Høringsuttalelse fra NUUG og EFN om elektronisk stemmegivning

Petter Reinholdtsen*
Leder i foreningen NUUG

2006-09-30

Foreningene NUUG og EFN er glade for å ha blitt invitert til å kommentere utredningen om elektronisk stemmegivning, og håper våre innspill kan komme til nytte. Denne uttalelsen er ført i pennen av NUUGs leder Petter Reinholdtsen med innspill fra Tore Audun Høie, Erik Naggum og Håvard Fosseng.

Når en vurderer elektronisk stemmegivning, så tror vi det er viktig å ha prinsippene for gode valg i bakhodet. Vi har tatt utgangspunkt i listen fra Cranor, L.F. og Cytron, R.K. i "Design and Implementation of a Security-Conscious Electronic Polling System", som oppsummerer hvilke egenskaper som er viktige:

- Nøyaktig - et system er nøyaktig hvis det ikke er mulig å endre en stemme, det ikke er mulig å fjerne en gyldig stemme fra den endelige opptellingen og det ikke er mulig for en ugyldig stemme å bli talt med i den endelige opptellingen. Fullstendig nøyaktige systemer sikrer at den endelige opptellingen er perfekt, enten ved sikre at unøyaktigheter ikke kan bli introdusert eller kan oppdages og korrigert for. Delvis nøyaktige systemer kan oppdage men ikke nødvendigvis korrigere unøyaktigheter.

- Demokratisk - et system er demokratisk hvis kun de som har lov til å stemme kan stemme, og det sikrer at hver av dem kun kan stemme en gang.

- Hemmelig - et system er hemmelig hvis ingen, hverken de som arrangerer valget eller noen andre kan knytte en stemmeseddel til den som avga den, og ingen stemmegiver kan bevise at han eller hun stemte på en bestemt måte. Dette er spesielt viktig for å hindre kjøp og salg av stemmer og at personer kan tvinges til å stemme på en bestemt måte.

- Etterprøvbart - et system er etterprøvbart hvis hvem som helst uavhengig kan kontrollere at opptellingen er korrekt.

Et demokratisk valg må sikre at disse punktene er oppfylt. Det er med den bakgrunn vi vurderer elektronisk stemmegivning.

Nøyaktig opptelling kan kun oppnås hvis alle steg i opptellingsprosessen kan kontrolleres og verifiseres. Det må ikke må være mulig å fjerne eller endre avgitte stemmer, og heller ikke mulig å legge inn flere stemmer enn det som faktisk er avgitt. Elektronisk lagring av avgitte stemmer kan gjør det svært enkelt å endre på avgitte stemmer uten at det er mulig å oppdage det i ettertid. Elektronisk lagring vil også gjøre det mulig å lagre en annen stemme enn det som er blitt avgitt, selv om det så korrekt ut for den som avga stemmen. Vi mener derfor det er viktig at elektronisk stemmegivning gjøres via papir eller tilsvarende, slik at de som stemmer kan kontrollere at den stemmen de har avgitt er den som blir talt opp. I Australia brukes det et system der de som stemmer gjør sitt valg på en skjerm, og stemmen så skrives ut på en papirrull som sjekkes av den som stemmer før papirrullen leses inn av opptellingssystemet. En sikrer slik at hver enkelt stemme kan kontrolleres på nytt.

Etterprøvbarhet kan kun oppnås hvis hver enkelt stemmegiver kan kontrollere hele systemet som brukes for stemmegivning. For at dette skal være mulig er en nødvendig betingelse at en har innsyn i hvordan systemene er satt sammen, og hvordan de brukes. Selv om de aller fleste ikke selv vil kunne gjennomføre en slik kontroll, er det viktig at flere uavhengige eksperter kan sjekke systemet. Velgerne bør kunne velge

*epost: pere @ hungry.com

hvilke eksperter de vil stole på. Dette forutsetter blant annet tilgang til kildekoden og informasjon om hvordan de ulike delene av det totale stemmegivingssystemet er koblet. Lukkede systemer der kildekoden ikke er tilgjengelig og en ikke kan kontrollere systemene som brukes under selve valgene, er sårbare for trojanere (programvare som gjør noe annet og/eller mer enn det leverandøren sier den skal, f.eks. endre sluttresulatet av en opptelling) og påvirkning fra leverandøren. Det er påstander om slikt i USA på maskiner fra Diebold og Siebel allerede. Det finnes i dag flere tilgjengelige fri programvaresystemer for elektronisk stemmegiving og opptelling. Fri programvare sikrer brukeren kontroll over datasystemene. Slike systemer er tilgjengelig fra OpenSourceVoting og ACTs elektroniske valgsystem som ble brukt i det australske parlamentvalget 2001 og 2004. For å sikre at det er mulig å gjennomføre omtellinger må hver enkelt stemme lagres på ikke-elektronisk format (f.eks. papir), og et slikt papirspor må sikres slik at de ikke kan endres i ettertid.

Vellykkede elektroniske valgsystemer

I Venezuela fungerte avstemmingsmaskinene slik at de som stemte markerte det de stemte på en skjerm, og valgene ble skrevet på en papirrull som den som stemmer så de kunne sjekke for å kontrollere at de valgene som ble gjort kom med på papirrullen. Deretter ble voteringstallene sendt elektronisk fra hver maskin til tre uavhengige opptellingsgrupper (hvorav en av dem var Carter-senteret), som talte opp stemmene. Alle måtte være enige for å godkjenne resultatet. Hvis det var avvik så kunne en gå helt ned på papirrull-nivå for å sjekke resultatet. Det har dog blitt hevdet at oppbevaringen av papirrullene ble overlatt til regimet, slik at kontrollmuligheten ble fjernet. Det er likevel mulig å organisere seg slik at det blir vanskelig å forfalske valgresultatet ved å bytte ut eller endre rullene.

India har et elektronisk voteringssystem som ble tatt i bruk i 1989. Det består av to ulike enheter, en opptellingsenhet og en avstemmingsenhet. Systemet sikrer hemmelig valg, er vanskelig å påvirke, men mangler oppbevaring av hver enkelt stemme på et ikke-elektronisk format, noe som gjør omtelling umulig.

Mindre vellykkede elektroniske valgsystemer

I USA finnes en rekke ulike leverandører av elektroniske valgsystemer, og det er dokumentert svakheter med flere av dem. F.eks. har forskerne Ariel J. Feldman, J. Alex Halderman, og Edward W. Felten ved Universitetet i Princeton dokumentert hvordan systemet fra Diebold kan manipuleres til gi uriktig avstemmingsresultat. Det er også indikasjoner på at noen av systemene kan påvirkes av leverandøren via telelinjer. Robert F. Kennedy Jr. har nylig i en artikkel fortalt om flere avvik fra valget i 2004. Norge bør unngå systemer som kan manipuleres slik det rapporteres om fra USA.

Universitetet i Oslo skal denne høsten gjennomføre elektronisk valg på Dekan ved Det teologiske fakultet. Universitetsstyret har godkjent et valgsystem der de som arrangerer valget har mulighet til å se hvem som har stemt hva, samt hver deltager i valget kan endre sin stemme i ettertid (ikke-hemmelig), de som administrerer datasystemet kan påvirke valgresultatet ved å endre, trekke fra eller legge til stemmer (ikke-nøyaktig), og det ikke nødvendigvis er mulig å oppdage at slik påvirkning har funnet sted (ikke-etterprøvbart). Webbaserte valgsystemer uten spesiell klientprogramvare vil ha flere av disse problemene.

Konkrete kommentarer til rapporten

Rapporten nevner ikke muligheten for å påvirke valgresultatet via trojansk type kode. Siebel blir beskyldt for dette i USA. Vi advarer mot bruk av lukket kildekode, fordi dette i prinsippet innebærer å stole blindt på leverandøren. Det bør ikke vere begrenset hvem som kan kontrollere at systemet gjør det det skal, og dette tilsier bruk av fri programvare.

Rapporten anbefaler lukket kode fordi kjeltringer kan finne ut sikkerhetsmekanismene ved å lese kode. Det er ikke en god idé å basere seg på at sikkerhetsmekanismene er beskyttet pga. at ingen kjenner til hvordan de fungerer. Som eksempelet fra USA viser, kan man godt mistenke leverandøren for å jukse med systemet. Selve det at en slik mistanke eksisterer, og ikke kan fjernes/reduseres ved uavhengig inspeksjon, er et problem for demokratiet. Et sikkert system må være sikkert selv om noen med uærlige hensikter kjenner til hvordan det fungerer. Australia har allerede gjennomført vellykkede valg basert på et fri programvaresystem.

Driften av totalsystemet blir ofret liten oppmerksomhet i rapporten. I et driftopplegg ligger mange sikkerhetsutfordringer som bør vurderes nøye.

Definisjonen av brannmur i rapporten er feil, for eksempel sies at "brannmuren er selv immun mot inntrengning". Dette er ikke riktig. Det er fullt mulig å ha brannmurer med sikkerhetsproblemer som utnyttes til å trenge inn i dem. I tillegg antar man at all trafikk går gjennom brannmuren. I store applikasjoner, som et valgsystem vil være, kreves et system av brannmurer og andre tiltak som vi kaller sikkerhetsarkitektur. Rapporten burde komme inn på behovet for en sikkerhetsarkitektur.. Selv med en gjennomarbeidet sikkerhetsarkitektur kan det være at man overser muligheter for å unngå brannmurene. Rapporten snakker om brannmur i entall, mens det nok er nødvendig å sikre et valgsystem med flere lag av sikringstiltak, og dermed vil være behov for flere brannmurer. En brannmur kan være bygd basert på visse antagelser og standarder. En annen brannmur kan bygge på et annet sett antagelser, og stoppe trafikk som den første ikke tar høyde for.

Rapporten indikerer dårlige kunnskaper om brannmur, og dette igjen antyder dårlige kunnskaper om datasikkerhet generelt, og dette bør forbedres. For eksempel er driften ansvarlig for operativ sikkerhetsarkitektur, og vi har hatt adskillige diskusjoner i NUUG om hvor vanskelig dette er. Hva hjelper en brannmur hvis den er feil konfigurert eller ikke oppdatert?

Muligheten for sikkerhetsovervåkning kan vi ikke se er nevnt i rapporten. Dette er vanskelig og dyrt, men bør vurderes for å kunne oppdage systemavvik under valget. Sikkerhetsovervåkning kan inngå som ledd i sikkerhetsarkitekturen.

Det har blitt rapportert i pressen at USA ikke bør kjøpe Lenovo-maskiner etter at selskapet som lager dem ble solgt fra IBM til et kinesisk selskap. I Norge kan vi ikke trekke tingene like langt da vi mangler nødvendig dataindustri, men vi bør satse på at applikasjoner viktige for rikets sikkerhet i størst mulig utstrekning kjører programvare der vi har innsyn i hvordan den er satt sammen. Det er viktig at vi sikrer at programvare viktige for rikets sikkerhet kan sjekkes/verifiseres av eksperter vi selv velger. Når det gjelder valgsystemer må «vi» være velgerne, ikke bare myndighetsapparatet. I tilfelle en ikke kan bruke fri programvare, bør en ivareta en sunn kritisk sans med hensyn til hvorfra og av hvem vi kjøper. På grunn av tendenser i USA til å i uheldig stor grad fokusere på kontrollmekanismer som eksempelvis Echelon og Palladium kan det hevdes at det hefter betenkeligheter ved innkjøp herfra.

Referanser

- Cranor, L.F. og Cytron, R.K., "Design and Implementation of a Security-Conscious Electronic Polling System" Washington University Computer Science Technical Report WUCS-96-02. February 1996
  http://www.cs.wustl.edu/cs/techreports/1996/wucs-96-02.ps.Z
- Det australske valgsystemet, inkludert kildekoden tilgjengelig som fri programvare
  http://www.elections.act.gov.au/Elecvote.html
- Smartmatics SAES voting system used in venesuela 2004
  http://www.smartmatic.com/solutions_03-1.htm
- Blackboxvoting, interessegruppe i USA med fokus på valgfusk vha. elektroniske valgsystemer
  http://www.blackboxvoting.org/
- VerifiedVoting, interessegruppe i USA med fokus på at også elektroniske valgsystemer må være etterprøvbare.
  http://www.verifiedvoting.org/
- Blue Screen Democracy - fri programvareprosjekt som har utviklet elektronisk stemmegivingssystem
  http://bluescreen.sourceforge.net/
- Indias elektroniske avstemmingssystem (Wikipedia)
  http://en.wikipedia.org/wiki/Indian_voting_machines

- Security Analysis of the Diebold AccuVote-TS Voting Machine av Ariel J. Feldman, J. Alex Halderman, og Edward W. Felten.

  http://itpolicy.princeton.edu/voting/

  http://coblitz.codeen.org:3125/itpolicy.princeton.edu/voting/videos/ts-voting.wmv

- Was the 2004 Election Stolen? av Robert F. Kennedy Jr.

  http://www.rollingstone.com/news/story/10432334/was_the_2004_election_stolen

- Styreframlegg om elektronisk votering ved UiO.

  http://www.admin.uio.no/kollegiet/moter/kart_prot2006/5/protokoll.xml

  http://www.admin.uio.no/kollegiet/moter/kart_prot2006/5/vsak-14.pdf

  http://www.admin.uio.no/kollegiet/moter/kart_prot2006/5/vsak-14-vedlegg.pdf

- Elektroniske valg - muligheter, problemer og noen løsninger
  Semesteroppgave i STV620 - Demokratiske valg

  http://www.afin.uio.no/forskning/notater/4_01.html

- NUUG - Norwegian Unix User Group

  http://www.nuug.no/

- EFN - Elektronisk forpost Norge

  http://www.efn.no/