Op blauwe ogen vertrouwen

Ir. drs. J. van der Vlugt RE

Identificatie en authenticatie blijven kardinale maar problematische kwesties. Nu partijen elektronisch steeds dichter bij elkaar komen maar voor elkaar steeds meer onzichtbaar blijven, en daardoor de controle moeilijker wordt, komen na tijdenlang in de onderzoekssfeer te hebben verkeerd biometriehulpmiddelen naar voren. Deze kunnen helpen om naast kennis en bezit ook het zijn als bron van authenticatie aan te wenden. Mits een aantal vraagtekens wordt weggewerkt en de selectie en implementatie netjes worden afgehandeld.

Inleiding

De laatste jaren begint het helaas steeds gemakkelijker te worden om in te breken op communicatieverbindingen, mede omdat die verbindingen steeds minder afhankelijk zijn van hun fysieke karakteristieken. Waar het voorheen bijvoorbeeld nodig was om een telefoonkabel op te graven om die te kunnen afluisteren (of aan een eindpunt of telefooncentrale in te breken om er een tap te plaatsen), kan tegenwoordig vanaf de eigen zolderkamer een Internetverbinding aan de andere kant van de wereld worden gevolgd en zelfs in die verbinding worden ingegrepen. Dit betekent dat de integriteit en vertrouwelijkheid van de (elektronische) communicatie in het geding is. Maatregelen tegen de bedreigingen zijn zeer wel denkbaar (zie het artikel over cryptografie elders in deze Compact), hoewel door implementatieslordigheden nog niet vanzelfsprekend waterdicht.

Een bijkomend probleem ontstaat doordat de elektronische communicatie steeds verder doordringt in de dagelijkse manier van werken. Wie aan e-commerce doet, zal – al was dat misschien niet in eerste instantie de bedoeling – al snel merken over de gehele wereld zaken te doen. En dat betekent een navenant stijgende behoefte aan informatie over de betrouwbaarheid van zakenpartners en consumenten. Daaraan valt gedeeltelijk tegemoet te komen door het gebruik van – noodzakelijkerwijs uitgebreide – netwerken van Trusted Third Parties en Certificate Authorities.
Ook voor die partijen blijft echter het probleem: hoe vast te stellen dat degene die zich meldt met een verzoek om authenticatie, ook daadwerkelijk die persoon is en geen ander?

De authenticatie aan de bron die bij elektronische zaken nodig is, treffen we ook dichter bij huis aan. Denk maar aan creditcards en pinpassen. Waar bij creditcardbetalingen een handtekeningcontrole vaak ostentatief wordt overgeslagen, dwingen geldautomaten en betaalautomaten nog tot het invoeren van pincodes. Maar of dit soort waarborgen voldoende is? De nogal vaak (in de mond-tot-mondpubliciteit) voorkomende gevallen beziend waarbij met valse adreswijzigingen en valse aanvragen voor nieuwe passen (met pincodes) wordt gesjoemeld, moet worden geconcludeerd dat authenticatie op basis van kennis (wachtwoord, pincode) en bezit nog niet waterdicht is[1].

1) Nota bene: bij computersystemen was het normaal om eerst alleen met user-ids en wachtwoorden te werken, tokenkaarten en dergelijke kwamen voor authenticatie op basis van bezit pas later in beeld. Terwijl met creditcards de *belofte* van betaling juist al decennia zo'n beetje alleen maar op basis van bezit werd geauthenticeerd.

De band met de fysieke persoon is dus nog niet onlosmakelijk. Waar zijn de tijden dat men een wederpartij op diens blauwe ogen kon vertrouwen? Die tijden zijn terug.

Biometrie, de kunde die zich bezighoudt met het vaststellen van identiteit op basis van unieke waarden voor biologische eigenschappen, bestaat al een tijdje. Het begon al met handtekeningen en/of zegelstempels, waarvan het uitgangspunt was dat die slechts door de 'eigenaar' zelf konden worden (zijn) gezet; het handschrift of de zegelring werden geacht niet te kunnen worden nagemaakt. In de jaren zestig (al bijna: '... van de vorige eeuw ...') begon de ontwikkeling van apparaten waarmee ook de veel uniekere drukpatronen van handtekeningen konden worden herkend, en doken in sciencefictionfilms vingerafdruk- en handpalmherkenners op. Zoals altijd bleken die films maar net een stapje verwijderd van wat state-of-the-art was. En toen werd het een tijdje stil.

Nu plotseling echter is er een aanzwellende stroom van commerciële biometrieproducten, niet alleen van marginale researchbedrijfjes maar ook van alle grote spelers op de IT-markten. Derhalve is het tijd voor een overzicht van wat er kan en niet kan.

Dit artikel behandelt eerst de fasen van inzet, betrouwbaarheid en technieken die heden ten dage voorhanden zijn. Daarna komen de doelen van biometrische hulpmiddelen aan bod. De middelen en doelen zorgen voor enkele generieke vraagtekens en kritieke succesfactoren, die apart worden besproken.

Huidige middelen

Deze paragraaf geeft een korte inleiding in de gangbare fasen van inzet voor gebruik van biometrische hulpmiddelen, behandelt de basisbegrippen inzake betrouwbaarheid en beschrijft een aantal van de recent op de markt verschenen producten. Het overzicht is overigens niet uitputtend, noch is enig waardeoordeel bedoeld – met zo'n vijfhonderd producten en snel opeenvolgende productintroducties is dat niet zinvol.

Fasen van inzet

De inzet van biometrie kent, na de systeemontwikkeling en -implementatie in engere zin, twee fasen:

Enrollment
In deze fase worden de gebruikers in het systeem opgevoerd om later te kunnen worden herkend. Dit gebeurt door een soort nulmeting te doen die leidt tot een eerste, vast te leggen meetwaarde (*template*).
Dit is een kritieke fase. Op een of andere wijze moet worden zeker gesteld dat gebruikers zich niet meermalen aanmelden, bijvoorbeeld door de ene keer de linkerwijsvinger te gebruiken en de andere keer de andere. Dit lijkt eenvoudig, door bijvoorbeeld een paspoort te vragen voor vergelijking van unieke (?) naam en pasfoto, maar een paspoort is, zoals vele politici bekend is, vrij eenvoudig te vervalsen. Hierdoor ontstaat het risico met een vervuilde verzameling combinaties van eventuele kennis, bezit en zijnswaarden te beginnen.
(Na enrollment kan 'binning' plaatsvinden, het sorteren van de database op biometrische waarden. Dit versnelt het latere opzoeken.)

Gebruik
Hierin zijn drie stappen te onderkennen:
* *Collection:* het proces van het meten van de biometrische eigenschap, en het omzetten ervan in een binaire representatie. Op dit grensvlak van analoge en digitale techniek, op de grens van hardware en software, biedt zowat iedere leverancier zijn eigen standaard aan.
* *Comparison:* de vergelijking van de binaire representatie met een opgeslagen waarde. Indien het gaat om een eigen opslagmedium (zie onder), kan dit razendsnel. Indien echter wordt gematcht tegen een (grote) database, kan nogal wat – hinderlijke – vertraging ontstaan. Het simpelweg eerst vragen van een user-id kan natuurlijk het zoeken aanzienlijk versnellen.
* *Pass/fail:* de beslissing of de gemeten representatie voldoende nauwkeurig overeenkomt met de meest passende c.q. op basis van de aangedragen user-id gevonden waarde.

In het bovenstaande wordt een onderscheid genoemd tussen toepassingen die zijn gebaseerd op een (centrale) database met biometrische gegevens, en toepassingen met een eigen opslagmedium. Dit onderscheid heeft theoretische en praktische consequenties.

Op het theoretische vlak geeft een database het voordeel van het centraal bijeen hebben van biometrische en andere gegevens, die daardoor eenvoudig onderling vergelijkbaar zijn en blijven. Dit maakt zowel het schonen van de database mogelijk (ontdubbelen, op basis van naam of op basis van extreem nauwkeurig overeenkomende biometriek) als het vaststellen van de toegestane c.q. vereiste foutmarge in de meting.

Mocht bijvoorbeeld, meer praktisch, blijken dat voor een zekere gemeten waarde plus of min de toegestane foutmarge misschien wel tien kandidaat-identiteiten in de database aanwezig zijn, dan kan het onderscheidingscriterium worden versmald. Bij het niet vinden van een juiste opgeslagen waarde binnen de vastgestelde foutmarge, zou door hermeting of door het opvragen van aanvullende gegevens (user-id) alsnog een waarde kunnen worden gevonden.

Tevens kan bij een centrale database biometrie als extra authenticatie worden ingezet, bijvoorbeeld als authenticatie van de identificatie door middel van user-ids en eventueel passwords.

Daar staat tegenover dat het idee van een centrale database op nogal wat, terechte en onterechte, bezwaren stuit (zie verderop de paragraaf 'Vraagtekens'). Een oplossing is om de opgeslagen, uit de enrollment volgende initiële waarde niet in een database onder te brengen maar aan iedere gebruiker individueel mee te geven. Hiervoor zijn vele middelen voorhanden; de bekendste zijn smartcards en polsbanden. Indien die in respectievelijk dicht genoeg bij een leesapparaat worden gehouden, kunnen ze worden uitgelezen en de ter plekke gemeten biometrische waarde kan worden vergeleken op voldoende overeenkomst met slechts die ene waarde. De vergelijking laat in dit geval vaak een wat grotere tolerantie in de vergelijking toe omdat sprake is van authenticatie van de andersoortige identificatie (user-id) en er dus nauwelijks verwarring met andere gebruikers mogelijk is.
Deze manier van werken brengt een additioneel voordeel met zich mee: de drager van de enrollment-meetwaarde doet tevens dienst als identificatie door bezit. De asielzoekers in Nederland kennen reeds het Elektronisch WeekDossier dat identificeert met smartcard en vingerafdruk. Maar de Schiphol Travel Pass volgens hetzelfde idee (voor 'frequent flyers' die ermee sneller door controles konden) is buiten de belangstelling geraakt; wellicht was de overhead toch relatief te groot.

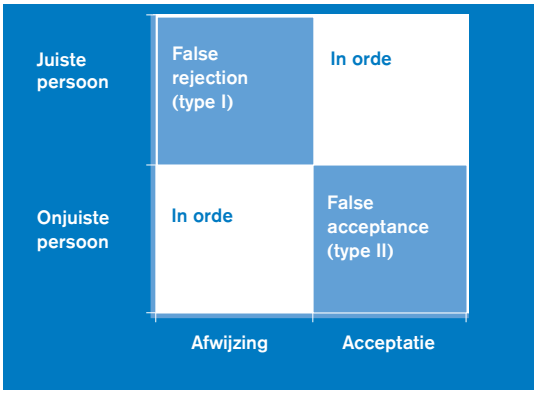
Een nadeel is dat er nog steeds sprake moet zijn van een eerste enrollment om de biometrische uitgangswaarde (template) op het medium te krijgen. Dubbelen (gebruikers die twee cards hebben) zijn heel wel mogelijk, en bij gebrek aan mogelijkheid tot centrale doorlichting, uiterst moeilijk op te sporen. Dit kan ook, bijvoorbeeld bij compromittatie, een voordeel zijn.

Betrouwbaarheidscriteria

Een belangrijke factor die telkens weer opduikt, is de betrouwbaarheid van biometrische systemen. Die is uit te drukken in diverse technische maten False Rejection Rate en False Acceptance Rate. Helaas – juist de zo nauwkeurige biometrische systemen geven geen nauwkeurige uitslag. Waar user-ids en wachtwoorden ten minste nog goed of fout zijn – een tussenweg is er niet – geven biometrische systemen wegens de meting van analoge eigenschappen een wat minder duidelijk antwoord.

De False Rejection Rate (FRR, Type-I-fout) is de kans dat een aanmelder ten onrechte wordt afgewezen op basis van de biometrische meetwaarde. Het doel is deze zo laag mogelijk te houden, om te voorkomen dat gebruikers klagen over onterechte afwijzingen. Dit vraagt om zo groot mogelijke meetmarges, zeker omdat rekening moet worden gehouden met veranderlijkheid van persoonlijke biometrische kenmerken, in de tijd en wegens de klimaatomstandigheden. Bovendien kan de technische kwaliteit van een systeem de meetmarge nog groter maken dan nodig zou zijn c.q. toelaatbaar is.

De False Acceptance Rate (FAR, Type-II-fout) is de kans dat een aanmelder ten onrechte wordt geaccepteerd op basis van de biometrische meetwaarde. Het doel is deze

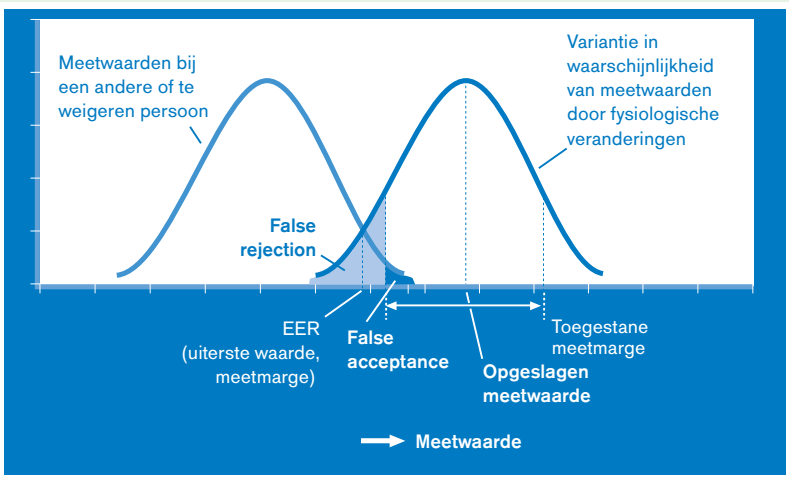


Figuur 1. False acceptance, false rejection.

zo laag mogelijk te houden, omdat uniciteit van de identificatie en authenticiteit wordt nagestreefd. Dit betekent een streven naar zo klein mogelijke meetmarges, ondanks de veranderlijkheid van biometrische karakteristieken.

Een derde maat die wordt gebruikt, is de Equal Error Rate (EER), die het punt aangeeft waarbij de FAR en FRR even groot zijn, hetgeen afhankelijk is van onder andere de toegestane meetmarge. De EER hangt samen met de D Prime-maat die aangeeft hoe 'goed' een middel twee individuen uit elkaar kan houden; een hogere D Prime is beter.
De false acceptance, false rejection en Equal Error Rate zijn in de figuren 1 en 2 weergegeven.

Sommigen in de biometriewereld werken met verwante, maar net wat andere begrippen. FAR en FRR richten zich namelijk op slechts een deelverzameling van de toepassingen. Een Type I-fout kan namelijk ook zijn wat juist wordt gezocht bij bijvoorbeeld fraudebestrijding: als een persoon die een enrollment wil in bijvoorbeeld een database van een sociale dienst, een biometrische waarde heeft die reeds in de database voorkomt, en een match geeft ('juiste persoon' in termen van figuur 1), dan willen we juist dat dit tot een Afwijzing leidt. (Dergelijk gebruik heet een Type B-applicatie, in tegenstelling tot de gangbare Type A-applicaties.) Andere toepassingen kunnen op eenzelfde manier een wat ander beeld geven. Vandaar dat in situaties waarin een en ander niet vanzelfsprekend duidelijk is, de termen 'false match' en 'false non-match' worden gebruikt; die zijn dan begrijpelijker.



Figuur 2. Variantie van meetwaarden, meetmarge, false acceptance/ rejection en EER.

In figuur 2 is de invloed van fysiologische veranderingen en de daarvoor vereiste meetmarge weergegeven. Duidelijk is dat een grotere veranderlijkheid een grotere meetmarge vereist om niet te veel false rejections te krijgen, maar dat dan anderzijds de false acceptance ook toeneemt.
Het streven zal dus moeten zijn naar (door meetomstandigheden, veroudering en dergelijke) niet of nauwelijks veranderende biometrieken zodat de variantie afneemt en de meetmarge omlaag kan. Daarnaast is er dan het zoeken naar biometrische kenmerken die zo uniek identificerend mogelijk zijn, zodat de getoonde curves verder uit elkaar zullen liggen – liefst helemaal geen overlap vertonen – en ongeacht de meetmarge de FAR en FRR laag zullen zijn.

Technieken

De heden ten dage voorhanden systemen baseren zich op de volgende biometrische kenmerken, te onderscheiden naar fysieke en gedragskarakteristieken:

Fysieke karakteristieken

Handtekeningen
Een klassieke; uitgangspunt was altijd dat die redelijkerwijs uniek was en niet eenvoudig na te maken[2]. Tegenwoordig is met name dat laatste een serieus probleem aan het worden. Niet alleen kan men door oefening een aantal handtekeningen vrij vloeiend neerzetten, ook wordt steeds meer een fax met handtekening geaccepteerd. Daarvan is niet meer af te lezen of die niet vanaf een (ander) geldig document is ingescand en eenvoudigweg weer uitgeprint.

Vingerafdrukken (dactyloscopie)
In principe een bekende methode en voor wat betreft zichtherkenning via inktafdrukken reeds sinds 1800 v.C., in Babylonië en China, en later ook in Europa, grootschalig in gebruik als handtekening (authenticatie) en in justitiële kringen voor identificatiedoeleinden. Tot voor kort was ook niet echt sprake van biometrie in de zin die in dit artikel wordt bedoeld; de vingerafdruk werd/wordt op zicht op een aantal karakteristieke punten vergeleken zonder dat een werkelijke unieke waarde (getal) werd berekend. De tegenwoordige automatische vergelijkingen op grote schaal die mogelijk blijken – de FBI doet het al vele jaren –, duiden echter op het (alsnog) gebruiken van biometrie.

De laatste paar jaar komen steeds eenvoudiger te hanteren en goedkopere vingerafdruklezers op de markt. Siemens levert bijvoorbeeld al toetsenborden met ingebouwde lezer, die een simpele login mogelijk maken. De Spaanse sociale dienst gebruikt reeds authenticatie op basis van vingerafdrukken om dubbelen in de 'cliënten'-database te voorkomen. De staat Texas is bezig eenzelfde systeem te implementeren ([Aren99]).

2) Nog wat verder terug in de geschiedenis komen we beeldmerken c.q. namen tegen op hiëroglyfen en kleitabletten. Praktisch gezien waren die uniek; het aantal hooggeschoolden dat voldoende goed kon beitelen, was beperkt en de sanctie op misbruik was eenvoudigweg de doodstraf. Sinds toepassing van die sanctie niet langer acceptabel was, werd het waarborgen van de uniciteit minder goed mogelijk en nam de inzetbaarheid als echtheidskenmerk af. De zegelring kent een vergelijkbaar probleem.

Handvorm- en handpalmlezers
Ook in (het totaal van) de twee- of driedimensionale vorm van de hand (totale maten, maten en plaats van vingers en knokkels) blijken voldoende unieke (combinaties van) kenmerken voor te komen. Handpalmlezers bepalen net als bij vingerafdrukken de – voldoende unieke – patronen van handlijnen. Zie de sciencefictionfilms waarin toegang tot geheime gangen wordt verleend met handpalmlezers; dat is kennelijk voldoende onderscheidend voor identificatie. Disney World gebruikt reeds handscanners voor de identificatie van abonnementshouders, Lotus gebruikt handvormlezers voor identificatie van afhalers bij de companycrèche, en Coca-Cola gebruikt hier en daar handvormlezers in plaats van de prikklok.

Handpalmlezers voor het openen van deuren, etc. richten zich (kennelijk) met name op identificatie, van authenticatie is vaak geen sprake, noch als doel van de handpalmlezer noch aanvullend met bijvoorbeeld een kennis- of bezitskenmerk.

Een variant is de vingerherkenner, die een driedimensionaal beeld van de vinger kan lezen.

Iris- en netvliespatronen (iris- en retinascanners)
Deze apparaten lezen met behulp van de reflectie van een lichtbundeltje de unieke (ader)patronen op de iris of op het netvlies, en vertrouwen dus in wezen op de blauwe ogen van de gebruiker. Een voordeel is dat geen fysiek contact met het leesapparaat (een camera) nodig is. Fabrikanten laten niet na erop te wijzen dat dit geen schade geeft; dit is niet voor niets, want de angst daarvoor weerhoudt acceptatie (vooralsnog?). Deze methoden blijken de beste, omdat de gelezen patronen redelijk uniek blijken. Dat wil zeggen, 98% zekerheid van identificatie van de juiste persoon blijkt haalbaar. Wie een blauw oog is geslagen, komt er dus waarschijnlijk niet in. Een combinatie met identificatie op andere basis zal uiteraard een veel hogere zekerheid van authenticatie kunnen bereiken. Een aantal Amerikaanse gevangenissen en kerncentrales (gemene deler: hoge veiligheidseisen) werkt reeds met irisscanners.

Een variant op deze methoden leest het unieke infraroodabsorptiepatroon van de pols, en leidt daaruit het aderpatroon af. Voorwaar een aantrekkelijke optie, want het leesapparaat kan in een horloge worden verwerkt.

Gezichtsvormherkenning
De middelen die hiervan gebruikmaken, bepalen een aantal (sommige tot negentig) dimensies van een (cameraopname van een) gezicht en vergelijken die met opgeslagen profielen. Om in termen van de betreffende systemen te blijven: de Eigenface en Eigenhead worden bepaald. Voor Roodkapje werd dat een probleem: ‘Maar oma! De vormkenmerken van uw mond en tanden komen niet overeen met het profiel dat ik in mijn geheugendatabase had opgeslagen!’; ‘Ja m’n kind, template aging (veranderen van biometrische karakteristieken in de loop der jaren, red.) is mogelijk...’. De systemen die nu commercieel beschikbaar zijn, claimen echter zelfs van brillen, make-up en een weekendbaardje geen last te hebben. Een extra complexiteit is dat in deze categorie systemen steeds meer gebruik wordt gemaakt van kunstmatige intelligentie, waarvan de sterkten en zwakten nog zullen moeten blijken. De werking zal toch bij voorkeur via een deterministisch proces moeten gebeuren vanwege de controleerbaarheid en herhaalbaarheid die bij bijvoorbeeld claims zal moeten worden aangetoond.

Gezichtswarmtebeeldherkenning
Deze methode is vergelijkbaar met de vorige, maar bepaalt niet de zichtbare dimensies maar de karakteristieken van een infrarood-warmtebeeld. Hiermee wordt voorkomen dat zomaar een foto voor de camera wordt gehouden. De basispatronen in het warmtebeeld van een gezicht blijken namelijk redelijk constant, ondanks invloeden van schommelingen in de omgevings- en in de gezichtstemperatuur.

Gedragskenmerken

Handtekening (uiterlijk en drukpatroon)
Er is een ontwikkeling te zien waarbij niet meer het uiterlijk maar het karakteristieke drukpatroon van het zetten van een handtekening het echtheidswaarmerk is. Opvallend is dat deze ontwikkeling eigenlijk al decennia loopt en kennelijk nog steeds slechts met moeite marktrijp is te maken. Dat een meegedragen of in centrale database opgeslagen normwaarde voor het drukpatroon tot voor kort moeilijk realiseerbaar was, kan hier debet aan zijn. Het eenvoudig leesbaar zijn van creditcards maakt opslag van het patroon op de magneetstrip daarvan tot een te groot risico. (Terwijl de minieme ruimte voor een vaak halfversleten handtekening in inkt op de achterzijde van een card kennelijk wel helpt ...)

Bovendien zal leesapparatuur nodig zijn in situaties waarin voorheen een gewone pen van een dubbeltje inzetbaar was. Dit kan een drukgevoelige plaat zijn waarop moet worden getekend en sinds kort is er ook een pen verkrijgbaar die de drukmetingen kan verrichten.
Een ander nadeel is dat een handtekening bij uitstek onderhevig is aan wijziging in de tijd, en de toleranties dus hoog moeten zijn.

Toetsaanslagdynamica (keyboard ballistics)
Juist passwords en andere familiaire tekst blijken door de rechtmatige eigenaar met een zeer specifiek ritme te worden ingetypt. Door deze snelheids- (en druk)patronen te vergelijken met het opgeslagen profiel – hoe handig, als toch het ingetypte user-id en password moeten worden opgezocht – kan wederom bij de kennis van (user-id en) het password een zijnskenmerk worden vergeleken.

Stemherkenning
Stemherkenning is iets anders dan spraakherkenning. Bij stemherkenning gaat het om de herkenning van de eigenaar van het stemgeluid (in casu van de karakteristieke frequentiecombinaties daarvan), bij spraakherkenning gaat het om woordherkenning n’importe wie de woorden uitspreekt – sterker nog, spraakherkenning wordt zo accentinvariant mogelijk gemaakt, terwijl de hier bedoelde stemherkenning juist zo specifiek mogelijk wil zijn. Canadezen die regelmatig Montana inreizen, kunnen inmiddels door middel van stemherkenning allerlei paspoortpoespas vermijden.

Uiteraard zijn naast 'text-dependent' middelen (die een vaste tekst vragen, bijvoorbeeld een password) ook 'text-prompted' (challenge-responsesystemen) ontwikkeld, alsmede 'text-independent' systemen waarbij de gebruiker gewoon voor de vuist weg wat kan vertellen.

Toepassing van technieken op basis van gedragskenmerken vereist een biometrieklezer dicht bij de centrale database.

Met name bij gedraggeoriënteerde systemen is er een risico op gebruikers wier gedragspatroon zodanig varieert dat ze ten onrechte door een systeem niet zullen worden herkend. Ook fysiek georiënteerde systemen kunnen hier last van hebben, al zal het deel van de gebruikers dat binnen een gedefinieerde marge zal blijven, groter zijn.

Bij al deze technieken valt op dat toepassing in de praktijk vaak nog alleen mogelijk is met de biometrieklezer die fysiek, maar ten minste logisch, dicht bij de centrale database c.q. het controlemechanisme is. Dit om snel de gemeten waarde of de opgeslagen tegenwaarde te kunnen opzoeken en om te voorkomen dat er weer allerlei communicatiekanalen moeten worden gebruikt die eventueel kwetsbaar zijn, bijvoorbeeld voor een Man in the Middle of een Denial-of-Service-aanval. Het tegendeel hiervan, met de vergelijkingstest juist ver weg – en 'off-line' – in een laboratorium, is:

* DNA-profielen vergelijken. Dit middel werd bijvoorbeeld gebruikt bij identificatie van een vermoedelijke dader in een seksschandaal waarbij een vooraanstaande Amerikaanse politicus betrokken was. Ziehier een voorbeeld van biometrie voor non-repudiation. Overigens zijn de DNA-methoden heel wat minder uniek identificerend dan wel wordt verondersteld; sommige onderzoeken komen niet verder dan een non-repudiation met 95 procent zekerheid. Zoals in het genoemde geval van de politicus kan een DNA-profiel echter wel worden gebruikt in combinatie met andere bewijsvoering, indien die op zich tekortschiet; het DNA-profiel wordt dan gebruikt als versterking (omdat eventuele andere verdachten een veel slechtere 'match' geven).

* Ten slotte zijn er ook systemen die op basis van lichaamsgeur individuele authenticatie mogelijk zullen moeten maken. De ontwikkelingen zijn nog wat prematuur, en over de FAR en FRR van lichaamsgeuren is nog weinig duidelijk. Een maaltijd met flink wat alcohol (of knoflook) zal immers geen belemmering mogen zijn om vervolgens aan het werk te kunnen.

De exotische toepassing van het gebruik van oorvormen zal vooralsnog buiten beschouwing blijven.

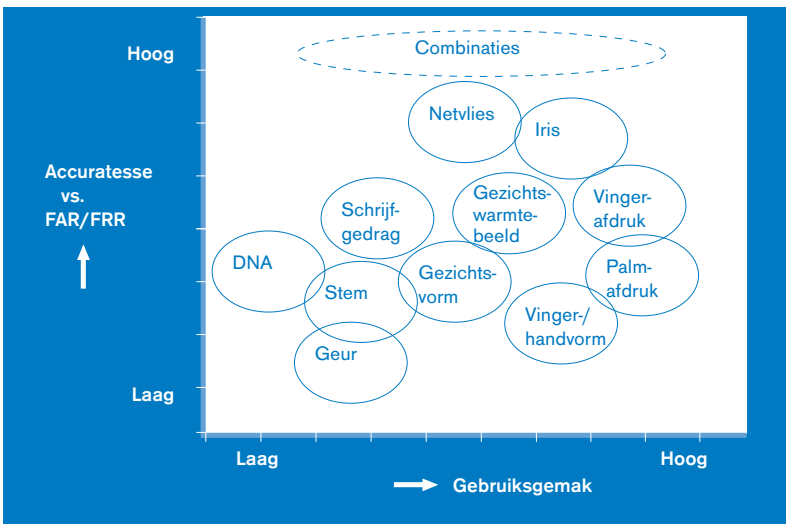
De inherente sterkten en zwakten van al deze technieken zijn niet eenvoudig onderling vergelijkbaar wegens de grote afhankelijkheid van meetomstandigheden (incidentele nauwkeurigheid van meetwaarden) en de kwaliteit van de implementaties (aantallen meetpunten, systematische nauwkeurigheid van meetwaarden in de software). Toch zijn kort-door-de-bocht, dus met de nodige voorzichtigheid, wel enige onderlinge verhoudingen te schatten; deze zijn weergegeven in figuur 3. Bij voortschrijdende techniekverbeteringen zullen de biometrieken naar rechtsboven in de figuur schuiven.

Voor latere selectie, implementatie en gebruik van middelen is het behulpzaam tevens de classificatie te hanteren die door de San José State University (SJSU) is samengesteld. De SJSU-classificatie wordt breed erkend en gehanteerd als gemeenschappelijk begrippenkader. De indeling onderscheidt de middelen naar:

* *coöperatief versus non-coöperatief*. Graadmeter is de bereidheid tot medewerking van de gebruiker. Als de gebruiker waarden wil afschermen, zal hij willen meewerken; als hij/zij eventueel door de mand valt als fraudeur, zal dat 'wat minder' het geval zijn. Dit heeft consequenties voor het al of niet 'fool proof'[3] moeten zijn van het gebruik.
* *openlijk versus verborgen*. De meeste toepassingen zullen openlijk, duidelijk zichtbaar zijn. Soms kan uit oogpunt van fraudepreventie echter juist het 'ongemerkt' gebruik van biometrie nodig zijn.
* *gewende versus nieuwe gebruiker*. Een gebruiker die regelmatig biometrische metingen ondergaat, kent de procedure en zal, bijvoorbeeld, zijn hoofd stilhouden voor een warmtebeeldopname. Een gebruiker die een en ander niet is gewend, zal hier minder op letten.
* *onder toezicht versus vrij*. Bij metingen onder toezicht (c.q. met hulp) van een ervaren gebruiker, instructeur of controleur is er minder opleidingsbehoefte dan bij systemen waarbij (ook nieuwe) gebruikers hun gang kunnen gaan.
* *standaardomgeving versus niet-standaardomgeving*. Een standaardomgeving kent minder storing door fysieke omgevingsfactoren; bij een niet-standaardomgeving tellen die nogal eens zwaar mee in de betrouwbaarheid.

3) 'Fool' zowel duidend op fouten die een gebruiker kan maken, als duidend op eventueel zijn intentie.

Figuur 3. Onderlinge kwaliteitsverhoudingen (naar [Stee98]).



Doel: authenticatie van de bron aan de bron met de bron

Een voornaam aspect dat een rol speelt, is het verschil tussen vertrouwelijkheid en exclusiviteit. Vertrouwelijkheid houdt in dat een verzonden bericht niet anders dan bij de bedoelde ontvanger(s) terechtkomt; logisch gezien dus een veel-naar-eenrelatie. Vertrouwelijkheid speelt daarom zo'n belangrijke rol bij bijvoorbeeld e-commerce voor consumenten: liefst zo veel mogelijk klanten willen ervoor zorgen dat hun creditcardgegevens alleen bij één Internet-boekhandel terechtkomen. Exclusiviteit gaat verder, en doelt op een een-op-eenrelatie.
Om het nog even recht te zetten: de bedoeling van (separate) authenticatie is een-op-veel, althans, zorgen dat dat 'een' aan wie dan ook duidelijk wordt. Ziedaar de reden om vertrouwelijkheid en authenticatie te combineren. En, mede belangrijk om in het achterhoofd te houden, authenticatie betekent meestal authenticatie van de identificatie; een garantie dat de identificatie – door de initiator of door de ontvanger – juist is.

In figuur 4 is de communicatiepijplijn (*vereenvoudigd*) schematisch weergegeven, voor een gebruiker die vanaf zijn toetsenbord, links in de figuur, en PC een (trans-) actie wil uitvoeren op een server, rechts, of aan een ontvanger aldaar een bericht wil doorgeven. Op de PC zelf zal al, door identificatie/authenticatie, moeten worden zeker gesteld dat alleen de juiste gebruiker/zender acties of een bericht kan invoeren. Vervolgens zal, door encryptie, moeten worden voorkomen dat op het netwerk wordt afgeluisterd, een Man in the Middle[4] een bericht oppakt en gemodificeerd doorstuurt, of dat de Man in the Middle zorgt dat het bericht bij de verkeerde ontvanger terechtkomt.
Bij de server aangekomen, zal moeten worden gecontroleerd dat het bericht ongestoord op het netwerk heeft kunnen reizen; vandaar de herhaalde authenticatie. Gelukkig zal zelden alleen authenticatie van de bron-PC plaatsvinden maar zal ook de feitelijke gebruiker opnieuw worden geauthenticeerd. Het grote probleem is echter hoe kan worden zeker gesteld dat een ontvangen bericht werkelijk van de aangegeven afzender stamt, en niet van een valse gebruiker, een overgenomen PC of een Man in the Middle.
Op de server zelf zal ten slotte autorisatie moeten worden gegeven, zowel aan de zender, om überhaupt een bericht te mogen aanleveren c.q. de gewenste transactie te mogen uitvoeren, als aan de ontvanger, om het bericht c.q. de transactie op te nemen.

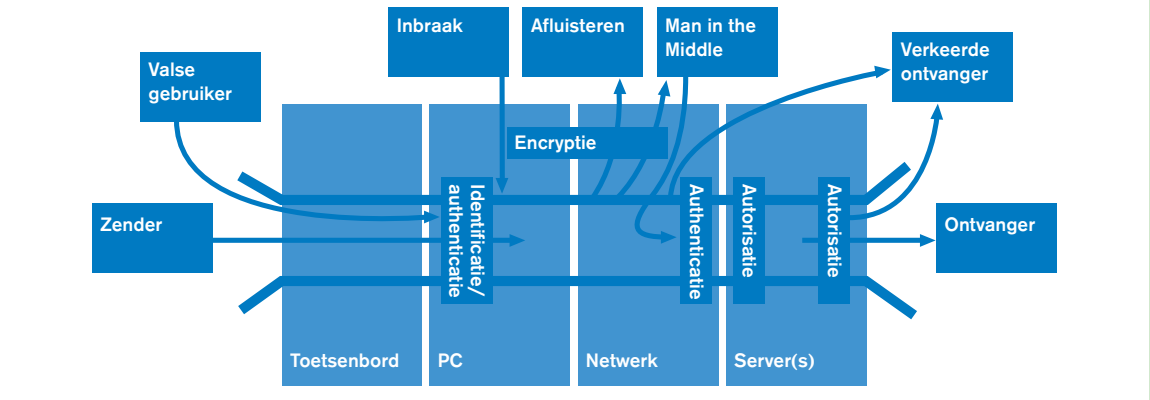
Het risico van inbraak is met identificatie/authenticatie, encryptie en autorisatie nog niet gemitigeerd. Een inbraak op de PC kan betekenen dat maatregelen verderop in/op de pijplijn buiten werking worden gesteld, en dan bijvoorbeeld een Man-in-the-Middle-aanval (vanaf een willekeurige PC) mogelijk maken. En een inbraak op een server kan uiteraard de autorisatie buiten werking stellen doordat de inbreker zich weet te presenteren als een geautoriseerde gebruiker – een lek op de server betekent immers dat er van 'geen belemmering wegens beveiliging' sprake is.

In dit artikel ligt de nadruk op biometrische hulpmiddelen voor authenticatie (verificatie van de identificatie, zogenaamde 'closed search') en voor identificatie (herkenning, zogenaamde 'open search') als aparte toepassing aan de, in termen van figuur 4, zender-kant. En bij ontbreken van een netwerk, tevens de authenticatie op de server. De mogelijkheden voor identificatie worden door diverse fabrikanten nogal eens benadrukt door te wijzen op de vijftig procent helpdeskcalls die betrekking hebben op vergeten passwords; die zouden met biometrische hulpmiddelen geheel zijn te vermijden. *Mits* de tools nauwkeurig genoeg zijn, zou sterkere beveiliging met biometrie bovendien nu eindelijk eens verlaging van overhead voor gebruikers en beheerders kunnen betekenen: er is geen passwordbeleid, -invoer en -beheer meer nodig.

De gezochte waarborgen voor uniciteit leiden ook tot bruikbare middelen voor non-repudiation (onweerlegbaarheid, het niet kunnen ontkennen een bericht te hebben verzonden); dit is vooralsnog een extraatje, dat ook door de vragende (authenticatie-eisende) partij als nevenvoordeel zal worden beschouwd.

De authenticatie zal zo dicht mogelijk op de werkelijke bron moeten plaatsvinden; iedere (technische) schakel is er één waar voorafgaand al een inbreuk kan zijn gedaan op de integriteit van de keten. Men denke bijvoorbeeld aan het geval van de bank waarvan de clientsoftware compromitteerbaar bleek en waar na compromittatie van die software de cliëntgegevens uit de banksystemen konden worden opgehaald – niet door de eigenaar maar door de hacker.

4) In het vervolg van dit artikel zal 'Man in the Middle' duiden op de entiteit die berichten afluistert, ze al of niet modificeert en al of niet doorgeeft, met de intentie die berichten voor authentiek te laten doorgaan. Voor het gemak is dus hier ook de 'gewone' afluisteraar onder de term geschaard.



Figuur 4. Communicatiepijplijn.

Doordenkend voldoet in zo'n geval alleen een 'water'-dichte PC of terminal; alleen dan kan worden zeker gesteld dat er geen screengrabbers, keystrokelezers of andere Trojaanse paarden kunnen worden binnengesmokkeld. In het geval van de bank was dat niet haalbaar, het betrof immers PC's bij de mensen thuis en verbindingen over het grote, open Internet. Er zal dus een middel nodig zijn dat niet (alleen) de over de lijn verzonden codes identificeert als behorende bij een zekere persoon, maar tevens vaststelt dat de bron in orde is.

Normaliter worden daarvoor middelen van kennis en eventueel bezit gebruikt, in casu wachtwoorden en allerhande tokenkaarten[5] met, in het gunstigste geval, one-time nonces uit challenge-responsemechanismen met pincodes erin versleuteld. Ofwel, het authenticatiebericht, de respons met nonce (berekend antwoord) kan hoogstwaarschijnlijk alleen zijn gegenereerd uit een unieke combinatie van token(reken)kaart, pincode en eenmalige, tijdelijk geldige challenge. Een dergelijk complex mechanisme garandeert redelijkerwijs kennis (wachtwoord/pincode), bezit (tokenkaart) en juiste adressering (adres voor de challenge). Dit laatste kan nog worden versterkt door gebruik te maken van callbackfaciliteiten, zodat een eerste contactpoging wordt tot een identificatie van het verzendadres.

Daar staat tegenover dat een Man in the Middle nog steeds op een bestaande verbinding, of een verbinding in opzet, kan inbreken. Dit kan met een juiste stapeling van encryptie- en andere exclusiviteitsmaatregelen – PC's en servers afschermen – worden tegengegaan.

Kennis en bezit blijken echter nog steeds, door toeval, list en bedrog of onder dwang, te kunnen worden ontnomen. Zie het genoemde voorbeeld van valse adreswijzigingen. Derhalve is er een behoefte aan nog sterkere mechanismen: onvervreemdbare individuele eigenschappen. Dergelijke eigenschappen worden vastgesteld met biometrie.

5) In de vorm van een rekenmachientje of smartcard.

Vraagtekens

Er is een aantal vraagtekens, soms zelfs 'tegens', die de doorbraak van grootschalig gebruik van biometrische hulpmiddelen hebben gehinderd:

* De kosten. Nog niet zo lang geleden was dit een factor van belang. Tegenwoordig valt dat wel mee, maar zijn het (nog steeds) de kosten van introductie en beheer – met name in de vorm van mensuren maal tarief – die een belemmering kunnen vormen. Simpele apparaatjes kosten nog slechts zo'n *f* 50 tot *f* 100 maar een rechttoe-rechtaan schatting is dat de beveiliging van één deur met een gezichtsherkenningssysteem zo'n *f* 10.000 tot *f* 20.000 kost ([Stee98]), terwijl soms niet duidelijk is wat de opbrengsten zijn in termen van eenvoudiger gebruik. De opbrengsten door minder fraude zullen heel wat eenvoudiger zijn vast te stellen, indien althans ervaringscijfers wat dat betreft voorhanden zijn. Anders blijft het moeilijk de voorkomen fraude te schatten.
Probleem is nu dat voor lage prijzen hoge (verkoop)volumes nodig zijn, die pas tot stand zullen komen bij lage prijzen.

* De technische kwaliteit, die tot nu toe magertjes was. Sensors bijvoorbeeld vielen al na een paar keer aanraken uit en een beetje statische vinger gaf ook al problemen. Zeker de systemen waarbij de vinger direct op een Digital Signal Processing-chip werd geplaatst, konden slecht tegen statisch zijn, warmte en vocht. Hetgeen door de fabrikanten momenteel ook in mindere of meerdere mate wordt toegegeven; die zouden wellicht niet zo 'eerlijk' zijn als hun nieuwe systemen niet beter zijn.

* De hygiëne van leesapparatuur. Hoe is het voldoende schoon houden van de leesplaat te bereiken als een vingerafdruklezer of handpalmlezer in publiek toegankelijke ruimten wordt geplaatst? Niet alleen zal het schoonhouden nodig zijn voor voldoende nauwkeurige meetwaarden, ook zal de hygiëne overduidelijk zichtbaar in orde moeten zijn om weerstand van gebruikers te overwinnen. Een veelbelovende ontwikkeling op dit vlak is de smartcard waarop het leesvlak zelf is ingebed zodat eenieder zelf heeft te zorgen voor het niet vervuilen – wie z'n handen niet heeft gewassen, komt er dan niet in.

* Bij andere apparatuur, met name bij iris- en netvlieslezers, is er huiver wegens het risico van fysieke schade. Dit risico wordt door fabrikanten nihil genoemd, maar dat is voor (potentiële) gebruikers weinig reden tot het laten varen van de tegenzin; als de claims van fabrikanten later toch onjuist zouden blijken te zijn, komen er claims van de gebruikers maar dan is het kwaad al geschied.

* In het algemeen blijkt het helaas mogelijk dat redelijk 'fool proof'-systemen toch door 'fools' (moeten) worden gebruikt en dat het mogelijk is een hand nou net verkeerd op een handpalmlezer te leggen. Dit gaat natuurlijk ten koste van de meetnauwkeurigheid en daarmee ook van de betrouwbaarheid.

* De robuustheid van systemen tegen incidentele storingen was tot nu toe bepaald niet altijd in orde. Een snee in een vinger moet bijvoorbeeld niet verhinderend zijn. Gelukkig hebben bijvoorbeeld vingerafdruklezers voor dergelijke gevallen soms de mogelijkheid een 'reservevinger' te registreren waarmee dan alsnog kan worden gematcht. Stemherkenners moeten robuust zijn tegen bijvoorbeeld een verkoudheidje of gehaastheid, hetgeen nog wel eens problemen opleverde.

* Het risico van vervalsingen is niet nul. Een (dunne) plastic handschoen met voorgedrukte vingerafdruk en een bandopname om een stemherkenner te misleiden, het zijn voorbeelden van risico's waarvan de onduidelijkheid over de omvang tot nu toe het vertrouwen in de kwaliteit van oplossingen (te) laag hield. Ook een contactlens met de juiste imprint zou irislezers kunnen misleiden.

* De technische haalbaarheid was nog niet in orde. Met name de koppeling aan operatingsystemen en applicaties was nog een probleem. Ook was nog onduidelijk in hoeverre de databases met biometrische templates 'proprietary', leverancierseigen, waren of juist open, door andere applicaties bruikbaar. De kans op een legacy-systeem waarbij gebruikers in geval van vervanging opnieuw zouden moeten 'enrollen', was reëel.
Maar sinds de 'proprietary'-toepassingen en -technieken samenklonterden tot substandaarden als SVAPI, HA-API, BAPI (van Intel en de OpenGroup) en AIS API (IBM), en de beide laatste zowel in de nieuwe BioAPI meedraaien als toch ook nog hun eigen varianten verder ontwikkeld zien, is het overzicht er niet beter op geworden.

* Gebruikers waren (en zijn) huiverig wegens de privacy- en beveiligingsaspecten. Met name de risico's dat een database met biometrische gegevens zou worden doorverkocht (gebeurde eens, maar moest onder luide publieke protesten worden teruggedraaid) en/of dat een inbreker de biometrische templates zou stelen, betekenden een weigerachtige houding van potentiële gebruikers.

* De privacy van biometrische gegevens was (en is) een onderwerp op zich. Niet alleen kan biometrie een inbreuk op de persoonlijke levenssfeer betekenen of een inbreuk op de persoonlijke (fysieke) integriteit, maar dat kan ook gelden voor het gebruik van een biometrische template als unieke sleutel voor de koppeling van allerlei persoonsgegevens en andere (koopgedrag)gegevens in grote databases. In de Verenigde Staten is aparte wetgeving inzake biometrische gegevens in ontwikkeling (zie onder andere [ICSA99] en [Rice99]); of wetgeving of zelfregulering de voorkeur verdient, is zelfs in de Verenigde Staten nog onduidelijk. De International Computer Security Association (ICSA) heeft reeds een verzameling zeer doorgedachte 'principles' beschikbaar.

Zie tevens kader 1, dat een reeks juridische kwesties opsomt. Waarbij nog de aantekening past dat kader 1 slechts die zaken weergeeft waarvoor nationale wetgeving een rol speelt. Men bedenke dat bij grensoverschrijdend gebruik en doorgifte van biometrische gegevens, even zo bredere wet- en regelgevingsaspecten van belang zijn.

* Religieuze groeperingen hebben, nog sterker dan bij andere computertoepassingen, bezwaar tegen gebruik van het Nummer van het Beest. Vraag is of daarop wel een tegenargument bestaat. Heel de mens wordt binair vastgelegd, gereduceerd tot een nummer ... Enige vervolgkwestie is of dit zal leiden tot een ontmenselijking van de wereld of dat de optimisten nu eens een keer gelijk krijgen. Deze kwestie kan binnen het kader van dit artikel niet afdoende worden uitgewerkt, maar is in maatschappelijk verband niet verwaarloosbaar.

* De non-repudiation kan te sterk zijn. Als er zo sterk op biometrie kan worden vertrouwd, zal dat ook gebeuren. Hoe nu te bewijzen dat een ander de biometrische template kan naspelen zodat die valse transacties kan doen?

Vragen in de juridische sfeer die verduidelijking behoeven (ontleend aan [Kral99]):

* Hoe past biometrie als beveiligingstechniek in de huidige wettelijke kaders inzake beveiliging?
* Kan het gebruik van biometrie een inbreuk maken op de persoonlijke levenssfeer en zo ja, kan dat als een inbreuk op een grondrecht worden aangemerkt?
* Mogen individuele toepassingsaanbieders biometrische gegevens verzamelen, gebruiken en beheren en mogen zij hiermee verificatiediensten ten behoeve van derden verrichten?
* Moeten andere instanties dan de huidige de bevoegdheid krijgen om de ware identiteit van een natuurlijk persoon te kunnen onderzoeken?
* Moet deze personalisatie niet onder de Wet op de identificatieplicht worden gebracht?
* Hoe is de bewijspositie van de gebruikers van chipkaarten bijvoorbeeld bij mogelijke fraude?
* Moeten via een vergunningenstelsel onafhankelijke instanties worden gecreëerd voor het beheer van de verificatiegegevens?

Op basis van nadere analyse zijn hierop de volgende (gedeeltelijke) antwoorden te geven:

* De gebruikte techniek kan van invloed zijn op het antwoord op de vraag of sprake is van een inbreuk op een grondrecht.
* Inbreuk op een grondrecht hangt ook af van het bestaan van een fall-backoptie.
* Niet alle vormen van biometrische gegevens en methoden van opslag van deze gegevens vallen onder de wettelijke regels inzake de bescherming van persoonsgegevens.
* In het algemeen moet er grote voorzichtigheid worden betracht bij het handelen zonder medeweten of toestemming van de betrokkene en met verplichte biometrische persoonsverificatie.
* Als de proportionaliteit uit het oog wordt verloren, zal biometrie kwetsbaar zijn.
* Aan de wettelijke vereisten inzake beveiliging zal niet altijd kunnen worden voldaan zonder biometrie toe te passen. Op dit moment bestaat er nog onvoldoende duidelijkheid over de vraag voor welke toepassingen biometrie (wettelijk) noodzakelijk is.
* Het beheer en de adequate bescherming van grote databanken met biometrische gegevens vragen de aandacht van beleidsmakers.
* Er dient aandacht te zijn voor de vraag of een kaarthouder/verdachte kan worden gedwongen tot medewerking bij het opheffen van een biometrische beveiliging.
* De overheid dient zich te beraden op de vraag of een instantie die de chipkaart heeft gepersonaliseerd, moet worden verplicht bepaalde maatregelen te treffen ten behoeve van het opheffen van een biometrische beveiliging.
* Biometrie mag er nooit toe leiden dat hieraan dwingende bewijskracht wordt toegekend.
* Aandacht zal er ten slotte moeten zijn voor de opslag en het beheer van biometrische gegevens.

Kader 1. Juridische aspecten (nationaal).

* Onduidelijk is ook wat te doen zou zijn indien inderdaad compromittatie wordt geconstateerd. Dit geldt zeker voor eventuele centrale databases; compromittatie van de biometrische gegevens (templates) daarin is in wezen de aangewezen weg om een dergelijk systeem te kraken. Daar veelal alleen de hashwaarden zijn opgeslagen – of de opgeslagen waarde lijkt daarop, door de praktische onherleidbaarheid tot fysieke details –, zal een inbraak niet direct veel opleveren, of het moet gaan om sleutelwaarden tot databases met (andere) persoonsgegevens. Maar daarnaast kan met de hashwaarde(n) wellicht wel een replay worden gedaan en dan komt het probleem rond non-repudiation weer om de hoek kijken. Hoe te bewijzen dat een biometrische hashwaarde is misbruikt?

En er is het verhaal uit Japan over gangsters die de vinger van een 'executive' zouden hebben afgehakt om daarmee te kunnen inbreken. Als antwoord is nogal eens sprake van vingerprintlezers die tevens bloeddruk of -warmte zouden kunnen lezen. Alsof die, met noodzakelijkerwijs grote vergelijkingsmarges tegen FRR, niet zouden zijn te vervalsen op dezelfde wijze als een vingerafdruk. Onduidelijk is in hoeverre het hier een Broodje-Aapverhaal betreft; het verhaal speelt immers 'aan de andere kant van de wereld' en is dus prima oncontroleerbaar.
(Overigens, bij iris- en netvlieslezers kan een pupilreflexmeting worden toegevoegd, tegen misbruik door middel van foto's.)

Concluderend blijkt het juiste *zijn* nog steeds niet absoluut onlosmakelijk te zijn gekoppeld aan de juiste persoon, of aan de persoon die een oorspronkelijke transactie wilde doen. Oplossing is nog dieper die persoon binnen proberen te komen, om tot een onafscheidelijk en uniek kenmerk te geraken. Wat is wezenlijk aan een mens? Wie hierover doorfilosofeert, belandt in 'cogito ergo sum', terwijl dit niets oplost om een sluitend 'ego sum' aan de andere kant van een netwerk te krijgen ... Voorwaar hinderlijk, want de doelstelling was juist om unieke authenticatie te verkrijgen.

De meest uitgebreide poging die zou kunnen worden ondernomen, zal dan ook uitgaan van kennis, bezit én zijn. [Rice99] geeft het voorbeeld van een polsband met smartcard en pincode plus asymmetrische cryptografische codering. De polsband meet de polsaders (zijnswaarde), de gebruiker wordt een pincode gevraagd en bovendien worden met een public/private-keyalgoritme en een challenge-responsemechanisme de diverse, waaronder biometrische, waarden versleuteld naar een (radio)ontvanger gestuurd om aldaar te bepalen of de kennis, het bezit en het zijn bij elkaar horen. Dit alles zonder dat centrale opslag van de gegevens nodig is.

Nadeel is dat er nog steeds geen middel is om overvallers tegen te houden. Onder bedreiging een pincode afgeven zal bij gebruik van biometrie niet meer voldoende zijn, maar onder bedreiging 'gewoon' geld opnemen en vervolgens moeten afstaan blijft natuurlijk mogelijk. Het enige redmiddel dat dan nog over is, heet een stil alarm. Sommige software bij vingerafdruklezers kent deze mogelijkheid door een 'alarmvinger' voor te programmeren; wordt die gebruikt, dan is er sprake van dwang in een noodsituatie. En ook tegen een alarmvinger bestaan alweer twee bezwaren:
* Hoe weten we dat een melding van misbruik eerlijk is? Een willekeurige oplichter kan zijn alarmvinger immers gewoon gebruiken om bijvoorbeeld geld op te nemen en vervolgens een overval te claimen. Bij gebruik van een geldautomaat kan dan nog een cameraatje worden ingebouwd ter controle, maar als thuisbankieren ingang vindt, is dat niet doenlijk.
* Het bestaan van een alarmvingermogelijkheid zal algemeen bekend moeten zijn, eenieder zal die immers bij enrollment moeten opgeven c.q. registreren. Een overvaller weet dat dus ook, en kan dus afdwingen dat de overvallene toch maar, voor de eigen gezondheid, beter niet de alarmvinger kan gebruiken.

De alarmvinger is in wezen een vorm van steganografie, het meesmokkelen van verborgen informatie in overigens regulier lijkende berichten. Dit valt buiten de reikwijdte van dit artikel en richt zich (hier en normaliter) ook eerder op andere delen van de communicatiepijplijn van figuur 4 dan identificatie/authenticatie of autorisatie door biometrie.

Kritieke succesfactoren

De genoemde vraagtekens zullen moeten worden geadresseerd; ze vormen in wezen de kritieke succesfactoren waar ook de IT-auditor zich op kan richten. Er is een onderverdeling te maken in twee categorieën: de vraagtekens uit de vorige paragraaf die moeten worden opgeheven, en de (projectmatige en inhoudelijke) overwegingen die in het selectie- en implementatietraject worden gehanteerd.

Wegnemen vraagtekens

De vraagtekens zullen een voor een worden behandeld. In een aantal gevallen valt niet eenduidig aan te geven hoe een nadeel kan worden verholpen; techniek- en situatieafhankelijkheid staan zo'n antwoord in de weg.

* Het onderwerp kosten zal een probleempunt blijven. De vicieuze cirkel (om de kosten omlaag te brengen, zullen leveranciers grote aantallen van hun apparatuur moeten produceren en afzetten, maar dat zal pas lukken als de kosten al omlaag zijn) kwam al ter sprake. Een inschatting van de langetermijnlevensvatbaarheid van de leverancier is dan ook van groot belang. Hier staat tegenover dat een beperkt aantal serieuze toepassingen samen al voldoende kritische massa kan hebben om de veelal kleine leveranciers overeind te houden.

* Zoals aangegeven, beamen de leveranciers de tot voor kort tekortschietende technische kwaliteit van de systemen. Of hieraan reeds is tegemoetgekomen, zal in realistische praktijktests (zie diverse punten hieronder bij Overwegingen) moeten blijken.

* De hygiëne rond meetapparatuur zal een probleem blijven als het dat al is. In de praktijk zal vooral eerst een voorselectie moeten worden gemaakt van methoden die in aanmerking komen en vervolgens zal per methode moeten worden bepaald of en zo ja, in welke mate deze

gevoelig is voor verstoring, gegeven de specifieke omstandigheden. Uiteraard verdient het de voorkeur hiervoor een worst-casescenario te hanteren.

* Het punt fysieke schade dient uitdrukkelijk te worden ondervangen. Het overnemen van de verklaringen van leveranciers is onvoldoende, hieraan wordt door uiteindelijke gebruikers weinig waarde gehecht. Het lijkt zinvol indien weerstand van gebruikers voorzienbaar is, een onderzoek door een (door gebruikers zo gewaardeerd) onafhankelijk instituut te laten uitvoeren naar de 'feitelijke' fysieke risico's.
Een andere oplossing is uiteraard, bij gebleken gelijke geschiktheid, de voorkeur te geven aan een 'non-intrusive' biometrisch hulpmiddel.

* Het al of niet opzettelijk fool proof zijn hangt sterk af van enerzijds de gebruikersinstructie – voorzover de gebruikers nog fools zijn – en anderzijds de fraudebestendigheid – voorzover de gebruikers willen foolen – die even goed door de techniek als door het gebruik wordt bepaald. De afweging of een biometrisch middel wat dit betreft een verbetering is, moet worden afgezet tegen de nu gangbare methoden van magneetstrippassen met pincodes die allesbehalve (in (veel?) mindere mate) fool proof zijn.

* De robuustheid is in wezen een combinatie van de kwaliteit van de hardware (zie hiervoor) en de stabiliteit van de software. Het eerste kwam hiervoor aan de orde, het laatste is en blijft een probleem. Het probleem geldt zeker indien geheel wordt vertrouwd op aangekochte software die niet zo rigoureus kan worden getest als zelfontwikkelde software. Het kunnen terugvallen op een reservevinger is reeds gemeengoed voor vingerafdruklezers; de praktijk heeft nog onvoldoende gegevens opgeleverd over andere vervalsingsmogelijkheden.
Verbetering op deze punten is uiteraard gewenst, en wordt ook continu aangepakt. Bovendien moet alweer de vergelijking worden gemaakt met bestaande technieken.

* De koppeling aan applicaties wordt steeds beter. Zeker de komst van de BioAPI, waarachter zich onder andere Microsoft, Novell (ja die twee samen), IBM en Compaq (idem) scharen, zal voor een veel eenduidiger standaard gaan zorgen.

* In dezelfde lijn ligt de verdergaande ontwikkeling van het testen van biometrische applicaties. Het ICSA heeft reeds een uitgebreide 'testsuite' ontwikkeld die in gestandaardiseerde en daardoor onderling beter vergelijkbare manieren van testen kan worden gebruikt. Een aantal applicaties heeft van ICSA reeds een certificaat gekregen (een plus voorzover de waarde van zo'n certificaat helder zou zijn).

* Een belangrijk aspect dat hiermee samenhangt maar in de vaart der ontwikkelingen vaak minder aandacht krijgt, is de inbedding in organisaties van de applicatie. In dit geval gaat het met name om (eventueel) sleutel- en kaartbeheer, het beheer en onderhoud van apparatuur, het beheer en onderhoud van koppeling(en) aan applicaties, etc. Maar met een beheerst implementatie- en beheertraject c.q. -organisatie valt hieraan wel tegemoet te komen.

* De angst inzake privacy is op twee wijzen te overwinnen: een moeilijke en een gemakkelijke manier. De keuze is niet vrij.
De moeilijke manier is alle beveiliging rond de database(s) met biometrische en ermee samenhangende gegevens te tonen. Deze optie zal moeten worden gekozen als een centrale database wegens de gebruiksmodus nodig is, bijvoorbeeld als gebruik voor identificatie nodig is. Het tonen van de beveiliging kan op velerlei manieren, bijvoorbeeld door regelmatige onafhankelijke toetsing waarvan het resulterende rapport voor eenieder ter inzage ligt.
De gemakkelijke manier is door af te zien van 'databasе'afhankelijke opslag. Het genoemde opslaan van de biometrische gegevens op een smartcard is daarvan een duidelijk voorbeeld. De gebruiker draagt dan zijn biometrische gegevens met zich mee – en de eraan ten grondslag liggende fysieke eigenschappen ook –; voorwaar een methode die ook voor veel andere privacygevoelige gegevens prettig zou zijn. Indien dit echter te veel wordt doorgezet, kan wel eens een situatie ontstaan waarin het verlies van een smartcard te ernstige gevolgen heeft – zeker als, hetgeen reeds is aangetoond, smartcards ook kraakbaar kunnen zijn.

De genoemde meer algemene juridische vraagstukken zullen niet (altijd) door de individuele organisaties die biometrie willen inzetten, worden opgelost. Succesfactor is in dit verband de grondigheid waarmee wordt onderzocht welke juridische dilemma's van toepassing zouden kunnen zijn in een voorgestelde toepassing, en of maatregelen zijn genomen waarmee de organisatie zich ongevoelig kan maken voor sommige van de juridische dilemma's. Door bijvoorbeeld (ook om deze reden) centrale opslag te vermijden en smartcards als opslagmedium te kiezen, kan een aantal kwesties rond de beveiliging van persoonsgegevens worden vermeden.

Er zal altijd een manier moeten zijn om anders dan via biometrische hulpmiddelen identiteit te kunnen bewijzen, en ontkennen!

* Bij de juridische kwesties kwam al even de noodzaak van een fall-backoptie naar voren. Zeker bij voortgaande ontwikkeling van de technieken zal te veel zekerheid kunnen worden gehecht aan de waarborgen van uniciteit, en daarmee aan non-repudiation van biometrische hulpmiddelen. Er zal altijd een manier moeten zijn om op andere wijze identiteit te kunnen bewijzen, en ontkennen! Hoe dat zou moeten, is een nog niet uitgekristalliseerd onderwerp; in voorkomende gevallen zal ieder middel moeten worden aangegrepen. Maar wie dat aangrijpen ook doet, het zal meestal niet de organisatie (moeten) zijn die het biometrische middel inzet; die probeert juist vaak non-repudiation te verkrijgen.

* Tegen compromittatie valt het nodige te doen door de beheerorganisatie op een hoog peil te brengen en te houden. Een grote database met biometriegegevens die

wordt gekraakt c.q. gestolen, zou een compleet nieuwe enrollment nodig maken, met nieuwe gegevens. Met tien vingers kan er nog wat worden vervangen, al geeft dat wat gewenningsproblemen – de wijsvinger is toch motorisch het gemakkelijkst en meest gebruikt –, maar wat te doen met stemherkenning? Moeten alle gebruikers een ander stemmetje opzetten? (Terwijl een goede stemherkenner daar juist, nu dus ongewenst, doorheen zou lezen!)

Compromittatie van een databaseloos systeem is veel moeilijker voor elkaar te krijgen, dit vergt op z'n minst een inbraak in de leesapparatuur plus begrip van de werking tot op bitniveau. Alleen dan valt een Trojan horse te planten waarmee waarden zouden kunnen worden onderschept die van en naar de smartcard en vergelijkingseenheid gaan. Vervolgens zal een smartcard moeten worden omgebouwd om bij de biometrische hash van de compromittant de 'gewenste' toegangsrechten op te slaan.

Beide manieren van inbraak zijn niet eenvoudig, maar wellicht uitvoerbaar. En overigens waarschijnlijk eenvoudig te verijdelen.

Dit staat dan tegenover wachtwoorden die eenvoudig vervangbaar zijn (en die juist zo regelmatig moeten worden vervangen omdat ze zo eenvoudig compromitteerbaar zijn) en tokenkaarten die kunnen worden gestolen of verloren kunnen gaan maar die eenvoudig vervangbaar zijn.

* Kortom, eens houdt de beveiligingswedloop op, en wel daar waar die economisch niet meer rendabel is. En een verzwaring van de toegangsbeveiliging met (biometrische) zijnskenmerken kan er wel voor zorgen dat crackers, van welke vorm dan ook, eerder hun 'heil' bij uw concurrent zullen zoeken.

Overwegingen

De vele vraagtekens c.q. kritieke succesfactoren geven al aan dat de introductie van biometrie niet licht moet worden opgevat.
Het volgende geeft een kort overzicht van de overwegingen en vragen die bij de selectie en implementatie van biometrische toegangsbeveiliging aan bod zouden moeten komen (ontleend aan [ICSA99]). De volgorde van items is niet verplichtend.

Wilt u Fort Knox of wilt u alleen een pincodesysteem vervangen?

1. Wat zijn de redenen om biometrie te gebruiken en wat zijn de zakelijke argumenten en randvoorwaarden? De 'business case' dient voorop te staan in de tijd en naar belang. De redenen dienen zakelijk verantwoord te zijn. En budgetten en deadlines dienen vooraf duidelijk te zijn, om technisch gefröbel te voorkomen. En de namen van de sponsor, trekker en projectteamleden dienen te worden ingevuld.

2. Wat voor beveiliging wordt er nu precies vereist? Inventariseer alle huidige zwakke plekken in de beveiliging, zowel logisch als fysiek. Maar ook alle voorzienbare sterke en zwakke plekken als biometrie wordt ingezet, zullen moeten worden onderzocht; niet alleen gaat het om huidige fysieke locaties waar in de toekomst biometrische metingen zouden kunnen worden gestoord, maar ook allerlei locaties waar het wellicht niet mogelijk is meetapparaten beschikbaar te hebben. Denk aan de trend richting telewerken: als één van uw medewerkers zodadelijk met zijn/haar geïntegreerde GSM-palmtop aan het strand zit en nog even wat werkdingetjes wil afronden, is het wat onhandig om een zware gezichtswarmtebeeldcamera te moeten meeslepen – of vindt u het juist wenselijk dat de medewerker zichzelf niet in z'n privé-tijd belast met werk?

3. Welk beveiligingsniveau wordt gewenst? Wilt u Fort Knox of wilt u alleen een pincodesysteem vervangen? Hierbij dient met name een afweging plaats te vinden tussen de business case en de nader inschatbare baten (besparingen en beveiligingsniveau) en kosten.

4. Is een biometrisch hulpmiddel überhaupt wel nodig? Wellicht kan bij nader inzien een bestaande vorm van beveiliging (kennis en bezit), ter aanvulling of vervanging van het huidige systeem, net zo gemakkelijk het gewenste beveiligingsniveau bereiken.

5. Is er een onderzoek uitgevoerd onder de uiteindelijke gebruikers en wat zijn daarvan de resultaten? Ten minste zal moeten worden onderzocht wat de houding tegenover de interactie met biometrische apparatuur is, en hoe de opslag van biometrische en eventueel andere gegevens eruit gaat zien.

Eerlijke voorlichting zal essentieel zijn voor uiteindelijke acceptatie. Als het gebruik van biometrie simpel wordt voorgesteld en later een zware belasting blijkt, zal de acceptatie laag zijn. Eveneens lijkt het raadzaam het gebruikersonderzoek te herhalen als er tijdens het verdere implementatietraject belangrijke koerswijzigingen nodig zijn, bijvoorbeeld door de omschakeling naar een andere vorm van biometrie dan aanvankelijk was voorzien.

6. De functionaliteit van het biometrische systeem dient van tevoren helder te worden gedefinieerd. Aan een systeem dat authenticatie van (hoe?) aangedragen identiteiten moet verzorgen, dienen andere eisen te worden gesteld dan aan een systeem dat in een database dubbele identiteiten moet voorkomen.

7. Gegeven dat een biometrisch systeem wordt geïmplementeerd, wat zijn dan de resterende mogelijke vormen van inbraak? De inventarisatie van zwakten zal moeten worden gemaakt ongeacht de inschatting van de hoogte van de risico's. Die kunnen namelijk (te) snel veranderen als biometrie meer gemeengoed wordt; beveiliging is een wapenwedloop ...

8. Wie gaat het systeem onderhouden? Is dit een aparte functionaris, of wordt het beheer bij diverse functionarissen ondergebracht? Zijn de vereiste technische en systeemkennis en (op te bouwen) -ervaring bij die personen

aanwezig? Wie is verantwoordelijk voor technisch onderhoud en wat zijn daarvoor de noodzakelijke bevoegdheden op het systeem? Uitgangspunt zal meestal zijn het beheer met de huidige staf van medewerkers te doen, hetgeen dan een opleidingsbehoefte betekent die – niet te vroeg, niet te laat – moet worden ingevuld.

9. Hoe wordt toegang tot biometrische gegevens beveiligd en waar? Het systeem op zich dient ook te worden beveiligd, en wel zwaar. Duidelijk moet zijn welke gegevens de ronde doen en waar die zich bevinden – in database(s), datacommunicatie, smartcards, etc.

10. Wie heeft toegang tot de biometrische gegevens? Zijn er naast de systeembeheerders uit punt 8 nog anderen die toegang hebben tot de gegevens? Hiervan dient een apart register te worden bijgehouden. Nodeloos op te merken dat de toegang tot het biometrische systeem en de biometrische gegevens controleerbaar (auditable) moet zijn en dat sluitende controles meer dan ooit noodzakelijk zijn.

11. Wat is de definitie van de groep uiteindelijke gebruikers? Schattingen van zowel het initiële als het uiteindelijke aantal gebruikers moeten in kaart worden gebracht, en onderzocht moet worden of expliciete toestemming van die gebruikers nodig zal zijn (praktisch en juridisch). Indien nodig, bepaal dan tevens hoe die toestemming zal moeten worden verkregen. Indien niet, bepaal dan hoe de gebruikers zullen worden ingelicht over de introductie van het biometrische systeem.

12. Wat is het beste moment voor enrollment en wat is het beste moment voor latere metingen?
Bij het bepalen van het beste moment voor enrollment dient te worden nagegaan of de gebruikers er apart voor moeten opdraven of dat het mogelijk is de enrollment te doen als de gebruikers zich melden voor diensten c.q. toegang – waarbij rekening moet worden gehouden met speciale controles op de gewenste identificatie bij enrollment. Namen, adressen, paspoorten, etc. zullen uitgebreid moeten worden nagetrokken om te voorkomen dat malafide personen door de enrollment komen.
Bij latere metingen, in het dagelijkse gebruik, zal moeten worden bepaald hoe snel de meting en toegangsverlening moet worden uitgevoerd; triviale zaken als bijvoorbeeld té traag openende deuren – als de handpalmlezer te dicht op de deur is gemonteerd, maar (nota bene) ook als de centrale database 'te ver weg' is voor snelle communicatie en matching – staan uiteindelijke acceptatie in de weg.

13. Wat is de schaalbaarheid van het systeem? De databases met biometrische gegevens kunnen wellicht de groei van de gebruikerspopulatie niet aan, naar omvang en/of naar snelheid van matching. Ook is er een (hoewel niet zeer groot) risico dat bij een sterk groeiende gebruikerspopulatie het aantal gevallen waarbij twee biometrische waarden moeilijk onderscheidbaar zijn, zal toenemen.

14. Waar dienen de gegevens te worden opgeslagen: in een database of ergens anders (magneetstrip of smartcard)? Op basis van de punten 1-13 zal hierover een principebesluit moeten worden genomen.

15. Welke omvang en aantal van templates is nodig? Gegeven de opslagmethode kan worden bepaald hoe groot de template moet zijn (simpelweg in bits) om voldoende onderscheidend te zijn. Een op smartcard opgeslagen template hoeft niet groot te zijn (en kan dat niet) omdat latere matching toch verifiërend zal zijn bij andersoortige identificatie. Een andere factor is het (uiteindelijke!) aantal gebruikers; als dat klein is, kan de template ook klein blijven om toch nog voldoende onderscheidend te zijn. Is de uiteindelijke gebruikerspopulatie zeer groot (bijvoorbeeld een bevolkingsadministratie) dan zal de template evenredig groter moeten zijn om 'dubbelen' qua templatewaarde te voorkomen.

16. Wat is de uiteindelijke fysieke omgeving? Bij punt 2 hierboven was al even sprake van de meetomgeving die de uiteindelijke waarde van de inzet van willekeurig welk biometrisch systeem zal bepalen. De antwoorden op de vorige vragen meegewogen, kan een meer gedetailleerde analyse worden gemaakt. De niveaus van (en fluctuaties in) temperatuur, vochtigheid, luchtdruk, natuurlijk en kunstmatig licht, achtergrondgeluid, netwerkruis, vuil en algemene hygiëne van de persoon, vervuiling van de omgeving en van de meetapparatuur en stroomvoorziening, om er een paar te noemen, beïnvloeden de meting; wellicht zelfs te veel om nog nauwkeurig genoeg te kunnen meten. Een alternatieve biometrische techniek kan dan misschien soelaas bieden.

17. Wat zijn de karakteristieken van de gebruikerspopulatie? Leeftijd[6], geslacht, etnische achtergrond, beroep, hobby's[7], culturele aspecten en andere persoonlijke factoren spelen alle een rol bij de keuze voor en van een biometrisch systeem. Dergelijke informatie is echter bij uitstek privacygevoelig. Bovendien moet voorzichtig worden omgegaan met de soms indringende vragen en zal het doel van de vragen helder moeten worden uitgelegd.

18. Welke (potentiële) juridische aspecten spelen een rol? Dit kan betrekking hebben op de privacy rond de biometrische gegevens en/of de ermee samenhangende opgeslagen gegevens, zowel in opslag (al of niet afhankelijk van de opslag in een centrale database of decentraal op smartcards, etc.) als tijdens transport over netwerken. Kader 1 geeft een – niet uitputtend – overzicht van de diverse (nationale) kwesties die een rol spelen.

19. Wat zijn de bestaande (legacy-?) systemen waarop het biometrische hulpmiddel moet aansluiten? Hierbij zijn zowel operatingsystemen, hardware, applicatiesoftware, als netwerkcomponenten van belang. Een duidelijk punt: als de biometrische beveiliging nergens aan vast is te knopen, is zij van geen enkel nut.

20. Wat is de langetermijnlevensvatbaarheid van de leverancier(s)? Voorkomen moet worden dat de ondersteuning door de leverancier na korte tijd wegvalt, zeker als de punten 21 en 22 wat minder zwaar blijken te hebben gewogen ...

21. Welke API's kunnen worden gebruikt? Zoals hiervoor reeds werd aangegeven, zal moeten worden voorkomen 'locked in' te raken in de toevallige hard- en software van het moment.

6) Die mede bepalend kan zijn voor de veroudering van templatewaarden.
7) Bijvoorbeeld voor een gedragsherkenningssysteem dat 'persoonlijke' vragen stelt.

22. Kan een toekomstig (ander) biometrisch systeem gebruikmaken van dezelfde database? Of zou er opnieuw moeten worden begonnen en zou een volledige her-enrollment van alle gebruikers nodig zijn?

23. Welke meetmarges zijn acceptabel? Bovengenoemde punten 1-5 en met name punt 3 bepalen welke meetmarges, FAR en FRR zijn toegestaan. Het te selecteren middel moet deze natuurlijk kunnen leveren.

24. Is een evaluatie van meer dan één technologie of systeem nodig? Zo ja, selecteer dan de relevante technologieën c.q. systemen en test ze in testomgevingen.

25 Is een veldproef nodig? Meestal zal het antwoord 'ja' zijn. Zorg daar dan voor, maar let er wel op dat:
* de proef grondig is voorbereid en gepland, om de resultaten representatief en zinvol te kunnen doen zijn;
* de proef representatief is, dus met het beoogde voorlichtingsmateriaal en onder realistische omstandigheden. Als de groep gebruikers zich te geprivilegieerd voelt (op basis van bijvoorbeeld persoonlijke kwaliteiten uitverkoren) kan een te grote acceptatie worden voorgespiegeld. Ook de meetomstandigheden etc. moeten representatief zijn voor de toekomstige gebruiksomgeving;
* de proef voldoende kritische massa heeft. Als de proef te veel naast het gewone werk moet worden gedaan, zal de test wellicht te expliciet als een wetenschappelijke proef worden behandeld en zullen de resultaten te kritisch kunnen worden beoordeeld. Dit 'objectiveren', rationaliseren van de eigen bevindingen, kan zowel positieve als negatieve vervorming geven;
* een goede evaluatie wordt gemaakt van de proef, met beoordeling op vooraf vastgestelde criteria en meetmethoden. De proef moet niet worden gezien als een noodzakelijk kwaad waarvan bij voorbaat de uitslag vastligt, noch moet een minder dan perfect resultaat reden zijn alles maar af te blazen.

Als de biometrische beveiliging nergens aan vast te knopen is, is zij van geen enkel nut.

26. Na de proef: hoe nu verder? Eerst dient een go/stop-go/no-go-beslissing te worden genomen. Waarbij de stop-go-optie – een adempauze inlassen om verbeteringen door te voeren (inclusief hertest) – niet hoeft te worden vergeten maar juist een gunstige oplossing kan zijn. Vervolgens zal een gedegen planning voor de roll-out nodig zijn.

Afsluitend

Samenvattend kan worden gesteld dat de biometrische hulpmiddelen zo langzamerhand technisch volwassen genoeg zijn geworden om een betrouwbare extra beveiliging te kunnen bieden. Behalve enige duidelijkheid die nog moet worden geschapen over juridische aspecten, zal het erop aankomen, zoals altijd, de selectie en implementatie consciëntieus te doen.

Vervolgens zal dan het beheertraject volgens het boekje moeten zijn ingericht om tot een succes te komen; ook dat is niets nieuws. Vanaf dat moment kan dan iedereen weer op zijn of haar blauwe ogen worden vertrouwd. Of op face value, of ...

Literatuur

[AG99]
Automatisering Gids redactioneel, *Biometrie voor herkenning vingerafdruk*, week 31, 31 juli 1998.

[Amer99]
W. Amerongen, *Roodkapje: biometrist 'avant la lettre'*, Computable nr. 15, 16 april 1999.

[Anch99]
ZDNet AnchorDesk, *The Biometrics Revolution*, www.zdnet.com/anchordesk, 19 mei 1999.

[Aren99]
L. Arent, *Texas Fingers Welfare Fraud*, Wired News, www.wired.com/news/print_version/technology/story/21195.html, 10 augustus 1999.

[Bass98]
T.A. Bass, *Dress Code*, Wired nr. 4, april 1998.

[Bloo98]
Bloomberg, *Biometrics moves to the fore*, CNet News.com, www.news.com/News/Item/0,4,29019,00.html, 18 november 1998.

[Brig99]
P. Briggs, *Siemens Launches Secure PCs*, TechWeb/CMPnet, www.techweb.com/wire/story/TWB19990511S0027, 11 mei 1999.

[Brow99]
B. Brown, *Biometric Evolution*, PC Magazine Online, www.zdnet.com/pcmag/stories/reviews/0,6755,400287,00.html, 3 mei 1999.

[Byte98]
Byte redactioneel, *Smartcards in Action*, www.byte.com/art/9804/sec19/art3.htm.

[Clar99]
T. Clark, *Speech recognition takes off*, CNet News.com, www.news.com/News/Item/0,4,18767,00.html, 3 februari 1999.

[Cost99]
T. Costlow, *Stung by sticky fingers, biometrics regroups*, EETimes/CMPnet, www.techweb.com/se/directlink.cgi?EET19990426S0008, 26 april 1999.

[Cryp98]
Crypsys, *Biometrie; het lichaam als wachtwoord*, Crypsys Contact, winter 1998.

[Davi97]
A. Davis, *The Body as Password*, Wired nr. 7, juli 1997.

[Decl98]
F. Declerq, *Biometrie: wordt zelf je wachtwoord*, Computable nr. 45, 6 november 1998.
[Flyn99]
H. Flynn, *Biometrics and Digital Signatures for Authentication*, Gartner Advisory Research Note, 30 april 1999.
[Guld98]
J. Guldentops, *Computers houden niet van klamme handen*, CM Corporate nr. 116, 23 september 1998.
[Gunn99]
G. Gunnerson, *Are You Ready for Biometrics?*, PC Magazine Online, www.zdnet.com/products/stories/reviews/0,4161,386987,00.html, 8 februari 1999.
[Harr99a]
K. Harris, *Biometrics: An ATM Identification Replacement?*, Gartner Advisory Research Note, 5 april 1999.
[Harr99b]
K. Harris, *A Guide to Evaluating Biometrics*, Gartner Advisory Research Note, 28 april 1999.
[IBIA99]
International Biometric Industry Association, *Facts About Biometrics, the Biometric Industry, and IBIA*, www.ibia.org/understa.htm, 28 maart 1999.
[ICSA99]
International Computer Security Association, *The Biometrics Industry*, www.icsa.net, januari 1999.
[Kral99]
J. van Kralingen, C. Prins en J. Grijpink, *Het lichaam als sleutel, Juridische beschouwingen over biometrie*, ITeR – Centrum voor Recht, Bestuur en Informatisering, http://cwis.jub.nl/~frw/people/prins/bio-nl.htm, 1999.
[Kriz99]
H. Kriz, *Boosting Biometric Privacy*, Wired News, www.wired.com/news/print_version/technology/story/18810.html?wnpg=all, 30 maart 1999.
[Mile99]
S. Miles, *Firm unveils fingerprint ID system*, CNet News.com, www.news.com/News/Item/0,4,32381,00.html, 12 februari 1999.
[Mosk99]
R. Moskowitz, *Are Biometrics Too Good?,* Network Computing/CMPnet, www.techweb.com/se/directlink.cgi?NWC19990125S0017, 15 januari 1999.
[PCMa99]
PC Magazine editorial, *Biometrics: 007-Worthy Security*, www.zdnet.com/products/stories/reviews/0,4161,2199371,00.html, 8 februari 1999.
[Rand99]
N. Randall, *Biometrics Basics*, PC Magazine Online, www.zdnet.com/pcmag/stories/reviews/0,6755,392609,00.html, 22 maart 1999.
[Rice99]
J. Rice, *A Third Way for Biometric Technology*, IS Audit & Control Journal, Volume III, 1999.
[SanJ99]
San Jose Mercury News, *Bank will ID its customers by pattern of eye's iris*, SiliconValley.com, www.mercurycenter.com/cgi-bin/edtools/printpage/printpage.pl, 13 mei 1999.
[Stee98]
E. van der Steen, *Biometrie: betrouwbare en comfortabele toegangscontrole zonder belemmeringen*, Security Management nr. 9, september 1998.
[Verh99]
B. Verhoeven, *Het lichaam als barcode*, De Ingenieur nr. 8, 5 mei 1999.
[Viol99]
B. Violino, A.K. Larsen en B. Davis, *More Options For Tighter Security*, InformationWeek/CMPnet, www.techweb.com/se/directlink.cgi?IWK199990215S0027, 15 februari 1999.

Ir. drs. J. van der Vlugt RE heeft zich binnen de business unit Technology & Assurance gespecialiseerd in de beveiliging en audit van netwerken, met het accent op Windows NT-systemen. Hij is contactpunt voor de activiteiten van KPMG EDP Auditors op het gebied van het Jaar 2000-probleem en is betrokken bij research naar (toepassing van) nieuwe technologieën. Hij is redacteur van Compact en vaktechnisch coördinator van de postdoctorale EDP-auditopleiding aan de Vrije Universiteit Amsterdam.