Deskundigenrapport dr. M. Rieback over gebruik vingerafdrukken voor paspoortbeveiliging 20-9-2016

1. Inleiding

De heer W.P. Willems verzocht mij, dr. M. Rieback (biografie als **bijlage 1**), om als objectieve deskundige te oordelen over de veiligheid van het systeem voor de opslag en controle van vingerafdrukken ten behoeve van paspoorten. In het voorliggende rapport zal ik toelichten welke risico's verbonden zijn aan dit systeem (**paragraaf 2**). Dit baseer ik op mijn kennis als deskundige van de literatuur (zie voor een selectie **bijlage 2**) en van de praktijk van beveiliging van chips en digitale systemen in het algemeen. Deze risico's heb ik aan de Afdeling bestuursrechtspraak van de Raad van State tijdens de zitting d.d. 3 december 2015 voorgehouden. Op het verloop van deze zitting en de uitspraak van de Afdeling gaat dit rapport ook in (**paragraaf 3**). Vervolgens ga ik in op de mogelijkheid om een ander middel dan vingerafdrukken te gebruiken voor paspoortcontroles (**paragraaf 4**). Dit rapport sluit af met een korte conclusie (**paragraaf 5**).

2. Veiligheid van opslag en controle van vingerafdrukken

In deze paragraaf zet ik eerst uiteen hoe vingerafdrukken misbruikt kunnen worden als een bepaalde partij daarover beschikt (*2.1.*). Daarna schets ik welke zwaktes het huidige nationale en Europese systeem voor opname en controle van vingerafdrukken ten behoeve van paspoorten vertoont, waardoor anderen over de vingerafdrukken kunnen beschikken (*2.2.*).

2.1. Misbruik van vingerafdrukken

Voorop gesteld zij: misbruik van vingerafdrukken kan zeer vergaande gevolgen hebben. Nagenoeg alle landen beschouwen vingerafdrukken als wettig bewijs (bijvoorbeeld om vast te stellen of iemand ergens is geweest). Als de vingerafdrukken misbruikt worden dan ondermijnt dat de waarde van vingerafdrukken als wettig bewijs en leidt het tot onjuiste veroordelingen van personen door rechterlijke instanties. Personen hebben daarom groot belang bij het beperken van de hoeveelheid partijen die kunnen beschikken over een kopie van hun vingerafdrukken. Dit aangezien er legio mogelijkheden tot misbruik van vingerafdrukken zijn.

Vingerafdrukken zijn namelijk zeer eenvoudig na te maken wanneer iemand over een kopie of een foto van een vingerafdruk beschikt. Het is mogelijk dat iemand, op basis van die kopie, op zijn vinger een laagje aanbrengt dat de vingerafdrukken van een ander simuleert. Het is ook mogelijk om met een dergelijke laagje paspoortcontroles met gemak door te komen. De uitleesapparaten die gebruikt worden bij paspoortcontroles zijn namelijk niet dermate geavanceerd dat zij een dergelijk laagje kunnen signaleren. De suggestie dat de verplichte afname van vingerafdrukken voor een paspoort identiteits- en paspoortfraude, in het bijzonder look-a-like fraude, voorkomt is derhalve onjuist.

Omdat vingerafdrukken makkelijk na te maken zijn, kan iemand – die over een kopie daarvan beschikt – ze ook op een plaats delict plaatsen. Dit met als doel om de persoon, van wie de vingerafdrukken zijn, als de dader te doen lijken.

Een andere vorm van misbruik bestaat uit het inbreken in apparaten en persoonlijke websites. Steeds meer technologie hanteert vingerafdrukken als een wachtwoord. Dat geldt bijvoorbeeld voor mobiele telefoons. Ook banken bieden de mogelijkheid om met vingerafdrukken te bankieren.[1] Websites voorzien steeds meer in een optie om met vingerafdrukken te betalen.[2] Als iemand eenmaal over een afbeelding van een vingerafdruk beschikt, dan is het risico op misbruik groot, maar ook levenslang. Een vingerafdruk kun je namelijk niet wijzigen om (verder) misbruik te voorkomen.

Kortom, wie een kopie van een vingerafdruk heeft, kan deze vingerafdruk (namaken en) gebruiken. Hierdoor is misbruik goed mogelijk. De mogelijkheden tot misbruik zullen in de toekomst nog groter worden nu steeds meer technologie vingerafdrukken als herkenningsmiddel gebruikt.

2.2. Zwaktes in het huidige systeem voor opslag en controle van vingerafdrukken ten behoeve van paspoorten

Onder het huidige systeem zullen veel ambtenaren in Nederland en andere Europese landen *geautoriseerde toegang* krijgen tot vingerafdrukken. Zij kunnen of met een uitleesapparaat de vingerafdrukken op de RFID-chip verkrijgen (optie 1). Of zij kunnen een paspoorthouder vragen om ter plekke vingerafdrukken af te geven zodat zij kunnen controleren of zijn vingerafdrukken overeenkomen met de vingerafdrukken op de RFID-chip (optie 2). Een complicaties is overigens dat een burger niet altijd kan weten of de ambtenaren van een bepaald land wel of niet bevoegd zijn om vingerafdrukken te vragen. In beide gevallen (optie 1 en 2) beschikken de betreffende ambtenaren over een beeld van de vingerafdrukken en is misbruik door die ambtenaren mogelijk. Nederland scoort weliswaar relatief goed op de corruptie-index, maar steeds vaker blijkt dat ambtenaren zich niet aan de regels houden. Een voorbeeld biedt een recente enquête onder strafpleiters waaruit blijkt dat de politieagenten in beslag genomen goederen stelen.[3] Andere landen scoren niet zo goed op de corruptie-index van 2015 die 168 landen betreft: Italië (nummer 61 wereldwijd), Kroatië (nummer 51 wereldwijd) Spanje (nummer 36 wereldwijd), waarbij geldt dat hoe hoger het getal hoe slechter het is gesteld met de corruptie.[4] De kans dat ambtenaren in Europa misbruik maken is niet te verwaarlozen. Verschillende landen buiten Europa gebruiken ook biometrie om paspoorten te controleren en scoren nog slechter op de corruptie-index: Irak (nummer 161 wereldwijd) en India (nummer 76 wereldwijd), Nigeria nummer

---

1 https://www.ing.nl/particulier/mobiel-en-internetbankieren/mobiel-bankieren/inloggen-met-uw-vingerafdruk/index.html

2 http://nieuws.nl/algemeen/20160307/vingerscan-of-selfie-om-te-betalen/

3 http://nos.nl/artikel/2107779-politie-drukt-waardevolle-spullen-criminelen-achterover.html

4 http://www.transparency.org/cpi2015

136 wereldwijd). Het is niet uitgesloten dat dergelijke landen op termijn de Nederlandse paspoorten ook kunnen lezen (zie hierna onder (ii)). In die landen is de kans op misbruik nog groter.

Naast misbruik door geautoriseerde toegang, baart ongeautoriseerde toegang ook grote zorgen. Het huidige systeem vertoont daarboven verschillende zwakke schakels. Illustratief is het feit dat in Frankrijk 10% van de uitgevaardigde biometrische paspoorten op basis van valse documenten is aangevraagd en dus volkomen onbetrouwbaar is. Dit laat zien dat het systeem en de mensen die dit systeem gebruiken, geen ondoorbreekbaar front vormen. Deze zwakke schakels kunnen ook hackers en andere partijen benutten om *ongeautoriseerde toegang* te krijgen tot de vingerafdrukken:

(i) De vingerafdrukken worden opgeslagen op de RFID-chip van het paspoort. Dit voldoet echter niet aan de hoogste veiligheidsmaatstaven. Op dit moment slaat de Nederlandse overheid het *volledige* beeld van de vingerafdrukken op in de RFID-chip, terwijl het veiliger is om alleen een *cryptografische template* van de vingerafdrukken in de RFID-chip op te nemen. Een dergelijke template bevat niet het volledige beeld van de vingerafdrukken maar slechts enkele unieke herkenningspunten. Het is dan mogelijk om bij controles na te gaan of de vingerafdrukken van de paspoorthouder overeenkomen met de template. Wat dat betreft is een template dus even effectief als een volledig beeld. Het voordeel van het gebruiken van een template is het volgende. Als iemand (ongeautoriseerde) toegang tot de chip krijgt, dan beschikt hij niet meteen over een volledige afbeelding van de vingerafdruk en kan hij de vingerafdruk niet namaken en misbruiken. Het hanteren van een cryptografische template is relatief makkelijk. Morpho de producent van de Nederlandse paspoorten, krijgt eveneens een volledig beeld van de vingerafdrukken met alle mogelijkheden tot misbruik van dien, terwijl een cryptografische template ook had volstaan.

    Dit illustreert al dat de opslag van de vingerafdrukken op de RFID-chip niet aan de hoogte veiligheidsmaatstaven voldoet.

(ii) De RFID-chip had ook, in aanvulling op de huidige publieke "versleutelingscodes"[5], beveiligd kunnen worden met een geheime persoonlijke code. Dit zou de paspoorthouder ook extra veiligheid geven wanneer hij reist naar landen die met veel corruptie kampen. Ten onrechte is daarvoor niet gekozen zodat ook daarom niet sprake is van het voldoen aan de hoogste veiligheidsmaatstaven. Verder is extra problematisch dat landen de publieke versleutelingscodes kunnen verkrijgen via een rechtmatige weg, namelijk via de Nederlandse overheid, maar ook op een onrechtmatige wijze, namelijk omdat deze codes lekken of gestolen worden door hackers. Deze laatste situatie is

[5] Het juiste woord is een geheime code of wachtwoord, maar aangezien de Afdeling van versleutelingscodes spreekt hanteer ik ter voorkoming van verwarring dat woord.

absoluut niet denkbeeldig. Een recent voorbeeld biedt de Diginotar-hack. De Nederlandse overheid maakte enkele jaren gebruik van het bedrijf Diginotar die certificaten voor grote delen van de Nederlandse overheid verzorgde. In 2011 werd dit bedrijf gehackt en maakten de hackers codes van Diginotar buit. Met deze codes konden de hackers gegevens van veel burgers verkrijgen. Het probleem werd niet direct door de overheid gedetecteerd.

Het is verder belangrijk om te realiseren dat systemen sterk kunnen zijn, maar de personen erachter zwak. Er hoeft maar één persoon uit de betrokken organisatie informatie (onbewust) door te spelen aan een verkeerde partij en de veiligheid van het gehele systeem is dan gecompromitteerd. Een nieuwe muur van bescherming is dan noodzakelijk. Als een RFID-chip ook beveiligd is met een persoonlijke code, dan zou het lekken van de publieke versleutelingscode niet altijd meteen ertoe leiden dat iemand de controle over zijn privégegevens verliest.

(iii) Bij de opname van vingerafdrukken en het controleren of de vingerafdrukken van paspoortdragers overeenkomen met de vingerafdrukken op de RFID-chip, gebruiken overheden het uitleesapparaat om vingerafdrukken ter plekke op te nemen. Dit apparaat kan gehackt worden, bijvoorbeeld door een virusprogramma erop te installeren dat de uitgelezen vingerafdrukken doorstuurt, met als gevolg dat de uitgelezen vingerafdrukken in handen komen van derden. Het certificeringsproces van de uitleesapparaten biedt geen garantie dat de uitleesapparatuur niet gehackt wordt. Dit in tegenstelling tot wat de Afdeling Bestuursrechtspraak van de Raad van State lijkt te impliceren in haar uitspraak van 25 mei 2016 (*rechtsoverweging 7.9. laatste alinea*). Zelfs als de leesapparatuur niet te hacken is, dan is misbruik van deze apparatuur alsnog mogelijk. Iemand kan dergelijke apparatuur namelijk stelen of op een andere onrechtmatige wijze in handen krijgen. Tijdens de zitting heb ik de Afdeling deze argumenten voorgelegd maar weigerde de Afdeling daarop in te gaan en heeft ze er verder geen aandacht aan geschonken zoals blijkt uit haar uitspraak.

(iv) De Nederlandse overheid vertrouwt de gegevens toe aan Morpho, het bedrijf dat de paspoorten vervaardigt, maar er is geen reden om te veronderstellen dat Morpho veiliger is dan Diginotar. Het is daarbij van belang om op te merken dat de Nederlandse overheid dacht toen deze Diginotar het beheer van certificaten toevertrouwde dat Diginotar veilig zou zijn. Overheden maken zich in toenemende mate ook zorgen over eventuele cyberaanvallen op biometrische data.

3. Zitting bij de Afdeling Bestuursrechtspraak van de Raad van State

Tijdens de zitting d.d. 3 december 2015 bij de Afdeling Bestuursrechtspraak van de Raad van State heb ik mijn analyse, zoals hiervoor vervat in dit rapport, gepresenteerd. Er vond hierover een uitgebreide discussie plaats, waarbij ook de deskundige van de andere partij deze knelpunten beaamde en onderkende. Helaas blijkt uit de uitspraak d.d. 25 mei 2016 in het geheel niet dat de Afdeling deze analyse mee laat wegen.

De Afdeling legt in de uitspraak een eenzijdige en verkeerde focus op de publieke codering van de RFID-chip. Uit bovenstaande analyse blijkt echter dat het systeem veel zwakke schakels kent. Die zwakke schakels kunnen benut worden voor misbruik van vingerafdrukken. De Afdeling gaat meer concreet niet in op het feit dat de vingerafdrukken beter als een cryptografische template opgeslagen kunnen worden, terwijl dit eenvoudig en goedkoop is maar het kopiëren van de opgeslagen vingerafdrukken bemoeilijkt (*zie paragraaf 2, onder (i)*). Dit laat in ieder geval zien dat bij de invoering van biometrie niet voldoende of goed is nagedacht over veiligheid. Ten tweede gaat de Afdeling in het geheel niet in op het feit dat Lidstaten de publieke codes, die toegang verschaffen tot de RFID-chip, mogen delen met niet-Europese overheden of dat deze codes kunnen lekken (*zie paragraaf 2, onder (ii) en (iv)*). Als niet-Europese overheden de codes krijgen, zal het risico op fouten en misbruik alleen groter worden. Het delen is namelijk voor een groot deel op vertrouwen gebaseerd. Dus Nederland moet vertrouwen dat andere Europese en niet-Europese landen haar codes verantwoordelijk gebruiken, bewaren en niet doorgeven aan andere landen of groepen. Zodra dit misgaat, en de kans daarop is zeker niet klein, is er geen barrière meer tegen misbruik van vingerafdrukken. Een persoonlijke pincode had een dergelijke barrière kunnen vormen, maar helaas is daarvoor niet gekozen. Het feit dat leesapparatuur gehackt of gestolen kan worden bespreekt de Afdeling evenmin (*zie paragraaf 2, onder (iii)*).

4. Andere mogelijkheden om paspoortcontroles te verrichten

De keuze voor vingerafdrukken als middel om paspoortcontroles uit te voeren is niet bepaald voor de hand liggend. Zij zijn, zoals eerder toegelicht, eenvoudig na te maken, waardoor het probleem van paspoortfraude niet opgelost wordt. Als een ander over de vingerafdrukken van een bepaalde persoon of een groep personen beschikt, dan heeft die persoon of groep personen daar voor altijd last van: zij kunnen immers hun vingerafdrukken niet wijzigen, en die ander kan deze vingerafdrukken onbegrensd en eenvoudig namaken.

In de financiële wereld is voor een beter systeem gekozen. Dit systeem gaat uit van een geheim persoonlijk wachtwoord dat de houder van een pas in moet voeren. Dit systeem bevat een betere barrière dan controle middels vingerafdrukken en is daardoor veiliger. Voordeel van dit systeem is bovendien dat een eenmaal gelekt wachtwoord gewijzigd kan worden.

Het systeem van de financiële wereld kunnen staten toepassen bij paspoortcontroles. Een paspoorthouder kan zijn paspoort in een apparaat zetten bij paspoortcontroles en een wachtwoord intoetsen en pas daarna komen de biometrische gegevens beschikbaar.

5. Conclusie

Kort en goed kunnen de bevindingen van dit rapport als volgt samengevat worden:

(i) Het is eenvoudig om vingerafdrukken na te maken. Dit biedt legio mogelijkheden tot misbruik: (a) het plegen van paspoortfraude, (b) de vingerafdrukken van een ander op een plaats delict plaatsen om deze als de misdadiger te doen lijken en (c) het verkrijgen van toegang tot digitale apparaten (bijvoorbeeld mobiele telefoons) en websites (bijvoorbeeld het internetbankieren) of het doen van betalingen via internet;

(ii) Door de afname en opslag van vingerafdrukken ten behoeve van paspoortcontroles krijgen ambtenaren een mogelijkheid om die vingerafdrukken te misbruiken. Dit gevaar is groot binnen Europa waar corruptie zich ook te vaak voordoet. Dit gevaar is nog groter in landen buiten Europa waar de corruptie groot is en waarvan niet is uitgesloten dat zij op termijn ook toegang kunnen krijgen tot de RFID-chip;

(iii) Het huidige systeem vertoont veel zwakke schakels die benut kunnen worden om een kopie van de vingerafdrukken te krijgen:

- op dit moment slaat de Nederlandse overheid een volledige afbeelding van de vingerafdruk, terwijl een cryptografische template veiliger is. De template geeft namelijk enkele unieke herkenningspunten en niet de hele vingerafdrukken weer, waardoor misbruik minder snel mogelijk is;

- de beveiliging van de RFID-chip bestaat enkel uit een publieke code. Dit is gevaarlijk aangezien ervaringen uit het verleden bewijzen dat dergelijke codes kunnen lekken. Als dit gebeurt is er geen andere barrière om paspoorten te beschermen tegen ongeautoriseerde toegang. Een persoonlijke code in aanvulling op de publieke code zou meer veiligheid bieden;

- de uitleesapparatuur kan eenvoudig gehackt of gestolen worden;

- Morpho kan, net als Diginotar, te maken krijgen met een hack of een medewerker die informatie lekt.

(iv) Vingerafdrukken zijn geenszins een voor de hand liggende keuze om paspoortcontroles te verbeteren. Zodra ze uitlekken verliezen zij hun waarde, aangezien zij makkelijk na te maken zijn. De (Europese) wetgever had beter kunnen aansluiten bij het systeem dat de financiële wereld gebruikt bestaande uit een pincode.

(v) De Afdeling Bestuursrechtspraak van de Raad van State negeerde de aspecten genoemd in (i) tot en met (iv). Dit ondanks het feit dat ik

tijdens de zitting d.d. 3 december 2015 deze aspecten naar voren bracht.

Amsterdam, 20 september 2016, dr. M. Rieback

Bijlagen

Bijlage 1: biografie

DR. MELANIE RIEBACK

Dr. Melanie Rieback is the CEO/Co-founder of Radically Open Security, the world's first non-profit computer security consultancy company. She is also a former Assistant Professor of Computer Science at VU who performed RFID security research (RFID Virus and RFID Guardian), that attracted worldwide press coverage, and won several awards (VU Mediakomeet, ISOC Award, NWO I/O award, IEEE Percom Best Paper, USENIX Lisa Best Paper). Melanie worked as a Senior Engineering Manager on XenClient at Citrix, where she led their Vancouver office. She was also the head researcher in the CSIRT at ING Bank, where she set up their Analysis Lab and spearheaded the ING Core Threat Intelligence Project. For fun, she co-founded the Dutch Girl Geek Dinner in 2008. Melanie was named 2010 ICT Professional of the Year (Finalist) by WomeninIT, one of the 400 most successful women in the Netherlands by Viva Magazine (Viva400) in 2010, and one of the fifty most inspiring women in tech (Inspiring Fifty Netherlands) in 2016.

Zie: https://radicallyopensecurity.com/team/MelanieRieback/

Bijlage 2: literatuurlijst (selectie)

- 29-10-2010 Wetenschappelijke Raad voor het regeringsbeleid, Happy Landings, Het Biometrische paspoort als zwarte doos, p. 147 e.v.: http://www.wrr.nl/fileadmin/nl/publicaties/PDF-webpublicaties/Happy_Landings_.pdf

- 4-11-2010 NL WRR publication 'Het biometrische paspoort in Nederland- crash of zachte landing' Max Snijder, p.142 e.v.: http://www.wrr.nl/fileadmin/nl/publicaties/PDF-webpublicaties/Het_biometrisch_paspoort_in_Nederland.pdf

- 8-3-2012 Electronic Frontier Foundation "A Time Bomb For Civil

Liberties": France Adopts a New Biometric ID Card https://www.eff.org/deeplinks/2012/03/french-national-assembly-proposes-new-alarming-biometrics-bill

- 19-4-2012 European Parliament debate biometric pasport MEP speeches & EU Comm Malmström in plenary, p.189 – 199: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+CRE+20120419+SIT+DOC+PDF+V0//EN&language=EN

- 2-10-2013 Wat gebeurt er met mijn vingerafdrukken: https://www.nrc.nl/nieuws/2013/11/02/wat-gebeurt-er-met-mijn-vingerafdruk-1310131-a1059121

- Cybersecuritybeeld Nederland 2016: Beroepscriminelen steeds groter gevaar voor digitale veiligheid in Nederland: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html

- Cyberattack on biometric data poses security risks at border, documents warn: https://www.thestar.com/news/canada/2016/09/15/cyberattack-on-biometric-data-poses-security-risks-at-border-documents-warn.html