Erki Suurjaak
LAP31
970772

Operatsioonidesüsteemide referaat

IEEE Computer Society liikmete arvamused krüptograafia kohta

Aprillis viidi Computer Society liikmete seas läbi küsitlus turvalisuse ja privaatsuse teemal. Küsitlus näitab CS liikmete arvamusi Ameerika Ühendriikide valitsuse rollist krüptograafiaalases uurimistöös ning krüpteerimise ja e-kaubanduse vahelisest suhest. Üldiselt on liikmete seas selgelt näha vastuseisu valitsuse püüetele krüptograafiat enda kontrolli all hoida.

Tagamaadest

Ameerika Ühendriikide valitsus püüab hoida krüptograafia levikut, arengut ja kasutust range kontrolli all. Põhjuseks on see, et riiklikel agentuuridel (CIA, FBI, NSA) on vaja jälgida teatud inimeste (kurjategijate või potentsiaalsete kurjategijate) omavahelist kommunikatsiooni. Kui neil inimestel on võimalus kasutada krüptograafiat, mida valitsus ei kontrolli, siis on agentuuridel põhimõtteliselt võimatu kättesaadud krüptogramme dešifreerida. Seega on valitsus sõltumatu krüptograafia vastu. Arusaadavalt tekitab selline seisukoht privaatsektoris pingeid.

Valitsusest

Valitsused ei suuda eriti hästi kontrollida krüpteerimistehnoloogia levikut kõrgelt motiveeritud kasutajate, näiteks teiste maade sõjaliste valitsuste, organiseeritud kuritegevuse, terroristide või eriliselt oma informatsiooni kaitsmisest huvitatud eraisikute seas. Mida valitsused aga suudavad teha, on aeglustada krüpteerimistehnoloogia sulandumist igapäevasesse kasutusse regulatsioonidega ja takistada selle tehnoloogia kerget sisseehitust tavaliste seadmete, nagu telefonide või e-posti tarkvara juures.

Ainult väga väike osa küsitletutest leidis, et valitsus peaks kontrollima krüpteerimistehnoloogiate levikut - see hakkab takistama tehnoloogia arengut. Pealegi oleks sel juhul garanteeritud varituru tekkimine, kuna seadust mittejärgivad inimesed nagunii kasutavad, mida tahavad, nii et piirangud avaldaksid mõju üksnes seadusekuulekatele inimestele. Krüptotehnoloogia arengu piiramine ei tule ka kasuks riiklikule turvalisusele, sest krüpteeritud kommunikatsioon teeb arvutisüsteemid turvalisemaks. Piirangud takistavad korralike krüpteerimisstandardite väljatöötamist ja majandus ei oleks siis enam turvaline. Tuleks edendada ülemaailmse krüptograafilise uurimistöö avalikustamist, nii et ükski maa ei saaks seda kasutada ülekaalu saavutamiseks, tuleks jätkata ülikoolide krüptograafiaalaste uuringute toetust ja koostada uurimisprogramme, mis tooksid kõikide poolte teadlased kokku.

Üldse arvati, et valitsus ei tohiks krüpteerimistehnoloogiate eksporti piirata. Igasugune ekspordiseadus peaks laskma firmadel äri ajada nii ekstensiivse krüpteeringuga, kui nood end konkurentide eest kaitsmiseks vajavad. Pealegi, Ameerika Ühendriigid ei ole ainuke maa, kus krüptograafiat arendatakse (kuigi on tõsi, et ta on

kõigist teistest maadest ees) ja suures plaanis selle tehnoloogia ohjeshoidmine riiklikku turvalisust ei kaitse. Riiklikud agentuurid peavad ise hakkama saama.

Kaubandusest

Kui kaubanduse definitsiooni kaasata ka "elutähtsa informatsiooni edastamine" (näiteks finants-, meditsiini- või kindlustustööstuses), siis saab Internetti kasutada ainult siis, kui on kindlustatud, et tähtsat informatsiooni võib lugeda ainult saatja ja adressaat. Firmad leiavad, et neil on moraalne kohustus tagada nende klientide informatsiooni turvalisus nii hästi kui võimalik. Ainus viis seda teha on tagada efektiivne krüpteerimine. Firmad suudaksid seda tagada, sest privaatsektoris ei jääks krüptograafia areng kunagi seisma. Ajad, mil ainult valitsused krüptograafiast midagi teadsid, on ammu möödas, ja isegi tundub, et valitsustel ei ole privaatsektorile midagi kasulikku anda. Kõik näitab hoopis, et nad on tööstusringkondadest maas. Näiteks leiti Suurbritannia valitsuse võtmehoiustusprotokollis ränkasid kujundusvigu. Ja Clipper-protokollis avastati vägagi tõsiseid möödalaskeid ja mõtlematust (Clipper on NSA poolt aretatud telefonikommunikatsiooni krüpteerimissüsteem. Võtmeid haldas valitsus ja spetsiaalse kiibi - "Clipper-kiibi", mida kavatseti igasse uude telefoni installeerida - abil võis valitsus kõnesid pealt kuulata). Ning katse juurutada Briti National Health Servive'is võtmehoiustuskrüptograafiat lõppes sellega, et tehnika vedas alt ja kogu operatsiooni üritati kinni mätsida.

Küsitlusel selgus, et enamus küsitletuist leiab, et eksporditavate või vabal turul müüdavate krüpteerimiskoodide tugevust peaks määrama turunõudlus, mitte valitsus või krüptograafiateadlased. Internet ei saa kunagi turvaliseks kanaliks rahvusvahelisele kaubandusele, kui hakatakse krüpteerimise efektiivsust piirama. Kui üldse tahetakse kunagi luua turvalist ülemaailmset elektroonilist infrastruktuuri, siis peab laskma krüptograafial piiramatult areneda. Valitsus võiks koguni praeguseid pidevas rünnakuohus olevaid krüpteerimistehnoloogiaid aitama olla vastastest üks samm eespool. Aga küsimus, kas oleks võimalik nii garanteerida riiklikku turvalisust kui lasta krüptograafial vabalt areneda, tekitas lahkarvamusi - pooled arvasid nii, pooled naa. Üldiselt võis selgelt näha vastuse geograafilist sõltuvust - üle poole Ameerika Ühendriikides asuvatest inimestest vastasid jaatavalt. See on ilmselt seletatav Ühendriikides elavate inimeste vastumeelsusega valitsuse kontrolli suhtes.

Oli huvitavaid ettepanekuid kahe turvalise infosüsteemi (valitsuse ja kaubanduse) kooseluks - kas krüpteerida kõik riiklikku turvalisust puudutav informatsioon eraldi koodiga, mida ei saa dubleerida; või kasutada kahte erinevat krüpteerimisliiki : üks valitsusele, teine kaubandusele või jagada Internet kahte ossa - OpenNet ja SecureNet. Viimast haldaks peale valitsuse veel mingi organisatsioon (näiteks National Science Foundation).

Oktoobris jõustus Euroopa Ühenduse Andmekaitsedirektiiv. See kohustab EÜ liikmesmaid reguleerima isikliku informatsiooni töötlemist. Antud sättel võib olla tähtsaid kaubanduslikke tagajärgi firmade jaoks, kes koguvad klientidelt ja töötajatelt Euroopas personaalset informatsiooni ja levitavad seda EÜst väljapool. Paljud Euroopa kaubanduspartnerid, nagu Ameerika Ühendriigid, Kanada, Jaapan ja Austraalia, peavad vajalikul määral tagama isikliku informatsiooni turvalisuse. Ilma vastava seadusandluse

või muude üksikisiku privaatsusõigusi kaitsvate mehhanismideta maad ei taga adekvaatset turvalisust. Seega kui krüptograafiat rangelt reglementeerida, kannatab selle all Ameerika Ühendriikide välismajandus.

On mitu viisi, kuidas tänapäeva arvutisüsteemide turvalisust parandada. Võib häiremehhanismina jälitada iga krüpteeritud informatsiooni voolu kuni allikani; võib kasutada allikast sihtpunktini viivaid kontrolljälgi, et teha kindlaks teadete saatjaid; võib tabada kahtlasi teateid kas allika juures enne kinnikrüpteerimist või sihtpunktis peale lahtikrüpteerimist. Võib suurendada karistusi krüptograafia kasutamisel seadusevastases tegevuses, selle asemel et krüptograafiat piirata; võib keskenduda infoühiskonnas teistele tehnoloogiatele ja võimalustele; võib viia läbi krüpteeritud kommunikatsiooniteenuste pakkujate range litsentsimine; või teha krüptograafiauurijad turvalisuse eest vastutavaks. Sest efektiivset šifreerimise levikut enam kontrollida ei saa. Valitsuse võiks suurendada toetusi krüptograafiauuringuile, hoides sedaviisi algoritmid koodimurdjatest ühe sammu eespool. Samuti võiks kohustuslikuks teha krüptograafiliste algoritmide registreerimise valitsuse juures. See oleks midagi võtmetaaste ja mittereguleerimise vahepealset.

Võtmetaastesüsteem on tänapäeval kõige levinum ja populaarsem krüpteerimisviis. See on kergelt mõistetav, lihtsasti kasutatav ja jätab võimaluse hädaolukorras krüptogramm dešifreerida. Tööandjatele annab see võimaluse oma töötajate tegevusi jälgida. Samuti sobib see valitsusele, kes püüab juurutada enda poolt jälgitavat ja hallatavat süsteemi. Võimalusi võtmetaastesüsteemi rakendada on mitu. Võib kasutada ühte võtmetaastesüsteemi ainult ühe firma piirides; anda võti ainult neile, kes on valmis võtme kaotsimineku või varguse korral tekitatud kahju hüvitama; või kasutada tsiviilkohtusüsteemi poolt hallatavat võtmehoiustussüsteemi, mis annab võtme vaid siis nõudjatele välja, kui tõestusmaterjal selgelt näitab, et see on õigustatud; või siis annab valitsus tarbijatele võtmed ja tehnoloogia tasuta ning seejuures on rangelt sätestatud valitsuse vahelesegamine ja jälgimine.

Küsitletud spetsialistid võtmetaastesse eriti hästi ei suhtunud. Leiti, et võtmetaastesüsteemid teevad valitsusele krüpteeritud info ilma loata valdamise liiga lihtsaks, samuti ei ole võtmetaastesüsteemid üldsegi tõhus viis võimaldada kohest seaduslikku dekrüpteerimist ilma turujõude segamata. Võtmetaaste või võtmehoiustus looksid vaid turvalisuse illusiooni, ainult igasuguste piirangute kaotamine sunniks valitsust ja organisatsioone arenema ja vaatama teiste tehnoloogiate poole.

Kokkuvõte

Seadusandjad ja kaubanduslikud organisatsioonid on püüdnud valitsuse ja tööstuse krüpteerimisalastest erimeelsustest üle saada. Valitsused tahavad seadusi täide viia ja kaitsta riiklikku turvalisust., aga ei saa kummagiga eriti hästi hakkama. Firmad tahavad ise otsustada, milliseid tooteid millistel turgudel müüa, ja nende innukus krüptograafia arendamisel oleks jätkuv ja jääv. Ilmselt ja loodetavasti nihkub asi selles suunas, et krüptograafia arengu ja vaba leviku piiramine lõpetatakse.

Kasutatud materjal :

"Members React To Privacy and Encryption Survey", Computer, september 1998

Tänusõnad

Vello Hansonile abi eest paari krüptograafiaalase termini tõlkimisel.