The Relationship Between Usability and Biometric Authentication in Mobile Phones

Carly Grace Allen[1][0000-1111-2222-3333] and Sashidharan Komandur[1][1111-2222-3333-4444]

[1] Norwegian University of Science and Technology, 2815 Gjøvik, Norway
carlygraceallen@gmail.com, sash.kom@gmail.com

Abstract. It is estimated that over 1 billion people are active mobile phone users in 2018. When using a mobile phone, there are a variety of ways to authenticate and "secure" the device, and biometric authentication is becoming an increasingly common way to do this, however, biometric authentication is not always as usable as it could be. Both usability and security are important, yet many people believe that there is a trade-off between the two. The focus of this paper was to better understand usability, computer security, and within computer security more specifically biometric authentication, and how all three can work together to create systems that are both usable and secure. A survey and interviews were conducted based on previous research to understand perceptions from the general population, usability experts, and security/biometrics experts. The results do indicate that there is indeed a perceived trade-off between usability and computer security.

Keywords: Usability, biometrics, authentication, security, mobile phone, user experience, computer security.

1 Introduction

Both usability and computer security are important, yet many people believe that there is a trade-off between the two [1, 12, 15]. A device that isn't usable won't be used, and if a device isn't secure, then it will be rendered useless [1]. This can often be seen with regards to mobile phones. With mobile phones being accessed and used by so many people, sometimes over 100 times a day [2], it is vital for these devices to have authentication methods that are both secure and usable. Biometric authentication is a growing option; however, it is not as widely adopted as many had thought it would be. Many people still rely on passwords, pins, patterns, or no authentication method because these are the methods they are used to. The problem that comes with these methods is that often, they are not very secure. Patterns leave smudges on screens, pins and passwords are often only a couple of digits or letters, and no authentication is an easy option. Biometric authentication could solve these problems. In theory, biometrics are both secure and usable, however in practice this is not always the case. Thus, it is important to understand how we can increase the usability and

security of biometric authentication together so that there is a stronger option for securing mobile phones.

2 Background

2.1 A Trade-off Between Usability and Security?

When computers were first built, they were predominantly used by experts, so security was a concern, not usability. Now with computers ranging in sizes, functions, and being used by millions of people, usability as well as security are important concerns. If it is not usable, it won't be used, and if it's not secure, then it will become useless [1]. There has been debate as to whether there is a trade-off between security and usability. Some research has stated that there is a trade-off showing that usability reduces security [10], that usability and security have different goals [14], or that this trade-off poses serious problems for system designers [15]. However, a majority of research today seems to go the other way; it predominantly depends on how security and usability are integrated into systems. The "'received wisdom' on the inherent conflict between usability and security goes against common sense" [1].

Discussions surrounding a trade-off between usability and security are often shallow [11]. There isn't discussion on the level of security that will be obtained and how usability will "hurt it" [11]. But usability can improve security. When usability and security are both incorporated into the design process, they can have the same goals [12]. And with an increased focus on users, there has been more research on the usability of security systems. Users make errors, so systems need to be designed to be either insensitive to those errors, to use metaphors and such to allow users to use security software more intuitively or provide users with the knowledge needed to make informed decisions [1]. When a system can interpret user desires correctly, then usability and security are working in harmony [12].

One problem that seems to arise is with the word "trade-off" itself. The way that security and usability are viewed must be changed and not thought of as a trade-off. When they are not integrated into the design process and are only seen as features, then there will of course be a trade-off. However, when viewed as qualities instead of features and are integrated into the design and development process, the perceived "trade-off" between usability and security can be reduced [12].

2.2 Biometric Security

Biometric authentication is about authenticating a person for who they are, not by what they remember or what they have with them [13]. It can be a more long-term and cost-efficient authentication method, and in theory it should be both secure and usable [17]. This is not always the case though. Each biometric trait has their own pros and cons, and some issues that can come up with biometrics are noise, distinctiveness, and non-universality [13,17]. These issues can cause problems in the enrollment and authentication modes [13].

A few errors that can arise in the enrollment and authentication modes are failure to enroll (due to noise, distinctiveness, or not being able to use a specific biometric trait), false acceptance rate (accepting a non-match as a match), and false rejection rate (not accepting the enrolled trait) [19]. These errors can greatly influence the usability of a mobile phone, and a balance is needed between the usability and security [16]. It is crucial when it comes to user safety; however, user interfaces for authentication often encourage either secure or insecure behavior depending on its security requirements [16].

2.3 Usability and Biometric Authentication in Mobile Phone Devices

Usability issues arise from a variety of sources. One large usability issue with regards to biometric authentication can come from the detection error trade-off curve. Unlike passwords, pins, and patterns that are either 100% correct or not, biometrics are based on how close of a match it is to the collected template from the enrollment mode [19]. The threshold that has been established will decide if the biometric is to be accepted or not. The accuracy and thresholds in biometric authentication do not always relate to the ease of use or convenience that users are used to and are looking for [19].

Some people believe that biometrics are not the default authentication mode due to usability and user experience [18]. Many users have not experienced a noticeable difference when using biometrics than using the authentication methods they have already been using [18]. A very common problem with usability in biometric authentication systems is that those who create a system or design often think that it is intuitive and that users will easily understand; that is rarely the case. There is almost nothing that is inherently usable, and biometrics is no exception [19]. That is why biometric authentication systems should be designed with usability and security in mind throughout the whole design and development process [10, 11, 16].

3 Methodology

An explanatory research design was followed by using a survey in phase 1 followed by interviews in phase 2. As most research on biometric authentication and usability in mobile phones has focused on the general population, the goal here was to gather data on perceptions of biometric authentication and usability not just from the general population, but also from those who work in or with usability, computer security, and within that biometrics in particular. To accomplish this, survey and interview methods were used. The first phase consisted of the survey which had three user groups: the general population, usability experts, and computer security/ biometrics experts. The second phase consisted of interviews with usability experts and computer security/ biometrics experts for more in-depth data collection based on the survey and its results. A majority of the survey questions were based on research previously conducted.

Questions such as gender [4, 6, 7], age [4, 5, 6, 7, 9], education level [6], knowledge about biometrics and usability [6, 4, 7], usability perceptions of biometrics [4], ease of

use as well as security of biometrics [4, 5], operating system [8, 9], security tools (or authentication methods) used [8, 9], convenience [8, 5, 7], frequency of authentication [8], experience with failure to authenticate [8], and why participants use biometric authentication or not [7, 9] were used in the survey.

The survey design ensures potential bias is minimal. Before conducting phase 1 and 2, pilot tests were conducted on both the survey and the interview questions. To recruit participants for the survey and interviews, multiple channels were used. They can also be characterized convenience sampling. The survey was posted on multiple usability, design, computer security, and biometrics forums, Facebook groups, and LinkedIn groups. Also, 250 emails were sent to usability, design, computer security, and biometrics companies across 10+ countries to find more diverse participants.

4 Results

4.1 Survey results

24% of participants work in biometrics, security, or related fields. 31% of participants work in usability, UX, UI, or related fields. The remaining 45% of participants worked in neither of those areas. 96% of participants in this study use some form of authentication for unlocking their device, 75% of whom have had issues with unlocking their phones. Those who work in usability, security, or related fields tended to say that biometrics were the most secure and easy to use authentication method (86% and 83% respectively) however, only 67% of those who worked in neither of those areas chose biometrics as the most secure or easy to use authentication method. Those working in security or related fields believed in a link (96%) and trade-off (65%) between usability and security at a much higher level than the other two participant groups (80% and 50% for usability participants respectively and 63% and 47% of general participants respectively). The percentage of participants who were uncertain if there was a link or a trade-off between security and usability increased from security participants (0% were uncertain of there being a link and 13% for a trade-off), to usability participants (3% were uncertain of there being a link and 17% for a trade-off), to general participants (28% were uncertain of there being a link and 37% for a trade-off). However, across the board, a majority of participants (63%) believe that mobile phones can be secure and usable, but they are not always like that today. When asked about their understanding of biometrics, the average understanding was a 3 on a scale of 1-6. 53% of general participants said that they had little to no understanding of biometrics, 60% of usability participants said that they had a novice to intermediate understanding of biometrics, and 57% of biometrics participants said that they have an advanced or expert understanding. When asked about their understanding of usability, the average understanding was a 4 on a scale of 1-6. 44% of general participants said that they had a novice to intermediate understanding of usability, 48% of security participants said that they had an advanced or expert understanding of usability, and 70% of usability participants said that they had an advanced or expert understanding of usability. 83% of security participants said that they have worked

with usability experts whereas only 33% of usability experts said that they have worked with security experts.

There was a high correlation between participants who use a particular well-known brand of mobile phones and use of biometrics (94%) and having the belief that biometrics are the most secure and easy to use authentication method. A majority of participants whose age was between 35-44 years old use biometrics (90%) and had perceptions of biometrics being the most secure (85%) and easy to use (91%) authentication method. 100% of participants over the age of 45 said that biometrics are the most secure and easy to use authentication method. Overall, as the understanding of biometrics and usability increased, so did the belief of a link between the two increase.

4.2 Interview results

One common theme that emerged from the interviews was about users of mobile phones. Several participants discussed how everything "goes back to the user" and how there is much that "depends on the person". These users discussed how users "shouldn't be locked into letting go of something or using something specifically", and that users will disable or circumvent security measures. Many people use the same passwords or pins "as their default method because they are used to it". Security measures now often depend on "what people are willing to do" or "what effort people are willing to make".

Another common theme that emerged was about the weaknesses of security in mobile phones. Multiple participants discussed margins of error, type I and type II errors, and how information is sent mainly around biometric authentication. When discussing the weaknesses of biometric authentication specifically, one participant said, "theoretically it can work and [security] can increase, but in practice it hasn't been that way", and another said that "when it comes down to it, it can be done, but at a cost". Another participant discussed how "you can use a backup method as heightened security, but... the methods used as a backup aren't secure methods".

In five of the six interviews when it came to the question about there being a trade-off or not between usability and security, it was mentioned that there needs to be a balance between usability and security; and even though there is a trade-off, it is not necessarily a bad thing or a problem. Another specific point that was discussed with four of the six participants was 2-factor authentication. Some of these participants mentioned how some data is stored due to two-factor authentication or that it is often recommended for heightened security, though it may be "overboard" or "not always practical for the end user".

There were a few phrases that participants said that were important to them. "Usability is the reason why biometrics are used". "Authentication needs to just work". "UX should not interrupt security". "Bigger phones" reduce the number of usable methods for authentication, although it was not clear what they meant by “bigger phones”. "There needs to be an explanation to the user". "Independent testing is so important". "There needs to be a way to protect the device even when there is no physical access to it". "There is always the question about what is the best option today".

5 Discussion

In general, the survey results showed corroboration with what [8], [3], and [5] stated in that overall there is a belief outside of the security profession that security is important.

Similar to what [3], 76% of participants said that biometrics were the most secure authentication option followed by pins and passwords (22%).

As the other studies mentioned showed as well, fingerprint authentication was the most preferred and used biometric.

Something that was noticed during data analysis was about perceptions and understanding of usability. There were more people than expected outside of the field of usability who said that they have an advanced or expert understanding of usability, and this could be due to the simple definition of usability provided in the survey.

Throughout the interviews there were some common factors that came up. Participants discussed how usability is a large reason as to why biometric authentication is used, and as of now there is a lot of variation between biometric authentication methods and their levels of usability. Humans are an important factor that are often overlooked or thought of as a problem when it comes to authentication. Several participants also mentioned how if security is not usable, then users will circumvent it. Usability should not get in the way of security and vice versa. It was also discussed how there is a trade-off between usability and security, however that it may not necessarily be a problem to have that trade-off. Perhaps by saying it is not a problem the users imply that a healthy balance can be reached through good design between a desirable level of usability and computer security.

6 Conclusion

All groups of users see a link between usability and computer security (specifically with biometric authentication). All groups of users see a trade-off between them and simultaneously believe that an optimum level of both is possible through good mobile phone design.

6.1 Future work

As of now we do not know exactly how the trade-off between usability and computer security manifests itself. We need to establish that they are related through objective data. As of now we have concluded the link based on subjective self-reported data from three categories of users. The interviews bring up several good hypotheses for future usability and computer security studies but each of them needs to be investigated in greater detail so that there are findings that can be in the form of clear design guidelines.

References

1. Cranor, L. and Garfinkel, S.: Guest editors' introduction: Secure or usable? Security & Privacy, IEEE 2(5), 16-18 (2004).
2. Griffin, A.: iPhones are unlocked 80 times per day, Apple says as part of security briefing, The Independent UK (2016).
3. Zirjawi, N., Kurtanovic, Z. and Maalej, W.: A survey about user requirements for biometric authentication on smartphones, 2015 IEEE 2nd Workshop on Evolving Security and PrivacyRequirements Engineering (ESPRE), 1-6 (2015).
4. Riley, C.W., Buckner, K., Johnson, G. and Benyon, D.: Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & Soc, 295-306 (2008).
5. Lovisotto, G., Malik, R., Sluganovic, I., Roeschlin, M., Trueman, P. and Martinovic, I.: Mobile Biometrics in Financial Services: A Five Factor Framework. University of Oxford (2017).
6. El-Abed, M., Giot, R., Hemery, B. and Rosenberger, C.: A study of users' acceptance and satisfaction of biometric systems. 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, 170-178 (2010).
7. Bhagavatula, C., Ur, B., Lacovino, K., Mon Kywe, S., Cranor, L., and Savvides, M.: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. Workshop on Usable Security at USEC '15 (2015).
8. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S. and Reich, C.: Security, privacy, and usability – a survey of users' perceptions and attitudes. Trust, Privacy, and Security in Digital Business, 153-168 (2015).
9. Ahmed, I.U.: Smartphone Authentication, User experience, expectation and satisfaction. Master's Thesis (2017).
10. Alshamari, M.: A review of gaps between usability and security/privacy. International Journal of Communications, Network and System Sciences, 413-429 (2016).
11. Sasse, M.A., Smith, M., Herley, C., Lipford, H. and Vaniea, K.: Debunking Security-Usability Tradeoff Myths. IEEE Security Privacy (2016).
12. Yee, K.P.: Guidelines and Strategies for Secure Interaction Design. Usability and Security: Designing Secure Systems That People Can Use (2005).
13. Böhm, I. and Testor, F.: Biometric Systems. Department of Telecooperation University of Linz (2004).
14. Sahar, F.: Tradeoffs between Usability and Security. International Journal of Engineering and Technology (2013).
15. Ben-Asher, N., Meyer, J., Möller, S. and Englert, R.: An Experimental System for Studying the Tradeoff between Usability and Security. 2009 International Conference on Availability, Reliability and Security (2009).
16. Oluwatosin Nwokedi ,U., Amunga, B. and Bashari Rad, B.: Usability and Security in User Interface Design: A Systematic Literature Review (2016).
17. Pocovnicu, A.: Biometric Security for Cell Phones. Informatica Economica (2009).
18. Brostoff, G.: Adoption problems? How UX could boost biometrics. Biometric Technology Today (2017).
19. Coventry, L.: Usable Biometrics. Security and Usability: Designing Secure Systems that People Can Use (2005).