Trust and Voice Biometric Authentication: Understanding the Levels of User's Trust on Authentication Methods

Alec Wells

Submitted in accordance with the requirements for the degree of

Master of Science by Research

York St John University

Department of Computer Science, School of Science, Technology and Health

March 2021

I, Alec Wells confirms that the work submitted is their own, except where work which has formed part of jointly authored publications has been included. The contribution of the myself and the other authors to this work has been explicitly indicated below. I confirm that appropriate credit has been given within the thesis where reference has been made to the work of others.

The following sections are up for possible publication:

- Chapter 2, Literature Review as: **Wells A. and Usman A. B.** "User Authentication Methods: Attacks, and Techniques" International Journal of Information Security, Volume 20, Issue 3.
- Chapter 4 & 5, Trust Model & Results as: **Wells A. and Usman A. B.** "Voice Biometrics Authentication: Users' Trust Level" Journal of Cybersecurity, Volume 7, Issue 2.

For both publications I, Alec Wells contributed the body of work and data collection for the publications with Aminu Usman assisting with editing, suggestions, and supervision.

Acknowledgments

This research has been carried out by a team which has included myself, Alec Wells and my supervisory team including Aminu Usman, Justin McKeown and Daniel Madigan. My own contributions, fully and explicitly indicated in the thesis, have been the writings in general, literature review, data collection, testing, data writeup, analysis and discussion. The other members of the group and their contributions have been as follows: Aminu has been my main supervisor who has assisted with editing, suggestion, proof reading and providing insight and ensuring the quality of the work, meanwhile Justin and Daniel have provided support such as proof reading and a communication point with the university.

I would like to thank all the members of the York St John Computer Science Staff, who have assisted me throughout the years, especially my main supervisor Dr Aminu Usman who has offered unparalleled support and advice. I would also like to thank Dr Justin McKeown, Dr Mike O'Dea, Dr Daniel Madigan & Dr Rob Sanders all of which have had a role of supporting me with this thesis.

I would also like to express my gratitude to each of my friends and family for being there during my studies, especially my parents Kevin and Sandra Wells.

Finally, I would like to thank all those that gave their time to participant within the study.

Abstract

Due to the singularity of the distinct biometric traits, biometric authentication factors have become increasingly prevalent in daily life and are predicted to target future authentication methods. Previous studies established that the human voice is one of the most natural, non-intrusive, and convenient behavioral biometric factors compared to other biometric authentication methods. Despite the non-intrusive characteristics of voice biometric authentication, it has been brought under scrutiny for many reasons, including the accuracy of biometric data, a general societal trust and distrust with technology and the risk of theft and imitation. Although, when it comes to trusting technology, users' perceptions change with time through continued use of technology, and thus allowing perceptions and opinions to change. However, there are fundamental factors that can contribute to how users develop trust with technologies over time. This study derived a realistic trust evaluation model that incorporates security, privacy, safety, usability, reliability, and availability factors into a trust vector for a flexible measurement of trust in the user accessing the technology. Based on the derived trust model, we experiment using quantitative method whether the users are willing to trust voice biometric authentication method over PIN, fingerprint, and token-based authentication and hence would be inclined to adopt and utilize it as a means of user authentication to access technology. We applied the Kruskal-Wallis H test and the post-hoc test to understand which authentication method the user trusts, based on statistical significance and which groups were found to have that statistical difference.

The result of the study suggests that users have less trust with voice compared to other authentication methods especially traditional means of knowledge-based authentication such as PIN's which consistently ranked much higher than voice in pairwise comparisons.

Table of Contents

List of Tables

List of Figures

Abbreviations Key

Table 1: Glossary of Meanings

Abbreviation	**Meaning**
PIN	Personal Identification Number
ID	Identity Document
DNA	Deoxyribonucleic Acid
NFC	Near Field Communication
RFID	Radio Frequency Identification
IP	Internet Protocol
KBA	Knowledge-Based Authentication
SMS	Short Message Service
SE	Social Engineering
BN-KBA	Bayesian Network Knowledge-Based Authentication
SSSS	Single-Source Single-Sample
SSMS	Single-Source Multi-Sample
MSSS	Multi-Source Single- Sample
MSMS	Multi-Source Multi- Sample
RGB-D	Red Green Blue Depth
RGB	Red Green Blue
VL	Visible Imaging
NIR	Near Infrared Imagine
ATM	Automated Teller Machine
CCD	Charged Coupled Device
VBA	Voice Biometric Authentication
FAR	False Acceptance Rate

FRR	False Rejection Rate
ICC	Integrated Circuit Chip
I/O	Input/Output
SSO	Single Sign ON
NFC	Near-Field Communication
RFID	Radio Frequency Identification
OTP	One-Time Password
SQL	Structured Query Language
LBA	Location-Based Authentication
LBC	Location-Based Client
VPN	Virtual Private Network
GPS	Global Positioning System
Std.	Standard
Dev.	Deviation
Asymp.	Assumed
Sig.	Significant
Adj.	Adjusted
AF	Authentication Factor

1. Introduction

This chapter presents the background behind the study as well as our primary motivations for undertaking the study. The chapter also presents what we intend to answer, the research hypothesis and research contributions.

1.1 Background

With the growth of smart technologies in many different sectors such as hospitals, financial sectors, the military, aviation, etc, there is an even greater need to determine the authenticity of a genuine user. Authentication can be defined as the process of verifying an identity claim using the users' knowledge (e.g., secret questions, passwords, PINs), their possessions (e.g., ID cards, mobile phones, tokens), their location, or their biometrics (e.g., biometrics, fingerprints, iris scans, signatures) all of which can be referred to as different authentication factors (Fu 2015). The classification of user authentication factors can be seen in Figure 1, the taxonomy we created, which classifies authentication factors into four main categories, Knowledge-based, Biometric (or inheritance)-based, Ownership-based, and Location-based authentication factors.

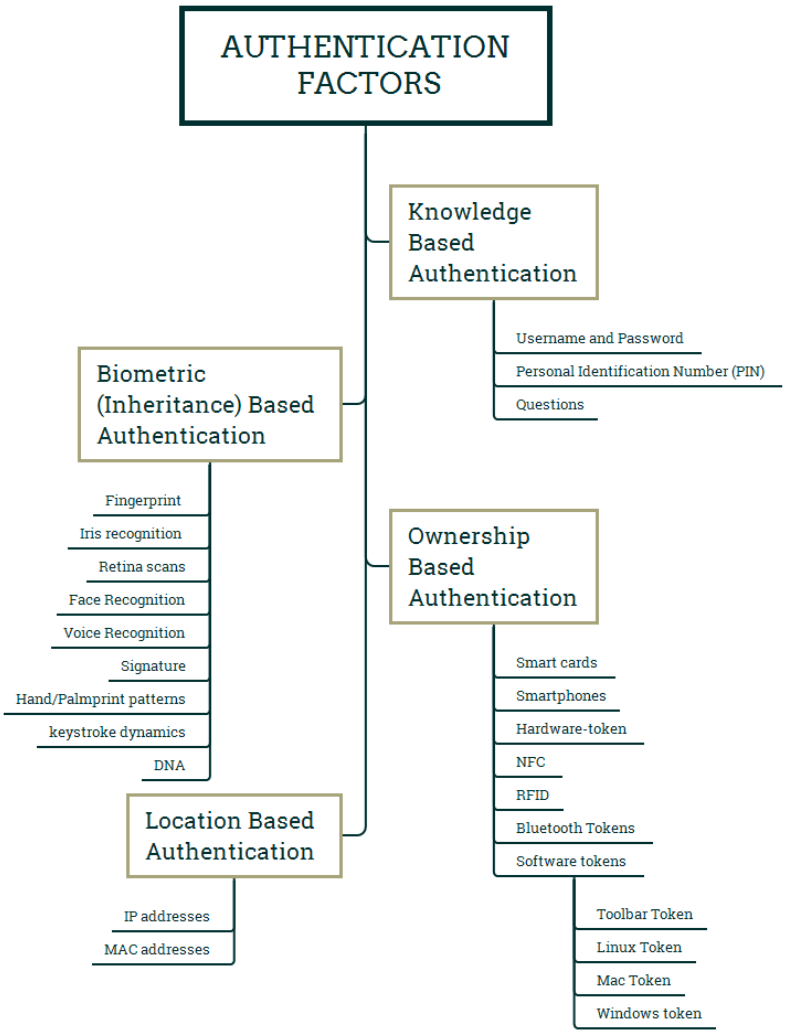

Figure 1: A Taxonomy of User Authentication Factors

The authentication process sets the tone of technologies, network systems, services, and applications. Sophisticated fraudsters and hackers are always on the lookout for vulnerable authentication methods in cyberspace or between digital interactions and transactions. Attacks and countermeasures on authentication factors are well-documented in the literature, thus, this thesis is a compendium of user authentication methods, attacks, and techniques; designed in a systematic way, with the hope that it would be valuable to the

researchers and engineers in the field of user authentication. We explore the literature to point out some open issues, challenges, and suggest future research trends.

The purpose of authentication is to establish confidence that the user trying to access a technology is not an imposter and to only allow the user access to their account/sensitive information. Strong authentication systems help to reduce potential fraudsters and other hackers from gaining access to sensitive information they should not have access to. There are several terms and jargons used to describe authentication systems.

On the other hand, the human body has many distinctive physiological and behavioural features, known as a person's biometric characteristics, that provide indispensable means for a secure authentication process. Biometric-based authentication employs many different modalities, factors, and algorithms to extract and process a user's biometric features for authentication purposes. The classification of biometric authentication techniques depends on the type of characteristics being evaluated: physiological or behavioural singularities. The physiological biometrics are traits that are part of the human body, such as fingerprints, iris, faces, retinas, or hand geometry (Zhang, D. et al. 2009). Behavioural biometrics meanwhile are traits that are distinctive behavioural characteristics, that are partially connected with the human brain activity, including the keystroke dynamics, voice biometrics speech analysis, and eye movement. (Zhang, D. et al. 2009).

Unlike knowledge-based, ownership-based, or location-based authentication factors, which are based on what the user knows, possesses, or where they visited; biometric-based authentication is based on the user themselves – scanning the body for measurements or characteristics to acquire data from an individual, then extracting that feature set from the data, and finally comparing that feature set with the feature set stored within a database.

Due to the singularity of the distinct biometric traits, biometric authentication factors have become increasingly prevalent in daily life and are predicted to replace other means of authentication, hence are considered be the target of future authentication methods (Ortega-Garcia et al. 2004). The human voice is one of the most natural, non-intrusive and convenient behavioural biometric factors in comparison to other biometric factors. Subsequently, the usage of voice biometric authentication is being heavily considered as a promising means of authentication for many reasons. These include not requiring the user to remember any pins or passwords, users constantly being verified - hence fraudsters are more easily caught, and verification being done over standard telephones lines through already implemented infrastructure (Tupman 2018).

Despite all the advantages and non-intrusive characteristics of voice biometrics over other biometric features, voice biometric authentication has been brought under scrutiny for many reasons including: the risk of theft and imitation, the accuracy of biometric data and a general societal feeling of distrust with the technology to handle their privacy-sensitive information and biometric data securely, thus preventing full adoption of voice biometric authentication systems. Other lingering concerns about the security of voice biometric systems include potential breaches of privacy, adversary attacks such as spoofing attacks (Marcel et al. 2019), presentation attacks (Korshunov and Marcel 2017) and replay-attacks (Lavrentyeva et al. 2017) all may cause a user to distrust technology.

Although, when it comes to trusting technology, users' perceptions are shown to change over the course of time through continued use of a technology, allowing for perceptions and opinions to change. However, there are fundamental factors that can contribute to how users develop trust to use with technologies over time. To understand those factors, a valid trust

model would be extremely helpful to arrive at a more realist definition of trust that can be applied in the context of user trust with technology.

1.2 Motivation

The escalating dynamism of current and emerging technologies, coupled with the wide-ranging impacts of technology in society, makes it increasingly important to understand the different dimensions of trust to technology and the algorithms behind those technologies. Since trusting technology beyond their functionality and capacity can present a high risk, a high cost, and compromise to a user's privacy and personal security. It is important to understand which trust evaluation model can be employed for flexible measurement of trust (in the context of availability, security, usability, privacy, reliability, willingness to use, and security) between the user and security-based authentication mechanisms, to access technology?

With voice biometric authentication being such a promising development when it comes to secure user authentication, it is of particular interest to consider the user's current perspectives of the authentication, to better understand if users would first be willing to use the technology, especially when compared with traditional means of authentication such as PINs and Tokens. Hence the study's motivation is to discern the relationship between users and voice biometric authentication and how that compares with traditional means of authentication, to understand if perceptions around voice biometric authentication need to change for it to be readily adopted.

1.3 Problem Statement

As it currently stands, for new technologies such as voice biometric technology to be adopted; users must overcome the challenges of trusting said technology. Thus, trust may be a crucial

factor for the successful introduction of new technology, products, and services (Hoffman, Lawson-Jenkins and Blum 2006). Other factors such as lack of clarity, confidence and poor user experience or expectation with the technology, may raise questions whether adopting the new technology will increase or decrease user trust to technology. Therefore, the study seeks to discern a trust model that reflects the nature of the flowing relationship between trust and technology, to see if the development of trust and voice biometric authentication needs to grow before it can be adopted.

1.4 Research Questions

1. The first question this thesis attempts to answer is: "Which method of user-based authentication mechanism could facilitate trust establishment between user and technology from the user's perspective?"

    1.1 To attempt question one, another question needs to be asked, "which trust evaluation model can be employed for flexible measurement of trust (in the context of availability, security, usability, privacy, reliability, willingness to use and security) between the user and security-based authentication mechanism to access technology?"

2. The second question this thesis seeks to answer is: "Based on the identified trust evaluation model from research question 1.1, are users willing to trust voice biometric authentication mechanism and hence would be inclined to adopt and utilize it as a means of user authentication method to access technology?"

    1.1 If the answer to the above question 2 is yes, at what level of trust could users prefer to use biometric authentication over other authentication methods.

1.2 If the answer to the above question 2 is no, at what level of trust could users prefer to use other authentication methods over the biometric authentication method?

1.5 Hypothesis

1. Users have varying degree of trust about user-based biometric authentication method to access technology based on the chosen trust evaluation model.
2. Users may be found to be willing to trust technology and voice-based biometrics as a method of user authentication.

1.6 Research Contribution

Our contribution in the work is three-fold; i. Motivated by the expanded trust model proposed by (Hoffman, Lawson-Jenkins and Blum 2006), we derived a realistic trust evaluation model that incorporates security, privacy, safety, usability, reliability, and availability factors into a trust vector, for a flexible measurement of trust in the context of user accessing the technology. ii. Based on the derived trust model we experiment using a quantitative method whether the user is willing to trust voice biometric authentication method over PIN, fingerprint and token-based authentication and hence would be inclined to adopt and utilize it as a means of user authentication to access technology. iii. We applied Kruskal-Wallis H test and the post-Hoc test to understand which authentication method the user trusts, based on statistical significance and which groups were found to have that statistical difference.

1.7 Thesis Outline

The thesis is structured as follows: Chapter one gives the study background as well as the primary motivations for undertaking the study. The chapter also presents what questions the

study intend to answer, research hypothesis and research contributions. Chapter two gives the discussion of related work around different authentication methods and related studies, with the hope to put the study in the context of related works. It also presents the concept of trust, both in a social and technological context and how the theory of the trust is applied in the context of the study, along with the trust model used in the study and the discussion of the trust's model metrics and elements. Chapter three presents the studies research framework – a framework that is adapted from traditional design science models with focused upon a researcher's perspective over an engineering perspective. Chapter four presented a collection of the results of the study, after performing the Kruskal-Wallis test. Chapter five meanwhile presents the results of the post-hoc test as well as a results analysis and discussion while in chapter six, we presented a conclusion and proposition of potential future work. At the end, a bibliography and appended material are included.

1.8 Publications

Up for possible publication:

- **Wells A.** and Usman A. B. "User Authentication Methods: Attacks, and Techniques" International Journal of Information Security, Volume 20, Issue 3.
- **Wells A.** and Usman A. B. "Voice Biometrics Authentication: Users' Trust Level" Journal of Cybersecurity, Volume 7, Issue 2.

2. Literature Review

This chapter presents a cohesive discussion about authentication methods. The chapter begins by discussing the types of authentication methods, then outlines the various types of authentication factors from knowledge-based, biometric-based, ownership-based and location-based. Within each section on authentication factors, we discuss the factors advantages and disadvantages as well as how they are used and attacked. For biometric-based authentication we thoroughly inspect the difference between physiological biometrics and behavioural biometrics – especially voice biometrics, a key interest of this study. We then finalise with a discussion around trust in a social and technological context, along with the trust model the study uses.

2.1 Chapter Background

The authentication process is still a problem in cyberspace when establishing the integrity and authenticity of the claimant while accessing technologies, applications, or network systems. Authentication is defined as the problem of verifying an identity claim using a person's knowledge, possessions, location, or biometric factors. A secure authentication ensures that the claimant is the legitimate user trying to access the system, and the authentication is not susceptible to misplacement, forgetfulness, or reproduction. Whilst technology continues to evolve regarding the authentication process, most of the authentication systems still have a large room for improvement, particularly in their accuracy, tolerance to various security attacks, noisy environments, and scalability as the number of individuals increases (Poh, Bengio and Korczak 2002).

The purpose of authentication is to establish confidence in that the user trying to access technology is the user themselves and only allow the user access to the accounts/sensitive

information. Strong authentication system helps to reduce potential fraudsters and other hackers from gaining access to sensitive information they should not have access to. There are several terms and jargons used to describe authentication systems.

With the growth of smart technologies in different sectors like hospitals, financial sectors, the military, aviation, etc, there is a greater need to determine the authenticity of a genuine user. Authentication systems in the context of user's accessing technologies; is the process that allows users to identify themselves by sharing a piece of information only they know (e.g., secret questions, passwords, PINs), own (e.g., ID cards, mobile phones, tokens) or information they inherit (e.g., biometrics, fingerprints, iris scans, signatures) often referred to as an authentication factor (Fu 2015). The classification of user authentication factors can be seen in Figure 1 (as seen in chapter 1, page 13), which classifies authentication factors in to four main categories, Knowledge-based, Biometric (inheritance) based, Ownership and Location-based authentication factors.

As the name suggests, knowledge-based authentication factors seek to prove the identity of the claimant accessing the technology or service by the user's knowledge of a private or secret piece of information to prove the claimant's identity. With ownership-based authentication factors, the authentications processes use something the user has such as a security token, implanted device, phone, software, or hardware token for authentication. Unlike knowledge or ownership factors, that are about what the user knows or has, inherence-based factors are based on the user themselves – using the body for measurements and characteristics. Meanwhile, location-based authentication factors use the claimant's identity to detect its presence at a distinct location (Trojahn and Marcus 2012).

2.2 Authentication Methods

There are two categories of authentication methods, namely, single-factor authentication and multi-factor authentication. Descriptions of the two user authentication methods are provided in the following sections.

2.2.1 Single Factor Authentication Methods

Single-factor authentication simply involves using only one method or 'factor' to verify the user's identity and authenticate themselves. These such factors include the usage of knowledge-based factors like passwords, pin numbers and other information the user would know, ownership-based factors such as bank cards or cell phones and inherence factors like a user's fingerprints or iris (Turner 2016).

Many pieces of literature, technology companies and agents consider single-factor authentication to be inadequate in preventing fraud, especially for that of high-risk transactions related to banking (Council, Federal Financial Institutions Examination 2005) (Tiwari et al. 2011). This is simply because if you only have one factor protecting your account, if that was to ever leak, then access to the account can be immediately gained by an intruder. Studies such as (Velásquez, Caro and Rodríguez 2018) suggest that regarding single-factor authentication with knowledge-based factors, users find it hard to remember passwords for a long time, or remember different passwords for multiple accounts, hence leakages are much more likely. This is especially a concern nowadays considering the amount of data breaches that have occurred in recent years where multiple users accounts and passwords have been leaked. Even disregarding data breaches, many passwords can be cracked due to users using weak or even default passwords allowing hackers easy access to accounts. When users are considering authentication, the main factors they consider are usability and security (Khan and

Zahid 2010). Although many users consider multi-factor authentication to be safer and more secure than single-factor, users do consider single-factor to be more user friendly. As shown in the study (Gunson et al. 2011) in which participants considered single factor to be easier, more straightforward, and quicker than multi-factor authentication.

2.2.2 Multifactor Authentication Methods

Multi-factor authentication utilises a similar process to that of single-factor authentication. However, the primary difference between the two is that multi-factor authentication will only authenticate the user after they have presented two or more factors to verify their identity (Turner 2016). Similar to single-factor authentication, these can be based on any factor, from the user's knowledge, things only they possess and biometrics they inherit. In multi-factor authentication, the authentication process can ask for pieces of evidence from the same type of factor i.e., two knowledge-based factors like a password and a pin code or from difference types of authentication factor such as a password and token.

While multi-factor authentication is considered much more secure than single-factor authentication, it does however have a few drawbacks. Two-factor authentication is not immune to being hacked and is just as vulnerable to attacks used on single-factor authentication. For example, two-factor authentication is also still susceptible to users having their credentials stolen from phishing-based attacks. An example of a phishing-based attack is man-in-the-middle attacks, where attackers will create spoofed versions of websites for users to type their credentials into for the attacker to steal and use on the real website. Alternatively, two-factor authentication is not immune to is the likes of trojan attacks where a hacker can piggyback on a user's login session to make their own fraudulent transactions (Schneier 2005). Another feasibility concern of two-factor is when using mobile authenticators,

as a mobile phone is not always available either because there is no signal, the phone's battery is dead, or it has been stolen.

The main deployment of multi-Factor authentication has been with phone authenticators tied to most online accounts. This authentication follows the method of first receiving credentials that have one identifier between a first and second principal (such as an email address). The user's knowledge of the first identifier is first verified (such as with a password) and an authentication credential is then generated (Burch and Carter 2010). This is often seen with smartphones via an app to generate codes for the user to receive and then enter when they sign in (Drokov, Punskaya and Tahar 2015). This has been one of the most common deployments of multi-factor authentication due to how integrated phones are in modern society – always being available.

Other prominent examples of multi-factor authentication are seen in the world of banking that utilises both knowledge and possession-based factors. In order to pay via a credit card in person, a user must have both the bank card itself to put in the card reader and know the pin code in order to complete the transaction. Alternatively, multi-factor authentication is seen for a network service by monitoring a session at a firewall applying a profile based on the new session and performing an action based on the authentication profile (Murthy et al. 2021).

Overall, despite single-factor authentication being considered inadequate at preventing fraud it is still commonly used as it is faster and more convenient for the user, compared to the safer yet slightly more cumbersome multi-factor authentication. Several important services, such as banking, have multi-factor authentication as a requirement, whereas less important services provide it as an option.

2.3 Knowledge Based Authentication

Knowledge-based authentication (KBA) is an indispensable tool in digital Identity proofing protocols and solutions. KBA can be offered in many formats, making it a valuable and flexible authentication mechanism in many cybersecurity architectures. Knowledge-based factoids are based on information only the user should know such as a username and password or personal identification number (PIN).

The two most widely used methods of users' authentication using KBA are: static (shared secrets) and instant (also known as dynamic KBA). Static KBA is based on a pre-defined set of questions or shared secret information between the authentication parties involved. Mostly, static KBA factoids include questions such as *what your mother's maiden name*. Or *what is your date of birth*, etc, and is commonly used by email providers, banks, financial services or companies to authenticate users.

On the contrary, instant KBA uses methods and algorithms to dynamically develop a set of personal questions and answers to authenticate a user, and it does not require the user to have provided the questions and answers beforehand (Fu 2015) . These dynamic questions provide randomized right and wrong answer choices based on data found for the subject by the KBA system. Regardless, in practical usage, both versions of KBA usually require a form of initial registration against an existing database to create the credentials. KBA then usually requires some online or remote access to the server to verify the factoids/credentials in the login mechanism (Chokhani 2004).

One of the attributes of KBA is password entropy - a measure of how unpredictable a password is. Password entropy estimates how many trials an attacker (either by guessing or brute force) would need, on average, to guess the password correctly. In other words, the

more difficult to predict or guess the password entropy, the more secure the KBA is. Given a password with a character size *L*, we can compute the password entropy using the following equation 1 below (MLB9252 2011).

$$E = log_2(R^L) \qquad (1)$$

Where E is the password entropy, R is the pool of unique password characters, and L is the number of characters in a given password. Subsequently, R^L is the number of possible password combination and $log_2(R^L)$ is the number of bits of entropy.

2.3.1 Security attacks on Knowledge Based Authentication Factors

There are three main categories of attacks to knowledge-based authentication: Social engineering attacks, guessing attacks, and brute force attacks, as presented in the taxonomy of KBA attacks, as shown in Figure 2. Each of the three types of attacks on KBA can be in different forms. We provided, in the following sections, a summary of the attacks.

The KBA attacks taxonomy we created in Figure 2, presents the classification of KBA attacks.

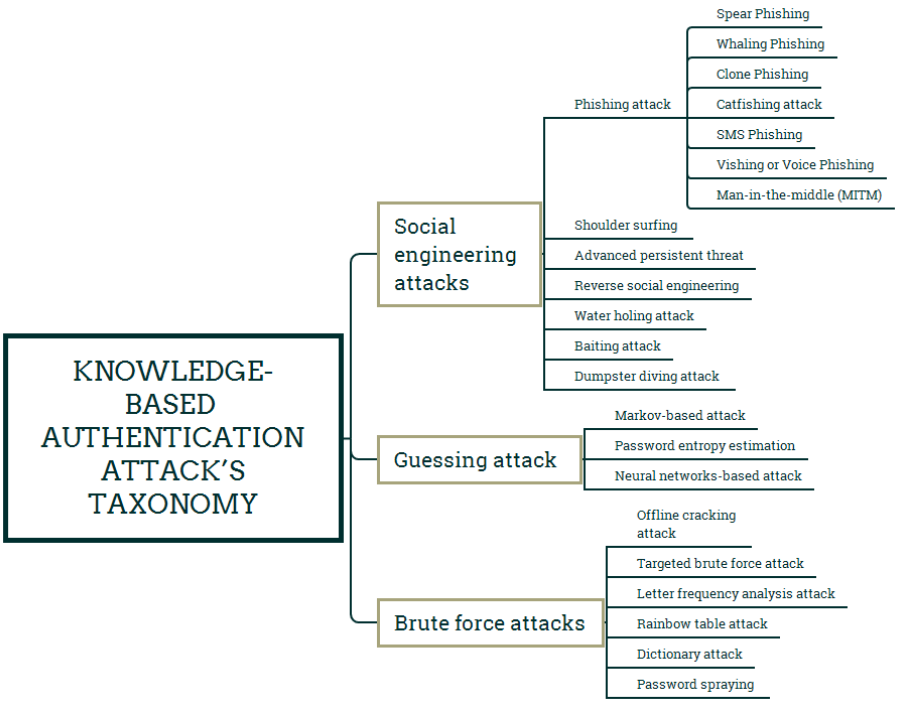

Figure 2: Knowledge-Based Authentication Attack's Taxonomy

Shoulder surfing attack is a form of social-based attack used to obtain information from the target using direct observation techniques, such as looking over victim's shoulder to obtain victims' passwords, PINs, or secret information. Dumpster diving attack is another form of social-based attack to recover information about the habits, activities, and interactions of individuals or organisation from discarded phone books, hard drives that have not properly been scrubbed or surfing through people's curb side garbage. A dumpster can be a valuable source of information for attackers, who may find personal data about employees, manuals, memos and even print-outs of sensitive information (Koyun and Al Janabi 2017).

2.3.2 Social Engineering Attacks on Knowledge Based Authentication Factors

The social engineering (SE) attack is manipulating the target (a person) to obtain information by a social engineer – an attacker. So far, SE is the most superior form of KBA attacks as users

themselves are the attacks' targets. Successful social engineering attacks can be incredibly damaging and highly lucrative. In the SE attack, the attacker took on legitimate personnel's disguise to convince the victim to give out their sensitive information. The attacker can execute the attack in person by interacting with the target to gather desired information about the target(s) or using specialized software. A distinctive feature of social engineering attacks to KBA compared with the other attacks on KBA attacks is social engineering attacks exploit human weaknesses and hence, may be challenging to address the problem of human weaknesses. The attacks' operators of Social Engineering attacks against KBA can be classified into social-based attack or computer-based attacks, physical, technical, and socio-technical. The social-based attacks are performed through relationships with the victims to play on their psychology and emotion to obtain information from the target. On the contrary, computer-based attacks are performed using devices such as computers or mobile phones to get information or to perform advanced attacks against the KBA.

Table 2 presents four different forms of social engineering attacks including physical (the use of physical actions to collect KBA information) (Aldawood and Skinner), technical SE (the use of sophisticated technical tools to obtain KBA information) (Krombholz et al. 2015) or social (using psychological skills to collect KBA information) (Granger 2001). Other types of attacks include technical approaches – using technical tools and methods to harvest users' KBA information. Mostly, the technical types of attacks to KBA are mainly carried out over the Internet using a specialised tool such as *Maltego* to gather and aggregate target's information from different web resources or social networks. The socio-technical types of attacks to KBA are currently one of the most powerful forms of KBA attacks used by of social engineers. Examples of these

forms of attacks include “road apples" attacks, an attack using a USB containing a trojan horse or baiting attacks (Stasiukonis 2006).

Reverse social engineering (RSE) attack has three stages: sabotage, advertising and assisting. Initially, an attacker can sabotage the companies or individual access credentials. The attacker can then convince the target that he/she is ready to solve the problem. When the victim asks for help, the social engineer will resolve the problem they created earlier while, e.g., asking the victim for their password (“so I can fix the problem”) or telling them to install certain software, etc (Krombholz et al. 2015). Other forms of SE attacks on KBA include water holing attacks (Edwards et al. 2017), spidering attacks (Loukas and Öke 2010), baiting attacks (Fan, Lwakatare and Rong 2017), advanced persistent threat attacks (Mazumdar and Nirmala 2018) and phishing attacks. We provided in the following a detailed description about phishing attacks on KBA.

Table 2: Social Engineering Attacks’ Operators on KBA

Attack’s Operator/Social Engineering attack on KBA	Shoulder Surfing	Dumpster Diving attacks	Reverse Social Engineering	Water holing attacks	Crawling or spidering attacks	Baiting attacks	Advanced Persistent Threat	Spear Phishing attacks	Vishing or Voice Phishing attacks	Man in the Middle attacks	SMS Phishing	Catphishing	Clone Phishing	Whaling Phishing
Social-based attack	x	x	x		x	x		x	x			x		

Computer - based attack		x	x	x	x	x	x	x	x	x	x	x	x	x

As presented in Figure 2 there are different forms of phishing attacks: whaling phishing, spear phishing attack, and vishing phishing, etc. Spear phishing attack is usually directed at specific individuals or companies to gather and use personal information about the target to increase chances of successful attacks (Ho et al. 2017). Whaling phishing (Whaling email) is a highly targeted phishing attack mostly against financial institutions and payment services. Through social engineering, the attacker can encourage the victim to perform a secondary action, such as initiating a wire transfer of funds. Whaling phishing is more sophisticated than generic phishing emails as they often target senior executives (Chiew, Yong and Tan 2018). Other forms of phishing attacks include catfishing attack (Simmons and Lee 2020), voice phishing (Choi, Lee and Chun 2017) and SMS phishing (Mishra and Soni 2019). In the man-in-the-middle (MITM) phishing attack, the phisher places himself or herself in the middle of two ways communication between the victim and a web-based application to eavesdrop and collect sensitive information that the victim is submitting to a web-based application (Chiew, Yong and Tan 2018).

2.3.3 Guessing attacks on Knowledge Based Authentication Factors

The popular methods of KBA guessing attacks can be classified into three types: Markov-based, neural networks-based, and entropy estimation. (Narayanan and Shmatikov 2005) argued that the distribution of letters in easy to remember KBA factor (e.g, passwords) is likely

to be similar to the distribution of letters in the users' native language. The authors applied Markov modelling techniques from natural language processing to reduce the size of the password space to be searched and increase the chance of guessing the password. (Dürmuth et al. 2015) prosed a Markov model-based password cracker that generates password candidates according to their occurrence probabilities. Other Markov model based KBA cracking tools include the study (Marechal 2008). (Weir, M. et al. 2009) applied a probabilistic context-free grammar based upon a training set of previously disclosed passwords template to generate word-mangling rules for password cracking. (Hitaj et al. 2019) applied machine learning algorithms to proposes password guessing technique based on generative adversarial networks (GANs) to learn users' password distribution information from password leaks.

The use of Bayesian network models in probabilistic reasoning and information theory provides a valid metric for entropy estimation of human-selected passwords. The proposed BN-KBA model in (Chen, Y. 2007) is intuitively appealing in that it captures two key metrics of KBA as the model parameters, particularly the likelihood memorability (probability that a claimant with true identity recalls the factoid correctly) and guessability (the probability that an impostor correctly guesses the factoid). In this vein, (Chen, Y. and Liginlal 2007) proposed a methodology for implementing a Bayesian network based KBA system. The findings in the study suggested that in the context of KBA, the personal knowledge revealed from a variety of online sources can be directly or indirectly be exploited by imposters to attack a KBA system using the two metrics (memorability and guessability). The other reason for KBA being compromised is due to the of predictability of user choice on the guessability of KBA. For

example, given a password, the guessability of the password factoids can be computed using the following equation 2 (Chokhani 2004).

$$P_{KBA,j} = \pi_i p_{i,j} \qquad (2)$$

Where $P_{KBA,j}$ is the probability of compromising KBA by j. The claimant type is j. The ith factoid is i and the probability to guess j by factoid i is $p_{i,j}$. Subsequently, the convenience of a KBA system is valued as important as the obscurity (difficulty of guessing) variable; thus, guessability of KBA can be a reason why alternative solutions are being explored, though the guessability of KBA is made worse by the fact that many users use common, easy to guess passwords, such as '123456' which was used by over 23.2 million breached (National Cyber Security Centre 2019a). In addition, with the rich data repository available on resources such as online social networks and the cutting-edge machine learning techniques, the guessability an attacker would achieve can be substantially improved. Subsequently resources such as online social networks, may put imprudent KBA designs at risk.

2.3.4 Brute Force attacks on Knowledge Based Authentication Factors

A brute force attack on KBA is the act of trial and error to gain access via trying multiple combinations of passwords. There are different forms of brute force attack to KBA including offline cracking attack (Blocki, Harsha and Zhou 2018), letter frequency analysis brute force attack (CRYPTO-IT 2020), or targeted brute force attacks which primarily uses input dictionary creation programs and password guess generators (Reusable Security Tools no date). Another form of brute force attack on KBA is Rainbow table attack which enables the recovery feasibility of long human chosen passwords (Marforio et al. 2016) (Zhang, L., Tan and Yu 2017).

A more refined version of the brute force attack is a dictionary attack, a type of attack that only utilises the possibilities most likely to succeed rather than cycling through every option like a brute force attack (Jablon 1997). Similarly, password spraying also utilises the most common passwords, but instead targets multiple accounts at once, to try to gain entry into any account regardless of the user (Joseph et al. 2020). There also exists the danger of password cracking, where attackers try recover passwords from data that has already been transmitted, usually via a brute-force attack, however since the password has already been transmitted the attackers know the cryptographic hash of the password, allowing them to brute-force more effectively (Weir, C. M. 2010). Finally, the last type of attack would be rainbow tables, which computes hashes of the large set of available strings, rather than specifically calculating a hash function for every string present and comparing them to the target (Dutt Parth 2021).

While there are many different attacks against knowledge-based factors, there are several countermeasures that users can do, to try make them as secure as possible. One of the simplest and yet best ways to deal with various attacks, is to have strong, uncommon passwords that utilise multiple different types of characters, numbers and case (Shay et al. 2014). By using stronger passwords, simple attacks such as brute-force and dictionary attacks are far less likely to succeed. Likewise, having different passwords for every account or changing passwords often can help keep accounts secure in the event of a data breach, though many would argue that changing password often can inflict needless pain, cost and risk to the user (Spitzner Lance 2019) though could still be considered good practice.

Beyond that, users should simply be careful to avoid any suspicious software/emails and always look for good identifiers such as the padlock in the address bar to signify the website

is encrypted. Depending on the types of attacks, other forms of attacks' countermeasures include multi-factor authentication, anti-phishing technologies, user training, and antivirus software.

Despite the perceived risk of KBA, it is still widely used and has many merits. KBA is extremely easy to use and easy to understand. This is because it has been one of the standard means of authentication and KBA, such as passwords, are the most common form of authentication (European Union Agency for Cybersecurity no date). Likewise, from an admin and logistical point of view, KBA is very attractive. It requires no additional hardware beyond a standard keyboard, unlike for instance biometrics, which means it can be easily used by anyone for anything and anywhere. Due to this, it is cheaper to implement for business than more costly methods, such as biometrics (Raza et al. 2012), and is also fairly easy to administer for both home and business owners.

2.4 Biometric Based Authentication

The human body provides indispensable sources of distinctive features suitable to be used for the task of authentication systems or recognition. The use of such distinctive features of the human body or a person's biometric characteristics is referred to as biometric-based authentication which employs different modalities and factors such as fingerprints, iris, voice recognition and face – using the body for measurements and characteristics. Biometric-based authentication can be split into two different categories. The first is physical biometrics, that uses physiological features of the human body for users' authentication, this includes methods such as using a fingerprint or iris scanning. Alternatively, there are behavioural biometrics, which utilise a pattern of behaviour that is specific to the user, this includes

methods such as voice recognition or alternatively could be the rhythm they users type on a keyboard (Chrobok Mateusz 2020).

There are different algorithms and techniques to extract the physical and characteristics for biometric or biometric traits such as palmprints, hand geometry, ears, nose, and lips. For example, the analysis of the retinal vascular pattern with respect to individuals (pattern of blood vessels), appears to be one of the main sources of biometric features in methods like the vein matching, and the retinal scan (Rigas, Abdulin and Komogortsev 2016). Other forms of biometric-based traits utilise behavioural distinctive characteristics and are partially connected with the brain activity include methods such as keystroke dynamics, voice recognition speech analysis, and eye movement driven biometrics.

2.4.1 Biometric Sensing Systems

There are two categories of Biometric sensing system, Unimodal and Multimodal. We created Figure 3 to present a taxonomy of Biometric Systems.

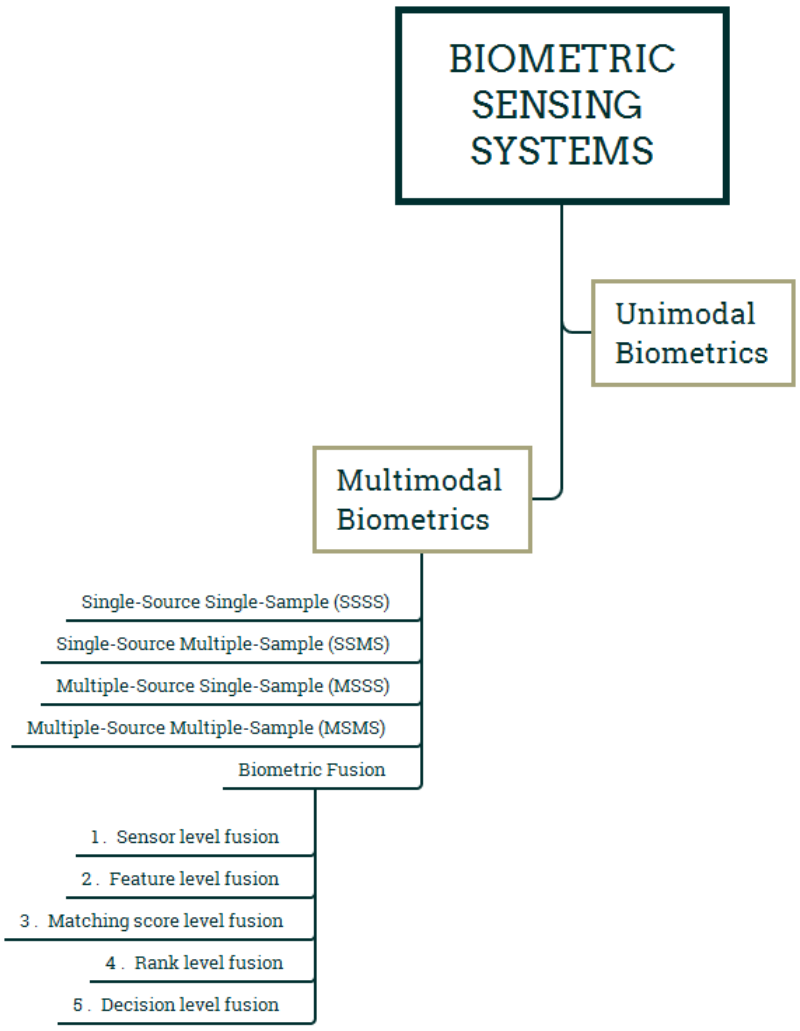

Figure 3: A Taxonomy of Biometric Sensing Systems

2.4.1.1 Unimodal Biometrics

Unimodal biometrics is a biometric sensing system where only a single biometric trait of the individual is used for identification and verification. When only one type of biometric data is being captured, the sensor can be considered more vulnerable to noisy or bad data – especially when using only a single-sample of biometric data. For instance, a facial scanner being affected by the illumination condition or facial expression. This also means the data is more susceptible to spoof attacks, since only one type of biometric is being compared in the database. Depending on the data being measured there could also be issues with unique

circumstances such as faded fingerprints or problems with inter-class similarities such as identical twins with facial recognition (Thakkar no date).

2.4.1.2 Multimodal Biometric System

Multimodal biometric system with fusion can be classified according to the source and samples used. A biometric source can be defined as a single biometric feature of the user like a fingerprint, voice sample, palm geometry etc. A biometric sample is a scanned copy of that source. A source can have multiple samples in a biometric system. Biometric systems can be Single-Source Single-Sample (SSSS), Single-Source Multiple-Sample (SSMS), Multiple-Source Single-Sample (MSSS) and Multiple-Source Multiple-Sample (MSMS) (Jain, Arun and Aggarwal 2012).

The multibiometric systems utilize the principle of *fusion* to combine information from multiple sources to improve recognition accuracy. In order to develop a multibiometric system, some of the important questions to answer include i. what to fuse, ii. when to fuse, and iii. how to fuse (Singh, Singh and Ross 2019)?

When using multi-sensor systems to combine information captured by multiple sensors to obtain the same biometric modality like in the study (Goswami, Vatsa and Singh 2014) which uses the depth information along with RGB images to create a more accurate facial recognition. Some multi-algorithm systems utilize multiple algorithms for processing an input sample. For example, in the study (Ross, Jain and Reisman 2003) a hybrid matching scheme is used that takes into account both minutiae and ridge flow information of fingerprints to construct a full feature map. A similar system is adopted in (Kumar and Zhang 2005) which uses different palmprint representations to extract different textures, lines etc to construct a more

detailed palmprint. Alternatively, multi-instance systems instead capture multiple instances of the same biometric trait. A typical example of such system includes the use of adaptive bloom filter-based transforms to mix binary iris biometric templates at feature level where iris-codes are obtained from both eyes of a single subject (Rathgeb and Busch 2014).

2.4.2 Biometric Fusion

With the existing abundance and growing discovery of new biometric-based modalities and the heterogeneity of the associated features, the need for better security of such systems will continue to evolve. One of the techniques that is being employed is the use of Information fusion to combine the information coming from different modalities (e.g., fingerprints, face, iris etc.) As presented in Figure 4 (Singh, Singh and Ross 2019), following, is the brief description of different level of fusions:

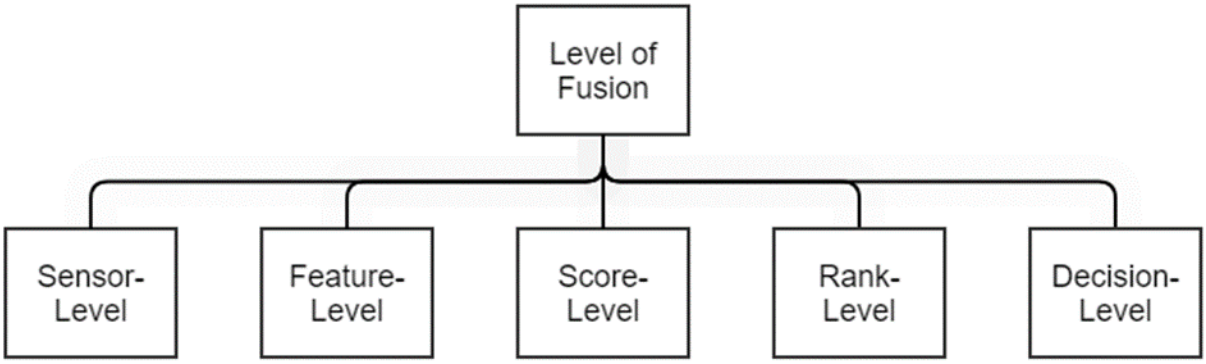

Figure 4: Levels Fusion can Take Place

1. Sensor level fusion – where data is fused immediately after being acquired by the sensor, for example, combining face images of the frontal, left and right profiles.
2. Feature level fusion – where data is fused by combining the features analysed; for instance, combining textures and lines to construct a more complete palmprint.
3. Matching score level fusion – can be done at the stage of user authentication when a newly generated image of the user matched against a previous image of that user in

the database or where fusion occurs where the match scores have been produced such as to create a mean score fusion or a max/min score of the fusion.

4. Rank level fusion – fusion can be performed after comparing the input probe with the templates in the gallery/database with a ranked list of matching identities being produced.
5. Decision level fusion – when the final decision is generated after a matcher module matches a fresh image in database and generates a matching score or when the fusion is done by comparing/combining the algorithms performed.

Compared to unimodal systems, multibiometric systems have many advantages in usage. Mainly in that it is much harder to spoof multiple biometric sensors and it is a lot more accurate at verifying the correct user again due to multiple metrics, helping to reduce data distortion (Shah et al. 2014). Multimodal systems have demonstrated higher accuracy since they use multiple biometric modalities and combine independent evidence to make a more informed decision (Krawczyk and Jain 2005).

2.4.3 Biometric authentications Factors

As mentioned previously, biometrics or biometrics-based authentication can be subdivided into physiological and behavioural factors. The physiological factors include fingerprints; iris retina, face, and ear geometry, etc. whereas, behavioural factors include signature recognition, voice recognition, keystroke dynamics, and gait analysis (Weaver 2006).

2.4.3.1 Fingerprint Recognition.

Fingerprints are one of the most widely known forms of biometric-based authentication. Research in fingerprints can be traced back to the 1600s and law enforcement have used

fingerprint identification for decades. Though this is also because fingerprints are one of the first instances of biometric authentication being widely used by the public as optional authentication in a commercial product such as smartphones, computers, etc.

Fingerprints are quite unique in how many minute details each one can have, there are six main classifications of fingerprint; arch, tented arch, right loop, left loop, whorl and twinloop (Jain, Anil K. et al. 1997). In order to discern if fingerprints match, fingerprint readers are used of which there are 3 main types. The first way of reading fingerprints is optical scanners, optical scanners capture an optical image and utilise algorithms to detect unique patterns and discern if it is a matching fingerprint. Capacitive scanners, meanwhile, use arrays of tiny capacitors to collect highly detailed images of the ridges and valleys of a fingerprint. The third one is ultrasonic scanners which capture the details of a fingerprint via an ultrasonic pulse transmitted against the finger to discern different ridges, pores etc. Optical scanners are the simplest form of scanning, simply being an image and are the easiest to fool but are cheaper and can still work even when the user has wet fingers. Capacitive scanners are much more secure and less easily fooled, but have trouble identifying the user with wet fingers. Whereas ultrasonic scanners are not only very secure and difficult to fool but have almost no trouble when the user's fingers are wet (General Post Blog 2019).

2.4.3.2 Iris Recognition

Iris recognition is another form of physical biometrics like fingerprint recognition, except it uses the user's eyes to verify their identity rather than their fingers. Similar to fingerprints, the structure of the iris is determined during embryonic development, thus, no two individuals, have the same iris patterns. Iris recognition involves taking a picture of the user's eyes and identifying a unique pattern of a user's iris to authenticate the user, this involves

looking at the eye's blood vessels and pigmentation to create a unique profile for the user (Daugman 2009).

There are two different types of iris recognition available: visible imaging (VL) and near infrared imaging (NIR). Primarily NIR technology is used, due to dark pigmentation in human eyes being predominant where VL struggles to reveal visible texture, however, NIR technology eliminates most of the rich melanin information as the chromophore of the human iris is only visible under the VL (is near always the best) (Abdullah et al. 2015).

In regard to commercial use, iris recognition as an authentication method has had more sparing use compared to fingerprint recognition however, iris recognition has been used by government agencies such as the FBI, in prisons and has been used for ATM identity verification. Iris recognition is also being deployed in newer smartphones and other handheld devices as an alternative security option. Smart phones often employ NIR sensors as studies often show that NIR systems are most cost effective and are able to easily identify fake images (Alonso-Fernandez and Bigun 2014) (Thavalengal, Bigioi and Corcoran 2015).

2.4.3.3 Retina Recognition

Retinal scan should not be confused with iris recognition. Retina scan involves the use of a low-intensity light source projected onto the retina, to illuminate the blood vessels when an individual looks through the scanner's eyepiece, for a minimum of ten to fifteen seconds. This allows the eye's blood vessel patterns to be photographed and analysed - whereas an iris scan can be conducted from a short distance away. As the blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person, a retina scan cannot be faked as it is currently impossible to forge a human retina or blood vessels of a human eyes (Bhattacharyya

et al. 2009). In terms of security and resistance to attack, retinal scan is by far the most secure biometric-based authentication system. Since the retina is located from within the structure of the eye itself, it is not prone to the harshness of the external environment like hand geometry or fingerprint recognition. However, the measurement of retina scan accuracy can be affected by illness such as cataracts, and astigmatism. Another disadvantage of retina scan is the scanning procedure is perceived by some as invasive and violation of users' privacy since diseases like AIDS and malaria can be detected from the user's retina scan image.

2.4.3.4 Facial Recognition

Facial recognition authentication is one of the most widely evolving means of biometric authentication system which involves the use of computer and algorithms to analysis facial landmarks (nodal points) such as the nose, cheekbones, shape, shape, and position of the eyes, to verify a person from a digital image or a video frame from a video source. By applying a face recognition application any photo or digital image can be converted to a mathematical code that describes an individual's face.

Improvement in technology continues to evolve more advanced methods of facial recognition including facial metric technology, Eigen faces and three-dimensional face recognition. The 3D facial recognition methods use 3D sensors to capture information about the shape of a face such as facial expressions, head orientation during imaging, or distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin.

2.4.3.5 Hand/Palmprint Recognition

Palmprint recognition like fingerprint recognition consists of a five-step process involving a scanner, prepossessing, feature extraction, matching and database illustration. Palmprints

consist of a few main features that are extracted – flexion creases (principal lines), secondary creases (wrinkles) and ridges with the 3 major flexion curses being genetically dependent, whereas secondary creases are not so, giving everyone unique palmprint patterns (Kong, Zhang and Kamel 2009)

Four main different types of sensors are used to capture palmprint scans, CCD-based palmprint scanners, digital cameras, digital scanners, and video cameras. CCD-based palmprint scanners require suitable conditions of light, lens and camera but can capture very high-quality images. Digital and video cameras can capture images without palmprint contact, but this can cause recognition problems or low-quality scans. Digital scanners meanwhile capture high quality images but require a long scanning time making them more impractical for real-time applications.

2.4.3.6 Voice Biometric Authentication

Voice biometrics (also referred to as speaker recognition by many) is the primary interest within this paper. Voice biometric is a form of inherence-based authentication factor in that it, like fingerprint, iris etc. is supposed to be unique to the user. Similar to other inherence-based authentication factors, the user uses their own voice to authenticate themselves. To do this, users will often use some form of microphone to record their voice, which is often verified in real time against their voice print that is on file (Uniphone 2018). While the technology for voice biometric authentication has been around for years now, only in recent years has it seen huge developments, primarily by companies such as Nuance, regarding it being applied commercially and being considered a secure way for users to authenticate themselves.

Voice biometric authentication requires the user to give a sample of their speech via talking into a microphone. This speech is then converted into a voiceprint that is stored in a database

of voiceprints, so it can be referred to and compared when required, sometimes as a waveform (Krawczyk and Jain 2005). One possible reason why voice biometrics can be considered an effective tool for authentication is because each human has their own unique voice and speech patterns, where they have unique tones, rhythms, frequency, pitch and speech patterns in how they utter phrases (Krom 1994).

2.4.4 Voice Biometric Variations

There are two main variations of voice biometric authentication, being text-dependent and text-independent. Text-dependent systems require the same specific phrase to by said by the user they used to set up the voice print, often called a passphrase. The more common, text-independent systems in contrast do not require the use of passphrases and instead the identification is often done without the user's knowledge (Microsoft 2006). To correctly authenticate users, a form of pattern recognition is utilised which involves many technologies and processes to store the voice prints and then compare them. The main technologies/processes used are the likes of frequency estimation (to correctly identify the frequencies of the voice recordings) and several models such as hidden Markov and Guassian mixture models to systematically model the process and its subpopulations, though these models can change depending on if the voice recognition is text-dependent, or independent.

In the case of hidden Markov models, after hearing the voice, the signal is converted into a digital signal, then each utterance is concerted to a Cepstrum domain. Afterwards the feature parameters of the user are compared with the voice simple which in turn produces a likelihood ration to discern is the user is an imposter or can be successfully authenticated (Shrawankar and Thakare 2013). In the Guassian mixture model approach, the system

recognizes the keyword and utilizes a modelled statistical distribution of the speaker's characteristics and isolated speech from utterance, the model of the user is both calculated and stored in a database during the in-training phase (Janicki and Biały 2006). Though many other ways to authenticate voice by recognition exist, these include pitch tracking, vector quantization, dynamic time warping, fusion classifiers system and several others.

Voice recognition software has also seen wide popular usage in voice activated assistants found in smartphones as well as smart speakers such as Amazon Alexa and Google Home. Smartphones are huge in modern day society with 2.9 billion people owning a smart phone in 2018 and projected to be 3.8 billion by 2021 (Statista 2019). Likewise, many households have already adopted smart speakers into their homes, though the industry is constantly growing, indicating that smart speakers will become an even greater asset to modern day society. While not identical to the voice biometric authentication utilised by banks etc. Voice activated assistants like Alexa, do utilise voice recognition software to recognise its users and fulfil their voice commands. Commands offered by smart speakers include playing music, purchasing products, acting as a calendar and many more. Similar voice recognition software is also seeing deployment into automobiles allowing drivers to issue voice commands to their car without removing attention from the road or taking their hands away from the wheel.

Voice assistants such as Alexa not only have many current features, but also have many developments over the course of the next few years. One such development is the speaker being able to perform person-to-person payments via voice commands (Crosman 2018). Currently, the devices are able to distinguish between users though soon enough speakers such as Alexa will have the ability to also perform verification on your identity to perform

bank payments. Speakers such as Alexa also have many developments into the medical field as well, such as assisting the NHS. The Alexa speaker intends on using the NHS website information in order to answer a user's health queries, as well as many other applications such as managing health-improvement goals, blood-sugar readings and booking appointments (Fleming 2019).

2.4.5 Benefits of Voice Biometric Authentication Factors

Voice biometric authentication (VBA) has many benefits regarding security. For instance, unlike other biometrics, no pictures or recordings are transferred during authentication as it is not done via specialist equipment, instead it can use things such as already existing telephones lines, smartphones, or web applications. Each of these are already widespread and affordable solutions; compared to other authentication methods which require specialist equipment such as sensors or expensive cameras (Vittori 2019). Likewise, authentication is also done in real-time, making the authentication much harder for fraudsters to attack, as there is no data stored on the system or the data can be swiftly deleted after authentication (Vittori 2019).

With the introduction of 'passive' voice-based authentication systems – systems that do not require a specific passphrase to be uttered like 'active' VBA; passive VBA is a lot more secure against potential spoofing from playback or text-to-speech attacks from fraudsters using voice recordings of the user. This 'passive' form of authentication is very advantageous as it does not require any personal or confidential data from the user to be verified and due to advances in A.I systems, can also identify callers under distress should they be in a situation forced to authenticate themself. This is especially useful now with Europe's recent GDPR

(General Data Protection Regulation) bill since no personal data beyond their voiceprint is required. Likewise, VBA can be very fluid in its authentication solutions, switching from passive to active authentication methods should it be required (Vittori 2019).

Another benefit of VBA over other forms of biometric authentication is being able to detect fraudsters in real-time automatically since voice is usually verified over a call. This has helped in reducing fraud, with one of the top three US financial institutions using voice biometrics to uncover fraud groups and patterns, including for example an Israeli bank having a ten-fold reduction in fraud (Beranek 2013). An additional benefit of VBA is in the event an attacker does somehow gain access through using a spoofed recording, providing that attempt is identified as being fraudulent, the organisation can then use that recorded audio to create a 'voice print' which they can blacklist as a fraudster, preventing further breaches occurring using that same 'voice print' (Vittori 2019).

Voice biometrics show many benefits to being used. The study (Wayman et al. 2005) suggests the ideal biometric has five qualities:

1. Robustness - unchanging on an individual over time.
2. Distinctiveness - great variation across all the population.
3. Availability - everyone has access to the measure.
4. Accessibility - easy to detect via a sensor.
5. Acceptability - population are willing to use the measure.

Voice biometrics seem like an excellent candidate, being able to be used by everyone and without any specialist equipment. Voice prints are also quite difficult to spoof due to the

intelligence of the sensor and are relatively unchanging over time. The main factor to voice biometrics being the ideal solution is the population having a willingness to utilise them.

2.4 6 Security attacks of Biometric-based authentication

While biometric systems enhance the user authentication process, they are also susceptible to various types of threats. Some of the threats to biometric systems are directed at the biometric template, which can affect the integrity of the biometric template including: (i) accidental template corruption due to a system malfunction such as a hardware failure, (ii) deliberate alteration of an enrolled template by an attacker, and (iii) substitution of a valid template with a bogus template for the purpose of deterring system functionality (Jain, Anil K., Ross and Uludag 2005).

In addition, with developments of extremely sensitive sensors, biometrics seem more secure than traditional means of authentication such as KBA. Though users can have issue with biometrics due alignment, as generally there is a difference in results between position users use for enrolment and recognition, hence biometric algorithms need good recognition algorithms, to strike a balance between being sensitive or not sensitive enough. Though biometric-based authentication has several other concerns and potential attacks hackers can use. One of the main issues with biometrics, unlike other forms of authentication, is they are not always private. For instance, while a password might only be known to the user, a user's face is constantly on display (unless covered) to any person or camera around (Karimovich and Turakulovich 2016). This is especially true due to the online social age we live in, where people share their lives online through social media, always having their faces on display. Factors such as fingerprints are not immune to this either and while are less on display than perhaps

facial features, fingerprints leave marks on surfaces they touch. While a user having their biometrics compromised, in the short term, is a concern, the greater more long-term issue is that unlike knowledge or ownership-based factors, biometrics are almost impossible to change and once hacked, could be hacked for life. Figure 5 presents the point of attacks to biometric authentication. The figure shows eight possible points hackers can attempt to attack biometric systems (Uludag and Jain 2004).

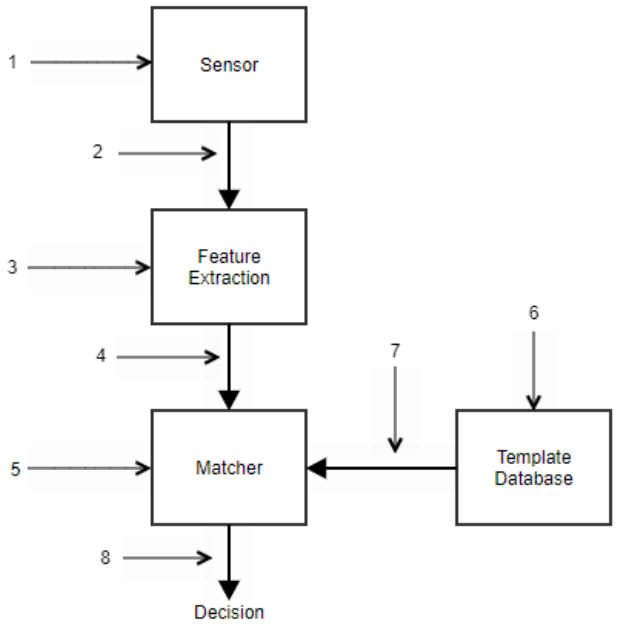

Figure 5: Point of Attacks on Biometric Fusion

At point 1, a presentation attack is used, where an imposter attempts to spoof a user's biometrics with some form of fake image. For instance, in a facial recognition system an attacker may try to spoof the system with a photograph of the user's face, alternatively in a fingerprint system they may use a mould of the user's fingerprint. At points 2, 3, 4 & 5, hackers may try a sensor output interception, which involves them intercepting or perhaps modifying

the data from the sensor with either a previously captured sample they substitute with a different individual's biometrics at the points of feature extraction or obtaining an artificially high matching score at the fifth point. Alternatively, attackers may even target the IT system the sensor is tied to. Perhaps stealing biometric data to use at point 1, or adding/modifying existing templates in the database, by attacking point 6 or altering the transmission at point 7. Alternatively, the attacker might just override the matcher result at point 8 (Uludag and Jain 2004) (National Cyber Security Centre 2019b).

2.4.7 Security attacks on Voice Biometric Authentication Factors

Voice biometrics do however have some concerns regarding the feasibility of the technology as well as the possible security risks of the technology. One of the primary security concerns of the technology is the ability 'spoof' a user by imitating a user's voice (Farmanbar and Toygar 2017). There are many ways for a hacker to attempt to spoof a user's voice, one such way is simply via impersonating the user voice, using a technology to create a synthetic impersonation of that user's voice (Pindrop no date) or even using a recording of that person's voice. Though each of these hacking methods is not without its limitations, given the sensitivity of many voice sensors.

Voice biometric authentication potentially has many other issues as well regarding potential feasibility and security breaches. One such issue that is true for most forms of authentication, is that after the user has been authenticated, the potential concern that afterwards, someone else takes control. This highlights a potential problem with voice biometrics in that once a user has been authenticated, another user may then take over the 'call'. This means that voice biometrics need to continually authenticate users even after the initial authentication entry

point has expired (Artzi 2018). This could however be treated as a strength over other means of authentication too, as unlike means such as passwords or other biometrics, voice can be continually authenticated as it acts as both the authenticator and the input method, allowing the input to continually be authenticated. However, continually authenticating users could possibly have certain issues. For instance, with the required precision needed to prevent fraudsters hacking into voice biometrics with synthesisers, could potentially backfire. In the event a user has a cold or develops a sore throat etc. their voice could sound different to the one on file, especially over a long authentication period caused by continuous authentication. This potentially could cause a user to be unable to access their own accounts due to their voice sounding different, given the high precision required of the voice recognition software as anything less than 100% probability of a match could be considered unacceptable for authentication (Pandya 2019). Another concern could potentially be the quality of the voice over a phone call, in areas with bad reception or slow internet connection could make the users voice sound distorted and unclear, making them unable to authenticate themselves, hence the algorithms need to be sophisticated enough to work around problems such as background noise or crosstalk (Beranek 2013). This is important as biometric data can often be noisy due to the environmental noise, or occlusion of the user's accessories that makes the biometric system less reliable (Krawczyk and Jain 2005). Likewise, many users are concerned with some VBA having users use overt passphrases as they are concerned attackers may hear them utter their passphrases (Beranek 2013). Another such issue is the breaching of the biometric data when it is being collected or stored. Tampering with the collection could mean that future authentication is invalid, or perhaps when the data is transferred and stored that data can be hacked and biometrics unlike other forms of authentication cannot be changed so easily (Bowman 2019).

Further, the technology behind voice biometric authentication is extremely precise in its ability to recognise and authenticate users correctly. Hence, attempting to simply impersonate the user would prove to be extremely difficult, as algorithms such as playback detection are used to see if a caller's speech is unnaturally similar to a past utterance (Beranek 2013). Likewise, to create a synthetic impersonation of a user, it in theory would require equally sophisticated technology to create an indistinguishable synthetic voice.

In regard to preventing a hacker from gaining access via a voice recording of the user, many companies that utilise VBA also employ real time authenticators, to ensure that the speaker on the other line is a real person rather than a recorded message of the user or a synthetic copy of that user. Some other potential attacks have been demonstrated by attacking speakers such as Alexa by sending ultrasonic messages that cannot be perceived by humans (Zhang, G. et al. 2017). However, this very much could be considered an arms race between hackers and security specialists in order to keep voice biometrics and real time authentications ahead of synthetic copies (PYMENTS 2018).

There are many different security attacks on biometric systems as presented in the taxonomy we created in Figure 6. We provide brief descriptions of those attacks below.

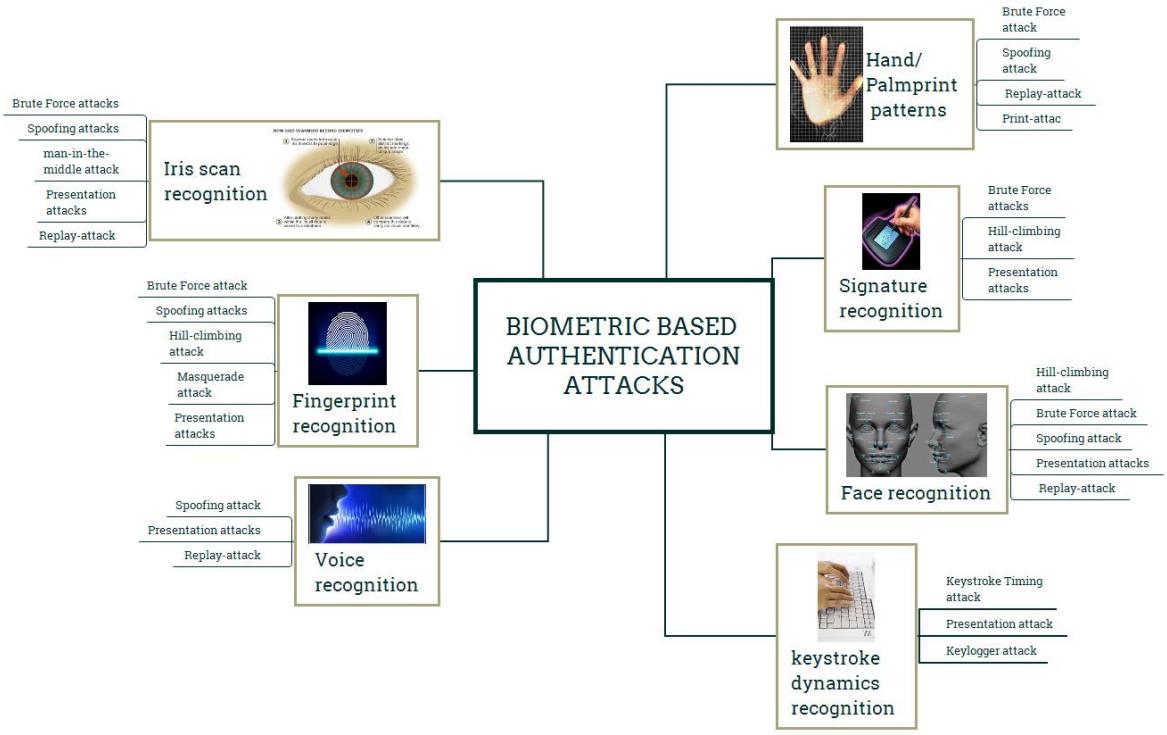

Figure 6: A Taxonomy of Attacks on Biometric Authentication Factors

Spoofing Attacks – Attacking a biometric system by either stealing, copying, or replicating a synthetic biometric trait in order to gain access to a system (Biggio et al. 2012).

Brute Force Attack – Attacking a biometric system by submitting a large number of attempts attempting to spoof the system, usually because the system has not got enough reliable information to discern between similar samples (Mihailescu 2007).

Blended Substitution Attack – An attacker changes the contents in the fuzzy vault, that is stored in the database. This either prevents the user from authentication, combines the user and attacker templates together to spoof the system, or inject their own data during a user's enrolment (Karimovich and Turakulovich 2016) (National Cyber Security Centre 2019) (Sarala, Karki and Yadav 2016).

Attack via Record Multiplicity – An attacker knows the secret access to the record database, collecting multiple enrolment templates to combine the data and at the minimum link records to access the user's biometric template (Karimovich and Turakulovich 2016) (Scheirer and Boult 2007).

Masquerade Attack – A type of spoofing attack, where an attacker attempts to spoof the channel between the sensor and feature extractor module by using false data that is commonly available such as digital facial images or digitised laten fingerprints (Karimovich and Turakulovich 2016) (Roberts 2007).

Attacks on Error Correcting Code – An attack against the fuzzy commitment and fuzzy extract, which abuses the sensors correction algorithm by inputting biometric data close to the user's which is then corrected by the system to false authenticate the attacker (Karimovich and Turakulovich 2016) (Stoianov, Kevenaar and Van der Veen 2009).

Chaff Elimination – The attacker removes chaff points from the user's biometric template to make the biometric sensor easier to spoof, by using similar biometric prints (Karimovich and Turakulovich 2016).

False Acceptance Attack – A form of bypass attack where the system accepts the user even though it is not the user by overriding the processing and decision data due to the biometrics being extremely similar (Karimovich and Turakulovich 2016) (Roberts 2007).

2.4.8 Comparison of Biometric Authentication Factors

In the context of biometric authentication, security can be defined as the strength of the biometric system in terms of covered risk and its efficiency to resist potential attacks; its

sophistication (Jain, Ross and Uludag 2005). We compare the presented authentication factors in Figure 6 in terms of security and accuracy. The comparison was presented in Table 3.

Accuracy

In terms of accuracy, there are two key performance metrics of evaluating biometric systems, namely false acceptance rate (FAR) and false rejection rate (FRR). FAR is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a template. FRR is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template (Arulkumar and Vivekanandan 2018).

Table 3: Comparison of Biometric authentication Factors

Biometric factors	**Security**	**Accuracy**
Fingerprint	Medium	High
Iris Recognition	High	High
Retina Scans	High	High
Face Recognition	Medium	Medium
Voice Recognition	Medium	Medium

Hand/Palmprint Patterns	High	Medium
Signature	Medium	Medium
Keystroke Dynamics	Low	Low

There are two generic approaches for securing biometric templates: biometric feature transformation and biometric cryptosystems.

One of the main countermeasures to biometric fraud from fake or dead fingerprints, is to develop precise sensors that cannot easily be spoofed by copies imitating a user's features (Finextra 2017). Likewise, it is also important that users use multiple-factor authentication to prevent just a single breach causing lots of problems either by combining inherence factors with other types of factors or more forms of biometric authentication, for instance the use of a fingerprint scanner and other forms of biometrics such as facial or iris.

2.5 Ownership Based Authentication

Ownership-based authentication factors are based on something the user has, such as cards, smartphones, or other tokens. For instance, one of the most prevalent examples of ownership-based factors are payment cards, utilised by banks that each possess a unique combination of numbers and security information from one another. Another example of ownership-based factors are tokens that are issued to the user to sign in. As we have moved into a more digital age, one of the most common forms of ownership-based factors is within mobile phones to deliver a single use code, either through receiving the code through text

messages or via an authentication-based app that would provide a code when you attempt to login.

Payment cards are an extremely common form of ownership-based factors and are usually issued by banks. A bank card has a unique string of numbers and data, such as an expiry date and security code that is tied to a user's bank account. Bank cards can come in many different forms, with the most common being credit and debit cards. Similarly, many banks also use tokens/one-time use passwords to authenticate users and the server. Authentication apps and messages are being used for a variety of online accounts to be used in conjunction with passwords as a form of two-factor authentication, some examples include the google authenticator and windows authenticator apps. Alternatively, mobile phones themselves can be used as a token, via Bluetooth wireless communication, using the phone token as a challenge-response protocol (Kunyu, Jiande and Jing 2009).

Another form of ownership-based factor is a smart card or integrated circuit card (ICC card) - an electronic authorization device, used to control access to a resource. The ICC card is typically a plastic credit card-sized card with an embedded integrated circuit (IC) chip (ISO/IEC 2007). A smart card can be in a form of card with a metal contacts to electrically connect to the internal chip, contactless, or in a both forms (Kuo and Lo 1999). Smart cards contain users' authentication, small data storage, and application processing components to perform Input/output (I/O) functions. In terms of applications, most organisations used smart cards for single sign-on (SSO) for pass-through authentication system. Other forms of ownership-based factors include NFC (Chen, W. et al. 2010), RFID (Lim and Kwon 2006), hardware-token (Shablygin et al. 2013), and cell-phones.

2.5.1 Categories of Hardware-token

There are two categories of Hardware-token, synchronous and asynchronous tokens. For synchronous tokens, time synchronization between the token and authentication server is used as part of the authentication process whereas in asynchronous they are not. The two types are shown in the taxonomy we creature below as Figure 7.

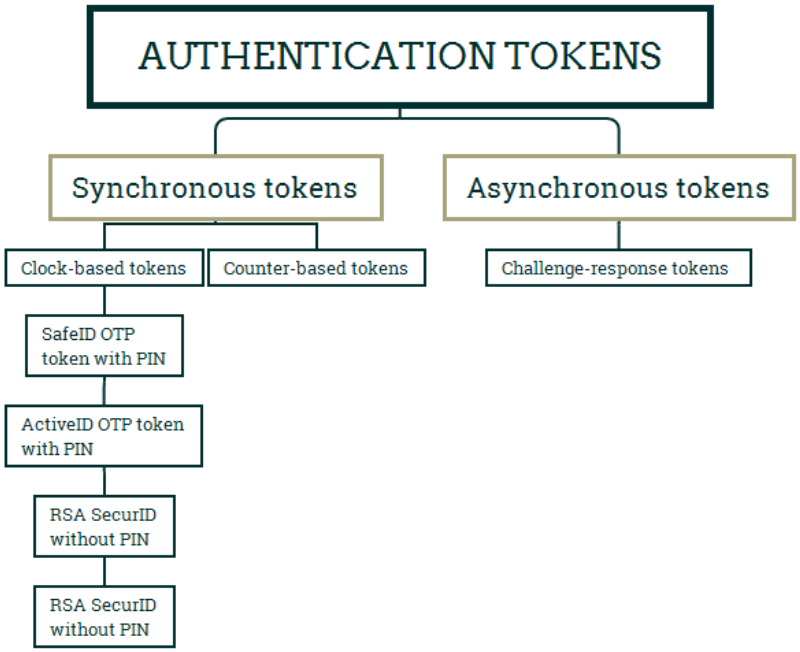

Figure 7: Categories of Authentication Tokens

2.5.1.1 Synchronous tokens

With synchronous tokens, a server keeps the records of a serial number of each authorized token, the user associated with that token, and the time. Using these three pieces of information, a server can predict the dynamic code generated by the token.

As illustrated in the taxonomy we created for Figure 7, synchronous tokens have two subcategories of which can be either clock-based or counter-based. The clock-based OTP tokens are dependent on the time-sensitive codes which must be used within a certain timeframe, often expiring if not used within the correct amount of time. Many authentication apps are time-based and will have to be used quickly before being replaced by another key.

This means usually only the user will have enough time to access the correct code within the necessary time window (Jøsang 2018). Example of the second type of synchronised token is counter-based OTP tokens. Counter-based OTP tokens (sometimes referred to as event-based OTP) generate a form of 'password' from two pieces of internal information. The two pieces of information are the secret key (or seed) which is only known by the token and the second piece of information is the moving factor, aka the counter. To give out a token, the OTP feeds the counter number into an algorithm with the token seed as the key; this produces a 160-bit value that is reduced usually to 6-8 digits for the user to use as an OTP. When the button for the token is pressed, the counter is incremented when an OTP is successfully validated. The key difference between counter and clock-based OTP is that counter-based uses purely internal data rather than external data (Smith 2018).

2.5.1.2 Challenge-Response tokens.

Alternative to synchronised tokens are challenge-response tokens. Challenge-response tokens will propose a challenge or question to the user. The user can then perform the challenge or task by using information only available to the user. Challenge questions can be static or dynamic. Static questions are predefined that the user has previously selected for instance "name of first pet" etc. Dynamic questions are created from extracting public data about the user such as a "previous street address" (Jøsang 2018) (Rouse 2018). Asynchronous tokens are not synchronized with a central server" and that, thus, the most common type is challenge-response tokens.

2.1.2 Security issues of Ownership-based factors

Ownership-based factors, however, are not immune to being hacked and too have disadvantages that can inconvenience the user. The simplest problem with ownership-based factors is in the event that the user loses possession of their factor, or worse it is stolen, they

therefore cannot access their account and the user would both require a replacement and for the old card/token to be made invalid.

Regarding banking cards such as debit/credit, the individual details on them are at risk of phishing-based attacks due to the rise of online commerce and banking. In 2016, of 1.09 million banking trojan attacks were detected and 47.78% of them were from the usage of a phony banking website/page to steal credentials from users (Moramarco Stephen 2019). Most phishing attacks are due the naivety of many users at identifying signs of phishing and being unable to distinguish real sites from fake sites. Many studies such as (Marforio et al. 2016) have investigated protocols that leverage communication between the service to provide security alert indications when in the presence of malicious applications for mobile devices, though even these require the user to be careful and alert for potential phishing.

There are studies that have found that utilising text message-based authentication can also be insecure, when researchers were able to get into a Gmail account to hack Gmail, all they required was a name and a phone number. The hackers were able to exploit a SS7 weakness to intercept SMS text messages from only knowing the number itself, allowing them access into Gmail accounts through password resetting and then proceed to do another reset (Brewster Thomas 2017). This shows the dangers of having multi-factor authentication can also add more vulnerabilities to security, as hackers could be intercepting the codes, despite the user having possession of the device.

The most common issue with ownership-based factors is the user either losing it, or having it stolen. In the event of having a card/token stolen, a user could be compromised, which is why ownership-based factors are usually used in conjunction with knowledge-based factors as

multi-factor authentication. However, credit cards are also vulnerable to SQL injection attacks as well as unpatched systems, or storage of unnecessary data (Braintree 2007). Tokens have many vulnerabilities, though given there are many different types of tokens, these are not mutually exclusive. For instance, any physical form of tokens, that is not part of the client computer, has the potential to be lost or stolen. Likewise, any system that utilises a network for authentication is vulnerable to man-in-the-middle attacks, where the attacker spoofs the "go-between" to solicit the token output from the user. Alternatively, a compromised token may be used for an SQL injection attack to tamper with the database containing user's data by exploiting input validation flaws.

2.6 Location Based Authentication

Location-based authentication (LBA) factors are quite uncommon compared to the likes of knowledge or ownership-based factors. LBA is based on the user (or an object) being located within a certain vicinity in order to correctly authenticate them. This usually involves the user using a location-based client (LBC) to verify with a server containing their location-based ID to authenticate themselves (Zhang, F., Kondoro and Muftic 2012), or a consumer, or a portable consumer device that is used to conduct a transaction at a merchant. Mostly, LBA is being used by financial industries to increase profitability of credit card companies by reducing the accumulated losses due to fraud.

Technology companies and network administrators are using building services that use geolocation security checks to verify the location of a user before granting access to an application, or network or systems. For example, network administrators are using IP addresses to access the origin of network traffic and to know ascertain the users' location

before granting service to the user. Even though, this can be bypassed using IP tunnelling, VPN, or anonymous routing protocols. In addition, MAC addresses, which are unique to individual computing devices, can be implemented as a location-based authentication factor to ensure that a system is only accessed from a limited number of authorized devices (Turnbull and Gedge 2012).

Location-based authentication can also be used as an indicator that a user has been hacked, for instance it would seem odd a user that usually logs in within a certain postcode would be logging in from a different machine perhaps located on the other side of the world. Location-based authentication with mobile devices transitions is mostly used in electronic transaction on a financial institution's online website. The process of authentication may involve verifying whether a mobile device (such as a cellular telephone) is proximate to a computer from which the transaction is being performed (Ashfield, Shroyer and Brown 2012). If the mobile device is not sufficiently proximate, then the transaction may be rejected. If the mobile device is sufficiently proximate, then the transaction may be approved.

To enable location-based authentication, a special combination of objects is required. First, the claimant must present a sign of identity. Secondly, the individual who is to be authenticated must carry at least one human authentication factor that may be recognized on the distinct location and thirdly, the distinct location must be equipped with a means capable to determine the coincidence of individual at this distinct location (Hammad and Faith 2017).

(Lehtonen, Michahelles and Fleisch 2007) investigated different forms of location-based authentication in a product supply chain based on machine-learning techniques (pattern

recognition problem). The results suggest that machine-learning techniques could be used to automatically identify suspicious products from the incomplete location information. (Eden and Avigad 2012) meanwhile presented a LBA system for detecting fraudulent transactions committed by means of misuse of payment cards. The proposed system performs a series of transaction analysis and generates a fraud-score which provides an indication as whether to authorize an attempted transaction or not.

2.6.1 Challenges of Location based authentication.

Location-based authentication is not without its issues however, for instance one large consideration about LBA is that the location used by a user is more publicly available knowledge than that of a password. Attackers could learn of a user's location through various tracking means and then appear at that same location. The accuracy of GPS signals is also crucial to the success of location-based authentication (Sharma 2005). Alternatively, more sophisticated hackers might be able to spoof their location through various means such as through a VPN, meaning that the location-based authentication would have to be more sophisticated to prevent this. Location-based authentication also relies on generating cryptographic keys based on the user's location which in turn could be brute-forced by an attacker, especially if that attacker knew the rough location of a user which would reduce the number of attempts for a brute-force attack dramatically.

Location-based authentication does however have many advantages. Primarily adding an extra layer to authentication as it will only allow sign in from specific locations. This could be useful for a company that would only want employees on site being able to login, or for regular users with home desktops, only specific locations such as their house or on mobile the

town/city they live in. Unlike ownership-based factors, location-based factors cannot be stolen. Also, if location-based factors were being used for a certain building or home, then unlike most other authentication factors there could be several physical layers of protection, primarily locks etc. to keep unwanted hackers from getting in. It also is not necessary to set up specialized infrastructure for location-based authentication as it can be built into existing devices and mobile networks (Zhang, Kondoro and Muftic 2012).

2.7 Trust in Social Context

While trust in a social context and trust with technology could be viewed as being one in the same, many would argue the two concepts have subtle differences, though the two concepts do have many overlaps. For the vast majority of literature, trust is viewed as an attribute to relationships and is a social construct between a person and attributes, it is extremely dynamic as well as subjective, it can evolve with time, a person's experiences and the environment that surrounds it. Likewise, trust is often seen as a unidirectional relation between social agents and is how social agents assess one another to perform actions or tasks with a certain level of probability (Usman and Gutierrez 2019). The study (Uslaner 2002) describes trust as "the chicken soup of social life" – it works mysteriously, and we often choose to develop trust only with agents that we have been exposed to for a long amount of time or are given credible reasons to form bonds of trust. However, many times agents are not provided this luxury and instead must choose to place their trust in agents they have not been exposed to much, to receive the benefits that come from trusting those agents. Distrust however, from a sociologist's point of view is often thought to stem from social aspects, such as an agent's background in social groups, education, income/work satisfaction and general happiness. These aspects are often thought to create more distrusting agents (Newton, Stolle and Zmerli 2018). In the study 'Trust as a Moral Value' (Uslaner 2008) states that another form of trust

exists, known as moralistic trust, which is defined as having faith in strangers regardless of your own life experiences, and goes as far as to say that Countries with more 'trusters' have better functioning governments, more open markets, and less corruption, as trusting people are more likely to volunteer themselves for charitable endeavours.

As previously stated, in order to obtain the many benefits of a service or agent, an agent must first place their trust in that service/agent, even if that service or agent is a stranger. Many would consider that to be taking a risk. The study Trust Building via Risk Taking: A Cross-Societal Experiment (Cook et al. 2005), delves into the idea that a series of risk-taking behaviours is indispensable to building trust, the study discovered that providing an opportunity to choose the level of risk involved in trust, increased the amount of mutual cooperation in participants. These results can infer the importance of the level of risk involved, when building trust. Similarly, in the study a survey of trust in social networks (Sherchan, Nepal and Paris 2013), where in building social networks, social trust is derived from social capital – the collective value associated with a social network, which can be harnessed to cultivate a user having trust with a social network.

Many pieces of literature define trust as an interpersonal concept (Rousseau et al. 1998). As such, some studies theorise that trust can be built in a slightly different way for instance, studies such as (Six 2007) specifically develop theories on interpersonal trust-building within organisations and state they rely on conditions to first be met in order to build trust. These include actors first having to remove thoughts of distrust and instead exchange positive relational signals with the organisation, while in turn avoiding negative signals and stimulating frame resonance (Six 2007). Similar studies such as (Van de Bunt, Gerhard G, Wittek and de Klepper 2005) suggest that the formation of interpersonal trust relationships in organisations generate

specific constraints on how trust can be formed due to the formality of the workplace and as such can be modelled around power and interdependence. Though both these studies only theorise about interpersonal trust specifically within organisations or the workplace. (Soboroff 2012) chooses to investigate the effect that group size has on participant reports. The study suggests that larger groups are less committed than that of smaller groups of 6 or lower. Hence, it could be inferred within large organisations it could be more difficult to develop a tight knit unit. Likewise, participants were more influenced by partners they could see, then those over distance or time zone. Once again it could be inferred that large companies will struggle to develop more trusting groups.

Some studies such as (Asan, Perchonok and Montague 2012) instead choose to look at the measurement of trust in websites, either those of commerce, health or news. The studies show that trust levels change over time regardless of a user's initial trust and having low trust in websites is extremely detrimental to the company itself, with users either not choosing to purchase from companies with untrustworthy sites or choosing not to return to news websites. Other studies such as (Jakubowski, Venkatesan and Yacobi 2010) attempt to quantify a trust model by first separating trust into local trust and then computing it as transitive trust. Local-trust is dependent on the information-gap between the behaviour and the expected behaviour of an agent in the same role. To build their trust model they then feed in the computation of transitive trust to get an average opinion from peers.

2.8 Trust in Technology Context

Trust in technology shares many similar principles with trust in a social context, however, the two perceptions of trust are not identical. For instance, whereas with trust in a social context, a trustee relies on an individual to behave in a reliable manner, though an individual can act

on their own since they have free will and hence can be unpredictable. Meanwhile a technology should consistently perform tasks in a predictable manner, however, unpredictability instead comes from issues such as reliability suffering failures (McKnight 2005). In addition, a user can often expect a technology to fulfil certain functionalities and produce correct results, whereas in a social context when a user depends on another human, they can often only expect that task to be done to the best of that person's capability (Barber 1983). Furthermore, when trusting in a social context with people, a user must consider that person's desire to help and availability to help, unlike with a technology in which that technology is always available (Rempel, Holmes and Zanna 1985).

Many studies such as (Mcknight et al. 2011) have proposed how measures are distinguished between trust with technology and trust within other scenarios, such as in social context or with people, by providing a framework pinpointing key measures specifically for trust with a technology, one such factor being trust developing over time. Akin to trust in a social context, to receive the benefits and features provided by a technology, a user will likely have to trust a piece of technology they are not familiar with.

When it comes to trust with technology many would note that perceptions change over the course of time through continued use and that users are unlikely to experiment with technologies they regard as having a significance level of risk associated with it (Agarwal and Prasad 1997). Often for new technologies to be adopted users must overcome the initial level of trust in order to receive the benefits of trusting a new technology (Gefen 2004). Hence many studies such as (Grabner-Kräuter and Kaluscha 2003), have observed how initial trust with technologies often has a positive correlation with overall trust, which indicates that social influences have some of the strongest effects on how initial trust is formed with technologies.

However, more recent research such as (Asan, Perchonok and Montague 2012) suggests that there is only at best a weak correlation between the initial trust a user has and the final trust a user has, as with continued interaction with a website, users were found that their opinion on the site changed as they were influenced by continued familiarity with the website.

Similarly, when a user wishes to use a service or product provided by a company, they must first provide their data with said company before they can receive the benefits of said service, the same is true for users trusting technology. When looking at human-robot interaction in the military for example, users must trust that their robotic teammates will perform as intended and in turn users must trust that the information provided by robotic teammates will be accurate and useful as well as follow their suggestions. Only by a user trusting a robotic teammate in that regard can they benefit from having them as part of their team. More often than not, the most important aspect for the level of trust with automation such as robots, is based on the reliability of the automation over a course of time by the user experiencing the technology and it is performing its function the same each time. Several studies have observed the relationship of trust and robotic/autonomous machines. Studies such as (Freedy et al. 2007) adopt a performance model to observe the psychology behind team performance, unnamed systems, mixed initiative systems and war fighting behaviour when looking at the relationship of users' trust with robots.

Alternatively, many studies have observed trust between automated self-driving cars and users. Some studies that observe this relationship, consider trust to be defined as a willingness to place themselves in a vulnerable position, with a confident assumption that the technology will perform as expected with a positive outcome (Mayer, Davis and Schoorman 1995). One such study investigated if the perception of trust with automated vehicles changes

after being exposed to experiences with vehicle automation in both the youth and elderly. The findings of this study equally support that more experience with the technology increased the level of trust users had with the technology, in this example it was also found that elderly participants were more trusting of the automated vehicles than younger participants. In a related study, that also investigated the effects of autonomous vehicles, it observed that each of the factors of performance, reliability, security, privacy, and trust all influenced the adoption of driverless cars again showing the factors involved when developing relationships with technology (Kaur and Rampersad 2018)

2.9 A Generic Trust Model Definition and Metrics

The escalating dynamism of current and immerging technologies coupled with wide-ranging impacts of technology in the society make it increasingly important to understand the individual different dimensions to trust on technology and the algorithms behind those technologies. Trust is commonly defined as a confident expectation about a situation leading to willingness to accept vulnerabilities that arise from risk and situational uncertainty (Dietz 2011). Trusting technology beyond their functionality and capacity can present high risk, cost as well as compromise the user's privacy and personal security.

In the first place, trust has to do with the belief, uncertainty, intention, and willingness to trust or not to trust (Usman and Gutierrez 2019). These attributes are behavioural characteristics which cannot be accurately measured and predicted with a high degree of accuracy. Measuring trust level of a user in a social setting or an agent in a distributed system can be a complex process because of the dynamic and unpredictable nature of trust. Metrics quantitative metrics (Cruz, Mishra and Bhunia 2019), qualitative metrics (Patent and Searle 2019),

fuzzy metrics, or a combination of these are used to measure trust levels with trust model and metrics has its own specific characteristics and requirements; nonetheless, their pattern and abstract scheme can be generalized.

Much of the prior research in a distributed system and the autonomous systems has focused primarily on the psychological aspect of trust in coming up with the definition of trust (Usman and Gutierrez 2018). This sometimes requires the linkage between psychological aspects of trust and the characteristics of the autonomous systems. For example, many attempts have been made to map psychological aspects of trust such as reliability, dependability, and integrity between social actors in a close relationship (Rempel, Holmes and Zanna 1985) with engineering trust issues such as reliability, dependability, and security (Usman, Gutierrez and Bichi 2019) in a network of distributed system. This gives researchers a flexible and realistic way of defining and interpreting such as a social construct and multidimensional phenomenon like trust.

Modifying the definition of trust proposed by (Hoffman, Lawson-Jenkins and Blum 2006), we define trust as the expectation and experience that a technology will provide the user with the sense of security, reliability, and confidence. With this definition, to derive users' trust, we identified five main key components of the trust definition. The five keywords are: usability, availability, security, privacy, and reliability. For a realistic adoption of the (Hoffman, Lawson-Jenkins and Blum 2006) trust model, we identified four other internal metrics that can contribute to the derivation of our trust model. The metrics are user experience, recommendation (trust propagation), knowledge and verification. Hence, based on our research behind what defines trust, we used the trust model proposed by (Hoffman, Lawson-

Jenkins and Blum 2006) over other similar models given it is a reasonably well cited article and expands on many metrics laid out by older trust models as shown in Figure 8.

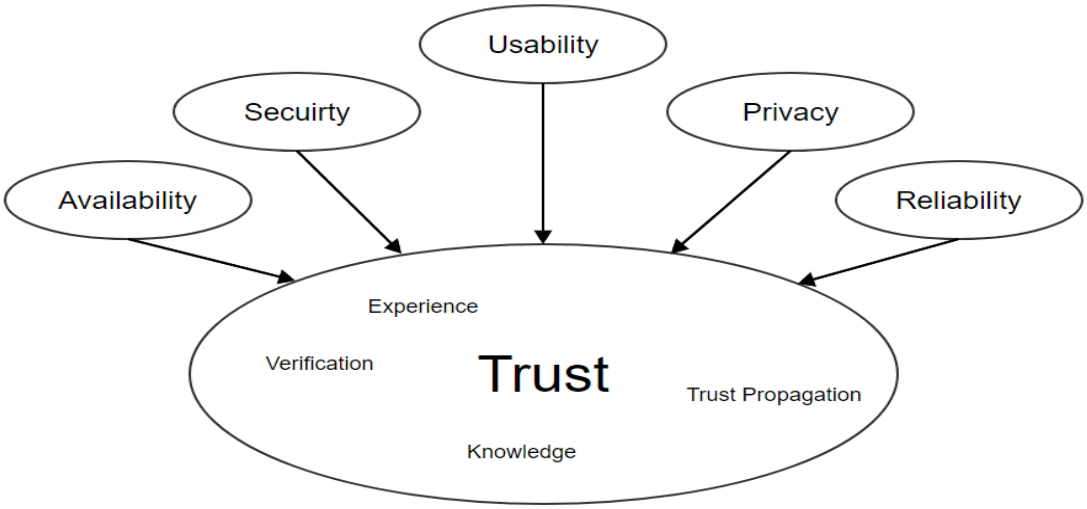

Figure 8: An Expanded Trust Model

2.10 Trust Metrics and Elements

We described the presented trust metrics and elements in Figure 8.

Availability – how widespread and utilised the technology is. From a user's point of view, availability means that they can access it whenever they require, regardless of specialist equipment being available to authenticate the user when needed, being widespread and being a common example of other authentication techniques.

Security - how secure the technology is from potential attacks. From a user's point of view, security is important in trusting that the authentication system will perform the users' intended functions with relative security, that the authentication method is not easily hacked, tampered with and that the method is able to differentiate the user with a degree of accuracy.

Usability – how easy a user can utilise the features of the authentication. From a user's point of view usability means they can use it without confusion meaning it is easy to use, easy to learn and is accessible to different needs such as a disability.

Privacy – how the method keeps user's sensitive information secure and protects the anonymity of a users' identity. From a user's perspective this means protecting their privacy from others, preventing others from seeing the contents of their data and allows the user to remain anonymous.

Reliability – the reliability of the technology in the eyes of the user as how the technology can consistently perform and function as expected by the user, performed the same each time it was used and will continue to perform as expected in further uses.

As can be seen, the trust model presented in Figure 8, incorporates aspects of security, usability, reliability, availability, safety, and verification mechanisms, as well as user privacy concerns, user experience, and user knowledge about the technology. The model also identified four key elements that contributed to formulation of trust.

The **experience** users have had with the method, such as have they used it many times before, do they use similar methods that are based on the same factors, or do they use different authentication methods often.

The **verification** the method provides the user with, the method provides by feedback to show it has been processed the authentication request correctly, an error had occurred or that it had been set-up correctly.

The **knowledge** of the method a user has, such as the understanding they have of the authentication method itself, how the overall authentication process works and why it is used.

The **propagation** of the method, or what experiences about the method they have shared, or been shared, such as good experiences, bad experiences or just their general perception of the methods reputation.

An example of how these factors interact could be from the user continuing to use the technology and the technology proving to be reliable by producing the same consistent results each time. This can give the user a good experience of the technology and build a more trusting relationship. Alternatively, a user might hear from a colleague about how easy a technology is to use, and that trust propagation helps to build a foundation level of trust with the user and that technology.

2.11 Chapter Summary

In this chapter we provided the foundations and concepts that this study draws upon which is already known on the research topic. Specifically, we provided a detailed look at various authentication methods and factors that we will be investigating in this study as well as how each of them are targeted by a variety of attacks and advantages the method provides. We also discussed trust in both a social and technological context and presented the trust model that will be used in the study to identify and understand the different levels of trust users have with different authentication methods.

3. Research Method

In this section the research method applied in this study is discussed. To conduct this study, a variation of the design science was adapted to try answer the research questions and prove or disprove the hypothesis's as follows. The philosophy behind this altered design science method, is to first identify the question proposed and the reason for why it is needed to be answered. The method then discusses how the data will be acquired via the experiment, followed by a discussion about the possible answer to the questions and a conclusion.

3.1 Research Framework

The studies research framework is adapted from traditional design science models to be more focused upon a researcher's perspective over an engineering perspective. The model is shown in Figure 9 and is broken into 5 stages.

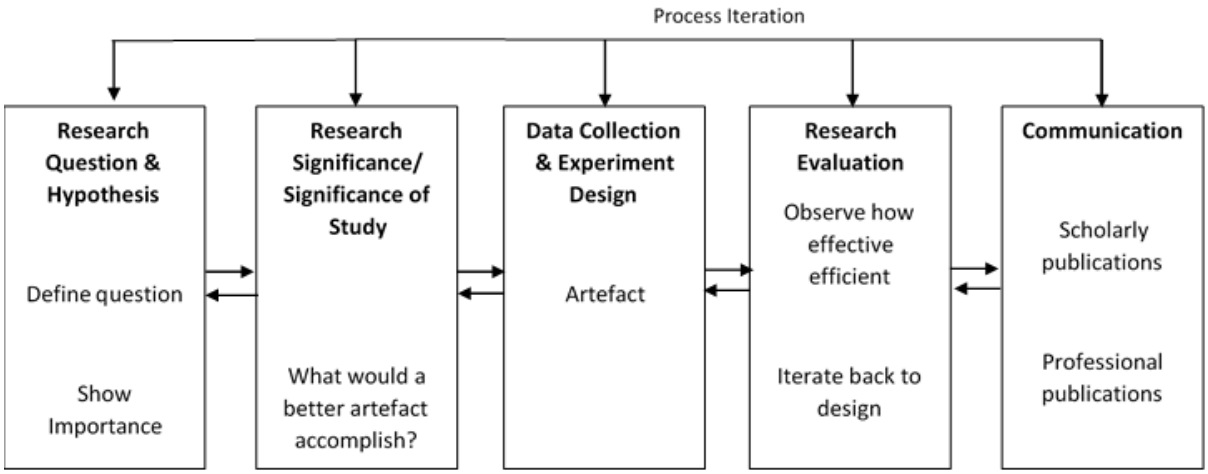

Figure 9: Design Science Model

The first stage is to identify the initial research question(s) that the study is seeking to answer. The questions need to be clearly defined.

The second aspect is to discuss the significance the study will have upon either the sphere of research or to companies and the mass public. This can include justification as to why the study is important to the field of research and how it can benefit people.

The third step is to design the parameters and constraints of whatever experiment is being run and then begin collecting said data, so that it can be analysed and discussed in the context of the study, to attempt to answer the research questions.

The fourth phase involves observing the results found in the data collection and to analyse and present them in a way that will hopefully answer the previously outlined research questions.

The fifth and final stage of the model is the communication aspect, which encompasses the discussion about the results and responding conclusions found from the data collection and analysis. Often this step results in possible future studies that could be iterated from the findings of the research. Despite this the study only utilised a few iterations, namely redefining research questions and debate around using Amazon MTurk when lockdown was first introduced, these were the only iterations the study had due to the limited time given to complete the entire thesis.

3.2 Experiment

3.2.1 Experiment Design

The experiment utilises a between-groups testing method. This means that each participant will only utilise one method of authentication (password, token, fingerprint, voice). Hence, each method of authentication will be assigned one group of participants that utilise it, though participants will be tested one at a time on their own. The opposite of this would be a repeated measures method, where each participant would utilise all authentication

methods and would give feedback on them all. The reason a between-groups method was chosen over a repeated measures method is that during a repeated measure, participants could have been influenced by their answers to previous authentication methods, which could cause them judge methods in a different light. Likewise, in the interest of running a more concise and credible experiment, a between-groups method will not only reduce experiment fatigue of participants, from having to utilise lots of authentication methods, but also forces the need for a greater number of participants which will hopefully improve the credibility of the results found. The dependent variable of the study is the measurement of trust. To gauge the measurement of users of trust, a questionnaire is utilised with questions based on the 'Generic Trust Model' as proposed in the study (Hoffman, Lawson-Jenkins and Blum 2006) found under Figure 8 in the previous chapter. The independent variables of the study are the various means of authentication that are utilised by participants, these include PIN, fingerprint, token and voice biometrics.

3.2.2 Materials

To test all methods of authentication covered by this study (PIN, fingerprint, token and voice biometrics) an android Samsung Galaxy S9 phone will be used alongside a standard university computer running windows 10 operating system. Each participant/control group will use the same model of phone. To test PIN & fingerprint, users will use the built-in settings to set up their authentication then unlock the phone. Control groups testing voice biometric authentication, they will use google assistant to unlock the phone via voice commands after setting up their voice profile. Meanwhile participants utilising tokens, will be provided a token through a windows application that they set up that will unlock the phone.

3.2.3 Measures

To try answer both research question 1 & 2 participants will need to be measured for the amount of trust they have with each authentication method. In order to do this, a proxy measure of trust will be utilised via a questionnaire. The questionnaire's questions will be based on the 'Generic Trust Model' which identifies the core aspects of availability, security, usability, privacy and reliability which each contribute to the acquisition of trust. The model also identifies from these 5 aspects of trust, there are connections which also affect the level of trust a user would have. There connections are the experience of the technology, the verification/feedback provided by the technology, the knowledge/understanding of how the technology functions and the propagation of good or bad experiences with the technology. Each of these core aspects and connections will have participants ranking them on a scale of 1-5 via a questionnaire which in turn can be analysed to see if the levels of trust are in any way significant between the technologies from a user standpoint. The model along with the measurement of trust is covered in more detail in the previous chapter.

3.2.4 Participants

In total, 60 participants took part in the experiment. Participants were aged between 18-60 of which, 46 were male and 14 were female. The participants were selected from around the university campus and colleagues with no bias as to who was selected, though all participants were English speakers and had varying previous amounts of exposure to the chosen authentication methods. Participants were allocated one of the four methods, with the next three participants doing the other three methods, before the next participant used the first method again. The study was conducted over the period of a month from the end of September 2020 to the end of October 2020.

3.2.5 Procedure

Participants first had to agree to participate in the study after being verbally briefed by the researcher that they would set up an authentication method, utilise it and then fill out a questionnaire, in total each participant took between 10-15 minutes to participate in the study. To confirm this, they filled out a written consent form opting into the study. Afterwards they would be required to utilise one of the 4 authentication methods (PIN, token, fingerprint, & voice) based on the control group they were placed in. Participants would first set up their authentication method, for fingerprint and PIN this involved using the in-built Samsung Galaxy settings, for voice they set up a voice print with google assistant and for token they provided their email address to a simple webpage that was on a university computer that would provide them with a token to unlock the phone. Participants then unlocked the phone using the authentication method they had set up prior. Afterwards they would fill out a questionnaire based on the expanded model of trust aspects (availability, security, usability, privacy and reliability) as well as the connections of trust the (experience of the technology, the verification/feedback provided by the technology, the knowledge/understanding of how the technology functions and the propagation of any good or bad experiences with the technology). This is shown in the appendix from figures 20-28. After the study, participants were debriefed about any concerns they may have had about the study being intentional and that their data was deleted, with only the questionnaire results being used in the study.

3.3 Chapter Summary

This chapter discussed the adapted version of design science that was used throughout the study. The approach focussed more so on a researcher's perspective rather than that of an engineering perspective as of traditional design science. The model devised by the thesis is included above. Rather than traditional design science, the model instead proposes a

question and possible hypotheses along with the approach taken to try answer and discuss them. This is instead of a traditional design science method of an engineer's approach, which is to analyse a problem and propose a solution rather than a question. Design science was adopted, despite its usual inclination towards engineers and problem solving, because the principal structure still applies and is able to offer a clear methodological framework to base the thesis process on. Finally, the chapter discussed the approach taken to find the possible answers to the research questions. In this case, an experiment was chosen, and the chapter goes on to discuss the various parts of the experiment including what was used, what was measured and the general procedure in its entirety, along with justification.

4. Results and Discussion Part 1: Kruskal-Wallis H Statistical Analysis

This chapter presents the results of the study after performing the Kruskal-Wallis H test. We present these findings, before then going on to discuss the overall findings about each question.

We analysed the results using the Kruskal-Wallis H test, to find which results were deemed statistically significant and test the hypothesis:

> Users have varying degree of trust about user-based biometric authentication method to access technology based on the chosen trust evaluation model.
>
> Users may be found to be willing to trust technology and voice-based biometrics as a method of user authentication.

Or the null hypothesis:

> Users have the same degree of trust about user-based biometric authentication method to access technology based on the chosen trust evaluation model.
>
> Users may be found to not be willing to trust technology and voice-based biometrics as a method of user authentication.

We used Kruskal-Wallis test instead of one-way ANOVA as there is no assumption that our data would have a normal distribution, hence we ran the non-parametric Kruskal-Wallis H test. To determine which specific groups had a statistical significance to one another, we then ran a post-Hoc test on the groups that had a statistical significance. We applied the mean rank as the average of the ranks for all observations within each sample of the collected data. Since we are using the Kruskal-Wallis H test (McKight and Najab 2010), we used SPSS to rank the combined samples by assigning the smallest observation a rank of 1, the second smallest

observation a rank of 2, and so on. In the event where the two or more observations are tied, SPSS assigns the average rank to each tied observation to calculate the mean rank for each sample. After ranking all values, the Kruskal-Wallis H statistic is calculated via:

$$H = \left[\frac{12}{n(n+1)}\sum_{j=1}^{c}\frac{T_j^2}{n_j}\right] - 3(n+1) \qquad (3)$$

Where: n = sum of sample sizes for all samples, c = number of samples, T_j = sum of ranks in the jth sample, n_j= size of the jth sample.

The results for each test are shown in table 4 below, with how each question performed, their mean rank which has a maximum value of 60 given our number of participants (the mean of the ranks assigned to the data since it is more appropriate to use ranks over values to prevent testing being affected by the presence of outliers), median for each group, standard deviation, Kruskal-Wallis H statistic, and the number of participants that used the method is shown in the final column. If the question has an assumed significance figure (p-value) that is less than the alpha value (significance level of) 0.05, it can be considered statistically significant, as indicated by an asterisk in the p-value column, else it is not statistically significant.

4.1 Kruskal-Wallis Result Table

Question		Sample Size (n)	Method	Mean Rank	Med-ian	Std. Dev.	H	p-value
Availability	Method is available when needed?	15	Voice	28.60	5	0.497	2.248	0.523
		15	PIN	33.10	5			
		15	Fingerprint	27.20	5			
		15	Token	33.10	5			
	The authentication method is widespread?	15	Voice	29.67	4	0.841	3.060	0.383
		15	PIN	36.50	5			
		15	Fingerprint	26.77	4			
		15	Token	29.07	4			
	A common example of authentication techniques?	15	Voice	25.40	4	0.848	3.704	0.295
		15	PIN	36.07	5			
		15	Fingerprint	29.40	5			
		15	Token	31.13	5			
Security	I believe the authentication method is not easily hacked?	15	Voice	18.07	3	1.136	15.199	0.002*
		15	PIN	30.10	3			
		15	Fingerprint	41.63	4			
		15	Token	32.20	4			
	Method is not easily tampered with?	15	Voice	21.63	3	1.031	6.547	0.088
		15	PIN	30.33	4			
		15	Fingerprint	35.87	4			
		15	Token	34.17	4			
		15	Voice	28.33	4	1.331	19.586	p < 0.001*
		15	PIN	23.97	4			

	Method is able to differentiate me?	15	Fingerprint	46.67	5			
		15	Token	23.03	3			
Usability	Learning to use the authentication method easy?	15	Voice	27.63	5	0.431	4.336	0.227
		15	PIN	33.53	5			
		15	Fingerprint	27.30	5			
		15	Token	33.53	5			
	I found the authentication method easy to use?	15	Voice	27.90	5	0.628	6.553	0.088
		15	PIN	36.00	5			
		15	Fingerprint	25.97	5			
		15	Token	32.13	5			
	Accessible to different needs?	15	Voice	33.40	4	1.017	1.392	0.707
		15	PIN	30.63	4			
		15	Fingerprint	31.47	4			
		15	Token	26.50	4			
Privacy	Protects my privacy from others?	15	Voice	15.50	3	1.030	22.332	p < 0.001*
		15	PIN	37.13	5			
		15	Fingerprint	42.07	5			
		15	Token	27.30	4			
	Prevents others from seeing my data?	15	Voice	19.50	3	1.039	9.503	0.023*
		15	PIN	35.77	4			
		15	Fingerprint	35.60	4			
		15	Token	31.13	4			
		15	Voice	22.80	3	1.307	8.198	0.042*

	Method allows me to remain anonymous?	15	PIN	38.23	4			
		15	Fingerprint	34.87	4			
		15	Token	26.10	3			
Reliability	Authentication functioned as I expected it to?	15	Voice	29.10	5	0.504	3.469	0.325
		15	PIN	35.00	5			
		15	Fingerprint	29.10	5			
		15	Token	29.10	5			
	Method performed the same each time?	15	Voice	24.83	4	0.813	11.205	0.011*
		15	PIN	40.50	5			
		15	Fingerprint	25.43	5			
		15	Token	31.23	5			
	Will continue to perform as expected in further uses?	15	Voice	25.60	4	0.701	16.310	0.001*
		15	PIN	41.50	5			
		15	Fingerprint	21.20	4			
		15	Token	33.70	5			
Experience	I used the authentication method many times before?	15	Voice	15.27	2	1.570	20.773	p < 0.001*
		15	PIN	39.53	5			
		15	Fingerprint	32.57	5			
		15	Token	34.63	5			
	I use similar authentication methods often?	15	Voice	19.43	2	1.448	12.370	0.006*
		15	PIN	39.53	5			
		15	Fingerprint	19.43	4			
		15	Token	33.57	5			
		15	Voice	34.80	5	1.247	5.056	0.168
		15	PIN	35.27	5			

	I use different authentication methods often?	15	Fingerprint	28.10	4			
		15	Token	23.83	4			
Verification	Feedback that authentication has processed correctly?	15	Voice	21.17	4	0.616	8.376	0.039*
		15	PIN	37.17	5			
		15	Fingerprint	32.37	5			
		15	Token	31.30	5			
	Feedback when a type of error has occurred?	15	Voice	20.70	3	1.145	18.475	p < 0.001*
		15	PIN	40.40	4			
		15	Fingerprint	39.27	4			
		15	Token	21.63	3			
	Good feedback that it has been set up correctly?	15	Voice	33.30	5	0.930	8.064	0.045*
		15	PIN	33.07	5			
		15	Fingerprint	35.03	5			
		15	Token	20.60	4			
Knowledge	I understand how the method works?	15	Voice	26.50	4	0.780	3.982	0.263
		15	PIN	36.80	5			
		15	Fingerprint	27.40	4			
		15	Token	31.30	5			
	I have a good understanding of the authentication process works?	15	Voice	23.27	4	0.914	9.184	0.027*
		15	PIN	37.87	5			
		15	Fingerprint	25.43	4			
		15	Token	35.43	5			

	Understanding of why authentication method is used?	15	Voice	23.30	4	0.623	6.022	0.111
		15	PIN	36.10	5			
		15	Fingerprint	29.43	5			
		15	Token	33.17	5			
Recommendation	I have heard others have good experiences with the authentication	15	Voice	19.07	3	1.152	12.951	0.005*
		15	PIN	37.77	5			
		15	Fingerprint	37.53	5			
		15	Token	27.63	4			
	I have heard others have bad experiences with the authentication	15	Voice	30.37	2	1.239	1.572	0.666
		15	PIN	29.77	3			
		15	Fingerprint	34.77	3			
		15	Token	27.10	2			
	The authentication method has a good reputation?	15	Voice	20.10	3	0.933	9.053	0.029*
		15	PIN	34.40	4			
		15	Fingerprint	37.00	4			
		15	Token	30.50	4			

Table 4: Kruskal Wallis Test Results

4.1.1 Availability

The results show that when asked if “The authentication method is available when needed?” there was no statistical significance between the authentication methods, X^2 (2) = 2.248, p = 0.523. Though in terms of mean ranking score, PIN & token tied as the highest with 33.10, voice came second with 28.60 and fingerprint came last with 27.20.

The results show that when asked if “The authentication method is widespread?” there was no statistical significance between the authentication methods, X^2 (2) = 3.060, p = 0.383. Though in terms of mean ranking score, PIN scored the highest with 36.50, voice came second with 29.67, token came third with 29.07 and fingerprint came last with 26.77.

The results show that when asked if “The authentication method is a common example of authentication techniques” there was no statistical significance between the authentication methods, X^2 (2) = 3.704, p = 0.295. Though in terms of mean ranking score, PIN scored the highest with 36.07, token came second with 31.13, fingerprint came third with 29.40 and voice came last with 25.40.

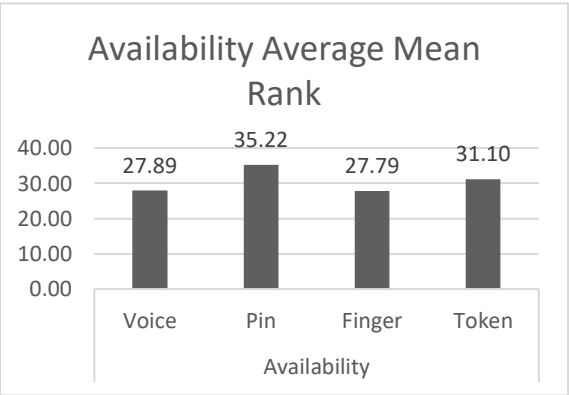

Figure 11: Availability Mean Rank

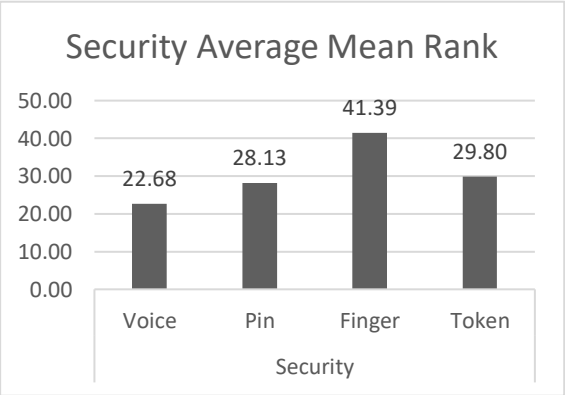

Figure 10: Security Mean Rank

4.1.2 Security

The results show that when asked if "I believe the authentication method is not easily hacked?" there was a statistical significance between the authentication methods, X^2 (2) = 15.199, p = 0.002. Though in terms of mean ranking score, fingerprint scored the highest with 41.63, token came second with 32.20, PIN came third with 30.10 and voice came last with 18.07.

The results show that when asked if "I believe the authentication method is not easily tampered with?" there was no statistical significance between the authentication methods, X^2 (2) = 6.547, p = 0.088. Though in terms of mean ranking score, fingerprint scored the highest with 35.87, token came second with 34.17, PIN came third with 30.33 and voice came last with 21.63.

The results show that when asked if "I believe the authentication method is able to differentiate me from others?" there was a statistical significance between the authentication methods, X^2 (2) = 19.586, p < 0.001. Though in terms of mean ranking score, fingerprint scored the highest with 46.67, voice came second with 28.33, PIN came third with 23.97 and token came last with 23.03.

4.1.3 Usability

The results show that when asked if "I found learning to use the authentication method easy?" there was a statistical significance between the authentication methods, X^2 (2) = 4.336, p = 0.227. Though in terms of mean ranking score, PIN & Token tied as the highest with 33.53, voice came second with 27.63 and fingerprint came last with 27.30.

The results show that when asked if "I found the authentication method easy to use?" there was no statistical significance between the authentication methods, X^2 (2) = 6.553, p = 0.088. Though in terms of mean ranking score, PIN scored the highest with 36.00, token came second with 32.13, voice came third with 27.90 and token came last with 25.97.

The results show that when asked if "I found the authentication method accessible to different needs?" there was no statistical significance between the authentication methods, X^2 (2) = 1.392, p = 0.707. Though in terms of mean ranking score, voice scored the highest with 33.40, fingerprint came second with 31.47, PIN came third with 30.63 and token came last with 26.50.

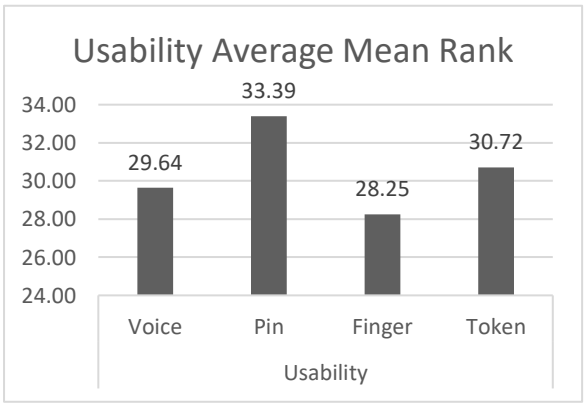

Figure 12: Usability Mean Rank

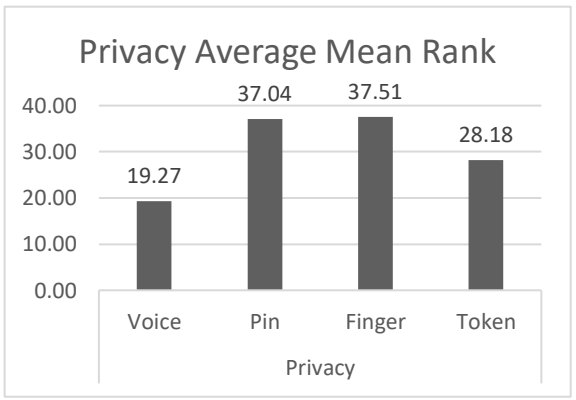

Figure 13: Privacy Mean Rank

4.1.4 Privacy

The results show that when asked if "I believe the authentication method protects my privacy from others?" there was a statistical significance between the authentication methods, X^2 (2) = 22.332, p < 0.001. Though in terms of mean ranking score, fingerprint scored the highest

with 42.07, PIN came second with 37.13, token came third with 27.30 and voice came last with 15.50.

The results show that when asked if "I believe the authentication method prevents others from seeing the contents of my data?" there was a statistical significance between the authentication methods, X^2 (2) = 9.503, p = 0.023. Though in terms of mean ranking score, PIN scored the highest with 35.77, fingerprint came second with 35.60, token came third with 31.13 and voice came last with 19.50.

The results show that when asked if "I believe the authentication method allows me to remain anonymous?" there was a statistical significance between the authentication methods, X^2 (2) = 8.198, p = 0.042. Though in terms of mean ranking score, PIN scored the highest with 38.23, fingerprint came second with 34.87, token came third with 26.10 and voice came last with 22.80.

4.1.5 Reliability

The results show that when asked if "The authentication functioned as I expected it to?" there was no statistical significance between the authentication methods, X^2 (2) = 3.469, p = 0.325. Though in terms of mean ranking score, PIN scored the highest with 35.00, with fingerprint, tokens and voice all scoring 29.10.

The results show that when asked if "The authentication method performed the same each time?" there was a statistical significance between the authentication methods, X^2 (2) = 11.205, p = 0.011. Though in terms of mean ranking score, PIN scored the highest with 40.50,

token came second with 31.23, fingerprint came third with 25.43 and voice came last with 24.83.

The results show that when asked if "The authentication method will continue to perform as expected in further uses?" there was a statistical significance between the authentication methods, X^2 (2) = 16.310, p = 0.001. Though in terms of mean ranking score, PIN scored the highest with 41.50, token came second with 33.70, voice came third with 25.60 and fingerprint came last with 21.20.

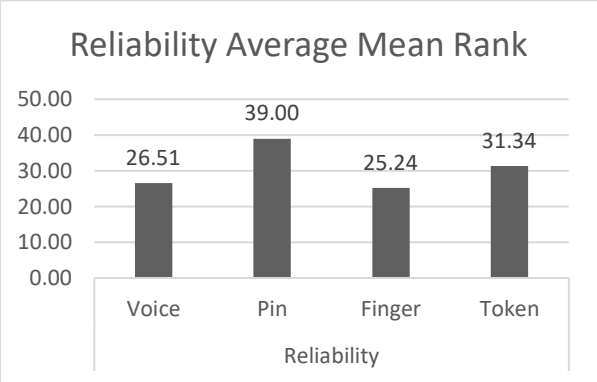

Figure 14: Reliability Mean Rank

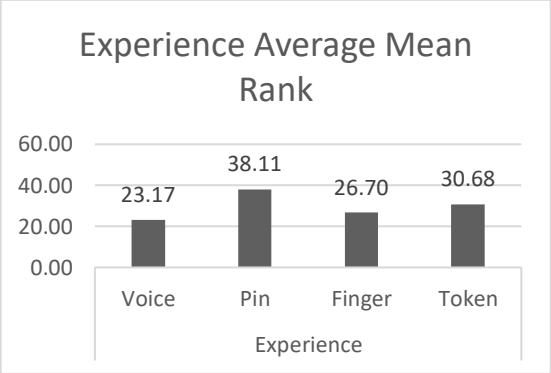

Figure 15: Experience Mean Rank

4.1.6 Experience

The results show that when asked if "I have used the authentication method many times before?" there was a statistical significance between the authentication methods, X^2 (2) = 20.773, p < 0.001. Though in terms of mean ranking score, PIN scored the highest with 39.53, token came second with 34.63, fingerprint came third with 32.57 and voice came last with 15.27.

The results show that when asked if "I use similar authentication methods often?" there was a statistical significance between the authentication methods, X^2 (2) = 12.370, p = 0.006.

Though in terms of mean ranking score, PIN scored the highest with 39.53, token came second with 33.57, fingerprint and voice tied for last with 19.43.

The results show that when asked if "I use different authentication methods often?" there was no statistical significance between the authentication methods, X^2 (2) = 5.056, p = 0.168. Though in terms of mean ranking score, PIN scored the highest with 35.27, voice came second with 34.80, fingerprint came third with 28.10 and token came last with 23.83.

4.1.7 Verification

The results show that when asked if "I believe the authentication method offers good feedback that my authentication has processed correctly?" there was a statistical significance between the authentication methods, X^2 (2) = 8.376, p = 0.039. Though in terms of mean ranking score, PIN scored the highest with 37.17, fingerprint came second with 32.37, token came third with 31.30 and voice came last with 21.17.

The results show that when asked if "I believe the authentication method offers good feedback when some type of error has occurred?" there was a statistical significance between the authentication methods, X^2 (2) = 18.475, p < 0.001. Though in terms of mean ranking score, PIN scored the highest with 40.40, fingerprint came second with 39.27, token came third with 21.63 and voice came last with 20.70.

The results show that when asked if "I believe the authentication method offers good feedback that it has been set up correctly?" there was a statistical significance between the authentication methods, X^2 (2) = 8.064, p = 0.045. Though in terms of mean ranking score,

fingerprint scored the highest with 35.03, voice came second with 33.30, PIN came third with 33.07 and token came last with 20.60.

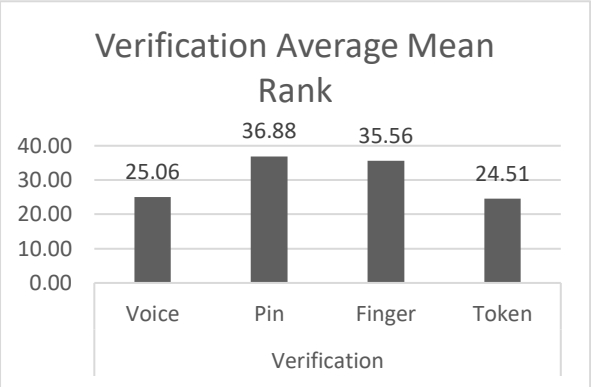

Figure 17: Verification Mean Rank

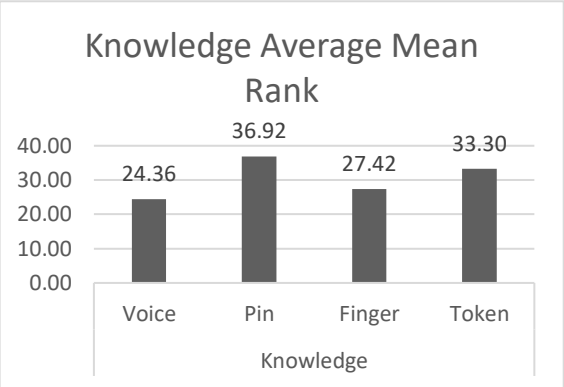

Figure 16: Knowledge Mean Rank

4.1.8 Knowledge

The results show that when asked if "I have a good understanding of how the authentication method works?" there was no statistical significance between the authentication methods, X^2 (2) = 3.982, p = 0.263. Though in terms of mean ranking score, PIN scored the highest with 36.80, token came second with 31.30, fingerprint came third with 27.40 and voice came last with 26.50.

The results show that when asked if "I have a good understanding of how the authentication process works?" there was a statistical significance between the authentication methods, X^2 (2) = 9.184, p = 0.027. Though in terms of mean ranking score, PIN scored the highest with 37.87, token came second with 35.43, fingerprint came third with 25.43 and voice came last with 23.27.

The results show that when asked if "I have a good understanding of why the authentication method is used?" there was no statistical significance between the authentication methods,

X^2 (2) = 6.022, p = 0.111. Though in terms of mean ranking score, PIN scored the highest with 36.10, token came second with 33.17, fingerprint came third with 29.43 and voice came last with 23.30.

4.1.9 Recommendation

The results show that when asked if "I have heard others have good experiences with the authentication method?" there was a statistical significance between the authentication methods, X^2 (2) = 12.951, p = 0.005. Though in terms of mean ranking score, PIN scored the highest with 37.77, fingerprint came second with 37.53, token came third with 27.63 and voice came last with 19.07.

The results show that when asked if "I have heard others have bad experiences with the authentication method?" there was no statistical significance between the authentication methods, X^2 (2) = 1.572, p = 0.666. Though in terms of mean ranking score, fingerprint scored the highest with 34.77, voice came second with 30.37, PIN came third with 29.77 and token came last with 27.10.

The results show that when asked if "The authentication method has a good reputation?" there was a statistical significance between the authentication methods, X^2 (2) = 9.053, p = 0.029. Though in terms of mean ranking score, fingerprint scored the highest with 37.00, PIN came second with 34.40, token came third with 30.50 and voice came last with 20.10.

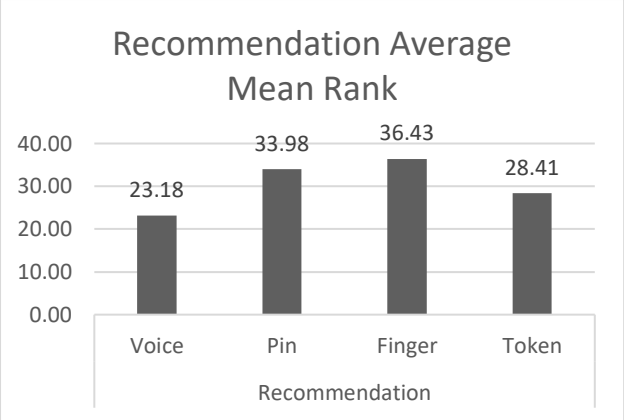

Figure 18: Recommendation Mean Rank

4.2 Chapter Summary

In this chapter we provided the results for our first test using the Kruskal-Wallis H Test. We presented those results in a table format and then reported our findings for each question. The Kruskal-Wallis H test tells us which methods had a statistical significance, of which we then proceed to perform the post-Hoc test as detailed in the next chapter.

5. Results and Discussion Part 2: Post Hoc Analysis

In this chapter we perform the post-Hoc test on the statistically significant questions, of which we provide reports for each question. We then go onto to discusses both the statistically significant and non-statistically significant questions to infer what the results tell us.

After conducting the experiment, the Kruskal-Wallis test tells us that 15 of the 27 questions were found to have a statistical significance between them. The remaining questions were not considered statistically significant; however, some conclusions may apprehensively be drawn from them. We then ran the post-Hoc test using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons on the statistically significant questions to determine which authentication methods specifically were significant to one another seeing if there were any pairwise comparisons between the methods. The reason we chose this test was because we have a small subset of all possible pairs. As shown in the tables below are the pairwise comparisons of the test. Std. Test Statistic being after the data has been standardised, so it can be compared to a 'normal' population.

Out of all methods, across all questions, voice consistently either tied as, or was ranked the lowest 17 times of which 13 of the questions were statistically significant. Vice versa, across all questions, the authentication method that ranked the highest most consistently was PIN, for a total of 19 questions, 10 of which were statistically significant.

5.1 Statistically Significant Questions

5.1.1 Security

"I believe the authentication method is not easily hacked?"

Table 5: Post Hoc 'Is not Easily Hacked'

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-PIN	12.033	6.087	1.977	.048	.288
Voice-Token	-14.133	6.087	-2.322	.020	.121
Voice-Finger	23.567	6.087	3.871	.000	.001*
PIN-Token	-2.100	6.087	-.345	.730	1.000
PIN-Finger	11.533	6.087	1.895	.058	.349
Token-Finger	9.433	6.087	1.550	.121	.727

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF (authentication factor) scores between the voice (3.00) and finger (4.00) (p = 0.001) but not with PIN (3.00), token (4.00) or any other group combination.

In regard to mean ranking fingerprint ranked the highest, followed by token, PIN and finally voice. Users perhaps considered fingerprint the hardest to hack due to it relying on inheritance-based authentication that only the user possess. Despite this however, voice another inheritance-based authentication ranked last, hence users felt as though voice was easily hacked, this might be because users believe the sensors can be easily spoofed due to issues with background noise or voice changing. Meanwhile both token and PIN ranked in between. This is likely because users are used to both these methods. There was a statistical significance found between the methods voice and fingerprint, hence it can be concluded that users consider fingerprint harder to hack than voice.

“I believe the authentication method is able to differentiate me from others?”

Table 6: Post Hoc ‘Differentiate me from Others’

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-PIN	-4.367	6.101	-0.716	.474	1.000
Voice-Token	5.300	6.101	0.869	.385	1.000
Voice-Finger	18.333	6.101	3.005	.003	0.016*
PIN-Token	0.933	6.101	0.153	.878	1.000
PIN-Finger	22.700	6.101	3.721	.000	0.001*
Token-Finger	23.633	6.101	3.874	.000	0.001*

Pairwise comparisons were performed using Dunn’s (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the finger (5) and voice (3) (p = 0. 016), finger and PIN (4) (p = 0.001) and finger and token (4) (p = 0. 001) but not with any other group combination.

In regard to mean ranking fingerprint again ranked the highest, followed by voice, PIN and finally token. Both the inheritance-based authentication methods ranked the highest, likely because users consider biometrics exclusive to just the user, whereas knowledge/owner-based methods ranked lower, likely because if another user used those methods the system would not be able to tell the difference. There was a statistical significance between fingerprint and voice, fingerprint and PIN and fingerprint and token, meaning that it can be

concluded that fingerprint was considered the best at being able to differentiate users from others.

5.1.2 Privacy

"I believe the authentication method protects my privacy from others?"

Table 7: Post Hoc 'Protects my Privacy from Others'

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-11.800	6.082	-1.940	.052	.314
Voice-PIN	21.633	6.082	3.557	.000	.002*
Voice-Finger	26.567	6.082	4.368	.000	.000*
PIN-Token	9.833	6.082	1.617	.106	.636
Token-Finger	14.767	6.082	2.428	.015	.091
PIN-Finger	4.933	6.082	.811	.417	1.000

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (3) and PIN (5) ($p = 0.002$) and voice and finger (5) ($p < 0.001$) but not with token (4) or any other group combination.

For mean ranking fingerprint ranked the highest, followed by PIN, then token and finally voice. Users found fingerprint to be the most likely to protect their privacy from others perhaps because people believe biometrics are extremely hard to spoof. However, voice ranked the lowest, meaning users do not believe that voice will protect their privacy because they

presumably believe that voice could be more easily spoofed compared to fingerprints. Both PIN and tokens ranked in the middle, less than fingerprint but more than voice, likely because they are used to those authentication methods. There was a statistical significance between voice with PIN and voice with fingerprint. Hence, it can be assumed that users believe PIN and fingerprint to be more likely to protect their user's privacy compared to voice.

"I believe the authentication method prevents others from seeing the contents of my data?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-11.633	6.071	-1.916	.055	.332
Voice-Finger	16.100	6.071	2.652	.008	.048*
Voice-PIN	16.267	6.071	2.679	.007	.044*
PIN-Token	4.633	6.071	.763	.445	1.000
Token-Finger	4.467	6.071	.736	.462	1.000
PIN-Finger	-.167	6.071	-.027	.978	1.000

Table 8: Post Hoc 'Prevents Others from Seeing my Data'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (3) and PIN (4) (p = 0.044) and voice and finger (4) (p = 0.048) but not with token (4) or any other group combination.

For mean ranking PIN ranked the highest, followed by fingerprint, token and finally voice. Voice ranked the lowest again likely because users believe that it can be easily spoofed and

hence does not protect the contents of their data. However, PIN ranked slightly higher than fingerprint. This is likely because users are most used to PIN and hence had more faith it would prevent others from seeing their data. There was a statistical significance between voice with PIN and voice with fingerprint. Hence, it can be assumed that users believe PIN and fingerprint to be more likely to prevent others from seeing their data compared to voice.

"I believe the authentication method allows me to remain anonymous?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-3.300	6.199	-.532	.594	1.000
Voice-Finger	12.067	6.199	1.947	.052	.310
Voice-PIN	15.433	6.199	2.490	.013	.077
Token-Finger	8.767	6.199	1.414	.157	.944
PIN-Token	12.133	6.199	1.957	.050	.302
PIN-Finger	-3.367	6.199	-.543	.587	1.000

Table 9: Post Hoc 'Allows me to Remain Anonymous'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed no statistically significant differences in median AF scores between any pairwise comparisons. The median scores were voice (3), PIN (4), finger (4) and token (3).

When concerned with mean ranking, PIN ranked the highest, followed by fingerprint, token and finally voice. Users ranked PIN the highest likely because users do not have to give any personal info or other accounts to utilise a PIN, whereas other methods like token usually require you to link some other device or account, hence users felt they remained less

anonymous. Both biometrics also ranked lower than PIN likely because users must use their personal inheritance features. The results were found to be statistically significant however there were no specific groups that were statistically significant to one another.

5.1.3 Reliability

"The authentication method performed the same each time?"

Sample 1-Sample 2	**Test Statistic**	**Std. Error**	**Std. Test Statistic**	**p value**	**Adj. p value**
Voice-Finger	0.600	5.316	.113	.910	1.000
Voice-Token	-6.400	5.316	-1.204	.229	1.000
Voice-PIN	15.667	5.316	2.947	.003	.019*
PIN-Finger	-15.067	5.316	-2.834	.005	.028*
Token-Finger	-5.800	5.316	-1.091	.275	1.000
PIN-Token	9.367	5.316	1.743	.081	.488

Table 10: Post Hoc 'Performed the Same Each Time'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (4) and PIN (5) (p = 0.019) and PIN and finger (5) (p = 0.028) but not with token (5) or any other group combination.

PIN ranked the highest followed by token, fingerprint and finally voice. Both authentication methods that use a keyboard to input ranked higher than the inheritance methods. This is likely because users have the most control over the input by inputting it themselves, whereas with inheritance-based methods it relies entirely on the sensor being able to recognise the

users' input. There was a statistical significance between voice and PIN as well as between PIN and fingerprint. Hence, we can conclude that users found PIN to perform more consistently than voice and fingerprint authentication methods.

"The authentication method will continue to perform as expected in further uses?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Finger	-4.400	5.445	-.808	.419	1.000
Token-Finger	-12.500	5.445	-2.296	.022	.130
PIN-Finger	-20.300	5.445	-3.728	.000	.001*
Voice-Token	-8.100	5.445	-1.488	.137	.821
Voice-PIN	15.900	5.445	2.920	.003	.021*
PIN-Token	7.800	5.445	1.433	.152	.912

Table 11: Post Hoc 'Perform as Expected in Further Uses'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (4) and PIN (5) ($p = 0.021$) and PIN and finger (4) ($p = 0.001$) but not with token (5) or any other group combination

For mean ranking, PIN ranked the highest, followed by token, fingerprint and finally voice. Likewise, much like the above concerns about the methods performing the same each time, the two methods that rely on the users to input the authentication themselves, users considered to be more reliable for further uses. Whereas the inheritance-based methods ranked lower, perhaps due to them relying on the sensor having to recognising the user. There was found to be a statistical significance again between PIN and voice as well as PIN and

fingerprint. Therefore, it can be concluded that users expect PIN to perform more consistently than both fingerprint and voice.

5.1.4 Experience

"I have used the authentication method many times before?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Finger	17.300	5.679	3.046	.002	.014*
Voice-Token	-19.367	5.679	-3.410	.001	.004*
Voice-PIN	24.267	5.679	4.273	.000	.000*
Token-Finger	-2.067	5.679	-.364	.716	1.000
PIN-Finger	-6.967	5.679	-1.227	.220	1.000
PIN-Token	4.900	5.679	.863	.388	1.000

Table 12: Post Hoc 'Used the Method Many Times Before'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (2) and finger (5) ($p = 0.014$), voice and token (5) ($p = 0.004$) and voice and PIN (5) ($p < 0.001$) but not with any other group combination.

PIN ranked the highest for mean ranking, followed by token, fingerprint and finally voice. Unsurprisingly traditional means of authentication such as PIN and token ranked the highest since they are the most common means of authentication. Voice ranked the last considering the authentication method is reasonably new. There was found to be a statistical difference between voice and PIN, voice and fingerprint and voice and token. Therefore, it can be

concluded that users have all used PIN''s, fingerprints, and tokens more than voice authentication.

"I use similar authentication methods often?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Finger	10.033	5.890	1.704	.088	.531
Voice-Token	-14.133	5.890	-2.400	.016	.098
Voice-PIN	20.100	5.890	3.413	.001	.004*
Token-Finger	-4.100	5.890	-.696	.486	1.000
PIN-Finger	-10.067	5.890	-1.709	.087	.525
PIN-Token	5.967	5.890	1.013	.311	1.000

Table 13: Post Hoc 'Used Similar Methods Often'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (2) and PIN (5) (p = 0.004) but not with finger (4), token (5) or any other group combination.

Once again PIN ranked the highest for mean ranking, followed by token and fingerprint and voice ranked last. PIN and token ranking high is likely because knowledge-based authentication and ownership-based authentication are more common whereas the biometric methods ranked much lower, likely because they are less common. There was found to be a statistical difference between voice and PIN. Therefore, it can be concluded that users use methods similar to PIN's far more often than they use methods similar to voice authentication.

5.1.5 Verification

"I believe the authentication method offers good feedback that my authentication has processed correctly?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-10.133	5.692	-1.780	.075	.450
Voice-Finger	11.200	5.692	1.968	.049	.295
Voice-PIN	16.000	5.692	2.811	.005	.030*
Token-Finger	1.067	5.692	.187	.851	1.000
PIN-Token	5.867	5.692	1.031	.303	1.000
PIN-Finger	-4.800	5.692	-.843	.399	1.000

Table 14: Post Hoc 'Authentication Processed Correctly'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (4) and PIN (5) (p = 0.030) but not with finger (5), token (5) or any other group combination.

For mean ranking, PIN ranked the highest, followed by fingerprint, token and finally voice. For mean ranking PIN ranked the highest, given users input the numbers themselves and are immediately singed-in providing they gave the correct PIN. Meanwhile, an authentication method such as fingerprint or voice can be inputted, yet it does not always sign the user in as what the sensor saw/heard did not exactly match. There was found to be a statistical difference between voice and PIN. Therefore, it can be concluded that users consider PIN to offer better feedback than voice that their authentication has processed correctly.

“I believe the authentication method offers good feedback when some type of error has occurred?”

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-.933	6.151	-.152	.879	1.000
Voice-Finger	18.567	6.151	3.018	.003	.015*
Voice-PIN	19.700	6.151	3.203	.001	.008*
Token-Finger	17.633	6.151	2.867	.004	.025*
PIN-Token	18.767	6.151	3.051	.002	.014*
PIN-Finger	-1.133	6.151	-.184	.854	1.000

Table 15: Post Hoc ‘Feedback When Error has Occurred’

Pairwise comparisons were performed using Dunn’s (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (3) and finger (4) (p = 0.015), voice and PIN (4) (p = 0.008), PIN and token (3) (p = 0.014) and token and finger (p = 0.025) but not with any other group combination.

In regard to mean ranking PIN ranked the highest, followed by fingerprint, token and finally voice. PIN again ranked the highest likely because when a user inputs the PIN, they are immediately either signed in or told the pin code was incorrect and a user knows a digit was wrong. Whereas a method such as voice will not sign in but there are a lot more factors as to why the voice print did not match, such as the voice itself or background noise. Token likewise ranked low as again there can be multiple reasons why the token was wrong i.e., had it been inputted wrong or had it expired. There was found to be a statistical difference between voice

and PIN, voice and fingerprint, PIN and token and fingerprint and token. Therefore, it can be concluded that users consider PIN and fingerprint to offer much better feedback when a type of error has occurred compared to voice and tokens.

"I believe the authentication method offers good feedback that it has been set up correctly?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
PIN-Token	12.467	5.743	2.171	.030	.180
Voice-Token	12.700	5.743	2.211	.027	.162
Token-Finger	14.433	5.743	2.513	.012	.072
Voice-PIN	-.233	5.743	-.041	.968	1.000
PIN-Finger	1.967	5.743	.342	.732	1.000
Voice-Finger	1.733	5.743	.302	.763	1.000

Table 16: Post Hoc 'Feedback When Set Up Correctly'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed no statistically significant differences in median AF scores between any pairwise comparisons. The median scores were voice (5), PIN (5), finger (5) and token (4).

Fingerprint ranked the highest for mean ranking, followed by voice, PIN and finally token. Fingerprint ranked the highest as in the setup of the method, it usually guides the user through building up their print slowly, likewise voice similarly builds up the print over a few recordings. Token meanwhile offers less feedback during setup and usually requires a test to

see that it has been set up correctly. The results were found to be statistically significant however there were no specific groups that were statistically significant to one another.

5.1.6 Knowledge

"I have a good understanding of how the authentication process works?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Finger	2.167	5.840	.371	.711	1.000
Voice-Token	-12.167	5.840	-2.083	.037	.223
Voice-PIN	14.600	5.840	2.500	.012	.074
Token-Finger	-10.000	5.840	-1.712	.087	.521
PIN-Finger	-12.433	5.840	-2.129	.033	.199
PIN-Token	2.433	5.840	.417	.677	1.000

Table 17: Post Hoc 'Understanding of How Process Works'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed no statistically significant differences in median AF scores between any pairwise comparisons. The median scores were voice (4), PIN (5), finger (5) and token (5).

For meaning ranking, PIN ranked the highest, followed by token, then fingerprint and finally voice. PIN and token ranked the highest likely due to them being more commonly used, hence users are much more likely to have an understanding of how the authentication process works. Whereas the less commonly used methods such as voice and fingerprint ranked lower, likely because users were less used to those methods. The results were found to be

statistically significant however there were no specific groups that were statistically significant to one another.

5.1.7 Recommendation

"I have heard others have good experiences with the authentication method?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-8.567	6.103	-1.404	.160	.963
Voice-Finger	18.467	6.103	3.026	.002	.015*
Voice-PIN	18.700	6.103	3.064	.002	.013*
Token-Finger	9.900	6.103	1.622	.105	.629
PIN-Token	10.133	6.103	1.660	.097	.581
PIN-Finger	-.233	6.103	-.038	.970	1.000

Table 18: Post Hoc 'Heard Good Experience'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (3) and finger (5) (p = 0.015) and voice and PIN (5) (p = 0.013) but not with token (4) or any other group combination.

For mean ranking PIN ranked the highest, followed by fingerprint, token and finally voice. Notably voice ranked the lowest here, having also been the method with the least prior usage by users. Users not hearing others have good experiences with the method could be why many users have not used voice. Meanwhile PIN and fingerprint both ranked much higher, surprisingly fingerprint ranked high despite only ranking third for users having used the

method before. There was found to be a statistical difference between voice and PIN, voice, and fingerprint. Therefore, it can be concluded that users find they have heard others have a better experience with PIN and fingerprint compared to voice.

"The authentication method has a good reputation?"

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	p value	Adj. p value
Voice-Token	-10.400	6.049	-1.719	.086	.513
Voice-PIN	14.300	6.049	2.364	.018	.108
Voice-Finger	16.900	6.049	2.794	.005	.031*
PIN-Token	3.900	6.049	.645	.519	1.000
Token-Finger	6.500	6.049	1.075	.283	1.000
PIN-Finger	2.600	6.049	.430	.667	1.000

Table 19: Post Hoc 'Method has Good Reputation'

Pairwise comparisons were performed using Dunn's (1964) procedure with a Bonferroni correction for multiple comparisons. Adjusted p-values are presented. This post hoc analysis revealed statistically significant differences in median AF scores between the voice (3) and finger (4) (p = 0.031) but not with finger (4), token (4) or any other group combination.

Fingerprint ranked the highest for mean ranking, followed by PIN, token and finally voice. Voice again ranked lower than other methods, indicating that many users would not want to use the authentication method as they feel as though they do not have a good reputation. Comparably the other biometric method fingerprint, ranked the highest in terms of reputation indicating many users believe fingerprint to have an excellent reputation. There was found to be a statistical difference between voice and fingerprint. Therefore, it can be

concluded that users consider fingerprint authentication to have a much better reputation compared to voice.

5.2 Non-Statistically Significant Questions

5.2.1 Availability

“The authentication method is available when needed?”

Both PIN and Token ranked the highest when asked if they were available, with voice coming second and fingerprint ranking last. This is likely due to fingerprints requiring a specific sensor to use, compared to the other methods which usually only require a keyboard or microphone. However, despite this, since there was no statistically significant difference between the groups, it is hard to suggest that any specific method was deemed more available than others.

“The authentication method is widespread?”

PIN again ranked the highest with voice coming second, token coming third and fingerprint coming last. Unsurprisingly the traditional knowledge-based authentication ranked the highest considering they are the most rooted in society, with banks, mobile phones etc all offering these methods. Surprisingly, fingerprint ranked the lowest despite it also being available for most smart phones, though this could be due to not many other venues accepting fingerprints. However, due to there being no statistical significance it is hard to suggest any method was deemed considerably more widespread than others.

“The authentication method is a common example of authentication techniques?”

PIN again ranked the highest most likely due to it being a traditional type of authentication due to it being the most rooted in society. Token ranked second, fingerprint ranked third and voice ranked last. Voice’s low ranking is likely due to it functioning quite different to other

forms of authentication with it constantly verifying the user. However, due to there being no statistical significance it is hard to suggest any method was deemed a common example of authentication more than the others.

5.2.2 Security

“I believe the authentication method is not easily tampered with?”

Fingerprint had the highest mean ranking, followed by token, PIN and finally voice. Fingerprints high ranking might be because users perceive fingerprints to be the hardest sensor to spoof through tampering. Users perhaps consider voice authentication more easily tampered with, due to several considerations about the quality of the audio recording, large amounts of background noise, or vocal variations, therefore they consider it more easily spoofed. However, no method was considered statistically significant over another hence, it is hard to suggest any method is deemed easier to tamper with than the other.

5.2.3 Usability

“I found learning to use the authentication method easy?”

Both PIN and Tokens ranked the highest with voice coming second and fingerprint coming last. PIN and Token ranked the highest, most likely because in both methods users had to enter the codes themselves to utilise them, which users would likely be most familiar with. Comparably, users found voice easy to learn, likely due to the naturalistic usage of speech. Fingerprint ranked last likely due to it using the most unfamiliar sensor. However, since the results were not statistically significant, no particular group was considered easier to learn how to use them, than the other.

“I found the authentication method easy to use?”

For mean ranking, PIN ranked the highest, token was second, voice was third and finally fingerprint was last. Once again both PIN and token ranked slightly higher than the other groups likely due to users being more familiar with key-based input devices. Fingerprint ranked last perhaps due to it having the most different input device whereas voice ranked third due to its naturalistic input method, but not quite as much as key-based input devices. Though again, no method was deemed considerably easier to use than the other as there was no statistical significance between any of the groups.

"I found the authentication method accessible to different needs?"

In terms mean ranking, this was the only question in which voice ranked the highest. Out of all the methods, voice authentication is quite user friendly to most disabilities, with exceptions being those with vocal or hearing issues. Fingerprint ranked second as it too is considered quite user friendly to those with disabilities, with PIN ranking third and token ranking last. This might be due to people considering them less accessible to those with eye issues, at least without specialist equipment. However, since there was no statistically significant difference between the groups it is hard to suggest that voice is significantly more accessible to those with disabilities than the other methods.

5.2.4 Reliability

"The authentication functioned as I expected it to?"

In terms of mean rank PIN came first and all other methods voice, fingerprint and token tied for second. PIN functioning as expected was likely due to users being most used to the method and hence knew what to expect from the method. As for the other methods they were all ranked second, meaning most users expected the authentication methods to perform as they

suspected. However, since there was no statistical significance, this means that the difference between PIN and the other methods was minimal.

5.2.5 Experience

“I use different authentication methods often?”

PIN ranked the highest, followed by voice, then fingerprint and finally token. PIN ranking highest might be because many users not only use PIN (or knowledge-based factors) by themselves and are encouraged to also use two-factor authentication with other methods along with PIN. Similarly, voice also ranked high, most likely due to not a lot of users using voice authentication or users also utilising two-factor authentication alongside voice. Fingerprint ranked third perhaps because people are inclined to just use just fingerprints when unlocking their phones. Lastly token came last due to people using mainly tokens to sign into their devices. However, since there was no statistical significance, it is hard to suggest any method found that they used different authentication methods more so than others.

5.2.6 Knowledge

“I have a good understanding of how the authentication method works?”

For mean ranking, PIN ranked the highest, followed by token, fingerprint and finally voice. Once again, both methods that employ the usage of key-based entry ranked the highest, most likely since users use them more often. Fingerprint ranking third is likely because it has slightly more exposure than voice, which came last likely because it is the least common of the four authentication methods. Though since there is no statistical significance, it is hard to conclusively say if there was any method which users had a better understanding of how they work.

“I have a good understanding of why the authentication method is used?”

PIN ranked the highest in terms of mean ranking, followed by token, then fingerprint and finally voice. The two methods that ranked highest are arguably the most common and simplest in function both using key-based inputs. Whereas the two more uncommon methods ranked lower. However, since there was no statistical significance there was no method where users had a better understanding of why the authentication was used.

5.2.7 Recommendation

“I have heard others have bad experiences with the authentication method?”

For mean ranking the method that ranked highest was fingerprint, followed by voice, then PIN and finally token. The two methods that are based around inheritance-based factors; both ranked higher than the knowledge and ownership factors. This is perhaps because users are more familiar and used to the other methods, hence they were less likely to have complaints about them, compared to the less common methods. However, since there was no statistical significance, it is hard to say any method users had more bad experiences with compared to any other.

5.3 Analysis

5.3.1 Voice

As discussed in the preface and across all questions, voice consistently ranked on the lower end of the 4 authentication methods, indicating that of all the methods, users considered voice to be the one of the methods they were least likely to trust. This was especially true when looking at the statistically significant results for users experience with the method, the reliability of the method and privacy of the method, with voice ranking lowest consistently across most questions in those categories. Meaning users have less exposure to the method

than the others, which means they consider it less reliable and harder to trust that it will keep their data safe.

5.3.2 Fingerprint

Fingerprint's rank fluctuated throughout the categories; sometimes scoring high and other times quite low. Fingerprint ranked the highest of all methods regarding security such as it is differentiating the user and keeping their data secure. Fingerprint also ranked quite high for the verification as they consider it to provide good feedback when setting up or attempting to login. However, fingerprint ranked much lower for aspects such as experience, reliability, and the user's knowledge about the verification. This is likely because the method is much newer, hence users have had less experience with the technology and therefore consider it less reliable and have less understanding about how it works.

5.3.3 PIN

PIN meanwhile consistently ranked the highest of the methods especially across the statistically significant categories, including privacy, reliability, experience, verification, knowledge, and recommendation. This indicates that of all methods, PIN was the method that users considered to be the one they would most likely trust. This is likely because users have the most experience and knowledge with the method, meaning they would be likely to recommend it to other users as they consider it to be the most reliable and likely to keep their data private.

5.3.4 Token

Token often ranked very middling for the statistically significant questions. Often being ranked as the second or third out of the methods leaving it to one of the least polarising methods. For questions around factors such as users experience with the technology, their

knowledge about the technology and how reliable they consider the technology to be – token ranked second likely because it is a more common authentication method and hence, they are more trusting of the method in these regards. However, for categories such as keeping their data private, recommending to others, and the verification feedback it provides, it ranked the second lowest, likely because although they have a good understanding of the method, they consider other methods stronger.

5.4 Chapter Summary

Within this chapter we presented our findings of the post-Hoc test following the Kruskal-Wallis test, we then presented discussion for each of the questions for both statistically significant and non-statistically significant questions before finally giving a summary about how each authentication method performed.

6. Conclusion

In this study, the expanded trust model (Hoffman, Lawson-Jenkins and Blum 2006) is used to find a proxy measure of trust between four different authentication methods: PIN, Tokens, Fingerprints and Voice. The purpose was to discern if users would be willing to utilise voice biometric authentication compared to traditional means of authentication, by comparing the levels of trust they have with each method. A Kruskal-Wallis H test was used to examine the collected data to find any statistical significance, those with a statistical significance were then further tested with a post-Hoc test to determine which groups specifically had a statistical significance.

15 of 27 questions were found to be statistically significant compared to one another, with the main trends suggesting that users were more likely to trust PIN out of the four methods, given it ranked the highest across categories such as privacy, reliability, experience, verification, knowledge, and recommendation. Voice, meanwhile, was the method that ranked the lowest most often, indicating that users would be unlikely to trust and therefore utilise voice biometric authentication over methods they had more trust with. Voice, therefore, would have to score much higher than the other three methods before users considered it a method they would trust over others. This implicates that voice still requires more before it is accepted by users as being a trustworthy piece of technology, considering users are still more likely to trust traditional methods over voice biometrics.

For our first research question of "Which method of user-based authentication mechanism could facilitate trust establishment between user and technology from the user's perspective?" we discovered that each authentication method shows some establishment of trust however, it is at varying degrees based on the model we identified, when we asked

“which trust evaluation model can be employed for flexible measurement of trust (in the context of availability, security, usability, privacy, reliability, willingness to use and security) between the user and security-based authentication mechanism to access technology?”.

For our second research question of “Based on the identified trust evaluation model from research question 1.1, are users willing to trust voice biometric authentication mechanism and hence would be inclined to adopt and utilize it as a means of user authentication method to access technology?” we discovered that compared to other authentication methods users would be inclined to trust traditional means of authentication such as PINs over voice biometric authentication. Hence, the answer to our other research question is that users would have to trust voice more than knowledge-based factors such as PINs and passwords for them to utilise voice biometrics and be their premier choice for safe authentication.

6.1 Open Issues

The study we conduced did have a few limitations, for example, we only compared four methods of authentication, the reason for this was to cover each of the main methods of authentication that are used: Knowledge, Ownership and Biometrics both physical and theoretical, though a more in-depth study could investigate more methods of authentication such as Palmprint or Facial recognition, though these maybe redundant as the purpose of this study was to primarily investigate how voice-biometric authentication compares to traditional means of authentication, with alternative methods such as Location-based authentication not being as commonly used as Knowledge-based, or if ever used as single-factor authentication.

Other limitations within the study could be the number of participants the study had, with 60, although this was deemed sufficient, the study could have a stronger statistical backing with more participants, though due to restrictions with COVID-19, more participants would have been difficult to obtain.

As discussed within the paper, there are some concerns specifically with voice biometric authentication. There are concerns about potential spoofing, even though it is extremely difficult to spoof a voice sensor, it is still a concern (Zhang, Y., Jiang and Duan 2021) . Likewise, there is the concern that once a biometric is compromised, that it will be compromised for a long time as biometrics cannot be changed like knowledge or ownership factors. Voice biometrics can also suffer from poor audio quality or background noise which can affect the sensor sensitivity.

Regarding the relationship with trust, there are a few issues that users can have with the technology, notably because VBA is a relatively new technology. This means not many users will have much, if any, experience utilising the technology and even less likely for users to be knowledgeable of the inner workings of the technology. This also means it is unlikely for much propagation of VBA to have occurred. Despite this however, VBA is quite secure, especially compared to traditional means of authentication and the fact it is quickly growing because its usage via already built infrastructure means it will soon be quite available, hence the potential for trust to develop is there (Vittori 2019). Although, compared to traditional means of authentication, which has had a lot more time for users to have experiences with and develop trust with, VBA requires some time before users are to accept and trust it.

6.2 Future Research

Possible future research directions from this study, for example could be a study that observes the change in trust over a longer period, observing how users trust changes with voice biometric authentication after using the technology for a longer period. It would be especially interesting to observe how long it takes for a method such as voice to be considered more trustworthy than methods such as PIN from the perspective of the user and how we can better change user's opinion of the authentication method to help build user's trust with the authentication method.

Likewise, within the study, participants only used one method each, a between-groups testing method. This was to prevent users being influenced by their answers to previous methods, however, different results might be received by using a repeated measures method and would be an interesting comparison from a different study.

Alternatively, given how single-factor authentication is mostly seen as outdated, it is important to study voice biometric authentication as a means of multi-factor authentication as well. Hence another possible study could be one that observes which authentication factor voice pairs best with, both from a logistical standpoint and from the users' standpoint; given users may feel more confident using voice biometric authentication if it were alongside another method of authentication.

Bibliography

Abdullah, M.A., Chambers, J.A., Woo, W.L. and Dlay, S.S. (2015) Iris biometrie: Is the near-infrared spectrum always the best? In: *2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR).*

Agarwal, R. and Prasad, J. (1997) The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies. *Decision Sciences,* 28 (3), pp.557-582.

Aldawood, H. and Skinner, G. An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications,* 975, pp.8887.

Alonso-Fernandez, F. and Bigun, J. (2014) Fake iris detection: A comparison between near-infrared and visible images. In: *2014 Tenth International Conference on Signal-Image Technology and Internet-Based Systems.*

Artzi, L. (2018) *Can you fool voice biometrics?*[Internet]. Available from https://www.nice.com/engage/blog/can-you-fool-voice-biometrics-2359/ [Accessed 7/01/2020].

Arulkumar, V. and Vivekanandan, P. (2018) An intelligent technique for uniquely recognising face and finger image using learning vector quantisation (LVQ)-based template key generation. *International Journal of Biomedical Engineering and Technology,* 26 (3-4), pp.237-249.

Asan, O., Perchonok, J. and Montague, E. (2012) Contextual differences in the dynamic measurement of trust in web sites across domains. *International Journal of Cyber Society and Education,* 5 (2), pp.91-110.

Ashfield, J., Shroyer, D. and Brown, D. (2012) *Location based authentication of mobile device transactions,* United States. Patent no. US8295898B2.

Barber, B. (1983) *The logic and limits of trust*Rutgers University Press New Brunswick, NJ.

Beranek, B. (2013) Voice biometrics: Success stories, success factors and what's next. *Biometric Technology Today,* 2013 (7), pp.9-11.

Bhattacharyya, D., Ranjan, R., Alisherov, F. and Choi, M. (2009) Biometric authentication: A review. *International Journal of U-and E-Service, Science and Technology,* 2 (3), pp.13-28.

Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G.L. and Roli, F. (2012) Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics,* 1 (1), pp.11-24.

Blocki, J., Harsha, B. and Zhou, S. (2018) On the economics of offline password cracking. In: *2018 IEEE Symposium on Security and Privacy (SP).*

Bowman, B. (2019) *Biometric hacking* [Internet]. Available from https://securityboulevard.com/2019/04/biometric-hacking/ [Accessed 6/01/2020].

Braintree (2007) *Top 5 vulnerabilities leading to credit card data breaches* [Internet]. Available from https://www.braintreepayments.com/blog/top-5-vulnerabilities-leading-to-credit-card-data-breaches/ [Accessed 01/09/2020].

Brewster Thomas (2017) *All that's needed to hack gmail and rob bitcoin: A name and A phone number* [Internet]. Available from https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/#338f7a5f41a4 [Accessed 12/12/2019].

Burch, L.L. and Carter, S.R. (2010) *Methods and systems for multifactor authentication,* United States. Patent no. US7739744B2.

Chen, W., Hancke, G.P., Mayes, K.E., Lien, Y. and Chiu, J.H. (2010) Using 3G network components to enable NFC mobile transactions and authentication. In: *2010 IEEE International Conference on Progress in Informatics and Computing.*

Chen, Y. (2007) A bayesian network model of knowledge-based authentication. *AMCIS 2007 Proceedings,* pp.423.

Chen, Y. and Liginlal, D. (2007) Bayesian networks for knowledge-based authentication. *IEEE Transactions on Knowledge and Data Engineering,* 19 (5), pp.695-710.

Chiew, K.L., Yong, K.S.C. and Tan, C.L. (2018) A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications,* 106, pp.1-20.

Choi, K., Lee, J. and Chun, Y. (2017) Voice phishing fraud and its modus operandi. *Security Journal,* 30 (2), pp.454-466.

Chokhani, S. (2004) Knowledge based authentication (KBA) metrics. In: *KBA Symposium-Knowledge Based Authentication: Is It Quantifiable.*

Chrobok Mateusz (2020) *Physical biometrics vs behavioral biometrics* [Internet]. Available from https://www.buguroo.com/en/blog/physical-biometrics-vs-behavioral-biometrics [Accessed 29th June 2020].

Cook, K.S., Yamagishi, T., Cheshire, C., Cooper, R., Matsuda, M. and Mashima, R. (2005) Trust building via risk taking: A cross-societal experiment. *Social Psychology Quarterly,* 68 (2), pp.121-142.

Council, Federal Financial Institutions Examination (2005) Authentication in an internet banking environment. *FFIEC Gencies (August 2001 Guidance),* pp.1-14.

Crosman, P. (2018) *Is amazon's alexa ready for person-to-person payments?*[Internet]. Available from https://www.americanbanker.com/news/is-amazons-alexa-ready-for-p2p-payments [Accessed 3/01/2020].

Cruz, J., Mishra, P. and Bhunia, S. (2019) The metric matters: The art of measuring trust in Electronics. In: *2019 56th ACM/IEEE Design Automation Conference (DAC).*

CRYPTO-IT (2020) *Frequency analysis* [Internet]. Available from http://www.crypto-it.net/eng/attacks/frequency-analysis.html#:~:text=Frequency%20analysis%20is%20one%20of,are%20used%20with%20different%20frequencies.&text=Based%20on%20that%2C%20one%20can,texts%20written%20in%20other%20languages. [Accessed 29th June 2020].

Daugman, J. (2009) How iris recognition works. In: Anonymous *The essential guide to image processing*. [Internet]Elsevier, pp. 715-739.

Dietz, G. (2011) Going back to the source: Why do people trust each other? *Journal of Trust Research,* 1 (2), pp.215-222.

Drokov, I., Punskaya, E. and Tahar, E. (2015) *System and method for dynamic multifactor authentication*
, United States. Patent no. US8943548B2.

Dürmuth, M., Angelstorf, F., Castelluccia, C., Perito, D. and Chaabane, A. (2015) OMEN: Faster password guessing using an ordered markov enumerator. In: *International Symposium on Engineering Secure Software and Systems.*

Dutt Parth (2021) *Understanding rainbow table attack* [Internet]. Available from https://www.geeksforgeeks.org/understanding-rainbow-table-attack/ [Accessed 14th July 2021].

Eden, T. and Avigad, B. (2012) *Location based authentication system,* United States. Patent no. US8285639B2.

Edwards, M., Larson, R., Green, B., Rashid, A. and Baron, A. (2017) Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security,* 69, pp.18-34.

European Union Agency for Cybersecurity (no date) *Authentication methods* [Internet]. Available from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods#:~:text=Password%20Recommendations,most%20common%20form%20of%20authentication. [Accessed 18/06/2020].

Fan, W., Lwakatare, K. and Rong, R. (2017) Social engineering: IE based model of human weakness for attack and defense investigations. *International Journal of Computer Network & Information Security,* 9 (1).

Farmanbar, M. and Toygar, Ö (2017) Spoof detection on face and palmprint biometrics. *Signal, Image and Video Processing,* 11 (7), pp.1253-1260.

Finextra (2017) *Precise biometrics debuts spoof tech to identify fake and dead fingers* [Internet]. Available from https://www.finextra.com/pressarticle/69825/precise-biometrics-debuts-spoof-tech-to-identify-fake-and-dead-fingers [Accessed 13/05/2020].

Fleming, N. (2019) *Does amazon have answers for the future of the NHS?*[Internet]. Available from https://www.theguardian.com/technology/2019/aug/24/alexa-nhs-future-amazon-artificial-intelligence-healthcare [Accessed 4/1/2020].

Freedy, A., DeVisser, E., Weltman, G. and Coeyman, N. (2007) Measurement of trust in human-robot collaboration. In: *2007 International Symposium on Collaborative Technologies and Systems.*

Fu, K. (2015) *Knowledge-based authentication (kba)* [Internet]. Available from https://www.hsgac.senate.gov/imo/media/doc/Testimony-Fu-2015-06-02-REVISED%2021.pdf [Accessed 01/09/2020].

Gefen, D. (2004) What makes an ERP implementation relationship worthwhile: Linking trust mechanisms and ERP usefulness. *Journal of Management Information Systems,* 21 (1), pp.263-288.

General Post Blog (2019) *3 different types of fingerprint scanner and how they work* [Internet]. Available from https://genolomu.wordpress.com/2019/03/08/3-different-types-of-fingerprint-scanner-and-how-they-work/ [Accessed 29th June 2020].

Goswami, G., Vatsa, M. and Singh, R. (2014) RGB-D face recognition with texture and attribute features. *IEEE Transactions on Information Forensics and Security,* 9 (10), pp.1629-1640.

Grabner-Kräuter, S. and Kaluscha, E.A. (2003) Empirical research in on-line trust: A review and critical assessment. *International Journal of Human-Computer Studies,* 58 (6), pp.783-812.

Granger, S. (2001) Social engineering fundamentals, part I: Hacker tactics. *Security Focus, December,* 18.

Gunson, N., Marshall, D., Morton, H. and Jack, M. (2011) User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security,* 30 (4), pp.208-220.

Hammad, A. and Faith, P. (2017) *Location based authentication,* United States. Patent no. US9721250B2.

Hitaj, B., Gasti, P., Ateniese, G. and Perez-Cruz, F. (2019) Passgan: A deep learning approach for password guessing. In: *International Conference on Applied Cryptography and Network Security.*

Ho, G., Sharma, A., Javed, M., Paxson, V. and Wagner, D. (2017) Detecting credential spearphishing in enterprise settings. In: *26th {USENIX} Security Symposium ({USENIX} Security 17).*

Hoffman, L.J., Lawson-Jenkins, K. and Blum, J. (2006) Trust beyond security: An expanded trust model. *Communications of the ACM,* 49 (7), pp.95-101.

ISO/IEC (2007) Identification cards — integrated circuit cards — part 2: Cards with contacts — dimensions and location of the contacts. (2).

Jablon, D.P. (1997) Extended password key exchange protocols immune to dictionary attack. In: *Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises.*

Jain, A.K., Ross, A. and Uludag, U. (2005) Biometric template security: Challenges and solutions. In: *2005 13th European signal processing conference.*

Jain, A.K., Hong, L., Pankanti, S. and Bolle, R. (1997) An identity-authentication system using fingerprints. *Proceedings of the IEEE,* 85 (9), pp.1365-1388.

Jain, A. and Aggarwal, S. (2012) Multimodal biometric system: A survey. *International Journal of Applied Science and Advance Technology,* 1 (1), pp.58-63.

Jakubowski, M.H., Venkatesan, R. and Yacobi, Y. (2010) Quantifying trust. *IACR Cryptology ePrint Archive,* 2010, pp.246.

Janicki, A. and Biały, S. (2006) Improving GMM based speaker recognition using trained voice activity detection. In: *5th Conference on signals and electronic systems, Lodz, Poland.*

Jøsang, A. (2018) *Lecture 9: User authentication* [Internet]. Available from https://www.uio.no/studier/emner/matnat/ifi/IN2120/h18/lectures/in2120-2018-l09-user-authentication.pdf [Accessed 29th June 2020].

Joseph, T., Bruchim, G.Z., Gofman, I. and Ashkenazy, I.G. (2020) *Credential spray attack detection,* United States. Patent no. US20200267178A1.

Karimovich, G.S. and Turakulovich, K.Z. (2016) Biometric cryptosystems: Open issues and challenges. In: *2016 International Conference on Information Science and Communications Technologies (ICISCT).*

Kaur, K. and Rampersad, G. (2018) Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. *Journal of Engineering and Technology Management,* 48, pp.87-96.

Khan, H.Z.U. and Zahid, H. (2010) Comparative study of authentication techniques. *International Journal of Video & Image Processing and Network Security IJVIPNS,* 10 (04), pp.9.

Kong, A., Zhang, D. and Kamel, M. (2009) A survey of palmprint recognition. *Pattern Recognition,* 42 (7), pp.1408-1418.

Korshunov, P. and Marcel, S. (2017) Impact of score fusion on voice biometrics and presentation attack detection in cross-database evaluations. *IEEE Journal of Selected Topics in Signal Processing,* 11 (4), pp.695-705.

Koyun, A. and Al Janabi, E. (2017) Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST),* 4 (6), pp.7533-7538.

Krawczyk, S. and Jain, A.K. (2005) Securing electronic medical records using biometric authentication. In: *International Conference on Audio-and Video-Based Biometric Person Authentication.*

Krom, G.d. (1994) Consistency and reliability of voice quality ratings for different types of speech fragments. *Journal of Speech, Language, and Hearing Research,* 37 (5), pp.985-1000.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015) Advanced social engineering attacks. *Journal of Information Security and Applications,* 22, pp.113-122.

Kumar, A. and Zhang, D. (2005) Personal authentication using multiple palmprint representation. *Pattern Recognition,* 38 (10), pp.1695-1704.

Kunyu, P., Jiande, Z. and Jing, Y. (2009) An identity authentication system based on mobile phone token. In: *2009 IEEE International Conference on Network Infrastructure and Digital Content.*

Kuo, C. and Lo, M. (1999) *Secure open smart card architecture,* United States. Patent no. US6003134A.

Lavrentyeva, G., Novoselov, S., Malykh, E., Kozlov, A., Kudashev, O. and Shchemelinin, V. (2017) Audio replay attack detection with deep learning frameworks. In: *Interspeech.*

Lehtonen, M., Michahelles, F. and Fleisch, E. (2007) Probabilistic approach for location-based authentication. In: *1st International workshop on security for spontaneous interaction IWSSI.*

Lim, C.H. and Kwon, T. (2006) Strong and robust RFID authentication enabling perfect ownership transfer. In: *International Conference on Information and Communications Security.*

Loukas, G. and Öke, G. (2010) Protection against denial of service attacks: A survey. *The Computer Journal,* 53 (7), pp.1020-1037.

Marcel, S., Nixon, M.S., Fierrez, J. and Evans, N. (2019) *Handbook of biometric anti-spoofing: Presentation attack detection*Springer.

Marechal, S. (2008) Advances in password cracking. *Journal in Computer Virology,* 4 (1), pp.73-81.

Marforio, C., Masti, R.J., Soriente, C., Kostiainen, K. and Capkun, S. (2016) Hardened setup of personalized security indicators to counter phishing attacks in mobile banking. In: *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices.*

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995) An integrative model of organizational trust. *Academy of Management Review,* 20 (3), pp.709-734.

Mazumdar, J.B. and Nirmala, S.R. (2018) Retina based biometric authentication system: A review. *International Journal of Advanced Research in Computer Science,* 9 (1).

McKight, P.E. and Najab, J. (2010) Kruskal-wallis test. *The Corsini Encyclopedia of Psychology,* pp.1.

Mcknight, D.H., Carter, M., Thatcher, J.B. and Clay, P.F. (2011) Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS),* 2 (2), pp.12.

McKnight, D.H. (2005) Trust in information technology. *The Blackwell Encyclopedia of Management,* 7, pp.329-331.

Microsoft (2006) *Speaker verification: Text-dependent vs. text-independent* [Internet]. Available from https://www.microsoft.com/en-us/research/project/speaker-verification-text-dependent-vs-text-independent/ [Accessed 19/05/2020].

Mihailescu, P. (2007) The fuzzy vault for fingerprints is vulnerable to brute force attack. *arXiv Preprint arXiv:0708.2974,*.

Mishra, S. and Soni, D. (2019) SMS phishing and mitigation approaches. In: *2019 Twelfth International Conference on Contemporary Computing (IC3).*

MLB9252 (2011) *How to calculate password entropy* [Internet]. Available from https://ritcyberselfdefense.wordpress.com/2011/09/24/how-to-calculate-password-entropy/ [Accessed 29th June 2020].

Moramarco Stephen (2019) *Phishing attacks in the banking industry* [Internet]. Available from https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-in-the-banking-industry/ [Accessed 16/12/2019].

Murthy, A.S., Ganesan, K., Mangam, P.M., Jandhyala, S.S. and Walter, M. (2021) *Multifactor authentication as a network service,* United States. Patent no. US10904237B2.

Narayanan, A. and Shmatikov, V. (2005) Fast dictionary attacks on passwords using time-space tradeoff. In: *Proceedings of the 12th ACM conference on Computer and communications security.*

National Cyber Security Centre (2019a) *Most hacked passwords revealed as UK cyber survey exposes gaps in online security* [Internet]. Available from https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security [Accessed 10/12/2019].

National Cyber Security Centre (2019b) *Biometric recognition and authentication systems* [Internet]. Available from https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked [Accessed 29th June 2020].

Newton, K., Stolle, D. and Zmerli, S. (2018) Social and political trust. *The Oxford Handbook of Social and Political Trust,* pp.37.

Ortega-Garcia, J., Bigun, J., Reynolds, D. and Gonzalez-Rodriguez, J. (2004) Authentication gets personal with biometrics. *IEEE Signal Processing Magazine,* 21 (2), pp.50-62.

Pandya, J. (2019) *Hacking our identity: The emerging threats from biometric technology* [Internet]. Available from https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/#761fbaa75682 [Accessed 5/1/2019].

Patent, V. and Searle, R.H. (2019) Qualitative meta-analysis of propensity to trust measurement. *Journal of Trust Research,* 9 (2), pp.136-163.

Pindrop (no date) *Voice security predictions in the age of iot: The internet of things and the future of voice security* [Internet]. Available from https://www.pindrop.com/blog/voice-security-in-the-age-of-iot/ [Accessed January 2 2020].

Poh, N., Bengio, S. and Korczak, J. (2002) A multi-sample multi-source model for biometric authentication. In: *Proceedings of the 12th IEEE Workshop on Neural Networks for Signal Processing.*

PYMENTS (2018) *Making voice biometrics harder to hack* [Internet]. Available from https://www.pymnts.com/news/security-and-risk/2018/hackers-biometrics-cybercrime-fraudsters-authentication/ [Accessed 8/01/2020].

Rathgeb, C. and Busch, C. (2014) Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. *Computers & Security,* 42, pp.1-12.

Raza, M., Iqbal, M., Sharif, M. and Haider, W. (2012) A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal,* 19 (4), pp.439-444.

Rempel, J.K., Holmes, J.G. and Zanna, M.P. (1985) Trust in close relationships. *Journal of Personality and Social Psychology,* 49 (1), pp.95.

Reusable Security Tools (no date) *Password cracking tools* [Internet]. Available from https://sites.google.com/site/reusablesec/Home/password-cracking-tools [Accessed 29th June 2020].

Rigas, I., Abdulin, E. and Komogortsev, O. (2016) Towards a multi-source fusion approach for eye movement-driven recognition. *Information Fusion,* 32, pp.13-25.

Roberts, C. (2007) Biometric attack vectors and defences. *Computers & Security,* 26 (1), pp.14-25.

Ross, A., Jain, A. and Reisman, J. (2003) A hybrid fingerprint matcher. *Pattern Recognition,* 36 (7), pp.1661-1673.

Rouse, M. (2018) *Challenge-response authentication* [Internet]. Available from https://searchsecurity.techtarget.com/definition/challenge-response-system [Accessed 01/09/2020].

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. (1998) Not so different after all: A cross-discipline view of trust. *Academy of Management Review,* 23 (3), pp.393-404.

Sarala, S.M., Karki, M.V. and Yadav, D.S. (2016) Blended substitution attack independent; fuzzy vault for fingerprint template security. In: *2016 International Conference on Circuits, Controls, Communications and Computing (I4C).*

Scheirer, W.J. and Boult, T.E. (2007) Cracking fuzzy vaults and biometric encryption. In: *2007 Biometrics Symposium.*

Schneier, B. (2005) *The failure of two-factor authentication* [Internet]. Available from https://www.schneier.com/blog/archives/2005/03/the_failure_of.html [Accessed 29th June 2020].

Shablygin, E., Zakharov, V., Bolotov, O. and Scace, E. (2013) *Token management,* United States. Patent no. US8555079B2.

Shah, H.N.M., Ab Rashid, M.Z., Abdollah, M.F., Kamarudin, M.N., Lin, C.K. and Kamis, Z. (2014) Biometric voice recognition in security system. *Indian Journal of Science and Technology,* 7 (2), pp.104.

Sharma, S. (2005) Location based authentication.

Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F. (2014) Can long passwords be secure and usable? In: *Proceedings of the SIGCHI conference on human factors in computing systems.*

Sherchan, W., Nepal, S. and Paris, C. (2013) A survey of trust in social networks. *ACM Computing Surveys (CSUR),* 45 (4), pp.47.

Shrawankar, U. and Thakare, V.M. (2013) Techniques for feature extraction in speech recognition system: A comparative study. *arXiv Preprint arXiv:1305.1145,*.

Simmons, M. and Lee, J.S. (2020) Catfishing: A look into online dating and impersonation. In: *International Conference on Human-Computer Interaction.*

Singh, M., Singh, R. and Ross, A. (2019) A comprehensive overview of biometric fusion. *Information Fusion,* 52, pp.187-205.

Six, F.E. (2007) Building interpersonal trust within organizations: A relational signalling perspective. *Journal of Management & Governance,* 11 (3), pp.285-309.

Smith, N. (2018) *HOTP vs TOTP: What's the difference?*[Internet]. Available from https://www.microcosm.com/blog/hotp-totp-what-is-the-difference [Accessed 01/09/2020].

Soboroff, S.D. (2012) Group size and the trust, cohesion, and commitment of group members.

Spitzner Lance (2019) *Time for password expiration to die* [Internet]. Available from https://www.sans.org/security-awareness-training/blog/time-password-expiration-die [Accessed 12/12/2019].

Stasiukonis, S. (2006) Social engineering, the USB way. *Dark Reading,* 7.

Statista (2019) *Number of smartphone users worldwide from 2016 to 2021* [Internet]. Available from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [Accessed 7/01/2020].

Stoianov, A., Kevenaar, T. and Van der Veen, M. (2009) Security issues of biometric encryption. In: *2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH).*

Thakkar, D. (no date) *Unimodal biometrics vs. multimodal biometrics* [Internet]. Available from https://www.bayometric.com/unimodal-vs-multimodal/ [Accessed 01/11/2020].

Thavalengal, S., Bigioi, P. and Corcoran, P. (2015) Iris authentication in handheld devices-considerations for constraint-free acquisition. *IEEE Transactions on Consumer Electronics,* 61 (2), pp.245-253.

Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S.J. and Sanyal, S. (2011) A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. *arXiv Preprint arXiv:1111.3010,*.

Trojahn, M. and Marcus, P. (2012) Towards coupling user and device locations using biometrical authentication on smartphones. In: *2012 International Conference for Internet Technology and Secured Transactions.*

Tupman, A. (2018) *5 reasons why voice biometrics is A game changer* [Internet]. Available from https://www.conn3ct.com/blog/five-reasons-why-voice-biometrics-is-a-game-changer [Accessed 25/05/2020].

Turnbull, R.S. and Gedge, R. (2012) *Location based authentication,* United States. Patent no. US8321913B2.

Turner, D.M. (2016) *Digital authentication - the basics* [Internet]. Available from https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics [Accessed 16/05/2020].

Uludag, U. and Jain, A.K. (2004) Attacks on biometric systems: A case study in fingerprints. In: *Security, steganography, and watermarking of multimedia contents VI.*

Uniphone (2018) *How does voice biometrics work?*[Internet]. Available from https://www.uniphore.com/how-does-voice-biometrics-work/ [Accessed 19/05/2020].

Uslaner, E.M. (2008) Trust as a moral value. *The Handbook of Social Capital,* pp.101-121.

Uslaner, E.M. (2002) *The moral foundations of trust*Cambridge University Press.

Usman, A.B. and Gutierrez, J. (2019) DATM: A dynamic attribute trust model for efficient collaborative routing. *Annals of Operations Research,* 277 (2), pp.293-310.

Usman, A.B., Gutierrez, J.A. and Bichi, A.B. (2019) Secure routing protocols using trust-based mechanisms in the internet of things for smart city environment challenges and future trends. In: Anonymous *Secure cyber-physical systems for smart cities*. [Internet]IGI Global, pp. 103-129.

Usman, A.B. and Gutierrez, J. (2018) Toward trust based protocols in a pervasive and mobile computing environment: A survey. *Ad Hoc Networks,* 81, pp.143-159.

Van de Bunt, Gerhard G, Wittek, R.P. and de Klepper, M.C. (2005) The evolution of intra-organizational trust networks: The case of a german paper factory: An empirical test of six trust mechanisms. *International Sociology,* 20 (3), pp.339-369.

Velásquez, I., Caro, A. and Rodríguez, A. (2018) Authentication schemes and methods: A systematic literature review. *Information and Software Technology,* 94, pp.30-37.

Vittori, P. (2019) Ultimate password: Is voice the best biometric to beat hackers? *Biometric Technology Today,* 2019 (9), pp.8-10.

Wayman, J., Jain, A., Maltoni, D. and Maio, D. (2005) An introduction to biometric authentication systems. In: Anonymous *Biometric systems*. [Internet]Springer, pp. 1-20.

Weaver, A.C. (2006) Biometric authentication. *Computer,* 39 (2), pp.96-97.

Weir, C.M. (2010) Using probabilistic techniques to aid in password cracking attacks.

Weir, M., Aggarwal, S., De Medeiros, B. and Glodek, B. (2009) Password cracking using probabilistic context-free grammars. In: *2009 30th IEEE Symposium on Security and Privacy.*

Zhang, D., Song, F., Xu, Y. and Liang, Z. (2009) *Advanced pattern recognition technologies with applications to biometrics*IGI Global.

Zhang, F., Kondoro, A. and Muftic, S. (2012) Location-based authentication and authorization using smart phones. In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.*

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T. and Xu, W. (2017) Dolphinattack: Inaudible voice commands. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.*

Zhang, L., Tan, C. and Yu, F. (2017) An improved rainbow table attack for long passwords. *Procedia Computer Science,* 107, pp.47-52.

Zhang, Y., Jiang, F. and Duan, Z. (2021) One-class learning towards synthetic voice spoofing detection. *IEEE Signal Processing Letters,* 28, pp.937-941.

Appendix

Consent Form

Consent Form

Voice Biometrics Authentication: A User Perspective

Name of Researcher - Alec Wells

Name of School – Engineering York St John university

Please read and complete this form carefully. If you are willing to participate in this study, ring the appropriate responses and sign and date the declaration at the end. If you do not understand anything and would like more information, please ask.

- I have had the research satisfactorily explained to me in a verbal and / or written form by the researcher.

  YES/NO

- I understand that the research will involve: setting up a means of authentication and using said authentication. Afterwards there will be a brief questionnaire to fill out that will take around 5-10 minutes.

  YES/NO

- I understand that I may withdraw from this study during the experiment without having to give an explanation.

  YES/NO

- I understand that once I have submitted my answers to the questionnaire, due to the anonymity of the questionnaire, I might be unable to withdraw my responses after that point. Contact via alec.wells@yorksj.ac.uk

  YES/NO

- I understand that all information about me will be treated in strict confidence and that I will not be named in any written work arising from this study.

  YES/NO

- I understand that my responses to the survey and any audiotape of me will be used solely for research purposes and will be destroyed on completion of your research.

  YES/NO

- I understand that you will be discussing the progress of your research with Aminu Usman & Justin McKeown at York St John University.

  YES/NO

- I consent to being a participant in the project.

  YES/NO

Signature: .....

Date: .....

Figure 19: Consent Form

Questionnaire

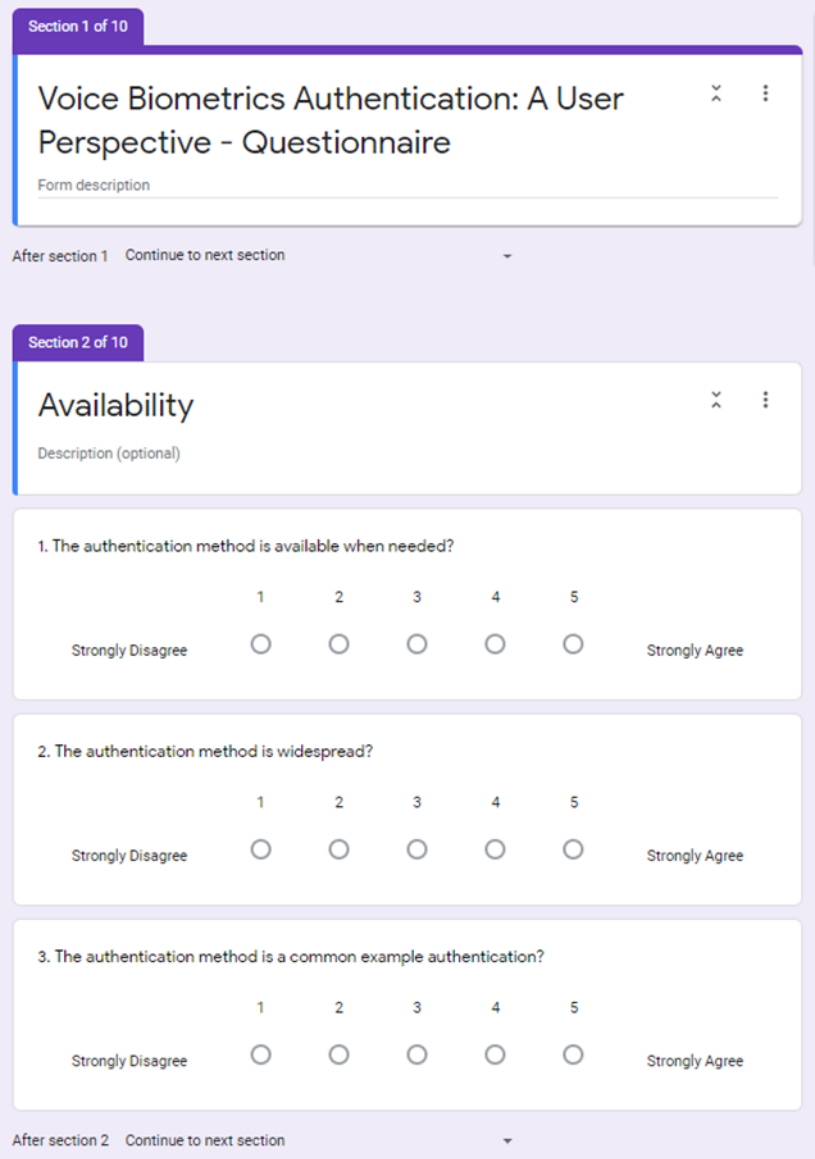

Figure 20: Questionnaire Availability

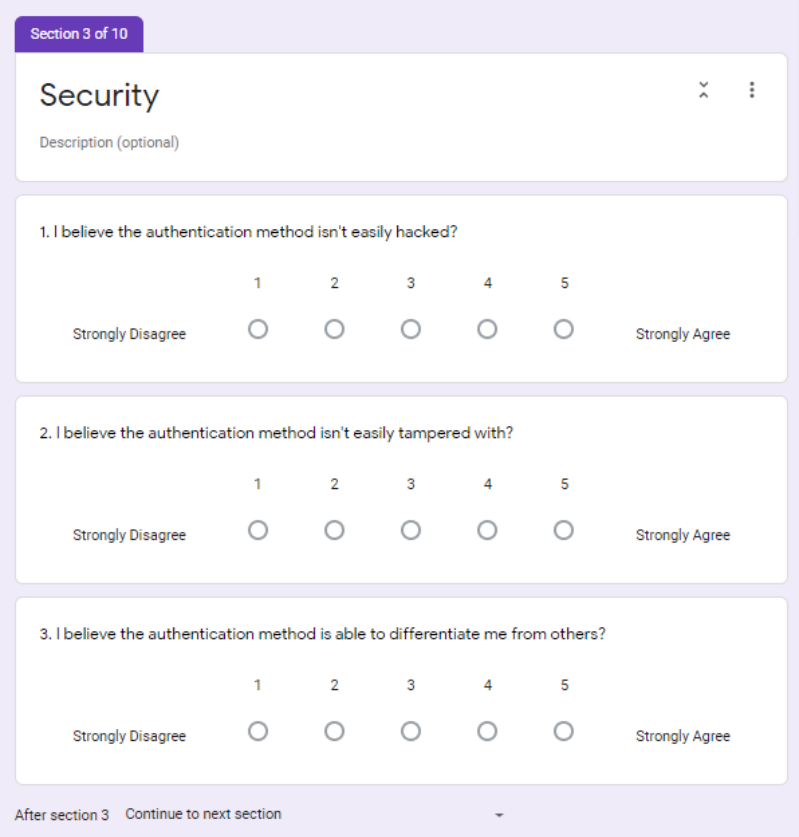

Figure 21: Questionnaire Security

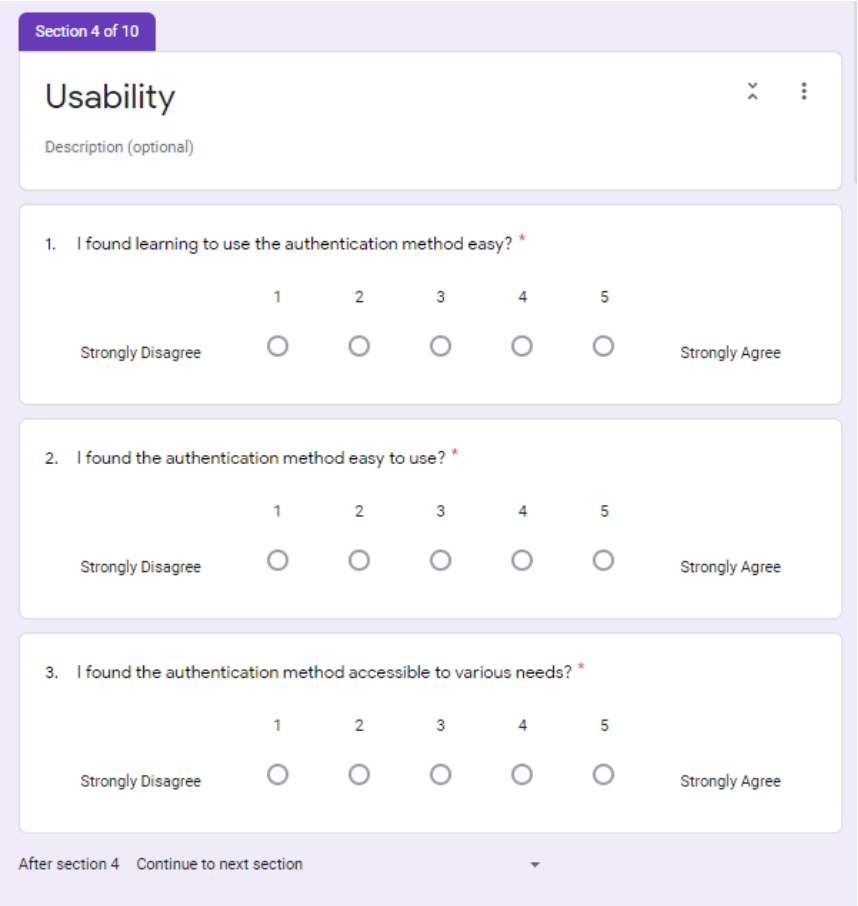

Figure 22: Questionnaire Usability

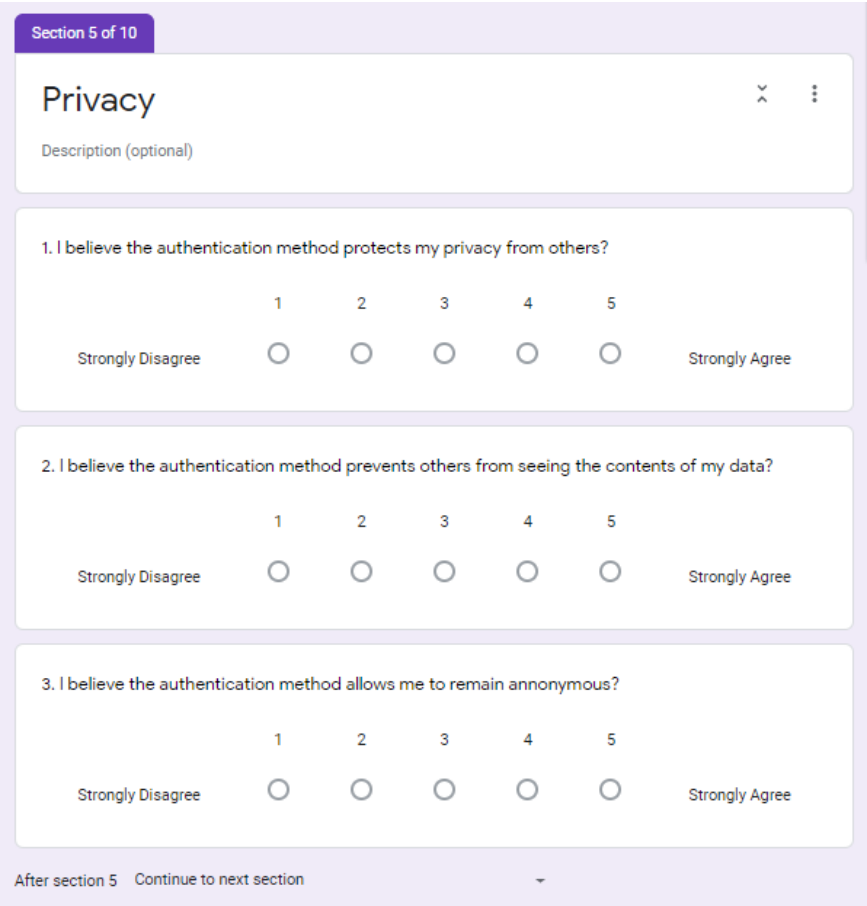

Figure 23: Questionnaire Privacy

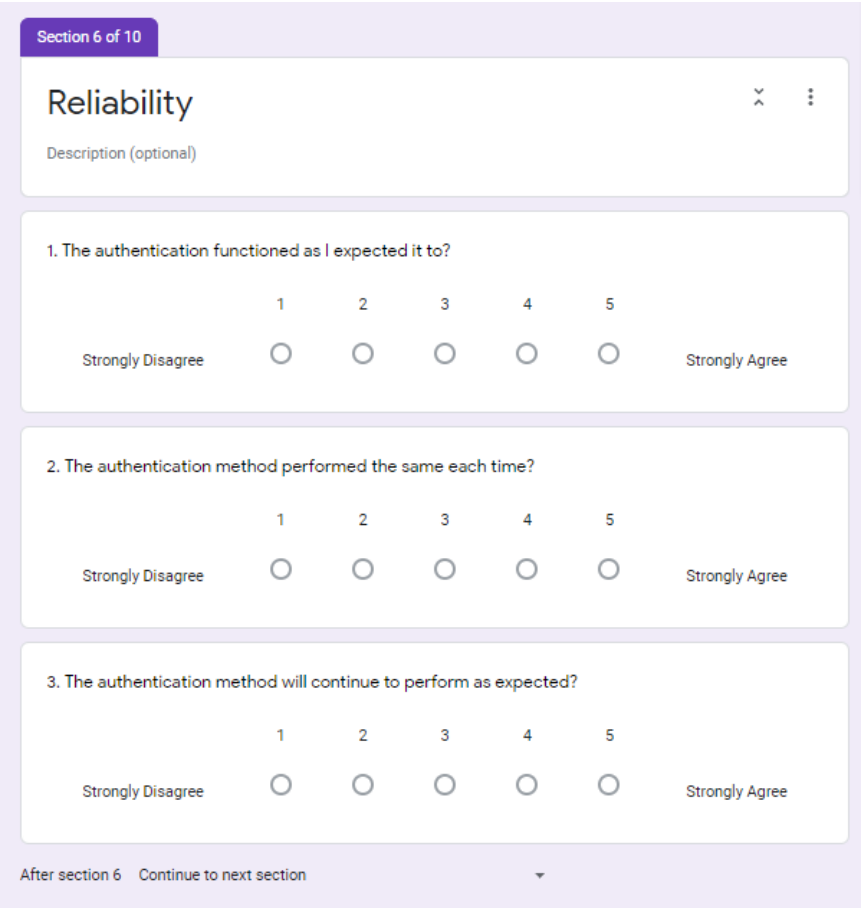

Figure 24: Questionnaire Reliability

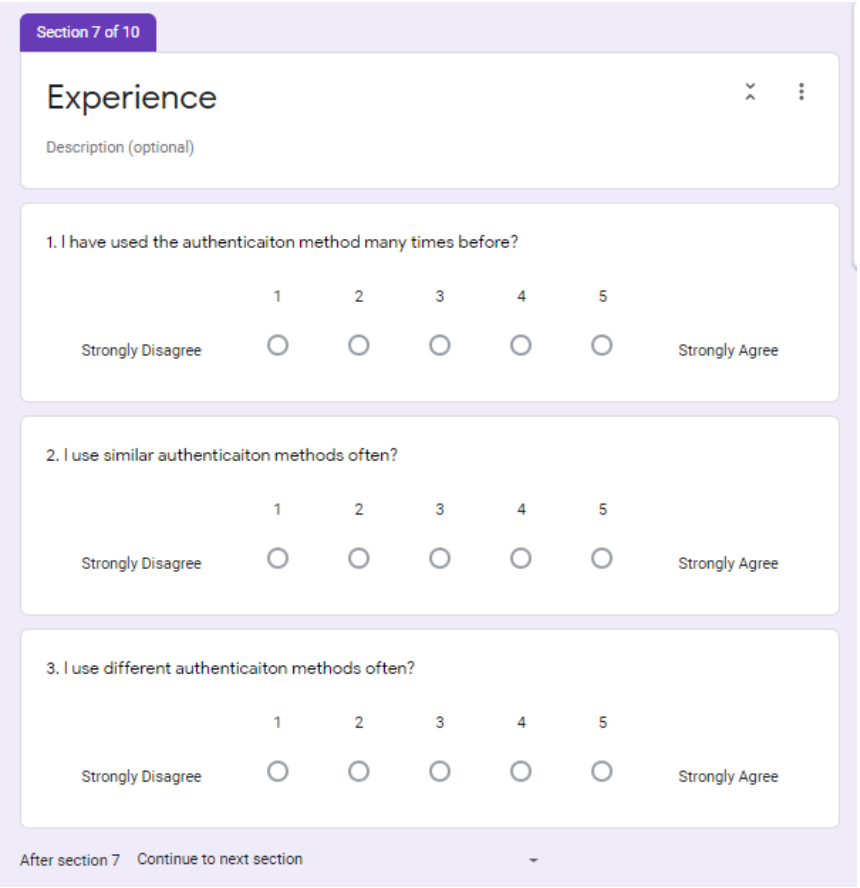

Figure 25: Questionnaire Experience

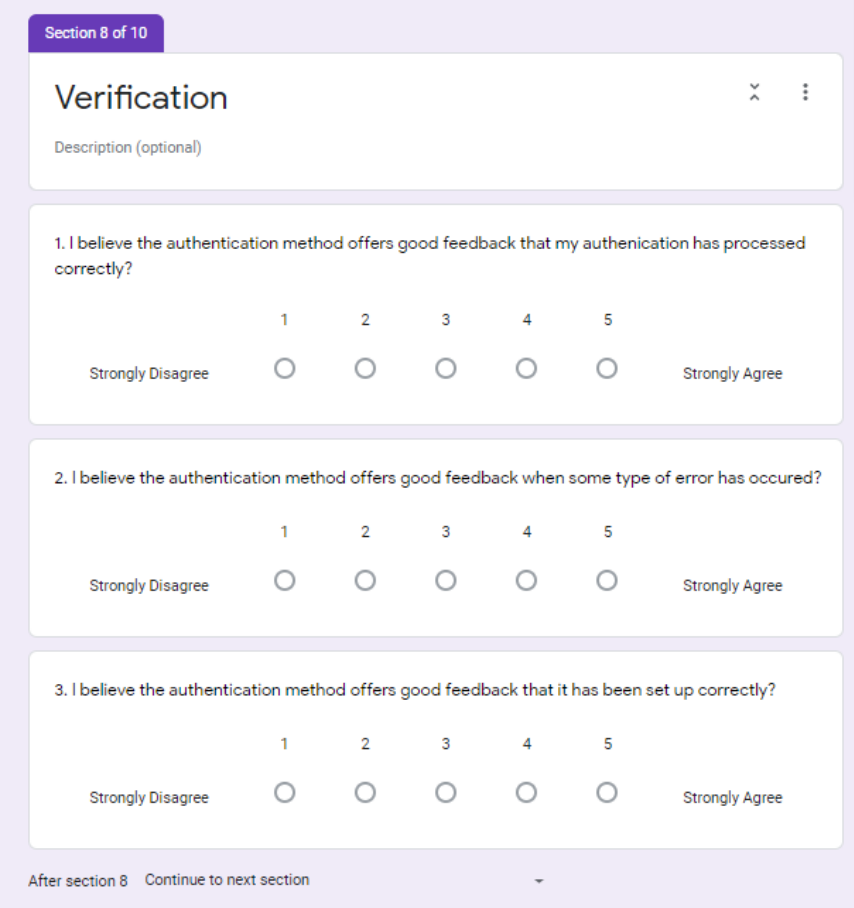

Figure 26: Questionnaire Verification

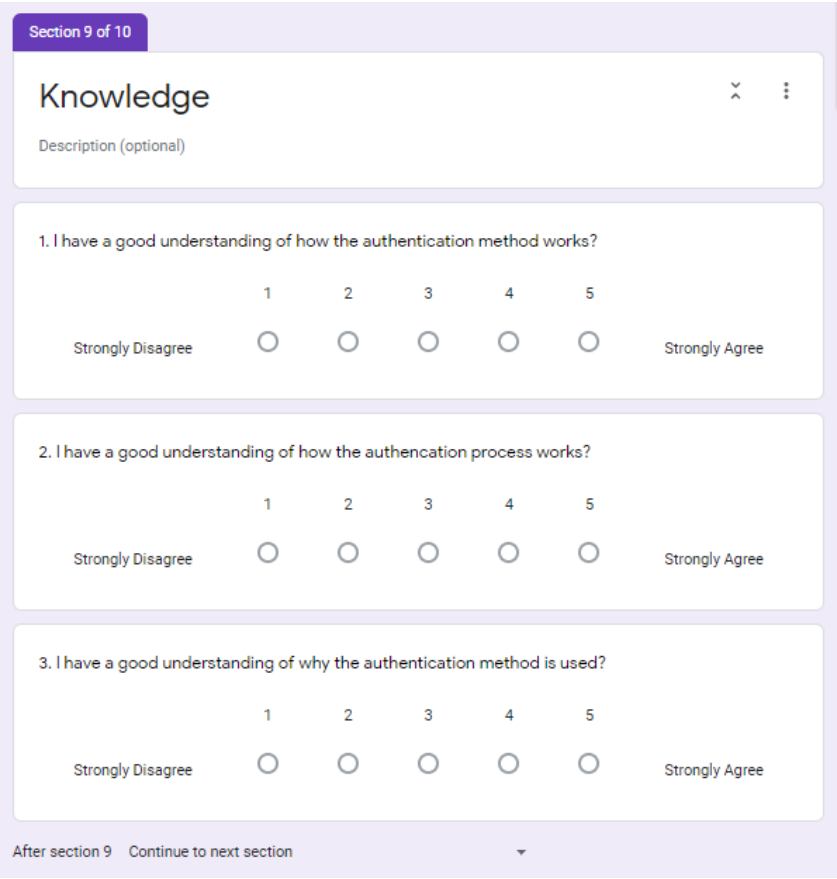

Figure 27: Questionnaire Knowledge

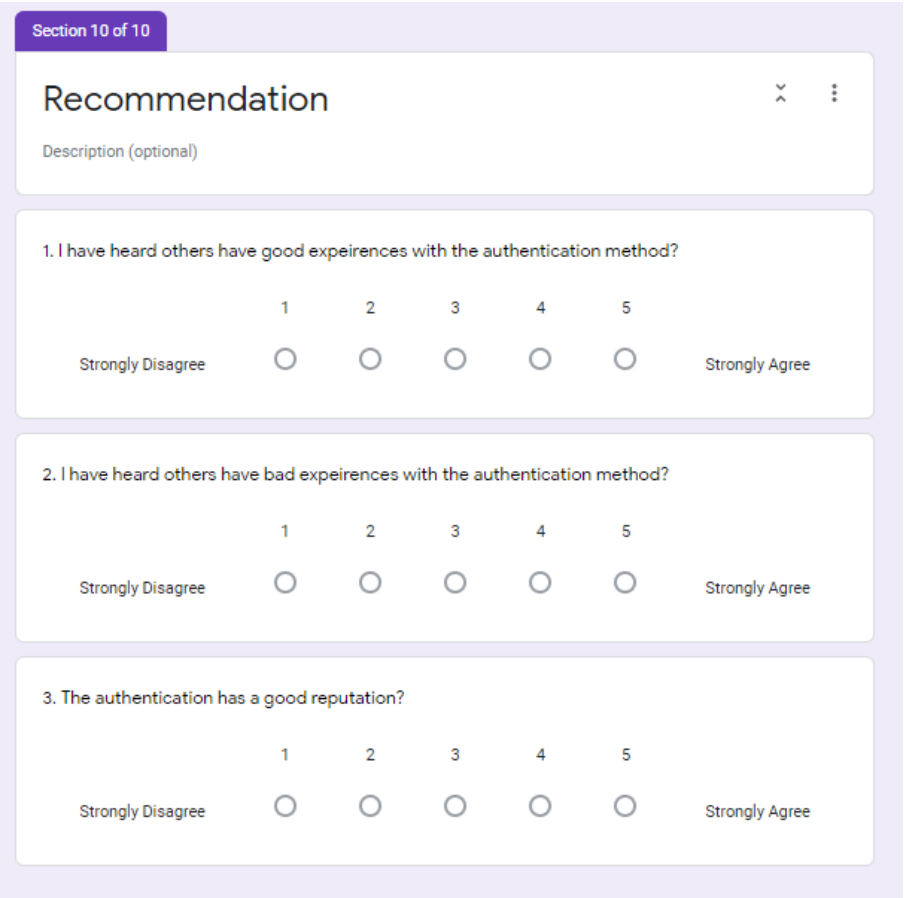

Figure 28: Questionnaire Recommendation

Participant Information Sheet

Name of school: School of Science, Technology & Health, York St John University

Title of study: Voice Biometrics Authentication: A User Perspective

---

Introduction

You have been invited to take part in a research project titled: Voice Biometrics Authentication: A User Perspective. The study intents to compare the different levels of trust users have with several different authentication methods. The study focusses on the user perspective of these methods and does so via a short study and questionnaire. Before you decide whether to take part or not, it is important that you understand why this research is being done and what it will involve. Please take time to read this information carefully and discuss it with the researcher if required.

If there is anything that is unclear or if you would like more information, please contact myself, Alec Wells, postgraduate student in the School of Science, Technology & Health, York St John University

or my supervisor; Aminu Usman, School of Science, Technology & Health, York St John University using the contact details found the following page.

What is the purpose of this investigation?

The aim of the investigation is to identify and discuss the different levels of trust users have with different methods of authentication. This will be done via a short study in which participants will use authentication method, and then fill out a questionnaire asking their opinions. In conducting this investigation, I am trying to find how voice biometric authentication compares to other authentication methods such as passwords or fingerprints from a user's perspective.

What will you do in the project?

After reading this form and if you provide consent, as a participant you will be asked to set up one type of authentication method (such as a password or fingerprint etc.) on the phone or computer provided, then try using that authentication method to sign in. Following this will be a short questionnaire about your opinions of the authentication method such as how secure you think it is, how easy it is to use, how reliable it is etc. This is done so as a participant, you can get a feel for the authentication method and then give your opinions via the questionnaire so I can discuss the difference between them from a user perspective. The investigation will take place in either an office or computer science lab with the researcher and will take around 10 minutes.

Do you have to take part?

No. It is up to you to decide whether you would like to take part in this study or not, but your contribution would be greatly appreciated. You will not be treated any differently, whether you choose to take part, or decide not to do so. If you do decide to take part, you may withdraw from the study without giving a reason and without penalty throughout the experiment. The responses to the questionnaire are anonymous so you will be unidentifiable, so please note that due to this, once you have submitted your responses to the questionnaire you may be unable to retract them as they will likely be indistinguishable from one another.

Why have you been invited to take part?

This research requires a sizable number of participants in order for it to have validity. As such, you have been invited to take part in this project because you are of adult age and able to give your own consent, as the study does not intent on asking vulnerable groups unable to give their own consent through any screening processes. The study intents to portray an accurate sample so participants will be asked regardless of their familiarity with the various authentication methods.

What are the potential risks to you in taking part?

During the experiment, you may have to set-up biometric data to sign into a mobile device. The study will only be using your questionnaire replies and will delete any biometric data once you a finished giving your questionnaire replies. You do have the right to withdraw from this project at any point, without giving a reason. You can withdraw from the project by informing me; Alec Wells via my email alec.wells@yorksj.ac.uk that you wish to do so or my supervisor Aminu Usman via email a.usman@yorksj.ac.uk . If you withdraw from the research, any words used by you will be removed from the data that has been collected. You may request that the information you have provided is removed from the study at any point until the questionnaire is submitted due to the anonymity of the replies.

What happens to the information in the project?

All questionnaire replies will remain confidential as they do not require any of your personal details. All data collected whilst conducting this investigation will be stored securely via the university, password protected email, linked with google drive and one drive storage systems. These are used for the storage of research data at York St John University, in line with the requirements of the General Data Protection Regulation. The information collected whilst conducting this project will be stored for a minimum of 6 months.

Thank you for reading this information – please ask any questions if you are unsure about what is written in this form.

What happens next?

If you are happy to take part in this project, you will be asked to sign a consent form in order to confirm this.

It is possible that the results of this research project will subsequently be published. If this is the case, appropriate steps will be taken to ensure that all participants remain anonymous.

If you do not want to be involved in the project, I would like to take this opportunity to thank you for reading the information above.

This investigation was granted ethical approval by the School of Science, Technology, and Health Research Ethics Committee.

Kruskal Wallis Output

(Credit SPSS)

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles 25th	50th (Median)	75th
Needed	60	4.70	.497	3	5	4.00	5.00	5.00
Widespread	60	4.27	.841	2	5	4.00	4.00	5.00
Common	60	4.40	.848	2	5	4.00	5.00	5.00
Hacked	60	3.38	1.136	1	5	3.00	3.00	4.00
Tampered	60	3.43	1.031	1	5	3.00	4.00	4.00
Differentiate	60	3.58	1.331	1	5	2.00	4.00	5.00
Learning	60	4.82	.431	3	5	5.00	5.00	5.00
Use	60	4.75	.628	2	5	5.00	5.00	5.00
Needs	60	4.02	1.017	1	5	3.00	4.00	5.00
Protects	60	3.92	1.030	1	5	3.00	4.00	5.00
Prevents	60	3.85	1.039	1	5	3.00	4.00	5.00
Anonymous	60	3.23	1.307	1	5	2.00	3.00	4.00
Expected	60	4.82	.504	2	5	5.00	5.00	5.00
Same	60	4.50	.813	2	5	4.00	5.00	5.00
Continue	60	4.52	.701	3	5	4.00	5.00	5.00
Used	60	3.90	1.570	1	5	2.25	5.00	5.00
Similar	60	3.85	1.448	1	5	2.25	5.00	5.00
Different	60	3.93	1.247	1	5	3.00	4.00	5.00
Processed	60	4.40	.616	3	5	4.00	4.00	5.00
Error	60	3.67	1.145	1	5	3.00	4.00	5.00
Set Up	60	4.32	.930	1	5	4.00	5.00	5.00
Works	60	4.37	.780	2	5	4.00	5.00	5.00
Process Works	60	4.25	.914	2	5	4.00	5.00	5.00
Why	60	4.53	.623	3	5	4.00	5.00	5.00
Good	60	3.83	1.152	1	5	3.00	4.00	5.00
Bad	60	2.70	1.239	1	5	2.00	3.00	4.00
Reputation	60	3.90	.933	1	5	3.00	4.00	5.00
Method	60	2.50	1.127	1	4	1.25	2.50	3.75

Figure 29: Kruskal Wallis SPSS Output

Post Hoc Output

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Needed is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.523	Retain the null hypothesis.
2	The distribution of Widespread is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.383	Retain the null hypothesis.
3	The distribution of Common is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.295	Retain the null hypothesis.
4	The distribution of Hacked is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.002	Reject the null hypothesis.
5	The distribution of Tampered is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.088	Retain the null hypothesis.
6	The distribution of Differentiate is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
7	The distribution of Learning is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.227	Retain the null hypothesis.
8	The distribution of Use is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.088	Retain the null hypothesis.
9	The distribution of Needs is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.707	Retain the null hypothesis.
10	The distribution of Protects is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
11	The distribution of Prevents is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.023	Reject the null hypothesis.
12	The distribution of Anonymous is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.042	Reject the null hypothesis.
13	The distribution of Expected is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.325	Retain the null hypothesis.

Figure 30: Post Hoc SPSS Output 1

14	The distribution of Same is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.011	Reject the null hypothesis.
15	The distribution of Continue is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.001	Reject the null hypothesis.
16	The distribution of Used is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
17	The distribution of Similar is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.006	Reject the null hypothesis.
18	The distribution of Different is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.168	Retain the null hypothesis.
19	The distribution of Processed is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.039	Reject the null hypothesis.
20	The distribution of Error is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
21	The distribution of Set Up is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.045	Reject the null hypothesis.
22	The distribution of Works is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.263	Retain the null hypothesis.
23	The distribution of Process Works is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.027	Reject the null hypothesis.
24	The distribution of Why is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.111	Retain the null hypothesis.
25	The distribution of Good is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.005	Reject the null hypothesis.
26	The distribution of Bad is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.666	Retain the null hypothesis.
27	The distribution of Reputation is the same across categories of Method.	Independent-Samples Kruskal-Wallis Test	.029	Reject the null hypothesis.

Figure 31: Post Hoc SPSS Output 2