Mat Hanson

11575596 | mathanson87@gmail.com

Biometrics for authentication: security and privacy implications

itc595 – information security

## Executive Summary

User authentication is the most popular form of security that users of technology utilise on a daily basis. The first instance of user authentication was introduced in the 1960s and that same authentication method is still the most popular method in use today. Other forms of authentication have been created and are being used regularly, but the industry standard method is passwords.

Passwords are notorious for being insecure and are regularly compromised, so much so that users are advised to regularly change passwords. The aim of this report is to investigate biometric authentication and the security and privacy implications of using such a system.

Table of Contents

[Executive Summary 1](#_Toc482654323)

[Introduction 2](#_Toc482654324)

[Security Concerns 3](#_Toc482654325)

[Privacy Concerns 4](#_Toc482654326)

[The Future of Biometric Authentication 5](#_Toc482654327)

[Learnings from Peer Review 6](#_Toc482654328)

[Conclusion 7](#_Toc482654329)

[Glossary 8](#_Toc482654330)

[References 9](#_Toc482654331)

## Introduction

The first programmable computer ever created, Colossus, was built in 1943 specifically to decrypt cyphertext radio messages created by Germany’s Enigma machine. It is no wonder that 74 years later, the computing industry is continually striving to make communications over networks more secure in order to stay ahead of unauthorised persons attempting to gain access. It is ironic however, that in a world full of advanced encryption algorithms like RSA, AES and PGP that the most frequently used authentication method today is the first authentication method that was ever implemented in computing (Pfleeger, Pfleeger, & Margulies, 2015, p. 40).

Many computer historians believe CTSS, MIT’s time-sharing computer in the mid-1960s, to be the first system to ever utilise passwords as an authentication method (McMillan, 2012, para. 3-4). These time-share systems required authentication for users so that they could keep their files private and to be allocated and accountable for their allowance of time for computer use. It was not long before the first breach of authentication security when in 1966, a bug displayed the password master file instead of the welcome message to users. Computers have advanced so much since then, the fact that authentication methods as antiquated as passwords are still the most frequently used, is astounding.

Users are constantly reminded about the importance of password length and complexity, not using dictionary words, having unique passwords for each website or account, regularly changing passwords, and are then expected to remember each and every one of these passwords. Yet all this extra diligence is purely to supplement an authentication method that is inadequate and the extra pressure on users to enhance the security of this method inadvertently only makes it weaker. In an investigative report in 2016, Verizon found that “63% of confirmed data breaches involved leveraging weak, default or stolen passwords” (Verizon, 2016, p. 3).

Pfleeger, Pfleeger and Margulies (2015) describe authentication as the method of proving the asserted identity of a user. There are three mechanisms with which authentication can be obtained; something the user is, something the user has, and something the user knows. Biometrics is described as the “automated recognition of individuals based on their biological and behavioural characteristics” (Jasserand, 2015, p. 69). Biometrics are currently used in criminal investigations, where authentication of a person is paramount, whether they be a victim, potential suspect or innocent suspect for that matter. For instance, The United States Department of Justice (2003) describe DNA technology as “increasingly vital to ensuring accuracy and fairness in the criminal justice system”.

Biometric authentication solves a lot of the common issues plaguing the other two mechanisms of authentication, but also introduces unique concerns with privacy and security due to the nature of the authentication method itself. It is possible and common to forget a password or lose a key, but you cannot forget your fingerprints or lose the unique way that you interact with your phone. In saying that, the current state of biometric authentication is not ideal. Samsung recently released their flagship phone, the S8, touting three modalities of biometric authentication - fingerprint scanner, iris scanner and facial recognition. The inclusion of multiple biometric authentication in a flagship phone is encouraging, however soon after launch hackers were able to successfully spoof the facial recognition biometric authentication with a photo of the pre-programmed user (“Samsung releases S8”, 2017, p. 1).

Biometric authentication is not necessarily secure by inheritance, however the security of using biometrics is not the only issue that needs to be addressed. The privacy of data captured to build a framework for biometric authentication is arguably far more important than the security of the authentication method in the first place. Take Samsung’s S8 for example, as soon as users are aware of the security issue pertaining to facial recognition, they can choose not to use that method of authentication. It is certainly not great if a user has enabled and configured facial recognition and consequently suffers an attack on their phone, but it will not have the same ongoing implications of a privacy breach of biometric authentication data.

## Security Concerns

One of the major security implications regarding using biometrics for authentication is the fact that current active biometric technologies rely on using static biometric data. If there were a breach to a database containing users’ biometric data, there is a potential to expose the user to a lifetime of risk since their biometric data cannot be changed like a password can.

There are several proven ways for unauthorised persons to spoof static biometric authentication methods. Fingerprint recognition is currently the most popular and widely used method (“Finger biometrics drive”, 2017, p. 3) for biometric authentication even though there are several ways that have shown to be effective in spoofing fingerprint authentication. Researchers at the Center for Identification Technology Research used a 3D printer and a photo to develop a mould that produced a piece of silicon that was able to spoof fingerprint recognition. A security researcher called Starbug utilised the same methods at the Chaos Computer Club conference in 2014 to create a working model of a fingerprint from a photograph of the German defence minister’s hand (Brandom, 2016, para. 3).

Even though the requirement of having a high-resolution photograph of a fingerprint is an obvious limitation to this method, gaining access to such an image is certainly possible. For instance, the US collects all 10 fingerprints of any non-US citizen, between the ages of 14 and 79, when entering the US (**U.S. Department of Homeland Security, 2009, para. 3**). Government databases are certainly not impervious to attack and have been the target of numerous successful hacks, like the breach of the Office of Personnel Management in December 2014 where hackers gained access to 4 million federal employees’ personal data (Nakashima, 2015, para. 1).

Another notable biometric authentication breach, which was mentioned briefly in the executive summary, was discovered shortly after Samsung released their latest flagship device, the Galaxy S8. The facial recognition software in the S8 was tricked using a photo of the user on another phone (Carman, 2017, para. 1). This breach is more concerning than the previously mentioned fingerprint breaches due to the availability of photos of users’ faces in comparison to users’ fingerprints. According to the Pew Research Center (2016), 79% of online American adults are Facebook users, of which a high percentage will likely have high definition photos of themselves available for viewing. The accessibility of this data solves the first problem for hackers looking to spoof biometric authentication on a device using facial recognition, acquisition of biometric data.

Iris recognition authentication is considered to be one of the most secure methods of biometric authentication, however Raghavendra and Busch (2015) have found that even iris recognition authentication systems are highly vulnerable to spoof attacks (p. 703).

Because of these spoofing vulnerabilities, the implementations of active biometric authentication will need to constantly evolve to keep up with potential future breaches.

## Privacy Concerns

Privacy is described as “the right to control who knows certain aspects about you, your communications, and your activities” (Pfleeger, Pfleeger and Margulies, 2015, p. 587). In 1948, the United Nations defined privacy as a basic human right when stating in the Universal Declaration of Human Rights that “No one shall be subjected to arbitrary interference with his privacy” (UN General Assembly, 1948). Information privacy is described by the IAPP as “the right to have some control over how your personal information is collected and used” (International Association of Privacy Professionals, 2017, para. 1).

Since biometric information has been classed as sensitive information in the *Commonwealth Privacy Act 1988*, information privacy could then be considered to be a subset of privacy and the importance of information privacy could follow on to also be considered a matter of human rights. The privacy of biometric data is of utmost importance because the data aren’t simply about that person, rather the data are specifically of that person.

There are several factors requiring consideration when implementing biometric authentication systems which include the eight dimensions of privacy described by Rezgui, Bouguettaya and Eltoweissy (2003) –

* Information collection
* Information usage
* Information storage
* Information disclosure
* Information security
* Access control
* Monitoring
* Policy changes

The Biometrics Institute have crafted a set of guidelines specifically for biometric use called The Biometrics Privacy Guidelines (Commissioner for Privacy and Data Protection, 2016, p. 6). This guideline outlines sixteen key principles that are to be followed when implementing a biometric system –

1. Respect for client privacy
2. Proportionality
3. Informed consent
4. Truth and accuracy in business operations
5. Protection of biometric data collected
6. Complaints and enquiries
7. Purpose
8. Anti-discrimination
9. Accountability
10. Sharing of biometric data
11. Provision of advance warnings of surveillance
12. Transmission of biometric data beyond national boundaries
13. Employee data must be protected
14. Limit the extent of personal data exchanged and retained
15. Maintain privacy logs, conduct Privacy Impact Assessments and privacy audits
16. Individual participation/subject access

The aim of these guidelines is to provide guidance to organisations looking to implement biometric systems which will inspire confidence in users that the privacy of their data is being handled correctly.

Even though these guidelines are not mandatory for organisations to follow, it is certainly within their best interests to do so, as Google recently discovered. A judge in the US has allowed a class action case to proceed against Google (“US judge greenlights”, 2017, p. 2). The class action alleges that Google acted against the privacy guidelines by collecting biometric data in the form of facial images without providing consent to the user. This class action proves that no entity is protected from properly handling the issues that are inherent of biometric authentication technologies.

Carpenter, McLeod, Hicks and Massberg (2016) recently performed a study on firefighters in the US showing that concerns specific to privacy largely affected the attitude towards using an authentication system based on biometrics (p. 11). The two concerns which were found to be most significant were the perceived accountability of the participant and the perceived vulnerability of the participant’s stored biometric data. Perceived accountability was described as participants believing that they would be held more accountable for their actions while using biometric authentication, rather than other authentication methods. The data storage concerns are based on the belief that the data might be susceptible to unauthorised access internally as well as external threats.

## The Future of Biometric Authentication

One area of biometric authentication which is showing promise to counter both biometric spoofing and privacy concerns is passive behavioural biometric authentication. The idea behind passive behavioural biometric authentication is that instead of using just one piece of static data for authentication, hundreds of sensors embedded in a device record behavioural data which is then dynamically filtered to identify how the authenticated user behaves and uses the device (Capps, 2017, p. 8).

The important aspect of this design is that there is not one piece of data that defines the user, rather the authentication is split into hundreds of small pieces of data that together define the authenticated user and their behaviour. A breach of the user data in this instance would not compromise the user’s future authentication as this authentication method is difficult to spoof by design.

Another area which is most important is the implementation of an Industry Standard for Biometrics. As previously mentioned in this report, Biometrics Institute have created a set of guidelines to advise organisations of best practice, however these guidelines are a recommendation and are not mandatory. The lack of mandatory standards in an industry with a potential for such a high risk to users is inadequate and creates a grey area for both users and implementers of the technology.

The success of biometric authentication technologies depends highly upon user acceptance and participation, however, without trust in the technology users will be unlikely to accept the technology and participate. A set of Industry Standards would encourage users to trust the technology as implementers within the industry would be required to become certified and abide by the Industry Standards. Users would then be able to easily identify if an implementer or implementation of this technology is to be trusted with his or her data.

## Learnings from Peer Review

In my peer review, I asked several questions of my peers of which were separated into two sections. The first section asked the following questions -

Do you currently have access to any authentication via biometrics? If you do, do you use it and do you have any privacy concerns in regards to your biometric data? If you don't have access to biometric authentication, would you have any privacy concerns in regards to your biometric data?

From the answers provided, I gathered that opinions vary greatly on the security and privacy of biometric authentication. Two of the three peers who participated reported that they do have access to biometric authentication and that they do use the technology. One of these participants however, stated that he only uses the authentication method at work and found that it was not useful on his phone. The third participant did not answer whether he had access to the technology but stated that he avoids using them at all costs. He explained that although he understands the value and importance in biometric authentication, he is not entirely comfortable in using it and finds the collected data to be extremely personal and easily subject to abuse.

Each of the opinions in this section are neither right nor wrong, rather each person has a differing level of trust or concern. I believe that the security of a user’s biometric data should be of utmost importance and without that security, the privacy of the user’s data is compromised. For this reason, I am cautious with the implementations of the technology that I use but am very excited for the future of biometric authentication.

The second set of questions were as follows -

Would you be comfortable using passive behavioural biometric authentication considering the profiling nature of the technology? Do you have any concerns in regards to this technology? Would you be more comfortable using static biometric data instead even though it would be less secure?

Two of the three peers partly answered this question and the consensus is that they would both be more comfortable with static biometric technology. One of the peers was open to the technology in the future when it is more mature, however the other peer was more accepting of static biometric data but would rather not use biometric authentication at all.

I believe that passive biometric authentication is likely to be the future of biometric authentication as it will be more secure by way of being more difficult to spoof and it will lessen the user’s interaction with the authentication system itself.

One issue that wasn’t discussed in the peer review is the concept of creating Industry Standards for biometric authentication. The implementation of these standards would be advantageous to all parties involved due to the reasons discussed earlier in this report, and this implementation would make the greatest impact in real life. Passive biometric authentication would be second in the impact in real life as the technology has the potential to change the way that users interact with authentication. A user would barely even notice that authentication is being executed at all times with this technology.

The most important lesson learned from this peer review is that trust in the technology is the one factor that is most important to the actual use and uptake of the technology. If users cannot trust that their data is going to be secure, they will not use the technology in fear of a data breach that compromises their privacy and possibly ruin their static biometric data forever.

## Conclusion

Biometric authentication is a powerful technology that introduces many security and privacy concerns which need to be addressed before the technology will be universally trusted and accepted by the public. People have varying levels of trust and concern towards their information privacy, however the technology needs to accommodate the highest level of concern not the lowest. There are several technologies that can be utilised to increase the security of biometric authentication but for the best outcome these need to be paired with administrative technologies like industry standards that will instil trust in users.

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| AES | Advanced Encryption Standard |
| CTSS | Compatible Time-Sharing System |
| IAPP | International Association of Privacy Professionals |
| MIT | Massachusetts Institute of Technology |
| PGP | Pretty Good Privacy (encryption) |
| RSA | Encryption algorithm, named after the creators, Ron Rivest, Adi Shamir and Leonard Adleman. |

## References

Brandom, R. (2016) Your phone’s biggest vulnerability is your fingerprint. Retrieved from <https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security>

Capps, R. (2017) The future of identity verification. *Biometric Technology Today*, *2017(3)*, 7-9. doi:10.1016/S0969-4765(17)30034-6

Carman, A. (2017). The Galaxy S8’s facial scanner can, unsurprisingly, be tricked with a photo. Retrieved from <https://www.theverge.com/2017/3/31/15136226/samsung-galaxy-s8-face-scan-security>

Carpenter, D., McLeod, A., Hicks, C., Massberg, M. (2016). Information Systems Frontiers. doi:10.1007/s10796-016-9667-5

Commissioner for Privacy and Data Protection. (2016). Biometrics and Privacy April 2016. Retrieved from <https://www.cpdp.vic.gov.au/images/content/pdf/CPDP_Information_Sheet_-_Biometrics_and_Privacy_April_2016.pdf>

Finger biometrics drive the global mobile biometrics market. (2017). *Biometric Technology Today*, *2017(2)*, 3. doi:10.1016/S0969-4765(17)30028-0

International Association of Privacy Professionals. (2017). What is privacy? Retrieved from <https://iapp.org/about/what-is-privacy/>

Jasserand, C. A. (2015). Avoiding terminological confusion between the notions of ‘biometrics’ and ‘biometric data’: an investigation into the meanings of the terms from a European data protection and a scientific perspective. International Data Privacy Law 2016, 6(1), 63-76. doi:10.1093/idpl/ipv020

Kwapisz, J. R., Weiss, G. M., & Moore, S. A. (2010). Cell phone-based biometric identification. Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on (pp. 1-7). doi:10.1109/BTAS.2010.5634532

McMillan, R. (2012). The World’s First Computer Password? It Was Useless Too. Retrieved from <https://www.wired.com/2012/01/computer-password/>

Nakashima, E. (2015). Chinese breach data of 4 million federal workers. Retrieved from <https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html?utm_term=.bd74f0ec46b5>

Pew Research Center. (2016). Social Media Update 2016. Retrieved from <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing (5th ed.)***.** Upper Saddle River, United States: Pearson Education.

Raghavendra, R., & Busch, C. (2015). Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. IEEE Transactions on Information Forensics and Security, 10(4), 703-715. doi:10.1109/TIFS.2015.2400393

Rezgui, A., Bouguettaya, A. Eltoweissy, M. Y. (2003). Privacy on the Web: Facts, Challenges, and Solutions. IEEE Security and Privacy. 1(6), 40-49. doi:10.1109/MSECP.2003.1253567

Samsung releases S8 with triple biometrics on-board. (2017). *Biometric Technology Today*, *2017(4)*, 1. doi:[10.1016/S0969-4765(17)30062-0](https://doi.org/10.1016/S0969-4765(17)30062-0)

The United States Department of Homeland Security (2009) New biometric technology improves security and facilitates U.S.: Entry process for international travellers. Retrieved from <https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf>

The UnitedStatesDepartmentofJustice.(2003). *Advancing Justice Through DNA Technology*.Retrieved from <https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-executive-summary>

UN General Assembly. (1948). "Universal declaration of human rights" (217 [III] A). Paris. Retrieved from  <http://www.un.org/en/universal-declaration-human-rights>

US judge greenlights Google privacy case. (2017). *Biometric Technology Today*, *2017(3)*, 2. doi:10.1016/S0969-4765(17)30044-9

Verizon. (2010). *2016 Data Breach Investigations Report: Executive Summary*. Retrieved from <http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf>