Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Biometrics As a Security Panacea? Far from It!

By: Darren Guccione

Users should think of biometrics as a key part of multi-factor authentication – not the only lock on the door

Crystal ball predictions are common in such a dynamic, fast moving environment as the computer industry. Some prove accurate, others quite the opposite. Now from some corners of the world of punditry comes this latest prognostication: That single-most familiar and ubiquitous computing practice of virtually every computer and device user – the password – is on its last legs, about to be replaced by biometrics.

Some surveys and studies recently seem to indicate a rising tide of confidence by consumers in the ability of biometrics to secure digital data, possibly even obviating the need for passwords. That is not only an incorrect assumption. But also it is a potentially dangerous one that could put your digital data at great risk.

So it is when it comes to passwords and biometrics. This is not to say that biometrics cannot be a significant part of an effective strategy to thwart hackers and cyber attacks, if not a very convenient and quick way of doing so. However the reality is that biometrics by itself cannot provide security on its own, but rather as a component of the kind of multi-factor authentication that virtually all security experts advocate today. In other words, as far as biometrics go, convenient – yes. Comprehensive – no.

Surveys point to increasing biometric confidence

This rising sentiment for biometrics is apparent in a recent survey of some 1700 users undertaken by Keeper Security. In that survey, 47 percent of all respondents believe that biometrics are convenient as well as hard to fake. Another 20 percent say biometrics offer strong authentication and accountability. But one in four – 25 percent - also say they would be uncomfortable using biometrics, with baby boomers leading the pack here at 28 percent compared with millennials (21 percent) and GenXers (23 percent). About one in four respondents reported they feel uncomfortable using biometrics.

Another recent survey found that only half of the 1,000 respondents were very familiar with biometrics, but nonetheless see certain biometric techniques such as fingerprint recognition and eye scanning as effective for securing online payments. However, that survey also found that half the respondents see biometrics as a means of eliminating password use and the issues created when passwords are forgotten. This is important, given that virtually *all* mobile digital devices will be equipped with biometric capabilities by 2020 – just two years out.

Things are not what they seem

Therein, however, lie the misperception that biometrics alone can do the job of securing digital data. This simply is not true. For one thing, when for example a fingerprint is used to unlock an iPhone, the user's password is 'unlocked' and still used to open the phone for use. That is, while

the fingerprint technique is convenient, it still does not secure or unlock the phone on its own. And if the underlying password is a weak one, the device is still very vulnerable to attack.

Also if a hacker discovers a weak password such as 123456, the attacker can then log into the compromised device and establish a new fingerprint – theirs! The only way around this vulnerability is to set up stronger passwords.

Breaks in the biometrics armor

Going "all in" for biometrics can be risky, costly, and dangerous. Consider what may be the world's most ambitious biometric identity project to date, the massive Aadhaar project wherein the central government of India has provided unique biometric identifiers for all 1.2 billion Indians. With the data stored in a massive database, an individual's identity can allegedly be verified in 200 milliseconds – about as long as it takes to blink. The main driver of this biometric project was to enable residents to more efficiently access various government benefits, such as food coupons and loans – all with assurances of the utmost security of highly personal data.

But various reports out of India in the last year show the biometric data is anything but safe and secure, little so that some people were selling biometric identification data to the highest bidders on WhatsApp. Various journalists and technologists have claimed the system can be compromised in various ways, including allowing certain third parties to access the data. This simply cannot be done in a system based on multi-factor authentication in which strong passwords are a central part of the solution.

Stop thief!

The seemingly easy theft of biometric data is not necessarily new. Just over two years ago the U.S. Office of Personnel Management (OPM) admitted that upwards of 5.6 million unique biometric identifiers - -fingerprints - of federal employees were swiped in a massive server breach. With the blame-game pointing fingers at possible national governments as the sources of the hack, such a government may now possess the fingerprint biometric ID of various U.S. government officials – an ID that can no more be changed by the victim than they could change the color of their eyes. By contrast a stolen or compromised password can be instantly replaced by a new password.

While these and other stories emerge of the failings of biometric-based security systems to protect sensitive personal data on their own, some of the best and brightest in the entire high-tech field are doing their part to boost the effectiveness of the tried and true password.

At the recent Consumer Electronics Show (CES), the Wi-Fi Alliance that sets voluntary safety standards for all wireless devices, announced a new and safer Wi-Fi to be unveiled later this year. The Alliance consists of major tech players like Microsoft, Apple, Samsung, Intel, and Cisco. With a core belief that passwords are at the heart of protection for new Wi-Fi Protected Access 3 (WPA3) standards the Alliance is promoting, the new standards will offer very strong data protection even when some users defer to notably bad and easily hacked passwords, such as 12345.

No substitute for strong passwords

In actuality there are several very good reasons why strong passwords are a fundamental part of a factor authentication strategy and will continue to be so for years to come. For one thing passwords can be changed from time to time. That is obviously not the case with fingerprint or facial or iris recognition.

Also because strong passwords exist only in the mind of the user, or more effectively held with a comprehensive password management solution, they are highly resistant to most attacks based on attempts at compromising passwords.

And data is generally encrypted for the utmost in security. Encryption requires a cipher key to

decrypt, a key that can only be derived from a strong password typed precisely (or entered by the password management solution).

Seen this way, it is clear that biometrics is surely convenient and growing in popularity, but cannot on their own be the primary and only defense against hacking. They are, however, an effective second or third component of multi-factor authentication.

Finally, survey after survey, including the recent one from Keeper, show continued poor password hygiene by many end users, such as the use of weak passwords or use of strong passwords frequently forgotten or use of the same passwords for access to different systems, devices, and sites. Users are well aware of the consequences of doing so, such as having to give up on online purchases when passwords are forgotten and cannot be easily achieved.

Conclusion

The simple and readily available and often free solution to all this is a comprehensive password management solution. Experience has shown these solutions can make proper password usage the norm, and greatly limit if not eliminate most of the successful attacks caused by weak passwords. Users need remember but one and only one password to unlock the underlying system that then generates and uses highly complex, strong passwords that are virtually unhackable.

Yes, biometrics is becoming more mainstream but it's important for the public to understand the difference between security and convenience. Every individual user and organization has a different level of risk aversion. Biometrics cannot provide security on their own merit, and a strong password management strategy is critical in preventing cyber attacks and data theft. The pairing of a comprehensive password management solution with a biometric solution offers the highest levels of data security in an increasingly dangerous cyber world.