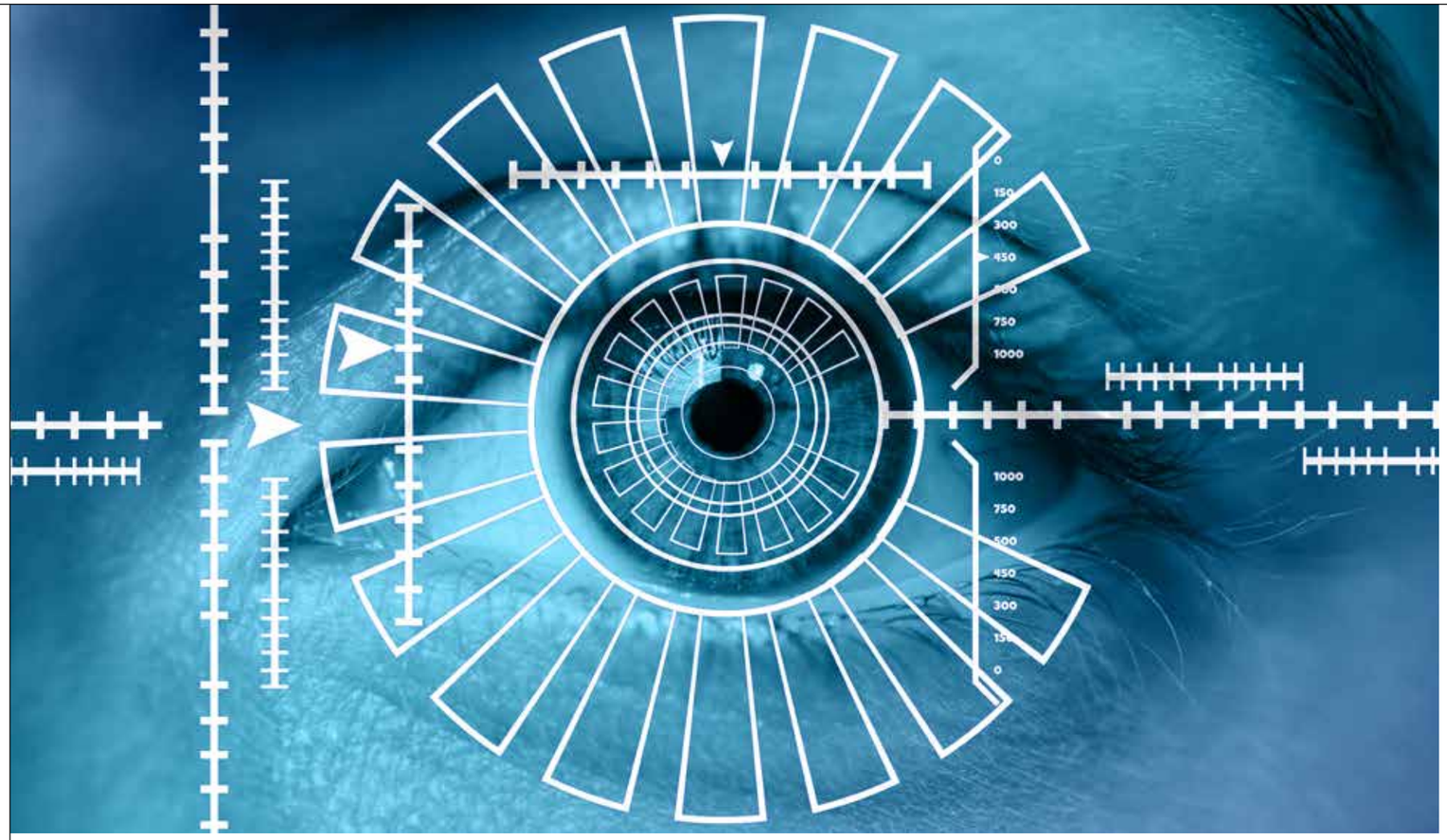

BIOMETRIC BUILDING BLOCKS

Biometric technology leverages a variety of inherent security features that help curb cyber crime

Fredrik Martinsson *explains how biological features hold the key to better*

Technology has altered the way we live and work. At work it has offered flexibility, productivity and scalability for businesses everywhere, yet there are two sides to this coin. As the world becomes increasingly digitised, cyber criminals can target an increasing number of connected devices and services, all of which host larger amounts of more sensitive data creating a much larger attack surface for criminals to exploit. Attacks can impact not only the individual or organisation, but their customers and wider stakeholders too.

It is no shock that cyber attack cases continue to rise year on year. Compared with H1 2022, H1 2023 witnessed overall increases in ransomware attack victims across almost all industries including banking, healthcare and IT. High-profile cases such as the cyber attack on document transfer service MOVEit – which led to a series of data breaches of companies including PwC, EY, Health Service Ireland and payroll provider Zellis – have highlighted that cyber crime does no discriminate when it comes to industry or company size. It not only damages an organisation's revenue, reputation and infrastructure, but the effects of malicious attacks are set to cost the world $10.5-trillion annually by 2025.

In light of this, meeting this challenge head on has become a top priority for security professionals globally. It's anticipated that investment in improving cyber security will surpass $260 billion by 2026 and stronger authentication is increasingly key to organisations' strategies.

Afterall, 80 percent of computer hacks and cyber crimes have come as a result of passwords being compromised. Not only are traditional passwords demonstrably unsecure in defending against the sophisticated attacks of today, they are not even that convenient. As many as 60 percent of consumers say they have too many passwords to remember, with some having over 85 for their professional and personal accounts. In addition, an alarming 41 percent of us re-use or only slightly vary our passwords.

Humans are a fundamental link in the IT security chain, with some even citing human error as the number one cyber security threat to businesses.

Despite all the operational benefits provided by digitisation, it is clear it is also causing many traditional security protocols/solutions to become redundant. It is essential that we evolve digital security in line with the threats of today and tomorrow. If we do not, we risk our current security practices becoming even more outdated and ineffective. An area of focus for this evolution should limit the effect humans have on the IT security chain.

It is impossible for users, technology vendors and organisations to be entirely immune to cyber attacks. Yet everyone can take steps to level-up security with more robust authentication methods that specifically serve their business's needs and fight against future breaches. Enter biometrics…

Biometric technology can form a fundamental building block, either independently or as an integrated part of multi-factor authentication process, in personal and organisational security. It is important to understand however that biometrics is not a one-size-fits-all solution. Organisations require varying levels of scalable security and authentication and not everyone is trying to protect Fort Knox.

Biometric technology leverages a variety of inherent security features that help curb cyber crime. For example, implementing biometrics makes an immediate jump from single-factor authentication – using only something you know (PIN/password) – to multi-factor, based on something you have and something you are.

As part of this, the management of personal, sensitive data (such as fingerprints) becomes paramount. Biometric authentication can utilise a 'privacy by design' approach that inherently protects end-user biometric data by doing everything on the same secure device. In other words, biometric data is captured, enrolled, stored and managed all on the same device, without ever leaving the device owner's control.

It is a common misconception that biometric data is stored as images that, if stolen, would permanently compromise the corresponding biometric credential and its use for any device or application. This is no longer the case. In the case of a fingerprint sensor, data from the biometric sensor is captured and stored as a template in the form of a mathematical representation. This ensures that hacking is useless, as the template code cannot be reverse engineered into the original fingerprint image, nor can it be linked to other services or personal data. All the hacker would see would be a series of meaningless numbers, with no way to translate the data.

BIOMETRIC TECH OFFERS ROBUST CYBER SECURITY OPTIONS TO SUIT AN ORGANISATION'S NEEDS

Back when biometric technology was first being introduced in a commercial format, spoofing only required a very high-quality photocopy of the required credential. You may have even seen gummi bears being used as a means to spoof fingerprint sensors – simply press the fingerprint on the back of the gummi bear and voila, you're a hacker.

Nowadays, extensive research and development has created advanced sensors and algorithms that are extremely difficult to spoof. A successful spoof today would require considerable care, skill, money and time. Also, a number of factors would need to come together perfectly, which is highly unlikely in reality, including:

A good latent print. To retrieve a latent print that's high-quality enough to work, either a willing volunteer or the commitment to stalk a victim until a viable print can be retrieved is needed.

Advanced Photoshop skills. Even if a quality latent print is secured, advanced editing skills are needed to get the level of 3D detail needed.

A lab environment – or very similar. To convert these prints into an effective mold usually requires a lab environment and significant effort.

Access to the device. To perform the hack, the attacker also needs access to the device in question for an extended period of time. Most people will report their device lost or stolen, or block their debit card, before anything can be achieved. Also, most devices only give attackers a small number of attempts to gain access before reverting to passphrase and locking.

This is a far cry from the days of the humble gummi bear.

Fingerprint sensor spoofing that you see in the media today is either a proof-of-concept or a cooperative spoof. These take months to work and rely on a highly skilled team of experts and a tailored scenario of circumstances.

Most criminals will only put the necessary time, effort and resources into a spoof if it can be replicated and scaled across multiple devices, people or companies. Spoofing a modern-day fingerprint sensor, if it was even possible on non-lab conditions, would only enable the criminal to access one person's devices and services, for a

limited time. Put simply, the risk and investment outweigh any potential reward.

Biometric technology offers various robust cyber security options to suit an organisation's specific needs or requirements. For example:moving away from passwords, PINs and token systems for everyday authentication.

THE USER ONLY NEEDS THEIR BIOMETRIC CREDENTIAL IN ORDER TO ACCESS THEIR DEVICE

Many of us still rely on the traditional PIN or password for security in our work and personal lives. Biometric technology provides a very real possibility for businesses and users to eradicate unsecure passwords and PINs entirely.

Using the example of a social engineering attack, criminals trick end-users into giving away sensitive security information – such as a PINs or passwords – this is called phishing. Phishing is the most common form of cyber crime, with reports estimating 3.4-billion malicious emails sent every day. It is these attacks that we as individuals and organisations are most vulnerable to.

Through leveraging consumer biometrics, the user needs only to present their required biometric credential in order to authenticate their device or service. Without the need for PINs or passwords, the user cannot share the required information needed to initiate the attack. This also addresses those cyber risks that are generated by mistakes or complacency, such as creating a password that is easily guessed or employed across multiple accounts.

Another way criminals initiate hacks is by shoulder surfing – glancing over a user's shoulder to spy sensitive security information. Biometric technology is not 'glanceable' like a PIN or password is. This removes the risks of shoulder surfing entirely.

Leveraging biometric technology for authentication doesn't add any additional steps to the authentication process. This means that not only does the technology immediately increase security, it also maintains, and often increases, convenience and user experience. A recent report found that 55 percent of individuals and IT specialists would rather protect their accounts by an alternative method that doesn't involve the use of passwords. In the digitised world of today where convenience reigns as king, a solution that can simultaneously enhance security and convenience poses an attractive proposition.

In the world of security, it is widely accepted that nothing can be 100 percent secure. Traditional physical access security solutions – like keys and safes – through to logical access security solutions – like biometrics and FIDO2 tokens – are there to make life difficult for criminals. Criminals don't want to deal with how time consuming, expensive and risky it can be if they were to try and hack into a device or application. In other words, most security solutions are deterrents, not preventative solutions.

Biometric technology offers a convenient route for people and organisations to move away from basic traditional security measures to more sophisticated, multi-factor digital security measures. This foundation can then be built on with different biometric systems and implementations that protect everything from smaller scale operations to those possessing high-value assets. Biometric technology offers choice and, more importantly, the ability to integrate security solutions that are tailored to specific needs, budget and existing infrastructure ●

Fredrik Martinsson
is Sr. Director Business Development at Fingerprints

Biometric technology provides a very real possibility for businesses and users to eradicate unsecure passwords and PINs entirely

Picture credit: Fingerprints