MTAT.07.006 Krüptograafia uurimisseminar
Jääkriski hindamine turvatud arenduskeskkonnas

Lauri Tulmin

2. mai 2007. a.

1 Sissejuhatus

Kuna tarkvaratootjad loovad järjest uusi rakendusi, muutub üha olulisemkas rakendustes oleva intellektuaalse omandi kaitsmine. Ettevõtted peavad tagama, et nende tarkvaras sisalduvad teadmised oleksid kaitstud piraatluse, varguse ja soovimatu muutmise eest, olenemata sellest, kes rakendust kasutab.

Käesoleva töö eesmärgiks on vaadelda riske tarkvara lähtekoodile (või mõnele muule ettevõtte jaoks olulisele infole) arenduskeskkonnas, mis on kaitstud väliste rünnete eest, ja kus töötajate juurdepääs lähtekoodi kriitilistele osadele on piiratud. Sellises keskkonnas on ainsaks riskiks ettevõtte oma töötajad, kes hoolimata neile seatud takistustest proovivad viia programmi algteksti majast välja. Töö 4. peatükkis uurime lähemalt võimalusi info kodeerimiseks arvuti ekraanile ja ekraanist tehtud foto alusel algse info taastamiseks.

2 Riskid intellektuaalsele omandile

2.1 Üldised riskid

Järgnevalt on loetletud mõned üldised tarkvara tootmise ja levitamisega seotud riskid, mis vähendavad tarkvaratootja tulu või põhjustavad lisakulutusi.

1. **Piraatlus.** Tarkvaratootja loob uue programmi. Mõne nädala pärast on sellele loodud võtmegeneraator või on programmi muudetud nii, et see töötab ilma litsentsita. Modifitseeritud programm või võtmegeneraator tehakse kättesaadavaks failivahetusvõrkudes. Ettevõte kaotab litsentside müügist saadava tulu.

2. **Tarkvara pahatahtlik muutmine.** Programmile lisatakse trooja hobune või mõni muu soovimatu omadus. Muudetud programmi levitatakse kui algset programmi. Trooja hobuse ilmsikstulek kahjustab

tarkvara tootja ja levitaja mainet. Soovimatu tarkvara eemaldamiseks tuleb teha lisakulutusi.

Näiteks CIH viirus [1], mis nakatas ligikaudu 600 000 arvutit ja põhjustas üle $250 miljoni dollari kahju jõudis mõningate pahaaimamatute kasutajateni koos legaalse tarkvaraga.

> "IBM ships a batch of new Aptiva PCs with the CIH virus pre-installed during March 1999, one month before the virus detonates its payload [2]."

> "As many as three European gaming magazines shipped demo CDs that were infected. One company went as far as including a note inside telling users to disinfect their machines after using the CD. A widely distributed version of Activision's game SiN was also infected. It should be noted that the infection did not originate at Activision [2]."

3. **Konkurents.** Konkurent pöördarendab programmi ja kasutab sealt saadud teadmisi oma tootes. Kuna tarkvara pöördarendamine on teatud tingimustel legaalne ollakse huvitatud selle võimalikult raskeks tegemisest.

4. **Koodileke.** Ettevõte kaotab eelise konkurentide ees. Ründajatel on lihtsam programmist turvaauke leida.

> "In 1997, the home of David Hawkins was raided, and the source code to Cisco Systems' PIX firewall was discovered on two of his machines. Hawkins, a former employee of TNI (Translation Networks Inc.), which built the original PIX and was later acquired by Cisco, was using the code as a base to launch his own firewall product. Charges were later filed against Hawkins, and in May a jury in Santa Clara, Calif.'s Superior Court convicted him [3]."

2.2 Oma töötajatega seotud riskid

Antiviiruse tootja McAfee poolt 2005 a. Euroopas läbi viidud uurimuses [4] jõutakse järeldusele, et töötajad ohustavad oma tööandjaid põhiliselt teadmatuse ja hoolimatusega.

Iga viies töötaja (21%) lubab on perekonnaliikmetel ja sõpradel kasutada tööandjalt saadud süle- ja lauaarvuteid interneti külastamiseks. Selline käitumine suurendab riski tööarvutile ja asutuse arvutivõrgule. Lisaks võivad tööalaseid dokumente vaadata inimesed, kes neid ei peaks nägema.

Rohkem kui pooled (51%) ühendavad oma tööarvuti külge isiklikke seadmeid (mälupulk, iPod jms.) ja veerand teeb seda iga päev. Ligikaudu 60%

tunnistas, et hoiavad tööarvutis isiklikke asju. Iga kümnes töötaja tunnistas, et nende tööarvutisse leidub programme või dokumente, mida seal ei tohiks olla. Natuke vähem kui iga viies hispaanlane (18%) tunnistas, et on oma arvutisse laadinud programme mis võivad suurendada turvariske või illegaalsel teel omandatud faile.

Kaks kolmandikku (62%) küsitletutest tunnistas, et nende IT turvalisusealased teadmised on piiratud. Üle poole (51%) küsitlusele vastanutest ei osanud uuendada antiviirustarkvara on tööarvutites.

Enamik töötajaid ohustas ettevõtet eelkõige oma teadmatuse ja hoolimatusega, ent leidus ka väike hulk töötajaid, kes ise otsisid viise oma tööandja huvide kahjustamiseks. Ligikaudu 5% küsitletud töötajatest tunnistas, et nad on vaadanud faile, millele neil ei tohiks juurdepääsu olla. Väga väike hulk töötajaid tunnistas, et on varastanud kompanii serverites olevat infot.

McAfee uurimuses eristateks nelja erinevat tüüpi töötajaid:

1. ***The Security Softie:*** sellesse rühma kuulub enamik töötajaid. Neil on vähesed teadmised andmeturbest. Ettevõttele põhjustavad nad turvaprobleeme viies tööarvuti koju ja lubades oma perekonnal ja tuttavatel tööarvutit kasutada internetis surfamiseks.

2. ***The Gadget Geek:*** omavad mitmesuguseid seadmeid, mida ühendavad tööarvuti külge.

3. ***The Squatter:*** need kes kasutavad ettevõtte IT ressursse ebasihipäraselt (st. mängivad mänge, tõmbavad filme).

4. ***The Saboteur:*** väga väike osa töötajatest. Sellesse gruppi kuuluvad töötajad proovivad juurde pääseda ettevõtte IT süsteemi osadele, kuhu nad ei tohiks pääseda või sihilikult nakatavad ettevõtte arvutisüsteeme.

2.3 Näiteid töötajate poolt tahtlikult põhjustatud kahjust

> "For Elite Web Hosting in Orlando, Fla., September, 2000, was a nightmare. A disgruntled former employee allegedly hacked into the company's computer system without authorization. He then allegedly sent e-mails that contained vulgar language and implying that Elite was moving into the Web porn business to every Elite customer. The missives further claimed that the company's majority owner, Augustino Mireles, had been raiding Elite's coffers for personal use. The impact on Elite was immediate. Thirty steady customers jumped ship, each taking $5,000 per month in revenue from Elite's cash flow [5]."

> "In 1998, a network administrator for Omega Engineering was accused of activating a digital time bomb that destroyed the company's most critical manufacturing software programs. The

> company claimed more than $10 million in damages and lost productivity [3]."
>
> "Earlier this year, an ex-employee of Intel Corp. pleaded guilty to charges of disrupting chip manufacturing: After Paul Barton was fired and his computer account was disabled, he dialed in remotely and deleted some files from one of the systems that controlled automated manufacturing [3]."

3 Turvatud arenduskeskkond

Turvalises arenduskeskkonnas on elimineeritud kõik väljastpoolt tulevad ohud. Arendajatel puudub internetiühendus ja arvutitele pole võimalik ühendada külge lisaseadmeid. Sisuliselt on kasutada ainult monitor, klaviatuur ja hiir. Programmi lähtekoodi hoitakse keskses repositooriumis, mida haldab usaldusväärne administraator.

Kuna turvalisuse tõstmiseks pole mõtet kulutada rohkem, kui kaitstav vara väärt on jääb alati võimalus koodi varguseks, kui ollakse valmis kulutama rohkem, kui vargusest saadav kasu. Arenduskeskkonna turvaliseks muutmiseks ei piisa range kontrolli kehtestamisest oma IT süsteemide ja töötajate üle, sama peavad tegema ka partnerid.

> "Early reports indicated, and Microsoft later agreed, that the real source of the leak was Mainsoft, a San Jose, Calif.-based maker of software to port Windows applications to other platforms, including Unix and Linux. A statement attributed to Mainsoft chairman Mike Gullard said, "Mainsoft has been a Microsoft partner since 1994, when we first entered a source code licensing agreement with Microsoft [6].""

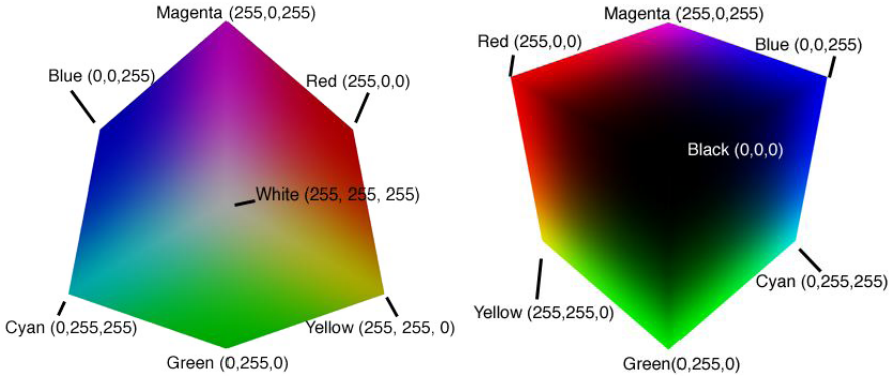
4 Info viimine turvatud arenduskeskkonnast digitaalkaamera abil

Oletame, et meie hüpoteetilises turvatud arenduskeskkonnas on arendajal võimalik teha pilti oma arvuti ekraanist. Kuna digitaalkaamerad on väikeste mõõtmetega ja võimaldavad teha palju hea kvaliteediga pilte, siis tekib küsimus, kui palju koodi on võimalik sellisel viisil viia väljapoole turvatud arenduskeskkonda.

4.1 *HSV* värviruum

Enamasti kasutatakse piltide digitaalsel kujul esitamiseks *RGB* värvimudelit [7]. Selles mudelis saadakse erinevad värvid kombineerides omavahel pu-

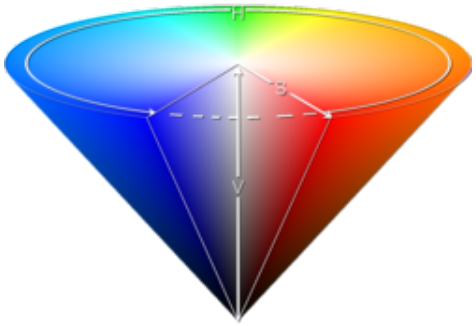
nast, rohelist ja sinist tooni. *RGB* värvimudelt võib kujtada ette kuubikuna (joonis 1).



Joonis 1: *RGB* värviruum

Analoogiliselt *RGB*'ga saadakse ka *HSV* värviruumis [8] erinevad toonid kolme komponendi omavahelisel kombineerimisel. *HSV* värviruumi võib ette kujutada kui koonust (joonis 2).

1. **Toon(*hue*).** Määrab ära värvuse(sinine, punane jne.). Kui koonuse põhi esitada polaarkoordinaatides, siis tooni määrab nurk.
2. **Kirkus/tooni puhtus(*saturation*).** Määrab värvi erksuse. Vähese kirkusega värvid tunduvad hallina olenemate toonist.
3. **Heledus(*value/brightness*).** Värvi heledus.



Joonis 2: *HSV* värviruum

4.2 Värvide vaheline kaugus *HSV* värviruumis

Värvide vahelise kauguse arvutamiseks võib värve vaadelda kui punkte *HSV* värviruumis. Olgu antud värvid $c = (h, s, v)$ ja $c' = (h', s', v')$, siis nende

vaheline kaugus on $d = |c - c'|$ [9]. Kui $0 \leq h \leq 1$, $0 \leq h' \leq 1$, $0 \leq s \leq 1$, $0 \leq s' \leq 1$, $0 \leq v \leq 1$ ja $0 \leq v' \leq 1$ siis saab eelmise valemi esitada kujul:

$$d = \sqrt{(v - v')^2 + (s \times cos(2\pi h) - s' \times cos(2\pi h'))^2 + (s \times sin(2\pi h) - s' \times sin(2\pi h'))^2}$$

4.3 Andmete kodeerimine pildile

Kodeeritav info esitatakse pildil mustal taustal värviliste ruutudena. Sisendandmed kodeeritakse pildile blokikaupda nagu kirjeldatud algoritmis 1. Kodeerija juures on oluline lihtsus, kuna arendajal pole turvatud keskkonda võimalik oma programme viia ja kodeerija tuleb kohapeal valmis kirjutada.

Sisend : Andmed S, bloki suurus bs(korraga kodeeritavate baitide arv) ja värvide arv n
Väljund: Pilt kodeeritud andmetega

leia väljundploki pikkus
$vs = \lceil bs \times log_n(256) \rceil$
while S *on veel andmeid* **do**
  $(b, s) \longleftarrow$ loe sisendist S n baiti
  kui sisendis oli vähem kui bs baiti siis arvuta väljundi suurus uuesti
  if $bs \neq s$ **then**
    $vs = \lceil s \times log_n(256) \rceil$
  end
  $d_0 d_1 d_2 ... d_{vs} \longleftarrow$ esita arv b positsioonilises arvusüsteemis alusel n
  for $v \longleftarrow d_0 ... d_{vs}$ **do**
    joonista pildile ruut värviga v
    $JoonistaRuut(v)$
  end
end

Algoritm 1: Pildile andmete kodeerimine

Kodeeritud pildid jäädvustatakse digitaalkaameraga ja dekodeeritakse hiljem algoritmi 2 järgi. Algoritm töötleb pilte mingil viisil proovides eemaldada pildistamisel tekkinud "müra". Foto töötlemine võiks koosneda järgmistest sammudest:

1. eemalda pildilt liiga tumedad toonid,
2. taasta pildistamise käigus muutunud värvid, et kodeeritud ruudud oleks selgelt eristatavad ja sama värvi nagu algselt,
3. dekodeeri pilt ruuthaaval.

Sisend : Pilt P, kodeerija bloki suurus bs ja värvide arv n
Väljund: Pildilt dekodeeritud andmed

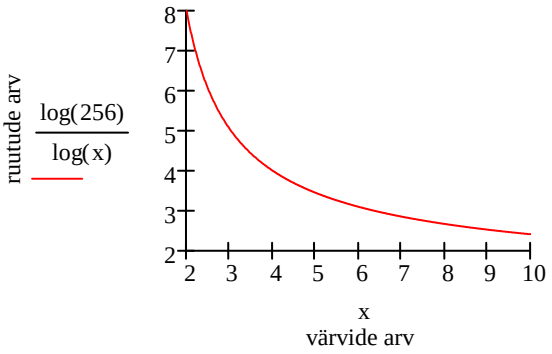
töötle pilti mingil viisil, et eemaldada pildistamisega tekkinud "müra";
$TöötlePilti(P)$

leia väljundploki pikkus
$vs = \lceil bs \times log_n(256) \rceil$
while P *on veel lugemata ruute* **do**
  $(b, s) \longleftarrow$ loe pildilt P vs ruutu
  kui loeti vähem kui vs ruutu siis arvuta bloki suurus uuesti
  if $vs \neq s$ **then**
    $bs = \lfloor s \times log_{256}(n) \rfloor$
  end
  $d_0 d_1 d_2 ... d_{bs} \longleftarrow$ esita arv b positsioonilises arvusüsteemis alusel 256
  for $v \longleftarrow d_0 ... d_{bs}$ **do**
    väljasta bait v
    $VäljastaBait(v)$
  end
end

Algoritm 2: Pildilt andmete dekodeerimine

4.4 Pildi mahutavus

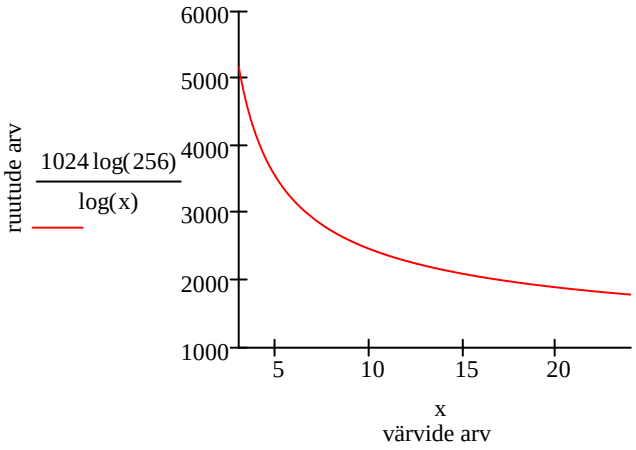
Pildile mahtuvate baitide arv sõltub kahest parameetrist - värvide arv ja ruutude arv. Joonisel 3 on näidatud kuidas sõltub ühe baidi kodeerimiseks vajalik ruutude arv kasutatavate värvide arvust.



Joonis 3: Ruutude arv ühe baidi kodeeerimiseks

Kuna ühe baidi kaupa kodeerimisel võib olenevalt valitud värvide arvust suur osa võimalikke ruutude kombinatsioone kasutuseta jääda, siis on efektiivsem kodeerida suuremate blokkide kaupa. Joonisel 4 on kujutatud ühe kilobaidise bloki kodeerimiseks vajalike ruutude arvu pildil sõltuvalt valitud

värvide arvust.



Joonis 4: Ruutude arv ühe kilobaidi kodeeerimiseks

5 Kokkuvõte

Pildile kodeeritava info hulk sõltub kasutatavate värvide arvust ja pildil olevate ruutude kogusest. Kuna digitaalkaamera moonutab värve olenevalt valgustingimustest, kaamera seadetest, kaamera kvaliteedist jms. võivad fotol olevad värvid olla algse pildi värvidest üpriski erinevad. Mõistliku digitaalkaameraga on enamasti kindlat tuvastatavad joonisel 1 kujutad kuubi tippudes olevad värvid. Sama tooni erinevad varjundid aga ei pruugi enam alati eristatavad olla. Näiteks ekraanil helesinisena paistev ruut võib fotol olla tumesinine. Samuti võivad ekraanil sama värvi olevad ruudud olla fotol erinevad sõltuvalt sellest, kas ruut asub pildi keskel või servas. Ka pildilt tuvastatavate ruutude arv sõltub eelkõige kaamerast. Kui ruudud on liiga tihedalt ja pildistamise hetkel kaamera liigub natuke võivad pildil kaks ruutu paista ühena. Eelnevalt toodud puudused piiravad oluliselt pildile mahtuva info hulka. Kui 1000×1000 pikslit pildile kodeerida info kasutades 7 värvi 25×25 piksli suuruste ruutudena ja iga ruudu vahele jätta 25 pikslit, siis mahub pildile 1600 ruutu, mis on võrdne 561 baidiga.

Viited

[1] Wikipedia. Cih virus, `http://en.wikipedia.org/wiki/CIH_virus`. (viimati külastatud: 1. aprill 2007. a.).

[2] Victor Latona. Cih: One year later, `http://news.zdnet.com/2100-9595_22-502294.html`. (viimati külastatud: 1. aprill 2007. a.).

[3] Greg Shipley. How secure is your network?, http://www.networkcomputing.com/1123/1123f1.html. (viimati külastatud: 1. aprill 2007. a.).

[4] The Register. The enemy within, http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/. (viimati külastatud: 1. aprill 2007. a.).

[5] BusinessWeek. When the hacker is on the inside, http://www.businessweek.com/bwdaily/dnflash/dec2000/nf20001213_253.htm. (viimati külastatud: 1. aprill 2007. a.).

[6] John Hogan. Anatomy of an intellectual property theft, http://searchwinit.techtarget.com/columnItem/0,294698,sid1_gci951584,00.html. (viimati külastatud: 1. aprill 2007. a.).

[7] Wikipedia. Rgb color model, http://en.wikipedia.org/wiki/RGB_color_model. (viimati külastatud: 2. aprill 2007. a.).

[8] Wikipedia. Hsv color space, http://en.wikipedia.org/wiki/HSV_color_space. (viimati külastatud: 2. aprill 2007. a.).

[9] R. B. Fisher. Change detection in color images.