...Continued from page 3

**technology. In the US, the *Federal Times* reports that the Pentagon is refining its use of biometrics to better identify, screen and search for individuals.**

According to John Boyd, director of Defense Biometrics and Forensics, speaking at the Biometric Consortium Conference and Technology Expo, budget constraints and a change in priorities as operations in Afghanistan wind down are among the factors driving a more refined focus in biometrics.

At the same event, NATO was reported to have revealed that its vision is to have interoperable biometrics capabilities throughout its membership. The organisation is increasing its biometrics expertise at its headquarters and has created the NATO Biometrics Work Program to issue consistent guidance, procedures and standards.

AUTOMOTIVE

## Moves to measure driver heart and brain wave biometrics

**Nissan has launched the Nismo Watch, which connects driver biometrics measurements in real time with in-car systems, while elsewhere researchers look into measuring brain waves as biometrics for on-demand driver authentication.**

The Nissan Nismo Watch will allow drivers to capture biometric data via a heart rate monitor. Earlier this year, Nissan launched the Nismo Lab, a mobile laboratory that features the latest, advanced biometric training tools such as brainwave technology and JukeRide, a performance analysis tool that captures live biometric and telematics data from racing cars and athletes during races.

### *"Conventional biometric systems mainly assume one-time-only authentication"*

This comes as researchers published a paper in the 'International Journal of Biometrics' (Int. J. of Biometrics, 2013 Vol.5, No.3/4, pp.288 – 305) that presents a way of using brain waves as biometrics for on-demand driver authentication. The researchers comment, "Conventional biometric systems mainly assume one-time-only authentication. If an imposter replaces a user after the authentication has occurred, the systems cannot detect such a replacement. One solution to this problem is on-demand authentication."

INDIA

## Biometrics for attendance and benefits face challenges in India

**Authorities in India are pushing ahead with biometrics implementations on a number of fronts, despite setbacks. Healthcare workers in the Indore district of India were to be paid on the basis of attendance registered on biometric devices by the end of September, according to local reports. Three years ago, machines were installed in local hospitals, but never used.**

Separately a biometric project in India that could require people to produce their biometric IDs to collect government subsidies has received a setback from the country's Supreme Court, which has ruled that people cannot be required to have the Aadhaar identification to collect state subsidies, according to *PC World*.

The Unique Identification Authority of India (UIDAI), which manages the project, has been trying to promote the Aadhaar number as proof of identity for a variety of services including banking. However it has also faced problems as the biometric authentication system appears to be failing to establish the identity of many genuine beneficiaries, mostly workers, as their hard manual labour has eroded the lines on their fingerprints.

## COMMENT

There was high excitement in the biometrics community when Apple launched its iPhone 5S complete with fingerprint scanner on the home button that not only enabled easy fingerprint access to the phone but also authenticated the user for purchases from the iTunes store. The financial press reported soaring shares and at last it seemed no-one be would ever again be asked, "What is biometrics?".

That was before the Chaos Computer Club came along and put a dampener on things with its announcement that it had been able to spoof the iPhone 5S' fingerprint recognition system.

There were many vested interests that were pleased to observe the CCC rain on the iPhone 5S parade. These included vendors of non-biometric security solutions who had been quick to spread scare stories about people losing their means of biometric authentication forever on a carelessly discarded wine glass.

And suppliers of just about every other biometric modality and those already offering smartphone biometric solutions who had not been invited to the iPhone 5S party may have allowed themselves a moment of schadenfreude.

The reality is that no-one ever claimed that any means of biometric authentication is either 100% reliable or 100% secure. Apple certainly did not as it seems to have been careful not to share its FAR and FRR testing process. But cracking the iPhone 5S' fingerprint security was not trivial, requiring an excellent quality fingerprint, specialist equipment to reproduce it and possession of the fingerprint owner's phone. Of course that would not stop a determined criminal, but nor would a PIN code screen.

As Richard Moulds, VP product strategy, Thales e-Security, comments in our lead news story this month, "Before we all get too excited, security is about swords and shields – bigger shields lead to bigger swords, and it's a constant battle to deal with the weakest links in a security system." In other words, even if fingerprint authentication were 100% secure, determined criminals would quickly find another way in, especially when the prize is access to corporate systems or financial details. The only way to truly secure systems is to take a holistic approach, encompassing technologies such as cryptography and key management.

Another alternative was presented only days after the iPhone 5S launch with the publication of a paper by researchers Asem Othman and Arun Ross that unveiled a method of mixing measurements from two fingerprints to create a single biometric template.

Industry observers would be forgiven for thinking there is no need to wait for the commercialisation of this type of cutting edge research, as the answer to the authentication issue is already staring us in the face – or screaming in our ear. Multimodal biometrics provide an excellent and doable solution. The iPhone, and other smartphones of course, could also incorporate facial recognition, voice recognition or even gait (movement) recognition that, combined with fingerprint, could reinforce authentication. We await the iPhone 6 with interest.

*Tracey Caldwell*