

# **Verslag workshop C – Secure Identification Technology**

Sentinels Security dag, 29 september 2005, Amsterdam  
Dr.ir. Asker M. Bazen

## **Inleiding Raymond Veldhuis**

Raymond licht de kant van het onderzoek naar biometrie toe.

Topics van de workshop:

- biometrie (techniek, toepassingen),
- privacy enhancing technologies (template protectie),
- content identification (watermarking, fingerprinting),
- value-paper protection (watermarking, koppeling document aan persoon).

Secure identificatie van personen, processen, systemen, en content. In deze workshop ligt de focus on mensen, dus biometrie. Daarbij speelt met name fysische en logische toegangscontrole. Een apart probleem is biometrische surveillance, waarbij zwarte lijnen en tracking (anoniem) kan worden gebruikt.

Uitdagingen:

- Performance (error rates, grote databases doorzoeken),
- Robuustheid (slechte omstandigheden, niet meewerkende personen, spoofing),
- Privacy (diefstal van identiteit, gevoelige data),
- Integratie (toepassing, context, apparatuur).

Bedreigingen:

- ‘Problem solved’ syndroom: men denkt dat het al is opgelost,
- Te hoge verwachtingen, maar tegenvallende resultaten.

## **Inleiding Max Snijder**

Max licht de business kant van de biometrie toe.

De belangrijkste observatie is dat biometrie wordt omarmd door politici, gebombardeerd tot de oplossing voor terrorisme, etc.

De uitdagingen zijn:

- Impact van biometrie op business cases/modellen en processen, toegevoegde waarde,
- Biometrie als integraal onderdeel van beveiligingsoplossing,
- Implementeren van standaards,
- Realiseren / controleren conformiteit en interoperabiliteit.

De business drivers voor biometrie (of eigenlijk voor security) zijn de volgende:

- Security
- Convenience
- Efficiency

Daarnaast spelen er onderliggend overal juridische en privacy aspecten mee.

## Aanwezigen

De volgende personen waren aanwezig bij workshop C:

- Raymond Veldhuis, UT, onderzoek biometrie
- Max Snijder, BEG, biometrische consultancy
- Asker Bazen, UT, onderzoek biometrie
- Woelders, Senter, subsidies, veel security
- Hulsker, Integrated Engineering, contactless smartcards, ICAO advise passports
- Gedrojc promotie TU delft, matching biometrische templates
- Tangelder, CWI, gezichtsherkenning, toepassen op lq video.
- Bart Jacobs, RUN, software security, identity management, privacy management
- Alberts, RUN, coord. Wetensch. Samenwerking, reflectie op maatsch aspecten ICT, vertrouwen in systemen
- Miner, Trimbos, geestelijke gezondh. Zorg, hier meer consument
- Vereijken, internet bankieren
- De Jonge, VU, security en privacy, privacy vriendelijke km-heffing, legitimatie ipv identificatie, convenience van pin-code.
- Wegdam, lucent bell labs, identity management iha, privacy aspecten, context awareness
- Emmens, consument benadering
- Kanters, creeren van awereness binnen bedrijven
- Kuipers, LogicaCMG, identity management, biometrie
- Teeuw, Telematica instituut, kennis vertalen naar innovaties, maatschappelijke veiligheid, architecturen, gezichtsherkeening, patroonherkenning. Technische problemement, bedrijfsvoering, juridisch, acceptatie.
- Samson, banken, adviseur informatica, info beveiliging gezamenlijk voor banken, biometrie in niches bij banken, wordt op afstand gehouden, wel identity management. E-awareness. Europese (of wereldwijde) oplossingen
- Balash (), UT,
- Tom Kevenaar, Philips, crypto / biometrie
- Ton Akkermans, Philips, crypto / biometrie, security groep. Personalisatie, template protectie.
- Kuiten, IBM nederland, interesse in security
- Kuilenburg, Vicar Vision, gezichtsherkenning en analyse
- Ter Berg, Vicar Vision, software ontwikkeling.

Dit is op te delen in een aantal groepen: academisch onderzoek (9 personen) technologie ontwikkeling (6 personen), applicatie ontwikkelaars (2 personen), en gebruikers (5 personen).

## **Discussies**

### **Banken**

Samson: een onderzoeksvorstel neerleggen kan ik niet zomaar. Er bestaat momenteel veel afstand tussen wetenschap en bedrijfsleven. Ik kan wel vertellen waar banken mee bezig zijn, misschien vinden we dan raakvlakken. Voor banken is het vertrouwen het allerbelangrijkst, met name in het betalingsverkeer. Hierbij gaat het om de kaarten: de (magstripe) pinpas en de creditcard. De wereldwijde trend is het voorzien van kaarten van een chip volgens de EMV standaard. In Nederland wordt met de credit cards hiermee net begonnen. Een 4-cijferige pin is erg gebruiksvriendelijk. Het doel van de chip is security, hierdoor kan ook betalen op Internet veel veiliger. De chip zorgt voor weinig wijzigingen in functionaliteit, maar wel voor het veiliger maken van business.

Hulsker: is dit wel secure identification, of meer voorkoming van fraude? In geval van identificatie via Internet m.b.v. een calculator of chip wel. Hier worden symmetrische oplossingen gebruikt. Het doel is security introduceren en secure transactions faciliteren. Het is een handel waarbij 3 partijen betrokken zijn: bank, winkel, klant. Het probleem blijft identity management, hoe hou je het probleem onder controle. Je moet zeker weten dat klant is wie hij is. Wat mij betreft zou biometrie wel een goede oplossing zijn. Het begint interessant te worden als de false acceptance rate van de biometrie gelijk is aan de pin security, en dat geldt nu al voor veel biometriën. Verder speelt ook de volwassenheid van een technologie een grote rol. De ING heeft een experiment met vingerafdrukken gedaan bij banken in US. Dat draaide uit op een flop omdat de helpdesk veel te vaak nodig was, waardoor de kosten met een factor 10 omhoog gingen.

### **Applicatie Ontwikkelaars**

Wegdam: Lucent ziet zichzelf zowel als technologie als applicatie ontwikkelaar. Identity management is voor ons de hele reeks aan identificatie technologieën, via de telefoon, internet, etc. Een belangrijk punt is dat een gebruiker zijn identiteit niet wil doorgeven aan derde partij waarvan hij een dienst wil krijgen. De operator moet de identiteit van gebruikers afschermen na authenticatie, en slechts selectief info doorgeven aan de dienst providers. De vraag is hoe dit af te schermen, en hoe identificatie zonder een unieke identiteit of identifier door te geven. Dit raakt aan privacy. Daar bestaan wettelijke regels voor, en anders komt er geen user acceptatie. Bij diensten in commerciële segment heeft de gebruiker een keuze of hij er wel of geen gebruik van maakt. Ons doel is een systeem te bouwen zodat gebruiker de authenticatie accepteert, en een deel van zijn privacy opgeeft, maar wel grenzen kan stellen. Hij moet ook duidelijkheid hebben wie wat doet met zijn gegevens. Lucent wil op dit gebied graag applicaties ontwikkelen, bijvoorbeeld een global weather service. De operator weet waar ik ben (zodat ik een lokale weersverwachting kan krijgen), en wie ik ben (zodat hij weet waar de sms en

rekening heen moeten). Het KNMI hoeft niet te weten wie ik ben. Dezelfde persoon heeft in dat geval verschillende identities.

Hulsker: wat zijn de risico's als iemand anders er gebruik van maakt? Banken zeggen dat een bepaald percentage fraude niet erg is, want zo komen ze (door minder te investeren in security) op minimale kosten uit.

Wegdam: de truuk is om gepersonaliseerde diensten aan te bieden, zonder dat deze gegevens op straat liggen. Privacy is een gevoelig iets.

De Jonge: banken hebben vertrouwen van de consument. Dat zelfde zou kunnen gaan gelden voor je gegevens / privacy. Banken weten al veel over je geld, mobiele operators over je whereabouts. Het zou goed zijn een nieuwe dienst op te richten die privacy gevoelige gegevens beheert (trusted third party, TTP) en alleen wat nodig doorgeeft.

Wegdam: er zou onderzoek kunnen gebeuren naar privacy perserving identity management, waarbij de eindgebruiker controle heeft over alle informatie. Het is een soort ambient intelligence situatie: de informatie is overal, maar wordt toch beheerd.

Teeuw: Of de eindgebruiker bepaalt wie welke gegevens krijgt, of de TTP. Telecom operators willen deze rol graag krijgen.

De Jonge: Banken worden uitgezocht op vertrouwen, maar mobiele operators op kosten. Daarom zou het niet goed zijn als die TTP zouden worden.

Wegdam: Een onderzoeksvraag kan zijn het bouwen van een architectuur die hier mee om kan gaan.

## **Technologie ontwikkelaars**

Hulsker: Hoe zorg je er voor dat er interoperability is. Er komen elektronische paspoorten in 188 landen die lid zijn van de ICAO. Dat is echter alleen een adviesorgaan, en heeft geen beslissingsbevoegdheid. Experimenten laten zien dat de interoperabiliteit dan tegenvalt. Bijvoorbeeld aan een kant maken de Amerikanen zich druk over skimming, terwijl de Europese maatregelen er voor zorgen dat de wachttijden worden erg lang worden. Daarom komt elektronische identificatie niet van de grond. Geen vertrouwen per land om bepaalde standaard te accepteren. Bijvoorbeeld: China wil na SARS geen aanraking, en daarom geen vingerafdrukken. Interoperabiliteit bepaalt het succes van secure identification.

Snijder: er betaamt veel e-authentication standaardisatie binnen Europa. Een onderzoek zou die onder de loep kunnen leggen?

Vicar Vision: Wij zitten in de eerste fase van het technische werk. Gezichtsherkenning is gewoon een heel moeilijk probleem. Vingerafdrukherkenning is veel gemakkelijker, maar die systemen zijn te spoofen m.b.v. valse vingers. De vraag is: hoeveel laat je over

aan techniek, en hoeveel aan menselijke operator? Er is een politieke boost van biometrie, terwijl gezichtsherkenning in de kinderschoenen staat. Dat is gevaarlijk want een afbrandrisico voor techniek.

Snijder: Een belangrijke vraag is hoeveel je aan de technologie kunt overlaten. Wij doen project in Amsterdam, maar we hebben bewust vooraf geen performance claims gedaan. Er komen heel veel verschillende aspecten aan bod in dit project. Wat betreft de technologie zoeken we uit hoe je het het best kunt toepassen dat het in de praktijk werkt, en wat kunnen we nog aan technologie moeten verbeteren.

Vicar Vision: Onze demo werkt gegeneraliseerd over personen. We kunnen hem ook personaliseren op een persoon. Het is geen herkenning, maar wel analyse van kenmerken van gezichten (expressie, geslacht, ethniciteit, baard, leeftijd, etc). Onze technologie zou wellicht ook als basis voor herkenning gebruikt kunnen worden.

Akkermans: Wij hebben template protectie (privacy protectie) ontwikkeld, en we werken aan nieuwe biometrieën die meer accuraat zijn. Onze grote vraag is: hoe krijgen we dit verkocht. Bij de template protectie is het privacy aspect erg belangrijk. Maar ook dan is het moeilijk de consument zo ver te krijgen dat ze het willen kopen of gebruiken. Ons standpunt is: we zouden met overheden kunnen praten, maar we proberen gewoon te beginnen met consumenten elektronica producten. Bijvoorbeeld een afstandsbediening die je herkent en personalisatie toe past, maar daar zijn wel templates in opgeslagen. Een inbreker zou deze uit je afstandsbediening kunnen halen, en voor andere (veel zwaardere) toepassingen gebruiken. Via de consumenten elektronica markt proberen we de consumenten enthousiast maken voor deze technologie. Als deze weet dat het via privacy protecting technieken werkt, kan de publieke opinie deze techniek pushen voor grotere systemen.

Hulsker: In Nederland is de privacy bij wet beschermt. Amerika is dat anders, daar wordt alleen 1:1 verificatie gedaan. Je biedt zelf je vingerafdrukken aan op het moment dat je herkend wilt worden. Een centrale database wordt gewoon niet geaccepteerd. Er zijn 4 staten met biometrie op het rijbewijs, maar dat is allemaal 1:1.

Snijder: In Nederland was vroeger ook het advies altijd 1:1, maar nu zie je steeds vaker ook 1:n worden toegepast. In Europa wordt wel vaak om template protectie geroepen, en daar liggen ook grote kansen voor grote landelijke databases.

Hulsker: Juridische maatregelen zijn belemmerend voor effectieve grenscontrole.

Snijder: De banken houden biometrie op het moment ver af. In Noorwegen worden de paspoorten uitgegeven door banken, en komt het budget uit nationale loterij. Kun je op deze manier van bank geen service centrum maken, waarin ook diensten van buiten de bank worden aangeboden, zoals bijvoorbeeld een uittreksels uit het bevolkingsregister? En waarom banken ook niet tot TTP voor biometrieën benoemen.

Jacobs: Wat zijn hier precies de onderzoeksvragen? Bij privacy enhancing technologies zijn er wel veel geschikte onderzoeksvragen.

Snijder: En bepaalde contexten ben je meer bereid privacy concessies te doen, dan in andere contexten.

Wegdam: Wat is het risico op uitlekken, en aan wie geef ik de gegevens?

Wegdam: Bluetooth en RFID zenden nummer uit, en zijn per definitie privacy schendend.

Jacobs: De oplossingen zijn meerdere identiteiten, certificaten, challenge response, betere protocollen.

Emmens: Wie heeft wat gedaan? Als het uitlekt wil ik weten wie daar verantwoordelijk voor is. Dat heeft te maken met vertrouwen. Ik ga pas ergens heen als ik weet dat ik ze kan vertrouwen.

Jacobs: De gegevens opslaande partijen hebben beheersprobleem. Apothekers beheren ook interessante databases. Hier zijn meer technische maatregelen nodig. De privacy discussie is vaak gebaseerd op mening gebruikers, maar de overheid zou zich er drukker over moeten maken vanwege identiteitsroof. Dan kun je je niet veroorloven. Daarmee is privacy bescherming meer dan individuele zaak. Je moet er meer beleidsmatig tegen aan kijken: grote databases geven een groot gevolg aan identiteitsroof, en dat moet je goed beschermen. Beleid kan technologie gestoeld zijn en technologie pushen.

De Jonge: Privacy en security zijn vaak moeilijk te combineren. Een oplossing is volledig gedistribueerde databases, iedereen heeft / beheert zijn eigen gegevens. We moeten ook zeker geen elektronische patienten dossiers introceren! Als je bewusteloos bent kan notaris best beslissen welke gegevens de dokter mag zien. Het praktisch probleem is wel wie de gemachtigde personen zijn.

Snijder: Je verplaatst daarmee het risico naar het pasje (verlies etc). Heel vaak moeten er gegevens worden geraadpleegd. Hoe vaak wordt je dan gebeld voor info?

Jacobs: Distributie versus privacy (bij het elektronisch patienten dossier) is een goede research vraag.

De Jonge: Dit zou vanuit de overheid moeten komen: hoe combineren we security en privacy?

Jacobs: Sentinels problemen zijn meer lange termijn.

Hulsker: overheden hebben niet genoeg expertise, daarom versnipperd het.

## Kennisinstellingen

Veldhuis: De kennisinstellingen gaan vertellen wat ze willen, daarna kunnen we de matches bekijken. Een voorbeeld (van de UT) is werken performance verbetering. Dat onderwerp is in principe te, maar als je daarmee iets nieuws mogelijk kunt maken is het wel interessant. Voorbeeld in de surveillance zou je kunnen werken aan performance, de context, het aantal camera's, meer realisaties een gezicht, minder last van pose etc. Dan kan gezichtsherkenning wel in surveillance worden toegepast.

Tangelder (CWI): Wij gaan werken aan de combinatie van beeld en geluid, waardoor we low-quality video voor biometrie identificatie kunnen gebruiken. Dit idee is ontstaan vanuit het Basis project (biometrie@home). We willen een gezicht van 20x20 pixels herkennen, en combineren met het geluid uit een ook microfoon. Dit gaan we toepassen in studentenhuizen en forensisch. Het project wordt ingediend samen met het NFI. Beelden van bewakingscamera's kunnen zo worden gebruikt voor automatische opsporing van verdachten. Daarnaast gaan we werken aan probabilistische modellen, om zo de rechter te overtuigen van de zekerheid van de automatische identificatie. Daarnaast gaan we de camera's in pin-automaten gebruiken voor gezichtsherkenning. De template komt op de bankpas, zodat er geen privacy probleem is. En als een pas gestolen is kan deze niet meer worden gebruikt. Ook werken we aan een biometrische mobiele telefoon die een persoon herkent aan de hand van geluid en beeld. Tot nu toe gaat gezichtsherkenning redelijk bij hoge resolutie, maar na 4 jaar onderzoek werkt het ook goed met lage resolutie beelden van 20x20 pixels.

Veldhuis: De fit met Sentinels moet zitten in de applicaties.

Hulsker: Veel vertragingen van vliegtuigen ontstaan doordat passagiers te laat bij de gate komen. Hier zou je gezichtsherkenning moeten toepassen voor het opsporen van missende passagiers op de luchthaven.

Snijder: De combinatie gezicht en iris kan veel performance verbetering brengen, met name bij video surveillance. Je kunt van afstand inzoomen op de iris.

Wegman: Gezichtsherkenning is een privacy violating biometrie, want de gebruiker heeft geen controle op wie je probeert te herkennen.

IBM: Binnen ons bedrijf hebben we te maken met steeds meer verschillende user IDs en passwords. Je moet ze allemaal maar onhouden, continu veranderen, etc. Mijn vraag is: hoe kun je dat goed beheren, zou bijvoorbeeld single sign-on een goed idee zijn?

De Jonge: Het zou interessant is om het gebruik van pincodes aan te pakken. Die kun je zo gemakkelijk afkijken, en pincode management is nog een probleem. Identity management is voor mij niet authenticatie. Praktisch gebruik van dingen die er zijn, maar is dat onderzoek of roll-out? Waarom bestaan er geen apparaten waarin alle pins in kunnen? Het nadeel is: als je device kwijt bent, ben je alle codes kwijt.

Hulsker: door biometrie ben je al dat gezeur kwijt. Waarom willen banken er niet aan?

Jacobs: Biometrische identificatie betekent hetzelfde als overal hetzelfde password gebruiken. Dus toepassing van biometrie is vanuit een security standpunt het stomste wat je kunt doen. Bovendien laat je je biometrieen overal achter.

De Jonge: Elke techniek is kwetsbaar. Je zou altijd alle 3 elementen moeten gebruiken: wat je hebt, wat je weet, en wat je bent. Pas dan haal je de hoogste veiligheid. Het hangt nog wel van de applicatie af.

Hulsker: vinger en gezicht zijn ontzettend onbetrouwbaar, de iris is veel beter.

Samson: biometrie is het derde kenmerk voor banken, dus we gaan de pas en de pin zeker niet vervangen.

Jacobs: In de eerste ronde is vooral actief gewerkt vanuit kennisinstellingen, die hebben bedrijven benaderd, etc. Dat heeft wel goede voorstellen opgeleverd. Het zou mooi zijn als het in tweede ronde vooral vanuit bedrijfsleven komt. Ik ben sinds kort ook 1 dag per week in Eindhoven aan het werk, waar ik me op ID management wil richten op protocol-niveau. Ik ben minder geïnteresseerd in biometrie op zich, daarvoor moet je in Twente of bij Philips zijn. Op protocol niveau kun je onderzoeken wat anonimiteit is. Mensen beschermen zichzelf als het niet vanuit overheid of systeem gebeurt. Mijn onderzoek zal gericht zijn op pseudo-identiteiten, tickets, in combinatie met template protectie, tijdelijke templates, etc. Protocollen moeten wel eerst bedacht en doordacht worden. Het is naïef om altijd alles vast te leggen, dat is nergens voor nodig. Veel transacties kunnen met veel minder informatie gedaan worden. We moeten nadenken over de vraag wat in welke situatie nodig is om weg te geven. Een interessang voorbeeld hiervan is de kilometer heffing. Het voorstel van Roel Pieper was om auto's uit te rusten met gps en gsm, en alles door te geven naar een centraal punt. Het is echter gevoelige informatie waar auto's geweest zijn. De oplossing was het definiëren van verschillende kleuren wegen met verschillende tarieven, en de ritten in de auto bij te houden. Dan hoef je alleen door te geven zoveel km op rode weg, zoveel op groene weg, etc is gerenden.

De Jonge: Als je iets nieuws wilt invoeren, moet je privacy goed in de gaten houden, anders is iedereen tegen.

## **Wrap-up**

Veldhuis: Biometrie is een herkennigstechnologie. Als je in staat bent te investeren in performance verbetering, ontstaat er dan een andere vraag in de wereld? Omgekeerd: wat zou je beter willen zien?

Snijder: Live and wellness detectie. Dan is er een zwak punt opgelost, en worden nieuwe toepassingen mogelijk. Dit is bijvoorbeeld een blokkade voor thuisgebruik. Voor veel toepassingen is dit het belangrijkste obstakel. Het is een wedloop, maar je moet hem wel aangaan. Als live detectie mogelijk is, ontstaat er een grote window of oppurtunities.

Wegdam: Het is juist de uitdaging om live detectie goedkoop te maken.

Hulsker: Welke identificatie middelen moet je samenvoegen voor combinatie van acceptabele performance en lage kosten. Je moet segmenteren: welke combinatie voor welke applicatie in welke context.

Akkermans: Wij zoeken naar biometrieën die zo moeilijk na te maken zijn.

Snijder: De definitie van acceptabele error rates is volledig afhankelijk van de toepassing. Dan hoeft niet altijd bijna 100% herkenning te zijn.