Veilig online stemmen vanuit San Francisco?

Wolter Pieters
Security of Systems groep
Radboud Universiteit Nijmegen
Postbus 9010
6500 GL Nijmegen
w.pieters@cs.ru.nl

Februari 2005

Internetstemmen is in. In Nederland hebben zowel bij de Europese verkiezingen als bij de verkiezingen voor de waterschappen experimenten plaatsgevonden met stemmen via het World Wide Web. Nederland eist daarmee een positie van internationale betekenis op. In deze context is het begrijpelijk dat ook binnen politieke partijen naar mogelijkheden wordt gezocht om interne stemmingen via internet mogelijk te maken. Bij D66 is deze wens tot uitdrukking gekomen in de zogenaamde "San Francisco-motie" (congres Maastricht, 2003). Hierin wordt het bestuur gevraagd de leden via internet te betrekken bij de besluitvorming. Met behulp van internet stemmen over moties is een onderdeel van de uitwerking hiervan.

Binnen de Security of Systems groep van de Radboud Universiteit Nijmegen hebben we al veel ervaring met de evaluatie van internetstemsystemen. In dit kader hebben we ook gekeken naar een experiment met de uitwerking van de San Francisco-motie. We zullen eerst internetstemmen in het algemeen introduceren, en daarna specifiek ingaan op de keuzes die gemaakt moeten worden bij de implementatie van de motie.

Internetstemmen

Bij internetstemmen kan een kiezer op een willekeurige computer met internetverbinding een stem uitbrengen. Deze stem wordt via het internet verstuurd, en komt binnen bij een elektronisch stembureau. Daar worden de elektronische stemmen verzameld. Uiteindelijk wordt het bestand met binnengekomen stemmen "verzegeld", en daarna kunnen de stemmen geteld worden.

De belangrijkste experimenten tot nu toe met internetstemmen in Nederland zijn uitgevoerd bij de Europese verkiezingen in 2004 (KOA, oftewel Kiezen Op Afstand: internetstemmen voor Nederlanders in het buitenland) en bij de waterschapsverkiezingen van de waterschappen Rijnland en Dommel in herfst

2004 (RIES). Hoewel de ontwikkelde systemen hetzelfde doel hebben, zijn ze in de praktische uitwerking nogal verschillend. Het blijkt dat de eisen die aan dergelijke systemen gesteld moeten worden op dit moment verre van duidelijk zijn. De ontwerpers zijn dus vrij eigen prioriteiten te stellen en eigen keuzes te maken.

Binnen de academische wereld is de heersende opvatting dat de uitdaging van internetstemmen niet volledig technisch kan worden opgelost. Dat wil zeggen dat het computersysteem niet zodanig kan worden ingericht dat daarmee alle fraude onmogelijk wordt gemaakt. Maar is dat wel nodig? Bij de huidige verkiezingen is fraude immers ook niet geheel uit te sluiten. Wel zijn er allerlei extra maatregelen om manipulaties tegen te gaan, in de vorm van procedures (hoe worden de resultaten van een stembureau verzonden?) en wetten (wat gebeurt er als je een machtiging vervalst?). Organisatorische en juridische maatregelen zullen ook een plaats moeten krijgen bij internetstemmen.

Beveiligingsmaatregelen

Een belangrijk thema bij discussies over internetverkiezingen ligt in het gebrek aan controle over de stemomgeving. Dit probleem doet zich overigens ook voor bij poststemmen. Als iemand in een stemhokje stemt, is de stemmer gegarandeerd vrij in zijn keuze, en kan hij ook niet achteraf bewijzen dat hij een bepaalde keuze heeft gemaakt. Dit maakt stemdwang en het verkopen van stemmen zo goed als onmogelijk. Als iemand echter vanaf zijn eigen computer of per post stemt, is er niets dat het afdwingen of opkopen van de stem in de weg staat. Iemand kan immers meekijken hoe je je stem invult en controleren dat je de "juiste" keuze maakt. Als we desondanks via internet willen stemmen, dan zullen er juridische maatregelen nodig zijn die deze vorm van fraude onaantrekkelijk maken.

Een ander belangrijk punt is de anonimiteit van de kiezer. Bij de huidige internetstemsystemen wordt gewerkt met toegangscodes, bijvoorbeeld een reeks van 8 cijfers en letters. Deze stemcode moet op de internetpagina worden ingevuld om te kunnen stemmen. Er zijn organisatorische maatregelen nodig om te zorgen dat deze codes alleen aan de kiezer bekend zijn. Je wilt immers niet dat iemand anders voor jou kan stemmen, zelfs niet de organisator van de verkiezingen. Een vergelijkbare procedure vinden we bij het versturen van PIN-codes van bankpassen. Deze worden met behulp van carbonpapier in een reeds gesloten envelop geprint, en mogen niet achterblijven in de computer van de drukker of de bank.

De vraag is nu hoe het elektronische stembureau kan controleren dat een binnengekomen stem geldig is, zonder zelf over de stemcode te beschikken. Hiervoor bestaat een technische truc, die bekend staat onder de naam *hash-functie*. Een hash-functie berekent een controlegetal van een stemcode. Uit dit controlegetal kan niet de stemcode worden afgeleid, maar met behulp van het controlegetal kan *wel* worden gecontroleerd of een ontvangen stem met stemcode geldig is. Natuurlijk moet dan nog steeds gezorgd worden dat niemand binnen het

elektronische stembureau de van de kiezer ontvangen stemcode te zien krijgt...

Secure Democracy?

In een experiment met de uitvoering van de San Francisco-motie wordt gebruik gemaakt van het internetstemsysteem SEDE (Secure Democracy). Leden van D66 kunnen daarmee via internet meestemmen over moties, ook als ze niet bij het congres aanwezig zijn. In tegenstelling tot andere systemen is SEDE gebaseerd op e-mail, en is het vrij te downloaden. Het lijkt daarom uitermate geschikt te zijn voor peilingen. Maar is het dat ook voor (geheime) stemmingen?

Omdat SEDE gebruik maakt van (onbeveiligde) e-mail, moet de kiezer zich realiseren dat het stemmen via SEDE overeenkomt met het opsteken van een hand, en niet met schriftelijke stemming. De stemming is dus niet anoniem. Het is immers mogelijk dat iemand de e-mail onderschept en leest. Voor het stemmen over moties hoeft dit geen probleem te zijn. Het is echter ook mogelijk dat iemand een e-mail *verandert*. Dit laatste zou overeenkomen met het wijzigen van je stem door je buurman tijdens een partijcongres, bijvoorbeeld door je hand vast te pakken en omhoog te steken, of juist omlaag te duwen. In dit geval moet je achteraf bij de verantwoordelijke voor de stemming aangeven dat je stem onjuist geregistreerd is, en dat deze alsnog gewijzigd moet worden. Hoewel dit absurd klinkt, is dit precies wat er bij SEDE gebeurt.

Een tweede probleem is dat er geen gebruik wordt gemaakt van een hash-functie. Alle stemcodes worden in het elektronische stembureau bewaard. Hierdoor kunnen mensen met toegang tot het elektronische stembureau eenvoudig stemmen vervalsen op basis van de beschikbare stemcodes. Het is daarom van groot belang dat kiezers hun stem achteraf controleren, zelfs als ze niet gestemd hebben. Dit is mogelijk in SEDE, maar dat neemt niet weg dat ook andere beveiligingsmaatregelen op hun plaats zijn. Het is namelijk maar de vraag of mensen ook daadwerkelijk hun stem zullen verifiëren. In feite legt de huidige versie van SEDE te veel macht bij degenen die toegang hebben tot het elektronische stembureau.

Naast deze technische opmerkingen valt ons ook op dat het voor een onervaren computergebruiker moeilijk zal zijn wijs te worden uit het e-mail stembiljet. Er zal onderzoek vanuit gebruikersperspectief nodig zijn om een degelijke interface voor SEDE te maken, bijvoorbeeld in de vorm van een webpagina. Daar wordt op dit moment aan gewerkt.

We kunnen concluderen dat SEDE is geschreven vanuit het perspectief van een handige computergebruiker, maar niet vanuit het perspectief van een beveiligingsexpert of een kiezer met weinig kennis van computers. Voor peilingen is het (mits er een goede interface beschikbaar is) een prima middel, maar voor serieuze verkiezingen zouden we de huidige versie niet willen aanraden. Het grote voordeel van SEDE is natuurlijk wel dat het open-source is, en gratis. Iedereen kan het dus gebruiken, en iedereen kan ook in principe controleren hoe het programma werkt. Vanuit beveiligingsperspectief vinden wij het erg belangrijk dat er openheid is over hoe systemen werken. Bij de stemmachines die nu bij

verkiezingen ingezet worden is dit helaas niet het geval, en dit is voor andere landen reden om ze niet te gebruiken.

We hopen met deze bijdrage de verdere ontwikkeling van open-source systemen zoals SEDE te kunnen ondersteunen. Met een aantal verbeteringen, waaronder het toevoegen van een hash-functie en het gebruik van een beveiligde internet-verbinding, kan al veel bereikt worden. Het blijft echter wel verstandig ook andere opties te overwegen voor de implementatie van de San Francisco-motie.

Conclusies

Internetstemmen biedt vele mogelijkheden, zeker als het gecombineerd wordt met andere vormen van online participatie in besluitvormingsprocessen. Het is daarmee uitermate geschikt voor een partij als D66, die dicht bij de burger wil staan. Het is wel verstandig duidelijk vast te stellen wat D66 precies verwacht van een internetstemsysteem voordat er keuzes worden gemaakt voor de implementatie. Het veranderen van de wijze van stemmen is iets dat direct raakt aan het democratisch proces, en verdient daarom de nodige zorgvuldigheid. Elke stem moet immers tellen, en — zoals D66 wil — er moet echt geluisterd worden naar de burger, niet naar een handige hacker.

Wolter Pieters is junioronderzoeker aan de Radboud Universiteit Nijmegen. Hij studeerde informatica en wijsbegeerte van wetenschap, technologie en samenleving aan de Universiteit Twente. Het hoofdonderwerp van zijn promotieonderzoek is de haalbaarheid van internetstemmen, zowel vanuit technisch als vanuit maatschappelijk perspectief. Een uitgebreider evaluatierapport over SEDE is op aanvraag beschikbaar.