Verkenning Risicobeperking internetstemmen voor stemmers buiten Nederland

Rapport

Management, Science & Technology

Verkenning Risicobeperking internetstemmen voor stemmers buiten Nederland

U2017/02168/HJO

van: dr. ir. Hugo Jonker
Open Universiteit
14 maart 2017

Open Universiteit
www.ou.nl

Inhoud

Management summary

Een groot voordeel van het gebruik van computers is dat processen makkelijk op te schalen zijn. Als voorbeeld: als men via een computer kan stemmen, dan is het makkelijk voor de overheid om stemmers in het buitenland te laten stemmen.
Dit voordeel werkt echter ook voor iemand die de verkiezingen wil aanvallen. Bij stemmen met pen en papier zal zo'n aanvaller in een stemlokaal moeten zijn, en dan slechts de stemmers die in dàt stemlokaal moeten stemmen kunnen aanvallen. Bij internetstemmen is het risico dat één aanvaller alle stemmers tegelijkertijd zou kunnen aanvallen.

Dit rapport maakt een inschatting van de risico's omtrent internetstemmen voor stemmers in het buitenland. Daarnaast bevat het een verkenning van verschillende systemen gebruikt in de praktijk en wetenschappelijke voorstellen om internetstemmen veilig te laten verlopen.

Het rapport concludeert het volgende:

- Stemmen via internet betekent stemmen in een ongecontroleerde omgeving.
  Dit brengt een aantal risico's met zich mee. Vandaar dat stemmen via internet alleen wenselijk is indien het opzetten van stemlokalen ter plekke niet realistisch is.
- Om het democratisch proces te waarborgen, moet een stemsysteem de verliezende partij kunnen overtuigen van zijn/haar verlies. Een stemsysteem dat aanvallen kan voorkomen, maar geen bewijs kan leveren, schiet dus tekort.
- Het is erg makkelijk voor een aanvaller om een computer van een stemmer in het buitenland volledig onder controle te krijgen, een zogenaamde *man-in-the-browser*.
- Dit geldt eveneens voor een smartphone.
  Een smartphone kan dus **niet** worden ingezet om internetstemmen veiliger te maken.
- De computer waarop gestemd wordt, mag dus niet vertrouwd worden.
  Vanuit veiligheidsoogpunt moeten we ervan uitgaan dat deze computer geheel onder controle van de aanvaller staat.
- Internetstemsystemen van andere landen waarbij de stemmer via internet stemt schieten te kort op het gebied van veiligheid.
- Het risico van internetstemmen kan alleen worden ingeperkt door buiten het zicht van de computer met de stemmer te communiceren.
- op drie manieren ingeperkt worden:
  - door internet enkel te gebruiken om blanco stembiljetten te leveren. De stemmer stemt dan via de post;
  - door *code voting*, waarbij de stemmer een uniek “wachtwoord” per kandidaat krijgt via de post;
  - door het gebruik van een speciaal ontwikkeld veilig apparaat dat via de computer met internet en het stemsysteem communiceert.
- Van deze drie sluit stemmen per post goed aan bij de huidige praktijk. Om internetstemmen op basis van code voting of veilige apparaten mogelijk te maken, moet nog een ontwerp- en ontwikkeltraject worden ingezet.

1 Inleiding

Stemmen op papier kan veilig gebeuren. maar de logistieke afhandeling is complex: hoe komen de stembiljetten veilig bij de stemmers, hoe kunnen de stemmers veilig de biljetten invullen en hoe worden de stemmen veilig geteld? Voor stemmers in het buitenland zijn antwoorden op deze vragen ingewikkeld. Dit leidt vaak tot een compromis tussen veiligheid en de mogelijkheid tot stemmen.

Het ligt dan ook voor de hand om te onderzoeken of veilig stemmen voor stemmers in het buitenland op een andere manier kan verlopen – bijvoorbeeld via Internet. Om hier een goed beeld van te krijgen, moeten een aantal zaken helder in kaart gebracht worden:

- Wat is het risico voor de uitslag?
  Stel dat het systeem aangevallen wordt en alle via het internet uitgebrachte stemmen van één aanvaller komen. Wat is de maximale schade die zo'n aanvaller kan doen?
- Kunnen stemmers als groep door een aanvaller aangevallen worden?
  Bijvoorbeeld: kan een aanvaller alle stemmers van een bepaalde werkgever uitsluiten? Of uit een bepaald land?
- Wat is het risico voor een individuele stem?
  Bijvoorbeeld: door wie kan een internetstem geblokkeerd worden? Waar en wanneer kan een aanvaller een internetstem veranderden? Kan een aanvaller een internetstem afluisteren?

Afbakening
Dit rapport focust enkel op één deel van de laatste vraag:
Wat zijn de risico's als de aanvaller de computer van de stemmer heeft overgenomen?
Een dergelijke aanvaller wordt ook wel een *man-in-the-browser* genoemd. Zo'n aanvaller kan bepalen wat er op het scherm gebeurt, en kan alle invoer van de gebruiker (toetsenbord, muis, camera, microfoon) afluisteren en zelfs bewerken voordat een ander programma er toegang toe krijgt. Hoofddoel van dit rapport is om de risico's van een *man-in-the-browser* aanvaller te verhelderen en mogelijkheden bespreken hoe deze risico's ingeperkt danwel ondervangen kunnen worden.

In de security-wereld wordt veiligheid standaard beschreven aan de hand van een beschrijving van drie pijlers:

- De eisen – wat moet er beveiligd worden? (sectie 2)
- De aanvaller – wat kan de aanvaller? (sectie 3)
- Het systeem – hoe werken bestaande systemen? (sectie 4)

Dit rapport houdt deze standaard aan en verduidelijkt aan de hand van de security-eisen en de capaciteiten van een aanvaller welke risico's er kleven aan verschillende types internetstemsystemen en hoe risico's ingeperkt kunnen worden. Aan de hand hiervan worden in sectie 5 de mogelijkheden voor het beperken van de risico's van internetstemmen op een rij gezet. Dit wordt gevolgd door de conclusies (sectie 6). Samenvatting en referenties zijn te vinden in de appendix.

2 Security en privacy eisen aan het stemproces

Onderstaande bekende en vaak herhaalde uitspraak vat de kern van security eisen aan het stemproces goed samen:

> *"Een goed stemsysteem moet de verliezers kunnen overtuigen dat ze terecht verloren hebben".*
> *Prof. dr. Dan Wallach, Rice University.*

Dit betekent dat een stemsysteem méér moet doen dan aanvallen voorkomen of afslaan. Een veilig stemsysteem moet kunnen bewijzen dat er geen aanval is geweest. Dit rust op aantoonbaarheid van de volgende pijlers[1]:

- **Controleerbaarheid**: de uitslag moet exact corresponderen met de uitgebrachte stemmen,
- **Vrijheid**: een stemmer moet zijn keuze in vrijheid, zonder dwang, kunnen maken.

De eerste voorwaarde waarborgt correctheid van de uitslag. De tweede voorwaarde waarborgt dat iedere stemmer onafhankelijk van invloed van buitenaf (bedreigingen, omkopingen, …) zijn/haar stem kan uitbrengen. Aan de hand van een algemene beschrijving van het stemproces kunnen deze voorwaarden preciezer worden gesteld.

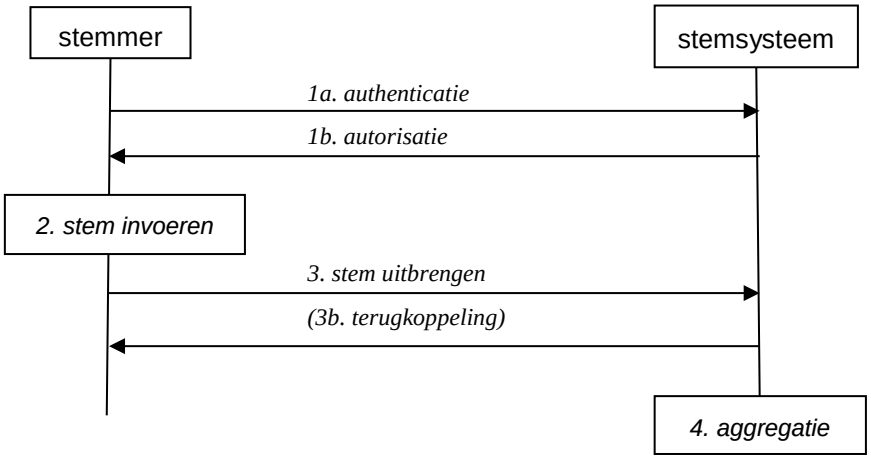

Fig. 1: Fasen in een stemsysteem

In stemsystemen zijn in het algemeen de volgende fasen te onderscheiden (zie ook figuur 1):

1. **Autorisatie**: een persoon autoriseert zich als iemand die een stem mag uitbrengen.
2. **Invoer**: de stemmer drukt zijn/haar stem uit.
3. **Stem uitbrengen**: de stemmer geeft deze stem aan het systeem.
   Eventueel volgt hierop een terugkoppeling naar de stemmer.
4. **Aggregatie**: alle stemmen worden geteld en de uitslag wordt bekend gemaakt.

Bijvoorbeeld: bij stemmen op papier is fase 1 het tonen van de identiteit en de stembrief van de persoon, waarna de stemmer een stembiljet krijgt. Fase 2 behelst het zetten van een rode stip naast een specifieke kandidaat op het stembiljet; fase 3 is het in de stembus stoppen van het stembiljet; in fase 4 ten slotte wordt de stembus geopend en het aantal stemmen per kandidaat geturfd.

1 Deze categorisatie omvat de eisen aan het verkiezingsproces zoals geformuleerd door de commissie Korthals-Altes [6]. De toepassing van deze categorisering op de genoemde fasen leidt tot een andere manier om deze eisen uit te drukken, waarbij de eis van toegankelijkheid buiten beschouwing blijft.

Merk op dat dit geen losstaande stappen mogen zijn: alleen stemmers die geautoriseerd zijn, krijgen een stembiljet en mogen dat biljet in de stembus stoppen. Bij stemmen in een stemlokaal wordt het koppelen van de autorisatie aan het uitbrengen van de stem gewaarborgd door waarnemers: de leden van het stembureau laten alleen geautoriseerde stemmers een stembiljet in de stembus stoppen. Bij het stemmen in het buitenland zijn er niet altijd waarnemers ter plekke, de autorisatie moet dan op een andere wijze aan de uitgebrachte stem gekoppeld kunnen worden.

In deze fasen wordt er als volgt tussen het stemsysteem en de stemmer gecommuniceerd:

1. **Autorisatie**: de uitgebrachte stem moet geautoriseerd zijn. Dat kan voorafgaand aan het stemmen (stap 1a, 1b in figuur 1), maar mag ook pas bij het uitbrengen van de stem worden gewaarborgd (in stap 3 in figuur 1). Indien een aparte autorisatie-stap wordt ingebouwd, dan verloopt de communicatie als volgt:
   - eerst van stemmer naar het stemsysteem (bewijs identiteit, stap 1a)
   - dan van stemsysteem naar stemmer (stembescheiden, zoals stembiljet, stap 1b)
2. **Invoer**: geen communicatie (stem wordt lokaal uitgedrukt).
3. **Stem uitbrengen**: van stemmer naar stemsysteem (stap 3 in figuur 1). Eventueel kan het systeem hierover een terugkoppeling terugsturen (bijv. een ontvangstbevestiging).
4. **Aggregatie**: geen communicatie.

Iedere communicatiestap kan in theorie verlopen via een willekeurig communicatiekanaal – per post, via internet, via SMS, via telefoon, etc. Daarbij moet zowel de controleerbaarheid als de veiligheid gewaarborgd blijven.

2.1 Controleerbaarheid

Om de controleerbaarheid te waarborgen, moet ieder van de fasen afzonderlijk te controleren zijn. Preciezer gezegd:

1. **Autorisatie**: mag deze persoon wel een stem uitbrengen?
   (is deze persoon inderdaad een stemmer wiens oproepkaart nog niet gebruikt is?)
2. **Invoer**: Telt de uitdrukking van de stem wel voor de gewenste kandidaat?
   (telt het rode stipje wel voor de kandidaat waarop de stemmer wil stemmen?)
3. **Stemmen**: is de stem correct in het systeem opgeslagen?
   (is het biljet, zoals het in de stembus zit, niet veranderd ten opzicht van toen de stemmer het in de stembus stopte?)
4. **Aggregatie**: wordt de opgeslagen stem correct geteld?
   (wordt het biljet bij het tellen ook daadwerkelijk als stem voor de gekozen kandidaat geteld?)

Bij stemmen op papier zijn al deze fasen eenvoudig te verifiëren: de stemmer kan het hele proces observeren en zien dat alles ordentelijk verloopt.

Internetstemsystemen kennen dezelfde fasen en moeten dus aan dezelfde eisen voldoen. In de praktijk is dit een uitdaging: hoe weet het systeem zeker dat degene achter de computer ook daadwerkelijk een stemmer is die nog mag stemmen? Hoe weet een stemmer zeker dat wat de computer op het beeldscherm beweert, ook daadwerkelijk is wat de computer over internet verstuurt? Wordt datgene wat de computer verstuurd ook zo opgeslagen? En wordt de opgeslagen stem dan ook wel correct geteld?

2.2 Vrijheid

Vrijheid van het stemproces kan worden gewaarborgd door de anonimiteit van de stemmer te verzekeren. In het extreemste geval moet dan zelfs gezorgd worden dat niemand überhaupt kan nagaan óf de stemmer heeft gestemd (laat staan voor wie): anders zou een aanvaller dwang kunnen uitoefenen ("niet stemmen of anders..."). Deze sterke eis wordt in de praktijk niet gerealiseerd, immers een stemlokaal moet openbaar toegankelijk zijn om de controleerbaarheid te waarborgen.
In de praktijk zorgt het huidige stemsysteem in Nederland dat de keuze van de stemmer niet gelekt[2] wordt.

Ook deze eis dient in ieder van de fasen te worden gewaarborgd:

1. **Authenticatie**: Houdt het systeem geheim dát de stemmer stemt/gestemd heeft? Zo ja, geheim voor wie?
2. **Invoer**: verbergt de uitdrukking van de stem de gemaakte keuze?
3. **Stemmen**: is de opgeslagen stem niet te koppelen aan de stemmer?
4. **Aggregatie**: is de getelde stem niet tegelijkertijd te koppelen aan zowel de opgeslagen stem als de kandidaat waarvoor de stem telt?

Deze eisen worden bij stemmen op papier gewaarborgd door de procedures in het stemlokaal. Bij internetstemmen kunnen er verschillende technische maatregelen genomen worden (zie sectie 4).

NB: zonder stemlokaal kunnen niet alle vrijheids- en controleerbaarheidseisen 100% gewaarborgd worden. Bijvoorbeeld: een internetstemsysteem kan niet voorkomen dat er iemand over de schouder van de stemmer meekijkt. Vandaar dat internetstemmen alleen wenselijk is indien het opzetten van stemlokalen ter plekke praktisch niet te realiseren is.

2.3 Het huidige systeem voor stemmers in het buitenland

Op dit moment stemmen stemmers in het buitenland via de post[3]. Ze schrijven zich via een brief in (stap 1a in figuur 1) en ontvangen vervolgens via de post twee retourenveloppen en een briefstembewijs (delen stap 1b). Het stembiljet ontvangen ze via post of email (andere deel stap 1b). Na invullen van het stembiljet (stap 2) wordt dit in de eerste retourenvelop gestopt. De eerste retourenvelop en het briefstembewijs wordt in de tweede retourenvelop gestopt en vervolgens via de post geretourneerd naar het stembureau in Den Haag (stap 3). Er volgt geen terugkoppeling of de stem is ontvangen (geen stap 3b). Dit systeem voldoet ten dele aan de eisen van controleerbaarheid en vrijheid:

Controleerbaarheid:

1. **Authenticatie**: **procedureel gewaarborgd.**
   Gewaarborgd tijdens registratie (kopie van identiteitsdocument) en door middel van het ondertekende briefstembewijs in de buitenste envelop.
2. **Invoer**: **ja.**
   Dit werkt precies hetzelfde als bij stemmen in een stemlokaal: de stemmer kan zelf controleren bij welke kandidaat de markering gezet is.
3. **Stemmen**: **nee**:
   Bij stemmen via de post zijn er **geen** speciale procedures genomen die verzekeren dat de stem ongeopend en onveranderd aankomt bij het stembureau in Den Haag.
4. **Aggregatie**: **praktisch onhaalbaar.**
   Het tellen zou openbaar moeten zijn, maar het is voor een stemmer in het buitenland niet praktisch om zelf ter plekke te observeren of het tellen van de stemmen correct verloopt.

2 Zogenaamde "stem-selfies" kunnen bewijzen hoe iemand gestemd heeft en zijn de enige op dit moment toegestane uitzondering op de vrijheids-eis.

3 Er zijn 2 alternatieven: 1) machtigen van iemand die in een stemlokaal kan stemmen; 2) een stempas aanvragen en zelf in een stemlokaal stemmen. Zie http://www.stemmenvanuithetbuitenland.nl/stemmen/ik-woon-elders-in-het-buitenland

Vrijheid:

1. **Authenticatie**: **nee.**
   Een brief van de stemmer naar het stembureau in Den Haag zal praktisch gezien alleen bij verkiezingen voorkomen.
2. **Invoer**: **procedureel gewaarborgd.**
   De binnenste envelop verbergt de gemaakte keuze.
3. **Stemmen**: **procedureel gewaarborgd.**
   Na openmaken van de buitenste envelop wordt het briefstembewijs gecontroleerd. De binnenste envelop wordt vervolgens doorgestuurd en elders geopend (tezamen met de andere binnenste enveloppen).
4. **Aggregatie**: **procedureel gewaarborgd.**
   De koppeling tussen stemmer en stem wordt verbroken na het controleren van de inhoud van de buitenste envelop.

“Procedureel gewaarborgd” wil zeggen dat indien alle procedures worden nageleefd en correct worden uitgevoerd, inbreuken op de eis dan detecteerbaar zouden moeten zijn.
Merk op dat het voor een stemmer in het buitenland praktisch onmogelijk is om te controleren of de procedures inderdaad worden nageleefd.

Een aantal zwakheden van het huidige systeem
Het huidige systeem vertoont een aantal zwakheden, zowel in uitvoering als ten opzichte van controleerbaarheid en veiligheid. Zo moeten stemmers vér van te voren registreren om de stembescheiden nog op tijd te ontvangen. Daarnaast is de post niet perfect: stembescheiden gaan verloren. Het is moeilijk de omvang hiervan in te schatten:

- Stemmen die opgestuurd zijn, maar niet aankomen, worden niet gemist. Ze zijn namelijk niet te onderscheiden van een stembiljet, dat de stemmer uiteindelijk niet opstuurt.
- Als de inschrijving niet aankomt, of de stembescheiden niet bij de stemmer aankomen, dan kàn de stemmer klagen. Sommigen zullen dat doen, sommigen niet. In sommige gevallen zullen de stukken na de klacht alsnog aankomen.

Ten slotte is er bij ieder systeem waarbij buiten een stemlokaal mag worden gestemd het zogeheten “*family voting*” probleem: een aanval waarin één huisgenoot de stemmen van de andere stemgerechtigden in het huis bepaalt (hetzij door onderschepping, hetzij door dwang). Dit probleem kan alleen voorkomen worden door in een gecontroleerde omgeving (zoals een stemlokaal) te stemmen.

3 Wat kan een aanvaller (hoe kwetsbaar is de hardware)?

Om een risico-inschatting te maken, is het belangrijk iets te weten over de aanvaller. Daarbij gaat het niet over *wie* het systeem aanvalt, maar *wat* de aanvaller aan mogelijkheden heeft. Er is duidelijk een verschil tussen wat een hacker op een zolderkamertje kan en de geheime dienst van een wereldmacht kan. Een wereldmacht kan namelijk dure, complexe, tijdrovende aanvallen uitvoeren die veel mankracht vereisen in verschillende landen – dat lukt de hacker niet.

Vanwege de in de opdracht voor dit rapport gestelde afbakening beperken we ons tot één use case: een stemmer die zijn stem uitbrengt via de computer. De gestelde vraag is: in hoeverre kan de gebruikte computer het stemproces aanvallen? In deze sectie schetsen we de mate waarin computers en smartphones vatbaar zijn voor aanvallen.

In de inleiding is reeds gemotiveerd dat voor een concrete uitspraak over risico's tevens de eisen en het gebruikte stemsysteem geconcretiseerd moeten worden. Echter, we kunnen al wel een tweetal scenario's schetsen dat de mogelijkheden van aanvallers schetst. Het eerste scenario illustreert waartoe een man-in-the-browser in staat is, terwijl het tweede scenario een indruk geeft hoe realistisch het is voor een aanvaller om

een specifieke computer van een willekeurige stemmer in het buitenland aan te vallen met een man-in-the-browser aanval. Tot slot gaan we kort in op de kwetsbaarheden van smartphones.

3.1 Het gevaar van een man-in-the-browser aanval

Bij een *man-in-the-browser* aanval heeft de aanvaller de browser geheel overgenomen. Dat wil zeggen: de aanvaller ziet wat de computer op het scherm zou willen zetten, en verandert dat naar zijn eigen inzicht. Daarnaast ziet de aanvaller de muis- en toetsenbord-invoer en geeft dat naar zijn eigen inzicht, al dan niet gewijzigd, door aan de website. De aanvaller heeft dus de volledige controle over wat de gebruiker ziet én over wat de gebruiker als invoer aan een website geeft. Hij kan zaken blokkeren, wijzigen of afluisteren.
Onderstaand voorbeeld uit de wereld van internetbankieren geeft een indruk van het gevaar.

Internetbankieren versus internetstemmen
Een veel gehoorde vraag is: “als bankieren via internet veilig is, waarom zou stemmen via internet dan niet kunnen?”

Allereerst: internetbankieren is niet volmaakt veilig. Bijvoorbeeld: de schadeposten van internet-bankieren waren in Nederland in 2015 € 3,7 miljoen [1], in 2016 € 148.000 [2].

Daarnaast: internetbankieren is fundamenteel anders dan internetstemmen. Het ene draait om geld, het andere om stemmen:
- enerzijds moet internetbankieren aan andere eisen voldoen dan internetstemmen,
- anderzijds is een aanvaller op iets heel anders uit bij internetbankieren dan bij internetstemmen.

Concreet: bij internetbankieren wordt anonimiteit niet vereist. Daardoor kan een fout hersteld worden en het slachtoffer gecompenseerd worden – met een gestolen of gemanipuleerde stem zou dat niet moeten kunnen.
Daarnaast maakt het de aanvaller niet uit van welke bank geld gestolen wordt – maar het maakt hem wel uit welke verkiezingen hij manipuleert.

Voorbeeld van man-in-the-browser aanval[4]
Een bepaalde man-in-the-browser aanval op internet-bankieren verloopt als volgt: de gebruiker logt in op zijn bankrekening. Het saldo is flink hoger dan verwacht door een onverwachte overschrijving (bijv. “jaarcontributie Jansen”). Deze overschrijving bestaat niet echt – de bank heeft hier geen weet van. Wat er is gebeurd: de man-in-the-browser heeft het scherm aangepast, zodat deze “overschrijving” op het scherm is ingevoegd. Ook het saldo wat wordt getoond is aangepast aan deze overschrijving. Vervolgens toont de man-in-the-browser een “mededeling” van de bank waarin staat dat er per ongeluk een overschrijving was gedaan. Het slachtoffer wordt vriendelijk verzocht dat bedrag “terug” te storten.
Het slachtoffer ziet geen probleem en boekt het bedrag “terug”. De bank ziet een geauthentiseerde opdracht van de ingelogde gebruiker voor een overschrijving en voert dus de overschrijving uit.

De *man-in-the-browser* aanval hoeft overigens niet per se zich te beperken tot een browser. Deze aanval kan ook tegen een operating systeem (Windows, OSX, Ubuntu, Android, iOS) worden uitgevoerd. Het resultaat is (vanuit het standpunt van een internetstemsysteem) hetzelfde: de aanvaller beheerst scherm en invoer volledig. Dit leidt tot het risico dat de computer een stem kan leren (voor wie is gestemd), blokkeren (niet doorsturen) of veranderen (op een andere kandidaat stemmen).

3.2 Infecteren van door stemmers gebruikte computers

Een man-in-the-browser aanval is een erg krachtige aanval – maar vereist vrijwel totale controle over de computer. Die aanname lijkt erg sterk. Hoe kan een aanvaller nou net die computers besmetten met zijn man-in-the-browser, die buiten Nederland zijn en wellicht door een stemmer gebruikt gaan worden? Per slot van rekening zijn er zo veel computers in het buitenland, dat het zoeken wordt naar een speld in een hooiberg. Het lijkt onmogelijk om überhaupt de juiste computers te vinden.

4 Deze beschrijving is geïnspireerd op informele discussies met professionals uit het bankwezen en de aanval beschreven op https://krebsonsecurity.com/2011/07/trojan-tricks-victims-into-transfering-funds/

Er is echter een ideale manier om de juiste computers te besmetten: zogenaamde *malvertisements* (samentrekking van malware en advertisement). Computers worden tegenwoordig vaak besmet via advertenties op websites. De advertenties bevatten dan malware, die automatisch geladen wordt. Zo werd in april 2016 een grootscheepse malvertisement-campagne gestart in Nederland [3]. Daarbij werden malvertisements verspreid door een aantal van de meest bezochte sites van Nederland, waaronder nieuwssites nu.nl, sbs6.nl en rtlnieuws.nl.

De drukstbezochte Nederlandse websites kunnen dus worden gebruikt om computers te besmetten met malware. Kan zo'n malvertisement-campagne ook op een bepaalde groep gebruikers gericht worden? Het antwoord is ontluisterend: ja, dat kan.
Dit zit in de wijze waarop bepaald wordt, welke advertenties er worden getoond op een webpagina. Tegenwoordig gaat dat via een veiling. Als een gebruiker een website bezoekt, wordt er achter de schermen razendsnel een veiling georganiseerd om advertentieruimte te verkopen.
De advertentieaanbieders in deze veiling krijgen wat informatie over de gebruiker, zodat ze de hoogte van hun bod kunnen bepalen. Een deel van deze informatie is de locatie en de gebruikte software van de gebruiker. Daarmee heeft een aanvaller genoeg om de computers van stemmers in het buitenland met behulp van malvertisements aan te vallen.

“Targeted malvertisement” aanval op stemmers in het buitenland
Een aanvaller ontwikkelt malvertisements voor de meest voorkomende browsers (bijv. Internet Explorer, Safari, Firefox, Chrome). Hij meldt zich aan als aanbieder van advertenties bij een advertentie-veilingsplatform waar drukbezochte Nederlandse sites advertentieruimte te koop aanbieden. Vervolgens biedt hij alleen voor locaties buiten Nederland.

Daarbij kan de aanvaller zich beperken tot het plaatsen van advertenties op Nederlandstalige nieuwssites. Er zijn maar weinig buitenlanders die niet in Nederland wonen, voldoende Nederlands beheersen om Nederlandstalig nieuws te volgen én daarbovenop ook de interesse hebben om dat nieuws te volgen. De kans dat een buitenlandse bezoeker van een nieuwssite een Nederlander is, is dus vrij groot.

3.3 Infecteren van smartphones

Smartphones zouden in een internetstemsysteem ook een rol kunnen spelen. Zo kan een smartphone uiteraard de rol van een computer overnemen. Daarnaast zijn er een aantal stemsystemen in de wetenschappelijke literatuur die gebruik maken van bevestigings-SMS berichten. Dit wordt gedaan om het man-in-the-browser probleem te omzeilen: de aanname is dan dat een aanvaller niet zowel de smartphone als de browser van een gebruiker kan overnemen.

Helaas is ook deze aanname te sterk. Ook smartphones kunnen met malvertisements besmet worden – de hierboven geschetste aanval werkt dus ook tegen smartphones. Onderzoekers van de Berner Fachhochschule hebben een aanval [4] op het Noorse internetstemsysteem opgezet, waarbij de bevestigings-SMS berichten werden onderschept door malware op de smartphone.
Daarnaast is sinds 2016 zogenaamde “cross-device tracking” software commercieel verkrijgbaar [5]. Het doel van zulke software is om te achterhalen welke verschillende apparaten (laptops, pc's, smart-tv's, smartphones) bij één persoon horen. Dit gebeurt door de verschillende apparaten met elkaar te laten communiceren.

3.4 Veilig communiceren met de stemmer

De conclusie van bovenstaande is dat er op stemsystemen die van een computer en/of een smartphone gebruik maken, aanvallen mogelijk zijn die essentiële eisen aan de veiligheid en controleerbaarheid van een stemsysteem kunnen schenden.
Deze aanvallen berusten op een gemeenschappelijk basisprincipe: de computer danwel smartphone weet welke keuze de stemmer maakt. Dit principe is echter niet noodzakelijk voor een internetstemsysteem.

4 Internetstemmen door andere landen

Verschillende landen hebben al een vorm van internetstemmen gebruikt. In deze sectie volgt een kort overzicht.

Verenigde Staten
De Verenigde Staten gebruiken internetstemmen voor stemmers in het buitenland. In dit geval wordt per email het stembiljet opgestuurd, dat vervolgens wordt uitgeprint en per post wordt geretourneerd. Het proces is vrijwel gelijk aan het huidige Nederlandse proces voor stemmers in het buitenland, als het stembiljet per email wordt verstuurd. De controleerbaarheid en veiligheid worden op dezelfde manier als bij het huidige Nederlandse proces gewaarborgd.

Estland
In Estland bestaat sinds 2005 de mogelijkheid om het gehele stemproces via internet uit te voeren. Om problemen met vrijheid te voorkomen, mag men via internet zo vaak stemmen als men wil: enkel de laatst uitgebrachte stem telt. Ook mag men daarnaast via een stemlokaal stemmen, in dat geval vervallen alle internetstemmen. Om de controleerbaarheid te borgen, gebruikt Estland een smart card reader in combinatie met de Estlandse ID kaart.

Dit systeem is uitgebreid gereviewd en bleek onveilig [7]. Het bleek onder andere mogelijk om de stem aan te vallen met een *man-in-the-browser* aanval. De onderzoekers konden met deze aanval de malware laten stemmen

Noorwegen
In het Noorse stemsysteem ontvangt iedere stemmer na registratie een gepersonaliseerd *code sheet* via de post. Op zo'n code sheet staat voor iedere kandidaat een unieke terugkoppelingscode (zie voorbeeld figuur 2). Om te stemmen, authentiseert de stemmer zich op de website van de verkiezingen, waarna er een SMS code naar de stemmer verstuurd wordt. Met deze code kan de stemmer vervolgens inloggen en een kandidaat naar keuze kiezen. Hierna ontvangt de stemmer een SMS met de terugkoppelingscode van de ontvangen kandidaat.

Net als in Estland, waarborgt het Noorse systeem de vrijheid door stemmers de mogelijkheid te bieden opnieuw te stemmen of door in een stemlokaal te stemmen en daarmee de internetstemmen te invalideren. Het systeem bleek vatbaar voor een aanval, waarbij malware op de telefoon samenspande met malware op de gebruikte computer: de computer bracht onmiddellijk nog een stem uit, terwijl de telefoon de 2^{e} terugkoppelings-SMS onderschepte [4].

.

Kandidaat	**terugkoppeling**
Partij 1 – kandidaat 1	Abdcegfh
Partij 1 – kandidaat 2	123fghi
…	…
Partij 2 – kandidaat 1	5igh43o
…	...

Fig. 2: Voorbeeld van terugkoppelingscodes voor één stemmer in het Noorse stemsysteem

Frankrijk
Het Franse systeem voor internetstemmen wordt uitsluitend gebruikt voor stemmers in het buitenland. Deze registreren zich met een email adres en een mobiel nummer. Op elk van deze ontvangt de stemmer dan een wachtwoord waarmee hij/zij op de website van het internetstemmen kan inloggen en vervolgens zijn/haar stem kan uitbrengen. Hiervoor wordt gebruik gemaakt van commercieel ontwikkelde software, waarvan de broncode door het bedrijf geheim is gehouden [7].
Dit systeem is in 2006 gereviewd [7] door prof. dr. Andrew Appel van Princeton University. De review is helder: noch vrijheid, noch controleerbaarheid worden door het systeem gewaarborgd. Het is volledig onmogelijk voor toeschouwers om na te gaan of het systeem daadwerkelijk registreert wat de stemmers invoeren. Inmiddels heeft de Franse regering besloten af te zien van internetstemmen bij de volgende verkiezingen [11,12].

Zwitserland
In Zwitserland wordt er op dit moment gewerkt aan de invoer van een internet-stemsysteem voor stemmen in de kantons Neuchâtel en Genève, zowel voor stemmers in het buitenland als voor lokale stemmers. Dit systeem wordt momenteel ontworpen. De volgende beschrijving van het technische ontwerp is gebaseerd op gesprekken met prof. dr. Reto Koenig (Bern University of Applied Sciences), nauw betrokken bij het ontwerpen van dit systeem.

De stemmers ontvangen per post een eerste en tweede wachtwoord en een boek met terugkoppelingscodes. Een stemmer logt in op de website met het eerste wachtwoord en klikt op de kandidaat van zijn/haar keuze. Hierop komt de bij de kandidaat horende terugkoppelingscode in beeld. Vervolgens bevestigd de stemmer zijn/haar stem door het tweede wachtwoord in te voeren.

De vrijheid wordt in dit ontwerp niet gewaarborgd – dat kan niet met enkel technische middelen, daar moeten organisatorische maatregelen voor worden genomen (zoals bijvoorbeeld de mogelijkheid tot het vaker uitbrengen van een stem).

De controleerbaarheid wordt op een aantal punten gewaarborgd: de terugkoppelingscode garandeert dat het stemsysteem de invoer heeft ontvangen, terwijl de bevestiging verzekert dat dit inderdaad de keuze van de stemmer was.

Prof. dr. Koenig geeft aan dat de browser in dit systeem vertrouwd moet worden – de browser leert zowel de wachtwoorden als de gemaakte keuze van de stemmer. Dit is bekend bij de ontwerpers en een bewuste keuze.

Conclusie
Er zijn twee typen systemen in gebruik waarbij internet een rol speelt:

- Stemsystemen waarbij de stembescheiden (inclusief blanco stembiljet) via internet worden geleverd, waarna de stemmer via de post stemt.
- Stemsystemen waarbij de stemmer via internet stemt.

Bij het eerste type kan controleerbaarheid enigszins procedureel gewaarborgd worden, vergelijkbaar met briefstemmen. Bij het tweede type kan de vrijheid enigszins procedureel gewaarborgd worden door herstemmen toe te staan en/of door stemmen in een stemlokaal de internetstem te laten overschrijven.

Bij het eerste type kan vrijheid niet technisch gewaarborgd worden. Bij alle varianten hierboven van het tweede type kan een *man-in-the-browser* aanvaller de keuze van de aanvaller leren, en bovendien de stem veranderen – hierdoor is de controleerbaarheid van de besproken systemen niet gewaarborgd.

5 Beperken van het risico van internetstemmen

Een van de problemen bij internetstemmen is dat de stemmer een computer gebruikt niet vertrouwd kan worden (man-in-the-browser). De man-in-the-browser kan een stem (zie sectie 3):

- te weten komen,
- blokkeren, of
- proberen te veranderen.

NB: als de stem via een computer wordt uitgebracht (stap 3 in figuur 1), kan een man-in-the-browser dit altijd blokkeren. Dit kan niet voorkomen worden, om toch een stem uit te brengen als een man-in-the-browser het stemmen blokkeert zal een andere computer gebruikt moeten worden.

Apart communicatiekanaal nodig

De enige manier om te voorkomen dat een man-in-the-browser een stem te weten komt of kan veranderen is om te zorgen dat de stemmer en het stemsysteem deels buiten de computer om communiceren. Via die communicatie kunnen ze de man-in-the-browser buiten de deur houden.

Een poging hiertoe waren de terugkoppelingscodes in het Noorse systeem(figuur 2): zolang de computer deze codes niet kent, kan de computer geen correcte terugkoppelingscode tonen. Echter, als de terugkoppelingscode via de computer bij de stemmer komt, dan leert de computer de koppeling tussen de terugkoppelingscode en de gekozen kandidaat. De computer kan nu de stemprocedure afbreken, zelf een stem uitbrengen en vervolgens de terugkoppelingscode van de door de stemmer gekozen kandidaat tonen.

Voorkomen dat de computer de stem leert: code voting

Een manier om dit te voorkomen is *code voting* [9]: iedere stemmer krijgt een gepersonaliseerd code-sheet thuisgestuurd met voor iedere kandidaat één stemcode en één terugkoppelingscode, zie figuur 3. De codes zijn volstrekt willekeurig en voor iedere stemmer anders. Een stemmer kan dan stemmen door de stemcode van de gekozen kandidaat in te geven. De computer ziet dan een stemcode, maar kan niet dat niet koppelen aan een kandidaat. Vervolgens komt er een terugkoppelingscode terug. De computer weet dan dat de code en de terugkoppelingscode bij elkaar horen, maar de computer kent geen enkele andere geldige code. Daarnaast heeft de computer ook geen idee welke codes bij welke kandidaten horen.

Kandidaat	**stemcode**	**terugkoppelingscode**
Partij 1 – kandidaat 1	2a8 – d5d – f9c – c37	abdc egfh
Partij 1 – kandidaat 2	b2a – e8f – 7e8 – f3e	123f ghij
…	…	…
Partij 2 – kandidaat 1	b2a – e8f – 7e8 – f3e	5igh 43xc
…	…	...

Fig. 3: Voorbeeld van een code sheet in Code Voting [9].

Code voting beschermt de uitgebrachte stem tegen manipulatie. Alleen een aanvaller die de code sheet van de stemmer kent, kan de stem manipuleren. Zonder code sheet kun je de stem hooguit blokkeren – de codes zijn zo lang dat het praktisch onmogelijk is om toevallig een andere code te raden.

Een nadeel van code voting is dat iedere stemmer zijn of haar persoonlijke code sheet moet ontvangen. Als dit via de computer zou gebeuren, dan kan de computer dit onderscheppen en alle codes te weten komen.

Dit geldt voor ieder geheim dat de gebruiker en het stemsysteem kennen, maar de computer niet. Op de een of andere manier zal het stemsysteem een geheim moeten delen met de stemmer zonder dat de computer dit geheim leert.

A**part communicatiekanaal moet veilig zijn**

Hier is een apart communicatiekanaal voor nodig – een kanaal waar de computer niet bij kan. Dit kanaal kan niet via een smartphone opgezet worden. Op zich staat een smartphone los van de computer, maar dankzij de aanval van Koenig et al. op het Noorse stemsysteem [4] weten we dat het mogelijk is om malware op een smartphone te laten samenwerken met malware op een computer. Het Amerikaanse standaardisatie-instituut NIST raadt SMS dan ook af als tweede verificatiekanaal [13].

Er blijven dan twee opties over:

i. Communiceren per post,
ii. Een speciaal veilig apparaat met beeldscherm en toetsenbord dat veilig met het stemsysteem kan communiceren.

Communiceren per post

Communicatie per post kan op twee manieren worden ingezet:

- het blanco stembiljet wordt op de computer aangeleverd, uitgeprint, ingevuld en per post teruggestuurd,
- per post worden geheimen naar de stemmer gestuurd (zoals bijvoorbeeld in code voting), waarmee de stemmer per internet kan stemmen zonder dat de man-in-the-browser iets van de stem te weten komt.

De eerste optie wordt op dit moment al deels gebruikt: het stembiljet kan per email worden opgestuurd. Echter, overige stembescheiden zoals de oproepkaart worden nog per post gestuurd.
Alle stembescheiden per email te sturen (dus: stap 1b uit figuur 1 via het internet) zal aanzienlijke tijdswinst opleveren ten opzichte van de huidige situatie. Dan bestaat uiteraard het risico dat een stemmer vaker dan eenmaal stemt, of dat een niet-ingeschreven persoon een stem instuurt. Het proces van het ontvangen en verwerken van de stem zal hiervoor moeten worden aangepast. In vergelijking met andere opties lijkt dit de kleinste en eenvoudigst uit te voeren oplossing.

De tweede optie kan het risico van een man-in-the-browser aanval significant inperken. Dat zal afgewogen moeten worden tegen de gebruikersvriendelijkheid: met 20 partijen met tot 40 kandidaten zijn er dus minimaal 60 (20+40) volstrekt willekeurige codes nodig die lang genoeg zijn dat een man-in-the-browser ze niet kan raden.

Stemmen met een veilig apparaat

Stemmen met behulp van een veilig apparaat zou kunnen lijken op internetbankieren zoals sommige Nederlandse banken dat doen, zie bijvoorbeeld figuur 4.
Het stemsysteem communiceert via een beveiligd kanaal met het apparaat. De communicatie verloopt via de computer (en dus via de man-in-the-browser), maar omdat het kanaal beveiligd is, kan deze niets veranderen. Daardoor zou een aanval van de man-in-the-browser voorkomen moeten worden.

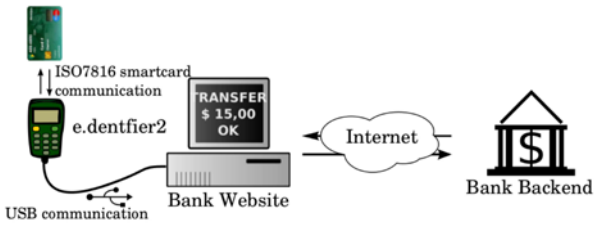

Fig. 4: Voorbeeld van een apparaat om man-in-the-browser aanvallen op internetbankieren te voorkomen, overgenomen uit [10].

Dat was echter niet het geval bij sommige van deze apparaten voor internetbankieren. Onderzoekers van de Radboud Universiteit creëerden man-in-the-browser malware die zorgde dat een malafide transactie werd goedgekeurd als de gebruiker ingelogd was [10].

Om dit type aanvallen op het stemsysteem te voorkomen, moet zo'n apparaat aan de volgende eisen voldoen:

- het apparaat toont uitsluitend berichten die van het stemsysteem afkomen
- het apparaat mag alleen iets terugsturen als
  - het apparaat eerst een zojuist ontvangen bericht op het scherm toont,
  - en de gebruiker daarna invoer heeft gegeven en bevestigd.

Een nadeel van het gebruik van veilige apparaten is dat iedere stemmer een apparaat nodig heeft om te kunnen stemmen. Als het apparaat geüpdatet moet worden, dan moet iedere stemmer een nieuw apparaat ontvangen.

6 Conclusie

Het risico van een *man-in-the-browser* kan theoretisch ingeperkt worden. Kleine fouten in de praktische uitvoering zouden het systeem echter alsnog kwetsbaar maken voor aanvallen. Het is triviaal om een succesvolle aanval op te schalen tot alle mogelijke gebruikers van het internetstemsysteem. Dit is niet te voorkomen, maar inherent aan het internet. Vanwege de triviale schaalbaarheid van aanvallen, **dient internetstemmen te allen tijde beperkt te blijven tot een kleine groep**.

Er zijn drie verschillende oplossingen geïdentificeerd die de risico's inperken:

- stemmen per brief, waarbij alle stembescheiden per email zijn ontvangen,
- code voting, waarbij de codes per post worden opgestuurd,
- veilige apparaten gebruiken om de veiligheid van internetstemmen te waarborgen.

Stemmen per brief sluit goed aan bij het huidige systeem, waar er al ervaring mee is. Nu wordt per email een blanco stembiljet gestuurd. Met een (relatief) kleine aanpassing kan het huidige systeem worden uitgebreid om alle stembescheiden per email te ontvangen. Dit vereist wel dat bij ontvangst controles worden ingevoerd om dubbelstemmen en stemmen van niet-geregistreerden af te vangen.

De andere twee oplossingen, code voting en gebruik van veilige apparaten, kunnen niet rechtstreeks ingepast worden. Om een van deze oplossingen te gebruiken, zal eerst een ontwerp- en ontwikkeltraject moeten worden ingezet.

Verantwoording

Dit rapport is samengesteld op basis van literatuuronderzoek en gesprekken met: prof. dr. Dan Wallach (Rice University, USA), prof. dr. Sjouke Mauw (University of Luxembourg, Luxembourg), prof. dr. Reto Koenig (Bern University of Applied Sciences, Zwitserland), prof. dr. Marko van Eekelen (Open Universiteit, Nederland).

Samenvatting

Dit rapport onderzocht hoe het risico van een *man-in-the-browser* aanvaller ingeperkt kon worden voor een internetstemsysteem voor Nederlandse stemmers in het buitenland. Daartoe is er exclusief gefocust op de veiligheid – andere aspecten zoals gebruiksvriendelijkheid zijn buiten beschouwing gelaten.

De grote winst van een internetstemsysteem is schaalbaarheid: het is makkelijk om het systeem wereldwijd uit te rollen via internet. Echter, ditzelfde geldt voor een aanvaller: als de aanvaller het systeem op één plek weet te breken, kan hij de aanval via internet makkelijk wereldwijd uitrollen.

Het rapport onderzocht wat een *man-in-the-browser* kan (sectie 3). Hier bleek dat internetstemmen en internetbankieren wezenlijk verschillen: gestolen geld wordt door de bank gecompenseerd, wat onmogelijk is met een gestolen stem. Daarnaast werd geschetst hoe een malware aanval op Nederlandse nieuwssites uit 2016 zou kunnen worden uitgebouwd om specifiek Nederlandse stemmers in het buitenland te infecteren. Tot slot werd getoond dat het mogelijk is om ook een smartphone te infecteren met malware, om vervolgens deze smartphone met de *man-in-the-browser* te laten samenwerken.

Vervolgens besprak het rapport kort hoe andere landen internetstemmen organiseren (sectie 4). De internetstemsystemen van Estland, Noorwegen en Frankrijk zijn allen onderzocht door security experts en onvoldoende bevonden. Het systeem van twee kantons in Zwitserland wordt momenteel ontworpen. De ontwerpers hebben hier een bewuste keuze gemaakt voor meer gebruiksvriendelijkheid ten koste van veiligheid van het stemsysteem. In het huidige ontwerp wordt de browser vertrouwd – dit ontwerp is dus niet bestand tegen een *man-in-the-browser*. Het systeem van de Verenigde Staten emailt blanco stembiljetten, die vervolgens per post worden geretourneerd. Dit is ook een mogelijkheid in het huidige Nederlandse systeem voor stemmers in het buitenland. De controleerbaarheid en veiligheid worden dan ook op dezelfde manier als bij het huidige Nederlandse stemmen voor stemmers in het buitenland gewaarborgd.

Tot slot schetste het rapport drie manieren om het risico van internetstemmen in te perken: stembescheiden per email ontvangen om ze per post te retourneren, code voting en het gebruik van veilige apparaten. In het huidige systeem wordt al per email een blanco stembiljet opgestuurd. Dit uitbreiden tot alle stembescheiden is een (relatief) kleine aanpassing. Echter: aan de ontvangende kant moeten dan controles worden ingevoerd om dubbelstemmen en stemmen van niet-geregistreerden eruit te filteren.
Code voting werkt door iedere stemmer buiten internet om een gepersonaliseerd *code sheet* te sturen. Op een *code sheet* staat per kandidaat één code. Omdat de codes volledig willekeurig zijn, kan de *man-in-the-browser* geen codes raden. Daardoor kan hij enkel nog het stemmen blokkeren.
De veilige apparaten die voor internetstemmen gebruikt zouden kunnen worden, lijken op de apparaten die door sommige banken voor internetbankieren worden gebruikt. Echter, de communicatie en de interactie moet wel veilig verlopen. Dit gebeurde niet bij alle internetbankier-systemen. De veiligheid van een ontwerp en een implementatie moeten dus onafhankelijk onderzocht worden.

Referenties

[1] Nu.nl, “Schade door fraude met internetbankieren stabiel in 2015”. http://www.nu.nl/economie/4287660/schade-fraude-met-internetbankieren-stabiel-in-2015.html, laatst bezocht op 8 februari 2017.

[2] Nederlandse Vereniging van Banken, “Hoe hoog is de schade door fraude met internetbankieren?”. https://www.nvb.nl/veelgestelde-vragen/veiligheid-fraude/1816/hoe-hoog-is-de-schade-door-fraude-met-internetbankieren.html, laatst bezocht op 9 februari 2017.

[3] Fox-IT, “Large malvertising campaign hits popular Dutch websites”. https://blog.fox-it.com/2016/04/11/large-malvertising-campaign-hits-popular-dutch-websites/, laatst bezocht op 9 februari 2017.

[4] Reto E. Koenig, Philipp Locher, Rolf Haenni, “Attacking the Verification Code Mechanism in the Norwegian Internet Voting System”. In: *Proceedings of the 4th International Conference on E-Voting and Identity (Vote-ID 2013)*, pp. 76-92, Springer, 2013.

[5] Dan Goodin, “Beware of ads that use inaudible sound to link your phone, TV, tablet, and PC”. Arstechnica, https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/, laatst bezocht op 9 februari 2017.

[6] Eindrapport Commissie-Korthals Altes, “Stemmen met vertrouwen”. 27 september 2007. https://www.kiesraad.nl/adviezen-en-publicaties/rapporten/2007/09/27/eindrapport-commissie-korthals-altes-stemmen-met-vertrouwen

[7] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, “Security Analysis of the Estonian Internet Voting System”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14),* pp 703-715, ACM, 2014. DOI: https://doi.org/10.1145/2660267.2660315; begeleidende video: https://www.youtube.com/watch?v=iit5WdLYwns

[8] Andrew W. Appel, “Ceci n'est pas une urne: on the Internet vote for the *Assemblée des Français de l'étranger*”. https://www.cs.princeton.edu/~appel/papers/, laatst bezocht op 7 maart 2017.

[9] David Chaum, “Surevote: Technical overview”. In *Proceedings of the Workshop On Trustworthy Elections (WOTE2001)*. Slides beschikbaar op http://www.iavoss.org/mirror/wote01/pdfs/surevote.pdf, laatst bezocht op 14 maart 2017.

[10] Arjan Blom, Gerhard de Koning Gans, Erik Poll, Joeri De Ruiter, and Roel Verdult. "Designed to fail: A USB-connected reader for online banking." In *Nordic Conference on Secure IT Systems*, Lecture Notes in Computer Science volume 7617, pp. 1-16. Springer, 2012.

[11] Marine Le Pennetier, Leigh Thomas, “France drops electronic voting for citizens abroad over cybersecurity fears”. Reuters, http://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233?il=0

[12] Jean-Marc Ayrault, “Arrêté du 17 mars 2017 relatif au vote par correspondance électronique pour l'élection de députés par les Français établis hors de France”. Journal officiel de la République française, 24 maart 2017. https://www.legifrance.gouv.fr/eli/arrete/2017/3/17/MAEF1708315A/jo/texte

[13] Paul Grassi et al, “DRAFT NIST Special Publication 800-63B Digital Identity Guidelines”. National Institute of Standards and Technology (NIST), 27 juli 2016. https://pages.nist.gov/800-63-3/sp800-63b.html