Tallinna Ülikool

Informaatika Instituut

Nutitelefonide turvalisus. Õppevahend

bakalaureusetöö

Autor: Mari Randmäe

Juhendaja: Erika Matsak

Autor: ..... „ ..... „2011

Juhendaja: ..... „ ..... „2011

Instituudi direktor: ..... „ ..... „2011

Tallinn 2011

Autori deklaratsioon

Deklareerin, et käesolev bakalaureusetöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikad ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) (autor)

Sisukord

Sissejuhatus

Mobiiltelefonid on tänapäeval muutunud väga populaarseks. Mõnikümmend aastat tagasi omasid neid vaid jõukamad ning tähtsamad inimesed, praeguseks võib leida telefoni omanike seast ka lasteaia lapsi. Lisaks tavapärasele helistamise ja sõnumisaatmise võimalusele pakuvad tänapäeva-telefonid võimalust nii kasutada Internetti kui ka palju muud. On nii-öelda nutitelefonide ajastu. Aga lisaks interneti kiirele arengule arenevad kiiresti ka seal levivad viirused ning juba on nad jõudnud ka nutitelefonide maailma. Peale viiruste on veel palju erinevaid turvalisuse aspekte, mida autor antud töös käsitleb.

Töö eesmärgiks on anda tavakasutajatele ülevaade, mis ohud kaasnevad nutitelefonide kasutamisega ning kuidas muuta kasutamine turvalisemaks. Eesmärgi saavutamiseks luges autor erinevaid artikleid, blogisid, Internetilehekülgi ning proovis omal käel nutitelefoni kasutamist ning sinna turvaliste rakenduste installeerimist ja kasutamist. Samuti on valmis videode puhul tehtud ka testimine.

Antud töö koosneb kolmest osast: Esimene neist annab ülevaate Eestis tuntud nutitelefonides levivatest operatsioonisüsteemidest (edaspidi OS), nende võimalustest ning rakendustest, lisaks on lühiülevaade ka Eestis vähemlevinud OS-dest.. Teine peatükk on turvalisusest ehk on kirjeldatud mobiilset turvalisust ning antud nõuandeid, kuidas muuta telefoni kasutamist turvalisemaks. Kolmas peatükk kirjeldab õpiobjekte, nende olemust, loomise põhimõtteid ning metaandmeid. Antud töö lisana on mõned videod veel nutitelefoni turvaliseks kasutamiseks. Need videod on loodud, kasutades Nuendo 4 võimalusi ning kokku pandud, kasutades SMIL programmeeriskeelt. Autor on filmimiseks kasutatud iPod Touchi (kuna antud seadmel toimivad ka iPhone erinevad rakendused), Android süsteemiga telefoni ning Symbian süsteemiga telefoni.

Siinkohal sooviks autor tänada Tallinna Ülikooli, Haridus ja Tehnoloogia keskust ning Tele2, kes laenutasid videote koostamiseks vajalikke vahendeid, kursusekaalasi ning loomulikult juhendajat Erika Matsakut, kes olid töö kirjutamise algusest peale toeks nii oma nõu kui ka jõuga.

1. Ülevaade nutitelefonide tarkvaradest

Teada on, et maailmas on palju erinevaid nutitelefonide platvorme, millest mõned on populaarsed ühes kohas, teised teises. Näiteks praegu USA-s väga populaarne BlackBird pole Eestis üldse levinud. Antud peatükis ongi esitatud ülevaade Eestis enamlevinud nutitelefonide platvormidest nagu Android, Symbian, iOS, Windows Phone ning Bada, nende võimalustest ning rakendustest.

1.1 Android

Android on platvorm telefonidele (samas ka tahvelarvutitele), mis hõlmab operatsioonisüsteemi, tarkvara ja rakendusi. Android SDK (ing k. *Software Development Kit*) võimaldab kasutada vajalikke vahendeid ja APIsid (ing k. *Application programming interface*), et alustada rakenduste programmeerimist Android tarkvaral kasutades Java programmeerimiskeelt. Android tugineb Linuxi 2.6 versioonile põhiteenustele nagu turvalisus, mälu ja protsesside haldus, võrkude rida ja draiverite mudelid. Kernel tegutseb ka abstraktse kihina riistvara ja muu tarkvara vahel [Android Developers, 2011]

1.1.1 Androidi võimalused

Androidil on väga palju erinevaid võimalusi, nagu näiteks riistvarast sõltuvad Bluetooth, EDGE (ing k. *Enchanged Data rates for GSM Evolution)*, 3G ja wifi. Allpool on toodud autori arvates veel mõned märkimisväärsed näited.

*** Dalvik virtuaalmasin, mis on tehtud just mobiilsetele seadetele.** Iga Androidi rakendus *käib* oma protsessis koos Dalviku virtuaalmasina näitega. Viimane on kirjutatud nii, et seade saab korraga töös olla mitu virtuaalmasinat väga efektiivselt. Dalviku VM tugineb Linuxi kernelile selliste funktsioonidega nagu *threading* ja madala-tasemeline mälu organiseerimine

*** Integreeritud veebibrauser,** mis põhineb vabavaralisel WebKiti masinal

*** SQLite -** võimas andmebaas struktureeritud andmete hoidmiseks, mis on kättesaadav kõigile rakendustele

*** Rikkalik arengu keskkond**, mis hõlmab seadme emulaatorit, vahendeid silumiseks, mälu ja jõudluse profilifeerimist ja Eclipse IDE pistikut [Android Developers, 2011]

1.1.2 Rakendused

Androidi kõik rakendused, sealhulgas kalender, erinevad kaardid, on kirjutades kasutades Java programmeerimiskeelt. Kuna Android võimaldab vabalt kasutatavat platvormi, pakub ta arendajatele võimalust ehitada väga rikkalike ja innovatiivseid rakendusi. Neil on vabadus

võtta kasu seadme riistvarast, saada ligipääs asukoha informatsioonile, lisada märkmeid staatuse ribale ja palju muud.

Rakenduste arhitektuur on disainitud lihtsalt ning taaskasutama erinevaid komponente; ükskõik milline rakendus võimaldab avalikustada selle võimalusi ja iga muu rakendus võib võtta kasu nendest avalikest rakendustest (seda tingimusel, et turvalisus oleks tagatud). Sama mehhanism võimaldab kasutajatel asendada erinevaid komponente. Sellised rakendused on näiteks Kontaktid ja Teadete haldur.[Android Developers, 2011].

1.2 Symbian

Symbiani operatsioonisüsteem on Symbian Ltd poolt loodud vaba operatsioonisüsteem, mida praegu kasutavad enamasti Nokia telefonid. See on loodud spetsiaalselt 2G, 2.5G ja 3G mobiiltelefonidele. [Nokia foorum, 2011]

Symbian on üles ehitatud C++ keeles ning tänu selle lubab ta kasutajatel saavutada kõrgetasemelist integratsiooni Symbiani funktsioonidega (nagu näiteks multimeedia ja 3D-ga töötamine, interneti ligipääsu saamine, kohaliku info juurde pääsemine)

1.2.1 Tunnused ja võimalused

Symbian peab oma põhilisteks tunnusteks järgmisi võimalusi:

Jõudlus. Symbian on disainitud just võtma vähest akust ning kasutama väikest mälumahtu

Multitasking – Kõik telefoni rakendused on loodud nii, et nad saaksid töötada paralleelselt teiste rakendustega

Standardid. Tehnoloogiate kasutamine põhineb kaasaegsetel standartidel, mis on Symbian OS alustaladeks ja mis lubavad rakendustel olla jõulised ja kaasaskantavad.

Objekt-orienteeritud tarkvara arhitektuur.

Mälu korraldus on optimeeritud kinnistatud tarkvara keskkonnale

Jooksvad mälumahu nõuded on minimaliseeritud ehk väga väike osa ROM-põhisest mälust käivitub korraga

Rakendustel on **rahvusvahelise keskkonna tugi** koos sisseehitatud Unicode karakteritega

Rikkalikud ja erinevad APId pakuvad ligipääsu ka taaskasutatavatele komponentidele arendajate rakendustes.

Turvamehhanism lubab turvalisi ühendusi ja turvalist andmete hoidmist. [Nokia foorum, 2011]

1.2.2 Rakendused.

Rakendused on kõrgetasemelised, sest Symbian C++ on spetsiaalselt disainitud mobiilsetele

seadmetele, millel on väike võimsuse tarbimine ja väike mälumaht. See keel võimaldab täita kasutajate ootusi erinevate rakenduste suhtes. Ovi rakendus on kanal, milla kaudu saab levitada oma rakendusi ja leida sobivaid rakendusi oma telefonile. [Nokia foorum, 2011]

1.3 Windows Mobile

Nagu nimestki aru saada on selle mobiilse operatsiooni süsteemi looja Windows. Kasutatakse võimsaid ja tuntud arendusvahendeid Microsoftilt, nii et arendajad saavad luua Windows Phone'le rakendusi kiirelt ja efektiivselt. [Microsoft, 2011]

1.3.1 Võimalused

Uusim operatsioonisüsteem Windows Phone 7 toob kokku informatsiooni, rakendused, tööriistad ja teenused, mis on vajalikud töö tegemiseks kiiresti ja lihtsalt. Võimalus on kasutada MS Office Mobiil ja MS SharePoint Serverit, samuti pakub MS outlook mobile võimalust lugeda oma emaile ja vaadata kalendrit otse telefonist väga kiiresti ja efektiivselt. Intuitiivse kasutajaliidesega saavad inimesed vaid erinevate sõrmeliigutustega (nagu näiteks koputamine) navigeerida oma telefonis.

Ka windows phone võimaldab telefoni varastamise või kadumise puhul telefon lukustada. Võimalik on veel hallara IT *policies*, mis sisaldavad süsteemi PIN koodi küsimisi, ja *Microsoft Exchange ActiveSync* tehnoloogia kasutamist.[Microsoft, 2011]

1.3.2 Rakendused

Windows Phone rakendused on loodud kasutades spetsiaalset keskkonda, kuhu kuuluvad Visual Studio 2010 Express for Windows Phone,Windows Phone Emulator, Silverlight for Windows Phone, XNA Game Studio ja Expression Blend 4 for Windows Phone.

Visual Studio lihtne ja võimas arendaja keskkonnas on olemas kõik alates disainist kuni testimiseni ja se ühildub hästi Expression Blendiga, mis aitab luua rakendusi antud operatsioonisüsteemile. Kõiki rakendusi saab enne telefonile panemist proovida ka Windows Phone Emulaatori peal. [Microsoft, 2010]

1.4 Apple iOS

Apple iOS on tuntud ka kui lihtsalt iPhone OS. iOS SDK on kombineeritud Xcode tööriistadega, mis teeb lihtsaks rakenduste loomise. Operatsioonisüsteemi põhitõed on võetud Mac OS X-lt ning on tehtud kompaktseks ja efektiivseks, et võtta maksimum iPad ja iPhone riistvarast. Tehnoloogiad on jagatud iOS ja Mac OS X vahel ning sisaldavad OS X kernelit, BSD pistikuid ja võrgustikke ja C/C++ *compilers for native performance* [Apple

tehnoloogiad, 2010]

Telefon on tehtud väga turvaliseks, nii et veebileht või rakendust ei saa teistelt rakendustelt infot. iOS 4 toetab krüpteeritud võrgustiku suhtlust, et kaitsta tundlikku infot. Valikuline vanemlik kontroll võimaldab kontrollida iTunesi tehinguid, Internetis surfamist ja ligipääsu detailsetele materjalidele. Et kontrollida privaatsust, rakendused on programmeeritud küsima kõigepealt kasutaja luba. Kui iPhone on varastatud või kadunud, võimaldab ta näha oma asukohta kaardil, lukustada ekraan ja kustutada kõik info. Kui telefon on kättesaadud saab kõik andmed taastada eelmisest *backup*ist.[Apple, 2011]

1.4.1 Võimalused

*** *FaceTime*** ehk videokõne võimalus. iPhone'l on kaks kaamerat üks telefoni ees ja teine taga. Kõne pidamise ajal saab edukalt vahetada ka seda, millise kaamera pilti näeb helistatav.

*** HD video lindistamine ning muutmine**.

*** 5 megapiksline kaamera koos LED välguga**. Pilte on võimalik teha ka hämaramas ruumis, kuna iPhonel on kaks kaamerat on ka endast lihtne pilte teha

* **Multitouch** liides, mis on disainitud just inimese sõrme jaoks ja võimaldab kontrollida kõike erinevate näpuliigutustega, nagu näiteks koputamine või lohistamine. Nii on võimalik tegelede erinevate rakendustega ning kiirelt liikuda nende vahel

***Retina ekraan**, mis väidetavalt on teravaim, kõrgeima resolutsiooniga telefoniekraan ning ka pikslite arv on 4 korda suurem kui eelmistel iPhonidel. Pikslid on nii tihedalt, et inimese silmal on ka raske neil vahet teha. Selline seade muudab teksti väga kargeks ning pildid teravaks. [Apple, 2011]

1.4.2 Rakendused

iOS pakub rohkem kui 350000 rakendust praktiliselt igas kategoorias, iOS 4 on maailma suurim mobiilsete rakenduste platvorm. Apple pakub arendajatele rikkaliku seadmete komplekti ja APIsid. Nad on loonud rakendusi ja mänge, mis näitavad, mida üks telefon teha saab. [Apple, 2011]

1.5 Bada

Bada (korea keeles „ookean" ja „rannik") on uus, 2010 aastal välja tulnud, Samsungi nutitelefonide platvorm, mis püüab näidata niiöelda avatud ookeani võimalusi: Arendajale on ta kui uus mobiilsete rakenduste sinine ookean ning kasutajatele lai valik nutitelefone hea hinnaga. [Samsung, 2011]

Bada visooniks on „nutitelefon kõigile“. Põhiliseks eesmärgiks ei ole võistelda teiste nutitelefonidega, vaid muuta Samsungi kasutajad hea hinnaga nutitelefonide kasutajaks. See tähendab, et Bada avab uue nutitelefonide turu, mis muutub uueks „siniseks ookeaniks“ [Samsung, 2011]

1.5.1 Võimalused

Samsung Bada sisaldab uue generatsiooni Samsungi puutetundliku UI-d (*User Interface).* See annab lihtsuse kasutuse tõhusust vähendamata, UI raamistik tutvustab vabalt lõppevat evolutsioonilist innovatsiooni praegusest puutetundlikust UIst kuni paremate kasutaja kogemusteni kinnitatud Adobe Flash mängijani. Lisaks on olemas ka kaardikontroll, mis sisaldab interaktiivset kaarti koos marsuutimise ja POI võimalustega. [Samsung, 2011]

1.5.2 Rakendused

Samsungi rakendused lubavad rakendusi kergelt alla laadida, rakendusi on palju erinevaid, sisaldades uudiseid, mänge, sotsiaalvõrgustikke jne. Samsung ütleb ka, et nende rakendused teevad nutitelefoni targemaks. Ka rakenduste brauser on kergesti kasutatav. Kui installeerida arvutisse Samsung Kies on võimalik rakendusi otsida ka läbi PC. [Samsungi rakendused, 2011]

Bada rakendused on kirjutatud kasutades C/C++ keelt. [Bada arendajad, 2011]

2. Turvalisus

Antud peatükis on antud ülevaade 2011 aasta häkkimisevõistluse Pwn2Own, mis seekord kaasas võistlusesse ka nutitelefonid, tulemustest. Samuti on esitatud ülevaade viirusetõrje programmide vajalikkusest ning toodud mõned programminäited. Antud peatüki viimane alampeatükk aga annab soovitusi, kuidas oleks nutitelefonide kasutamine turvalisem.

2.1 Häkkimise võistlus Pwn2Own

Nutitelefonid võivad tunduda päris turvalised, kuid ometi valitseb neis mitmeid erinevaid turvaohte. Turvaaukude leidmiseks nii arvutitel kui ka telefonidel korraldatakse erinevaid häkkimise võistlusi. Juba viiendat aastat toimus käesoleval aastal võistlus Pwn2Own, kus seekord lisaks arvutitele olid proovile pandud ka nutitelefonid, kuid mitte kõik, vaid kasutatud oli Dell Venue Prod(Windows Phone 7), Apple iPhone 4 (iOS), BlackBerry Torch 9800 (Blackberry 6) ja Nexus S (Android).

Kuna Safari, Chrome, iPhone, Android ja Blackberry kasutavad kõik oma brauserites WebKiti (mis tähendab, et nad on vastuvõtlikud brauseri ärakasutamisele), siis sealt kaudu rünnatigi iPhone ja Blackberryt. Võistlejatel võttis aega kaks päeva, et kräkkida sisse iOS-i ja Blakberry operatsioonisüsteemidesse. Samal ajal Androidi ja Windows Phone 7 versioonidesse ei suudetud terve konkursi ajal (3 päeva) sisse kräkkida. [Bonnington, 2011]

2.2 Viirusetõrjed mobiilidele

Lisaks arvutiviirustele on tänapäeval levima hakanud ka viirused nutitelefonidele ning seetõttu on viirusetõrjetootjad hakanud valmistama ka vahendeid telefoni kaitseks. Telefoni kaitsmiseks on olemas mitu põhjust, näiteks see, et telefon on esmane suhtlusvahend ning ta sisaldab tavaliselt palju isiklikku ja konfidentsiaalset informatsiooni. Mobiilseid turvariske on päris palju: Telefoni kadumisel võidakse seal leiduvat informatsiooni kurjasti ära kasutada, mobiilne nuhkvara võimaldab salvestada kõnesid (ja ka sõnumeid) ja need kurjategijatele edastada, levivad viirused võivad põhjustada suuri mobiiliarveid ning pahavara võib rikkuda kogu telefoni. Mobiilste viirusetõrjete eelkäijaks nimetatud F-Secure Mobile pakub nii vargavastast kaitset (võimaldab telefoni kadumise või varastamise puhul telefoni lukustada ja sealt kõik andmed kustutada ning tagasisaamisel parooli abiga kõik failid taastada), nuhkvaratõrjet, antiviirust, tulemüüri kui ka automaatseid uuendusi. Antud rakendust on võimalik ka tasuta 7 päeva jooksul proovida. [F-Secure korporatsioon, 2009]

Lisaks F-Securele pakub mobiilset kaitset ka Eset, kellelt tuntud nod32 on sülearvutites päris

populaarne. Eseti mobiilne viirusetõrje pakub reaalajas kaitset igasuguste ohtude vastu ilma seadme tööjõudlust mõjutamata, kuna sisaldab endas nii rämpspostifiltrit, tulemüüri lahendusi kui ka heuristika mootorit. Samas on rakendusel pakkuda ka vargusevastane süsteem, mis toimib sarnaselt F-Secure rakendusele. Eseti peamiste võimalustena on välja toodud telefonis olevate failide skänneerimine, tulemüür, mis jälgib vastavalt paika pandud reeglitele sissetulevat ja väljaminevat kommunikatsiooni, SMS/MMS rämpspostifilter, mis võimaldab tundmatud numbrid ära blokeerida ning tõhusam turvasüsteem, mille kaudu saav kustutada olulisi andmeid ning vältida lubata juurdepääsu telefonile. Eset on tõhustanud ka turvalisuse funktsiooni kaug-kustutamise, sim-kaardi tuvastamise, karantiini ja turvalisuse auditi näol. Neist esimene funktsioon kujutab endast andmete kustutamist telefonist vaid ühe Smsi teel. Sarnase sõnumiga saab kustutada ka andmed seadmesse sisestatud mälukaardilt. Sim kaardi tuvastamine võimaldab koostada nimekiri sim-kaartidest, mida võib antud seadmesse sisestada ning kui sisetada vale telefonikaart, siis saadetakse automaatselt teade telefoni numbri ja IMSI-ga. Karantiin pakub võimalust valida, kas ohud eemaldada kohe, need isoleerida või taastada objektid, mille kasutaja osutub ohutuks.Turvalisuse audit käivitab nõudmisel põhjaliku telefoni kontrolli kõigile olulistele funktsioonidele (sh ka aku tase, seadme nähtavus, bluetooth ühendus jne). Antud rakendust on võimalik proovida tasuta 30päeva jooksul. [Eset]

2.3 Olulisemad turvalisuse soovitused

Järgnevad soovitused on kogutud Jon Heimerli blogist „Top 10 soovitust nutitelefonide turvamiseks“ ning Androidi blogist, Andre Kameka poolt kirjutatud artiklist „ Kaitse faile oma Androidis“

Kaitse telefoni ennast! Kuna nutitelefon sisaldab palju isiklikku informatsiooni alates piltidest ja muusikast kuni e-posti paroolideni, siis on tark tegu kaitsta teda ennast. Esmane viis selleks on hoida teda kindlas kohas, näiteks oma taskus, mitte laua peal või mõnel muul kõigile nähtavas kohas (Vaata pilt 1).

Pilt 1. Telefoni hoidmiseks ebasobiv koht. [Boxall, 2009]

Lisaks telefoni kindlas kohas hoidmisele tasuks määrata ka avamiseks pin-kood või androidi puhul avamise muster (vaata video 1 ja video 2). Mõni kannatlik inimene võib küll selle lahti murda, kuid lihtinimene oma pead tavaliselt nii palju ei vaeva. Ainuke miinus on see, et kui telefon ära kaotada ning mõni aus inimene selle leiab, siis ei pääse ta ligi viimati helistatud kontaktidele, et telefoni leidmisest teatada.

Peida failid Astroga! Kui telefonis on pilte, mida ei soovita teistele näidata, siis on Androidil selleks sobiv võimalus – Androidi Piltide rakendus ei näita pilte, mis on salvestatud kaustadesse, mis algavad punktiga. Nii saab neid näha ainult Astro või teise taolise failihalduriga.

Tee varukoopia(*Backup)* oma andmetest! See on vajalik selleks, et kui telefon ära kaob jääb vähemalt kogu vajalik ja oluline info alles. *Back-up* tegemiseks on palju erinevaid tarkvarasid, iPhoned saavad näiteks kasutada iTunesi, Androidid MyBackup, Badad Kiesi, Windows Phone Zune, Symbianid Rsevenit.

Nagu kasutades sülearvutit, tuleks ka nutitelefonidega **olla ettevaatlik wi-fi kasutamisel!** Eriti on see oluline kui kasutada avalikku turvamata wi-fi võrku (mis on tavaliselt lennujaamades, kohvikutes või muudes avalikes kohtades), sest on võimalik, et keegi jälgib seda, mida parajasti tehakse. Ei ole soovitatav teha pangatehinguid, osta läbi interneti või teha midagi muud väga isiklikku. Siit ka järgmine soovitus, **surfa targalt!** Pangatehingute tegemiseks on kõige turvalisem kasutada oma panga rakendust, kui neil ei ole seda, tuleb alati jälgida, et ollakse https leheküljel. Internetis surfates peaks aegajalt ka **vahemälu tühjendama!** Andoridil saab valida, et ta ei jätaks meelde erinevaid vorme ja salasõnu. IPhone puhul tuleks aegajalt kustutada vahemälu, ajalugu ja küpsised (ing k. *Cookies*). Samuti, kui kasutada panga või ostu rakendusi, tuleks vaadata nende seadetest, et salasõnu ei jäetaks meelde ning tuleks ka vahemälu kustutada.

Kasuta failide kaitseks BioWalletit! Mobeeli poolt loodud Biowallet kasutab biomeetrilist karakteristikat (silma, hääle, allkirja tuvastus), et kaitsta dokumente, kaustu, säilitada paroole ja nii edasi. Silmatuvastuse tehnoloogia kasutab mobiili kaamerat, et tunda ära kasutaja silmaiiris. Väidetavalt on silmatuvastus üks usaldusväärsemaid biomeetrilisi meetodeid, nimelt on virtuaalselt võimatu leida kahte täpselt ühesugust silmaiirist. Allkirja tuvastus laseb kasutajal ekraanile kirjutada oma allkirja ning selle järgi lubatakse tal faile vaadata. [Mobbeel, 2011] Koduleheküljel on kirjas, et antud tarkvara toetavad kõik eespool mainitud operatsioonisüsteemid, kuid kahjuks õnnestus autoril see tööle saada vaid Android süsteemiga (Vaata video 3**)**

Leia oma kadunud telefon! Telefoni asukoha määramiseks on erinevatel süsteemidel erinevad rakendused, nii näiteks on Apple'l MobileMe, Androidil „Where's My Android“, Symbianil Mtracker ning Windows Phone „Find my Phone“. Nende tarkvaradega saan telefoni jälgida ning kui see on kadunud või varastatud on lihtne asukoht üles leida, sellekson vaja vaid arvutit koos internetiga. Lisaks on võimalik nendega ka tööle panna telefoni kõlarid ning selle järgi otsida.

Enne rakenduste allalaadimist mõtle, mida alla laed! Kindlasti tuleks ka uurida, millist infot rakendus kasutamiseks vajab. Näiteks omades Android telefoni ning allalaadides Androidi laheda *screensaver*i, avastatakse, et ta tahab ligipääsu ka telefoni seadetele, süsteemi ning asukoha infole. Tuleb välja, et tegemist pole ainult ekraanisäästjana. Turvafirmade tehtud testid näitavad, et 30% iTunesi ja Androidi rakendusi koguvad infot ka kasutaja kohta ning teevad selle avalikuks mõnel soovimatul lehel, näiteks reklaamitootjatele. Rakenduste allalaadides on soovitatav vaadata ka arendaja reputatsiooni, mitte allalaadida suvalisi asju

Kontrolli oma telefoniarvet! Kui on alla laetud ja installeeritud mõni rakendus, siis tasuks alati kuu lõpus ka oma telefoniarvet kontrollida. Võib juhtuda, kui laetakse alla tasuta rakendus, millel on väikselt lisatud, et peab kuus maksma mingi summa selle uuendamise või litsensti eest. Mida varem see avastada, seda varem saab ka selle lõpetada :)

Ära viska oma nutitelefoni ära. Aja jooksul on nutitelefoni kogunenud palju tähtsaid andmeid ning informatsiooni nagu näiteks sirvimise ajalugu, vahemälus salvestatud paroolid, sinu aadressiraamat jne. Enne oma nutitelefonide ära viskamist (ära andmist) tasuks telefon isiklikest failidest puhtaks teha. Märkimisväärne number telefoni ümbertöödeldakse iga aasta ning suur protsent neist sisaldab informatsiooni eelmise omaniku kohta. Kindlasti tasub eemaldada telefonist ka kõik mälukaardid

3. Õpiobjektid

Kuna antud töö eesmärk on luua ka õpiobjekte, siis järgnevas peatükis on lühidalt kirjeldatud õpiobjektide olemust, metaandmeid ning loodud õpiobjekte. Samuti on kirjeldatud ka testimise tulemusi.

3.1 Õpiobjekti olemus

Õpiobjekt tuleneb inglise keelsetest sõnadest *Learning Object* tähendades uut tüüpi arvutil põhinevaid instruktsioone, mis põhinevad omakorda objekt-orienteeritud paradigmal. Objekt-orientatsioon paneb suurt rõhku komponentide ehk objektide loomisele, mida saab uuesti kasutada paljudes kontekstides. Õpiobjektid on üldiselt arusaama järgi digitaalsed, võimaldades neid mööda internetti laiali saata paljudele erinevatele isikutele ning kasutada neid korraga paljudes kohtades (erinevalt traditsioonilistest videokassettidest, mis eksisteerivad korraga ühes kohas). Veelgi enam, õpiobjektid saavad suhelda teiste objektidega ning saada kasu nende uutest versioonidest.[Wiley]
Õpiobjektidel on järgmised tunnused [Põldoja, 2008]:

- Käideldavus (accessability) ehk õpiobjekt on lihtsalt kättesaadav
- Koostalitlusvõime(interoberability) ehk õpiobjekt töötab erineva riist- ja tarkvaraga
- kohandatavus (adaptability) ehk õpiobjekti on võimalik kohandada õpilasele ja õppeolukorrale
- korduvkasutatavus (reusability) ehk õpiobjekt saab korduvalt kasutada
- vastupidavus (durability) ehk õpiobjekt töötab ka uuemal riist-ja tarkvaral
- Granulaarsus (granularity) ehk objekti on võimalik teha väiksemateks osadeks

3.2 Õpiobjektide loomise kriteeriumid

Õpiobjektide loomiseks on olemas ka erinevaid kriteeriume, millised nad peaksid välja nägema. Sisu peab olema terviklikult käsitletud, sealhulgas loogiliselt liigendatud ning üles ehitatud. Oluline on, et juurde lisatud meediaelemendid (nagu näiteks helid, videod, pildid) haakuvad vajalikul määral sisuga. Töös mainitud faktid peavad olema õiged ehk ei tohi esineda faktivigu, võimalusel viidatakse algallikale.

Õppematerjal peaks olema selge ning lihtne aru saada, selle struktuur on kooskõlas vormi ning temaatikaga. Kasutamine peaks olema jõukohane tavakasutajale ning kättesaadav vabavaralise tarkvara toel. Vastasel korral lisada juurde vajalikud juhendid. Kindlasti tuleks lisada juurde ka autori nimi. [Tiigrihüppe Sihtasutus, 2009]

Lisaks tasub õpiobjektide koostamisel silmas pidada seda, et antud tööd loetakse/vaadatakse läbi arvutiekraani, võib olla ka võimalus selle väljaprindiks. [Budris, 2008]

3.3 Metaandmed

Kokkuvõtlikult ja lühidalt öeldes on metaandmed andmed andmete kohta. Levinud on ka mõiste metadata ning kõiki õppematerjalidega seotud metadatat nimetatakse Learning Object Metadata-ks ehk LOMiks. Üldiselt käivad õpiobjekti metaandmete alla järgmised punktid: pealkiri, keel, sisukirjeldus, teema, sihtgrupp, autori nimi, materjali kasutuse tingimused. Antud punktid ei ole kindlad ning võivad olla ka teistsugused.

Ei ole ka oluline, kus metaandmed on esitatud, kas õppematerjali sees või kuskil varjatud kujul. Tihti on olulised andmed ka puudu. Metaandmete olulisus seisnebki selles, et suurendada õppematerjali leitavust. Oluline on ka see, kuidas metaandmeid kirjutada, nad peaksid olema kooskõlas rahvusvaheliselt kokkulepitud reeglitega. See võimaldab lihtsamini otsida erinevatest haridusportaalidest. [Tiigrihüppe sihtasutus, 2009]

4 Arendus

Antud bakalaureuse töö raames oli lisaks soovitustele eesmärk luua ka õpiobjekt, et tavainimesel oleks lihtsam mõnest soovitusest (näiteks kuidas kasutada biowalletit) parem arusaam ning ta teaks, miks seda kasutada.

Ajaliselt oli videode tegemine piiratud, kuna autori kasutada oli kaks nädalat iPod touch, nädal aega symbian ning paar tundi android telefon. Ja enne videode tegemist tutvus autor ka natuke telefoniga ja proovis rakendusi läbi, et ei peaks väga palju videost materjali välja lõikama.

Valik, millised videod teha, tuli kättesaadavusest ja vajalikkusest. Need on valitud soovitustest. Lisaks oli plaan teha ka video sellest, kuidas leida oma kadunud telefoni, kuid enamus neid rakendusi on tasulised. Autor tahtis proovi teha iPhone peal, nende MobileMe-l oli 30päevane tasuta testiperiood, aga kuna ka seal oli vaja krediitkaardi numbrit ning autori virtuaalne krediitkaart ei sobinud, siis jäi selle vide tegemine ära. Tegemiseks läksid videod: Kuidas kasutada avamise mustrit Androidi puhul, kuidas määrata pinkood, kuidas kasutada viirusetõrjet ning kuidas kasutada biowalletit. Kuna autor ei ole ka ise varasemalt nutitelefonidega kokku puutunud, siis tundusid need videod igati sobilikud alguseks, näiteks ei teadnud ta,kuidas määrata pinkoodi iPhonele, leidis internetis ühe inglisekeelse juhendi ning proovis selle kodus läbi. Tundus nagu oleks see funktsioon olnud natuke peidetud, seepärast sai ka see videode hulka valitud.

Androidi avamise muster tundus ka huvitav ning autor oli kuulnud sellest võimalusest, aga ei teadnud, kuidas seda teha või mis moodi see toimib.

BioWalleti puhul sai otsustavaks tema uudsus ning huvitav idee failide kaitseks(ehk siis võimalus kaitsta neid allkirjaga või parooliga). Autor oleks soovinud proovida ka, kuidas töötab silmaiirise tuvastus, aga kahjuks ei õnnestunud seda võimalust otsimisel üles leida.

Viirusetõrjeprogrammi näidet soovitas ka autori juhendaja, kuna tänapäeval on liikvel ka erinevaid viiruseid nutitelefonidele. Selle käsitlemist proovis autor läbi mitu korda enne kui läks päris filmimiseks.

Juba alguseprotsessis otsustas autor, et videod meeshäälega tunduvad usaldusväärsemad ning seetõttu on ka heli ja video eraldi tehtud ning nende kokkupanemine võttis kokkuvõttes kauem aega. Heli luges sisse autori kursusekaaslane. Kuna ta luges sisse lihtsalt autori etteantud jutu ja parandas seda natuke, siis on tehtud ka päris palju lõikamist ning proovitud seda parimat moodi videoga kokku sobitada.

Lõpuks kui video oli heliga kooskõlas toimus videode testimine (tulemustest lähemalt järgmises peatükis) ning valmis õpiobjekt SMIL keeles

SMIL oli autori jaoks uudne ning ta polnud seda varem kasutanud, seetõttu kulus pisut aega ka selle õppimiseks. Kuna ta on üsna xmli sarnane ning toimib ka htmlis,siis ei olnud õppimine raske. Autor vaatas läbi SMILi tutvustavad leheküljed ning proovis läbi näiteid ning tegi siis oma videod õpiobjektis (õpiobjektide valmimised peatükis 4.2). Kuigi keel tundus lihtne, kulus selle valmimiseks siiski aega, kuna enamus Smili näiteid oli tehtud SMIL HTMLi sees, aga autor soovis ilma HTMLita ja tundus, et näiteks ainult teksti puhtas SMILis ei saa, aga kui ta on HTMLi sees, siis saab. Esialgu oli soov võimaldada õpiobjektis ka rohkem funktsionaalsust, näiteks,et paremal pool on sisukord ning seal klikkides tuleb ette sobiv video, kuid kuna videode valmistamine ja monteerimine võttis rohkem aega, kui oli planeeritud, siis ei tulnd õpiobjektid nii funktsionaalsed, kui algselt oli plaanitud. Kindlasti oleks tulevikus otstarbekas õpiobjekte täiendada.

4.1 Videode valmimine

Nende valmimiseks on kasutatud BB Flashback Pro Recorderit, Nuendo 4 ja windows movie makerit. BB FlashBack Recorderit kasutati ekraanivideote tegemiseks, Nuendo 4 heli töötlemiseks ning Windows Movie Makerit heli ja video kokkupanemiseks.

Esimest neist kasutati ekraanivideode tegemist, teist videodele peale loetud hääle töötluseks ning kolmandat, et kokku panna hääl ja video. Lisaks eelmainitud tarkvarale on kasutatud veel ka SMIL (*Synchronized Multimedia Integration Language*) keelt, mille abil videod õpiobjektideks tehti ehk lisati juurde ka metaandmed. SMIL on keel, mis on just spetsiaalselt loodud multimeedia presentatsioonide kirjeldamiseks.

Kõik videod on tehtud lihtsalt ja arusaadavalt, kasutades Android ja Symbian süsteemiga nutitelefone ning iOS süsteemiga iPod Touch tahvelarvutit. Antud tahvelarvuti osutus valituks, sest sel töötavad samad rakendused mis iPhones ning ühtlasi oli kättesaadavam ka autorile testimiseks.

Videosid on testinud autori kursusekaaslased, kes ei ole varasemalt nutitelefonidega lähemalt kokku puutunud. Toodi välja, et antud videod on otsast lõpuni arusaadavad ning lihtne jälgida. Ka esitlejal on selge diktsioon ning ekraanil tehtavad liigutused on täpsed. Teema oli uus ja huvitav ning arvati, et nendest on kindlasti kasu, et oma nutitelefoni turvalisemaks muuta. Vigadest toodi välja vaid see, et operaatori ja monteerija töö oleks võinud natuke kvaliteetsem olla. Allpool on toodud eraldi kommentaarid videode kohta.

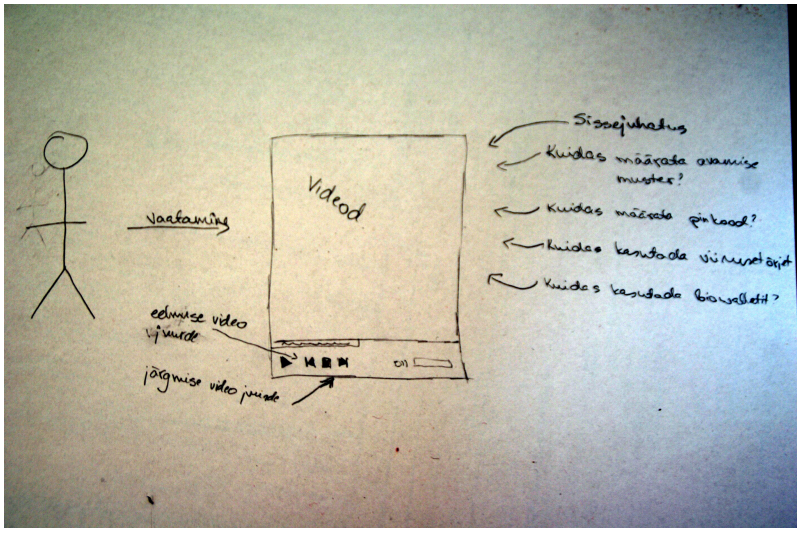
Video1. Kuidas määrata telefonile pinkood. Väga arusaadav, kuigi uut infot ei sisaldanud.
Tekst ja pilt olid hästi sünkroonis.

Video2. Kuidas määrata avamise muster. Videomaterjal on arusaadav ning info on uus, kuna ei teatud, et telefoni kaitseks selline võimalus on. Vigadena on välja toodud, et videopilt venib laiaks, kui hakatakse mustrit sisestama ning mõne koha peal on tekst natuke kiire võitu

Video3. Kuidas kasutada viirusetõrje programmi. Arusaadav ja loogiline, saadi uut infot telefonidele mõeldud viirusetõrjete kohta.Vigadena toodi välja videopildi kõikumist ning seda, et mõne koha peal ei ole video ja heli nii sünkroonis kui võiks olla.
Video4. Kuidas kasutada bioWalletit. Video oli arusaadav ning arusaamine raskusi ei tekitanud. Samuti peetakse videot kasulikuks, sest saadi uut informatsiooni failide krüpteerimise kohta. Miinuseid ei osatud välja tuua peale taustaks oleva kajaka hääle.

4.2 Õpiobjekti valmimine

Nagu juba eelpool mainitud, on videod kokku pandud õppematerjaliks, kasutades SMIL programmeerimiskeelt. SMIL (*Synchronized Multimedia Integrated Language*) on audiovisuaalsete presentatsioonide jaoks loodud keel.



Pilt 2. Skeem õpiobjektist

Õpiobjekti vaadates on kasutajal võimalus vaadata antud videot, minna järgmise video juurde või vaadata eelmist videot. Õpiobjekti puhul on kõigepeal loodud päisesse metaandmed (autori nimi, aasta ning materjali pealkiri) ning seejärel tehtud .png formaadis pilt sissejuhatuses, kuna SMIL toetab multimeedia objekte. Sissejuhatuses on öeldud millise õpiobjektiga on tegu, millist vahendit on vaja, et seda vaadata, millised videod on tulemas ning kuidas minna järgmisele slaidile. Sissejuhatus valmis arutelu käigus koos autori kursusekaaslasega.

Pilt 3. Ekraanipilt õpiobjektist

Peale sissejuhatust tulevad videod sealmainitud järjekorras. Kuidas määrata avamise muster,seejärel video2 – kuidas määrata pinkood, video3 – kuidas kasutada viirusetõrjeprogrammi ning video4 – kuidas kasutada bioWalletit

Ning kui antud video ei paku huvi, siis saab minna koha järgmise peale või vaadata veekord eelnevat.

Selleks, et vaadata SMILiga tehtud esitlusi peab olema arvutis seda toetav mediaplayer, näiteks realPlayer või windows media player.

Kokkuvõte

Käesolevas bakalaureusetöös oli ülevaade Eestis populaarsematest nutitelefonide platvormidest nagu Android, Symbian, Windows Phone, Bada ja iOS ning erinevatest lahendustest, kuidas kaitsta oma nutitelefoni ja muuta selle kasutamine turvalisemaks.

Nutitelefonide platvormid on kõik sarnased ja samas ka erinevad, pakkudes erinevaid rakendusi ning võimalusi, kuigi põhivõimalused nagu internetis lehitsemine, kaamera kasutamine, suhtlusportaalide rakendused on kõigil olemas. Kõigi nende jaoks on võimalik ka rakendusi kirjutada, laadides alla selleks vajalikud tööriistad.

Tänapäeva nutitelefonid on tehtud päris turvaliseks, näiteks käesoleval aastal toimunud häkkerite võistlusel Pwn2Own jäid Windows Phone ja Android kräkkimata, samas kui BlackBirdi ja iOSi murti sisse juba teisel päeval.

Sellest, kui turvaline on kasutaja telefon, sõltub temast endast. Tuleb järgida erinevaid lihtsaid põhimõtteid ja arusaamu ning veelgi turvalisemaks kasutamiseks tuleks kasutada ka mõnda rakendust. Mobiiltelefonide kaitse algab juba sellest, kuidas teda hoida, näiteks kuskil laua peal või tagataskus hoides on vargal seda lihtne ära võtta. Tark tegu on kasutada oma telefonil ka Pin koodi või androidi puhul avamise mustrit. Samuti oleks tark tegu peale rakenduste allalaadimist kontrollida kuu lõpus ka telefoni arvet, et mingit lisaraha ei ole seal juures. Lisaks neile elementaarsetele tarkustele on võimalik kaitsta telefonis olevaid faile mitmete rakendustega. Androidi market pakub näiteks BioWalletit, mis kaitseb faile, kas parooli või allkirjatuvastuse kaudu. Samuti on neil võimalus ka tuvastada neid silmaiirise kaudu. Samuti pakuvad erinevad tarkvarad erinevaid võimalusi kadunud telefoni üles leidmiseks, nii näiteks on Androidil „Where's my Android“, iOS'l MobileMe, Symbianil Mtracker ning Windows Phone-l „Find my Phone“. Lisaks neile rakendustele tuleks kasutada ka viirusetõrje programmi, sest juba on levinud ka erinevad viirused.

Käesolevas töös sai eesmärk enamvähem täidetud. Välja sai toodud põhilised nõuanded, kuidas telefoni kaitsta ning tehtud ka mõned videod. Videod said testitud autori kursusekaaslaste poolt. Enamasti olid nende kohta positiivsed kommentaarid, kuid leiti ka, et mõned videod võiksid olla hääle ja pildiga paremini sünkroonis. Töö edasi arendamiseks võiks juurde teha videosid ning teha neid ka Bada ning Windows Phonega, kuna antud töös on lihtsamad õppevideod vaid Android, Symbiani ning iPhonega. Samuti võiks ära parandada ka antud videodes testijate poolt leitud mõningad pisivead ning muuta õpiobjekt funktsionaalsemaks.

Summary

The topic of this bachelor thesis is „Smartphone Security. Learning tool“. Main purpose, why author wrote it is, that in the world and also in Estonia smartphones are becoming more and more popular. People use them and they do not think that even these phones can carry viruses or be unsecure.

In the thesis, there was overview about most popular smartphone platforms, like Android, Symbian, Windows Mobile, Bada and iOS, in Estonia, and different solutions, how to protect or make smartphone more secure.

Nowadays, smartphones are quite secure, for example this year’s hacking competition Pwn2Own also included smartphones to their tests. During first two days Blackbird and iOS where cracked, but Windows Phone and Android survived till the end of that competition.

The thing, how secure is smartphone actually does not depends so much on the brand, which is used, but the person, who is using it. There are several things how to make it more secure, more safe. For example, easiest things to do is to put the pincode (or set unlock pattern in Android), keep it safely in pocket and using carefully wi-fi in public places. Also, there are much possibilities to protect files, like using Astro (in android) and biowallet. Last one checks iris (or signature) to find out, if the right person is trying to view files. There is also possibility to find lost phone. Android uses „Where is my Android?“, “, iOS MobileMe, Symbian Mtracker and Windows Phone-l „Find my Phone“. These applications will show the right coordinates of the phone and also, it is possible to put the phone to ring. So it would be easier to find it in the forest. In addition, there are also antivirus softwares for phones. Author recommends to use them.

To make thesis more like a learning tool, there are added some learning objects – videos. They are made by using BB FlashBack Pro Recorder (for making screenvideos), Nuendo 4 (to work with audio), Windows Media player (to put together audio and video) and SMIL (to make learning tools from usual videos).

Author thinks that the purpose of this thesis was almost completed. There were basic tips about making smartphones safer to use and also some videos. Also, testing was made by authors class-mates. Most of the comments were positive, but they also said, that in some videos sound and video should be better synchronized. To make this work better, there should be more videos and also they should be done also with Windows Phone and Bada. Also, the small mistakes mentioned in testing should be resolved and also learning tool should be made more functional.

Kasutatud Kirjandus:

1. Android Developers (2011). What is Android? Viimati vaadatud 27.aprill 2011, aadressil http://developer.android.com/guide/basics/what-is-android.html
2. Apple (2011). iPhone 4. In so many ways, it's a first. Viimati loetus 27.aprill 2011, aadressil http://www.apple.com/iphone/features/
3. Apple (2011). iOS 4. Viimati loetud 27.aprill 2011, aadressil http://www.apple.com/iphone/ios4/
4. Apple tehnoloogiad (2010). Developer for iOS. Viimati loetud 27.aprill 2011, aadressil http://developer.apple.com/technologies/ios/
5. Bada arendajad (2011). FAQ. Viimati loetud 27.aprill 2011, aadressil http://developer.bada.com/apis/docs/commonpage.do?menu=MC01240100#a2-2
6. Bonnington, C (2011). Hacking Competition Leaves Android and Windows Phone 7 Devices Undefeated. Viimati vaadatud 27.aprill 2011, aadressil http://www.wired.com/gadgetlab/2011/03/hacking-android-windows-phone/
7. Boxall, A (2009). Mobile Security – Think You Can Make it Better? Viimati vaadatud 27.aprill 2011, aadressil http://blog.dialaphone.co.uk/2009/04/21/mobile-security-think-you-can-make-it-better-the-mobile-phone-security-challenge/
8. Budris, S. (2008) Multimeediumipõhiste õpiobjektide koostamine. Magistritöö. (juhendajad Kai Pata, Andrus Rinde) Viimati loetud 27.aprill 2011, aadressil: http://www.cs.tlu.ee/instituut/opilaste_tood/magistri_tood/kevad_2008/Sirle_Budris/Sirle_Budris_Magistri_Too.pdf
9. Eset. ESET Mobile Security. Viimati vaadatud 27.aprill 2011, aadressil https://www.nod32.ee/eset-mobile-antivirus-2/
10. F-Secure Korporatsioon (2009). Mobile Security. Viimati vaadatud 27.aprill 2011, aadressil http://www.f-secure.ee/mobile-security/index.html
11. Heimerl, J (2011). Top 10 Recommendations for Smartphone security. Viimati vaadatud 27.aprill 2011, aadressil http://blog.solutionary.com/blog/bid/56476/Top-10-Recommendations-for-Smartphone-security
12. Kameka, A (2009). Tips: Protect files on your Android phone. Viimati vaadatud 27.aprill 2011, aadressil http://androinica.com/2009/02/tips-protect-files-on-your-android-phone/

13. Microsoft (2011). Windows Phone. Enterprise. Viimati loetud 27.aprill 2011, aadressil http://www.microsoft.com/windowsphone/en-ww/features/business/enterprise.aspx

14. Microsoft (2010). Micorsoft/ Express. Phone. Viimari loetud 27.aprill 2011, aadressil http://www.microsoft.com/express/Phone/

15. Mobbeel. Tehnoloogiad. Viimati loetud 27.aprill 2011, aadressil http://www.mobbeel.com/technology/

16. Nokia Foorum (2011). Symbian Wiki. Viimati vaadatud 27.aprill 2011, aadressil http://wiki.forum.nokia.com/index.php/Symbian_OS

17. Nokia foorum (2011). Symbian C++. Viimati loetud 27.aprill 2011, aadressil http://www.forum.nokia.com/Develop/Other_Technologies/Symbian_C++/

18. Põldoja, H (2008). Õpiobjektid ja metaandmed. Viimati vaadatud 27.aprill 2011, aadressil http://www.slideshare.net/hanspoldoja/piobjektid-ja-metaandmed-presentation

19. Samsung (2011). Bada. Smartphone for Everyone. Viimati loetud 27.aprill 2011, aadressil http://www.bada.com/

20. Tiigrihüppe Sihtasutus (2009).LOM. Viimati vaadatud 27.aprill 2011, aadressil http://koolielu.ee/pg/pages/view/5199/

21. Tiigrihüppe Sihtasutus (2009). Koolielu portaali õppematerjali kvaliteedinõuded. Viimati vaadatud 27.aprill 2011, aadressil http://koolielu.ee/pg/info/readpage/8927

22. Wiley, D. A. Connecting learning objects to instructional design theory: A definition, a metaphor, and a taxonomy. Viimati vaadatud 27.aprill 2011, aadressil http://www.reusability.org/read/chapters/wiley.doc

Lisad

Lisa1. Videode tekstid

Video1. Kuidas määrata telefoni kaitseks pinkood. Iphone näitel. Selleks valime Settings – General ning Passcode Lock. Klikime nupule Turn Passcode on, mille järel peame sisestama pin koodi. Pin koodi kinnitamiseks peame sisestama sama koodi uuesti. Nüüd saame valida, millal küsitakse salasõna: *Immediately* teeb seda telefoni igakordsel avamisel, valides ajaks *one minute* või rohkem saame peale avamist antud aja jooksul telefonis toimetada enne kui küsitakse meilt pin koodi. Samalt lehelt saame ka valida *erase data*, mis tähendab parooli 10kordsel valesti sisestamisel kõikide andmete telefonist kustutamist. Nüüd vaatame tulemust: telefoni avamisel küsitakse pin koodi.

Video2. Kuidas määrata Androidi avamise muster. Kõige lihtsam viis telefoni kaitsmiseks on pin kood või androidi puhul avamise muster. Proovimegi eelnimetatud varianti Androidil. Valime menüüst *settings, security&location* ning sealt *set unlock pattern.* Omavahel peame ühendama vähemalt neli punkti, mustri kinnitamiseks peame ta sisetsama teistkordselt. Mustri rakendamiseks klikime *confirm* ning edaspidisel telefoni avamisel küsitakse meilt salvestatud mustrit.

Video3. Kuidas kasutada viirusetõrje programmi. Kõigepealt valime rakenduste seast omale sobiva tarkvara. Antud juhul on kasutatud Eset antiviiruse prooviversiooni. Selleks laadisime kõigepealt tarkvara oma arvutisse ning seejärel lisame ta Mass memory – Installs kausta telefoni. Telefonis avame seaded-rakenduste haldur – installifailid ning eset antiviirus. Sellel klikkides saame tarkvara installida. Kõigepealt kuvatakse eseti info, seejärel saab valida keele ning nõustumiseks vajutage ok, et sulgeda installeerimist segavad rakendused. Installeerimise lõppedes antakse sellest teada. Rakenduse olemasolus veendumiseks liigume tagasi ning kasuta installeerituditud rakendused, näeme, et Eset on seal täiesti olemas. Rakendusel klikkides näeme selle infot. Liigume tagasi rakenduste alla ning valime sealt äsja installeerituditud viirusetõrje. Valides menüüs activate käivitame rakenduse. Kasutajanime ning paroolina sisestame andmed, mis saabusid rakenduse allalaadimisel meie meili kontole.Valides menüüst activate, peame valima sobiva internetiühenduse.

Toiming sooritatud, aktiveeritakse rakendus, tarkvara aktiveerimise õnnestumisel antakse teada millal antud toote litsents aegub. Rakenduse korrektseks tööle rakendumiseks tuleb seadmele teha ka restart. Peale telefoni taaskäivitumist avame uuesti antiviiruse, ning valime menüüst– action. Esmalt heidame pilgui Security audi'ile. Antud funktsioon näitab infot seadme funktsioneerimise kohta. Seadmele viirusekontrolli sooritamiseks valime menüüst – action ning Scan device.Toimub telefoni skänneerimine, mille lõppedes kuvatakse tulemuste logi.

Video4. Kuidas kasutada BioWalletit. Biowallet Signature saab alla laadida Androidi

marketist. Peale selle allalaadimist valime rakenduste alt BioWalleti ning nõustume litsentsi tingimustega. Et Biowalletit kasutada, peame end registreerima vähemalt ühe võimaluse kasutajaks, kas siis BioWallet Signature või Biowallet password. Kõigepealt valime endale kasutajanime ning valime Biowallet Signature. Nüüd on kõigepealt üks kord oma allkirja harjutamiseks ning peale seda peame kuus korda sisestama oma allkirja. Kui telefon leiab kolm neist omavahel olevat piisavalt sarnased, siis on registreerimine õnnestunud. Klikime Finish ning meid suunatakse tagasi avalehele. Valime encryption ning kausta või faili, mida soovime kaitsta soovimatute silmade eest. Sellele failile vajutades küsitakse, kas soovime faili teisaldada biowalletisse või teha sellest sinna koopia. Võimalik on ka kustutada ta algasukohast. Toimub faili enkrüptimine, peale mida tuleb teade õnnestumise kohta. Valides avalehelt explorer, näeme kõiki salastatud faile erinevates kaustades. Meie fail on kõige lõpus. Sellele vajutades saame muuta ka faili nime.

Läheme tagasi avalehele. Valime menüü ja settings – security ning valime sealt logout when locked ehk telefoni klahvide lukustumisel logitakse ka biowalletist välja. Proovime nüüd uuesti biowalletisse sisse logida peale klahvide lukustamist. Sissesaamiseks küsitakse allkirja ning selle õigesti panemisel antakse ligipääs failidele

Lisa2. Küsitlus

1. Kas video on arusaadav? Kui ei, siis miks?
2. Kui kasulik oli video vaatamine, kas said uut infot?
3. Mis võiks olla antud videos teistmoodi?