Henri Jussila

Tekniikat internet-reititysten kaappaamisen estämiseksi

Tietotekniikan kandidaatintutkielma

9. toukokuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Henri Jussila

Yhteystiedot: henri.m.jussila@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Tekniikat internet-reititysten kaappaamisen estämiseksi

Title in English: Techniques to stop internet-routing hijacking

Työ: Kandidaatintutkielma

Opintosuunta: Kaikki opintosuunnat

Sivumäärä: 25+0

Tiivistelmä: Tutkielmassa tarkastellaan Border Gateway Protocollan tietoturvaongelmia, sekä kuinka nämä ongelmat mahdollistavat Internet-reitityksen kaappaamisen. Tietoturvaongelmiin etsitään ratkaisuja vertailemalla kirjallisuudessa esitettyjä parannuksia Border Gateway Protocollaan, ja selvitetään syitä miksi mitään parannusta ei ole otettu laajasti käyttöön. Parannuksia vertailtaessa havaitaan, että kaikilla vertailtavilla ratkaisuilla on omat heikkoutensa ja vahvuutensa, minkä seurauksena yksittäinen ratkaisu ei kykene täyttämään kaikkien tahojen tarpeita, vaan joudutaan tekemään kompromissi.

Avainsanat: BGP,S-BGP,ROVER,PGBGP,ARGUS,tietoturva

Abstract: The thesis looks at the Border Gateway Protocol and the security problems it has, and how these problems allow the hijacking of internet-routing. The thesis looks at possible solutions to these problems by comparing improvements to the Border Gateway protocol that have been proposed in research literature, and why none of the proposed solutions has reached widespread adoption. During the comparision it is found that all the proposed solutions have their strengths and weaknesses. This leads to the implication that there is not a single solution that would fix the security problems in Border Gateway Protocol, instead if there is to be a solution it needs to be a compromise.

Keywords: BGP,S-BGP,ROVER,PGBGP,ARGUS,security

Taulukot

Sisältö

1 Johdanto

Internet koostuu joukosta internet-operaattoreiden hallinnoimia verkkoja, jotka ovat yhteydessä toisiinsa. Jotta liikenne internetin osaverkkojen välillä toimii, tarvitaan yhteinen protokolla, jonka avulla verkkojen operaattorit pystyvät kommunikoimaan keskenään liikenteen ohjaamisesta osaverkosta toiseen. Border Gateway Protocollaa (BGP) (Rekhter, Li ja Harres 2006) käytetään internetin reitti-ilmoitusten jakamiseen operaattoreiden välillä.

BGP:ssä ei ole protokollaan sisäänrakennettua tietoturvaa, joka mahdollistaisi reitti-ilmoituksen lähettäjän henkilöllisyyden varmistamisen tai ilmoituksen sisällön oikeellisuuden tarkastamisen. Nämä tietoturvapuutteet tekevät BGP:stä alttiin, sekä tarkoituksellisille kaappauksille, että myös inhimillisille näppäilyvirheille, joiden seurauksena internetin reitityksen turvallisuus saattaa vaarantua. Kirjallisuudessa on esitetty useita mahdollisia ratkaisuja, joilla BGP:n turvallisuutta voitaisiin parantaa. Tutkielmassa tarkastellaan esitetyistä ratkaisuista Secure Border Gateway Protocollaa (Kent, Lynn ja Seo 2000), Route Origin Verificationia (Gersch ja Massey 2013), Pretty Good Border Gateway Protocollaa (Karlin, Forrest ja Rexford 2006) ja ARGUS:ta (Xiang ym. 2011).

Tutkielman tavoitteena on selvittää syitä miksi BGP-kaappausten estämiseksi ei ole otettu konkreettisia toimenpiteitä, vaikka mahdollisia ratkaisuja on esitetty kirjallisuudessa useiden vuosien ajan. Tutkielman alussa käsitellään BGP:n toimintaa sekä syitä miksi BGP:n tietoturva on heikko. Tämän jälkeen tarkastellaan yllä mainittujen tekniikoiden toimintaa tarkemmin. Lopuksi tutkielmassa vertaillaan tekniikoita keskenään ja yritetään selvittää mahdollisia syitä, jotka tekevät yhdestä tekniikasta muita paremman tai huonomman.

2 BGP-reititysprotokolla

BGP on protokollana vanha. Alkuperäinen versio protokollasta on vuodelta 1990 (Lougheed ja Rekhter 1990). Protokollan uusin versio on vuodelta 2006 (Rekhter, Li ja Harres 2006). Vuoden 2006 jälkeen protokollaan on tehty useita lisäyksiä, mutta itse protokollaa ei ole vuoden 2006 jälkeen päivitetty. Protokollaan iästä johtuen protokollasta puuttuu paljon ominaisuuksia, joita nykyään pidettäisiin itsestäänselvinä. Ensimmäisessä alaluvussa käsitellään protokollan toimintaa teknisellä tasolla, sekä tarkastellaan protokollan puutteita ja näistä puutteista aiheutuvia tietoturvaongelmia. Luvun toisessa alaluvussa käsitellään tietoturvaongelmien seurauksia, joita hyödyntämällä BGP:n reitityksen toimintaa voidaan häiritä.

2.1 BGP-protokollan tekninen toiminta

BGP-protokollan toiminta on määritelty RFC-dokumentissa 4271 (Rekhter, Li ja Harres 2006). BGP on sovelluskerroksen (application layer) protokolla, jolla BGP-operaattori pystyy käyttämään reitti-ilmoituksia ilmoittamaan kohteita, joihin operaattori pystyy ohjaamaan internet-liikennettä. BGP:n kommunikaatio voi tapahtua autonomisen järjestelmän (Autonomous System, [AS]) (Hawkinson ja Bates 1996) sisällä olevien kahden reitittimen välillä, jolloin sitä kutsutaan Internal BGP:ksi (IBGP). Mikäli kommunikaatio tapahtuu kahdessa eri autonomisessa järjestelmässä sijaitsevien reitittimien välillä, kutsutaan kommunikaatiota silloin External BGP:ksi (EBGP).

Protokollan määritelmän (Rekhter, Li ja Harres 2006) mukaan reitti-ilmoitukset välitetään "UPDATE"viestillä, jolla voidaan ilmoittaa käytöstä poistuneet reitit sekä samalla ilmoittaa uudesta reitistä. Yksittäinen UPDATE viesti voi sisältää poistoja, lisäyksiä tai molempia näistä (Rekhter, Li ja Harres 2006). BGP:n viestiliikenne kuljetetaan TCP-protokollalla (Postel 1981). TCP takaa viestiliikenteen virheettömyyden, mutta TCP:ssä ei ole sisäänrakennettua tietoturvaa, joten TCP ei takaa viestin lähettäjän oikeellisuutta, tai että viestiä ei olisi muokattu matkalla.

Protokollan nykyisin käytössä oleva neljäs versio (Rekhter, Li ja Harres 2006), vaatii MD5-hajautusalgoritmin (Rivest 1992) käyttämistä osapuolten identiteetin. MD5:n algoritmissa on

kuitenkin jälkeenpäin havaittu merkittäviä heikkouksia. Näiden heikkouksien seurauksena MD5:lla tehty allekirjoitus kyetään väärentämään, eikä MD5 ole siten enään nykyään turvallista käyttää henkilöllisyyden varmentamiseen. MD5:n sisältämiä heikkouksia on tarkasteltu tarkemmin muun muassa teoksessa (Stewens, Lenstra ja Weger 2012). Myöhemmässä kirjallisuudessa on esitetty keinoja BGP:n turvallisuuden parantamiseksi, kuten (Touch, Mankin ja Bonica 2010) on käsitellyt, mutta BGP-protokollaa ei ole päivitetty versiosta neljä hyödyntämään näitä esitettyjä keinoja, tai vaatimaan ajantasaisen salauksen käyttämistä. Tilanteesta seuraa se, että BGP-protokolla ei vaadi käytettäväksi turvallista tapaa varmentaa reitin ilmoittajan oikeellisuus, tai ilmoitetun reitin oikeellisuus (Bakkali, Benaboud ja Ben Mamoun 2013). Nämä tekijät yhdistettynä TCP:n (Postel 1981) turvattomuuteen avaavat mahdollisuuden sekä tarkoituksellisille BGP-kaappauksille, että myös tahattomille inhimillisille virheille, joista molemmat voivat vaarantaa internetin yleisen toiminnallisuuden (Murphy 2006). Seuraavissa alaluvuissa käsitellään kuinka BGP-kaappaukset voivat konkreettisesti tapahtua, sekä kuinka kaappausten tapahtumista voidaan torjua.

2.2 BGP-reitityksen häiriöt

BGP-reitityksen häiriöt voidaan jakaa kahteen erilliseen kategoriaan, riippuen siitä aiheuttiko häiriön tarkoituksellinen kaappaus, vai tahaton inhimillinen virhe. Ensimmäiseksi luvussa käsitellään tarkoituksellisien kaappauksien syitä, sekä mahdollisia seurauksia ja hyötyjä kaappaajalle. Tämän jälkeen tarkastellaan lyhyesti tahattomia kaappauksia.

Kaappaajalla on useita mahdollisuuksia tarkoituksellisen kaappauksen toteuttamiseksi. Kaappaaja voi ilmoittaa toisen tahon omistaman verkko-osoitteen (Fuller ja Li 2006) omana ilmoituksenaan, ja mikäli reitti käyttäjältä kaappaajaan on lyhempi, kuin reitti oikeaan kohteeseen, ohjaa BGP-protokolla liikenteen kaappaajalle. Toinen mahdollinen kaappaustekniikka on ilmoittaa alkuperäistä ilmoitettua osoitetta tarkempi osoite, ja näin lähettää kaikki liikenne kaappaajalle reitin pituudesta huolimatta (Rashevskiy ja Shaburov 2017).

Tarkoituksellisella BGP-kaappauksella voidaan ohjata liikenne alkuperäisestä kohteesta eroavaan kohteeseen. Liikennettä voidaan uudelleenohjauksen aikana salakuunnella ja tallentaa, ennen kuin liikenne kuljetetaan alkuperäiseen kohteeseensa (Murphy 2006). Tällöin käyttä-

jä ei välttämättä edes huomaa hyökkäyksen tapahtuvan, koska internet-liikenne ei keskeydy, se vain hidastuu hieman kaappauksen aikana. Toinen mahdollinen hyöty tarkoituksellisesta BGP-kaappauksesta on liikenteen pysäyttäminen kokonaan. Tässä tapauksessa liikenne ei koskaan saavuta tarkoitettua kohdettaan, eikä käyttäjä pysty käyttämään haluamaansa internet-palvelua (Murphy 2006).

Tahattomat kaappaukset ovat yleensä seurausta inhimillisestä virheestä, kun BGP-reitittimeen konfiguroidaan reittiä, ja tallentaja tekee näppäilyvirheen, kirjoittamalla esimerkiksi numeron 9 sijaan numeron 8 (Cho ym. 2019). Tahattomalla kaappauksella on pitkälti samat seuraukset kuin tarkoituksellisellakin kaappauksella. Reitti-ilmoitus voi muuttaa reittiä, jonka tieto kulkee saavuttaakseen tarkoitetun kohteensa, joissain tapauksissa on myös mahdollista, että reitin muutos estää tietoa kokonaan saavuttamasta tarkoitettua kohdettaan (Rashevskiy ja Shaburov 2017)

2.3 BGP-reitityksen turvaaminen

Koska sekä tarkoituksellinen että tahaton reitin kaappaus johtavat pitkälti samaan tilanteeseen, jossa BGP-reitit muuttuvat, ja tietoliikenteen toimivuus vaarantuu, molemmat ongelmatapaukset voidaan periaatteessa ratkaista, jos pystytään varmentamaan reitti-ilmoituksen oikeellisuus sekä tarkoituksellisuus. Osaongelma reitti-ilmoituksen varmentamisessa on aikaisemmin esitetty ilmoittajan oikeellisuuden varmentamisen puute (Bakkali, Benaboud ja Ben Mamoun 2013). Mikäli BGP-operaattorit varmentaisivat saamiensa BGP-viestien lähettäjän, pystyttäisiin valtaosa tarkoituksellisista kaappauksista estämään, koska kaappaajalla ei ole keinoa vahvistaa henkilöllisyyttään, ellei kaappaaja ole saanut käsiinsä varmennukseen käytettävää avainta.

Viestin lähettäjän varmentaminen ei kuitenkaan pelkästään riitä, koska BGP-operaattori saattaa tehdä näppäilyvirheen, joka hyväksytään varmennuksessa, koska ilmoitus tulee oikealta taholta. Tässä tilanteessa tarvitaan toisenlainen ratkaisu, joka pystyy tunnistamaan poikkeuksellisen reitti-ilmoituksen, ja estämään sen. Seuraavassa luvussa käsitellään ratkaisuja, joilla edellä esitetyt ongelmat voidaan ratkaista.

3 Ratkaisut BGP-reitityksen turvaamiseksi

Edellisessä kappaleessa esitettiin kaksi konkreettista ongelmaa: omistajan varmentaminen, sekä ilmoituksen oikeellisuuden tarkastaminen. Kirjallisuudessa on esitetty useita ratkaisuja molempiin esitettyihin ongelmiin, mutta tutkielman laajuus rajoittaa tarkasteltavien teknologioiden määrän neljään. Omistajan varmennuksen ratkaisuun tutkielma käsittelee kahta tekniikkaa: S-BGP ja ROVER. Ilmoituksen oikeellisuuden tarkastamisen ratkaisemiseksi tarkastelussa ovat PGBGP sekä ARGUS.

3.1 Varmennustekniikat

Varmennustekniikat perustuvat tietokantaan, joissa säilytetään ajantasaista tietoa siitä, kuka omistaa tietyt IP-osoitteet, ja saa ilmoittaa niitä. Tietokannan toteutukselle on olemassa useita erilaisia ratkaisuja. Tutkielmassa käsitellään näistä kahta, joista ensimmäinen on sertifikaattipohjainen (Cooper ym. 2008) Secure Border Gateway Protocol, ja toinen on DNS-järjestelmään (Mockapetris 1987) tukeutuva ROVER. Näiden teknologioiden lisäksi on olemassa muitakin varmennustekniikoiksi luettavia ratkaisuja, kuten CP-BGP (Wu, Yu ja Wang 2018), ja RPKI (Bush ja Austein 2013). Varmennustekniikat vaativat toimiakseen laaja-alaisen käyttöönoton, jossa operaattorit lisäävät omistamiensa IP-osoitteiden tiedot tietokantaan varmennusta varten, koska mikäli IP-osoitteen tietoja ei ole lisätty tietokantaan, ei IP-osoitteen omistajuutta pystytä varmentamaan.

3.1.1 Secure Border Gateway Protocol

Secure Border Gateway Protocol (S-BGP) on käsiteltävistä ratkaisuista vanhin, ja perustuu julkisten avainten käyttöön (Public Key Infrastructure, [PKI]) (Cooper ym. 2008), sekä X.509 pohjaisiin sertifikaatteihin. X.509 on International Telecommunications Unionin (ITU) ylläpitämä standardi, joka määrittelee sertifikaatissa käytettävän rakenteen ja toiminnan, sekä sen kuinka sertifikaatti voidaan tarvittaessa perua. Sertifikaatissa sidotaan IP-osoite(et) julkiseen avaimeen, jonka IP-osoitteen omistaja pystyy yksityisellä avaimellaan allekirjoittamaan, ja näin osoittamaan olevansa IP-osoitteiden omistaja.

Sertifikaatteja voidaan allekirjoittaa ketjussa alaspäin. Esimerkiksi ICANN voisi allekirjoittaa juurisertifikaatin (Root certificate), joka kattaa kaikki IP-osoitteet, mutta tämän jälkeen sertifikaattien myöntämistä voidaan jakaa esimerkiksi maantieteellisesti pienempiin ja pienempiin osiin, kunnes saavutetaan yksittäisen operaattorin taso, joka voi myöntää sertifikaatit omille IP-osoitteilleen (Kent, Lynn ja Seo 2000).

Jotta järjestelmä on toimiva, täytyy pitää yllä listaa (Certificate Revocation List (CRL)) sertifikaateista, jotka niiden myöntäjä on perunut ennenaikaisesti. Listan hyötynä on, että mikäli ylempänä ketjussa oleva sertifikaatti perutaan. Peruuntuvat automaattisesti kaikki ketjussa alempana olevat sertifikaatit, koska ne on allekirjoitettu käyttäen ylempää sertifikaattia. Toimiakseen järjestelmän täytyy ylläpitää lista kaikista sertifikaateista, joilla reittien aitous voidaan vahvistaa, sekä toinen lista sertifikaateista, jotka on jostain syystä peruttu.

Järjestelmän toiminta perustuu kahdenlaisiin vahvistuksiin. Osoitteenvahvistus, sekä reitinvahvistus (Kent, Lynn ja Seo 2000, 5). Osoite vahvistuksella osoitetaan, että reitin mainostajalla on oikeus mainostaa reittiä. Reittivahvistuksella osoitetaan, että kuljettavalla AS:lla on oikeus kuljettaa tietoa eteenpäin. Kun uusi reitti ilmoitetaan UPDATE-viestillä, tarkistetaan, että sekä reitin ilmoittajalla että reitin varrella olevilla AS:illä on oikeat vahvistukset liikenteen kuljettamiseksi, ja osoiteryhmä on myönnetty reitin ilmoittajalle.

3.1.2 Route Origin Verification System

Route Origin Verification Systemin (ROVER) (Gersch ja Massey 2013) toiminta perustuu kahteen lisäykseen. Ensimmäinen lisäys on nimeämisjärjestelmä, jonka avulla pystytään antamaan jokaiselle ilmoitettavalle IP-osoiteryhmälle yksilöllinen nimi, jolla osoiteryhmä voidaan tunnistaa muista osoiteryhmistä. Toinen lisäys on uusi tietue, joka lisätään DNS-järjestelmään (Mockapetris 1987). Tietueeseen tallennetaan tieto sallituista mainostajista. Tietueen tyyppi on "SRO"(Secure Route Origin), ja rakenne on yksinkertainen, sen nimenä käytetään nimeämisjärjestelmän osoiteryhmälle antamaa nimeä. Tietue sisältää vain yhden sisältökentän, jossa ilmoitetaan AS:n numero(t) jotka saavat mainostaa osoiteryhmää.

ROVER:in hyödyntämiseen esitetään mallia, jossa jokainen BGP-ilmoitus tarkastetaan, ja se luokitellaan automaattisesti yhteen kolmesta kategoriasta: "VALID", "INVALID"tai "NOT-

FOUND". VALID-luokitus annetaan, kun ilmoitus pystytään vahvistamaan oikeaksi, INVALID-luokitus tulee antaa, kun pystytään vahvistamaan, että reitti-ilmoituksessa on virhe. Muissa tilanteissa tulee antaa NOTFOUND-luokitus reitille. ROVER ei ota kantaa siihen, miten BGP-operaattori käyttää tätä reitille annettua luokitusta, ja eroaa siten merkittävästi S-BGP:stä (Kent, Lynn ja Seo 2000), joka määrittelee toteutuksen kaikki vaiheet tarkasti. BGP operaattori voi halutessaan liittää ROVER:in suoraan reitittimiinsä, tai vain antaa ilmoituksen, kun kaappaus havaitaan, johon ihminen voi reagoida haluamallaan tavalla.

ROVER käyttää toteutuksessaan DNS-palvelimia, joten on tärkeää ottaa huomioon ROVER:in käytön mahdolliset vaikutukset DNS-infrastruktuuriin. Tutkijoiden käyttämän vuoden 2013 aineiston (Gersch ja Massey 2013, 8) mukaan globaalissa reititystaulussa oli noin 400 tuhatta osoitetta. Pahimmassakin tapauksessa yhteen serveriin kohdistunut kuorma oli vain 464 pyyntöä sekunnissa mikä on vähän pyyntöjä DNS serverille. Esimerkiksi Googlen julkinen DNS infrastruktuuri vastasi yli 70 miljardiin pyyntöön päivässä vuonna 2012 (Chen 2012), mikä vastaa noin 810 tuhatta pyyntöä sekunnissa. Nykyään osoitteiden määrä globaalissa reititystaulussa on kaksinkertaistunut yli 820 tuhanteen osoitteeseen (Huston, Smith ja Bates 2020). Reititystaulun kasvun mahdolliset vaikutukset DNS-palvelimiin aiheutettuun kuormaan tulisi tarkastaa nykytiedon valossa, koska mikäli aiheutettu kuorma on merkittävä, vaatisi nykyinen DNS järjestelmä päivityksiä, mikä aiheuttaisi lisää kuormaa ympäristölle.

3.2 Tarkastustekniikat

Tarkastustekniikat perustuvat varmentamisen sijaan siihen, että ylläpidetään tietoa "normaalista tilasta", ja verrataan uusia BGP-ilmoituksia "normaaliin tilaan". Mikäli ilmoitettu reitti sopii normaaliin tilaan, hyväksytään reitti-ilmoitus. Mikäli reitti ei täytä "normaalin tilan"ehtoja, hylätään reitti-ilmoitus. Hylätylle reitille tehtävät toimenpiteet riippuvat käytettävästä tekniikasta. Pretty Good Border Gateway Protocol (Karlin, Forrest ja Rexford 2006) asettaa hylätyt reitit karanteeniin, josta ne otetaan käyttöön vain, jos ne ovat määritellyn ajan jälkeen edelleen voimassa. ARGUS (Xiang ym. 2011) lähettää hylkäystilanteessa varoituksen, johon operaattori voi reagoida haluamallaan tavalla. Tarkastustekniikat eroavat varmennustekniikoista myös siten, että ne eivät tarvitse laajaa käyttöönottoa, vaan operaattori voi halutessaan ottaa tekniikan käyttöönsä yksin. Muita tarkastustekniikoiksi luettavia

ratkaisuja ovat esimerkiksi: HC-BGP (Zhang ym. 2009), ARTEMIS (Sermpezis ym. 2018) ja Hijacking Event Analysis Program (Schlamp ym. 2016).

3.2.1 Pretty Good Border Gateway Protocol

Pretty Good Border Gateway Protocol (PGBGP) (Karlin, Forrest ja Rexford 2006) käyttää tietoa aikaisemmin käytössä olleista reiteistä päättäessään, onko reitti oikea, vai onko se virheellinen. Reitti voi olla virheellinen kahdesta syystä. Ensimmäisessä tapauksessa reitti-ilmoitukseen on tullut vahingossa virhe, toisessa tapauksessa reitti-ilmoitus on tehty tarkoituksellisesti, niin että reitti vaikuttaa kolmannen osapuolen toimintaan (Cho ym. 2019).

Koska PGBGP käyttää reittien oikeellisuuden määrittelyyn historiallista tietoa reiteistä, on käyttöönottovaiheessa hyväksyttävä kaikki reitit, jotta voidaan muodostaa "normaali"jota vastaan uusia reitti-ilmoituksia voidaan verrata. Normaalin muodostuksen ollessa valmis, uudet reitit sijoitetaan karanteeniin, josta ne liitetään osaksi normaalia vain, jos ne ovat edelleen olemassa määritellyn ajan kuluttua reitin ilmoituksesta. Myös vanhat reitit tulee poistaa normaalista, mikäli ne eivät ole olleet määriteltyyn aikaan käytössä. (Karlin, Forrest ja Rexford 2006)

On tärkeää että karanteenin pituus, sekä aika jossa vanhat reitit poistuvat normaalista on määritelty sopiviksi. Mikäli karanteenin pituus on liian lyhyt, saatetaan hyväksyä virheellisiä reittejä järjestelmään, mutta jos karanteeni on liian pitkä, jäävät oikeat reitti-ilmoitukset sinne turhaan. Mikäli vanhojen reittien säilytysaika on liian lyhyt, tullaan reittejä asettamaan turhaan karanteeniin. Säilytysajan ollessa liian pitkä, tullaan hyväksymään reittejä, jotka eivät välttämättä enää ole samassa käytössä missä ne olivat, kun ne hyväksyttiin säilytykseen. Näiden aikaikkunoiden määrittelyyn ei ole yhtä ainoaa oikeaa vastausta, vaan joudutaan löytämään tasapaino. Tutkijat esittävät karanteenin pituudeksi 24 tuntia, ja säilytysajaksi 10 vuorokautta. (Karlin, Forrest ja Rexford 2006, 4)

3.2.2 ARGUS

ARGUS (Xiang ym. 2011) eroaa muista käsitellyistä ratkaisuista merkittävästi siten, että ARGUS saa datansa yhden operaattorin sijaan BGPMON (“BGPMON” 2020) palvelulta.

Koska ARGUS saa dataa useammalta kuin yhdeltä BGP-operaattorilta. ARGUSin on helpompi havaita kaappausyritys. ARGUS koostuu kolmesta erillisestä moduulista. Moduuleista ensimmäinen on Anomaly Monitoring Module (AMM), joka seuraa BGPMON:in avulla globaalia BGP-liikennettä, ja tarkastaa uudet ilmoitukset. Mikäli BGP-ilmoitusta ei löydetä AMM tietokannasta, siirtää AMM ilmoituksen Hijacking Identification Modulelle (HIM), joka tekee päätöksen ilmoituksen oikeellisuudesta. ARGUSin kolmas moduuli on Live-IP collection Module (LCM), joka kerää IP osoitteet jokaiselle reititettävälle osoiteryhmälle.

HIM käyttää mahdollisten kaappausten tarkistamiseen niin kutsuttuja katselupalvelimia (looking glass server), joissa ARGUS käynnistää kahdenlaisia säikeitä: C-säikeitä sekä D-säikeitä. C-säikeillä ARGUS selvittää katselupalvelimelta lyhimmän BGP-reitin mahdolliseen kaappaukseen. C-säie palauttaa 0, mikäli reitiltä havaitaan AMM:n löytämä poikkeus. Mikäli poikkeusta ei löydetä, reitiltä palauttaa säie 1. D-säie taas käyttää "ping"komentoa tarkistaakseen, pystyykö palvelin vastaamaan siihen. Mikäli ping saa palvelimelta vastauksen, palauttaa D-säie yksi, muissa tapauksissa 0. Mikäli useat katselupalvelimilla ajetut C-ja D-säikeet palauttavat samaan aikaan saman tuloksen (0 tai 1 molemmista säikeistä), voidaan tällöin olettaa todennäköisesti kyseessä olevan BGP-kaappaus (Xiang ym. 2011, 46). C- ja D-säikeiden korrelaatio ei kuitenkaan ole absoluuttinen, joten ennen kaappaushälytyksen antamista ARGUS vertaa C- ja D-säikeiden korrelaatiokerrointa, joka saadaan C- ja D-säikeiden keskiarvojen summien avulla (Xiang ym. 2011, 46). Mikäli korrelaatiokerroin on lähellä arvoa yksi, antaa ARGUS kaappaushälytyksen.

ARGUSin toiminta loppuu kaappaushälytyksen antamiseen. Mitä kaappaushälytykselle tehdään on täysin operaattorin päätettävissä. Yksi mahdollisuus on automatisoida reittien hylkääminen hälytyksen saapuessa. Toinen mahdollisuus on ilmoittaa havaitusta kaappauksesta teknikolle, joka voi tarkastaa hälytyksen todenperäisyyden, sekä tarvittaessa poistaa reitin.

4 Tekniikoiden vertailu

Tässä luvussa käsittellään edellisessä luvussa esitettyjä tekniikoita kolmesta erilaisesta näkökulmasta. Ensimmäisenä näkökulmana tarkastellaan tekniikoiden käyttöönoton vaatimia investointeja. Toisena tarkasteltavana näkökulmana käsitellään tarvittavaa yhteistyön määrää. Kolmantena näkökulmana käsitellään tekniikan luotettavuutta, ja sitä kuinka tehokkaasti tekniikka poistaisi BGP-kaappaukset. Viimeisessä alaluvussa pohditaan tekniikoiden vahvuuksia, ja heikkouksia toisiinsa nähden. Tutkittavat näkökulmat valikoituvat osittain teoksen (Butler ym. 2010) pohjalta, näkökulmia kehitettiin edelleen teoksessa (Gersch ja Massey 2013). Jokaiselle tekniikalle annetaan jokaisesta alaluvusta arvosana. Näiden arvosanojen kriteerit esitetään alalukujen alussa.

4.1 Takautuva toimivuus ja investointitarve

Takautuva toimivuus on syytä ottaa huomioon tekniikoita tarkateltaessa, koska jos tekniikan käyttöönotto vaatii infrastruktuurin uudistamista, on kyseessä merkittävä pakollinen sijoitus operaattoreille, joka saattaa vaikeuttaa johdon tuen saamista hankkeelle. Johdon tuen puute on havaittu merkittäväksi osatekijäksi hankkeiden epäonnistumisessa esimerkiksi teoksissa (Kappelman, McKeeman ja Zhang 2006) sekä (Hughes, Rana ja Simintiras 2017). Toiseksi kaikesta nykyisestä BGP-infrastruktuurista tulisi käyttökelvotonta, ja nykyinen infrastruktuuri jouduttaisiin kierrättämään ja/tai hävittämään. Tämä aiheuttaisi nousun jo nyt merkittävään määrään vuosittaista elektroniikkajätettä (Baldé ym. 2017).

Kategoriasta annetaan luokitukset seuraavien kriteereiden mukaan:

- **Vähäinen** luokitus annetaan, mikäli teknologia voidaan ottaa käyttöön ilman, merkittävää investointia ja BGP-protokollan päivitystä.
- **Huomattava** luokitus annetaan, mikäli teknologia vaatii joko merkittävän investoinnin tai BGP-protokollan päivityksen.
- **Merkittävä** luokitus annetaan, mikäli teknologia vaatii merkittävän investoinnin sekä BGP-protokollan päivityksen.

S-BGP vaatii käsitellyistä tekniikoista suurimman panostuksen, koska S-BGP käyttää toteutuksessaan sertifikaatteja (Kent, Lynn ja Seo 2000), jotka tarvitsevat taustalle uuden infrastruktuurin niiden myöntämiseen, sekä BGP-protokolla täytyy uudistaa sisältämään sertifikaattien lähettäminen sekä tarkastaminen reitti-ilmoituksien yhteydessä. Uudistettu protokolla tulee vaatimaan ainakin ohjelmistopäivityksen reitittimiin, mahdollisesti joitain reitittimiä ei pystytä päivittämään tähän uuteen versioon protokollasta, ja reitittimet täytyy tällöin päivittää. S-BGPn investoinnin tarve voidaan luokitella merkittäväksi

ROVER:in toiminta perustuu S-BGP:n (Kent, Lynn ja Seo 2000) tavoin reitti-ilmoituksen varmentamiseen, joten mikäli ROVER otettaisiin käyttöön, tarvittaisiin BGP-protokollasta uusi versio, johon sisältyy ROVER:in vaatima tuki DNS tietojen tarkastamiseen. Koska ROVER käyttää olemassa olevaa DNS järjestelmää S-BGP:n sertifikaatti järjestelmän sijaan, ei ROVER tarvitse merkittävää toissijaista infrastruktuuriinvestointia. Näin ollen ROVER edellyttää huomattavan investoinnin.

PGBGP:n toiminta perustuu S-BGP:n (Kent, Lynn ja Seo 2000) sekä ROVER:in (Gersch ja Massey 2013) tavoin lisäykseen BGP-protokollaan, jossa odotetaan tietty aikaikkuna ennen kuin uudet reitit hyväksytään osaksi reititystaulua. PGBGP eroaa kuitenkin ROVER:ista sekä S-BGP:stä siinä, että se ei käytä ulkoista infrastruktuuria toimintaansa, vaan toiminta perustuu kokonaan reitittimen tallentamaan tietoon. Koska PGBGP tarvitsee protokollapäivityksen, mutta ei ulkoista infrastruktuuria. BGP-protokollan muutoksen takia PGBGP saa luokituksen huomattava.

ARGUS (Xiang ym. 2011) eroaa merkittävästi kaikista muista käsitellyistä tekniikoista siinä, että ARGUS:in toiminta ei perustu reitittimiin, tai niissä käytettävään BGP-protokollaan, vaan ARGUS käyttää avoimia olemassa olevia palvelimia tarkistaessaan onko reitti palvelimelle estynyt. ARGUS ei tarvitse investointia uuteen infrastruktuuriin, vaan se pystyy toimimaan kokonaan jo olemassa olevan infrastruktuurin varassa. ARGUSilla ei ole merkittäviä vaatimuksia, joten ARGUS luokitellaan vähäiseksi.

4.2 Yhteistyön tarve

Yhteistyön tarve on merkittävä tarkasteltava tekijä, koska jos tekniikka tarvitsee kaikkien tai lähes kaikkien operaattoreiden yhteistyön, kestää tekniikan käyttöönotossa merkittävästi pidempään, koska siirtymästä täytyy sopia globaalisti, sekä täytyy saavuttaa kompromissi, jonka kaikki voivat hyväksyä. Ei myöskään ole itsestään selvää, että kyetään löytämään hyväksytty kompromissi vaan, on mahdollista, että tekniikkaa ei saada yhteistyöhalun puuteen takia edes käyttöön.

Kategoriasta annetaan luokitukset seuraavien kriteereiden mukaan:

- **Vähäinen** luokitus annetaan, mikäli teknologia voidaan ottaa käyttöön ilman yhteistä käyttöönottoa eikä teknologia käytä tietoa ulkopuoliselta taholta.
- **Huomattava** luokitus annetaan, mikäli teknologia vaatii joko laajan yhteisen käyttöönoton tai käyttää toiminnassaan ulkopuoliselta taholta saatavaa tietoa.
- **Merkittävä** luokitus annetaan, mikäli teknologia vaatii laajan yhteisen käyttöönoton ja käyttää toiminnassaan ulkopuoliselta taholta saatavaa tietoa.

S-BGP:n toiminta perustuu PKI:hin (Cooper ym. 2008), jossa kaikkien BGP-operaattoreiden tulee vahvistaa antamansa ilmoitukset allekirjoittamalla ne omalla avaimellaan (private key), ja vastaanottaja varmentaa ilmoituksessa olevan allekirjoituksen, ennen reitin hyväksymistä (Kent, Lynn ja Seo 2000, 5-6). Mikäli tekniikkaa ei oteta laajasti käyttöön, reitti-ilmoitusten oikeellisuutta ei pystytä teknologian avulla varmentamaan. S-BGP tarvitsee toimiakseen vahvistukset muilta operaattoreilta, ja on siten merkittävästi riippuvainen muista operaattoreista.

ROVER:in toiminta perustuu S-BGP:n (Kent, Lynn ja Seo 2000) tavoin ilmoituksen varmentamiseen ennen reitin hyväksymistä, mutta ROVER käyttää ilmoituksen varmennukseen PKI:n sijaan DNS-järjestelmää. Koska myös ROVER vaatii, että ilmoitus varmennetaan tarkastamalla, onko ilmoittajan AS lisätty IP-osoitteen sallittujen ilmoittajien listaan DNS-järjestelmässä (Gersch ja Massey 2013), kärsii siten ROVER:kin samasta ongelmasta, jossa ilmoituksen oikeellisuutta ei pystytä varmentamaan, mikäli ROVER:ia ei oteta laajalti käyttöön, sekä muiden operaattoreiden tulee ylläpitää DNS järjestelmässä olevaa tietoa sallituista ilmoittajista, jonka seurauksena ROVER vaatii merkittävää yhteistyötä toimiakseen.

PGBGP ei käytä toiminnassaan ulkoista tietoa reitin varmentamiseen kuten S-BGP (Kent, Lynn ja Seo 2000) sekä ROVER (Gersch ja Massey 2013) käyttävät omissa toteutuksissaan. Vaan PGBGP tallentaa tietoa yleisistä reiteistä, ja vertaa uusia reittejä tallennettuun tietoon (Karlin, Forrest ja Rexford 2006). Koska PGBGP käyttää toiminnassaan vain lokaalia tietoa, PGBGP ei ole riippuvainen muiden BGP-operaattoreiden toimista, tai siitä päättävätkö muut BGP-operaattorit ottaa samaa tekniikkaa käyttöönsä. PGBGP:n tarvitsema yhteistyö on vähäistä.

ARGUSin toiminta eroaa muista esitetyistä tekniikoista siten, että ARGUS testaa konkreettisesti, aiheuttiko uusi reitti häiriön internet liikentessä. Mikäli liikenteessä tapahtui häiriö, nostaa ARGUS hälytyksen (Xiang ym. 2011). ARGUS:in toiminta ei siis ole riippuvainen muista BGP-operaattoreista, vaan julkisista palvelimista, joista käsin ARGUS testaa saavuttaako liikennee tarkoitetun kohteensa, vai jääkö liikenne välille. ARGUS käyttää toiminnassaan ulkoisia palvelimia, joka nostaa luokituksen huomattavaksi.

4.3 Tekniikan virhealttius

Tekniikan luotettavuuden huomioon ottaminen tekniikoita vertailtaessa on tärkeää. Mikäli tekniikka ei pysty luotettavasti varmentamaan mahdollisia kaappauksia on riski että kaappaukset jäävät huomaamatta, sekä se että normaaleja tilanteita ilmoitetaan kaappauksina. Tällöin tekniikasta ei ole merkittävästi apua BGP-kaappausten estämiseksi.

Kategoriasta annetaan luokitukset seuraavien kriteereiden mukaan:

- **Vähäinen** luokitus annetaan, mikäli teknologia varmentaa ilmoitukset omistajalta saadulla tiedolla ja teknologian tuottama tulos on aikariippumaton
- **Huomattava** luokitus annetaan, mikäli teknologia ei varmenna ilmoituksia omistajalta saadulla tiedolla tai teknologian tulos on aikariippuvainen.
- **Merkittävä** luokitus annetaan, mikäli teknologia ei varmenna ilmoituksia omistajalta saadulla tiedolla sekä teknologian tulos on aikariippuvainen.

S-BGP (Kent, Lynn ja Seo 2000) käyttää ilmoituksen varmentamiseen sertifikaatteja, jotka omistaja on allekirjoittanut omalla avaimellaan (Cooper ym. 2008). Ajantasaisella PKI

toteutuksella tehdyn sertifikaatin väärentäminen on käytännössä mahdotonta. S-BGP:n toimintaan ei myöskään vaikuta aika tai jokin muu muuttuja, joten S-BGP:n virhealttius luokitellaan vähäiseksi.

ROVER (Gersch ja Massey 2013) toimii pitkälti samalla tavalla kuin S-BGP (Kent, Lynn ja Seo 2000). ROVER varmentaa ilmoituksen oikeellisuuden DNS-järjestelmästä, jonne osoitteen omistaja on lisännyt tiedon tahoista, jotka saavat mainostaa reittiä. ROVER:in toimintaan ei myöskään vaikuta aika tai jokin toinen muuttuja, joten myös ROVER:in virhealttius on vähäistä.

PGBGP (Karlin, Forrest ja Rexford 2006) käyttää toiminnassaan keräämäänsä historiallista tietoa, jonka avulla PGBGP päättää tuleeko reitti hyväksyä sellaisenaan, vai tuleeko reitti asettaa karanteeniin. PGBGP ei käytä toiminnassaan tietoa omistajalta ilmoituksen varmentamiseen. PGBGP:n toiminta on riippuvainen ajasta, koska mikäli ilmoituksen reitti sisältyy historialliseen dataan, hyväksytään reitti, mutta mikäli reitti on poistunut historiallisesta datasta, tullaan reitti asettamaan karanteeniin. PGBGP on aikariippuvainen, joka nostaa sen virhealttiuden huomattavaksi.

ARGUSin (Xiang ym. 2011) toiminta perustuu konkreettisiin testeihin, joita ajetaan useilta palvelimilta. Testit tarkastavat saavutetaanko ilmoituksen kohdetta enään reitin muuttumisen jälkeen. ARGUS ei siten käytä ilmoituksen varmentamiseen omistajalta saatua tietoa, mutta ARGUS ei ole riippuvainen ajasta, koska ARGUSin toiminta perustuu konkreettisiin testeihin, jotka ovat samat jokaisella testikerralla. ARGUS ei käytä varmennukseen omistajalta saatua tietoa, joten ARGUSin virhealttius on huomattava.

4.4 Pohdinta

Edellisissä alaluvuissa käsiteltiin teknologioita erilaisista näkökulmista käsin. Näiden näkökulmien havainnot on koottu yhteen alla olevaan taulukkoon 1.

Takautuvuudessa ARGUS (Xiang ym. 2011) on muita teknologioita parempi, koska ARGUS ei tarvitse toimiakseen muutoksia reitittimiin, ja siten sen käyttöönotto ei tarvitse merkittävää investointia. ROVER (Gersch ja Massey 2013) sekä PGBGP (Karlin, Forrest ja Rexford

Nimi	Takautuvuus	Yhteistyö	Virhealttius
S-BGP	Merkittävä	Merkittävä	Vähäinen
ROVER	Huomattava	Merkittävä	Vähäinen
PGBGP	Huomattava	Vähäinen	Merkittävä
ARGUS	Vähäinen	Huomattava	Huomattava

Taulukko 1. Teknologioiden tulokset

2006) kytketään suoraan reitittimiin, ja siten niiden käyttöönotto vaatii BGP-protokollan päivittämisen, joka vuorostaan vaatii kansainvälisen ymmärryksen. S-BGP (Kent, Lynn ja Seo 2000) vaatii sekä edellä mainitun protokollan päivittämisen, että myös merkittävän uuden kansainvälisen taustainfrastruktuurin toimiakseen.

Yhteistyön tarvetta tarkasteltaessa havaitaan, että varmennusteknologiat S-BGP (Kent, Lynn ja Seo 2000) sekä ROVER (Gersch ja Massey 2013) pärjäävät heikosti tarkastusteknologioita PGBGP:tä (Karlin, Forrest ja Rexford 2006) sekä ARGUSta (Xiang ym. 2011) vastaan. Varmennusteknologiat tarvitsevat toimiakseen laaja-alaisen käyttöönoton, tarvittavan käyttöönoton laajuutta on vaikea määritellä tarkasti, mutta tekniikoiden toimivuus paranee mitä lähemmäs sadan prosentin käyttöönottoa päästään. Tarkastusteknologiat voidaan ottaa käyttöön tai poistaa käytöstä operaattoritasolla, ilman että sillä on vaikutusta muihin operaattoreihin. On kuitenkin tarpeellista mainita, että ARGUS käyttää toiminnassaan ulkoisia palvelimia, joten ARGUSin toiminta ei ole täysin muista tahoista riippumatonta, kuten PGBGP:n toiminta taas on.

Virhealttiudessa havaitaan, että yhteistyötä vaativilla teknologioilla saavutetaan parempia tuloksia virhealttiudessa. Varmennusteknologiat S-BGP (Kent, Lynn ja Seo 2000) ja ROVER (Gersch ja Massey 2013) ovat molemmat vähemmän virhealttiita, kuin tarkastusteknologioita PGBGP:tä (Karlin, Forrest ja Rexford 2006) sekä ARGUSsta (Xiang ym. 2011) perustuvat tiedon varmentamisen sijaan arvion tekemiseen, jonka pohjalta määritellään, onko kyseessä kaappaus vai ei. Arvion pohjalta päätösten tekeminen antaa molemmille tarkastustekniikoille heikommat arvosanat, kuin varmennusteknologioille.

Tutkielman alussa motivaationa oli löytää mahdollisia syitä sille, miksi BGP-kaappausten

estämiseksi ei ole otettu merkittäviä toimenpiteitä, vaikka ongelma on ollut tiedossa jo useiden vuosien ajan. Teknologioiden keskinäinen vertailu osoitti, että jokaisella teknologialla on oma heikkoutensa valittujen arviointikriteerien valossa. S-BGP (Kent, Lynn ja Seo 2000) tarvitsee merkittävän investoinnin, sekä globaalin käyttöönoton, mutta se on vertailluista tekniikoista todennäköisesti turvallisin, kun taas PGBGP (Karlin, Forrest ja Rexford 2006) voidaan ottaa paikallisesti käyttöön, mutta se ei ole yhtä luotettava, kuin S-BGP.

Tutkielman tulosten perusteella voidaan esittää mahdollisena vastauksena tutkimuskysymykseen, että BGP-kaappausten estämiseen ei ole olemassa yksittäistä ratkaisua, joka ratkaisee ongelman, koska yhdelle käyttäjälle takautuvuus saattaa olla merkittävä kriteeri, kun taas toiselle käyttäjälle luotettavuus saattaa olla kaikkia muita esitettyjä kriteereitä tärkeämpi kriteeri.

Näkökulmat olivat tässä tutkimuksessa tasa-arvoisia toisiinsa nähden. Tulevaisuudessa olisi kuitenkin hyvä asettaa enemmän painotusta virhealttiuteen, kuin yhteistyön määrään, koska standardeja tehdessä tarvittavalla ajankäytöllä voidaan neuvotella kompromisseja, joilla yhteistyöhön liittyviä ongelmia voidaan vähentää. Toiseksi IT-maailmassa infrastruktuuria tullaan joka tapauksessa päivittämään ajan kuluessa, ja olemassa olevan infrastruktuurin hukkaaminen voidaan minimoida sillä, että koordinoidaan muutos sopivan pitkällä siirtymäajalla, jotta tahot voivat varautua siihen. Joka tapauksessa mahdollisissa tulevissa tarkasteluissa, sekä tarkastelukriteerejä, että niiden keskinäistä painotusta tulisi tarkastella enemmän.

5 Yhteenveto

BGP on vanha protokolla, jossa on merkittäviä tietoturvapuutteita, jotka mahdollistavat BGP:n viestiliikenteen kaappaamisen, sekä joissain tilanteissa viestien väärentämisen. Tieturvan parantamiseksi on esitetty kirjallisuudessa useita ratkaisuja. Kuitenkaan ratkaisuista yhtäkään ei ole otettu laaja-alaisesti käyttöön. Jokaisella tutkielmassa käsitellyllä ratkaisulla BGP:n tietoturvaongelmaan on omat heikkoutensa sekä vahvuutensa. Tämä johtaa siihen, että ei ole olemassa yksittäistä ratkaisua, joka täyttää kaikkien tahojen tarpeet täydellisesti. Täten kokonaisvaltaista ratkaisua etsittäessä joudutaan tekemään kompromisseja.

Tulevaisuudessa mahdollisia tutkimushaaroja voisivat olla arviointikriteerit sekä niiden mahdollinen keskinäinen painottaminen. Esimerkiksi tuleeko ratkaisun valinnassa painottaa enemmän luotettavuutta, kuin takautuvuutta, sekä ovatko nämä kolme nykyistä kriteeriä hyvät arviointikriteerit vai eivät. Toinen mahdollinen tutkimushaara on useamman teknologian yhtäaikainen käyttö. Esimerkiksi käytetään varmennustekniikkaa saapuviin reitti-ilmoituksiin, mutta mikäli varmennusta ei voida suorittaa käytetään varalla tarkastusteknologiaa.

Lähteet

Bakkali, S., H. Benaboud ja M. Ben Mamoun. 2013. “Security problems in BGP: An overview”. Teoksessa *2013 National Security Days (JNS3),* 1–5. Huhtikuu. doi:10.1109/JNS3.2013.6595458.

Baldé, C.P., V. Forti, V. Gray, R. Kuehr ja P. Stegmann. 2017. “The Global E-waste Monitor – 2017”. Viitattu 21. maaliskuuta 2020. http://collections.unu.edu/eserv/UNU:6341/Global-E-waste_Monitor_2017__electronic_single_pages_.pdf.

“BGPMON”. 2020. Viitattu 29. tammikuuta. https://www.bgpmon.io/.

Bush, R., ja R. Austein. 2013. “The Resource Public Key Infrastructure (RPKI) to Router Protocol”. Viitattu 22. huhtikuuta 2020. https://tools.ietf.org/html/rfc6810.

Butler, K., T. R. Farley, P. McDaniel ja J. Rexford. 2010. “A Survey of BGP Security Issues and Solutions”. *Proceedings of the IEEE* 98, numero 1 (tammikuu): 100–122. ISSN: 1558-2256. doi:10.1109/JPROC.2009.2034031.

Chen, J. 2012. “Google Public DNS: 70 billion requests a day and counting”. Helmikuu. Viitattu 19. maaliskuuta 2020. https://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html.

Cho, S., R. Fontugne, K. Cho, A. Dainotti ja P. Gill. 2019. “BGP hijacking classification”. Teoksessa *2019 Network Traffic Measurement and Analysis Conference (TMA),* 25–32. Kesäkuu. doi:10.23919/TMA.2019.8784511.

Cooper, D., S. Santesson, S. Farrell, S. Boeyen, R. Housley ja W. Polk. 2008. “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. Maaliskuu. Viitattu 29. tammikuuta 2020. https://tools.ietf.org/html/rfc5280.

Fuller, V., ja T. Li. 2006. “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan”. Viitattu 25. maaliskuuta 2020. https://tools.ietf.org/html/rfc1321.

Gersch, J., ja D. Massey. 2013. “ROVER: Route Origin Verification Using DNS”. Teoksessa *2013 22nd International Conference on Computer Communication and Networks (ICCCN),* 1–9. Heinäkuu. doi:10.1109/ICCCN.2013.6614187.

Hawkinson, J., ja T. Bates. 1996. “Guidelines for creation, selection, and registration of an Autonomous System (AS)”. Viitattu 25. maaliskuuta 2020. https://tools.ietf.org/html/rfc1930.

Hughes, D. L., Nripendra P. Rana ja Antonis C. Simintiras. 2017. “The changing landscape of IS project failure: an examination of the key factors”. *Journal of Enterprise Information Management* 30 (1): 142–165.

Huston, G., P. Smith ja T. Bates. 2020. “CIDR REPORT for 19 Mar 20”. Maaliskuu. Viitattu 19. maaliskuuta 2020. https://www.cidr-report.org/as2.0/.

Kappelman, Leon A., Robert McKeeman ja Lixuan Zhang. 2006. “EARLY WARNING SIGNS OF IT PROJECT FAILURE: THE DOMINANT DOZEN”. *Information Systems Management* 23, numero 4 (FallFall): 31–36.

Karlin, J., S. Forrest ja J. Rexford. 2006. “Pretty Good BGP: Improving BGP by Cautiously Adopting Routes”. Teoksessa *Proceedings of the 2006 IEEE International Conference on Network Protocols,* 290–299. Marraskuu. doi:10.1109/ICNP.2006.320179.

Kent, S., C. Lynn ja K. Seo. 2000. “Secure Border Gateway Protocol (S-BGP)”. *IEEE Journal on Selected Areas in Communications* 18, numero 4 (huhtikuu): 582–592. ISSN: 1558-0008. doi:10.1109/49.839934.

Lougheed, K., ja Y. Rekhter. 1990. “A Border Gateway Protocol (BGP)”. Viitattu 17. huhtikuuta 2020. https://tools.ietf.org/html/rfc1163.

Mockapetris, P. 1987. “Domain Names - Implementation and Specification”. Marraskuu. Viitattu 28. tammikuuta 2020. https://tools.ietf.org/html/rfc1035.

Murphy, S. 2006. “BGP Security Vulnerabilities Analysis”. Tammikuu. Viitattu 4. maaliskuuta 2020. https://tools.ietf.org/html/rfc4272.

Postel, J. 1981. “TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION”. Syyskuu. Viitattu 4. huhtikuuta 2020. https://tools.ietf.org/html/rfc793.

Rashevskiy, R. B., ja A. S. Shaburov. 2017. “«BGP-hijacking» attacks: Theoretical basis and practical scenarios”. Teoksessa *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus),* 208–212. Tammikuu. doi:10.1109/EIConRus.2017.7910530.

Rekhter, Y., T. Li ja S. Harres. 2006. “A Border Gateway Protocol 4 (BGP-4)”. Tammikuu. Viitattu 28. tammikuuta 2020. https://tools.ietf.org/html/rfc4271.

Rivest, R. 1992. “The MD5 Message-Digest Algorithm”. Viitattu 25. maaliskuuta 2020. https://tools.ietf.org/html/rfc1321.

Schlamp, J., R. Holz, Q. Jacquemart, G. Carle ja E. W. Biersack. 2016. “HEAP: Reliable Assessment of BGP Hijacking Attacks”. *IEEE Journal on Selected Areas in Communications* 34 (6): 1849–1861.

Sermpezis, P., V. Kotronis, P. Gigis, X. Dimitropoulos, D. Cicalese, A. King ja A. Dainotti. 2018. “ARTEMIS: Neutralizing BGP Hijacking Within a Minute”. *IEEE/ACM Transactions on Networking* 26 (6): 2471–2486.

Stewens, Marc., Arjen K. Lenstra ja Benne de. Weger. 2012. “Chosen-prefix collisions for MD5 and applications”. Viitattu 25. maaliskuuta 2020. https://infoscience.epfl.ch/record/164548/files/IJACT020403%5C%20STEVENS.pdf.

Touch, J., A. Mankin ja R. Bonica. 2010. “The TCP Authentication Option”. Kesäkuu. Viitattu 4. huhtikuuta 2020. https://tools.ietf.org/html/rfc5925.

Wu, Y., R. Yu ja R. Wang. 2018. “A Fraud Prevention BGP Protocol: CP-BGP”. Teoksessa *2018 International Conference on Computational Science and Computational Intelligence (CSCI),* 124–127.

Xiang, Y., Z. Wang, X. Yin ja J. Wu. 2011. “Argus: An accurate and agile system to detecting IP prefix hijacking”. Teoksessa *2011 19th IEEE International Conference on Network Protocols,* 43–48. Lokakuu. doi:10.1109/ICNP.2011.6089080.

Zhang, Y., Z. Zhang, Z. M. Mao ja Y. C. Hu. 2009. “HC-BGP: A light-weight and flexible scheme for securing prefix ownership”. Teoksessa *2009 IEEE/IFIP International Conference on Dependable Systems Networks,* 23–32.