AK juurdepääsupiirang kehtetuks tunnistatud RIA peadirektori 15.11.2021 käskkirjaga nr 1.1-2/21-099

JUURDEPÄÄS AINULT TEADMISVAJADUSE
JA JUURDEPÄÄSUÕIGUSE ALUSEL

ASUTUSESISESEKS KASUTAMISEKS
Riigi Infosüsteemi Amet
märge tehtud 20.12.2011 a
Juurdepääsupiirang kehtib kuni 20.12.2016 a
Alus: AvTS § 35 lg 1 p 9 ja 10

Lisa 3. Eesti ID-kaardi v3.0 koodi analüüs Joe-Kay Tsay raporteeritud PKCS#1 ründe valguses, 12.12.2011
Martin Paljak

Riigi Infosüsteemi Amet
reg kp 20.12.2011
reg nr 1-6/11-6-5-3

Taust
Käesoleva töö eesmärk on kontrollida Jay-Kay Tsay raporteeritud PKCS#1 versioon 1.x (PKCS#1 v1) polsterduse rünnet Eesti ID-kaardi (2011. aasta versiooni) kontekstis. Lisaks teostatakse ID-kaardi 2011 versiooni algkoodi analüüs lähtudes seotud standarditest, parimatest tavadest ja vastavusest esitatud dokumentatsioonile.

RSA dekrüpteerimise rünne PKCS#1 polsterduse oraakli abil
Daniel Bleichenbacher-i poolt avaldatud rünne võimaldab PKCS#1 v1 polsterdusega krüpteeritud avateksti avastada, omamata otsest ligipääsu privaatvõtmele või tavapärase eduka dekrüpteerimise tulemusel saadavale avatekstile.

Rünne toimub konstrueeritud krüptogrammide saatmisega oraaklile:
ründaja omab PKCS#1 polsterdusega krüpteeritud avateksti
ründaja konstrueerib spetsiaalsed krüptogrammid ja edastab need ohvrile dekrüpteetimiseks
ohver avaldab ründajale tahtmatult infot dekrüpteerimisel tekkiva PKCS#1 vormingu vea kohta
tulenedes lekkinud infole, kas dekrüpteeritud blokk vastas PKCS#1 vormingule või mitte, muudab ründaja dekrüpteerimisele saadetavaid krüptogramme
edu korral saab ründaja kätte algse avateksti

Kuna RSA puhul toimub dekrüpteetimine ja signeerimie sama tehtega (modulaarne astendamine salajase eksponendiga) on ebapiisava formaadikontrolliga võimalik lisaks avateksti avastamisele ka allkirja (krüpteeringu) võltsimine.

PKCS#1 polsterduse oraakli rakenduvus ID-kaardi kontekstis
Ründe edukaks läbiviimiseks on vajalikud eeldused:
ründaja saab ohvri privaatvõtit hoidvale seadmele või rakendusele edastada suvaliselt valitud krüptogramme dekrüpteerimiseks
ründaja saab ohvri seadmes või rakenduses toimuva dekrüpteerimise tulemuse PKCS#1 formaadi mittevastuavuse puhul veateate
ründajal on eelnevad võimalused pikema aja jooksul

Bleichenbacheri ründe praktiline demonstratsioon (Klima et al) on olnud SSL-is kasutatava sessioonivõtme avastamine. Sellise ründe puhul on oraakliks veebiserver, mida pommitatakse halvasti vormistatud krüptogrammidega, ja leitavaks avatekstiks eelnevalt salvestatud SSL-i sessiooni võti. Rünne on võimalik, kuna SSL-i puhul ei ole iga serveri privaatvõtmega toimuvate operatsioonide autoriseerimine mõeldav (tavaline on serveri käivitamisel operaatori kohalolek kas võtit kaitsva parooli sisestamiseks või siis HSM-is võtme aktiveerimiseks, edaspidiseid operatsioone ei piirata). Teisisõnu on oraakli ründed võrreldavad "vähendatud päringutega brute force" ründega.

Jah-Kay Tsay kirjeldatud rünne põhineb Bleichenbacheri ja Klima rünnete optimeerimisel ja vajalike dekrüpteerimiste vähendamisel (65%) kuid see number on endiselt suur, ID-kaardi puhul väidetavalt keskmiselt 57000 operatsiooni (mis kaardi kiirust arvestades teeb ajaliselt 1..2 ööpäeva).

ASUTUSESISESEKS KASUTAMISEKS
Märge tehtud: 21.12.2016
Kehtib kuni: 21.12.2021
Alus: AvTS §35 lg 1 p 9,10
Teabevaldaja: Riigi Infosüsteemi Amet

Ligipääs privaatvõtit hoidvale seadmele
ID-kaardi puhul tähendab ligipääs privaatvõtmele kas:
1. füüsilist ligipääsu kaardile ja PIN koodi(de) teadmist (kaardi omanik)
2. pahavara kaardi omaniku arvutis ja sisestatud kaardi PIN koodi(de) teadmist (praktikas sama mis punkt 1 aja jooksul, mil kaart on lugejas)
3. pettuse abil kasutaja kaardile valesti koostatud blokkide edastamist (ja kirjeldatud ründe puhul PKCS#1 formaadi vea kommunikeerimist ründajale)
4. pahavara abil valideeritud PIN koodiga kaardi ära kasutamist (praktikas enamalt jaolt sama mis punkt 2)

Rünne krüptosüsteemile pole vajalik, kui ründajal on ligipääs kaardile ja PIN koodile, mis võimaldab ründaja käsutuses oleval koodil kaardiga opereerida samades õigustes kui kaardi omanik.
Vähendamaks punktis 2 kirjeldatud võimalust pahavaral PIN kood varastada ja seda hiljem oma äranägemise järgi kasutada, on loodud eraldi klahvistikuga kaardilugejad, mille puhul klahvistiku kaudu sisestatud PIN kood ei satu kordagi pahavara valduses olevasse arvutisse. Nende levik pole massiline ja ei takista pahavaral PIN koodi teades võtmete kasutamist kaardiomaniku teadmata.
Klahvistikuga kaardilugejate edasiarendused ei luba ka PIN koodi sisaldavate käskude edastamist arvutist, vaid nõuavad PIN koodi sisestamist füüsilise klahvistiku kaudu. Sellise kaardilugeja kasutamine jätab pahavarale ainsaks võimaluseks ära kasutada ID-kaardi omadust PIN1 koodiga kaitstud operatsioonide lubamist kuni kaardi eemaldamiseni lugejast või deaktiviseerimiseni tarkvara poolt. Viimast ei realiseeri baastarkvara, kuna pidev PIN1 koodi sisestamine muudaks veebiportaalide kasutamise praktikas väga tülikaks või suisa ebameeldivaks kogemuseks.
Dekrüpteerimist toetav laiatarbe tarkvara
Nii allkirjastamine kui SSL-i abil veebis autentimine põhineb RSA krüpteerimisel, seejuures toimub PKCS#1 polsterduse lisamine kiipkaardis (ehk alati õige formaadiga). Dekrüpteerimine on kasutusel ainult väikeses osas tarkvarast, näiteks:
- Windowsi domeeni logimisel
- DigiDocCrypto puhul
- S/MIME e-kirjade krüpteerimisel

Isegi kui ründajal on võimalus üle võrgu saata halvasti koostatud krüptogramme, ei ole praktikas võimalik automaatselt saada tagasi vajalikku infot kaardil toimunud krüpteerimise ebaõnnestumise kohta.

Privaatvõtmega operatsioonide autoriseerimine
Kõik ID-kaardi operatsioonid privaatvõtmetega eeldavad kontrollitud PIN koodi, kusjuures operatsioonid signeerimisvõtmega eeldavat uut PIN koodi sisestust enne igat toimingut (või käsu kaitsmist vastava kaardihalduseks kasutatava võtmega). Algkood ja praktiline katse kinnitavad seda.

Ründe raporteerijal võis jääda ekslik mulje, et kaardilugejasse sisestatud kaart, mida on korra juba kasutatud (näiteks veebis sisse logimiseks) jääb autentimisvõtit kaitsev PIN1 kood kontrollitud olekusse kuni kaardi eemaldamiseni lugejast või tarkvara poolt antava reset käsuni. See võimaldab ka pahavaral näiliselt PIN1 koodi küsimata kaarti kasutada oraaklina. Samas võib pahavara antud situatsioonis kasutada kaardil olevat võtit tavapäraselt, nii krüpteerimiseks (autentimisvõtmega allkirjastamiseks) kui dekrüpteerimiseks. Kurivaraga nakatunud arvutis ID-kaardi kasutamine on üldjuhul kurivara alati paremas seisus kui kasutaja.

ASUTUSESISESEKS KASUTAMISEKS
Riigi Infosüsteemi Amet
märge tehtud 20.12.2011 a
Juurdepääsupiirang kehtib kuni 20.12.2016 a
Alus: AvTS § 35 lg 1 p 9 ja 10

Autentimisvõtme ja signeerimisvõtme erisus
Rünne kirjeldab ainult ID-kaardi autentimisvõtme kasutamist. Teoreetiliselt oleks sama rünne rakendatav mistahes võtme puhul, millega on võimalik dekrüpteerida, kuid raporteerija väitel ei toeta ID-kaart digiallkirja võtmega dekrüpteerimist.
ID-kaardi baastarkvaras realiseeritud teegid sätivad eksponeeritud võtmetele lubatud operatsioonidena sertifikaadi võtme kasutusest tulenevad võimalused:
Autentimisvõtmel: Digital Signature, Key Encipherment, Data Encipherment (kõik RSA operatsioonid PKCS#11 tasemel)
Signeerimisvõtmel: Non Repudiation (ainult RSA signeerimine PKCS#11 tasemel)
Kaardirakendus aga lubab dekrüpteerimist ka allkirja võtmega. Selleks tuleb kas käsitsi vastavad käsud kaardile edastada või modifitseerida ID-kaardi baastarkvara.
PIN koodi kontroll rakendub siiski, sarnaselt digiallkirjaga tuleb PIN2 sisestada iga operatsiooni eel (iga alustatav operatsioon signeerimisvõtmega deaktiveerib PIN-i kontrollitud staatuse)

Dekrüpteerimine signeerimisvõtmega ei ole toetatud baastarkvara poolt. Kui ID-kaardi tellijal/haldajal pole selget vajadust allkirjavõtmega dekrüpteerimiseks, tuleks see võimalus kaardirakendusest eemaldada.
Kokkuvõte
Kirjeldatud ründel puudub praktiline väärtus. Kuigi PKCS#1 formaadi viga kommunikeeritakse kaardilt väljapoole, ei ole see kasutatav ründajale. ID-kaart kontrollib enne operatsioone privaatvõtmetega korrektselt PIN koodi. Edukas rünne eeldab kurivara kasutaja arvutis ja selle olemasolul on palju lihtsamaid ja efektiivsemaid lahendusi nii krüpteeritud avatekstide leidmiseks kui ka allkirjade võltsimiseks (PIN koodi vargus pahavara poolt, kaardile saadetavate räside ja krüptogrammide asendamine ründaja poolt valituga jne).

Viited
[1] EstEID kaardi kasutusjuhend - http://www.id.ee/public/EstEID_kaardi_kasutusjuhend.pdf
[2] EstEID turvakiibi rakendus ja liides - http://www.id.ee/public/EstEID_Spetsifikatsioon_v2.01.pdf
[3] Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring - http://www.riso.ee/et/files/kryptoalgoritmide_elutsykli_uuring.pdf
[4] Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1 - http://www.bell-labs.com/user/bleichen/papers/pkcs.ps
[5] Attacking RSA-based Sessions in SSL/TLS - http://eprint.iacr.org/2003/052.pdf
[6] E-hääletamise organisatsiooniline ja tehniline kontseptsioon - http://www.vvk.ee/public/dok/Kontsept-03.pdf
[7] ID-kaardi tehnoloogia lähteuuring - http://www.id.ee/public/cyberaruanne_20070322030353.pdf
[8] ID-kaartdi lähteuuringu aruanne - http://www.id.ee/public/aptaruanne.pdf