2014/2500M-0009

ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-2634-5

TIIVISTELMÄRAPORTTI (SUMMARY REPORT)

Tietoverkkojen luotettavuus palvelunestohyökkäyksen aikana

Tuomas Aura, Aapo Kalliola, Sanja Šćepanović, Jaakko Salo
Aalto University, Department of Computer Science and Engineering
Contact: tuomas.aura@aalto.fi, aapo.kalliola@aalto.fi

Tiivistelmä

Kolmivuotisen tutkimusprojektin (2012-2014) tavoitteena oli kehittää edullisia menetelmiä palvelunestohyökkäysten torjumiseen. Uhkamallissa hyökkääjä lähettää Internetissä toimivalle palvelimelle viestitulvan, joka ylikuormittaa joko itse palvelimen tai tietoverkon sen edessä. Tutkimuksessa huomioitiin niin laajakaistaiset, väärennettyjä lähettäjäosoitteita käyttävät hyökkäykset kuin bottiverkon hajautetut hyökkäykset. Projektissa kehitetty puolustusmenetelmä perustuu pakettien suodattamiseen palomuurissa tai muussa verkkoelementissä ennen kohdepalvelinta. Suodatuksen toimivuus osoitettiin matemaattisella mallilla, simulaatioin ja kokeellisella toteutuksella. Tutkimuksen kolmantena vuonna 2014 tehty prototyyppitoteutus käyttää hyväksi uutta OpenFlow-kytkintä, joka pystyy laajakaistaisen tietovirran käsittelyyn ja johon on mahdollista toteuttaa uusia ominaisuuksia ohjelmallisesti. Suodatus on tulevaisuudessa mahdollista hajauttaa tietoverkkoon ja yhdistää muihin palvelunestohyökkäysten torjuntamenetelmiin.

1. Johdanto

Internetistä on muodostunut osa yhteiskunnan kriittistä infrastruktuuria, jonka toimivuudesta yhä useammat yritykset ja julkiset palvelut ovat riippuvaisia. Näin on tapahtunut siitä huolimatta, että tietoverkko toimii *best effort* -periaatteella eikä sen palvelun laatua periaatteessa ole taattu. Internet on avoin verkko, johon kuka tahansa voi liittyä, ja useimmat verkossa toimivat palvelut ovat avoimia kenelle tahansa. Tällaisessa verkossa vihamielisen hyökkääjän on mahdollista lähettää kohdepalveluun niin suuri määrä viestejä, että palvelu ylikuormittuu tai sen Internet-yhteys tukkeutuu. Verkon ja palveluiden avoimuuden takia on myös vaikeaa erottaa rehellisten käyttäjien viestejä haittaamistarkoituksessa lähetetyistä. Näistä syistä viestitulvaan perustuvat palvelunestohyökkäykset ovat yksi Internetin keskeisistä tietoturvaongelmista ja osa verkossa toimivien palveluiden arkipäivää.

Tyypillisiä palvelunestohyökkäysten kohteita ovat esimerkiksi poliittisesti kiistanalaiset ja kantaa ottavat verkkosivustot, pelipalvelimet ja kilpailevien pelaajien verkkoyhteydet sekä erilaisten mielenosoitusten ja kampanjoiden kohteeksi joutuvat kaupalliset ja julkiset palvelut. Verkosta riippuvaiset yritykset voivat joutua myös kiristyksen kohteeksi, ja osassa hyökkäyksistä saattaa olla kyse kybersodankäynnin harjoittelusta. Hyökkäyksiä helpottaa se, että rikollisilta markkinoilta on mahdollista vuokrata miljoonien kaapattujen tietokoneiden muodostamia ns. bottiverkkoja, jotka voidaan valjastaa laajaan samanaikaiseen hyökkäykseen yhtä kohdetta vastaan. Joitain, esimerkiksi yliopistoihin kohdistuvia hyökkäyksiä on vaikea selittää, ja ne saattavat yksinkertaisesta johtua siitä, että palvelunestohyökkäys on niin helppo toteuttaa.

Lähes mikä tahansa Internetissä toimiva palvelu on haavoittuvainen palvelunestohyökkäykselle, jos hyökkääjällä on riittävä lähetyskapasiteetti. Vain suurimmilla globaaleilla yrityksillä on varaa niin suureen ylikapasiteettiin ja globaaliin hajautukseen, että ne pärjäävät hyökkääjille. Kaupallisia palvelunestohyökkäysten suodatuspalveluita on saatavana, mutta niiden kustannukset ovat kohtuuttomia esimerkiksi pienille yrityksille, oppilaitoksille tai vapaaeh-

toisorganisaatioille. Lisäksi yksityisyyden suojan vaatimukset voivat estää globaalin hajautuksen ja ulkomailla sijaitsevien suojauspalveluiden käytön. Näistä syistä on tärkeää kehittää suojausmenetelmiä, jotka toimivat paikallisesti ja joilla mikä tahansa Internet-palvelu voi suojata itseään. Hypoteesina tässä tutkimuksessa oli, että vaikka täydellinen suojautuminen palvelunestohyökkäyksiltä on mahdotonta, on hyökkäyksen vaikutuksia mahdollista lievittää ja potentiaalisten hyökkääjien määrää vähentää kohtuullisin kustannuksin hyökkäysten paikallisella suodatuksella.

2. Tutkimuksen tavoite ja suunnitelma

Tutkimuksen ensimmäisenä vuonna kehitettiin teoreettinen kehys palvelunestoyökkäysten suodattamiseen. Kehitetty suodatusmenetelmä perustuu koneoppimiseen: hyökkäyksen normaalikäyttäjistä luodaan jatkuvasti ylläpidettävä malli, johon hyökkäyksen aikaista liikennettä verrataan. Tällainen malli luo automaattisesti tarkemman kuvan niistä IP-osoiteavaruuden alueista, joissa on paljon rehellisiä palvelun käyttäjiä, ja antaa vähemmän huomiota osoitteille, jossa asiakkaita ei normaalisti ole. Hyökkäyksen aikana mallia käytetään suodatuksen perusteena niin, että normaaliliikenteen malliin parhaiten sopiva osa liikenteestä palvellaan ja loput palvelimelle saapuvat viestit jätetään käsittelemättä.

Hyökkäyksen alkaminen tunnistetaan yksinkertaisesti siitä, että palvelimen kapasiteetti ylittyy. Kirjallisuudessa on pohdittu paljon tahallisen hyökkäyksen ja rehellisten käyttäjien ylikuormittaman palvelun eroja. Tässä tutkimuksessa otettiin lähtökohdaksi, että kaikissa ylikuormitustilanteissa osa asiakkaiden viesteistä jää käsittelemättä, ja saman suodatusstrategian pitää toimia sekä tahallisessa että tahattomasti aiheutetussa ylikuormitustilanteessa. Tavoitteeksi otettiin palvelun vakioasiakkaiden palveleminen myös hyökkäyksen aikana.

Toisena vuonna suodatusmenetelmää optimoitiin ja sen toimivuutta arvioitiin simulaatioilla ja ryhmän aiempaan työhön pohjautuvalla peliteoreettisella mallinnuksella. Mallinnuksen tavoitteena oli päätellä simulaatioita varten, mikä on pahin mahdollinen hyökkäysstrategia ja paras puolustus siltä suojautumiseksi. Simulaatioilla arvioitiin suodatusmenetelmän toimivuutta erilaisten hyökkäystyyppien torjunnassa. Tavoitteena on torjua niin bottiverkon hajautetut hyökkäykset kuin väärennetyllä lähdeosoitteella lähetetyt paketit. Koska bottiverkko pystyy siirtämään hyökkäystään joustavasti protokollapinon eri tasojen välillä, on puolustajan otettava huomioon niin verkkoyhteyden tukkiminen esimerkiksi SYN-pakettitulvalla kuin palvelun tahallinen ylikuormittaminen sovellustasolla.

Tutkimuksen kolmantena eli viimeisenä vuonna suodatusmenetelmästä toteutettiin prototyyppi. Toteutuksen vaikein kohta on saapuvan laajakaistaisen liikenteen käsittely. Esimerkiksi vuonna 2014 tyypillinen palvelunestohyökkäys on ollut yli 10 gigabittiä sekunnissa. Tällaisen datavirran suodattaminen vaati aiemmin joko kalliin palomuurilaitteen tai kuormanjakajan, jolla se pystytään jakamaan suodatusta tekeville prosessoreille. Tutkimuksen aikana markkinoille alkoi kuitenkin tulla kohtuuhintaisia ohjelmistolla ohjattavia kytkimiä, jotka pystyvät käsittelemään 10 Gbps tai suurempiakin datavirtoja. Näiden kytkinten hallintatason ohjelmallinen toteutus mahdollistaa niiden luovan käytön uusiin tarkoituksiin, kuten tässä tapauksessa pakettien suodattamiseen opitun normaaliliikenteen mallin perusteella. Toteutetun suodatuksen suorituskykyä päästiin kokeilemaan laboratoriossa todellisella lähes 10 Gbps pakettitulvalla.

3. Aineisto ja menetelmät

Normaaliliikenteen mallintamisessa käytettiin datan klusterointia, joka on koneoppimisen menetelmä. Palvelimelle saapuneet paketit tai pyynnöt jaettiin klustereihin lähettäjän IP-osoitteen perusteella niin, että kussakin klusterissa on suurin piirtein saman verran normaaliliikennettä. Klusterointiin käytettiin ns. *hierarcical heavy hitter* -algoritmia. Mallia päivite-

tään säännöllisesti niin, että se kuvaa esimerkiksi viimeisen viikon liikennettä. Klusterointi voidaan tehdä pakettivirrasta satunnaisesti otettujen näytteiden perusteella, eikä pakettivirtaa tarvitse käsitellä reaaliajassa. Esimerkki klustereista puumaisessa IP-osoiteavaruudessa on kuvassa 1.

Kuva 1: Esimerkki web-palvelun normaaliliikenteen klustereista

Palvelimen ylikuormittuessa aletaan havainnoida muutoksia siinä, miten datavirta jakautuu mallin eri klustereihin. Tämäkin vaihe voidaan toteuttaa näytteitä ottamalla ilman koko datavirran reaaliaikaista käsittelyä. Kullekin klusterille lasketaan pakettimäärien suhteellinen muutos normaaliliikenteeseen verrattuna, ja niitä IP-osoiteavaruuden osia, joissa liikenne on kasvanut suhteessa vähiten, palvellaan ensin. Oletuksena on, ettei hyökkääjä pysty imitoimaan luonnollisen liikenteen lähdeosoitejakaumaa ainakaan kovin tarkasti, jolloin suurin osa hyökkääjän liikenteestä osuu pieneen osaan klustereista. Silloin rehellisten käyttäjien liikenne niissä klustereissa, joihin hyökkääjän paketteja tulee vain vähän, pystytään palvelemaan kokonaan.

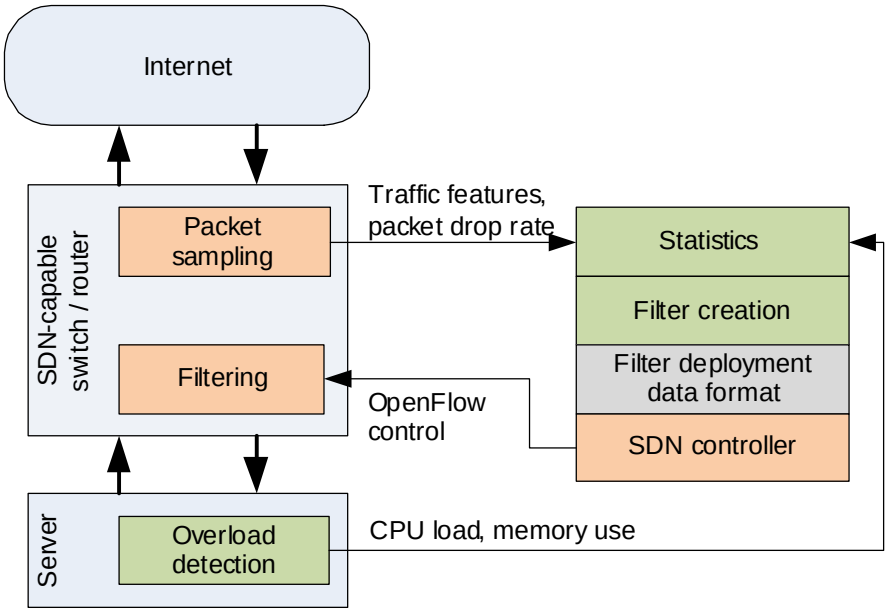
Esimerkiksi jos suojellaan yliopiston web-palvelinta, normaaliliikenne tulee pääosin kampukselta ja sen lähialueilta sekä yliopiston sidosryhmien osoiteryppäistä. Klusterimalli kuvaa tarkimmin nämä osat IP-osoiteavaruudesta. Hyökkääjän käyttämien lähdeosoitteiden jakautuminen IP-osoiteavaruuteen riippuu hyökkäystyypistä. Yksittäistä tai muutamaa lähdeosoitetta käyttävä hyökkääjä sijoittuu vain yhteen tai muutamaan klusteriin, jotka tietenkin

suodatetaan pois. Satunnaisesti generoidut väärennetyt lähdeosoitteet taas ovat hajautuneet tasaisesti ympäri IP-osoiteavaruutta, jolloin suurin osa hyökkäyspaketeista osuu 5-20 prosenttiin klustereista. Suuren bottiverkon aitojen IP-osoitteiden kohdalla tilanne on sama. Joka tapauksessa suurimmassa osassa klustereista on hyökkäyksen aikanakin lähes pelkästään rehellisiä käyttäjiä. Välttääkseen suodatuksen hyökkääjän pitäisi matkia tarkasti rehellisten käyttäjien jakautumista osoiteavaruuteen niin, että hyökkäys tulisi tasaisesti kaikista mallin klustereista.

Kehitetyn suodatusmenetelmän toimivuutta arvioitiin ja optimoitiin matemaattisella mallinuksella, simulaatioin ja kokeellisella toteutuksella. Joka vaiheessa opittiin menetelmän toiminnasta uusia piirteitä. Tutkimusryhmän luomalla peliteoreettisella mallilla osoitettiin, mikä on optimaalinen hyökkäys- ja puolustusstrategia eri tilanteissa. Projektissa kehitetty suodatus perustuu optimaaliseen puolustajan strategiaan, kun oletetaan puolustajan pystyvän mukautumaan hyökkääjää nopeammin. Tällaisen strategia valitseminen on perustelua, koska hyökkääjän optimaalinen strategia vaatii lähdeosoitteiden väärentämissä, minkä takia hyökkääjä ei saa reaaliaikaista osoitekohtaista palautetta hyökkäyksen tehosta. Suodatuksen etuna on, että se ei koskaan johda huonompaa tilanteeseen kuin pakettien harkitsematon, satunnainen pudottaminen.

Simulaatioilla selvitettiin klusterointimenetelmän optimaalisia parametreja kuten klusterien määrää ja klusteroinnissa käytettäviä IP-pakettien piirteitä. Simulaatiot toteutettiin ensin abstraktina liikennemallina ja sitten realistisemmin NS3-simulaattorissa. Simulaatioissa pyrittiin ennen kaikkea kokeilemaan laajaa valikoimaa hyvin erityyppisiä hyökkäyksiä sovellustason ylikuormituksesta SYN-pakettitulvaan ja suuresta bottiverkosta keskitettyyn hyökkäykseen. Bottiverkon osoitteiden jakaumaa mallinnettiin ensin haittaohjelman epideemisellä leviämistä kuvaavalla mallilla. Myöhemmissä simulaatioissa käytettiin oikean bottiverkon osoitteita, joita alkoi olla julkisesti saatavilla. Myös IP-paketin muiden piirteiden kuin lähdeosoitteen käyttöä suodatuksessa kokeiltiin. Ei kuitenkaan pystytty osoittamaan, että ne lisäisivät suodatuksen tehokkuutta merkittävästi, joten tässä tutkimuksessa päädyttiin käyttämään suodatukseen pelkästään lähettäjän IP-osoitetta tai lähettäjän ja kohdepalvelun yhdistelmää.

Projektin alkaessa ei ollut tiedossa, miten suodatus pystyttäisin toteuttamaan ilman kymmenientuhansien eurojen laitteistoa. Tämä oli ehkä suurin tutkimuksen riskeistä. Ensin ajattelimme ratkaisuksi erilaisia hajautuksen ja rinnakkaislaskennan menetelmiä, esimerkiksi GPU-laskentaa. Tutkimuksen aikana markkinoille tuli ohjelmallisesti ohjattavia verkkokytkimiä, jotka toteuttavat OpenFlow-standardin. Tämä *software defined networking* -tutkimusalue on nopeasti noussut tietoverkkotutkimuksen keskeiseksi trendiksi. Perusajatus on, että verkkolaitteet ovat mahdollisimman yksinkertaisia ja keskittyvät vain pakettien nopeaan käsittelyyn, ja että niitä ohjataan ulkoisella ohjelmistopohjaisella kontrollerilla. Tällöin verkkolaitteille on mahdollista kehittää uusia toimintoja, kuten tässä tapauksessa klusterimalliin perustuva pakettien suodatus. OpenFlow-tekniikkaa toteuttavissa kytkimissä on vielä huomattavia suorituskyky- ja luotettavuusongelmia, mutta koska suodatuksessa tarvitaan vain kaksi nopeaa kytkimen porttia ja klustereiden määrää pystytään säätämään kytkimen rajoitusten mukaan, on suodatusmenetelmän toteutus OpenFlow-tekniikalla mahdollista. Tämän hetken kohtuuhintaisissa kytkimissä on kaksi 10 Gbps tai 100 Gbps porttia, jotka on tarkoitettu kahdennetulle ulkoiselle Internet-yhteydelle. Ohjelmoimalla ohjauslogiikka uudelleen ne voidaan valjastaa myös muuhun käyttöön, kuten tässä tapauksessa portista toiseen virtaavan liikenteen suodattamiseen.

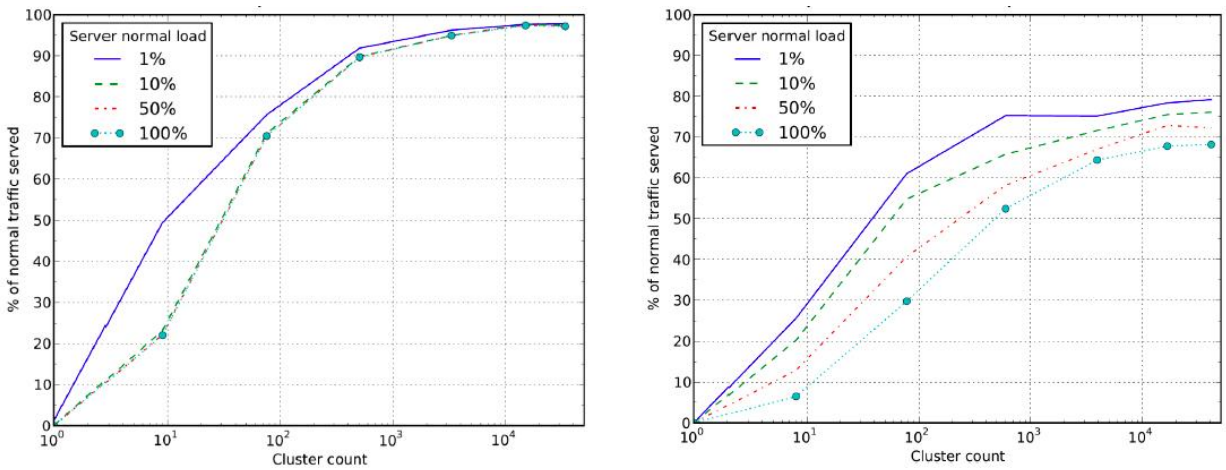


Kuva 2: Suodatuksen arkkitehtuuri

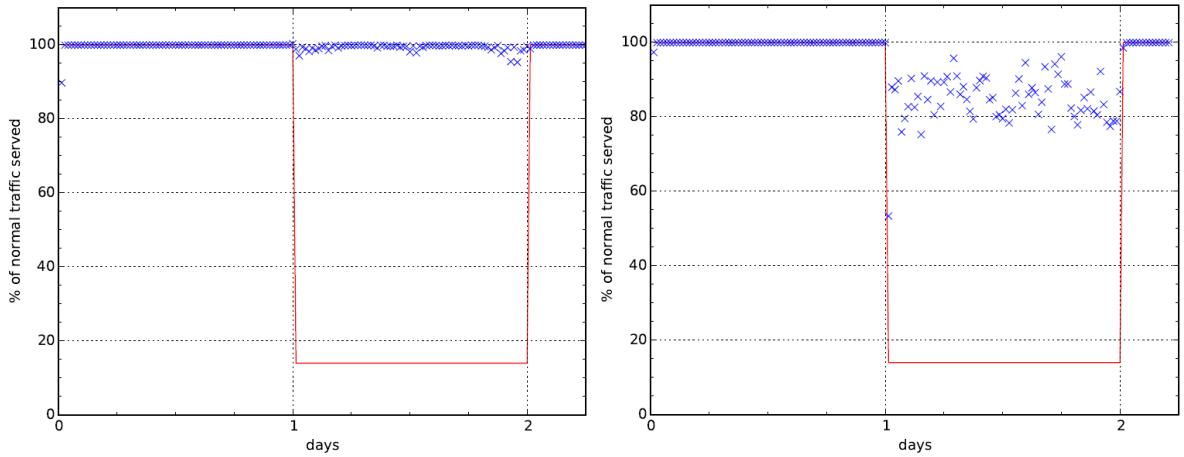
Kuvassa 2 näkyy suunnitellun suodatusjärjestelmän arkkitehtuuri. Palvelimen edessä on eräänlaisena palomuurina toimiva OpenFlow-kytkin, joka sekä ottaa näytteitä lävitsensä kulkevista paketeista että suodattaa niitä. Kytkintä ohjataan tavallisella tietokoneella, joka ylläpitää normaaliliikenteen klusterimallia, tarkkailee verkon ja palvelimen kuormitusta sekä kääntää klusterimallin kytkimen ymmärtämiksi osoiteprefikseiksi. Kytkin tallentaa nämä tietovirtatauluunsa. Ylikuormitustilanteessa ohjain käskee kytkintä suodattamaan osan liikenneklustereista pois. Hyökkäyksenaikainen kontrollisilmukka, siis suodatuksen mukautuminen hyökkäysliikenteeseen, kestää nykyisessä toteutuksessa joitain sekunteja, mutta voisi olla alle yhden sekunnin.

4. Tulokset ja pohdinta

Kuva 3 kertoo simulaation perusteella, miten suodatuksen toimivuus riippuu mallin kompleksiuudesta eli klusterien määristä. Vasemmassa kuvassa hyökkääjä on pieni bottiverkko. Tällöin suuremmalla klusterimäärällä saavutetaan tarkempi suodatus aina noin 10,000 klusteriin asti, jolloin noin 97 % rehellisten käyttäjien viesteistä käsitellään. Tällä klusterimäärällä suodatus on jo liiankin tarkkaa, ja ylioppiminen voi johtaa suodatustuloksen heikkenemiseen, jos hyökkäys kestää pitkään ja normaaliliikenne muuttuu. Oikeanpuoleisessa kuvassa hyökkäysliikenteen lähdeosoitteet ovat satunnaisia. Suodatuksen optimi saavutetaan jo noin 1000 klusterilla ja lähes 80 % rehellisistä käyttäjistä palvellaan. Yleensä noin 1000–2000 klusteria riittää lähes optimaaliseen suodatustulokseen, joka myös pysyy hyvänä usean päivän ajan rehellisten käyttäjien liikenteen muutoksista huolimatta. 1000-2000 klusteria on siinäkin mielessä sopiva määrä, että edullisimmat OpenFlow-kytkimet pystyvät käsittelemään saman verran osoiteprefiksejä.



Kuva 3: Simulaatio suodatuksesta, kun hyökkääjällä (a) pieni, tuhansien koneiden botti-verkko tai (b) satunnaiset lähettäjäosoitteet. X-akselilla liikennemallin klusterien määrä, Y-akselilla palveltujen rehellisten asiakkaiden osuus.



Kuva 4: Suodatuksen OpenFlow-toteutuksen toimivuus laboratoriokokeessa; (a) yksi hyökkääjän osoite (b) satunnaiset lähettäjäosoitteet.

Kuva 4 kertoo, miten suodatus toimi laboratoriokokeissa. Hyökkäysliikenteen määrä esimerkissä ylittää palvelimen kapasiteetin noin seitsemänkertaisesti. Ohut punainen viiva näyttää, mikä osuus rehellisten käyttäjien paketeista pääsee läpi hyökkäyksen aikana (seitsemäsosa). TCP-protokollalla kommunikoiva palvelu, esimerkiksi web-sivusto, lakkaa silloin toimimasta kokonaan, eikä asiakkaista yksikään tavoita palvelua. Siniset ristit kertovat tilanteen suodatuksen ollessa käytössä. Vasemmanpuoleisessa kuvassa hyökkäys tulee yhdestä lähettäjän osoitteesta, jolloin suodatus on tehokkaimmillaan (hyökkäysliikenne osuu vain yhteen klusteriin) ja lähes kaikki rehellisten käyttäjien viestit käsitellään. Oikeanpuoleisessa kuvassa hyökkääjä käyttää satunnaisia väärennettyjä IP-osoitteita. Silloinkin noin 80 % rehellisistä käyttäjistä palvellaan, eivätkä he välttämättä huomaa hyökkäystä lainkaan tai se aiheuttaa vain pieniä viipeitä. Lopuille 20 %:lle rehellisistä asiakkaista palvelu tässäkin tapauksessa lakkaa vastaamasta, mutta parannus tilanteeseen ilman suodatusta on silti huomattava.

Käytössä olleella OpenFlow-kytkimellä suodatus pystyttiin toteuttamaan 7 Gbps kaistanleveydellä. Teho noussee kytkimen täyteen 10 Gbps kapasiteettiin, kun laitteen valmistaja

korjaa raportoimamme lastentaudit. Yllättäen suurimmaksi ongelmaksi ei muodostunut suodatuksen nopeus vaan liikennenäytteiden ottamisen rajoitukset. Suodatuksessa tarvitaan hyökkäyksen aikana melko laajakaistaista näytteenottoa, jotta hyökkäysliikennettä pystytään vertaamaan reaaliajassa normaaliliikenteen malliin. Ilmeisesti laajakaistaista näytteenottoa kytkimen täydellä nopeudella ei kytkimen tavallisissa sovelluksissa ole tarvittu. Laitevalmistajan intresseistä on kuitenkin, että ohjelmistolla ohjattavat kytkimet ovat mahdollisimman monikäyttöisiä. Suodatukseen käytetyn laitteiston hinta on vain muutamia tuhansia euroja. Suodatustehoa olisi mahdollista nostaa kymmenkertaiseksi siirtymällä kytkimeen, jossa on kaksi 100 Gbps porttia, mikä riittäisi lähes kaikilta tämän hetken pakettitulvahyökkäyksiltä puolustautumiseen.

Suodatukseen valmistautuminen ja sen käyttöönotto palvelimen ylikuormittuessa tapahtuu kokonaan automaattisesti, eikä vaadi ylläpitäjän toimenpiteitä. Tämä on eduksi, koska palvelunestohyökkäysten suurin vaikutus on usein psykologinen ja kohdistuu ylläpitäjän tai verkkoyhteyden tarjoajan sietokykyyn. Suodatus erillisellä kytkimellä ei myöskään heikennä palvelun toimivuutta normaalikäytössä. Tahattoman ylikuormituksen sattuessa menetelmä johtaa palvelun vakioasiakkaiden priorisointiin.

Yksi menetelmän mahdollinen heikkous on siinä, että hyökkääjät saattavat oppia matkimaan kohdepalveluiden vakiokäyttäjien jakaumaa IP-osoiteavaruudessa. Tämä vaatisi hyökkääjältä huomattavaa työmäärää kunkin kohdepalvelun analysoimiseksi Nykytilanteessa hyökkäyksen käynnistämiseen uutta kohdetta vastaan riittää antaa bottiverkolle yksi komento. Lisäksi IP-pakettien topologien suodatus ja bottiverkkojen kasvanut koko on johtanut siihen, ettei palvelunestohyökkäyksissä enää kovin usein käytetä väärennettyjä IP-osoitteita. Joka tapauksessa kehittämämme suodatus pakottaa hyökkääjän sovellustasolta matalan tason pakettitulvaan, kuten SYN-hyökkäykseen. Tällainen hyökkääjän toimintavapauden rajoittaminen pakottamalla hyökkäys alaspäin protokollapinossa on tyypillistä palvelunestohyökkäyksen suojausmenetelmille.

Lupaava jatkokehityskohde on suodatuksen hajauttaminen OpenFlow-tekniikkaa käyttävään ohjelmallisesti ohjattuun tietoverkkoon niin, että suodatus tehdään mahdollisimman aikaisessa vaiheessa. Näin voisi olla mahdollista estää myös tietoverkon laajemmalta alueelta tukkivat, erittäin laajakaistaiset hyökkäykset. Toinen jatkotutkimuksen suunta on kehitetyn suodatuksen yhdistäminen muihin palvelunestohyökkäysten torjuntamenetelmiin. Projektissa kokeiltiin muita palvelunestohyökkäyksiltä suojautumiseen liittyviä menetelmiä, joita ei kuitenkaan ole vielä kehitetty yllä esitettyä suodatusta vastaavalla tasolle. Erityisesti kokeiltiin pakettien katoamisesta selviävää kuljetuskerroksen protokollaa, josta valmistui projektissa diplomityö.

5. Loppupäätelmät

Lähettäjän IP-osoitteisiin ja normaaliliikenteen määrään perustuva klusterointi osoittautui sekä simulaatioissa että laboratoriokokeissa tehokkaaksi menetelmäksi palvelunestohyökkäysten suodattamiseen. Puolustusmenetelmä suojasi hyvin sekä laajan bottiverkon hyökkäykseltä että keskitetyltä laajakaistaiselta pakettitulvahyökkäykseltä - vaikka hyökkääjä käyttäisi satunnaisia väärennettyjä lähdeosoitteita. Suodatuksen käynnistyttyä yli 80 prosenttia kohdepalvelun vakiokäyttäjistä pystyisi jatkamaan palvelun käyttöä lähes häiriöittä. Samaa suodatusmenetelmää voidaan käyttää suojaamaan sekä sovellustason viesteihin perustuvalta palvelunestohyökkäykseltä että IP-pakettitulvalta.

Suodatuksen laite- ja ylläpitokustannukset ovat selvästi pienemmät kuin tarjolla olevissa kaupallisissa palveluissa, joten myös pienen palvelun on mahdollista suojata itseään kohtuullisilla kustannuksilla ainakin tyypillistä, keskitason tulvahyökkäystä vastaan. Menetelmän mahdolliset rajoituksen liittyvät siihen, miten hyvin hyökkääjät oppivat matkimaan

kohdepalveluiden vakiokäyttäjien IP-osoitejakaumaa. Joka tapauksessa suodatus aina parantaa palvelun toimivuutta hyökkäyksen aikana, eikä se vaikuta palvelun toimivuuteen normaalioloissa.

Kokonaisuutena kolmivuotinen projekti on saavuttanut tavoitteen edullisen ja automaattisesti toimivan, paikallisesti käyttöön otettavan palvelunestohyökkäysten suodatusmenetelmän kehittämisestä. Menetelmä on tarkoitettu erityisesti pienille organisaatioille, joilla ei ole mahdollisuutta ostaa suojauspalveluita palvelunestohyökkäysten varalta tai hajauttaa palvejaan globaalisti.

6. Tutkimuksen tuottamat tieteelliset julkaisut ja muut mahdolliset raportit

Tutkimuksen tuloksia on toistaiseksi julkaisu alla luetelluissa konferenssiartikkeleissa, joista ensimmäinen sai Nordsec 2014 -konferenssin parhaan paperin palkinnon. Lisäksi on tekeillä lehtiartikkeli jossa esitetään kokeelliset tulokset menetelmän toimivuudesta.

1. Aapo Kalliola, Tuomas Aura and Sanja Šćepanović. Denial-of-service mitigation for Internet services. Proceedings of Nordic Conference on Secure IT Systems (NordSec 2014), October 2014. Lecture Notes in Computer Science LNCS 8788. Springer.
2. Aapo Kalliola, Tuomas Aura. Spatially aware malware infection modeling framework. The 14th IEEE International Conference on Computer and Information Technology (CIT 2014), Xi'an, China, September 2014. IEEE Computer Society Press.
3. Jaakko Salo: Packet loss tolerant stream transport protocol, diplomityö 2014.