Het biometrische experiment en de risico's van naïef vertrouwen in technologie

Geert-Jan van Bussel

Biometrie
Biometrie is de geautomatiseerde identificatie of autorisatie van individuele lichaamskenmerken van een levend persoon (of beter: van levende wezens, want het is niet beperkt tot mensen, maar daar gaan we hier verder niet op in). Het is een identificatietechniek gebaseerd op niet veranderlijke biologische kenmerken, de psychologische – en/of gedragskarakteristieken van een persoon. Dit kenmerk wordt vervolgens electronisch opgeslagen en kan worden vergeleken met een op een ander tijdstip verkregen versie. Biometrie kent al vele toepassingen, maar aangezien het een vakgebied is dat sterk in ontwikkeling is, verschijnen nog regelmatig nieuwe toepassingen. Biometrie kan pasjes, wachtwoorden, foto's, handtekeningen e.d. gaan vervangen, of in ieder geval gecombineerd daarmee de beveiliging sterker maken. Om fraude uit te sluiten worden bij voorkeur meerdere kenmerken tegelijkertijd gebruikt, al of niet in combinatie met een PIN-code.

Biometrische karakteristieken kunnen fysiologisch of gedrag-georiënteerd zijn. Fysiologische kenmerken zijn gerelateerd aan het lichaam. De oudste vorm van biometrische techniek, al vanaf 1858 in gebruik, is de vingerafdruk. Andere voorbeelden van fysiologische karakteristieken zijn gelaatsherkenning, handgeometrie en irisherkenning. Gedragskenmerken zijn gerelateerd aan het gedrag van een persoon. De eerste karakteristiek (ook al eeuwen oud) is de handtekening. Modernere vormen van gedragsbiometrie zijn 'keystroke dynamics' (de exacte bepaling van de wijze waarop en wanneer iemand de toetsen op een toetsenborg indrukt) en stemherkenning. Een stem is in principe een fysiologische karakteristiek (vanwege het afwijkende timbre), maar stemherkenning is met name gericht op de manier waarop iemand spreekt. En dat kan als een gedragskarakteristiek worden gezien.

Andere biometrische technieken richten zich op de manier waarop mensen lopen, de retina, handpatronen, gehoorkanalen, gezichtswarmte, lichaamsgeur en DNA. Ook deze technieken zijn ofwel fysiologisch ofwel gedrag-georiënteerd

Identificatie en verificatie
Biometrie wordt voor twee verschillende functies gebruikt: verificatie en identificatie. Bij verificatie authentiseert het gebruikers door de biometrische karakteristiek te vergelijken met het opgeslagen biometrische patroon op een smartcard of in een database en combineert dat met een gebruikersnaam of identiteitsnummer, eventueel opgeslagen op een smartcard. Bij identificatie wordt de biometrische karakteristiek vergeleken met alle records in een database en wordt een 'match' gezocht, die binnen een bepaalde marge mag liggen om geaccepteerd te worden.

Biometrie rukt snel op in de (tele)communicatie middels internet en andere vormen van electronische communicatie. Daardoor neemt de anonimiteit van gebruikers hand over

hand toe. Het 'kennen' van de identiteit van gebruikers is van groot belang voor de meeste vormen van electronische communicatie. Daarnaast is authenticatie van groot belang voor allerlei vormen van douane-, politie- en justitiedoeleinden. De authenticatie, het vaststellen van de identiteit van de gebruiker, kan met biometrie worden gewaarborgd, zeker als dat wordt gecombineerd met wachtwoorden en smartcards.

Belang van authenticatie

In een steeds groeiende elektronische communicatiemaatschappij is het van belang de identiteit van allerlei soorten gebruikers vast te stellen voor bijvoorbeeld:

- Internet-transacties bij electronic banking en e-commerce;
- Immigratie (legaal versus illegaal);
- Criminaliteitsbestrijding;
- Diefstal van en fraude met identiteit;
- Toegangscontrole van gebouwen;
- Bescherming van (geheime) gegevens door toegangsbeveiliging van de PC op de werkplek met toegang tot computernetwerken (intra- en extranetten, inclusief toegang tot computers op afstand);
- Registratie van de tijd dat iemand in een gebouw aanwezig is (of moet zijn); enz.

Biometrische technieken kunnen ervoor zorgen dat de identiteit van personen op meer verantwoorde wijze wordt vastgesteld. Een biometrisch kenmerk levert in principe een hogere betrouwbaarheid op dan enkel een wachtwoord of een inlogcode. Maar hoe staat het met de betrouwbaarheid ervan ?

Betrouwbaarheid

Geen enkel systeem is foutloos, ook biometrische systemen niet. Dat is dan ook een reden tot zorg, gezien het feit dat biometrische gegevens persoonsgegevens *in extremis* zijn. Er is dus een goede reden tot grote voorzichtigheid met biometrische experimenten. Corien Prins, hoogleraar Recht en Informatisering aan de Universiteit van Tilburg, heeft niet veel vertrouwen in die 'voorzichtigheid'. In de Automatisering Gids van 18 april liet ze weten dat toepassers van biometrie beslissen en handelen 'vanuit naïef en blind vertrouwen in de technologie'. Ze accepteren biometrische systemen als een 'black box' (waar ze veel te weinig van afweten) en brengen het als een neutraal beleidsinstrument, dat zonder al te veel problemen toe te passen is. Uiteindelijk blijkt dat vele toepassingen interorganisatorische implicaties hebben en dat nooit is bepaald wie de eindverantwoordelijke is.

Betrouwbaarheid van biometrie staat niet alleen. Er zijn een aantal parameters te noemen die met elkaar in evenwicht moeten zijn om de geschiktheid van een bepaalde techniek te kunnen bepalen. Anin Jain is daar in artikelen in 2004 en 2006 nader op in gegaan en heeft een matrix ontwikkeld waarmee de verschillende technieken met elkaar zijn te vergelijken.

Laten we eerste de verschillende parameters eens onderscheiden:

1. Universeel: iedereen moet de betreffende karakteristiek vertonen;
2. Uniek: de karakteristiek moet individueel uniek zijn om te kunnen onderscheiden;
3. Permanent: een karakteristiek moet identiek, onderscheidend en toewijsbaar blijven

met het ouder worden van een persoon;
4. Verwerving: een karakteristiek moet betrekkelijk eenvoudig te meten zijn;
5. Performance: de accuraatheid, snelheid en robuustheid van de gebruikte techniek;
6. Acceptatie: de mate waarin de technologie door het publiek wordt geaccepteerd;
7. Ontwijkbaarheid: het gemak waarmee eventueel een 'substituut' kan worden gebruikt.

Jain heeft de biometrische technieken afgezet tegen deze parameters en dat leidt tot een aantal verrassende conclusies. Geen van de bij Jain genoemde biometrische technieken (gezichtsherkenning, vingerafdruk, handgeometrie, 'keystrokes', iris- en retinascan, handtekening, stemherkenning, gezichtswarmte, lichaamsgeur, DNA, manier van lopen en gehoorkanaal) kan aan de eerste vier parameters voldoen. DNA voldoet aan vier van de eerste vijf parameters en heeft alleen problemen daar waar het de eenvoudigheid van de meting betreft. Ook qua ontwijkbaarheid en performance presteert DNA goed. Het grote probleem echter is dat het publiek een dergelijke biometrische techniek nog niet accepteert. De qua parameters best presterende biometrische technieken (DNA, Iris- en retinascan) kunnen op de minste acceptatie rekenen van het publiek.

Dat wantrouwen betekent dus dat er een grote mate van voorzichtigheid in acht genomen moet worden bij het implementeren van biometrische technologie. Dat wordt alleen nog maar bevestigd als we de staat van de techniek afzetten tegen de prestaties over de tijd heen. Een onderzoek uit 2002 laat zien dat bij gezichtsherkenning (een techniek die volgens Jain niet aan de parameter uniekheid kan voldoen) na anderhalf jaar 2 % ten onrechte wordt doorgelaten en 43 % ten onrechte geweigerd. Volgens het Nederlands Forensisch Instituut in Den Haag hebben die cijfers hun geldigheid nog niet verloren. Dat wordt bevestigd door andere onderzoeksresultaten. Een onderzoek inzake gezichtsherkenning eveneens uit 2002 stelt dat uit meer dan 37.000 scans 1 % onterecht wordt toegelaten, en 10 % onterecht wordt geweigerd. Voor vingerafdrukken blijkt in 2003 dat van 25.000 metingen nog steeds 1% onterecht wordt toegelaten en 0,1 % wordt geweigerd. Bij irisscans blijkt in 2005 een onterechte acceptatie in 0,94 % van de gevallen en een onterechte afwijzing in 0,99 % van de gevallen. Stemherkenning leidt in 2004 tot een onterechte toelating van 2 % en een onterechte afwijzing in 10 % van de gevallen. Voor DNA hebben we geen gegevens beschikbaar. Het is niet iets om onvoorwaardelijk optimistisch over te worden. Ook hier: de uit praktijkonderzoek best presterende techniek wordt het minst door het publiek geaccepteerd. Uiteraard spelen omgevingsfactoren een zeer belangrijke rol op acceptatie of weigering door een biometrische techniek: warmte, vochtigheid , vuile handen, veranderingen in leeftijd, het dragen van een bril of contactlenzen e.d.

Twee soorten biometrische systemen
Biometrische systemen bestaan grofweg uit twee onderdelen:
• Een apparaat om een kenmerk te meten van het menselijk lichaam en om dat gegeven om te zetten in een serie nummers;
• Een grote database, die de miljoenen biometrische metingen van mensen vastlegt.
Door middel van het verzamelen van specifieke biometrische gegevens wordt een uniek

ijkpunt (template) gemaakt. Zo wordt van iemand een biometrisch profiel gemaakt en vastgelegd in een gegevensbank, in een biometrisch controlesysteem, op een smartcard of in een barcode. Biometrie is gebaseerd op rekenregels (algoritmen) om twee templates met elkaar te vergelijken. De gebruiker wordt vergeleken met een enkele template, waarvan hij of zij beweert dat het die van hem of haar is. Gedurende de controle wordt de actuele informatie vergeleken met de opgeslagen template. Als de gebruiker is voor wie die zich uitgeeft zullen de twee beelden overeen komen of binnen een bepaalde marge van afwijking blijven en is iemands identiteit vastgesteld.

Authentisering

De discussie over de toepassing van biometrische technieken is tot nu toe bijna volledig gericht op identificatie van personen. Een voor informatiebeheerders en –verwerkers belangrijk aspect is de authentisering van informatie, gegevens en documenten door daartoe bevoegde functionarissen in een organisatie. Tot voor kort werden authentieke documenten voorzien van de handtekening van de betreffende partijen, zodat daarmee de documenten een status van betrouwbaarheid hadden. De digitale handtekening begint langzaam een opmars te maken, maar die gaat veel langzamer dan in eerste instantie verwacht was.

Daarbij komt dat de bestaande digitale handtekening eerder het transport van de data verzekerd en aangeeft dat tijdens dat transport geen veranderingen in de gegevens zijn aangebracht en dat het bestand integer is overgekomen. Maar zegt dat eigenlijk wel dat het bestand is zoals het zou moeten zijn ? Is er vóór dat de digitale handtekening werd geplaatst ook sprake van integriteit ? Hoe wordt verzekerd dat interne documenten, die volgens interne regels moeten worden geauthentiseerd, integer zijn ?

Vele aanvraag- en bevestigingsformulieren, brieven, uitspraken en andere binnen juridische procedures bewijsleverende bestanden zijn nu digitaal, hoewel vaak een papieren versie beschikbaar is, vaak met een handtekening daarop. Als de digitale handtekening en/of biometrische identificatie daadwerkelijk worden ingevoerd kan die backup wegvallen.

Daartoe dient bekend te zijn dat digitale documenten zijn goedgekeurd en/of geauthentiseerd door de daartoe bevoegde persoon. Een van de beste opties daartoe is om in in de toegankelijke metadata van het te authentiseren document een melding op te nemen dat de identificatie van de functionaris op basis van zijn biometrische gegevens heeft plaatsgevonden, accoord is bevonden, onmiskenbaar behoort aan degene die ondertekent en dat daardoor het document is geauthentiseerd, met een exacte tijdsindicatie van het plaatsen van de biometrische gegevens. Dit betekent dat bij het authentiseren van documenten specifieke biometrische systemen beschikbaar moeten zijn. Vingerafdruklezers kunnen in deze al voldoende zijn. Over het algemeen staan de meeste mensen neutraal tegenover een vingerafdruk als biometrisch gegeven. Voor authentisering is het dan ook een acceptabel middel. Deze optie betekent het vastleggen van extra metadata (enkel bestemd voor de authentisering van het betreffende bestand of document), vast gekoppeld aan het document

en onmuteerbaar ter beschikking gedurende de totale bewaartermijn.

Er moeten zeer hoge eisen gesteld worden aan het beheer van de geauthentiseerde documenten en bestanden. De bewijs- en rechtspositie van een organisatie of een individueel persoon is er van afhankelijk. Het voordeel van een dergelijke aanpak is dat de enorme papieren backup tot het einde kan gaan behoren. Dat scheelt niet alleen in de kosten, het levert ook milieuvoordelen op.

Bezwaren
Tegen biometrische identificatie en authentisering zijn nogal wat bezwaren aan te voeren, die vooral te maken hebben met de beveiliging van de biometrische bestanden. Geen enkele wijze van vastlegging van deze gegevens blijkt echt veilig te zijn en brengt dus risico's met zich mee.

Centrale databases zijn nooit volledig te beveiligen en de kans dat kwaadwillenden toegang tot deze gegevens krijgen (hoe klein die kans ook is !) mag niet worden veronachtzaamd. Het College Bescherming Persoonsgegevens wijst uit privacy-overwegingen centrale opslag af. In de optiek van het College hoeft geen kopie van een biometrisch bestand in een centrale database te worden opgeslagen. Ze gaat uit van decentrale toepassing: de persoon legt bijvoorbeeld zijn vingertop op een leesapparaat, dat het binaire patroon vaststelt en dit vergelijkt met de template op de chipkaart. Met die werkwijze hoeft geen enkele instantie kopieën van biometrische bestanden te bewaren. De wijze waarop de IT-organisatie van de overheid georganiseerd is (zie de voortdurende rapporten van onder andere de Algemene Rekenkamer) is het onverstandig het bewaren van die gegevens daaraan toe te vertrouwen.

De keuze echter voor decentrale of gepersonificeerde opslag op smartcards blijkt recent ook beveiligingsproblemen op te leveren. Het uitgangspunt hierbij is dat personen hun biometrische gegevens zelf, op een chipkaart, bij zich dragen. Het gemak waarmee uiteindelijk de OV-chip-kaart werd gekraakt en het bericht dat ook de chip van het nieuwe Nederlandse paspoort (dat biometrische gegevens bevat) kraakbaar is, doet twijfelen aan ook deze wijze van opslag.

Volgens Prins gaan beleidsmakers wel heel erg makkelijk en naïef ervan uit dat dit risico zo klein is dat er geen rekening mee gehouden hoeft te worden. Belangrijke problemen zijn dat biometrische algoritmes niet gevalideerd zijn en dat niet of nauwelijks bekend is hoe ze werken. Dat is riskant, zeker omdat de overheid biometrie wil gebruiken om burgers te profileren, te categoriseren en uiteindelijk (en veelal onbewust) te discrimineren. Doorgevoerde biometrie verandert de verhouding tussen overheid en burger op een wijze die mogelijkerwijze onacceptabel is. En, zo zegt Prins, 'De burger komt in een andere bewijspositie. Er wordt gezegd dat biometrische kenmerken uniek zijn. Honderd procent identificatie. Hoe moet ik straks aantonen dat de overheid mij in de verkeerde categorie heeft ondergebracht ?' Maar zoals we hiervoor hebben gezien: sommige biometrische karakteristieken zijn uniek, andere niet, maar er is er tot nu toe niet een die honderd procent

identificeert.

Willen wij er naar toe dat de overheid voor ons bepaalt wie we zijn op basis van techniek die niet volledig betrouwbaar is ?