Biometrics: Addressing Fear and Enhancing Trust

Given the ability of threat actors to attack password-protected platforms, the digital trust community is continuously looking for more secure login methods. "Passwordless" authentication is gaining traction as a result. Biometrics doesn't require a specific hardware device, a separate authenticator application, or links or one-time passwords sent via email or SMS (both of which are vulnerable to attack), setting it apart to emerge as an attractive option for passwordless authentication.

Why We Like Biometrics

As a customer, I want painless identity verification, and I also want to believe that my access is secure. Like most people, I have a variety of shopping or rewards apps on my smartphone, and several apps provide the option of either logging in via a password or biometrics (fingerprint scan or facial recognition). If I want to show my membership number for the cashier to scan or to select a predefined payment method so I don't have to reach for my wallet, I need to go through this authentication process. Holding my finger over a scanner is substantially easier and quicker than typing a password, even if I have it saved on the device. Vendors who provide this biometric option get my business, and my trust, over those who don't, unless there are other factors that cause me to see that organization as distrustful.

K. BRIAN KELLEY | CISA, CDPSE, CSPO, MCSE, SECURITY+

Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server, and Windows Server. He has served in a myriad of other positions, including senior database administrator, data warehouse architect, web developer, incident response team lead, and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps, and user groups.

Moreover, biometrics are increasingly being used to vet users for services such as hotel check-in, car-sharing, or verifying users when they visit their financial institution for banking services. Organizations providing solutions that reduce friction are surging ahead of their competitors.[1] There is increased trust in these organizations because they provide better features in terms of quality of service. Better quality tends to generate increased trust.

Why We Fear Biometrics

When any of our biometrics are captured, there is a privacy risk. Since our biometrical attributes can't be altered as easily as a password or physical device, once any of our biometric data is captured, it could be misused. There is also the possibility that sensors and related devices used to capture our biometric data can collect more data than we want, and certainly, more than is necessary for the purposes of identification. These concerns led the US Federal Trade Commission to publish a warning to consumers, albeit one that didn't get much attention from the general public. The FTC said, "the increasing use of consumers' biometric information and related technologies, including those powered by machine learning, raises significant consumer privacy and data security concerns and the potential for bias and discrimination."[2]

Part of the warning focused on the fact that biometrics could help track individuals in ways previously not possible. For instance, stores such as Walmart acknowledge the use of facial recognition technology for security and operational purposes and indicate that such data is used to help ensure security, prevent theft and fraud, and help maintain the safety of individuals and properties.[3] Already, most retail stores track purchases against credit card numbers or other identifiers. With the data collected, these retailers can predict your buying habits. This came to the forefront about a decade ago when news broke that Target had used data collection and analysis methods to predict which customers could be pregnant, allowing for targeted marketing in a way never seen before.[4] The use of biometrics adds

yet another mechanism of tracking and prediction, which may be used by retailers in unexpected—and potentially unwanted—ways.

Opting out of biometric mechanisms comes with its own challenges, though. There are reports of a US senator who declined facial recognition at an airport and encountered issues with the US Transportation Security Administration as a result.[5] Opting out of biometric mechanisms may also mean we are no longer able to access information and systems we need. Case in point: a number of years ago, I was at a data center facility that had switched over to a fingerprint scan biometrics system to gain access to the area where our hardware was racked and running. One of our database administrators, citing privacy concerns, did not want to register his fingerprint in the system. This put our team in a bind because there was no other option available for him to gain access to the room. He relented and agreed to have his thumbprint scanned, but had he not done so, we would have had to operate one person short for the week.

Addressing the Fear

The accuracy of Target's model and its subsequent actions to use the insights gleaned from that model reveal the dark side of data collection, even without biometrics. The issue with the targeted ads is an ethical one. Target dealt with this issue by randomizing the ads to hide the fact that their model was able to predict what shoppers might need (pregnancy-related items).[6] While this dealt with the immediate public perception problem, the lack of transparency could have come back to hurt the retailer. So, how can organizations address the fear of data misuse, especially biometric misuse?

From a digital trust perspective, there are a number of recommendations for best practices on data privacy for biometric data. For instance, the International Biometrics and Identification Association (IBIA) has its best practice recommendations for commercial biometric usage that closely resemble recommendations for any type of digital data collection, and include notification of use, ability to opt-out when possible, transparency on data use, data protection mechanisms (including encryption), auditing, and the like.[7]

Most consumers will accept the collection of data for the purposes intended, especially if it

reduces the friction of transactions and obtaining services. Organizations that follow the best practice recommendations will certainly have an advantage in the digital trust ecosystem. If I know an organization is going to minimize what data it collects and only use it for the purposes I authorize, then I'm going to feel more favorable and trust that organization more than a competitor who doesn't offer similar transparency and protection. Most of us would agree.

Issues with Biometric Solutions and a Silver Lining

Biometric solutions are not the silver bullet to kill the identity theft werewolf. These solutions can have bugs just like any other technical software. For instance, one particular biometric solution was found to have a number of vulnerabilities, including SQL injection.[8] These solutions can be bypassed, and biometric data can be stolen, depending on the severity and reach of the vulnerability.

However, the reality is that quite a bit of biometric information is already out and available in the public domain. For instance, photos appear on social media sites such as Facebook, X, Bluesky, and LinkedIn, to name a few. Theft of a picture from a biometric system isn't necessarily more destructive than someone successfully digital stalking a target and gathering relevant pictures.[9]

LOOKING FOR MORE?

- Read *Biometrics Audit Program.* *https://www.isaca.org/biometrics-audit-program*
- Learn more about, discuss, and collaborate on privacy and security in ISACA's Online Forums. *https://engage.isaca.org/onlineforum*

Passwords can be reset, but biometrics cannot. Once someone's biometrics are compromised, there is no tabula rasa for bringing identity back to an uncompromised state.

Fingerprints aren't so easily gathered, and they don't change, so their theft is more significant. That said, physical proximity is required to use fingerprints, and while earlier solutions could be fooled by gelatin fake fingers with the fingerprint ridges molded on, many solutions now include thermal scanners which can detect the temperature difference between the ridges and valleys, making it harder to fool the systems.

Because fingerprints can be used to positively identify someone, their theft can cause problems in ways we don't normally consider. While the organization collecting biometric data may have done everything correctly from a privacy perspective, a threat actor who gains said data in a data breach is unlikely to hold to the same ethics. For instance, in the 2015 US Office of Personnel Management (OPM) breach, some 5.6 million fingerprints were stolen. As a result, the Central Intelligence Agency (CIA) pulled officers from the US Embassy in Beijing to prevent their compromise.[10] Passwords can be reset, but biometrics cannot. Once someone's biometrics are compromised, there is no tabula rasa for bringing identity back to an uncompromised state. OPM responded as we often see organizations do when they experience a data breach around identifiable data: they offered some duration of identity theft and fraud prevention services. While this does help to restore some trust in an organization, it won't return trust back to its state prior to the data breach.

Biometrics Aren't Going Away

The use of biometrics for authenticating identity is increasing, and no one expects that trend to slow down any time soon. Passwords are increasingly a poor mechanism to secure identity, and they are slow and cumbersome compared to a biometric solution. As customers demand more biometric solutions, companies that choose to offer such solutions gain advantages in trust over competitors that are slower to implement. In general, biometrics are safer, and even if they weren't, they feel easier and safer than traditional password solutions. However, in our rush to implement such solutions, we must properly address data privacy and security concerns. After all, misuse of data or a data breach could undo any advantage we may have gained by giving the customers the ease they want.

Endnotes

1 Stowell, T.; "How Biometrics Are Transforming the Customer Experience," *Harvard Business Review*, 29 March 2023, *https://hbr.org/2023/03/how-biometrics-are-transforming-the-customer-experience*

2 Federal Trade Commission, "FTC Warns About Misuses of Biometric Information and Harm to Consumers," 18 May 2023, *https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers*

3 Walmart, "Walmart Customer Privacy Notice (Online and In-Store)," 6 March 2025, *https://corporate.walmart.com/privacy-security/walmart-privacy-notice*

4 Wagstaff, K.; "How Target Knew a High School Girl Was Pregnant Before Her Parents Did," *Time Magazine*, 17 February 2012, *https://techland.time.com/2012/02/17/how-target-knew-a-high-school-girl-was-pregnant-before-her-parents/*

5 Pallardy, C.; "The Tug of War Between Biometrics and Privacy," *InformationWeek*, 13 August 2024, *https://www.informationweek.com/cyber-resilience/the-tug-of-war-between-biometrics-and-privacy*

6 Berkley Fung Institute for Engineering Leadership, "Avoiding the Traps of Big Data," 29 October 2013, *https://funginstitute.berkeley.edu/news/avoiding-the-traps-of-big-data/*

7 International Biometrics & Identification Association, "IBIA Privacy Best Practice Recommendations for Commercial Biometric Use," 8 August 2014, *https://www.ntia.gov/files/ntia/publications/ibia_privacy_best_practice_recommendations_8_18_14.pdf*

8 Nelson, N.; "Scores of Biometric Bugs Emerge, Highlighting Authentication Risks," *DarkReading*, 12 June 2024, *https://www.darkreading.com/vulnerabilities-threats/scores-of-biometrics-bugs-emerge-highlighting-authentication-risks*

9 Nelson; "Scores of Biometric Bugs"

10 Global Resilience Institute at Northeastern University, "5.6 Million Fingerprints Stolen in OPM Data Breach," *https://globalresilience.northeastern.edu/5-6-million-fingerprints-stolen-opm-data-breach/*