Aleksi Tarakkamäki

Capture The Flag -mallin soveltuminen kyberturvallisuuden opetukseen

Tietotekniikan kandidaatintutkielma

29. huhtikuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Aleksi Tarakkamäki

Yhteystiedot: aleksi.tarakkamaki@gmail.com

Ohjaaja: Sanna Juutinen

Työn nimi: Capture The Flag -mallin soveltuminen kyberturvallisuuden opetukseen

Title in English: Using Capture The Flag -model in cybersecurity education

Työ: Kandidaatintutkielma

Sivumäärä: 21+0

Tiivistelmä: Kyberturvallisuus on noussut jatkuvasti tärkeämmäksi osa-alueeksi nykypäiväisessä yhteiskunnassa. Jatkuva kehitys tuo mukanaan uusia haavoittuvuuksia, joiden avulla voidaan toteuttaa kyberuhkia. Toisaalta myös kyberturvallisuuden opiskelu ja yleinen kiinnostus kyberturvallisuutta kohtaan on ollut nousussa. Esimerkiksi Capture The Flag -haasteet ovat saaneet viime vuosina laajemmin huomiota. Tässä tutkielmassa tarkastellaan CTF -haasteita, sekä niiden soveltamista kyberturvallisuuden opettamiseen.

Avainsanat: CTF, Capture the flag, opetus, kyberturvallisuus, tietoturva

Abstract: Cybersecurity has steadily become an increasingly important part of today's society. Constant development brings with it new vulnerabilities to cyber threats. On the other hand, cybersecurity studies and public interest in cybersecurity have also been on the rise. For example, Capture The Flag -challenges have received wider attention in recent years. This paper examines the CTF -challenges and their application to cybersecurity education.

Keywords: CTF, Capture the flag, education, cybersecurity, information security

Termiluettelo

Capture The Flag	Capture The Flag on kyberturvallisuuteen liittyvä haaste tai joukko haasteita, jotka yleensä jaetaan internetin välityksellä kaikkien saataville. Haasteita löytyy monen tasoisia, joten kaikilla on mahdollisuus osallistua niihin. Haasteita on myös pelillistetty esimerkiksi pisteytyksillä sekä aikarajoilla. Usein haasteiden voittajille on luvassa myös palkinto. Taitavimmat osallistujat voivat liittyä turnauksiin, joissa on suurempia rahapalkintoja sekä haastavampia tehtäviä. Haasteiden tarkoituksena on tehdä kyberturvallisuuden harjoittelusta ja siihen tutustumisesta mielekkäämpää.
Tietoturva	Tietoturvalla tarkoitetaan nimenomaan tiedon turvaamiseen kohdistuvaa toimintaa. Tietoturvauhat sisältävät sekä fyysiset tietoturvamurrot, kuten rakennukseen murtautumisen ja sitä kautta fyysisten tietojen varastamisen, että verkon kautta tapahtuvat tietomurrot.
Kyberturvallisuus	Kyberturvallisuudella tarkoitetaan kaikkea sähköiseen ja verkostoituneeseen infrastruktuuriin liittyvää toimintaa, jossa ehkäistään, tunnistetaan ja varaudutaan näiden järjestelmien häiriöihin ja niiden vaikutuksiin. Kyberturvallisuus sisältää myös tietoturvallisuuden osa-alueita, kuten verkon kautta tehtävät tietomurrot, muttei fyysistä murtautumista.

Kuviot

Sisältö

1 Johdanto

Yleinen kiinnostus kyberturvallisuutta kohtaan on ollut jatkuvassa nousussa (Google 2020) teknologian kehittyessä ja tullessa yleisemmin saataville. Kyberinfrastruktuurin kehittyessä löydetään jatkuvasti myös uusia haavoittuvuuksia, usein hyvin suosituista ja laajasti käytössä olevista laitteista ja ohjelmista. Uutiset toistuvista tietovuodoista, palvelunestohyökkäyksistä, viruksista ja huijauksista ovat jo arkipäivää yleisessä mediassa. Kyberuhkien määrä nousee uusien teknologioiden nousun mukana ja samoin näyttäisi nousevan kyberhyökkääjien taitotaso, mikä ilmenee jatkuvasti kehittyvistä hyökkäysstrategioista.

Kyberturvallisuus on todella laaja käsite, joka pitää sisällään useita eri tietotekniikan opetuksen osa-alueita. Kyberturvallisuuteen onkin mahdollista suuntautua useilla eri koulutustasoilla, kuten esimerkiksi maisteriopinnoissa. Kyberturvallisuuteen tulisi kuitenkin kiinnittää huomiota myös muilla tietotekniikan suuntautumisen osa-alueilla. Kyberuhat koskettavat nykyään lähestulkoon jokaista meistä, joten yleinen kyberturvallisuus tulisi saada sille tasolle, että jokainen tietotekniikan ammattilainen kykenee minimoimaan kyberuhat omassa työssään. Kyberturvallisuuden opetuksen saatavuuteen, mielekkyyteen ja tehokkuuteen onkin siis syytä perehtyä tarkemmin.

Tämän tutkimuksen tarkoituksena on tarkastella Capture The Flag (CTF) -haasteiden mallin mahdollista soveltumista opetuskäyttöön. CTF on yleensä kilpailu tai nettiin ladattu haaste tai joukko haasteita, jossa on tarkoituksena esimerkiksi etsiä pienestä ohjelmanpätkästä haavoittuvuus tai purkaa jonkin tiedoston salaus, minkä avulla ohjelmasta kaivetaan "flag"eli vastaus (Leune ja Petrilli 2017). Saatuaan vastauksen, haasteen tekijä palauttaa sen nettisivulle ja saa haasteesta sovitun pistemäärän. Tekemällä useita haasteita pelaaja saa enemmän pisteitä. Jonkin tietyn ajan päästä CTF -haaste päättyy ja voittajat yleensä palkitaan. Maailmalla pidetään myös suuria CTF -turnauksia, joissa on suuremmat palkintosummat. Turnauksissa haasteet koostuvat esimerkiksi muiden joukkueiden palvelimia vastaan hyökkäämisestä ja heidän hyökkäyksiltä puolustautumisesta. CTF on siis hyvin pelillistetty tapa tutustua, oppia ja haastaa itseään kyberturvallisuuteen liittyvissä asioissa. Tämän takia malli voisi soveltua hyvin myös kyberturvallisuusopetukseen.

Tutkielman alussa avataan tarkemmin Capture The Flag -haasteen käsitettä, sekä tarkastellaan sen taustaa, tyyppejä, tarkoitusta ja toimintaa. Seuraavaksi selvitetään laajemmin kyberturvallisuutta. Myöhemmin tarkastellaan kyberuhkia sekä niiden ehkäisyä ja torjumista. Lisäksi tarkastellaan uhkien luokittelua ja merkittävyyttä. Loppua kohden käsitellään hasatelähtöistä oppimista, sekä CTF -mallin soveltumista opetukseen. Lopussa käydään vielä läpi tutkielmassa käsitellyt asiat.

2 Capture The Flag

Ensimmäinen virallinen Capture The Flag -kilpailu järjestettiin vuonna 1996 Las Vegasissa, DEF CON -tapahtumassa. Tällöin kilpailun pisteytyksestä päätti ensimmäistä kertaa tuomari. Aluksi kilpailut olivat hyvin kaoottisia ja epäselviä puuttuvan standardin takia. Ajan myötä kilpailut ovat kuitenkin kehittyneet sekä automatisoituneet suurelta osalta. Kilpailuihin pääsee nykyään usein mukaan suoriutumalla karsinnoista, jotka ovat avoimia kaikille. (DDTek 2020)

Capture The Flag on oikeastaan vain yksi tyyppi Wargame -nimellä kutsutuista kyberturvallisuushaasteista. CTF -haasteiden katsotaan usein pitävän sisällään kolmea tai viittä erilaista haastemuotoa: aarteenmetsästys, hyökkäys/puolustus, tietovisa, laitteisto, sekä vuorenvaltaus. Tunnetuimmaksi sekä eniten käytetyksi haasteeksi kilpailuissa on muodostunut hyökkäys/puolustus -muoto. Tässä pelaajat pyrkivät pitämään omalla palvelimella olevan lippunsa turvassa samalla kun, he pyrkivät korruptoimaan toisten joukkueiden lippuja. Jokainen joukkue saa erilaisen palvelimen, jonka tulee kyetä tiettyihin toimintoihin, jotta joukkue saa pisteitä. Mikäli palvelin kykenee näihin toimintoihin, voi joukkue saada lisäpisteitä korruptoimalla muiden palvelimia. Mikäli palvelimen toiminta on estynyt, joukkue ei saa pisteitä vaikka saisi korruptoitua muiden palvelimia. (**Defending** ; Conti, Babbitt ja John 2011; Eagle 2013)

Kilpailujen ulkopuolella tunnetuin muoto on aarteenmetsästys (engl. scavenger-hunt). Puhuttaessa Capture The Flag:sta tarkoitetaan yleensä jotakin CTF -kilpailua. Capture The Flag -haasteesta puhuttaessa voidaan tarkoittaa mitä tahansa haastetyyppiä, mutta useimmiten sillä viitataan nykyään aarteenmetsästykseen. (Cowan ym. 2003; Leune ja Petrilli 2017)

Capture The Flag -kilpailuista on pyritty tekemään mahdollisimman viihdyttävää myös katsojille. Sääntöjä on muokattu viihdealalle sopivimmiksi, mikä tarkoittaa suurta määrää haavoittuvuuksia osallistujien palvelimissa, sekä helpoimpien puolustus- ja hyökkäysstrategioiden kieltämistä. Viihdealalle sovittamisen voi huomata varsinkin DEF CON Capture The Flag -turnauksen sivuhaasteista, kuten valinnaisesta laitteisto osuudesta, jossa joukkueet pyrkivät tuhoamaan kovalevyn suurikaliiperisella aseella mahdollisimman pieniksi palasiksi.

Parhaiten kovalevyn tuhonnut joukkue saa ylimääräisiä pisteitä tai mahdollista apua muihin haasteisiin. (Cowan ym. 2003)

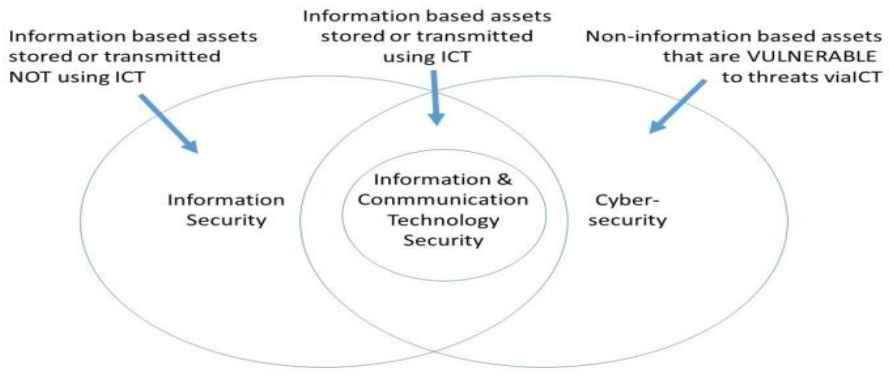
Alun perin Capture The Flag oli siis turnaustyylinen kilpailu, jossa joukkueet kilpailivat toisiaan vastaan kyberturvallisuuteen liittyvissä tehtävissä. Ajan myötä Capture The Flag -haasteista on kuitenkin muodostunut yleisemmin tunnettu käsite, jossa kuka tahansa voi yrittää suorittaa nettiin ladattuja aarteenmetsästyshaasteita. Nämä haasteet toimivat usein myös karsintahaasteina suuremmille Capture The Flag -turnauksille. Esimerkiksi Googlella on oma Capture The Flag -turnaus, johon liittyvällä nettisivulla voi tutustua aloittelijan haasteisiin, suorittaa karsintahaasteita tai osallistua karsintoihin.

Aarteenmetsästyshaasteissa käytettäviin tehtäviin luodaan yleensä hyvinkin leikkimielisiä taustatarinoita ja syitä sille, miksi haaste tulisi ratkaista. Varsinkin aloittelijoille suunnatuista haasteista löytyy usein hyvin pelillistettyjä tehtäviä. Tarkoituksena on saada haasteisiin tutustumisesta mahdollisimman hauskaa, kiinnostavaa ja motivoivaa. Samalla voidaan kuitenkin vaatia haasteen tekijää opettelemaan monimutkaisiakin asioita suoriutuakseen tehtävästä. Haasteet eivät itsessään kuitenkaan usein sisällä minkäänlaista opetusta tehtäviin vaadittavista taidoista tai edes mainitse mitä itse tehtävän läpäiseminen vaatii. Haasteen tekijä joutuu itse päättelemään, etsimään tai opettelemaan tehtävään vaadittavat asiat ja taidot. Helppojenkin tehtävien ratkaisu voi siten viedä huomattavan määrän aikaa, mikäli haasteen tekijä ei tiedä mitä etsiä.

3 Kyberturvallisuus

Kyberturvallisuuden ja tietoturvan käsitteitä käytetään usein toistensa synonyymeinä, vaikka ne tarkoittavat hieman eri asioita. Kyberturvallisuus on huomattavasti laajempi käsite kuin tietoturva, joka usein määritellään vanhan CIA -kolmion perusteella. CIA -kolmion mukaan tietoturva kattaa kaikenlaisen tiedon luottamuksellisuuden (confidentiality), eheyden (integrity) sekä saatavuuden (availability) turvaamisen (Solms ja Niekerk 2013). Kyberturvallisuus kuitenkin kattaa hyvin paljon muutakin kuin tiedon suojelun. Kyberturvallisuudesta onkin menneen reilun vuosikymmenen aikana tullut toistuva puheenaihe sekä valtava haaste yksityishenkilöille, yrityksille ja valtioille. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa pyritään kaiken sähköisen- ja verkostoituneen infrastruktuurin suojaamiseen. Tähän kuuluu uhkien tunnistaminen, ennakoiminen, torjuminen, minimoiminen sekä toteutuvien uhkien varalle valmistautuminen. (Turvallisuuskomitea 2013)

Kyberuhat sisältävät tietoturvauhkien verkon kautta toteutettavien hyökkäysten lisäksi esimerkiksi verkon kautta suoraan yksittäistä henkilöä kohtaan tehtävät hyökkäykset. (Solms ja Niekerk 2013; Turvallisuuskomitea 2013) Artikkelissaan Solms ja Niekerk (2013) esittävät esimerkiksi neljä kyberuhkaa, joita tietoturvan käsite ei pidä sisällään: verkkokiusaaminen, kodin automaation hakkerointi, digitaalinen piratismi ja kyberterrorismi. Erojen havainnollistamisen apuna käytetään usein Kuvio 1 kaltaisella Venn-diagrammilla.



Kuvio 1. Tietoturvan ja kyberturvallisuuden eroja kuvataan usein vastaavalla Venn-diagrammilla

(Solms ja Niekerk 2013)

3.1 Kyberuhkien luokittelu

Kyberuhkia on hyvin monenlaisia ja ne voivat kohdistua sekä aiheuttaa harmia tai tuhoa niin yksittäiselle henkilölle kuin kokonaiselle valtiolle. Uhkia on pyritty luokittelemaan yleisyyden ja haitallisuuden mukaan. Luokitteluun voidaan käyttää esimerkiksi kolmio -mallia. Kolmio -mallissa pohjalla on yleisimmät ja vähiten harmia aiheuttavat kyberuhat. Kolmion huipulla taas sijaitsevat harvinaisemmat sotatilassa ilmenevät kyberhyökkäykset.

1. Kolmion pohjalle voidaan sijoittaa kyberuhat, joiden toteuttaminen ei yleensä ole rikollista. Tähän luokkaan kuuluu esimerkiksi nettikiusaaminen, trollaaminen ja väärän tiedon jakaminen. Tämän luokan uhat eivät yleensä tuota taloudellista tai fyysistä haittaa, mutta ovat epämiellyttäviä näille altistuville henkilöille ja tahoille.

2. Toiselle tasolle voidaan sijoittaa luonnonkatastrofit sekä rikollinen toiminta. Luonnonkatastrofien yleisyyttä ja uhkan vakavuutta on hankala arvioida. Suurta katastrofia seuraavat vahingot voivat lamauttaa suuren osan valtion toiminnasta, minkä seurauksena tyytymättömät kansalaiset voivat aiheuttaa lisävahinkoja. Rikollisen toiminnan haittojen suuruus vaihtelee myös huomattavasti. Yksittäisen henkilön salasanojen kalastelulla ei yleensä ole valtavia haittavaikutuksia, mutta tunnetun yhtiön tietojen vuotaminen voi pilata koko brändin maineen. Yleisiä kyberrikoksia ovat esimerkiksi DoS -hyökkäykset, haittaohjelmien levittäminen, petos ja rahanpesu. (Sisäministeriö 2020)

3. Viimeinen suhteellisen yleinen kyberuhka on kybervakoilu. Kybervakoilu voidaan jakaa pääsääntöisesti kahteen kategoriaan: yritysvakoiluun sekä valtiovakoiluun. Yritysvakoilun tarkoituksena on lähes aina saada jonkinlaista taloudellista hyötyä, haittaa tai etulyöntiasemaa. Valtiovakoilussa pyritään etsimään tietoa sekä keinoja vaikuttaa toisen valtion toimintaan. Vakoiluun voi kuulua niin poliittiset, taloudelliset kuin sotilaalliset tarkoitusperät.

4. Harvinaisempiin uhkiin lukeutuu kyberterrorismi. Kyberterrorismilla tarkoitetaan perinteisen terrorismin keinojen käyttämistä kyberympäristössä. Terrorismin tarkoituksena voi olla luoda pelkoa, tuottaa vahinkoa tai kiristää jotakin tahoa toimimaan. Kyberterrorismi on osoittautunut tehokkaaksi työkaluksi terroristijärjestöille, sillä se on

halpaa, suhteellisen anonyymiä, saavuttaa suuren joukon kohteita sekä voidaan suorittaa mistä tahansa. (Weimann ja Peace 2004)

5. Kolmion huipulle voidaan sijoittaa kybersodankäynti. Turvallisuuskomitea määrittelee kybersodankäynnin seuraavasti: "tietoverkkoja ja niiden haavoittuvuuksia hyödyntävä, valtioiden välinen vihamielinen toiminta", jossa on lisähuomautuksena: "Tietoverkkosodankäynnin käsite on kiistanalainen, sillä sotaa ei voi rajata vain yhteen toimintaympäristöön" (Sanastokeskus 2018). Kybersodankäynnissä pyritään kuitenkin vaikuttamaan toisen valtion toimintaan kyberinfrastruktuuriin kautta sellaisella negatiivisella tavalla, joka heikentää kyseistä valtiota jollain tavalla. (Parks ja Duggan 2001)

3.2 Merkittävimmät kyberuhat

Merkittävimpiä kyberuhkia ovat pääasiassa laitteet, jotka ovat osa lähes jokaisen arkea. Ne ovat laajassa käytössä, jolloin niissä toteutuva kyberuhka tuottaa haittaa suurelle määrälle henkilöitä. Nämä kyseiset laitteet ovat usein myös yhteydessä muihin laitteisiin, jotka voivat joutua hyökkäyksen kohteeksi alkuperäisen laitteen kautta. Käyttäjä ei monessa tapauksessa voi vaikuttaa uhkan torjumiseen, vaan laitteen, palvelun tai sovelluksen tarjoaja on siitä vastuussa. Usein kuitenkin myös käyttäjän toiminta johtaa suoraan kyberuhan toteutumiseen.

3.2.1 IoT ja älypuhelimet

IoT -laitteiden määrä on ollut valtavassa nousussa. Vuonna 2015 yhdistettyjen IoT -laitteiden määrän arvioitiin olevan noin 15 biljoonaa ja vuonna 2019 noin 26 biljoonaa (Statista 2016). Näitä lukuja käytetään useissa lähteissä, vaikka luku perustuu vuosina 2015 - 2016 kerättyjen tietojen pohjalta tehtyyn arvioon. Tärkeintä kuitenkin on tietää, että IoT -laitteiden määrä on todella suuri. Monissa IoT -laitteissa ei ole juurikaan minkäänlaista suojausta. Laitteet käyttävät usein täysin salaamatonta viestintää, oletus käyttäjätunnuksia ja salasanoja tai eivät ole salasanalla suojattuja lainkaan. Haavoittuvia IoT -laitteita voidaan valjastaa esimerkiksi palvelunestohyökkäyksiin ja käyttää tietojen kalasteluun. (Lehto ym. 2017)

Älypuhelimet ovat toinen todella laajassa käytössä oleva kyberuhka. Puhelimiin liittyy useita merkittäviä kyberuhkia. Jatkuvasti mukana olevat älypuhelimet ovat varsin käteviä työkaluja

vakoiluun ja tietojenkeräämiseen. Lukuisat applikaatiot keräävät käyttäjästä tietoja, joiden keräämiseen käyttäjä on voinut tietämättään suostua. Sovelluksien maksupäätejärjestelmillä voidaan yrittää tuottaa taloudellista vahinkoa. Avoimiin wifi-verkkoihin liittyminen tuo mukanaan myös useita haavoittuvuuksia hyökkäyksille, kuten mies välissä -hyökkäykselle sekä kirjautumistietojen varastamiselle. Älypuhelimilla kontrolloidaan jatkuvasti myös useita muita laitteita, jolloin haavoittuvuuksilla voi olla vaikutuksia useampiin laitteisiin. (Lehto ym. 2017)

3.2.2 Web

Web-palveluihin kohdistuvat uhat pitävät sisällään hyvin suuren määrän erilaisia hyökkäyksiä. Usein uhkien toteuttamisen mahdollistaa web-palveluiden omistajien palvelimien ja sivustojen päivittämättä jättäminen. Artikkelissaan Lehto ym. (2017) vertaavat tätä ikkunan auki jättämiseen rikollisille. Vuosina 2014 - 2017 skannatuista web-palveluista yli 75% sisälsi Symantecin arvion mukaan päivittämättömiä haavoittuvuuksia, joista 15% oli luokiteltu kriittisiksi vuonna 2015. Lisäksi web-hyökkäysten määrä oli tuplaantunut vuonna 2015. Tälle annetaan erääksi syyksi hyökkäysvälineiden laaja saatavuus, sekä hyökkäyksien toteuttamisen helppous. (Lehto ym. 2017)

3.2.3 Sosiaalinen media

Sosiaalisen median yksi yleisimmistä uhista on sosiaalinen manipulointi. Sosiaalisessa mediassa hyökkääjän on usein hyvin helppo selvittää kohteestaan tietoja, joita voidaan mahdollisesti käyttää muiden hyökkäysten edesauttamiseksi. Tietojenkalasteluhyökkäysten lisäksi voidaan niistä saatuja tietoja käyttää hyödyksi esimerkiksi tekaistujen maksujen perimisessä. (Lehto ym. 2017)

4 Capture The Flag -malli opetuksessa

Capture The Flag -haasteet pohjautuvat laajalti haastelähtöiseen oppimiseen, jossa on tarkoituksena oppia samalla kun ratkaistaan jotain reaalimaailman haastetta. Capture The Flag -mallin käytöstä opetuksessa ei vielä löydy laajempaa tutkimusta, joten mallin soveltumista täytyy tarkastella pitkälti haastelähtöisen oppimisen kautta, sekä pienempien CTF -kilpailuihin liittyvien tutkimusten pohjalta. Haastelähtöisen oppimisen on tutkittu voivan huomattavasti tehostaa oppimista, esimerkiksi Johnson ym. (2009) ja Johnson ja Brown (2011) osoittavat tutkimuksissaan lupaavia tuloksia.

4.1 Haastelähtöinen oppiminen

Haastelähtöinen oppiminen on opettajien ja oppilaiden yhteinen oppimiskokemus, jossa työskennellään yhdessä, tavoitteena oppia tuntemaan oikeita ongelmia, ehdottaa niihin ratkaisuja sekä toimia niiden ratkaisemiseksi. Tämä lähestymistapa pyrkii saamaan opiskelijoita reflektoimaan omaa oppimistaan, miettimään tekojensa seurauksia sekä julkaisemaan ratkaisunsa maailmalle. Haastelähtöinen oppiminen yhdistää usein eri tieteenaloja ratkaisujen etsimisen ja toteuttamisen aikana (Johnson ja Brown 2011).

Tutkimuksessaan Johnson ym. (2009) selvittivät haastelähtöisen oppimisen vaikutuksia useissa kouluissa. Tutkimukseen osallistui yhteensä seitsemän avustavaa ammattilaista, 29 opettajaa sekä 321 oppilasta. Oppilaat olivat enimmäkseen 9. luokalta, loput noin 20% olivat 10. luokalta tai 11. luokalta ***(high school)***. Jokaiselle koululle annettiin eri haaste, johon oppilaiden tuli kehittää ratkaisu ja esittää tämä ratkaisu muille ryhmille.

Kyseisen tutkimuksen Johnson ym. (2009) tulokset osoittavat haasteiden tulosten ylittäneen sekä opettajien että oppilaiden odotukset. 97% opettajista koki että oppilaat oppivat enemmän kuin mitä oli odotettu ja 100% opettajista oli sitä mieltä että oppilaiden työskentely ylitti heidän odotuksensa. Niissä kouluissa, joissa haasteen aihe oli hyvin oleellinen opiskelijoille, todettiin syntyvän parempi laatuisia lopputuloksia. Opettajat tunnistivat oppilaiden kehittäneen uusia ajattelutapoja, ympäristön huomioimista sekä asian tutkimista ennen vastaukseen hyppäämistä. Tärkeä huomio tutkimuksessa on se, että projektin jälkeen 100% opettajista ko-

ki, että oppilaat hallitsivat aihealueen tarpeelliset tiedot ja taidot, jotka opetussuunnitelmassa oli määritelty.

Johnson ym. (2009) tutkimus toi esille kuitenkin myös haasteita niin opettajien kuin oppilaidenkin näkökulmasta. Jopa neljäsosalla oppilaista oli jonkinlaista ongelmaa ryhmätoimintaan liittyen. Muita oppilailla ilmenneitä ongelmia olivat muun muassa tehtävän valmiin suunnan ja ajan puute sekä tutkimustyön tekeminen. Opettajien suurimmat haasteet koostuivat aikatauluihin liittyvistä huolista, teknologisista ongelmista sekä projektin sovittamisesta opetusohjelmaan. Suuri osa ongelmista ja huolista kuitenkin lieveni tai hävisi kokonaan projektin edetessä pitemmälle.

Johnson ja Brown (2011) teki myöhemmin Johnson ym. (2009) tutkimuksen pohjalta vastaavan tutkimuksen, jossa todettiin hyvin samankaltaisia tuloksia. Johnson ja Brown (2011) toi tutkimuksen pohjalta esille suosituksia, jotka pyrkivät vähentämään opetuksessa vastaan tulleiden haasteiden määrää. Suuri osa suosituksista koskettaa opettajia, joille suositellaan seuraavia toimia ennen projektin aloittamista:

- Alkeellisen videoeditoinnin opettelu
- Haastelähtöiseen oppimiseen tutustuminen
- Ajan varaaminen valmistautumiseen sekä itse projektiin
- Sopivan ryhmäjaon suunnittelu
- Haasteen relevanttiuden varmistaminen
- Ratkaisujen pohjalta toimimisen varmistaminen

(Johnson ja Brown 2011)

4.2 CTF -opetuksessa

CTF -kilpailuja käsittelevissä tutkimuksissa on tutkittu monipuolisesti kyseisten haasteiden vaikutusta opiskelijoiden osaamiseen ja ajatteluun sekä kilpailukokemuksen parantamiseen. Tutkimuksissaan sekä Cheung ym. (2011) että Leune ja Petrilli (2017) selvittivät oppilaiden osaamisen kehittymistä CTF -kilpailuun osallistumisen jälkeen. Cheung ym. (2011) selvittivät oppilaiden itsearviointia tietokonetaidoista, kyberturvallisuustaidoista, kiinnostuksesta

kyberturvallisuuteen, kyvystä opettaa muita turvallisuuteen liittyvissä asioissa sekä tutkimukseen osallistumisen hyödyllisyyttä. Oppilaat raportoivat selkeätä nousua jokaisella kyselyn alueella. Kaikista huomattavin nousu oli nähtävissä oppilaiden kiinnostuksessa kyberturvallisuutta kohtaan. Niiden oppilaiden määrä, jotka antoivat kiinnostukselle täydet kymmenen pistettä, nousi lähes seitsemänkertaiseksi. Myös Leune ja Petrilli (2017) osoittivat tutkimuksessan oppilaiden olleen hyvin kiinnostuneita kilpailussa suoritettaviin haasteisiin, sekä saaneen itseluottamusta kyberturvallisuuteen liittyvissä asioissa. Oppilaiden kiinnostus, motivaatio ja itseluottamus aihetta kohtaan ovat tärkeä osa oppimista, jotka välittyvät lähes suoraan oppimistulokseen (Leune ja Petrilli 2017).

Leune ja Petrilli osoittivat tutkimuksessaan CTF -kilpailun kehittäneen huomattavasti opiskelijoiden kyberturvallisuuden käytännön taitoja. Oppilaiden teoreettisten taitojen kehittymisessä ei huomattu juurikaan eroa, minkä Leune ja Petrilli (2017) uskoo johtuvan haasteiden tyypistä. Haasteissa vaadittiin yhtäaikaa käytännön ja teorian taitoja. Jakamalla haasteet erillisiin käytännön ja teorian haasteisiin voitaisiin nähdä parempia tuloksia teoreettisen osaamisen kehittymisessä (Leune ja Petrilli 2017).

Artikkelissa “The Value of Capture-the-Flag Exercises in Education: An Interview with Chris Eagle” Eagle toteaa kyberharjoitusten voivan houkutella nuoria opiskelijoita kyberturvallisuuden pariin. Hän kertoo hyvien haasteiden kehittämisen olevan keskeisenä ongelmana sekä ehdottaa DEFCON CTF -kilpailun mallin noudattamista. Eaglen ehdottama malli muistuttaa paljolti Yhdysvalloissa yleisessä käytössä olevaa mallia. Siinä esimerkiksi useilla urheilulajeilla on omat koulukohtaiset joukkuuet, jotka harjoittelevat ja kilpailevat muiden koulujen joukkueiden kanssa. Hänen mielestään ylä-aste- ja lukioikäisten tietotekniikkaopetuksessa on keskitytty liiaksi tietokoneen käyttöön, verkkosivujen suunnitteluun sekä alkeelliseen ohjelmointiin. Hän uskoo nuorten jo osaavan suuren osan näistä asioista, joten he tylsistyvät, eivätkä siten innostu tietotekniikan opiskelusta. "Haluamme itsenäisiä oppijoita, ja tätä voidaan motivoida kyberhaasteilla"(suomennos), hän selittää. Eagle tahtoisi myös mahdollistaa opintopisteiden saannin niistä asioista, jotka opiskelija osaa jo etukäteen. Täten opiskelijan ei tarvitsisi osallistua kursseille, joilla käydään jo hänelle tuttua asiaa. (Irvine 2011)

5 Yhteenveto

Kyberturvallisuus on osa lähes jokaisen jokapäivästä elämää. Se sisältää laajasti käsitteitä nettikiusaamisesta ja tietojenkalastelusta hakkerointiin sekä kyberterrorismiin. Uusien teknologioiden mukana saapuu uusia mahdollisia kyberuhkia, joihin meidän tulisi varautua. Kyberturvallisuuden opetus on avainasemassa nykyisiä ja tulevia kyberuhkia vastaan taisteltaessa.

Capture The Flag on kyberturvallisuus kilpailu, jossa joukkuuet kilpailevat keskenään useissa erilaisissa haasteissa. CTF -haasteet ovat kyberturvallisuuteen liittyviä tehtäviä, joiden avulla kuka tahansa voi turvallisessa ympäristössä tutustua kyberturvallisuuteen ja opetella siinä käytettäviä taitoja. Usein haasteissa etsitään ohjelmanpätkästä haavoittuvuus, jonka avulla ohjelmasta löytää "lipun"eli vastauksen. Ymmärrettyään miten haavoittuvuus toimii, tulisi haasteen suorittajan ymmärtää myös miten siltä suojaudutaan.

Tutkimuksessa käytiin läpi kyberuhkien luokittelua sekä merkittävimpiä kyberuhkia, joiden torjumisen opettamiseen tulisi kiinnittää huomiota. Useita näitä kyberuhkia mallinetaan CTF -haasteissa. Tulevissa tutkimuksissa voitaisiin selvittää, minkä ikäisille oppilaille erilaisilta uhilta suojautumista voisi opettaa.

Haasteiden opetusmetodi pohjautuu haastelähtöiseen opetukseen, jonka on todettu motivoivan oppilaita sekä tuottavan hyviä oppimistuloksia. Myös itse CTF -haasteisiin liittyvät tutkimukset ovat osoittaneet oppilaiden kiinnostuvan huomattavasti enemmän kyberturvallisuudesta haasteisiin osallistuttua. Samalla oppilaat raportoivat itseluottamuksen sekä osaamisen kehittyneen. Lisäksi tutkimuksessa todettiin CTF -haasteiden kehittävän osallistujien käytännön taitoja huomattavasti, mutta osallistujien teorian osaaminen osoitti vain pientä kehitystä.

CTF -haasteiden sisällytys opetukseen voi tuoda mukanaan myös haasteita toteutuksesta riippuen. CTF -haasteiden implementaatio itsessään voi jo tuottaa ongelmia, sillä haasteiden sijoittaminen osaksi kurssia tai opetusohjelmaa vaatii suunnittelua. Haasteiden kehittäminen voi viedä todella paljon resursseja, mikäli opettaja aikoo suunnitella haasteet itse. Ongelmaksi voi ilmetä myös huijaaminen, mikäli haasteiden suoritus on suoraan suhteessa kurssin arvosanaan.

Tutkielmassa havaitut asiat osoittavat kuitenkin pitkälti siihen, että CTF -mallia voisi käyttää kyberturvallisuusopetuksen kehittämisessä. Aihe vaatii kuitenkin lisää tutkimusta, etenkin CTF -haasteiden käytöstä itse opetuksessa.

Lähteet

Cheung, Ronald S., Joseph P. Cohen, Henry Z. Lo ja Fabio Elia. 2011. “Challenge Based Learning in Cybersecurity Education” [kielellä English], 1–6. Copyright - Copyright The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) 2011; Last updated - 2013-01-23. Viitattu 27. maaliskuuta 2020. https://search-proquest-com.ezproxy.jyu.fi/docview/1272087912?accountid=11774.

Conti, Gregory, Thomas Babbitt ja Nelson John. 2011. “Hacking Competitions and Their Untapped Potential for Security Education”. *IEEE Security Privacy* 9 (3): 56–59. Viitattu 27. maaliskuuta 2020. https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/5772962.

Cowan, C., S. Arnold, S. Beattie, C. Wright ja J. Viega. 2003. “Defcon Capture the Flag: defending vulnerable code from intense attack”. Teoksessa *Proceedings DARPA Information Survivability Conference and Exposition,* nide 1, 120–129 vol.1. Viitattu 27. maaliskuuta 2020. https://ieeexplore.ieee.org/abstract/document/1194878.

DDTek. 2020. “A history of Capture the Flag at DEF CON”. Viitattu 27. maaliskuuta 2020. https://www.defcon.org/html/links/dc-ctf-history.html.

Eagle, Chris. 2013. “Computer Security Competitions: Expanding Educational Outcomes”. *IEEE Security Privacy* 11 (4): 69–71. Viitattu 15. huhtikuuta 2020. https://ieeexplore.ieee.org/abstract/document/1194878.

Google. 2020. “Google Trends: Cybersecurity”. Viitattu 15. huhtikuuta 2020. https://trends.google.com/trends/explore?date=today%205-y&q=Cybersecurity.

Irvine, Cynthia. 2011. “The Value of Capture-the-Flag Exercises in Education: An Interview with Chris Eagle”. *IEEE Security Privacy* 9 (6): 58–60. Viitattu 27. maaliskuuta 2020. doi:10.1109/MSP.2011.177.

Johnson, Larry, ja Samantha Brown. 2011. “Challenge Based Learning: The Report from the Implementation Project”. (Austin, Texas). Viitattu 29. huhtikuuta 2020. https://www.learntechlib.org/p/49837.

Johnson, Laurence F., Rachel S. Smith, J. Troy Smythe ja Rachel K. Varon. 2009. “Challenge-Based Learning: An Approach for Our Time”. Viitattu 15. huhtikuuta 2020. https://eric.ed.gov/?id=ED505102.

Lehto, Martti, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi ja Mirva Salminen. 2017. “Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”. Viitattu 15. huhtikuuta 2020. https://tietokayttoon.fi/julkaisu?pubid=17805.

Leune, Kees, ja Salvatore J. Petrilli. 2017. “Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education”. Teoksessa *Proceedings of the 18th Annual Conference on Information Technology Education,* 47–52. SIGITE ’17. Rochester, New York, USA: Association for Computing Machinery. ISBN: 9781450351003, viitattu 27. maaliskuuta 2020. doi:10.1145/3125659.3125686. https://doi.org/10.1145/3125659.3125686.

Parks, Raymond C., ja David P. Duggan. 2001. “Principles of Cyber-warfare”, 9:30–35. 5. Viitattu 15. huhtikuuta 2020. https://ieeexplore.ieee.org/abstract/document/6029360.

Sanastokeskus, TSK. 2018. “Kyberturvallisuuden sanasto”. Viitattu 15. huhtikuuta 2020.

Sisäministeriö. 2020. “Information networks and crime”. Viitattu 15. huhtikuuta. https://intermin.fi/en/police/cybercrime.

Solms, Rossouw von, ja Johan van Niekerk. 2013. “From information security to cyber security”. Cybercrime in the Digital Economy, *Computers Security* 38:97–102. ISSN: 0167-4048, viitattu 27. maaliskuuta 2020. doi:https://doi.org/10.1016/j.cose.2013.04.004. http://www.sciencedirect.com/science/article/pii/S0167404813000801.

Statista. 2016. “Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025”. Viitattu 15. huhtikuuta 2020. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

Turvallisuuskomitea. 2013. “Suomen kyberturvallisuusstrategia”. Viitattu 15. huhtikuuta 2020. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/.

Weimann, G., ja United States Institute of Peace. 2004. *Cyberterrorism: How Real is the Threat?* Cyberterrorism: How Real is the Threat?, nid. 31. United States Institute of Peace. Viitattu 15. huhtikuuta 2020. https://books.google.fi/books?id=sxuSAAAAMAAJ.