliselle käyttäjälle etusijalla on palveluiden ja laitteiden käytettävyys. Tietoturva voi vaikuttaa käytettävyyteen, mutta sen ei välttämättä tarvitse. Insinöörityössä tarjotaan keinot laitteiden suojaamiseen ilman, että niiden käytettävyys kärsii.

Insinöörityön tekeminen vaatii runsaasti tiedon etsintää Internetistä, jolloin pitää harjoittaa lähdekriittisyyttä. Internetistä löytyy lähes jokaiselle väittämälle sitä tukeva lähde, jos vain osaa etsiä. Internet-sivuja lähteinä käytettäessä pitikin tutkia artikkeleiden ja

sivustojen käyttämät lähteet ja joskus jopa etsiä väittämille muita lähteitä, jotta pystyi varmistumaan tiedon oikeellisuudesta.

2 Tietoturvan määritelmä

Tietoturvalla tarkoitetaan erilaisten tietojen, järjestelmien, palveluiden sekä tietoliikenteen asianmukaista suojaamista. Tietoturvan uhkia ovat luvaton pääsy, tiedon luvaton käyttö, salaisen tiedon paljastuminen, tiedon sekaannus, tiedon muuntuminen, salaisen tiedon tutkituksi tuleminen, tiedon kopioituminen ja tiedon häviäminen. [1.] Tietoturva määritellään kolmen käsitteen avulla:

Käytettävyydellä tai saatavuudella tarkoitetaan sitä, että järjestelmien tiedot ja palvelut ovat niihin oikeutettujen henkilöiden käytettävissä. Se varmistetaan fyysisellä suojauksella ja kaksinkertaistamalla laitteistoja.

Luottamuksellisuus tarkoittaa että, tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus. Tämä toteutetaan salauksen, pääsynvalvonnan, todennuksen, valtuutuksen ja fyysisen turvallisuuden avulla.

Eheys tarkoittaa että, tietojen tulee olla luotettavia, oikeita ja ajantasaisia. Tiedot eivät muutu tai ole muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena. Tietoaineiston eheys varmistetaan varmuuskopioilla, tarkistussummilla ja tietoja korjaavilla koodeilla. [2; 3.]

Näiden lisäksi on vielä AAA-protokolla, joka on menetelmä toisen osapuolen tunnistamiseen tietoverkossa. Lyhenne tulee sanoista authentication (todentaminen tai autentikointi), authorization (valtuutus) ja accounting (tilastointi).

Todennuksen tarkoituksena on tunnistaa käyttäjä tietoverkon käyttöoikeuden omaavaksi käyttäjäksi. Tunnistus voi tapahtua käyttäjätunnus-salasanayhdistelmällä, digitaalisella varmenteella tai tiettyyn puhelinnumeroon soittamalla, milloin todentaminen tehdään sen perusteella mistä numerosta soitto on tullut.

Valtuutuksella määritellään käyttäjälle käyttöoikeudet, mitä palveluita pääsee käyttämään ja mitä ei. Käyttöoikeudet voivat perustua käyttäjään itseensä tai esimerkiksi palvelua käyttävän fyysiseen sijaintiin tai kellonaikaan.

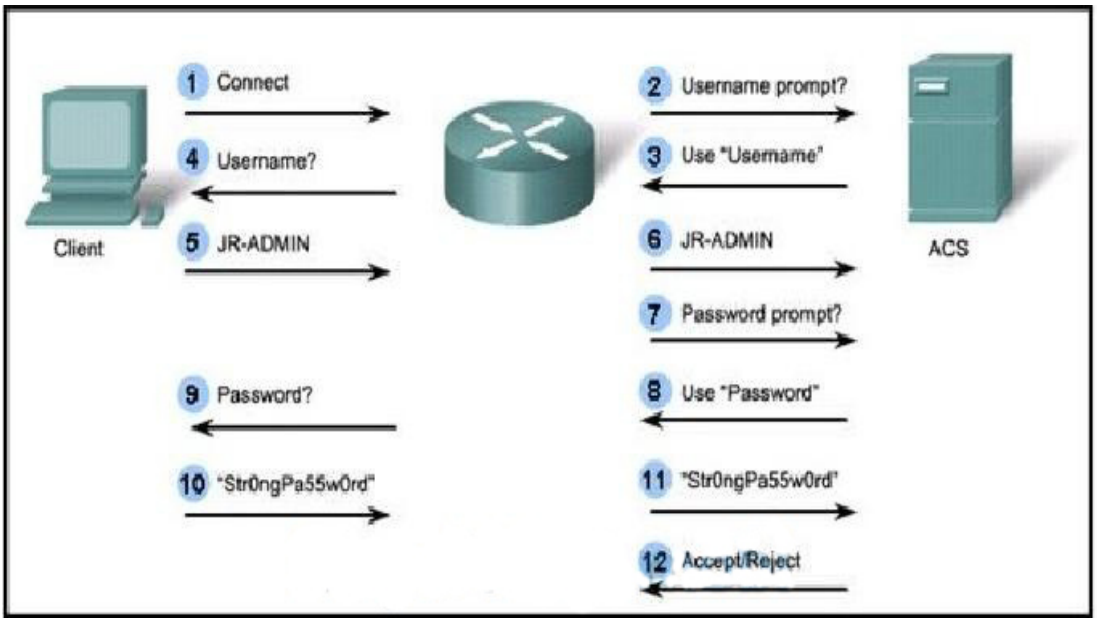
Tilastointipalvelulla pystytään keräämään käyttäjistä tilastotietoja. Näitä tietoja voivat olla muun muassa yhteyden muodostus- ja päättymisaika, mitä palveluita käytettiin, tehtiinkö muutoksia johonkin ja käyttäjätunnus sekä IP-osoite. [4.]

3 Verkkotyypit

Ihmiset käyttävät kolmentyyppisiä verkkoja: koti-, työ- ja julkisia verkkoja. Jokaisella verkkotyypillä on erilaiset tietoturvavaatimukset. Julkisessa verkossa ei yleensä ole minkäänlaisia tietoturvaa parantavia ominaisuuksia käytössä. Langattomassa kotiverkossa on oletusasetuksena vähintään verkon salasana käytössä. Työpaikan verkossa voi yhtiön panostuksesta riippuen olla useitakin tietoturvaa parantavia ominaisuuksia. Tässä luvussa esittelen mahdollisia tietoturva-asetuksia edellä mainituille verkkotyypeille.

3.1 Työpaikkaverkko

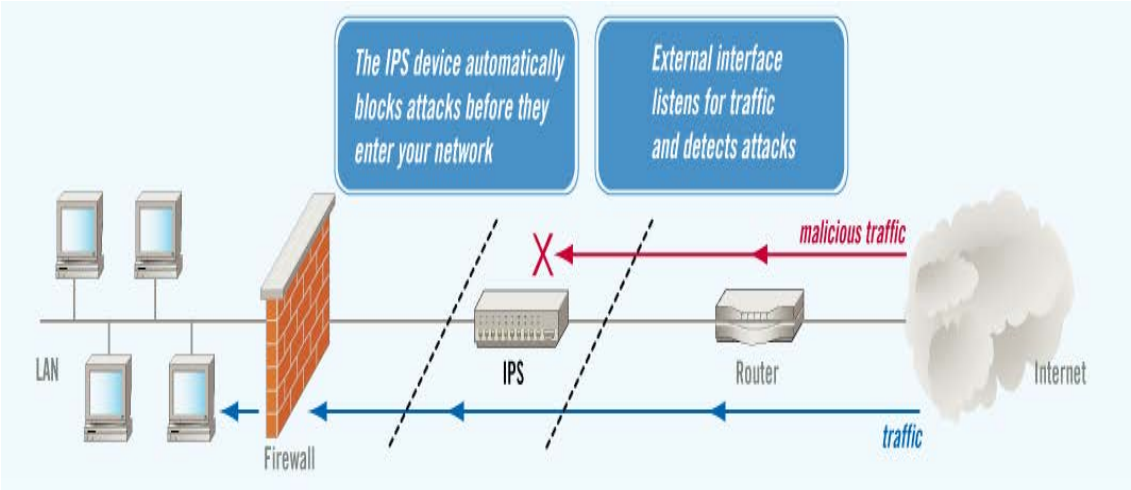
Työpaikkaverkoissa käytetään yleisesti AAA-protokollasta ainakin kahta ensimmäistä eli todennusta ja valtuutusta. Ennen kuin verkkoa pääsee käyttämään, varmistetaan, että käyttäjällä on oikeudet verkon käyttöön ja lisäksi voidaan määritellä, mitä palveluita tällä on käytössään. Langatonta verkkoa käytettäessä voidaan tarvita vielä verkontunnus ja salasana. Yhteys muodostetaan tukiasemaan (eng. Access Point), joka lähettää yhteyspyynnön eteenpäin pääsynvalvontapalvelimelle (eng. Access Control Server), missä on tietokanta, joka sisältää sallitut käyttäjänimi-salasanaparit. Palvelimen hyväksyttyä käyttäjän tämä saa pääsyn verkkoon. Kuvassa 1 on asiakaslaitteen, tukiaseman ja palvelimen välinen todennusprosessi kuvattuna vaihe vaiheelta. [5.]



Kuva 1. Verkkoyhteyden muodostus todennusta käyttävään verkkoon.[68.]

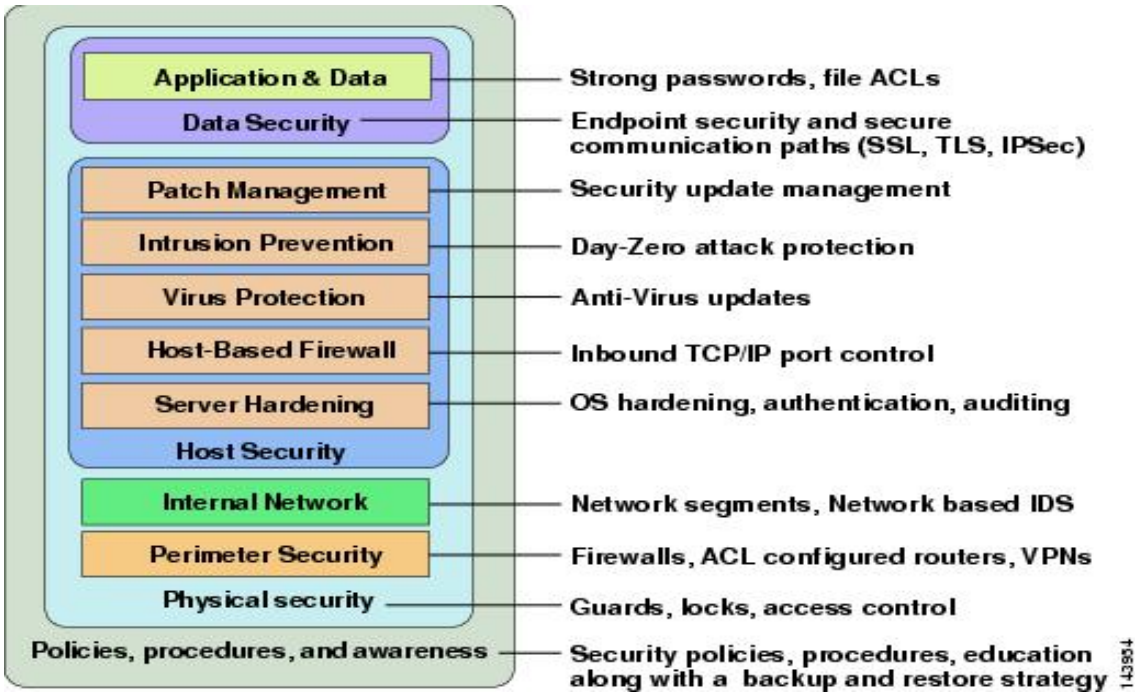
Edellä kuvatun lisäksi luvattomalta verkon käytöltä voidaan suojautua esimerkiksi poistamalla käytöstä kaikki käyttämättä olevat Ethernet-portit ja lisätä käytössä oleviin portteihin MAC-osoitesuodatin, jolloin vain laitteet, joiden verkkosovittimen MAC-osoite löytyy pääsynvalvontalistasta, voivat muodostaa verkkoyhteyden. Langattomassa verkossa voidaan myös käyttää MAC-osoitesuodatusta. Lisäksi verkkotunnuksen lähettäminen voidaan poistaa käytöstä, jolloin käyttäjän täytyy tietää se saadakseen yhteyden verkkoon. [5.]

Työpaikkaverkkojen suojaamiseen käytetään vähintään palomuuria, päivitettyjä käyttöjärjestelmiä ja ohjelmia sekä virustorjutaohjelmistoa. Näiden lisäksi yleinen ratkaisu tietoturvan parantamiseksi on IPS (Intrusion Prevention Systems) eli hyökkäyksen estojärjestelmä. IPS analysoi liikennettä tarkemmin kuin palomuuri. Se vertaa jokaista pakettia tietokantaan, joka sisältää tunnettuja hyökkäyksiä. Jos IPS tunnistaa haitallisen yhteyden, se estää yhteyden. Kuva 2 havainnollistaa verkkotopologiaa, jossa on käytössä IPS ja palomuuri. [5.]



Kuva 2. Verkkotopologia, jossa IPS ja palomuuri. [5.]

Edellä esiteltiin vähimmäistietoturva-asetuksia, joiden pitäisi löytyä jokaisen yhtiön verkosta, jossa on useita työntekijöitä ja arkaluonteista dataa. Tietoturvan rakentamiseen löytyy useita menetelmiä, yksi käytetyistä on kerroksittainen arkkitehtuuri. Siinä verkko jaetaan kerroksiin ja määritellään ratkaisut, joilla tietoturvaa parannetaan. Ciscon käyttämiä kerroksia ovat käytännöt, fyysinen turva, ulkoreuna- turva, sisäinen verkko, isäntä- ja dataturva. Kuvassa 3 esitellään eri kerrokset ja käytettyjä suojauskeinoja.[6.]



Kuva 3. Kerroksittainen arkkitehtuuri. [6.]

3.2 Kotiverkko

Tavallisessa kotona käytettävässä langattomassa verkossa riittävä tietoturvan taso saavutetaan helpommin kuin työympäristössä. Salausta käyttävässä kotiverkossa käyttäjän todennus tehdään verkon salasanalla, jonka verkkoa ylläpitävä laite tarkistaa ennen yhteyden muodostamista. Salasanaa käytetään myös tietoliikenteen salaamiseen. Kotiverkon suojaamiseen voi käyttää muun muassa seuraavia tekniikoita:

- Vahva salasana,
- MAC-osoitesuodatus,
- verkkotunnuksen lähetyksen käytöstä poistaminen,
- signaalin lähetystehon pienentäminen, jolloin verkon kantama pienenee. Jotta joku voisi murtautua verkkoon, täytyy hänen olla sen kantaman sisällä.

Edellä mainittuja keinoja voi käyttää verkkonsa suojaamiseen, mutta osaavaa hyökkääjää ne eivät estä ainoastaan hidastavat. Vahva salasana on paras keino suojata verkko luvattomalta käytöltä. Vahva salasana muodostuu isoista ja pienistä kirjaimista, numeroista ja erikoismerkeistä. Pituutta salasanalla voi olla enintään 64 merkkiä käytettäessä WPA2 (Wi-Fi Protected Access 2)-salausta, suositeltava vähimmäispituus on 16 merkkiä. [7.]

3.3 Julkinen verkko

Julkisessa langattomassa verkossa ei ole käytössä mitään tietoturvaa parantavia ominaisuuksia. Sen tehtävä on vain tarjota yhteys Internetiin ja tietoturva on verkon käyttäjän vastuulla. Tietoturvaa voi parantaa virustorjuntaohjelmistolla, palomuurilla, VPN (Virtual Private Network)-yhteydellä ja päivitetyillä ohjelmilla. Luvuissa 7 ja 9 julkisten verkkojen vaaroista ja suojaustumiskeinoista kerrotaan tarkemmin.

4 Verkkotekniikat

4.1 IEEE 802.11g/n

IEEE 802.11 on joukko standardeja langattomille WLAN (Wireless Local Area Network) -verkoille. IEEE (Institute of Electrical and Electronics Engineers) käyttää numerointijärjestelmää eri standardeille, numero 802 viittaa lähi- ja laajaverkkoihin, numero 11 osoittaa, että kyseessä ovat langattomat verkot ja kirjain lopussa kertoo protokolla version, joka määrittää taajuuden ja kaistanleveyden. Käytetyimmät WLAN-standardit ovat 802.11g (yhteyden maksiminopeus, 54Mbps) ja 802.11n (nopeuden vaihteluväli 54-600Mbps). Uusin käytössä oleva standardi on 802.11ac (500–1000Mbps). Kaikki tekniikat ovat taaksepäin yhteensopivia, joten uudellakin laitteella voi käyttää vanhalla standardilla toimivaa verkkoa.

Käyttäjän kannalta uudet standardit näkyvät suurempina siirtonopeuksina ja 802.11n standardista lähtien myös mahdollisten häiriöiden vähenemisenä. 802.11n:stä lähtien on ollut mahdollista käyttää 5 GHz:n taajuusaluetta 2,4 GHz taajuusalueen lisäksi. 2,4 GHz:n taajuudella toimivassa verkossa saattaa esiintyä häiriöitä. Näitä aiheuttavat samalla taajuudella toimivat laitteet, esimerkiksi langattomat näppäimistöt, mikroaaltouunit, puhelimet ja bluetooth. Korkeampi taajuus mahdollistaa suuremmat datasiirtonopeudet, mutta huonontaa esteiden läpäisykykyä, joka näkyy lyhempänä kantamana. [8; 9.]

4.2 TCP/IP -viitemalli

Tietokoneiden välisessä kommunikoinnissa verkon yli käytetään protokollaviitemalleja. Yleisin niistä on TCP/IP (Transport Control Protocol/ Internet Protocol)-viitemalli. Protokollaviitemalli koostuu kerroksittaisesta arkkitehtuurista, missä jokainen kerros kuvaa jotain funktiota, jonka protokolla voi suorittaa. Yhdellä kerroksella on yleensä monta protokollaa, jotka voivat hoitaa kyseisen kerroksen tehtävät. TCP/IP-viitemallia pidetään yleisesti neljä kerroksisena. Viitemallin kerrokset ovat s*ovelluskerros* (Application Layer), eli ohjelmat ja prosessit, jotka käyttävät kuljetuskerroksen protokollia siirtääkseen dataa päämääränä oleville tietokoneille. Tällä kerroksella on useita protokollia, joita ohjelmat käyttävät kommunikointiin alemman kerroksen kanssa. Näistä eniten käytettyjä ovat: HTTP(S), FTP ja SNMP. [10.]

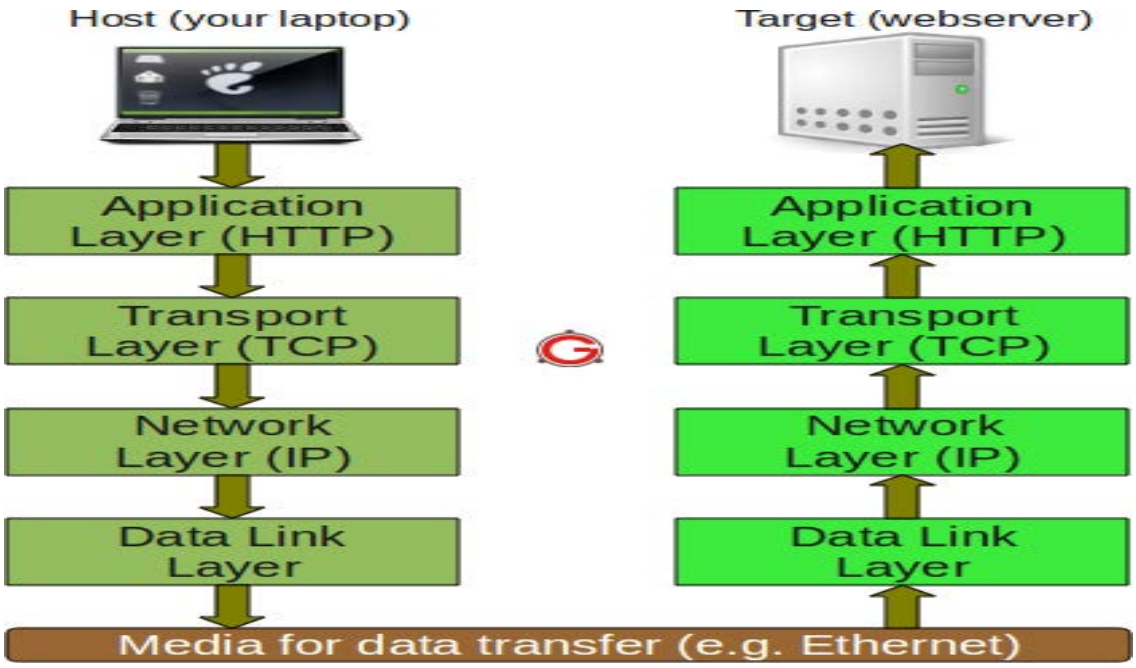
Kuljetuskerros (Transport Layer) on kahden laitteen välisen tiedonsiirron selkäranka. Tälläkin kerroksella on useita protokollia, mutta kahta käytetään selvästi eniten, nämä ovat TCP ja UDP. TCP-protokollaa käytetään, kun on tarvetta ”luotettavalle yhteydelle”, UDP (User Data Protocol) -protokollaa käytetään, kun riittää ”epäluotettava yhteys”. [10.]

TCP-protokolla jakaa datan, joka tulee sovelluskerrokselta, sopivan kokoisiin segmentteihin ja lähettää ne verkkoon. Se vahvistaa paketit vastaanotetuiksi, odottaa vahvistusta lähetetyistä paketeista ja asettaa aikakatkaisun uudelleen lähettämistä varten, jos vahvistusta ei ole tullut määritellyssä ajassa. Termiä ”luotettava yhteys” käytetään silloin kun on toivottavaa, ettei siirretystä datasta katoa bittiäkään. TCP-protokolla tarjoaa tarvittavan mekanismin tämän varmistamiseen. Tämän tyyppistä yhteyttä tarvitaan esimerkiksi tiedoston latauksessa, jolloin puuttuva data saattaisi johtaa tiedoston korruptoitumiseen. [10.]

UDP-protokolla tarjoaa hieman yksinkertaisemman, mutta epäluotettavamman palvelun pakettien lähettämiseen koneelta toiselle. Protokolla ei varmista millään tavalla, onko lähetetty data saapunut perille vai ei. Termiä ”epäluotettava yhteys” käytetään silloin kun kaiken datan ei tarvitse saapua perille suoritettavan asian onnistumiseksi. UDP-protokollaa käytetäänkin muun muassa reaaliaikaista siirtoa vaativissa palveluissa kuten median suoratoistossa ja VoIP-palveluissa. Data- ja puhepakettien siirrossa ei ole haittaa, vaikka osa datasta jäisi saapumatta, koska uusi saapuva data muuttaa edeltänyttä tilaa. [10.]

Verkkokerros (Network Layer) tunnetaan myös Internet-kerroksena. Kerroksen päätehtävä on organisoida ja hoitaa datan reitittäminen verkossa. Pääasiassa IP-protokolla hoitaa tämän kerroksen tehtävät. Muita protokollia tällä kerroksella ovat muun muassa IGMP- ja ICMP-protokollat. Tällä hetkellä vielä IPv4 on pääasiassa käytössä, lähivuosina tapahtuu siirtyminen uudempaan Ipv6:een. [10.]

Siirtokerroksesta (Data Link Layer) käytetään myös nimeä verkkosovitinkerros, joka koostuu käyttöjärjestelmän laiteajureista ja laitteiden verkkokorteista. Laiteajurit ja verkkokortti hoitavat kommunikoinnin yksityiskohdat tiedonsiirtovälineen kanssa. Tämä väline on yleensä Ethernet-kaapeli tai muu tiedonsiirrossa käytettävä media. Kerroksen käytetyimmät protokollat ovat ARP- ja PPP-protokollat. Kuvassa 4 tietokoneen ja palvelimen välinen yhteys verkkokerroksittain. [10.]



Kuva 4. TCP /IP -viitemallin kerrokset. [10.]

4.3 Osoitteistus

4.3.1 IP-osoite

Jotta Internet toimisi eli välittäisi tietoa laitteelta toiselle, tarvitaan keino yksilöidä laitteet. Internet-protokollaosoite, IP-osoite, suorittaa tämän tehtävän. Se antaa jokaiselle verkkoon kuuluvalle laitteelle uniikin 32-bittisen numeerisen arvon, joka toimii laitteen osoitteena. Tämän avulla laite pystyy lähettämään ja vastaanottamaan IP-paketteja. Tällä hetkellä on vielä käytössä IP:n versio 4, joka mahdollistaa noin 4,3 miljardia (2^32) osoitetta. Vaikka osoitemäärä on iso, on se kuitenkin nykyään riittämätön laitteiden suuren määrän vuoksi. Tämän ongelman ratkaisuksi kehitettiin osoitteenmuunnos (eng. NAT). Osoitteenmuunnoksen avulla useat koneet, jotka ovat samassa aliverkossa, voivat lähettää ja vastaanottaa Internet-liikennettä käyttäen vain yhtä julkista IP-osoitetta. Osoitteenmuunnoksen suorittaa useimmiten reititin tai palomuuri. Yhden julkisen IP-osoitteen alla voi olla useita aliverkkoja, jotka kommunikoivat keskenään ja Internetin kanssa. Tällöin käytetään porttimuunnosta (eng. PAT). Porttimuunnoksessa muodostetaan IP-osoite-porttipareja yksilöimään laitteet. Osoitteenmuunnoksen käyttötarve tähän tarkoitukseen poistuu tulevaisuudessa, kun otetaan käyttöön IP-versio 6. Siinä on osoitteita noin 340 sekstiljoonaa (2^128). [11.]

4.3.2 MAC-osoite

MAC-osoite (eng. Media Access Control) on uniikki tunniste verkkosovittimessa, joka mahdollistaa yhteydet fyysisellä verkkosegmentillä. MAC-osoitteita käytetään verkko-osoitteena suurimmassa osassa IEEE 802-verkkoteknologioita, mukaan lukien Ethernet ja Wi-Fi. MAC-osoite ja IP-osoite kumpikin yksilöivät laitteen, mutta ne toimivat eri tasoilla TCP/IP-viitemallissa. MAC-osoitetta käytetään tunnistamaan laitteet samassa verkossa siirtokerroksessa, se toimii siis linkkien välillä. IP-osoite on globaali osoite, jota käytetään verkkokerroksessa tunnistamaan tietokoneet eri verkoissa. [12.]

4.3.3 Portit

Portit ovat TCP/IP-viitemallia käyttävissä tietokoneissa olevia numeroituja palvelupisteitä. Verkossa kommunikoitaessa IP-osoitetta käytetään lähettäjän ja määränpään tunnistamiseen, portteja käytetään määrittämään haluttu palvelu. Jokaisella ohjelmalla joka on verkkoon yhteydessä on oma porttinumero, jonka avulla tietokone tietää, mihin palveluun yritetään ottaa yhteyttä. Eri koneilla voi olla ohjelmia, jotka käyttävät samaa porttia, mutta jos ohjelmat ovat samalla koneella, pitää niillä olla eri porttinumerot. Ohjelmalla on porttinumero väliltä 0-65535; nämä numerot on jaettu kolmeen kategoriaan, jotta ohjelmat eivät käyttäisi päällekkäisiä porttinumeroita. [13.]

Portit välillä 0–1023 ovat niin kutsuttaja ”hyvin tunnettuja portteja”. Nämä porttinumerot on varattu tavallisimmille palvelinprosesseille, kuten HTTP (portti nro 80) ja HTTPS (portti nro 443). [13.]

Rekisteröidyt portit ovat väliltä 1024–49151, IANA (Internet Assigned Numbers Authority) voi rekisteröidä pitkään käytetylle palvelulle pysyvän portin tältä alueelta. Esimerkiksi porttinumero 3389 on varattu Microsoftin RDP-protokollalle. [13.]

Kolmas kategoria on dynaamiset tai yksityiset portit, näiden porttien alue on 49152–65535. Näitä portteja ei ole pysyvästi assosioitu millekään palvelulle. [13.]

4.4 Protokollat

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) on kahden Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä. IP-protokolla on alin yhtenäinen Internetin protokolla. IP-paketteihin on sisällytetty kaikki ylempien kerrosten protokollat. Vaikka TCP/IP-protokollaperheeseen kuuluu monia muitakin protokollia, pääosa liikennöinnistä tapahtuu TCP-yhteyksinä IP-protokollien päällä. TCP-protokolla luo yhteydet tietokoneiden sovellusten välille käyttäen IP-paketteja. [14.]

HTTP/HTTPS

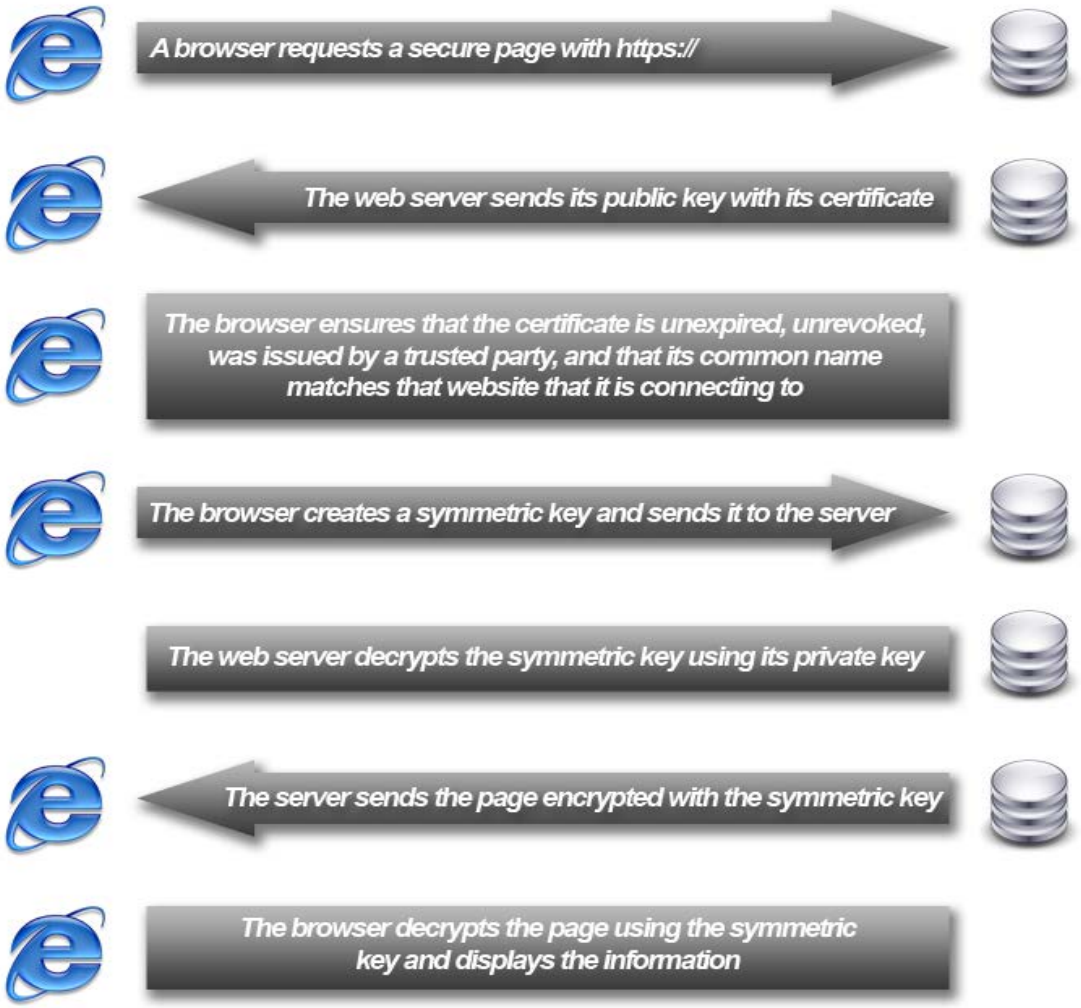
HTTP (Hypertext Transfer Protocol eli Hypertekstin siirtoprotokolla) on protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon. HTTP:aa käytettäessä asiakaskoneen ja palvelimen välinen dataliikenne on salaamatonta ja näin ollen ulkopuolinen voi salakuunnella liikennettä. HTTP:aa käytettäessä ei pitäisikään koskaan siirtää arkaluontoista tietoa, kuten henkilötietoja tai maksutietoja. HTTPS (Hypertext Transfer Protocol Secure) on HTTP:n ja SSL/TLS-protokollan yhdistelmä, jota käytetään arkaluonteisen datan siirtoon Internetissä. Tiedot salataan ennen lähettämistä SSL-protokollan (tai uudemman miltei samanlaisen TLS-protokollan) avulla. HTTPS-yhteyksiä käytetään kun on tarvetta salata liikenne, esimerkiksi luottokortti- tai henkilötiedot ovat tallaisia tietoja. [15; 16.]

SSL/TLS

Vanhalta nimeltään Secure Socket Layer (SSL), nykyisin Transport Layer Security (TLS), on salausprotokolla. Sitä käytetään salaamaan Internet-sovellusten välinen tietoliikenne IP-verkkojen yli. Se on nykyisin yksi tavallisimpia tapoja suojata tietoliikennettä. Protokollan toiminta perustuu varmenteisiin, joilla sivustot todistavat olevansa niitä mitä väittävät. [17; 18.]

Varmenne on digitaalinen identifikaatio, jota käyttäen palvelun tarjoaja voi todistaa olevansa luotettava. Varmenteita myöntää Certification Authority (CA). Suomen valtion virallinen varmentaja on Väestörekisterikeskus. Kansainvälisesti luotettuja varmentajia ovat muun muassa Verisign ja Entrust. Varmenteen saadakseen hakijan pitää läpäistä

tiukka hyväksymisprosessi. Jotta varmenteet toimisivat, niiden täytyy olla rakenteeltaan samanlaisia riippumatta varmenteen myöntäjästä. Tähän käytetään PKI:a (Public Key Infrastructure, julkisten avainten hallintojärjestelmä), joka koostuu protokollista, standardeista ja palveluista. X.509-standardi,jota käytetään SSL /TLS-protokollassa on yksi näistä standardeista. Varmenteen salauksen vahvuus voi vaihdella mutta yleisin käytetty on 128-bittinen. Kuvassa 5 on HTTPS-yhteyden muodostamisen vaiheet esitettynä. [19.]



Kuva 5. HTTPS-yhteyden muodostus prosessi. [69.]

5 Käyttöjärjestelmät

5.1 Microsoft Windows

Microsoftin kehittämä Windows on maailman suosituin käyttöjärjestelmä tietokoneissa, yli 90 %:n markkinaosuudellaan. Windowsista löytyy useita eri versioita mutta suosituin on Windows 7, noin 55 % kaikista koneista käyttää sitä. [20.] Windows on saanut nimensä siitä, että ohjelmia käytetään ikkunoissa (eng. windows), tämä helpottaa useiden ohjelmien samanaikaista käyttämistä. Windowsin tietoturva riippuu paljolti käytettävästä versiosta ja päivitysten tuoreudesta, Microsoft julkaisee aktiivisesti tietoturvapäivityksiä uusimpiin versioihin (Vista, 7, 8 ja 8.1) mutta Windows XP:tä ja tätä vanhempia versioita ei enää tueta. Windows eri versioineen on ollut jo vuosikymmeniä haittaohjelmien tekijöiden pääkohde. Windowsille suunnatut haittaohjelmat käyttävät niin käyttöjärjestelmistä kuin ohjelmista löytyviä haavoittuvuuksia hyväkseen. Haittaohjelmien suureen määrään vaikuttaa Windowsin suosio, joten yhdellä toimivalla haittaohjelmalla on mahdollista saastuttaa miljoonia koneita. [21.]

Microsoft on pyrkinyt tekemään Windowsista turvallisemman ja käyttöjärjestelmästä löytyikin vuonna 2014 vähiten tietoturva-aukkoja. Samaan aikaan kilpailevat käyttöjärjestelmät ovat kasvattaneet suosiotaan, erityisesti tabletti- ja kännykkämarkkinoilla, missä Microsoftin mobiilikäyttöjärjestelmällä on vain muutaman prosentin markkinaosuus. Mobiilipuolen laitteiden suosion kasvusta löytyykin yksi syy, miksi esimerkiksi Applen käyttöjärjestelmistä löytyy enemmän haavoittuvuuksia kuin aikaisemmin. Sitä mukaa kun käyttäjäkunta kasvaa, siirtyy haittaohjelmien tekijöiden mielenkiinto kyseiseen järjestelmään. Viime vuonna eniten tietoturva-aukkoja löytyi Applen tietokoneille suunnatusta Mac OS X:stä ja saman yhtiön mobiilikäyttöjärjestelmästä iOS. [21.]

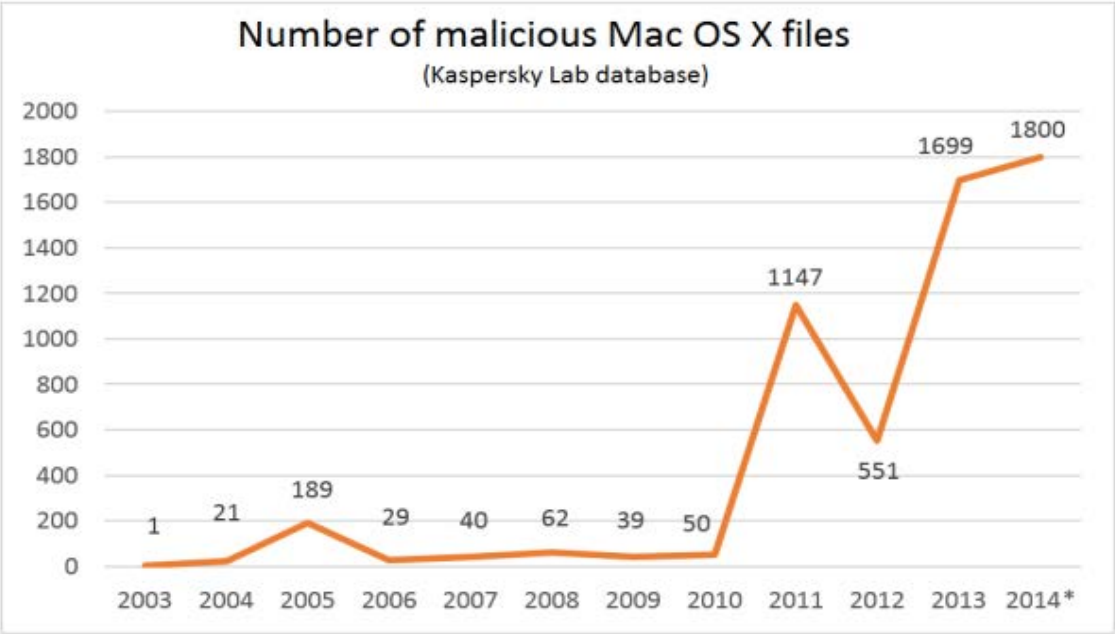
Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

Taulukko 1. Löydetyt haavoittuvuudet käyttöjärjestelmistä vuonna 2014. [22.]

5.2 Apple OS X

Apple OS X suunniteltu toimimaan Macintosh-koneilla, joihin se on esiasennettu vuodesta 2002 lähtien. OS X on kymmenes versio Applen käyttöjärjestelmästä Macintosh-tietokoneille. Windows-versioita on samanaikaisesti käytössä useita, mutta OS X on julkaisustaan lähtien päivitetty jokaiselle käyttäjälleen. Ensimmäinen vuoden 2002 versio 10.0 oli koodinimeltään ”Cheetah”, sen jälkeen käyttöjärjestelmä on saanut kymmenen suurta päivitystä ja nykyinen on versio 10.10 ”Yosemite”. [23.]

Applen OS X:ntä on pidetty turvallisempana vaihtoehtona Windowsille, vaikka maine ei välttämättä täysin pitänytkään paikkaansa OS X:n paremman koodauksen, vaan pienemmän suosion takia. Viime vuosiin asti OS X:tä käyttäviä laitteita on ollut suhteellisen vähän verrattuna Windows-laitteisiin, joten tietoturva-aukkojen etsiminen ja haittaohjelmien kehittäminen ei ole ollut taloudellisesti erityisen kannattavaa. Applen laitteiden suosion kasvettua on tilanne muuttunut. Haittaohjelmia kehitetään enenevissä määrin Macintosh-koneille ja Applen valmistamille mobiililaitteille, jotka käyttävät iOS-mobiilikäyttöjärjestelmää. Kuten taulukko 1 osoittaa, vuonna 2014 löydettiin Applen järjestelmistä eniten haavoittuvuuksia. Tätä ei pidä kuitenkaan sekoittaa haittaohjelmien määrään, OS X on haittaohjelmien määrässä vielä kaukana Windowsin luvuista, vaikkakin kasvu on ollut viime vuosina nopeaa, mikä käy ilmi tietoturvayhtiö Kaspersky Labin julkaisemasta tilastosta, joka on esitettynä kuvassa 6. [23.]



Kuva 6. OS X haitallisten ohjelmien määrä. [70.]

5.3 Mobiilikäyttöjärjestelmät

Android

Android on Googlen kehittämä Linux-pohjainen mobiililaitteille suunnattu käyttöjärjestelmä. Käyttöliittymä on suunniteltu erityisesti kosketusnäytöllisille laitteille, kuten älypuhelimille ja tablettikoneille. Android on suosittu teknologia yhtiöiden keskuudessa, jotka tarvitsevat valmiin, halvan ja kustomoitavan käyttöjärjestelmän laitteisiinsa. Android on avoimen lähdekoodin ympäristö, joka onkin innostanut suuren joukon kehittäjiä ja harrastelijoita luomaan erilaisia sovelluksia ja käyttöjärjestelmä versioita. [49.]

iOS

iOS on Applen kehittämä käyttöjärjestelmä joka on käytössä vain Applen omissa tuotteissa, kuten iPhone, iWatch. iOS perustuu Darwin BSD-käyttöjärjestelmään ja joihinkin Mac OS X-jakelun komponentteihin. Kuten Andoid on iOS:kin suunniteltu käytettäväksi kosketusnäytöllä. [50.]

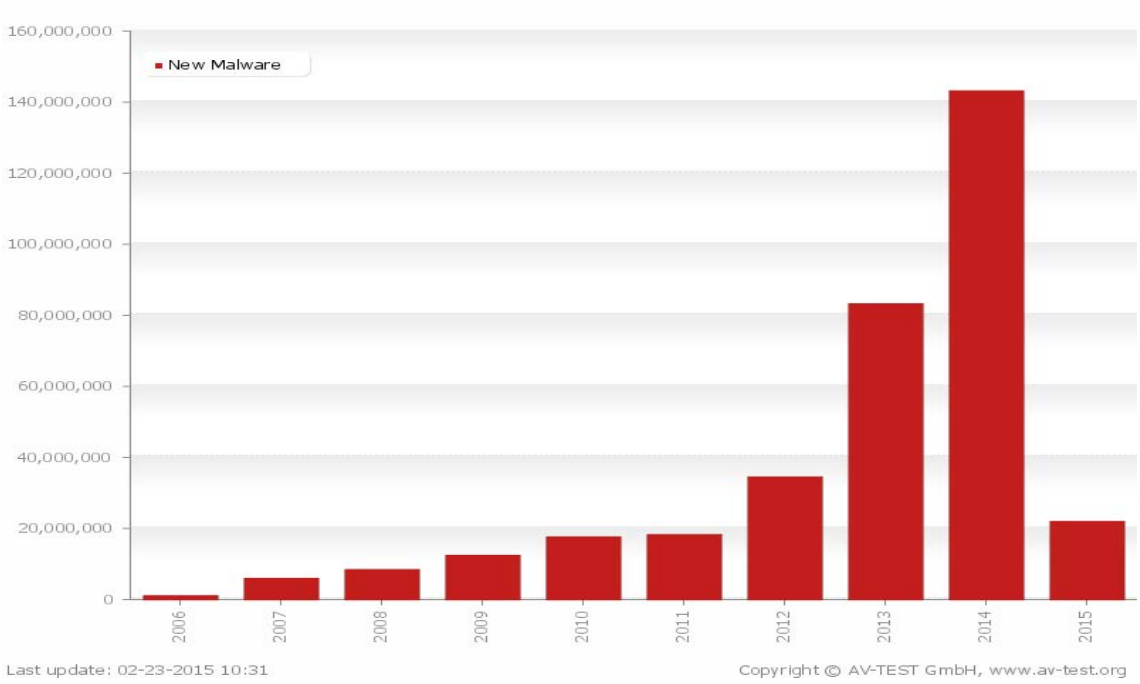
Windows Phone

Windows Phone (WP) on osa käyttöjärjestelmien tuoteperhettä, jonka on kehittänyt Microsoft. WP kehitettiin seuraajaksi Windows Mobilelle (WM) ja Zunelle. Päinvastoin kuin WM, WP on kehitetty pääasiassa kuluttajamarkkinoille eikä yritys käyttöön. Microsoft julkaisee Windows Phonelle seuraajan vuoden 2015 aikana Windows 10 myötä. Uuden käyttöjärjestelmän on tarkoitus tarjota yhtenäinen kokemus mobiili- ja PC-puolen välillä. [51.]

6 Haittaohjelmat

Haittaohjelma on yleiskäsite tietokoneohjelmille, jotka tarkoituksellisesti aiheuttavat ei-toivottuja tapahtumia tietokoneessa tai tietojärjestelmässä. Nämä ohjelmat voidaan jaotella sen mukaan, miten ne leviävät, tekevät tai suoritetaan. Haittaohjelmien aiheuttamat ongelmat eivät ole vain harvojen käyttäjien riesa. Arviolta 32 % maailman tietokoneista on saastunut jonkin tyyppisellä haittaohjelmalla. Saastuneet koneet eivät jakaudu tasaisesti eri maiden kesken. Pahiten haittaohjelmista kärsivä maa on Kiina, jossa yli 50 %:ssa koneista on haittaohjelma, Aasian maissa on muutenkin keskiarvoa enemmän saastuneita koneita. Puhtaimmat koneet löytyvät Euroopasta, Ruotsissa 20 %:ssa koneista on haittaohjelma, Suomen vastaava luku on noin 22 %. [24.]

Haittaohjelmat eivät aiheuta vain riesaa uhreilleen vaan jopa huomattavia taloudellisia tappioita. Vuonna 2014 pelkästään Yhdysvalloissa taloudelliset menetykset olivat arviolta 4,55 miljardia dollaria. Yhdysvalloissa haittaohjelmat aiheuttavat monia muitakin ongelmia: arviolta 24 miljoonaa kotitaloutta kärsii suuresta roskipostimäärästä, 16 miljoonalla on ollut viruksista aiheutuneita ongelmia viimeisen kahden vuoden aikana, 8 miljoonalla on ollut ongelmia vakoiluohjelmista edellisen puolen vuoden aikana ja miljoona kotitaloutta on menettänyt rahaa tai heidän tilejään on käytetty luvattomasti haittaohjelman avulla. Taloudellisten hyötyjen ollessa suuret haittaohjelmien määrä vain jatkaa kasvuaan, viime vuonna luotiin keskimäärin 74 000 uutta haittaohjelmaa joka päivä. Kuva 7 esittää haittaohjelmien kasvun vuositasolla, kuvassa 8 on erilaisten haittaohjelmatyyppien prosentuaalinen jakauma kaikista haittaohjelmista. [24.]



Kuva 7. Vuosittainen uusien haittaohjelmien määrä. [71.]

Virukset

Virukset ovat haittaohjelmia, jotka ovat kykeneviä monistamaan itsensä ja leviämään tietokoneesta toiseen. Virukset leviävät kiinnittymällä johonkin tiedostoon. Virukset eivät kuitenkaan käynnisty ilman käyttäjän toimia. Tietokoneen käyttäjän täytyy suorittaa ohjelma tai avata tiedosto, johon virus on piiloutunut, jotta virus voi suorittaa itsensä. Viruksia voi käyttää useisiin tehtäviin, muun muassa varastamaan tietoa, vahingoittamaan tietokonetta tai tietoverkkoa sekä bottiverkkojen luomiseen. [25; 26.]

Troijalainen

Troijalaiset eli Troijan hevoset ovat tietokoneohjelmia, joita levitetään hyödyllisiltä ohjelmilta vaikuttavien ohjelmien avulla. Käyttäjiä houkutellaan avaamaan troijalaisen sisältämä ohjelma tietokoneellaan, jotta ohjelmaan kätketty ominaisuus pääsisi saastuttamaan tietokoneen. Tämän jälkeen krakkerit voivat etsiä tartunnan saaneita tietokoneita omilla ohjelmillaan ja ottaa tietokoneen haltuunsa troijalaisen avulla. Saatuaan pääsyn tietokoneeseen hyökkääjä voi muun muassa varastaa dataa, asentaa lisää haittaohjelmia, monitoroida uhrin koneen käyttöä, käyttää konetta bottiverkon osana ja piilottaa toimiensa luoman verkkoliikenteen. [25; 26.]

Madot

Madot ovat yksi yleisimmistä haittaohjelmatyypeistä. Ne leviävät itsenäisesti ja lähettävät verkkoon itsestään täydellisiä kopioita käyttäen hyväkseen käyttöjärjestelmistä löytyviä haavoittuvuuksia. Madot leviävät yleensä hyvin nopeasti, sillä ne voivat lähettää itsensä esimerkiksi kaikille sähköpostiohjelman osoitekirjan kontakteille. Madot voivat levitessään aiheuttaa myös haittaa tietoverkoille käyttämällä verkon siirtokaistaa ja rasittamalla web-palveluita. Matoja voidaan käyttää myös kuljettamaan haitallista koodia, joka voi vaikuttaa tietokoneeseen muutenkin kuin vain levittääkseen matoa. Nämä haittakoodit on yleensä suunniteltu varastamaan dataa, tuhoamaan tiedostoja tai luomaan bottiverkkoja. [25; 26.]

Rootkit

Rootkitit ovat haittaohjelmatyyppejä, jotka on suunniteltu luomaan etäyhteys tai ottamaan haltuunsa tietokone ilman että koneen käyttäjä tai tietoturvaohjelma huomaa sitä. Rootkitin asennuttua koneelle hyökkääjä voi etänä suorittaa ohjelmia, varastaa dataa, muokata järjestelmäasetuksia ja muunnella ohjelmistoja, erityisesti tietoturvaohjelmia jotta ne eivät havaitse sitä. Rootkit leviää harmittomilta näyttävien ohjelmien tai virusten mukana. [25; 26.]

Mainosohjelmat

Mainosohjelmat näyttävät tietokoneen näytöllä mainoksia automaattisesti ilman käyttäjän lupaa. Yleensä toiminta näkyy pop-up-ikkunoina saastuneella koneella. Mainosohjelmat on yleensä liitetty maksullisten ohjelmien ilmaisversioiden asennustiedostoon. Suurin osa mainosohjelmista on mainosyhtiöiden luomia ja ne toimivat osana yhtiön tulojen muodostamista. Mainostajat saavat rahaa jokaisesta näyttämästään mainoksesta. [25; 26.]

Vakoiluohjelmat

Vakoiluohjelmien tarkoituksena on kerätä dataa ilman käyttäjän tietoa. Keräystapoja ovat muun muassa: toimintamonitorointi, datan kerääminen, näppäinpainallusten tallentaminen. Vakoiluohjelmat pystyvät myös muuttamaan ohjelmien tietoturva-asetuksia tai vaikuttamaan selaimen verkkoyhteyksiin. Vakoiluohjelmat leviävät hyväksikäyttä-

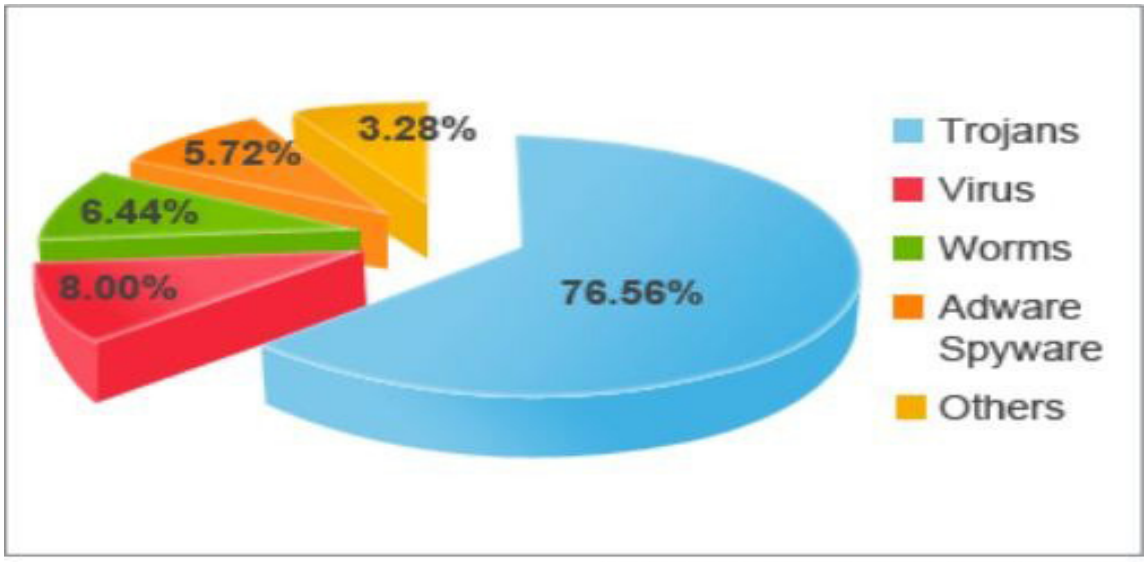
mällä ohjelmistojen haavoittuvuuksia, piiloutumalla laillisiin ohjelmiin tai troijalaisten mukana. [25; 26.]

Kiristysohjelmat

Kiristysohjelmat ovat suhteellisen uusi lisä haittaohjelmaperheeseen. Ne käytännössä pitävät tietokonetta panttivankina ja vaativat lunnaita. Kiristysohjelma rajoittaa koneen käyttäjän pääsyä koneella oleviin tiedostoihin, joko salaamalla osan kovalevystä tai lukitsemalla käyttäjän koko järjestelmän ulkopuolelle. Tämän lisäksi ohjelma näyttää viestejä, joissa uhria pyydetään maksamaan ”lunnaat” saadakseen tietokoneen kontrollin takaisin. Kiristysohjelma leviää tietokoneelle ladatun tiedoston mukana tai verkkopalvelussa olevan haavoittuvuuden kautta. [25; 26.]

Botit

Botti on ohjelma, joka suorittaa automaattisia tehtäviä internetissä. Normaalisti botit suorittavat tehtäviä, jotka ovat yksinkertaisia ja itseään toistavia. Botit pystyvät tekemään tehtävät moninkertaisella nopeudella ihmiseen verrattuna. Alkujaan botteja käytettiin webbisivujen indeksointiin hakukoneita varten. Nykyään botteja käytetään myös haitallisiin tarkoituksiin. Niiden avulla voidaan luoda bottiverkko, ryhmä tietokoneita, joita voidaan käyttää palvelinestohyökkäyksiin. [25; 26.]



Kuva 8. Haittaohjelmatyyppien jakauma. [27.]

7 Julkisen verkon hyökkäystekniikat

7.1 Urkinta

Julkisessa langattomassa verkossa reititin lähettää saapuvan datan kaikille verkossa oleville laitteille. Asiakaslaite tunnistaa sille kuuluvan datan MAC-osoitteen perusteella. Datan lähettäminen koko verkkoon mahdollistaa hyökkääjän ottamaan muidenkin laitteiden liikenteen vastaan ja saamaan haltuunsa Internet-istuntojen evästeet. Evästeiden avulla hyökkääjä voi kaapata muiden käyttäjien Internet-istunnot.[28.]

Verkkoliikenteen urkintaan löytyy monia ohjelmia. Joidenkin ohjelmien käyttäminen on tehty helpoksi eikä vaadi juurikaan tietoteknistä osaamista. Tunnetuimmat ohjelmat tähän tarkoitukseen ovat Firefox-selaimen lisäosa Firesheep ja Wireshark. Wiresharkin käyttö vaatii ohjelman tuntemista ja apuohjelmia istunnon kaappaamiseen. Firesheep suorittaa istunnon kaappauksen vaivattomammin. Ohjelman tekijä Eric Butler halusi herättää ihmiset huomaamaan kuinka helppoa tavallisen käyttäjän on toteuttaa hyökkäys. [28.]

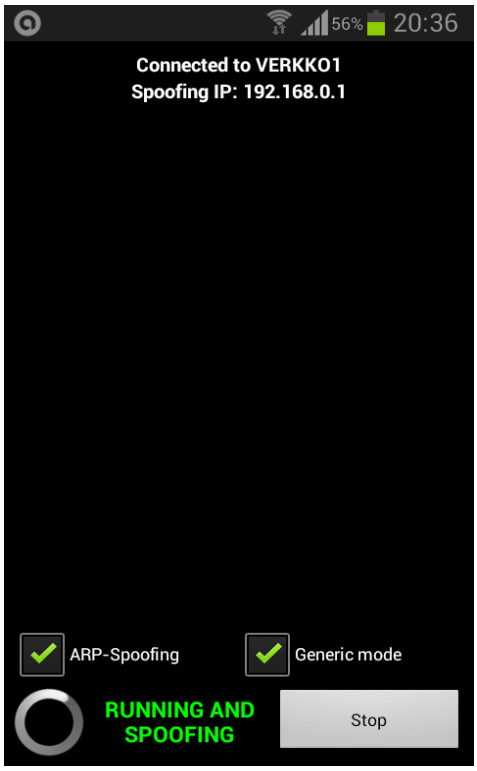
Firesheep

Käyttäjän vierailu sivustolla alkaa usein antamalla käyttäjänimi ja salasana. Seuraavaksi palvelin tarkistaa, löytyvätkö vastaavat tiedot ja jos löytyvät, se lähettää selaimelle evästeen. Selain tallentaa evästeen ja käyttää sitä kaikkiin tulevaisuudessa sivustolle tehtäviin pyyntöihin. Suurin osa Internet-sivustoista salaa sisään-kirjautumisen, käyttäen HTTPS-protokollaa. Sisäänkirjautumisen jälkeen käytetään kuitenkin salaamatonta HTTP-protokollaa. Tämän johdosta istunnon eväste on mahdollista kaapata. HTTP-istunnon kaappaamisessa (eng. sidejacking) hyökkääjä kopioi uhrin evästeen. Eväste sisältää uhrin istuntotunnisteen, jonka avulla palvelin tunnistaa eri käyttäjien istunnot. Evästeen saatuaan hyökkääjä voi sitä käyttäen avata omassa selaimessaan saman istunnon kuin uhrinsa. Julkisessa verkossa evästeet ovat käytännössä kaikkien näkyvillä, mikä tekee tämän tyyppiset hyökkäykset erittäin helpoiksi. [29.]

Urkinnan toteuttaminen

Firesheep-ohjelmasta ei ole julkaistu uutta versiota useaan vuoteen ja ohjelma ei toimi uudemmilla Firefox-selaimen versioilla. Joten urkinnan suorittamiseen käytettiin ohjelman Android versiota nimeltä Droidsheep.

Verkkoliikenteen urkintaa esitellään käytännössä, jotta lukija ymmärtäisi julkisen verkon käytön riskit paremmin. Tavoitteena oli kaapata kohdekoneen Internet istunnon evästeet ja näin mahdollistaa istunnon kaappaus. Urkinta tehtiin koulun tietoverkkolaboratoriossa luomalla julkinen langaton verkko, jossa oli kaksi laitetta. Toinen oli kohdetietokone, jonka evästeitä yrittäisin kaapata, ja toinen oli Android-puhelin, jossa oli Droidsheep asennettuna. Tässä tapauksessa kohdekoneita ei ollut kuin yksi, mutta Droidsheep kaappaa kaikki salaamattomat evästeet, riippumatta siitä, montako laitetta verkossa on.



Kuvassa 9 aloitusnäkymä ohjelman käynnistyttyä, puhelimella on yhteys verkkoon ja ARP-väärennös on automaattisesti käynnistetty.

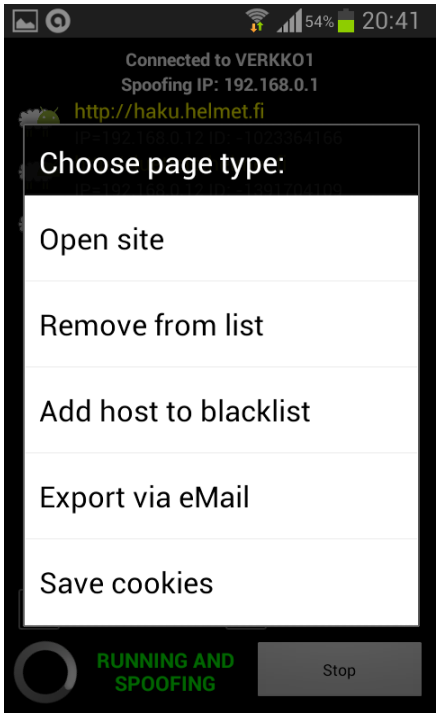
ARP-Spoofing eli ARP-väärentäminen on käynnissä, puhelimen MAC-osoite on sama kuin verkon reitittimellä, joten puhelin ottaa vastaan muiden laitteiden ja reitittimen välisen liikenteen.

Generic mode tarkoittaa että ohjelma näyttää kaikki mahdolliset istunnot, joissa käytetään käyttäjätiliä.

Kuva 9. Aloitusnäkymä.

Kirjauduin kohdekoneella kirjaston Helmet-palveluun. Sivusto käyttää HTTPS-yhteyttä sisäänkirjautumisessa, mutta tämän jälkeen siirtyy takaisin HTTP-yhteyteen. Tässä vaiheessa Droidsheep pystyy kaappaamaan evästeet, jotka sisältävät istuntotunnisteen. Kuvassa 10 on ohjelman kaappaamat evästeet.

Kuva 10. Evästeiden kaappaaminen.



Evästeiden kaappaamisen jälkeen tarvitsee vain valita eväste ja painaa avautuvasta valikosta ”Open site”. Kuva 11 esittää mahdolliset toimenpiteet, jotka voi tehdä valitulle evästeelle.

Kuva 11. Valikkonäkymä.

”Open site” -toiminnon jälkeen aukeaa puhelimessa oleva Internet-selain ja kaapattu istunto. Tässä tapauksessa toisella koneella käynnissä oleva Helmet-palvelun istunto. Kohdekoneella istunnossa ei tapahtunut mitään muutosta.

Hyökkäys ei toimi sivuilla, jotka käyttävät sisäänkirjautumisen jälkeenkin HTTPS-protokollaa. Tällaisia sivuja ovat mm. Facebook ja Gmail. Kuvassa 12 on avattu puhelimen selain ja onnistuneesti kaapattu istunto.

Kuva 12. Onnistunut istunnon kaappaus.

7.2 Väliintulohyökkäys

Väliintulohyökkäys eli MITM (Man-in-the-middle) -hyökkäys on erittäin yksinkertainen perusidealtaan. Hyökkääjä asettaa itsensä kahden osapuolen väliin, niin että liikenne kulkee hänen kauttaan. Hyökkäys on erityisen helppo toteuttaa julkisessa verkossa. Hyökkääjä voi joko luoda oman verkon, jolla on uskottavalta kuulostava nimi, esimerkiksi lähellä sijaitsevan kahvilan nimi. Verkossa, missä hyökkääjällä on käyttöoikeudet reitittimelle, hän voi valvoa kaikkea verkossa tapahtuvaa liikennettä. [31.]

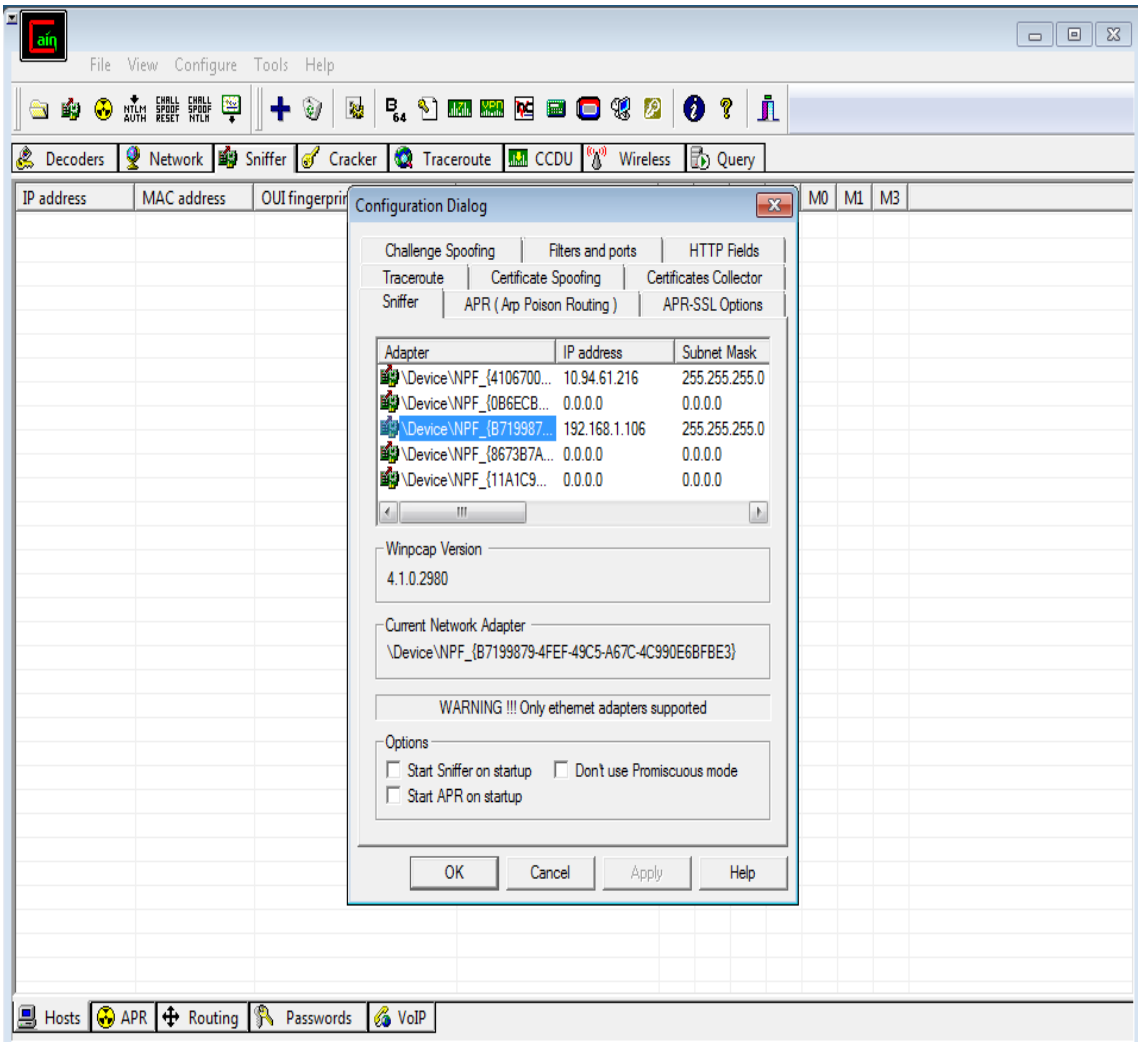
MITM-hyökkäys voidaan toteuttaa myös verkossa, joka ei ole hyökkääjän luoma. Tämä onnistuu ARP-väärennöksellä. ARP (Address Resolution Protocol) -protokollaa käytetään selvittämään verkkokerroksen IP-osoitetta vastaavan siirtokerroksen MAC-osoite. [30.] ARP-väärennöksessä hyökkääjä muuttaa oman tietokoneensa MAC-osoitteen samaksi kuin verkon reitittimen MAC-osoite. Tämä aiheuttaa sen, että muut verkossa olevat koneet luulevat hyökkääjän tietokonetta reitittimeksi ja lähettävät liikenteensä sille, mistä se jatkaa reitittimelle ja Internetiin. Verkon toiminta jatkuu muuten entisellään. [31.]

Hyökkääjä ei kuitenkaan näe pelkästään ARP-väärennöksen avulla HTTPS-suojausta käyttävän yhteyden liikennettä. Tähän vaaditaan vielä lisäksi SSL Strip- hyökkäys. Tämä onnistuu iskemällä käyttäjän liikenteeseen juuri ennen HTTPS-yhteyden muodostamista. Yleensä suojattu yhteys muodostetaan käyttäjän siirtyessä tavalliselta HTTP-sivustolta sisäänkirjautumissivulle, joka on HTTPS-suojattu. Tässä vaiheessa hyökkääjä kaappaa liikenteen ja luo HTTPS-yhteyden omalta tietokoneelta sähköpostipalvelimelle ja näiden välille muodostuu suojattu yhteys. Käyttäjän ja hyökkääjän välinen yhteys pysyy selkokielisenä ja mahdollistaa tietojen kaappaamisen. Kuva 13 havainnollistaa väliintulohyökkäyksen toimintaa. [31.]

Kuva 13. Väliintulohyökkäys topologia. [72.]

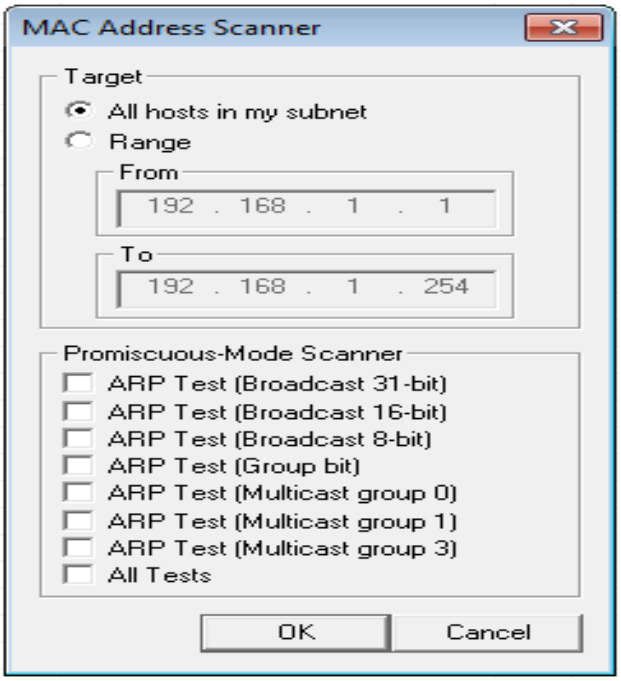
7.3 Väliintulohyökkäyksen toteuttaminen

Väliintulohyökkäys toteutettiin koulun tietoverkkolaboratoriossa. Testejä varten luotiin julkinen langaton verkko johon liitettiin kolme tietokonetta. Kohdekoneessa oli Windows 7 -käyttöjärjestelmä kaikki päivitykset asennettuina ja uusin versio Mozillan Firefox-selaimesta. Hyökkäyskoneelle asennettiin Windows-koneille tehty Cain & Abel, joka pystyy tekemään ARP-väärennöksen ja lähettämään väärennettyjä varmenteita sekä Wireshark liikenteen analysointiin. Kolmannelle koneelle ei kohdistettu hyökkäystä, vaan sillä testattiin verkon käyttöä, kun ARP-väärennös oli käynnissä kohdekoneella. Verkko toimi normaalisti koneen kannalta koko testin ajan. Tavoitteina oli asettaa hyökkäyskone väliintulohyökkäys asemaan kohdekoneeseen nähden ja yrittää kaapata HTTPS-yhteydellä suojatusta istunnosta käyttäjänimi-salasana pari. Cain & Abel pyrkii toteuttamaan tämän lähettämällä kohdekoneelle väärennettyjä varmenteita. Näistä johtuivat Firefox-selaimen antavat varoitukset.

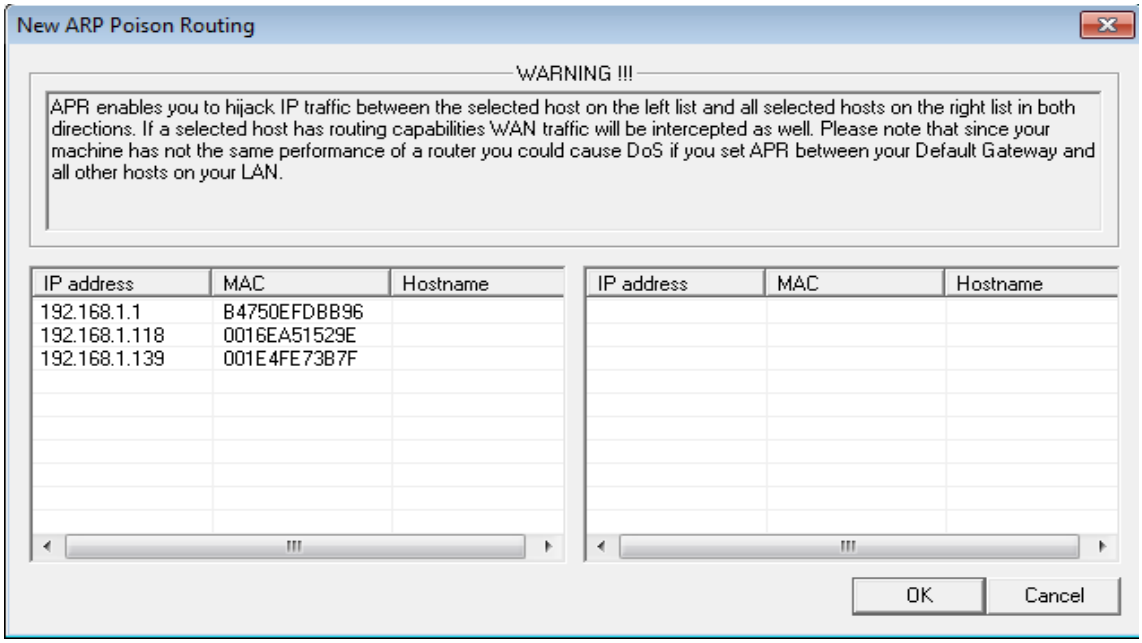


Kuva 14. Verkkosovittimen valinta.

Cain & Abelin käynnistyksen jälkeen valitaan verkkosovitin, jolla on yhteys verkkoon. Kuvassa 14 on verkkosovittimen valintanäkymä ja haluttu verkkosovitin valittuna. Tämän jälkeen verkosta etsitään skannaamalla MAC-osoitteet, jotta löydetään siihen yhteydessä olevat laitteet. Kuvassa 15 on MAC-osoite skannerin valikko. Siinä on valittuna kaikkien laitteiden etsintä aliverkosta.



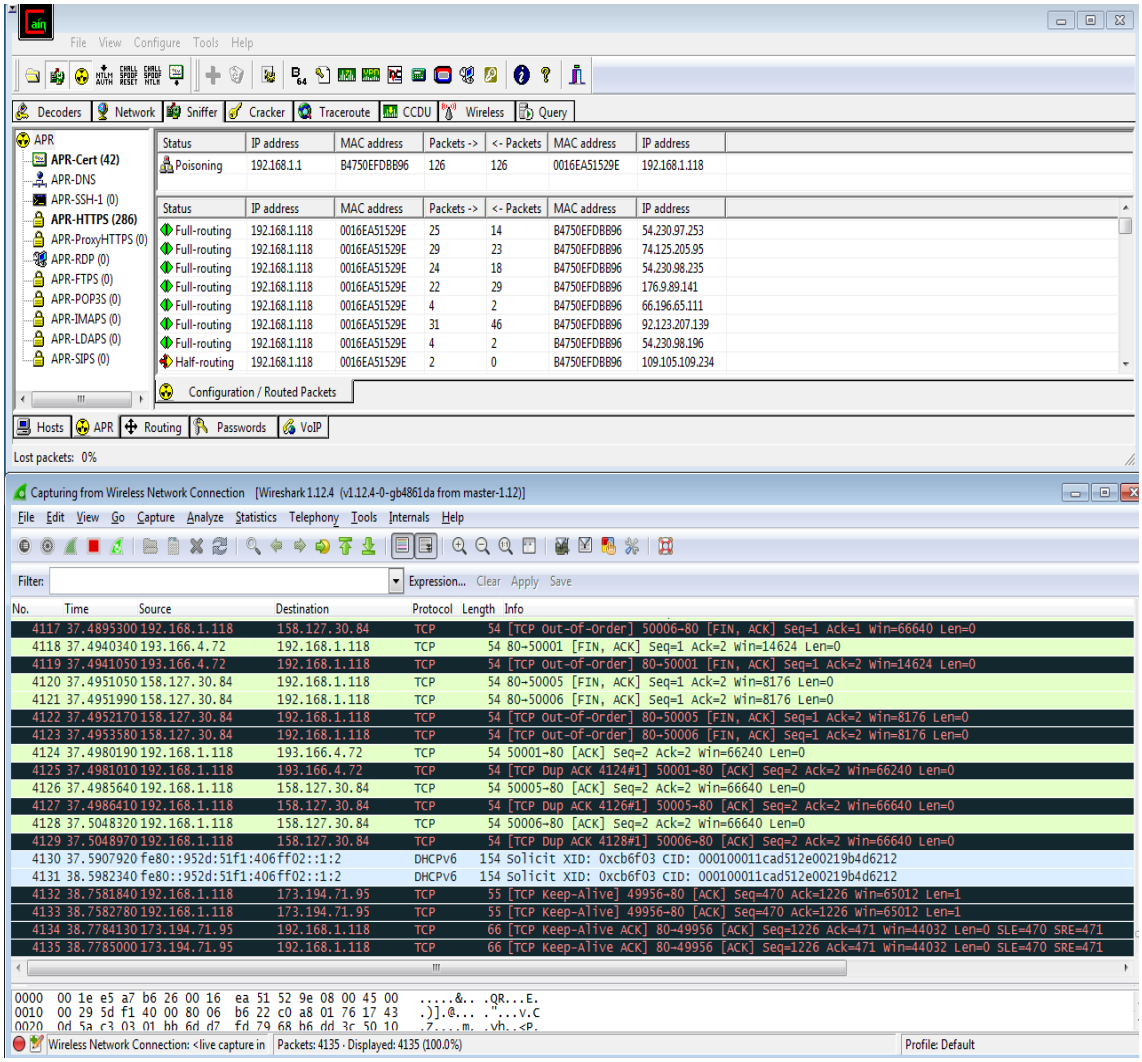
Kuva 15. Mac-osoitteiden skannaus.



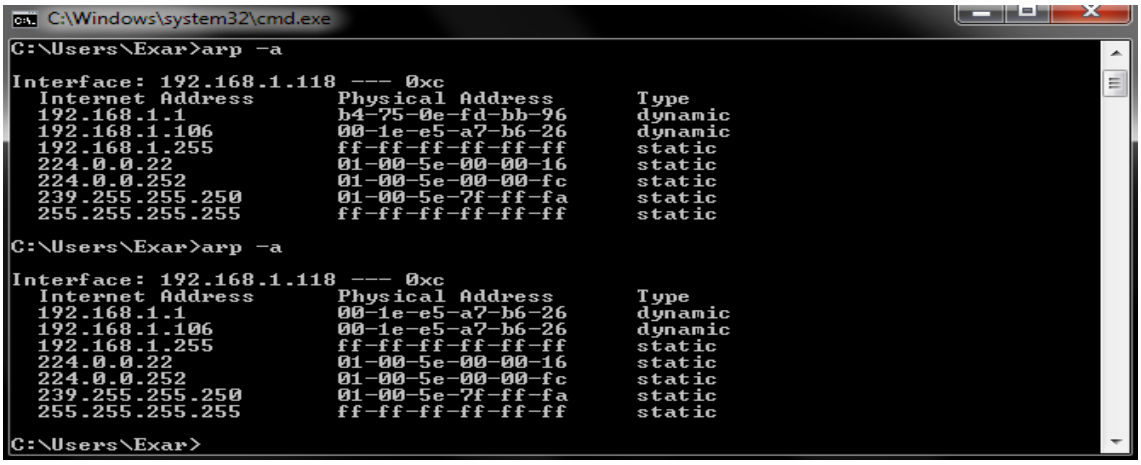
Kuva 16. Kohteen valitseminen.

Skannauksen jälkeen aukeaa uusi ikkuna, jossa näkyy löydetyt laitteet listattuna, kuten kuvassa 16. Ensin vasemmalta valitaan verkon reitittimen oletus yhdyskäytävä, joka oli tässä tapauksessa 192.168.1.1. Valinnan jälkeen oikealla olevaan valintaruutuun tulee

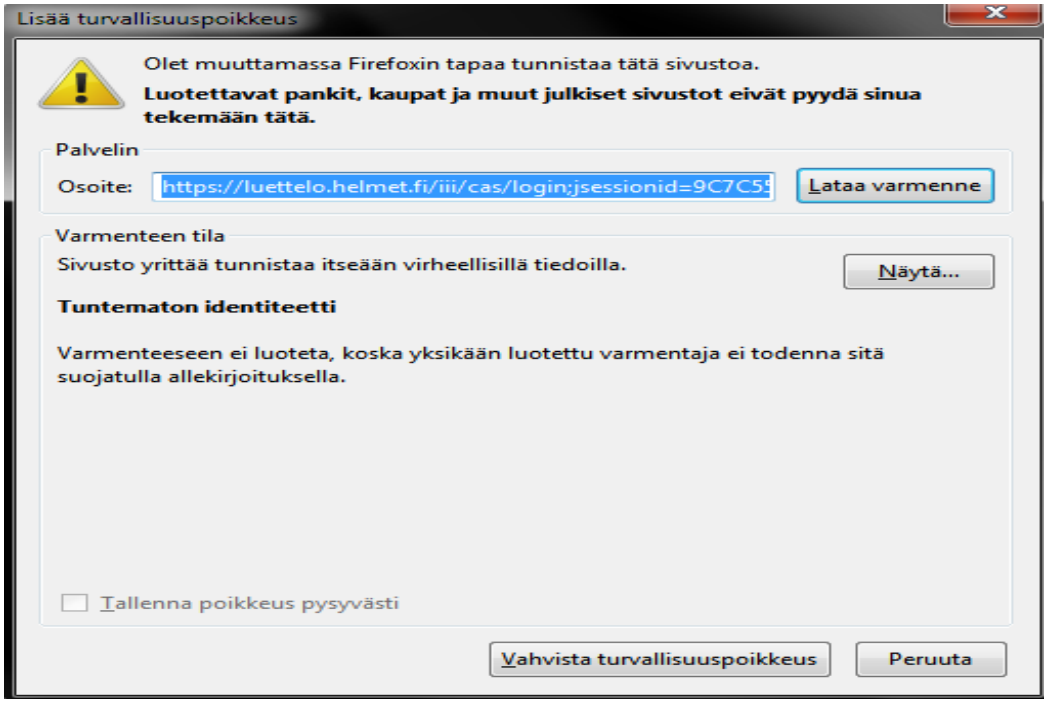
näkyviin mahdollisten kohdekoneiden IP-osoitteet. Niistä valitaan halutut osoitteet ja painetaan ”OK”. Kohdekoneen IP-osoite oli 192.168.1.118. Kohteen valinnan jälkeen aloitetaan ARP-väärennös. Kuvan 17 yläosassa on näkymä Cain & Abelista, kun ARP-väärennös on käynnistetty. Kuvan 17 alaosassa on hyökkäyskoneella käynnistetty Wireshark ja tarkistettu, että kohdekoneen liikenne ohjautuu hyökkäyskoneen kautta. Lisäksi vielä kohdekoneella tarkistettiin, että väliintulohyökkäyksen topologia on onnistunut. Tämä tehtiin käyttämällä komentokehoitteen komentoa ”arp -a”, siitä tarkistettiin, että oletus yhdyskäytävän MAC-osoite oli vaihtunut samaksi kuin hyökkäyskoneen MAC-osoite. Kuvassa 18 on kohdekoneen ARP-taulu ennen ja jälkeen ARP-väärennöksen käynnistämistä.



Kuva 17. ARP-väärennös käytössä ja Wiresharkin näkymä liikenteestä.

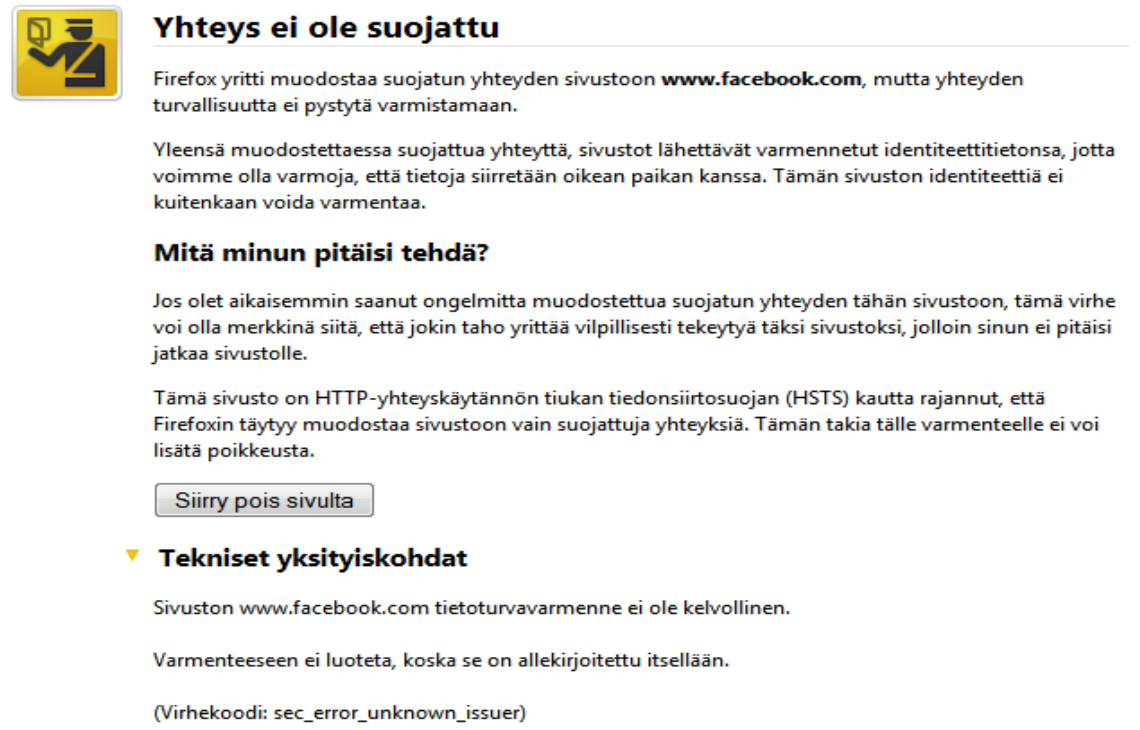


Kuva 18. Kohdekoneen ARP-taulu ennen ja jälkeen väärennöksen käynnistämisen.



Kuva 19. Firefoxin varoitusilmoitus.

Seuraavaksi testasin useita sivustoja, joissa on käytössä HTTPS-yhteys. Suurimmalle osasta sivuista Firefox-selain päästi kuvassa 19 olevan varoituksen jälkeen. Kuvassa 20 on Firefoxin ilmoitus kun yritetään ottaa yhteyttä osoitteeseen Facebook.com. Tätä varoitusta ei voi ohittaa ja yhteys haluttuun sivustoon estyy. Tämä johtuu Facebookin käyttämästä HTTP Strict Transport Security (HSTS) -mekanismista. Se pakottaa selaimen muodostamaan HTTPS-yhteyden, ja koska varmenteet olivat väärennettyjä kohdekoneella, ei selain kyennyt muodostamaan sivustoon HTTPS-yhteyttä.



Yhteys ei ole suojattu

Firefox yritti muodostaa suojatun yhteyden sivustoon **www.facebook.com**, mutta yhteyden turvallisuutta ei pystytä varmistamaan.

Yleensä muodostettaessa suojattua yhteyttä, sivustot lähettävät varmennetut identiteettitietonsa, jotta voimme olla varmoja, että tietoja siirretään oikean paikan kanssa. Tämän sivuston identiteettiä ei kuitenkaan voida varmentaa.

Mitä minun pitäisi tehdä?

Jos olet aikaisemmin saanut ongelmitta muodostettua suojatun yhteyden tähän sivustoon, tämä virhe voi olla merkkinä siitä, että jokin taho yrittää vilpillisesti tekeytyä täksi sivustoksi, jolloin sinun ei pitäisi jatkaa sivustolle.

Tämä sivusto on HTTP-yhteyskäytännön tiukan tiedonsiirtosuojan (HSTS) kautta rajannut, että Firefoxin täytyy muodostaa sivustoon vain suojattuja yhteyksiä. Tämän takia tälle varmenteelle ei voi lisätä poikkeusta.

Siirry pois sivulta

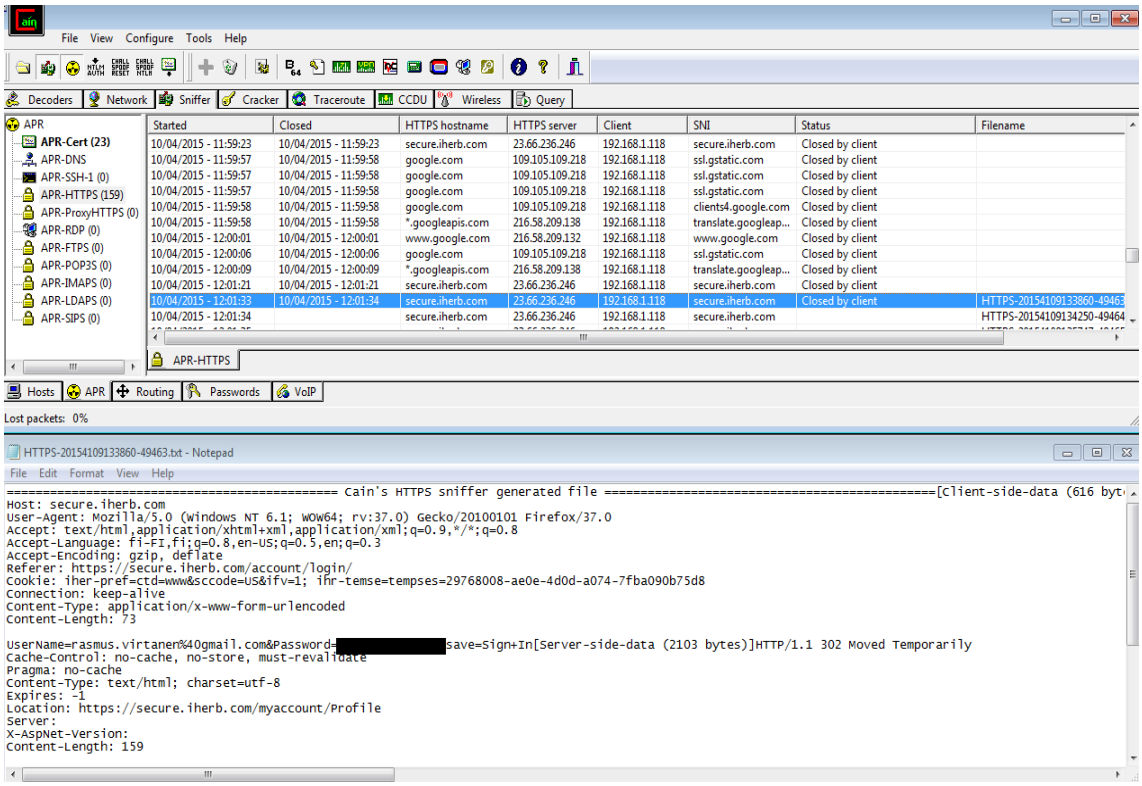
Tekniset yksityiskohdat

Sivuston www.facebook.com tietoturvavarmenne ei ole kelvollinen.

Varmenteeseen ei luoteta, koska se on allekirjoitettu itsellään.

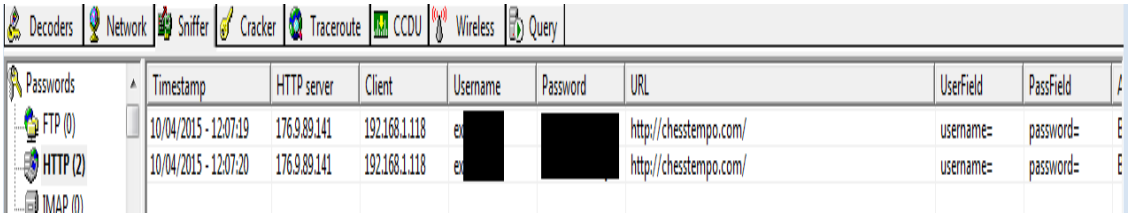
(Virhekoodi: sec_error_unknown_issuer)

Kuva 20. Yhteyden muodostaminen estetty.



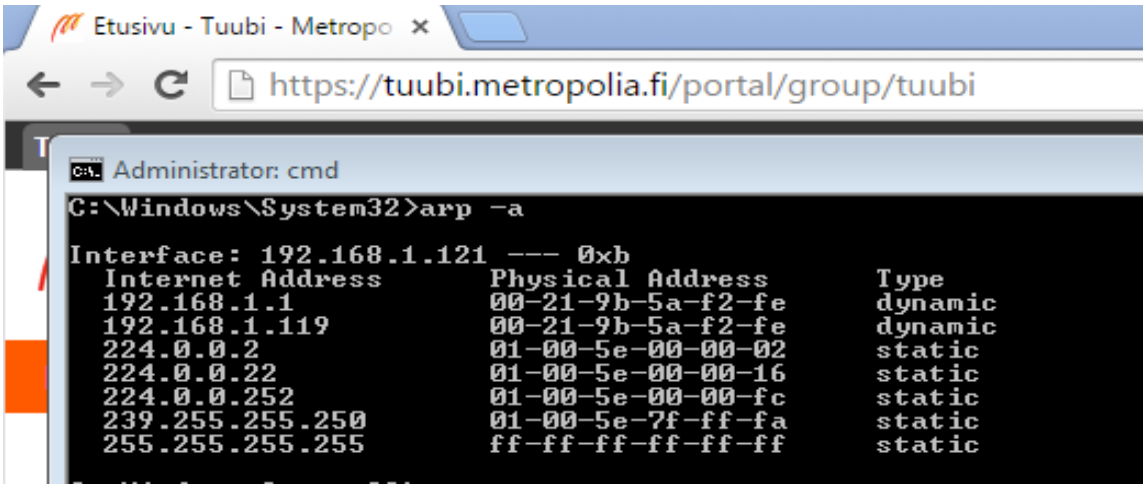
Kuva 21. Iherb.com-sivulta kaapattu salasana.

Iherb.com ei siirry HTTPS-yhteyteen ennen sisäänkirjautumisvaihetta eikä käytä HSTS-mekanismia. Sisään kirjautuessa näytettiin sama varoitus kuin kuvassa 19. Tämän jälkeen sisäänkirjautuminen tapahtui normaalisti ilman ongelmia. Kuvassa 21 näkyy Cain & Abelin kaappaamat tiedot sisäänkirjautumisesta. Cain & Abel luo automaattisesti tekstitiedoston, joka sisältää käyttäjänimen ja salasanan. Lisäksi Cain & Abel kaappaa kaikki HTTP-istuntojen käyttäjänimi/salasana parit ja listaa ne. http-istunnoista kaapatut tiedot näkyvät kuvassa 22.



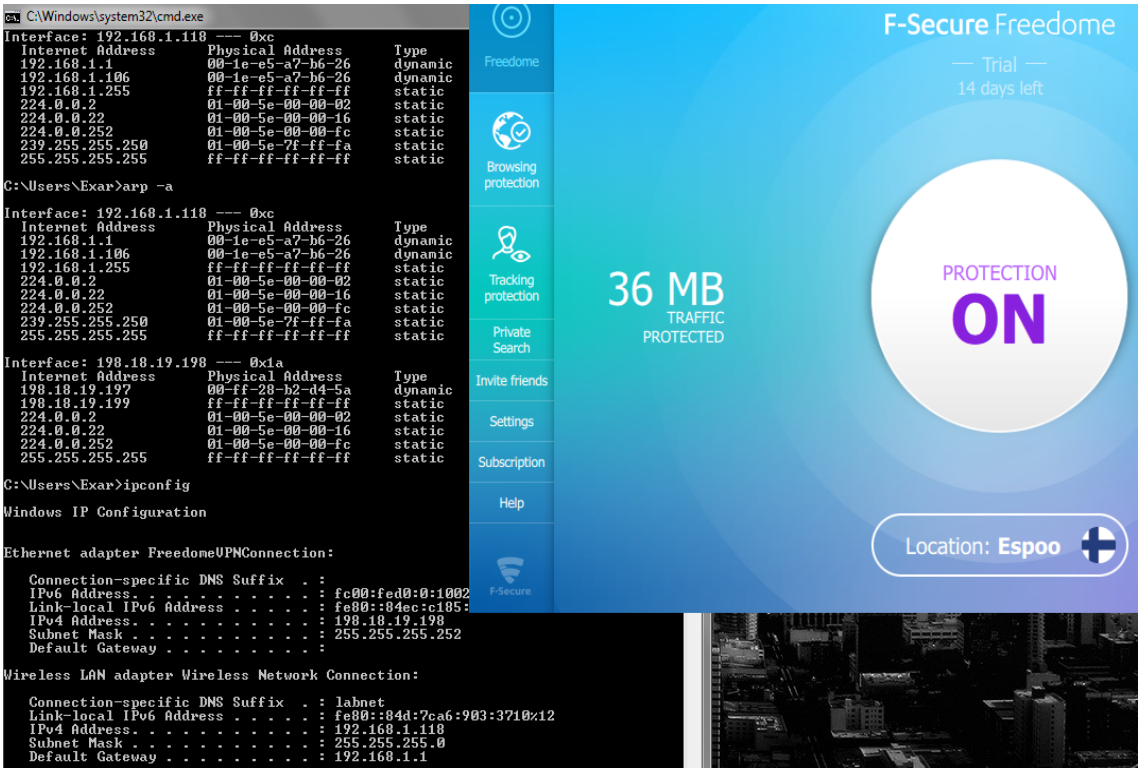
Kuva 22. HTTP-istunnoista kaapatut kirjautumistiedot.

Vielä muutama vuosi sitten MITM–hyökkäys ja SSL strip olisi toiminut ilman varoituksia kohdekoneella. Useat sivustot ovat kuitenkin siirtyneet kokonaan pois HTTP:n käytöstä, jopa Google.com-osoitteeseen ei pääse ilman HTTPS-yhteyttä. Tämän lisäksi saatetaan käyttää vielä HSTS-mekanismia. SSL/TLS:n turvallisuus perustuu varmenteisiin. Ilman aitoa varmennetta, jota lähettää hyökkäyskoneelta kohdekoneelle ei selaimen varoituksista pääse eroon. Cain & Abel tarjoaa kuitenkin kiertotien tähän. Ohjelmalla on mahdollista tehdä varmenteita, joko käyttäen kaapattua varmennetta pohjana tai luoda kokonaan keinotekoinen. Luotuani varmenteen, siirsin sen USB-tikulla kohdekoneelle ja asensin varmenteen selaimeen. Kuvassa 23 on ruutukaappaus Metropolia-sivustosta. Sivulle pääsi kirjautumaan ilman varoituksia ja osoitekentässä näkyy HTTPS-etuliite, vaikkakin ilman lukko ikonia. Kuvassa 23 on lisäksi kohdekoneen ARP-taulu, mistä näkee oletus yhdyskäytävän ja hyökkäyskoneen MAC-osoitteiden olevan sama. Esimerkiksi kahvilassa, jossa olisi julkinen verkko, varmenteen asentaminen USB-tikulta koneelle kestäisi vain muutaman sekunnin skriptin avulla. Toinen mahdollinen tapa käyttää väärennettyä varmennetta olisi uudelleen ohjata kohdekoneen liikenne aidolta näyttävälle sivulle. Tämä onnistuu Cain & Abel-ohjelmalla käyttämällä ARP-DNS-väärennöstä. Väliintulohyökkäys ei ole yhtä vaarallinen kuin muutama vuosi sitten, mutta jossain määrin toimiva tekniikka vieläkin.



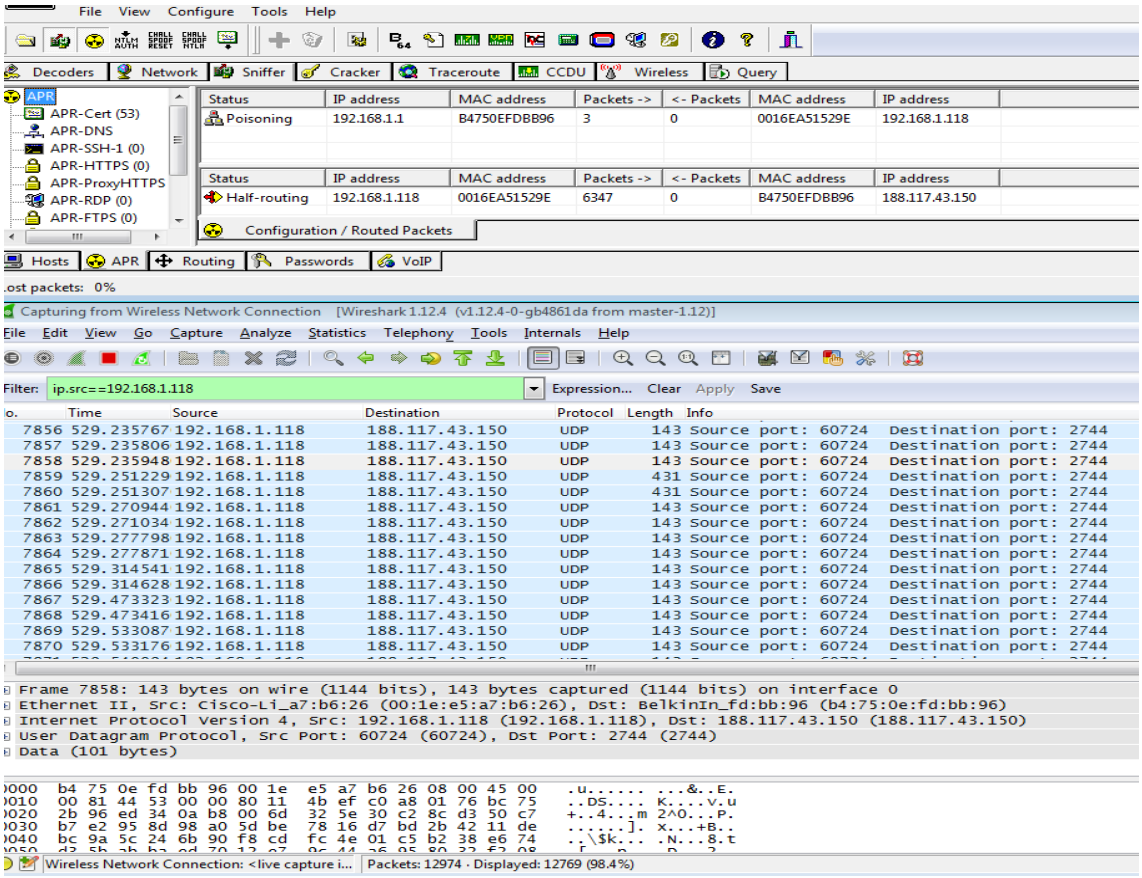
Kuva 23. HTTPS-istunto väärän varmenteen avulla.

Lopuksi testasin VPN-yhteyttä. VPN-ohjelmaksi valikoitui F-Securen Freedome, valintaan vaikutti ilmainen kahden viikon kokeiluaika. Freedomen asentaminen ei vaatinut muuta kuin sen lataamisen ja asennusohjelman suorittamisen. Ohjelman käynnistämisen jälkeen käyttäjän tarvitsee vain painaa ”protection off” valintaa jolloin se muuttuu kuvan 24 mukaiseen ”protection on” muotoon. Tällöin VPN-yhteys on käynnistetty.



Kuva 24. VPN toiminnassa.

Freedomen käynnistämisen jälkeen ARP-taulussa näkyy uusi verkkosovitin, jonka IP-osoite on 192.168.19.198. ARP-väärennös oli koko ajan käynnissä, mutta VPN suojasi tietoliikenteen. Wiresharkilla näkee vain UDP-protokollaliikennettä, kuten kuvassa 25.



Kuva 25. Liikenne Wiresharkilla kaapattuna VPN:in ollessa päällä.

8 Tietokoneen käyttäjän ohjeita

Luvuissa 8 ja 9, joissa annetaan suosituksia ja ohjeita tietoturvan parantamiseksi, piti päättää mitä asioita ottaa mukaan ja mitä jättää pois. Tietoturvaa parantavia asioita käsiteltäessä täytyy tehdä rajaus tavoitteen mukaan. Tavoite oli tarjota tavalliselle Internetin käyttäjälle keinoja parantaa tietoturvaa. Esitellyt keinot eivät kuitenkaan saisi olla hankalia toteuttaa tai huonontaa käyttökokemusta. Näiden syiden takia päädyin kaksi osaiseen lähestymistapaan. Ohjelmallisesti tietoturvaa voi parantaa vain tiettyyn pisteeseen asti. Tietoturvan suurin uhka on ihminen itse, joten ohjelmista kertomisen lisäksi esittelen myös turhia riskejä aiheuttavia Internetin käyttötapoja. Ohjelmien ja riskien välttämisen yhdistelmällä pystytään saavuttamaan hyvä tietoturva.

Tietokoneen haittaohjelmista puhtaana pitämisessä on hyvä muistaa, että tietokoneen käyttäjän toimet ovat suurin riski. Haittaohjelmat leviävät virustorjuntaohjelmalla, palomuurilla ja päivitetyillä ohjelmilla varustettuihin koneisiin, jos käyttäjä sen toimillaan aiheuttaa. Eri ohjelmien varoituksiin ja ohjeisiin on suositeltavaa reagoida, oli se sitten Internet-selaimen varoitus varmenteesta tai ohjelman ilmoitus saatavilla olevasta päivityksestä. Internetin käyttäjän tulisi välttää maksullisten ohjelmien piratisoituja versioita, estää sivustoilla olevat mainokset, varoa huijauksia sekä ladata ilmaisohjelmat valmistajan sivuilta. Windowsia käyttävissä tietokoneissa tietoturvaa voi myös parantaa käyttämällä normaalia käyttäjätiliä, järjestelmävalvojan tilin sijaan. Tietoturva-yhtiö Avecton mukaan käytettäessä normaalia käyttäjätiliä voidaan vähentää kriittisiä haavoittuvuuksia Microsoftin ohjelmissa 97 %:lla. Kaikista Microsoftin ohjelmia koskevista haavoittuvuuksista vähenisi 80 %. [32.]

Erityisesti kannettavien laitteiden suojaamisessa pitää ottaa huomioon niiden suuri riski joutua varastetuksi tai kadota. Tällaiset laitteet tulisi suojata vähintään salasanalla, jotta laitteen luvaton käyttö estyy. Salasana ei välttämättä yksinään riitä suojaamaan laitetta, niiden ohittamiseksi tai murtamiseksi löytyy useita keinoja. Lisäksi laitteen kovalevy voidaan salata. Tähän tarkoitukseen osasta käyttöjärjestelmiä löytyy valmiiksi ohjelma, lisäksi saatavilla on useita tarkoitukseen tehtyjä ohjelmia. Salauksessa käytettävä salasana yhdessä salaus algoritmin kanssa muuttavat kovalevyn sisältämän tiedon lukukelvottomaan muotoon, jota ei voi lukea ilman salasanaa. Kovalevynkin salaus voidaan murtaa, siihen vaikuttaa algoritmin lisäksi salasanan vahvuus. Salasana on sitä vahvempi mitä pidempi se on. Vahvuutta voi parantaa käyttämällä erikoismerkkejä, isoja ja pieniä kirjaimia sekä numeroita ja tehdä siitä mahdollisimman satunnainen merkkijono. Ennen kovalevyn salausta on suositeltavaa tehdä varmuuskopio salattavasta sisällöstä.

8.1 Vertaisverkkosivut

Vertaisverkkosivuilla jaetaan pääasiassa tekijänoikeudella suojattua materiaalia, kuten elokuvia, musiikkia ja ohjelmistoja. Tiedostojen jakosivustoilla kukaan ei tarkista sinne jaettaviksi laitettuja tiedostoja, joten niiden sisällöstä ei ole takeita. Tämä antaakin haittaohjelmien levittäjille mahdollisuuden saastuttaa suuri määrä koneita, piilottamalla haittaohjelma ladattavien tiedostojen joukkoon. Itävallassa sijaitsevan Wienin yliopiston tekemässä tutkimuksessa ladattiin 43 900 latauslinkin sisältö, jotka sisälsivät suosi-

tuimpia ohjelmia ja pelejä. Ladatut tiedostot tutkittiin Virustotal-ohjelmalla, joka käyttää 43:a eri anti-virusskanneria. Tuloksena oli, että noin puolet ohjelmista olivat saastuneita jonkin tyyppisellä haittaohjelmalla. [33.]

8.2 Haittaohjelmamainonta

Haittaohjelmamainonta (eng. Malvertising) on levinnyt kaikkialle. Monet sivustot myyvät mainostajille tilaa sivuiltaan. Mainostajat puolestaan myyvät ostamaansa tilaa edelleen, jota haittaohjelmien levittäjät ovat alkaneet ostamaan ja upottamaan mainoksiin haittaohjelmia. Tällä tavoin haittaohjelmat saadaan myös hyvämaineisille sivustoille ja maksimoidaan mahdollisten uhrien määrä. Tämä keino ei ole uusi mutta se on nopeasti kasvava. Vuonna 2013 haitallisia mainosnäyttöjä havaittiin 12,4 miljardia, kasvua vuodesta 2012 on 225 %. [34.]

Haittaohjelman leviäminen mainoksen avulla tapahtuu kahdella eri tavalla. Joko sivustolla vierailevа klikkaa mainosta ja yllytetään asentamaan koneelle jokin ”tärkeä” ohjelma. Toinen tapa on niin sanottu ”drive-by download”, jolloin pelkkä sivun lataaminen riittää. Tässä tapauksessa mainos sisältää iframen, joka toimii kuin selain selaimen sisällä. Iframe sisältää linkin kolmannelle sivulle. Sieltä selain hakee ilman käyttäjän tietoa linkin sisällön, joka on yleensä valikoima haittaohjelmia. Nämä haittaohjelmat testaavat tunnettuja haavoittuvuuksia, kunnes jokin niistä toimii. Tämän jälkeen haavoittuvuuden kautta asennetaan ”sillanpää” haittaohjelma, jonka avulla koneelle voidaan asentaa muita haittaohjelmia. Tällä tavalla voidaan levittää melkein mitä tahansa haittaohjelmatyyppiä, yleisimpiä ovat: troijalaiset, kiristys- ja vakoiluohjelmat. [34.]

Tämän tyyppisiä mainoksia ei voi välttää, koska niitä voi olla missä tahansa. Näitä vastaan on kuitenkin monia suojautumiskeinoja. Tavalliset keinot ovat: päivitetyt ohjelmat ja virustorjuntaohjelma. Lisäksi voidaan selaimesta poistaa käytöstä Java ja Flash, mutta tämä vaikuttaa useiden sivustojen toimintaan. Parhaan lisäsuojan antaa selaimeen asennettava lisäosa, joka estää mainokset. Tällaisia ovat esimerkiksi Adblock ja Adblock Plus. [34.]

8.3 Ilmaiset ohjelmat

Internet on tulvillaan ilmaisia ohjelmia jokaiseen kuviteltavissa olevaan tarkoitukseen. Jotta ohjelmat voivat olla ilmaisia. Niistä on karsittu ominaisuuksia verrattuna saman ohjelman maksulliseen versioon tai sitten asennusohjelman yhteydessä tarjotaan muita ohjelmia. Maksullisten ohjelmien ilmaisversiot ovat yleensä puhtaita ylimääräisistä ohjelmista. Ilmaisten ohjelmien tekijät saavat rahaa niputtaessaan (eng. bundle) kolmannen osapuolen ohjelmia asennusohjelmaansa. Suurin osa mukana tulevista ohjelmista on haittaohjelmia. Ilmaisohjelmia asennettaessa tulisi asennusvaiheessa olla tarkkana, osaa mutta ei kaikkia haittaohjelmista voidaan estää asentumasta poistamalla asentamisen valinta ohjelman kohdalta. Ohjelmien lataaminen on suositeltavaa tehdä valmistajan omilta sivuilta. Internetin latauspalvelu sivustot usein lisäävät alkuperäiseen asennusohjelmaan muita ohjelmia. Nämä ylimääräiset ohjelmat voivat muun muassa: vaihtaa selaimen kotisivua, asentaa selaimeen hakupalkkeja tai jopa ohjata kaiken verkkoliikenteen välityspalvelimen kautta. [35; 36.]

8.4 Tietojenkalastelu

Tietojenkalastelu on verkkotoimintaa, jossa yritetään saada kohde antamaan henkilökohtaista tietoa, kuten verkkopankkitunnuksia, maksukortti- tai kirjautumistietoja. Yleensä tietojenkalastelussa käytetään sähköpostia, joka näyttää tulevan luotetulta lähteeltä kuten verkkopankilta. Viestissä pyydetään kirjautumistietoja jonkin tekosyyn avulla ja tarjotaan linkki, josta pääsee sivulle. Linkki ohjaa aidolta näyttävälle sivulle, mutta todellisuudessa sillä ei ole mitään tekemistä oikean sivun kanssa. Sivun ylläpitäjä saa kaikki käyttäjän sivulle syöttämät tiedot. [37.]

Palomuuri, virustorjuntaohjelma ja selaimien sisäänrakennetut mekanismit suojaavat käyttäjiä tietojenkalastelulta. Ne eivät kuitenkaan pysty tarjoamaan aukotonta turvaa. Käyttäjän oma valveutuneisuus on paras suoja. Yksikään palvelu ei pyydä käyttäjiltään tili- tai kirjautumistietoja sähköpostilla. Epäilyttävien viestien linkkejä ei pidä koskaan painaa tai liitetiedostoja avata. Viesti voi olla niin hyvin tehty, ettei sitä erota aidosta, tällöin voi itse ottaa yhteyttä palveluun, mistä viesti on lähetetty. [37.]

9 Tietokoneen ohjelmallinen suojaaminen

9.1 Päivitykset

Tietokoneen käyttöjärjestelmän päivittäminen on erityisen tärkeää, kuten jo vuonna 2004 tehty testi osoitti. Kevin Mitnick, entinen hakkeri, nykyisin tietoturvakonsultti, teki testin yhdessä Avantgarde-yhtiön kanssa. Siinä käytettiin Internetin selaamiseen konetta, jossa oli suojaamaton ja päivittämätön Windows XP service pack 1. Konetta ehdittiin käyttää vain neljä minuuttia verkossa ennen kuin se oli saastunut haittaohjelmalla.[38.] Vaikka kokeilusta on aikaa yli vuosikymmen, on se vieläkin hyvä muistutus päivitysten tärkeydestä. Kymmenessä vuodessa Internet ei ole muuttunut tietoturvan kannalta parempaan suuntaan.

Kuten luvussa 6 esiteltiin, haittaohjelmatyyppejä löytyy useita erilaisia, mutta kaikilta pystytään suojautumaan pienellä vaivalla. Niin ohjelmista kuin käyttöjärjestelmistä löydetään jatkuvasti uusia haavoittuvuuksia, jotka mahdollistavat esimerkiksi tietokoneen etähallinnan ilman koneen omistajan lupaa taikka tietoa. Taulukossa 2 on löydetyt haavoittuvuudet eräistä suosituista ohjelmista, haavoittuvuudet ovat jaoteltu vakavuuden perusteella. Paras keino suojautua ohjelmistoissa olevilta tietoturva-aukoilta on pitää ne päivitettyinä. Tämä käy helpoimmin ottamalla automaattiset päivitykset käyttöön.

Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

Taulukko 2. Ohjelmista löydetyt haavoittuvuudet vuonna 2014. [22.]

9.2 Virustorjuntaohjelmat

Virustorjuntaohjelmat suojaavat tietokonetta eri tallennusmedioiden ja verkon kautta saapuvilta haittaohjelmilta. Yleensä virustorjuntaohjelmat päivittävät itsensä automaattisesti verkkoyhteyden ollessa auki. Virustorjuntaohjelmien yleisimmät ominaisuudet on esitelty seuraavassa:

- Ohjelma tarkistaa reaaliaikaisesti jokaisen tiedoston, jonka käyttäjä avaa. Tiedostoja verrataan haittaohjelmatietokantaan ennen kuin järjestelmä saa avata sen. Tämä ei vielä takaa koneen puhtaana pysymistä, vaan koneelle voi päästä haittaohjelma, jos se ei ole vielä tietokannassa.

- Järjestelmän skannauksessa tarkastetaan kaikki tiedostot haittaohjelmien varalta. Tämä on juuri siltä varalta, että koneelle on päässyt huomaamatta jotain.

- Virusmääritelmiä käytetään virusten tunnistamiseen, edellä mainitut asiat eivät auta millään tavalla elleivät määritelmät ole ajan tasalla.

- Heuristiikkaa käyttäen virusohjelma osaa myös tunnistaa mahdollisia haittaohjelmia vaikka niitä ei löytyisi virusmääritelmistä. Virustorjuntaohjelma osaa tarkkailla tunnettujen haittaohjelmien mukaista käyttäytymistä ja näin estää niiden toiminnan. Tämä tekniikkaa aiheuttaa myös välillä ”vääriä positiivisia” eli saattaa estää turvallisen ohjelman toiminnan. [39.]

Virustorjuntaohjelmia on niin ilmaisia kuin maksullisia. Ne eroavat toisistaan yleensä ominaisuuksien määrällä. Ilmainenkin ohjelma voi olla riittävä tietoturvan kannalta. Ohjelmaa valitessa tulisi kiinnittää huomiota testitulosmenestykseen. Testejä suorittaa useampikin riippumaton taho, yksi tunnetuimmista on AV Comparatives. Vuoden 2014 voittaja oli Bitdefender. Muita erinomaisen arvosanan saaneita ohjelmia olivat AVG, AVIRA, Emsisoft, ESET, F-Secure, Fortinet ja Kaspersky Lab. [40.]

9.3 Palomuuri

Palomuuri hallinnoi sisään tulevaa ja ulos menevää tietoliikennettä asetettujen sääntöjen mukaisesti. Palomuureja on ohjelmisto- sekä laitteistopohjaisia. Monet laitteistopoh-

jaiset palomuurit voivat tarjota muitakin toimintoja kuten toimia DHCP-palvelimena verkolle jota se suojaa. [41.] Palomuurit voivat suojata lähiverkossa myös verkkotiedustelulta eli porttiskannaukselta. Se on toimenpide, jonka avulla pyritään selvittämään tietojärjestelmän tietoliikenneporteissa toimivia ohjelmia ja käyttöjärjestelmiä sekä niiden haavoittuvuutta. [66.] Internet operaattorit suojaavat asiakkaitaan tämän tyyppisiltä hyökkäyksiltä. Useat operaattorit rajoittavat asiakkaidensa kykyä suorittaa porttiskannausta, asiakas voi ainoastaan skannata portteja omassa kotiverkossaan. Samassa verkossa, kuten julkisessa langattomassa verkossa, tapahtuvalta porttiskannaukselta suojaa palomuuri .[67.] Palomuurit jaotellaan tyyppeihin sen mukaan millä kerroksella ne toimivat. [41.]

Pakettisuodatinpalomuurit toimivat TCP/IP-viitemallin verkkokerroksella. Näillä palomuureilla on kaksi alakategoriaa tilalliset (eng. stateful) ja tilattomat (eng. stateless). Tilallinen palomuuri pitää kirjaa aktiivisista yhteyksistä. Jokainen verkkoyhteys voidaan kuvata usealla ominaisuudella, muun muassa lähde ja kohde IP-osoitteella, UDP- tai TCP–portilla sekä yhteyden eliniän mukaan. Silloin kun paketti ei kuulu yhteydelle, joka löytyy palomuurin tilataulusta, tarkistetaan se säännöstöä vastaan, jonka jälkeen yhteys joko sallitaan tai lopetetaan. Tilaton palomuuri on yksinkertainen ja vähän muistia käyttävä. Se vertaa jokaista pakettia säännöstöön, jos paketti ei ole sallittu, sitä ei välitetä eteenpäin. [41.]

Sovelluskerroksella toimivat palomuurit tutkivat kaikki paketit, joita sovellus lähettää tai vastaanottaa. Koska kaikkien pakettien sisältämä data tutkitaan, voivat tällä kerroksella toimivat palomuurit estää matojen ja troijalaisten leviämisen. Sovelluskerroksen palomuurien toimintaa on määrittää pitäisikö prosessin hyväksyä yhteys. Ne suorittavat tehtävän suodattamalla yhteydet porttien perusteella. [41.] Tiettyyn porttiin tuleva paketti tutkitaan laittomien komentojen varalta, se voi myös esimerkiksi estää HTTP–paketeista tunnettuja turvallisuusaukkoja hyödyntävät murtoyritykset. [42.]

9.4 EMET-apuohjelma

Enchanced Mitigation Experience Toolkit (EMET) -apuohjelma auttaa estämään ohjelmiston heikkouksien onnistuneen hyödyntämisen. EMET käyttää suojausrajoitustekniikoita, jotka vaikeuttavat heikkouksien hyödyntämistä. Sillä on mahdollista ottaa käyttöön Windowsin sisäänrakennettuja tietoturva tekniikoita. [43.] Kuten tietojen

suorittamisen estäminen (DEP) ja Address space layout randomization (ASLR). DEP suojaa tietokonetta valvomalla sitä, että ohjelmat käyttävät järjestelmän muistia turvallisella tavalla. Jos se havaitsee, että tietokoneessa oleva ohjelma käyttää muistia väärin, se sulkee ohjelman. [44.] Yhdessä DEP:in kanssa toimiva ASLR antaa lisäsuojaa, vaikeuttamalla return-to-libc-hyökkäyksiä, jossa hyökkäyskoodi yrittää asiattomasti kutsua jotain tärkeää järjestelmätoimintoa. ASLR sijoittaa nämä toiminnot ympäri muistia sattumanvaraisiin sijanteihin, jolloin hyökkäystä on vaikea saada toimimaan. [45.]

EMET tarjoaa myös versiosta 4.0 lähtien Internet Explorer-selaimelle ”varmenne luottamus” (eng. certificate trust) -ominaisuutta. Ominaisuuden tarkoituksena on estää MITM-hyökkäykset estämällä väärennettyjen varmenteiden käytön. Käyttäjän pitää liittää aidot varmenteet palvelimilta yhteen tai useampaan luotettuun varmenteen myöntäjä tahoon. Tämän jälkeen, jos EMET havaitsee muutoksia varmenteen myöntäjässä palvelimella, se varoittaa mahdollisesta MITM–hyökkäyksestä. EMET-apuohjelma tekee tietokoneesta turvallisemman, mutta siinä käytetyt suojausmekanismit voivat estää turvallisiakin ohjelmia toimimasta. [46.] Ohjelman käyttäminen vaatii ymmärtämystä ohjelmien toiminnasta, eikä sitä voi suositella kokemattomalle käyttäjälle.

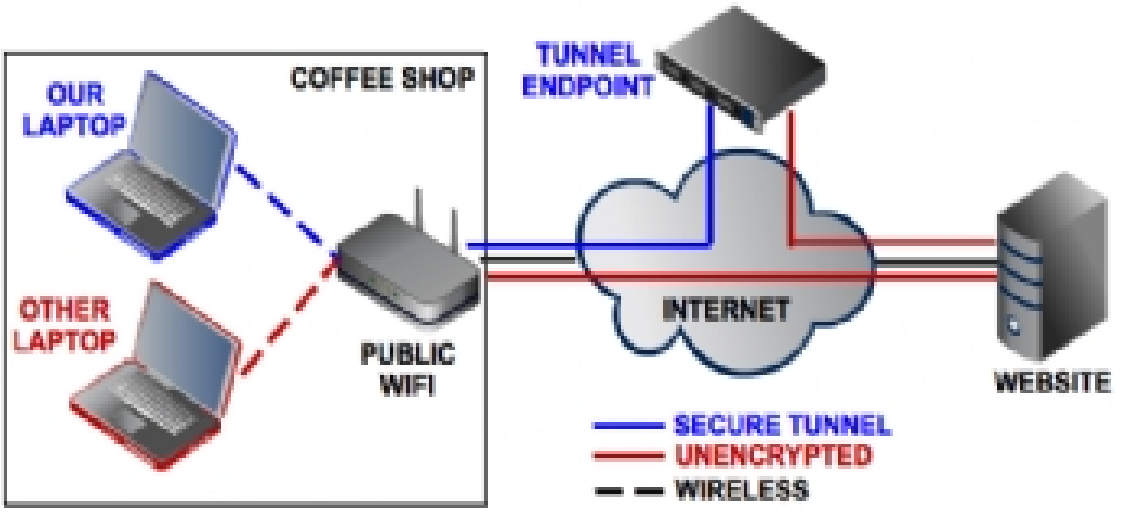
10 Suojautuminen julkisessa verkossa

10.1 HTTPS-protokollan käyttö

Julkisessa verkossa tapahtuvalta urkinnalta on mahdollista suojautua muutamalla keinolla. Varmin keino on olla käyttämättä mitään verkkoa, missä on muita käyttäjiä. Tämä ei tosin ole käytännöllistä. HTTPS-protokollan käyttäminen tarjoaa suojan urkinnalta. Suosituimpiin selaimiin on saatavilla lisäosa ”HTTPS everywhere”. Lisäosa pakottaa selaimen ottamaan sivustoon salatun yhteyden, jos se vain on mahdollista. Vaikka HTTPS-protokolla ei anna täyttä turvaa on sitä kuitenkin suositeltavaa käyttää. Kaikki, mikä vaikeuttaa mahdollisia hyökkäyksiä, on hyödyksi. [47.]

10.2 VPN

Varmin tapa suojautua julkisessa verkossa tapahtuvalta urkinnalta on käyttää VPN-yhteyttä (Virtual Private Network eli virtuaalinen erillisverkko). VPN-yhteyttä käytettäessä luodaan virtuaalinen tunneli käyttäjän ja VPN-palvelimen välille, tällöin tietokone ja palvelin ovat käytännössä samassa verkossa riippumatta fyysisestä sijainnista. Kaikki liikenne käyttäjältä kulkee tunnelia pitkin ja siirtyy julkisen Internetin puolelle vasta tunnelin toisessa päässä eli palveluntarjoajan päässä. Tunnelissa kulkeva data myös salataan siltä varalta, että joku onnistuisi murtautumaan tunneliin. VPN-yhteys tarjoaa myös mahdollisuuden kiertää maakohtaisia sivujen käyttökieltoja sekä useiden palveluiden maakohtaisia rajoituksia. [48.]



Kuva 26. VPN tunneli. [73.]

VPN:in turvallisuustekniikat

VPN-yhteys ei tee verkkoyhteydestä täysin anonyymiä mutta se parantaa yksityisyyttä ja tietoturvaa verrattuna tavalliseen yhteyteen. VPN tarjoaa tietoturvaa käyttämällä tunnelointiprotokollia ja tietoliikenteen salausta. VPN-yhteydet noudattavat myös turvamallia, jolla pyritään varmistamaan,

- luotettavuus, vaikka verkkoliikenne olisi kaapattu pakettitasolla, hyökkääjä näkisi vain salatun datan,

- lähettäjän todennus, jotta luvattomat käyttäjät eivät pääse käyttämään VPN:ia,

- viestien eheys jotta huomataan mahdollinen lähetettyjen viestien peukalointi. [48.]

11 Mobiililaitteet

Tablettikoneiden ja puhelimien yleistyttyä viime vuosina myös suurempi osa Internetin käytöstä tapahtuu näillä laitteilla. Julkista langatonta verkkoa käytettäessä näillä laitteilla on samat riskit kuin tietokoneella. Mobiililaitteella on kuitenkin helppo välttää käyttämästä perinteisiä langattomia yhteyksiä, sillä melkein kaikki laitteet tukevat mobiilidata yhteyksiä.

11.1 Sovellukset

Eri valmistajien puhelimet ovat suurin piirtein samanlaisia teknisiltä ominaisuuksiltaan sekä hinnaltaan. Ostopäätökseen vaikuttaakin suuresti, mikä käyttöjärjestelmä laitteessa on asennettuna. Ulkonäön suhteen niissä on eroja, mutta ominaisuuksien osalta ei juurikaan. Tärkein tekijä onkin saatavilla olevien sovellusten määrä ja laatu. Näitä sovelluksia voi ladata laitteelleen joko Internetistä tai käyttöjärjestelmän omalta kauppapaikalta.

Google Play

Google Play, vanhalta nimeltään Android Market, on digitaalinen jakelualusta, joka avattiin vuonna 2008 lokakuussa. Se on virallinen sovelluskauppa Android-laitteille, missä voi selata ja ladata sovelluksia jotka on kehitetty Androidille. Sieltä löytyy sovellusten lisäksi digitaalista mediaa, musiikin, lehtien, kirjojen, elokuvien ja televisio ohjelmien muodossa. Google Play:ssa on yli 1,43 miljoonaa sovellusta, ja niitä on ladattu yli 50 miljardia kertaa. [52.]

Google valvoo sovellusten sisältöä, muun muassa. seksuaalinen ja väkivaltainen sisältö ovat kiellettyjä. Kauppapaikalla kiellettyjä ohjelmia voidaan kylläkin jakaa Internetissä

apk-tiedostoina, jolloin niitä pystyy asentamaan Android-laitteelle. Haittaohjelmia vastaan Google käyttää automatisoitua antivirusohjelmaa nimeltä Google Bouncer. [53.]

Googlen julkaisemasta Androidin turvallisuusraportissa kerrotaan Androidin haittaohjelma tilanteesta. Googlen järjestelmät tarkkailevat säännöllisesti niin Google Playn sovelluksia kuin muitakin Android-laitteille asennettuja sovelluksia haitta-ohjelmien varalta. Google myös ilmoittaa sovelluskehittäjille sovelluksista löytyneistä haavoittuvuuksista ja heikkouksista. Viime vuonna yli 25 000 sovellusta päivitettiin Googlen huomautuksen perusteella. Raportin mukaan kaikista Android-laitteista alle yksi prosentti sisälsi jonkinlaisen haittaohjelman. Vain Google Playstä asennettuja sovelluksia käyttävistä laitteista haittaohjelman sisälsi vain 0,15 prosenttia. [54.]

App Store

Applen App Store -sovelluskauppa avattiin heinäkuussa 2008. Siellä myydään sovelluksia Applen iOS-laitteisiin. Sovelluksia kehittävät pääasiassa ulkopuoliset sovelluskehittäjät Applen tarjoamilla kehitystyökaluilla. [55.] Store kauppapaikalta löytyy yli 1,4 miljoonaa sovellusta ja niitä on ladattu yli 75 miljardia kertaa. App Storen sovellukset ovat lähes haittaohjelmista vapaita. Tämä johtuu Applen erittäin tiukasta laatukontrollista kauppapaikalle tulevien sovellusten suhteen. Apple tarkistaa jokaisen sovelluksen ennen sen pääsyä App Storeen. Haittaohjelmien torjumista helpottaa myös, että iOS on suljettu ympäristö, joten kehitystyökalut eivät ole jaossa kenelle tahansa. iOS-sovelluksia ei myöskään voi ladata mistään muualta kuin App Storesta. Kesäkuuhun 2014 mennessä App Storesta oli löytynyt vain 11 haittaohjelmaa ja niistä 8 toimi ainoastaan puhelimissa, joiden käyttöjärjestelmien tietoturva-ominaisuuksia oli muunneltu käyttäjän toimesta. [56.]

Windows Phone Store

Windows Phone Store on Microsoftin sovelluskauppa, joka avattiin lokakuussa 2010. Microsoftin ulkopuoliset kehittäjät saavat julkaista sovelluksia kauppapaikalle vuosimaksua vastaan. Microsoft tarkistaa sovellukset haittaohjelmien ja suorituskykyongelmien varalta. Kuten Applellakin sovelluksia ei voi ladata muualta kuin Windows Phone Storesta. [57.] Kauppapaikasta löytyy yli 300 000 sovellusta, ja niitä on ladattu yli 4 miljardia kertaa. [58.]

11.2 Haittaohjelmat

Haittaohjelmien määrään vaikuttaa käyttöjärjestelmän suosio eli markkina-osuus ja sovelluskaupan laadunvalvonta sekä voiko ohjelmia asentaa muualta. Tietokoneissa avoimen lähdekoodin Linux on vuosikausia ollut turvallisin alusta, mikä saattaa osittain johtua pienistä käyttäjämääristä. Mobiilipuolella avoimen lähdekoodin Androidille löytyy ylivoimaisesti eniten haittaohjelmia. F-Securen mukaan vuoden 2014 alkupuolella yli 99 % uusista mobiililaitteiden haittaohjelmista tehtiin Androidille, vuotta aikaisemmin vastaava luku oli 91 %:a. Alle 1 % kaikista haittaohjelmista tehtiin muille alustoille. [59.]

Mobiililaitteille suunnatut haittaohjelmat eivät toiminnaltaan juurikaan eroa tietokoneiden haittaohjelmista. Mobiililaitteiden käyttäjät harvoin tietävät, että heidän laitteensa voivat saastua haittaohjelmalla ja näin ollen laitetta ei ole suojattu laisinkaan. Mobiililaitteillekin on suositeltua asentaa virustorjuntaohjelma ja pitää laitteen ohjelmat päivitettyinä.

11.3 Yksityisyys

Yksityisyys on mobiililaitteilla suuremmassa vaarassa kuin tietokoneilla. Erityisesti älypuhelimet kulkevat käyttäjän mukana kaikkialle. Ne voivat sisältää kirjautumistiedot käytettyihin palveluihin, maksukorttitietoja, valokuvia sekä tekstiviesti- ja puhelu-historian. Näiden tietojen lisäksi käytettävät sovellukset keräävät käyttäjästään tietoja, kuten tehtyjä Internet-hakuja ja sijaintitietoja. Erityisesti sijaintitietojen kerääminen on helppoa älypuhelimien lukuisten yhteyksien takia, niistä löytyy yleisesti GPS, bluetooth, WLAN ja mobiilidata. Kaikkia näitä voidaan käyttää paikantamiseen ja nämä yhteydet ovat yleensä päällä kun puhelinkin on päällä. Data yhteyksien jatkuva päällä pitäminen altistaa myös hyökkäyksille. Yleensä WLAN on konfiguroitu yhdistymään automaattisesti tuntemiinsa verkkoihin. Hyökkääjä voi luoda langattoman verkon, jolla on täysin samat tiedot, kuin esimerkiksi suositun kahvilan verkolla. Tällöin laitteet ottavat automaattisesti yhteyden tähän ”pahan kaksosen” (eng. Evil Twin) verkkoon. Bluetooth-yhteyttäkin voidaan käyttää hyväksi. Hyökkääjä voi luoda laitteeseen etähallintayhteyden, jolloin on mahdollista muun muassa tehdä puheluita, tutkia laitteen sisältämää dataa ja käyttää laitteen mikrofonia salakuunteluun.[60.] Lisäksi mobiililaitteilla on riski kadota tai joutua varastetuksi, jolloin kaikki laitteen sisältämät tiedot voivat päätyä vääriin käsiin. Yksityisyyden parantamiseksi voidaan, tehdä seuraavaa:

- sammuttaa yhteydet silloin, kun niitä ei käytetä,
- ottaa käyttöön lukitusnäyttö, jolloin laitteen sisältämiin tietoihin ei pääse käsiksi ilman tunnusta. Lisäksi tärkeimmät tiedot voidaan suojata erillisillä salasanoilla,
- varmuuskopioida tiedot katoamisen tai varkauden,
- paikallistaa ja lukita laite ja tuhota siitä tiedot etähallinnan avulla. [61.]

11.4 Mobiililaajakaista

Suurimmasta osasta älypuhelimia ja tablettikoneita löytyy mobiililaajakaista, joka käyttää 3g- tai 4g-yhteyttä. Nimet viittaavat kolmanteen ja neljäteen sukupolveen. Tässä ajattelussa ensimmäistä sukupolvea edustavat analogiset teknologiat kuten NMT ja toista sukupolvea digitaaliset teknologiat kuten GSM. [62.] Mobiililaajakaista mahdollistaa langattoman tiedonsiirron melkein missä vain, Suomessa 3g-verkko kattaa melkein koko maan ja 4g-verkko toimii suurimmissa kaupungeissa.

Mobiililaajakaistaa käytettäessä liikenne on salattu vähintään laitteelta lähimmälle tukiasemalle. 3g-yhteyttä käytettäessä salaus jatkuu operaattorin runkoverkossa, kunnes siirrytään signaali protokollista IP-protokollan käyttöön. Suomessa 4g-yhteyden salaus loppuu jo tukiasemaan. Tämä johtuu siitä että 4g-standardissa verkkoliikenteen suojaus on vapaaehtoinen, 3g-standardissa operaattorit velvoitetaan salaamaan liikenne. Suomessa yksikään operaattori ei salaa 4g-liikennettään runkoverkossa. Tämä mahdollistaa liikenteen sieppaamisen, jos pääsee tukiasematiloihin. Kaupunkialueilla ne on sijoitettu rakennusten kellareihin, joiden katolta löytyy tukiasema. [63.] Edellä mainittu mahdollisuus huomioon ottaen mobiililaajakaista tarjoaa turvallisen vaihtoehdon julkiselle langattomalle verkolle. Älypuhelimille on saatavilla ohjelmia, joilla sen voi muuntaa langattomaksi reitittimeksi, mikä mahdollistaa tietokoneella yhteydenoton siihen ja mobiililaajakaistan käytön Internet-selailuun.

12 Yhteenveto

Insinöörityössä esiteltiin julkisen langattoman verkon hyökkäyksiä sekä erilaisia haittaohjelmia. Haittaohjelmien määristä ja taloudellisista haitoista löytyikin tietoa ja lukuja, mutta urkinnasta ja MITM-hyökkäyksistä ei löytynyt etsinnästä huolimatta tilastoja. Julkisen verkon käyttäjistä sen sijaan löytyi tilastoja, jotka antavat karun kuvan tavallisen käyttäjän tietoturvan tasosta. Kaspersky Labin ja B2B internationalin vuonna 2013 suorittaman kyselyn mukaan: 70 % vastaajista käytti mobiililaitteella julkista langatonta verkkoa. Näistä 34 % ei suojaa verkon käyttöään millään tavoin ja 14 % vastasi tekevänsä verkko-ostoksia ja käyttävänsä verkkopankkia. Verkon käyttötapojen lisäksi kysyttiin tietoturvaohjelmien käytöstä mobiililaitteissa, älypuhelinten omistajista 40 % ja tablettikoneiden omistajista 42 % kertoi käyttävänsä niitä. Lopuksi selvitettiin ovatko vastaajat joutuneet haittaohjelmien uhriksi. 27 %:lla oli laite saastunut viimeisen vuoden aikana. Haittaohjelmat aiheuttivat 20 %:lle arkaluonteisen tiedon menetyksiä ja 36 %:lle rahallisia menetyksiä tai kuluja. [64.] Luvut osoittavat, että tietämys tietoturvasta ei ole pysynyt tekniikan kehityksen mukana. Edellä mainitut luvut toimivat myös lisä motivaationa lopputyön tekemisessä.

Osasyynä loppukäyttäjien huonoon tietoturvaan voi olla myös vähäinen uutisointi yksityisten ihmisten tietoturva ongelmista. Uutisointi keskittyy ymmärrettävästi isoihin tietomurtoihin, jotka ovatkin suurin syy henkilökohtaisten tietojen leviämiseen Internetiin. Pelkästään Yhdysvalloissa vuoden 2013 aikana 110 miljoonan yksittäisen käyttäjän henkilökohtaisia tietoja vuodettiin Internetiin tietomurron seurauksena. Kaiken kaikkiaan 432 miljoonan tilin tiedot julkistettiin. [65.]

Yhtiöiden tietomurtoihin ei voi ulkopuolinen vaikuttaa, mutta omilla toimilla voi vähentää mahdollisesta murrosta aiheutuvaa haittaa. Kirjautumistiedoissa voi käyttää sähköpostiosoitetta mitä ei käytetä mihinkään muuhun ja luoda jokaiseen palveluun uniikin salasanan.

Insinöörityötä tehdessä heräsi kysymys: mikä on riittävä tietoturvan taso? Käytännössähän jokainen varokeino lisää hyökkäyksen onnistumiseen vaadittavaa työtä, mutta monet tekniikat, mitkä vaikeuttavat hyökkäyksiä vaikuttavat myös käytettävyyteen. Internet-sivuilla voi estää Flashin ja Javan toiminnan, mutta silloin sivut eivät välttämättä toimi oikein. Yksityisyyttään voi suojata käyttämällä Tor-verkkoa, joka anonymisoi liikenteen kierrättämällä sen kolmen välityspalvelimen kautta. Haittapuolena on tosin

yhteyden nopeus, joka on vain murto-osa yhteyden kapasiteetista. Lopulta tulin tulokseen, että riittävä tietoturvan taso saavutetaan insinöörityössä esitellyillä keinoilla. Lähes jokaisen järjestelmän ollessa Internetissä on yksityishenkilön turhaa pyrkiä ”täydelliseen” suojaan. Vaikka kuinka suojaisi omat toimensa, voi tietomurto muualle paljastaa henkilökohtaisia tietoja. Edward Snowdenin tekemät paljastukset tiedustelupalveluiden keinoista ja kyvyistä osoittivat, että tietoturvallista järjestelmää tuskin on olemassa.

Lähteet

1 Tietoturvan periaatteet. 2015. Verkkodokumentti. Helsingin yliopisto. <http://blogs.helsinki.fi/tvt-ajokortti/5-tietoturva/5-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset/>. Luettu 20.2.2015.

2 Tietoturvan perusteet. 2012. PDF-tiedosto. Helsingin yliopisto. <http://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf>. Luettu 20.2.2015.

3 Tietoturva. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Tietoturva>. Luettu 20.2.2015.

4 AAA-protokolla. 2014. Verkkodokumentti. Wikipedia. http://fi.wikipedia.org/wiki/AAA-protokolla. Luettu 6.4.2015.

5 Layered network security: A best-practices approach. 2003. PDF-tiedosto. StillSecure. http://stillsecure.com/sites/default/files/documents/StillSecure_LayeredSecurity.pdf>. Luettu 08.04.2015.

6 Securing Unified CCE. 2009. Verkkodokumentti. Security Layers. Cisco. <http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/srnd/7x/c7scurty.html#wp1064762>. Luettu 08.04.2015.

7 5 Tips for Securing Your Wireless Network. 2015. Verkkodokumentti. About.com <http://netsecurity.about.com/od/secureyourwifinetwork/a/5-Tips-For-Securing-Your-Wireless-Network.htm>. Luettu 09.04.2015.

8 Electromagnetic interference at 2.4 GHz. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz>. Luettu 25.2.2015.

9 IEEE 802.11. 2015. Verkkodokumentti. Wikipedia. http://en.wikipedia.org/wiki/IEEE_802.11>. Luettu 25.2.2015.

10 TCP/IP protocol fundamentals explained with diagram. 2011. Verkkodokumentti. The Geek Stuff. <http://www.thegeekstuff.com/2011/11/tcp-ip-fundamentals/>. Luettu 04.04.2015.

11 IP address. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/IP_address>. Luettu 05.04.2015.

12 MAC address. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/MAC_address>. Luettu 05.04.2015.

13 Network basics: networking port overview. 2015. Verkkodokumentti. Dummies.com. <http://www.dummies.com/how-to/content/network-basics-networking-port-overview.html>. Luettu 05.04.2015.

14 TCP/IP. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/TCP/IP>. Luettu 31.03.2015.

15 HTTPS. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/HTTPS>. Luettu 31.03.2015.

16 HTTP. 2015. Verkkodokumentti. Wikipedia. < http://fi.wikipedia.org/wiki/HTTP>. Luettu 31.03.2015.

17 Transport Layer Security. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Transport_Layer_Security>. Luettu 31.03.2015.

18 TLS. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/TLS>. Luettu 31.03.2015.

19 Digital Certificates Explained. 2015. Verkkodokumentti. Knowledge Base. <https://sites.google.com/site/amitsciscozone/home/security/digital-certificates-explained>. Luettu 01.04.2015.

20 Desktop Operating System Market Share. 2015. Netmarketshare. <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. Luettu 22.02.2015.

21 Microsoft Windows. 2015. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Microsoft_Windows>. Luettu 15.2.2015.

22 Forget Windows, the most vulnerable operating systems in 2014 were MAC OS X and iOS. 2015. Verkkodokumentti. Winbeta. <http://winbeta.org/news/forget-windows-most-vulnerable-operating-systems-2014-were-mac-os-x-and-ios>. Luettu 15.2.2015.

23 OS X. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/OS_X>. Luettu 15.2.2015.

24 How Infected Are We? 2015. Verkkodokumentti. TopTenReviews.com. <http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html>. Luettu 29.03.2015.

25 Common malware types: Cybersecurity 101. 2012. Verkkodokumentti. Veracode. <https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/>. Luettu 29.03.2015.

26 Haittaohjelmilta suojautuminen. 2015. Verkkodokumentti. Helsingin Yliopisto. <http://blogs.helsinki.fi/tvt-ajokortti/5-tietoturva/5-2-suojautuminen-uhkatekijoilta/haittaohjelmilta-suojautuminen/>. Luettu 29.3.2015.

27 Asian countries found to lead top 10 malware-infected countries in 2012. 2013. Verkkodokumentti. Spywareremove. <http://www.spywareremove.com/asian-countries-top-10-malware-countries-2012.html>. Luettu 29.03.2015.

28 Why using a public Wi-Fi network can be dangerous, eve when accessing encrypted websites. 2014. Verkkodokumentti. How-To Geek. <http://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/>. Luettu 26.03.2015.

29 Firesheep. 2010. Verkkodokumentti. Codebutler. <http://codebutler.com/firesheep/>. Luettu 22.03.2015.

30 Address Resolution Protocol. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Address_Resolution_Protocol>. Luettu 20.03.2015.

31 What is a man-in-the-middle attack?. 2013. Verkkodokumentti. Kaspersky. <http://blog.kaspersky.com/man-in-the-middle-attack/>. Luettu 20.03.2015.

32 Removing admin rights mitigates 97% of critical Microsoft vulnerabilities. 2015. Verkkodokumentti. Avecto. <http://www.avecto.com/news-and-events/press-releases/removing-admin-rights-mitigates-97-of-critical-microsoft-vulnerabilities>. Luettu 12.04.2015.

33 File sharing, privacy and malware. 2010. Verkkodokumentti. University of California, San Diego. <http://acms.ucsd.edu/students/resnet/malware_filesharing.html>. Luettu 09.04.2015.

34 Malvertising is here: How to protect yourself. 2014. Verkkodokumentti. Tom´s Guide. <http://www.tomsguide.com/us/malvertising-what-it-is,news-19877.html>. Luettu 13.04.2015.

35 Here´s what happens when you install the top 10 download.com apps. 2015. Verkkodokumentti. How-To Geek. <http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/>. Luettu 13.04.2015.

36 Potentially unwanted program borrows tricks from malware authors. 2014. Verkkodokumentti. Malwarebytes. <https://blog.malwarebytes.org/fraud-scam/2014/12/potentially-unwanted-program-borrows-tricks-from-malware-authors/>. Luettu 13.04.2015.

37 Don´t get caught in the phish net. 2015. Verkkodokumentti. Komodo. <https://www.comodo.com/resources/home/what-are-phishing-scams.php>. Luettu 14.04.2015.

38 Microsoft Windows. Security. 2015. Verkkodokumentti. Wikipedia. <https://en.wikipedia.org/wiki/Microsoft_Windows#Security>. Luettu 18.02.2015.

39 HTG explains: how antivirus software works. 2012. Verkkodokumentti. How-To Geek. <http://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/>. Luettu 10.03.2015.

40 AV-comparatives names product of the year for 2014. 2015. Verkkodokumentti. Security Watch. <http://securitywatch.pcmag.com/security-software/331532-av-comparatives-names-product-of-the-year-for-2014>. Luettu 10.03.2015.

41 Firewall (computing). 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Firewall_(computing)>. Luettu 02.04.2015.

42 Palomuuri. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Palomuuri>. Luettu 02.04.2015.

43 Enhanced Mitigation Experience Toolkit-apuohjelma. 2015. Verkkodokumentti. Microsoft. <https://support.microsoft.com/en-us/kb/2458544/fi>. Luettu 14.04.2015.

44 Mitä on tietojen suorittamisen estäminen?. 2015. Verkkodokumentti. Windows. <http://windows.microsoft.com/fi-FI/windows-vista/What-is-Data-Execution-Prevention>. Luettu 14.04.2015.

45 Tietojen suorittamisen estäminen. 2007. Verkkodokumentti. Neko.kapsi.fi. <http://neko.kapsi.fi/ohje/Windows_7-vinkit/DEP.html>. Luettu 14.04.2015.

46 EMET 4.0´s certificate trust feature. 2013. Verkkodokumentti. Technet. <http://blogs.technet.com/b/srd/archive/2013/05/08/emet-4-0-s-certificate-trust-feature.aspx>. Luettu 14.04.2015.

47 A guide to sniffing out passwords and cookies (and how to protect yourself against it). 2011. Verkkodokumentti. Lifehacker. <http://lifehacker.com/5853483/a-guide-to-sniffing-out-passwords-and-cookies-and-how-to-protect-yourself-against-it>. Luettu 01.04.2015.

48 Virtual Private Network. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Virtual_private_network>. Luettu 02.04.2015.

49 Android (operating system). 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Android_(operating_system)>. Luettu 09.04.2015.

50 iOS. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/IOS>. Luettu 09.04.2015.

51 Windows Phone. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Windows_Phone>. Luettu 09.04.2015.

52 Google Play. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Google_Play>. Luettu 09.04.2015.

53 Google Play. Application approval. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Google_Play#Application_approval>. Luettu 09.04.2015.

54 Androidin haittaohjelma asennukset puolittuivat vuonna 2014. 2015. Verkkodokumentti. Mobiili.fi. <http://mobiili.fi/2015/04/02/androidin-haittaohjelma-asennukset-puolittuivat-vuonna-2014/>. Luettu 10.04.2015.

55 App Store. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/App_Store>. Luettu 10.04.2015.

56 Does iOS malware actually exist? 2014. Verkkodokumentti. ZDnet. <http://www.zdnet.com/article/does-ios-malware-actually-exist/>. Luettu 10.04.2015.

57 Windows Phone Store. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Windows_Phone_Store>. Luettu 10.04.2015.

58 Microsoft: Windows Phone Store hosts more than 300000 apps. 2014. Verkkodokumentti. Phonearena.com. <http://www.phonearena.com/news/Microsoft-Windows-Phone-Store-hosts-more-than-300000-apps_id59112>. Luettu 10.04.2015.

59 Essentially all mobile malware still targets Android: F-Secure. 2014. Verkkodokumentti. Securityweek. <http://www.securityweek.com/essentially-all-mobile-malware-still-targets-android-f-secure>. Luettu 10.04.2015.

60 Eight ways to keep your smartphone safe. 2014. Verkkodokumentti. Bullguard. <http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-protection-resources/8-ways-to-keep-your-smartphone-safe.aspx>. Luettu 16.04.2015.

61 Get smart about mobile phone safety. 2014. Verkkodokumentti. Microsoft. <http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx>.Luettu 15.04.2015.

62 3G. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/3G>. Luettu 14.04.2015.

63 Suomessa 4g-dataa voidaan varastaa - ”salataan vasta, kun jollakin operaattorilla tapahtuu jotain”. 2014. Verkkodokumentti. MPC. <http://www.mpc.fi/uutisia/suomessa+4gdataa+voi+varastaa++quotsalataan+vasta+kun+jollakin+operaattorilla+tapahtuu+jotainquot/a979312>. Luettu 15.04.2015.

64 Survey finds 34% of users take no security measures on public Wi-Fi. 2013. Verkkodokumentti. Private Wi-Fi. <http://www.privatewifi.com/survey-finds-34-of-users-take-no-security-measures-on-public-wifi/>. Luettu 20.03.2015.

65 Staggering figures: Half of all US adults hacked in last 12 months. 2014. Verkkodokumentti. RT. <http://rt.com/usa/162376-47-percent-americans-hacked-year/>. Luettu 24.03.2015.

66 Verkkotiedustelu. 2013. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Verkkotiedustelu>. Luettu 16.04.2015.

67 Port scanner. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Port_scanner>. Luettu 16.04.2015.

68 CCNA security final exam. 2012. Verkkodokumentti. Aguezstw blog. <https://aguezstw.wordpress.com/ccna-security-exam/ccna-security-final-exam/>. Luettu 04.05.2015.

69 SSL details. 2015. Verkkodokumentti. SSLShopper. <https://www.sslshopper.com/ssl-details.html>. Luettu 04.05.2015.

70 The evolution of OS X malware. 2014. Verkkodokumentti. Eugene Kaspersky. <http://eugene.kaspersky.com/2014/09/29/the-evolution-of-os-x-malware/>. Luettu 04.05.2015.

71 Malware. 2015. Verkkodokumentti. AV-test. <http://www.av-test.org/en/statistics/malware/>. Luettu 04.05.2015.

72 Eavesdropping on enterprise apps. 2013. Verkkodokumentti. SC Magazine. <http://www.scmagazine.com/eavesdropping-on-enterprise-apps/article/316361/>. Luettu 04.05.2015.

73 How (and why) to set up a vpn today. 2013. Verkkodokumentti. PCWorld. <http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html>. Luettu 04.05.2015.

Muistilista

- Käyttöjärjestelmän ja ohjelmien pitäminen päivitettyinä
- Virustorjuntaohjelman käyttö, mielellään kolmannen osapuolen.
- Palomuurin käyttäminen, erillinen ohjelma tai virustorjuntaohjelman mukana tuleva.
- Julkisten verkkojen käyttäjille: maksullinen VPN-ohjelma tai käyttää puhelinta reitittimenä. Tällöin tietokone käyttää puhelimen datayhteyttä Internetiin pääsemiseksi.
- Tietokoneelle tulevia yhteyksiä ei pidä hyväksyä, jos ei tiedä mikä tai kuka ottaa yhteyttä.
- Sähköpostien sisältämiä linkkejä tai liitetiedostoja ei pidä avata. Erityisesti jos lähettäjä on tuntematon, tunnetunkin lähettäjän viestin kohdalla pitää noudattaa varovaisuutta jos viesti vaikuttaa epäilyttävältä.
- Selaimeen kannattaa asentaa mainostenesto-ohjelma, esim. Adblock tai Adblock Plus.
- Vertaisverkoista saatavien ohjelmien käyttöä on syytä välttää.
- Selaimesta tulisi laittaa päälle HTTPS-yhteyden pakottaminen. Löytyy laajennuksena suosituimpiin selaimiin nimellä, HTTPS Everywhere.
- Windows-koneissa ei pidä käyttää järjestelmävalvojan tiliä. Normaali käyttäjätili riittää päivittäiseen käyttöön.