Publiekelijk raadpleegbare broncode internetstemsysteem

Security of Systems Group, Radboud Universiteit Nijmegen
oktober 2007

Radboud Universiteit Nijmegen

1. Achtergrond en aanleiding

De Directie Informatie- en Innovatiebeleid Openbare Sector (DIIOS) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft ICTU opdracht gegeven voor het programma BVIS (Basisvoorziening Internetstemmen). Het lange termijn doel van het project is om een internetstemdienst te organiseren die ingezet kan worden voor kiezers buiten Nederland. Het korte termijn doel van het project is onder meer de mogelijkheden voor verwerving door BZK van een dergelijke dienst in kaart te brengen.

In deze rapportage hanteren wij de volgende terminologie. De *internetstemdienst* is opgebouwd uit een *stem-beheerorganisatie* en een (technisch) *internetstemsysteem*. Het internetstemsysteem bestaat uit de applicatieve programmatuur die wordt geïmplementeerd en beheerd door de stem-beheersorganisatie (ICT technisch, facilitair, personeel etc.). Als onderdeel van het programma BVIS worden functionele eisen opgesteld waaraan het internetstemsysteem dient te voldoen.

Het programma BVIS heeft de Security of Systems groep van de universiteit van Nijmegen gevraagd middels een korte literatuurstudie te onderzoeken of het wenselijk is dat de broncode van het internetstemsysteem publiekelijk raadpleegbaar is. Hierbij dienen de volgende aspecten meegewogen te worden:

1. Maatschappelijke gewenstheid vanuit het beginsel van transparantie
2. Beveiligingsrisico's

Dit rapport is als volgt opgebouwd:

- Hoofdstuk 2 bevat de eindconclusie van deze memo
- In Hoofdstuk 3 verduidelijken wij de centrale vraagstelling van deze memo en relateren dit met het begrip 'open source software'
- In Hoofdstuk 4 wordt aan de hand van een viertal gezaghebbende bronnen de gewenstheid geïnventariseerd van het publiekelijk raadpleegbaar maken van de internetstemsysteem broncode
- In Hoofdstuk 5 wordt een inschatting gegeven van de additionele risico's van het publiekelijk raadpleegbaar maken van de internetstemsysteem broncode in vergelijking met de situatie waarin dit niet het geval is
- Hoofdstuk 6 bevat verwijzingen naar de gebruikte bronnen

2. Eindconclusie

- Vanuit een viertal recente, gezaghebbende bronnen (de Adviescommissie inrichting verkiezingsproces [1.], de Commissie Besluitvorming Stemmachines [2.], de Raad van Europa [3.], en de Organisatie voor Veiligheid en Samenwerking in Europa ([4.]) concluderen wij dat het publiekelijk raadpleegbaar maken van de internetstemsysteem broncode een vereiste is vanuit het beginsel dat een verkiezingsproces transparant moet zijn voor de burger.
- Het publiekelijk raadpleegbaar maken van de broncode kan op verschillende wijzen plaatsvinden. Een veelgenoemde wijze bestaat eruit het internetstemsysteem te ontwikkelen als zogenaamde Open Source Software. Hierbij kan de software niet alleen door een ieder worden geraadpleegd maar kan deze ook vrijelijk worden hergebruikt. Dat laatste is vanuit het transparantiebeginsel niet noodzakelijk en kan op weerstand stuiten bij leveranciers en/of onnodig hoge kosten met zich meebrengen. Er zijn ook andere mechanismen mogelijk om software publiekelijk raadpleegbaar te maken waarbij hergebruik van de software wordt beperkt of zelfs is uitgesloten. Het laatst genoemde mechanisme wordt nu bijvoorbeeld reeds toegepast bij het bekende commerciële encryptiepakket PGP ('Pretty Good Privacy'). Door nu slechts als eis te formuleren dat de broncode publiekelijk raadpleegbaar moet zijn, ontstaat bovendien een betere onderhandelingsruimte met potentiële leveranciers.
- Op basis van een op hoofdlijn uitgevoerde risicoanalyse schatten wij in dat de beveiligingsrisico's verbonden met het publiekelijk raadpleegbaar maken van de internetstemsysteem broncode vergelijkbaar zijn met de situatie waarin dit niet het geval is. Dit laat daarmee onverlet dat in beide situaties informatiebeveiliging adequaat moet zijn geborgd in het softwareontwikkelingsproces (vergelijk [10.]). Verder moet de overheid door actieve communicatie (bijvoorbeeld voordrachten, prijsvragen) wel stimuleren dat de aandacht vanuit de 'goedwillende' hackersgemeenschap minstens zo groot is als die vanuit de 'kwaadwillende' hackersgemeenschap.

3. Open source software versus software met broncode die publiekelijk raadpleegbaar is

3.1 Analyse

Softwareontwikkelaars beschrijven de (beveiligings)logica van een informatiesysteem zoals een internetstemsysteem in een hogere programmeertaal (bijvoorbeeld Java of C++); het geheel van deze programmaregels heet ook wel de *broncode*. De broncode wordt gecompileerd tot een vorm (machinetaal) die de computer kan uitvoeren.

Idealiter is de (technische) werking van een informatiesysteem beschreven in ontwerpdocumentatie en hoeft men de broncode niet te analyseren om de werking te doorgronden. Als men echter zekerheid wil over de veilige werking van een informatiesysteem, dat wil zeggen dat er geen (on)bedoelde 'achterdeurtjes' in de software zijn opgenomen, dan ontkomt men er niet aan de broncode aan een veiligheidsanalyse te onderwerpen.

Vanuit verschillende gezaghebbende bronnen (zie het volgende hoofdstuk) wordt aangegeven dat de *transparantie* voor de burger van het verkiezingsproces essentieel is. Binnen een internetstemdienst vormt het (technische) internetstemsysteem een cruciaal onderdeel. Vanuit het transparantiebeginsel is het daarom van groot belang dat het publiek zekerheid heeft, of kan krijgen, dat de werking van het internetstemsysteem veilig is. Dit betekent dat er een veiligheidsanalyse moet zijn uitgevoerd waarbij de vraag is wie deze analyse uitvoert. Een dergelijke analyse kan worden uitgevoerd binnen het ontwikkelteam zelf ('peer review') of door een onafhankelijke IT auditor die daarover publiekelijk rapporteert. In het volgende hoofdstuk zullen wij vanuit het transparantiebeginsel beargumenteren dat iedereen ('de burger') een veiligheidsanalyse moet kunnen uitvoeren van het internetstemsysteem. Dit betekent in het bijzonder dat deze broncode publiekelijk raadpleegbaar moet zijn.

Het kunnen raadplegen van de broncode van een informatiesysteem wordt vaak gelijk gesteld met dat het informatiesysteem onder een zogenaamde Open Source Software licentie moet zijn ontwikkeld. Een bekend voorbeeld van een dergelijk licentie is GPL ('Gnu Public Licence', zie [5.]) waar ondermeer Linux onder valt. Dergelijke open licenties corresponderen met maatschappelijke – veelal internetgedreven – bewegingen waarbij de softwareontwikkeling plaatsvindt binnen een vaak informele groep van personen. Software (en de broncode daarvan) die onder een dergelijk schema valt, mag vrijelijk worden gedistribueerd, aangepast en hergebruikt, ook in een commerciële context. Dit betekent aldus in het bijzonder dat de broncode van Open Source Software publiekelijk raadpleegbaar is. Het omgekeerde is echter niet altijd het geval: niet alle software die publiekelijk raadpleegbaar is, is ook vrijelijk herbruikbaar.

Het verschil tussen beide situaties lijkt misschien onbeduidend. Immers, als men de broncode kan raadplegen kan men deze in technische zin ook weer hergebruiken. Er kunnen echter goede argumenten zijn waarom een leverancier wel zijn broncode publiekelijk raadpleegbaar wil laten zijn maar toch hergebruik in formele zin niet wil toelaten, bijvoorbeeld:

- De gebruikersdoelgroep van de software is zodanig gezagsgetrouw dat verwacht kan worden dat men geen illegaal hergebruik gaat toepassen. Deze aanname is waarschijnlijk niet van toepassing als het *gaming* software betreft, maar mogelijk wel bij internetstemsoftware waar de doelgroep voornamelijk bestaat uit overheden en grote organisaties.
- De werking van de software is gebaseerd op een geoctrooieerde uitvinding; deze werking is aldus al publiekelijk bekend maar als hergebruik van de software vrij is, zal de eigenaar van het octrooi daar mogelijk een (hoge) vergoeding voor willen ontvangen.

Hoewel het zeker niet gebruikelijk is dat de broncode van een informatiesysteem raadpleegbaar is zonder dat het informatiesysteem Open Source Software is, komt dit wel voor. En juist in situaties

waar de kwaliteit van de beveiliging in de software cruciaal is. Een bekend voorbeeld is dat van het bekende commerciële encryptieprogramma PGP ('Pretty Good Privacy'). Hiervan kan de broncode wel worden gedownload zodat gebruikers zelf kunnen vaststellen dat er geen (cryptografische) kwetsbaarheden in aanwezig zijn. Anders dan bij Open Source Software mogen de gebruikers de broncode niet gebruiken om aangepaste versies van het PGP programma te maken (zie [6.]). Een vergelijkbaar voorbeeld is dat van het product Cryptophone (zie[12.]) waarmee GSM verkeer kan worden versleuteld. Ook dat product biedt gebruikers de mogelijkheid de broncode te zien maar verbiedt verder gebruik daarvan. Overigens is een van de initiatiefnemers van "Wij vertrouwen stemcomputers niet" een van de medeoprichters van Cryptophone. Tot slot noemen we nog het 'Shared source initiative' van Microsoft (zie [11.]). Hierbij kunnen gebruikersorganisaties (met name overheden) de broncode van Microsoft programmatuur raadplegen om de beveiliging daarvan te kunnen analyseren.

Er zijn verschillende manieren waarop broncode van een internetstemsysteem publiekelijk raadpleegbaar kan worden gemaakt:

- De software kan vanaf de start als Open Source Software worden ontwikkeld, zodat niet alleen de broncode van het eindproduct te raadplegen is maar ook alle eerdere versies. Nadeel is dat de overheid mogelijk onvoldoende sturing heeft op het ontwikkelproces.
- De software kan initieel privaat worden ontwikkeld waarbij de broncode van het eindproduct in opdracht (en tegen betaling) van de overheid als Open Source Software wordt gepubliceerd. Op deze wijze zijn ondermeer het product A-select (de motor van DigiD initieel ontwikkeld door Alfa & Ariss) en het stemsysteem gebruikt in Kiezen Op Afstand 1 (ontwikkeld door LogicaCMG) open source software geworden. Nadeel hierbij is dat het mogelijk lastig is om een actieve ontwikkelgemeenschap te creëren die het product wil 'adopteren'. Ter illustratie, er is blijkbaar zo weinig interesse in het KOA1-stemsysteem dat de broncode niet (eenvoudig) te vinden is op het internet, laat staan dat er een actieve ontwikkelgemeenschap rond ontstaan is.
- De software kan privaat worden ontwikkeld waarbij de broncode van het eindproduct in opdracht van de overheid publiekelijk en min of meer anoniem raadpleegbaar is. Door het downloaden van de software is een licentieovereenkomst van toepassing die het hergebruik van de broncode beperkt of zelfs uitsluit.
- De software kan privaat worden ontwikkeld waarbij de broncode van het eindproduct in opdracht van de overheid publiekelijk raadpleegbaar is maar waarbij een geïnteresseerde eerst een licentieovereenkomst moet tekenen die het hergebruik van de broncode beperkt of zelfs uitsluit.

3.2 Deelconclusie

Vanuit het transparantiebeginsel van verkiezingen is het wel of niet publiek raadpleegbaar maken van de internetstemsysteem broncode de essentiële kwestie, het vrije hergebruik van de broncode, zoals binnen Open Source Software, speelt geen rol vanuit het transparantiebeginsel.

4. Gewenstheid van publiekelijk raadpleegbare broncode

4.1 Analyse

Om de wenselijkheid van publiek raadpleegbare broncode van een internetstemsysteem te duiden hebben wij een viertal recente, gezaghebbende bronnen geraadpleegd:

- de Adviescommissie inrichting verkiezingsproces [1.]
- de Commissie Besluitvorming Stemmachines [2.]
- de Raad van Europa [3.]
- de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE, zie [4.])

Vanuit deze bronnen wordt unaniem aangegeven dat de *transparantie* van het verkiezingsproces voor de burger essentieel is. In de woorden van de Adviescommissie inrichting verkiezingsproces ([1.]): "Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is, zodat in beginsel iedereen inzicht in de structuur ervan kan hebben. Er zijn in het verkiezingsproces geen geheimen. Vragen moeten beantwoord kunnen worden; de antwoorden moeten controleerbaar en verifieerbaar zijn."

De belangrijke vraag is of in de context van een internetstemdienst deze beginselen en aanbevelingen moeten worden geïnterpreteerd als eis om de broncode van de onderliggende internetstemsysteem publiekelijk raadpleegbaar te laten zijn of dat bijvoorbeeld zou kunnen worden volstaan met een onafhankelijke audit die de broncode van de internetstemdienst onderzoekt tegen gepubliceerde normen en daar een (publieke) verklaring over afgeeft.

Wij analyseren de uitspraken van de genoemde vier bronnen:

- De bovengenoemde omschrijving van transparantie door de Adviescommissie inrichting verkiezingsproces suggereert al dat de broncode niet 'geheim' kan zijn en dus dat deze publiekelijk raadpleegbaar zou moet zijn. In het rapport van de Adviescommissie inrichting verkiezingsproces ([1.]) staat verder op pagina 34: "De transparantie van stemmen per internet en telefoon hangt in grote mate af van het systeem dat wordt gebruikt. Alleen als de systemen volledig "open" zijn, bijvoorbeeld door het gebruik van opensourceprogrammatuur, is er sprake van enige transparantie." Hieruit kan geconcludeerd worden dat de adviescommissie van mening is dat het een vereiste is dat de broncode van het internetstemsysteem door iedereen raadpleegbaar is.
- De aanbevelingen van de Raad van Europa inzake e-voting (geadopteerd door het comité van ministers van de lidstaten, zie [3.]) bespreekt de wens/eis rond raadpleegbaarheid van de broncode van internetstemsystemen niet expliciet. Wel wordt gesteld dat de beveiliging van dergelijke systemen onafhankelijk moet worden geverifieerd. De aanbevelingen van de Raad van Europa sluiten echter niet uit dat de broncode van internet stemsystemen door iedereen raadpleegbaar zijn. Zie ook het volgende punt.
- In het rapport van de Commissie Besluitvorming Stemmachines (zie [2.]) staat op pagina 33 de conclusie: "Het referentiekader van de Raad van Europa moet worden vertaald naar de Nederlandse situatie. Kernbegrippen daarbij zijn transparantie en controleerbaarheid. De mogelijkheid voor de kiezer te controleren of de stem juist is opgeslagen, het introduceren van de mogelijkheid van een echte hertelling en de weg naar het gebruik van open-bron (source) software zijn drie belangrijke elementen in het nieuwe referentiekader." Uit dit citaat kan worden geconcludeerd dat de Commissie Besluitvorming Stemmachines van mening is dat het een vereiste is dat de broncode van een (internet) stemsysteem publiekelijk raadpleegbaar is. Verder kan uit dit citaat worden geconcludeerd dat de commissie meent dat daarmee ook invulling wordt gegeven aan de eerdergenoemde aanbevelingen van de Raad van Europa.

- Het OVSE rapport bevat een verslag van een waarnemingsmissie die zij stuurde naar de Tweede Kamer verkiezingen van november 2006. Daarbij werd ook het RIES (Rijnland Internet Election System) internetstem systeem gebruikt. Op pagina vijftien wordt gesteld "Development of an open source version of RIES, free of proprietary issues and secret components, should be encouraged". Hieruit kan geconcludeerd worden dat de OVSE van mening is dat het een vereiste is dat de broncode van het internetstemsysteem publiekelijk raadpleegbaar zou moeten zijn.

4.2 Deelanalyse

Op basis van de analyse van de gezaghebbende bronnen Adviescommissie inrichting verkiezingsproces, Commissie Besluitvorming Stemmachines, Raad van Europa en de OVSE concluderen wij dat voor invulling van het transparantiebeginsel bij een internetstemdienst het publiekelijk raadpleegbaar maken van de broncode van het onderliggende internetstemsysteem een vereiste is.

5. Het raadpleegbaar maken van broncode vanuit beveiligingperspectief

5.1 Analyse

Zoals beargumenteerd in het vorige hoofdstuk is het publiekelijk raadpleegbaar maken van de broncode van een internetstemsysteem gewenst vanuit het transparantiebeginsel. Vanuit dit beginsel zijn vanuit democratisch perspectief alleen voordelen te behalen en geen nadelen. In dit hoofdstuk onderzoeken wij dit vanuit het perspectief van beveiliging. Wij zullen daartoe een inschatting geven van de mogelijke *additionele* risico's van het publiek raadpleegbaar maken van de internetstemsysteem broncode in vergelijking met de situatie waarin dit niet het geval is.

Wij voeren daarvoor een hoofdlijn risico analyse uit in de lijn van de (internationale) ISO standaard 27001 (zie [9.]) voor informatiebeveiliging die ook is geadopteerd vanuit het Voorschrift Informatiebeveiliging Rijksdienst 2007. De standaard stelt dat een beveiligingsrisico een functie is van:

- bedreigingen (zaken die kunnen optreden)
- kwetsbaarheden (zaken die mogelijk maken dat een bedreiging manifest kan worden)
- de kans dat een bedreiging manifest kan worden
- de impact als een bedreiging daadwerkelijk manifest wordt

De bedreiging die we centraal stellen is die van kwaadwillende organisaties of (kleine) groepen van personen die beveiligingstekortkomingen in het internetstemsysteem vinden en deze exploiteren tijdens of na de verkiezingen met als mogelijke effecten:

- wantrouwen in het stemproces door het publiek, of zelfs
- ongeldigheid verklaring van de uitgevoerde verkiezingen

De kwetsbaarheid die hiermee verband houdt, is het mogelijk bestaan van (grote) beveiligingstekortkomingen in het internetstemsysteem. Uiteraard is de beveiliging van de stembeheersorganisatie ook een fundamenteel aspect van de beveiliging van de internetstemdienst, maar dat is voor deze discussie weinig relevant.

In onze analyse zullen wij drie typen kwaadwillende organisaties of personen onderscheiden:

- Type I: beperkte kennis en geld, veel tijd
  Dit type aanvaller staat ook wel bekend als 'script kiddie', een persoon die uit nieuwsgierigheid allerhande 'inbreektools' downloadt en hiermee probeert in te breken. Een dergelijk type aanvaller heeft weinig inhoudelijke kennis van de 'inbreektools'. Als deze niet werken dan geeft dit type aanvaller de aanval op.
- Type II: kennis en tijd, beperkte hoeveelheid geld
  Dit type aanvaller beschikt over kennis en tijd maar slechts over beperkte financiële middelen. Aanvallen worden uitgevoerd als 'hobby' of om aan te tonen dat men ertoe in staat is of om een organisatie te kijk te zetten. Er is in beginsel geen sprake van geldelijk gewin voor de aanvaller. Voorbeelden zijn personen die zich bezighouden met 'defacing' van websites (het 'troffeematig' en onbevoegd veranderen van websites), zie [7.]. Ook de groep 'Down Under Crew' die naar verluidt in januari 2002 een aanval uitvoerde op de *chatsessie* tussen het publiek en Prins Willem-Alexander en Prinses Maxima, valt waarschijnlijk in deze categorie.
- Type III: veel kennis, tijd en geld
  Dit type aanvaller beschikt over veel kennis, tijd en over ruime financiële middelen. Aanvallen worden uitgevoerd met als doel de democratische rechtsorde in Nederland te ondermijnen, bijvoorbeeld om bepaalde politieke beslissingen uit te stellen of te manipuleren. Indirect kan daar ook geldelijk gewin door de aanvaller (of zijn opdrachtgever) een rol bij spelen. Een dergelijk

type aanvaller kan gezocht worden onder (vijandige) buitenlandse inlichtingendiensten en terroristische organisaties. Aanvallers van dit type lijken mogelijk ver gezocht. Echter, een veelgehoord motief (vergelijk [8.]) voor de timing van de terroristische aanvallen in Madrid op 11 maart 2004 was de (uitslag van) de verkiezingen die drie dagen later plaatsvonden zodanig te beïnvloeden dat Spanje zijn troepen uit Irak snel zou terugtrekken, hetgeen overigens ook gebeurd is.

De waarschijnlijkheid dat de bedreiging manifest wordt, is gerelateerd aan de kans dat de kwetsbaarheid (beveiligingstekortkomingen in het internetstemsysteem) optreedt en dat deze door de aanvaller wordt ontdekt. In onderstaande tabel hebben wij per type aanvaller de verschillen in deze waarschijnlijkheid ingeschat in de situatie waarin de broncode publiekelijk raadpleegbaar is en de situatie waarin dit niet het geval is. Daarbij doen wij dus uitspraken over relatieve waarschijnlijkheden en nadrukkelijk niet over absolute waarschijnlijkheden.

Type	Waarschijnlijkheid dat bedreiging manifest wordt	Verschil
I	Voor een type I aanvaller maakt het niet substantieel uit of de broncode wel of niet raadpleegbaar is daar dit type aanvaller niet de kennis heeft of de moeite neemt om een veiligheidsanalyse uit te voeren op de broncode.	Geen
II	Dit type aanvaller zal zondermeer een veiligheidsanalyse uitvoeren op de broncode. Echter de verwachting is dat parallel aan deze kwaadaardige hackers ('blackhat') er ook goedwillende hackers ('whitehat') zullen zijn die een dergelijke veiligheidsanalyse zullen uitvoeren, zeker gezien de aandacht die er is naar de betrouwbaarheid van stemcomputers vanuit diverse universiteiten en bezorgde burgers zoals verenigd in de organisatie 'Wij vertrouwen stemcomputers niet'. De goedwillende hackers zullen echter wel tijdig beveiligingsproblemen signaleren zodat de kwaadwillende hackers ze niet meer kunnen exploiteren. De overheid moet door actieve communicatie (bijvoorbeeld voordrachten, prijsvragen) wel stimuleren dat de aandacht vanuit de 'goedwillende' hackersgemeenschap minstens zo groot is als die vanuit de 'kwaadwillende' hackersgemeenschap. Noot: Wij merken op dat als informatiebeveiliging adequaat is geborgd in het ontwikkelingsproces (vergelijk [10.]) de kans dat een type II aanvaller een groot beveiligingsprobleem ontdekt bijzonder klein zou moeten zijn. Ter illustratie, de broncode van het eerste Kiezen Op Afstand experiment ontwikkeld door LogicaCMG is na afloop van de verkiezingen als Open Source Software gepubliceerd. Er zijn hierdoor geen kwetsbaarheden aan het licht gekomen (zie [9]). Het niet aan het licht komen van kwetsbaarheden hoeft evenwel niet te betekenen dat deze er ook niet zijn; mogelijk is er gewoon 'niemand' geïnteresseerd om dit te onderzoeken.	Geen
III	Ook dit type aanvaller zal zonder meer een veiligheidsanalyse uitvoeren op de broncode en wel een met zeer grote diepgang. Wij verwachten echter dat voor een dergelijk type aanvaller niet substantieel uitmaakt of de broncode raadpleegbaar is of niet, daar dit type aanvaller wel op andere manieren aan de broncode kan komen. Bijvoorbeeld door deze gewoon te kopen van de commerciële partij die het internetstemsysteem heeft geproduceerd of door deze bijvoorbeeld door middel van reverse engineering te verkrijgen.	Geen

5.2 Deelconclusie

Op basis van bovenstaande risicoanalyse verwachten wij dat de beveiligingsrisico's verbonden met het publiekelijk raadpleegbaar maken van de broncode van een internetstemsysteem vergelijkbaar zijn met de beveiligingsrisico's met de situatie dat de broncode niet publiekelijk raadpleegbaar is. Dit laat daarmee onverlet dat in beide situaties de informatiebeveiliging adequaat moet zijn geborgd in het ontwikkelingsproces (vergelijk [10.]) om de absolute waarschijnlijkheden van manifestatie van de bedreigingen zo klein mogelijk te houden.

6. Referenties

[1.] "Stemmen van vertrouwen", Adviescommissie inrichting verkiezingsproces, 27 september 2007.

[2.] "Stemmachines, een verweesd dossier", Commissie Besluitvorming Stemmachines, april 2007.

[3.] "Legal, Operational and Technical Standards for E-Voting", Recommendation Rec(2004)11 adopted by the committee of ministers of the Council of Europe on 30 september 2004.

[4.] "The Netherlands, Parliamentary elections 22 November 2006", Organisatie voor Veiligheid en Samenwerking in Europa (OVSE), 12 maart 2007.

[5.] http://www.gnu.org/copyleft/gpl.html

[6.] https://www.pgp.com/downloads/sourcecode/

[7.] http://www.zone-h.org

[8.] http://www.washingtonpost.com/wp-dyn/articles/A38817-2004Oct16.html

[9.] "Information security management systems – requirements", ISO 27001, 2005-10-15.

[10.] 'Security Considerations in the Information System Development Life Cycle', NIST special publication 800-64, juni 2004. Zie http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf.

[11.] http://www.microsoft.com/resources/sharedsource/Licensing/GSP.mspx

[12.] http://www.cryptophone.de/background/published_source

[13.] Persoonlijke communicatie met lid van het Kiezen op Afstand 1 project.