



Questafette



'Geautomatiseerde surveillance op globale schaal is geen winst'

Naam:
Maurice Wessling

Werkzaam bij:
Bits of Freedom

Ervaring met informatiebeveiliging sinds:

Mijn ervaring met IB is zijdelings, nooit primair. Vanaf 1997 toen ik het openlucht hacker festival Hacking in Progress (HIP) organiseerde.

Vindt ten aanzien van de stelling 'De in opkomst zijnde sterke authenticatiemiddelen (zoals het paspoort met biometrie) zijn goed voor de burger, omdat hiermee het risico van identiteitsfraude afneemt':

"Hoeveel zijn iemands biometrische kenmerken waard? Het ministerie van Binnenlandse Zaken heeft op deze

moeilijke vraag een antwoord gevonden. Voor een proef met biometrische paspoorten, die in zes steden loopt, geldt een speciale actiekorting. 'Doe mee aan de praktijkproef biometrie en ontvang tien euro korting!', aldus een folder van het agentschap BPR van het ministerie.

Tijdens de proef worden de paspoorten voorzien van een chip met biome-

trische kenmerken. De contactloze chip zal zowel een digitale foto van het gezicht bevatten als twee vingerafdrukken (beide wijsvingers). In de steden Almere, Apeldoorn, Eindhoven, Groningen, Rotterdam en Utrecht hoopt het ministerie met de korting 15.000 burgers te verleiden tot deelname.

Nederland is niet het enige land dat een paspoort met biometrische kenmerken invoert. Onlangs besloten de landen van de EU om biometrie in het paspoort verplicht te stellen. Wetgeving in de VS is de drijvende kracht achter een snelle implementatie.

De US Enhanced Border Security and Visa Reform Act verplicht landen waarvan de burgers geen visum voor de VS nodig hebben (het zogenaamde Visa Waiver Program dat voor vrijwel alle EU landen geldt) per oktober 2005 paspoorten met biometrie uit te geven. De VS bepalen daarmee het tempo van de invoering. Toch is het niet zo dat Nederland slechts onder Amerikaanse druk een biometrisch paspoort krijgt. Plannen voor een dergelijk paspoort bestaan in Nederland al sinds 1998. Het lijkt er meer op dat de Amerikaanse eisen de invoering versnellen en vergemakkelijken. Beleidsmakers kunnen immers voor de noodzaak tot invoering verwijzen naar een externe factor waarop zij geen of weinig invloed hebben.

Voormalig Minister van Bostel heeft de Tweede Kamer beloofd dat Nederland de biometrische kenmerken niet centraal zal opslaan. Dat is een goede beslissing. Op die manier kan met behulp van de biometrische kenmerken alleen bepaald worden dat een paspoort en de houder bij elkaar horen. Als de technologie zo goed is als de overheid hoopt dan lijkt identiteitsfraude bij grensovergangen zoals op Schiphol een stuk moeilijker. De meest voorkomende fraude betreft immers de zogenaamde look-a-likes;

personen die een paspoort van iemand anders kunnen gebruiken omdat ze een gelijkenis met de foto in dat paspoort vertonen. Een paspoort met biometrische kenmerken kan dat voorkomen.

Maar daarmee is natuurlijk niet identiteitsfraude in het algemeen te voorkomen. Het veel voorkomende phishing op internet laat zien hoe makkelijk het is om gegevens zoals creditcardnummers aan naïeve gebruikers te ontfutselen. Het valt dus te betwijfelen of de individuele burger veel voordelen merkt van het biometrisch paspoort. De belofte is natuurlijk dat de biometrische gegevens een deels geautomatiseerde grenscontrole mogelijk maken. Reizigers zouden daarmee tijd kunnen besparen op vliegvelden. Maar veel andere veiligheidsmaatregelen en controles zullen die besparing weer tenietdoen.

Het biometrisch paspoort levert de houder ervan echter wel een heel nieuw scala aan vragen en problemen op. Hoe zijn de lees- en schrijfrechten met betrekking tot de chip geregeld? Kan iedereen zomaar de gegevens uitlezen? Krijgen we te maken met een heel nieuwe variant van skimming (onopgemerkt en niet-geautoriseerd lezen)? Over de standaardisatie van de chip wordt overlegd binnen het ICAO (icao.int/mrtd). De chip zal worden beveiligd met behulp van PKI. Maar het is evident dat andere landen leesrechten zullen krijgen voor de Nederlandse paspoorten. Vervolgens kunnen die landen de biometrische gegevens opslaan en combineren met andere data. Hoewel Nederland heeft besloten de gegevens niet centraal op te slaan, staat het andere landen vrij dit wel te doen.

Over een aantal jaar zullen de VS en een heleboel andere landen een database hebben met de vingerafdrukken en digitale foto's van alle Nederlanders die de betreffende landen hebben

bezocht. Deze databanken kunnen bovendien nog worden gevoed met passagiersgegevens. Ook hebben de landen de mogelijkheid om de biometrische gegevens te delen met derden. In de 'privacy-verklaring' van het US-VISIT programma (waarin nu al vingerafdrukken van Nederlanders worden genomen) staat een uitputtende opsomming: 'federal, state, local, tribal, and foreign government law enforcement agencies'. Dat is dus wat de Nederlandse paspoorthouder kan verwachten; zijn of haar biometrische gegevens worden gedeeld met 'tribal agencies'.

Hoewel geautomatiseerde gezichtsherkenning volgens veel deskundigen een nog niet volwassen technologie is, lijkt mij dit slechts een kwestie van tijd. De digitale foto in het paspoort heeft in elk geval tot doel deze later voor geautomatiseerde gezichtsherkenning te gebruiken. Wanneer landen de foto's van Nederlandse reizigers bij aankomst opslaan, ontstaan geheel nieuwe mogelijkheden. Theoretisch is het dan mogelijk om personen te identificeren aan de hand van andere beelden, bijvoorbeeld die van videocamera's. Niet alleen op het vliegveld, maar ook daarbuiten.

Het biometrisch paspoort roept een groot aantal nieuwe privacykwesties op. Op het gebied van identiteitsfraude valt misschien winst te behalen, maar het biometrisch paspoort heeft alles in zich om te ontwikkelen tot een platform voor geautomatiseerde surveillance op globale schaal. Dat is geen winst."

Geeft estafettestokje door aan:
Rop Gonggrijp van CryptoPhone.

Met de stelling:
In de informatiebeveiliging wordt de nadruk gelegd op het beveiligen van data. Dat is curieus aangezien juist de interceptie en compromitering van spraak het meest voorkomt.