princeton IDENTITY

BIOMETRICS BRING MULTI-FACTOR AUTHENTICATION TO THE NEXT LEVEL

The conflict in Ukraine has heightened concerns that Putin and his allies will escalate cyberattacks against the west. As sanctions continue to squeeze the Russian economy, The Harvard Business Review argues that U.S. and Western corporations may now face the most acute cyber risks ever as Russia strikes back using its considerable cyber capabilities.[1] The CISA, FBI, and NSA recommend that organizations enhance their cyber posture, including the use of multi-factor authentication for all users of identity and access management applications.[2]

The most familiar form of multi-factor authentication combines a username and password with a randomly generated SMS code. When we're asked to enter the texted code before accessing a software application or online service, the host is attempting to verify that we are who we say we are. It assumes that we're probably not an imposter if we can retrieve the code. Other examples of multi-factor authentication are access control readers that require both a card and PIN code to enter a building, or software that asks a series of security questions – like the name of our first pet or elementary school – after we provide a username and password.

Unfortunately, none of these forms of multi-factor authentication are as secure as we once thought them to be. Many of us have bypassed them ourselves, on occasion, without thinking twice. For example, maybe you've logged into Netflix using a friend's account, and the friend has texted you the SMS code they received so that you can enter it and fool the system. Or, you've shared a single software license with multiple colleagues, texting the SMS code to each other as needed.

The security of dual PIN and card readers may also be circumvented. While the PIN requirement may prevent a stolen card from being used, family members, friends, and colleagues sometimes share cards and PIN codes with each other, or use a code that's easy to guess.

Hackers, too, have found ways to bypass multi-factor authentication. Through phishing and social engineering, users unwittingly provide them with the information they need to redirect where SMS texts are sent or answer personal knowledge questions.

[1] https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

[2] https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

Yahoo and LinkedIn have both suffered massive security breaches, despite having two-factor authentication in place at the time of their respective attacks. Since 2012, usernames and passwords for three billion Yahoo users and 167 million LinkedIn users have been compromised.[3]

Now, with cyber threats ratcheted to new heights, how can organizations ensure that their multi-factor authentication is infallible? The answer lies in biometrics. Biometric identity solutions can be integrated within physical and logical security applications, creating a virtually impenetrable obstacle for imposters.

Biometrics replace knowledge-based identifiers with physiological ones, like fingerprints, vein patterns, or facial geometry. The patterns within the iris, for example, are so unique to each individual that a false match occurs less frequently than once in one million. Furthermore, bad actors cannot reverse engineer an "iris" to match that of an enrolled user. When combined with another form of authentication – be it a secondary biometric modality, a physical card or fob, a mobile credential, or password – there is no more secure identity management solution available.

Biometrics are already making inroads in physical security applications. They're being used to secure mission-critical locations like data centers, utilities, building infrastructure, bank vaults, drug closets, and laboratories. Dual authentication is achieved by storing an enrollee's biometric data on a 13.56 MHz access control SmartCard or smartphone. Possessing the credential is no longer sufficient to gain entry. Users must also physically match the biometric data stored on the presented credential.

Biometrics can also play a role as companies seek to implement Zero Trust policies to protect their networks. Zero Trust architecture requires users to verify and authenticate their identity each time they initiate an interaction with the server. Opening software, opening a file, editing a file, saving a file, and sending an email all require verification and authentication. It is far faster and easier for an employee to place a finger on a reader or look into a camera than it is to enter a long, difficult password over and over again. It's also much more secure. As most companies intend to maintain a hybrid workforce moving forward, biometric solutions tied to Zero Trust protocols can ensure employees VPN-ing from home pose no greater risk to network security than those on site.

In our digitally interconnected world, practicing good cyber hygiene and investing in necessary security technologies should not be new to any organization. Hopefully, your company has systematically reviewed and upgraded its cyber posture over time. However, implementing cyber best practices has never been more critical than now. All U.S. government security agencies advocate the use of multi-factor authentication. Incorporating biometrics as part of your plan will deliver the greatest efficacy. Today's systems are surprisingly affordable and easy to install. And, by any measure, they're a true bargain compared to the cost of a crippling, devastating network breach.

ABOUT PRINCETON IDENTITY

Princeton Identity is the identity management company powered by biometrics, making security more convenient, accurate, and reliable than ever before. Leading the revolution toward a more intuitive, efficient, and natural security experience that keeps people and businesses moving, Princeton Identity uses iris recognition, face recognition, and other biometric technology to enable businesses, governments, and global organizations to streamline identity management, resulting in improved safety and protection. Formerly a division within SRI International, Princeton Identity spun out as an independent venture in August 2016.

[3] https://www.forbes.com/sites/forbestechcouncil/2018/02/21/when-two-factor-authentication-fails-rethinking-the-approach-to-identity-security/?sh=4ba9326e6fea