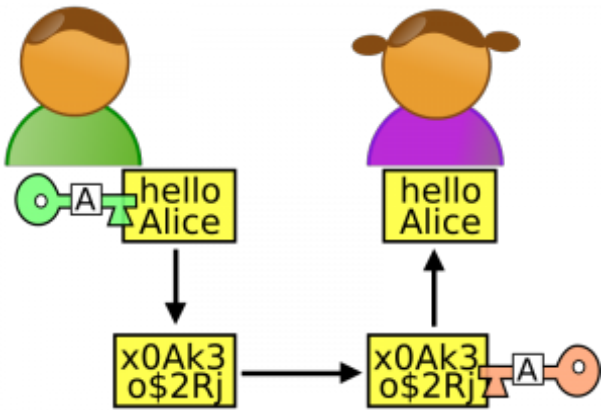
https://blog.ria.ee/elasid-kord-kruptograafid-ehk-kuidas-me-eesti-e-edulugu-kaitsma-peame/

Elasid kord … krüptograafid ehk kuidas me Eesti e-edulugu kaitsma peame



Allikas: Wikimedia Commons, autor: odder.

Priit Roosimägi, RIA arendus- ja uurimistegevuse osakonna juhataja

Ajalugu

Elasid kord Whitfield Diffie ja Martin Hellman. Muidu ontlikke mehi vaevas üks ränkraske probleem – kuidas teha nii, et Bob ja Alice võiksid omavahel turvaliselt tutvuda ning seejärel veel ka turvaliselt suhelda, ilma et suvaline Mike või Jane neid pealt kuulata saaks. Aasta siis oli seitsekümmend kuus.

Vaid aasta varem oli sõjameeste viljakas rüpes tärganud Interneti otsene eelkäija ARPANET, kompuutrimälu oli pesumasinatest suurem ning rohi oluliselt rohelisem kui tänavu Hiiumaal. Reklaamfilme e-valimistest, digiretseptist, „täiustatud reaalsust“ pakkuvast HoloLens’ist ja elektrooniliste andmete krüpteerimise kaudu väljapressimisega tegelevast CryptoLockerist oli seks ajaks ehk näidatud vaid ekstsentriliste ulmekirjanike unenägudes. Kuid Whitfield ja Martin olid tulevikku näinud ning sünnitasid seetõttu 1976. aastal teadusarendustegevuse tulemusel Diffie-Hellmani nimelise võtmevahetusprotokolli, mis Bobi ja Alice’i mure lahendas.

Tänapäev

Nüüd, ligi 40 aastat hiljem, põhineb sellel protokollil meie tänapäev – seda kasutab pea kogu Interneti teel toimuv turvatud andmevahetus. Teisalt pole aga arvutusvõimsuse kasvu tõttu Diffie-Hellmani võtmevahetuses pruugitava krüptograafia aluseks olevad rasked probleemid enam nii rasked kui aastal 1976. Kas see tähendab, et interneti vahendusel saadetavad sõnumid (nt pangaülekanded, e-valimised) pole enam turvalised?! Kui salastuse tagamiseks kasutataks samu krüptoalgoritme, mis 40 aastat tagasi, siis tõesti poleks need turvalised. Õnneks nii see pole ja aega

mööda on rakendustes algoritme üha uuendatud selleks, et need oleksid pidevalt eespool kasvava arvutusvõimsusega saavutatavast murdmisvõimekusest.

Sõnumisaladus

Sõnumisaladus on üks potentsiaalselt ohtlik asi. Selle abil saab küll internetis turvaliselt rahvasaadikuid valida, pangas käia, Amazonist raamatuid tellida ja e-koolis oma rübliku õpitulemustega tutvuda, kuid teisest küljest saab seda ära kasutada ka kurjadel eesmärkidel: planeerida terroriakte, äritseda illegaalsete narkootikumidega ja pidada sõnumivahetust, mis muul moel ei allu kas seaduste või ühiskonna kõlblusnormidele. Mõistagi tundub seetõttu eri osapooltele, et neil on õigustatud huvi sõnumisaladust väärata. Lubagu seda siis Bob, Jumal või riigiaparaat.

“Aga Whitfield ja Martin koos Roni, Adi ja Leonardiga, kes leiutasid avaliku võtme krüptosüsteemi, millele panid kõrgelennulist fantaasiat rakendades oma perekonnanimede esitähtede järgi nimeks RSA, on ju juba pea 40 aastat meie sõnumisaladust edukalt kaitsnud?” Jah, on küll, aga…

40 aastat on pikk aeg. IT-maailmas pea igavik. Vahepeal on mõnedest krüptograafiliselt ränkraskeks peetud probleemidest saanud lahendatavad probleemid (slaid 66). Samuti osatakse tarkvara arendamisel tehtud vigu järjest tõhusamalt ära kasutada selliste eesmärkide saavutamiseks, mida tarkvara looja ette ei näinud – näiteks sõnumisaladuse vääramiseks. Rääkimata riiklikest huvidest, mis on samuti eri intensiivsusega mõjutanud tugevate krüptoalgoritmide kasutamist.

Katkised kastid

Üldiselt ei jää haavatavaid krüptoteostusi aja jooksul vähemaks, vaid neid luuakse üha juurde. Sageli mitte pahatahtlikult ega isegi teadlikult. Krüptograafiliste funktsioonide programmeerimine nii, et lõpptulemus oleks tõesti turvaline, on keeruline. Paraku on suur osa tänasest infotöötlusest ja andmevahetusest seotud ühel või teisel moel krüptograafiaga, mis tähendab, et seda tuleb moel või teisel rakendada pea kõigil riist- ja tarkvaraliste lahenduste loojatel. Arvestades seda, kui palju on erinevaid tootjaid ning kui suur on konkurents, ei ole vist kuigi suur üllatus see, et krüptograafias ja selle rakendatuses tõeliselt pädevaid spetsialiste lihtsalt ei jätku kõikjale ja/või on nende teenuse kasutamine oma rakenduste loomisel liiga kallis. Nii luuakse lahendusi, mis on kombinatsioonina teadmatusest, kulude kontrolli all hoidmisest ja kiirustamisest (ning teatud määral ka hoolimatusest) auklikud.

Nagu 2014. ja 2015. aasta on näidanud, pole peamine probleem krüptoalgoritmide matemaatilises tugevuses, vaid selles, kuidas need on reaalsuses rakendatud. Heartbleed, FREAK, LogJam – vaid mõned näited sellest, kuidas rakendused on katki, kuigi selle aluseks oleval krüptoalgoritmil pole iseenesest suurt viga midagi. Nii tulebki pidevalt hoida silmad ja kõrvad lahti ning käed tegutsemisvalmis, et kui järjekordne „haartbliid“ välja kargab, asuda aktiivselt süsteeme paikama ning uusimaid rakendusversioone installeerima.

Valmis peab olema ka selleks, et teatud haavatavuste parandamine võib mõnedes seadmetes olla kas väga keeruline või isegi võimatu. Sellisel juhul aga tuleb vastu võtta raske otsus ja taoliste seadmete

kasutamisest loobuda. Katkiste kastide kasutamine on võimalik ainult juhul, kui selle omanikku ei häiri asjaolu, et andmed kastist pidevalt väljapoole lekivad, mis võib tähendada teistpidi seda, et leket pealt kuulaval pahalasel tekib võimalus ka kastis sees olevaid andmeid muuta. Sisuliselt on väga keeruline ette kujutada Internetti ühendatud masinat, mille puhul omanikul oleks täiesti ükskõik, kes ja kuidas seda enda huvides kasutab. Ei tasu endale luua pettekujutelmi: katkiste kastide puhul just selline olukord valitseb. Infosüsteemide haldajad peavad harjuma olukorraga, kus nende vahendid on alati haavatavad, aga samas peavad nad oma kasutajaid kaitsma paremini kui seni.

Tervikluskadu >> teenus on maas

Tarkvaras võidakse selliseid vigu leida sisuliselt üleöö. Tagajärjeks on vähemalt konfidentsiaalsuse kadu, aga teatud juhtudel ka kontrolli kaotamine kastide ja nendes olevate andmete üle (käitluskadu, tervikluskadu). Kõige lihtsam on, kui mõni kast lihtsalt lakkab töötamast ehk teenus kukub maha. See on kohe silmaga näha ja käega katsutav, mis tähendab, et küllalt kiiresti on viga teada ja saab hakata seda parandama. Palju keerulisem lugu on aga siis, kui löögi alla on sattunud andmete terviklus. Sellisel juhul on viga palju varjatum: kast ju töötab, kõik teenused on püsti. Aga see, millise aja jooksul keegi suudab avastada, et andmed, mida kastis käideldakse, pole päris õiged, sõltub juba sellest, kui kavalalt on pahard osanud nendega manipuleerida.

Jõhkraid näiteid saab konstrueerida meditsiinivaldkonnas: kui patsiendi andmed pole kättesaadavad (käitluskadu), tuleb arstidel, õdedel uuesti võtta vereproovid ja teha patsiendiga muid toiminguid ning raviks vajalikud andmed suudetakse üldjuhul taastada. Kui patsiendi andmed (näiteks veregrupp, analüüside tulemused, arsti määratud ravidoosid vm) on aga salaja muudetud, võib see välja tulla alles siis, kui patsiendi tervislik seisund on oluliselt halvenenud. Sama analoogiat saab üle kanda aga paljudele teistelegi valdkondadele: elektritootmine ja -ülekanne, veevarustus, kanalisatsioon, liiklusfoorid, radari- ja relvajuhtimissüsteemid jms. Katkised kastid on probleem pea igal pool, kuhu IKT oma kombitsad laiali on ajanud. Ja nagu me teame, on ta need Eesti-suguses infoühiskonnas ajanud praktiliselt kõikjale…

Liiga tugev krüptograafia?

Krüptograafiliste algoritmide puhul aga ei leita vigu üldiselt ootamatult. Nende murenemine käib vaikselt, tasahilju, kuid mitte magamistoas teki all, vaid heledalt valgustatud kontorihoonetes, kus toimetavad nimetud kavalpead, kel ülesandeks terrorismi või muu kuritegevusega võidelda. Ja tõesti, suure ressursiga saab liigutada mägesid ning murda krüptot (vähemasti teatud maani). See, kas pingutused (ja kulutatud raha) ka siis midagi väärt on, kui tehtud töö tulemusi on mõni kaasosaline valmis mingil põhjusel avalikustama ja/või mõnele muule suurvõimule üle andma, on eraldi teema.

Väidetavalt Edward Joseph Snowdeni varastatud ning viimase kahe aasta jooksul poliitiliselt sobivatel hetkedel eri allikate avaldatud teave on ühiskonnas tekitanud uusi küsimusi, millele maailmas selgeid avalikke vastuseid veel pole. Kuivõrd Eesti on aga digiarengutelt avangardis, võib juhtuda, et vähemalt osad vastused neile küsimustele peavadki tulema meilt.

Kuidas mõjub sõnumisaladuse tagamiseks ning digitaalallkirjade tervikluse tõestamiseks kasutatavate meetodite usaldusväärsuse kangutamine demokraatiale, meie e-ühiskonnale üldisemalt? Põhineb me e-eluviis ju sõnumisaladusel, andmete terviklusel ning elektrooniliste kanalite usaldatusel. On väga kaheldav, kas Eesti riik on jätkusuutlik juhul, kui kodanike usaldus e-eluviisi vastu peaks lakkama. E-eluviis tagab efektiivsuse ja kulude kokkuhoiu, mis võimaldab riigil pakkuda avalikke teenuseid selle kõige laiemas mõttes. Avalikud teenused on aga ainus riigi olemasolu põhjus ja põhjendus. E-eluviisi suhtes langeva usalduse tagajärjel peaksime tagasi minema paberi ja pliiatsi, büroohoonete ja letiteeninduse juurde. See kõik on aga väga kallis ning vajab kogu seni ehitatu lammutamist ja hoopis teisel moel ümber ehitamist. Kui riik ei suuda kodanikele õigeaegselt kõiki vajalikke avalikke teenuseid pakkuda, langeb kodanike usaldus riigi vastu ning suureneb vastuvõtlikkus võõrvõimu suhtes, kes on valmis ise avalikke teenuseid tulema osutama. Usaldusega ei tohi seega mängida!

Nõrk krüpto pole Eesti huvides

Siin- ja sealpool suurt lompi esitatakse viimasel ajal üha enam mõttekäikusid, mille kohaselt võiksid kasutatavad krüptolahendused sisaldada teatud nõrkusi või tagauksi. See tagaks justkui riigiaparaadi võimekuse võidelda terrorismi ja muu kuritegevusega, kuna võimaldab pealt kuulata pahalaste omavahelist suhtlust. Taoline käsitlus ei sobi kuidagi kokku Eesti e-eluviisiga, kuna õõnestab selle aluseks olevat usaldust e-lahenduste vastu. Ka riiklikult sanktsioneeritud nõrkused ja tagauksed on kokkuvõttes sellised, mis muudavad lahendused väheturvaliseks tervikuna. Pole mõtet petta end lootusega, et kontroll mingisuguse nõrkuse üle jääb ainult riigi valdusesse. Paraku võib kohe, kui tagauks avaneb võõrvõimule või kurjategijatele, kogu senise e-eluviisi korstnasse kirjutada. See tähendaks sisuliselt kogu Eesti riikluse küsimuse alla sattumist.

Samuti pole mõtet loota, et need, kelle tõttu üldse vastavaid nõrkusi tuleb justkui juurutada (kurjategijad, terroristid, üldiselt halvad inimesed), vastavaid nõrkasid krüptolahendusi kasutaks. Me ei ela enam 20. sajandil, kui info liikumist oli võimalik suhteliselt hõlpsalt ohjata ja seega oli ka võimalik omada teatud ulatuses riiklikku kontrolli selle üle, kes millist krüptolahendust on võimeline kätte saama ja seda kasutama. Võib olla täiesti kindel, et tegelikult ühiskonnale ohtlikud inimesed on piisavalt organiseeritud selleks, et leida krüptolahendused, millel poleks riigi poolt sokutatud tagaust sees ning nagu kipub kõiksugu piirangute puhul juhtuma, on peamiseks kannatajaks ikka tavaline keskmine seadusekuulekas kodanik.

Eesti riigi ja Eesti kodanike vahel on tänaseni kokkulepe, et üksteist usaldatakse ja e-eluviisi aluseks olevate rakenduste turvalisust tagatakse heas usus nii hästi kui võimalik. Kodanikud usaldavad riiki ja riik kodanikke. Kurjategijate tabamiseks ei seata ohtu kõigi kodanike heaolu ega omariiklust. Vastastikuse usalduse murd(u)misel muutuks meie riik. Ja seda üsna drastiliselt – elektrooniline identiteet, X-tee, turvalised pangateenused, i-valimised, hõlbus tulude deklareerimine ja kõik muu, mida me ise enam tähelegi ei pane, on nagu kõrge viskoossusega õli väga hästi timmitud ralliauto mootoris. Ja selle õlita me rallit ei sõida. Võib-olla teised riigid, kellel taolist ralliautot e-ühiskonna näol veel arendatud pole, saavad endale ühiskondlikku madalamat usaldust lubada, aga meie ei saa.

Krüptouuring

Õnneks tegeletakse krüptograafiliste algoritmide aluseks olevate raskete probleemide lahendamisega ka mitte-salajastes uurimisasutustes. Nendelt uurijatelt pärineva teabe põhjal saame ennustada, millal mõne krüptograafilise algoritmi eluaeg lõpeb, et siis selle teabe põhjal e-riigi usaldusväärsuse aluseks olevates süsteemides õigeaegselt muudatusi teha. Kui me krüpto murenemisega sammu ei pea ning ID-kaarte, seotud seadmeid, tarkvara jms õigeaegselt välja ei vaheta, võib meie e-riik oma e-eesliite kaotada ka tehnilistel põhjustel.

Seetõttu peame riigina lisaks rahvusvahelistele poliitilistele tõmbetuultele hoolikalt jälgima ka krüptograafia enda arenguid ning krüptograafiliste algoritmide ja nende teostuste uurimise tulemusel selguvaid nõrkusi ning vajadusel tegema selle teabe põhjal Eesti jaoks oluliste infosüsteemide puhul kiireid ja radikaalseid otsuseid. Kui peaks selguma, et mõni krüptoalgoritm on murdumisohus, peame suutma selle kasutamise lõpetada enne, kui seda nõrkust meie riigi või meie kodanike vastu ära kasutatakse.

Just selliste probleemide avalikuks teadvustamiseks ja võimalike probleemide ennetamiseks koostasime juba kolmandat korda (varem 2011 ja 2013) krüptograafiliste algoritmide elutsükli uuringu, mida soovitame kõigil huvilistel kindlasti lugeda.