Tijdens de Tweede Kamerverkiezingen op 22 november 2006 is er een experiment gehouden met stemmen via internet voor Nederlandse kiezers in het buitenland. De vakgroep Security of Systems van de Radboud Universiteit Nijmegen (RUN) volgt de ontwikkelingen rond internetstemmen al geruime tijd op de voet. Hoe lang duurt het nog voordat iedereen via internet kan stemmen? En direct dringt ook de vraag zich op: hoe veilig is internetstemmen? Een gesprek met RUN-onderzoeker Engelbert Hubbers. *Door Mirjam Dijkema*

Hoe veilig is stemmen via internet?

Al in 2004 schreven Engelbert Hubbers en Bart Jacobs (beide RUN) een artikel[1] over stemmen via het Rijnland Internet Election System (RIES); hoe werkt het, hoe veilig is het en waar zitten de zwakke plekken? Conclusie: het systeem is veilig genoeg. De kracht zit hem in het achteraf kunnen controleren van de stem door de kiezer zelf. Pas dan kan de volledige betrouwbaarheid worden gegarandeerd. Om dit mogelijk te maken ontwikkelde Hubbers een stemcontroledienst. 'Het achterliggende doel is om meer vertrouwen te kweken bij het publiek in de uitslag', vertelt Hubbers. 'Daar waar het op dit moment bij stemcomputers nog onduidelijk is hoe de uitslag wordt vastgesteld, kunnen bij internetstemmen met dit systeem onafhankelijke controles uitgevoerd worden door de kiezer zelf.'

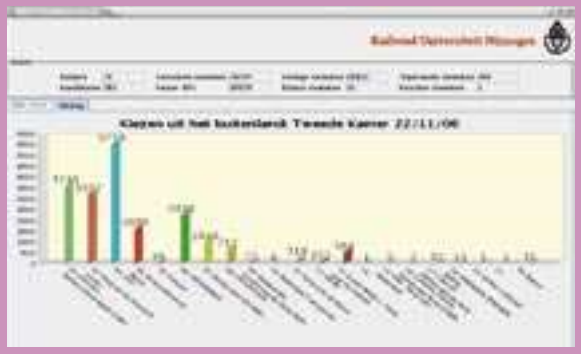
Van de stemmers die tijdens de laatste Tweede Kamerverkiezingen aan het internetexperiment meededen, heeft een half procent de controle daadwerkelijk uitgevoerd. Hubbers: 'Als je bedenkt dat de kracht van dit systeem van internetstemmen zit in het kunnen controleren, valt dit resultaat erg tegen. Het is duidelijk dat internetstemmen nog in de experimentele fase zit. De huidige kieswet is niet klaar voor het op grote schaal gebruik maken van internetstemmen.' De kieswet bepaalt namelijk dat er een stemgeheim moet zijn. In het bijzonder mag niet kunnen worden bewezen op wie er gestemd is, want dat kan ertoe leiden dat stemmen verkocht worden. Bij het systeem RIES KOA vormt de technische stem (zie kader) zo'n bewijs. Hubbers: 'De vraag is nu: moet de wet worden aangepast of moeten er systemen komen die aan de huidige wet voldoen? Dit verlangt nog een uitgebreide maatschappelijke discussie.'

En dan is er ook nog een technische hobbel die genomen moet worden, namelijk die van de schaalbaarheid. Hubbers: 'Nu ging het om een verkiezing met 20.000 kiezers en een kleine 600 kandidaten. Dat leverde tabellen op van 300Mb in gezipte vorm. Omgerekend naar 10 miljoen kiezers is dit 150Gb. Voor de stemserver hoeft dit geen struikelblok te zijn, maar voor de gemiddelde eindgebruiker die zijn stem wil controleren wel. Juist die controle maakt het systeem betrouwbaar. Maar voor lokale verkiezingen waar de belangen iets minder groot en de aantallen kandidaten en kiezers kleiner zijn, lijkt RIES KOA prima geschikt.'

Het controleren is erg eenvoudig en gebruiksvriendelijk. De stemmer hoeft alleen zijn technische stem in te voeren en het systeem doet de rest: het opzoeken van de statusbits, deze interpreteren en als tekst aan de kiezer tonen. En dat alles zonder dat er grote files hoeven te worden gedownload. Ook de veiligheid van de controle zelf is gegarandeerd. 'De connecties naar de site zijn via SSL beveiligd zodat je kunt controleren of je echt met de Radboud Universiteit Nijmegen praat. Daarnaast is alle verkeer tussen de pc van de stemmer en de server van de RUN versleuteld, zodat het niet af te luisteren is,' verzekert Hubbers. I/O

Meer informatie is te vinden op https://www.sos.cs.ru.nl/research/sosries/

[1] E.-M.G.M. Hubbers and B.P.F. Jacobs. Stemmen via internet geen probleem. Automatisering Gids #42, okt. 2004, p. 15



De werking van RIES KOA en de stemcontroledienst

Het gebruikte systeem bij het stemmen via internet is RIES KOA (een doorontwikkelde versie van RIES 2004). Dit systeem werkt met verschillende versleutelingen, zogenaamde hashes. De organisator genereert voor elke kiezer een geheime sleutel en een tabel waarin zo'n hash wordt gekoppeld aan een specifieke kandidaat. De kiezer ontvangt zijn geheime sleutel en berekent hiermee een eerste hash, de zogenaamde technische stem. Vervolgens kan er met een andere hash-functie (zonder sleutel) uit die technische stem worden bepaald op welke kandidaat er is gestemd. Het innovatieve aan het systeem zit hem in de combinatie van het gebruik van hashes met sleutels (omdat alleen de kiezer een stem mag genereren), hashes zonder sleutels (omdat iedereen een onafhankelijke controle moet kunnen uitvoeren) en de publicatie van alle mogelijke uitslagen voor de verkiezingen en alle uitgebrachte stemmen na de verkiezingen. Hierdoor is het voor elke kiezer mogelijk om na afloop te controleren of zijn stem goed is verwerkt.

Hubbers: 'Deze methode maakt het ook mogelijk dat wij met een zelfgeschreven Java-programma een onafhankelijke uitslag kunnen bepalen (zie afbeelding). Als iemand tijdens het stemmen zijn zogenaamde technische stem heeft onthouden, kan hij via onze website zelf controleren wat er met zijn stem gebeurd is. Die stem kunnen wij op twee manieren testen. Ten eerste ten opzichte van de officiële file die het stembureau heeft gemaakt met de status van elke stem. Ten tweede heeft ons telprogramma ook zo'n file met statusbits opgeleverd. En als het goed is zijn in beide systemen dezelfde stemmen goedgekeurd.'