



Biometrics Threat Report

CYBER THREAT INTELLIGENCE REPORT

Compiled by Liam Ryan
Date: 22 October 2024

Executive Summary

A biometric system is a technology that uses unique physical or behavioral characteristics, such as fingerprints, facial recognition, voice patterns, gait analysis, or eye scans, to identify and verify individuals. They consist of four main modules: sensor, feature extractor, matcher, and decision. These systems can be localized or centralized, with centralized systems often raising higher privacy concerns.

Despite their perceived security, biometric systems are not infallible and can be bypassed, especially if users are not educated on cyber threats.

- Threats to biometric systems include limited revocation of biometric data, wide credential spread, biased models, and the potential for deep fake attacks. Attackers may exploit vulnerabilities through spoofing, replay attacks, brute force, and other methods.
- Although attackers have exploited biometric systems in the past, they are not currently being targeted at an alarming rate. This is likely because traditional methods, like phishing, are still more cost-effective for attackers.
- As is the case with passwords, it is recommended to combine biometrics with multi-factor authentication (MFA) to enhance security, as relying solely on biometrics is not sufficient.
- Privacy and regulatory risks are significant, particularly with centralized storage of biometric data. While biometric data is typically stored as non-reversible hashes, misuse by custodians of this data has led to breaches. Some jurisdictions in Canada, the US, and the EU have placed strict limitations on its use.

Organizations should not expect that switching to biometrics alone will improve their security. If the industry continues to trend towards biometrics, the targeting landscape may shift. While biometrics offer convenience and some security improvements, they should be part of a layered defense strategy to effectively mitigate risks.

Introduction

Unlike traditional systems that rely on something you have or know; biometrics use unique personal traits—something you are. This makes them more convenient as users do not need to use ID badges which they can lose, or passwords which can be tedious to remember and rotate. Moreover, biometric authentication is often seen as more secure than traditional authentication methods.

For these reasons, they have been amassing popularity since their commercial debut in the early 2000s. In 2020, the global market for biometric authentication and identification was valued at over 3.5 billion U.S. dollars, and it is expected to more than double by 2026 ([Borgeaud, 2024](#)). While different sources may vary on the exact figures, they all agree that biometrics are on an upward trend.

Despite this trend, concerns have been raised about the efficacy of these systems and the privacy risks they pose. This report examines the current threat landscape of biometrics and alludes to the privacy risks associated with these systems.

System Overview

To understand the threats to biometric systems, it helps to know how they work at a high level. Biometric systems operate in two main ways:

- **Identification:** This is a one-to-many comparison that determines "Who am I?" For example, a police fingerprint database. Privacy concerns are usually higher in this context.
- **Verification:** This is a one-to-one comparison that answers "Am I who I claim to be?" This is typical of local biometric authentication systems, such as Windows Hello for desktop and mobile fingerprint scanners.

In addition to these two modes of operation, most biometric systems generally consist of four modules ([Jain & Kant, 2015](#); [Uludag et al., 2004](#); [Alaswad et al., 2014](#)):

- **Sensor module** that reads raw physiological or behavioral data.
- **Feature extractor** module that algorithmically extracts important features from the raw data.
- **Matcher module** that compares the extracted features to a template and generates a similarity score.
- **Decision module** that accepts or rejects based on the similarity score using some threshold.

Biometric systems can be either localized or centralized, depending on where the database is stored relative to the application.

- **Localized:** The database and matcher module are on the same system or network, so authentication occurs without external communication.
- **Centralized:** The matcher module connects to a remote database where all credentials are stored for authentication. Privacy concerns are usually higher in this context.

Threats

Threats to biometric systems involve adversaries who have the intent, opportunity, and capability to inflict harm. The specific nature of these threats can differ based on the context and objectives of both the organization or individual and the attackers involved. Additionally, there are threats arising from the biometric systems themselves, primarily concerning privacy and regulatory risks for users. While these are often an extension of the threats to biometric systems, they warrant special attention due to growing concerns about user privacy.

Threats to Biometric Systems

Opportunities

Biometric authentication systems face threats like those encountered by any system with a similar purpose. However, they also have unique vulnerabilities not found in standard authentication systems that create new opportunities for attackers ([Schlabs & Krissler, 2013](#); [GDPR Advisor, n.d.](#); [CCCS, 2024](#); [Singer & Metz, 2019](#); [Thanawala, 2023](#); [Hallman, 2022](#); [Firc et al., 2023](#)).

- **Extremely Limited Revocation:** Revocation in the context of passwords and traditional authentication refers to the process of invalidating a password to prevent further access. Biometric revocation involves invalidating a user's biometric data, such as fingerprints or facial recognition, to prevent access. Unlike passwords, which can be easily changed, revoking biometric access is more complex, as users cannot change their biological traits.
- **Wide Credential Spread:** Fingerprints are left on every surface you touch, including authentication devices. This is akin to leaving a sticky note with your passphrase on everything you touch. These issues also exist for other forms of biometrics, your face exists on social media, and your voice may exist online, both of which can be recorded without your knowledge.
- **Biased Models:** Several reports have indicated that many facial recognition systems are more prone to error on certain ethnic groups. This opens a pathway for increased targeting of such individuals by attackers who know systems are more likely to misbehave with certain data.
- **Artificial Intelligence:** With the advent of audio and visual deep fakes, the threat of hyper-realistic deep fakes bypassing these systems is a reality we are already confronting.

Figure 1 shows eight points of attack, including the modules themselves and the communication channels between the modules. Threats looking to compromise biometric systems will target vulnerabilities at these points in various ways including spoofing, replay attacks, brute force attacks, bypasses, denial of service attacks, identity theft, presentation attacks, supply chain attacks, and other common means.

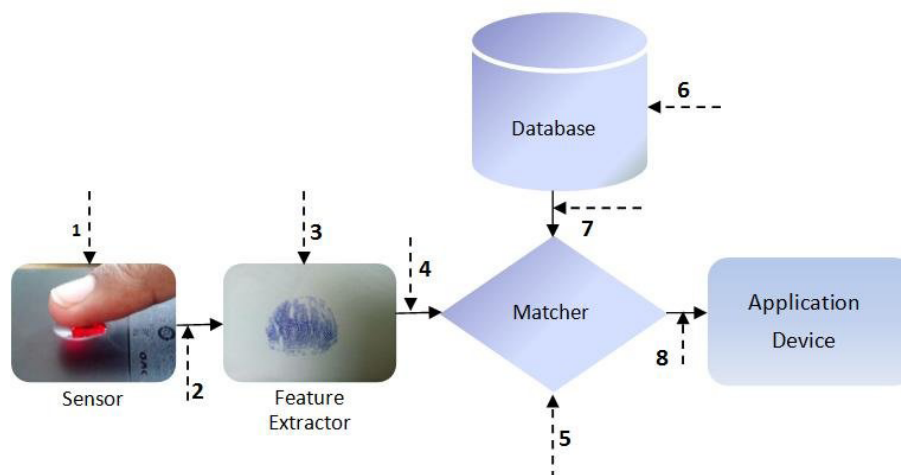


Fig 1: the four modules and eight attack points of a biometric system ([Jain & Kant, 2015](#))

Intent and Capability

As illustrated above, the opportunity for attackers to exploit biometric systems does exist, but this alone does not constitute a threat. For there to be a threat, the intent and capability to cause harm must be demonstrated.

Biometric verification systems are often viewed as the best option for sensitive situations because they are generally more difficult to exploit than traditional systems. Unlike passwords, biometric traits, such as facial features are not private, requiring these systems to be nearly flawless to remain secure. Assuming a near perfect system, only nation-state actors with the intent and resources to steal this data are likely to attempt such attacks. However, there is plenty of reporting that demonstrates that biometric systems are not infallible, and neither are their users ([Schlabs & Krissler, 2013](#); [Sheridan, 2020](#); [Montalbano, 2023](#); [MITRE, n.d.](#); [Plumb, 2024](#); [Nelson, 2024](#); [Lemos, 2023](#)).

- Liveness detectors have been bypassed allowing actors to spoof biometrics and impersonate users.
- Using biometrics means little if users are not educated on cyber threats, as new forms of malware have tricked users into providing attackers with face scans.
- Biometric systems are fundamentally code and thus have plenty of vulnerabilities.
- Most biometric verification systems allow for passwords as backups, something attackers have taken advantage of in the past.

The capability to exploit biometric verification systems has been demonstrated; however, the intent appears low for the time being. Most conventional threat actors, such as financially motivated cybercriminals, are more likely to stick to tried and trusted exploitation methods such as phishing. However, as the industry shifts towards biometrics, one can expect attackers to invest more in biometric exploits.

Threats From Biometric Systems

There are significant privacy and regulatory concerns regarding biometric systems, particularly with centralized databases used for identification. Modern biometric systems store hashes of extracted features instead of fingerprint images, ensuring users maintain control over their data ([CCCS, 2024](#)). This aligns with rulings from the state of Illinois and the European General Data Protection Regulation (GDPR) (Turner, 2024). The Office of the Privacy Commissioner of Canada (OPC) is currently updating its guidance on this matter, but views biometric systems as collecting personal information ([OPC, 2011](#)).

On May 31st, 2024, the Office of the Information Privacy Commissioner (OIPC) requested an amendment to the Personal Information Privacy Act (PIPA) to classify biometric data as sensitive information. They emphasized that biometric data is highly sensitive because it is biologically core to the individual and cannot be reasonably changed if compromised ([OIPC, 2024](#)).

In Quebec, Law 25 expanded privacy regulations to cover biometric data under the Quebec Privacy Act. When seeking to utilize or build biometric systems in Quebec, organizations must navigate both the Quebec Privacy Act and the Quebec IT Act. While this does improve the security of biometric data, it does complicate compliance ([Guilmain et al., 2024](#)). Additionally, they must obtain approval from the privacy commissioner of Quebec to use biometric data and systems, creating a single approval funnel.

Privacy risks vary by product and depend on how the data is processed, stored, and used. While biometric data's uniqueness makes it valuable to attackers, most breaches currently appear to result from misuse by custodians of this data rather than cyberattacks. The misuse of biometric data has resulted in serious fines, and in extreme cases, the all-out banning of products from Canada and other countries ([Hill, 2022](#)). It is crucial that organizations adhere to applicable privacy laws and employ proper encryption techniques to minimize such risks.

Recommendations

Biometrics authentication is not infallible, but it is often used in highly sensitive systems and can improve security of the authentication process. The OPC recommends that companies consider “whether [biometric solutions] are necessary, effective, and proportional to the potential privacy risks, and whether there is a less privacy invasive way to identify or authenticate an individual” (OPC, 2016). Should an organization commit to biometrics, they must consider the following implementation success factors:

Do Not Rely Solely on Biometrics for Verification

Biometrics offer convenience and security but should be used with MFA ([CCCS, 2024](#); [Alaswad et al., 2014](#)). They can enhance security against fraud and improve non-repudiation, but they are unlikely to reduce the overall volume of attacks as most threat actors do not target these systems. A layered defense is essential; no single control should be solely relied upon.

Exercise Caution when Acquiring Biometrics

Privacy concerns are valid since biometric data is valuable to attackers due to its uniqueness. However, most privacy breaches involving biometrics appear to result from misuse by data custodians rather than cyberattacks. Buyers’ due diligence is necessary to avoid misuse issues.

Adhere to Applicable Privacy Regulation

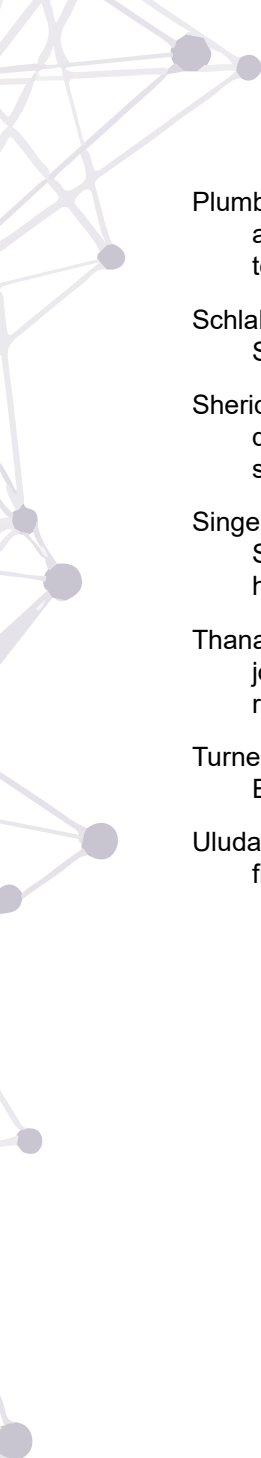
Organizations seeking to implement biometric systems should confer with the privacy legislation they are subject to and perform a privacy impact analysis prior to implementation. Being proactive will help ensure compliance and mitigate potential risks related to data privacy and security.

Conclusion

Biometrics are often perceived as the most advanced and secure form of authentication, influenced by their depiction in popular media. However, they have their own vulnerabilities and risks, making them roughly as secure as other standard authentication methods. While biometrics can offer advantages over passwords alone, they are not infallible. The most robust security is achieved by combining biometrics with traditional authentication methods, such as multi-factor authentication, to provide a layered defense against unauthorized access.

References

- Alaswad, A., Montaser, A., & Mohamad, F. (2014). Vulnerabilities of Biometric Authentication “Threats and Countermeasures.” *International Journal of Information & Computation Technology*, 4(10), 947–958. https://www.ripublication.com/irph/ijict_spl/ijictv4n10spl_01.pdf
- Borgeaud, A. (2024, April 8). Biometric authentication market by end user 2020-2026. Statista. <https://www.statista.com/statistics/1299001/biometric-authentication-and-identification-market-by-end-user/>
- CCCS. (2024, February). Biometrics (ITSAP.00.019). Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/guidance/biometrics-itsap00019>
- Firc, A., Malinka, K., & Hanáček, P. (2023, April). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, 9(4), e15090. <https://doi.org/10.1016/j.heliyon.2023.e15090>
- GDPR Advisor. (n.d.). GDPR and Biometric Data: Privacy Implications and Regulatory Compliance. GDPR Advisor. https://www.gdpr-advisor.com/gdpr-and-biometric-data-privacy-implications-and-regulatory-compliance/#Biometric_Data_and_Privacy_Implications
- Guilmain, A., Bigras, M.-A., Boileau, J., & El Zir, N. (2024, January 23). Biometrics and compliance: Navigating Québec's Legal Framework. *Gowlingwlg.com*. <https://gowlingwlg.com/en/insights-resources/articles/2024/biometrics-navigating-quebec-legal-framework>
- Hallman, J. (2022, August). Deepfakes expose vulnerabilities in certain facial recognition technology | Penn State University. *Psu.edu*. <https://www.psu.edu/news/information-sciences-and-technology/story/deepfakes-expose-vulnerabilities-certain-facial>
- Hill, K. (2022, September 18). Clearview AI, Used by Police to Find Criminals, Now in Public Defenders' Hands. *The New York Times*. <https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html>
- Jain, R., & Kant, C. (2015). Attacks on Biometric Systems: An Overview. *International Journal of Advances in Scientific Research*, 1(7), 283. <https://doi.org/10.7439/ijasar.v1i7.1975>
- Lemos, R. (2023, June 1). Biometric Bypass: BrutePrint Makes Short Work of Fingerprint Security. *Www.darkreading.com*. <https://www.darkreading.com/endpoint-security/bruteprint-short-work-fingerprint-security>
- MITRE. (n.d.). Lockscreen Bypass, Technique T1461 - Mobile | MITRE ATT&CK®. *Attack.mitre.org*. <https://attack.mitre.org/techniques/T1461/>
- Montalbano, E. (2023, December 21). Chameleon Android Trojan Offers Biometric Bypass. *Darkreading.com*. <https://www.darkreading.com/endpoint-security/chameleon-android-trojan-offers-biometric-bypass>
- Nelson, N. (2024, June 12). Scores of Biometrics Bugs Emerge, Highlighting Authentication Risks. *Www.darkreading.com*. <https://www.darkreading.com/vulnerabilities-threats/scores-of-biometrics-bugs-emerge-highlighting-authentication-risks>
- OIPC. (2024). Submission for Review of the Personal Information Protection Act. <https://oipc.ab.ca/wp-content/uploads/2024/06/OIPC-Submission-to-PIPA-Review-May-2024.pdf>
- OPC. (2011, February). Data at Your Fingertips Biometrics and the Challenges to Privacy. *Www.priv.gc.ca*. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/
- OPC. (2016, June 22). Guidelines for identification and authentication - Office of the Privacy

- 
- Plumb, T. (2024, February 21). Face off: Attackers are stealing biometrics to access victims' bank accounts. VentureBeat. <https://venturebeat.com/security/face-off-attackers-are-stealing-biometrics-to-access-victims-bank-accounts/>
- Schlabs, B., & Krissler, J. (2013, September 25). Fingerprints are not fit for secure device unlocking. Srlabs.de. <https://www.srlabs.de/blog-post/spoofing-fingerprints>
- Sheridan, K. (2020, April 8). Researchers Fool Biometric Scanners with 3D-Printed Fingerprints. Www.darkreading.com. <https://www.darkreading.com/endpoint-security/researchers-fool-biometric-scanners-with-3d-printed-fingerprints>
- Singer, N., & Metz, C. (2019, December 19). Many Facial-Recognition Systems Are Biased, Says U.S. Study. The New York Times. <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>
- Thanawala, S. (2023, September 25). Facial recognition technology jailed a man for days. His lawsuit joins others from Black plaintiffs. AP News. <https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7>
- Turner, A. (2024, September 4). Understand Biometric Security and Set Workable Policies. IANS Ask-An-Expert Writeups; IANS.
- Uludag, U., Ross, A., & Jain, A. (2004). Biometric template selection and update: a case study in fingerprints. Pattern Recognition, 37(7), 1533–1542. <https://doi.org/10.1016/j.patcog.2003.11.012>