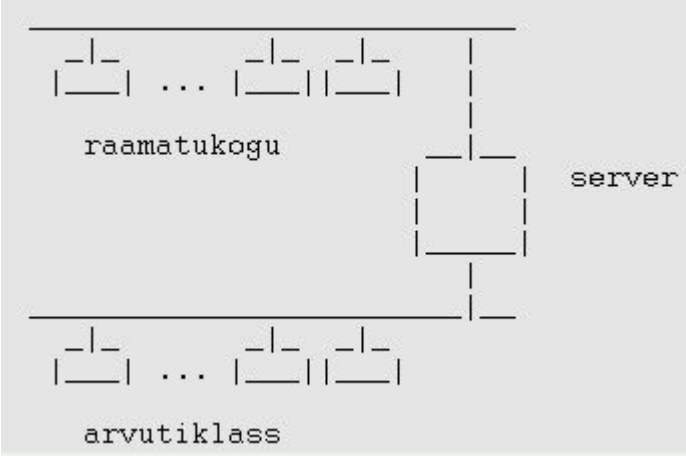
Arvutivõrgud II osa

Kohtvõrguks (ingl. k. LAN - Local Area Network) nimetatakse sellist arvutivõrku, mis asub füüsiliselt piiratud alal ning mille võrguteenused on mõeldud kasutamiseks sama võrgu klientidele. Tüüpiliselt on kohtvõrgud ehitatud kasutades Etherneti tehnoloogiat – arvutid on omavahel ühendatud koaksiaal- või keerupaari kaablitega. Kohtvõrk võib koosneda mitmest alamvõrgust, mis on omavahel ühendatud sobivate võrguseadmetega.

Näide:

Koolimajasisene arvutivõrk, kus serveriga on ühendatud kaks alamvõrku (raamatukogu ja arvutiklass). Koolimaja serveris asuvad kasutajate kodukataloogid, sealt kontollitakse, millist printerit saab keegi kasutada ja server korraldab kohalikele kasutajatele e-posti vahetamist.



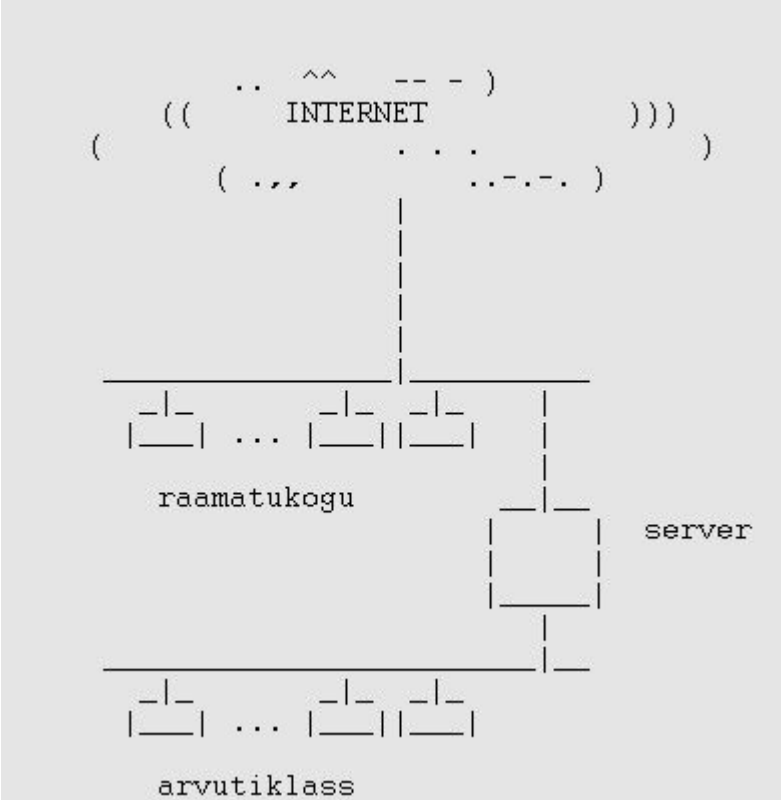
Hiljem või varem nõuavad süsteemi kasutajaid lisaks kohtvõrgu teenusetele võimalust kasutada Internetis pakutavaid teenuseid - veeb, e-post, FTP arhiivid ja kõikvõimalikud nendest tuletatud teenused, näiteks veebipank.

Tehniliselt on Internet ***laivõrk*** (ingl. k. WAN - Wide Area Network), koosnedes paljudest omavahel ühendatud kohtvõrkudest. Kohtvõrkude omavaheliseks ühendamiseks kasutatakse näiteks telefoniliine, raadiosidet, valguskaablit.

Ühendades kohtvõrgu Internetti saab lisaks väliste teenuste kasutamisele hakata kohtvõrgu seest pakkuma ka teistele sealhulgas oma kasutajatele väljapoole teenuseid, näiteks kohalik veebiserver ja e-post.

Järgmine skeem kujutab Internetti ühendatud kohtvõrku, kuid mis ei ole alati parim lahendus.

Koostanud: Merike Hein



Kohtvõrgu ühendamisest Internetti tulenevad turvaprobleemid, nimelt kujutab Internet potsensiaalselt ohtu kohtvõrgule ja vastupidi. Mõlemad vajavad ***kaitset*** :

- Kohtvõrku ja selle kasutajaid tuleb kaitsta võimalike väljast sisse tulevate rünnakute eest.
- Internetti tuleb kaitsta võimalike seest välja minevate rünnakute eest.
- Kohtvõrku tuleb kaitsta seestpoolt tulevate selle sama kohtvõrgu ja tema kasutajate vastu suunatud rünnakute eest.

Töötavas süsteemis peab lisaks nimetatud kaitsete realiseerimisele jääma kasutajatele võimalus süsteemi tarvitada. Mida turvalisem on süsteem, seda ebamugavam on ta reeglina kasutaja jaoks. Oskuslikul konfigureerimisel tunnevad kasutajad end suhteliselt normaalselt ning ka süsteem on suhteliselt turvaline. Sõltuvalt pakutavatest ja tarvitatavatest teenustest võib olla selle saavutamine lihtsam või keerulisem.

Tänapäeval on tundlikku informatsiooni sisalduvad serverid piisavalt hästi kaitstud ja seega on põhiline ründaja motivatsioon sportlik huvi või lihsalt soov segadust tekitada. Eristakse kolme rünnaku eesmärki, üks võib tuua kaasa teise:

- sissetung - tulemusena saab ründaja süsteemi kasutaja või administraatori õigused ning kontrollib süsteemi.

Koostanud: Merike Hein

- DoS (ingl. k. Denial of Service) - näiteks "uputab" keegi teie süsteemi saates sinna suurtes kogustes e-posti; tulemusena ei saa ründaja küll midagi olulist kätte va süsteemi töö halvamine.
- info vargus - näiteks ühendatakse andmeliinile füüsiliselt külge pealtkuulamisseade so vastavalt konfigureeritud arvuti ning salvestatakse kõik või teatud tunnustega andmed; tüüpiliselt kasutatakse saadud andmeid edasiseks sissetungiks.

Kõige primitiivsemaks sissetungi mooduseks on püüda aimata ära mõne süsteemi legaalse kasutaja kasutajanimi ja parool ning sisse logida. Teine populaarne sissetungi viis on kasutada ära mõne kohtvõrgu avaliku serveri programmivigu, mida tõenäoliselt igasugune tarkvara sisaldab. Näiteks e-posti serverina kasutatav programm Sendmail peab tavaliselt olema nõus suhtlema igasuguste "külalistega". Sendmail võimaldab kliendil anda protokolliga ettenähtud korraldusi ning seejärel täidab neid. Eeldatavasti ei kujuta see ohtu süsteemile ja äärmisel juhul lihtsalt toimib DoSina. Teatud puhkudel saab serveri protokolli ja selle realiseerimise piiril tegutsedes keelitada süsteemi tegema midagi, mida ta teha ei tohiks. Näiteks saatma e-postiga välja kohaliku süsteemi kasutajate paroolifaili. Seda omades on aga sissetungijal juba hõlpsam edasi tegutseda.

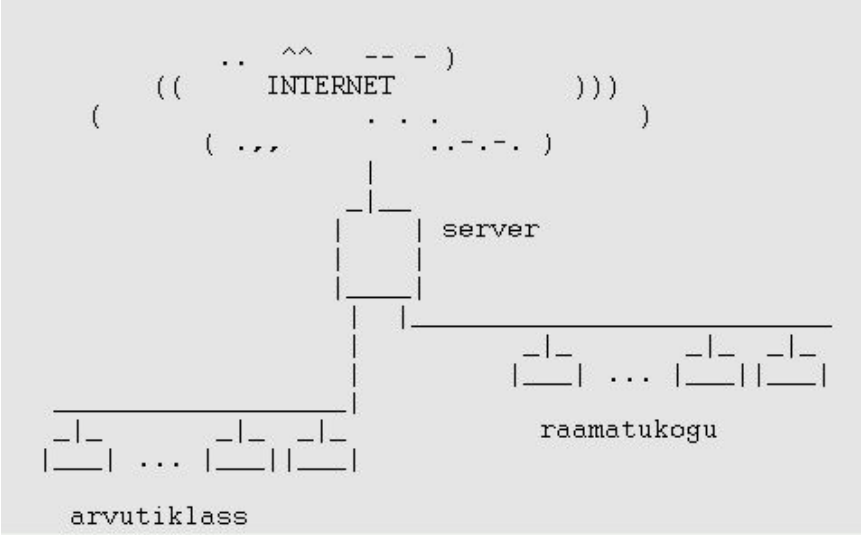
Osutub, et kõige raskem on süsteemi kaitsta seestpoolt tulevate rünnakute eest ning neid esineb ka kõige sagedamine. Süsteemi on seestpoolt rünnata lihsam juba seetõttu, et ollakse süsteemi kasutaja ning omatakse ligipääsu, sealhulgas füüsilist ligipääsu. Tegemist võib olla tõeliselt pahatahtlike kohalike kasutajatega või lihtsalt teadmatusega. Näiteks valivad kasutajad endale liiga kergesti äraaimatava parooli või ei hoia seda endateada.

Kaitse eemärk on väärata väljast sisse tulevad nii serveri kui üksikute kohtvõrgu arvutite vastu suunatud rünnakud. Samuti kaitsta seest lähtuvate võimalike rünnakute eest kohalikke ja väljaspool asuvaid masinaid.

Kasutades eelmisel skeemil toodud arvutite paigutust, tuleks vähemalt kõiki raamatukogu arvuteid ja serverit iga eraldi kindlustada. See vastab ***masina-taseme kaitsele*** (ingl. k. host-level security) ja on suheliselt töömahukas.

Kasutades samu riistvaralisi vahendeid, saab kaitse realiseerimist oluliselt lihtsustada, paigutades kohtvõrgu arvutid selliselt:

Koostanud: Merike Hein



Antud juhul liiguvad andmed kohtvõrgu arvutite ja välismaailma vahel mõlemas suunas läbi ühe sõlmpunkti (ingl. k. choke point), see on antud juhul serveri. Kuna sõlmpunktiks olev arvuti saab seda liiklust kontrollida ja otsustada milliseid ühendusi lubatakse, siis nii tööle seatud arvutit nimetatakse ***tulemüüriks***. Selline skeem vastab ***võrgu-taseme kaitsele*** (ingl. k. network-level security), kuivõrd ühe arvutiga on kaitstud terve arvutivõrk, antud juhul isegi kaks.

Ennekõike peab tulemüür olema ise võimalikult raskesti sissetungitav. Näiteks kui pahalane on saanud haarata tulemüüris juurkasutaja õigused, saab ta antud juhul kuulata pealt kõike alamvõrkudes toimuvat.

Kaitse algab sellest, et teadvustatakse endale ohud ning otsustatakse kuidas neile vastu seista. Kaitse peab muuseas võimaldama võimalikult vara aru saada, et tunneb teie süsteemi vastu kahtlast huvi. Näiteks saab enamuse serverid konfigureerida nii, et nad logivad teatud tunnustega pöördumisi.

Tulemüüri konfigureerimisel soovitatakse lähtuda sellest, et keelatud on kõik väljaarvatud see, mis on lubatud. Näiteks soovides lubada välismaailmal külastada vaid veebiserverit, tuleb keelata kõik sissetulevad ühenduse loomise katsed ja lubada ligipääs ainult sellele pordile, millele vastab veebiserver.

Tulemüür töötab tavaliselt kahel tasemel:

- võrgutase - kontrollitakse IP pakettide liiklust, näiteks IP filter.
- rakendustase - kontrollitakse erinevate rakenduste protokollide tasemel andmevahetust, näiteks vahendusservereid (ingl. k. Proxy).

Tüüpiliselt kasutatakse tulemüüris andmete liikumise kontrollimiseks ***IP filtrit***. IP filtri abil saab hõlpsasti reguleerida IP pakettide liiklust vastavalt IP paketi päises olevate andmetele, näiteks

lähte- ja sihtaadressi ja vastavate portide järgi.

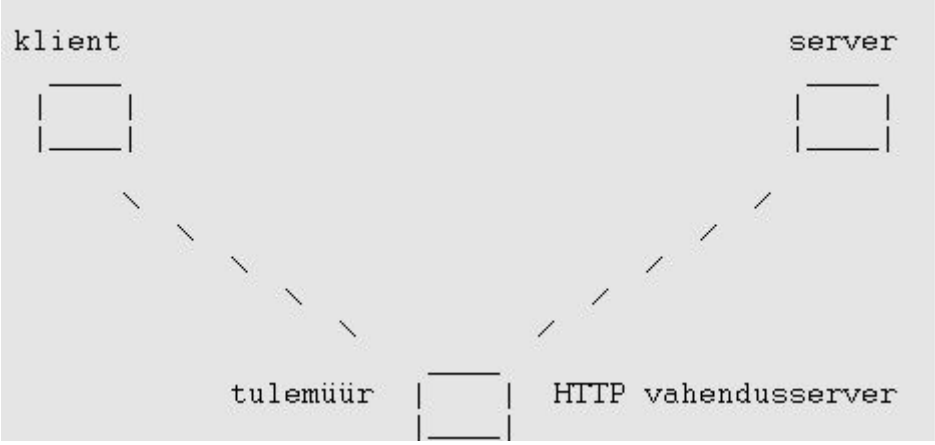
IP filtri kasutamise eelised on:

- ühte kohta saab luua sõlmpunkti, mis reguleerib liiklust kahe või enama alamvõrgu vahel, näiteks kahe alamvõrgu ja Interneti vahel.
- tulemüür on kasutajale nähtamatu - kui vastavaid pakette lubatakse läbi, siis ühendus toimub, kui mitte, siis ühendust ei toimu; kasutaja ei pea omama tööjaamas spetsiaalset tarkvara ega tarvitama standardset tarkvara erilisel viisil.

IP filtri kasutamise puuduseks on, et kuna filter toimib nii madalal tasemel (IP tasemel), siis on raske kontrollida millise-sisulisi ühendusi peetakse. Logimisel ei saa olulist infot.

Äärmuslikul juhul saab rakendada tulemüüris IP filtrit selliselt, et IP paketid ei saagi otse tulemüürist läbi. Tulemüür eraldab kohtvõrgud Internetist. Et siiski kohtvõrgu kliendid saaksid väliseid teenuseid pruukida, kasutatakse tulemüüris vahendusserverid, mis on olemas enamusele olulistele teenustele.

Kui klient soovib näiteks külastada välist veebiserverit, siis esitab ta vastava päringu HTTP vahendusserverile, ning too võtab omakorda ühendust välise veebiserveriga. Väline veebiserver saadab andmed vahendusserverile ning too omakorda kliendile.



Kliendile jääb illusioon, et ta suhtleb otse välise severiga, kuid välisel serveril jääb mulje, et temaga suhtlevaks kliendiks ongi vahendusserver ise. Nii toimivat vahendusserverit nimetatakse ***rakendus-taseme vahendusserveriks*** (ingl. k. application-level proxy) ning tema eeliseks on, et lisaks vahendustegevusele on võimalik tulemüüris sekkuda andmevahetusse sealhulgas logida suhteliselt põhjalikult, kuna tegutsetakse kõrgel tasemel (protokolli tasemel).

Tavaliselt saab rakendus-taseme vahendusserveri kasutamisel tarvitada neid samu klientprogramme mida tavaliselt, kuid nad tuleb vastavalt konfigureerida või kasutamise käigus näidata, millise vahendusserveri kaudu toimetatakse (ingl. k. custom user procedures for proxying).

Koostanud: Merike Hein

Näiteks tuleb Lynxi jaoks väärtustada keskkonnamuutuja HTTP_PROXY masina nime ja pordi numbriga, kus HTTP vahendusserver töötab.

Praktiliselt võimaldavad vahendusserverid andmeid ka ladustada. Näiteks kui üks klient esitab HTTP vahendusserverile päringu, siis ta saadab talle vastuseks soovitud andmed ning salvestab need teatud ajaks ka endale lattu. Kui tuleb järgmine päring samale aadressile ning vahepeal pole möödunud liiga palju ega, siis ei pruugi vahendusserver enam neile andmetele uuesti järele minna, vaid annab pärijale andmed oma laost.

Kokkuvõtvalt:

Kohtvõrk (LAN) on piiratud territooriumil paiknev arvutivõrk, kus kokkuleppeliselt arvutitevaheline kaugus ei ulatu üle 1000 m.

Laivõrk (WAN) on üksteisest füüsiliselt kaugel (kokkuleppeliselt üle 1 km kaugusel) asuvate arvutite ühendamiseks mõeldud arvutivõrk. Laivõrgule on tavaliselt iseloomulik aeglasem andmevahetuskiirus kui kohtvõrgus.

Koostanud: Merike Hein