Tarkvara 29.11.2007

Agenda:

- Tarkvara ja programm – mis on programm, mis on tarkvara;
- Tarkvara liigid – erinevad vaatevinklid;
- Piraatlus ja selle vormid;
- Tarkvara kaitsmine;
- Tarkvara paigaldamine;
- Tarkvara eemaldamine;
- Nuhkvara, reklaamvara, troojalased jne.

Programm ja tarkvara

Programm - *arvuti operatsioonide kindlaotstarbeline järjend (ÕS 2006).*

Tarkvara - *kõik see, mis on vajalik riistvara töölepanekuks, nt reeglid, programmid, juhendid (algselt andmetöötlussüsteemis, hiljem mujalgi) (ÕS 2006).*

Arvutitarkvara all peetakse silmas programmide ja dokumentatsiooni kogumit, mis on tarvilikud mingite tööde teostamiseks arvutisüsteemil. Termin koondab endas kasutajatele otsest kasu andva rakendustarkvara (*application software*) nagu nt tekstitöötlusprogrammid, süsteemse tarkvara (*system software*) nagu nt operatsioonisüsteemid, mis teevad üldse võimalikuks arvuti ressursside kasutamise ning *middleware'*i, mis kontrollib ja koordineerib hajussüsteemide vahelist suhtlust, kliendi ja andmebaasi suhtlust vms. See loetelu ei ole muidugi ammendav – võimalusi ning kriteeriumeid, mille järgi tarkvara liigitada saab, on väga palju erinevaid.

Tarkvara liigid – „programmeerija seisukohast"

Süsteemne tarkvara (*system software*) – tarkvara, mis teeb võimalikuks olemasoleva riistvara, arvutisüsteemi kasutamise. Termin hõlmab endas operatsioonisüsteeme, seadme juhtimisprogramme (*device driver*), diagnostilisi vahendeid ja utiliite (kitsalt spetsiifilist ülesannet täitvad programmid), servereid jne. Süsteemse tarkvara peamine eesmärk on peita süsteemi (peaasjalikult riistvara) detailid ja iseärasused rakendustarkvara (rakendustarkvara loojate) eest. St, et nt kontoritarkvara loomisel ei ole vaja laskuda eraldi iga konkreetse arvutitüübi protsessori või mälukasutuse detailidesse või õppida tundma iga üksiku printeri tööpõhimõtteid ja eripärasid – seda aitavad teha operatsioonisüsteem, draiverid jms.

Programmeerimistarkvara (*programming software*) – programmeerijat tarkvara loomisel abistavad vahendid, mis võimaldavad erinevaid programmeerimiskeeli kasutades programme mugaval viisil kirjutada. Need on tekstiredaktorid (*text editors*), kompilaatorid (*compilers*), interpretaatorid (*interpreters*), debuggerid (programmi töö samm-sammulist jälgimist võimaldav programm) jne.

Rakendustarkvara (*application software*) – võimaldab lõppkasutajatel teostada mingeid kindlaid (igapäevaseid) töid. Rakendustarkvara hõlmab endas nt äritarkvara, koolitustarkvara, meditsiinitarkvara, andmebaase, mänge jne. Kõige suurem rakendustarkvara kasutajate grupp on ilmselt äritarkvara kasutajad, kuid ühel või teisel viisil kasutatakse rakendustarkvara pea igas eluvaldkonnas.

Tarkvara liigid – tavakasutaja seisukohast

Platvormi tarkvara (*platform software*) – sisaldab endas püsivara (*firmware*), juhtimisprogramme (*device drivers*), operatsioonisüsteeme, graafilist kasutajaliidest (GUI), mis lõpuks lubab kasutajal

arvutit ning tema välisseadmeid (*peripheral devices*) kasutada (vrd süsteemse tarkvaraga). Platvormi tarkvara on suuremal või väiksemal määral komplektne arvutiga, kuid sageli (nt PC-l) on võimalik platvormi tarkvara muuta.

Rakendustarkvara (*application software)* – on see, mida inimesed enamasti silmas peavad, kui räägitakse tarkvarast. Tüüpilised näited on kontoritarkvara paketid, mängud jms. Rakendustarkvara ei tule enamasti koos riistvaraga, vaid see muretsetakse eraldi. Vahel küll „tuleb ta koos arvutiga" (nt eelnevalt paigaldatud kontoritarkvara, viirusetõrjeprogrammid jms poest arvuti ostmisel), kuid oma olemuselt on nad ikkagi iseseisvad ja sõltumatud. Seejuures on nad enamasti ka platvormist sõltumatud, kuid siis on neist erinevad väljalasked, rahuldamaks platvormist tingitud eripärasid (nt Windows vs Linux).

Kasutaja poolt kirjutatud tarkvara (*user-written software*) – sageli muudetakse või kohandatakse programmi nii, et see rahuldaks teatud vajadusi ja oleks mugavam kasutada. Nt luuakse malle (*templates*), tekstitöötluse makrosid (*macros*), kootatakse aruandeid etteantud objekte kasutades, skripte pilditöötlusel jne. Isegi e-posti filtrid on mingis mõttes kasutaja poolt loodud tarkvara.

Tarkvara liigid – õiguste ja tasulisuse seisukohast

Litsents - kasutatava tarkvaraga kaasneb peaaegu alati mingi litsents – see on leping, millele peab kasutaja andma oma nõusoleku, et vastavat tarkvara kasutada saaks. Litsentse on palju erinevaid ning sellest lähtuvalt erinevad ka piirangud ja võimalused, mida antud tarkvara kasutades silmas pidama peab. Nii võib olla tarkvara kasutamine võimalik ainult „raha eest", tarkvara võib olla rangelt seotud konkreetse riistvaraga (OEM litsents), tarkvara võib olla vaba vaid kasutamiseks, kuid vaba võib olla ka selle muutmine ja levitamine. Üks võimalikke jaotusviise, kuidas nende kriteeriumite järgi tarkvara liigitada, oleks järgmine:

Tasuline tarkvara (*commercial software*) – kommertstarkvara, tarkvara, mille kasutamise eest tuleb alati maksta sõltumata sellest, kes seda kasutab.

Vaba tarkvara, vabavara (*free software*) - FSF'i (Free Software Foundation) poolt levitatav avatud koodiga tarkvara, mida kasutajatel on õigus paremaks muuta ja levitada kas tasuta või tasu eest. Tingimuseks on seejuures, et muudatused oleksid korralikult dokumenteeritud ja lähtekood jääks avatuks.

Priivara, tasuta tarkvara (*freeware*) - autoriõigusega kaitstud tarkvara, mida autor lubab tasuta kasutada kas kõigil soovijatel või teatud kasutajate rühmal, näit. haridusasutustel. Priivara kasutamine oma isiklikuks tarbeks on vaba, kuid seda ei tohi edasi müüa (levitada kommertseesmärkidel). Tavaliselt kirjutab autor täpselt ette, mida konkreetse priivaraga tohib teha ja mida mitte ning teeb seda eesmärgiga „anda ühiskonnale midagi", kuid seejuures säilitada kontroll tarkvara edasise arenduse üle. Priivara ei ole sama, mis vabavara!

Jaosvara, ühiskasutusega tarkvara (*shareware*) - algselt nimetati jaosvaraks sellist tarkvara, mida jaotati n.ö. aumeeste mängu põhimõttel. Autor lubas jaosvara teatud aja vältel tasuta proovida ja kui see teile meeldis, siis paluti annetada autorile väike rahasumma. Nüüdseks on jaosvara mõiste sisu muutunud. Seda saab endiselt tasuta alla laadida, kuid kasutusaeg on piiratud (nn. prooviaeg, näit. 1 kuu) või on osa funktsioone blokeeritud. Kui soovite jaosvara kasutada ka pärast prooviaja lõppu või aktiveerida kõik funktsioonid, siis tuleb tasuda nõutud summa. Kui olete maksnud, registreeritakse teid jaosvara pakkuja juures ning te hakkate regulaarselt saama kõnealuse tarkvara täiendusi, uusi versioone ja uudiskirju. Jaosvara on odav, sest selle on tavaliselt kirjutanud eraisikust programmeerija või mõni väike firma ja seda pakutakse üle Interneti otse klientidele. Jaosvara erineb

avalikust tarkvarast (*public domain software*) selle poolest, et jaosvara autoriõigused on kaitstud, s.t. seda ei tohi oma nime all edasi müüa.

*** Jäänukvara või aegunud tarkvara (*abandonware*)** – viitab tarkvarale, mille kasutamine ei ole enam aktuaalne. Algselt viidati sellise terminiga vananenud arvutimängudele, kuid seda kasutatakse vahel ka teiste tarkvaraklasside puhul. Aegumise definitsioon võib mõnevõrra kõikuda – see võib olla, kas a) kasutusel tarkvara korral, mis ei ole enam laialdaselt kättesaadav või seaduslikul (ostmise) teel omandatav või b) on teatud vanusega.

Tarkvara liigitus - nuhkvara, reklaamvara, …

Nuhkvara (*spyware*) - on tarkvara, mis paigaldatakse arvutisse salaja, kasutaja teadmata eesmärgiga osa võtta kasutaja tegevustest või sekkuda neisse ilma, et selleks kasutaja arvamust küsitaks või teda sellest teavitataks. Kuigi termin „nuhkvara" viitab sellele, et programm jälgib salaja kasutaja tegevusi ja käitumist, on tegelikkuses nuhkvara võimalused ja funktsioonid palju suuremad kui ainult jälgimine. Nuhkvara kogub isiklikku informatsiooni, kuid võib ka tegevustesse vahele sekkuda ja kontrolli arvutis üle võtta, paigaldada veel lisaprogramme, suunata brauserit soovimatutele lehtedele (mis võivad veel rohkem kahju põhjustada jne). Samuti võivad nad muuta arvuti seadeid, mõjutada võrgu kiirust jms.

Reklaamvara (*adware* või *advertising-supported software*) – tarkvarapakett, mis sisaldab endas funktsionaalsust, mis automaatselt mängib, näitab või laeb alla reklaammaterjali peale seda, kui põhiprogramm on paigaldatud ja seda on kasutama hakatud. Tavaliselt nähakse sellist tüüpi tarkvara võlu selles, et programmi looja saab niimoodi kompenseerida esialgse programmi loomisele tehtud kulutusi. Nt lubatakse mõningatel juhtudel programmi kasutada tasuta, kui reklaamvara on peal – sellest vabanemiseks tuleb maksta.

Klahvinuhk *(keylogger)* – klahvinuhk on oma olemuselt nuhkvara, mis salvestab kõik klahvivajutused algul failina arvuti kõvakettale ja hiljem saadab need üle Interneti ettenähtud e-posti või FTP aadressile. Klahvinuhk võib olla realiseeritud ka riistvaraliselt ja selle võib paigutada klaviatuurijuhtme pistiku ja pesa vahele või monteerida klaviatuuri sisse. Sellised klahvinuhid salvestavad klahvivajutused oma sisemällu. Kui riistvaralised klahvinuhid salvestavad tõepoolest ainult klahvivajutusi, siis tarkvaralised klahvinuhid salvestavad ka ekraanipilte ja hiireklõpse.

Klahvinuhk installeeritakse teie arvutisse teie teadmata ja seda võivad teha lapsevanemad, teie asutuse süsteemiülem, valitsuse jälitusorganid jt, kellel ongi õigus teie tegevust kontrollida. Nii saab jälgida, milliseid veebisaite te külastate, millest lobisete jututubades, kellega vahetate e-posti ja mis on nende sõnumite sisu jne. Seejuures registreeritakse ka iga tegevuse täpne aeg. Enamasti tegelevad klahvinuhkide installeerimisega aga kurjategijad, kes soovivad välja nuhkida teie paroole, krediitkaardinumbreid jms informatsiooni, et teha tühjaks teie pangaarve, võtta teie nimel laenu, ajada teie kaela oma kuritegusid jne.

Trooja hobune *(Trojan horse)* - kasuliku programmi või andmete sisse manustatud kahjulik programmiosa, mis täidab tegelikult mingit varjatud ülesannet, näiteks muudab teatud tingimustel andmeid, rikub kõvakettal failipaigutustabeli (FAT) või teeb arvutis muud kurja. Trooja hobust nimetatakse vahel ka arvutiviiruseks, kui see laialt levib, kuigi erinevalt viirusest see ise ennast ei paljunda. Enamasti kasutatakse terminit "Trooja hobune" siiski ainult nende kuritahtlike programmide kohta, mis ise ei paljune ning isepaljunevaid programme nimetatakse viirusteks.

Arvutitarkvara ja piraatlus

Autoriõigustega on kaitstud kõikvõimalikud teosed paljudest erinevatest eluvaldkondadest. Eesti

Vabariigis kehtiva “Autoriõiguse seaduse” §4 lg 3 p 3 järgi kuuluvad arvutiprogrammid Autorikaitse alla sarnaselt kirjandusteostele – st programme käsitletakse kui kirjatükke. Kaitse laieneb arvuti-programmi mis tahes väljendusvormile ning kehtib ka programmi loomise lähtematerjalidele.

Kuigi arvutitarkvara lahutamatuks osaks loetakse ka kasutusjuhendid, tarkvarakirjeldused jne, on kõige tähtsamaks osaks arvutiprogramm. Tarkvara litsentseerimisel annab programmi looja kliendile tarkvara kasutamiseks litsentsilepingus sätestatud tingimustel. Lepingu tingimused on autori määratavad, kuid on mõningal määral piiratud kehtiva “Autoriõiguse seadusega”. Näiteks ei ole “Autoriõiguse seaduse” §18 lg 2 p 4 järgi lubatud arvutiprogramme reprodutseerida isiklikeks vajadusteks ilma autori nõusolekuta ja autoritasu maksmiseta, kuid sama seaduse §24 kohaselt on see erandkorras lubatud programmis olevate vigade parandamiseks, programmi kasutamiseks seadmetel, ulatuses ja eesmärkidel, milleks programm omandati ning lubatud on ka varukoopia tegemine hävinud, kadunud või kasutuskõlbmatuks muutunud programmi taastamiseks. Samuti on lubatud §25 alusel dekompileerimine, kui see on hädavajalik informatsiooni saamiseks algsest programmist sõltumatult loodud programmi ühilduvuse tagamiseks teiste programmidega. Dekompileerimise võimalikkus soodustab aga konkurentide poolset koodivargust.

Tarkvara ostes (või ka tasuta saades) ei ole, lähtuvalt “Autoriõiguse seadusest” oluline, kas tarkvara omandati edasimüüjalt või otse selle loojalt, kasutades andmekandjana CD-d, disketti, Internetti või muud kanalit, kuna erinevalt tavalisest ostu-müügi tehingust ei omanda ostja programmi, vaid saab selle kasutusõiguse just selliste piirangute ja õigustega, nagu seda näeb ette litsentsileping. Programm ise jääb oma autori omandiks, kasutaja nõustub autori esitatud tingimustega ning on vastutav, kui rikutakse lepingu tingimusi.

Piraatkoopiaks loetakse arvutiprogrammi mis tahes riigis reprodutseeritud koopiat, kui seda on tehtud ilma autori või autoriõiguste omaja loata. Samuti loetakse piraatkoopiaks sellist koopiat, mis on reprodutseeritud välisriigis autoriõiguste omaja loal, kuid mida levitatakse või kavatsetakse levitada Eestis ilma autoriõiguste omaja loata. “Autoriõiguse seaduse” §82 kohaselt loetakse piraatkoopiaga kauplemiseks piraatkoopia müüki, rentimist, müügile pakkumist või rendile pakkumist, samuti piraatkoopia ladustamist, hoidmist või edasitoimetamist ärilisel eesmärgil.

Tarkvarapiraatluse vormid

Tarkvarapiraatlusel on mitmeid erinevaid vorme ning see, kuidas neid liigitada ja milliseid neist välja tuua, on mõneti meelevaldne. Üks võimalik jaotus on järgmine:

- Tarkvara võltsimine (*counterfeiting*);
- Litsentsita tarkvara installeerimine (*hard-disk loading*);
- Piraatkoopiate levitamine Internetis ja allalaadimine Internetist (*Internet piracy*);
- Tarkvara reprodutseerimine (*end-user copying*);
- Rentimine või laenutamine (*renting or leasing*).

Tarkvara võltsimine on illegaalne ning enamasti suuremahuline autorikaitse alla kuuluva tarkvara reprodutseerimine ja levitamine (müük). Erinevalt tavalisest piraatkoopiast näeb võltsing tihti välja autentne – reeglina kuulub sinna juurde originaali täpselt matkiv pakend, aga võimalik, et lisaks on veel ka kasutusjuhend, libalitsentsid ja isegi originaalile sarnanevad turvaelemendid.

Seetõttu võib osutuda originaali ning piraatkoopia vahel vahet tegemine üsnagi raskeks. See omakorda võimaldab võltsingut müüa originaalilähedase hinnaga ning saada suuremat kasumit. Tarkvara võltsimine rikub autori varalisi õigusi, kaubamärgi omaniku õigusi ning selle kasutamine on käsitletav seaduserikkumisena, kuna puudub autori luba (litsents) toodet kasutada.

Litsentsita tarkvara installeerimise ehk *hard-disk loadingu* all peetakse silmas illegaalse tarkvara paigaldamist arvuti kõvakettale. Sellisel juhul puuduvad dokumendid, mis tõestaksid inimese õigust kasutada antud tarkvara ning samuti ei ole tarkvara kasutajal originaalandmekandjaid (CD-d, disketid)

ja muid komponente, mis sama tarkvara legaalse vormiga alati kaasas käivad. Selline teguviis on levinud esmajoones väiksemate (ja vähemtuntud) arvutifirmade seas, kes üritavad müüdavat riistvara lisatava (litsentsita) tarkvara abil atraktiivsemaks muuta. Piraatkoopiate levitamine Internetis ja allalaadimine Internetist (nimetagem seda inglisekeelse vaste (*Internet piracy*) eeskujul edaspidi Internetipiraatluseks) on tarkvarapiraatluse üks nooremaid vorme. Sellest hoolimata on tegemist piraatluse vormiga, mis tarkvara tootjatele (ning laiemalt võttes kõigile, kes oma autoriõigusi kaitsta soovivad) vast kõige enam peavalu valmistab. Internetipiraatlusele aitavad kaasa Interneti kasutajate arvu plahvatuslik kasv, suhteliselt väike vahelejäämise risk, suurenevad andme-edastuse kiirused jms. Enimtuntud vahendid, mille kaudu piraattarkvara Internetis liigub, on ftp-serverid, failivahetusprogrammid ning tavalised veebiserverid.

Tarkvara reprodutseerimine on reeglina ebaseaduslik ning selle võib jagada tinglikult kaheks:

- Reprodutseerimine otsese tulu saamise eesmärgita;
- Reprodutseerimine otsese tulu saamise eesmärgil.

Esimesse kategooriasse langevad juhud, kus arvutisse on installeeritud reprodutseeritud tarkvara ilma sellekohase litsentsi ja autoriõiguste omaja loata või on tarkvara paigaldatud rohkematesse arvutitesse, kui seda lubab omandatud litsents (kasutatakse inglise keelset terminit *softlifting*). Siia alla kuulub ka teine litsentsi ületarvitamise võimalus – tarkvara installeeritakse kesksesse serverisse ning see on kasutamiseks kättesaadav klientarvutites, kuid kasutajaid on litsentsiga lubatust rohkem (*client-server overuse*). Ka sõbrale laenamise või töölt koduarvutisse tehtud koopia korral võib rääkida ebaseaduslikust tarkvara reprodutseerimisest. Tegemist on maailmas enim levinud tarkvarapiraatluse vormiga, mis moodustab rahaliselt mõõtes enam kui poole piraatluse tõttu saamatajäänud tuludest.

Ebaseadusliku reprodutseerimise teise kategooria moodustavad juhtumid, mida ei saa klassifitseerida võltsinguks, kuna isegi ei püüta kopeeritud isendist jätta muljet kui originaalist, ent sarnaselt võltsingule on tarkvara kopeeritud tulusaamise eesmärgil ehk müügiks. Sellised piraatkoopiad on enamasti kordades või isegi suurusjärgu võrra odavamad originaalist. Selleks, et autoriõigusi kurjasti ära kasutada, ei pruugi tarkvara olla illegaalse päritoluga, vaid ka täiesti seaduslikult soetatud tarkvara laenamine või rentimine võib olla vastuolus litsentsilepinguga ning on sellest johtuvalt karistatav tegevus. “Autorikaitse seaduse” järgi võib õiguste omanik laenamist või rentimist lubada (AutÕS §13 p 2), kuid ta ei pruugi seda sugugi teha. Siinjuures on oluline kahel mõistel vahet teha – kui rentimine on tarkvara või selle koopia andmine ajutiseks kasutamiseks otsese või kaudse tulu saamise eesmärgil, siis laenutamise puhul mingit tulu saamise eesmärki kaasatud ei ole.

Seadusandlikud meetmed tarkvara kaitsmiseks

Autoriõigus

“Autoriõiguse seaduse” kohaselt tekib arvutiprogrammidele ning nende mis tahes väljendus-vormidele automaatselt autoriõigus, kuid seaduse viienda paragrahvi 8nda punkti kohaselt ei kaitsta ideid ning põhimõtteid, millele rajanevad programmi elemendid. Seega ei ole “Autoriõiguse seaduse” järgi kaitstav idee iseenesest, küll on aga kaitstud selle idee väljendusvorm – programmikood.

Kuna enamasti ei ole kommertstarkvara loojate huvides, et nende ideid ning algoritme konkurendid kerge vaevaga ära saaksid kasutada, jääb siin “Autoriõiguse seaduse” poolt pakutavast kaitsest väheks, kuna see käsitleb peamiselt vaid loata tarkvara kopeerimist ning sellele järgnevat kuritarvi-tamist. Samuti püsib koodifragmentide kopeerimise seaduslikkuse küsimus. Seetõttu ei piisa tarkvarakaitseks kindlasti mitte ainult kõnealusest seadusest.

Patendiõigus

Sarnaselt autoriõigusele ei kaitse ka patendiõigus ideed, vaid leiutist e. mingi probleemi uudset lahendust. “Patendiseaduse” [2] §6 lg 2 p 5 järgi ei loeta leiutise objektiks muu hulgas arvutialgoritme ja -programme ning seega ei saa ka neid otseselt patenteerida, kuid seda on võimalik teha, kui

programm on seotud mingi leiutise objektiga. Kuigi tarkvarale patendi taotlemine võib võtta rohkem aega, kui on toote enda eluiga ning lisaks sellele on protsess ka kulukas, seda vahelduva eduga ikkagi kasutatakse (eriti USA-s). Patendiõiguse rakendamise kasuks räägib asjaolu, et võrreldes autoriõigusega antakse patendi omajale laiemad õigused: kui autorikaitse rikkumiseks ei loeta identse teose loomist iseseisvalt, siis sama lahenduse väljatöötamine iseseisvalt teise isiku poolt loetakse patendiõiguse rikkumiseks.

Ärisaladuse õigus

Ärisaladuse õigus võimaldab keelata teistel isikutel kasutada või avalikustada toote kohta käivat salajast informatsiooni, kui see on vastuolus pooltevahelise lepinguga. Ärisaladuse valdajal ei ole õigust takistada ärisaladuse objektiks oleva teabega identse teabe väljatöötamist, kuid üheks ärisaladuse tunnuseks loetakse, et kaitstavat teavet peab olema võimatu legaalsete vahendite abil reprodutseerida. Ärisaladuse õigusega võib olla kaitstud erinevalt autorikaitse õigusest tarkvara mõni funktsioon, idee, algoritm vms, mis annab tarkvarakaitsele uued mõõtmed ning seda kasutatakse üsna laialdaselt.

Lepinguõigus

Tarkvara litsentsilepingul on kaks peamist eesmärki:

- Määrata kindlaks tarkvara kasutamise tingimused;
- Tagada lepingutingimuste rikkuja vastutusele võtmise võimalus.

Tavaliselt keelatakse litsentsilepinguga tarkvara reprodutseerimine, selle levitamine, muutmine, dekompileerimine ja muud tegevused, mis mingil viisil võivad seada ohtu toote autori või autoriõiguste omaja huvid. Tihti on litsentsilepinguga määratud ka tarkvaraga kaasas oleva dokumentatsiooni ning kasutusjuhendite kasutustingimused. Litsentsilepingu ning tehniliste meetmete koosrakendamisega võidakse sundida kasutajat loobuma “Autoriõiguse seadusega” tagatud õigustest. Näiteks võib olla kasutaja sunnitud litsentsilepinguga nõustudes aktsepteerima tarkvara tootja poolt tehniliste vahenditega tarkvarast koopia tegemise võimatuks muutmist, kuigi “Autoriõiguse seadus” lubab erijuhtudel tarkvarast koopiaid teha.

Seadusandlike meetmete tõhusus

Eelpool loetletud seadusandlike meetmete tõhusus sõltub ennekõike riigi õigussüsteemist ning konkreetse kaitstava objekti iseärasustest. Kõigi nende ühiseks puuduseks on aga see, et kokkuvõttes ei hoita mis tahes seadusandliku meetme või nende komplekti rakendamisel midagi ära, vaid luuakse ainult baas, mille alusel võimalikke rikkumisi klassifitseerida. Ükski seadus ega leping ei anna kaitset rünnete eest, vaid annab võimaluse võidelda tagajärgedega. See on aga reeglina keeruline ja aeganõudev protsess.

Tehnoloogilised meetmed

Kuna seadusandlikud meetmed annavad meile parimal juhul vahendid võitlemaks tagajärgedega, kuid ei hoia ära ründeid, on efektiivseks tarkvara kuritarvitamise vastaseks kaitseks vaja rakendada ka tehnoloogilisi meetmeid. Tehnoloogilised meetmed, mille abil püütakse tagada, et toodetud tarkvarast ei tehtaks piraatkoopiaid, et neid ei dekompileeritaks, muudetaks jne, jagatakse esmalt kahte suurde klassi – tarkvaral ja riistvaral põhinevad vahendid.

Riistvaralised meetmed

Erinevalt seadusandlikest vahenditest pakuvad riistvaralised vahendid reaalset, ennetavat rünnetevastast kaitset. Enamasti on riistvaralised meetmed suunatud tarkvara illegaalse kopeerimise vastu, st püütakse vältida tarkvara kopeerimist ja litsentseerimata kasutamist, kuid muud tarkvarakaitse vaatevinklist olulised aspektid on katmata. Ilma riistvaralise kaitse abita on mis tahes programm (kui tahes krüpteeritud, sogastatud vms) oma olemuselt lihtsalt bitijada, mida on võimalik alati kopeerida, oma masinal käivitada ja uurida. Peamised riistvaralised tarkvara kaitsmise meetmed on järgnevad:

Kaitstud protsessor (*shielded CPU*) ja krüpteeritud andmed;

- Limiteeritud installeerimised;
- Pordilukk (*dongle*);

- Kaitstud andmekandja;
- Peidetud seerianumbrid;
- *CD-key*.

Parima võimaliku kaitse tarkvarale annaks füüsiliselt kaitstud eriotstarbeliste arvutite (nt mängukonsoolid) müümine koos vastava tarkvaraga, kuid praeguseid tehnoloogilisi võimalusi ning üldotstarbelistele arvutitele suunatud tootmist arvestades on see praktiliselt välistatud. Hoopis reaalsem on kasutada täielikult eriotstarbelise süsteemi asemel nö tarkvara-riistvarapaketti (*SH-packet ehk software-hardware-packet* [4]), mis koosneb kaitstud protsessorist ning krüpteeritud tarkvarast. Sellise lahenduse puhul on protsessori eriotstarbelisse ROM mällu talletatud krüpteerimisvõti, mille abil mälusttoodud krüpteeritud andmed dekrüpteeritakse, tööks kasutatakse, seejärel uuesti krüpteeritakse ning mällu kirjutatakse. Sealjuures on kaitstud ainult protsessor – mälu ning muud komponendid, kus krüpteeritud programm ja andmed paiknevad, ei pea olema kaitstud. Tegemist on keeruka ent kahtlemata efektiivse võimalusega, mis lisaks piraatkoopiate tegemise välistamisele ka dekompileerimist ja pöördprojekteerimist oluliselt raskendab.

Üheks koopiate tegemise vastaseks meetmeks on andmekandjale maksimaalse võimaliku installeerimiste arvu määramine. See eeldab tarkvara levitamist korduvkirjutataval andmekandjal nagu näiteks disketil. Iga kord, kui selliselt andmekandjalt toimub uus installeerimine, suurendatakse loendurit ning kindlaks määratud arvu ületades enam järgnevaid installeerimisi ei lubata. Antud meetodi töötamiseks peab olema loendurit sisaldav fail krüpteeritud ja hästi peidetud, et seda ei saaks muuta. Samuti on oluline, et andmekandjat ei saaks tavalisel viisil kopeerida, kuna sel juhul kaotaks loendur mõtte. Seda meetodit kasutatakse suhteliselt vähe, kuna piirangu seab andmekandja korduvkirjutatavuse nõue. Samuti ei ole võimalik sel viisil kaitstavat tarkvara levitada Interneti vahendusel, kuna tarkvara peab olema spetsiaalsel andmekandjal.

Pordiluku all mõistetakse mis tahes piraatlusevastast elektroonilist lisaseadet. Tänapäeval on valdavalt kasutusel USB-porti paigaldatavad pordilukud, kuid on ka printeri või *serial* porti kasutavaid seadmeid. Kaitstav tarkvara müüakse komplektina koos ainulaadse pordilukuga, mille olemasolu programmi käivitamisel kontrollitakse ning selle mitteleidmisel programmi käivitamine peatatakse. Kuigi enamasti on pordiluku ülesandeks kaitsta tarkvara ebaseaduslike koopiate loomise eest, võib seda kasutada ka paljudel muudel eesmärkidel – tarkvara litsentseerimine, andmebaasi juurdepääsu kontroll, erinevate loendurite rakendamine, versiooni kontroll jne.

Pordiluku miinusteks on Interneti kaudu levitamise võimatus (iga tootega peab olema kaasas kindel füüsiline seade), selle rakendamiseks võib vaja minna spetsiaalseid draivereid, iga seade hõivab ühe pordi ning nende kasutamine võib olla tülikas. Oluline on, et rakendatavate meetmete efektiivsus ei sõltu mitte pordilukust, vaid tarkvarasse programmeeritud mehhanismide keerukusest – kui kontroll- ja/või lukustusmehhanismid on kergesti kõrvaldatavad või välditavad, ei ole ka pordilukust suuremat kasu.

Tarkvara installeerimise käigus võidakse luua juhuslik ning arvutisse krüpteeritud kujul peidetav seerianumber. Selleks, et saavutada programmi täielik funktsionaalsus või et üldse programmi käivitamine võimalik oleks, tuleb võtta ühendust tarkvara müüjaga, kes annab kliendile tema seerianumbrile vastava parooli. Programmi käivitamisel kontrollitakse seerianumbri ja parooli vastavust, mille sobides programm käivitub. Selle meetmega kaasnevad ka omad ebameeldivused – kuna seerianumbrit sisaldav fail paikneb kasutaja kõvakettal, tuleb nt peale operatsioonisüsteemi vahetust või tarkvara uuesti installeerimist see ka uuesti registreerida, kuna seerianumber lihtsalt süsteemist kaob või genereeritakse uus ja senise parooliga mittesobiv seerianumber. Samuti on võimalik seerianumbrit sisaldav krüpteeritud fail süsteemist üles leida ning selle abil ikkagi ebaseaduslikke koopiad teha.

Vast kõige enam on tavakasutaja kokku puutunud nö *cd-key*'ga, mis kujutab endast tähtede ja numbrite kombinatsiooni, mida nõutakse enne tarkvara installeerimise alustamist CD-lt. Kui sisestatud sõne ei klapi CD-l oleva tarkvarasse sisseprogrammeerituga, installeerimisprotsess

katkestatakse. Olenevalt tarkvarast võib olla iga kasutaja jaoks eraldi *cd-key* või kõigile üks ühine. Siiski ei ole seegi vahend eriti turvaline, kuna on võimalik kasutada ühte võtit piiramatu arv kordi. See teeb kergeks piraatkoopia ja sellele sobiva võtme levitamise füüsilisel kujul või ka Interneti teel.

Tarkvaralised meetmed

Tänapäeval on tarkvarakaitse riistvaraliste meetmete kasutamise esimeseks vastuargumendiks Interneti teel tarkvara levitamise võimaluse välistatus, kuna kõik eelpool toodud meetmed eeldavad mingit spetsiaalset andmekandjat või arvutiarhitektuuri. Kuigi riistvaraliste vahendite kasutamine pakub seadusandlike meetmete kõrval tarkvarale lisakaitset, ei piisa tarkvara efektiivseks kaitsmiseks ainult neist.

Tarkvara vastu on kolm põhilist erinevate eesmärkidega ründeviisi ning seetõttu on vaatluse all ka kolm erinevat vastumeedet – vesimärgistamine (*watermarking*) piraatkoopiate tegemise vastu, koodi terviklikkuse kontrollimine (*integrity check*) omavolilise modifitseerimise vastu ning sogastamine (*obfuscation*) pöördprojekteerimise vastu.

Tarkvara paigaldamine

Tarkvara paigaldamine (*installation*, *setup*) hõlmab endast tegevusi, mis on vajalikud selleks, et mingi programm oleks arvutisüsteemis käivitatav ja kasutatav – st kasutajale mingil viisil kasutoov.

Enamus programmidest müüakse ja levitatakse nö pakitud kujul –st, et programmi kasutamiseks tuleb eelnevalt (vastavaid vahendeid kasutades) lahti pakkida ning korrektsel (see sõltub platvormist) kujul arvutisse paigaldada. Tihti on kasutajal võimalik arvestada paigaldamise käigus ka enda nõudmiste, soovide ja harjumustega, et programmi vastavalt oma äranägemisele seadistada. Paigaldamise käigus sooritatakse mitmeid teste kontrollimaks süsteemi antud programmi jaoks sobivust ning arvuti seadistatakse vastavalt, et vajalikud failid ning seaded oleks sellised, et programm töötaks korrektselt.

Kuna need protsessid on erinevad iga programmi ja iga arvuti jaoks, on enamus programmidel (ka operatsioonisüsteemid) kaasas spetsiifiline paigaldaja (*dedicated installer*) – spetsiaalne programm, mis automatiseerib enamuse programmi seadistamiseks vajalikust tööst.

Mõningad programmid on aga sellised, mille paigaldamine seisneb üksnes vajalike failide tõstmises soovitud kohta ja eraldi paigaldamisprotsessi kui sellist polegi – see on nt tavaline MAC OS X programmide juures ning kasutatakse sageli ka Windowsi programmide korral. Leidub ka operatsioonisüsteeme, mis ei vaja installeerimist, vaid on jooksutatavad kohe eriotstarbelise CD, DVD või USB draivi kaudu ilma, et kuidagi mõjutataks olemasolevat operatsioonisüsteemi (nt Knoppix Linux). Paigaldamist vajavad ka erinevad pistikprogrammid (*plugins*) ja juhtprogrammid (*drivers*), mis ei ole ise otseselt programmid.

Tavalised operatsioonid, mis programmi paigaldamisel tehakse on järgmised:

- Tekitatakse jagatud (*shared*) ja jagamata (*non-shared*) programmifailid
- Tekitatakse kaustad (*folders/directories*)
- Tekitatakse registri kanded (ainult Windows'is)
- Konfigureeritakse programm ja süsteem
- Luuakse ja väärtustatakse keskkonnamuutujad
- Luuakse lingid ja otseteed

Tarkvara eemaldamine

Programmide eemaldaja (*uninstaller, deinstaller*) on programm, mis on loodud teiste programmide või rakenduste eemaldamiseks süsteemist. Enamus tarkvaraloojaid annavad nii nagu paigaldajagi tarnitava programmiga kaasa ka uninstalleri, kuid on olemas ka kolmanda osapoole (*third party*) unistallereid, mille töö on soovimatute programmide eemaldamine. Nendega on võimalik arvutist eemaldada palju erinevaid programme (erinevalt neist uninstalleritest, mis tulevad koos konkreetse programmiga ja on kitsalt ühe programmi ning sellega kaasneva eemaldamiseks loodud).

Ühest küljest kolmanda osapoole uninstallerite kasutamine tasapisi hääbub, kuna suurel osal kasutatavast tarkvarast on vastavad uninstallerid juba tootja poolt kaasas ning need teevad üldjuhul oma tööd paremini kui üldotstarbelised isendid. Samas, selleks, et kolmanda osapoole uninistallerid siiski välja ei sureks ja neid ostetaks, teevad nad tänapäeval tihtilugu rohkemat kui ainult programmi eemaldamine (nt vahemälu tühjendamine, ebavajalike failide leidmine ja eemaldamine jne).

Mõjukamad põhjused, miks kolmanda osapoole uninstallereid kasutada, on nt järgmised:

- Keerulised programmid teevad süsteemi muudatusi, mille olemasolust selle autorid pole teadlikud, ignoreerivad või on unustanud.
- Paljudel programmidel on küljes lisavidinad (*add-ons*), olgu see siis nuhkvara (*spyware*) või mitte, mis tulevad kaasa rohkem või vähem tahtmatult ja märkamatult ning mida ei eemaldata põhiprogrammi eemaldamise käigus.
- Praegusel ajal, kui reklaamvara, nuhkvara jms, tähendab meid igapäevaselt varitsevat ohtu, on paljude programmide paigaldamisega kaasnev risk suur. Juhul, kui tahtlikult või tahtmatult sai süsteemi paigaldatud soovimatu programm, on selle eemaldamisel uninstaller asendamatu abivahend.

Praktikum

1. Paigaldada valikuliselt üks kahest programmist – kas Adaware või Spybot. Need saab nt järgmistelt lehtedelt (kohti on kindlasti muidki):

   - Adaware - http://www.lavasoftusa.com/
   - Spybot - http://www.safer-networking.org/en/download/index.html

   - Paigaldamisel jälgi milliste seadetega seda teed ning kuhu kausta programm pannakse.
   - **Kui kahtled milleski, küsi!**
   - Käivita programm ning otsi oma arvutist kahjulikke ning ebavajalikke asju.
   - Kirjuta mõni skaneerimise käigus leitud pahalase nimetus üles – seda on vaja koduse töö jaoks.

2. Lae alla programm järgmiselt aadressilt:
   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

   - Milline link valida? Miks?
   - Paigalda antud programm. Mille poolest erines selle programmi paigaldamine Spyboti või Adaware paigaldamisest?
   - Kuidas sellest programmist lahti saada?
   - Kuidas võiks see programm olla kasulik Tartu Ülikooli üliõpilasele?

3. Eemaldame eelnevalt paigaldatud programmi – st siis kas Adaware või Spyboti.
   - Selleks vaatame ka Control Panel -> Add/Remove Programs ning otsime ta üles
   - Kuid eemaldame tarkvaratootja poolt pakutud uninstallerit – kust selle üles leiab?
   - Mis jäi süsteemi alles? Mida uninstaller ei eemaldanud?

Kodune töö

- Paigalda iseseisvalt teine praktikumi käigus välja pakutud programmidest (st, siis kas Spybot või Adaware).
- Skaneeri sellega oma arvuti. Kas see programm leidis midagi, mida praktikumi käigus paigaldatud programm ei leidnud?
- Ilmselt siiski leidis. Kirjuta lühidalt (kuni kümme lauset) leitud pahalasest (või praktikumi käigus leitud pahalasest) ning saada see aadressile Kersti.Taurus@ut.ee või võta paberil järgmisel korral kaasa.
- **Tähtaeg – 3.12.2007 (k.a)**