Stemmen via internet *geen* probleem

Engelbert Hubbers, Bart Jacobs

In: Automatisering Gids #42, 15 okt. 2004, p.15

Internetstemmen kan op een veilige manier gebeuren. Eind september, begin oktober is ervaring opgedaan met het 'Rijnland Internet Election System' bij de waterschapsverkiezingen voor het Hoogheemraadschap Rijnland. Bart Jacobs en Engelbert Hubbers analyseren wat er precies gebeurt als er via internet wordt gestemd, hoe veilig het is en waar de zwakke plekken zitten.

Van 25 september tot en met 6 oktober 2004 hebben de waterschapsverkiezingen voor het Hoogheemraadschap van Rijnland plaatsgevonden. De vorige verkiezingen voor dit bestuursorgaan verliepen via poststemming, maar deze keer was het voor het eerst mogelijk dat de kiesgerechtigden ook via internet hun stemmen doorgeven. Dat laatste is door iets meer dan 70.000 mensen gedaan. Hiervoor heeft Rijnland zelf een systeem laten ontwikkelen: RIES, het Rijnland Internet Election System, dat zonder noemenswaardige problemen gefunctioneerd heeft. Dit artikel beschrijft de werking van RIES, niet in alle details, maar wel met de de gebruikte elementaire cryptografische operaties.

De drijvende krachten achter RIES zijn de projectleider Simon Bouwman van het Hoogheemraadschap, de ontwerper Piet Maclaine Pont van Mullpon en de bouwer Arnoud Hannink van MagicChoice. Naast Rijnland gaat ook het waterschap De Dommel gebruik maken van dit systeem. Op de belangrijkste constructie-onderdelen van RIES is een internationale patent aanvraag gedaan, gezamenlijk door Rijnland en de ontwerper Maclaine Pont.

Hoewel in het daadwerkelijke systeem er ook nog een mogelijkheid is om per post te stemmen, gaan wij in deze beknopte beschrijving alleen uit van pure internetstemmen. Daarbij zullen we buiten beschouwing laten hoe het systeem vaststelt of een bepaalde kiezer al gestemd heeft of niet, zonder de identiteit van die kiezer te kennen. Dit is namelijk niet van belang voor de werking van het systeem.

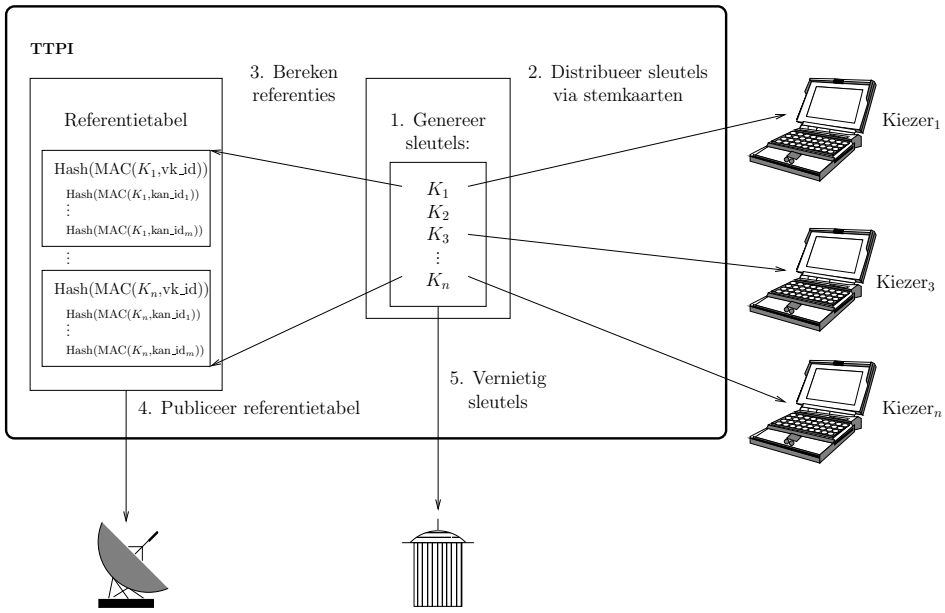
Het systeem is gebaseerd op de afstudeerscriptie van Herman Robers: *Electronic Elections employing DES Smartcards*, geschreven in 1998 aan de TU Delft. Zoals de titel al aangeeft werd daar echter gebruik gemaakt van een chipkaart om de kiezers cryptografische berekeningen te laten doen. In verband met de kosten en de eis dat kiezers geen nieuwe hardware hoeven te installeren, is dit protocol zodanig aangepast dat de cryptografische berekeningen nu via JavaScript in de browser van de kiezer worden gedaan. Er worden slechts twee

soorten cryptografische berekeningen uitgevoerd: een one-way hash (MDC-2) en een MAC (DES). Zie kader 1 voor een uitleg. Het systeem is verder het beste te beschrijven door een splitsing te maken in fasen: voor, tijdens en na de verkiezingen.

Voor de stemming

Het meeste werk voor de verkiezingen wordt gedaan door het bedrijf TTPI, een samenwerkingsverband tussen Mullpon en MagicChoice. Om te beginnen genereert TTPI voor elke kiesgerechtigde i een DES sleutel K_i. Deze sleutels worden door de drukker op de stemkaarten gezet waarbij zij gerepresenteerd worden in het zogenaamde AN34 formaat. Dit formaat heeft als voordeel dat er minder digits nodig zijn om grote getallen op te slaan: met vier digits kan men in ons gebruikelijke decimale stelsel de getallen 0,...,9999 weergeven en in AN34 0,...,1336335. Gevolg is dat er langere sleutels kunnen worden gebruikt, zonder dat de kiezer langere codes hoeft in te tikken. Verder gebruikt TTPI deze sleutels om voor elke kiesgerechtigde een tabel met referentiewaarden te berekenen. Voor een systeem met n kiesgerechtigden en m kandidaten levert dat de referentietabel op uit kader 2.

Deze tabel wordt op het internet gepubliceerd en via MD5 hashes beschermd tegen manipulaties. Vervolgens worden de gebruikte sleutels K_i vernietigd. Zie figuur 1.



Figuur 1: Fase 1: voor de stemming

One-way hash	Populair gezegd kan een one-way hash worden gezien als een vingerafdruk. Formeel is het een afbeelding $H(M)$ die bij invoer M van willekeurige lengte volgens een bekend proces een karakteristieke waarde h van vaste lengte uitrekent, zodanig dat: gegeven M het makkelijk is om $H(M) = h$ uit te rekenen, gegeven h het moeilijk is om M te vinden met $H(M) = h$ en gegeven M het moeilijk is om een andere M' te vinden met $H(M) = H(M')$.
MAC	Message Authentication Code. Dit is een speciale hash functie die voor het berekenen van de karakteristieke waarde een geheime sleutel gebruikt. Zonder die sleutel is het ondoenlijk om die karakteristieke waarde uit te rekenen en om uit zo'n waarde de oorspronkelijke input weer te berekenen.
DES	Data Encryption Standard. Symmetrisch algoritme: voor encryptie en decryptie wordt dezelfde sleutel gebruikt.
MDC-2	Een one-way hash algoritme van IBM dat 128bits uitvoer oplevert, gebaseerd op het DES algoritme. Tegenwoordig onder andere geïmplementeerd in het vrij beschikbare `openssl`.
MD5	Een one-way hash algoritme van Rivest dat 128bits uitvoer oplevert.
AN34	Wiskundig getalstelsel met grondtal 34. Werkt op dezelfde manier als ons decimale getalstelsel alleen zijn er nu 34 verschillende digits 0,1,2,...,9,a,b,...,k,m,n,p,...,z. Merk op dat l en o niet voorkomen in verband met mogelijke verwarring met 1 en 0.

Kader 1: Definities

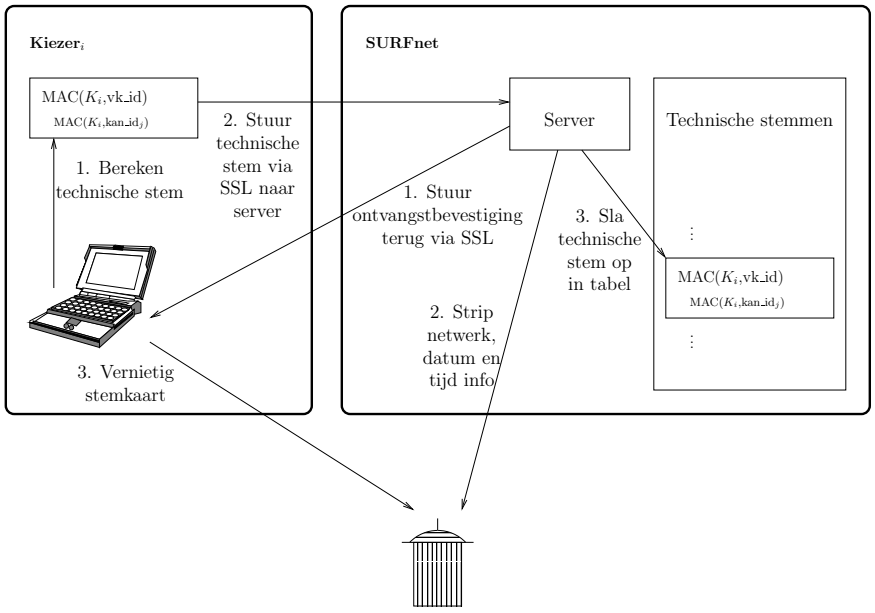
Hash(MAC(K_1,vk_id))	Hash(MAC(K_1,kan_id$_1$)) — kan_id$_1$ Hash(MAC(K_1,kan_id$_2$)) — kan_id$_2$ $\vdots$ Hash(MAC(K_1,kan_id$_m$)) — kan_id$_m$
Hash(MAC(K_2,vk_id))	Hash(MAC(K_2,kan_id$_1$)) — kan_id$_1$ Hash(MAC(K_2,kan_id$_2$)) — kan_id$_2$ $\vdots$ Hash(MAC(K_2,kan_id$_m$)) — kan_id$_m$
$\vdots$	
Hash(MAC(K_n,vk_id))	Hash(MAC(K_n,kan_id$_1$)) — kan_id$_1$ Hash(MAC(K_n,kan_id$_2$)) — kan_id$_2$ $\vdots$ Hash(MAC(K_n,kan_id$_m$)) — kan_id$_m$

Kader 2: Referentietabel. Hierbij is vk_id de verkiezings-id en kan_id$_j$ de unieke id van kandidaat j.

Tijdens de stemming

Tijdens de verkiezingen zijn er twee partijen actief: de stemserver die beheerd wordt door SURFnet en natuurlijk de kiezers zelf.

Kiezer i voert de deelnamegroep, stemcode en wachtwoord in die op zijn stemkaart staan op de webpagina `internetstemmen.nl`. Hierdoor stelt hij zijn persoonlijke sleutel K_i beschikbaar aan de JavaScript interpreter van zijn browser. Vervolgens klikt hij zijn favoriete kandidaat j aan. Zijn browser zal nu twee waarden uitrekenen: MAC(K_i,vk_id) en MAC(K_i,kan_id$_j$). Samen vormen deze twee waarden de zogenaamde technische stem. Het eerste deel is bedoeld om de authenticiteit van een kiesgerechtigde vast te stellen zonder zijn anonimiteit te schenden. Het tweede deel wordt gebruikt om te bepalen op wie er gestemd is. Deze technische stem wordt naar de stemserver gestuurd via een SSL verbinding. In het bijzonder wordt K_i dus niet opgestuurd, maar wel, en dat is cruciaal, iets dat alleen met K_i gemaakt kan worden. De server stuurt vervolgens een ontvangstbevestiging terug, ontdoet de stem van datum, tijd en netwerkadressen en slaat hem vervolgens op. Er vindt op dit moment dus ook geen controle op geldigheid plaats. Als de kiesgerechtigde verstandig is, vernietigt hij zijn stemkaart zorgvuldig zodat zijn persoonlijke sleutel niet in omloop komt. Zie figuur 2.



Figuur 2: Fase 2: tijdens de stemming

Na de stemming

Op het moment dat de verkiezingen worden gesloten, komen twee partijen in actie. SURFnet berekent een hash over het bestand met alle binnengekomen technische stemmen. Deze hash dient om te kunnen controleren dat TTPI het bestand niet verandert. Vervolgens worden die stemmen overgedragen aan TTPI om de uitslag te bepalen.

Dit doet TTPI door van de twee delen van elke technische stem weer de MDC-2 hash te berekenen. Wil een stem geldig zijn, dan moet de combinatie van deze twee hashes in de referentietabel van voor de verkiezingen voorkomen. Stemmen waarbij dat niet het geval is worden dan ook meteen ongeldig verklaard en tellen niet mee. Als die combinatie wel voorkomt, wordt gekeken of de stem misschien om een andere reden ongeldig is. Bijvoorbeeld doordat twee keer is gestemd op een verschillende kandidaat. Voor alle stemmen die om wat voor reden dan ook ongeldig worden verklaard, wordt bijgehouden op grond waarvan dat is gebeurd. Bij controle kan men dan zien waarom een bepaalde stem niet is meegeteld. Vervolgens worden dubbele stemmen uit het systeem gefilterd. Het vaststellen van de uitslag gebeurt nu door alle hashes op te sporen in de referentietabel en de daar gevonden bijbehorende kandidaat een stem toe te kennen. Vervolgens zal het stembureau de door TTPI berekende resultaten bekendmaken. Zie figuur 3.

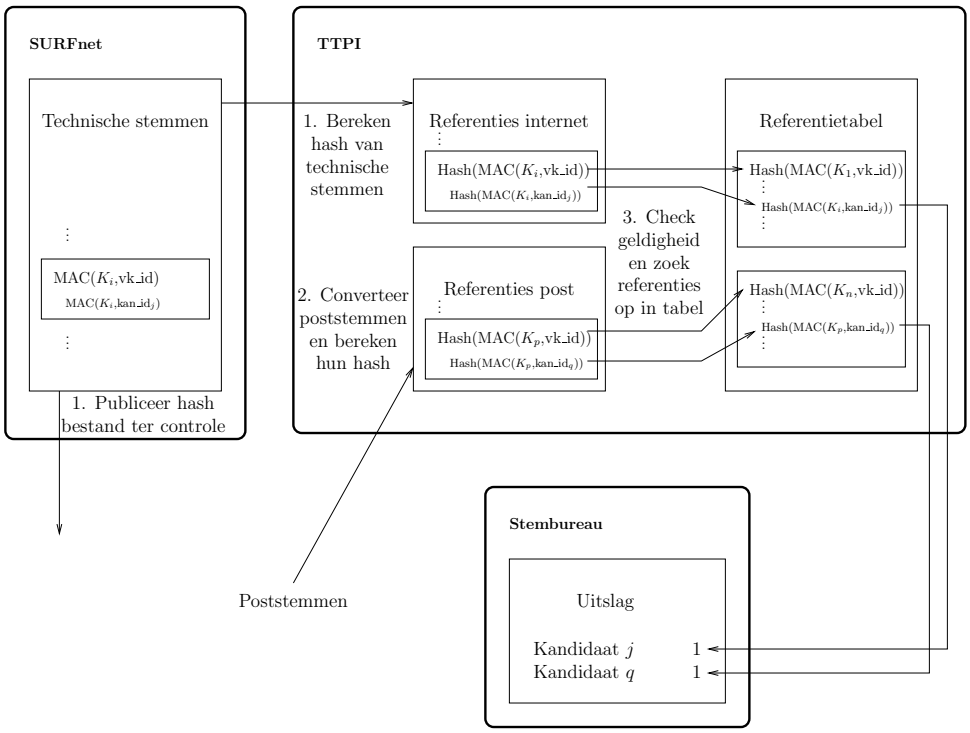
Controle

Het systeem is zo opgezet dat elke kiezer na afloop kan controleren of zijn stem is meegeteld. Daarvoor is het belangrijk dat hij zijn technische stem (die twee MAC's) bewaard heeft.

De kiezer kan de controle aan de hand van de website doen, maar helemaal overtuigend is dat natuurlijk niet, gezien het feit dat die controle dan wordt uitgevoerd door de partij die ook de stem heeft verwerkt.

Gelukkig kan de kiezer de controle in principe ook zelf doen. Hij moet dan in de gepubliceerde tabel met de ontvangen stemmen controleren dat zijn stem inderdaad is ontvangen. In het bestand met de door TTPI verwerkte stemmen moet te zien zijn dat zijn stem ook geaccepteerd is als geldige stem. Door vervolgens de hashes van de technische stem te berekenen kan de kiezer ook zelf in de referentietabel controleren dat zijn geaccepteerde stem voor de juiste kandidaat is meegeteld.

Bij het gebruik van stemmachines en eerdere initiatieven voor elektronisch stemmen (KOA, zie kader 3) is open source een belangrijk onderwerp. Hier is dat minder relevant, door de controleerbare aard van de resultaten. Verder is de (JavaScript) code bij de kiezer direct in zijn browser te bekijken en dus al automatisch open source. De verwerkingssoftware op de server is relatief eenvoudig. De telsoftware zou wel nog openbaar gemaakt kunnen worden, daar het proces dat daaraan ten grondslag ligt weer een stuk bewerkelijker is.



Figuur 3: Fase 3: Na de stemming

Zwakheden

Hoewel het systeem in zijn algemeenheid goed doordacht lijkt, kent het toch enkele zwakheden. Zo is het mogelijk aan de hand van de technische stemmen te achterhalen op welke kandidaat er gestemd is. In theorie is het niet mogelijk om hierbij ook te achterhalen welke kiezer hier bij hoort. Maar als het strippen van netwerkadressen bijvoorbeeld niet goed gedaan is, kan een bepaalde keuze tot een bepaald netwerkadres (ip) worden herleid. Formeel geeft dat natuurlijk geen link met kiesgerechtigden, maar het geeft wel vermoedens. Doordat er SSL gebruikt wordt voor het versturen van de stemmen, is het niet mogelijk om uit pakketjes die worden afgeluisterd voor zij de server bereiken de technische stemmen te achterhalen.

Een tweede punt is de afhankelijkheid van de betrouwbaarheid van de systeembeheerder. Zo kan een systeembeheerder bijvoorbeeld gericht binnengekomen stemmen weglaten. Door namelijk de juiste hashes te berekenen kan hij zien voor wie een stem bedoeld is. Als hij dit maar doet voor het vastleggen van de ontvangen stemmen via een hash aan het eind van de verkiezingen, zal dit lastig te traceren zijn. Daarvoor is het van belang dat individuele kiezers inderdaad achteraf hun stem gaan controleren, zodat dergelijke fraude zichtbaar

wordt. Andersom kan niet: een systeembeheerder kan geen geldige stemmen voor bepaalde kandidaten toevoegen, omdat hij niet beschikt over de daarvoor benodigde sleutels K_i. Het systeembeheer is in handen van SURFnet. Er is geen veiligheidsonderzoek uitgevoerd naar deze beheerders. Er wordt hier vertrouwd op het feit dat een gerenommeerde instelling als SURFnet zich geen misdragingen kan veroorloven.

Zoals altijd is ook bij dit systeem het sleutelbeheer belangrijk. TTPI beschikt voor de verkiezingen over alle sleutels. Volgens het officiële stemprotocol (gepubliceerd op Rijnlands verkiezingsinformatie site) worden die 'door hen na gebruik vernietigd en in bewaring gegeven bij de notaris'. Als de sleutels inderdaad vernietigd zijn is er geen probleem, maar als TTPI tijdens het opmaken van de uitslag nog steeds over de sleutels beschikt hebben zij in principe de mogelijkheid om stemmen te vervangen. Als ontwerpers van het systeem kennen zij natuurlijk als geen ander de mogelijkheden die er zijn om te frauderen. Dit gevaar wordt overigens beperkt door de hash die gemaakt wordt van de ontvangen stemmen door SURFnet voordat zij aan TTPI worden doorgegeven.

Verder is het sleutelbeheer ook aan de kant van de kiezer van belang. Op de stemkaart staat immers de sleutel voor die kiezer. Mocht deze sleutel gekopieerd worden of anderszins beschikbaar komen, bestaat de mogelijkheid om een reeds uitgebrachte stem van de kiezer zelf, ongeldig te maken door nog minimaal twee keer te stemmen met die sleutel waarbij er op verschillende kandidaten wordt gestemd. Ongeacht de oorspronkelijke keuze van de kiezer zelf, wordt zijn stem nu zeker als ongeldig aangemerkt.

Het laatste aspect dat wij hier noemen is inherent aan alle verkiezingen die niet op een stembureau plaatsvinden: ze zijn gevoelig voor het zogenaamde *family voting*. Oftewel, de dominante huisgenoot die afdwingt dat door alle bewoners op een bepaalde kandidaat gestemd wordt. Verder kan een kiezer zijn stem verkopen. Als hij zijn technische stem namelijk verkoopt voordat de lijst met ontvangen stemmen is gepubliceerd, heeft de koper een bewijs dat er inderdaad op de afgesproken kandidaat is gestemd. De grootschalige invoering van elektronisch stemmen vraagt dan ook om een zorgvuldige (politieke) afweging van deze risico's.

Conclusie

Verschillende partijen –waaronder de auteurs– hebben naar de veiligheid van het systeem gekeken en hebben vooral opgemerkt dat het systeem veilig is in die zin dat fraude gedetecteerd kan worden. Er is echter ruimte voor meer compartimentalisatie, waarbij verschillende, onafhankelijke partijen verantwoordelijk zijn voor de sleutelgeneratie, het tellen van de elektronische stemmen, de controle software voor kiezers, en voor het samenvoegen van elektronische stemmen en poststemmen. Belangrijk is dan ook dat na afloop een andere partij dan TTPI ook daadwerkelijk alle ingebouwde checks naloopt om te kunnen concluderen dat er niet gefraudeerd is.

Samenvattend gaat het hier om een relatief eenvoudig, origineel en inzichtelijk systeem, dat met de nodige zorgvuldigheid en transparantie is ingevoerd.

Zoals in iedere nieuwe procedure zijn punten van verbetering mogelijk. De ervaring die met dit systeem wordt opgedaan is ongetwijfeld waardevol. Als het dan ook gaat om het gebruik van RIES bij deze waterschapsverkiezingen, stemmen wij duidelijk voor!

`www.internetstemmen.nl` Rijnland, stemsite
`www.iscit.surfnet.nl/team/Herman/verslag.html` ISCIT, Scriptie Herman Robers
`www.ososs.nl/article.jsp?article=9698` OSOSS, KOA, Kiezen op Afstand nu open source
`www.rijnlandkiest.nl` Rijnland, verkiezingsinformatie
`www.surfnet.nl/bijeenkomsten/ries` SURFnet, Workshop RIES

Kader 3: Info op het web

Bart Jacobs en Engelbert Hubbers

Prof.dr. Bart Jacobs is hoogleraar beveiliging en correctheid van programmatuur aan het Nijmeegs Instituut voor Informatica en Informatiekunde (NIII) van de Radboud Universiteit Nijmegen (`bart@cs.ru.nl`). Dr. Engelbert Hubbers is verbonden aan hetzelfde instituut. Zijn onderzoek spitst zich toe op smartcards en beveiliging.