Turvalise arenduse suunised nutitelefoni rakenduste väljatöötajatele

ENISA dokument, 25. november 2011

Selle aruande edasiarendajad

Dokument on koostatud koostöös OWASPiga (*Open Web Application Security Project*) ja selle koostamises osalesid:

- Vinay Bansal, Cisco Systems,
- Nader Henein, Research in Motion,
- Giles Hogben, ENISA,
- Karsten Nohl, Srlabs (SD/SIM-kaardi turvalisuse teema),
- Jack Mannino, nVisium Security Inc,
- Christian Papathanasiou, Royal Bank of Scotland,
- Stefan Rueping, Infineon (SD/SIM-kaardi turvalisuse teema),
- Beau Woods, Dell Secureworks.

Tänuavaldused

Samuti täname kommentaaride ja tehtud panuse eest Nick Kralevichi Google'ist ja OWASPi mobiiliturbe postiloendi liikmeid.

Teave ENISA kohta

Euroopa Võrgu- ja Infoturbeamet (ENISA) on ELi, selle liikmesriikide, erasektori ja Euroopa kodanike võrgu- ja infoturbe oskusteabe keskus. ENISA teeb nende rühmadega koostööd, et töötada välja infoturbe hea tava nõuandeid ja soovitusi. ENISA abistab ELi liikmesriike asjakohaste ELi õigusaktide rakendamisel ning töötab Euroopa kriitilise informatsiooni taristu ja võrkude vastupidavuse parandamise nimel. ENISA eesmärk on parandada ELi liikmesriikides olemasolevat oskusteavet, toetades nende piiriüleste kogukondade arengut, kes on pühendunud võrgu- ja infoturbe parandamisele kogu ELis. Lisateavet ENISA ja selle tegevuse kohta leiate veebiaadressilt www.enisa.europa.eu.

Kontaktandmed

Kui soovite ENISAga ühendust võtta või küsida turvalise nutitelefoni rakenduste arenduse kohta üldiselt, siis kasutage alljärgnevaid andmeid:

- e-post: giles.hogben [at] enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Õigusteave

Sisukord

Sissejuhatus / selle dokumendi taust

See dokument töötati välja koostöös OWASPi mobiiliturbe projektiga. See avaldati ka ENISA dokumendina 2011. aasta töökava kohaselt. See on kirjutatud nutitelefoni rakenduste arendajatele turvaliste rakenduste väljatöötamise suunisena. Samuti võib see huvi pakkuda nutitelefoni arendusprojektide juhtidele.

Kümne põhilise turvameetme kirjapanemisel võtsime arvesse kümmet nutitelefoni kasutajate jaoks kõige olulisemat riski dokumentides (1) ja (2) toodud kirjelduse alusel. Järeltööna tegeleme platvormispetsiifiliste juhiste ja koodinäidiste koostamisega. Loodame, et need turvameetmed annavad mõned lihtsad reeglid, millele tuginedes saate kõrvaldada oma koodist kõige levinumad nõrkused.

Nende turvameetmete rakendamine ja pingutus koodi turvaliseks muutmiseks peaksid olema kooskõlas rakenduse riskidega. Näiteks kui olete täiesti kindel, et teie rakenduse abil ei hakata töötlema isiku- ega muid tundlikke andmeid (see pole alati ilmne), pole teil võib-olla vaja muretseda andmete säilitamise maksimumperioodi pärast.

1. Tundlike andmete tuvastamine ja kaitsmine nutitelefonis

Riskid: tundlike andmete ebaturvaline talletamine, ründed kasutusest kõrvaldatud telefonidele, andmete tahtmatu avaldamine. Mobiilseadme puhul on kaotamis- ja varguserisk suurem (sest tegu on hinnalise mobiilse seadmega). Selleks et vähendada seadmes asuvate tundlike andmete kaotuse riski, tuleb rakenduses kasutusele võtta asjakohased maandamismeetmed.

1.1. Disainifaasis tuleb klassifitseerida andmete võimalikud salvestuskohad ja andmete tundlikkusest lähtuvalt võtta kasutusele turvameetmeid (nt paroolid, isikuandmed, tõrkelogid jne). Andmete töötlemine, salvestamine ja kasutamine peab toimuma selle klassifikatsiooni kohaselt. Tundlikele andmetele rakendatavate API-pöörduste turvalisus tuleb valideerida.

1.2. Tundlikud andmed tuleb salvestada serverisse, mitte kliendi seadmesse. Selle soovituse alus on eeldus, et turvalise võrguühenduse võimalus on piisavalt kättesaadav ning serveris on kasutusel paremad kaitsemehhanismid. Kliendi- ja serveripoole turvalisust tuleb võrdlevalt hinnata iga juhtumi korral eraldi (vt ENISA pilveriskide hinnangut (3) või OWASPi kümmet pilvandmetöötluse põhipunkti (4) otsustamise toetamiseks).

1.3. Andmete seadmesse salvestamisel tuleb kasutada operatsioonisüsteemi või muu usaldusväärse allika pakutavat failide krüpteerimise APIt. Osa platvorme pakub failide krüpteerimise APIsid, mis kasutavad seadme lukust vabastamise koodiga kaitstud salajast võtit, mida on võimalik kaughalduse teel kustutada. Kui see on olemas, tuleks seda kasutada, sest see suurendab krüpteerimise turvalisust lõppkasutajat täiendavalt koormamata. Samuti on salvestatud andmed siis kaotamise või varguse puhul kindlamalt kaitstud. Tuleb aga meeles pidada, et isegi seadme lukust vabastamise koodiga kaitstult sõltub seadmesse salvestatud andmete turvalisus seadme lukust vabastamise koodi turvalisusest, kui võtme kaugkustutamine pole mingil põhjusel võimalik.

1.4. Tundlikke andmeid (sealhulgas võtmeid) ei tohi krüpteerimata kujul salvestada ega vahemällu kirjutada. Võimaluse korral tuleks need salvestada urkimistõrjega (*tamper-proof*) kaitstud alasse (vt turvameede 2).

1.5. Kaaluge tundlikele andmetele juurdepääsu piiramist kontekstist lähtuvalt, näiteks asukoha alusel (nt rahakotirakendust ei saa kasutada, kui GPSi andmed näitavad, et telefon asub väljaspool Euroopat, autovõtit ei saa kasutada autost üle 100 meetri kaugusel jms).

1.6. Ajaloolisi GPSi / asukohaandmeid või muud tundlikku teavet ei tohi salvestada seadmesse kauemaks, kui on vajalik rakenduse tööks (vt turvameetmeid 1.7, 1.8).

1.7. Tuleb eeldada, et ühine salvestusruum on ebausaldusväärne: igasugusest ühisest salvestusruumist võib teave hõlpsasti ja ootamatul viisil lekkida. Konkreetsemalt tuleb silmas pidada järgmist:

- Vahemälud ja ajutine salvestusruum on võimalikud lekkekanalid, kui need on ühiskasutuses teiste rakendustega.
- Võimalikud lekkekanalid on avalikud ühised salvestusruumid, näiteks aadressiraamat, meediumigalerii ja helifailid. Näiteks kui meediumigaleriisse salvestatakse pildid koos asukoha metaandmetega, on võimalik seda teavet ettekavatsemata viisil jagada.
- Ajutisi / vahemällu salvestatavaid andmeid ei tohi hoida kõigile loetavas kataloogis.

1.8. Tundlike isikuandmete puhul tuleb ajastada kustutamine maksimaalse säilitusperioodi alusel, et hoida ära näiteks andmete lõpmatult vahemällu alles jäämine.

1.9. Praegu puudub välkmälu jaoks standardne turvaline kustutamisprotseduur, peale kogu andmekandja/kaardi füüsilise kustutuse. Seetõttu on andmete krüpteerimine ja turvaline võtmehaldus eriti olulised.

1.10. Rakenduse kirjutamisel tuleb arvesse võtta kogu andmete elutsükli turvalisust (kogumine võrgu kaudu, ajutine talletamine, vahemällu salvestamine, varundamine, kustutamine jms).

1.11. Tuleb rakendada vähima avalikustamise põhimõtet: koguda ja avalikustada üksnes andmeid, mis on vajalikud rakenduse ärikasutuseks. Disainifaasis tuleb välja selgitada vajalikud andmed, nende tundlikkus ning kas kõigi nende andmete kogumine, talletamine ja kasutamine on vajalik.

1.12. Kui vähegi võimalik, tuleb kasutada ebapüsivaid identifikaatoreid, mis pole ühised teiste rakendustega, näiteks mitte kasutada identifikaatorina seadme ID-numbrit, kui selleks pole mõjuvat põhjust (kasutada tuleks juhuslikult genereeritud numbrit, vt punkti 4.3). Rakenduseseansside puhul tuleb järgida samu andmete minimeerimise põhimõtteid nagu HTTP seansside/küpsiste jms puhul.

1.13. Hallatavates seadmetes paiknevad rakendused peaksid ära kasutama kaugkustutus- ja kaugtapulülitiga APIsid, et kõrvaldada seadme varguse või kaotamise puhul sellest tundlik teave. (Tapulüliti on mõiste, mida kasutatakse operatsioonisüsteemi tasandi või sihtotstarbeliselt loodud vahendi kohta, mille abil saab kaugühenduse kaudu rakendusi ja/või andmeid eemaldada.)

1.14. Rakenduste väljatöötajal võib tekkida vajadus lisada oma toodetesse rakenduse jaoks eraldi „andmetapulüliti", et vajaduse korral oleks võimalik kustutada nende rakenduse tundlikke andmeid ühe rakenduse kaupa (niisuguse funktsiooni kuritarvitamise ärahoidmiseks on vajalik tugev autentimine).

2. Parooli turvaline käsitlemine seadmes

Riskid: nuhkvara, jälgimine, finantskahjurvara. Varastamise korral tagab kasutaja ligipääsuinfo mitte üksnes volitamata juurdepääsu mobiilseadme tugiteenusele, vaid võib rikkuda ka muud teenused ja kontod, mida kasutaja tarvitab. Seda riski suurendab kasutajate komme paroole eri teenustes korduvkasutada.

2.1. Tuleb kaaluda paroolide asemel selliste pikemaajaliste volitamistõendite kasutamist, mida on võimalik turvaliselt seadmesse salvestada (OAuthi mudeli kohaselt). Edastamise ajaks tuleb tõendid krüpteerida (SSL/TLSi abil). Tõendid saab väljastada tugiteenus pärast kasutaja volituste esmast kontrollimist. Tõendid peaksid olema ajaliselt seotud konkreetse teenusega ja ka tühistatavad (kui võimalik, siis serveri poolelt), mis viiks miinimumini võimaliku seadme kaotusega kaasneva kahju. Kasutada tuleb autoriseerimisstandardite uusimaid versioone, näiteks OAuth 2.0. Tuleb tagada, et need tõendid aeguksid nii sageli, kui see on praktikas otstarbekas.

2.2. Kui on vaja salvestada seadmesse paroole, tuleb paroolide, parooliekvivalentide ja volitamistõendite turvaliseks talletamiseks kasutada seadme operatsioonisüsteemi pakutavaid krüpteerimis- ja võtmehalduse mehhanisme. Avatekstina paroole salvestada ei tohi. Paroole ega pikaajalisi seansiidentifikaatoreid ei tohi salvestada ilma asjakohase räsimise või krüpteerimiseta.

2.3. Osa seadmeid ja lisasid võimaldab arendajatel kasutada turvaelementi, nt (5), (6) – mõnikord SD-kaardi mooduli kaudu. Seda funktsiooni pakkuvate seadmete arv tõenäoliselt suureneb. Arendajad peaksid kasutama selliseid võimalusi võtmete, volituste ja muude tundlike andmete salvestamiseks. Niisuguste turvaelementide kasutamine annab suurema kindluse koos standardse krüpteeritud SD-kaardiga, mis on sertifitseeritud standardi FIPS 140-2 tasemele 3. Ehkki SD-kaartide kasutamine teise autentimistegurina on võimalik, ei soovitata seda aga teha, sest pärast

sisestamist ja turvamist muutub see sisuliselt seadme lahutamatuks osaks.

2.4. Mobiilseadme kasutajale tuleb anda võimalus seadmes paroole muuta.

2.5. Korrapärasel varundamisel tohib paroolid ja volitused kaasata ainult krüpteeritud või räsitud kujul.

2.6. Nutitelefonid pakuvad võimalust kasutada visuaalseid paroole, mis aitavad kasutajal paroole suurema entroopiaga meelde jätta. Neid tuleks aga kasutada üksnes siis, kui on võimalik tagada piisav entroopia. (7)

2.7. Liigutustel põhinevad visuaalsed paroolid on vastuvõtlikud plekirünnete suhtes (parooli äraarvamine puuteekraanile jäänud rasujääkide järgi). Plekirünnete nurjamiseks tuleb kasutusele võtta meetmed nagu näiteks korduvad mustrid. (8)

2.8. Tuleb kontrollida kõigi paroolide, sealhulgas visuaalsete, entroopiat (vt allpool punkti 4.1).

2.9. Tuleb tagada, et paroolid ja võtmed poleks nähtavad vahemälus ega logides.

2.10. Paroole ja muud salajast infot ei tohi rakenduse koodi sisse kirjutada . Ei tohi kasutada universaalset ühissaladust tugisüsteemiga integreerimiseks (näiteks koodi sisse manustatud parool). Mobiilirakenduste binaarfaile saab hõlpsasti alla laadida ja pöördprojekteerida.

3. Tundlike andmete kaitse tagamine andmete edastamisel

Riskid: võrgupetteründed, jälgimine. Suurem osa nutitelefonidest on suutelised kasutama mitmeid võrgumehhanisme, sealhulgas Wi-Fi, teenusepakkuja võrk (3G, GSM, CDMA ja muud), Bluetooth jms. Kanalid iseenesest on ebaturvalised ning nendes liikuvaid andmeid võidakse pealt kuulata. (9) (10)

3.1. Tuleb eeldada, et teenusepakkuja võrgukiht ei ole turvaline. Nüüdisaegsed võrgukihi ründed suudavad dekrüpteerida teenusepakkuja võrgu krüpteeringu ja puudub garantii, et Wi-Fi võrk on nõuetekohaselt krüpteeritud.

3.2. Tundliku teabe saatmisel võrgu kaudu või raadio teel peavad rakendused looma otspunktide vahelise turvalise kanali (näiteks SSL/TLSi) (kasutades näiteks Strict Transport Securityt – STSi (11)). See hõlmab ka kasutaja volituste ja teiste võrdväärsete autentimisvahendite edastamist. See tagab konfidentsiaalsuse ja tervikluse kaitse.

3.3. Tuleb kasutada tugevaid ja hästituntud krüpteerimisalgoritme (nt AES) ning asjakohaseid võtmepikkuseid (kontrollige soovitusi algoritmide kohta nt dokumendist (12) leheküljel 53).

3.4. Kasutada tuleb usaldusväärsete sertifitseerimisteenuse pakkujate allkirjastatud sertifikaate. Omaallkirjastatud sertifikaatide lubamisel tuleb olla väga ettevaatlik. SSLi ahela valideerimist ei tohi keelata ega eirata.

3.5. Tundlike andmete puhul tuleb vahendusrünnete (näiteks SSL-proksi, SSL-paljastamine) riski vähendamiseks kontrollida serveri identiteeti enne krüpteeritud kanali loomist. Seda on võimalik saavutada, kui SSL-ühendus rajatakse ainult otspunktidega, mille võtmeahelas on olemas usaldusväärsed sertifikaadid.

3.6. Kasutajaliides peaks tegema sertifikaadi kehtivuse väljaselgitamise kasutajale võimalikult lihtsaks. Sisuliselt ei peaks kasutaja seda üldse nägema, välja arvatud potentsiaalse vea olukorras.

3.7. Tundlike andmete edastamiseks ühest mobiilotspunktist teise ei tohi kasutada SMS- või MMS-sõnumeid ega muid teateid.

4. Kasutajate autentimise, volituste kontrolli ja seansihalduse korrektne realiseerimine

Riskid: volitamata isikud võivad omandada juurdepääsu tundlikele andmetele või süsteemidele autentimissüsteemidest möödahiilimise (kasutajatunnused) või kehtivate tõendite või küpsiste korduva kasutamise teel. (13)

4.1. Rakendusse sisenemiseks tuleb nõuda kasutaja asjakohase tugevusega autentimist. Kasulik võib olla tagasiside andmine parooli tugevuse kohta parooli esmakordsel sisestamisel. Kasutatava autentimismehhanismi tugevus peab sõltuma sellest, kui tundlikke andmeid rakendus töötleb, ja juurdepääsust väärtuslikele ressurssidele (nt raha kulutamine).

4.2. On oluline tagada, et pärast esimest autentimist käsitletaks seansihaldust õigesti asjakohaste turvaliste protokollide abil. Näiteks võiks nõuda iga edaspidise päringu korral volituste või tõendite uuesti edastamist (eriti kui päring annab eelisjuurdepääsu või võimaldab teha muudatusi).

4.3. Tuleb kasutada suure entroopiaga seansiidentifikaatoreid, mida pole võimalik prognoosida. Arvestage, et juhuslike arvude generaatorid toodavad etteantud seemne põhjal üldjuhul juhusliku, ent prognoositava väljundi (st iga seemne põhjal luuakse sama juhuslike arvude jada). Seetõttu on oluline anda juhuslike arvude generaatorile ette mitteprognoositav seeme. Tavameetod, mille puhul kasutatakse kuupäeva ja kellaaega, ei ole turvaline. Seda saab parandada, kasutades näiteks kuupäeva ja kellaaja kombinatsiooni, telefoni temperatuuriandurit ning hetke x-, y- ja z-magnetvälju. Nende väärtuste kasutamisel ja kombineerimisel tuleb valida põhjalikult testitud algoritmid, mis entroopiat võimalikult palju suurendavad (nt võib juhuslike väärtuste kombineerimiseks ja seejuures maksimaalse entroopia säilitamiseks rakendada mitu korda SHA-1, eeldusel, et seemne maksimumpikkus on konstantne).

4.4. Autentimise turvalisemaks muutmiseks tuleks kasutada konteksti, nt IP-aadressi kohast asukohta jms.

4.5. Kui võimalik, tuleb kaaluda täiendavate autentimistegurite kasutamist rakenduste puhul, mis annavad juurdepääsu tundlikele andmetele või liidestele, nt hääl, sõrmejälg (kui on saadaval), „keda-tunnete", käitumuslikud tegurid jms.

4.6. Kasutada tuleb autentimist, mis on seotud lõppkasutajaga (mitte seadmega).

5. Tagasüsteemi APIde (teenuste) ja platvormi (serveri) turvalisena hoidmine

Riskid: ründed tugisüsteemide vastu ja andmete kaotus pilvsalvestuse kaudu. Suurem osa mobiilirakendustest vahetab tugisüsteemi APIdega andmeid RESTi/veebiteenuste või firmapäraste protokollide abil. Nende APIde või teenuste ebaturvaline realiseerimine ja tugisüsteemi platvormi tugevdamata/paikamata jätmine võimaldab ründajatel rikkuda mobiilseadmes asuvad andmed nende edastamisel tugisüsteemi või rünnata mobiilirakenduse kaudu tugisüsteemi ennast. (14)

5.1. Kontrollige oma koodi spetsiifiliselt tundlike andmete ettekavatsemata edastamise ja igasuguse andmete edastamise suhtes mobiilseadme ja veebiserveri tugisüsteemi ning muude välisliideste vahel (nt kas faili metaandmed sisaldavad asukoha- või muud teavet).

5.2. Kõiki mobiilirakenduste jaoks ette nähtud tugiteenuseid (veebiteenused/REST) tuleks korrapäraselt nõrkuste suhtes kontrollida, nt kasutades testimiseks ja turvadefektide leidmiseks koodi analüsaatoreid ja ründetesti vahendeid.

5.3. Tuleb tagada, et tugiplatvorm (server) töötaks tugevdatud konfiguratsiooniga, kus operatsioonisüsteemile, veebiserverile ja muudele rakenduse komponentidele on rakendatud uusimad turvapaigad.

5.4. Tuleb tagada, et tugisüsteemis säilitatakse piisavad logid intsidentide avastamiseks ja neile reageerimiseks ning kohtuekspertiisi tegemiseks (andmekaitseseadusega lubatud piirides).

5.5. DDoS rünnetest tingitud riskide vähendamiseks tuleks kasutada edastuskiiruse/sessioonide arvu piiramist kasutaja/IP-aadressi kaupa (kui on võimalik kasutaja tuvastamine).

5.6. Tuleb testida, kas leidub DoS nõrkusi, mille korral teatud intensiivselt ressursse kasutavad rakendusepöördused võivad serveri üle koormata.

5.7. Veebiteenustel, RESTil ja APIdel võib olla veebirakendustega sarnaseid nõrkusi:

- lisaks positiivsete kasutusjuhtumite testimisele tuleb testida ka kuritarvitusjuhtumeid;
- nõrkuste väljaselgitamiseks tuleb testida tugisüsteemi veebiteenust, RESTi või APId.

6. Turvaline andmete integratsioon kolmandate isikute teenuste ja rakendustega

Riskid: andmeleke. Kasutajad võivad installida rakendusi, mis võivad edastada isikuandmeid (või muid salvestatud tundlikke andmeid) kuritahtlikel eesmärkidel.

6.1. Kontrollige igasuguste mobiilirakenduses kasutatud kolmandate osapoolte koodi/teekide turvalisust/autentsust (nt veenduge, kas need pärinevad usaldusväärsest allikast, neil on hooldustugi, ei ole tagasüsteemi Trooja hobuseid).

6.2. Jälgige kõiki mobiilirakenduses kasutatud kolmandate osapoolte raamistikke/APIsid turvapaikade suhtes. Neid kolmandate osapoolte APIsid/raamistikke kasutavates mobiilirakendustes tuleb samuti teha vastav turvauuendus.

6.3. Erilist tähelepanu tuleb pöörata kõigi ebausaldusväärsetest kolmandate osapoolte rakendustest (nt reklaamivõrgu tarkvara) vastu võetud ja neisse saadetavate andmete valideerimisele enne nende töötlemist rakenduses.

7. Eritähelepanu kasutaja andmete kogumise ja kasutamise kohta nõusoleku võtmisele ja talletamisele

Riskid: isiku- või privaatsete andmete ettekavatsemata avalikuks tulemine, ebaseaduslik andmetöötlus. Euroopa Liidus on kohustuslik saada isikutuvastusteabe (PII) kogumiseks kasutaja nõusolek. (15) (16)

7.1. Tuleb luua isikuandmete kasutamist käsitlev privaatsuspoliitika ja teha see kasutajale kättesaadavaks, eriti nõusolekuvalikute tegemisel.

7.2. Nõusoleku võtmiseks on kolm peamist moodust:

- installimise/paigaldamise ajal;
- käitusajal andmete saatmisel;
- keeldumismehhanismide kaudu, mille puhul on realiseeritud vaikeseadistus ja kasutaja peab vaikeseadistuse välja lülitama.

7.3. Tuleb kontrollida, kas rakendus kogub isikutuvastusteavet – see ei pruugi alati ilmne olla –, näiteks kas kasutate püsivaid unikaalseid identifikaatoreid, mis on seotud isikuandmeid sisaldavate kesksete andmehoidlatega.

7.4. Tuleb auditeerida sidemehhanisme, et kontrollida, kas esineb ettekavatsemata lekkeid (nt piltide metaandmed).

7.5. Isikutuvastusteabe edastamise nõusolek tuleb salvestada ja säilitada. See salvestis peab olema kasutajale kättesaadav (tuleb ka kaaluda, kas oleks väärtuslik hoida serveri poolel igasuguste talletatud kasutajaandmetega seotud kirjeid). Niisuguste

kirjete puhul tuleks miinimumini viia nendes endas salvestatud isikuandmete hulk (nt räsimise teel).

7.6. Tuleb kontrollida, kas nõusoleku võtmise mehhanism kattub või on vastuolus (nt avaldatud andmetöötlustavas) mõne muu olemasoleva ja seotud nõusoleku võtmisega (nt rakenduse oma + veebikomplekti HTML) ning lahendada igasugused vastuolud.

8. Turvameetmed vältimaks volitamata juurdepääsu ressurssidele (rahakott, SMS, telefonikõned jne)

Riskid: nutitelefoni rakendused annavad programmi tasemel (automaatse) juurdepääsu kõrgema hinnaga telefonikõnedele, SMSile, rändlusandmetele, NFC maksetele jms. Rakendused, millel on eelisjuurdepääs niisugustele APIdele, peavad eriti hoolikalt kuritarvitusi ära hoidma, võttes arvesse, milline mõju on nõrkustel, mis annavad ründajatele juurdepääsu kasutaja rahalistele ressurssidele.

8.1. Tasulistele ressurssidele juurdepääsu kohta tuleb pidada salgamatus vormingus logisid (nt usaldusväärse serveri tugisüsteemi saadetav allkirjastatud kviitung – kasutaja nõusolekuga) ja teha need lõppkasutajale jälgimiseks kättesaadavaks. Logisid tuleb volitamata juurdepääsu eest kaitsta.

8.2. Tuleb kontrollida ebaharilike kasutusmustrite esinemist tasuliste ressursside puhul ja käivitada uuesti autentimine näiteks juhul, kui asukoht muutub kiiresti olulisel määral, muutub kasutuskeel vms.

8.3. Kaaluda tuleb valge nimekirja mudeli vaikimisi kasutamist tasuliste ressursside aadresside puhul, näiteks aadressiraamat üksnes juhul, kui on konkreetselt antud volitused telefonikõnede tegemiseks.

8.4. Autentida tuleb kõik API-pöördused tasulistele ressurssidele (nt rakenduse väljatöötaja sertifikaadi abil).

8.5. Tuleb tagada, et rahakoti-API tagasihelistused ei edasta avatekstina teavet konto/hindade/arvelduse/artiklite kohta.

8.6. Rakenduse käitumise igasugustest rahalistest tagajärgedest tuleb kasutajat hoiatada ja saada vastav nõusolek.

8.7. Et signaaliedastuse koormus tugijaamadele oleks võimalikult väike, tuleb rakendada head tava, näiteks kiire jõudeolek (3GPP spetsifikatsioon), vahemällu salvestamine jms.

9. Mobiilirakenduste turvalise levitamise/soetamise tagamine

Riskid: turvalise levitamise tava kasutamine on oluline kõikide ENISA kümne põhiriski hulgas kirjeldatud riskide leevendamiseks.

9.1. Rakendused peavad olema disainitud ja soetatavad selliselt, et on võimalik uuendamine turvapaikade lisamiseks, võttes arvesse rakenduste poodide nõudeid ja sellega kaasnevat lisaviivitust.

9.2. Enamik rakenduste poode jälgib rakendusi ebaturvalise koodi suhtes ja on intsidendi korral suutelised rakendusi lühikese etteteatamisega kaugelt eemaldama. Rakenduste levitamine ametlike rakendusepoodide kaudu annab seega toimemehhanismi juhuks, kui rakenduses peaks esinema tõsiseid turvaauke.

9.3. Kasutajatele tuleb anda tagasisidekanalid turbeprobleemidest teatamiseks, näiteks e-posti aadress algusega „security@”.

10. Koodi interpreteerimisel tekkivate vigade ja tõrgete haldus

Riskid: koodi interpreteerimisel esinev tõrge või veaolukord võib anda ründajale võimaluse anda kontrollimata sisendit, mida interpreteeritakse koodina, näiteks mängu lisatasemed, skriptid, interpreteeritavad SMS-sõnumi päised. See annab kahjurvarale võimaluse mööda hiilida rakendusepoodides kasutatavatest turvameetmetest. See võib kaasa tuua ründed, mille tagajärjeks on andmeleke, jälgimine, nuhkvara ja helistusvara.

Tuleb arvestada, et alati pole ilmne, kas kood sisaldab interpretaatorit. Otsida tuleks igasuguseid võimalusi, millele juurdepääsuks on vaja kasutaja sisestatud andmeid ja kolmandate autorite APIsid, mis võivad kasutaja sisendit interpreteerida, nt JavaScripti interpretaatoreid.

10.1. Käitusaegne interpreteerimine ja interpretaatorite pakutavad võimalused tuleb viia miinimumini: interpretaatoreid tuleb käitada kõige väiksemate õigustega.
10.2. Tuleb vajadust mööda määratleda igakülgne katkestussüntaks.
10.3. Interpretaatoritele tuleb teha ründetest.
10.4. Interpretaatorid tuleb paigutada liivakasti (*sandbox*).

1. Lisa A: asjakohane üldine hea koodikirjutamistava

Mobiilirakenduste koodi seisukohast on eriti asjakohane osa üldisest heast koodikirjutamistavast. Oleme siin kirja pannud mõned kõige olulisemad nõuanded:

- lisaks positiivsete kasutusjuhtumite testimisele tuleb testida ka kuritarvitusjuhtumeid;
- kogu sisend tuleb valideerida;
- ridade arvu ja koodi keerukust tuleb vähendada miinimumini; tsüklomaatiline keerukus (17) on kasulik mõõdik;
- tuleb kasutada turvalisi keeli (nt puhvri ületäitumise suhtes);
- tuleb sisse seada turvaraportide käsitlemise protsess (aadress) security@example.com;
- turvadefektide leidmiseks tuleb kasutada koodi staatilisi ja lähtekoodi analüsaatoreid ning ründetestide tegemise vahendeid;
- tuleb kasutada turvalisi stringifunktsioone, hoida ära puhvri ja täisarvu ületäitumine;
- rakendusi tuleb käitada vähimate õigustega, mis on operatsioonisüsteemis rakenduse jaoks nõutavad; tuleb teadlik olla õigustest, mille APId vaikimisi annavad ja need vajadusel keelata;
- ei tohi lubada koodi/rakenduse käivitamist juurkasutaja/süsteemiadministraatori õigustes;
- testida tuleb alati nii tava- kui ka eeliskasutajana;
- tuleb hoiduda rakendusele spetsiifiliste ühendusmehhanismide loomisest klientseadmes; tuleb kasutada operatsioonisüsteemi pakutavaid sidemehhanisme;
- enne rakenduse avaldamist tuleb eemaldada kogu testkood;
- tuleb tagada asjakohane logimine, kuid mitte salvestada liigseid logisid, eriti niisuguseid, mis sisaldavad tundlikku kasutajateavet.

2. Lisa B: erisuunised ettevõtetele

- Kui seadmesse tuleb soetada äriliselt tundlik rakendus, peaksid rakendused jõustama seadmes turvalisema režiimi (näiteks PIN-kood, kaughaldus/-kustutus, rakenduse jälgimine).
- Seadme tugevamaks autentimiseks võib kasutada seadmesertifikaate.

3. Viited

1. **ENISA.** Top Ten Smartphone Risks. [Võrgus] http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks.
2. **OWASP.** Top 10 mobile risks. [Võrgus] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks.
3. Cloud Computing: Benefits, Risks and Recommendations for information security. [Võrgus] 2009. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
4. OWASP Cloud Top 10. [Võrgus] https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project.
5. Blackberry developers documents. [Võrgus] http://www.blackberry.com/developers/docs/7.0.0api/net/rim/device/api/io/nfc/se/SecureElement.html.
6. Google Seek For Android. [Võrgus] http://code.google.com/p/seek-for-android/.
7. Visualizing Keyboard Pattern Passwords. [Võrgus] cs.wheatoncollege.edu/~mgousie/comp401/amos.pdf.
8. *Smudge Attacks on Smartphone Touch Screens.* **Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith.** s.l. : Department of Computer and Information Science – University of Pennsylvania.
9. Google vulnerability of Client Login account credentials on unprotected . [Võrgus] http://www.uni-ulm.de/in/mi/mitarbeiter/koenings/catching-authtokens.html.
10. SSLSNIFF. [Võrgus] http://blog.thoughtcrime.org/sslsniff-anniversary-edition.
11. [Võrgus] http://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-02.
12. NIST Computer Security. [Võrgus] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf.
13. Google's ClientLogin implementation . [Võrgus] http://www.uni-ulm.de/in/mi/mitarbeiter/koenings/catching-authtokens.html.
14. [Võrgus] https://www.owasp.org/index.php/Web_Services.
15. EU Data Protection Directive 95/46/EC. [Võrgus] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
16. [Võrgus] http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/Testimony_05.04.11_Spafford.pdf.
17. [Võrgus] http://www.aivosto.com/project/help/pm-complexity.html.
18. [Võrgus] http://code.google.com/apis/accounts/docs/AuthForInstalledApps.html.
19. Google Wallet Security. [Võrgus] http://www.google.com/wallet/how-it-works-security.htm.

P.O. Box 1309, 71001 Heraklion, Kreeka
www.enisa.europa.eu