HAAGA-HELIA
ammattikorkeakoulu

Selainten tietoturva

Aki Riionheimo

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

21.3.2011

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

Tietojenkäsittely

Tekijät Aki Riionheimo	**Aloitusvuosi** 2006
Opinnäytetyön nimi Selainten tietoturva	**Sivu- ja liitesivumäärä** 46 + 6
Ohjaaja tai ohjaajat Titta Ahlberg	

Tämän opinnäytetyön tavoitteena oli selvittää vuoden 2010 yleisimmät verkon tietoturvauhkat, tutkia mitkä niistä kohdistuvat selaimeen, sekä selvittää mikä selain tarjoaa parhaat edellytykset näitä uhkia vastaan suojautumiseen. Tutkittavien selainten määrä rajattiin kolmeen markkinaosuudeltaan suurimpaan selaimeen, jotka ovat Windows Internet Explorer, Mozilla Firefox ja Google Chrome.

Vuoden 2010 yleisimmät tietoturvauhkat selvitettiin kirjallisuuskartoituksen avulla ja yleisimmiksi uhkiksi osoittautuivat XSS-hyökkäykset, haittaohjelmat, tietojenkalastelu, plugin-haavoittuvuudet, sosiaaliset verkot, botnet-verkot, roskaposti sekä käyttöjärjestelmien haavoittuvuudet. Kirjallisuuskartoituksen avulla myös selvitettiin, millaisia tietoturvaominaisuuksia tutkittavat selaimet tarjoavat uhkia vastaan.

Selainten arviointi suoritettiin vertailulla, jossa selainten tietoturvaominaisuudet pisteytettiin sekä analysoitiin, ja lopuksi verrattiin keskenään. Vertailun lisänäkökulmaksi valittiin kirjallisuuskartoituksen avulla selvitetyt selaimista vuoden 2010 aikana löytyneet haavoittuvuudet ja niihin julkaistut korjaukset.

Tutkimuksessa selainten välille muodostui eroja suuntaan ja toiseen. Internet Explorer suoriutui ominaisuusvertailussa tasaisen vahvasti, mutta haavoittuvuuksien korjaamisessa se jätti toivomisen varaa. Mozilla Firefox puolestaan oli ominaisuuksiltaan muita hieman heikompi, mutta haavoittuvuustilastoissa se pärjäsi erinomaisesti. Google Chromen suoritus oli kiitettävää molemmilla osa-alueilla.

Vaikka selainten välille syntyikin tutkimuksessa eroja, ei niistä yhtäkään voida pitää tietoturvan osalta riittämättömänä, sillä järjestelmän tietoturva ei ole yksin selaimen harteilla. Selaimen tietoturvaan vaikuttavat myös monet selaimesta riippumattomat seikat, kuten plugin-haavoittuvuudet. Tietoturvauhkien monimutkaistuminen vaatii myös käyttäjältä yhä enemmän valppautta.

Asiasanat
Selain, tietoturva, internet

HAAGA-HELIA
ammattikorkeakoulu

Business Information Technology

Abstract

Authors Aki Riionheimo	**Year of entry** 2006
The title of thesis Web browser data security	**Number of pages and appendices** 46 + 6
Supervisors Titta Ahlberg	

The purpose of this thesis was to determine the most common data security threats in 2010, to study which of these threats are targeted at web browsers and ultimately to investigate which browser offers the best qualities against these threats. The number of investigated browsers was limited to the three most popular ones: Windows Internet Explorer, Mozilla Firefox and Google Chrome.

The most common data security threats were determined by means of a literature study. The most common threats were cross-site scripting attacks, malware, phishing, plug-in vulnerabilities, social networks, botnets, junk mail and OS vulnerabilities. In addition, the browsers' security features were also determined by means of a literature study.

The evaluation of the browsers was carried out with a comparison in which the browsers' security features were analyzed and given a score. An additional viewpoint to the study was the browsers' vulnerability statistics for the year 2010, which were researched through literal sources.

The study indicated some differences between the browsers. Internet Explorer fared well in the feature comparison, but it has some unpatched vulnerabilities. Mozilla Firefox, on the other hand, lacks some key security features, but its vulnerability patching was excellent. Google Chrome's performance was outstanding in both areas.

Although the study indicated quite a few differences between the browsers, not one is inadequate in terms of data security, especially since data security is not just the browser's responsibility. The browser data security is also affected by many outside matters, for example, third party plug-ins. Also the rising complexity of security threats demands increasing awareness from users.

Key words
Browser, data security, internet

Sisällys

1 Johdanto

Tietotekniikka ja internet ovat jo kauan olleet täysin arkipäiväisiä asioita, joita käytetään niin työntekoon kuin vapaa-ajalla viihtymiseen. Verkossa liikkuvien ihmisten määrä kasvaa kasvamistaan, kun tietotekniikan halpenemisen myötä myös kehittyvien maiden asukkaat pääsevät hiljalleen käyttämään uutta teknologiaa. Palvelut ovat muutaman klikkauksen päässä ja tiedonhaku on helpompaa kuin koskaan. Kolikolla on myös kääntöpuolensa, sillä siellä missä on ihmisiä, on myös rikollisuutta. Internetistä on viime vuosien aikana tullut verkkorikollisten pelikenttä, jossa pahaa-aavistamattomia käyttäjiä huijataan ja ihmisten käyttäjätunnukset ja luottokorttitiedot ovat haluttua kauppatavaraa. Käynnissä on sähköinen sota, jossa kaikki keinot ovat sallittuja. Sota, joka asettaa muun muassa internet-selainten kehittäjille entistä suuremman haasteen.

1.1 Tutkimuksen tavoite, rajaukset ja tutkimusongelma

Monia yksityiselämän päivittäisiä askareita hoidetaan nykyään verkossa. Samoin yritysmaailmassa niin sanotut pilvipalvelut, eli sovellusten ja järjestelmien käyttäminen verkon yli, yleistyvät kasvavaa vauhtia. Monia näistä järjestelmistä käytetään selaimella, joten selainten tietoturvan tutkimiselle on suurta sosiaalista kysyntää.

Tämän opinnäytetyön tavoitteena on selvittää verkon yleisimmät tietoturvauhkat vuonna 2010, sekä tutkia mitkä niistä kohdistuvat selaimiin ja mikä selain tarjoaa parhaimmat edellytykset näitä uhkia vastaan suojautumiseen. Tutkittavien selainten määrä on rajattu kolmeen markkinaosuudeltaan suurimpaan selaimeen, jotka ovat Windows Internet Explorer, Mozilla Firefox ja Google Chrome. Selainten markkinaosuudet on esitetty taulukossa 1. Lisärajauksena tutkimuksessa toimii Windows-käyttöjärjestelmäympäristö, sillä Internet Exploreria ei enää kehitetä muille alustoille.

Windows Internet Explorer	57 %
Mozilla Firefox	23 %
Google Chrome	10 %
Apple Safari	6 %
Opera	2 %
Muut	2 %

Taulukko 1. Selainten markkinaosuudet joulukuussa 2010 (Net Applications 2010).

Tutkimustavoitteesta on koostettu seuraava tutkimusongelma ja sen alaongelmat:

- Mikä on tietoturvallisin selain vuoden 2010 yleisimpiä tietoturvauhkia vastaan?
  - Mitkä ovat vuoden 2010 yleisimmät tietoturvauhkat?
  - Mitkä uhkista kohdistuvat selaimiin?
  - Mikä selain tarjoaa parhaat edellytykset kyseisiä uhkia vastaan?

1.2 Tutkimuksen rakenne

Pääluvuissa 2-3 käsitellään aiheen teoriaa. Toisessa luvussa esitellään lyhyesti tietoturvauhkien historiaa sekä kahden tunnetun tietoturvayhtiön raporteista kootut yleisimmät verkon tietoturvauhkat. Kolmannessa luvussa selvitetään kirjallisuuskartoituksen avulla tutkittavien selainten tietoturvaominaisuuksia ja niiden suojautumiskykyä luvun 2 tietoturvauhkia vastaan. Kolmannessa luvussa on lisäksi selvitetty selainten haavoittuvuustilastot vuoden 2010 ajalta.

Pääluvut 4-5 käsittelevät itse tutkimusta. Neljännessä luvussa aluksi analysoidaan luvussa kaksi selvitetyt tietoturvauhkat ja selvitetään mitkä niistä kohdistuvat ensisijaisesti selaimiin, sekä lopuksi suoritetaan tutkittavien selainten vertailu ja esitetään vertailusta syntyvät tulokset. Viidennessä luvussa ovat tutkimuksen yhteenveto, johtopäätökset sekä jatkotutkimusehdotukset.

2 Verkon tietoturvauhkat

Tietoturva on sähköisten järjestelmien, tietoliikenteen ja datan suojaamista. Tietokoneiden ja -verkkojen yleistyttyä ja verkkorikollisuuden nostettua vuosien saatossa päätään tietoturvaan alettiin kiinnittää yhä enemmän huomiota.

Verkkorikollisuus on nykyään niin monimuotoista, että hyvään tietoturvaan vaaditaan useampia osa-alueita. Tietoliikennettä suojataan palomuureilla, tiedostoja virustorjuntaohjelmistoilla, käyttäjien liikkumista verkossa selainten tietoturvaominaisuuksilla sekä yleistä tietoturvaa esimerkiksi käyttöjärjestelmien ja ohjelmien tietoturvapäivityksillä.

Tässä tutkimuksessa keskitytään selainten tietoturvaan, eli selainten kykyyn suojata verkossa liikkuvia käyttäjiä erilaisia tietoturvauhkia vastaan. Tässä luvussa käsitellään tietoturvauhkien historiaa sekä vuoden 2010 yleisimmät verkon tietoturvauhkat.

2.1 Tietoturvauhkien historiaa

Ensimmäiset tietoturvauhkat juontavat juurensa ajalle kauan ennen internetin yleistymistä. Jo 1970-luvun alussa internetin esi-isästä, ARPAnet-tietoverkosta, löydettiin Creeper-niminen mato, joka kopioitui modeemien välityksellä järjestelmästä toiseen tulostaen ruudulle tekstin ”Minä olen Creeper. Ota kiinni jos saat!”. 1970-luvulla tavattiin myös muutamia muita verrattain harmittomia viruksen esiasteita. Ensimmäinen varsinainen virus oli vuonna 1981 Apple II -koneilla levinnyt Elk Cloner. (Solomon & Slade 2009.)

Tiettävästi ensimmäinen PC-virus oli tammikuussa 1986 havaittu Brain, joka levisi DOS-käyttöjärjestelmissä levykkeiden välityksellä. Brain-virus oli siitä erikoinen, että sen koodi sisälsi tekijöidensä tarkat yhteystiedot. Brain ei ollut varsinaisesti haitallinen virus, sillä sen tarkoitus oli seurata ja estää toisen ohjelmiston piraattilevitystä. (Linnake 2011.)

Internetin ja Windows-käyttöjärjestelmien yleistyessä 1990-luvun alussa virusten ja muiden haittaohjelmien määrä alkoi kasvaa räjähdysmäisesti. Hyökkäykset olivat myös

entistä kohdennetumpia; vuosina 1995-1998 nähtiin omat virukset muun muassa Windows 95:lle, Linuxille, Word- ja Excel-ohjelmille sekä Java-kehitysympäristölle. 1990-luvun virukset ja haittaohjelmat keskittyivät lähinnä leviämään laajalle ja aiheuttamaan vahinkoa tartuttamissaan järjestelmissä muun muassa tiedostoja tuhoamalla. (Solomon & Slade 2009.)

2000-luvulla verkon tietoturvauhkat monipuolistuivat entisestään ja verkkorikolliset alkoivat tavoitella toimillaan entistä enemmän taloudellista hyötyä. Hyökkäykset kohdistuivat käyttäjien henkilökohtaisiin tietoihin, muun muassa käyttäjätunnuksiin ja luottokorttitietoihin, ja sosiaalisten verkkojen suosio tarjosi tietojenkalastelulle otollisen alustan. (Solomon & Slade 2009.)

Verkkorikollisuus saattaa olla matkalla kohti valtioiden välistä sähköistä sodankäyntiä. Tästä saatiin esimakua heinäkuussa 2010 havaitun Stuxnet-madon muodossa. Stuxnet on yksi kaikkien aikojen taidokkaimmista haittaohjelmista, jonka ainoa tehtävä on saastuttaa ja uudelleenohjelmoida tiettyjä Siemensin valmistamia teollisuuden ohjausjärjestelmiä, joita käytetään muun muassa ydinvoimaloissa. Stuxnetin kehityksen on epäilty tapahtuneen valtiotasolla ja sen pääasiallisena kohteena on pidetty Iranin ydinvoimaloita. (McMillan 2010.)

2.2 Yleisimmät verkon tietoturvauhkat

Seuraavissa alaluvuissa on tarkasteltu yleisimpiä verkon tietoturvauhkia vuonna 2010. Uhkat on koottu tietoturvayhtiö Kaspersky Labin (2010) osavuosikatsauksesta sekä tietoturvayhtiö Sophoksen (2010) puolivuosittaiskatsauksesta. Uhkat eivät ole tärkeysjärjestyksessä.

2.2.1 Botnet-verkot

Botnet-verkolla tarkoitetaan lukuisten tietokoneiden muodostamaa verkkoa, jossa koneet on saastutettu yleensä rootkit-tyyppisellä haittaohjelmalla, joka antaa verkkorikolliselle mahdollisuuden hallita verkon koneita käyttäjien tietämättä. Haittaohjelma pyrkii myös peittämään jälkensä ja läsnäolonsa, tehden sen tunnistamisesta ja poistamisesta

vaikeaa. Tällaista ”zombie”-koneiden verkkoa käytetään moniin laittomiin tarkoituksiin. (Kayne 2011.)

Yleinen botnet-verkon käyttötarkoitus on saastuneiden koneiden käyttäminen roskapostin lähettäjinä. Botnet-verkon ylläpitäjä joko suorittaa roskapostitusta itse, tai vaihtoehtoisesti vuokraa verkkoaan muille roskapostittajille. Tavallisen roskapostin lisäksi botnet-verkon välityksellä levitetään myös tietojenkalastelutarkoituksiin räätälöityjä, väärennettyjä sähköpostiviestejä sekä haittaohjelmia. (Kayne 2011.)

Rahan ansaintatarkoitusten lisäksi botnet-verkkoja käytetään haitan aiheuttamiseen verkkopalveluille hajautettujen palvelinestohyökkäysten muodossa. Hajautetussa palvelinestohyökkäyksessä kaikille botnet-verkon koneille lähetetään käsky ottaa toistuvasti yhteyttä johonkin tiettyyn verkkopalvelimeen samanaikaisesti. Yhteyksien määrä kasvaa niin suunnattomaksi, että web-palvelimen toiminta yleensä ensin hidastuu ja lopulta palvelin kaatuu kokonaan. Palvelunestohyökkäyksien kohteeksi joutuvat useimmiten tunnettujen suuryritysten verkkopalvelut. (Kayne 2011.)

2.2.2 Cross-site scripting (XSS)

Cross-site scripting (XSS) on tämän hetken yksi hyödynnetyimmistä tietoturvaongelmista. XSS-hyökkäykset ovat web-palvelimien haavoittuvuuksia hyödyntäviä hyökkäyksiä, jossa vihamielisiä skriptejä piikitetään muutoin luotettuihin web-sivustoihin. Kun skripti on saatu palvelimelle, hyökkääjä voi lähettää skriptin palvelimella vierailevalle käyttäjälle. Käyttäjän selain ei voi tietää, että skripti on epäluotettava, joten se suorittaa skriptin. Koska selain luulee, että skripti tuli luotetusta lähteestä, skriptillä on pääsy kaikkiin käyttäjän evästeisiin, istuntoavaimiin ja muihin arkaluontoisiin selaimen säilömiin tietoihin. Toinen yleinen XSS-hyökkäyksen tavoite on ohjata käyttäjä hyökkääjän hallinnoimaan web-palveluun, esimerkiksi väärennettyyn verkkopankkiin. (OWASP 2010.)

Perinteinen XSS-hyökkäys voi olla esimerkiksi seuraavanlainen: hyvämaineisen verkkokaupan web-palvelimelta löydetään XSS-haavoittuvuus ja hyökkääjä piikittää kaupan URL-osoitekenttään haitallista koodia, joka ohjaa kaupan asiakkaan väärennetylle,

verkkokaupan sivua muistuttavalle sivulle. Väärennetyllä sivulla ajetaan lisää haitallista koodia, jonka tavoitteena on ladata käyttäjän koneelta verkkokaupan asettama eväste. Evästeen saatuaan hyökkääjä voi ottaa käyttäjän verkkokauppaistunnon hallintaansa ja esimerkiksi varastaa verkkokaupan asiakastietoihin mahdollisesti tallennetut luottokorttitiedot. XSS-hyökkäyksissä ei siis fyysisesti hyökätä sivustoja vastaan, vaan hyödynnetään web-palvelimilta löytyviä skriptaushaavoittuvuuksia. (Guillaumier 2007.)

2.2.3 Roskaposti

Roskaposti on useimmiten sähköpostin välityksellä tapahtuvaa massapostitusta, johon ei ole vastaanottajan suostumusta. Roskapostin avulla mainostetaan tuotteita ja palveluja sellaisten yritysten toimesta, joihin vastaanottajilla ei useinkaan ole minkäänlaisia kytköksiä. Tavallinen roskaposti on käyttäjille lähinnä riesa, mutta roskaposti voi olla vaarallistakin, sillä sen avulla levitetään yhä enemmän haittaohjelmia ja huijausyrityksiä. Roskapostin lähettäminen on laitonta useissa maissa. (Black 2011.)

Jotta roskapostin lähettäjien jäljittäminen olisi mahdollisimman hankalaa, roskapostittajat käyttävät postin lähettämiseen botnet-verkkoja, eli tavallisten käyttäjien kaapattuja tietokoneita. Tällä tavoin tavalliset käyttäjät osallistuvat tietämättään roskapostin lähetykseen ja varsinaisten roskapostittajien kiinni saaminen on erittäin vaikeaa. Muutaman viime vuoden aikana myös kaapattuja internet-sähköpostitilejä, muun muassa Hotmail- ja Gmail-palveluista, on alettu käyttämään roskapostin lähettämiseen. (Sophos 2010, 20.)

Vaikka roskapostin pääasiallinen jakelukanava on sähköposti, on se levinnyt myös muihin sähköisiin medioihin. Muun muassa pikaviestinohjelmissa ja sosiaalisissa verkoissa levitetään roskapostia tekaistuilla tai kaapatuilla käyttäjätileillä. Myös keskustelufoorumeilla ja verkkoblogeissa levitetään roskapostiviestejä kuhunkin palveluun räätälöidyillä keinoilla. (Sophos 2010, 21.)

2.2.4 Haittaohjelmat (Malware)

Yleisin ja laajin verkon tietoturvauhka on Malware (Malicious Software, haittaohjelma). Malware-käsitteen alle on koottu useita erityyppisiä haittaohjelmia, joiden tarkoituksena on aiheuttaa tuhoa tai tunkeutua tietokonejärjestelmiin ilman käyttäjän tietämystä tai lupaa. Kuten biologisella viruksella, myös haittaohjelmalla ensimmäinen tavoite on levitä mahdollisimman laajalle, tuhon aiheuttaminen tai tiedon varastaminen ovat toissijaisia tavoitteita. (Kassner 2009.) Yleisimpiä haittaohjelmatyyppejä ovat muun muassa seuraavat (Kassner 2009):

- **Virus**: haittaohjelma, joka kykenee saastuttamaan tietokoneen, mutta tarvitsee jonkin toisen keinon levitäkseen koneesta toiseen. Tällainen keino on viruksen kiinnittäminen johonkin ajettavaan ohjelmakoodiin, esimerkiksi sähköpostin PDF-liitteeseen.
- **Mato (worm)**: virusta kehittyneempi haittaohjelma, joka pystyy levittämään itseään käyttäjän toimista riippumatta verkkoyhteyksien avulla. Yleisin malwaretyyppi, joka sai alkunsa jo vuonna 1988.
- **Takaportti (backdoor)**: kuin etähallintaohjelma, mutta haittaohjelma silloin kun se asennetaan järjestelmään ilman käyttäjän lupaa. Asentuu järjestelmään joko tietoturva-aukkoja hyödyntämällä tai huijaamalla käyttäjää itse asentamaan takaportin esimerkiksi clickjackingia hyödyntämällä. Mahdollistaa hyökkääjälle järjestelmän täyden hallinnan.
- **Troijalainen (trojan horse)**: haittaohjelma, joka nimensä mukaisesti vaikuttaa olevan hyödyllinen ohjelma, mutta kätkee sisäänsä haitallisia toimintoja. Pyrkii eri tavoilla muuntamaan muotoaan hämätäkseen järjestelmän turva-ohjelmistoja.
- **Rootkit**: vaarallinen haittaohjelmien yhdistelmä, joka muodostuu yleensä troijalaisesta ja takaportista. Rootkiteistä on monia variaatioita, joista pahimmat asentuvat samalle tasolle käyttöjärjestelmän kanssa, tehden niistä todella vaikeasti poistettavia.

Haittaohjelmat ovat jo pitkään olleet verkkorikollisten suosituin työkalu, joiden kehitykseen panostetaan ja joilla ansaitaan helposti rahaa. Yksi tämän hetken suosituimmista työkaluista on ”scareware”, eli tekaistut tietoturvailmoitukset, joiden tarkoituksena

on saada käyttäjä uskomaan, että tämän tietokoneella on tietoturvaongelma, johon ilmoituksessa tarjotaan ratkaisua. Scarewarea levitetään pääasiassa sivustoille asetettuina pop-up -ikkunoina, roskapostina tai sosiaalisten verkkojen välityksellä. (Sophos 2010, 22.)

Vallitseva taloustaantuma ei ole verkkorikollisuuteen vaikuttanut, sillä haittaohjelmien tuotanto on nopeampaa kuin koskaan, kun verkkorikolliset yrittävät pysyä tietoturvayhtiöitä aina askeleen edellä. Esimerkiksi tietoturvayhtiö Sophoksen (2010, 24.) laboratoriot vastaanottivat vuoden 2010 ensimmäisellä puoliskolla noin 60 000 eri haittaohjelmanäytettä päivässä.

2.2.5 Tietojenkalastelu (phishing)

Tietojenkalastelu on yksi vanhimmista verkkorikollisuuden muodoista, joka juontaa juurensa jo internetin yleistymisen aikoihin 1990-luvun loppupuoliskolle. Tietojenkalastelu on toimintaa, jolla pyritään hankkimaan henkilökohtaisia tietoja naamioitumalla joksikin luotettavaksi tahoksi, esimerkiksi pankiksi. Tietojenkalastelussa halutuimpia tietoja ovat esimerkiksi käyttäjätunnukset, pankkitunnukset ja luottokorttitiedot. Internetin alkutaipaleella, jolloin käyttäjät eivät vielä olleet kovinkaan valveutuneita tietoturva-asioissa, tietojenkalasteluun riitti huonolla kieliopilla muotoiltu roskapostiviesti, joka vaikutti tulevan esimerkiksi joltakin rahoituslaitokselta ja jossa pyydettiin käyttäjää klikkaamaan linkkiä ja antamaan käyttäjätunnuksensa. Internetin vaarat nousivat nopeasti julkisuuteen ja käyttäjät alkoivat olla verkossa enemmän varuillaan, joten tietojenkalastelijoiden oli kehitettävä metodeitaan. (Robson 2010.)

Perinteistä roskapostia käytetään vielä nykyäänkin tietojenkalasteluun, mutta sen käyttötapa on kehittynyt. Viestien ulkoasuun ja sisältöön kiinnitetään entistä enemmän huomiota, viesteissä käytetään kuvia ja yritysten logoja, sekä väärennetyistä linkeistä pyritään tekemään mahdollisimman aidon oloisia. Uusimpia keinoja on XSS-hyökkäyksen ja tietojenkalastelun yhdistäminen siten, että sähköpostiviestin linkki ohjaa käyttäjän aidolle sivustolle ja sivuston XSS-haavoittuvuutta hyödynnetään käyttäjän tietojen keräämiseen. (Robson 2010.)

Sosiaalisten verkkojen räjähdysmäinen kasvu ei ole jäänyt verkkorikollisilta huomaamatta. Sosiaalisten verkkojen sadat miljoonat käyttäjät henkilökohtaisine tietoineen ovat tietojenkalastelijoille varsinainen kultakaivos. Sosiaalisissa verkoissa levitetään perinteisiä linkkejä sisältäviä viestejä esimerkiksi väärennettyjen käyttäjätilien avulla ja verkkojen Chat-palveluissa. Kuten perinteisen roskapostin tapauksessa, myös sosiaalisissa verkoissa yhdistellään erilaisia hyökkäystapoja tietojenkalasteluun, muun muassa vuonna 2006 MySpace-palvelussa levisi käyttäjäprofiilien linkkejä muokkaava haittaohjelma ja Facebookissa ovat viime aikoina yleistyneet ClickJacking-hyökkäykset. (Robson 2010.)

2.2.6 Käyttöjärjestelmien haavoittuvuudet

Käyttöjärjestelmistä löytyvät haavoittuvuudet ovat verkkorikollisille erittäin kiinnostavia, sillä niiden hyödyntäminen mahdollistaa usein koko järjestelmän kaappaamisen. Haavoittuvuuksia etsitään varsinkin Microsoftin Windows-tuoteperheestä, joka on eri versioineen maailman ylivoimaisesti käytetyin käyttöjärjestelmä.

Vuoden 2009 loppupuolella julkaistu Windows 7 on otettu hyvin vastaan ja se on tarjonnut huomattavasti turvallisemman alustan kuin edelleen laajasti käytössä oleva Windows XP. Windows 7:n suosion kasvaessa verkkorikolliset käyttävät sen analysointiin yhä enemmän resursseja ja käyttöjärjestelmälle onkin jo kehitetty erilaisia räätälöityjä hyökkäyksiä ja haittaohjelmia, muun muassa scareware-tuotteita. (Sophos 2010, 25.)

Myös aiemmin erittäin turvallisena pidetyn Applen OS X -käyttöjärjestelmän koskemattomuus on alkanut rakoilla. Applen tuotteet ovat viime vuosina saaneet entistä enemmän käyttäjiä, joten OS X:stä on tullut verkkorikollisia kiinnostava kohde. Tästä johtuen Apple on ottanut uusimmassa OS X:n 10.6-versiossa ensimmäistä kertaa käyttöön anti-malware -suojauksen, joka on kuitenkin vielä melko alkeellinen. Haittaohjelmien lisäksi OS X:stä on vuoden 2010 aikana löytynyt lukuisia haavoittuvuuksia, joten Applenkaan käyttöjärjestelmää käyttävällä ei ole varaa luottaa pelkästään käyttöjärjestelmän kykyyn suojautua uhkia vastaan, vaan on syytä käyttää ajantasaisia tietoturvatuotteita. (Sophos 2010, 26.)

2.2.7 Plugin-haavoittuvuudet

Koska internetissä tietoa ja multimediaa esitetään useilla keskenään kilpailevilla ja selaimista riippumattomilla tekniikoilla, selaimet eivät niitä kaikkia oletuksena tue. Tätä varten ohjelmistotalot ovat kehittäneet selaimeen asennettavat liitännäiset, pluginit. Tällaisia ovat esimerkiksi Adoben Flash Player- ja PDF-liitännäiset sekä Sun Microsystemsin Java-ohjelmistoalusta.

Suosituimmat selainliitännäiset ovat levinneet todella laajalle. Millward Brown -tutkimusyhtiön joulukuussa 2010 tekemän tutkimuksen mukaan esimerkiksi Flash Player on asennettu 99:än, Java 80:an ja Applen QuickTime 57:en prosenttiin internetiin kytketyistä tietokoneista. Erilaisia selainliitännäisiä käyttävät siis sadat miljoonat ihmiset ympäri maailmaa. (Adobe 2010.)

Liitännäisten laaja käyttäjäkunta on verkkorikollisille houkutteleva ympäristö, joten liitännäisten analysointiin käytetään paljon resursseja ja niistä etsitään jatkuvasti uusia tietoturva-aukkoja. Esimerkiksi vuoden 2010 kolmannella neljänneksellä kymmenestä yleisimmästä haavoittuvuudesta puolet sijaitsi eri selainliitännäisissä. (Namestnikov 2010.)

2.2.8 Sosiaaliset verkot

Viimeksi kuluneen vuoden aikana sosiaaliset verkot ovat integroituneet pysyväksi osaksi valtavirtamediaa ja muodostuneet yhdeksi henkilökohtaisen ja yritysviestinnän työkaluista. Yritykset käyttävät sosiaalisia verkkoja tuotteiden ja palveluiden markkinoimiseen, ja verkkojen integroiminen laitteisiin on suuri myyntivaltti elektroniikkavalmistajille. On siis selvää, että sosiaaliset verkot ovat houkutteleva kohde myös verkkorikollisille.

Aiemmin sosiaalisten verkkojen haitat yrityksissä rajoittuivat lähinnä haaskattuun työaikaan ja verkon tarpeettomaan kuormitukseen, mutta nyttemmin haittaohjelmat ja tietojenkalastelu ovat nousseet merkittäviksi ongelmiksi. Roskaposti on sosiaalisissa verkoissa yleistä ja käyttäjiä yritetään saada paljastamaan arkaluontoisia tietoja tai klikkaamaan

vaarallisia linkkejä. Asia on huomattu myös yrityksissä, sillä vuoden 2009 aikana sosiaalisista verkoista peräisin olevan roskapostin tai malwaren kohteeksi joutuneiden yritysten määrä kasvoi 70 prosentilla. (Sophos 2010, 7-8.)

Sosiaalisten verkkojen kasvaneista uhista ollaan syystäkin huolissaan, sillä useimmat haittaohjelmat ja roskapostittajat käyttävät hyväkseen varomattomia käyttäjiä. Esimerkiksi pahamaineinen Koobface-haittaohjelmaperhe toimii juuri tällä tavalla. Koobfacen tekniikka on hyvin monipuolinen: se kykenee luomaan automaattisesti Facebook-tilin, aktivoimaan tilin vastaamalla Facebookin vahvistusviestiin, lisäämään kavereiksi täysin tuntemattomia ihmisiä, liittymään satunnaisiin ryhmiin ja lähettämään edellä mainituille vaarallisia linkkejä sisältäviä viestejä. Lisäksi Koobface pyrkii välttämään ylimääräistä huomiota rajoittamalla päivittäin lisättävien kavereiden määrää. Facebookin lisäksi Koobface-perhe on muutaman viime vuoden aikana laajentunut toimimaan muun muassa MySpacen, Bebon, Friendsterin ja Twitterin kanssa. Tulevaisuudessa tullaan todennäköisesti näkemään vieläkin kehittyneempiä sosiaalisten verkkojen uhkia. (Sophos 2010, 9.)

Toinen yleinen sosiaalisissa verkoissa hyödynnetty hyökkäyskeino on eräänlainen linkin kaappaus, Clickjacking, jonka tarkoituksena on saada käyttäjä klikkaamaan jotain, mitä hän ei näe. Clickjackingia hyödyntämällä hyökkääjä voi naamioida vaarallisen linkkinsä osaksi jotakin käyttäjälle tuttua elementtiä, esimerkiksi Facebookin ”Tykkää”-painiketta. Käyttäjälle painike näkyy täysin normaalina, mutta linkkikuvan alle on kätketty hyökkääjän vaarallinen linkki, joka esimerkiksi lisää käyttäjän Facebook-sivulle muita hyökkääjän linkkejä tai yrittää ladata käyttäjän koneelle haittaohjelmia. Clickjacking-hyökkäyksiä esiintyi kesällä 2010 erityisen runsaasti varsinkin Facebookissa ja satoja tuhansia käyttäjätilejä saastui. (Sophos 2010, 10.)

3 Selainten tietoturvaominaisuudet

Selain on www-sivujen esittämiseen ja niillä vuorovaikuttamiseen käytettävä tietokoneohjelma. Selaimella katsellaan niin internetissä kuin yksityisverkoissakin olevia sivuja. Selaimen käyttö on lisääntynyt myös yritysmaailmassa, sillä useita järjestelmiä käytetään verkosta selaimen avulla.

Selaimen tietoturvaan vaikuttavat muutkin seikat kuin itse selaimen tietoturvaominaisuudet. Suuressa roolissa ovat myös kolmansien osapuolien kehittämät selaimen liitännäiset ja lisäosat, joiden kehitys ei ole selainvalmistajien vastuulla. Välillisesti selaimen tietoturvaan vaikuttavat myös verkkosivustojen alustoina toimivat web-palvelimet ja niiden mahdolliset haavoittuvuudet.

Tässä luvussa selvitetään tutkittavien selainten tietoturvaominaisuudet. Ominaisuudet perustuvat selainvalmistajien listauksiin omista tietoturvaominaisuuksistaan.

3.1 Internet Explorer 8

Windows Internet Explorer (aiemmalta nimeltään Microsoft Internet Explorer) on Microsoftin kehittämä selain, joka toimitetaan yrityksen Windows-käyttöjärjestelmien mukana. Net Applicationsin (2010) mukaan Internet Explorer on maailman ylivoimaisesti suosituin selain 57,08 % markkinaosuudellaan (joulukuu 2010).

3.1.1 Tietoturvaominaisuudet

Cross-site scripting -suodatin

Cross-site scripting -hyökkäyksiä vastaan on Internet Explorer 8:ssa kehitetty Cross-site scripting (XSS) -suodatin. XSS-suodatin tarkkailee URL-kenttää ja sivustojen välillä liikkuvia HTTP POST -sanomia vihamielisen JavaScript-koodin varalta. Mikäli sanoma sisältää JavaScript-koodia, suodatin tarkistaa sen ja etsii eräänlaista ”heijastusta”; tietoa joka lähetettäisiin takaisin mahdolliselle kolmannen osapuolen hyökkäyssivustolle, mikäli sanoman sallittaisiin kulkea vapaasti selaimen läpi. Mikäli sanoma tunnistetaan

mahdolliseksi hyökkäysyritykseksi, XSS-suodatin puhdistaa alkuperäisen sanoman siten, ettei hyökkäyssivuston lisäämää JavaScript-koodia suoriteta. Alkuperäinen sanoma siis suoritetaan, ja käyttäjälle ilmoitetaan, että Internet Explorer on havainnut hyökkäysyrityksen ja muokannut sanomaa sen mukaisesti. (MSDN Library.)

InPrivate-tila ja InPrivate-suodatus

Koska internetiä käytetään nykyisin myös yleisessä käytössä olevilla laitteilla, esimerkiksi internet-kahviloissa ja kirjastoissa, on tärkeää suojata yksittäisen käyttäjän selaustoimet uteliaiden katseilta. Tätä varten on Internet Explorer 8:ssa kehitetty InPrivate-tila, jota käyttämällä selaimeen ei tallennu mitään tietoja käyttäjän istunnosta. Kun InPrivate-tila otetaan käyttöön, selaimessa tapahtuvat muutokset ovat (Microsoft Co. 2009, 14) seuraavat:

- Liitännäiset ja työkalupalkit poistetaan käytöstä.
- Uusia evästeitä ei tallenneta. Mikäli sivusto yrittää asettaa pysyvän evästeen, tallennetaan se istuntoevästeenä ja poistetaan istunnon päättyessä.
- Sivuhistoriaa ei tallenneta.
- Väliaikaiset internet-tiedostot poistetaan istunnon päättyessä.
- Lomaketietoja ja salasanoja ei tallenneta.
- Osoitekenttään kirjoitettuja osoitteita ja hakukenttiin kirjoitettuja hakutermejä ei tallenneta.

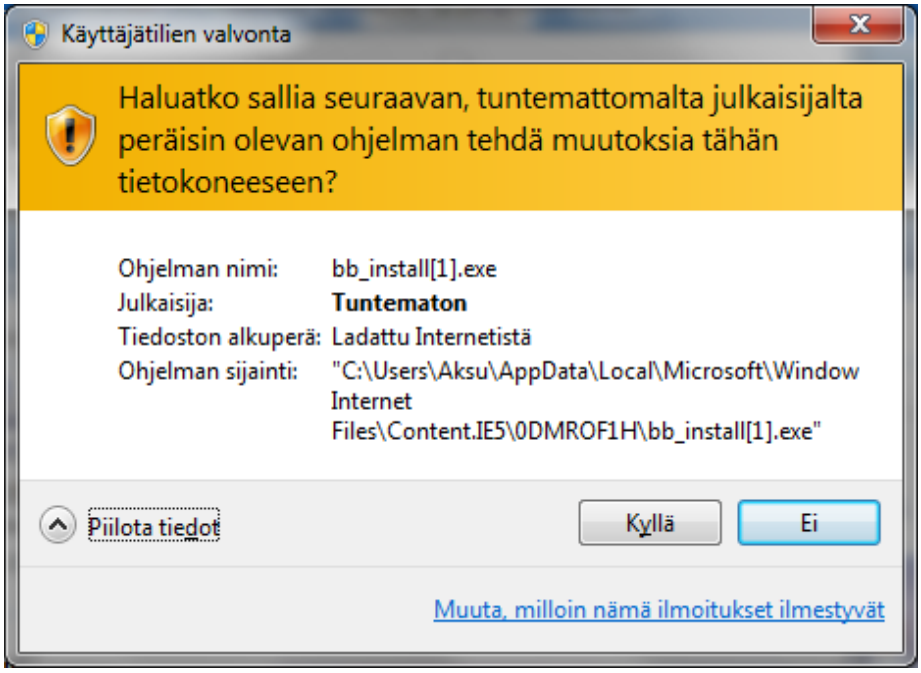
Käyttäjän selaustottumuksia on mahdollista seurata myös pidemmällä aikavälillä. Erilaisilla kolmansien osapuolien skripteillä ja seurantaevästeillä kerätään tietoa verkon käyttäjistä ja heidän selaustottumuksistaan, useimmiten täysin laillisiin ja käyttäjiä hyödyttäviin tarkoituksiin. Toisinaan kuitenkin tällaisia työkaluja käytetään rikollisiin tarkoituksiin, tavoitteena käyttäjän historia- ja muiden henkilökohtaisten tietojen kalastelu.

Tällaista toimintaa voidaan Internet Explorerissa rajoittaa uudella InPrivate-suodatuksella. Suodatin tarkkailee eri sivustojen asettamia evästeitä ja estää ne, mikäli sama eväste kohdataan useammalla kuin kymmenellä eri sivustolla. Käyttäjä voi myös

itse muokata InPrivate-suodatuksen asetuksia ja sallia tai estää tiettyjä sivustoja. (Microsoft TechNet 2009.) InPrivate-suodatus ei ole oletuksena käytössä, vaan se pitää aktivoida jokaisessa istunnossa erikseen.

Attachment Execution Service

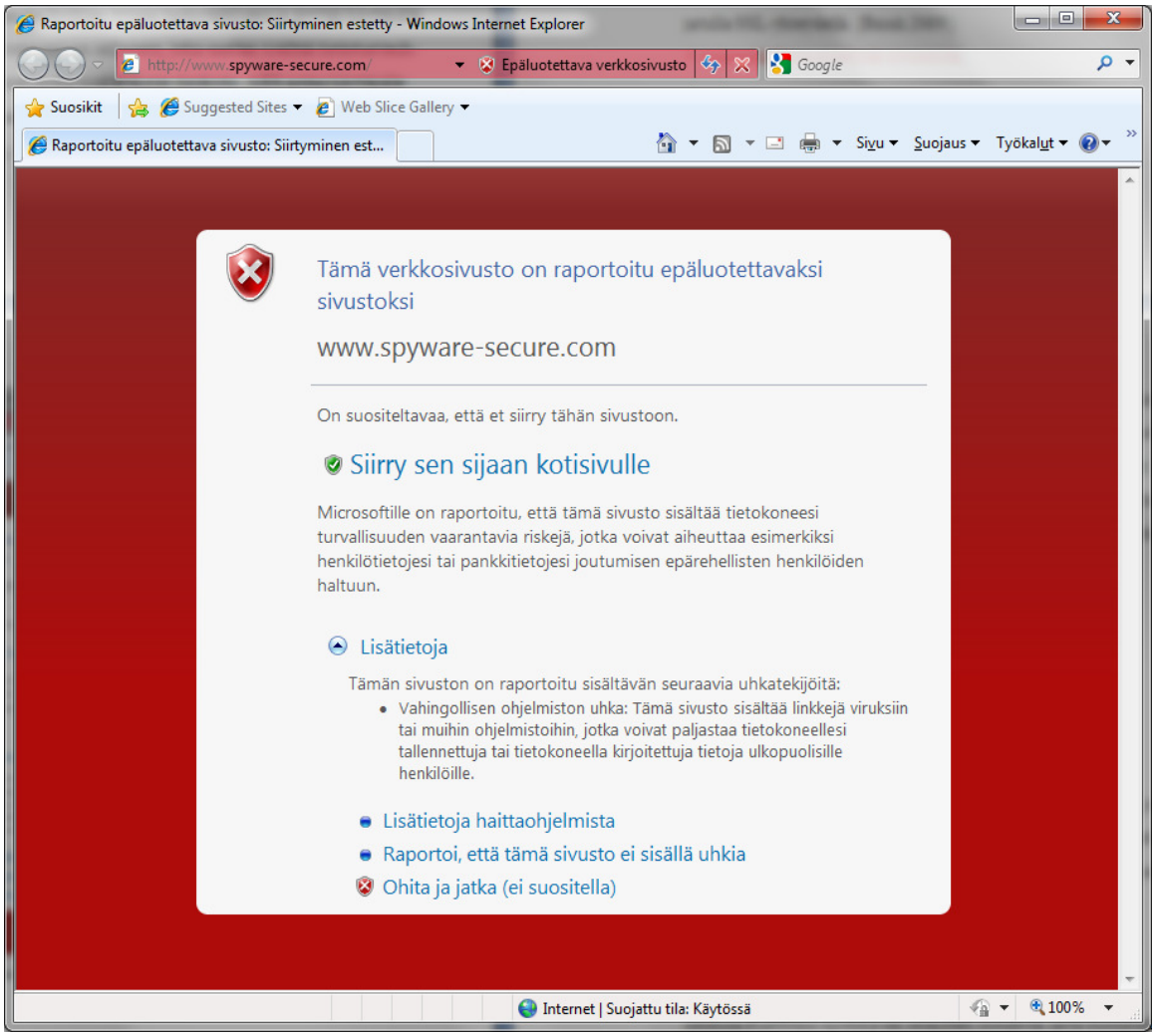
Internet Explorerin versiosta 6 lähtien selaimessa on ollut käytössä selaimen välityksellä ladattavia tiedostoja tarkkaileva Attachment Execution Service -palvelu (AES). Palvelu on käyttöjärjestelmän ominaisuus, jota käytetään myös Outlook Express -sähköpostiohjelmassa ja Windows Messenger -pikaviestinohjelmassa. Internet Explorer käyttää AES-palvelua ladattavien tiedostojen tyypin tarkistamiseen ja pyytää käyttäjältä latausvahvistusta, mikäli tiedostotyyppi on sellainen, joka saattaa sisältää tietoturvauhkia, esimerkiksi ajettavaa ohjelmakoodia sisältävä exe-tiedosto. AES antaa käyttäjälle aiempaa enemmän ja selkeämpää informaatiota tiedostoista kuin aiemmat Internet Explorerin versiot. Tiedostokoon, -tyypin ja -lähteen lisäksi AES pyrkii ilmoittamaan myös latauksen jälkeen suoritettavan tiedoston julkaisijan, ja esittää käyttäjälle selkeän varoitusilmoituksen, mikäli tiedoston julkaisija on tuntematon. (Microsoft 2004, 11-15.) Selaimen käyttäjälle esittämä ilmoitus on havainnollistettu kuvassa 1.



Kuva 1. Tuntemattoman tiedoston AES-ilmoitus Internet Explorerissa.

SmartScreen-suodatin

Internet Explorer 8:n uutena ominaisuutena on SmartScreen-suodatin, joka tarkkailee selaimessa avattavia sivustoja ja auttaa tietojenkalastelusivustojen tunnistamisessa. SmartScreen analysoi sivustoja ja vertaa niitä aktiivisesti päivitettävään estolistaan. Jos käyttäjä on aikeissa vierailla sivustolla, joka on listalla, näyttöön tulevassa ilmoituksessa kerrotaan, että sivusto on turvallisuuden vuoksi estetty. SmartScreen-suodatin tarkkailee myös ladattuja tiedostoja ja vertaa niitä estolistaan. Mikäli tiedosto on ladattu estolistalla olevalta sivustolta, käyttäjälle ilmoitetaan, että tiedosto on turvallisuuden vuoksi estetty. SmartScreen-suodatin lähettää Microsoftille raportteja internet-osoitteista suojatulla SSL-yhteydellä. (Brink 2009.) SmartScreen-suodattimen toimintaa on havainnollistettu kuvassa 2.



Kuva 2. SmartScreen-suodattimen ilmoitus Internet Explorerissa.

Protected Mode

Internet Explorerin versiossa 7 otettiin käyttöön uusi ominaisuus nimeltään Protected Mode (Suojattu tila), joka toimii vain Windows Vista ja Windows 7 -käyttöjärjestelmissä. Se perustuu Windows Vistassa esiteltyyn uuteen tietoturvamalliin, joka määrittää prosesseille ja muille käyttöjärjestelmän suojausta vaativille komponenteille eräänlaisen koskemattomuustason. Esimerkiksi uusien ohjelmien asentaminen tai käyttöjärjestelmän rekisterin muokkaaminen edellyttää korkean tason (järjestelmänvalvoja) oikeuksia ja käyttäjän kotikansioon kirjoittaminen ja sen tiedostojen muokkaaminen keskitason oikeuksia. Matalan tason oikeuksilla varustetut prosessit voivat kirjoittaa vain toisiin matalan tason prosesseihin. (Silbey & Brundrett 2009.)

Kun Internet Explorer käynnistetään Suojatussa tilassa, sillä on matalan tason oikeudet. Selaimella ja sen laajennuksilla ei siis ole kirjoitusoikeuksia käyttäjän tiedostoihin, järjestelmäkomponentteihin, tai edes selaimen asetusten muuttamiseen. Selain voi ilman käyttäjän suostumusta kirjoittaa vain muihin matalan tason kohteisiin, joita ovat muun muassa sivuhistoria, evästeet, ja väliaikaiset internet-tiedostot. Koska selaimella ei ole oletuksena oikeuksia juuri muuhun kuin internet-sivujen esittämiseen, ominaisuus vähentää saastuneen selainprosessin aiheuttamaa vahinkoa tuntuvasti. (Silbey & Brundrett 2009.)

3.2 Mozilla Firefox 3.6

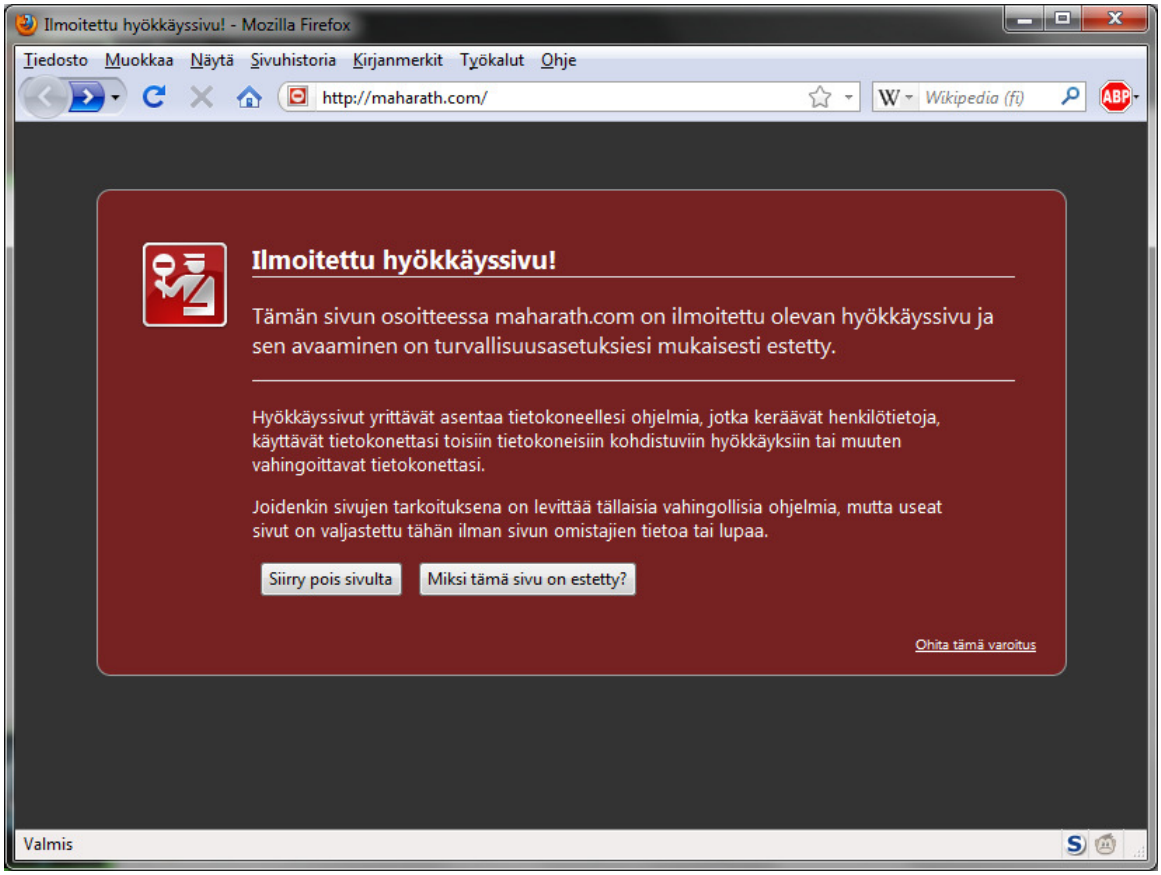
Mozilla Firefox on avoimeen lähdekoodiin perustuva selain, jota ylläpitää ja kehittää Mozilla-säätiö sekä sen alaisuudessa toimiva Mozilla Corporation -tytäryhtiö. Net Applicationsin (2010) mukaan Mozilla Firefox on maailman toiseksi käytetyin selain 22,81 % markkinaosuudella (joulukuu 2010).

3.2.1 Tietoturvaominaisuudet

Phishing and Malware Protection

Versiosta 3 lähtien Firefoxissa on toiminut sisäänrakennettu suoja tietojen kalastelu- ja hyökkäyssivustoja vastaan. Ominaisuus hyödyntää Safe Browsing -palvelua, joka on

Googlen ylläpitämä estolista vaarallisiksi raportoiduista sivustoista. Lista ladataan selaimeen, ja kaikkia selaimessa avattavia URL-osoitteita verrataan estolistaan. (Google a.) Mikäli vastaavuus löytyy, Firefox estää pääsyn sivustolle ja ilmoittaa siitä erilaisilla näkyvillä varoituksilla sen mukaan, onko kyseessä mahdollinen tietojen kalastelu- vai hyökkäyssivusto. Estolistaa päivitetään noin puolen tunnin välein. (Mozilla b.) Firefoxin ilmoitus estetystä sivustosta on esitetty kuvassa 3.



Kuva 3. Mozilla Firefoxin ilmoitus estetystä hyökkäyssivustosta.

Component Directory Lockdown

Firefoxin versiossa 3.6 on otettu käyttöön uusi ominaisuus, Component Directory Lockdown. Aiemmin kolmannen osapuolen Firefox-lisäosien kehittäjillä on ollut mahdollista ujuttaa ajettavaa koodia käyttäjän tietämättä suoraan Firefoxin components-hakemistoon, jossa suuri osa selaimen omaa koodia sijaitsee. Tällä tavalla asennetut lisäosat eivät näy käyttäjälle selaimessa mitenkään, eikä niitä pysty myöskään hallinnoimaan normaalisti. Ratkaisu ei ole ollut virallisesti tuettu missään vaiheessa, ja versiosta

3.6 lähtien tämä mahdollisuus on poistettu kokonaan käytöstä. Ominaisuus lisää erityisesti selaimen vakautta, sillä kun kaikki lisäosat asennetaan Firefoxin oman pakettihallinnan kautta, pystyy selain valvomaan yhteensopivuusongelmia entistä paremmin. Myös tietoturvan taso nousee, sillä selaimeen ei enää pysty syöttämään haitallista koodia kolmannen osapuolen lisäosan mukana käyttäjän tietämättä. (Keizer 2009.)

Private Browsing

Internet Explorerin tapaan myös Firefoxissa on yksityiseen selaukseen tarkoitettu tila nimeltään Private Browsing. Tilan ollessa käytössä muun muassa sivuhistoriaa, hakutermejä, salasanoja, evästeitä ja väliaikaisia internet-tiedostoja ei tallenneta selaimen arkistoihin. Poikkeuksia ovat kirjanmerkit ja ladatut tiedostot, jotka tallennetaan normaalisti. Asiasta informoidaan myös käyttäjää, kun yksityinen selaus kytketään päälle. Käyttäjälle myös kerrotaan, ettei yksityinen selaus tee hänestä näkymätöntä verkossa, sillä esimerkiksi internet-palveluntarjoaja tai työnantaja voi yksityisestä selaustilasta huolimatta seurata millä sivuilla selaimella on vierailtu. (Mozilla c.)

Ladattavat lisäosat

Firefoxin avoin lähdekoodi on mahdollistanut laajan lisäosien kehitysyhteisön muodostumisen selaimen ympärille. Selaimeen itse asennettavia lisäosia löytyy laidasta laitaan; jotkut lisäosat lisäävät selaimeen täysin uusia ominaisuuksia, osa taas muokkaa ja parantaa jo olemassa olevia ominaisuuksia. Myös tietoturvan parantamiseen on olemassa muutamia todella varteenotettavia lisäosia.

Adblock Plus on mainoskuvia ja muita mediaelementtejä estävä lisäosa. Mainoskuvien lisäksi Adblock osaa estää myös Flash-animaatioita ja JavaScriptiä. Toimintaperiaatteeltaan Adblock on yksinkertainen: se tarkistaa kaikki web-sivujen tekemät kutsut ja elementtien URL-osoitteet ja estää ne, mikäli elementin osoite vastaa suodatuslistalla olevia sääntöjä. Automaattisesti päivittyviä suodatuslistoja on useita erilaisia ja niitä voi tilata lisäosan asetuksista, ja suodatussääntöjä voi luoda myös itse. Adblockin pääkäyttötarkoitus on käyttäjää häiritsevien mainosten poistaminen, mutta se parantaa samalla

tietoturvaa estämällä kuviin mahdollisesti piilotetut vihamieliset linkit ja Flash- sekä JavaScript-tietoturva-aukkoja hyödyntävät elementit.

NoScript on yksinomaan tietoturvan parantamiseen suunnattu lisäosa. Nimensä mukaisesti se estää oletusarvoisesti kaiken web-sivustoilla olevan suoritettavan ohjelmakoodin, ellei käyttäjä niitä erikseen salli. Tämä koskee niin Javaa, JavaScriptiä, Flashia, Silverlightia, sivustoille upotettuja videotiedostoja ja PDF-dokumentteja, sekä muita mediaelementtejä. Sivustolle mennessä NoScript esittää selainikkunan alareunassa käyttäjälle ilmoituksen, jossa on listattu ne toimialueet, jotka yrittävät kyseisellä sivustolla ohjelmakoodia ajaa. Käyttäjällä on mahdollisuus hyväksyä toimialue joko väliaikaisesti tai pysyvästi, tai merkitä se epäluotettavaksi, jonka jälkeen NoScript estää aina kyseisen toimialueen eikä kysy siitä enää uudelleen. (Maone 2010.)

NoScript-lisäosa sisältää myös Cross-site scripting (XSS) -suodattimen. Se tarkistaa jo kertaalleen hyväksytyt toimialueet ja niiden ajamat ohjelmakoodit siltä varalta, että jokin kolmas osapuoli yrittää ajaa niiden sisään omaa ohjelmakoodiaan. Mikäli tällainen hyökkäysyritys löytyy, NoScript suodattaa vihamielisen ohjelmakoodin ja ilmoittaa tästä käyttäjälle. XSS-suodatin on NoScriptissä oletuksena käytössä. (Maone 2010.)

Mozilla Security Bug Bounty Program

Jo Firefoxin julkaisuvuodesta 2004 lähtien Mozilla-säätiö on ylläpitänyt erityistä Bug Bounty -ohjelmaa, jolla halutaan rohkaista kehittäjiä ja muita tietoturvasta kiinnostuneita etsimään haavoittuvuuksia Firefoxin lähdekoodista. Jokaista kriittisen tai korkean tason haavoittuvuutta kohden, joka pystytään toistamaan Firefoxin uusimmassa versiossa ja jota ei vielä ole raportoitu, on löytäjälle luvassa 3000 dollarin palkkio. Palkkio ei koske Mozilla-säätiön työntekijöitä eikä sen koodin kirjoittajia, josta haavoittuvuus on löytynyt, joten ohjelma on tehokas tapa saada Firefoxista tietoturvallisempi selain ulkopuolisella työpanoksella. (Mozilla a.)

Tietoturva-aukkojen julkinen listaus

Mozilla-säätiö pyrkii Firefoxin kehityksessä avoimuuteen myös tietoturvaan liittyvissä asioissa. Tästä hyvä esimerkki on Mozilla-tuotteista löydettyjen ja jo korjattujen tietoturva-aukkojen julkinen listaus Mozillan web-sivustolla. Jokaisesta tietoturva-aukosta on ilmoitettu sen kriittisyystaso, mistä tuotteesta aukko on löydetty, missä versiossa aukko on korjattu, sekä kuvaus tietoturva-aukosta ja sen aiheuttamista haavoittuvuuksista. (Mozilla d.)

3.3 Google Chrome 8.0

Google Chrome on Googlen kehittämä selain, joka perustuu avoimen lähdekoodin Chromium-projektiin. Chromen lähdekoodi on avointa BSD-lisenssillä, joka mahdollistaa koodin hyödyntämisen edelleen sekä avoimen että suljetun lähdekoodin ohjelmistoissa. (Paul 2008.) Net Applicationsin (2010) mukaan Google Chrome on maailman kolmanneksi käytetyin selain 9,98 % markkinaosuudella (joulukuu 2010).

3.3.1 Tietoturvaominaisuudet

Sandbox

Google Chromen arkkitehtuuri jakaa selaimen komponentit karkeasti kahteen osaan: selaimen ohjelmaytimeen eli kerneliin, sekä renderointimoottoriin. Kernelin tehtävänä on hallinnoida selaimen pysyvää tietoa, kuten evästeitä ja salasanatietokantaa, ajaa renderointimoottorin eri instansseja sekä keskustella käyttöjärjestelmän kanssa. Renderointimoottorin, joka sisältää muun muassa HTML-parserin, JavaScript-moottorin sekä Document Object Model -ohjelmarajapinnan, tehtäväksi jää varsinaisten websivustojen esittäminen käyttäjälle. Google Chromen keskeisin tietoturvaominaisuus on renderointimoottorin ajaminen ”hiekkalaatikossa”, Sandboxissa. (Barth, Jackson, Reis & Google Chrome Team, 1-4.)

Sandboxin tarkoituksena on estää renderointimoottorin suora kommunikointi muun järjestelmän kanssa ja pakottaa se käyttämään kernelin rajapintaa, joka jakaa rendoroin-

timoottorille tarvittavat – mahdollisimman suppeat – oikeudet käyttöjärjestelmän kanssa kommunikointiin. Rendorointimoottorilla ei esimerkiksi ole mitään oikeuksia päätelaitteen tiedostojärjestelmään ja jopa käyttäjälle esitettävät web-sivut kierrätetään kernelin rajapinnan kautta. (Barth ym., 5.)

Tällä hetkellä Sandbox toimii Windows-käyttöjärjestelmän ominaisuuksiin perustuen. Sandboxin sisällä oleva renderointimoottori ei käytä käyttäjän Windows-turvatokenia, vaan erillistä, erittäin rajoitettua turvatokenia. Aina kun renderointimoottori yrittää päästä käsiksi järjestelmän tietoihin, Windowsin Security Manager tarkistaa onko renderointimoottorin turvatokenilla tarvittavia oikeuksia päästä sen pyytämiin tietoihin käsiksi. Sandbox rajoittaa moottorin turvatokenin oikeudet siten, että Security Managerin tarkistus ei mene läpi ja renderointimoottorin itse tekemät pyynnöt hylätään lähes aina. (Barth ym., 5.)

Cross-site scripting -suodatin

Cross-site scripting -hyökkäyksiä vastaan Google Chromessa on jo versiosta 4.0 alkaen ollut Cross-site scripting (XSS) -suodatin. XSS-suodatin tarkkailee URL-kenttää ja sivustojen välillä liikkuvia HTTP POST -sanomia vihamielisen JavaScript-koodin varalta. Mikäli sanoma sisältää JavaScript-koodia, suodatin tarkistaa sen ja etsii eräänlaista ”heijastusta”; tietoa joka lähetettäisiin takaisin mahdolliselle kolmannen osapuolen hyökkäyssivustolle, mikäli sanoman sallittaisiin kulkea vapaasti selaimen läpi. Mikäli sanoma tunnistetaan mahdolliseksi hyökkäysyritykseksi, XSS-suodatin puhdistaa alkuperäisen sanoman siten, ettei hyökkäyssivuston lisäämää JavaScript-koodia suoriteta. Chromen XSS-suodatin toimii samalla periaatteella kuin Internet Explorerin vastaava, mutta Chromessa suodatin on integroitu suoraan selaimen renderointimoottoriin, joten se on aina käytössä. (Barth 2010.)

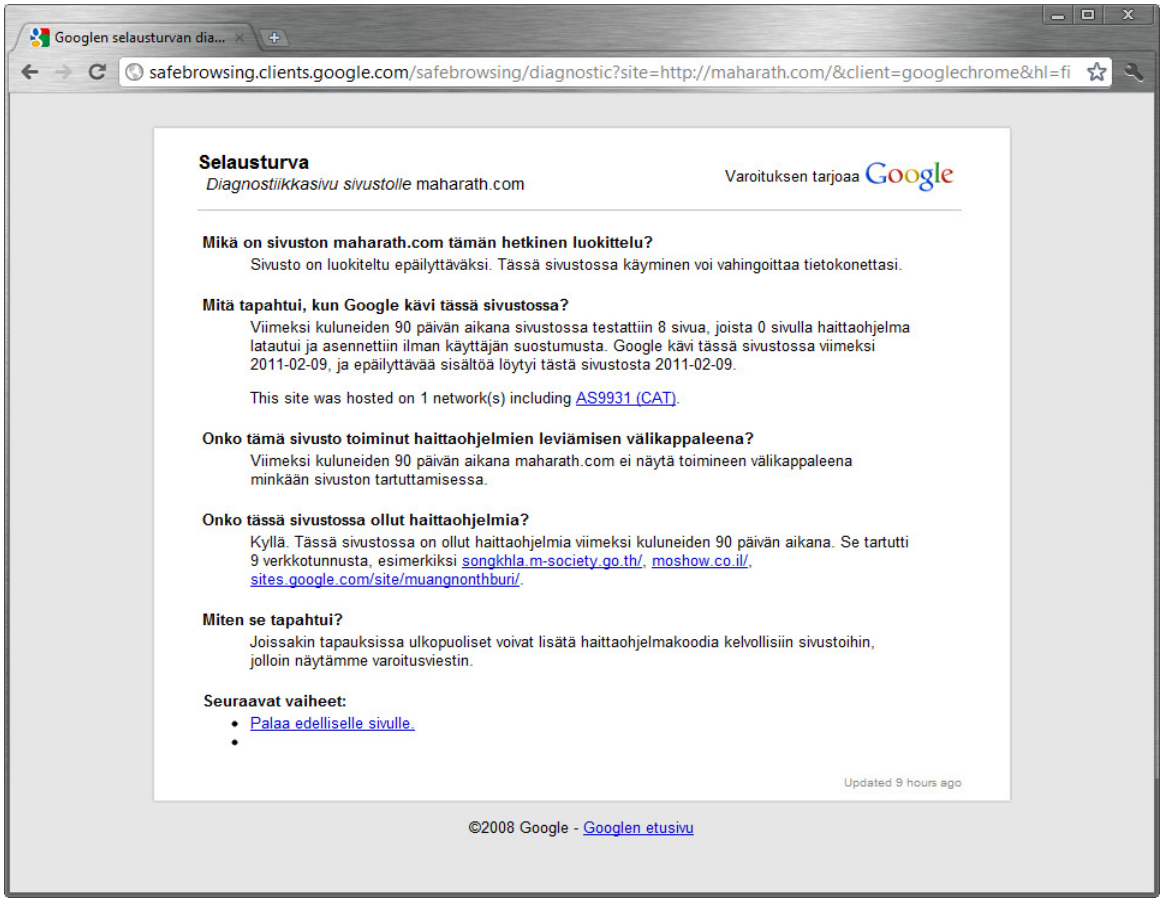
Incognito-tila

Kilpailevien selainten tapaan myös Google Chromesta löytyy erillinen tila yksityiseen selailuun, jonka aikana käyttäjän selausistunnosta ei tallennu tietoja selaimen arkistoi-

hin. Incognito-tilan ollessa käytössä muun muassa sivuhistoriaa, evästeitä ja käyttäjän tekemiä hakuja ei tallenneta, mutta kirjanmerkit ja selainasetuksiin tehdyt muutokset tallentuvat normaalisti. Chrome myös ilmoittaa käyttäjälle selkeästi, ettei Incognito-tila tee käyttäjästä näkymätöntä internetissä, vaan esimerkiksi internet-operaattori voi edelleen seurata millä sivuilla käyttäjä on vieraillut. (Google b.)

Google Safe Browsing

Tietojenkalastelua ja haittaohjelmia levittäviä sivustoja vastaan Chromessa käytetään Googlen itse kehittämää Safe Browsing -palvelua, joka on estolista tunnetuista hyökkäyssivustoista. Samaa palvelua käytetään myös Mozilla Firefoxissa, ja se on esitelty tarkemmin luvussa 3.2.2. Google Safe Browsing tarjoaa myös diagnostiikkasivun estetyistä sivustoista, jota on havainnollistettu kuvassa 4.



Kuva 4. Google Safe Browsing -diagnostiikkasivu Google Chromessa.

Plugin-suojaukset

Google Chromen käyttämä Sandbox-tekniikka ei vielä tällä hetkellä ulotu kattamaan kovinkaan monia kolmannen osapuolen liitännäisiä yhteensopivuuden takaamiseksi. Tämä kuitenkin asettaa haasteita tietoturvalle, sillä liitännäiset suoritetaan vapaassa ympäristössä käyttäjän täysillä oikeuksilla. Ongelman todellinen korjaaminen vaatii ohjelmistokehittäjiltä liitännäisten päivittämisen sandbox-yhteensopiviksi. Tällä hetkellä Chromessa ajetaan liitännäisiä, kuten Adoben Flashia ja Readeria, kutakin omassa prosessissaan. Tämä ei estä liitännäisten haavoittuvuuksien hyödyntämistä, mutta lisää selaimen vastustuskykyä sellaisia hyökkäyksiä vastaan, joilla pyritään esimerkiksi kaatamaan käyttäjän koko selain. (Barth ym., 4.)

Adoben Flash-liitännäinen on myös integroitu suoraan Chromen asennuspakettiin, toisin kuin muissa selaimissa. Flash myös päivittyy automaattisesti Chromen oman päivitystyökalun kautta, joten käyttäjien ei itse tarvitse huolehtia Flashin päivityksestä ja vanhojen versioiden tietoturva-aukoista. (Upson 2010.) Flash-liitännäisestä on myös julkaistu ensimmäinen, vielä kehitysasteella oleva sandbox-yhteensopiva versio joulukuussa 2010 (Schuh & Pizano 2010).

3.4 Selainhaavoittuvuudet vuonna 2010

Tutkittavien selainten haavoittuvuustilastot vuoden 2010 ajalta on koottu taulukkoon 2.

	Internet Explorer	**Mozilla Firefox**	**Google Chrome**
Lukumäärä	11	11	20
Kriittisiä	8	10	18
Paikkaamattomia	3	0	0

Taulukko 2. Selainhaavoittuvuudet vuonna 2010 (Secunia a-g 2010).

Vuoden 2010 aikana Internet Explorerista ja Firefoxista löydettiin kummastakin 11 haavoittuvuutta ja Google Chromesta peräti 20 haavoittuvuutta. Chromen kohdalla on huomionarvoista, että vuoden 2010 aikana selaimesta ilmestyi viisi eri versiota: 4.0

(tammikuu), 5.0 (kesäkuu), 6.0 (syyskuu), 7.0 (lokakuu) ja 8.0 (joulukuu). Taulukossa 2 on esitetty kaikkien versioiden haavoittuvuudet yhteenlaskettuna.

Internet Explorerista löydetyistä haavoittuvuuksista neljä on luokiteltu äärimmäisen kriittiseksi, neljä hyvin kriittiseksi, yksi kohtalaisen kriittiseksi sekä kaksi haavoittuvuutta ei ollenkaan kriittiseksi. Näistä kohtalaisen kriittinen haavoittuvuus on edelleen osittain korjaamatta sekä kaksi ei-kriittistä haavoittuvuutta kokonaan korjaamatta. (Secunia a 2010.)

Mozilla Firefoxin haavoittuvuuksista vain yksi on luokiteltu äärimmäisen kriittiseksi, yhdeksän hyvin kriittiseksi, sekä yksi lievästi kriittiseksi. Haavoittuvuuksista kaikki on onnistuttu korjaamaan vuoden 2010 aikana. (Secunia b 2010.)

Google Chromen haavoittuvuuksista kaksi on luokiteltu äärimmäisen kriittiseksi, peräti 16 hyvin kriittiseksi, sekä kaksi haavoittuvuutta lievästi kriittiseksi. Chromen muista poikkeava versionumerointi on aiheuttanut sen, että Chromen versioissa 5-7 raportoidaan olevan kolme korjaamatonta haavoittuvuutta. Google ei julkaise Chromen versioihin juurikaan pienempiä tietoturva- tai muita päivityksiä, vaan uusi merkittävä versio ilmestyy parhaimmillaan muutaman kuukauden välein. Korjaamattomiksi raportoidut kolme haavoittuvuutta on siis korjattu Chromen versioissa 6-8 ja Chromen uusimmassa versiossa ei ole yhtäkään korjaamatonta haavoittuvuutta. (Secunia c-g 2010.)

4 Selainten vertailu ja lopputulokset

Tämän tutkimuksen tavoitteena on selvittää verkon yleisimmät tietoturvauhkat vuonna 2010, sekä tutkia mitkä niistä kohdistuvat selaimiin ja mikä selain tarjoaa parhaimmat edellytykset niitä vastaan suojautumiseen. Tutkimuksen pääongelmana on: mikä on tietoturvallisin selain vuoden 2010 uhkia vastaan? Tähän liittyvät alaongelmat ovat: mitkä ovat vuoden 2010 yleisimmät tietoturvauhkat, mitkä niistä kohdistuvat selaimeen, sekä mikä selain tarjoaa parhaat edellytykset näitä uhkia vastaan suojautumiseen?

Ensimmäisen alaongelman vastaus on esitetty toisessa pääluvussa, jossa selvitettiin että vuoden 2010 yleisimmät tietoturvauhkat ovat botnet-verkot, roskaposti, käyttöjärjestelmähaavoittuvuudet, XSS-hyökkäykset, haittaohjelmat, tietojenkalastelu, plugin-haavoittuvuudet sekä sosiaaliset verkot. Toisen alaongelman vastaus, selainten lopullinen arviointi ja vertailu, sekä tutkimuksen pääongelman ratkaisu käsitellään tässä luvussa.

4.1 Tutkimusmenetelmät

Tutkimuksen ensimmäisen alaongelman tutkimusmenetelmäksi valittiin kirjallisuuskartoitus, joka on käsitelty pääluvussa 2. Kartoituksessa valittiin kahden tunnetun tietoturvayhtiön osavuosittainen katsaus, joiden perusteella tutkimukseen valikoitui kahdeksan yleisintä tietoturvauhkaa vuonna 2010. Katsauksia valittiin vähintään kaksi, jotta niiden väliset mahdolliset näkemyserot yleisimmistä tietoturvauhkista nousisivat esiin. Koska valituissa kahdessa katsauksessa esiintyivät samat tietoturvauhkat erittäin tarkasti, ei useamman katsauksen ottamista tutkimuksen piiriin katsottu tarpeelliseksi. Lisäksi molemmat tietoturvayhtiöt alallaan kokeneita ja arvostettuja, joten valittuja katsauksia ja tätä tutkimusmenetelmää voidaan pitää varsin luotettavana.

Tutkimuksen toista alaongelmaa lähestyttiin yksinkertaisella analyysillä, jossa pääluvussa 2 selvitetyt tietoturvauhkat käytiin yksitellen lävitse ja pohdittiin kohdistuuko kyseinen uhka selaimeen vai johonkin muuhun tietotekniikan osa-alueeseen.

Tutkimuksen kolmas alaongelma ratkaistiin kahdessa osassa. Kun vuoden 2010 yleisimmät tietoturvauhkat olivat selvillä, kirjallisuuskartoituksen avulla selvitettiin, millaisia suojausominaisuuksia tutkittavista selaimista löytyy. Tämä on käsitelty pääluvussa 3. Ominaisuuksien selvityksen jälkeen suoritettiin suoraviivaiseen pisteytykseen perustuva vertailu selainten kesken.

Vertailussa painopiste oli selainten kyvyllä suojautua toisessa pääluvussa selvitettyjä, selaimeen kohdistuvia tietoturvauhkia vastaan. Jokaisesta kutakin uhkaa vastaan suojaavasta ominaisuudesta/ominaisuuksista selain ansaitsi yhden pisteen. Mikäli selain ei tarjoa jotakin uhkaa vastaan lainkaan suojaa, oli tuloksena nolla pistettä. Miinuspisteiden antaminen ei ollut tässä tutkimuksessa tarkoituksenmukaista, sillä selain on vain yksi osa laajempaa suojausketjua. Koska keskeisimpien tietoturvauhkien lähteinä käytetyissä tietoturvaraporteissa ei ole laitettu uhkia erityiseen tärkeysjärjestykseen, ei sitä tehty myöskään tässä tutkimuksessa. Mikään uhka ei siis saanut erityistä painoarvoa.

Koska selainten vertailu perustuu teoriaan, eikä esimerkiksi käytännön testeihin, on toiseksi vertailunäkökulmaksi valittu selaimissa vuoden 2010 aikana esiintyneet haavoittuvuudet ja niihin julkaistut korjaukset. Lukuun 3.4 koottiin tunnetun tietoturvayhtiön tilastojen perusteella selvitys siitä, paljonko ja minkä luokituksen haavoittuvuuksia vertailtavissa selaimissa on vuoden 2010 aikana esiintynyt, sekä onko selainvalmistaja onnistunut julkaisemaan haavoittuvuuksiin korjauksen. Haavoittuvuustilastojen pohjalta selaimille ei jaettu pisteitä tai muitakaan arvosanoja, vaan niitä käytettiin vain lisänäkökulmana selainten vertailussa ja tutkimuksen johtopäätöksissä.

Tarkasteltavat haavoittuvuustilastot valittiin vuoden 2010 ajalta siitä syystä, että ne sopisivat mahdollisimman hyvin yhteen selvitettyjen yleisimpien tietoturvauhkien kanssa, jossa tarkastelujaksona oli myös vuosi 2010. Tutkimuksen luonne haluttiin muutenkin pitää mahdollisimman ajankohtaisena. Haavoittuvuustilastoja olisi toki voinut tarkastella useamman vuoden ajalta tai verrata eri vuoden tilastoja keskenään, mutta Google Chromen verrattain nuoren iän vuoksi tämän olisi katsottu suosivan liikaa markkinoilla pidempään toimineita vertailukumppaneita.

4.2 Tietoturvauhkien analysointi

Tässä luvussa selvitetään pääluvussa 2 käsitellyistä uhkista ne uhkat, jotka kohdistuvat ensisijaisesti selaimeen ja siten kuuluvat tämän tutkimuksen piiriin.

Botnet-verkot

Botnet-verkkoja käytetään pääasiassa tietoliikenteen häiritsemiseen, muun muassa palvelunestohyökkäyksiin, sekä roskapostin massalähetykseen. Botnet-verkkoja käytetään paljon myös verkkopalvelujen salasanojen murtamiseen. Vaikka botnet-verkot välillisesti liittyvätkin selaimiin roskaposteissa levitettävien haittaohjelmien muodossa, ei niitä voida pitää ensisijaisesti selaimeen kohdistuvana uhkana.

Cross-site scripting (XSS)

XSS-hyökkäykset ovat web-palvelimien haavoittuvuuksia hyödyntäviä hyökkäyksiä, joiden tarkoituksena on ohjata käyttäjä esimerkiksi hyökkääjän väärentämälle vihamieliselle verkkosivulle. Näin ollen XSS-hyökkäykset ovat web-palvelimien kautta selaimeen kohdistuva uhka.

Roskaposti

Roskaposti on sähköpostilla tapahtuvaa haitallista massapostitusta, johon ei ole vastaanottajan lupaa. Vaikka roskapostien sisältämät haitalliset linkit kohdistuvatkin selaimeen, on niiden torjunta pääasiassa sähköpostisovellusten ja virustorjuntaohjelmistojen vastuulla. Roskapostia ei siis voida pitää ensisijaisesti selaimeen kohdistuvana uhkana.

Haittaohjelmat (Malware)

Haittaohjelma on yleisnimitys joukolle tietokoneohjelmia, joiden tavoitteena on aiheuttaa ei-toivottuja tapahtumia tietojärjestelmissä tai käyttäjien tietokoneissa. Aiemmin haittaohjelmat levisivät lähinnä sähköpostin liitetiedostoina tai levykkeillä, mutta nyt-

temmin niiden leviämiskeinot ovat laajentuneet muun muassa verkkosivuille, sosiaalisiin verkkoihin ja muihin selaimella käytettäviin järjestelmiin. Haittaohjelmia voidaan siis nykyään pitää selaimeen kohdistuvana uhkana.

Tietojenkalastelu (phishing)

Tietojenkalastelu on rikollista toimintaa, jolla pyritään saamaan käyttäjä luovuttamaan henkilökohtaisia tietojaan, kuten käyttäjätunnuksia tai henkilö- ja tilitietoja. Kalastelu tapahtuu useimmiten pikaviestimissä ja sähköpostiviestien muodossa, mutta on siirtynyt myös väärennetyille verkkosivuille ja sosiaalisiin verkkoihin, joten sen voidaan katsoa olevan selaimeen kohdistuva uhka.

Käyttöjärjestelmähaavoittuvuudet

Käyttöjärjestelmähaavoittuvuudet ovat käyttöjärjestelmistä löytyviä ohjelmointivirheitä, joita hyödyntämällä verkkorikolliset saavat pahimmillaan koko järjestelmän hallintaansa. Vaikka haavoittuvuuksia hyödynnetäänkin selaimen kautta leviävillä haittaohjelmilla, on niiden torjunta käyttöjärjestelmän valmistajan vastuulla, joten kyseessä ei ole selaimeen kohdistuva uhka.

Plugin-haavoittuvuudet

Plugin-haavoittuvuudet ovat selainliitännäisistä löytyviä haavoittuvuuksia, joita hyödyntämällä verkkorikolliset voivat suorittaa järjestelmässä eriasteisia toimintoja, pahimmillaan ottamaan koko järjestelmän hallintaansa. Selainliitännäiset ovat selaimeen asennettavia komponentteja, joten kyseessä on selaimeen kohdistuva uhka.

Sosiaaliset verkot

Sosiaaliset verkot eivät niinkään ole uhka itsessään, vaan ne toimivat alustana muille tietoturvauhkille. Sosiaalisille verkoille räätälöidyt versiot haittaohjelmista ja tietojenka-

lastelusta ovat yleistyneet kovaa vauhtia. Koska sosiaalisia verkkoja käytetään selaimella, on kyseessä ensisijaisesti selaimeen kohdistuva uhka.

Selaimeen kohdistuvat vuoden 2010 yleisimmät tietoturvauhkat ovat siis

- XSS-hyökkäykset
- haittaohjelmat
- tietojenkalastelu
- plugin-haavoittuvuudet
- sosiaaliset verkot.

4.3 Internet Explorer 8

Cross-site scripting (XSS)

XSS-hyökkäyksiä vastaan Internet Explorer 8:sta löytyy XSS-suodatin, joka tarkkailee selaimessa liikkuvia sanomia mahdollisen vihamielisen ohjelmakoodin varalta. XSS-suodatin on Internet Explorerissa oletuksena päällä, joten käyttäjän ei itse tarvitse huolehtia sen käynnistämisestä. Huomionarvoista on lisäksi se, että XSS-suodatin on päällä myös selaimen heikoimmalla suojaustasolla, ja sen kytkeminen pois päältä vaatii käyttäjältä suojauksen lisäasetusten muokkaamista.

XSS-suodattimesta Internet Explorer ansaitsee vertailussa yhden pisteen.

Haittaohjelmat (Malware)

Malwaren ollessa ylivoimaisesti laajin tietoturvauhka, on varsin luontevaa että sitä vastaan on selaimessa enemmän kuin yksi suojauskeino. Internet Explorerissa keinoja on tällä hetkellä kolme.

Tärkein niistä on Protected Mode, joka tosin teknisten rajoitusten vuoksi ei toimi Windows XP:ssä, vaan ainoastaan Windows Vistassa ja 7:ssä. Protected Mode estää selain-

prosessin pääsyn tärkeisiin käyttöjärjestelmätiedostoihin ja muun muassa käyttäjän omiin tiedostoihin, joten malwaren saastuttama selain ei pääse aiheuttamaan suurta vahinkoa. Protected Mode on Internet Explorerissa oletuksena päällä kaikilla suojaustasoilla.

Toinen malwarea vastaan suojaava ominaisuus on SmartScreen-suodattimen tiedostotarkistus. SmartScreen-suodatin tarkistaa selaimella ladattavat tiedostot estolistaa vasten ja estää latauksen, mikäli tiedosto on peräisin tunnetulta malwarea levittävältä sivustolta. SmartScreen-suodatin on oletuksena päällä kaikilla suojaustasoilla.

Kolmas Internet Explorerin malware-suojaus on Attachment Execution Service -palvelu, joka tarkistaa selaimella ladattavat tiedostot ja vaatii käyttäjältä latausvahvistuksen, mikäli tiedosto saattaa sisältää malwarea. AES-palvelu pyrkii antamaan käyttäjälle mahdollisimman paljon informaatiota ladattavasta tiedostosta. AES on Windows-käyttöjärjestelmän ominaisuus, joten se on Internet Explorerissa aina käytössä, eikä sitä saa pois päältä.

Koska Internet Explorerin kaikki malware-suojausominaisuudet ovat oletuksena käytössä, ansaitsee se niistä vertailussa yhden pisteen.

Tietojenkalastelu (phishing)

Tietojenkalastelua vastaan Internet Explorerissa on kaksi suojausta. Malwarea vastaan suojaavaa SmartScreen-suodatinta käytetään myös tietojenkalastelusivustojen tunnistamisessa. Toinen suojaus on InPrivate-tila ja erityisesti InPrivate-suodatus, joista ensiksi mainittu ei tallenna käyttäjän selausistunnosta mitään tietoja ja jälkimmäinen tarkkailee eri sivustojen asettamia evästeitä ja estää tietojenkalasteluksi tulkittavat seurantaevästeet. Tietojenkalastelusuojauksista SmartScreen-suodatin on oletuksena päällä kaikilla suojaustasoilla, mutta InPrivate-tila ja -suodatus on käynnistettävä manuaalisesti joka istunnon alussa.

Koska InPrivaten kaltaiset yksityiset selaustilat toimivat kaikissa selaimissa samalla, manuaalisesti käynnistettävällä tavalla, ei siitä tässä tutkimuksessa rangaista, vaan Internet Explorer ansaitsee tietojenkalastelusuojauksistaan vertailussa yhden pisteen.

Plugin-haavoittuvuudet

Plugin-haavoittuvuuksia vastaan Internet Explorer 8 ei tarjoa suojauksia tai muitakaan ominaisuuksia, joten tällä osa-alueella se ei ansaitse vertailussa pisteitä.

Sosiaaliset verkot

Sosiaalisten verkkojen tapauksessa suojausominaisuudet eivät ole aivan yksiselitteisiä, sillä sosiaalisilta verkoilta itseltään ei tarvitse suojautua, vaan ne toimivat lähinnä alustoina muille tietoturvauhkille, erityisesti tietojenkalastelulle, malwarelle ja XSS-hyökkäyksille. Kuten edellä on jo kuvattu, löytyy Internet Explorerista oletuksena käytössä olevat suojaukset kaikkia näitä uhkia vastaan, joten sosiaalisten verkkojen osa-alueelta se ansaitsee yhden pisteen.

4.4 Mozilla Firefox 3.6

Cross-site scripting (XSS)

XSS-hyökkäyksiä vastaan Mozilla Firefox ei sisällä sisäänrakennettua suodatinta tai muita suojauksia, mutta ladattavalla NoScript-lisäosalla selaimeen saa tehokkaan ohjelmakoodi- ja XSS-suodattimen. NoScriptin käyttöönotto vaatii kuitenkin käyttäjän toimia ja hieman konfigurointia.

Koska Firefox ei oletuksena sisällä XSS-suojausta, mutta se on mahdollista toteuttaa lisäosalla, ansaitsee selain tältä osa-alueelta puoli pistettä.

Haittaohjelmat (Malware)

Malware-hyökkäyssivustoja vastaan Mozilla Firefoxissa on sisäänrakennettu suodatin, joka hyödyntää Googlen ylläpitämää Safe Browsing -estolistaa, jota vasten sivustot tarkistetaan. Suodatin on selaimessa oletuksena käytössä, joten Firefox ansaitsee tältä osa-alueelta yhden pisteen.

Tietojenkalastelu (phishing)

Tietojenkalastelua vastaan Mozilla Firefox käyttää samaa suojausta kuin malwareakin vastaan, eli Google Safe Browsing -estolistaa hyödyntävää suodatinta, joka on selaimessa oletuksena käytössä. Lisäksi seurantaevästeiden kaltaiselta tietojenkalastelulta voi Firefoxissa suojautua yksityisellä selaustilalla nimeltään Private Browsing, joka ei tallenna selausistunnon tietoja muistiin. Firefoxissa yksityinen selaustila pitää muiden selainten tapaan käynnistää manuaalisesti istunnon alussa.

Tietojenkalastelusuojauksistaan Mozilla Firefox ansaitsee vertailussa yhden pisteen.

Plugin-haavoittuvuudet

Plugin-haavoittuvuuksia vastaan Mozilla Firefox ei tarjoa suojauksia tai muitakaan ominaisuuksia, joten tällä osa-alueella se ei ansaitse vertailussa pisteitä.

Sosiaaliset verkot

Sosiaalisten verkkojen tapauksessa suojausominaisuudet eivät ole aivan yksiselitteisiä, sillä sosiaalisilta verkoilta itseltään ei tarvitse suojautua, vaan ne toimivat lähinnä alustoina muille tietoturvauhkille, erityisesti tietojenkalastelulle, malwarelle ja XSS-hyökkäyksille. Mozilla Firefoxista löytyy oletuksena käytössä olevat suojaukset malwarea ja tietojenkalastelua vastaan, mutta ei sisäänrakennettua XSS-suojausta. Osittain puutteellisten suojausten takia Firefox ansaitsee tältä osa-alueelta vain puoli pistettä.

4.5 Google Chrome 8.0

Cross-site scripting (XSS)

XSS-hyökkäyksiä vastaan Google Chromessa on XSS-suodatin, joka tarkkailee selaimessa liikkuvia sanomia mahdollisen vihamielisen ohjelmakoodin varalta. XSS-suodatin on Google Chromessa sisäänrakennettu suoraan renderointimoottoriin, joten se on oletuksena käytössä, eikä sitä saa selaimen asetuksista muutettua.

XSS-suodattimesta Google Chrome ansaitsee vertailussa yhden pisteen.

Haittaohjelmat (Malware)

Malware-hyökkäyssivustoilta suojautumiseen Chromessa on sisäänrakennettu suodatin, joka hyödyntää Googlen itse ylläpitämää Safe Browsing -estolistaa, jota vasten sivustot tarkistetaan. Suodatin on selaimessa oletuksena käytössä, joten Chrome ansaitsee tältä osa-alueelta yhden pisteen.

Tietojenkalastelu (phishing)

Myös tietojenkalastelua vastaan Chrome käyttää Google Safe Browsing -estolistaa hyödyntävää suodatinta, joka on selaimessa oletuksena käytössä. Lisäksi seurantaevästeiden kaltaiselta tietojenkalastelulta voi Chromessa suojautua muistakin selaimista löytyvällä yksityisellä selaustilalla nimeltään Incognito, joka ei tallenna selausistunnon tietoja muistiin. Chromessa yksityinen selaustila pitää muiden selainten tapaan käynnistää manuaalisesti istunnon alussa.

Tietojenkalastelusuojauksistaan Google Chrome ansaitsee vertailussa yhden pisteen.

Plugin-haavoittuvuudet

Myös plugin-haavoittuvuuksiin on Google Chromessa kiinnitetty muista selaimista poiketen huomiota. Kaikkia kolmannen osapuolen liitännäisiä ei vielä pystytä ajamaan

Chromen sandbox-tekniikan sisällä, mutta tällä hetkellä liitännäisiä ajetaan omissa prosesseissaan, joka lisää hieman selaimen vastustuskykyä niissä esiintyviä haavoittuvuuksia vastaan. Chromen asennuspakettiin on myös integroitu sandboxin sisällä toimiva PDF-lukija sekä Adoben Flash-liitännäinen, joka päivittyy normaalisti Chromen mukana. Chrome myös varoittaa liian vanhoista liitännäisistä ja poistaa ne käytöstä, mikäli niissä on tiedossa olevia haavoittuvuuksia.

Plugin-haavoittuvuuksien suojausominaisuuksistaan Google Chrome ansaitsee ainoana selaimena yhden pisteen.

Sosiaaliset verkot

Sosiaalisten verkkojen tapauksessa suojausominaisuudet eivät ole aivan yksiselitteisiä, sillä sosiaalisilta verkoilta itseltään ei tarvitse suojautua, vaan ne toimivat lähinnä alustoina muille tietoturvauhkille, erityisesti tietojenkalastelulle, malwarelle ja XSS-hyökkäyksille. Google Chromessa on oletuksena käytössä olevat suojaukset kaikkia näitä uhkia vastaan, joten sosiaalisten verkkojen osa-alueelta se ansaitsee yhden pisteen.

4.6 Loppuvertailu

Luvun 4.5 vertailussa selainten ansaitsemat pisteet on koottu taulukkoon 3.

	Cross-site scripting	Malware	Tietojen-kalastelu	Plugin-haavoittuvuudet	Sosiaaliset verkot	**Yhteensä**
Internet Explorer	1	1	1	0	1	**4**
Mozilla Firefox	0,5	1	1	0	0,5	**3**
Google Chrome	1	1	1	1	1	**5**

Taulukko 3. Selainten vertailussa ansaitsemat pisteet.

Vertailun tulokset ovat osin yllättäviä. Internet Explorer, jota on jo kauan julkisuudessa parjattu huonosta tietoturvan tasosta, suoriutuu ainakin tietoturvaominaisuuksiensa valossa hyvin. Vaikuttaakin siltä, että Internet Explorer kärsii jossakin määrin menneisyyden painolastista, sillä kilpailevien selainten aiheuttamat paineet ovat selvästi saaneet Microsoftin panostamaan enemmän tietoturvaan Internet Explorerin uusimmissa versioissa. Internet Explorerin suojausominaisuuksia voidaan pitää lähes erittäin hyvinä,

sillä se tarjoaa suojauksen plugin-haavoittuvuuksia lukuun ottamatta kaikkia yleisimpiä selaimen tietoturvauhkia vastaan. Plugin-suojausten puutettakaan ei voida pitää kovin vakavana seikkana, sillä vastuu niistä on ensisijaisesti liitännäisten kehittäjillä.

Yllättävää oli myös julkisuudessa turvallisena pidetyn Mozilla Firefoxin tietoturvaominaisuuksien osoittautuminen vertailun heikoimmiksi. XSS-suodattimen ja ClickJacking-suojauksen puute laskee Firefoxin arvosanaa, mutta suojaukset ovat kuitenkin toteutettavissa selaimeen asennettavien lisäosien avulla. Mikäli Firefoxissa olisi esimerkiksi NoScript-lisäosan kaltaiset ominaisuudet oletuksena, olisi se tietoturvaominaisuuksiltaan tasoissa Internet Explorerin kanssa. Tällaisenaan Mozilla Firefoxia voi pitää ominaisuuksiltaan hyvin turvallisena selaimena vain kokeneemmille käyttäjille, jotka hallitsevat lisäosien asennuksen ja niiden konfiguroinnin.

Googlen Chrome-selain on tietoturvaominaisuuksiltaan omassa luokassaan, sillä se tarjoaa oletuksena suojan kaikkia tutkimuksessa selvitettyjä tietoturvauhkia vastaan. Chromen tiivis kehitystahti ja keskittyminen tietoturvaan ovat antaneet Googlelle etulyöntiaseman kilpailijoihin nähden. Chromen kaikki tietoturvaominaisuudet ovat myös oletuksena käytössä, joten sitä voi pitää tietoturvaominaisuuksiensa puolesta vertailun parhaana selaimena kaikille käyttäjille.

Vaikka vertailtavien selainten välille syntyikin selviä piste-eroja, ei yhdenkään ominaisuuksia voida pitää tietoturvan osalta riittämättömänä. Selain on vain yksi osatekijä, joka muiden tietoturvatuotteiden ja käyttäjän kanssa muodostaa toimivan kokonaisuuden. Vertailun kaikki selaimet sisältävät vähintään kohtuulliset tietoturvaominaisuudet, joten ne kaikki ovat riittäviä toimimaan osana tietoturvaketjua ilman, että niistä muodostuu heikoin lenkki. Google Chrome ja Internet Explorer vain hoitavat tehtävänsä hieman Firefoxia paremmin.

Mozilla Firefoxin ja Internet Explorerin väliset voimasuhteet tasoittuvat jonkin verran, kun tarkastellaan luvussa 3.4 esitettyjä selainten haavoittuvuustilastoja. Internet Explorerista vuonna 2010 löydetyistä haavoittuvuuksista kaikki äärimmäisen kriittiset ja hyvin kriittiset on korjattu selainpäivityksillä, mutta löydetty kohtalaisen kriittinen haavoittu-

vuus on korjattu päivityksellä vain osittain. Lisäksi molemmat ei-kriittiset haavoittuvuudet ovat edelleen korjaamatta. Internet Explorerin haavoittuvuustilastot jättävät kokonaisuudessaan siis hieman toivomisen varaa.

Mozilla Firefoxin vuoden 2010 haavoittuvuustilastot näyttävät huolestuttavilta, sillä yli 90 prosenttia löydetyistä haavoittuvuuksista on vähintään hyvin kriittisiä. Tämä kuvastaa osaltaan sitä, että maailman toiseksi käytetyimpänä selaimena Firefox kiinnostaa selainta analysoivia verkkorikollisia ja tietoturva-asiantuntijoita jo siinä missä käytetyin Internet Explorerkin. Haavoittuvuuksien korjaamisessa Mozilla on kuitenkin kunnostautunut avoimen kehitysyhteisönsä ansiosta erinomaisesti, sillä kaikki vuoden 2010 haavoittuvuudet on korjattu päivityksillä.

Google Chromen haavoittuvuustilastot näyttävät melko huolestuttavilta, sillä löydettyjä haavoittuvuuksia on huomattavasti enemmän kuin kilpailijoilla. Tämä selittyy selaimen nuorella iällä ja sen kiinnostavuudella. Nuorena selaimena Chrome elää jatkuvaa muutosaikaa, kun olemassa olevia ominaisuuksia muokataan ja uusia lisätään. Uudet ominaisuudet tuovat mukanaan uusia haavoittuvuuksia. Toisaalta Chromen räjähdysmäisesti kasvanut suosio kiinnostaa myös verkkorikollisia, joten selaimen analysointiin käytetään enemmän resursseja.

Avoimen kehitysyhteisönsä ansiosta Google Chromen suoritusta haavoittuvuuksien korjaamisessa voidaan haavoittuvuuksien suuresta määrästä huolimatta pitää kiitettävänä, sillä selaimen kaikki 20 haavoittuvuutta on korjattu päivityksillä.

5 Yhteenveto ja johtopäätökset

Tässä tutkimuksessa selvitettiin verkon yleisimmät tietoturvauhkat vuonna 2010, tutkittiin mitkä uhkista kohdistuvat selaimeen ja mikä selain tarjoaa parhaat edellytykset näitä uhkia vastaan suojautumiseen. Tutkittavat selaimet olivat Windows Internet Explorer, Mozilla Firefox sekä Google Chrome.

Tutkimuksessa selvisi, että julkisuudessa toisinaan kiivastakin kritiikkiä saanutta Internet Exploreria voidaan ainakin tietoturvaominaisuuksiensa osalta pitää nykyään hyvänä, sillä selaimesta löytyy suojaukset lähes kaikkia yleisimpiä tietoturvauhkia vastaan. Suurin osa ominaisuuksista on myös oletuksena käytössä, joten Internet Explorer on tietoturvallinen selain myös tietoturvaan perehtymättömälle käyttäjälle.

Haavoittuvuuksien korjaamisessa Internet Explorer jätti kuitenkin toivomisen varaa, sillä selaimen uusimmassa versiossa on vuoden 2010 aikana löydetyistä haavoittuvuuksista osittain korjaamatta yksi ja kokonaan korjaamatta kaksi haavoittuvuutta. Kokonaan korjaamattomat haavoittuvuudet eivät ole kriittisiä, mutta tapaus osoittaa silti, ettei Microsoft ota selaimensa tietoturvaa aivan sataprosenttisen vakavasti. Pahimpien kilpailijoiden nollatoleranssin rinnalla Internet Explorerin paikkaamattomat haavoittuvuudet näyttävät entistä huonommalta.

Mozilla Firefoxin tulokset vertailussa olivat osin yllättäviä, sillä selaimesta puuttuu muutama kilpailevista selaimista löytyvä tietoturvaominaisuus. Puutteet eivät ole kriittisiä, sillä ne on mahdollista lisätä selaimeen pätevien kolmansien osapuolien lisäosien avulla, mutta tämä vaatii käyttäjältä hieman normaalia enemmän tietoteknistä osaamista. Oletusasetuksillaan Mozilla Firefox ei siis ole tietoturvaominaisuuksiensa osalta peruskäyttäjälle kaikkein ihanteellisin selain.

Minkä Firefox menettää tietoturvaominaisuuksissa, se korvaa haavoittuvuuksiensa korjaamisella. Mozilla on korjannut kaikki selaimestaan vuonna 2010 löydetyt haavoittuvuudet, myös vähemmän kriittiset. Suoritusta voidaan pitää erittäin kiitettävänä, varsinkin Internet Explorerin tuloksiin verrattuna.

Google Chromen tulokset olivat vertailussa omaa luokkaansa, sillä selaimesta löytyy tietoturvaominaisuudet kaikkia yleisimpiä tietoturvauhkia vastaan. Ominaisuudet ovat myös yhtä lukuun ottamatta oletuksena käytössä, joten käyttäjän ei tarvitse erikseen huolehtia selaimen tietoturva-asetuksista.

Googlen panostaminen tietoturvaan näkyy myös Chromen haavoittuvuuksien korjaamisessa. Chromesta on vuoden 2010 aikana löydetty kilpailijoita huomattavasti enemmän haavoittuvuuksia, mutta tämä selittyy selaimen nuorella iällä, uusien ominaisuuksien lisääntymisellä ja sen suosion kasvulla. Vaikka haavoittuvuuksia on löydetty todella paljon, on ne kaikki myös onnistuttu vuoden 2010 aikana korjaamaan.

Selaimia ja varsinkin niiden haavoittuvuustilastoja vertaillessa huomio kiinnittyi vahvasti suljetun ja avoimen lähdekoodin vaikutukseen selainten kehityksessä. Vaikka Microsoftin kaltainen IT-jättiläinen panostaa varmasti Internet Explorerin kehitykseen rahaa ja henkilötyövuosia kilpailijoitaan enemmän, tulee se todennäköisesti vielä olemaan suurissa vaikeuksissa avoimen lähdekoodin Firefoxin ja Chromen kanssa. Avoin kehitysyhteisö mahdollistaa suljetun ympäristön jähmeää hierarkiaa joustavamman ja nopeamman kehityksen. Lisäksi avoimen yhteisön etuja on avoimuus myös tietoturva-asioissa, josta hyvä esimerkki on Mozillan ja Googlen myöntämät rahapalkinnot henkilöille, jotka onnistuvat löytämään kehittäjien selaimista kriittisiä haavoittuvuuksia. Tämänkaltaiset erot kehitysfilosofioissa ovat mahdollisia syitä siihen, miksi Internet Explorerissa on paikkaamattomia haavoittuvuuksia, mutta Firefoxissa tai Chromessa ei lainkaan.

Tutkimuksen tulosten perusteella voidaan siis todeta, että tutkimuksessa käytettyjen rajausten puitteissa Googlen nuori Chrome-selain tarjoaa kattavimmat ominaisuudet hyvän tietoturvan tarjoamiseen sekä haavoittuvuuksien ripeän korjaamisen. Internet Explorerin tulosta jarruttaa kilpailijoita heikompi haavoittuvuuksien korjaaminen, ja Mozilla Firefoxia puolestaan muita hieman puutteellisemmat tietoturvaominaisuudet.

Mitä tämä kaikki sitten tarkoittaa? Voiko esimerkiksi Google Chromea käyttämällä olla turvassa kaikelta vihamieliseltä toiminnalta verkossa? Vastaus on yksiselitteinen ei. Tie-

tokoneen onnistuneen tietoturvan tie on pitkä ja kivikkoinen, ja tämä ketju on ainoastaan yhtä vahva kuin sen heikoin lenkki. Selaimessa haitallisen linkin klikkaamisen ja tietokoneen saastumisen välillä on monta estettä, joita selaimen lisäksi ovat muun muassa web-palvelimen paikatut haavoittuvuudet, käyttöjärjestelmän päivitykset, liitännäisten päivitykset, palomuuri, virustorjuntaohjelmisto sekä tietysti itse käyttäjä. Ihannetilanteessa käyttäjä voisi huoletta klikata vihamielistä linkkiä ja järjestelmän tietoturvan eri osa-alueet pitäisivät huolen siitä, ettei mitään haitallista pääse järjestelmässä tapahtumaan.

Todellisuus on kuitenkin kaukana ihannetilanteesta, sillä tietoturvaketjun heikoimmaksi lenkiksi nousee hieman yllättäen käyttäjä, mutta ei kokonaan tämän omasta syystä. On totta, että käyttäjät saattavat enempiä miettimättä luovuttaa käyttäjätunnuksiaan muille, sähköpostin liitetiedostoja avataan huolettomasti ja verkossa jaetaan henkilökohtaisia tietoja miettimättä kuka kysyy, miksi kysyy tai miten kysyy. Osa tapauksista on toki käyttäjien omaa huolimattomuutta, mutta oman haasteensa on tuonut viime vuosina tietoturvauhkien monipuolistuminen etenkin sosiaalisissa verkoissa.

Sosiaalisten verkkojen yleistyminen on tietoturvan kannalta ongelmallista sekä käyttäjille että selaimille, sillä mahdollisten uhkien tunnistaminen on vaikeutunut. Sosiaalisissa verkoissa haitalliset linkit ja haittaohjelmat leviävät kaverilistojen kautta tuttujen ihmisten kesken, ja tutulta käyttäjältä tullutta linkkiä, vaikkakin epämääräistä, ei aivan heti miellä vaaralliseksi. Vaikka selaimen tietoturvaominaisuudet näistä käyttäjää varoittaisivatkin, saattaa käyttäjä varoitukset helposti ohittaa, sillä linkki vaikuttaisi tulevan luotettavasta lähteestä. Samankaltainen ongelma ovat verkkorikollisten murtamat web-palvelimet, joissa jokin käyttäjille tuttu ja turvallinen palvelu käännetään heitä vastaan. Tutuilla sivustoilla vaaraa ei osata odottaa.

Verkkorikollisten fokus on siis siirtynyt entistä kierompaan suuntaan. Verkon käyttäjät ovat oppineet suojautumaan perinteisempiä uhkia vastaan, joten verkkorikollisten on kehitettävä uusia menetelmiä. Naamiointi, väärentäminen ja kaappaukset ovat tämän hetken avainsanoja. Nyt ollaan pisteessä, jossa parhaimmatkaan tietoturvatuotteet eivät enää riitä, vaan myös käyttäjältä vaaditaan paljon. Hyvä verkon tietoturva on siis mo-

nen tekijän summa, jossa turvallinen selain yhdessä muiden osatekijöiden kanssa voi auttaa käyttäjää tekemään oikeita päätöksiä. Mutta vain jos käyttäjä itse niin haluaa.

5.1 Tutkimuksen luotettavuus ja jatkotutkimusehdotukset

Tässä tutkimuksessa selvitettiin kahden tunnetun tietoturvayhtiön listaamat vuoden 2010 yleisimmät tietoturvauhkat, tutkittiin mitkä niistä kohdistuvat selaimeen sekä selvitettiin ja vertailtiin kolmen selaimen tietoturvaa näitä uhkia vastaan. Selaimia tutkittiin monipuolisesti tietoturvaominaisuuksien ja selaimista löydettyjen haavoittuvuuksien näkökulmista. Tutkimusta voidaan siis pitää luotettavana valituista tutkimusnäkökulmistaan tarkasteltuna, mutta niiden perusteella ei kuitenkaan voida julistaa absoluuttisesti parasta selainta. Selain on vain osa laajempaa tietoturvaketjua, johon kuuluvat muun muassa palomuuri- ja virustorjuntaohjelmistot sekä käyttöjärjestelmän päivitykset. Absoluuttisesti tietoturvallisimman selaimen selvittäminen vaatisi näiden muiden osatekijöiden poissulkemista, sekä tutkimuksessa selvitettyjen tietoturvaominaisuuksien käytännön testauksia suljetussa laboratorioympäristössä.

On myös syytä huomioida, että selainten tietoturva ja verkon tietoturvauhkat ovat alati muuttuvia pelikenttiä. Esimerkiksi vuoden kuluttua tilanne saattaa olla aivan toinen, jos tietoturvauhkat entisestään vaarallistuvat tai mikäli selaimiin kehitetään mullistavia tietoturvaominaisuuksia.

Tutkimuksen aihepiiri ja käytetyt rajaukset antavat paljon mahdollisuuksia selainten tietoturvan jatkotutkimuksille. Ilmeisin vaihtoehto olisi tuoda tutkimuksen piiriin muitakin markkinoilta löytyviä selaimia ja suorittaa selainten tietoturvaominaisuuksille käytännön testauksia mahdollisimman eristetyssä testiympäristössä. Muidenkin selainten tutkimisen avulla voisi esimerkiksi selvittää, löytyykö pienemmistä selaimista joitakin hyödyllisiä ominaisuuksia, jotka suositummista kilpailijoista uupuvat. Yksi mahdollisuus olisi myös nostaa Pugin-haavoittuvuuksia entistä suurempaan rooliin, sillä vaikuttaa siltä, että näitä haavoittuvuuksia tullaan tulevaisuudessa hyödyntämään yhä enemmän ja enemmän. Mielenkiintoinen tutkimuskohde olisi myös Internet Explorerin, Firefoxin ja Chromen seuraavat merkittävät versiot, joiden uusista tietoturvaominaisuuksista on julkisuudessa käyty jo innokasta keskustelua.

Lähteet

Adobe. 2011. Flash content reaches 99% of Internet viewers. Luettavissa: http://www.adobe.com/products/player_census/flashplayer/. Luettu: 5.2.2011.

Angwin, J. 9.7.2009. Sun Valley: Schmidt Didn't Want to Build Chrome Initially, He Says. Luettavissa: http://blogs.wsj.com/digits/2009/07/09/sun-valley-schmidt-didnt-want-to-build-chrome-initially-he-says/. Luettu: 25.9.2010.

Barth, A. 26.1.2010. The Chromium Blog. Security in Depth: New Security Features. Luettavissa: http://blog.chromium.org/2010/01/security-in-depth-new-security-features.html. Luettu: 30.8.2010.

Barth, A., Jackson, C., Reis, C., Google Chrome Team. The Security Architecture of the Chromium Browser. Luettavissa: http://seclab.stanford.edu/websec/chromium/chromium-security-architecture.pdf. Luettu: 30.8.2010.

Black, K. 19.2.2011. What is Spam? Luettavissa: http://www.wisegeek.com/what-is-spam.htm. Luettu: 19.3.2011.

Brink, S. 6.1.2009. Internet Explorer SmartScreen Filter - Turn On or Off. Luettavissa: http://www.sevenforums.com/tutorials/1406-internet-explorer-smartscreen-filter-turn-off.html. Luettu: 3.10.2010.

Google a. Google Safe Browsing Service in Mozilla Firefox Version 3 FAQ. Luettavissa: http://code.google.com/intl/fi/apis/safebrowsing/firefox3_privacy_faq.html. Luettu: 26.9.2010.

Google b. Tabs and windows: Incognito mode (private browsing). Luettavissa: http://www.google.com/support/chrome/bin/answer.py?answer=95464&hl=en. Luettu: 26.10.2010.

Guillaumier, J. Syyskuu 2007. Cross Site Scripting - XSS - The Underestimated Exploit. Luettavissa: http://www.acunetix.com/websitesecurity/xss.htm. Luettu: 31.1.2011

Kaspersky Lab. 23.8.2010. Information Security Threats in the Second Quarter of 2010. Luettavissa: http://www.securelist.com/en/analysis/204792133/Information_Security_Threats_in_the_Second_Quarter_of_2010. Luettu: 11.11.2010.

Kassner, M. 11.5.2009. The 10 faces of computer malware. Luettavissa: http://blogs.techrepublic.com.com/security/?p=1565&tag=leftCol;post-881. Luettu: 11.11.2010.

Kayne, R. 3.2.2011. What is a Botnet? Luettavissa: http://www.wisegeek.com/what-is-a-botnet.htm. Luettu: 14.3.2011.

Keizer, G. 17.11.2009. Firefox 3.6 locks out rogue add-ons. Luettavissa: http://www.computerworld.com/s/article/9141044/Firefox_3.6_locks_out_rogue_add_ons?taxonomyId=17&pageNumber=1. Luettu: 26.9.2010.

Linnake, T. 24.1.2011. F-Secure kerää kysymyksiä Brain-viruksen tekijöille. Luettavissa: http://www.digitoday.fi/tietoturva/2011/01/24/f-secure-keraa-kysymyksia-brain-viruksen-tekijoille/20111112/66?rss=6. Luettu: 6.2.2011.

Maone, G. 2010. NoScript features. Luettavissa: http://noscript.net/features. Luettu: 26.10.2010.

McMillan, R. 14.7.2010. Siemens: Stuxnet worm hit industrial systems. Luettavissa: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142. Luettu: 6.2.2011.

Microsoft. 2004. Windows XP Service Pack 2 Overview. White Paper. Luettavissa: http://download.microsoft.com/download/6/6/c/66c20c86-dcbe-4dde-bbf2-ab1fe9130a97/windows%20xp%20sp%202%20white%20paper.doc. Luettu: 3.10.2010.

Microsoft TechNet. 4.6.2009. Introducing Internet Explorer 8.0 Security. Luettavissa: http://technet.microsoft.com/en-us/library/dd919181%28WS.10%29.aspx. Luettu: 30.8.2010.

Microsoft Co. 2009. Internet Explorer 8 Desktop Security Guide - Enhancing Security & Privacy for Desktop Users. Luettavissa: http://download.microsoft.com/download/8/F/8/8F8025A0-C2C3-4825-8A5D-C152C652F021/Internet%20Explorer%208%20%20Desktop%20Security%20Guide.docx. Luettu: 3.10.2010.

Mozilla a. Mozilla Security Bug Bounty Program. Luettavissa: http://www.mozilla.org/security/bug-bounty.html. Luettu: 25.9.2010.

Mozilla b. Phishing and Malware Protection. Luettavissa: http://www.mozilla.com/en-US/firefox/phishing-protection/. Luettu: 26.9.2010.

Mozilla c. Firefox Knowledge Base: Private Browsing. Luettavissa: http://support.mozilla.com/en-us/kb/private+browsing. Luettu: 26.10.2010.

Mozilla d. Known Vulnerabilities in Mozilla Products. Luettavissa: http://www.mozilla.org/security/known-vulnerabilities/. Luettu: 26.10.2010.

MSDN Library. Event 1046 - Cross-Site Scripting Filter. Luettavissa: http://msdn.microsoft.com/en-us/library/dd565647%28VS.85%29.aspx. Luettu: 26.10.2010.

Namestnikov, Y. 17.12.2010. IT Threat Evolution for Q3-2010. Luettavissa: http://www.securelist.com/en/analysis/204792153/IT_Threat_Evolution_for_Q3_2010#9. Luettu: 6.2.2011.

Net Applications. 2010. Browser Market Share, December 2010. Luettavissa: http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0&qpcal=1&qpcal=1&qpcal=1&qptimeframe=M&qpsp=143. Luettu: 25.9.2010.

OWASP. 20.10.2010. Cross-site Scripting (XSS). Luettavissa: http://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29. Luettu: 11.11.2010.

Paul, R. 2.9.2009. Google unveils Chrome source code and Linux port. Luettavissa: http://arstechnica.com/open-source/news/2008/09/google-unveils-chrome-source-code-and-linux-port.ars. Luettu: 25.9.2010.

Pichai, S., Upson, L. 1.9.2008. Official Google Blog: A fresh take on the browser. Luettavissa: http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html. Luettu: 25.9.2010.

Rakowski, B. 8.12.2009. Google Chrome for the holidays: Mac, Linux and extensions in beta. Luettavissa: http://googleblog.blogspot.com/2009/12/google-chrome-for-holidays-mac-linux.html. Luettu: 25.9.2010.

Rakowski, B. 25.5.2010. A new Chrome stable release: Welcome, Mac and Linux!. Luettavissa: http://chrome.blogspot.com/2010/05/new-chrome-stable-release-welcome-mac.html. Luettu: 25.9.2010.

Robson, D. 13.8.2010. A Brief History of Phishing. Luettavissa: http://www.brighthub.com/internet/security-privacy/articles/82116.aspx. Luettu: 31.1.2011.

Schuh, J. & Pizano, C. 1.12.2010. Rolling out a sandbox for Adobe Flash Player. Luettavissa: http://blog.chromium.org/2010/12/rolling-out-sandbox-for-adobe-flash.html. Luettu: 6.2.2010.

Secunia a. 2010. Vulnerability Report: Microsoft Internet Explorer 8.x. Luettavissa: http://secunia.com/advisories/product/21625/?task=statistics_2010. Luettu: 7.2.2011.

Secunia b. 2010. Vulnerability Report: Mozilla Firefox 3.6.x. Luettavissa: http://secunia.com/advisories/product/28698/?task=statistics_2010. Luettu: 7.2.2011.

Secunia c. 2010. Vulnerability Report: Google Chrome 4.x. Luettavissa: http://secunia.com/advisories/product/28713/?task=statistics_2010. Luettu: 7.2.2011.

Secunia d. 2010. Vulnerability Report: Google Chrome 5.x. Luettavissa: http://secunia.com/advisories/product/30134/?task=statistics_2010. Luettu: 7.2.2011.

Secunia e. 2010. Vulnerability Report: Google Chrome 6.x. Luettavissa: http://secunia.com/advisories/product/31928/?task=statistics_2010. Luettu: 7.2.2011.

Secunia f. 2010. Vulnerability Report: Google Chrome 7.x. Luettavissa: http://secunia.com/advisories/product/32718/?task=statistics_2010. Luettu: 7.2.2011.

Secunia g. 2010. Vulnerability Report: Google Chrome 8.x. Luettavissa: http://secunia.com/advisories/product/33215/?task=statistics_2010. Luettu: 7.2.2011.

Silbey, M. & Brundrett, P. 2009. Understanding and Working in Protected Mode Internet Explorer. Luettavissa: http://msdn.microsoft.com/en-us/library/bb250462%28VS.85%29.aspx. Luettu: 3.10.2010.

Solomon, A. & Slade R. 8.5.2009. Virus History Summary. Luettavissa: http://www.cknow.com/cms/vtutor/virus-history-summary.html?page=1. Luettu: 6.2.2011.

Sophos. 2010. Security Threat Report: Mid-year 2010. Luettavissa: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-midyear-2010-wpna.pdf. Luettu: 11.11.2010.

Upson, L. 30.3.2010. Bringing improved support for Adobe Flash Player to Google Chrome. Luettavissa: http://blog.chromium.org/2010/03/bringing-improved-support-for-adobe.html. Luettu: 27.10.2010.

Liitteet

Liite 1. Loppuraportti

PROJEKTIN LOPPURAPORTTI

Selainten tietoturva

Aki Riionheimo

20.3.2011

Taustaa

Tämän opinnäytetyön aihe lähti liikkeelle ennen kaikkea omista kiinnostuksen kohteista. Tietoturvan ajankohtaisuus, uutisointi ja jatkuvat muutokset ovat saaneet minut seuraamaan tietoturva-asioita entistä enemmän. HAAGA-HELIA tarjosi opintojeni varrella muutaman tietoturvakurssin, joissa sivuttiin selainten tietoturvaa, ja tämä opinnäytetyö on kursseille luonnollinen jatkumo.

Tällä opinnäytetyöllä ei ole toimeksiantajaa eikä se kuulu mihinkään kehittämiskokonaisuuteen tai teemaryhmään. Projekti on siis lähtöisin puhtaasti tekijän omasta suunnitelmasta.

Saavutetut tulokset

Projektin tavoitteena oli projektisuunnitelman mukaan tuottaa HAAGA-HELIAn ohjeistuksen mukaan laadittu opinnäytetyö projektihallinnallisine dokumentteineen, sekä tietysti oppia projektityöskentelyä ja tieteellisen tekstin tuottamista. Nämä tavoitteet saavutettiin.

Projektin alkuperäinen laadullinen tavoite ei täyttynyt, sillä projektia ei kyetty saattamaan päätökseen alkuperäisen aikataulun puitteissa. Projektin piti alun perin valmistua viikolla 49, mutta työkiireiden ja sairastelujen vuoksi aikataulua jouduttiin muuttamaan kahteenkin otteeseen. Muutokset olivat kuitenkin hallittuja ja nyt työ on menossa arviointiin 7.4.2011.

Tulosten laadunvarmistus on suoritettu edistymisraporteilla, ohjauskokouksilla ja epävirallisilla sähköpostikeskusteluilla. Lisäksi opinnäytetyön ohjaaja on varmistanut, että opinnäytetyö on suoritettu HAAGA-HELIAn käytäntöjen mukaisesti.

Työn eteneminen

Projekti aloitettiin aihe-ehdotuksella ja aloituskokouksella 31.8.2010. Projektisuunnitelma hyväksyttiin aloituskokouksessa sovituilla pienillä muutoksilla. Projektisuunnitelmassa päätettiin, että työ valmistuu viikolla 49. Projektin edistymistä seurattiin edistymisraporteilla ja ohjauskokouksilla, joita pidettiin kaiken kaikkiaan kahdeksan kappaletta alkuperäisen kolmen sijaan. Edistymisraportteja tuotettiin yhteensä viisi.

Ensimmäinen seurantajakso piti sisällään lähinnä suunnittelua sekä teoriataustan alustavaa koostamista. Projektin ongelmat alkoivat jo ensimmäisellä seurantajaksolla projektipäällikön yli viikon kestäneellä sairastelulla. Tämän lisäksi projektia verottivat työkiireet, sillä opinnäytetyötä tehtiin normaalin työnteon ohella. Toteutuneet työtunnit jäivät kauas suunnitellusta.

Toinen seurantajakso kattoi ensimmäiseltä jaksolta tekemättä jääneet tehtävät sekä teoriataustan koostamista. Toinen seurantajakso sujui kohtuullisesti, mutta suunnitellut työtunnit eivät silti täyttyneet, koska tunteja oli lisätty ensimmäiseltä seurantajaksolta.

Kolmannen seurantajakson aikana alkoi näyttää siltä, ettei projekti tule valmistumaan suunnitellussa aikataulussa. Työskentely sujui hyvin, mutta ensimmäisen seurantajakson aiheuttama lumipalloefekti aiheutti edelleen paineita. Tässä vaiheessa alkoi myös tuntua siltä, että projekti oli alun perinkin mitoitettu liian tiiviiksi.

Neljännellä seurantajaksolla aikataulua muutettiin, sillä projektia ei ollut enää mitenkään mahdollista saada valmiiksi alkuperäisessä aikataulussa. Aikataulua jatkettiin siten, että uuden suunnitelman mukaan työ olisi valmis viikkojen 6 ja 7 vaihteessa. Projektipäällikköllä sattui kuitenkin työn tutkimusosuuden kanssa suuremman luokan ajatusvirhe, joka esti työn hyväksyttävän suorittamisen ja vaati työn osittaista uudelleensuunnittelua. Aikataulua jouduttiin toistamiseen muuttamaan ja lopulliseksi valmistusajankohdaksi sovittiin 21.3.2011. Tähän tavoitteeseen lopulta päästiinkin.

Vaikka työn aikataulutuksessa olikin kuvattuja ongelmia, pystyttiin niihin reagoimaan ajoissa ja muutokset olivat hallittuja ja ohjausryhmän hyväksymiä. Kokonaisuutena projektia voidaan siis pitää onnistuneena ja tavoitteita saavutettuina.

Kustannukset

Projektille ei tehty kustannusarviota, koska välineiden hankinnalle tai muille kustannuksia aiheuttaville toimenpiteille ei ollut tarvetta. Omille työtunneillekaan ei asetettu hintaa. Projekti ei tästä arviosta poikennut.

Resurssien käyttö

Projektisuunnitelmassa työhön oli resursoitu 395 tuntia. Lopullinen toteutunut tuntimäärä on 437 tuntia, eli noin kymmenen prosenttia suunniteltua enemmän.

	projektin alusta		
	suunniteltu	toteutunut	
Henkilö/tehtävä	tuntia	tuntia	%
Aki Riionheimo projektipäällikkö	395	437	110
Yhteensä	**395**	**437**	**110**

Suunniteltua suurempi työtuntien määrä selittyy yksinomaan työn tutkimusosuudessa tapahtuneesta ajatusvirheestä, joka aiheutti aikataulun pitkittymistä ja työn osittaista uudelleensuunnittelua. Tämä antoi osaltaan enemmän aikaa myös työn hienosäätöön ja viimeistelyyn, johon käytettiinkin suunniteltua enemmän tunteja. Toteutuneet työtunnit koko projektin ajalta on kuvattu liitteessä 1.

Kokemukset

Näin jälkikäteen projektia tarkastellessa voi todeta, että alussa ei oikein ollut käsitystä mitä pitäisi tehdä, mutta projektin jälkeen on selvää, mitä **olisi** pitänyt tehdä. Projektin kaksi suurinta opetusta olivat ehdottomasti suunnittelun tärkeys ja aikataulun sovitus riittävän väljäksi. Suurimmat opetukset nämä ovat tietysti siksi, että niissä molemmissa

epäonnistuttiin tässä projektissa. Alkuperäinen suunnittelu ei sinänsä suoraan epäonnistunut, mutta opinnäytetyö vain on niin laaja kokonaisuus, että se vaatii runsaasti suunnittelua vielä projektin edetessäkin. Projektin laajuuteen liittyy myös aikataulutuksen tärkeys. Riittävän väljällä aikataululla on helppo reagoida yllättäviin muutoksiin ja muihin ongelmiin.

Kokonaisuutena opinnäytetyöprojektin kokemukset olivat kuitenkin myönteiset, vaikka välillä työskentely olikin erittäin raskasta ja työn valmistuminen vaikutti miltei mahdottomalta. Uusi väljempi aikataulu kuitenkin mahdollisti muutamien viikkojen loman pitämisen opinnäytetyöstä, joka osoittautui kullanarvoiseksi. Loman aikana projektiin pystyi ottamaan etäisyyttä ja ajatukset selkiytyivät. Tällaisten taukojen pitämistä suosittelen tuleville opinnäytetöiden tekijöillekin.

Myös projektille asetetut oppimistavoitteet täyttyivät mielestäni hyvin. Hallittua projektin läpivientiä tuli opeteltua kantapään kautta, joka on toki tehokas oppimistapa. Tieteellinen kirjoitustyyli ja ennen kaikkea lähdekriittisyys tulivat tutuiksi projektin edetessä. Yksinomaan sähköisistä lähteistä koostuneen lähdeaineiston luotettavuuden arviointia oli suoritettava jatkuvasti. Loppukevennyksenä voi todeta, että projekti opetti myös rutkasti paineensietokykyä ja kärsivällisyyttä.

Ehdotukset jatkotoimenpiteiksi

Vaikka opinnäytetyöllä ei ollutkaan toimeksiantajaa, voi siitä olla hyötyä muille tahoille. Mahdollisesti inspiraation lähteenä tuleville opinnäytetöiden tekijöille, tai muuten vain selainten tietoturvasta kiinnostuneille lukijoille.

Liitteet

Liite 1. Toteutuneet työtunnit

teht.no.	tehtävä	vastuuhenkilö	tunnit	33-34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	1	2	3	4	5	6	7	8	9	10	11
1	**projektin käynnistäminen ja hallinta**	**pp**	**106**																														
1.1	aiheeseen tutustuminen	pp	20	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	0
1.2	projektisuunnitelman laatiminen	pp	25	20	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	0
1.3	projektin käynnistäminen	pp	10	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	0
1.4	ohjauskokousten valmistelut ja jälkityöt	pp	51	5	2	0	0	5	2	0	0	0	6	3	0	5	2	5	2	0	0			3	0	0	3	3	0	0	3	2	0
2	**suunnittelu**	**pp**	**60**																														
2.1	dokumentin rakenteen laatiminen	pp	10	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	0
2.2	tutkielman rungon suunnittelu	pp	15	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	5	0	0	0	0	0
2.3	teoriataustan suunnittelu	pp	35	0	0	12	12	0	0	0	0	0	0	0	0	0	0	0	6	0	0			0	0	0	0	5	0	0	0	0	0
3	**toteutus**	**pp**	**254**																														
3.1	teoriataustan koostaminen	pp	93	0	0	8	15	15	10	10	0	0	0	0	14	14	0	0	0	2	0			0	0	0	0	0	0	5	0	0	0
3.2	tulosten analysointi	pp	56	0	0	0	0	0	10	10	11	0	0	0	5	5	0	0	0	5	5			0	0	0	0	0	0	5	0	0	0
3.3	dokumentin työstäminen	pp	80	0	0	0	0	0	0	0	0	10	10	5	10	10	0	0	0	0	0			0	5	5	5	5	0	0	10	5	0
3.4	työn viimeistely	pp	25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	10	10	5
4	**projektin päättäminen**	**pp**	**17**																														
4.1	loppuraportin kirjoittaminen		8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	8
4.2	loppukatselmointi	pp	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	5
4.3	projektin päättäminen / tuloksen luovutus	pp	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			0	0	0	0	0	0	0	0	0	4
		yhteensä	**437**																														