

Luottamus tietoverkoissa

Internet kehittyi ympäristöstä, jossa käyttäjät olivat kavereita keskenään ja heitä yhdistivät yhteiset akateemiset arvot. Käyttäjät luottivat toisiinsa ja käyttöä voitiin ohjata itsesäätelyn keinoin. Viimeiset 15 vuotta Internet on kuitenkin ollut kaupallinen verkko, jossa käyttäjät eivät luota toisiinsa, jossa pieni osa käyttäjistä ansaitsee rahaa enemmistön hyväksikäytöllä ja jossa siksi ei-toivottu liikenne on jokapäiväinen ilmiö.

Internetissä leviävät haittaohjelmat, epätoivotut mainokset ja epätoivottu sähköposti eli SPAM. Spammaus on liiketoimintaa, joka on parin sadan toimijan käsissä. Siitä kärsivät kaikki loput 1.7B Internetin käyttäjää. Langattomuus kärjistää ongelmaa, koska ilmarajapinnan taajuudet ovat rajallinen luonnonvara. Spammareista alkaa yksi Internetin harmaan talouden arvoketju, jossa ovat mukana mm. ammattihakkerit. Toiminta on kannattavaa, koska palvelumaksut eivät riipu lähetetyn liikenteen määrästä ja koska Internetin ”best effort” periaate tarkoittaa, että verkko tekee kaikkensa palvellakseen lähettäjä. Tulos on, että kommunikaation kustannuksen kantaa vastaanottaja tuhlattuna aikana sekä ylläpito ja hankintakustannuksina.

Suojellakseen verkkojaan ja omia käyttäjiään, yritykset käyttävät verkoissaan yksityisiä IP-osoitteita, joihin ei voi aloittaa liikennöintiä suoraan Internetistä päin. Yritysverkon käyttäjän asiakasohjelman on tehtävä aloite. Yritykset suojelevat omia verkkojaan lisäksi palomuuureilla. Myös käyttäjien omista koneista on nykyään palomuuriohjelmisto. Mitkään näistä eivät ole osa Internetin ”virallista” arkkitehtuuria.

Lähivuosina IPv4 osoitteet ovat loppumassa. Samaan aikaa lisää erityisesti langattomia laitteita liitetään verkkoon. Viralliseksi ratkaisuksi tulevaisuuden Internetin tekniikaksi tarjotaan IPv6:sta. Siinä osoitteen pituus on 16 oktetia. Osoitekenttä tekee mahdolliseksi antaa eri osoite noin 50 000 triljoonalle triljoonalle laitteelle jokaista maapallon asukasta kohti.

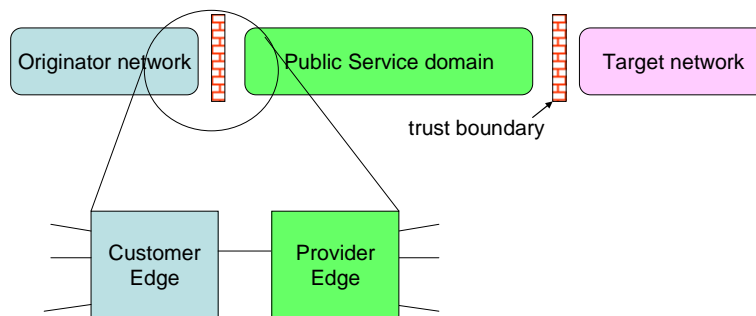
Minä ainakaan en kaipaa sitä, että kuka tahansa muu Internetin käyttäjä näkisi verkossa sinne ehkä kytkemäni triljoonat laitteet, jotka vaikkapa liittyvät kotini turvallisuuteen, lämmitykseen tai jääkaapin sisältöön. Eli luultavaa on, että myös IPv6 maailmassa käyttäjät haluavat piiloutua yksityisiin osoitevaruuksiin ja suojata itsensä palomuurilla. Ratkaisu, jossa palomuri on vasta langattomassa laitteessa, ei liioin toimi. Epätoivottu liikenne pitää torjua jo ennen kuin se kuluttaa langattoman laitteen akkua tai ilmarajapinnan kapasiteettia.

Onkin perusteltua kysyä: mihin tuota suurta IPv6:n osoitevaruutta tarvitaan? Olen viime aikoina levittänyt ajatusta, ettei mihinkään. Siitä on enemmän haittaa kuin hyötyä. Se vaan pahentaa Internetin skaalautuvuus ongelmia ja lisää haittaliikennettä.

Mielestäni tulevaisuuden Internet pitää ajatella luottamusalueiden muodostamaksi verkoksi. Jokaisella luottamusalueella on omat osoitteet. Alueet eivät koskaan näytä osoitteita toisilleen. Jokaisessa paketissa on osoitteen lisäksi vastaanottajan ja lähettäjän identiteetti. Luottamusrajalla on kuhunkin kahden tai useamman käyttäjän kommunikaatioon liittyvä tila, joka löytyy identiteettien avulla ja jonka varassa rajan laite voi suorittaa yhteyteen liittyviä tarkastuksia haluamassaan laajuudessa. Poliitikasta riippuen rajan laite voi päästää tulevat uudet pakettivuot suoraan läpi tai vaikkapa tunnistaa lähettäjän jonkin verkon tukeman menetelmän avulla. Ratkaisussa voimme jatkaa IPv4:n käyttöä isäntäkoneissa.

Jokainen yritys ja koti on luonnollinen oma luottamusalue. Skaalautuvuuden takia julkista palvelua antavat IP-verkot voisivat muodostaa yhden luottamusalueen ja säädellä keskinäisiä suhteitaan ei pakettikohtaisesti vaan tausta-ajona toimivalla ylempien tason järjestelmällä.

Palomuurit ja yksityiset osoitevaruudet ovat reaktiivisia suojakeinoja. Tiedämme, että epätoivotun liikenteen ongelma ei ratkea puolustamalla. Kuten sodassa, niin myös tässä voitto vaatii hyökkäystä. Siksi tueksi tarvitaan järjestelmä, joka jäljittää ja arvioi lähettäjät ja lähettävät verkot sen suhteen kuinka paljon lähettäjän liikenteestä on haitallista. Tämä voisi olla lähtökohta sille, että kommunikaation kustannuksia ryhdyttäisiin vyöryttämään vastaanottajalta lähettäjälle.



Tässä asiasta käyttämäni kuva, jos siitä nyt on apua....