USB-Väylän uhat

Sami Mehtonen

2025 Laurea

Laurea-ammattikorkeakoulu

USB-Väylän uhat

Sami Mehtonen

Tietojenkäsittelyn koulutus

Opinnäytetyö

Huhtikuu, 2025

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutus
Tradenomi (AMK), tietojenkäsittely

Sami Mehtonen
USB-Väylän uhat
Vuosi 2025 Sivumäärä 47

Tämän opinnäytetyön tarkoitus on kerätä tietoa yhteen USB-väylän hotplug-hyökkäysten välineistöstä, historiasta ja asettamasta uhasta. Teoriapohja opinnäytetyössä perustuu aiempaan tutkimustyöhön, sekä kirjallisuuskatsaukseen aiheen teknologiaa käsitteleviin julkaisuihin. Tietoperustaa on hyödynnetty muodostamaan ymmärrys uhan yleistymisestä, sen teknologioista, mahdollisuuksista, sekä estämistavoista.

Tutkimuksen ja uhka-arvion osoittaa USB-väylään kohdistuvien hyökkäysten historiallisen trendin olevan kasvussa, uhan koskettaessa useita suuria yhteiskunnallisia toimintoja ja toimialoja. Lisätutkimusta vaaditaan koskien USB-väylän hyökkäyksiä, ja suojakeinoja löydettyihin haavoittuvuuksiin on tarvetta kehittää yhdessä USB-väylän varsinaisen teknologisen kehitystyön rinnalla.

Asiasanat: USB, hotplug, BadUSB, uhka-arvio

Laurea University of Applied Sciences **Abstract**
Information Processing, cybersecurity
Bachelor of Business Administration (University of Applied Science), information processing

Sami Mehtonen
USB threats
Year 2025 Pages 47

The purpose of this thesis is to collate information on the equipment, history, and threat posed by USB hotplug attacks. The theoretical foundation of this thesis is based on previous research as well as a literature review of publications covering the technology related to the subject. This knowledge base has been utilized to form an understanding of the increasing prevalence of the threat, its technologies, possibilities, and prevention methods.

The result of the research and threat assessment indicate that the historical trend of attacks targeting the USB is on the rise, with the threat impacting several major societal functions and industries. Further research is required on attacks concerning USBs, and protective measures need to be developed to address vulnerabilities found alongside the actual USB technological development itself.

Keywords: USB, hotplug, BadUSB, threat-assessment

Sisällys

1 Johdanto

USB, Universal Serial Bus (Universaali sarjaväylä), on laajalti levinnyt suosittu teknologian väyläliitännän standardi. Sen käyttö on viime vuosien – tai vuosikymmenten – aikana korvannut useita sarja- ja rinnakkaisporttien käyttökohteita. USB verrattuna edeltäjiinsä tarjoaa suuria siirtonopeuksia, helpon fyysisen kytkettävyyden ilman laitteiden uudelleenkäynnistyksen tarvetta, plug-and-play (PnP) toiminnon – joka mahdollistaa laitteen tunnistuksen ja käyttöönoton automaattisesti käyttöjärjestelmän toimesta kytkennän jälkeen, sekä kyvyn tarjota suoraan lisälaitteen tarvitsema virta USB-portin kautta. (Dung, et al., 2010, p. 1)

USB on standardi, joka löytyy lähes kaikista laitteista tänä päivänä. Sen kautta on mahdollista kytkeä erilaisia laitteita toisiinsa tiedonsiirtoa, latausta, tai kommunikaatiota varten. USB standardi sisältää määrittelyn ihmisten syötelaitteille (HID; Human Interface Device), jotka lähes kaikissa tapauksissa käyttöjärjestelmä hyväksyy käyttöön suoraan fyysisen porttiin kytkennän jälkeen. Tämä mahdollistaa sarjan USB-portteihin kohdistuvia hotplug-hyökkäyksiä, joita kutsutaan yleisnimityksellä BadUSB. (Cannols & Ghafarian, 2017, p. 66) Niiden kohteiksi voivat joutua niin tietokoneet, tabletit, älypuhelimet kuin reitittimet, älyjääkaapit tai lähes mitkä tahansa muut laitteet, joissa on minkäänlainen USB-portti.

United States Computer Emergency Readiness Team, US-CERT (Yhdysvaltojen Tietokonehätätilan valmiusryhmä), on jo yli vuosikymmenen painottanut pienikokoisten kannettavien laitteiden uhkaa niiden käytön kasvaessa. Kannettaviksi laitteiksi lasketaan niin muistitikut, mediasoittimet, tabletit kuin älypuhelimetkin. Ne kaikki asettavat kohonneen riskin datan menetykselle, datan paljastumiselle sekä verkon kautta tapahtuville hyökkäyksille. Datan menetyksellä tarkoitetaan sen katoamista tai tuhoutumista, joko tahallisen sabotaasin, tai kadonneen laitteen aiheuttamana. Datan paljastumisella tarkoitetaan informaation luovuttamista, vuotamista tai päätymistä julkiseen tietoon tai muille kuin sille tarkoitetuille tahoille. (Walters, 2012, pp. 1-2)

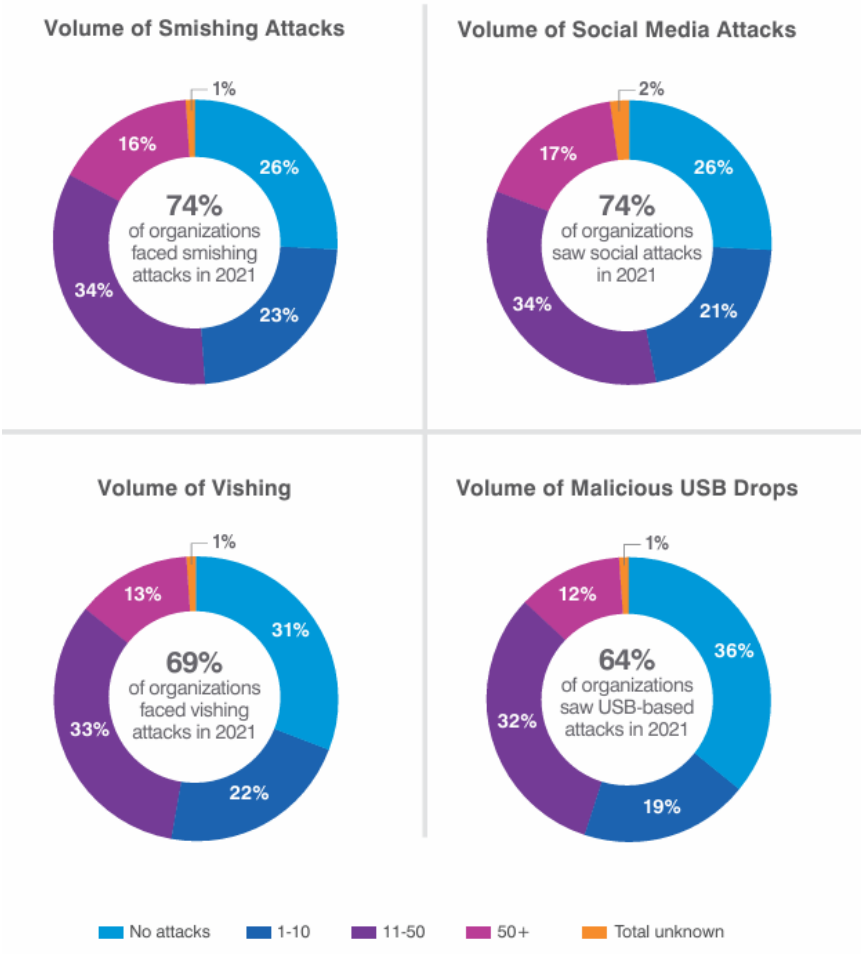
Yhdeksän kymmenestä huoltoinsinööreistä teollisuudessa käyttää USB-yhteyttä yhdistääkseen teollisuuslaitosten laitteisiin. (Honeywell, 2020, p. 3) Tietoteknisen työn maailma ylipäätään on vahvasti riippuvainen Universaalin Sarjaväylän (Universal Serial Bus), USB:n, tuomasta joustavuudesta niin tiedonsiirtoon kuin laitteiden yhdistämiseen.

Dung et al. Nimeää vuodesta 2005 lähtien yrityssektorin suurimmaksi huoleksi datan anastamisen USB-laitteilla, USB2.0 standardin yleistyttyä. (Dung, et al., 2010, p. 1) USB-väylän yleistyminen hyökkäysvektorina ei ole ainakaan vähentynyt.

Selitykseksi hyökkäysten yleisyydelle Honeywell antaa Johtajatason tiivistelmässään ”USB Security – Myths vs. Reality” neljä yksinkertaista syytä. USB-muistit ja -laitteet ovat helppoja kantaa mukana, käyttää ja niin yleisiä ettei suuri osa käyttäjistä ajattele niitä riskinä. USB-portista latautuvat laitteet voivat tehdä paljon muutakin kuin vain vastaanottaa virtaa akun latauksen nostamiseen. (Honeywell, 2020, p. 4)

USB-laitteen muoto hyökkäyskäytössä voi vaihdella, ja lähes mikä vain väylään kytkettävä laite voi olla hyökkäyskäyttöön muokattu. Tämän väitteen pohjana on, että sulautettujen järjestelmien, kuten USB-massamuistitikun sirun laiteohjelmiston uudelleenohjelmointi mahdollistaa normaalienkin USB-laitteiden muuttamisen edistyneiksi hyökkäystyökaluiksi. (Nohl, et al., 2014) Lisäksi USB-tikun löytäneet ihmiset ovat todennäköisiä yhdistämään sen tietokoneeseen, 45-98% kampusalueille levitellyistä muistitikuista päätyi tietokoneeseen kiinni, mediaaniväliajalla 6.9 tuntia muistitikun pudottamisesta (Tischer, et al., 2016, pp. 4-5). USB-laite on voinut myös vaarantua jo tehtaalla tai kuljetuslaitoksella ennen päätymistään kuluttajan, tai työntekijän käsiin. Haittaohjelmalla tartutetut, tai haitalliseen toimintaan uudelleenohjelmoidut laitteet voivat vahingossa päätyä loppukäyttäjälle. (Honeywell, 2020, p. 4) Honeywellin oma ”Industrial USB Threat Report”, teollisen alan USB uhkien raportti (johon johtotason tiivistelmä viittaa) sai selville, että 44% sijainneista oli huomannut ja estänyt vähintään yhden haitallisen tai epäilyttävän tiedoston, joka edustaa turvallisuusuhkaa. (Honeywell, 2020, p. 5)

64% kansainvälisistä organisaatioista vuonna 2021 on raportoinut USB-pohjaisia hyökkäyksiä. Vuonna 2020 tämä luku oli 15% vähemmän. (Rose, 2022) Luvut pohjautuvat Proofpoint-yrityksen vuoden 2022 ”State of the Phish” raporttiin. (Proofpoint, 2022, p. 7)



Kuvio 1: 64% yrityksistä kohtasi USB hyökkäyksiä vuonna 2021

2 Hotplug ja BadUSB esiteltynä

Hotplug-hyökkäyslaitteet ovat harmittoman ja viattoman oloisia laitteita (usein pieniä), jotka laukaisevat esiohjelmoidun iskun uhrin yhdistettyä hotplug-välineen kohdelaitteeseen. (Masters & Madisetti, 2024, p. 434)

BadUSB tarkoittaa hyökkäystekniikkaa, jossa harmittoman näköisen USB-lisälaitteen sisältämät osat tai laiteohjelmisto on muokattu hyökkäyskäyttöön. Kun USB-laite, esimerkiksi muistitikku, kytketään uhrin tietokoneeseen (tai muuhun laitteeseen), se rekisteröi itsensä HID-laitteena (Human Interface Device); HID-laitteet ovat ihmisen ohjauksen mahdollistavat lisälaitteet – näppäimistöt, hiiret ja niin edelleen. (Cannols & Ghafarian, 2017, p. 66) BadUSB:stä on myös terminä tullut yleisnimitys, ikään kuin kattotermi, USB-väylään kohdistuville hotplug-hyökkäyksille.

Alkuperäisessä Security Research Labs:in alla tehdyssä BadUSB-selvityksessä sulautettujen laitteiden mikro-ohjainten laiteohjelmiston uudelleenohjelmoinnista hyökkäyskäyttöön löydettiin noin puolet USB-siruista olevan yhteensopivia hyökkäystekniikkaan uudelleenohjelmointia varten. (Nohl, et al., 2014, p. 21)

Perinteisen BadUSB-hyökkäyksen toteuttamiseen tarvitaan Phison 2303 mikro-ohjaimen sisältävä USB3.0-muistitikku (Nicho & Sabry, 2023, p. 504).

Kierznowski & Mayes kehittivät konseptia BadUSB hyökkäyksistä sulautetuilla järjestelmillä eteenpäin kehittäessään BadUSB2.0 arviointityökalua. Toisin kuin BadUSB hyökkäys vuodelta 2014 keskittyi USB laiteohjelmistoon, keskittyy BadUSB2.0 itse USB-johtoon. (Kierznowski & Mayes, 2015, p. 2)

Honeywellin GARD-tiimi on havainnut vuoden 2024 tutkimusasiakirjassa ”Honeywell GARD USB Threat Report 2024” suurimman käytössä olevan kategorian olevan skriptaus ja komentorivin hyödyntäminen. Löydöksissään he toteavat myös suurimman osan edistyneistä uhista hyödyntävän tietokoneiden olemassa olevia ominaisuuksia, antivirusohjelmien havaittavissa olevien näkyvien erillisesti asennettujen haittaohjelmien sijaan. (Honeywell, 2024, p. 5) Tähän tehtävään BadUSB-tekniikat HID-teeskentelyhyökkäyksillä ovat tehokkaita ja vaikeasti estettäviä työkaluja. GARD on Honeywellin Global Analysis, Research and Defense-tiimi (Maailmanlaajuinen Analyysi, Tutkimus ja puolustustiimi). (Honeywell, 2024, p. 2)

3 Historialliset hyökkäykset

Hacksaw oli Hak.5-organisaation yhteisön tuottama projekti, jossa kehitettiin konfiguroitava flash-muistitikku; ”Universal Serial Bus (USB) Hacksaw”. Laitteen tarkoitus oli tuottaa USB-muistitikku, joka sisältää CD-ROM (compact-disc read-only memory) levyosion. Tähän prosessiin tarvittiin SanDisk-valmistajan U3-standardiin (Anderson & Anderson, 2010, p. 6) yhteensopiva muistitikku, jonka konfigurointiin käytettiin muokattua versiota valmistajan LaunchPad-ohjelmistosta. U3-älylevystandardin kehitti yhteistyössä SanDisk ja M-Systems vuonna 2005. Näin flash-muistilliselle USB-muistitikulle saatiin windows-järjestelmän tunnistama toinen levyosio, josta voitiin käynnistää automaattinen isku autorun.inf-tiedostosta. (Anderson & Anderson, 2010, pp. 1, 5)

Samaa autorun.inf-tiedoston automaattista käynnistystä käytettiin monissa aikakauden asennusohjelmissa, sekä esimerkiksi USB-modeemien ajureiden asentamisessa tietokoneeseen kytkennän yhteydessä USB-väylän kautta.

Ennen Hacksaw-laitteen kehitystä tyypillisin USB-väylän hyökkäys oli tiedostojen suora kopioiminen flash-muistille hyökkääjän toimesta. Hacksaw kuitenkin asensi haitallisen ohjelmistonsa

suoraan tietokoneen luontaisten tiedostojen joukkoon, toimien jatkuvana sisäisenä uhkana, jonka laukaisemiseen vaaditaan vain uuden flash-muistitikun kytkeminen tietokoneeseen. Tietokoneen USB-laiteneuvottelun aikana Hacksaw:n infektoima pääte toteuttaa Hacksaw-hyökkäyksen oman autorun.inf tiedoston ajamisen (esimerkiksi muistitikun ajurien sijasta), jolloin tiedostot voivat joutua varastetuiksi. (Anderson & Anderson, 2010, p. 17)

”USB Switchblade” on Hacksaw:n tapaan Hak.5-yhteisön aikaansaannos. USB Switchblade voi aiheuttaa enemmän vahinkoa järjestelmään kuin edellä mainittu Hacksaw. USB Switchblade vaatii toiminnallisuuteensa järjestelmänvalvojan suoritusoikeudet. Laitteen tarkoitus oli mahdollistaa Windows-järjestelmän tai sitä ympäröivän verkon tiedon kerääminen talteen. Laitteen modulaarinen luonne mahdollisti kehittäjien uusien työkalujen lisäämisen. USB Switchbladea voidaan pitää enemmänkin tapana kerätä lukuisat järjestelmänvalvojien tiedonkeruutyökalut yhteen käytännölliseen pakettiin, kuin omana täysin uutena novellina keksintönään. (Anderson & Anderson, 2010, p. 27)

Laitteen sisältämät ohjelmistot olivat alun perin järjestelmänvalvonnan käytössä, järjestelmien – tai niiden datan – suojaamiseksi. Ohjelmistojen mahdollistama salasanojen, avainten ja muiden järjestelmän kriittisten elementtien palauttaminen ja esille tuominen voi hyödyttää myös hyökkääjiä. (Anderson & Anderson, 2010, p. 31)

Stuxnet-matoa kutsuttiin 2015 Royal Holloway:n artikkelissa BadUSB2.0-työkalusta ”herätyskutsuksi” USB:n ja sulautettujen laitteiden käytöstä kaikkien järjestelmien, myös ilmaraotettujen, vaarantamiseen. (Kierznowski & Mayes, 2015, p. 2) Ilmaraotetut (air-gapped) verkot ja laitteet on kytketty erilleen laajemmasta verkosta. Suoraa yhteyttä eristetystä verkosta muihin ympäröiviin verkkoihin ja laitteisiin ei siis ole lainkaan.

Kuten mitkä tahansa muutkin tavat altistaa järjestelmä haittaohjelmille, myös USB-väylä tarjoaa keinon syöttää haitallista koodia tai haittaohjelmia itsessään suoraan kohdelaitteelle – ja sitä kautta kohdeverkkoon. Haittaohjelmien tuottamat riskit vaikuttavat niin datan tuhoutumiseen, resurssien kulumiseen, ajankäyttöön, liikesalaisuuksien paljastumiseen sekä henkilökohtaisesti tunnistettavan datan vuotamiseen. (Anderson & Anderson, 2010, p. 88)

4 Teknologia 1: USB

USB spesifikaatio kehitettiin vuonna 1996. Ensimmäinen versio tunnetaan nykyään USB1.0-versiona. USB standardoitiin USB-Implementers Forum:in toimesta, jolloin syntyi USB-IF – teollisuudenalan elin, joka sisällytti useita tietokone- ja elektroniikka-alan tunnetuimpia ja suurimpia vaikuttajia. (Anderson & Anderson, 2010, p. 5)

USB-spesifikaatiosta on 4 pääversiota – versiot USB 1.0, USB 1.1, USB 2.0 sekä USB 3.0. USB 1.0-version aikaan oli vain vähän USB-laitteita, ja väylän tuki oli heikoimmillaan. USB-versio 1.1 lisäsi uuden tiedonsiirtotekniikan, interrupt OUT-komennon. USB 2.0 spesifikaatio vuonna 2000 julki tuotu versio, joka nosti tiedonsiirtonopeuksia 480Mbps-luokkaan. Tämä mahdollisti paitsi nopeamman tiedonsiirron, myös vaativampien lisälaitteiden yhdistämisen. USB 2.0-spesifikaatio on yhteensopiva vanhempien USB 1.0-laitteiden ja porttien kanssa. USB 2.0-versiota voi pitää käännekohtana, jolloin USB-väylän hyökkäykset alkoivat jalostua hienostuneemmiksi. USB 3.0-versio julkaistiin vuonna 2008. USB 3.0-version tuoma lisäominaisuus oli kaksiväyläisyys – väylä koostui kahdesta rinnakkaisesta väylästä fyysisesti, kymmenkertaistaen USB 2.0-version nopeuden. USB 3.0-versio mahdollistaa kahden väylänsä ansiosta myös tiedonsiirron kaksisuuntaisesti yhtä aikaa. Myös väylään kytkettyjen laitteiden virransaantia ja tiedonsiirtotehokkuutta nostettiin versiopäivityksen myötä. (Axelson, 2009, pp. 11-14)

Tässä opinnäytetyössä keskustellut hyökkäykset ja tekniikat sijoittuvat 2000-luvulle, joten niiden käytös varhaisilla USB-versioilla on epävakaa tai toimimaton. Tästä syystä USB versioihin ei oteta kantaa hyökkäyksien toimivuutta arvioidessa tässä opinnäytetyössä. USB-spesifikaatio erittelee kolme määritelmää, joiden ymmärtäminen on väylään kohdistuvissa hyökkäyksissä olennaista: Toiminnallisuus, laite sekä portti. Näiden lisäksi väylän toimintaan liittyvissä prosesseissa on useita termejä, jotka on spesifikaatiossa nimetty: Laitetunnistus – eli enumeraatio, laitekuvaaja - eli device descriptor, sekä kuvaajan tyyppitunniste – eli type.

Toiminnallisuus on sarja toisiinsa liittyviä rajapintoja, jotka toteuttavat jonkin toiminnallisuuden. Kaiuttimet, hiiri, datan siirrettävä tallennustila ovat kaikki toiminnallisuuksia. Yksi laite voi sisältää useita toiminnallisuuksia – tulostin/skanneri, musiikkisoitin/tallennustila ja niin edelleen. (Axelson, 2009, pp. 18-19)

Laitteella tarkoitetaan USB-spesifikaation yhteydessä loogista tai fyysistä entiteettiä, joka toteuttaa yhtä tai useampaa toiminnallisuutta. Lisälaitteet, jakajat ja keskittimet ovat kaikki laitteita. Jokaisella laitteella on yksilökohtainen osoite, jonka isäntä (tietotekninen laite, jonka väylään laitteet on kytketty) jakaa väylään kytketyille laitteille. (Axelson, 2009, p. 19)

Laiteportti on tietokoneen osoitteella varustettu sijainti, joka on yhteydessä sitä ympäröiviin piireihin. Portin piirien päätöspiste voi olla irrotettava johtoliitäntä, tai kiinteästi kytketty laite. Isäntäsovellukset eivät voi suoraan kommunikoida USB-porttien kanssa, vaan toteuttavat toimintonsa laitteille osoitettujen ajureiden kautta. USB-isäntäohjain voi sijaita keskusprosessorin saavutettavien porttien kanssa sarjassa, mutta nämä portit ovat erillään itse väyläporteista USB-spesifikaatiossa. (Axelson, 2009, p. 19)

Laitetunnistus USB-väylässä toimii seuraavasti: Keskitin käynnistyy, ja antaa tiedon kaikista kytketyistä USB-laitteista isäntälaitteelle. Prosessia kutsutaan enumeraatioksi. Prosessin aikana isäntälaite määrittää väylälle oikean nopeuden, nimittää osoitteen laitteelle ja pyytää

laitteelta lisätietoja. Jos väylään kytketty laite poistetaan tai kytketään uudelleen, tekee keskitin isännän tietoiseksi tästä – ja isäntä suorittaa enumeraatio-prosessin uudelle laitteelle, vastaisesti poistaen irti kytketyt laitteet sovelluksille saatavien laitteiden listauksesta. (Axelson, 2009, p. 20)

Axelson kuvaa USB2.0-laitteen enumeraation erittäin yksityiskohtaisesti. Karkeisiin askeliin jakaen vaiheet ovat (Axelson, 2009, pp. 90-95):

1. Käyttäjä liittää uuden laitteen isäntäjärjestelmään
2. Järjestelmän Keskitin havaitsee USB-laitteen
3. Isäntäjärjestelmä saa tietää uudesta laitteesta
4. Keskitin havaitsee onko laite alhaisen- vai korkean nopeuden laite
5. Keskitin nollaa laitteen
6. Isäntälaite saa tietää tukeeko täyden nopeuden (full speed) laite korkeaa nopeutta (high speed)
7. Keskitin muodostaa signaalipolun laitteen ja keskittimen välille
8. Isäntälaite pyytää maksimi pakettikoon kuvaajaa (Descriptor)
9. Isäntälaite määrittää osoitteen laittelle
10. Isäntälaite saa tietää laitteen ominaisuuksista ja kyvyistä
11. Isäntälaite määrittää ja lataa käyttöön laiteajurin (device driver)
12. Isäntälaitteen laiteajuri valitsee konfiguraation

USB Descriptor, eli laitekuvaaja on datarakenne, jonka avulla isäntälaite käsittelee USB-väylään kytkettyä laitetta. Kuvaajia on useita tyyppejä, jotka mahdollistavat eräänlaiset ”asetuspaketit” jotka väylälaite voi kommunikoida isäntälaitteelle. USB standardi määrittää, että väylälaitteiden on varastoitava laitekuvaajansa, ja vastattava isäntälaitteen pyyntöihin laitekuvaajasta poikkeuksetta. (Axelson, 2009, p. 97)

Kuvaajan tyyppi määrittää mitä tyyppiä itse kuvaaja on; se voi olla laitekuvaaja, asetuskuvaaja, merkkijono, nopeuden määrittäjä, virranpyyntö tai muita lukuisista vaihtoehdoista. Nämä erilaiset kuvaajan tyypit määrittävät mitä dataa laitekuvaaja sisältää, sekä mitä dataa isäntälaite väylälaitteelta pyytää. (Axelson, 2009, pp. 97-99)

Kuten laitteen enumeraation askelista ja kuvaajien vaihteluista on nähtävillä, jo pelkkä USB-spesifikaatio sisältää monta askelta, joissa hyökkääjä voi puuttua tilanteeseen tai muokata isäntälaitteen ja usb-lisälaitteen välistä kommunikaatiota.

4.1 HID

HID on laiteluokka ihmisinteraktiolaitteille. HID-laitteet (Human Interface Device) sisältävät lisälaitteet, joiden kautta tietokone voi lukea ja reagoida ihmisten syötteisiin. HID-luokka sisältää siis mm. hiiret, näppäimistöt, osoituslaitteet, peliohjaimet. Viivakoodinlukijat voivat toimia HID-laitteina näppäimistönä, jos viivakoodit edustavat näppäinsyötteiden emulointia. Jotkin näytöt käyttävät HID-laiteluokkaa asetusten määrittelemisessä. HID-luokan ajurit ovat sisältyneet Windows-käyttöjärjestelmiin (sekä muihin käyttöjärjestelmiin) USB-spesifikaation varhaisimmista vaiheista asti. (Axelson, 2009, p. 180) Luokan yleisyys ja laaja tuki valmistajakohtaisille erityistoiminnoille mahdollistaa tässä opinnäytetyössä mainituista hyökkäyksistä suurimman osan.

4.2 CCB painikkeet

CCB viittaa termiin Consumer Control Button(s). Consumer Control on alaosio USB-toiminnallisuudesta, jonka avulla käyttäjä voi aktivoida ohjelmistoja ja toimintoja yhdellä painalluksella; esimerkiksi joissain näppäimistöissä olevat niin kutsutut ”mediapainikkeet”. Toisin sanoen, yksittäinen näppäin, jota painamalla aukeaa tietty sovellus (esimerkiksi sähköposti), tai aktivoituu tietty toiminto (esimerkiksi Äänenvoimakkuus Päälle/Pois-pikakäsky), kyseessä on Consumer Control-luokan alle kuuluva toiminto. Tätä toiminnallisuutta hyväksikäytettiin USB HID & Run-hyökkäyksen suunnittelussa, kuvauksessa ja esityksessä, jonka dokumentaatio löytyy käyttäjänimen piraija github-sivulta. (Alm & Aaris-Larsen, 2023)

Tiimin, joka kehitti USB HID & Run-hyökkäyksen tavoitteina oli emuloida CCB-toimintoja mikro-ohjaimella, määritellä miten CCB-painikkeet eroavat normaaleista Windows-pikakomennoista sekä tutkia miten CCB-painikkeet mahdollistavat hyökkäyksiä kioskimallisiin laitteisiin; esimerkiksi pankkiautomaatit ja muut julkisille paikoille sijoitetut ”suljetut” järjestelmät. (Alm & Aaris-Larsen, 2023)

CCB-hyökkäyksiä voi estää Windows-laitteilla rajoittamalla Human Interface Device-palvelun päällä oloa. Powershell komennolla ’sc config hidserv start=disable’ voidaan kioskikäytössä estää palvelun käynnistyminen, joka sulkee näppäimistön pikanäppäinten toiminnot pois. Tämä estää CCB-pohjaisen hyökkäysvektorin käytön laitetta vastaan. (Alm & Aaris-Larsen, 2023)

Tiimi, joka tutki CCB-painikkeita kioskeihin kohdistuvassa hyökkäyskäytössä kehitti myös Flipper Zero laitteelle ”USB Consumer Control”-sovelluksen, joka mahdollistaa Flipper Zero laitteella medianäppäinten emuloinnin.

5 Teknologia 2: Hyökkäyslaitemallit

USB Rubber Ducky on Hak5:n kehittämä näppäimistöä imitoiva HID (Human Interface Device) hyökkäyslaite. Se toteuttaa sille tekstitiedostona DuckyScript-skriptauskielellä annetut ohjeet, syöttäen näppäimistösyötteinä ohjeistetut painallukset. USB Rubber Ducky muistuttaa ulkoisesti merkitsemätöntä USB-muistitikkua. Sisäisesti se muistuttaa microDS-muistikorttiadapteria, USB-A malliseen väylään. Laite voi siis hämätä maallikkoa sen sisäistä piirilevyäkin tarkastellessa. (Queppet, 2018, pp. 1-2)

Laitteessa on värillinen LED-valoilmaisin, jonka avulla voi viestiä käyttäjälle, milloin skripti on ajettu loppuun, eli suoritettu. Laitteessa on myös painike, jonka avulla voi käsin uudelleen aloittaa hyökkäysskriptin suorituksen, mikäli suoritus halutaan ajoittaa, tai sen suoritus epäonnistui. (Queppet, 2018, pp. 3-4)

Laitteen hyökkäys toimii täten: Laitteen prosessori on suunniteltu käynnistämään toiminnot automaattisesti käynnistyksen yhteydessä (laitteen saadessa virtaa sen kytkettyä USB-porttiin). USB Rubber Ducky rekisteröi itsensä tietokoneelle HID näppäimistönä, ja antaa muistikortilla olevan skriptin mukaisesti komentoja tietokoneelle, matkien ihmiskäyttäjän kirjoitusta näppäimistöllä. (Queppet, 2018, p. 1; 5)

Rubber Duckyn sisältämä mikro-ohjainpiiri on laiteohjelmistoltaan hyvin uudelleenohjelmoitava. Laitteen ominaisuuksien laajennuksia auttaa JTAG (Joint Test Action Group (Gallagher, 2020)) liitäntä, jonka kautta laitteen sisäisiä yhteyksiä voi testata. Laitteen laiteosia voi siis muokata, testata ja joitain jo olemassa olevia laitekomponentteja voidaan ohjelmoida ohjelmistoiltaan uudelleen JTAG-liitännän kautta. Rubber Ducky-laitteeseen voidaan lisätä laitteistoa, sekä ohjelmistoja. (Queppet, 2018, p. 6)

Bash Bunny on laiteimplantti, joka emuloi useita luotettuja laitteita: gigabit Ethernet sovitinta, sarjaporttia, muistitikkua ja näppäimistöä – useampaa yhtäaikaisesti (Blue Goat Cyber, 2025). Bash Bunny laitteen alkuperäinen kehittäjä on Hak5. Laite juontaa juurensa USB Rubber Ducky-implanttiin (Blue Goat Cyber, 2025).

Laite pystyy myös toimimaan tietokoneeseen secure shell-yhteydellä (SSH) kytkettynä erillisenä linux-tietokoneena. Laite pystyy jakamaan isäntälaitteen verkkoyhteyden, ja myös luomaan oman valeverkkonsa, jonka kautta isäntälaitteen voi yhdistää haittaohjelman lailla. (Hak5, 2024)

Laitteessa on microSD-muistikorttipaikka skriptien ja tiedostojen varastointiin. Tiedostotilan lisäksi laitteessa on kytkin sen tilanhallintaan, laitteessa on kaksi kytkimeen sidottua ”muistipaikkaa” hyökkäysskripteille. Laitteen käytön avustamiseen laitteessa on RGB-LED valo, joka toimii indikaattorina laitteen tilasta. (Hak5, 2024)

Laite tukee erityissarjaa DuckyScript-komentoja. Tämän lisäksi laite voi ohjausskriptissä kääntää suoraan DuckyScript komennot, erityiskomennolla QUACK; QUACK toimii käskynä kääntää sitä seuraava DuckyScript-komento komennoksi, jota Bash Bunny tukee. (Hak5, 2024)

Bash Bunny-laitteen suurimpia vahvuuksia on datan suora anastaminen. Laite pystyy teeskentelemään sallittuja USB-laitteita, ja suorittamaan monimutkaisia hyökkäyksiä, joiden kautta se voi kopioida kokonaisia levyasemia sisäänrakennettuun muistiinsa, jos ne ovat riittävän pieniä mahtuakseen siihen. (Blue Goat Cyber, 2025)

O.MG-Cable on autotallissaan projektin alun perin luoneen MG:n (pseudonyymi, alias) luoma naamioitu USB-implantti. Vuonna 2019 hän alkoi kehittämään harrasteprojektistaan kaupallista tuotetta, saaden kehitystyön taakse kokonaisen tiimin. Tuote päätyi myöhemmin samana vuonna myyntiin Hak5-yrityksen verkkokauppaan. (mg, 2019)

Laitteesta on useita versioita, Elite ja Basic toiminnallisuuden kannalta; liitännän kannalta USB-C, USB-A, Lightning, sekä USB-micro liittimillä. Myös muovikuoren väritys on vaihdettavissa. (Hak5, 2025)

O.MG-Cable Hak5:n omien tuotetietojen mukaan omaa runsaasti samankaltaisuutta NSA:n COTTONMOUTH-I implanttiin, he viittaavat tuotteen hinnassa NSA-implantin 20,000 USD hintaan perustellakseen omaa hinnoitteluaan. (Hak5, 2025) COTTONMOUTH-I implantti löytyy tämän laitelistan loppupäästä.

Laite tukee DuckyScript-skriptausta versiolla DuckyScript 2.0 (MG, 2023). Laite voi toimia näppäinpainallusten syöttäjänä, matkien näppäimistöä ja ihmisen tekemiä syötteitä kohteeseen. Laite pystyy matkimaan myös hiiren toimintaa ja liikuttamaan kursoria näytöllä. Laitteessa on useita muistipaikkoja hyökkäysskripteille, ja sitä on mahdollista hallita etänä. Laitteen hyökkäyksen ajoituksen voi asetuksista säätää riippuvaiseksi esimerkiksi tietyn Wi-Fi-tukiaseman läsnäolosta, tai muista Geofencing-tyyppisistä aluerajoituksista riippuen. (Hak5, 2025)

Flipper Zero on visuaalisesti ulkoisesti lelumainen signaalianalyysin monitoimityökalu. Sillä voi analysoida ja hyökätä monien teknologioiden kautta; muun muassa RFID, infrapuna, tietyt radiotaajuudet (n.s. Sub-GHz-taajuudet, alle gigahertsin taajuudet), sekä USB-väylä. (Flipper, 2025)

Laitteessa on avonaiset GPIO-nastat (General Purpose Input/Output), joiden kautta sen toiminnallisuutta voi laajentaa, tai yhdistää sen suoraan aktiiviseen piiriin käyttöä varten. Laitteessa on painikkeita sekä pieni yksivärinen LCD-näyttö sen käyttöä varten. Status-LED-valo antaa yksinkertaista palautetta käyttäjälle, kuten myös värinämoottori fyysisesti tuntuvaan värinällä luotuun palautteeseen. MicroSD-muistikorttipaikka mahdollistaa tiedostojen (ja skriptien) tallentamisen suoraan laitteelle. (Flipper, 2025)

Bad USB-käytössä laite mahdollistaa perustason hyökkäyksien lisäksi joitain omia laajennettuja lisäkomentojaan. Virallisesti laite käyttää laajennettua Ducky Scriptiä (johtuen sen omista lisäkomennoista). Ducky Script versioiden tuki loppuu laitteella kuitenkin Ducky Script 1.0-versioon. (Flipper, 2025)

BadUSB2.0-laitteet ovat muokattuja USB-laitteita, joiden mikro-ohjaimen laitekoodia muuttamalla annetaan niille kyky matkia muita laitteita implanttikäytössä. Se voi esiintyä näppäintallenteita kaappaavana laitteena, näppäimistöä matkivana laitteena, tai alkuperäisen BadUSB:n mallisena laitteena. Näiden eri tekniikoiden yhdistely reaaliajassa mahdollistaa useiden hyökkäystapojen analysoinnin ketjutetuissa hyökkäyksissä. Ohessa on taulukko (TAULUKKO BBP20) BadUSB2.0-tekniikoista, jotka on onnistuttu demonstroimaan laboratorioympäristössä kehitystyön yhteydessä. (Kierznowski & Mayes, 2015, pp. 3-4) Vastaavia hyökkäyksiä on ollut kenttäkäytössä aktiivisten ammattitoimijoiden osalta, yksi esimerkki tästä on Cottonmouth-tuoteperhe.

Ohessa lista BadUSB2.0-tekniikoista, jotka on demonstroitu toimiviksi Kierznowski:n ja Mayes:in toimesta (Taulukko 1):

Taulukko 1: Demonstroidut BadUSB2.0-tekniikat

Tekniikka	Tarkoitus
Eavesdropping	Näppäinpainallusten nauhoitus
Sending Keystrokes	Näppäinpainallusten lähettäminen
Replaying Logon Credentials	Kirjautumistunnusten uudelleentoisto
Character Substitution Attack	Reaaliaikainen näppäimistön ja isäntälaitteen välisten viestien muokkaaminen
Data Exfiltration	Datan ulosvienti huomaamattomasti HID-protokollalla
Interactive Shell over USB-HID	Interaktiivinen komentokehoite

BadUSB	BadUSB-laitteen tunnistautumisen uudelleenrekisteröinti eri laitteena

5.1 NSA ANT-Catalogue 30C3

ANT on NSA:n jaosto, jonka tehtävänä on tuottaa implantteja sekä valvontateknologiaa Five Eyes valtioille, NSA:lle (Amerikan Kansallinen Turvallisuusvirasto) itselleen, sekä GCHQ:lle (Iso-Britannian tiedusteluviranomainen). ANT Catalogue on vuodelta 2008 salaiseksi luokiteltu dokumentti, jonka 50-sivua sisältävät mm. Cottonmouth-tuoteperheen, jota tässä käytetään esimerkkinä hotplug hyökkäysten varhaisesta kehityksestä. (Digital Citizenship and Surveillance Society, 2015)

NSA:n ANT USB 30C3-katalogi sisältää tietoja useista omana aikanaan ennenkuulumattoman edistyneestä työkalusta – nimeltään Cottonmouth-sarja. Käytän laitteiden kuvauksen lähteenä itse ANT katalogia, että Jacob Applebaumin 30 joulukuuta 2013 tekemää saksankielistä kuvausta, joka löytyy Archive.org-kopion alusta. (Applebaum, 2013)

Seuraavat laitteet ovat NSA:n kenttävälineiden ANT-Catalogue 30C3-katalogista löytyneitä laiteimplantteja.

ANT Katalogi itsessään kuvaa ensimmäistä Cottonmouth-laitetta, CM-I USB laiteimplantiksi, joka tarjoaa langattoman sillan kohdeverkkoon, ja voi ladata haittaohjelmia kohdetietokoneille. Se kykenee myös luomaan langattoman yhteyden toiseen Cottonmouth-implanttiin. (Applebaum, 2013, p. 1)

CM-I toimii ”persistenttinä ohjelmistona”, eli se luo kestävän palautettavan yhteyden kohteeseen. Sen kautta voidaan sekä infiltroida, eli syöttää laitteeseen sisään dataa ja komentoja, että exfiltroida tietoa, eli ladata sitä ulos kohdetietokoneesta. (Applebaum, 2013, p. 2)

Toinen Cottonmouth-laite, CM-II mahdollistaa tietokoneen etähallinnan. Sen parina toimii tietokoneen kotelossa oleva radiomoduuli. Tämä yhdistelmä mahdollistaa merkittävästi pidemmän kommunikaatiomatkan. (Applebaum, 2013, p. 1)

Cottonmouth-II on USB Hardware Host Tap, eli laitepohjainen salakuunteluväline USB-väylään. Sen etu CM-I laitteeseen verrattuna on kohdelaitteeseen piilotettu pitkän kantaman radiotoistin, long haul relay. (Applebaum, 2013, p. 3)

Kolmas sarjan laite, Cottonmouth-II, CM-II, on luotu yhteyden muodostamiseen verkosta eristettyihin koneisiin. Sen parina toimii tietokoneen kotelossa oleva radiomoduuli. CM-III implantti voi muodostaa yhteyden operaattoriin, tai muihin Cottonmouth-laitteisiin. Sen käyttö

mahdollistaa offline-toiminnassa oleviin, verkosta pois kytkettyihin tietokoneisiin hyökkäämisen etäyhteyden avulla. (Applebaum, 2013, p. 1)

CM-III yhdistää aiempia ominaisuuksia, ja vaikuttaa katalogin kuvauksen perusteella olevan viimeistellympi laite kuin CM-II. (Applebaum, 2013, p. 4)

Firewalk on implantti, jonka fyysisenä muotona on joko Ethernet-portti, tai USB-portti. Sen sisältämät komponentit mahdollistavat datan sekä liikenteen portin läpi kaappaamisen. Sen kautta voi myös syöttää aktiivisia hyökkäyksiä radioyhteyden välityksellä. (Applebaum, 2013, p. 5)

6 USB-väylä hyökkäyskanavana

USB-laitteet ovat yleisiä ja viattomana pidettyjä tunnettuuden takia. USB ekosysteemi itsessään on monimutkaisuutensa takia niin hedelmällinen kenttä uusien hyökkäyksien kehittämiseen, kuin vaikeasti suojattava monimutkaisen rakenteensa takia. Käyttöjärjestelmät sisältävät syvälle ulottuvat tekniset rakenteet, jotka mahdollistavat USB-väylän monipuolisen käytön – ja hyväksikäytön. (Nicho & Sabry, 2023, p. 503)

Laitteet, jotka viestivät tietokoneelle olevansa HID-laitteita ovat poikkeuksellisen suora hyökkäystapa; HID-laitteisiin kuuluvat näppäimistöt ja hiiret ovat ihmisten käyttämiä välineitä, joilla tietokoneita käytetään. HID-laitteita tarvitaan monissa toimistoissa päivittäisten tehtävien hoitoon. Ne ovat tästä syystä suurimmassa osassa käyttöjärjestelmiä suoraan hyväksyttyjä ohjelmiston tasolla, käyttöjärjestelmän itsensä on vaikea tunnistaa mikä on oikea näppäimistö, mikä vain näppäimistöä teeskentelevä laite. (Cannols & Ghafarian, 2017, p. 67)

Näppäimistön teeskentelyä tehokkaasti rajoitetuista ympäristöistä pakenemiseen käyttää hyökkäysluokka ”USB HID & Run”, joissa mikro-ohjainta käyttäen emuloidaan CCB-painikkeita, eli Consumer Control Button-näppäimiä. Tällaisesta rajatusta ympäristöstä pakenemista kutsutaan ”Breakout”-tekniikaksi. Näitä näppäimiä löytyy monista laitteista, esimerkiksi kannettavien tietokoneiden painikkeet, jotka muuttavat äänenvoimakkuutta, tai sulkevat kameran tai estävät kosketushiirilevyn käytön ovat CCB-näppäinten kategoriaan kuuluvia. Tällaisia medianäppäimiä käyttämällä on USB HID & Run-hyökkäyksiä tutkinut tiimi paennut rajoitetuista kioskitietokoneiden ympäristöistä. Yleinen käyttö on esimerkiksi syöttää ”lähetä eteenpäin sähköpostilla” tai ”tulosta” komennot CCB-näppäinkoodilla, jolloin sähköpostin tai tulostuksen esikatselu aukeaa joissain tapauksissa. Tässä uudessa näkymässä voidaan hyödyntää olemassa olevia haavoittuvuuksia laitteen rajoituksista ulos pääsemiseen. Julkisilla paikoilla olevat kioskit voivat näitä hyökkäyksiä käyttäen tarjota helposti lähestyttävän fyysisen tietokoneen, jonka avulla suorittaa iskuja ja aiheuttaa haittaa. (Alm & Aaris-Larsen, 2023)

Syynä USB-väylään kohdistuvien iskujen tehokkuuteen voidaan osittain pitää HID-laiteluokan asemaa käyttäjän näkökulmasta itsessään. HID-laitteet (ihmisiltä komentoja vastaanottavat laitteet, näppäimistöt, hiiret jne.) eivät itsessään luonnollisesti ole haitallisia, joten niiden ajureihin ei normaalisti kohdistu käyttöjärjestelmän tasolla tarkistuksia. Yhdistyttyään tietokoneeseen voi HID-laitteeksi tunnistautunut USB-laite kytkeä itsensä tietokoneeseen näppäimistönä, hiirenä tai muuna laitteena. (Nicho & Sabry, 2023) Tietokoneen havaitsema identiteetti riippuu laitteen itsensä välittämästä tunnisteesta.

Laitteen teeskennellessä USB-verkkokorttia se voi anastaa dataa verkkoyhteyden kautta muokkaamalla tietokoneen DNS-asetuksia (Domain Name Server, nimipalvelin), sekä DHCP-asetuksia (Dynamic Host Configuration Protocol). (Nohl, et al., 2014) Tällaisella manipulaatiolla kohteen lähettämät DNS-pyynnöt uudelleenohjataan hyökkääjän DNS-palvelimelle (Cannols & Ghafarian, 2017, p. 67).Täten on mahdollista, että käyttäjä pääsee esimerkiksi verkkopankkiin, mutta tunnukset syötetään väärälle palvelimelle; hyökkääjän palvelimelle. Verkko vaikuttaa toimivalta tässä tapauksessa, ja itse sivu on oikea. (Nohl, et al., 2014)

Laajemman skaalan tietoverkkoympäristöissä yleisessä Windows-arkkitehtuurin Group Policy Object konfiguraatiossa löydettiin heikkouksia Nichon ja Sabryn toimesta heidän tutkimuksessaan sivukanavahyökkäyksistä monikerroksisen suojauksen läpi USB-väylää käyttäen (”Bypassing Multiple Security Layers Using Malicious USB Human Interface Device”). Haavoittuvuus koskee Group Polic Object-sääntöä, joka kieltää kaikkien irrotettavien tallennustilojen, kuten USB-muistitikkujen, käytön ja toiminnallisuuden. Tämä ”deny access to all removable storage classes”-vaihtoehto ei estä irrotettavia lisälaitteita, kuten näppäimistöjä ja hiiriä. HID-laitteina esittäytyvät haitalliset USB-laitteet pysyvät siis toiminnassa tämän suojatoimen jälkeen. (Nicho & Sabry, 2023, p. 503)

USB-väylän hyökkäyksiä estäviä tekijöitä on kehitetty. Verkon pääsynhallintajärjestelmät ja pääteasemien turvallisuus ovat kehittyneet. Myös puolustuskeinoja USB-väylän hyökkäyksiin on keretty kehittää jo vuoden 2014 BadUSB-hyökkäyksen ja vuoden 2015 BadUSB2.0-työkalun välissä. (Kierznowski & Mayes, 2015, p. 3)

RubberDucky tyyppisten BadUSB-hyökkäysten toteuttamiseksi tarvitaan fyysinen pääsy saada laite kytketyksi (joko hyökkääjän tai laitteen käyttäjän toimesta) kohteeseen. Laitteen käyttämä haittaohjelma pitää myös kirjoittaa, tai hankkia verkosta kohteen ja tarkoituksen mukaisesti. (Cannols & Ghafarian, 2017, p. 67) Joissain tilanteissa tämä voi vaatia merkittävää työpanosta hyökkääjän toimesta.

7 USB väylän tunnetuimmat hyökkäystekniikat

Benoit Badrignans piti 2012-2013 SSTIC konferenssissa presentaation, jossa hän toi esille USB-väylään kytkettävien laitteiden hyökkäystekniikoita (Badrignans, 2013, p. 98). Hänen alun perin ranskankielistä tutkimustuloksiansa esittelevää työtään käytti Stéphanie Blanchett artikkelissaan ”BadUSB, the threat hidden in everyday objects” (Blanchet, 2018). Tätä osin Badrignansin ranskankieliseen konferenssiasiakirjaan pohjautuvaa käännöstä käyttäen, sekä Blanchettin työstä kuviota lainaten ja sen kääntämällä, voidaan haitallisten USB-laitteiden hyökkäykset jakaa ainakin viiteen alakategoriaan: Hyökkäykset USB ajureihin (Attacks on USB drivers), Hyökkäykset HID-tunnistuksen kautta (Attacks via HID), Hyökkäykset USB massamuistin kautta (Attacks via USB mass storage), Datan hankkiminen isäntä-järjestelmästä (Data Acquisition on the host system), sekä DMA hyökkäykset ja Väylän vakoilu (Bus Snooping). (Blanchet, 2018, p. 3)

Taulukko 2: USB-väylän laitteiden hyökkäystekniikoita

Haitallisten USB-laitteiden kautta hyökkäys (B. Badrigans, 2012)
Hyökkäykset USB-ajureihin
Käyttöjärjestelmän rajoitukset haitallisen laitteen avulla poistamalla mahdollistuu luku- ja kirjoitusoikeuden lisääminen käyttöjärjestelmään. Tämän kautta mahdollistuu varmentamattoman koodin suorittaminen.
HID-protokollan kautta hyökkääminen
Näppäimistön ja hiiren matkiminen ilman käyttäjän tietoisuutta asiasta haitallisen USB-laitteen kautta voi käynnistää automaattisesti ohjelmia, tai varastaa käyttöoikeudet käyttäjältä. Myös tekstitiedoston avaaminen, base64-enkoodatun viruksen luominen ja tallentaminen kohdelaitteelle on mahdollista…
USB-massamuistin kautta hyökkääminen
USB-laitteen laiteohjelmiston uudelleenohjelmoimalla, voi hakkeri muokata liikkeessä olevaa sisältöä levyosiolla, tai mitä tahansa määrää tiedostoja. Periaate koostuu järjestelmän pakottamisesta uudelleenlukemaan tiedosto sen jälkeen, kun sen digitaalinen varmiste on jo tarkistettu: Tämä toinen lukukerta ei tuota samaa data kuin ensimmäinen, mahdollistaen sen sijaan hyväksymättömän koodin asentamisen järjestelmään.
Isäntä-järjestelmällä datan hankkiminen

Riippuen käyttöjärjestelmän tavasta lukea USB-laitteen kuvaaja, voi haitallinen USB-massamuisti tunnistaa käyttöjärjestelmän ja sopeuttaa strategiansa heikkouksiin, jotka kussakin järjestelmässä ovat toivottuja kohteita.
DMA Hyökkäykset & Väylän vakoilu
On-The-Go USB-laitteiden avulla, jotka voivat esittäytyä joko lisälaitteina tai USB-isäntinä itsessään, on mahdollista hyökätä suoraan muistiin; Direct Memory Access (DMA)-hyökkäyksillä. Lisäksi haitallinen laite voi helposti anastaa välistä data jota vastaanottavat kaikki muut laitteet jotka ovat liitettyinä USB-isäntäohjaimeen.

Pod-slurping-hyökkäykset ovat kannettavien mediasoittimien (kuten Apple iPod, Creative Zen ja muut) yleistyttyä esille noussut keino viedä dataa luvattomasti suojatuista ympäristöistä. Moni USB-väylällä varustetuista laitteista oli yhteensopiva muidenkin kuin tarvitsemiensa ja tukemiensa tiedostomuotojen kanssa. Tämä mahdollisti niin kutsuttujen MP3-soitinten tallennustilan käytön muunlaisen datan varastoimiseen – ja siitä seuranneeseen salakuljettamiseen. (Anderson & Anderson, 2010, p. 155)

Termin Pod-slurping keksi tietoturva-asiantuntija Abe Usher vuonna 2005. Hänen kehittämänsä tekniikka sisällytti iPod-musiikkisoittimeen ohjelman, joka skannasi laitteen ja sitä ympäröivän verkon kriittisen datan kannalta, ja kopioi sitä löytäessään sen iPod-laitteen massamuistiin. Moni tällainen tekniikka käyttää Windows-käyttöjärjestelmien sisäänrakennettuja komentoja, powershell-skriptejä tai python-skriptejä. (Anderson & Anderson, 2010, pp. 155-156)

Nykyisten älypuhelinten yleisyys on mahdollistanut Pod-slurping hyökkäykset entistä näkymättömämmin. Muokattu älylaite mahdollistaa useita USB-väylän hyökkäyksiä, ja muokkaamatonkin älylaite suuressa osassa malleja mahdollistaa tiedon kopioinnin USB-yhteydellä laitteen muistiin. (Anderson & Anderson, 2010, pp. 160-161) Älypuhelinten lataus tietokoneen portista on yleinen tapa.

Hyökkäykset USB-väylään voivat myös olla ajuripohjaisia. Nykypäivänä usein törmätään SteeFox hakkeriryhmän luomiin ”bring your own vulnerable driver”-hyökkäyksiin (tuo oma haavoittuvainen ajurisi-hyökkäys), joiden toiminta on periaatteiltaan sama; tässä tapauksessa haavoittuvuus luodaan hyödyntämällä kykyä lisätä haavoittuvainen ajuri laitteeseen (Liucveikis, 2024). Ajuripohjainen hyökkäys on USB-pohjainen hyökkäys, jossa haitallinen USB-laite lataa tai asentaa isäntäkoneeseen haitallisen ajurin. Tämä haittaohjelmana toimiva ajuri käynnistää haittaohjelman koodin, tai hyväksikäyttää tietokoneen haavoittuvuutta. (Nicho &

Sabry, 2023, p. 502) Haitallinen ajuri voi olla myös haavoittuvuudella varustettu ajuri, jonka haavoittuvuus mahdollistaa hyökkäyksen.

Palvelunestohyökkäykset USB-väylän kautta ovat tapa tuhota tietoa tai sabotoida laitteen toimintaa. Tällaisena keinona toimii mm. USB Killer-hyökkäys. Onnistuneena palvelunestohyökkäyksenä Nicho & Sabry pitävät ”Stuxnet” matoa. (Nicho & Sabry, 2023, pp. 502-503) ”USB Kill” on muokattu USB-muistitikun näköinen laite, joka kondensaattoreita etäohjauksella käyttäen syöttää USB-liittimen datalinjaan korkeajännitepiikin, joka useimmiten rikkoo emolevyn, tai aiheuttaa muita vikoja itse laitteeseen (USBKill.com, 2025). Tällainen suoraviivainen tuhon aiheuttaminen on karkeasta lähestymistavastaan huolimatta tehokasta palvelunestoa sabotaasin muodossa.

Madisetti & Masters tutkimuksessaan sivukanavahyökkäyksistä nimesivät 3 sivukanaviin kohdistuvaa hyökkäystekniikkaa: Hotplug-laitteet, Powerhammer-haittaohjelman, sekä Covid-bit-hyökkäyksen. Kaksi jälkimmäistä perustuu PLC-pohjaisiin iskuihin. (Masters & Madisetti, 2024, p. 434) Sivukanavahyökkäyksiä kuvaa Liu et al-tiimi ”hyökkäyksiksi, jotka hyväksikäyttävät järjestelmän hallitsemattomia ominaisuuksia” hyökkäyksen aikaansaamiseksi (Liu, et al., 2021, p. 4).

PLC tarkoittaa Power Line Communication-teknologiaa. PLC-teknologiaa käytetään pääosin virrantoimitusalalla, sähkövoimateollisuudessa. Virallisessa käytössään sen avulla voidaan valvoa tukiasemien toimintaa, ja kommunikoida niiden kanssa ilman erillisiä datalinjoja, joita pitkin informaatio kulkee. PLC-teknologia sisältää eräänlaista sisäänrakennettua tietosuojaa; sen käyttöä varten pitää olla pääsy itse infrastruktuuriin sähköntoimituksessa – perinteisesti. PLC on kuitenkin langallinen tiedonsiirron tapa, ja lähes kaikki hyökkäystavat on mahdollista kääntää kohdistumaan PLC-tiedonsiirtoon. (Masters & Madisetti, 2024, pp. 433-434)

Powerhammer-haittaohjelma hallinnoi keskusprosessorin (CPU, Central Processing Unit) käyttörasitusta ja virransyöttöä vaikuttaakseen tietokoneen tai laitteen kokonaisvirrankulutukseen. Tämä virrankulutuksen heilahtelu toimii signaalina, jota hyökkääjä voi kuunnella ja kääntää luettavaan muotoon raa’asta sähköisestä signaalidatasta. (Masters & Madisetti, 2024, p. 434)

Covid-bit-hyökkäys on tekniikka, jossa hyökkääjä kuuntelemalla lähietäisyydeltä (n. 6 jalkaa, referenssi Covid-viruksen turvaväliin) virtalähteen yliäänitaajuksilla olevia ääniä. Nämä ylitaajuusäänet vaihtelevat virran moduloinnin aikana, mahdollistaen datan vuotamisen virtalähteen kautta. (Masters & Madisetti, 2024, p. 434)

Latauspistokkeeksi naamioitu hyökkäysväline, joka hyväksikäyttää PLC-teknologiaa on monin puolin käytännöllinen tapa toteuttaa piilotettu isku – sekä naamioida sen lähettämä liikenne. Masters & Madisetti kuvaavat tällaisen lataussovittimeksi muokatun laitteen parhaita puolia

pieneksi kooksi, edullisuudeksi sekä normaaliksi standardiulkonääöksi. He kuvaavat tällaista toteutustapaa voimakkaaksi ja hyödylliseksi välineeksi hyökkääjän käyttöön. Heidän prototyyppinsä tällaisesta sähköpistoke-pohjaisesta hyökkäysvälineestä on nimeltään Thundermole (Ukkosmyyrä – viitannee myös termin ’mole’ käyttöön sisäpiirin vakoojana, myyränä). (Masters & Madisetti, 2024, p. 435)

Latauspistokkeisiin ja -asemiin asennetut hyökkäyslaajennokset ovat myös muissa sivukanavien hyökkäyksiä koskevissa katsauksissa esille tulleita tekijöitä. Shandong University-yliopiston tiimi löysi useita sähkömagneettisen spektrin alueen hyökkäystapoja, tietovuotoja, sekä latureihin liittyviä tekniikoita. (Liu, et al., 2021, pp. 1, 3)

Thundermole-työkalu keskittyy varastamaan tietoa kohdelaitteen ja seinäpistokkeen välistä – toisin sanoen se ottaa paikkansa samaan tapaan kuin muokatut USB-johdot hyökkäyskäytössä, joskin seinäpistokkeen ja laitteen välissä eikä kahden laittaan USB-väylän välissä (vrt. O.MG-Cable). (Masters & Madisetti, 2024, p. 440)

Masters & Madisetti ehdottavat myös haittaohjelman toimivuutta samankaltaisessa käytössä – jos infektoitunut laite voi moduloida sen virran kulutusta (ominaisuus, jota he demonstroivat käyttämällä Arduino Nano-laitetta ”infektoituneena uhrina”), se voi kommunikoida PLC-teknologiaa vastaavalla tavalla latausjohtoaan pitkin. (Masters & Madisetti, 2024, p. 439)

Samoja tekniikoita, joita Thundermole-väline käyttää, voidaan heidän (Masters & Madisetti) tutkimuksensa perusteella jatkojalostaa koskemaan kannettavia lisävirta-akkuja, kannettavien laitteiden latureita, virranjakopistokkeita, UPS-varavirtalähteitä ja niin edelleen. (Masters & Madisetti, 2024, p. 441)

8 Uhka-arvioinnin metodiikat ja mittaristot

Uhkia voi analysoida prosessissa, jossa tutkitaan mikä voi mennä vikaan ilman että sitä välttämättä halutaan – tai voidaan – arviota tehdessä mitata tai määrällistää kvantitatiivista analyysiä varten. Kvalitatiivisella analyysillä – keskittymällä laadullisiin tekijöihin ja uhan luonteeseen - voidaan muodostaa yleinen kuva uhasta ja verrata sen relevanssia muihin karkeammalla tasolla. (Conklin, n.d.)

Tämän luvun lopussa on ”Taulukko 4 – Uhkamatriisien/-Metodien vertailutaulukko”, johon olen yhteen paikkaan kerännyt karkean vertailun eri uhkamatriisien ja uhkien arviointimetodien toteutustekniikoista, tuottaman arvion tyylistä, sekä tavoitteista. Seuraavissa alaluvuissa esittelen uhka-arvioissa käytettäviä toimintatapoja ja luokittelujärjestelmiä.

Taulukko 3 - Uhkamatriisien/-Metodien vertailutaulukko

Matriisin/Metodi	Tekniikka	Tyyli	Tavoite
DREAD	Pisteytys	Kuvaava	Luokittelu/Vertailu
STRIDE	Kaaviot	Kuvaava	Uhkien & Suojakontrollien vertailu
TARA	Tärkeysjärjestys	Määrällinen	Uhkien arvojärjestys & Analyysi
MORDA	Hyökkäyspuumallit	Määrällinen	Päätöksenteko & Analyysi
CVSS	Pisteytys	Määrällinen	Uhkien arvojärjestys & Vertailu

8.1 Microsoft DREAD

Microsoft DREAD on Microsoftin 2003 julkaisema luokittelujärjestelmä uhille. Se toimii Uhka-Arvion tapaan, mutta kvantitatiivisten uhkien jaottelujen sijaan se tuottaa pisteytetyn kategorioinnin uhille – mahdollistaen eri uhkien vertaamisen toisiinsa yhteisen luokittelun kautta. DREAD keskittyy uhan vaikutuksiin ja seurauksiin. (Heymann, et al., 2023, p. 1)

DREAD-järjestelmä on vanhentunut Microsoftin käytössä, sen siirtyessä uudemman STRIDE-järjestelmän tieltä. (Heymann, et al., 2023, p. 2) DREAD-järjestelmä muistuttaa CVSS-järjestelmää uhkien pisteytyksessä. (Heymann, et al., 2023, p. 2)

DREAD Uhkien Luokittelujärjestelmä jakaa uhkien pisteytyksen viiteen kategoriaan, Vahinkopotentiaaliin (Damage Potential; D), Toistettavuuteen (Reproducibility; R), Hyväksikäytettävyyteen (Exploitability; E), Vaikutettaviin Käyttäjiin (Affected Users; A) sekä Löydettävyyteen (Discoverability; D). (Heymann, et al., 2023, p. 1)

Jokaisen luokan pisteytys on skaalalla 0-10, lukujen kuvauksen merkityksen vaihtuessa hieman alaluokkien mukaan. Esimerkkejä näistä seuraavissa alaluvuissa. Näiden alaluokkien yhteenlaskettu pistemäärä on DREAD-arvion kokonaispisteytys, jota muiden uhkien kokonaispisteisiin vertaamalla voidaan saada karkea arvio uhkien priorisointia varten. (Heymann, et al., 2023, p. 1)

DREAD toimii hyvänä tukena STRIDE-järjestelmään, joka keskittyy siihen, miten uhka aiheuttaa vauriota. (Heymann, et al., 2023, p. 1)

D – Damage Potential – Vahinkopotentiaali

Kategorian pisteytys toimii seuraavasti: Asteikko 0-10. 0 indikoi ettei organisaatiolle ole tullut lainkaan minkäänlaista vahinkoa. Asteikon puoliväli, 5, indikoi että tietovuoto on tapahtunut; jonkinlaista tietoa on vuodettu organisaation ulkopuolelle. 8 indikoi ei-salaisen tai ei-suojatun käyttäjädatan saattamista vaaraan; tämä voi tarkoittaa normaalin käyttäjän tai asiakkaan tietojen anastamista, tuhoamista tai muita ei-toivottuja toimenpiteitä luvattomasti dataan kohdistuen. Pisteytys 9 indikoi ei-salaisen tai ei-suojatun järjestelmänvalvonnan tai hallinnollisen datan saattamista vaaraan; järjestelmälle tärkeää dataa on voitu anastaa tai tuhota, aiheuttaen vahinkoa organisaatiolle sen hallinnon tai järjestelmien valvonnan tietoihin vaikuttamalla. Pisteytys 10 indikoi koko tietojärjestelmän täydellistä tuhoamista; se voi tarkoittaa koko järjestelmän pyyhkimistä, fyysisien palvelinten ja varmuuskopioiden tuhoutumista, tai jopa krypto-haittaohjelman aiheuttamaa tiedonmenetystä – kunhan tuhoutumisen skaala on riittävä. (Heymann, et al., 2023, pp. 1-2)

Huomattavaa on, että kategorian pisteytystapa itsessään ei ota kantaa onko kyseessä vahinko, luonnonilmiö, laajempi tapaturmainen tapahtuma vai pahantahtoinen sabotööri. Niin tulipalot, ammattimaisesti toimivat valtiontason hyökkääjät, tulvat kuin huolimattomat järjestelmänvalvojatkin voivat aiheuttaa vahinkoa koko laajalla pisteytysskaalalla.

R – Reproducibility – Toistettavuus

Kategorian pisteytys toimii seuraavasti: Asteikko 0-10. 0 indikoi että hyökkäys on vaikeasti toistettavissa. Saman tekijän tai toisen tekijän on vaikea suorittaa sama hyökkäys uudelleen. 5 indikoi että hyökkäyksen toistaminen uudelleen on monimutkaista; se voi vaatia enemmän resursseja, tai sen onnistumisen takana oli joitain sattumanvaraisia tai yhä tuntemattomia syitä. 7,5 indikoi että hyökkäys on helppo toistaa; sen uusimiseen ei ole suuria esteitä. Esimerkiksi hyökkäyksen tekijöillä on yhä sama pääsy järjestelmään kuin alkuperäisessä hyökkäyksessä, tai hyökkäyksen uusiminen ei edellytä suurempia määriä resursseja, eikä siihen liity mitään tekijöitä, joiden hyödyntäminen olisi poissuljettu. 10 indikoi että hyökkäys on erittäin helppo toistaa; prosessin uusiminen on lähes rutiininomaista. Hyökkäyksen toteutuksessa ei tarvita muutoksia eikä suurempaa uudelleensuunnittelua. Esimerkiksi haittaohjelman lähettäminen sähköpostitse roskapostiohjelmilla on hyökkäys jonka uusiminen on äärimmäisen helppoa. (Heymann, et al., 2023, p. 2)

Tämä kategoria ei ota kantaa hyökkäyksen vaarallisuuteen. Sen pisteytys on erillään muista tekijöistä, perustuen vain siihen mitkä tekijät mahdollistavat hyökkäyksen, ja miten vaivalloista saman tai eri tekijän on toteuttaa sama hyökkäys uudelleen.

E – Exploitability – Hyväksikäytettävyys

Kategorian pisteytys toimii seuraavasti: Asteikko 0-10. 2.5 indikoi että haavoittuvuuden hyväksikäyttöön tarvitaan erityisosaamista ohjelmoinnissa ja verkonhallintataidoissa. 5 indikoi että tarjolla on valmiita työkaluja, joita tarvitaan haavoittuvuuden hyväksi käyttämiseen. 9 indikoi että web-sovelluksen välityspalvelimia tarvitaan haavoittuvuuden hyväksi käyttämiseksi. 10 indikoi että haavoittuvuuden hyväksikäyttöön vaaditaan verkkoselain. (Heymann, et al., 2023, p. 2) Kategorian pisteytys kuvaa lähinnä verkkohaavoittuvuuden hyväksikäyttöön vaadittavia taitoja tai työkaluja.

A – Affected Users – Vaikutettavat Käyttäjät

Kategorian pisteytys toimii seuraavasti: Asteikko 0-10. 0 indikoi ettei hyökkäys vaikuta yhteenkään käyttäjään. 2.5 indikoi hyökkäyksen mahdollisesti vaikuttavan vain muutamaan yksittäiseen käyttäjään. 6 indikoi hyökkäyksen vaikuttavan muutamiin käyttäjiin. 8 indikoi hyökkäyksen vaikuttavan järjestelmänvalvojien käyttäjiin. 10 indikoi hyökkäyksen vaikuttavan kaikkiin käyttäjiin. (Heymann, et al., 2023, p. 2)

D – Discoverability – Löydettävyys

Kategorian pisteytys toimii seuraavasti: Asteikko 0-10. 0 indikoi haavoittuvuuden olevan vaikeasti löydettävissä. 5 indikoi haavoittuvuuden olevan löydettävissä tavallisilla http Request-pyynnöillä. 8 indikoi haavoittuvuuden löytyvän julkisesta tietolähteestä avoimesti saatavilla. 10 indikoi haavoittuvuuden löytyvän web osoitepalkista tai lomakkeesta. (Heymann, et al., 2023, p. 2)

8.2 STRIDE-järjestelmä

STRIDE-järjestelmä on eräänlainen tehokas akronyymi yleisimpien uhkien muistamiseen; sitä käytetään myös uhkien arvioiden tekemiseen kaavioiden avulla. STRIDE koostuu termeistä Spoofing (S, Huijaus), Tampering (T, Peukalointi), Repudiation (R, Kiistäminen), Information Disclosure (I, Tietovuoto), Denial of Service (D, Palvelunesto), Elevation of Privilege (E, Oikeuksien korottaminen). (Conklin, n.d.) Ohessa kääntämäni taulukko STRIDE-järjestelmän sisältämistä uhista dokumentista ”Threat Modeling Process” (Conklin, n.d., pp. 11-12)

Taulukko 4 - STRIDE-järjestelmän sisältämät uhat

Tyyppi	**Kuvaus**	**Suojakontrolli**
Spoofing/	Uhkatoiminta tähtää toisen käyttäjän tunnuksien	Tunnistautuminen

Huijaus	käyttämiseen, esim. Käyttäjänimi ja salasana.	
Tampering/ Peukalointi	Uhkatoiminta aikoo muokata tai muuttaa pysyvää dataa, kuten tietokantamerkintöjä tai verkon välillä siirrettyä dataa.	Eheys
Repudiation/ Kiistäminen	Uhkatoiminnan tavoite on suorittaa kiellettyjä toimintoja järjestelmässä joka ei kykene jäljittämään suoritettujen toimintojen alkuperää tai järjestystä/ajankohtaa.	Kiistämättömyys
Information disclosure/ Tietovuoto	Uhkatoiminnan tarkoitus on lukea tiedosto johon ei ole sallittu pääsyoikeuksia, tai lukea data liikkeessä.	Luotettavuus
Denial of service/ Palvelunesto	Uhkatoiminta yrittää estää oikeutettujen käyttäjien pääsyn järjestelmään, tai haitata järjestelmän käytettävyyttä. Esim. Verkkosivun kaataminen, kirjautumisen esto.	Saatavuus
Elevation of privilege/ Oikeuksien korottaminen	Uhkatoiminnan aikomus on Saada korotetut oikeudet resursseihin, jolloin voi käsitellä rajatun saatavuuden tietoja, tai altistaa järjestelmän syvemmille hyökkäyksille.	Valtuutus

Hotplug hyökkäyksillä ja BadUSB-tekniikoilla voidaan kohdistaa kaikkia näitä uhkia kohteeseen. STRIDE-pohjaiset uhkalistat ovat hyödyllinen apuväline uhkien tunnistamiseen yhteydessä hyökkääjän tavoitteisiin (Conklin, n.d.).

8.3 TARA-järjestelmä

TARA, eli Threat Assessment and Remediation Analysis on monialainen uhkien tutkimis- ja tunnistamisjärjestelmä. TARA-prosessissa ensimmäinen osapuoli tunnistaa ja järjestää hyökkäysvektorit arvojärjestykseen arvioidun riskin perusteella. Toinen osapuoli tunnistaa ja valitsee vasta- ja suojaustoimet perustuen arvioituun hyödyllisyyteen ja kustannuksiin. TARA-järjestelmän päätarkoitus on siis suunnittelumetodina tunnistaa ja arvioida kyberuhkia ja haavoittuvuuksia. TARA on monin tavoin samanakaltainen STRIDE- ja MORDA-järjestelmien kanssa. (Wynn, 2014, pp. 1-3)

Vaikka TARA-järjestelmän rakenne ja sisältö arvioinnissa vaihtelee, koostuu se pääosin kolmesta vaiheesta: Cyber Threat Susceptibility Analysis (CTSA), Cyber Risk Remediation Assessment (CRRA) sekä Knowledge Management (KM). (Wynn, 2014, pp. 4-5)

CTSA analysoi järjestelmän teknisiä yksityiskohtia, koittaen tunnistaa edustavan haavoittuvuuksien ryhmän perustuen hyökkäysvektoreihin. Sen alkuvaihe on tunnistaa eri tavat, joilla hyökkääjä voi saada pääsyn järjestelmään. Tämä tapahtuu rakentamalla mallinnus järjestelmästä ja sen yksityiskohdista. CTSA:n tojnen vaihe on tunnistaa näistä havainnoista uskottavat hyökkäysvektorit, käyttäen hyväksi TARA-katalogia. Viimeisessä CTSA-vaiheessa tehdään riskiarvio. (Wynn, 2014, pp. 6-8)

CRRA arvostelee, organisoi tärkeysjärjestykseen ja valitsee vastatoimet katalogista perustuen TARA-katalogin vastatoimien vaikutus kartoituksiin. Sen tarkoitus on tunnistaa mitkä vastatoimet ja riskiä vähentävät tekijät ovat uskottavia vaihtoehtoja. Vastatoimien hyödyllisyyden ja kustannusten arvioiminen on CRRA-prosessin seuraava vaihe. Lopuksi CRRA-vaiheessa suoritetaan vastatoimien ja riskiä vähentävien toimien valinta. (Wynn, 2014, p. 9) Tämä on tämän opinnäytetyön laajuuden ulkopuolelle putoava toimenpide.

KM-vaihe kehittää eteenpäin katalogin sisältöä. Sen vaiheet ovat informaatiotarpeiden priorisointi ja kartoitus, ulkoisten tiedonlähteiden tunnistus ja arviointi sekä katalogin datan päivittäminen. (Wynn, 2014, p. 14) Tämä prosessin vaihe kehittää ja ylläpitää itse TARA-järjestelmän toiminnallisuutta ja hyödyllisyyttä.

TARA-järjestelmä ei ole tämän opinnäytetyön tavoitteisiin sopiva ottaen huomioon opinnäytetyön painopisteet ja laajuuden.

8.4 MORDA

MORDA, eli Mission Oriented Risk and Design Analysis (Tehtävään Orientoitu Riski ja Suunnittelu Analyysi), on uhkien arvionnin kvantitatiivinen metodiikka, joka luottaa hyökkäyspuumallien (Attack Tree), tiedon varmistuksen mallien, sekä monitavoitteisen päätöksenteon analyysimenetelmien käyttöön. (Parnell & Saydjari, 2005, p. 20)

MORDA-mallin tukena käytetään laajennosta SOCRATES-mallista. Molemmat ovat kvantitatiivisia malleja, joiden käyttö ei ole näin laajan kokonaisen uhkavektorin arviointiin järkeväksi perusteltua. (Parnell & Saydjari, 2005, pp. 21-23) Jos uhka-arviota tehtäisiin tiettyyn spesifiseen kohteeseen, voisi MORDA-mallinen monialan yhteistyöllä toimiva laajempi kvantitatiivinen arvio olla tehokas ratkaisu.

8.5 CVSS-järjestelmä

CVSS (Common Vulnerability Scoring System) on avoin yleinen haavoittuvuuksien arviointijärjestelmä. Sen avulla voidaan pisteyttää eri haavoittuvuuksia ja uhkia, joka luo karkean vertailun niiden arvojärjestyksestä. CVSS järjestelmässä on useampi mittaristo, niin sanottu pohjamittaristo (Base Metrics) joka pisteyttä haavoittuvuuden hyväksikäytettävyyden (Exploitability) useilla eri arvoilla, sekä haavoittuvuuden vaikutuksen (Impact) myös useilla arvoilla. (FIRST, 2024, pp. 4, 7-17)

CVSS-järjestelmän perusmittariston ohella voi käyttää myös Threat Metrics-mittaristoa, joka arvioi uhkaa itsessään sen saatavuuden ja tekniikoiden nykytilan kannalta. Perusmittaristolle annetaan arvot 0.0-10.0-asteikolla. Tätä voidaan laajentaa syvemmäksi arvioksi käyttämällä Threat Metrics- sekä Environmental Metrics-mittaristoja, joskin niiden käyttö ei ole pakollista tulosten saamiseksi. (FIRST, 2024, p. 6)

Exploitability

Exploitability Metrics kuvaa itse ”asiaa, joka on haavoittuvainen”, toisin sanoen järjestelmää tai kohdetta, johon hyökätään. CVSS-mittariston arviossa on perusoletuksena, että hyökkääjällä on edistynyttä tietoa kohteesta, sen yleisestä kokoonpanosta sekä oletusarvoisista suojakeinoista, joita kohteeseen sisällytettäisiin. Erilaiset kohdekonfiguraatiot eivät siis ole CVSS-mittaristoa oikein käyttäessä tuloksiin vaikuttava tekijä – hyökkääjän oletetaan soveltavan keräämänsä tiedot kohdistaakseen hyökkäyksen oikein. (FIRST, 2024, p. 8)

Attack Vector (AV)

AV-mittarilla kuvataan hyökkäyksen mahdollistavaa kontekstia. Sen arvo on sitä korkeampi mitä loogisesti tai fyysisesti kauempana kohteesta hyökkääjä voi olla haavoittuvuuden hyväksi käyttämiseksi. Esimerkkioletuksina pidetään esimerkiksi sitä että verkon yli toimivien

hyökkääjien lukumäärä on suurempi, kuin fyysisesti paikan päällä laitteen yhteyteen pääsyä vaativissa hyökkäyksissä. (FIRST, 2024, p. 8)

Attack Complexity (AC)

AC-mittarilla kuvataan mitattavien toimien vaatimuksia puolustavien tekijöiden välttämiseksi, tai suojauksien kiertämiseksi hyökkääjän toimesta. Nämä tekijät ovat paikalla olevia lisäjärjestelmiä, toimia, tai ominaisuuksia, jotka lisäävät laitteen suojausta – tai monimutkaistavat hyökkäyksen suunnittelua ja toteutusta. Haavoittuvuus, joka on toteutettavissa ilman kohdetta varten suunniteltuja konfiguraatioita on monimutkaisuudeltaan alhaisempi kuin hyökkäys, jonka toteuttaminen vaatii vähäistä konfiguraatiota suurempia muutoksia hyökkäyksen skriptauksessa, suunnittelussa tai toteutuksessa. AC-mittari ei ota kantaa siihen montako yritystä tai kauanko hyökkäyksen toteuttamiseen menee – mittarissa on kyse vain toimenpiteistä ja muutoksista, jotka on pakko suorittaa – tai hyökkäys epäonnistuu aina. (FIRST, 2024, p. 9)

Attack Requirements (AT)

AT-mittaristolla mitataan ennakkovaatimuksia, jotka haavoittuvaisessa järjestelmässä on hyökkäyksen mahdollistamiseksi. Toisin sanoen kuvataan haavoittuvaisen järjestelmän toteutusta, suoritusolosuhteita tai muuttujia, joissa haavoittuvuus tai hyökkäyksen mahdollistavat tekijät piilevät. Ero aiempaan AC-mittaristoon o siinä, että AT-mittaristossa ei mitata suojaustekijöitä tai turvallisuutta edistävien järjestelmien puutetta, vaan luonnostaan haavoittuvaisen järjestelmän käyttöönotosta tai muutoksista johtuvia luonnollisia seurauksia. Jos tällaisia haavoittuvuuksia ei järjestelmästä löydy, pitää hyökkääjän oletuksena luoda nämä otolliset olosuhteet – tai hyökkäys epäonnistuu aina. (FIRST, 2024, p. 10)

Privileges Required (PR)

PR-mittaristossa kuvataan järjestelmä- tai käyttäjäoikeuksia, jotka hyökkääjällä on oltava ennen onnistunutta hyökkäystä. Mittaristossa ei oteta kantaa siihen mitä kautta nämä ylennetyt kredentiaalit, järjestelmänvalvojan tunnukset tai muut lisä- tai vaaditut oikeudet on hankittu. Pisteytys on sitä korkeampi, mitä vähemmän erityisiä korotettuja oikeuksia hyökkäykseen tarvitaan. Korkein tulos on hyökkäys, jonka toimivuus toteutuu ilman mitään erityisoikeuksia järjestelmässä tai käyttäjänä. Huomiona mittaristossa annetaan arvo None (ei vaadittuja oikeuksia) yleisesti, jos hyökkäyksen toteutukseen vaaditaan social enginering tekniikoita, käyttäjäoikeudet on valmiiksi kovakoodattu kohteeseen, tai oikeuksina riittää oletuskäyttäjä, joka laitteella on. (FIRST, 2024, pp. 11-12)

User Interaction (UI)

UI-mittaristo mittaa ihmiskäyttäjältä vaadittujen toimien monimutkaisuutta, aikomusta tai määrää. Ihmiskäyttäjällä tässä mittaristossa tarkoitetaan hyökkääjän ulkopuolista henkilöä –

luonnollista työntekijää, haitallista sisäpiiriläistä tai muuta vaadittua osallistumista onnistuneeseen haavoittuvuuden hyväksi käyttöön. Mittaristossa pyritään erottamaan hyökkäys, joka on toteutettavissa täysin hyökkääjän tahdonalaisuuden kautta milloin vain, verrattuna erilliseen käyttäjään, jonka on otettava osaa jonkinlaisiin toimiin jollain tavalla hyökkäyksen mahdollistamiseksi. Mittaristossa käytetään esimerkiksi termiä Passive (Haluton, passiivinen) kuvaamaan käyttäjää, jonka ottamat toimet ovat tahdottomia, vahingossa tehtyjä, ja jotka eivät vaadi aktiivista suojaustoimien purkamista tai kiertämistä hyökkäyksen onnistumiseksi. Active (Aktiivinen, tietoinen) osallistuja tarkoittaa käyttäjän tietoisesti tekemiä toimia suojauksen kiertämiseksi tai poistamiseksi järjestelmästä, mahdollistaen hyökkäyksen. (FIRST, 2024, p. 12)

Impact

Impact mittaristo mittaa onnistuneen hyökkäyksen tai haavoittuvuuden hyväksi käyttämisen aiheuttamia seurauksia. Seuraukset on pyrittävä CVSS-ohjeistuksen mukaan pitämään kohtuullisina ja järkeenkäypinä lopullisina tuloksina, jotka hyökkääjän voidaan itsevarmuudella todeta saavuttavan. Seurauksina huomioon otetaan vain korottunut pääsy järjestelmiin, korottuneet suoritusoikeudet, tai muut haitalliset tulokset, joita hyökkäyksen onnistuminen aiheuttaa. CVSS-ohjeistus antaa esimerkin hyökkäyksestä, jossa hyökkääjä käyttää vain-luku oikeuksia hyökkäyksessään- Hyökkäys mahdollistaa kirjoitusoikeuden saamisen järjestelmään. Vain Integrity (koskemattomuus)-mittariston muutos on pisteytettävä, sillä hyökkäyksellä ei ollut vaikutusta Confidentiality (luottamuksellisuus)- eikä Availability (Saatavuus)-mittaristossa. (FIRST, 2024, p. 13)

Confidentiality (VC/SC)

VC/SC-mittaristo mittaa luotettavuuden menetystä tiedosta, jota hyökkäyksen kohde hallinnoi. Luottamuksellisuus tarkoittaa tiedonsaannin rajoittamista, ja tiedon paljastamista. VC-puoli Confidentiality mittaristosta koskee vaikutusta itse haavoittuvaan järjestelmään (Vulnerable System, VC). VC-asteikon skaala on kolmpiportainen asteikko luotettavuuden säilymisestä (Ei menetettyä luotettavuutta, ei vaikutusta luotettavuuteen) aina täyteen luotettavuuden menetykseen (Kaikki tieto haavoittuvasta järjestelmästä on vuodettu hyökkääjälle. SC-puoli (Subsequent System) Confidentiality mittaristosta koskee vaikutusta loppujärjestelmään – toisin sanoen tietovuodon ylettymistä kaikkiin resursseihin koko jäljellä olevasta laajemmasta järjestelmästä. Kolmiportainen SC-asteikko kulkee luottamuksen säilymisestä (Ei menetettyä luotettavuutta, ei vaikutusta luotettavuuteen) aina täyteen luotettavuuden menetykseen (Kaikki tieto koko loppujärjestelmästä haavoittuneen järjestelmän ulkopuolelta on vuodettu hyökkääjälle). (FIRST, 2024, pp. 14-15)

Integrity (VI/SI)

VI/SI-mittaristo mittaa vaikutusta tiedon paikkaansapitävyyteen onnistuneen hyökkäyksen tuloksena. Integrity-arvo viittaa tiedostojen säilyneeseen laatuun, muuttumattomuuteen ja koskemattomuuteen – tietoja ei ole muokattu, eikä niiden sisältämiin tietoihin vaikutettu. VI-puoli (Vulnerable System) mittaristosta viittaa tiedon koskemattomuuden vaikutuksiin haavoittuvaisessa järjestelmässä. SI-puoli (Subsequent System) mittaristosta viittaa tiedon koskemattomuuden vaikutuksiin koko haavoittuvaisen järjestelmän ulkopuolella. (FIRST, 2024, pp. 15-16)

Availability (VA/SA)

VA/SA-mittaristo mittaa vaikutettujen järjestelmien saatavuutta. Se siis koskee itse kohteena tai vaikutuksena olevan järjestelmän itsensä saatavilla olemista, sen saattamista epäkuntoon tai verkosta uloskytkemistä. VA-osio (Vulnerable System) mittaa hyökkäyksen vaikutusta itse haavoittuvaisen järjestelmän saatavuuteen. SA-osio (Subsequent System) mittaa hyökkäyksen vaikutusta itse haavoittuvaisen järjestelmän ulkopuoliseen loppujärjestelmään – laajempaan verkkoon, palvelimiin ja niin edelleen. (FIRST, 2024, pp. 16-17)

Threat

Threat, eli uhkamittaristo, mittaa nykyhetkessä saatavilla olevia hyökkäystekniikoita sekä haavoittuvuuksiin liittyvää lähdekoodia. (FIRST, 2024, p. 17)

Exploit Maturity (E)

E-mittaristo mittaa todennäköisyyttä, että haavoittuvuuteen kohdistuu hyökkäys. Se perustuu tämänhetkisien tekniikoiden, valmiin koodin ja aktiivisten käynnissä olevien hyökkäysten määrään ja saatavuuteen. Julkisesti helposti löytyvät valmiit hyökkäykseen käytettävät skriptit tai ohjelmat edesauttavat osaamattomampien hyökkääjien aktivoitumista aktiivisiksi uhiksi. Samoin proof-of-concept koodi ja erilaiset löydetyt haavoittuvuudet ja niistä julkaistu tieto voivat edesauttaa myös haittatoimijoita hyväksikäyttämään haavoittuvuuksia. Asteikko on kolmiportainen, edeten aina saatavilla olevista proof-of-concept teorioista ja tekniikoista, meneillään oleviin aktiivisiin hyökkäyksiin saman haavoittuvuuden suhteen. Kolmas porras on Määrittämätön, Not Defined, X-arvo. Tätä käytetään, kun ei ole tiedossa uhkatietoa jonka perusteella täyttää hyökkäyksen kypsyyden asettama uhka pistearvoina. (FIRST, 2024, pp. 17-18)

9 Puolustuskeinot uhkien vähentämiseen

Uhkien vähentämiseen ja riskien pienentämiseen on lukuisia keinoja, joita voidaan luokitella useilla tavoilla. Riskejä altistua USB-väylän hyökkäyksille voi vähentää estämällä hyökkäyslaitteen pääsy kohteeseen, estämällä hyökkäyslaitetta aloittamasta hyökkäystä, tunnistamalla hyökkäys ennen kuin se aiheuttaa vahinkoa sekä kasvattamalla yrityksen käytäntökulttuuria siten, että loppukäyttäjät ovat tietoisia USB-väylään liittyvistä riskeistä.

9.1 Fyysiset suojauskeinot

Hyökkääjällä tulee olla pääsy saada USB Hotplug-hyökkäyslaite kytketyksi kohteeseen hyökkäystä varten. Toisin sanoen, laite pitää joko saada ”drop point”-tekniikalla uhrille, supply-chain attack-tekniikoita käyttäen, tai social engineering hyökkäyksen avulla uhrille. (Kierznowski & Mayes, 2015, p. 6) Fyysinen kulunvalvonta voi tarjota tehokkaan ratkaisun vähentää riskejä.

Kaksivaiheinen tunnistautuminen on tapa tarjota käytönvalvontaa, jolla voidaan vähentää haitallisten toimijoiden pääsyä laitteille ilman tietoa järjestelmän kiertämisestä. Jos kirjautumishetkellä, tai käskyn suorituksen aloittaessa tulee tunnistautua jollain välineellä joka sallitulla käyttäjällä on, tai sallitun käyttäjän omalla ominaisuudella (biometrisellä tunnisteella), tämä estää tehokkaasti salasanojen uudelleentoistohyökkäyksen (n.s. Replay-Attack). (Kierznowski & Mayes, 2015, p. 6)

USB portit voi tukkia fyysisesti, kytkeä laiteohjelmistossa tai käyttöjärjestelmässä pois päältä, tai ulkoisia apuohjelmia käyttäen rajoittaa. Fyysisen porttien tukkimisen voi toteuttaa jopa liimaamalla portin umpeen. Tämä estää laitteiden kytkemisen, ja liiman poistaminen voi vahingoittaa itse porttia – sen lisäksi että se vie hyökkääjältä aikaa. Ohjelmistoratkaisuja käyttäen USB-portit voi kytkeä pois käytöstä BIOS-järjestelmässä (Basic Input/Output System), Windows Rekisterissä, Group Policy Object-määritelmällä, sekä kolmannen osapuolen lisäohjelmilla. Lisäohjelmia käyttäen voi sallia vain tietyt laiteluokat, tai laitevalmistajat. (Dung, et al., 2010, p. 2) Porttien tukkiminen ei kuitenkaan estä sitoutunutta hyökkäystoimijaa fyysisesti kajoamasta laitteisiin, jolloin hän voi kiertää tukitut portit (Nicho & Sabry, 2023, p. 507).

9.2 Heuristiset käytösanalyysin keinot

Heuristiikka, eli käytösanalyysi, mahdollistaa hyökkäystekniikoiden käytön tunnistamisen. Raja-arvon asettaminen Caps-Lock, Scroll-Lock sekä Num-Lock näppäimille on ensisijainen yksinkertainen tunnistustapa. Moni hyökkäys luottaa näiden painikkeiden painamiseen datan lähettämiseksi ei-standardeilla tavoille. (Kierznowski & Mayes, 2015, p. 5)

Sekundäärisen, toissijaisen lisälaitteen tunnistuksen (Secondary Device Detection) tarkoitus on tunnistaa jos ”ylimääräiseksi” luokiteltava laite on lisätty kohdetietokoneeseen. Esimerkiksi toinen näppäimistö, kun yksi on jo kytketty laitteeseen, täyttäisi tämän kriteerin; kuten myös ylimääräinen verkkokortti. (Kierznowski & Mayes, 2015, p. 5)

USB-Lisälaitteiden päätepisteiden numerot mahdollistavat laiteseurannan. USB-laitteet käyttävät ominaisuuksia, joilla on vakioidut päätepisteiden numerot. Ne on kovakoodattu laiteohjelmistoon. Jos isäntäjärjestelmään kytketty lisälaite yhtäkkiä vaihtaa päätepisteiden numeroita, se voi indikoida todennäköistä hyökkäystä. (Kierznowski & Mayes, 2015, p. 6)

Rubber Ducky-tyyppiset laitteet voivat piiloutua myös Windows-järjestelmän tehtävienhallinalta. Tällöin laite ei välttämättä näy suoraan ohjelmistotarkistuksissa. Fyysisillä mittauksilla laitteen toiminnasta ja virrankäytöstä se voidaan havaita. (Cannols & Ghafarian, 2017, p. 67)

Samalla tavalla voidaan tunnistaa rikosteknisissä tutkimuksissa hyökkäyksen alkamisaika, käyttäen hyväksi päätepistenumeroita ja laitteen fyysisten ominaisuuksien muutoksia. Esimerkiksi USB-väylän lisälaitteen yllättävät, normaalista poikkeavat, käyttöjännitteen muutokset voivat toimia indikaattorina hyökkäysprosessin alkamisesta. (Kierznowski & Mayes, 2015, p. 6)

Suuri osa hyökkäyksistä sisältää ”kirjoitetussa muodossa näppäiltynä” haittaohjelman, jonka avulla isäntäjärjestelmästä (host system) saadaan varastettua dataa. Tällainen koodi voidaan havaita antivirus ohjelmilla joissain tapauksissa, tai sovellusten erillisellä sallimislistalla. Jos kaikki erikseen ei-sallittu on estetty, ei haittaohjelmaa voida suorittaa oletusarvoja käyttämällä. (Kierznowski & Mayes, 2015, p. 5)

9.3 Pääsynhallintaluettelo-pohjaiset keinot

Laitteiden lisääminen tunnisteiden tai niiden rekisteröimisprosessin perusteella erikseen sallittujen laitteiden listaan on perustason konfiguraatio, jolla voidaan rajat laitetyypit joita kohdekoneessa on mahdollista käyttää. Kaikki muut väylän lisälaitteet ovat ei-sallittuja, eli niiden käyttö on estetty ohjelmistotasolla. (Kierznowski & Mayes, 2015, p. 5)

Automaattisen käynnistyksen ja ohjelmien ajon estäminen USB-laitteita kytkettäessä vähentää todennäköisyyttä altistua hotplug-hyökkäykselle huomaamatta. Datan suojaaminen sekä ennen tiedon siirtoa että sen jälkeen salaustekniikoilla, enkryptiolla, on tehokas keino varmistaa tiedon suojaus. Käyttäjien ja työntekijöiden pääsy niin kriittisille palvelimille kuin kriittisen datan luokse on rajattava. Siirrettävien tietojen maksimikoon rajoittaminen USB-laitteille on hyödyllinen tapa vähentää kokonaisia levyjä kopioivien hyökkäysten toiminnallisuutta. (Dung, et al., 2010, p. 2)

USBFILTER-järjestelmä tarjoaa ohjelmistopohjaisen valikoivan suojan. USBFILTER on eräänlainen pakettipohjainen palomuuri USB-väylälle, joka voi estää tai sallia USB-toiminnot (Nicho & Sabry, 2023, p. 506). USBFILTER voi sallia tietyt ohjelmat käyttämään USB-lisälaitteita, estäen haittaohjelmien pääsyn laitteiden ominaisuuksiin. Esimerkiksi web-kamera toimisi näin vain videopuheluita tehdessä varmistetulla ohjelmistolla. (Nicho & Sabry, 2023, p. 506)

Kun käyttöjärjestelmä tunnistaa USB-lisälaitteen kytkemisen, voi Anti-Virus ohjelma keskeyttää prosessin, kunnes käyttäjä suorittaa varmentavan lisätoimen. Tällainen prosessi tapahtuu USB Link Layer-tasolla USB-standardia noudatettaessa. Esimerkkinä tästä näppäimistöä kytkettäessä ohjelma voi pyytää näppäilemään näytöllä olevan tunnistekoodin näppäimistöllä todisteena siitä, että se on käyttäjän itse kytkemä – eikä haittaohjelman, joka matkii näppäimistösyötteitä. (Nicho & Sabry, 2023, p. 507)

9.4 Käytäntöpohjaiset suojaukset

Käyttäjien koulutus ja opettaminen auttaa kehittämään kyberturvallista kulttuuria. Koska moni vaarallisista BadUSB/Hot Plug-hyökkäyksistä toimitetaan Social Engineering-tekniikoilla, on olennaista ylläpitää käyttäjien tietotasoa ja tietoisuutta uhista. Tätä vastaan toimii turvallisuuskulttuuri ja käyttäjien valistus. Käyttäjille pitää tarjota tietotaito säännöllisesti tarkistaa tietokoneensa ilmiselvien ylimääräisten implanttien varalta. (Kierznowski & Mayes, 2015, p. 6) Suosittu tapa naamioida implantit on kirjoittaa ”DO NOT REMOVE -I.T.” laitteisiin teipillä. Tämä toiminta voi hämätä maallikkoa, jolle tietotekniikan tukitiimin toimet ovat saattaneet jäädä varjoon. Täten auditointia IT-kyberturvallisuushenkilöstön toimesta voidaan suositella, kuten myös luvattomien langattomien lisäverkkojen ilmestymisen varmistamista säännöllisillä skannauksilla alueella.

Hyväksyttävän käytön käytäntö (Acceptable Use Policy, AUP) on USB-väylän turvallisuusratkaisuista keskustellessa melko yleinen termi. Se on käytäntö, joka toteutuu käyttäjien koulutuksen ja turvallisuuskulttuurin kehityksen yhteisvaikutuksesta. Käyttäjien tietoisuutta turvallisuusongelmista ja epäkohdista lisäämällä on mahdollisuus pienentää todennäköisyyttä onnistuneesta BadUSB-hyökkäyksestä tietämättömän käyttäjän toimesta. AUP on yleisesti melko taloudellinen vaihtoehto, vaatien lähinnä koulutusta ja tapakulttuurin ohjausta yritysympäristössä. (Dung, et al., 2010, p. 2)

Kannettavien tietokoneiden käyttämistä voi pitää yksinkertaisena estona osalle Hot Plug-hyökkäyksistä, jos työpaikan säännöt kieltävät ulkoisten lisänäppäimistöjen ja näyttöjen käytön. Kannettaviin integroidut näytöt ja näppäimistöt tarjoavat kiinteän ratkaisun, ja sulkee pois osan siirrettävien laitteiden tuomista hyökkäyssuunnista. (Kierznowski & Mayes, 2015, p. 6)

Säännöllinen tekninen auditointi voi saada kiinni luvattomat langattomat tukiasemat, joita moni USB-väylän hyökkäyslaite luo lähettääkseen dataa ulkopuolelle, tai vastaanottaakseen komentoja hyökkääjältä. (Kierznowski & Mayes, 2015, p. 6)

BadUSB2.0 hyökkäykset mahdollistivat laiteohjelmistojen kryptografinen allekirjoittamattomuus, toisin sanoen tietojen kiistämättömyys on vaarantunut. Datan alkuperä pitäisi myös varmistaa tiivistearvoilla, tai muilla kryptografian keinoilla. (Kierznowski & Mayes, 2015, p. 6)

10 Uhka-arvio USB-väylän hotplug hyökkäyksistä

Uhka-arvio tässä opinnäytetyössä on luotu käyttämällä karkeaa jakoa toiminnallisiin sektoreihin. Sektorit, joita näissä esimerkeissä käytetään ovat julkinen sektori, infrastruktuuri sekä palveluntarjoajat.

Näille sektoreille kuvataan niiden toimialoille kuuluvia esimerkkiyrityksiä ja -toimintoja. Lisäksi näiden toimialojen yritysten osalta kuvataan avainvarat joihin hyökkäykset voivat kohdistua, avainuhat, jotka näihin varoihin kohdistuvat tai vaikuttavat, sekä avaintavoitteet, joilla tarkoitetaan hyökkääjän motivaatioita, tarkoitusperiä tai ansioita.

Käytän tämän karkean uhka-arvion toteutuksessa DREAD-matriisia, sen tiiviyden ja avoimuuden takia. DREAD-matriisijärjestelmä sopii erinomaisesti kuvaamaan tällaisia laajempia hyökkäyksen mahdollisuuksia. Tarkemmat järjestelmät kuten STRIDE tarjoavat lisäarvoa erityisesti käsitellessä tiukemmin tiettyjä kohteita. CVSS-järjestelmällä saataisiin helpommin numeraalisesti ilmaistu uhka-arvio, jossa voidaan eritellä eri riskitekijöitä. Taulukko 4 alla kuvaa uhan tasoja pisteväleinä selkeyttävin kuvauksin DREAD-järjestelmässä, taulukko on EC-Council organisaatiolta peräisin, käännöstyö itseltäni (EC-Council, n.d.). DREAD-järjestelmä tuottaa selkeän priorisointijärjestyksen uhille.

Taulukko 5 - DREAD-matriisin uhkatasot pisteytysväleinä

Uhan taso	Pisteväli	Kuvaus
Kriittinen	40-50	Kriittinen haavoittuvuus, korjattava välittömästi
Korkea	25-39	Vakava haavoittuvuus, sisällytettävä harkintaan ratkaistavaksi pian
Keskitaso	11-24	Kohtuullinen riski, arvioitava kriittisen ja korkean tason riskien jälkeen

Matala	1-10	Alhainen riski infrastruktuuriin ja dataan

10.1 Julkinen Sektori

Julkisella sektorilla tässä arviossa tarkoitetaan terveydenhuoltoa, koulutuslaitoksia sekä rahoitus- ja pankkialan palveluita. Tällaiset instituutiot käsittelevät asiakas-, potilas- ja työntekijätietoja. Henkilökohtaisesti tunnistettavia tietoja, sekä erityisherkkiä salassa pidettäviä tietoja – esimerkiksi terveys-, talous-, ja suoritusrekisteritietoja.

Avainvara: Data. Henkilötiedot, yksilöllisesti tunnistettavat tiedot, terveys- ja suoritustiedot. Rahallinen informaation. Hyökkäys näihin kohteisiin altistaa suuria määriä tietoa hyväksikäytön alle.

Avainuhat: Tietomurto. Datan anastaminen ja muokkaaminen, tai tuhoaminen. Uhka tiedon luotettavuudelle ja laadulle. Yhteiskunnallisten palveluiden katkokset tai häiriö.

Avaintavoite: Rahallinen motivaatio. Kiristysohjelmat ja -toimet. Yksilöihin vaikuttaminen tietovuodoilla. Datan myyminen harmailla markkinoilla.

Taulukko 6: Julkisen sektorin DREAD-pisteytys

DREAD-Akronyymi	DREAD-Taso	Syy Tason Pisteytykseen
D – Vahinkopotentiaali	9	Käyttäjien herkkien tietojen vuoto, johtotason käyttäjien datan altistuminen
R - Toistettavuus	7	Hyökkäystapoja on useita, toistaminen helppoa
E - Hyväksikäytettävyys	7	Vaatii keskimääräistä teknologian ymmärtämistä
A – Vaikutetut käyttäjät	9	Vaikutus henkilöiviin tietoihin, yksityiseen tietoon, sekä rekisterien käytettävyyteen

D - Löydettävyys	6	Uhan toteutusväylä ei ole julkisessa tiedossa

Perustelut: Julkinen sektori käsittelee yksityistietoja, joita säätelee ja varjelee lukuisa määrä lakeja ja asetuksia niiden salassapidosta ja luotettavuudesta. Julkisen sektorin toimiala ei ole teknologialtaan ja rakenteiltaan julkisessa tiedossa, mutta USB-väylän hyökkäykset voivat silti kohdistua niihin. Johtuen julkisen sektorin usein hieman vanhemmista järjestelmistä ja ohjelmistoista, ei niihin kohdistuvien hyökkäyksien kohdalla tarvita syvää erityisosaamista – mikäli teknisiä tietoja saadaan kalasteltua, vakoiltua tai haitallisen sisäpiiriläisen toimesta hankittua.

Tulos DREAD-arvostelussa: 38 (Korkea Riski, ylärajalla)

10.2 Infrastruktuuri

Infrastruktuurin toimijat ovat osa teollisia yhteiskunnan palveluita. Sähkön jakeluverkko, kommunikaatioyhteydet sekä energialaitosten voimantuotto ovat infrastruktuurin palveluita. Näillä toimijoilla on paitsi hallussaan joitain tunnistettavia tietoja, myös pääsy julkiseen infrastruktuuriin sekä teollisien järjestelmien verkkoon. Katkokset infrastruktuurin palveluissa vaikuttavat kaikkiin palvelun alueella, ja voivat aiheuttaa merkittävää yhteiskunnallista haittaa tehokkuudelle ja hyvinvoinnille.

Avainvara: Infrastruktuuri ja yhteiskunnalliset palvelut. Kallis laitteisto ja järjestelmä. Infrastruktuuri ja pääsy teollisiin verkkoihin- ja järjestelmiin.

Avainuhat: Palvelukatkokset, yhteiskunnallinen häiriö, laaja-alainen sabotaasi.

Avaintavoite: Yhteiskunnallinen haitta. Sabotaasi, terrorismi. Uhkailu- ja kiristystoiminta.

Taulukko 7: Infrastruktuurin DREAD-pisteytys

DREAD-Akronyymi	DREAD-Taso	Syy Tason Pisteytykseen
D – Vahinkopotentiaali	7	Laaja-alainen palvelukatkos, julkiset häiriöt
R - Toistettavuus	5	Hyökkäyksen toisintaminen mahdollista. Vaatii erityisosaamista

E - Hyväksikäytettävyys	4	Vaatii erikoisosaamista teollisuuslaitteissa
A – Vaikutetut käyttäjät	10	Palvelukatkokset koskevat kaikkia palvelun alueella
D - Löydettävyys	4	Hyökkäystapa tunnistettavissa, vaatii erityisosaamista löytää

Perustelut: Yhteiskunta on modernisoitunut ja riippuvainen toimivasta yhteiskunnallisesta infrastruktuurista. Niin kommunikaatioyhteyksien, sähkönjakelun, vedenpuhdistamoiden kuin minkä tahansa muun julkisen kiinteästi kytketyn infrastruktuuripalvelun häirintä aiheuttaa laajamittaista häiriötä ja lieveilmiöitä. Palvelukatkokset koskevat kaikkia palvelun alueella olevia, mutta toimialan erityisteknologia, laitosten omat käytännöt sekä yleisestä normista poikkeavat järjestelmät vaativat kuitenkin keskimääräistä enemmän erityisosaamista haavoittuvuuden löytämiseen, ymmärtämiseen ja hyväksi käyttämiseen.

Tulos DREAD-Arvostelussa: 30 (Korkea Riski, keskitasossa)

10.3 Palveluntuottajat

Palveluntuottajilla tässä esimerkissä tarkoitetaan mm. pilvipalveluita yrityksille ja yksityishenkilöille ylläpitäviä yhtiöitä, tietoturvasektorin yrityksiä, kirjapainoja ja -kustantamoita, sekä yleisesti muita toimialan toimijoita, joilla on yritysasiakkaita, joiden palveluiden ylläpitäminen kuuluu toimialan tehtäviin.

Avainvara: Yritysten toiminta ja palvelut. Asiakkaiden tiedot ja salassapidettävä informaatio. Pääsy asiakkaiden verkkoihin.

Avainuhat: Palvelunesto, liikkuminen asiakkaiden verkostoihin, tietovuodot teollisuuden sisäisistä tiedoista.

Avaintavoite: Yrityskohteisiin isku. Sabotaasi, yritysvakoilu. Rahallinen hyöty. Palvelunesto.

Taulukko 8: Palveluntuottajien DREAD-pisteytys

DREAD-Akronyymi	DREAD-Taso	Syy Tason Pisteytykseen

D – Vahinkopotentiaali	7	Vahinko palvelun käyttäjiin asiakasyrityksiin
R - Toistettavuus	6	Hyökkäystapoja on useita, toistaminen helppoa
E - Hyväksikäytettävyys	6	Toteutettavissa olemassa olevilla työkaluilla
A – Vaikutetut käyttäjät	6	Vaikuttaa asiakasyritysten toimintaan
D - Löydettävyys	6	Hyökkäystekniikka- ja väylä löydettävissä keskimääräisellä vaivalla

Perustelut: Palveluntuottajat hoitavat asiakasyritystensä yhteyksiä, verkko- ja pilvipalveluiden jatkuvuutta ja laatua, tietoturvaa, sekä varmuuskopioiden ylläpitämistä. Tuotanto-prosessien osalta katkokset aiheuttavat rahallista haittaa asiakasyrityksille, ja mainehaittaa heidän asiakkaidensa kautta. Yritysten välillä on kuitenkin verkkorakenteita, ja palveluntoimittajilla on usein erillinen pääsy hallinnoimaan järjestelmiä. Mahdolliset tietovuodot ja häiriöt tulevat pääasiassa koskemaan todennäköisimmin yrityksiä ja niiden tietoja, kuin henkilöitä ja heidän yksityistietojaan. Laaja-alainen tietovuoto voi kuitenkin vahingoittaa koko palvelun asiakaskuntaa, esimerkiksi uuden haavoittuvuuden tullessa esille ja vaatiessa kokonaisen palvelun refaktorointia.

Tulos DREAD-Arvostelussa: 31 (Korkea Riski, keskitasossa)

11 Jatkotutkimus

Hotplug-hyökkäyksien kenttä on jatkuvien USB-standardin päivitysten myötä jatkuvan kehityksen ja tutkimuksen alla. USB-standardeja ylläpitävät tahot viralliselta kannaltaan kehittävät USB-väylää ja sen käyttöä, eivät sen turvamekanismeja. Erilaisilta uusilta hyökkäystavoilta suojautuminen siis jää erillisen kyberturvallisuustutkimuksen varaan. USB-väylän yleisyyden, ja etenkin uuden USB-C-mallisen väylän standardoiminen älylaitteiden kommunikaatio- ja latausportiksi luo otolliset olosuhteet uusille uhille, joita vastaan tulee varautua tutkimuksella hyvissä ajoin.

Uhka-arviota voi jatkossa kehittää täsmentämällä arvioitavaa kohdetta, sekä jakamalla se pienempiin yksiköihin, joita tarkastellaan erikseen. Arvion toteuttaminen muillakin

matriisijärjestelmillä, ja vertaamalla näiden pisteytyksiä voidaan teoriassa luoda mitattava määrällistetty tutkimus väylän uhista.

Suojauksen kannalta tehokkaista käytännöistä yhdessä selkeiden tosielämän esimerkkien kanssa voi luoda ohjeistuksen, jonka täsmentäminen mahdollisen kohdeyrityksen omiin käytäntöihin ja varoihin voi kehittää turvallisuuskulttuuria pidemmälle.

Tässä opinnäytetyössä ei paneuduttu laitteiden ohjelmistoon. Mikro-ohjainten laiteohjelmisto on sulautettujen järjestelmien kehityksessä keskeinen teema, ja mikro-ohjaimien suojaus- ja ylikirjoituskeinoja on historiallisesti kierretty ja purettu hakkerien toimesta. BadUSB-hyökkäysten ohjelmoinnista olisi hyödyllistä tehdä kokoonpaneva resursseja yhdistävä laajempi katsaus – nykyiset laitekohtaiset ohjelmoinnit niin mikro-ohjaimen tasolla kuin itse laitteiden skriptauksessa ovat rönsyilleet niin laajalle, että käytännön testeissä usein kohtaa epäselvyyksiä ja sekaannuksia. Tällaiset tilanteet johtuvat esimerkiksi skriptauskielien (kuten DuckiScript) useista versioista, ja kohdelaitteiden erityisominaisuuksista.

Läheskään kaikkia valmiita laiteimplantteja ei ole kerätty tähän tutkimukseen. Uhkien kattavaan selvitykseen olisi tärkeää luoda katsaus laitteiden kenttään saatavuuden ja kustannuksien näkökulmasta.

Hotplug-implanteilla voidaan luoda useita uusia teoreettisia hyökkäyskenttiä, joitten tekninen testaaminen ja jälleen kehittäminen voi tuottaa käytettävää tutkimustietoa hyökkäysten uhan pienentämiseen. Muiden kuin USB-väylien implanttien tutkiminen yhdessä USB-väylän implanttien kanssa olisi hyvä ristiin vertailun kohde. Lisäksi älylaitteiden ominaisuus toimia niin isäntä- kuin vieraslaitteena voi luoda erilaisia hyökkäystilanteita.

USB-standardissa on lukuisia kohtia, jotka voivat vielä sisältää virheitä, heikkouksia tai ominaisuuksia, joiden hyötykäyttö hyökkäyksissä voi olla mahdollista – mutta vaatii testausta ja kehitystyötä.

12 Tulos

USB-väylään kohdistuvat hyökkäykset ovat paitsi yleistyneet, myös kehittyneet. Tilannekuvaa ei paranna USB-väylän yleistyminen ehkä maailman käytetyimmäksi portiksi tietotekniikassa. USB-C-tyyppisiin USB-väyliin on lisätty hybriditoiminnallisuus virran vastaanottamiseksi kannettavien tietokoneiden lataamiseksi. Tämä mahdollistaa hybridikäytöksellä uudenlaisia moniulotteisia BadUSB-tekniikoita, joissa voidaan yhdistellä erilaisia sivukanavatekniikoita ja laitetunnisteita luoden uusia hyökkäyksen variaatioita.

Kaikkien arvioitujen toimialojen riskin taso oli korkea. Tämä tarkoittaa, että hyökkäysväylänä USB-laitteet ja niiden ympäröivä kenttä vaatii huomiota ja tulevia toimenpiteitä. Uhka ei ole juuri nyt kriittinen DREAD-matriisissa, mutta se ei tarkoita, etteikö aiheutunut haitta aiheuttaisi kriittisiä toiminnallisia häiriöitä eri sektoreilla.

Hotplug-hyökkäyksiä vastaan puolustaminen on paitsi haastavaa, myös aiheuttaa rajoitteita laitteiden käytettävyydelle sekä käyttäjille. Tämä monimutkaistaa tilannetta, vaatien myös kokovaltaista turvallisuuskulttuurin muutosta, jotta vastoinkäymisiltä vältyttäisiin.

USB-väylä on yleisyydestään johtuen historiallisesti niin käytännössä kuin teoriatasolla portti, joka avaa hyökkäysmahdollisuuden lähes kaikkiin kohteisiin. Lisäongelmana ja riskitekijänä voidaan pitää väylään kohdistuvien iskujen monimuotoisuuttaa ja monikäyttöisyyttä – iskut usein aiheuttavat sivuhaittoja ja lieveilmiöitä, jotka kohdistuvat muihin verkkoihin, kohteisiin, tai uhreihin alkuperäisen iskun kohteen lisäksi ja ympäriltä.

Lisätutkimusta sekä uusia tehokkaampia puolustuskeinoja tarvitaan kipeästi. Standardi itsessään tarjoaa tekniset puitteet väylän toiminnoille ottamatta kantaa turvallisuuteen. Väylän suojaamisen tulee siis pysyä jatkuvasti USB-standardin päivitysten mukana uusien toiminnallisuuksien ja laitekategorioiden lisäyksien yhteydessä.

Tarve suojata USB-väyliä, sekä kehittää jatkuvasti uusia tekniikoita niiden puolustamiseen on todellinen. Uhkaa voidaan pitää merkittävänä, vaatien jatkokehitystä sekä omistautuneisuutta sen vähentämiseen ja riskien pienentämiseksi.

Lähteet

Alm, E. & Aaris-Larsen, A., 2023. *USB Hid-and-Run.* [Online]
Available at: https://github.com/piraija/usb-hid-and-run
[Accessed 16 January 2025].

Anderson, B. & Anderson, B., 2010. *Seven Deadliest USB Attacks.* Burlington, USA: Syngress (an Imprint of Elsevier, Inc.).

Applebaum, J., 2013. *NSA ANT USB, 30C3,* s.l.: s.n.

Axelson, J., 2009. *USB Complete: The Developer's Guide.* Fourth Edition ed. Chinook Ln.: Lakeview Research LLC.

Badrignans, B., 2013. *Attaques applicatives via périphériques USB modifiés : infection virale et fuites d'informations.* s.l., s.n.

Blanchet, S., 2018. BadUSB, the threat hidden in ordinary objects.

Blue Goat Cyber, 2025. *Hacking Tool: Bash Bunny.* [Online]
Available at: https://bluegoatcyber.com/blog/what-is-a-bash-bunny/
[Accessed 30 01 2025].

Cannols, B. & Ghafarian, A., 2017. Hacking Experiment by Using USB Rubber Ducky Scripting.

Conklin, L., n.d. *Threat Modeling Process.* [Online]
Available at: https://owasp.org/www-community/Threat_Modeling_Process
[Accessed 16 January 2025].

Digital Citizenship and Surveillance Society, 2015. *Ant Catalogue.* [Online]
Available at: https://dcssproject.net/ant-catalogue/index.html
[Accessed 25 01 2025].

Dung, V. P., Syed, A., Mohammad, A. & Halgamuge, M. N., 2010. *Threat analysis of portable hack tools from USB storage devices and protection solutions.* Karachi, Pakistan, IEEE.

EC-Council, n.d. *EC-Council Cybersecurity Exchange.* [Online]
Available at: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/
[Accessed 21 04 2025].

FIRST, n.d. *Common Vulnerability Scoring System version 4.0: Specification Document.* [Online]

Available at: https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf
[Accessed 08 02 2025].

Flipper, 2025. *Flipper Zero - Portable Multitool for Geeks.* [Online]
Available at: https://flipperzero.one/
[Accessed 30 01 2025].

Flipper, 2025. *Flipper Zero Documentation, Bad USB.* [Online]
Available at: https://docs.flipper.net/bad-usb
[Accessed 30 01 2025].

Gallagher, S., 2020. *Introduction to JTAG and the Test Access Port (TAP).* [Online]
Available at: https://www.allaboutcircuits.com/technical-articles/introduction-to-jtag-test-access-port-tap/
[Accessed 28 01 2025].

Hak5, 2024. *Bash Bunny by Hak5 Product Documentation.* [Online]
Available at: https://docs.hak5.org/bash-bunny
[Accessed 30 01 2025].

Hak5, 2025. *OMG-Cable.* [Online]
Available at: https://shop.hak5.org/products/omg-cable
[Accessed 31 01 2025].

Heymann, E., Miller, B. P. & Kohnfelder, L., 2023. *Introduction to Software Security, Chapter 2.4: Microsoft DREAD Threat Classification.* [Online]
Available at: https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/Chapters/2_4-DREAD-Threat-Categories.pdf
[Accessed 16 January 2025].

Honeywell, 2020. *USB SECURITY- MYTHS VS. REALITY.,* Houston, TX: Honeywell Process Solutions .

Honeywell, 2024. *HONEYWELL GARD USB THREAT REPORT 2024,* s.l.: Honeywell.

Kierznowski, D. & Mayes, K., 2015. *BADUSB 2.0: EXPLORING MAN-IN-THE-MIDDLE ATTACKS.* s.l.:Royal Holloway.

Liucveikis, K., 2024. *PCrisk.* [Online]
Available at: https://www.pcrisk.com/internet-threat-news/31448-steelfox-seen-using-qbring-your-own-vulnerable-driverq-tactics
[Accessed 10 04 2025].

Liu, H. et al., 2021. USB powered devices: A survey of side-channel threats and countermeasures. *High-Confidence Computing,* 1(1).

Masters, A. & Madisetti, V. K., 2024. Side-Channel Attacks & Data Exfiltration Using Wall Outlet USB Power Adapters. *Journal of Information Security,* Volume 15, pp. 433-447.

mg, 2019. *omg-cable.* [Online]
Available at: https://mg.lol/blog/omg-cable/
[Accessed 31 01 2025].

MG, 2023. *a few questions regarding the cable.* [Online]
Available at: https://forums.hak5.org/topic/58216-a-few-questions-regarding-the-cable/
[Accessed 31 01 2025].

Nicho, M. & Sabry, I., 2023. *Bypassing Multiple Security Layers Using Malicious USB Human.* Lisbon, Portugal, SCITEPRESS, pp. 501-508.

Nohl, K., Krißler, S. & Lell, J., 2014. *BadUSB — On accessories that turn evil.* Tokyo, Japan, Pacsec 2014.

Nohl, K., Lell, J. & Krißler, S., 2014. *BadUSB - On accessories that turn evil.* Las Vegas, USA, Blackhat USA 2014.

Parnell, G. & Saydjari, O., 2005. Mission Oriented Risk and Design Analysis of Critical Information Systems. *Military Operations Research,* Volume March, pp. 19-38.

Proofpoint, 2022. *State of the Phish 2022,* s.l.: DXC Technology.

Queppet, J., 2018. *The Hardware Components of a USB Rubber Ducky,* s.l.: s.n.

Rose, A., 2022. *Cybercriminals bring the USB back, with a Vengeance.* [Online]
Available at: https://www.itp.net/insight/cybercriminals-bring-the-usb-back-with-a-vengeance
[Accessed 23 01 2025].

Tischer, M. et al., 2016. *Users Really Do Plug in USB Drives They Find.* San Jose, CA, USA, IEEE.

USBKill.com, 2025. *USBKill.com.* [Online]
Available at: https://usbkill.com/
[Accessed 10 04 2025].

Walters, P., 2012. *The Risks of Using Portable Devices,* s.l.: s.n.

Wynn, J., 2014. *Threat Assessment and Remediation Analysis (TARA)*. [Online]
Available at: https://www.mitre.org/sites/default/files/2021-10/pr-14-2359-tara-introduction-and-overview.pdf
[Accessed 16 January 2025].

Kuviot

Taulukot