

Aanvallen op het stemgeheim via elektromagnetische effecten

Uittreksel

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.

Inhoudsopgave

1	Inleiding	1
2	Verkorte conclusies	2
3	Dreigingsscenario	3
4	Aanvalsscenario's	4
5	Sdu NewVote	5

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 5.2. 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 zijn¹.

2.2 Conclusies

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

Op basis van het succesvol reproduceren van de scherm inhoud 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.

2.3 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 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.

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

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

4 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.

4.1 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 (verborgen) 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.

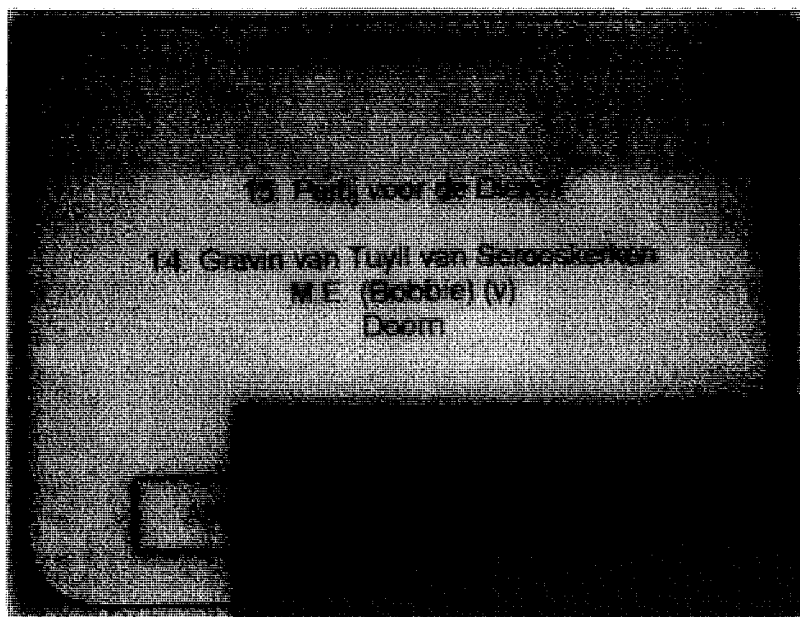
4.2 Afstanden

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



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.

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.

5 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.

5.1 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 die zodanig is ingesteld dat deze binnen de parameters van publiek bekende aanvallen valt, [2, 3]. Het beeld dat de kiezer op het stembord 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 meelesen 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 dipool-antenne bestaande uit twee snoertjes. Dit bleek tot gelijkwaardige resultaten te leiden. De enige min of meer bijzondere component in de opstelling is een apparaat 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.

5.2 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 "ploggeluiden" die een GSM op een radio tweegbrengt.

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.

5.3 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.

5.4 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, mogelijkserwijs volstaat een nieuwe behuizing.

5.5 Conclusies

Op basis van het succesvol reproduceren van de scherm inhoud 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 gebreken².

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.

²Dit zou eventueel beperkt kunnen blijven tot een nieuwe behuizing, maar dit kan niet met zekerheid worden vastgesteld zonder metingen aan zo'n nieuwe behuizing.