Samenvatting

Het Ministerie van Verkeer en Waterstaat heeft Fox-IT gevraagd te assisteren bij het beoordelen van de internetstemvoorziening die door de waterschappen is ontworpen voor de waterschapsverkiezingen van november 2008. De organisatie waarin de waterschappen samenwerken, het Waterschapshuis, heeft daartoe documentatie ter beschikking gesteld en medewerking verleend aan aanvullend onderzoek door Fox-IT.

Op basis van dit onderzoek constateert Fox-IT dat de internetstemvoorziening in opzet een elegant en doordacht systeem voor internetstemmen is. Echter, over de huidige uitwerking van het concept moet worden vastgesteld dat dit kwaadwillenden diverse mogelijkheden biedt om de uitslag te beïnvloeden, het verkiezingsproces te saboteren en/of om binnen afzienbare tijd te herleiden wie op wie heeft gestemd.

Deze constatering is gebaseerd op de volgende waarnemingen:

- Het gebruik van een gedateerde versleutelingsmethode in combinatie met het opnemen van individuele burgerservicenummers (BSN) in de versleutelde verkiezingsuitslag betekent dat het stemgeheim maximaal tot 2030 kan worden gewaarborgd. Met andere woorden, uiterlijk in 2030, doch waarschijnlijk (veel) eerder, zal het mogelijk zijn te reconstrueren welke kiezer op welke kandidaat stemde in 2008.

- Met de kracht van de huidige generatie PC's is het berekenen van geldige stemcodes haalbaar binnen maximaal 30 uur. De informatie die hiervoor nodig is wordt voorafgaand aan de stemperiode gepubliceerd, waarna de berekening kan starten. Aangezien de stemperiode twee weken duurt zou een kiezer die over de juiste software beschikt minimaal 11 geldige stemmen kunnen uitbrengen op een kandidaat naar keuze.

  Kwaadwillenden die de controle hebben over meerdere PC's en/of gespecialiseerde apparatuur kunnen evenredig meer stemmen uitbrengen. Er zijn gevallen bekend van cybercriminelen die meer dan een miljoen computers onder hun controle wisten te krijgen (1)(2). Met de in dit document beschreven methode zouden dergelijke criminelen de uitslag van de waterschapsverkiezingen vrijwel volledig kunnen controleren.

- De huidige implementatie van het internetstemsysteem (het programma dat de internetstemsite en bijbehorende schermen voor beheerders en stembureaus zoals gebruikt in de ketentest juni 2008) vertoont beveiligingsproblemen waardoor diverse controlemaatregelen in het verkiezingsproces kunnen worden omzeild. Zo was het voor de onderzoekers van Fox-IT mogelijk om via het internet toegang te krijgen tot diverse beheerschermen waarin bijvoorbeeld de verkiezingen konden worden stopgezet, en om via deze beheerschermen de database met uitgebrachte stemmen uit te lezen en te manipuleren.

Tot slot is het van belang te vermelden dat gedurende de periode van onderzoek (juni 2008) oordeelsvorming niet mogelijk was met betrekking tot de beveiliging van gebruikte netwerk- en serverinfrastructuren, aangezien deze nog slechts in voorlopige versies beschikbaar waren. Ook een oordeel over de geplande opzet is niet te geven aangezien ontwerpdocumentatie voor netwerken en serversystemen slechts op hoofdlijnen beschikbaar was.

FOX-IT
EXPERTS IN IT SECURITY

Tussenadvies

Advisering toelaatbaarheid internetstemvoorziening waterschappen

Classificatie **VERTROUWELIJK**

Opdrachtgever Ministerie van Verkeer en Waterstaat
SSO F&I, kamer B-1.21
Postbus 20901
2500 EX Den Haag

Betreft Advisering toelaatbaarheid internetstemvoorziening waterschappen

Project nr./Ref. nr. PR-080099
Datum 30-06-2008
Versie 1.0
Auteur Matthieu Hueck, Bartek Gedrojc, Mark Koek, Hans Hoogstraten
Business Unit Forensics, Audits & Training
Pagina's 17

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMRO
no. 55.46.97.041
Chamber of Commerce
Haaglanden no. 27301624

VERTROUWELIJK
Dit document is geclassificeerd als vertrouwelijk. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n) in de distributielijst op de pagina Document Management. Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is mogelijkerwijs vertrouwelijk van aard en valt eventueel onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT BV

Olof Palmestraat 6
2616 LM Delft

P.O. box 638
2600 AP Delft

The Netherlands

Phone: +31 (0)15 284 7999
Fax: +31 (0)15 284 7990
E-mail: info@fox-it.com
Internet: www.fox-it.com

Inhoudsopgave

De status van dit rapport is vertrouwelijk. De appendices bevatten concrete technische informatie die beschrijft hoe in de stemvoorziening kan worden ingebroken. Het is van belang voor de integriteit van de in ontwikkeling zijnde stemvoorziening dat deze "recepten" (nog) niet publiekelijk bekend worden.

1 Inleiding

1.1 Status van deze rapportage

In opdracht van het Ministerie van Verkeer en Waterstaat voert Fox-IT een onderzoek uit naar de internetstemvoorziening die de waterschappen voorbereiden voor de waterschapsverkiezingen van november 2008. In deze tussenrapportage stellen wij u graag op de hoogte van onze voorlopige bevindingen.

Deze bevindingen worden op dit moment nog nader onderzocht en zijn nog in diverse stadia van toetsing en afstemming. Dit tussenadvies mag dan ook niet worden opgevat als definitieve rapportage, slechts om een beeld te geven van de huidige stand van het onderzoek. In het definitieve rapport kunnen elk van de genoemde bevindingen gewijzigd of in het geheel niet terugkeren. Ook kunnen nog bevindingen worden toegevoegd.

1.2 Aanpak

Op basis van de aanvankelijk d.d. 21 mei 2008 door het Waterschapshuis aangeleverde documentatie hebben wij vastgesteld waar naar onze mening nader onderzoek noodzakelijk was om een gefundeerd advies te kunnen geven. De belangrijkste gebieden waar dit tot bevindingen leidt zijn:

a. Een technisch onderzoek naar de beveiliging van de actuele versies van de stemsite en de achterliggende technische componenten zoals netwerken, servers, databases etc.;
b. Een theoretisch onderzoek naar de cryptografische fundamenten van het systeem.

In overleg met het Ministerie en het Waterschapshuis zijn interviews gehouden met de ontwerpers, bouwers en beheerders van het voorgestelde internetstemsysteem, en zijn beveiligingstests uitgevoerd gedurende het "ketenonderzoek" dat in de maand juni heeft plaatsgevonden.

1.3 Objecten van onderzoek

Een problematiek waarmee Fox-IT werd geconfronteerd bij het uitvoeren van het onderzoek is dat de internetstemvoorziening op dit moment nog sterk in ontwikkeling is. Dat betekent dat veel van de documentatie met betrekking tot eerder onderzoek in meer of mindere mate verouderd is, m.a.w. geen betrekking meer heeft op de huidige versie van het ontwerp en de implementatie.

Derhalve is onderzoek uitgevoerd naar:

- Het systeemontwerp zoals dat door het Waterschapshuis d.d. 21 mei 2008 aan Fox-IT is aangeleverd (RIES-2008: Design Information for purposes of evaluation, auteur: Piet Maclaine Pont, MullPon vof, voor Het Waterschapshuis, Versie 0.92);
- De internetstemsite, actief op http://stem.surfnet.nl/ gedurende de tweede ketentest, van 16 t/m 24 juni 2008.

1.4 Opbouw van dit document

Dit document geeft in hoofdstuk 2 algemene (voorlopige) conclusies van het onderzoek zoals dat er op dit moment (30 juni 2008) voor staat. In drie bijlagen wordt vervolgens specifieker ingegaan op de voorlopige bevindingen.

1.5 Nog niet volledige onderzoeksresultaten

Tot 1 juli kan het Waterschapshuis documentatie aanleveren ter ondersteuning van de bewering dat de concept-internetstemvoorziening voldoet aan de wet- en regelgeving en de aanbevelingen van de Raad van Europa. De inschatting van Fox-IT van deze documenten kan dan ook nog niet worden gegeven op dit moment.

Ook is Fox-IT nog in overleg met het Waterschapshuis over een beveiligingstest van het beheerportal voor de Waterschappen, die in de test tijdens het tweede ketenonderzoek ontbrak. Ook heeft het Waterschapshuis nog niet op alle door Fox-IT gedane voorlopige bevindingen kunnen reageren, waardoor ook dit aspect in deze tussenrapportage nog deels ontbreekt.

2 Algemene voorlopige conclusies

Op dit moment luiden de belangrijkste technische conclusies van Fox-IT voorlopig als volgt:

2.1 Veiligheid internetstemsite

- In de internetstemsite zelf lijken de conclusies en aanbevelingen van eerdere reviews op een adequate manier te zijn opgevolgd. Naast enkele kleinere aandachtspunten heeft Fox-IT één tamelijk ernstige onvolkomenheid in de site geconstateerd.

  Deze onvolkomenheid bestaat erin dat de stemkeuze van de kiezer aan het stembureau ter kennis kan komen als de kiezer niet op 'Stemmen' maar op 'Stoppen' klikt. De site doet veel moeite om juist te voorkomen dat het stembureau individuele stemmen kan inzien, echter door een onzorgvuldige implementatie van de knop 'Stoppen' kan deze informatie toch naar het stembureau worden verstuurd.

- Via de internetstemsite trof Fox-IT beheerschermen aan waar zonder het invoeren van wachtwoorden willekeurige verkiezingen konden worden gestart en gestopt, en waar tussenuitslagen konden worden aangemaakt.

- Deze beheerschermen vertoonden ernstige gebreken in de beveiliging waardoor de gehele database met (versleutelde) uitgebrachte stemmen kon worden uitgelezen via het internet. Het is niet uit te sluiten dat op deze manier ook schrijftoegang tot de database kan worden verkregen.

  Navraag bij het Waterschapshuis heeft geleerd dat het hier niet ging om beheerschermen ten behoeve van medewerkers van de waterschappen maar om noodschermen voor technisch beheerders, die alleen op de fysieke locatie van de stemservers toegankelijk horen te zijn.

  Het feit dat deze schermen via het internet toegankelijk waren werd veroorzaakt door het feit dat systeemsoftware nog niet up-to-date was gebracht, en dat de noodschermen op dezelfde servers zijn ondergebracht als de internetstemmenapplicatie.

- Conform eerder gedane bevindingen door anderen constateert Fox-IT dat weinig tot geen actuele documentatie beschikbaar is van server- en netwerkconfiguraties in het achterliggende netwerk. Het is daardoor moeilijk om een oordeel te vormen.

  Het Waterschapshuis heeft nadere documentatie toegezegd, waarbij moet worden opgemerkt dat pas in augustus definitief over de netwerk- en serverconfiguratie zal worden besloten.

2.2 Cryptografisch fundament

In aanvulling op bevindingen die in 2004 zijn gedaan door Cryptomathic en in 2008 door EiPSI constateert Fox-IT het volgende:

- De cryptografiestandaard die wordt gebruikt in de internetstemvoorziening is door de vaststeller van de standaard, het Amerikaanse National Institute for Standards in Technology (NIST), niet meer te vertrouwen na 2030. Dat betekent dat vanaf naar schatting 2030 er organisaties bestaan die over zodanige rekenkracht beschikken dat dan kan worden vastgesteld wat een kiezer in 2008 bij de waterschapsverkiezingen heeft gestemd, gegeven het BSN-nummer van die individuele kiezer.

- Het is mogelijk om binnen de duur van de verkiezingen (2 weken), tenminste 1 geldige stem op een gegeven kandidaat te berekenen, op basis van de vooraf gepubliceerde kandidaat/kiezercombinaties, met behulp van apparatuur ter waarde van maximaal 12.000 euro.

Bovenstaande bevindingen worden op dit moment nog nader onderzocht en zijn nog in diverse stadia van toetsing en afstemming. Dit tussenadvies mag dan ook niet worden opgevat als definitieve rapportage, slechts om een beeld te geven van de huidige stand van het onderzoek. In het definitieve rapport kunnen elk van de genoemde bevindingen gewijzigd of in het geheel niet terugkeren. Ook kunnen nog bevindingen worden toegevoegd.

Appendix 1 Bevindingen beveiligingstest stem.surfnet.nl

Deze bijlage bevat de bevindingen gedaan tijdens de beveiligingstest die Fox-IT heeft uitgevoerd tijdens de tweede ketentest, tussen 16 en 24 juni 2008. Waar nodig zijn de bevindingen bijgesteld op basis van een reactie van het Waterschapshuis.

Bevinding 1.1

De geselecteerde partij en kandidaat worden meegestuurd naar de server wanneer tijdens het kiezen het stemproces wordt afgebroken of de keuze wordt gewijzigd. De informatie wordt meegestuurd in respectievelijk de parameters `radio_group` en `candidate`.

Risico

Hoewel het systeem grote moeite doet om de feitelijke stem van de kiezer niet zichtbaar te laten zijn voor de stemserver gebeurt dat op eenvoudige wijze toch als de kiezer op een verkeerde button klikt.

Bewijs

Door het stemproces af te breken op het moment dat een kandidaat is geselecteerd worden er diverse parameters, waaronder de op dat moment geselecteerde partij en kandidaat naar de server gestuurd. De applicatie verstuurt de volgende HTTP-aanvraag als de gebruiker wil annuleren:

```
POST /server HTTP/1.1
Host: stem.surfnet.nl
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.14)
Gecko/20080419 Ubuntu/8.04 (hardy) Firefox/2.0.0.14
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain
;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: https://stem.surfnet.nl/server
Content-Type: application/x-www-form-urlencoded
Content-Length: 694

pageid=A025&elid=8001&actionreq=stop&language=NL&sessiondata=aWdub3Jlc3Rh
dHVzPWZhbHNlJnJlc3BpZD1mY2QxNDRmNTUwNDFhZTU3N2RmYmI1YThkNTI2MTc1YyY%3D&te
xt_group=Selecteer+de+lijst+van+uw+voorkeur+of+selecteer+%27blanco+stem%2
7%3Cbr%3E+en+klik+op+%27Verder%27.%3Cbr%3E+&text_candidate=Maak+uw+keuze+
en+klik+op+%27Verder%27.&text_group_infomsg=Er+zijn+nog+meer+lijsten%2C%3
Cbr%2F%3E+klik+op+de+scrollbar+--
%3E&text_candidate_infomsg=Er+zijn+nog+meer+kandidaten%2C%3Cbr%2F%3E+klik
+op+de+scrollbar+--
%3E%3Cbr%3E%3Cbr%3E&text_backbutton=Wijzigen&radio_group=8001000103%3A03%
3AWater+Ja%2C+natuurlijk&candidate=8001000103%3A03%3AWater+Ja%2C+natuurli
jk%3A800100010303%3ALeliveld%2C+K.L.N.+%28M%29%3AVinkeveen
```

Bevinding 1.2

De Apache Tomcat webservice die bereikbaar is via de systemen `195.169.124.82` en `192.87.106.194` geeft het versienummer van de software weer.

Risico

Met kennis van het versienummer van de Apache Tomcat webservice kan door kwaadwillende gebruikers gericht worden gezocht naar bekende kwetsbaarheden voor de betreffende versie van de Apache webservice.

Bewijs

Wanneer een niet-bestaande pagina wordt opgevraagd in één van de directories `/test` of `/server`, wordt de volgende regel onderaan de foutpagina weergegeven:

```
Apache Tomcat/5.5.9
```

Het is denkbaar dat het gegeven versienummer niet het daadwerkelijke versienummer is, o.m. doordat het gebruikte besturingssysteem vaak beveiligingsupdates aanbrengt in oude versies zonder versienummers te updaten. Uit tests op bekende beveiligingsproblemen is echter gebleken dat daadwerkelijk versie 5.5.9 (of ouder) van Apache Tomcat in gebruik is.

Bevinding 1.3

De gebruikte versie van de Apache Tomcat webservice is verouderd en bevat meerdere publiekelijk bekende kwetsbaarheden.

Risico

De gebruikte Apache Tomcat versie bevat meerdere publiekelijk bekende kwetsbaarheden. Enkele van deze kwetsbaarheden maken het mogelijk om informatie over de server of de webapplicatie op te vragen. Andere kwetsbaarheden stellen een kwaadwillende mogelijk in staat om Cross-Site Scripting (XSS) of Denial of Service (DoS) aanvallen uit te voeren.

Of de kwetsbaarheden daadwerkelijk kunnen worden uitgebuit hangt van de configuratie van de webservice af. Desondanks is Fox-IT van mening dat het gebruik van een verouderde Apache Tomcat versie een hoog risico met zich meebrengt.

Bewijs

De volgende versie van de Apache Tomcat webservice is door Fox-IT gedetecteerd:

```
Apache Tomcat/5.5.9
```

Een overzicht van de bekende kwetsbaarheden voor deze versie van Tomcat is te vinden op de volgende pagina:

```
http://tomcat.apache.org/security-5.html
```

Bevinding 1.4

Het is mogelijk om van enkele directories op de Apache Tomcat server de inhoud op te vragen.

Risico

Het toestaan van directory listings stelt gebruikers in staat om de aanwezige bestanden in de betreffende directory te bekijken. Deze bestanden kunnen gevoelige informatie bevatten.

Bewijs

De volgende URL's tonen aan dat de Apache Tomcat webservice directory listings toestaat:

```
https://stem.surfnet.nl/server/%5c../css/
https://stem.surfnet.nl/server/%5c../images/
https://stem.surfnet.nl/server/%5c../work/
```

In de directory `work` trof Fox-IT de volgende bestanden aan welke mogelijk gevoelige informatie bevatten:

```
sessions.ser
tldCache.ser
```

Bevinding 1.5

De inhoud van de tabel in de kwitantie (PDF-bestand) kan door de gebruiker worden bepaald. De inhoud van de parameter `tsinfo` in de HTTP-aanvraag bepaalt de inhoud van de tabel in de PDF.

Risico

Indien een kwaadwillende in staat is om de HTTP-aanvraag voor de kwitantie te manipuleren dan kan deze de inhoud van de PDF deels beïnvloeden, waardoor het vertrouwen in het RIES internetstembureau mogelijk kan worden misbruikt voor bijvoorbeeld phishing-aanvallen.

Bewijs

De volgende URL toont een gemanipuleerde kwitantie waarbij de waarde van `ontvangstbevestiging` staat ingesteld op `http://www.fox-it.com`:

```
https://stem.surfnet.nl/pdf?tsinfo=80010001|Hoogheemraadschap%20van%20Rij
nland|700a76ba928c6036-
d7f181f9ccc44df1|%68%74%74%70%3a%2f%2f%77%77%77%2e%66%6f%78%2d%69%74%2e%6
3%6f%6d
```

Bevinding 1.6

Het is mogelijk om de technische stemcodes te achterhalen uit de browsergeschiedenis van kiezers. Bij het downloaden van de kwitantie wordt de parameter `tsinfo` als `GET`-variabele naar de server verstuurd.

Risico

Een kwaadwillende die fysiek toegang heeft tot de computer van een kiezer kan mogelijk de technische stemcodes van deze kiezer achterhalen uit de browsergeschiedenis. In combinatie met eventuele kwetsbaarheden in de browser kan deze kwetsbaarheid mogelijk ook van afstand worden misbruikt.

Bewijs

Na het succesvol uitvoeren van een stem en het downloaden van een kwitantie bleef de volgende URL achter in de browsergeschiedenis:

```
https://stem.surfnet.nl/pdf?tsinfo=80010001|Hoogheemraadschap%20van%20Rij
nland|700a76ba928c6036-d7f181f9ccc44df1|6D72CFFA
```

Bevinding 1.7

De RIES Beheer Portal kan geopend worden vanaf elke plaats op het internet, zonder authenticatie.

Uit de reactie van het Waterschapshuis blijkt dat het hier gaat om noodschermen voor technisch beheerders die alleen op de fysieke locaties van de stemservers bereikbaar zouden moeten zijn. Het betreft dus niet de portalschermen voor de stembureaus bij de waterschappen.

Risico

De RIES Beheer Portal stelt kwaadwillenden in staat om onder andere verkiezingen te starten en te stoppen, statusoverzichten op te vragen en resultaten te bekijken.

Bewijs

De volgende URL toont aan dat de RIES Beheer Portal bereikbaar is vanaf het internet:

```
https://stem.surfnet.nl/server/%5C../admin/
```

Bevinding 1.8

De RIES Beheer Portal bevat kwetsbaarheden die een Cross Site Scripting (XSS) aanval mogelijk maken. Gebruikersinvoer wordt zonder validatie op de betreffende pagina's overgenomen.

Risico

XSS kan gebruikt worden om de bij een gebruiker getoonde website te veranderen of Javascript code uit te voeren op de computer van een gebruiker, waarbij het lijkt alsof deze code afkomstig is van de RIES Beheer Portal. Het is bijvoorbeeld mogelijk om pagina's aan te passen zodat gegevens die worden ingevoerd in wachtwoordvelden niet alleen naar de RIES Beheer Portal gestuurd worden, maar ook naar een aanvaller. Geavanceerdere toepassingen van XSS kunnen het voor aanvallers mogelijk maken om de computer van de gebruiker als een zogeheten 'stepping stone' te gebruiken om verdere aanvallen uit te voeren op het interne netwerk van de gebruiker.

Bewijs

De volgende URL toont aan dat de RIES Beheer Portal kwetsbaar is voor XSS:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001<script>alert('XSS')</script>
```

Bevinding 1.9

Het is mogelijk om met één HTTP-aanvraag een oneindige reeks van HTTP-aanvragen te veroorzaken. Dit gedrag treedt op wanneer een HTTP-aanvraag naar de Apache Tomcat service wordt verstuurd waarin een directory wordt opgevraagd die begint met een ';'-teken.

Risico

Deze zogenaamde "loop" van HTTP-aanvragen en antwoorden kan een onnodig hoge belasting van de webservices veroorzaken. Mogelijk kan deze kwetsbaarheid door een aanvaller worden misbruikt om een Denial of Service (DoS) van de RIES stemserver te versterken.

Bewijs

De volgende URL veroorzaakt een loop van HTTP-aanvragen naar de RIES stemserver:

```
https://stem.surfnet.nl/server/%5C../;images/
```

Bevinding 1.10

De RIES Beheer Portal geeft een fysiek pad op de server vrij. Het fysieke pad wordt weergegeven in een foutmelding.

Risico

De weergeven van teveel informatie in foutmeldingen helpt aanvallers om de applicatie of de achterliggende structuur in kaart te brengen. De informatie kan mogelijk worden gebruikt in verdere aanvallen.

Bewijs

De volgende URL geeft een fysiek pad op de server vrij:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001*
```

Het fysieke pad dat wordt vrijgegeven is:

```
/data/ries/work/reports/
```

Bevinding 1.11

De RIES Beheer Portal is kwetsbaar voor SQL injection. Gebruikersinvoer wordt zonder validatie of met onvoldoende validatie overgenomen in database queries.

Risico

Een kwaadwillende gebruiker kan met behulp van SQL injection de achterliggende database rechtstreeks aanspreken om zo gegevens in de database op te vragen, waardoor onder andere de vertrouwelijkheid van de informatie in de database in gevaar komt. Daarnaast kan deze kwetsbaarheid worden misbruikt om verdere informatie over de gebruikte database software en het besturingssysteem te verkrijgen, waarmee mogelijk verdere toegang tot de database of de server kan worden verkregen. Niet uitgesloten is dat deze kwetsbaarheid het ook mogelijk maakt om gegevens in de database te wijzigen of te verwijderen.

Bewijs

De volgende URL's tonen aan dat de RIES Beheer Portal kwetsbaar is voor SQL injection:

De databasegebruiker is 'ries':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(select%20count(*)%20from%20mysql.user
)%3E0%20/*
```

De naam van de database is 'ries':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20database()='ries'/*
```

Een tabel met de naam 'status':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20count(*)%20from%20status)%3E
0/*
```

Een tabel met de naam 'votes':

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20count(*)%20from%20votes)=262
6/*
```

De eerste vier karakters uit het bestand '/etc/passwd' op de server:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20substr(load_file('/etc/passwd'),1,4)='
root'/*
```

Bevinding 1.12

De gebruikte versie van MySQL de de RIES stemserver is verouderd en bevat meerdere publiekelijk bekende kwetsbaarheden.

Risico

De gebruikte versie van MySQL bevat diverse publieklijk bekende kwetsbaarheden waarmee een kwaadwillende een Denial of Service (DoS) kan veroorzaken of de inhoud van de database kan wijzigen. Of de kwetsbaarheden daadwerkelijk kunnen worden uitgebuit hangt van de configuratie van MySQL af.

Bewijs

Met behulp van de volgende twee URL's kan worden geconcludeerd dat het versienummer van de MySQL software `4.1.20` is:

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20/*!40120%2010*/%20)=10/*
```

```
https://stem.surfnet.nl/server/%5C../admin/server?req=results&subreq=stor
e&pageid=select&elid=8001'%20and%20(SELECT%20/*!40121%2010*/%20)=10/*
```

Bevinding 1.13

De webservices op de systemen `195.169.124.82` en `192.87.106.194` bieden ondersteuning voor het cryptografisch onveilige SSL versie 2.0 protocol aan browsers die erom vragen.

Risico

Het toestaan van verouderde SSL protocollen maakt het mogelijk voor een kwaadwillende gebruiker om de communicatie tussen webserver en gebruiker zodanig te manipuleren dat de encryptie gekraakt kan worden. Vervolgens is het mogelijk om met behulp van een zogenaamde man-in-the-middle attack informatie af te luisteren en/of te manipuleren.

Bewijs

Als een browser wordt ingesteld om alleen SSL-versie 2.0 te ondersteunen dan kan er toch verbinding gemaakt worden met de server.

Appendix 2 Bevindingen cryptografische analyse

Onderstaande bevindingen zijn nog in onderzoek en nog niet voorgelegd aan het Waterschapshuis.

A2.1 RIES 2008 in 2030

Deze bevinding beschrijft een dreiging die op kan treden in 2030 als het RIES 2008 systeem zo geïmplementeerd wordt als beschreven is in de aangeleverde documentatie. Dit hoofdstuk is niet bedoeld als uitleg hoe het gehele RIES 2008 systeem werkt, maar tracht alleen de noodzakelijke informatie te geven voor één mogelijke dreiging. Voor andere opmerkingen en commentaren op het RIES 2008 system verwijzen wij naar andere hoofdstukken.

Sleutelgeneratie
De laatste versie van RIES is een opvolging van RIES-KOA, RIES 2004 en het systeem van Robers [14]. Het RIES 2008 systeem kenmerkt zich vooral door het toevoegen van een cryptografische hardware module, de IBM 4764 [12]. Hiermee is het nu mogelijk om het sleutelbeheer veilig uit te voeren zonder dat iemand de geheime sleutels hoeft te zien.

Als eerste moet er een hoeveelheid publieke data gegenereerd worden [3, blz. 10]. Er moet bijvoorbeeld een lijst van alle kiezers gemaakt worden. Hierbij krijgt elke kiezer zijn eigen publieke identiteit *VnID*, welke is gekoppeld aan je Burger Service Nummer (BSN) [6]. Ook wordt er elke stemronde een deelnemers groep gedefinieerd genaamd *ParGp.*, welke gelijk blijft voor de gehele verkiezing. Als laatste moet er een verkiezingscode *ElID* gegenereerd worden die aangeeft in welke verkiezingsronde elke kiezer mag stemmen.

Met deze gegevens (*VnID, ParGp, ElID*) wordt er voor elke kiezer (circa 13 miljoen mensen) een geheime sleutel *Kp* gegenereerd. Je persoonlijke sleutel is dus verbonden aan je publieke identiteit via je *VnID* en je *BSN* [6, blz. 14-15].

De kiezer zijn persoonlijke sleutel *Kp* is eigenlijk een 8 byte DES sleutel [2,4]. Deze sleutel wordt gebruikt om alle mogelijke keuzes van elke kiezer te versleutelen en te publiceren voordat de verkiezingen beginnen. Deze gepubliceerde lijst wordt als referentie lijst gebruikt om zo na de verkiezingen te kunnen bepalen op wie er allemaal gestemd is. De charme van het systeem is dat het verifiëren door iedereen gedaan kan worden.

Voordat we verder gaan met het algoritme en het gebruik van de *Kp* DES sleutel leggen we uit hoe *Kp* gegenereerd wordt. Hiervoor wordt een extensie op het DES algoritme gebruikt, namelijk door drie maal een bericht te versleutelen, een zogenaamde Triple DES (3DES) [5,13]. Met 3DES zijn er twee modi, de drie verschillende sleutels modus (3TDES) en de twee sleutel modus (2TDES). Met 3TDES heb je drie sleutels van in totaal 168 bits lengte (3 x 56 bits) en bij 2TDES heb je twee sleutels van in totaal 112 bits lengte (2 x 56 bits). Als een bericht *M* versleuteld wordt dan wordt hij eerst vercijferd (E) met sleutel *K1*, daarna ontcijfert (D) met sleutel *K2* en vervolgens nog eens versleuteld (E) met sleutel *K3*:

$$E_{K3}(D_{K2}(E_{K1}(M))) \tag{1}$$

Bij 3TDES zijn de sleutels $K1 \neq K2 \neq K3$, terwijl bij 2TDES $K1=K3$, $K1 \neq K2$ en $K3 \neq K2$.

Formule (2) geeft weer hoe *Kp* gegenereerd wordt:

$$Kp = 2TDES_{Kgenvoterkey}(VnID \,//\, ParGp \,//\, ElID) \tag{2}$$

Kp is een 56 bits (8 byte) DES sleutel die wordt bij RIES 2008 gegenereerd door een twee-sleutel triple DES (2TDES) genaamd *Kgenvoterkey*. Deze *Kgenvoterkey* heeft een sleutel lengte van 112 bits (16byte) [1]. Alle *Kp*'s worden tijdens een verkiezing gegenereerd door dezelfde *Kgenvoterkey*. Daardoor zijn alle *Kp*'s afhankelijk van elkaar. Omdat *VnID, ParGp* en *ElID* publiekelijk zijn kan bij bekend wording van *Kgenvoterkey* elke *Kp* gegenereerd te worden. Met dit gegeven zijn er een aantal vragen:

- Hoe waarschijnlijk is het dat *Kgenvoterkey* gevonden word en hoe lang kan dat duren?

- Wat voor een impact heeft het als *Kgenvoterkey* gevonden wordt? Wat kan een aanvaller allemaal leren?

Hoe lang is *Kgenvoterkey* nog veilig?
Een belangrijk veiligheidsaspect is de lengte van de sleutel en het gebruikte algoritme. Er zijn een aantal gerenommeerde instituten die hierover uitspraken doen gebaseerd op uitgebreid onderzoek.

Het Nationaal Instituut voor Standaarden en Technologie (NIST) is een agentschap van de Amerikaanse overheid. In hun laatste rapport [9] uit 2007 geven zij aanbevelingen aan federale agentschappen over het gebruik van sleutel lengtes in combinatie met cryptografische algoritmen. Uit hun aanbeveling komt de volgende tabel:

Tabel 1. Aanbeveling sleutel lengtes en algoritmen NIST 2007

Datum	Minimale sleutel lengte (bits)	Symmetrisch Algoritme
2008 t/m 2010	80	**2TDES**
2011 t/m 2030	**112**	**3TDES**
> 2030	128	AES-128
>> 2030	192	AES-192
>>> 2030	256	AES-256

De tabel geeft weer dat tot en met 2010 algoritmes met een sleutel lengte van 80 bits nog acceptabel zijn. Tussen 2010 en 2030 zijn algoritmen met sleutel lengtes van 112 bits nog te gebruiken, et cetera. Hierbij valt dus op dat het NIST aanraad dat 2TDES gebruikt kan worden tot en met 2010. Een kanttekening bij dit gegeven is dat 2TDES een sleutel lengte heeft van 112 bits, maar als een aanvaller de beschikking heeft over 2^{40} klaretekst en cijfertekst paren dan is het algoritme zo verzwakt dat het maar een sleutel lengte heeft van 80 bits. Mocht dit niet het geval zijn dan is 2TDES nog veilig tot en met 2030.

Een ander onderzoeksinstituut, het Europese Netwerk van Excellentie in Cryptografie (ECRYPT) heeft in 2007 een rapport [8] uitgebracht over algoritmen en sleutel lengtes. Het rapport wordt gedreven door het veiligheidsniveau dat iemand wil bereiken. Bij elk van deze niveaus hoor een bepaalde sleutel lengte. De veiligheidsniveaus van de symmetrische algoritmen staan in de tabel hieronder aangegeven en komen uit het laatste rapport van ECRYPT

Tabel 2. Veiligheids niveaus van symmetrische algoritmen ECRYPT 2007

Veiligheids niveau	Sleutel lengte (bits)	Bescherming	Commentaar
1.	32	Aanvallen in 'real-time' bij individuele	Alleen acceptabel voor authenticatie tokens.
2.	64	Heel erg korte termijn bescherming tegen kleine organisaties	Zou niet gebruikt moeten worden voor confidentialiteit in nieuwe systemen
3.	72	Korte termijn bescherming tegen medium organisaties, middellange termijn bescherming tegen kleine organisaties	
4.	80	Erg korte termijn bescherming tegen agentschappen, lange termijn bescherming tegen kleine organisaties	Kleinste gebruik voor algemene doeleinden , ≤ 4 jaar bescherming
5.	96	Standaard bescherming	**Gebruik van 2TDES beperkt tot ~10^6 klareteksten / cijferteksten dan ≈ 10 jaar bescherming**
6.	**112**	Middellange termijn bescherming	**≈ 20 jaar bescherming**
7.	128	Lange termijn bescherming	Goed, generieke applicatie onafhankelijke aanbeveling , ≈ 30 jaar bescherming
8.	256	'Nabije toekomst'	Goede bescherming tegen Quantum computers

In tabel 2. is te zien dat als er ongeveer 10^6 klareteksten en cijferteksten paren bekend zijn van 2TDES, de bescherming nog maar ongeveer 10 jaar standhoud m.a.w. tot en met ≈ 2017. Is dit niet het geval dan zou 2TDES ongeveer 20 jaar standhouden tot en met ≈ 2027.
We concluderen uit de rapporten van deze twee onafhankelijke instituten dat de confidentialiteit niet meer gegarandeerd kan worden rond 2030 als informatie versleuteld is met 2TDES. Anders geformuleerd, als er in 2008 verkiezingen zijn geweest waarbij een geheime 2TDES sleutel is gebruikt van 112 bits, kan deze dan rond 2028 gemakkelijk worden achterhaald door particulieren.

Enkele opmerkingen over het genereren van sleutels: Sleutels moeten volgens [8] zo willekeurig (random) mogelijk worden gegenereerd en sleutels zouden nooit gebruikt mogen worden, volgens [8] voor twee verschillende doeleinden. Applicaties zoals verkiezingen vallen onder erg lange termijn bescherming [8].

Wat gebeurt er als *Kgenvoterkey* wordt gevonden?
Theoretisch is een aanvaller dus in staat om achter *Kgenvoterkey* te komen rond 2030. Mocht dit de aanvaller lukken, wat kan hij dan allemaal achterhalen?

De kracht van RIES is dat iedereen achteraf kan bepalen of de verkiezing goed is verlopen. Maar dit kan ook leiden tot verschillende bedreigingen. Een van de eisen van stemmen is dat een aanvaller niet in staat moet zijn te bepalen wat iemand gestemd heeft of dat iemand überhaupt heeft gestemd of niet.

Als eerste moet de aanvaller in bezit zijn van een geldige persoonlijke sleutel *Kp* zodat van daaruit de *Kgenvoterkey* achterhaald kan worden d.m.v. brute force sleutel zoeken (in 2030). Deze *Kp* kan van hemzelf zijn of van iemand die graag mee wil werken aan zijn aanval, er zijn tenslotte 13 miljoen geldige *Kp*'s in omloop. De aanvaller heeft dus maar 1 geldige *Kp* nodig.

Zoals we in formule (2) konden zien zijn de *Kp*'s opgebouwd door middel van een vaste structuur, *VnID, ParGp* en *ElID*. Omdat ParGp en *ElID* vaste waarden zijn voor de verkiezing, hoeft de aanvaller alleen maar alle *VnID*'s te genereren. VnID is een unieke identiteit van een stemgerechtigde en gekoppeld aan zijn unieke BurgerService Nummer (BSN) of indien niet beschikbaar het A-nummmer [6]. Het BSN bestaat uit 9 cijfers en moet volstaan aan een zogenaamde elfproef. De aanvaller is dus in staat om alle mogelijke BSN's te genereren en deze in te vullen in formule (2).

Tijdens de voorbereiding van de verkiezing in 2008 worden alle mogelijke stemmen van elke kiezer versleuteld en gepubliceerd zodat deze lijst als referentie gebruikt kan worden om na de verkiezing alle geldige stemmen te tellen. Deze lijst, *RnPotVote* wordt per kiezer op de volgende manier gegenereerd [3, blz. 10].

$$RnPID_n = MDC[DESmac_{Kp_n}(f(ElID))] \quad (3)$$

$$RnC1_n = MDC[DESmac_{Kp_n}(f(C1, ElID, AbelPI_n))] \text{ - Kandidaat 1} \quad (4)$$

$$RnC2_n = MDC[DESmac_{Kp_n}(f(C2, ElID, AbelPI_n))] \text{ - Kandidaat 2}$$

$$\vdots$$

$$RnCm_n = MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))] \text{ - Kandidaat } m$$

$$RnPID_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(ElID))]$$

$$RnC1_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(C1, ElID, AbelPI_{n+1}))] \text{ - Kandidaat 1}$$

$$RnC2_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(C2, ElID, AbelPI_{n+1}))] \text{ - Kandidaat 2}$$

$$\vdots$$

$$RnCm_{n+1} = MDC[DESmac_{Kp_{n+1}}(f(Cm, ElID, AbelPI_{n+1}))] \text{ - Kandidaat } m$$

... Etcetera...

De lijst bevat de waarden *RnPID* welke bedoel zijn om te bepalen of een kiezer mag meestemmen in de verkiezing. *RnCM* maakt het mogelijk om te bepalen waarop iemand heeft gestemd en bestaat uit alle kandidaten, *C1* t/m *Cm*, waarop de kiezer mag stemmen. Achter elke *RnCm* wordt vermeld bij welke kandidaat dit hoor. *AbelPI* zijn de laatste twee cijfers van het geboortejaar van de kiezer en worden gebruikt ter controle bij de stemmen, maar hebben verder geen invloed op deze bedreiging.

Zonder geldige *Kp* valt uit de lijst niet te halen wie er allemaal mogen stemmen. Met deze lijst en alle mogelijke *Kp*'s die hij heeft gegenereerd aan de hand van alle mogelijke BSN's, is de aanvaller in staat om te verifiëren of een bepaalde BSN mee mocht doen. Hij is hiertoe in staat door zelf formule (3) te berekenen voor een willekeurige BSN en te vergelijken met de gepubliceerde lijst *RnPotVote*. De aanvaller kan formule (3) berekenen omdat MDC een door IBM ontworpen DES-hash in MDC-2 formaat is en publiekelijk bekend is [7]. De functie *f(.)* is een padding functie die de ruimte opvult met nullen. *ElID* en DESmac publiekelijk bekend zijn.

De aanvaller kan dus bepalen welke BSN's er allemaal mochten stemmen in 2008.

Tijdens de verkiezing in 2008 worden de stemmen van een kiezer (*VnPID* en *VnCx*) uitgerekend op zijn computer. Deze zogenaamde technische stemmen worden vermeld in tabel 3., waarbij *VnPID* de pseudo identiteit van een kiezer is en *VnCx* is de stem van de kiezer.

Tabel 3. *VnPID en VnCx*

VnPID	VnCx	
$VnPID = DESmac_{Kp}(f(ElID))$	$VnCx = DESmac_{Kp}(f(C2, ElID, AbelPI))$	(5)

Deze waarden worden dmv SSL naar een verkiezingsserver gestuurd die ze vervolgens hashed met MDC-2 [7]. Als de verkiezing is afgesloten en alle stemmen zijn ontvangen, wordt er een lijst gepubliceerd *RecVote* met alle ontvangen stemmen, zie tabel 4.

De lijsten *RecVote* en *RnPotVote* worden nu met elkaar vergeleken om zo te bepalen wie de meeste stemmen heeft ontvangen. Hierbij wordt eerst gekeken of er een *VnPID* voorkomt in *RnPotVote*, m.a.w. of er een *RnPID* aanwezig is. Als dat zo is, wordt er gekeken of *VnCx* ook voorkomt in de lijst van *RnPotVote*, m.a.w. of er een *RnCn* is die gelijk is aan *VnCx*. We gaan hier niet verder op in hoe meerdere stemmen of valse stemmen uit het systeem worden gehaald. Dit valt buiten de scope van deze bedreiging.

Tabel 4. *RecVote*

VnPID	VnCx	
$VnPID = MDC[DESmac_{Kp_1}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_1}(f(C2, ElID, AbelPI_1))]$	(6)
$VnPID = MDC[DESmac_{Kp_2}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_2}(f(C8, ElID, AbelPI_2))]$	
...	...	
$VnPID = MDC[DESmac_{Kp_x}(f(ElID))]$	$VnCx = MDC[DESmac_{Kp_1}(f(C7, ElID, AbelPI_n))]$	

Hierdoor ontstaat de situatie dat een aanvaller voor elk BSN kan bepalen of hij heeft gestemd. Zo ja, wat hij heeft gestemd. Het BSN nummer is een uniek nummer, maar geen geheim nummer. Het BSN staat op vele documenten vermeld: paspoort, rijbewijs, loonstrookje. Een aanvaller hoeft alleen maar het BSN te weten van een individu zodat hij kan bepalen wat deze persoon heeft gestemd.

Wetgeving

30 September 2004 heeft 'The Committe of Ministers of the Council of Europe' een aanbeveling geschreven [10] waarin beschreven wordt waar een e-voting system technisch, juridisch en operationeel aan zou moeten voldoen. In totaal zijn dit 112 punten of ook wel standaarden genoemd met daarbij nog enkele opmerkingen.

Op pagina 10 van [10] onder standaard 17. staat: "The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter".

Opmerking 47 op pagina 33, behandeld standaard 17: "This standard provides that it must never be possible to reconstruct the content of any voter's vote and link it to the voter who cast it."

Bij de opmerking 51. pagina 34: "The moment of inserting a vote into the electronic ballot box is the latest point in time at which the vote must be separated from the information on who has cast it – without any possibility of reconstructing this link"

In de nadere regelgeving waterschapswet, waterschapsbesluit [20] staat onder artikel 2.58 1.e. vermeld: "De identiteit van de kiezer wordt door de voorziening geanonimiseerd geregistreerd;".

Als een e-voting systeem zoals RIES 2008 wil voldoen aan deze aanbeveling dan mag een stem van een kiezer nooit gekoppeld (linked) worden aan die kiezer, dus ook niet in 2030 of later.

Conclusie en aanbevelingen
Op lange termijn (circa 20 jaar) zijn onze stemmen niet veilig genoeg als er gebruik wordt gemaakt van 2TDES binnen RIES 2008. Ten eerste zijn alle geheime sleutels *Kp* afhankelijk van een sleutel *Kgenvoterkey* die even veilig is als 2TDES. Ten tweede is elke geheime sleutel *Kp* gekoppeld aan een unieke BSN van een burger. Omdat RIES 2008 opgebouwd is om vertrouwen te wekken aan zijn gebruikers en alle stemmen publiceert, ontstaat er een reële mogelijkheid dat iemand jaren na de verkiezing toch kan achterhalen wat iemand heeft gestemd. Alle informatie is immers publiekelijk beschikbaar en die zal in 2030 ook nog steeds beschikbaar zijn.

De verwachting van het NIST [9] en ECRYPT [8] is dat dit zeker in 2030 mogelijk is door individuen. In de tussen tijd (voor 2030) zijn er grote organisaties of agentschappen die het wellicht eerder kunnen uitvoeren (zoals Google) zolang ze maar genoeg computer kracht hebben.

Om er voor te zorgen dat een stem nooit gekoppeld kan worden aan een individu is het ten eerste noodzakelijk om de sleutels zo willekeurig mogelijk te genereren, zie ook [8]. In [11, pagina 3, voetnoot 1] wordt commentaar gegeven op RIES 2004 waarbij is aanbevolen dat de sleutels in een zo onvoorspelbare manier gegenereerd moeten worden. Als de sleutels wel uniek zijn maar niet gekoppeld aan een BSN, kan de aanvaller niet bepalen wat iemand heeft gestemd, ook niet in 2030 of later. Hij kan dan alleen leren dat iemand met een bepaalde *Kp* gestemd heeft op een kandidaat. Ongeacht welk soort algoritmen gebruikt wordt om *Kp*'s te genereren, het zal nooit gekoppeld moeten worden aan een unieke persoonlijke nummer zoals het BSN omdat het dan nooit willekeurig gegenereerd kan worden.

Meer informatie over sleutellengtes is te vinden op: http://www.keylength.com/

A2.2 Genereer een stem

Het analyserapport van EIPSI over RIES [19, pagina 44] beschrijft een aanval om valse stemmen te genereren binnen RIES. Deze actieve aanval kan uitgevoerd worden tijdens de verkiezingen voordat de stemmen geteld zijn. EIPSI beschrijft als mitigerende factor dat de aanvaller toegang moet krijgen tot de geleverde stemmen en wellicht tot de stemserver.

Onderstaande aanval is zoals gezegd gebaseerd op [19] maar behoeft geen toegang te krijgen tot de stemserver en kent de mitigerende factor van EIPSI dus niet. Ten opzichte van [19] is deze aanval complexer maar nog steeds uit te voeren door een individu.

MDC
Voor de verkiezingen wordt de lijst *RnPotVote* gepubliceerd met de waarden *RnPID* en *RnCx*. De aanval in [19] richt zich op *RnCx* terwijl wij ons richten op *RnPID*:

$$RnPID = MDC[VnPID] = MDC[DESmac_{Kp}(f(ElID))]$$

MDC [7] is een 128 bits hash waarde terwijl de input *VnPID* een 64 bits waarde is. Een aanvaller hoeft alleen de 64 bits input ruimte aan te vallen, m.a.w. 64 bits i.p.v. 128 bits.

Als we er vanuit gaan dat er 13 miljoen stemgerechtigden zijn is dat ongeveer gelijk aan 2^{23} geldige stemmen. De kans is dus erg klein om een geldige stem willekeurig te kiezen, de kans daarop is 2^{-41}.

We zoeken x van MDC(x) door MDC(1), MDC(2), ..., MDC(n) te berekenen. Dan zullen we 2^{41} waarden moeten genereren om een waarschijnlijkheid van 1 te krijgen dat een geldige MDC(x) is gevonden. Dit is nog steeds minder dan brute-force. Ook hoeven we maar 64 bits van de 128 bits op te slaan daardoor hebben we 2^{41}*8 byte, circa 17 TeraByte, aan opslag nodig. Aangezien een harddisk van 1 TeraByte ongeveer 150 euro kost, zal dit geen grote kostenpost zijn. Deze bevinding is besproken in [19] en verder uitgebreid tot een aanval waarbij gegenereerde stemmen worden verwisseld op de stem server gebruikmakend van een aanvaller die toegang heeft tot de stem server.

Brute-Force
In plaats van verder te gaan, gaan we terug naar onze formule van *RnPID* waarbij we zien dat er eigenlijk maar 1 onbekende in zit, namelijk *Kp*. De functie *f(.)* is bekend en dit is een simpele padding functie. *ElID* is ook bekend en is voor de gehele verkiezing hetzelfde. We weten ook dat *Kp* een 56 bits DES sleutel is en dat *DESmac* ook maar een 64 bits output heeft. We hebben geconstateerd dat er 13 miljoen kiezers zijn dus er zijn ook 13 miljoen unieke *Kp*'s.

De aanvaller gaat nu niet MDC(x) zoeken maar hij gaat nu *Kp* op laten lopen van 1 t/m 2^{56}. Hij berekend dus:

$$MDC[VnPID] = MDC[DESmac_1(f(ElID))]$$
$$MDC[VnPID] = MDC[DESmac_2(f(ElID))]$$
M
$$MDC[VnPID] = MDC[DESmac_{2^{56}}(f(ElID))]$$

Omdat MDC en DESmac gebaseerd zijn op DES moet het relatief makkelijk zijn om de copacobana DES craker deze berekeningen te laten uitvoeren (http://www.copacobana.org/). Deze heeft gemiddeld 6.4 dagen nodig om een DES sleutel te breken en maximaal 12.8 dagen om alle sleutels te proberen. De prijs van een copacobana is minder dan 9000 euro.

Als er 2^{41} waarden zijn berekend dan is de kans 1 dat er een geldige *Kp* tussenzit en bij 2^{56} waarden zijn alle geldige *Kp*'s gevonden. Hoeveel Kp's er nodig zijn is een tijdskwestie en afhankelijk van de implementatie van de hardware. Er moeten nu meerdere DES waarden berekend worden maar die zouden ook serieel berekend kunnen worden door meerdere DES krakers te gebruiken. Bijvoorbeeld, de eerste kraker berekend de DESmac waarde, geeft zijn output aan een volgende DES kraker die de MDC waarde berekend. Daarna worden de waarden vergeleken met de gepubliceerde tabel *RnPotVote*.

Met alleen de beschikking over veel opslag ruimte en 1 DES kraker is het wellicht verstandiger om 2^{41} MDC waarden te genereren en daarna per gevonden DESmac waarde een *Kp* te vinden gebruik makend van een DES kraker. Het genereren van de waarden zal ongeveer 1 dag in beslag nemen en een DES kraker heeft gemiddeld 6.4 dagen nodig om een sleutel te vinden. De kosten bedragen tussen de 10.000 euro a 15.000 euro. Dus voor 15.00 kan iemand een stem kopen.

AbelPI
Om een stem uit te kunnen brengen moet een aanvaller ook de beschikking hebben over de AbelPI welke de laatste twee cijfers zijn van het geboorte jaar van de kiezer. Deze waarde wordt niet op het stembiljet gedrukt en wordt als bekend geacht bij de kiezer. Wel is deze waarde verbonden aan de stemkeuze van de kiezer in *RnCx*. *RnCx* bevat alle mogelijke stemmen van een kiezer en fungeert als een onderdeel van de lijst *RnPotVote* als referentielijst. Deze lijst wordt gebruikt om na de verkiezing te kunnen bepalen hoeveel stemmen er zijn uitgebracht en op wie.

$$RnPID_n = MDC[DESmac_{Kp_n}(f(ElID))]$$
$$RnC1_n = MDC[DESmac_{Kp_n}(f(C1, ElID, AbelPI_n))] \text{ - Kandidaat 1}$$
$$RnC2_n = MDC[DESmac_{Kp_n}(f(C2, ElID, AbelPI_n))] \text{ - Kandidaat 2}$$
$$\vdots$$
$$RnCm_n = MDC[DESmac_{Kp_n}(f(Cm, ElID, AbelPI_n))] \text{ - Kandidaat } m$$

Voor elke kandidaat wordt een lijst van mogelijke kandidaten waarop hij kan stemmen gegenereerd, zie hierboven. Omdat bij elke gevonden *Kp* ook *RnPID* bekend is, kan in de lijst gevonden worden wat de bijhorende RnCx waarden zijn.

We weten dus dat voor een *Kp*, kandidaat 2 een waarde *RnC2* hoort. De enige onbekende is dus nog *AbelPI*. De meeste kiezers zullen jonger zijn dan 80 jaar en minimaal 18 jaar oud. Dus de laatste cijfers van het geboortejaar lopen van 28 t/m 90. We kunnen dus berekenen:

$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID, 28))]$$
$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID, 29))]$$
$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID, 30))]$$
M
$$RnC2 = MDC[DESmac_{Kp}(f(C2, ElID, 90))]$$

Een van deze 62 waarden zal de juiste AbelPI opleveren bijhorend bij een *Kp*. We kunnen dus elke waarde vergelijken met de waarde in de tabel. De enige gelijke waarde staat gelijk aan het ingevulde geboortejaar. Nu we *Kp* hebben en de bijhorende *AbelPI*, zijn we instaat om een geldige stem uit te brengen.

ElID
Als ElID, de verkiezings identiteit VOOR de verkiezing bekend is, kan de aanvaller de meeste berekeningen voor de verkiezingen doen, hij genereert dan minimaal 2^{41} *Kp*'s (17 TB). Het is ondoenlijk om 2^{56} *Kp*'s aan data te genereren omdat daar 570.000 TB voor nodig is.

Conclusie
Door een zwakke implementatie van de MDC hash functie is het mogelijk geworden om binnen korte tijd een brute-force aanval uit te voeren op RIES 2008. Een hulpmiddel hierbij is *RnPotVote* die voor de verkiezingen gepubliceerd wordt. Omdat de lijst met hash waarden gepubliceerd wordt voor de verkiezingen is het mogelijk om te verifiëren welke gegenereerde waarden stem gerechtigd zijn. Doordat er maar een sleutel van 56 bits gebruikt wordt per gebruiker, moet de aanvaller nu maximaal 256 waarden genereren. Hier geldt dus de regel van de zwakste schakel. Er is wel een hash waarde van 128 bits, maar de inputs is maar een 64 bits DESmac waarde die gegenereerd wordt door een 56 bits DES sleutel. En aangezien *ElID* publiekelijk bekend is behoeft een aanvaller alleen alle mogelijke *Kp*'s te genereren.