2699057101

Aanvallen op het stemgeheim via elektromagnetische effecten

Algemene Inlichtingen- en Veiligheidsdienst
Directie Beveiliging
Nationaal Bureau voor Verbindingsbeveiliging

27 oktober 2006

Samenvatting

Dit rapport beschrijft de uitkomsten van een onderzoek dat door het Nationaal Bureau voor Verbindingsbeveiliging is uitgevoerd naar het stralingsgedrag van stemmachines van twee fabrikanten. Doel van het onderzoek is aanvallen te identificeren die het stemgeheim van individuele kiezers opheffen. Voor de Sdu NewVote machine zijn twee eenvoudig uit te voeren aanvallen op het stemgeheim gevonden. De Nedap/Groenendaal stemmachines blijken beter bestand tegen aanvallen via elektromagnetische effecten, zij het met enkele eenvoudige modificaties.

Inhoudsopgave

1 Inleiding

Naar aanleiding van berichten in de media op basis van een rapport van de stichting "Wij vertrouwen stemcomputers niet", [1], heeft het Nationaal Bureau voor Verbindingsbeveiliging opdracht gekregen een onderzoek uit te voeren naar mogelijke schending van het stemgeheim via elektromagnetische effecten uit stemmachines.

De basisvraag zoals die is gesteld is de volgende: "Is het denkbaar dat het stemgeheim van een kiezer kan worden geschonden door het opvangen van (elektromagnetische) straling vanuit een stemmachine." Hierbij is onderscheid gemaakt naar twee situaties:

1. afluisteren van het stemmen in het stemlokaal (onopvallende, kleine apparatuur waarbij de aanvaller de stemmer direct ziet) via:
   (a) de 'CDA detector' zoals genoemd in [1] (op de Nedap/Groenendaal apparatuur);
   (b) een algemene aanval via elektromagnetische straling, dat wil zeggen detectie van individuele stemmen.
2. afluisteren van het stemmen vanaf een locatie buiten het stemlokaal, via:
   (a) de 'CDA detector' (op de Nedap/Groenendaal apparatuur);
   (b) een algemene aanval via elektromagnetische straling, dat wil zeggen detectie van individuele stemmen.

Voor alle aanvallen die hier worden beschreven is uitgegaan van een kennisniveau dat correspondeert met dat van de auteurs van het rapport van de stichting WVSN, [1]. Deze inschatting is gebaseerd op het genoemde rapport en relevante open publicaties.

Dit rapport neemt geen stelling over andere aspecten dan het elektromagnetisch gedrag en de aanvallen op het stemgeheim die hiermee kunnen worden uitgevoerd. In dit rapport zijn technische details weggelaten die derden in staat stellen de aanvallen makkelijk te reproduceren. In dit rapport zijn geen vertrouwelijke bedrijfs- of fabricagegegevens opgenomen.

2 Verkorte conclusies

De belangrijkste conclusies van het onderzoek worden hieronder kort weergegeven. In volgende secties worden de achtergronden en de geconstateerde resultaten verder toegelicht.

2.1 Sdu NewVote

Succesvolle aanvallen op de Sdu NewVote machine blijken mogelijk te zijn onder alle beschouwde scenario's. Voor deze stemmachine is het mogelijk om op afstanden tot 40 meter – hierbij is rekening gehouden met een muur tussen aanvaller en stemmachine – het beeld dat de kiezer op het scherm ziet te reproduceren. Er kan 'live' worden meegekeken met de kiezer met apparatuur die door amateurs kan worden gebouwd, zonder dat kennis van het exacte ontwerp van de NewVote machine benodigd is.

Een eenvoudiger aanval op de NewVote machine kan op basis van alleen hoorbare signalen worden uitgevoerd met bescheiden middelen. Deze audio aanval kan over grotere afstanden worden uitgevoerd. Extrapolatie van de meetgegevens impliceert dat een aanvaller met een redelijke wereldontvanger of scanner op afstanden groter dan 50 meter onderscheid naar partijen kan maken. Merk op dat, in tegenstelling tot de hierboven beschreven aanval, voor

deze aanval een referentie nodig is, zie ook Sectie 6.2. Deze referentie kan worden verkregen door eenmalige toegang tot het systeem als normale kiezer.

Voor de Sdu NewVote machine zijn geen maatregelen gevonden die de gesignaleerde stralingsproblemen kunnen wegnemen en die op korte termijn realiseerbaar zijn[1].

2.2 Nedap/Groenendaal ES3B, ESN1, ESD1

Voor alle onderzochte types[2] van de Nedap/Groenendaal stemmachines geldt dat het stralingsgedrag sterk onder dat van de Sdu machine ligt. Een aanval waarbij het scherm meegelezen kan worden is daarmee onwaarschijnlijk, anders dan op zeer korte afstand (kleiner dan 5 meter.) Zoals al in het rapport van de stichting WVSN, [1], is beschreven, kan op afstand een hoorbaar signaal worden waargenomen dat afhangt van het gebruik van diakritische tekens, zoals de 'è' in appèl.

Deze aanval is initieel geverifieerd voor de ES3B stemmachine en kon ook succesvol worden toegepast op het type ESD1. De ESN1 blijkt niet gevoelig voor deze aanval. Uit experimenten blijkt dat een aanvaller op het gehoor onderscheid kan maken naar het aantal verschillende diakritische tekens dat op het display wordt getoond. Via het tellen van diakritische tekens blijkt één kandidaat wegens de drie verschillende diakritische tekens in zijn achternaam uniek identificeerbaar. Op basis van de meetgegevens mag worden verwacht dat met nabewerking van het opgevangen audiosignaal ook unieke kenmerken van partijen en kandidaten kunnen worden bepaald. Dit is inmiddels experimenteel geverifieerd.

De gevonden resultaten zijn gelijk voor zowel de originele stemgeheugens als door Nedap/Groenendaal aangepaste stemgeheugens. Doel van de aanpassing was de gepubliceerde 'CDA detector' te voorkomen, dit blijkt niet effectief.

Voor de Nedap/Groenendaal machines zijn drie simpele maatregelen gevonden die de bestaande problemen wellicht kunnen beperken:

- toepassen van ferrietkernen op de individuele flatcables tussen de centrale behuizing en het beeldscherm;
- het aanbrengen van stralingswerende middelen op het display en in de displaybehuizing;
- alle gebruikte diakritische tekens altijd op het display weergeven.

Voor elk van deze mogelijke oplossingen geldt dat verificatie van de effectiviteit noodzakelijk is. Daarbij geldt dat de daadwerkelijke oplossing ligt in het onderdrukken van de compromitterende elektromagnetische effecten.

2.3 Conclusies

Uit het onderzoek zoals dat is uitgevoerd blijkt dat aanvallen via elektromagnetische effecten uitvoerbaar zijn.

[1] De genoemde aanvallen kunnen naar verwachting slechts via een herontwerp worden weggenomen.

[2] Het type ES3A stemmachine is niet onderzocht aangezien de leverancier dit type niet kon leveren.

Op basis van het succesvol reproduceren van de scherminhoud van de NewVote machines op genoemde afstanden, luidt de conclusie dat het stemgeheim bij verkiezingen met behulp van dit apparaat bij een aanval geschonden kan worden.

Op basis van het succesvol identificeren van de partij waarop de kiezer wenst te stemmen bij gebruik van de NewVote machines via audiosignalen, luidt de conclusie dat het stemgeheim bij verkiezingen met behulp van dit apparaat kan worden geschonden voor wat betreft de partij waarop wordt gestemd. De mate waarin de aanvaller onderscheid kan maken is bepaald door de hoeveelheid referentiesignalen die via een geregistreerde kiezer simpel kan worden gegenereerd.

Op basis van de aanval op de Nedap/Groenendaal stemmachines waarmee het aantal verschillende diakritische tekens op het scherm kan worden geteld, kan worden geconcludeerd dat één kandidaat uniek kan worden bepaald via een wereldontvanger of scanner. Daarnaast kan op basis van het aantal diakritische tekens met redelijke zekerheid worden bepaald of een kiezer CDA of EénNL stemt.

2.4 Aanbevelingen

Hoewel elektronische apparatuur van nature elektromagnetische effecten voortbrengt kunnen de effecten die de beschreven aanvallen mogelijk maken in de ontwerpfase worden ingedamd. Expliciete eisen aan stemmachines op dit gebied worden daarom aanbevolen.

3 Elektromagnetische effecten – een inleiding

Elektronische apparatuur produceert elektromagnetische effecten (EM) die storing kan veroorzaken in de ontvangst van radio en televisie signalen. EM straling is in feite 'gewone' radiostraling, de effecten die hier worden bedoeld zijn de onbedoelde emissies die als bij-effect optreden. Dit feit is al bekend zolang er elektronische apparatuur bestaat.

In 1985 werd met de publicatie van het artikel "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" van Wim van Eck, [2], het eerste publieke verslag gedaan van exploitatie van de informatie in dergelijke straling. In de elektromagnetische effecten die een apparaat uitzendt, lift namelijk ook informatie mee die direct afhankelijk is van interne processen in het apparaat. Door de elektromagnetische effecten te onderscheppen, kan een aanvaller meer te weten komen over wat er in het systeem plaatsvindt.

Voor zijn aanval maakte Van Eck gebruik van: "a little knowledge of the principles of TV reception and an investment of about $5." De informatie die hij terug wist te vinden in de straling bestond uit de aansturingsinformatie van een computermonitor. Door de onderschepte informatie aan een andere monitor aan te bieden, werd het beeld op afstand gereproduceerd. Voor het afstemmen van de ontvanger werd bij deze experimenten gebruik gemaakt van standaard elektronische testapparatuur. De demonstraties die in Nederland en Engeland op televisie werden gegeven baarden redelijk wat opzien.

Na het artikel van Van Eck zijn ook eerdere aanvallen op basis van elektromagnetische effecten beschreven. Tegengaan van elektromagnetische effecten

is echter voornamelijk bestudeerd in het kader van tegengaan van storingen en dus het minimaliseren van elektromagnetische effecten. Dit laatste vakgebied komt bijvoorbeeld tot uiting in CE stralingsnormen (EMC) waaraan elektronica dient te voldoen.

Het gebruik van gemeten elektromagnetische effecten om informatie uit een gesloten systeem te reconstrueren dook pas in het begin van de jaren 90 weer op in de literatuur. Sinds eind jaren 90 is vooral ook Markus Kuhn van de universiteit van Cambridge een belangrijke speler op dit gebied in de open literatuur. In dit rapport is het werk van Kuhn dan ook als een belangrijke maatstaf gebruikt, met name het technische rapport op basis van zijn proefschrift [3].

4 Dreigingsscenario

In het beschouwde dreigingsscenario wordt uitgegaan van een strikt passieve aanvaller. Deze aanvaller beschikt alleen over door de stemmachine uitgezonden elektromagnetische effecten. Een strikte aanname in het dreigingsscenario is dat de aanvaller hooguit als legitieme kiezer toegang tot de stemmachine heeft of heeft gehad, waarmee modificatie van stemmachines wordt uitgesloten. De kieslijsten worden verondersteld bekend te zijn bij de aanvaller, aangezien deze worden gepubliceerd.

Voor de uitgevoerde tests is uitgegaan van kennis en middelen die publiekelijk voorhanden zijn. Dit sluit aan bij het beeld van een competente amateur die werkt volgens gepubliceerde aanvallen en met relatief goedkope commerciële apparatuur met eventueel zelfgebouwde componenten. Beschreven methoden en technieken uit het rapport van de stichting WVSN over de Nedap/Groenendaal ES3B machine vormen een belangrijke ingrediënt voor dit model.

Daarnaast is uitgegaan van aanvallen met een minimum aan specialistische nabewerking. Een aanval die met weinig tot geen instructie uitgevoerd kan worden, op basis van aangeleverde apparatuur, wordt gezien als een grotere bedreiging dan een aanval die in alle stadia een hoog kennisniveau vraagt.

Een specifieke klasse van aanvallen die is uitgesloten van dit onderzoek zijn EM effecten in het visuele spectrum: zichtbaar licht.

5 Aanvalsscenario's

Voor de daadwerkelijke aanval heeft de aanvaller twee gegevens nodig: informatie over de identiteit van de kiezer en diens uitgebrachte stem. Combinatie van beide gegevens betekent schending van het stemgeheim voor de betreffende kiezer.

5.1 Identiteit van de kiezer

Aangezien de naam van de kiezer hardop wordt voorgelezen door de leden van het stembureau, mag worden gesteld dat de aanvaller de identiteit van de stem kan vaststellen.

Voor aanvallen waarbij de aanvaller zich buiten het stemlokaal bevindt, is het mogelijk dat een tweede persoon in het lokaal meeluistert en via bijvoorbeeld mobiele telefoon de namen doorgeeft. Andere mogelijkheden via (verbor-

gen) microfoons, opname apparatuur en dergelijke zijn hierbij ook mogelijk. In dit rapport wordt uitgegaan van instantane koppeling tussen een identiteit en een stem.

Buiten deze aanname kan door middel van correlatie van de geobserveerde tijd van binnenkomst van een stemmer – zeg via een verrekijker of videocamera – en tijdstip van het daadwerkelijk registreren van de stem door een aanvaller op afstand, een zeer nauwkeurige verbinding worden gemaakt tussen personen en hun stem. Hiermee is alleen de naam nog onbekend in het algemene geval, tenzij de aanvaller na de verkiezing de oproepkaarten in volgorde zou kunnen bemachtigen of bijvoorbeeld videomateriaal weer aan identiteiten kan koppelen.

5.2 Afstanden

Voor aanvallen op afstand is de daadwerkelijk haalbare afstand uiteraard van belang. In dit rapport houden wij de volgende onderverdeling aan:

- in het stemlokaal (binnen 10 meter);
- dichtbij het stemlokaal (10 tot 40 meter);
- lange afstand (meer dan 40 meter).

Deze genoemde afstanden zijn gekozen op persoonlijke ervaringen met stembureaus van het testteam. Het is belangrijk te onthouden dat in het geval van radiostraling verschillende factoren van belang zijn voor de sterkte van het signaal. Gezien de mogelijkheid om via een verkenner in het stemlokaal tenminste een lijst met opeenvolgende kiezers samen te stellen, zijn aanvallen waarbij apparatuur buiten het stemlokaal wordt opgesteld praktisch uitvoerbaar. Dit heeft ondermeer effect op de maximale grootte van antenne en overige apparatuur.

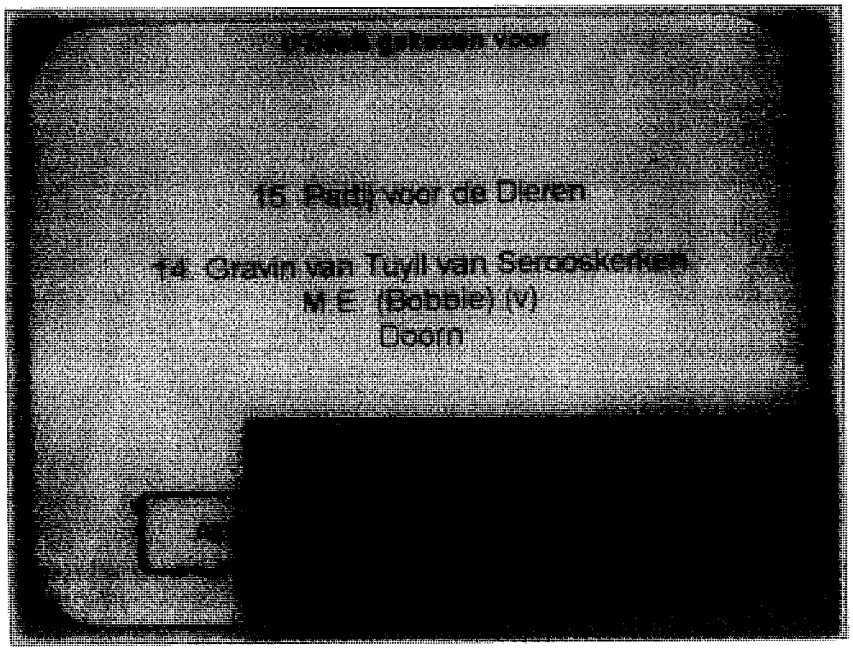
Aangezien in de uitgevoerde testen geen maatregelen zijn genomen om ontvangen signalen op te schonen, te versterken of na te bewerken, kunnen de genoemde afstanden als minimumafstanden worden geïnterpreteerd. Intentie van de testen is het toetsen van haalbaarheid, daarom is in de beperkte beschikbare tijd voorbijgegaan aan optimalisaties zoals die in de publiek beschikbare literatuur worden beschreven.

6 Sdu NewVote

De Sdu NewVote machines zijn vergelijkbaar met een standaard personal computer. Enkele functionaliteiten die op de gemiddelde PC voorkomen zijn niet aanwezig of worden niet gebruikt. Het systeem wijkt ondermeer af van een PC qua behuizing en op het feit dat het een touchscreen bevat in plaats van een toetsenbord/muis combinatie.

6.1 Schermreproductie op afstand

De eerste succesvolle aanval op basis van opgevangen elektromagnetische effecten uit de Sdu NewVote machine is uitgevoerd binnen twintig minuten na het aanzetten van de eerste machine. Hiervoor is een meetopstelling gebruikt



Figuur 1: Een voorbeeld van de schermreproductie van de Sdu NewVote stemmachine. Beide afbeeldingen zijn met een fototoestel direct van de schermen genomen. De effectieve afstand van antenne tot stemmachine is ongeveer 25 meter, er zijn geen voor- of nabewerkingen op het signaal uitgevoerd.

die zodanig is ingesteld dat deze binnen de parameters van publiek bekende aanvallen valt, [2, 3]. Het beeld dat de kiezer op het stemscherm ziet wordt bij deze aanval op een generieke computermonitor gereproduceerd, zodat de stem eenduidig kan worden bepaald. Deze ruwe opzet leverde meetresultaten die op afstanden voor succesvol meelezen impliceert van 30 tot 40 meter.

Voor deze eerste aanval was geen speciale kennis nodig van de machine anders dan visuele inspectie van de machine. Bij overdracht van de machines is door medewerkers van Sdu Uitgevers een korte uitleg gegeven over de verschillende aspecten van het systeem, hierbij zijn effecten in het elektromagnetisch spectrum niet anders dan globaal ter sprake gekomen.

Zodra een werkende opstelling is gebouwd is geen speciale kennis meer nodig. Een aanvaller hoeft slechts op de basisfrequentie af te stemmen die bij de stemmachines hoort. Deze frequenties verschillen van exemplaar tot exemplaar, zodat de aanvaller alleen nog moet 'scherpstellen.' Verschillende stemmachines die naast elkaar staan kunnen apart worden bekeken. De aard van de aanval staat toe dat op de ochtend van de verkiezingsdag op het startscherm van de NewVote stemmachine kan worden scherpgesteld waarna alle volgende stemmen kunnen worden gevolgd.

Om te testen of de aanval haalbaar zou zijn met zeer beperkte middelen is de antenne gedurende de initiële testen vervangen door een zogenaamde dipoolantenne bestaande uit twee snoertjes. Dit bleek tot gelijkwaardige resultaten te leiden. De enige min of meer bijzondere component in de opstelling is een ap-

paraat dat de synchronisatiesignalen voor de gebruikte monitor toevoegt aan de opgevangen elektromagnetische effecten van de stemmachine. Dergelijke apparatuur is goed beschreven in de publieke literatuur en ligt binnen het bereik van een gevorderde amateur.

Uiteindelijk is aan vijf NewVote machines gemeten op de sterkte van het uitgestraalde elektromagnetisch veld. De resultaten laten zien dat reproductie van het scherm op een afstand van 40 meter haalbaar is zonder nabewerking of versterking, conform de aanvalsscenario's.

Benodigde middelen voor de beschreven aanval zijn relatief bescheiden. Hoewel met duurdere specialistische apparatuur betere resultaten kunnen worden behaald, volstaat een aantal componenten dat in het gemiddelde huishouden kan worden gevonden:

- tuner uit een televisietoestel;
- antenne, simpele draadjes volstaan;
- computer monitor.

Daarbij is echter een speciale component noodzakelijk die de synchronisatie van het beeld op de ontvangende monitor invult. Voor de uitgevoerde testen is een speciaal apparaat gebruikt. Bij bekende beeldfrequenties kan dit met een relatief eenvoudige schakeling die door een amateur gebouwd kan worden.

6.2 Aanval op basis van karakteristieke audiosignalen

De frequentie waarop het scherm wordt opgebouwd en ververst ligt binnen het hoorbare bereik (bromtonen tot fluittonen.) Via door de stemmachine uitgestraalde elektromagnetische effecten kan dit signaal meeliften en weer terug worden gehaald. Dit is vergelijkbaar met de "plopgeluiden" die een GSM op een radio teweegbrengt.

Via een relatief eenvoudige scanner – een wat geavanceerde radio ontvanger – of een wereldontvanger kunnen de signalen uit de Sdu stemmachine hoorbaar worden gemaakt. De toonhoogte correspondeert met de lay-out en inhoud van het scherm dat de kiezer voor zich ziet. Vooral de schermen waarop de kandidaten per kieslijst worden getoond, blijken een karakteristieke toon voort te brengen die door mensen makkelijk te onderscheiden is. Daarbij is het startscherm van de overige schermen te onderscheiden, zodat de laatstgehoorde karakteristieke toon de partij is waarop een stem is uitgebracht.

Op basis van een eerste verkenning door de aanvaller of een handlanger waarbij alle schermen met lijsten worden doorlopen – een handeling die zo'n 30 tot 40 seconden kost – zijn de karakteristieke tonen aan de partijen te koppelen. Na deze actie kan de aanvaller op het gehoor de tonen naar partijen herleiden. De signalen zijn dermate karakteristiek dat de verkenning slechts op een enkele stemmachine uitgevoerd hoeft te worden. De referentiesignalen kunnen dan tegen alle andere stemmachines worden ingezet, tenminste die in hetzelfde kiesdistrict. Deze laatste nuance geldt vanwege de verschillen in de kieslijsten per district.

Deze aanval levert op meer dan 50 meter afstand betrouwbare resultaten, een extrapolatie gebaseerd op de sterkte van het signaal. Wegens gebrek aan tijd is deze aanval niet verder verfijnd. Het is echter waarschijnlijk dat op basis

van de audiosignalen ook de gekozen kandidaat uniek kan worden bepaald. Daarvoor is echter enige bewerking van het ontvangen signaal en mogelijke enige nabewerking nodig. Een dergelijke aanval ligt in de lijn van de "CDA detector" zoals door de stichting WVSN is gepubliceerd.

6.3 Haalbaarheid van de aanvallen

In het kader van de uitgevoerde testen op de Sdu NewVote apparatuur zijn de gebruikte meetinstrumenten opzettelijk zodanig beperkt ingesteld dat een aanval door een goed onderlegde amateur wordt gesimuleerd. Hierbij zijn publieke bronnen geraadpleegd die vergelijkbare aanvallen beschrijven. Daarbij wordt verder uitgegaan van vergelijkbare kennis en middelen als de auteurs van het rapport van de stichting WVSN hebben gedemonstreerd. Op basis van de behaalde resultaten, luidt de conclusie dat een aanvaller in staat moet worden geacht om binnen het stemlokaal of relatief in de nabijheid van het stemlokaal het beeldscherm te reproduceren.

Voor de aanval via audio kan met behulp van een scanner of wereldontvanger en een simpele verkenning een vergelijkbare aanval worden opgezet. In combinatie met een (handheld)computer kan deze aanval verder worden verfijnd.

6.4 Tegenmaatregelen

In het geval van de Sdu NewVote apparatuur zijn enkele standaardmethoden om elektromagnetische effecten te dempen denkbaar. Hierbij zijn alleen eenvoudige externe maatregelen beschouwd vanwege de beperkt tijd die voor de testen beschikbaar was en het feit dat de behuizing niet is geopend. Afdekken van het scherm met stralingsremmende folie is een methode die in veel gevallen significante resultaten oplevert. In het geval van de NewVote bleek het gemeten effect van deze maatregel echter vrijwel nihil. Dit is voldoende indicatie dat andere externe maatregelen eveneens niet effectief zullen zijn.

Om het elektromagnetisch stralingsgedrag van de NewVote machines te verbeteren is een herontwerp van de machine noodzakelijk. Zonder kennis van details van het binnenwerk van de machine kan de impact van deze conclusie niet worden bepaald, mogelijkerwijs volstaat een nieuwe behuizing.

6.5 Conclusies

Op basis van het succesvol reproduceren van de scherminhoud van de NewVote machines op genoemde afstanden, luidt de conclusie dat het stemgeheim, bij gebruik van de Sdu NewVote stemmachine onder druk staat.

De mate waarin de aanvaller onderscheid kan maken naar de partij waarop een kiezer stemt, is bepaald door de hoeveelheid referentiesignalen die via een geregistreerde kiezer simpel kan worden gegenereerd.

Gezien de sterkte van de uitgezonden elektromagnetische effecten en het gemak waarmee deze signalen kunnen worden gekoppeld aan de daadwerkelijk uitgebrachte stem, blijft alleen een herontwerp van de stemmachine een echte oplossing voor de geconstateerde gebreken[3].

[3]Dit zou eventueel beperkt kunnen blijven tot een nieuwe behuizing, maar dit kan niet met

7 Nedap/Groenendaal ES3B, ESN1, ESD1

Nedap/Groenendaal levert in Nederland vier verschillende types stemmachines. Drie van de vier types – ES3B, ESN1 en ESD1 – zijn in het onderzoek beschouwd, het type ES3A kon niet door Nedap/Groenendaal geleverd worden. Het type met de aanduiding ES3B, is onderwerp van het rapport van de stichting WVSN, [1]. Met name de aanval waarvan wordt geclaimd dat deze CDA stemmers kan identificeren is onderzocht.

Het algemene elektromagnetisch stralingsgedrag van de Nedap/Groenendaal machines ligt significant onder dat van de Sdu NewVote stemmachines. Een belangrijke reden daarvoor is het feit dat in de ES3B machine verschillende stralingsremmende maatregelen zijn getroffen. Deze maatregelen zijn, getuige de gemeten resultaten, ook genomen in de ESD1 en ESN1 types. Het gehele display – waarop de kiezer ondermeer de gekozen kandidaat ter bevestiging ziet – ligt bij alle types echter inclusief aansturing buiten deze maatregelen.

7.1 Aanval op basis van diakritische tekens

De plaatsing van het display op de Nedap/Groenendaal stemmachines maakt het mogelijk om elektromagnetische effecten die deze display veroorzaakt op te vangen tot op afstanden rond de 20 meter met behulp van een scanner of wereldontvanger. Gebruik van diakritische tekens op het display – zoals de 'è' in appèl – verstoort de normale aansturing waardoor karakteristieke signalen opgevangen kunnen worden. Deze signalen zijn qua toon op het gehoor te onderscheiden. Deze claim uit het rapport van de stichting WVSN is geverifieerd op de ES3B en ESD1 stemmachines. Het type ESN1 stemmachine blijkt niet gevoelig voor de aanval op basis van het aantal diakritische tekens.

Nader onderzoek heeft aangetoond dat de opgevangen toon varieert op basis van het aantal verschillende diakritische tekens op het scherm. Via het gehoor kan dus worden bepaald hoeveel verschillende diakritische tekens op het scherm staan. Dit leidt ertoe dat bijvoorbeeld de kandidaten – zonder diakritische tekens in hun naam – van CDA of de lijst EénNL en de lijsttrekker ChristenUnie dezelfde signatuur laten horen. Eén kandidaat van het CDA, met in totaal 4 diakritische tekens op het display, is uniek te identificeren ten opzichte van alle andere kandidaten.

In antwoord op de in het rapport van de stichting WVSN gepubliceerde 'CDA detector' heeft Nedap/Groenendaal een tegenmaatregel voorgesteld. Tijdens de testen is deze tegenmaatregel[4] van Nedap/Groenendaal ook geëvalueerd. De maatregel blijkt geen effect te hebben, anders dan het verhogen van het aantal gedetecteerde verschillende diakritische tekens met één. Daarbij bleek met deze maatregel de blanco stem uniek identificeerbaar.

Er mag worden verwacht dat op basis van de audio informatie meer dan alleen het aantal diakritische tekens kan worden bepaald. Dit vergt nabewerking die, hoewel in de lijn van de "CDA detector", om specialistische kennis en duurdere apparatuur vraagt die niet binnen het in dit rapport beschouwde dreigingsscenario passen.

zekerheid worden vastgesteld zonder metingen aan zo'n nieuwe behuizing.

[4]Via het stemgeheugen werd aan alle partijnamen een extra karakter – een tilde – toegevoegd.

7.2 Meekijken op het scherm

Gezien de mate van afscherming in de behuizing zelf, is de belangrijkste bron van elektromagnetische effecten de display-unit. Gegeven de huidige kennis van dit display mag niet worden uitgesloten dat het gehele scherm meegelezen kan worden. Het stralingsprofiel van de stemmachine laat echter zien dat dit tot afstanden tot ongeveer 5 meter realistisch is, gegeven de beschouwde aanvalsscenario's. De Nedap/Groenendaal ESN1 stemmachine blijkt het meest gevoelig voor een dergelijke aanval, maar de sterkte van de elektromagnetische effecten impliceert afstanden van minder dan 5 meter.

Vanwege de beperkte beschikbare tijd is deze aanval niet daadwerkelijk uitgevoerd. Gezien de verwachte maximum afstand en gegeven de hieronder beschreven tegenmaatregelen, lijkt een dergelijke aanval weinig kansrijk.

7.3 Haalbaarheid

In het geval van de Nedap/Groenendaal stemmachines is de aanval op basis van diakritische tekens dé serieuze aanval. Qua investeringen kan deze aanval makkelijk worden opgezet, terwijl de kennis via het rapport van de stichting WVSN vrij toegankelijk is.

7.4 Tegenmaatregelen

Bij het onderzoek naar de Nedap/Groenendaal stemmachines is vastgesteld dat de meeste componenten relatief goed zijn afgeschermd op het gebied van elektromagnetische effecten. De display-unit – inclusief de bekabeling vanuit het binnenwerk – is een kritisch punt voor wat betreft deze effecten. Hierdoor mag worden verwacht dat het mogelijk is om met relatief simpele maatregelen de maximum afstand te beperken waarop een aanvaller kan 'meeluisteren'.

Beschouwde mogelijkheden zijn:

- het aanbrengen van ferrietkernen op de flatcable tussen de behuizing en het display;
- het aanbrengen van stralingswerende middelen op het display en in de displaybehuizing;
- alle gebruikte karakters met diakritische tekens altijd op het display vertonen (Ç, Ö, Ü, Ä, Ï , Ë, Ó, É, Á en È).

Elk van deze maatregelen moet worden beschouwd als een voorlopige maatregel totdat in het ontwerp van de stemmachines de nodige wijzigingen kunnen worden doorgevoerd. Alleen de eerstgenoemde maatregel is daadwerkelijk getest.

De eerste twee maatregelen zijn relatief simpel uit te voeren. Het gaat letterlijk om het losmaken van twee schroeven in het eerste geval en vier schroeven in het tweede geval. De derde maatregel is wellicht de meest simpele, maar neemt de oorzaak van het fundamentele probleem niet weg. Daarbij geldt dat de daadwerkelijke oplossing ligt in het onderdrukken van de compromitterende elektromagnetische effecten.

7.5 Conclusies

Op basis van de aanval waarmee het aantal verschillende diakritische tekens op het scherm van de ES3B en ESD1 kan worden onderscheiden, kan worden geconcludeerd dat één kandidaat uniek kan worden bepaald via een wereldontvanger of scanner. Daarnaast kan op basis van het aantal diakritische tekens met redelijke zekerheid worden bepaald of een kiezer CDA of EénNL stemt, zij het met enige ruis vanwege kandidaten met een diakritisch teken in voor- of achternaam.

Het type ESN1 lijkt vooralsnog niet vatbaar voor de beschreven aanval. Hier mogen vooralsnog geen conclusies aan worden verbonden. Het stralingsniveau is vergelijkbaar met dat van de andere types.

Vanwege de gevonden tegenmaatregelen kan echter worden gesteld dat het stralingsgedrag van de Nedap/Groenendaal apparatuur waarschijnlijk voldoende kan worden beperkt om de risico's van de beschouwde aanvallen te beperken.

Referenties

[1] Rop Gonggrijp, Willem-Jan Hengeveld, Andreas Bogk, Dirk Engling, Hannes Mehnert, Frank Rieger, Pascal Scheffers, Barry Wels. "Nedap/Groenendaal ES3B voting computer – a security analysis." Stichting "Wij vertrouwen stemcomputers niet", October 4, 2006 17:21, `http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf`

[2] Wim van Eck. "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" Computers and Security, 4(4), 1985.

[3] Markus G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays." Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.