



biometric TECHNOLOGY TODAY

ISSN 0969-4765 November/December 2010

www.biometrics-today.com

CONSUMER

Fingerprint verification wins consumer trust

Consumers trust fingerprint biometrics over photo identification, PIN numbers or handwritten signatures to verify their identities when using a credit card or requesting personal information, according to a poll by Unisys Corporation.

Unisys has heralded the results of the poll as an indication of an apparently increasing consumer acceptance of biometric technologies to secure financial transactions and combat identity fraud.

Responding to the question, "Which do you believe is the safest method to prove your credit

card is being used by you?" the online poll found that 63% of more than 300 respondents preferred fingerprints as the best method for identity verification and authentication, compared to photo identification (20%), PIN numbers (13%) and handwritten signatures (6%).

Also in a move marking further consumer acceptance of fingerprint id technology, Ceelox is to offer its products to consumers via Amazon.com. The company's initial offering will be its Ceelox ID(R) PC Edition coupled with a fingerprint biometric sensor. Each user authenticates their identity via fingerprint scanner.

RESEARCH

Madrid scientists research spoofing

Scientists from Carlos III University of Madrid (UC3M) are analysing possible attempts at fraud in biometric identification systems to improve the security of facial, iris, fingerprint or vascular recognition.

The research aims to evaluate the strength of biometric systems in the face of various types of attacks, and create algorithms, devices and collateral techniques and usage policies that avoid and detect these attempts at fraud.

"We are working very intensely on the ocular iris as well as written signatures, although

previously we have worked on fingerprints, and in the near future we will be working on facial recognition," says a representative from UC3M's Electronic Technology Department.

Research on sources of noise and the most common falsifications in recognition systems based on iris identification has concluded that the robustness of the recognition algorithm and the inclusion of antifraud mechanisms in it are essential to keeping falsifications such as impressions of photographs of the iris, prostheses, or contact lenses from successfully violating the security of the systems.

IBIA slams NRC report summary as inaccurate

The International Biometric and Identification Association (IBIA) has slammed the National Research Council (NRC) report summary 'Biometric Recognition: Challenges and Opportunities', charging it with creating an inaccurate and outdated impression that biometrics is flawed and not ready for general use.

The IBIA points out that experience over the past decade has shown that 'biometric technology significantly enhances the effectiveness of many identity-based systems and constitutes an important tool in protecting our borders, reducing entitlement fraud, enforcing our laws, securing networks and facilities and protecting personal information from unauthorised access'.

Continued on page 2...

Contents

News

Fingerprint verification wins consumer trust	1
Madrid scientists research spoofing	1
IBIA slams NRC report summary as inaccurate	1
Accenture goes large scale with id matching	2
Finger and face secure access to mobile phones	2
Iscon enhances body image scanner	3
New Zealand to trial biometrics as US immigration hails success of programme	3
UK plans to capture biometric data of visa extension applicants	3
Stork pilots set a course for id interoperability across Europe	3
eGo shows its first prototype	12
Pilot licences stall while driving licences get face recognition	12

Features

Mobile boost for voice adoption	
Development of mobile-based security solutions may represent a key moment for voice biometrics, finds Benoit Fauve of ValidSoft.	5
Military biometrics on the frontline	
Steve Gold provides an update on how biometric technology is being used and developed by the military.	7
Signature and gesture – dynamic biometrics for remote login	
Jeff Maynard, Biometric Signature ID, examines dynamic biometrics for remote login.	9

Regulars

Events Calendar	3
News in Brief	4
Product News	4
Company News	4
Comment	12

Photocopying

Single photocopies of single articles may be made for personal use as allowed by national copyright laws. Permission of the publisher and payment of a fee is required for all other photocopying, including multiple or systematic copying, copying for advertising or promotional purposes, resale, and all forms of document delivery. Special rates are available for educational institutions that wish to make photocopies for non-profit educational classroom use.

Editorial Office:

Elsevier Ltd
The Boulevard
Langford Lane
Kidlington
Oxford OX5 1GB, UK
Fax: +44 (0) 1865 843973
Email: tracey.caldwell@btconnect.com
Website: www.biometrics-today.com

Publisher: Laurence Zipson

E-mail: l.zipson@elsevier.com

Editor: Tracey Caldwell

Email: tracey.caldwell@btconnect.com

Production Support Manager: Lin Lucas

Email: l.lucas@elsevier.com

Subscription Information

An annual subscription to Biometric Technology Today includes 10 printed issues and online access for up to 5 users.

Prices:

€998 for all European countries & Iran

US\$1080 for all countries except Europe and Japan

¥132 700 for Japan

(Prices valid until 31 December 2010)

To subscribe send payment to the address above.

Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971

Email: commsales@elsevier.com,

or via www.biometrics-today.com.

Subscriptions run for 12 months, from the date payment is received. Periodicals postage is paid at Rahway, NJ 07065, USA. Postmaster send all USA address corrections to: Biometric Technology Today, 365 Blair Road, Avenel, NJ 07001, USA

This newsletter and the individual contributions contained in it are protected under copyright by Elsevier Ltd, and the following terms and conditions apply to their use:

Permissions may be sought directly from Elsevier Global Rights Department, PO Box 800, Oxford OX5 1DX, UK; phone: +44 1865 843830, fax: +44 1865 853333, email: permissions@elsevier.com. You may also contact Global Rights directly through Elsevier's home page (www.elsevier.com), selecting first 'Support & contact', then 'Copyright & permission'. In the USA, users may clear permissions and make payments through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA; phone: +1 978 750 8400, fax: +1 978 750 4744, and in the UK through the Copyright Licensing Agency Rapid Clearance Service (CLARCS), 90 Tottenham Court Road, London W1P 0LP, UK; phone: +44 (0)20 7631 5555; fax: +44 (0)20 7631 5500. Other countries may have a local reprographic rights agency for payments.

Derivative Works

Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution. Permission of the Publisher is required for all other derivative works, including compilations and translations.

Electronic Storage or Usage

Permission of the Publisher is required to store or use electronically any material contained in this journal, including any article or part of an article. Except as outlined above, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the Publisher. Address permissions requests to: Elsevier Science Global Rights Department, at the mail, fax and email addresses noted above.

Notice

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made. Although all advertising material is expected to conform to ethical (medical) standards, inclusion in this publication does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

02265

Pre-press/Printed by
Mayfield Press (Oxford) Ltd.

...Continued from front page

It provides a number of examples of successful deployments ranging from commercial to defence in support of its argument.

The IBIA believes that the NRC report's press release and summary highlighting the probabilistic nature of biometric matches as a key weakness of biometric systems is unhelpful as, the IBIA argues, similar uncertainties exist in other automated identification mechanisms such as PINs and passwords.

INDUSTRY

Accenture goes large scale with id matching

Accenture has unveiled a new large-scale biometric identity matching solution to help public service agencies verify the identity of individuals, whether for the purposes of detecting potential national security threats or for improving the delivery of benefits and services.

The solution is able to de-duplicate all identity data including biographic and, if available, biometric data.

Cyrille Bataller, director for Accenture Technology Labs Europe, told BTT the solution builds on the work Accenture has done in large scale matching at US-Visit, with the EC to support biometric visas and in India with the Unique ID authority (UIDAI).

"What we have seen in the biometrics space is an evolution of requirements from the demands of criminal investigations in the Eighties and Nineties to the first implementations for visas to increase security of border control. What we are seeing now is a third generation of requirements for projects like Unique ID in India where the scale is an order of magnitude larger than the IDENT database for US-Visit which we operate, where response times need to be real time and availability is paramount," says Bataller.



University of Manchester face tracking on a Nokia N900 mobile.

Accenture's large scale matching approach is a key component of the virtual labour market systems developed in Germany and France. These systems feature search and match capabilities to link worker profiles with the requirements of open jobs to match job seekers with job offers.

MOBILE

Finger and face secure access to mobiles

Biometric access to mobile phones is progressing on commercial and academic fronts. AuthenTec has launched its TrueSuite Mobile mobile identity management software while scientists at the University of Manchester have developed software for mobile phones that can track facial features in real time.

At present the Manchester-developed software does not offer recognition but the hope is eventually it will be able to tell who the user is, where they are looking and how they are feeling.

Scientists believe their method is unrivalled for speed and accuracy and could lead to facial recognition replacing passwords and PIN numbers to log into internet sites from a mobile phone.

Phil Tresadern, lead researcher on the project says, "Our model runs in real time and accurately tracks a number of landmarks on and around the face such as the eyes, nose, mouth and jaw line.

"A mobile phone with a camera on the front captures a video of your face and tracks 22 facial features. This can make face recognition more accurate, and has great potential for novel ways of interacting with your phone."

The software, built on 20 years of research at the university, has been demonstrated on a Nokia N900 mobile phone for the EU-funded Mobile Biometrics (MoBio) project.

AuthenTec's TrueSuite Mobile mobile identity management software is available now, designed to enhance the features and functions of AuthenTec smart sensors in mobile phones. TrueSuite Mobile facilitates applications that allow users to log in to mobile apps with the swipe of a finger.

TrueSuite Mobile includes a simplified API, designed for the application developer community to facilitate biometric feature access and secure management of passwords and PINs. It is compatible with multiple mobile operating systems including Android, Windows Phone 7 and Symbian.

PRODUCTS

Iscon enhances body image scanner

Isccon is introducing an enhanced version of its 1000D whole body scanner equipped with optional biometric technologies and identity verification techniques.

The Iscon body imaging portal uses thermo-conductive infrared technology to complete a 360 degree scan in 30 seconds without penetrating clothing, so there are no privacy or radiation issues. It can detect the thermal imprint of objects such as thin plastic, wood, powder, pills and drugs paper money, liquids and ceramics.

E-BORDERS

New Zealand to trial biometrics as US immigration hails success of programme

Imigration New Zealand has announced a trial biometric programme to confirm the identity of New Zealand visa applicants and first time travellers to the country. This comes as US Immigration and Customs Enforcement (ICE) announced it has removed more illegal aliens in fiscal 2010 than in any other period and attributed this largely to its biometrics programme.

The New Zealand Immigration department plans to incorporate biometric technology in its new immigration management system that is expected to cost more than \$60m.

Immigration New Zealand is working with Australian biometric firm Daon to evaluate whether the use of technology to capture biometric data at the visa application stage and at the border would speed passenger processing.

The Immigration Act 2009, which will come into effect in November 2010, allows the department to collect biometric data to verify identities and prevent immigration and visa fraud. The trial is expected to start soon and last 10 months.

In the US, ICE removed more than 392,000 illegal aliens, more than 195,000 of whom were convicted of crimes, including murder, sex offences and drug violations. The ICE-led programme, Secure Communities uses biometric technology to identify aliens who have been booked into state and local jails. Once identified,

these criminal aliens are processed for removal rather than released back into communities.

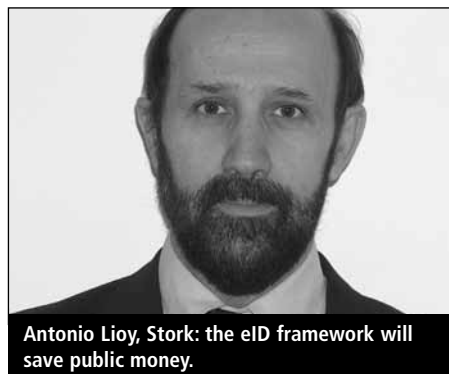
UK plans to capture biometric data of visa extension applicants

Migrants who apply to extend their stay in the UK will need to enrol their fingerprints and photograph as part of their UK visa application from 14 December 2010, if proposed regulations get the green light.

Under Tier 1 or Tier 5 (temporary worker) of the points-based system migrants need to apply to permission to stay and are currently provided with stickers or vignettes in their passports.

The government plans to set up biometric enrolment centres with facilities at a limited number of post offices. The passport agency will take a digital photograph of a person's face and scan fingerprints.

EUROPE



Antonio Lioy, Stork: the eID framework will save public money.

Stork pilots set a course for id interoperability across Europe

Stork has made six pilots available for public access. The Stork project sets out to implement an EU-wide platform for interoperability of electronic identities (eIDs) via electronic cards or 'other means'. In a separate European eID development, German citizens have this month started to receive ID cards containing biometric details, which will allow them to identify themselves on the internet and to authenticate digital signatures.

The six Stork pilots are 'cross border authentication for electronic services'; 'SaferChat'; 'student mobility'; 'cross border eDelivery'; 'change

Continued on page 12...

EVENTS CALENDAR

5-10 December 2010

Florianopolis, Brazil

XXVth International Biometric Conference

Organised by the Brazilian and Argentinean regions of the International Biometric Society. Held at Federal University of Santa Catarina.

More information: www.rbras.org.br/~ibcfloripa2010/

7-9 December 2010

Paris, France

Cartes & Identification

The 25th CARTES trade show covering payment and e-money, bringing together the digital security, payment and contactless community.

More information: bit.ly/bttev-psc-can

10 December 2010

Wellington, New Zealand

NZ Member Meeting

Hosted by New Zealand Customs Service.

More information: member@biometricsinstitute.org

9-10 December 2010

Brussels, Belgium

RISE Multi-stakeholder Conference "Ethics and governance of biometrics and identification technologies"

The EU funded initiative RISE is convening the multi-stakeholder conference which will advance and further promote stakeholder involvement including regulators, responsible agencies, lawmaking bodies, industry, third party privacy solutions providers and consumer representatives in setting technology security policy in Europe. High-level speakers from policy, research, industry and from user groups will address the conference, that will be held in conjunction with the HIDE project final conference.

More information: <http://bit.ly/8XfsDC>

15-17 March 2011

Singapore

Global Security Asia

The fourth GSA event focuses on counter terrorism in the region. The event is supported by the Biometrics Institute.

More information: www.globalsecasia.com

29-31 March 2011

AsiaWorld-Expo, Hong Kong

CARTES in Asia

Event for the identification industry in the Asia Pacific region with a focus on biometrics.

More information: www.cartes-asia.com

4-6 April 2011

London, UK

Security Document World 2011

This event brings together the full industry spectrum including anti-counterfeiting experts, passport-issuing agencies, immigration officials, customs, police, civil aviation and other border control and security authorities.

More information: www.sciencemediapartners.com

6 April 2011

Wellington, New Zealand

Biometrics Institute New Zealand, 7th Conference

This one-day event will provide an insight into the latest developments in biometric technologies. Free to attendees of 'Applying Biometrics' course on 4-8 April.

More information: <http://bit.ly/cab6v6>

NEWS IN BRIEF

BIO-key International, provider of finger-based biometric identification solutions for the healthcare industry, and Medflow electronic health records software developer dedicated to eye care physicians, have announced the release of TruStaff fingerprint biometric login for securing access to Medflow Electronic Health Records (EHR).

Northrop Grumman Corporation and the US Department of Homeland Security's Federal Emergency Management Agency (FEMA) coordinated a nationwide demonstration deploying a common, interoperable credentialing system that enables electronic identity authentication for government and industry personnel. The demonstration, called 'Autumn Blend', was of standardised personal identity credentials operating across multiple domains, such as a government's or company's credential authentication infrastructure, for access management decisions, situational awareness, cyber-secure capabilities and post-event reconstruction. Participants included federal, state, local, and private sector emergency response and recovery officials who are assigned to the front lines for rescue or recovery missions.

MaxID Corp has received two new certifications from the Federal Bureau of Investigation (FBI) for its iDL500 device. The FBI has certified the unit for mobile and fingerprint capture specifications.

Fingerprint Cards AB (FPC) has won the 2010 Frost & Sullivan Europe Product Line Strategy Award in Fingerprint Verification Components and Systems. FPC focuses on its core technology of fingerprint biometrics.

According to the Australian *Port Macquarie News*, ID cards enabled with smartcard and biometric technology will be used with flash drives to monitor a gambler's progress on electronic poker machines, which will be fitted with fingerprint scanners to verify identification.

PRODUCT NEWS

Epicor is introducing biometric POS sign-on via integration with DigitalPersona's UrU fingerprint biometrics. Retailers can leverage fingerprint identification for user authentication, manager authorisation of transactions, and staff time clock activities, reducing unauthorised overrides and preventing 'buddy punching' where staff clock in for each other.

Sarnoff Corporation and ePortation have demonstrated the Glance iris recognition system for high-speed biometric identification at ports and

other critical infrastructure. Using Sarnoff's iris image capture system that images the iris of a person in motion and at a distance, the system offers high-speed identity verification in the harshest outdoor climates. Combined with ePortation's real time access and rule management solutions, the system allows a facility to be secured according to local policies while linking multiple site locations for an overall view of access activity.

Fujitsu Frontech North America has integrated its PalmSecure palm vein biometric authentication technology with the Crystal IT Avert Access Control system. The joint solution combines biometrics and RFID technologies to deliver endpoint security for individual workstations, preventing unauthorised user access, protecting proprietary information, and eliminating passwords. Fujitsu Frontech has recently implemented PalmSecure at Vantage Data Centers' Santa Clara campus. Vantage Data Centers provides energy-efficient, scalable, wholesale data center solutions to enterprise customers.

Morpho has won a Security Innovation Award for its MorphoSmart Finger VP, the multimodal finger vein and fingerprint device.

ValidSoft has introduced VALid fraud prevention technology for combating malicious cyber attacks that captures passwords, account numbers, and other data used to log onto online banking accounts. VALid offers a mutual, multi-factor authentication and transaction verification process that combats fraud across multiple banking channels (web, phone and call centre). It protects banks' customers that use online banking, mobile banking, telephone banking and contact centres.

MobileFrame has announced the release of the MobileFrame Healthcare Application Suite. This suite of mobile applications enables any size of healthcare organisation to eliminate paper-based data collection. All the applications provide the ability to securely collect rich data types including digital photos, barcode scans, digital signature capture, sketches, voice notes, GPS, RFID and biometrics.

Neurotechnology has released MegaMatcher Accelerator 3.0, a packaged multi-biometric software and hardware solution for high volume, high-speed fingerprint and iris identification. This latest version of MegaMatcher Accelerator includes very fast iris matching capabilities of up to 200m irises per second, with increased fingerprint matching speeds of up to 100m fingerprints per second. Either iris or fingerprint modes can be used as primary, fast-identification biometrics, or

both can be used together for more accurate multi-biometric identification. Additionally, MegaMatcher Accelerator can check identification results with other biometric data from any Neurotechnology-supported modality, including fingerprint, iris, face or palmprint, for applications such as voter duplication detection, passport issuance, border crossings or other national-scale projects.

COMPANY NEWS

Kratos Defense & Security Solutions is to acquire homeland security solutions provider Henry Bros. Electronics. HBE is a leading pure play provider of homeland security solutions, products and system integrations services, including the design, engineering and operation of command and control systems for the protection of strategic assets and critical infrastructure in the US. HBE also has particular expertise in the design, engineering, and deployment of specialised surveillance, thermal imaging, analytics, radar, and biometrics technology based security systems. The purchase price will be approximately \$45m in cash, or \$7 per HBE share of common stock.

SAB is setting up a network of European authorised dealers. SAB is a Spanish company devoted to the research, manufacture and marketing of biometric solutions. It works with ADI Global International and EULEN Security in Spain and Portugal. The City Police of Valencia has recently implemented SAB products.

Bayometric's fingerprint-based biometric visitor registration solution helped the Vishvas Foundation, a non-profit, educational foundation, improve its registration process helping in quicker identification of attendees. The visitor attendance platform runs on VB6 and SQL Server. The second phase of the project will see data centralised on a secured server. Once this is done, automated handheld devices with identification modules will also be used as part of the system.

Science Applications International Corporation (SAIC) has been awarded a follow-on contract by the US Department of Defense (DoD), Biometrics Identity Management Agency (BIMA) to continue providing biometric support services to the US Central Command's area of responsibility. The task order has a total value of more than \$23m. Collecting and registering personnel into biometric databases is key to helping identify insurgents. SAIC will provide the US military and coalition partners with biometric enrolment support at entry ports throughout Iraq.

Mobile boost for voice adoption

Benoit Fauve, ValidSoft



Benoit Fauve

Many indicators – market growth, number of players, new deployments – show that voice biometrics has turned into an established market. But despite this positive evolution and welcome maturity, it seems that little has changed when voice biometrics is brought up in conversation; responses are either over-optimistic or negative.

Voice biometrics is gaining ground but despite some interesting examples, it has not reached the point of widespread use yet. Historically business implementation of voice biometrics has been difficult. In the case of secure authentication, practical applications call for short duration testing, typically repeating a passphrase a few times when enrolling a voiceprint and repeating that passphrase when authenticating. With some early pilots for financial institutions based on too-simple solutions and too-difficult conditions, it has sometimes been perceived as not robust enough. It is fair to say that some first trials have not met early and probably unreasonably high expectations, especially when the voice check is based only on a short passphrase.

More recently, with closer work between biometrics and security providers, voice biometrics has developed alongside existing solutions, rather than as a replacement. A key element for success is a better understanding of the balance between the level of security needed and the convenience that the biometric technology brings. A good example of a new real life implementation comes from the call centre service at Australian Health Management (AHM), where a voice check is performed (callers say their customer number) prior to transferring calls to an operator.

“Recent developments have seen the appearance of mobile-based solutions to secure online channels”

Traditional authentication methods are still used if the check is unsuccessful. In this case voice biometrics fit with the existing solution. The productivity gain and ROI are in the reduction of time spent by the operator doing identity checks, not the total suppression of the time needed for traditional checks.

Voice is now part of wider security solutions that are multi-factor, multi-channel and multi-layered. Recent developments have seen the

appearance of mobile-based solutions to secure online channels. With mobile phones being a natural fit for voice biometrics this may mark a market shift for biometrics.

The second part of this article will describe in more detail these new mobile-based solutions and the multi-factor and multi-layered security approaches, in order to further understand where the opportunities for voice biometrics lie. But first this paper will discuss some very interesting recent developments in the core technology.

Research challenge

Speech technology in general, including speech recognition and speaker recognition, is an area of research that has been extensively studied over the past five decades. Consequently voice is one of the most researched biometric modalities, with initial studies starting long before the relatively recent interest in biometrics.

In recent years a predominant stimulus for research came from the US Governmental bodies Linguistic Data Consortium (LDC) and the National Institute of Standards and Technology (NIST), who respectively collect large-scale speech databases and organise regular independent evaluations of speaker verification systems.

In this context state of the art approaches have improved dramatically over the past few years. Progress has been made through sophisticated modelling obtained from large speech databases where speakers are recorded over several sessions and different days. With example recordings of hundreds of speakers, variations in the voice signal are estimated and neutralised, making the full speaker verification process more robust.

Given that the ‘long task’ (involving minutes of conversation in the voice print enrolment and testing) is a compulsory condition for NIST evaluation entry, inevitably this condition has received by far the greatest attention in the literature. However, commercial and practical situations call for speaker verification using much shorter speech durations.

Over the past few years some publications have started to focus on the difficulties of accommodating these new techniques to more challenging real world conditions when only seconds of speech are involved.

“Some publications have started to focus on the difficulties of accommodating these new techniques to more challenging real world conditions when only seconds of speech are involved”

Of great interest are some isolated initiatives making interesting complements to NIST evaluations, first by being closer to real world applications and by offering new languages and recording conditions to test newly developed techniques.

Among others, Evalita is an interesting evaluation with speech in Italian language and some short testing conditions. A more recent example is Mobio, an EU-funded FP7 project with an evaluation organised on text-independent scenarios and a database recorded with elements to assess text-dependant scenarios.

A further interesting aspect of the Mobio project was the initiative to set up a community of interest, getting together research and commercial partners.

Voice biometrics technology today is quite different from the technology used just a few years back and more robust. Also in many cases when the industry develops closer links with fundamental research, innovation to product times are very short.

Multi-layered security

Recently, the security of a web-based process involving two parties – for example a transaction between a consumer and a seller or a login process between an employee a company’s server – has been enhanced by using Out Of Band (OOB) mobile channel and One Time Password (OTP) solutions. It is important to understand the security issues behind the deployment of such a solution.

“Man-in-the-Browser, a variant of a Man-in-the-Middle attack, has shown how web channels, even when protected by digital certificates, can be compromised”

The sophisticated fraudulent technique known as Man-in-the-Browser (MitB), a variant of a Man-in-the-Middle (MitM) attack, has shown how web channels, even when protected by digital certificates, can be compromised. In this attack the fraudster intercepts, possibly modifies and relays information between both parties involved in a way invisible to them.

The most effective way to deal with this attack, and what makes the use of mobile phones an interesting solution, is to use an extra communication out of reach and hence not compromised by the attacker – hence the term OOB – to confirm the authentication.

On this channel the operation details are shared and checked between the two parties to make sure they have not been modified to the benefit of a fraudster. The authentication model is based on an OTP, however the actual process that occurs on the secondary channel is configurable and extensible. This is done in a wider flow with several stages to form a layered security solution including:

- 1 Authenticate the user with strong authentication including configurable challenge(s)
- 2 Replay the details of the process (for example transaction details) on a real-time OOB channel
- 3 Record the user agreeing to the replayed process
- 4 Sign and encrypt the entire audit log

To make the full process stronger and more convenient for the user, stages one and three can take advantage of voice biometrics. By understanding why mobile devices have become important in such security solutions, and where speaker verification can be applied, voice biometrics solution providers can deliver dedicated tools that will improve the strength and enhance the user friendliness of such multi-layered solutions.

Furthermore, with information processing (including the biometric data processing) done remotely, these solutions are ready for widespread deployment (mobile ownership being widespread) without the need to upgrade to new devices.

Multi factor for strong authentication

Multi-factor authentication is a familiar concept within the biometric community. In the context of authentication with use of a mobile phone these factors are:

- * Something you know – knowledge data
- * Something you have – mobile phone
- * Something you are – voice biometric
- * Somewhere you are – proximity / location

An authentication solution that brings together at least two of these factors (with generally at least a knowledge question) is known as strong authentication. The combination of knowledge data when combined with voice biometrics provides what IBM refers to as ‘conversational biometrics’, which is regarded by some observers as the strongest form of authentication available.

Voice biometrics is a particularly good fit for working in a multi-factor environment. It is convenient, reducing the time needed to go through a full identification process.

On the other hand, if the voice verification evidence is not strong enough, eg, the verification score is either below the acceptable minimum limit or borderline, or if external conditions (for example excessive background noise detected by speech quality measures) make the biometric verification process impossible, there is an alternative mechanism available for performing strong authentication.

“It is important that voice biometrics enable an alternative authentication mechanism where the client is informed of the authentication result to avoid a fraudster operator from asking unnecessary extra personal pieces of information”

When a client contacts a call centre, he or she goes through the voice authentication system. They are then put in contact with the operator and both the client and operator know if further authentication is needed. With increasing call centre outsourcing, it is important that voice biometrics enable an alternative authentication mechanism where the client is informed of the authentication result to avoid a fraudster operator from asking unnecessary extra personal pieces of information.

Also the last factor listed here – somewhere you are – is rarely referenced when multi-factor approaches are mentioned. It represents an interesting addition when basing security solutions on mobile phones. When a location factor is brought in, we might think of GPS tracking technology, often perceived as too intrusive or limited to only consumers possessing the very latest GPS enabled smartphones.

But in practice a location factor does not need to be that precise nor require advanced

devices. To illustrate this point with a concrete example, a major source of card fraud comes from cross-border transactions when fraudsters based in a foreign country use the cardholder details for fraudulent transactions.

Solutions now exist to determine if a physical transaction involving a payment card is in proximity to a mobile phone linked to the actual cardholder. In this particular case, proximity correlation analysis, without the need for GPS or triangulation methods, is enough to dramatically reduce false positive rates that occur when a genuine transaction is blocked. With the right design it is possible to provide such a service for all mobile phone users in compliance with privacy laws.

Hence, with current technology any mobile device already supports the deployment of strong four-factor authentication. When voice is integrated in such a wide and flexible solution, the number of potential applications is large.

E-government

One area of development lies in e-government applications. The first objectives of such solutions are users’ convenience and cost reduction, with the idea being to get citizens to use self-service instead of basing staff in local administrative offices. A multi-factor solution including voice biometrics is well suited to avoid collusion, when an action is undertaken by another complicit person, for example claiming a state benefit while not in the country. A very interesting extension of the technology with big potential is to combat fraud with an offline speaker identification process crosschecking voiceprints to identify potential fraudster using multiple identities.

We are at a very interesting point in the development of voice biometrics technology. Over the past few years there have been significant improvements on the core technology at research level. Also, because of its limitations, the technology development is strongly linked to the right interaction with other security products, and the understanding of security market needs in terms of strength and convenience is very important. Today any mobile device can be used for ultra-strong authentication, opening the door to potentially large-scale innovative applications.

About the author

Benoit Fauve is a senior research and development engineer at security company ValidSoft UK Ltd < <http://www.validsoft.com> > with a mix of professional and academic experience. His career has focused on the optimisation, transfer and product development of signal processing and machine learning-based applications. Though an expert in signal processing in general, Benoit Fauve’s main interest is in speech processing and biometrics. He holds a PhD degree for his work on speaker verification.

Military biometrics on the frontline

Steve Gold, freelance journalist

The use of biometrics in military circles has increased significantly in recent years. Steve Gold spoke to some of the experts in this highly specialised area of biometrics and asked them how the technology is being used and developed.

The US military, as well as UK Ministry of Defence and NATO forces are making increasing use of biometrics in countries their personnel are based in, using the technology to identify non-military personnel quickly and accurately, cross-matching the biometric data to their own databases.

But the technology's usefulness doesn't just stop there. The US Department for Homeland Security (DHS), for example, is piloting the use of a 'fidget factor' behavioural biometrics system to determine whether or not interviewees are hostile to the US.

According to Starnes Walker, the DHS' director of the research, science and technology directorate, the Future Attribute Screening Technology (FAST) platform is being used to measure responses to the question 'do you intend to cause harm to America?'

Speaking at the Biometric Consortium Conference in Florida last September, Dr Walker and his team said that the technology is still in its infancy, but shows great promise.

Afghanistan

The DHS is reportedly investing millions of dollars in biometrics technology for use in military deployments. In Afghanistan, for example, the DHS is working with NATO and the Kabul government to issue biometrics-based smart ID cards to 1.6 million Afghans. The card issuance started in at the beginning of 2010 and should be completed by May 2011. According to NATO, the aim of the programme is to monitor movements of militants around Afghanistan, as well as keep Taliban infiltrators out of the Afghan army. Early

reports indicate that the Afghan biometrics ID card programme is catching between 20 and 25 people a week who would otherwise have been missed by conventional screening, although NATO officials are predicting this figures could well rise in the near future.

"There are two main biometric projects in active use in Afghanistan"

There are two main biometric projects in active use in Afghanistan, the first of which uses fingerprint readers, iris scanners and digital cameras to capture information on detainees and what NATO calls 'other persons of interest'. The Biometric Automated Toolset, as it is known, has reportedly generated more than 400,000 sets of biometric data in its 18 months of operation.

The second biometrics project, the Afghan Automated Biometric Identification System

(AABIS), developed by the DHS and NATO in close co-operation with the Afghan National Army, collates facial and fingerprint biometric data from army and police applicants.

The data is scanned and logged in the field, and periodically downloaded to a central database in Kabul, where it is cross-matched with databases operated by the Afghan National Detention Facility, the Kabul Central Police Command, the Counter-narcotics Police of Afghanistan and FBI prison enrolments from Kabul, Herat and Kandahar.

One of the vendors whose kit is being using in the AABIS project is Cogent Systems, whose biometrics technologies were some of the first to be certified as compliant with the FBI's Next Generation Identification (NGI) Initiatives and Integrated Automated Fingerprint Identification System (IAFIS) image quality specifications in 2009.

According to Cogent, its Fusion, Mobile Ident II, and Mobile Ident III systems were approved, following testing by the Technology Evaluation Standards Test Unit, part of the Biometric Centre of Excellence, Criminal Justice Information Services Division.

Geoff Hunt, Cogent UK's project manager for the firm's defence lead, told BTT that the ruggedised Fusion device has been in active development with military clients such as NATO and other forces for almost two years.

Externally, the unit looks like a giant dymo tape machine, but contains an iris image capturing system, latent fingerprint capture system and a one square inch 500 DPI optical fingerprint scanner. The unit, which is Electronic Biometric Transmission Specification (EBTS) compliant, has integrated Bluetooth, GSM/GPRS and wifi communications and was developed in the US to precise US military and NATO specifications.

Development process

While there are a number of hardware vendors in the military biometrics space, the real intelligence of the systems in active use in the battlefield is in the software that drives the systems.

According to Jon Busby, product manager with Liverpool, UK-based Human Recognition



Steve Gold



Cogent's Fusion has been in development with NATO for almost two years.



Systems, the software in biometrics systems, in which HRS specialises, undergoes rigorous testing by the US military and NATO forces before it is released into the field.

"It's all about complying with the needs of the military," he says, referring to the close liaison his company has with the Ministry of Defence (MoD) and NATO.

HRS was formed in 2002 and now has more than 40 staff involved mostly in biometrics software development. "I joined the company when it was first formed and met with the MoD that first year in 2002 when we held a series of workshops to better understand what they were looking for," he says.

HRS, he went on to say, follows a US model when it comes to developing biometric systems for use in the battlefield. The US and UK military specify what hardware they want to use, and HRS then develops the software to support the facilities the military client wants.

"There are a number of differences in the way the US military and the MoD operate when it comes to developing biometric products for use in battlefield"

He told BTT there are a number of differences in the way the US military and the MoD operate when it comes to developing biometric products for use in battlefield and similar conditions. Despite these differences, he says, the end products that are used by military clients have a set of common core characteristics, including a platform that is easy to use, even under battle conditions.

"The military have to have confidence the biometrics system will work under all conditions. It simply has to work, even when the staff using the technology are under fire. It's that critical," he says.

Another feature of military biometrics systems used in a theatre situation, says Busby, is that the hardware is almost exclusively developed in the West, despite the technical prowess of Far Eastern nations.

Battlefield deployments

According to John Christensen, a biometrics director with Northrop Grumman Corporation, in the military, there is the concept of blue, grey and red people in hostile territory. Blue people are defined as friendly, whilst grey are an unknown status and red are defined as the enemy. Biometrics, he says, allow military personnel to quickly and accurately determine the probability of whether a grey category person falls into the blue or red category.

This simple analysis, he told an audience at the recent Biometrics 2010 event in London, can mean the difference between life and death in a hostile situation.

"In Iraq soldiers collated a vast amount of data on civilians they encountered, but then discovered that one database does not work with another"

Despite biometrics assisting military personnel in the field, there are times when biometrics can cause more problems than it may be worth. For example, says Christensen, the US military has made some mistakes with its biometrics

technology, such as in Iraq, where soldiers collated a vast amount of data on civilians they encountered, but then discovered that one database does not work with another.

"We realised early on that there is a need for interoperability of data," he told his audience, adding that, with the right operating system in place you can use and re-use the same biometrics data to great effect.

He points out that military biometrics were originally developed to make sure that personnel taking their military examinations were who they said they were. "The problem in the military is that you are all buddies, and you have buddies taking exams for their buddies," he says.

Back in the battlefield and hostile country arena, biometrics technology has a major role to play, with iris scanning technology playing an integral role in force protection, base access and detention operations.

"The Department of Defense (DoD) are the biggest user of biometrics outside the Department for Homeland Security. We use the technology on a day-to-day basis in Afghanistan," he says.

One of the most interesting aspects of biometrics usage in the military, says Christensen, is the fact that it's often the same people in the field that collate the data as those who use it. Against this backdrop, it is important to process this data in a timely and effective manner, for which the DoD has developed its own biometrics enterprise architecture.

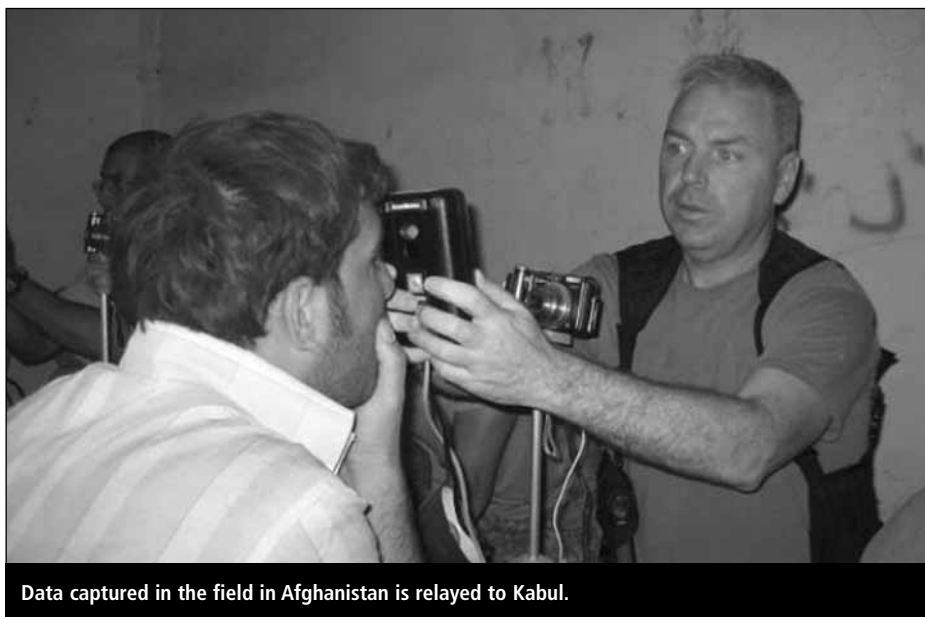
Data captured in the field is collated and used in real time and in the field then batch processed and relayed to Kabul in the Afghan conflict, where it is stored centrally and replicated to other databases across Afghanistan and back in the US. The biometrics data in the US is then shared between the DoD, the Department for Homeland Security and the FBI, he explained.

This sharing of data is the direct result of the lessons learned from the 09/11 tragedy, as the aftermath analysis of that event showed how vital it is for all US agencies to share their information, including its biometric data on anyone in the field.

In Afghanistan, he says, the US military is fortunate to have a permissive environment. "We are not always going to have this in every battlefield environment, so we need to take a federated approach to our biometric databases, since they are a powerful weapon that can be used in peacetime, as well as on the battlefield," he says.

The last mile

Christensen's comments at Biometrics 2010 were echoed by William E Vickers, a director of biometrics and forensics with the US Office of the Under Secretary of Defense for Intelligence,



Data captured in the field in Afghanistan is relayed to Kabul.

who said that biometrics is incredibly important in the last tactical mile in the battlefield.

“We have created a MESH wireless network to share data in the field, using a variety of technologies – WiFi, WiMax, 3G broadband and satellite – to intercommunicate the data,” he says.

Once the biometric data has been collated and stored, Vickers says that the next step is to analyse that data whenever the need arises. Forensics, he told his audience, is the number one method of identifying improvised explosive devices (IEDs) in the field, and the biometric data that is collated from personnel allows military staff to make an informed decision about how to proceed when dealing with an IED.

Because of its criticality, Vickers says that biometrics in the battlefield needs to be capable of withstanding extreme weather conditions, and be resistant to sudden changes in tempera-

ture and moisture, as well as withstanding high levels of vibration.

“On top of that, the biometrics devices have to be portable, meaning that size, weight and power requirements are crucial,” he says, adding that interoperability with other systems is also critical.

“The US military is working on biometrics technology that works with existing digital devices including the civilian smartphone”

For the future, Vickers says that the US military is working on biometrics technology that works with existing digital devices that military personnel have on them, including their regular civilian smartphone. Most military staff in

Afghanistan, he explained, have their mobile phones in their side pockets, so using that resource makes a lot of sense.

It is almost certain, he went on say, that biometrics databases will, in the future, be shared between users in the field, using a cloud computing approach that shares discoverable data between multiple databases in real time.

About the author

Steve Gold has been a business journalist and technology writer for 26 years. A qualified accountant and former auditor, he has specialised in IT security, business matters, the Internet and communications for most of that time. He is technical editor of Infosecurity and lectures regularly on criminal psychology and cybercrime.

Signature and gesture – dynamic biometrics for remote login



Jeff Maynard

Jeff Maynard, Biometric Signature ID

There is increasing demand to communicate and execute purchases and agreements electronically over the Internet. One of the biggest issues however is the trust factor and consumer and corporate confidence that security needs are being met is at an all time low.

We are entering an era in which businesses cannot rely simply on user names and passwords as single credentials to validate the identity of users. It is just too easy to steal, hack or borrow single credentials like pins, passwords or tokens. Consumers are requesting higher standards of privacy protection, even electing to spend their own money on credit card identity theft monitoring.

The problem that government, institutions, companies and merchants face is authenticating identity before secure transactions or access take place. Current identity proofing methods do not identify the physical user. They are typically centred on predicting identity or behaviours, based on whether the user is who they say they are because they possess knowledge supposed to be known only by the individual (pins, security questions or passwords), or they verify

that a piece of hardware (ie tokens, geolocation, device ID) is working and assume it is in the hands of the intended user.

“With the Internet’s wide appeal comes the ability to easily uncover most of a users’ personal credentials”

However with the Internet’s wide appeal comes the ability to easily uncover most of a user’s personal credentials, including but not limited to date of birth, address, social security number and financial information. This information is obtained through simple searches using common Internet search engines, reference web sites, social web sites, personal blogs, and more. Popular applications available in the virtual world and

companies doing business online are finding it necessary to augment current security to involve multi-factor authentication.

User experience

The issue with multi-factor authentication however is not so much the security. It is becoming all about the user experience. You can have the highest level of biometrics like iris scans but the practical nature of implementation and user experiences will reduce uptake in all but severely mandated environments.

“You can have the highest level of biometrics like iris scans but the practical nature of implementation and user experiences will reduce uptake”

If consumers and employees have to make extra effort such as install something, take a long time to answer questions, write everything down somewhere, constantly change

passwords, struggle with fingerprint readers that don't work or take too long, give up their privacy, give up personal identifying information, take training or pay something they will find ways to avoid or rationalise why they won't use this new security. That is just human behaviour.

However there are two levels of security aimed at two very different groups. Security measures that are supposed to work to stop the bad guys require the highest possible level of security tools that usually include, fingerprint, iris scans or other solutions. Let us call this group A.

However let us look at the other side at Group B. Group B is mostly concerned about day-to-day lives. Group B people don't know what a false positive or FRR is or what a one in 1000 value level means. They probably don't know what NIST is and have no idea how to use a token let alone an iris scan. They may realise passwords are not secure anymore and most have been educated to not release their social security numbers over the Internet. They do

not want to be victims of identity theft yet don't want any security solutions that compromise their life and take time.

Vendors have tried to take some of the same tools that are hardware-based solutions (tokens, fingerprint readers, bingo cards, smart cards etc) and make it useful for commercial users. Often, it just does not work because the nuisance factor of implementing these is just too much for Group B commercial users.

Group B would like better security than they have today but this does not have to be so secure that it will stop the terrorists. It just has to be better than pins and passwords.

Dynamic biometrics

Dynamic biometrics uses a behavioural-based approach to authenticate people. Signature, gestures, voice and keyboard form the mainstay of dynamic biometrics. Dynamic biometrics allows the enrollee to introduce a secret code into the biometric process. The users can enrol with a code or drawing of their choice, which is their secret code.

Dynamic biometrics combines secrets with biometric samples (a unique way of drawing for example) to provide two-factor authentication in one process supported by signature/gesture software.

It should also be noted that if a fraudster attempting to enrol under an assumed identity is asked to provide a biometric, he/she is likely to go away rather than provide the biometric. Lexis Nexis has reported a 30-50% walk away rate. It stands to reason then that if there are several deterrents – multiple layers – in front of the fraudster it might increase the walk away rates even further.

"Revocation is instant and replacement is only a re-enrolment. If a fingerprint is hacked its security is gone forever"

Dynamic biometrics allow for an infinite number of different secret biometric samples (codes, images, and numbers) to be generated by the same individual. Revocation is instant and replacement is only a re-enrolment. If a fingerprint is hacked its security is gone forever.

Applications

The US Higher Education Opportunity Act of 2008 (HEOA) requires accreditors to assure that an institution that offers courses or programmes at a distance have a process in place to establish that a student who registers in a course or programme is the same student who participates in and receives the corresponding credits.

The US Department of Education's regulations for accreditors went into effect in July 2010, and require institutions to verify students' identities through secure logins and passwords, proctored tests, or 'new identification technologies and practices as they become widely accepted'.

This rule was put in place to counterbalance the high growth rate in online courses (18% per year) and the increasing perception of academic cheating. The federal government was concerned to ensure that students who receive degrees and financial aid are the same students who are actually taking the courses.

This new rule threw the 4000 higher education institutions into a quandary. Several vendors anticipated this new law and came out with hardware-based approaches involving webcams and fingerprint scanners. Others came out with security-based questions combined with a webcam.

BioSig-ID Online™ Hello, bob3@test.com » My Account

Home About Us Service FAQ Contact Us Sign Out

Enroll BioSig-ID Profile

Directions:

- Select 3 or more different characters/initials/shapes to use as your personal ID (see example)
- Using your mouse, hold the left mouse button down
- Draw these different characters/initials/shapes in the space provided
- Use the lines as the reference
- Select "Next" after completed

Example: 5346

Success Tips: Write slow & move your mouse with consistent speed and direction.

2920

Check box to enable invisible ink
 Uncheck box to remove grid lines

Flash Client Version : 1.1

Clear Next Re-enroll

Recommended browsers: Internet Explorer 8.
 Copyright ©2007-2008 by VerifyExpress.com. If you would like to know more about our products, please [click here](#).

Users enrol with a code or drawing of their choice.

Most of these security products were just trying to replace proctored exams. This is where the online student would have to personally go to a physical facility so someone could watch them take their exam and ensure they did not cheat. Proctored exams are a large expense and inconvenient for students who chose an online course so they did not have to show up at a classroom.

"Proctored exams are a large expense and inconvenient for students who chose an online course so they did not have to show up at a classroom"

For example, one large university administers 10,000 worldwide sites where their students must go to take a proctored exam. Many institutions would prefer to avoid this expense and have their students take an online exam from home. They need to have a solution that can identify the identity of a student without creating an expense or inconvenience for the student. This is a competitive area and every institution has to be aware that students have many choices of virtual universities. Any extra burden to the student will have them choose another institution.

Telecampus

The University of Texas TeleCampus (UTTC), which has recently become the University of Texas Online Consortium, was concerned that it complied with the newest revision of the Education Act to increase course integrity and verify students' identities. Not every course has a final exam and for many courses grades are given for participation on discussion boards or interactive sessions.

UTTC ran a pilot to gauge user acceptance and user friendliness of signature/gesture software. A secondary goal was to develop optimal enrolment and authentication procedures. The technology employs a dynamic gesture/movement technology to authenticate student identity remotely from their computers using just their mouse or touchpad without the need for any special hardware or installation.

Over a six-week period 167 students from nine campuses volunteered to authenticate their identity from their own computers using BioSig-ID and Click-ID software. Test subjects were asked to enrol, create a profile and authenticate their identity 10 times during their course. 167 students registered in the software and 90 completed the required 10 authentications. Audit trails were analysed of all activity and an online survey was administered for all students who completed the pilot.

The signature/gesture software gathers data on a student's mouse, stylus, or touchpad characteristics such as the speed, direction, height, length, width, and angle of the student's movements. The student is authenticated when his or her actions match the unique profile on subsequent logins"

The signature/gesture software gathers data on a student's mouse, stylus, or touchpad characteristics such as the speed, direction, height, length, width, and angle of the student's movements.

The student is authenticated when his or her actions match the unique profile on subsequent logins. The biometric authentication is one aspect of a three-part authentication, which also included complex security questions.

Results

100% of participants were able to enrol and validate in the pilot. 80% responded to a survey and of those, 98% found the verification system easy to use. Average authentication took 21.5 seconds and one call to the helpdesk was recorded. Additionally 81% of students spent more of their own personal time using the system that was asked for. For example they went in after the pilot was finished or completed more authentications than they were asked.

In many cases the challenge is not to stop terrorists but to put the highest possible deter-

rent in front of fraudsters so they cannot gain access to personal or corporate digital assets.

"In many cases the challenge is not to stop terrorists but to put the highest possible deterrent in front of fraudsters so they cannot gain access to personal or corporate digital assets"

Applications for dynamic biometrics like signature/gestures might include employees gaining access to their PC at work, employees sending confidential materials over the Internet, logging in to online bank accounts, logging in to the cloud, or authenticating Internet purchases.

Future is dynamic

As more commercial entities and government agencies demand better multi-factor security, dynamic biometrics are likely to find use in a wider number of applications.

Uptake may be predicted to be higher with dynamic biometrics like signature gestures because they do not require any hardware with corresponding lower costs while offering convenience and security for users.

About the author

Jeff Maynard is the CEO and founder of Biometric Signature ID <<http://www.biosig-id.com>>. He is the creator of inventions using handwriting biometrics and image pattern technologies to verify identity. He is a former CEO running two divisions using biometrics in healthcare for a public traded company. Previously Jeff Maynard was a partner in a software firm that created predictive modelling software for large healthcare clients like United Healthcare. He received his undergraduate degree from York University, Toronto and completed executive training from Harvard/MIT, and Kellogg School of Business. He is a committee member for the INCITS/NIST 'Study Report on Biometrics in e-authentication 2007' and a member of Center for Ethical Identity Assurance



A SUBSCRIPTION INCLUDES:

- 10 printed issues
- Online access for 5 users
- A four-year archive of back issues
- Free delivery

www.biometrics-today.com

...Continued from page 3

of address' and 'commission services'. The pilots are intended to test the integration into existing real live portal services of the underlying STORK interoperability platform.

Stork co-chair, Antonio Lioy from the Politecnico di Torino in Italy, says: "The pilots will highlight the added value citizens will receive by being able to assert their identities electronically in a protected, secure and private environment." He adds: "The eID framework will save public money, reduce time for both government and citizens, lessen the risk of misuse or fraud and create a wealth of opportunities. It is one more step towards a borderless EU marketplace."

The German government has started issuing new ID cards to citizens featuring the cardholder's biographical and biometric details on the chip as well as the card, and will be issued to citizens whose existing ID cards expire this year. They will be rolled out to other citizens after that.

eGo shows its first prototype

The first prototype from the eGo Project will be demonstrated at Cartes 2010 in Paris. The eGo Project is a group of companies and academics funded by the Catrene programme to design, develop and promote a new technology named eGo. Catrene (Cluster for Application and Technology Research in Europe on NanoElectronics) is a four-year European Union programme to deliver nano and microelectronics solutions.

The eGo project proposes an innovative way to establish secure, bidirectional wireless channels between objects or individuals in the future internet of things. This will open the path to new and intuitive ways of interaction for electronic transactions.

The prototype, produced by Gemalto, does not yet have its planned biometric fingerprint sensor. IDEX and Precise Biometric technology will be integrated next year. A spokesman for eGo says, "We expect a fully functional eGo device by Q4/2011 and a family of commercial products by 2013."

A number of companies and academics are contributing to the project. Decawave provides the UWB module, STm provides

the battery and the secure microcontrollers, IDEX and Precise Biometrics provide the biometry technology based on the fingerprint sensor, Gemalto provides the IBC (IntraBody Communication) module and the secure operation system.

VERIFICATION

Pilot licences stall while driving licences get face recognition

Driving licences are increasingly incorporating biometrics to assist with identification but US politician John Mica has raised concerns about the failure to include them in US commercial pilots licences

Under the 2004 Intelligence Reform and Terrorism Prevention Act, The Federal Aviation Administration was scheduled to

begin issuing improved pilot licences that include a photograph of the licensee and are capable of accommodating a digital photograph, biometric identifier, 'or any other unique identifier' by December 2005.

In a letter to the FAA administrator, Mica requested an update on progress and dubbed the lack of progress towards biometrically enabled licences 'disturbing'.

In Australia biometric drivers licences are closer to implementation. According to *Computerworld Australia* the Queensland Government's biometric driver's licences are expected to go live by the end of the year following a successful trial in August and September.

The new licence uses 16-point facial recognition technology, according to *Computerworld Australia*. When drivers renew or apply for a licence, a digital photograph will be taken and stored. When the licence is renewed the system will access the image and use the facial recognition technology.



COMMENT

There was a real buzz at the Biometrics 2010 event in October. The sense of excitement was pervasive as delegates soaked up the latest in a technology that is coming of age. The conference began with a focus on state of the art border and citizen identification and closed with sessions on biometrics used for law enforcement around the world.

In between NIST took delegates to the frontiers of biometrics research into handling non-ideal biometric capture, ranging from covert capture to difficult conditions such as low light. NIST's PJ Grother identified video as an untapped biometrics resource and demonstrated how it might be possible to start measuring the behaviour of a subject captured on video in conversation. NIST is also looking at ocular biometrics, encompassing characteristics of the whole eye not just iris recognition.

At the frontiers of fraud prevention the Biometrics Institute in Australia presented some fascinating research on spoofing that should be of interest to everyone in the industry. The Institute has been working on a vulnerability methodology to provide an assessment of how vulnerable biometrics devices are to artefact attack, whereby fake

biometrics such as fingertip covers, glass eyes and contact lenses may be used to fool fingerprint reading devices and iris scanners. Of 50 attempts to fool a fingerprint scanner with silicone fingertip covers, 49 were successful, for example.

More prosaically the conference was an opportunity to see the results of some real life implementations of biometrics solutions across many sectors from health to retail. US Army staff also provided an insight as to how biometrics are being used on the front-line of the battlefield.

Two men at the helm of the ambitious Indian project to uniquely identify 1.2 billion Indian residents, RS Sharma and Srikanth Nadhamuni, gave a confident assessment of the project so far. Sharma hailed the project as one that would provide proof of identity to people who did not previously have it to access services and benefits. Six states are already live with data coming in, Sharma told delegates.

According to Sharma, the only constraint to the success of the project, which is enrolling one million people a day, is the supply of devices and he called upon the industry to create a new model for high volume, low priced devices. The industry watches with interest as this landmark project unfolds

Tracey Caldwell