Kyberverkot

Tulevaisuuden tietoliikenne

Mikko Kurki-Suonio

Kyberverkot ovat vaikea aihe peleissä. Monikaan pelaaja ei tiedä miten ne toimivat tai mitä niillä voi tehdä. Pelkinjnohtajat pelkäävät avaavansa Pandoran lippaan verkon kautta. Eikä tilannetta paranna se, ettei useimmilla pelintekijöilläkään näytä olevan minkäänlaista aavistusta asiasta. Ikävä kyllä se ei ole estänyt heitä kirjoittamasta sääntöjä...

Mistä on kyse?

Kyberpunkin kuvaa tietoverkoista on hyvin pitkälle muokannut William Gibsonin Neuromancer, kyberpunkin perusteos. Gibson tosin kirjoitti Neuromancerin mekaanisella kirjoituskoneella, eikä hänellä tuolloin ollut juurikaan ymmärrystä tietokoneiden sielunelämästä.

Kyberpunk on kuitenkin olevinaan jossain määrin realistinen maailmakuva, joten lienee aiheellista tarkastella asiaa hieman tarkemmin. Värikkäät kuutiot, picassotron visiot ja keinotodellisuus ovat tietysti hirveän näyttäviä ideoita, mutta perimmäinen kysymys on kuitenkin: “Kuka sen maksaa?”

Minkäänlaisen kyberverkon toteuttaminen ei ole erityisen halpaa puuhaa, joten maksumiehet on pakko löytää. Ja ne, jotka maksavat todellisista kyberverkoista eivätkä ainoastaan keinotodellisuussovelluksista, odottavat jotain hyötyä investoinneilleen. Kyberverkko on työkalu suuryrityksille. Sitä ei ole luotu hakkerien leikkikentäksi. Kirjanpitäjällä tai pörssimeklarilla ei ole juurikaan käyttöä värikkäille avaruusgeometrian kuvioille.

Miten se toimii?

Miltä kuulostaa 64 kilobittiä sekunnissa, tavallisen puhelinlinjan yli, ilman kalliita laitteita? Modemistit voivat pyyhkiä kuolan ja lyödä päänsä seinään. Tuo on nimittäin nykyajan teknologiaa, nimeltään Integrated Services Digital Network, ISDN. Sitä vain ei ole otettu käyttöön. Se on täysin mahdollinen eikä edes älyttömän kallis jo nykyisellä teknologialla. Ongelma vain on siinä, että investoinnin täytyy lähteä puhelinyhtiöiden tasolta, eikä Forssan mummo takuulla suostu ISDN:n maksumieheksi.

Kyberverkko on aina teknisen toteutuksensa vanki. Vaikka digitaaliset matkapuhelinverkot tulevatkin yleistymään, mikään ei lähitulevaisuudessa korvaa vanhaa kunnon kaapelia, oli se sitten kuparia tai optista kuitua. Tämän seurauksena bitit pysyvät ahtaasti tunneleissaan ja paras työkalu tietoturvan takaamiseksi on edelleen sakset. Kyberverkossa liikkuminen tulee edelleen pohjautumaan erilaisiin yhteyksiin, joista voi kyllä muodostua monimutkainenkin verkko.

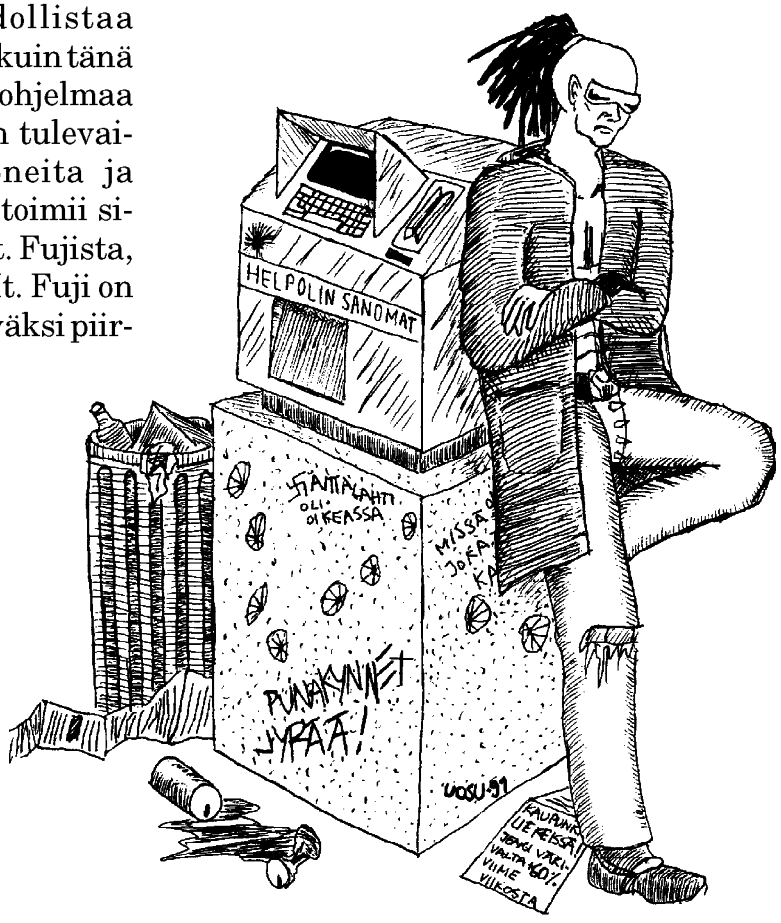
Käyttöliittymä

Perinteinen kyberverkon käyttöliittymä on tietysti keinotodellisuus. Jos jätämme neuroteknologian väliin, ei se itse asiassa ole kovinkaan kaukaa haettu mahdollisuus. Idean ytimenä on kuitenkin, ettei keinotodellisuuden täydelliseen muovaamiseen tarvittavan tietomäärän kuljettaminen verkon läpi ole kannattavaa, vaikka se mahdollista ehkä olisikin. Sen sijaan erikoistunut pääteohjelma käyttäjän päässä voi mahdollistaa keinotodellisuuden käytön. Niin kuin tänä päivänä yhdistetään kaksi peliohjelmaa tietoliikenneyhteydellä, voidaan tulevaisuudessa yhdistää keskuskoneita ja keinotodellisuuspäätteitä. Idea toimii siten, ettei verkossa kulje kuva Mt. Fujista, vaan pelkästään informaatio "Mt. Fuji on tässä". Sitten jää päätteen tehtäväksi piirtää ruudulle vuori tai muuten kertoa tiedosta. Tähän perustuu myös se, että päätekäyttäjä voi ohjelmaansa muokkamaalla vaikuttaa siihen, miltä eri asiat näyttävät, joskin Gibsonistista näkymää tukee se, että geometristen kuvioiden piirtäminen on nopeaa ja ne voidaan välitää hyvin lyhyessä muodossa matemaattisina kaavoina. Jonkin tietyn näkymän pakkosyöttäminen verkon yli on hidasta, kallista ja yleensä turhaa.

Miksi sitten joku haluaa katsella värikkäitä kuutioita ja palloja? Pilviveikot sikseen, kyberverkon maksajat tekevät sillä työtä. Jos jonkinlaiseen käyttöliittymään päädytään, sen tarkoituksena on helpottaa työntekoa. Symbolisten objektien käyttö helpottaa ihmiselle tiedon ja sen rakenteiden hahmottamista. Maccien suosio tietotekniikkaa taitamattomien ihmisten keskuudessa perustuu hyvin pitkälle tähän. Objektien käsittelyn tulisi tietysti olla myös mahdollisimman intuitiivista. Siirteleminen on itsestään selvyys, mutta esimerkiksi tekstitiedoston esitysmuoto olisi hyvin todennäköisesti kirja, olkoonkin että sinne voi itse kirjoittaa väliin vapaasti marginaaleja täyttämättä. Keinotodellisuus palvelee käyttöliitymänä tätä tavoitetta, myös verkon ylitse.

Verkossa liikkuminen

Käyttäjä on kuitenkin ohjelmien vanki. Biti eivät pompi johdosta toiseen, eikä



käyttäjäkään voi tehdä kaikkea. Keinotodellisuus on vain kuva, normaalit luonnonlait eivät tietenkään päde siellä. Vaikka jokin paikka kuvautuisikin laajaksi nurmikentäksi, ei siellä voi liikkua kuin niihin suuntiin, joihin sattuu johtoja menemään. Siksi minusta "dungeon"-tyylinen verkkoesitys on realistisempi kuin Gibsonistinen kyberavaruus.

Siirtyessään noodista toiseen käyttäjä jättää jälkeensä vanan tietoliikenneyhteyksiä, eräänlaisen elämänlangan. Tätä lankaa pystyy tietysti seuraamaan takaisinpäin, mutta sen voi myös katkaista. Käyttäjän kimppuun pystyy siis hyökkäämään muualtakin, kuin sieltä missä hän sattuu juuri oleilemaan.

Lähtöruutu

Mitä näkyy, kun kyberterminaali ensin laitetaan päälle? Gibsonistinen neonmaisemako? Ikävä kyllä, todennäköisesti ei mitään. Ensimmäinen askel on luoda yhteys jonnekin. Se voi olla yhtiön keskuskone tai puhelinyhtiön vaihde, jonka kautta lähdetään luomaan yhteyttä kohdenoodiin. Tai jos suoravalintanumero on tiedossa, voi sitä kokeilla. Loppujen lopuksihan muun muassa tavalliset puhelinyhteydet kulkevat samojen yhteyksien läpi.

Tietoturva

Kyberpeleissä tietoturvan käsittely on sanalla sanoen naurettavaa. Nykyään on käytössä erinomaisen tehokkaita systeemejä, miksi niitä ei muka voisi enää käyttää vuonna 2020?

Yksinkertaisin turvatoimenpide on katkaista kaikki yhteydet. Jos koneen omistaja ei halua mahdollistaa ulkopuolisia yhteyksiä, ei tunkeileva hakkeri voi asialle juurikaan mitään. Tällaisia koneita ovat esimerkiksi yhtiöiden tutkimustietokoneet. Verkkoon liittäminen maksaa, joten etenkin hakkerien ollessa todellinen uhka, ei sinne liitetä kuin ne koneet, joiden toiminnalle tietoliikenne on edellytys.

Turvallisuusrako syntyy siitä, että kyberverkko ylipäätänsä on olemassa. Jotta se olisi olemassa, jonkun täytyy tarvita sitä, ja nämä koneet ovat kiinni verkossa tavalla tai toisella. Hakkeri voi murtautua onnistumalla huijaamaan systeemejä luulemaan itseään lailliseksi käyttäjäksi.

Miten sitten yhteyden saa aikaan? Se voi hoitua joko suoralla yhteydellä eli koneen omalla modeeminumerolla, tai toisen koneen läpi, joko verkon kautta tai kiinteän kaapelin läpi. Tietyllä koneeella voi olla kaikki tai ei yhtään tapaa käytössä.

Suora yhteys

Suora yhteys on periaatteessa perinteinen puhelinnumero. Helpoin tapa suojata sitä on tietenkin pitää se salassa. Hakkerilla ei ole mitään mahdollisuutta ottaa yhteyttä tähän numeroon, ellei hän saa sitä ensin selville. Tosiasissa suuri osa hakkerien työstä ei siksi tapahdukaan koneen ääressä lainkaan, vaan esimerkiksi valehtelemassa numerotiedustelussa tai roskapönttöjä penkomassa.

Perinteisten salasanojen ja vastaavien lisäksi suoria yhteyksiä voi suojata myös niin sanotuilla callback -modeemeilla. Tällainen laite soittaa itse takaisin saatuaan soiton. Ellei tunkeutuja satu soittamaan numerosta, johon callback -modeemi on ohjelmoitu soittamaan takaisin, ainoa toivo on ensin murtautua, usein fyysisesti, puhelinyhtiön keskukseen ja saada se sekoittamaan numerot.

Suoria yhteyksiä ilman callback - varmistusta tulisi olla yleisesti ottaen vain koneissa, joiden halutaan pystyvän ottamaan vastaan yhteyksiä mistä tahansa. Käytännössä näillä koneilla on siis jonkinasteinen asiakaspalvelurooli.

Suora yhteys voi olla myös yksisuuntainen eli se ainoastaan joko vastaanottaa tai lähettää. Tämä voidaan tehdä helposti laitteistotasolla, joten sen murtaminen on mahdotonta. Lukitsemalla linjoja esimerkiksi pelkkään ulossoittoon voidaan varmistaa tietoyhteyksien toiminta hätätilanteessa - jos systeemi haluaa yhteyden jonnekin, se vain soittaa ulos. Ulkopuolinen taho sen sijaan saa soittaa niin paljon kuin lystää, kukaan ei tule vastaamaan. Lukitsemalla linjat vastaanottaviksi pyritään estämään systeemin käyttö välietappina muiden systeemien murtamiseen, puhelinlaskujen kurissapitämisen ohella.

Verkkoyhteys

Verkkoyhteys voidaan luodaan koko tietoverkon, erilaisten tietoliikennesiltojen ja reitittimien kautta. Se on erittäin joustava tapa ja siksi myös yhteyksien normi.

Fyysisesti yhteys voi kulkea monenkin koneen kautta, mutta verkon luonteeseen kuuluu, etteivät ne juurikaan puutu tiedonkulkuun. Ilkeämielinen hakkeri tai puolustaja tosin voivat muuttaa niiden toimintaa tässä suhteessa. Toiminta on kuitenkin aika karkeaa, sillä tällä tasolla edes täsmällinen kohdekone ei ole välttämättä tiedossa, käyttäjätunnuksista puhumattakaan.

Kiinteä kaapeli

Kiinteä kaapeli on tietoturvan kannalta varmin tapa liittää kaksi konetta toisiinsa. Tiedonsiirtonopeuden kannalta se on myös paras vaihtoehto. Ikävä kyllä, koneiden määrän kasvaessa, tarvittavien kaapelien määrä nousee huimiin lukemiin. Niinpä kiinteä kaapeli on käytössä verkon pääkanavien massaliikenteen lisäksi korkeaa tietoturvaa tarvitsevissa kohteissa, kuten esimerkiksi pankkien tietokonejärjestelmissä.

Suojauksessa kaapelin idea perustuu siihen, että tietoliikenne saadaan kanavoitua. Asiakaspalvelusta, postinkulusta ja muusta voi huolehtia täysin erillinen kone, jonka tehtäviin kuuluu myös tietovuon suodattaminen ja valvominen toista konetta varten. Samalla saadaan tärkeä kone piilotettua uteliailta silmiltä.

Matkalla

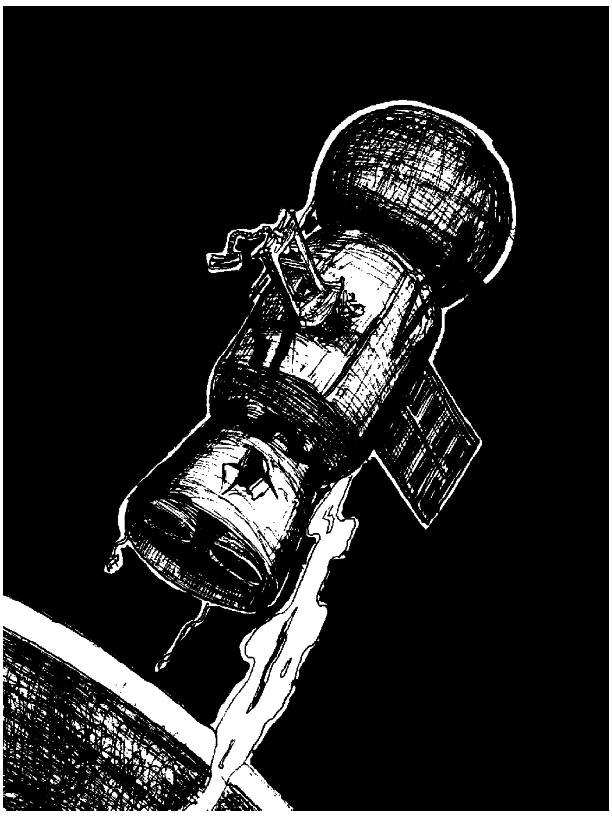
Tietoturvan murtamisen ei tarvitse lähteä yhteenkään koneeseen tunkeutumisesta. On täysin mahdollista iskeä niiden välisiin tietoliikenneyhteyksiin ja poistaa, lisätä tai muuttaa siellä kulkevaa liikennettä.

Ainoa toimiva tapa torjua tätä on salata kulkeva tieto - jopa valokaapelia pystyy salakuuntelemaan. Onneksi modernit salausmemetelmät ovat siinä määrin tehokkaita, että niiden purkamiseen menee yleensä niin paljon aikaa, että tieto

menettää arvonsa sinä aikana. Kuitenkin jokainen salaus murtuu kyllä aikanaan, jos joku käyttää siihen riittävästi aikaa ja vaivaa. Todella salaiset tiedot eivät koskaan kulje elektronisen median läpi.

Sisällä!

Tärkeintä on muistaa, että joku on laittanut koneet ja verkon pystyyn tehdäkseen niillä töitä. Jos systeemi on ylikuormitettu täyteen erilaisia turvatarkastuksia, ei traktorien myynnin neljännesvuosiraportin kirjoittamisesta tule mitään. Kun systeemiin on kerran päässyt sisälle, ei se ole synkkä verkosto täynnä verenhimoisia suojaohjelmia. Jotkin erityiset ohjelmat tai tiedostot saatetaan suojata vielä kertaalleen, mutta jos niihin ei kajoa, ei mitään pelättävää ole. Tämä johtuu yksinkertaisesti siitä, että ylipäätänsä päästäkseen sisään, hakkerin täytyy onnistua vakuuttamaan systeemi siitä, että hän on laillinen käyttäjä. Eikä laillisten käyttäjien aivoja käristetä, jos nämä sattuvat näppäilemään väärän komennon.



Samaten systeemi todennäköisesti pyrkii olemaan luulemalleen lailliselle käyttäjälle mahdollisimman avulias. Koko tietojärjestelmän käyttämisen hyöty katoaa, jos todellisia käyttäjiä vaaditaan muistamaan absurdeja asioita ulkoa tietoturvan nimissä. Security through obscurity ei yksinkertaisesti toimi, vaikka sitä eräät tietokonevalmistajat yrittävätkin syöttää.

Normaaleilla käyttäjillä tulee olla mahdollisuus toimia systeemissä. Tämän vuoksi suojaohjelmien täytyy pystyä tunnistamaan heidät, mikä käytännössä toteutetaan tarvittaessa erilaisilla salasanoilla tai suoraan käyttäjätunnusten perusteella. Hakkerin ongelmaksi tulee siis vakuuttaa systeemille olevansa ei ainoastaan laillinen käyttäjä, vaan joku tietty laillinen käyttäjä.

Mitä tehdä?

Kyberverkko ei ole jokin mystinen astraalitaso tai magiamuoto, jonka avulla voi tehdä mitä lystää. Jos jokin laite tai tieto on kytketty verkkoon, siihen on hyvä syy.

Esimerkiksi teollisuuskompleksien turvajärjestelmien kytkeminen kyberverkkoon on aikalailla typerää. Systeemi voi muutenkin soittaa ulos, eikä toisaalta verkkoon kytkemisellä saavuteta mitään olennaista. Mikäli verkkoyhteys on tällaisiin turvatoimiin erikoistuneeseen koneeseen, se on kiinteä kaapeli johonkin toiseen systeemiin.

Toinen asia on tiedon löytäminen. Kyberverkko pursuaa tietoa. On vain osattava hakea sitä oikeasta paikasta ja pystyttävä suodattamaan olennainen asia tietotulvan seasta.

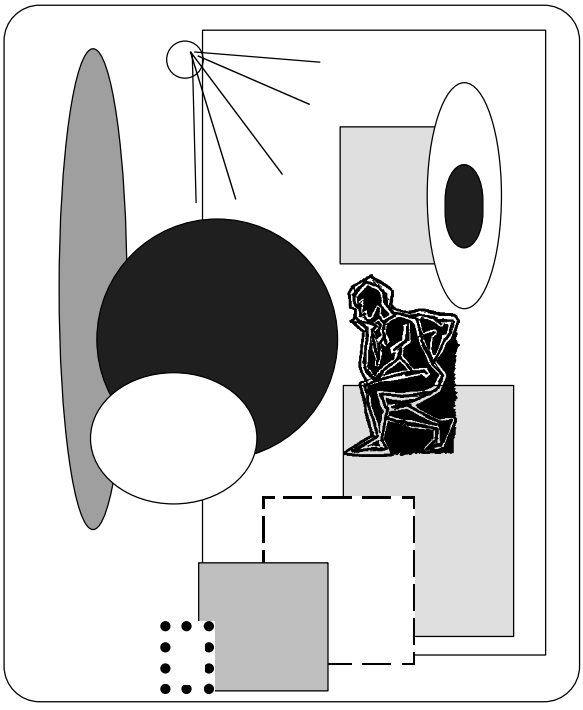
Ehdottoman ensimmäinen asia on tietää, mitä etsii. Esimerkiksi pelkästään "epäilyttävien" asioiden etsiminen vie iän ja terveyden, ellei järkeä.

Seuraavaksi siis pitää löytää systeemi, jossa haluttu tieto voisi olla. Toisinaan tämä on yksinkertaista, toisinaan joudutaan etenemään kiertoteitä. Esimerkiksi jos halutaan paikallistaa joku henkilö, luottokorttifirmalta saattaa löytyä tieto, missä viimeksi muovirahaa tuli käytettyä tai puhelinyhtiöltä, mistä viimeksi soitettua.

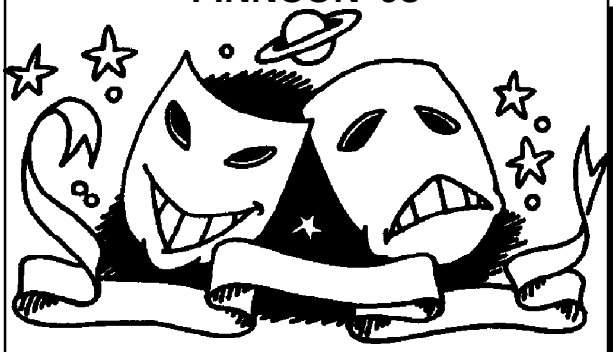
Sitten pitää löytää tieto miljardien bittitovereidensa seasta. Etenkin suuria tiedostoja kahlattaessa tulee vastaan tietokannan rakenne ja eritoten sen indeksointi. Tietokanta indeksoidaan tietysti yleisimpien hakukriteerien mukaan. Eli esimerkiksi väestörekisteri nimen ja henkilötunnuksen. Indeksin mukaan etsiminen on helppoa ja nopeaa. Sen sijaan jos pitää etsiä -07 syntyneitä punatukkaisia kääpiöitä, tietokannan kahlaaminen hidastuu olennaisesti. Erityisesti kannattaa ottaa huomioon, että indeksointi kuvan mukaan on aika lailla mahdotonta.

Lopuksi

Kyberverkon hyväksikäyttö ei suinkaan siis korvaa aivotyötä, ainoastaan jalkatyötä.



FINNCON '93



N A A M I A I S E T

Piakkoin jo perinteeksi muodostuvaan tapaan Finncon '93:n yhteydessä järjestetään taas naamiaiset, joiden voittajille satelee, jos ei vallan maallista mammonaa, niin ainakin mainetta ja kunniaa.

Naamiaiset pidetään Vanhan yo-talon pääsalissa lauantaina 7. elokuuta klo 18 alkaen. Käytännön järjestelyjen helpottamiseksi toivomme, että osallistujat **ilmoittautuisivat ennakkoon 31.5.1993 mennessä.** Jos inspiraatiosi kuitenkin iskee vasta viime hetkellä, voit ilmoittautua myös paikan päällä.

Kerro ilmoittautuessasi esityksesi nimi, mahdollisen ryhmäsi osanottajien nimet (tai ainakin lukumäärä) sekä tietenkin oma nimesi, osoitteesi ja puhelinnumerosi. Kesäkuun alkupuolella saat postitse tarkempia tietoja järjestelyistä. Voit myös esittää toivomuksia taustamusiikin ja valojen suhteen - näitä toteutamme mahdollisuuksien mukaan.

Ilmoittautumiset pyydämme toimittamaan osoitteella:
HYSFK
Marja Sinkkonen
Mannerheimintie 5 B 5.krs
00100 HELSINKI
Voit myös jättää soittopyynnön vastaajaamme, puh. 90-634 918.

Kiittäen
Finncon '93 järjestelytoimikunta