E-Valimiste Projekt

E-valimiste turvalisus — krüptograafi vaatevinkel

Helger Lipmaa
Helsinki University of Technology
helger@tcs.hut.fi

Ülevaade ettekandest

- E-valimised — turvamehe vaatevinkel
- Põhilised mured
- Lahendused (kui on)
- Ettepanekud
- Avatud küsimused

E-valimised: valimised uuel meedial

- Meedia: Koduarvutid, Internet, keskserverid
- Osa üldisest protsessist “tava-X” $\rightarrow$ “e-X”
  - Veel protsesse: sularaha, oksjonid, laenutamine, . . .
- Aastasadade või -tuhandete jooksul välja kujunenud protseduurid üritakse kanda digitaalsesse keskkonda . . .
- . . . mõne aastaga
- Tekivad probleemid, mille lahendamiseks on vaja kulutada inimaastaid, ning kasutada ära teiste riikide kogemusi

- *Samas saab e-teel ka suurendada turvalisust*

Põhilised mured 1: Usability

- Inimesed on harjunud vanade protseduuridega
- Nad teavad kuidas need töötavad.
- Uued protseduurid vajavad harjumust, ja ümberõpet.

Märkus: tegu ei ole murede tähtsusjärjekorraga.

Põhilised mured 2: Turvalisus

- Aastasajad tavalisi valimisi (jms) on välja toonud erinevad puudused vastavates protseduurides
- Riigid ja inimesed on, kuigi aeglaselt, võtnud omaks järjest enam meetmeid nende protseduuride turvamiseks
- E-protseduuride turvalisust on küll uuritud krüptograafide poolt, kuid vaid viimase 25 aasta jooksul

Põhilised mured 2: Turvalisus

- Puuduvad suuremastaabilised kogemused e-valimiste alal, pole teada, millised krüptograafide poolt oluliseks peetud turvakriteeriumid on ka praktikas olulised

- Kogemus näitab, et parem karta kui kahetseda — e-protseduurid tuleb teha võimalikult turvaliseks, vastasel korral on karta nii ründeid mis võivad nurjata e-valimised tehniliselt, kui ka kriitikat mis võib nurjata e-valimised poliitiliselt.

Põhilised mured 3: Turvalisus + Usability

- *Valdavalt* inimesed teavad, kuidas käituda selleks, et vanad protseduurid töötaksid
- Kui nemad ei tea, on olemas nõunikud ja/või vastava koolituse saanud spetsialistid, kes seda teavad
- Teadagi arvutite turvaline kasutamine käib enamus inimestele üle jõu

Nõuded: Usability

Usability pole minu eriala, kuid e-protseduur *peab* olema

- Turvaline. Piisavalt turvaline, et sellega jääksid rahule erinevad sõltumatud spetsialistid nii Eestist kui välismaalt. Ainult nii saab garanteerida usalduse selle vastu

- Lihtne auditeerida. Inimene ise ei pea aru saama, miks protseduur turvaline on, kui Eestis on olemas rohkem kui 4 (pigem 40) spetsialisti, kes suudavad turvalisust iseseisvalt sertifitseerida

- Lihtne kasutada enda turvalisust ohtu panemata.

- Üldkättesaadav ja ikkagi turvaline.

Lahendused: Usability — kirvereeglid

- E-protseduur peab olema turvaline (vt järgmisi slaide) ja samas lihtne kasutada
- E-protseduur peab olema piisavalt lihtne, et olla auditeeritav 0.01% elanikkonna poolt (Eestis siis 150 inimest).
- *Algusest peale tuleb rõhku panna turvalisusele, lihtsusele*

Usability — soovitused, veel

- Regulaarsete seminarid e-valimiste protseduuri väljatöötamise jaoks, kus haritakse ka turvapoolt mittetundvaid kodanikke. Usalduse tagamiseks peaksid seminarid olema avalikud

- Pärast protseduuride väljatöötamist peab tekkima tuumikrühm, kes täielikult valdab protseduuride siseelu, ning oskab neid ka õpetada.

- Seejärel tuleb korraldada (pool)avalikke kursusi e-valimiste alal. Riigi teenistuses peab olema vähemalt 2–3 e-valimisi põhjalikult tundvat (mitte ainult) IT-spetsialisti. Tagatud peaks olema ka järelkasv tudengite näol, kes tulevikus vastavale riigitööle võiks asuda, või tööle erafirmadesse, kes osutaksid e-valimisalaseid teenuseid või konsultatsioone.

Mured: turvalisus

- E-valimised kasutavad uut meediat: valimisplatvorm + võrk + keskserverid
- Valimisplatvormi (koduarvuti? mobiiltelefon? pihuarvuti?) kasutatakse valimiste jaoks.
- Hääled kanduvad üle võrgu (Internet/GPRS/GSM/CDMA/. . .)
- Hääled loetakse kokku keskserveris (või serverites)
- *Süsteem ei ole turvalisem kui tema kõige turvalisem lüli*

Turvalisus: koduarvutid

- Valimisplatvorm on küll näiliselt inimeste enda “kontrolli” all, kuid tegelikkuses on kõige raskemad turvaprobleemid just siin
- Platvormi turvalisus sõltub sellest, kas saab usaldada operatsioonisüsteemi tootjat, erinevate rakendusprogrammide tootjat, kas arvutit saab rünnata väljaspoolt (erinevad ussid, viirused, trooja hobused)
- Ideaalis peaks olema tegu platvormiga, mida ei saaks rünnata, ning milles olevaid programme me saaksime usaldada

Turvalisus: valimisplatvorm

- PC + Windows: pidev turvaauk. (Cf. hiljutine Blaster uss.) Kuna operatsioonisüsteemi koodile puudub ligipääs, ei saa seda ka auditeerida. Ühelegi teisele platvormile pole ka nii palju viiruseid.

- Macintosh: parem, kuid mitte palju. Enamuste rakenduste koodile pudub ligipääs; viirusi on vähem, kuid oma rolli mängib siin ka platvormi vähene levi. Miinuseks on hind.

- PC + Linux: kood on kättesaadav, seda võivad auditeerida paljud. On olemas “turvalised” Linuxi distributsioonid, mida võib eriti usaldada. Miinuseks on Linuxi vähene kasutajasõbralikkus ning ka see, et inimesed lihtsalt ei tunne seda.

Turvalisus: valimisplatvorm

- Mobiil (laaditavate rakendustega, ntks Nokia 3650): hetkel vähelevinud platvorm, mis mõne aasta pärast võib muutuda aga üldlevinuks. Lähtekood pole kättesaadav, samuti pole teada eriti turvalisuse kohta, kuna tegu on uue platvormiga. Samas hõlbus kasutada ja pidevalt käejuures ning võrgus.

- PDA — Eestis mitte väga levinud. Hõlpsam kasutada kui mobiil, Palm on kauem tuntud kui ntks Nokia Series 60 ja tema turvalisusest teatakse rohkem. Enamus PDA-sid pole otse võrgus.

Turvalisus: võrk

- Võrk ei ole ei valijate ega riigi kontrolli all (väga hea!), seetõttu tundub, et tegu on kõige nõrgema lüliga
- Tegelikkuses on võrk turvalisim lüli: Enamus ründeid võrgus saab vältida turvalise krüptograafia kasutamisega
- Ainsaks (suureks) mureks on teenusetõkestuse (DoS) ründed — mis juhtub, kui valijate hääled lihtsalt ei jõua kohale
- DoS võib ka juhtuda valimissüsteemi ebaotstarbeka ülesehituse korral, selleks pole vaja ründajaid — kes poleks teist üritanud saata SMSi uusaastaööl, sama kogemus võib ees oodata valimispäeval.

Turvalisus: keskserver

- Keskserver(id) on riigi kontrolli all. Riik saab palgata endale spetsialiste, kes auditeerivad servereid, ning veenduvad nende turvalisuses
- Privaatsus: riigi kontrolli all olemine tähendab ka seda, et triviaalsete lahenduste korral teab riik (või riigi IT-spetsialistid) täpselt, kes kelle poolt hääletas. Sabotaaž, . . .
- Korrektsus: Riik (või keegi teine) saab muuta ka kontrollimatult häälte väärtusi. See muudaks valimised ebalegitiimseks

Lahendused: valimisplatvorm

- Linux (või OpenBSD, ntks) on parim platvorm, kuid inimeste jaoks võõras
- Lahenduseks oleks uniformsete CD-de tootmine, kus oleks peal minimaalne turvaline Linuxi konfiguratsioon koos e-valimistarkvaraga
- CD oleks “buuditav”, mittekirjutatav meedium, seega saaksid kasutajad olla kindlad, et nende platvorm on turvaline
- Tarkvara peaks olema lihtsalt kasutatav (fakti, et tegemist on Linuxiga, saab ideaalsel juhul peita), ilma kellade ja viledeta, juhendid selle tarkvara käsitsemise kohta peaksid olema üldiselt kättesaadavad

Soovitatud variandi probleemid

- CD-de turvaline ja ülerahvuslik distributsioon
- Tarkvara enda turvalisus ja auditeeritavus. Õnneks on Linuxi-auditeerijaid Eestis rohkem kui krüptograafe
- Linuxi distributsioon peaks sisaldama tuge kõikide erinevate võrgukaartide jms asjade jaoks. See võib ohtu seada valimiste üldisuse, kui CD-ga just mingit standardset, odavat, võrgukaarti kaasa ei anta. (Tarkvara võib olla tekstirežiimis, kaotaks vajaduse hiire ja graafikakaartide toetuse järgi.)
- ID-kaart + Linux — pole näinud, et töötaks

Lahendused: valimisplatvorm, alternatiivid

- Alternatiivsete platvormide olemasolu — signeeritud rakendused mobiiltelefonidele, jms?

- ?

Lahendused: võrk

- Kõik andmed üle võrgu peavad liikuma krüpteeritult ja audenditult
- Suuremastaapsete teenusetõkestamise rünnete vastu aitab ainult valimisperioodi pikendamine ning dubleeritud valimisserverite olemasolu erinevate Eesti ISP-de tegualas
- ?

Lahendused: keskserverid

Valimisprotokollid peavad olema sellised, et

- Ei riik (kes kontrollib kõiki servereid) ega (ühte, kahte, kolme. . .) keskserverit kompromiteerinud ründaja saaks teada üksikhääletajate eelistusi

- . . . ega muuta antud hääli

Keskserverid, 1: Dubleerimine

- Servereid peab olema rohkem kui üks
- Iga server peab olema hallatud sõltumatu osapoole poolt (erinevad parteid, Teaduste Akadeemia, Muinsuskaitse Selts, ülikoolid, kodanike ühendused)
- Protokollid peavad olema disainitud selliselt, et kui vähemus serveritest on korrumpeerunud, siis ei ole rikutud ei privaatsust ega korrektsust
- *Küsimus: kas see on poliitiliselt reaalne nõue? Kas meil on piisavalt sõltumatuid osapooli?*

- Krüptograafiliselt oleks see võimalik

Lühike krüptograafiline diskursus ja narratiiv

- Vähemefektiivne: “mix-net”
- Efektiivsem: homomorfne krüptograafia

Mix-net: häälte kogumine

- Krüpteeritud ja autenditud hääled kogutakse kokku dubleeritud kogumisserverite poolt
- Iga valija saab oma häält muuta, kui ta soovib
- Kogumisserverid saadavad andmed edasi mix-serveritele
- Kogumisserverid ei oska dekrüpteerida!

Mix-net: häälte miksimine

- Mix-server 1 võtab hääled, järjestab need ümber ja “pimendab”. Tulemuseks saab ta samad hääled, kuid erinevas järjekorras, nii et pole võimalik kindlaks teha, kellele antud hääl kuulus

- Mix-server 1 kirjutab oma väljundi üldiselt loetavasse kohta, koos tõestusega, et ta käitus korrektselt (“nullteadmustõestused”). Igaüks võib tõestust kontrollida. (Võimalik kuid aeganõudev)

- Seejärel teevad sedasama kõik ülejäänud serverid

Mix-net: Pilt

Salajane ümberjärjestamine	Mix-Server 1
Salajane ümberjärjestamine	Mix-Server 2
Salajane ümberjärjestamine	Mix-Server 3...n-1
Salajane ümberjärjestamine	Mix-Server n

Mix-net: häälte dekrüpteerimine

- Pärast miksimist näevad kõik miksimisserverid krüpteeritud hääli mingis järjekorras
- Nad saavad veelkord kontrollida, et miksimine oli tehtud korrektselt *ilma leidmata*, kuidas mingi server miksis
- Pärast kontrolli dekrüpteerivad mix-serverid lõpphääled üheskoos, saades teada häälte statistika, kuid mitte selle, kuidas keegi täpselt hääletas
- Siin kasutatakse *läviusaldusega krüptograafiat*, kus krüpteerimine on nagu krüpteerimine ikka, aga dekrüpteerimiseks peavad osalema vähemalt pooled n serverist

Mix-net: turvaomadused

- Iga serveri mitte-miksimist saab tuvastada, ja tema seejärel eemaldada
- Kui vähemalt 1 server kustutab ära andmed oma miksimise detailide kohta, pole pärast võimalik taastada seost häälte vahel enne tema ja pärast tema teostatud miksimist, v.a. juhul kui ründaja teab enamuse serverite salajasi võtmeid
- Kui enamus serveritest kustutab ära oma salajased võtmed, pole pärast seda enam võimalik dekrüptida vahepealseid hääli ja seega muutub skeem täielikult privaatseks juhul kui eelmine punkt on täidetud
- Täiendav turve: hoida võtmeid riistvaras vms

Diskursus 2: Homomorfne krüptograafia

- Krüptosüsteem on selline, et a ja b krüpteerimise tulemusel saadud krüptogramme kokku korrutades saadakse summa $a+b$ krüptogramm

- E-valimiste idee (lihtsustatud): iga hääletaja saadab oma hääle krüptogrammi kogumisserveritele, serverid korrutavad krüptogrammid kokku, saavad häälte “summa” krüptogrammi.

- Viimane edastakse dekrüpteerimisserveritele koos tõestusega, et tegu on korrektse käitumisega. (Tavaliselt kogumisserverid = d-serverid.) Tõestused lähevad läbi kui enamus kogumisserveritest on ausad.

- Kui vähemalt pooled d-serveritest teevad koostööd, saavad nad dekrüpteerides kätte häälte “summa”

Homomorfne krüptograafia — turvaomadused

- Funktsioneerimiseks on vaja enamuse koostööd
- Privaatsus ja korrektsus on tagatud kui enamus serveritest on ausad — ei krüpteeri üksikuid hääli vaid ainult nende summat.
- . . . ning kustutavad oma salajased võtmed mingi aja möödudes.

Võrdlus

- Mix-net (täpsemalt): privaatsus on tagatud juhul kui enamus serveritest dekrüptib ainult lõplikke hääli ning kustutab hiljem oma salajased võtmed.

- Homomorfne krüpto: sama!

- Homomorfne on tavaliselt efektiivsem

Mõtlemiseks: Randomized Response Technique

- Tuntud statistiline võte selleks, et toimetada sensitiivseid küsitlusi (kas te olete poes varastanud?)
- Inimene ei vasta enamasti õieti, kui ta võib pärast seda oodata “aktsioone”
- RRT idee: inimene vastab valesti *teatud* tõenäosusega
- Pärast seda saab küsitleja teada suure täpsusega häälte “summa”, kuid iga üksiku hääletaja hääle teadasaamine on statistiliselt lootusetu

Randomized Response Technique, näide

- Oletame, et tegu on kahe kandidaadiga, Jüri ja Mari. Jüri poolt hääletades öeldakse J tõenäosusega 0.6, M tõenäosusega 0.4. Mari poolt hääletades öeldakse M tõenäosusega 0.6, J tõenäosusega 0.4

- Oletame, et 10-liikmeline valijaskond evib selliseid eelistusi: (J,J,J,M,M,M,M,M,M,M)

- Täringut visates hääletavalt nad järgmiselt (*-ga valijad hääletavad vastupidiselt oma eelistustele): (J,M*,J,M,J*,M,M,M,M,J*)

- Resultaadina saab Jüri 4 häält, kuigi tal on 3 valija süda. Mida rohkem on valijaid, seda täpsemalt kajastab tulemus valijate arvamusi

Randomized Response Technique, statistika

- Iga üksiku valija korral pole teada, kas ta valetas (tõenäosusega 0.4) või rääkis tõtt: tõenäosus, et ta valetas, on liiga suur.

- Lihtne valem: inimeste proportsiooni, kes eelistab J-i, lähendab arv

$$\frac{p-1}{2p-1} + \frac{L}{N} \cdot \frac{1}{2p-1} \ ,$$

  kus N on valijate koguarv, L on J-i poolt valinute arv, ning $p = 0.6$ on tõenäosus, et vastatakse õieti.

Randomized Response Technique, statistika

- Eelmises näites toodud arvud on liiga väiksed, et seda valemit kasutada: valem annaks, nagu eelistaks Jürit tegelikult -5 inimest!

- Kui on tegu ntks 10000 valijaga ning 5400 hääletab Jüri poolt, saame me aga tulemuseks, et tegelikult eelistas Jürit 7000 inimest, kuid suvalise 10-inimeselise populatsiooni eelistuste kohta ei saa me midagi öelda.

RRT, krüpto

- Kui valija vastab “õigesti” vale tõenäosusega, võib ta mõjutada valimistulemusi. See on krüptograafiliselt välditav.

- Kui kombineerida RRT-d ja eelnevalt tutvustatud meetodeid, saame olukorra kus isegi häälte dekrüpteerimine (kui serverid on tõesti korrumpeerunud) ei anna serveritele midagi üksikindiviidide kohta põhimõtteliselt.

- Kas selline lahendus on poliitiliselt vastuvõetav?

Lahtisi küsimusi

- Turvalisuseks on vaja suurem arv sõltumatuid servereid. Kas seda saab tagada? Kas see on poliitiliselt vastuvõetav?
- Kas saab tagada, et enamus serveritest on ausad?
- Kas saab tagada koduarvutite turvalisust?
- Kas RRT on poliitiliselt vastuvõetav?
- Selles ettekandes käsitlemata: häälte ostmine, suurte jaoskondade vajadus, tavavalimiste vajalikkus

Enda publikatsioone. . .

- Helger Lipmaa, N. Asokan, Valtteri Niemi, Secure Vickrey Auctions without Threshold Trust. In Matt Blaze, editor, *Financial Cryptography 2002*, volume 2357 of *Lecture Notes in Computer Science*, Southampton Beach, Bermuda, 11–14 March 2002. Springer-Verlag.

  E-oksjoniskeem, kuid selle lihtsustus on sobiv ka valimisteks. (Homomorfne krüpto.)

- Helger Lipmaa. On Diophantine Complexity and Statistical Zero-Knowledge Arguments. In Chi Sung Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume ? of *Lecture Notes in Computer Science*, pages ?–?, Taipei, Taiwan, November 30–December 4 2003. Springer-Verlag. To appear.

  Kirjeldab, kuidas viimases artiklis toodud lahendust efektiivsemaks teha. Kõige efektiivsem hetkeks tuntud homomorfsel krüptol põhinev e-valimiste skeem!

- Andris Ambainis, Markus Jakobsson, Helger Lipmaa, ‘Cryptographic Randomized Response Techniques”, Cryptology ePrint Archive, Report 2003/027, 2003.

  Konverentsile esitamisel. Räägib krüpto ja RRT seostest.

- Helger Lipmaa. Verifiable Homomorphic Oblivious Transfer and Private Equality Test. In Chi Sung Laih, editor, *Advances on Cryptology — ASIACRYPT 2003*, volume ? of *Lecture Notes in Computer Science*, pages ?–?, Taipei, Taiwan, November 30–December 4 2003. Springer-Verlag. To appear.

  Kirjeldab protokolli, mis kergelt parandab eelmist artiklit.