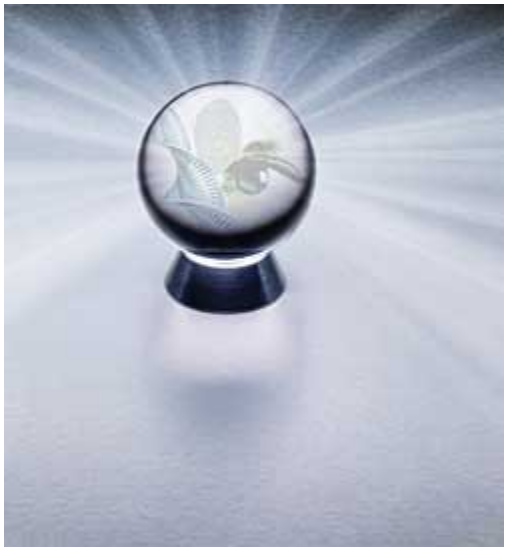
SECURITY PRODUCTS MAGAZINE
http://www.secprodonline.com/



Dispelling the Myths

By Mizan Rahman · August 2007

Misguided beliefs about biometrics should be investigated for proper understanding of the technology

DISPELLING myths and misunderstandings about biometrics and its increasingly common use in everyday professional and personal lives is a tough task, even in these modern, technologically-advanced times.

Sometimes these myths can perpetuate to the point of blatant banning tactics by people and organizations who are confident that the use of biometrics will cause more harm than help the should-be beneficiaries.

Sure, it can be intimidating to scan a fingerprint, hand, iris, retina, face or DNA, even considering the fact that many people don't understand, or don't want to understand, how the biometric system works and how it uses identifying characteristics.

Understanding exactly how biometric technology uses a scan of someone's fingerprint in a variety of applications may be the only hurdle these skeptics and banners need to jump before they are able to ultimately embrace these solutions.

Biometric identity management technology is based on who you are, rather than your possession of an ID card or knowledge of a password. Biometrics is not meant to entirely replace the existing methods of identification, but to build on them in order to strengthen and enhance security benefits.

Today, fingerprint scanning or reading is the oldest and most pervasively-used biometric science. Fingerprint hardware and software technology is being increasingly used in point-of-sale solutions, law enforcement, security, education, fitness, child care, banking, healthcare and the restaurant and hospitality markets.

Fingerprinting is feared because of its association with criminal identification and the government. Biometrics did get its start in these fields, but just as cell phones and the Internet have consistently evolved, biometric technology has advanced far beyond its initial application.

Fingerprint-based authentication provides a rather elegant solution to all of the problems associated with remembering passwords and codes, numerous hardware tokens and swipe cards. Since fingerprint technology has become affordable and reliable, its use in identity authentication is rapidly on the rise.

Because of its advancement and popularity, more myths exist about fingerprint scanning than about any other biometric technology. Two of the most prevalent myths include the notions that fingerprinting used anywhere, in any form, is a sign of Big Brother monitoring and fingerprint scanning is nothing more than the legal crime of identity theft.

The Security of Biometrics

Fingerprint scanning is used in a variety of commercial applications, such as time tracking, door entry, member or customer identification, cafeteria lines, computer access and retail smart cards. With each of these applications, it is important for the user to understand exactly how the system recognizes identity and what happens to a person's fingerprint once it has been enrolled in the system.

There has been much confusion as to what an algorithm actually is and how it is used by the biometric software. Essentially, when a fingerprint is scanned, the extraction algorithm used in the software recognizes unique points of the person's fingerprint. Based on these points, it creates a string of numbers—called a biometric identity template—that are assigned to this fingerprint only. Then, when an

person scans their fingerprint at any point after enrollment, those unique points are recognized by the fingerprint software, and a matching algorithm is called upon to recognize which person belongs to this print template.

The most important point to remember is that the biometric identity template that is created and stored cannot be reconstructed into the fingerprint image. In other words, the extraction algorithm that creates the identity template is one-way. The algorithm used is not standard across any centralized database, such as those maintained by state agencies and the FBI. In addition to these safeguards, all system data is AES encrypted, which is the same encryption standard that is used by the government and the NSA for top-secret information.

Understanding this process is vital to realizing how the danger of identity theft or a security breach is significantly lessened, if not completely eliminated, through the use of a proprietary algorithm with no stored image or encrypted data. A universal fingerprint database is not being created. Even if someone meant to harness identity data by breaking into a system, they would only find useless strings of numbers, as no image of any fingerprint is ever stored within the system.

Myths, fears or concerns regarding the security of biometric recognition technology can quickly be dispelled just by researching and understanding the process that is involved in the correct identification of each fingerprint.

A Tale of Two Schools

A common application of fingerprint scanning technology over the past several years has been its integration into cafeteria POS systems. Two school districts have recently had two very different experiences with their implementation or, in the case of one school, attempted implementation.

The Taunton, Mass., School District ultimately abandoned a plan that would have allowed students to pay for lunch by scanning a fingerprint. This decision by the Taunton School Committee came after a small team of parents and the American Civil Liberties Union cried out to "Ban the Scan" in every public meeting on the issue.

The lack of understanding among this small group of parents was evident in a final comment to the committee.

"You wouldn't want your children's or grandchildren's fingerprint information entered into a district-wide database," said a parent.

Clearly, this was a misunderstanding, as the fingerprint recognition technology was going to be used to identify the students through a proprietary system that would recognize unique points of a student's fingerprint and was not to be used to verify them within a district-wide database.

Due to this unfortunate misunderstanding, Taunton students, parents and the school administration missed out on the impressive benefits that biometric recognition technology offers, including approximately 20-percent increases in student cash deposits; elimination of burdensome and often hard-to-remember passwords, PINs, ID cards or lunch tickets; decreased acts of bullying or injuring of students for lunch money; reassurance to parents that their children will never be served food to which they are allergic; parents' knowledge of what their child is eating and the ability to monitor choices to ensure a healthy diet; quicker lunch lines; increased privacy for student's of subsidized food programs; improved accounting; improved overall efficiencies and increased revenue, which in turn, would improve the education experience of each child.

The Douglas County School District, based in Minden, Nev., has been reaping these benefits. The nutrition, IT and school administration departments for the district collaborated to integrate and test fingerprint scanning POS technology in two schools this past year.

The most obvious difference between the Taunton and Douglas school districts was the desire of the Douglas officials to truly understand the processes involved in biometric identification and to test the system.

A Common Misconception

A sense of skepticism toward unknown technology is an admirable quality inherent to intelligent individuals, and protecting children from an Orwellian world is a cause that any parent should advocate. However, distrusting a technology without gathering a detailed understanding of the benefits the innovation will provide or without even testing the technology can be detrimental to the future of the same children we are trying so hard to protect.

In the Taunton situation, fear, rather than fact, was perpetuated by a handful of people. Fingerprint technology cannot harm children in any way. Software has been developed with privacy concerns in mind.

Most people carelessly give away private information each day. People state their Social Security number when asked. Bank statements are thrown away where they could easily be retrieved. We pay for EZ passes can give the state location information each time a person passes through a toll. And wireless devices emit a signal that can easily be traced.

With all of this information readily available, a worthless, binary representation of a fingerprint within a secured system seems like the last place a potential thief would turn for identity information.

If for some reason a fingerprint was truly desired, it would be easier to lift the print from something that the child had held rather than to try to piece together an insolvable mathematical representation. To impugn that fingerprint technology is a sign of Big Brother preying on children is a misconception. The technology is meant to ease the worries associated with protecting secure information, not to create more.

The Future of Biometrics

Biometric software, SDKs and hardware solutions should allow developers to rapidly and easily integrate into network systems and applications for a complete system with little development effort. Biometric service and software product providers also should enable engineers to support multiple algorithms.

Overall, products should help engineers avoid the headaches of long-term integration, burdensome internal development and ongoing maintenance requirements, thus furthering the credibility and goodwill of biometrics among buyers and users of this evolving technology.

Educating the current and future users about the facts and benefits of biometric technology is another key contributor to its credibility and acceptance. Educational outreach activities from responsible experts on both sides will only further the adoption of truths, which dispel the myths of this exciting technology. Vehicles of information have the ability to spread the credible and beneficial messages about biometrics and are needed in more abundance.

Biometric technology has proven both effective and safe for a wide variety of applications. People should take the necessary actions to obtain a detailed knowledge and understanding of innovations like biometrics before hindering a progress to a bright and technologically-advanced future.

About the author

Mizan Rahman

Mizan Rahman is the founder, CEO and chief software architect of M2SYS, a biometric fingerprint identity management company.

SECURITY PRODUCTS MAGAZINE
http://www.secprodonline.com/

For further info, please contact:
Central Time Clock, Inc.
5-23 50th Avenue
Long Island City, NY 11101
Ph#: 718-784-4900