The Mobile-powered Planet

Blog post 3/3 - By Philippe Le Pape, identity and security expert, VP Partnerships and Presales within the Digital Security and Authentication Division of Safran Identity & Security (formerly known as Morpho).

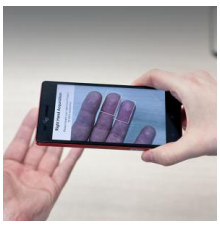
IDENTITY

POSTED ON 06.30.16

Earlier, we touched on how mobile devices now dominate our lives – whether for entertainment, communication, work, or shopping. Mobile technology, in the form of phones, tablets and notebooks, has changed our lives faster than any technology before it. It has achieved this in many ways, not least by making communications routine, irrespective of time and place.

Biometrics as a password replacement for computers isn't new; **fingerprint scanners** have been common on laptops since the launch of Windows XP in 2001. However, it is the shear ubiquity of mobile devices that is likely to drive biometrics as the preferred method of authentication. Already, fingerprint scanners and **facial recognition** software have made their way on to these devices.

Ironically, it is the very form-factor that mobile devices employ that has driven the need for an alternative to traditional passwords. Small screen sizes, with tiny-keyed clumsy keyboards make it difficult to enter complex passwords. More so, as devices are typically used 'on-the-go'. As a Band-Aid, most devices offer features to "remember" passwords, making them less secure, particularly as mobile devices are far more prone to being lost or stolen. On top of that, mobile applications, including those that may have access to saved passwords, have proven difficult to vet. Such rogue apps have been identified as a major attack vector by Security Analysts, but even the major App Stores have fallen foul to privacy-raiding apps over the last year. In 2014, Symantec found that 17% of all Android apps (nearly one million total) were actually malware in disguise. All of these factors expose the identities of mobile device users to additional risk. New biometric services are evolving to meet these new security needs; for instance, **MorphoTrust's US-based Identix Trusted Identity-as-a-Service (TIaaS) platform**, enables developers to bring **identity verification to mobile devices** across a wide range of services.



It is interesting to note at this point the economics that are, in effect, driving the consumerization of the biometrics marketplace; the worldwide device market in 2015 was around 2.5bn units. It should also be noted the considerable efforts by all the major payment vendors to make the smartphone the platform of choice for **contactless payments**. A perfect storm is coming that will drive the need for industrial-strength biometrics on consumer devices. The Mobey Forum predicts this storm will drive rapid adoption and that over a billion people will be using biometric systems to interface with online banking systems by the end of 2017.

It's The R&D, Stupid!

Fingerprints authentication Safran To be a leader in biometrics requires considerable investment in R&D and expertise in a range of complementary disciplines; these disciplines include image acquisition and processing, shape recognition algorithms to create templates, cryptography to secure the template, database architecture know-how to build a template database, algorithms for template verification, and more. Today, the leading players in biometrics invest heavily in optimization and interoperability of algorithms; according to the Mobey report the resulting advances in accuracy and speed of biometric solutions are such that the US government federal resource on biometrics.

> *Most biometric systems have a high accuracy (over 95 percent and many approach 100 percent).*
>
> *biometrics.gov*

At a more practical level, biometric solutions have driven innovation in deployment and ease-of-use as demand for solutions with minimal training requirement for operators, such as in border control, has risen. Consumerization of biometrics, where ease-of-use and overall 'user experience' are even more important, will drive this further. A classic example of this is the inclusion of **fingerprint scanners** in smartphones; no one remembers the first smartphone to include a scanner – the Motorola Mobility Atrix 4G in 2011. However, people do remember Apple introducing a fingerprint scanner on the iPhone 5s. The difference was deep integration with the iPhones operating system and Apple's well known ease-of-use. As the Mobey report notes, this led to an immediate jump in the use of the iPhones security features.

To Serve And To Protect

> *As a strong advocate of **biometrics** for **authentication** I am sure that users will benefit from the ease-of-use, increased accuracy, reliability and security that biometrics will introduce to their digital transactions. Of course, biometrics aren't a cure-all for online fraud, but can – and will – provide a robust solution to many of the issues faced by both service providers and their customers.*
>
> *Philippe Le Pape*

But: the need for **multi-factor authentications** will not go away; in fact, well-designed systems will insist on it. I am absolutely certain that the devices we use in the very near future will contain a fusion of **biometric authentication** features for increased security, as well giving the user options should the device become confused (for instance, the need to bypass the fingerprint scanner following a hand injury).

One of the problems faced by those of us either deploying services or creating security for those services is the disconnect in understanding by individual consumers of the threat level that exists to any device connected to the internet. Symantec recorded 348 million exposed identities through attacks in 2014, almost 90 million coming from financial and government sectors. There is still a job of work to be done in raising awareness of cyberspace issues. President Obama's CNAP and the EU **Cybersecurity** Strategy are a start, but there is a global education role for the industry to play too.

Lastly, something else I am an advocate of: that the role of biometrics is to ensure that the security and privacy of an individual's data (or, indeed, an enterprise) is not undermined at any point in a digital transaction. Its role is to serve and protect, not to be an Orwellian oppressor.