EAB POSITION PAPER

iPhone 5S: heralding a paradigm shift?

by the European Association for Biometrics (EAB) and the EAB Advisory Council

Introduction

On 10 September 2013 the world witnessed a long anticipated event, heralding a paradigm shift: Apple's launch of a new iPhone with a fingerprint reader underneath the home button. The use case: to unlock the phone and authorize purchases in Apple's iStore. Literally one day after the iPhone hit the shelves, a hacker team claimed to have circumvented the biometric technology by getting the phone to accept a plastic 'spoofed' fingerprint.

The European Association for Biometrics (EAB), Europe's premier organization of stakeholders and experts on these technologies, together with its advisory committee (EABAC), welcomes the widespread use of automated authentication, with the proviso that privacy and security must be safeguarded. Biometric characteristics, unlike passwords, are personal and irrevocable,and, therefore, should be used in a secure and privacy-protective way. For this reason, we have prepared this statement.

Although this statement coincides with the launch of a particular smartphone, our comments address the use of biometrics in mobile devices in general and are not always specifically directed at the iPhone, the latest in a long line of smartphones and laptops equipped with fingerprint recognition.

In drafting this statement, the EAB seeks to offer the suppliers of mobile devices, service operators and the user a perspective on how to assess this kind of technology - and in particular its security and usability.

Fingerprinting on the home-button: what do we know?

To date, most of the applications of biometrics have been in the area of law enforcement, border security and public security. We are now seeing what biometrics can offer in terms of an improved user experience and increased convenience. Where the trend in information storage is firmly to the "cloud", the iPhone 5S brings storage of important data back to the device.

We are told that biometric data relating to your fingerprint is securely stored in a chip which is not accessible to third party applications. That seems to be a good decision for the privacy of the user as it limits the opportunities for function creep. Additional claimed security features include encryption of the data and software to ensure that the fingerprint image cannot be recreated. As having a choice is a major consideration in providing users a fair opportunity to decide whether or not to use a certain feature, a fair question may be whether

the fingerprint sensor is actually shut off when deactivated by the user. With concerns about the collection and reuse of personal data by internet-based companies running high, is the current level of information sufficient for the user to make a balanced assessment of risk?

The EAB and the EABAC believe that purchasers of devices using biometric data are entitled to further detail, and look forward to an independent assessment of its security.

A paradigm shift or just a step forward?
One reason for the delayed take-up of large scale biometric applications by the commercial sector seems to relate to the privacy concerns. Indeed, in some EU countries, there appears to be significant resistance to the expanding use of biometrics, in line with the increased emphasis on the protection of personal data and privacy. A question that innovative companies such as Apple need to address is how to reassure the public that use of these technologies will not inadvertently allow opportunities for surveillance and misuse of the data by either large corporations or unprincipled government departments.

Although these questions could have been posed when earlier fingerprint devices were introduced into smartphones and laptop computers, the adoption now of biometric technology by a major supplier makes our questions particularly timely.

Standing back to see the big picture
The use of fingerprint biometric technology should be seen against the wider range of possible ways of securely authenticating the user of a mobile device. Certainly the new technology has merit as a contact pattern matching system: 'contact' as requiring a physical connection from a finger, or some other object, to a sensor, and 'pattern matching' as the biometric software creates reference data for the finger image when the user first enrols, with the user being recognized when the pattern developed in a subsequent contact is sufficiently similar to the reference data. Users might like to be informed of how much similarity between the enrolled reference and the subsequent pattern is expected. More security is offered when the match is required to be very close, while the usability improves if a wider tolerance of variation is allowed, for example in positioning of the finger or in accepting poorer quality images when fingers are too dry.

As the widely publicised spoofing attacks have demonstrated, use of artefact patterns other than fingerprints are possible when matching against the reference image, thereby allowing an element of secrecy under the control of the user. One can view this as replacing a single authentication factor (the PIN) with two authentication factors: the knowledge about the enrolled patterns (was it the left index finger or the right little finger, a combination of those in a specific order, or an artefact pattern?) and the pattern itself. Such an approach is an example of Privacy by Design, responding to the concerns of both the user and the privacy regulator. Therefore, and in addition to other examples of Privacy by Design, organizations that capture and/or process biometric data should take the opportunity to draw on procedures of audits and certification carried out by trusted third parties.

The relevance of values in applying biometrics: do these still count?
In assessing whether an application using biometrics is 'fit for purpose', the biometrics community has asked questions, amongst others, about the balance of costs against benefits – not just the financial costs and benefits, but also the balance of usability against security – and about trustworthiness of the software, hardware and the operator.
Trust in the components of the application and the business or government organisation running a service using biometrics is paramount. How easy would it be for other organisations to harvest biometric data of millions of users by exploiting weaknesses in the design of the device or the service? How much data could be gathered that does not

necessarily recreate the original image of a fingerprint but still allows matching to fingerprints obtained by other means? An insecure implementation by one vendor could impact on the perception of the security of biometric recognition by other, more conscientious, suppliers.

The EAB proposes that openness and transparency in the information made available to the biometrics community will not compromise the security of devices, but will ensure that consumers will be able to rely on privacy-compliant, secure and user-friendly smartphones and laptops.

November 2013
Contact: secretariat@eab.org

About the EAB
The EAB is a non-profit organization seeking to advance the proper and beneficial use of biometrics in Europe, taking into account the interests of European citizens, industries, academia and governments. The European Association for Biometrics (EAB) is the primary European multi stakeholder platform for biometrics.

The EAB targets its activities at the following areas of interest:
- Communication and community building
- Training and education
- Research and programme development

The EAB engages stakeholders from all European countries including the European Commission and the European Parliament, by establishing a pan European network of national contacts points and platforms and by providing a programme that appeals to common needs. The EAB is committed to contribute to the development of technologies and services that ensure safety, security, interoperability and the protection of human rights, including the right to privacy.

About the EABAC
The EAB Advisory Council (EABAC) is the organization's internal advisory body, as laid down by the EABs constitution. It consists of the chairs of the constituted EAB committees and working groups, and elected representatives from the wider biometrics and identity community, including from outside Europe. Members of the EABAC are nominated by EAB members at the General Assembly and appointed by the Board of the EAB.
The EABAC provides advice to the Board of the EAB and other constituent bodies in matters of fundamental importance. It issues recommendations concerning directions for the EAB's strategy and activities. Furthermore, the EABAC can issue statements of advice concerning the creation of new committees or the change or closure of existing committees and EAB activities. According to the EAB strategy the EABAC has identified four key audiences/groups that are the focus of its activities: Policy, Industry, Research & Academia and the Citizen. As a result, the EABAC will try to ensure that there is even representation from each of these four key audiences or groups.

The EABAC seeks to enhance information exchange and cooperation in the area of biometrics on European and international levels by coordinating experts' responses and providing a platform to work towards a concerted approach to the proper and beneficial use of biometrics.