Master's Thesis

Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Thomas Augustine MacKinnon
TP066728

Master of Science in Cyber Security
APDMF2204CYS(PR)
Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia-57000

supervised by
Dr. Julia Juremi

DECLARATION OF THESIS CONFIDENTIALITY

Author's full name: **THOMAS AUGUSTINE MACKINNON**

IC No./Passport No.: **535468399**

Thesis/Project title: **ACCESS CONTROL EVALUATION AND IMPROVEMENT OF SMART CARD AND FACIAL RECOGNITION TECHNOLOGY TO CREATE A SECURE WORKPLACE**

I declare that this thesis is classified as:

☐ CONFIDENTIAL

☐ RESTRICTED

☑ OPEN ACCESS

I acknowledged that Asia Pacific University of Technology & Innovation (APU) reserves the right as follows:

1. The thesis is the property of Asia Pacific University of Technology & Innovation (APU).
2. The Library of Asia Pacific University of Technology & Innovation (APU) has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Author's Signature:

Date: 5 May 2023

Supervisor's Name: **DR. JULIA JUREMI**

Date: 5 May 2023

Signature: ....

DECLARATION OF SUPERVISOR(S)

"We hereby declare that We have read this thesis and in our opinion this thesis is sufficient in terms of scope and quality for the award of the degree of
Master of Science in Software Engineering"

Name of Supervisor:	**DR. JULIA JUREMI**
Signature:	....
Date:	5 May 2023

DECLARATION OF ORIGINALITY AND EXCLUSIVENESS

I declare that this thesis entitled

ACCESS CONTROL EVALUATION AND IMPROVEMENT OF SMART CARD AND FACIAL RECOGNITION TECHNOLOGY TO CREATE A SECURE WORKPLACE

is the result of my own research work except as cited in the references. This thesis has not been accepted for any degree and it is not concurrently submitted in candidature of any other degree.

Signature:

Name: Thomas Augustine MacKinnon

Date: 5 May 2023

Acknowledgements

I would like to thank my excellent supervisor Dr. Julia Juremi for her invaluable help throughout this project. Her calm yet motivating support throughout the project lifecycle allowed me to explore the topic in my own manner without judgment or interference. I am very lucky with my Supervisor and happy to end my Masters with the first person who made me feel welcome at A.P.U.

I would also like to thank my Father and Mother, whose impact on my life cannot be understated, encouraging me to make the best decision of my life. I am truly blessed to have such amazing parents, words cannot express how much I love them.

Lastly, I'd like to thank my wonderful friends, who have made my time in Malaysia so amazing. I am so glad to have known them, even if it was not for long.

Abstract

Access Control is the process of managing who can and cannot enter restricted areas. Access Control comes in many forms, from historic lock and key, to modern solutions through Facial Recognition and Smart Cards. These technologies are used by the majority of businesses to keep their assets and employees safe from outside threats, but are they really secure? or simply the illusion of safety.

This project aims to answer this question, through extensive research, experimentation, and testing into Access Control, uncovering the hidden vulnerabilities waiting to be exploited. Smart Cards are the most common form of Access Control used, with Facial Recognition looking like the replacement in the near future. Both of these technologies were pushed to their limits to expose the issues they bring to a security system. Smart Cards were tested thoroughly to find the best methods for exploitation, whilst every option for obfuscating Facial Recognition was employed to find how a Malicious Actor would likely tackle physical security.

The results revealed a lot of worrying facts on the nature of Access Control, and how easy exploitation is highly effective against current security in most organisations. This is not without hope, as a series of solutions are created in order to mitigate the vulnerabilities found, helping SOC teams keep assets and employees safer for the future.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Cybercrime has seen a dramatic rise over the last ten years, with the Federal Bureau of Investigation reporting that complaints almost doubled during 2020, as seen in Figure 1.1. The Coronavirus has only increased this figure, with reports suggesting that a 600% rise has occurred over the pandemic (PurpleSec, 2022). COVID-19 saw many businesses switch to purely online models to deal with quarantine mandates, which naturally led to Security Operations Center (SOC) teams focusing their effort on digital security. The worst of the Coronavirus is luckily in the past, with physical stores and workplaces reopening, but the prioritisation of digital security could have left a gap in defences.

Physical Security is also a key part of a SOC team's responsibility, by protecting staff and assets from malicious actors entering restricted areas. Attacks are not restricted to just digital mediums, in fact, by being physically on premises a hacker has a lot more potentially damaging Cyberattacks without the need to bypass external layers of security, like firewalls (Akati & Conrad, 2021). Tailgating is a common method to gain access to restricted areas, where a malicious actor will follow someone with legitimate access. This form of attack can give hackers staff level access to databases and assets, and with a high success rate of 68% in one experimental study conducted in U.S. airports (Chan et al. 2012). This is shocking considering that U.S. airports are infamous for their high levels of security, it is likely that this figure would be much higher in other scenarios.

Access Control has been the standard solution for SOC teams in worries on physical security, using technologies like biometric scanners, pins, and even facial recognition. However, the primary method at this time is through the use of Smart Cards, which is a piece of plastic containing an embedded chip to verify if the owner can open a locked door, activate an entry turnstile, or even allow access to a digital workspace or database. Smart Cards are the most popular form of technological access control, but in the future Facial Recognition may dethrone it, as it is far more secure and already seeing use by large companies and Governmental bodies who can afford the upgrade. This does leave the question on how secure are these new forms of physical security? traditional locks have been known as the illusion of security, as any criminal with a pick set and a little skill could have a door open in no time (Hopkins, 2018). It begs the question of is Facial Recognition and Smart Cards a secure form of Access Control? or is it simply another illusion.

This project aims to answer this question through varied experiments and research to fully test this technology. This paper is split into seven sections, each contributing to the final research and results of Access Control. An Introductory chapter will begin the document, featuring a background review of the subject, whilst setting the research questions and other metric to be used later in the

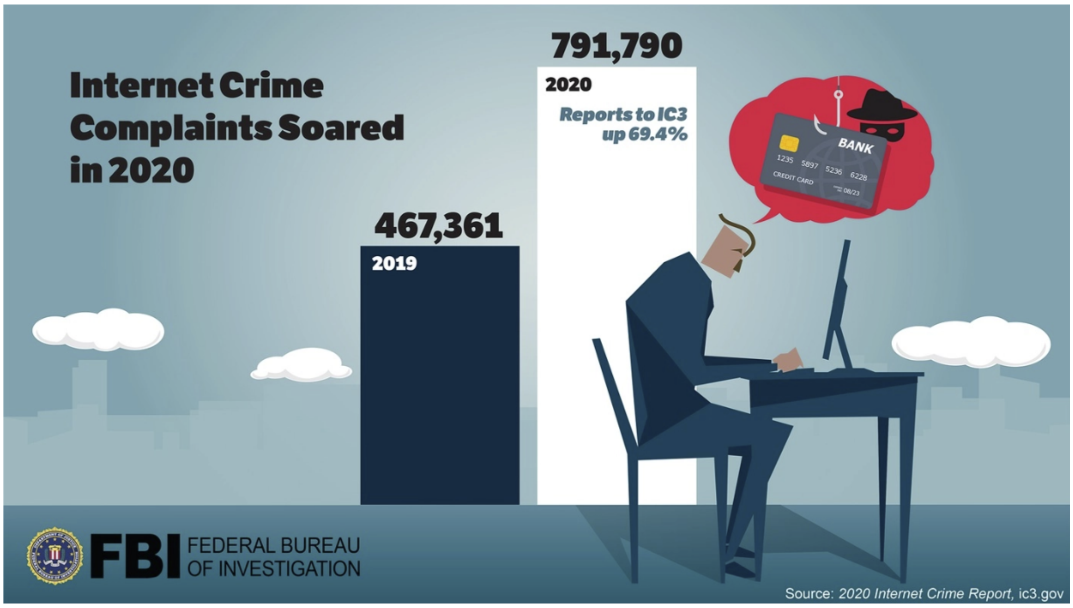


Figure 1.1: IC3 reported cases from 2020 compared to 2019 (FBI, 2021)

Evaluation of Success. Chapter two will cover an in-depth Literature Review into the subject of Access Control, allowing understanding of existing work from Authors. The Methodology will cover all the plans for how the project will be conducted, from what design approach used to how time will be managed, and identifying risks to mitigate. Chapter Four, The Procedure, will feature all the work actually done for the project, such as experimentation into technologies, building testing environments, and discussing all the tools available for exploiting Access Control. Thorough testing will then be conducted in Chapter Five, through three expansive tests aiming to gather Quantitive and Qualitative data. A Discussion will then follow, exploring the reality of the project, from initial plans to analysis of results, with the goal of identifying what this research contributes to the state of security. Chapter Seven will conclude the paper, finalising the findings and offering potential avenues for future work.

1.1 Background

To better understand the subject of Access Control, several Academic Papers were reviewed, which aided in finding the problem area for this proposed project.

Chan et al. (2012) researched the topic of Access Control in their excellent paper on tailgating. The authors discuss how the key purpose of Access Control is to prevent Malicious Actors gaining access to restricted areas. The problem arises with getting the right balance of security and ease of use, as if staff find measures put in place to protect them too irritating it is likely that they will find a way to bypass them, which opens up vulnerabilities to be exploited. The researchers primarily discuss the issue of tailgating, which was discussed in the Introduction, but conclude that the use of Smart Cards and detection cameras were the best way to stop this issue. Interesting the paper does not bring up Facial Recognition, but as it is a decade old maybe it was just a limitation of the time.

Kim et al. (2019) expands on this topic by discussing the modern stance on Access Controls, and agrees with Chan et al. (2012) on the knife-edge problem when it comes to implementing the right level of security. The authors discuss how many forms of Access Control are outdated, and that it is likely a push will occur to more futuristic technologies, such as Facial recognition.

Büttner et al. (2020) highlights that this change will not happen for many years in their paper on the security of Access Control. The researchers state that by far the most popular form of Access Control is through Smart Cards, which contain a Microprocessor to authenticate users (or various other purposes like pay for transportation). Around 50% of Danish companies with over 250 employees use Smart Cards as its primary source of Access Control, but that this technology is inherently weak, with many methods to crack, clone, or destroy security tokens found inside.The authors discuss many other issues with this form of Access Control, but the key point is that if Smart Cards are this vulnerable, what other aspects of security are the same?

Abellon et al. (2021) delves far more into this topic in their paper on duplicating Smart Cards using tools like MIFARE Classic (which is the main brand of Smart Cards used) and an NFC mobile application. The researchers were successfully able to clone Smart Cards and gain unauthorised access, and used this to show the potential this "Security Mechanisms" could have in a Social Engineering attack. This paper is an excellent first step into exploitation of Smart Cards, but could be more thorough and extensive in the methods of finding exploits.

The subject of Facial Recognition was brought up by several authors as a viable method for Access Control in the future (as it is too expensive for most organisations to implement at this time). It is likely that this will one day be the normal method of verifying people, but Milossi (2021) brings up the ethical concerns of the technology. The author states that Facial Recognition can lead to issues with Free Speech and Privacy, as a surveillance state like China demonstrates, where the technology is misused to oppress its citizens. The author concludes that Facial Recognition is never 100% accurate, which can lead to false positives, and lead to innocent people receiving undue punishments. From a security perspective, this is worrying, as the trend of Facial Recognition being the primary source of Access Control is riddled with the inaccuracies and ethical issues.

Kasthuriarachchi et al. (2021) discussed the subject further, bringing up the effects masks have on recognition capabilities. Surgical masks prevent most low level Facial Recognition systems from working (with more advanced systems being able to recognise from eyes and nose features), but more covering masks can obviously reduce this further. The research mainly discussed other ethical issues of the technology, such as the lack of consent in Government Facial Recognition systems that could violate the General Data Protection Act, but does not delve further into the methods to prevent a successful recognition. It is very likely that a Malicious actor would try to hide their face when intruding in a businesses premises, as to avoid being recognised by cameras. There was little research into this method of avoiding detection, which would likely be a key technique used to bypass SOC teams security, and prevent being caught afterwards.

1.2 Problem Statement

The literature reviewed revealed a gap in the field of Cybersecurity, being the study of physical security mechanisms, and how effective are they at protecting an organisation from Malicious actors. Plenty of studies discussed the ethics of facial recognition, and how it can be used for security, but this was never backed up with experimentation to truly test the technology that businesses entrust their security to.

The same can be said for smart cards, which were discussed in length relating to their technical features, but little research was done on how the technology can be cracked to exploit security systems, and none which conducted experiments on a variety of systems. This gap will become more and more critical over the coming years, Social Engineering is already one of the most popular attack methods for Malicious actors, it is not unlikely that hackers will use this technique to exploit physical security mechanism, or more likely already are.

1.3 Research Question

This project aims to answer each research question presented below, through experimentation, literature, and surveying. The purpose of these questions is to keep the methodology of the project on track, and evaluate the results after finishing all the elements of practical work. The research questions are:

1. How effective is Facial Recognition as a security mechanism?
2. How secure are Smart cards as a form of access control?
3. How successful would a malicious actor exploiting these technologies be against a business?

These questions cannot be answered objectively at this time, but a hypothesis can be formulated to test further the preconceived notions that the author is carrying. These hypotheses will also be used later with the results from the project to see if these thoughts were correct or not, and what can be learnt from these early predictions. The hypothesised answer to the research questions are:

1. Facial recognition is a very effective tool for security, with little methods to exploit it.
2. Smart Cards are an insecure form of access control, with many ways to exploit the technology to gain illegitimate access.
3. A malicious actor would not be able to use Facial recognition exploits to their advantage, as it is hypothesised that any usable exploit will either be impracticable or obvious to any security staff. Exploited Smart cards on the other hand will be an incredibly useful tool in any malicious actor's arsenal, and prove to be a key concern to any business using it as a form of security.

1.4 Aim and Objectives

The aim of this project is to demonstrate the risks and the inherent weaknesses in standard physical security mechanisms through the use of experimentation and exploit development.

There are also several objectives that will hopefully be achieved during this project, which are:

- Find a way to prevent facial recognition without just covering the subject's face.
- Discover if security will stop a subject who is deliberately trying to hide their face.
- Develop a Skeleton key for a Smart card system.
- Replicate another Smart Card without the use of simply cloning the card.

1.5 Scope and Significance

This project will cover the breaking and exploitation of commonly used Smart Cards through various method, which will be explored through experimentation. The exploitation will be done through accessible techniques and tools, aiming to push the technology to the limits without delving into unknown territory. This project will not try to break Smart Cards through radical methods, nor build solutions from the ground up, simply testing the capability of Smart Cards in the hands of a hacker

Facial Recognition will be tested through tangible methods, rather than through digital hacking of the software or algorithm that allows the cameras to work. Essentially, this project aims to find out how effective a malicious outsider could be at exploiting and bypassing physical security mechanism in a real world scenario

The Significance of this will show how secure the physical security mechanisms that organisations and businesses are in reality. This could be an enlightening, if worrying, project, that could see the true nature of these technologies that so many trusts to keep them safe. If the results are particularly shocking, it could lead to changes in security standards and usage of this technology, which would result in organisations being much safer for the future. Even if these proposed experiments fail, it will demonstrate that there is nothing to fear in using Facial Recognition technology and Smart Cards, allowing SOC team to be reassured in their efforts towards security and safety.

Chapter 2

Literature Review

This chapter will cover a review of existing academic literature relating to Access Control, Smart Cards, Facial Recognition, and any other area of interest that could prove beneficial to the project. The papers collated were found on reputable sources, such as the Institute of Electrical and Electronics Engineers (IEEE) or the Association for Computing Machinery (ACM) Digital Library. The Majority of papers were dated less than five years from writing, with some notable exceptions for papers that added a historic context to the subject or whose value was not lost with the advancing technological landscape.

2.1 The Need for Access Control

Access control is one of the most important factors when it comes to a Security Operation Center (SOC) team securing an organisation. It is imperative that authorised user have access to contents in order to perform their job, whilst keeping out any malicious actors that wish to cause harm. Chan et al. (2012) in [14] state that level of security in an organisation is highly dependent on usage of Access Control. Too strict or intrusive access control leads to authorised users getting annoyed and finding loopholes, which in turn aid attackers. This could be in the form of leaving locked doors open, or passwords on stick notes so that employees do not need to remember them. If the access control is too weak then the malicious actor will have no problem getting past whatever mechanism is in play, and illegitimate access to restricted areas will be easier.

Access Controls are important in order to avoid various attacks and data leakages that would not be possible otherwise. Physical security plays a big part in the overall Cyber defence of an organisation, as devices already within a network have much more sensitive information and potential for attacks than external devices. Kim et al. (2019) in [20] highlight this in their paper regarding the future of access controls, as organisations with relaxed security mechanisms could suffer large fines, loss of revenue, become tarred with a negative reputation amongst the public, and much more. The researchers state that it is important that SOC teams implement the right level of access control to restricted areas and sensitive information, and recommend future technologies to have a better Cyber defence. The authors focus on Activity control, where unusual activity alerts the SOC team to potential intrusion, which can save an organisation from a potential attack.

Altawy & Youssef. (2016) in [6] state that many of the standard access control are outdated, as they were formed in the 1980s, so SOC teams should consider looking towards new technologies. The pair agree with the points made by Kim et al. (2019) and Chan et al. (2012) on finding the right level of security is critical for employee safety, highlight with the example of modern crash features in cars. The researchers state that a safety feature in certain car manufacturers (which they left unnamed to prevent any crime inspired by their paper) would automatically unlock all the car doors if the vehicle is rolled over so that the passengers can escape quickly. This unfortunately resulted in criminals jumping on top of car roofs to exploit the safety feature and unlock the car. Clearly, Access Control is vital to any organisation of any size, and must be handled with care and effectiveness to get the best results.

This Literature review will discuss two of the most prevalent types of Access control in-depth, being Facial Recognition and Smart cards, seeing the underlying technologies, history, and usage seen in modern examples. Security flaws will also be reviewed, aiming to see what potential issues SOC teams might face in using these forms of Access Control, and what areas of research are missing that could further improve the Cyber defence of an organisation.

2.2 Smart Cards

Smart Cards were first introduced in the 1950s in Diners throughout the United States of America, and later adopted by banks. The original Smart Cards were simply plastic with customer numbers printed on the side, but later evolved into the format seen today. Attoh-Okine & Shen (1995) in [7] describe this and more in their historic paper on Smart cards, stating how the original cards were developed by Roland Moreno in 1974 using a Japanese patent (created by Kunitaka Arimura in 1970). The pair go onto explain how the original concept was to make fare collection easier and more flexible for customers, whilst being able to keep better financial records.

Microprocessors were added to Smart Cards in the 70s, with further advances throughout the years to become the Access control mechanism known today. Alazmi et al. (2018) in [4] details all this and more throughout their research into the subject in the modern age, showing the evolution of cards with the potential to execute commands, run programs, and send data. The researchers differentiate the various types of Smart cards, which are as follows:

- **ID cards -** Government issued cards, can be used in Airport Immigration, or various other uses.
- **Transportation -** Used to access Public transportation or pay road tolls without the need of physical cash, such as Touch n' Go cards found in Malaysia.
- **Telecommunication -** Sim cards used to access mobile networks.
- **Healthcare -** Used in hospitals to access patient data, medical history, and billing information.
- **Electronic Payment -** Card used for general paying without cash.
- **Security Card -** Used to access restricted areas, such as employee area or private floor of an apartment building.

There are two types of Smart cards as described by the researchers, firstly being centralised, where cards each have unique identifiers stored on the smart chips, which is compared to a database of permissions for that user. Secondly, there are distributed access cards, where the grouped permissions are instead stored on the card itself, meaning no network connection is needed. Each has its benefits and downsides, depending on the scenario at hand.

Carreira et al. (2020) in [13] adds to this by detailing how storage tends to work on Smart Cards, as seen in Figure 2.1. The green section indicates the Unique Identifier, which is the primary part of any Smart Card, whilst the Orange sections represent the Security Blocks, everything is an unallocated data. The researchers do not do on to describe what Security Blocks consist of, but it can be assumed from other authors that this is where any encryption algorithms or other security mechanism is stored.

Alamzi et al. 2018 predict that Smart cards uses will become more and more varied as time goes on, and eventually be used for all types of activities. This seems unlikely, as other technologies are already replacing the need for Smart cards, such as Biometrics, Facial recognition, and mobile applications (as seen with Apple Pay or Google Wallet). This statement also contradicts with the thoughts presented by other researchers that will be discussed later on. The research presented into the history and types of cards is very valuable, but overall the paper lacks depth into any new fields, and ignores more pressing technologies.

```
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: B4 FA AC BF
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15     63   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         62   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         61   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         ...
   3     15   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         14   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         13   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         12   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   2     11   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         10   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          9   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   1      7   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          6   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          5   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   0      3   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          2   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          1   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          0   B4 FA AC BF  5D 08 04 00  62 63 64 65  66 67 68 69  [ 0 0 0 ]
```

Figure 2.1: How Storage works in a Smart Card (Carreira et al. 2020 in [13])

Modern Smart Cards were originally intended to be the safer alternative to traditional payment cards, which used a magnetic strip encoded with information to make transactions, often referred to as "magstripe". Magstripe cards were infamously easy to clone, leading to a lot of fraud and unauthorised access (when it comes to magstripe cards being used for access control). Ahmad et al. (2016) details how Smart Cards used a chip instead to send transactions securely, which only worked when supplied power by a reader such as an Automated Teller Machine (ATM) or door scanner. Radio Frequency Identification (RFID) is then used to transmit the data from the card to the scanner and then to the backend server to verify the request, as seen in Figure 2.2.

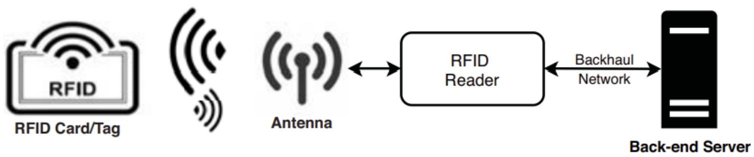


Figure 2.2: How a Smart Card works with RFID (Carreira et al. 2020 in [13])

Smart Cards used for financial purposes also included the "EMV" protocol, named after Europay, Mastercard, and Visa respectively, to add to the security of their cards. This protocol would generate a unique secret cryptographic key for each transaction to make cloning that occurred on antiquated magstripe cards impossbile on the new EMV cards.

Payment Smart Cards often utilise Personal Identifying Numbers (PIN) to enhance security. Benes et al. (2017) in [9] suggest that this system could also be used in traditional Smart Cards used for

Access Control in their paper on enhancing the security of the technology. The researchers state that PINs serve as a great countermeasure against cloning and theft of cards in the banking industry, so it reasonable to suggest that businesses using the technology to make this upgrade.

The authors also suggest changing the encryption methods found on cards, as it is outdated, and instead use better options such as AES-GCM-128bit-129ICV or ECDHE-RSA. The authors further add a lockout feature to their recommendation to prevent brute force attacks against PINs. Overall, this paper presents an incredibly effective and thought out solution to the insecurity found in Smart Cards, whilst giving good background on the technology as a whole.

Smart Cards offer an affordable option for improving security in an organisation, as Khan & Sakamura (2016) in [21] discuss in their paper. The researchers focus on the issue of cybercrime and healthcare, reporting that around 80% of United States' Health organisations have been the victim of some kind of digital threat. This type of crime is potentially devastating to hospitals, as medical records are very sensitive and could lead to serious Identity fraud. Hospitals found guilty of not securing facilities correctly could face large fines from Health Insurance Portability and Accountability Act (HIPAA), which can cripple life-saving services, as hospitals do not have the funds to deal with these financial burdens.

The pair suggest that a form of physical security token through the use of Smart Cards is not only the best affordable solution but also the easiest and fastest to implement. The authors present an excellent solution and understanding of the technology for the case at hand, but fail to bring up some of the security issues present in Smart Cards, which could lead to further trouble down the line. Smart Cards do have a lot of issues that could cause problems in an organisation, this topic has also been researched to fully understand the role this technology has in a SOC teams defence.

2.3 Issues with Smart Cards

Smart cards are widely used throughout the world, Büttner et al. (2020) in [12] state that in 2019 49% of Danish companies with over 250 employees use Smart cards as a security access control. The researcher's paper explored the security of this form of access control, stating that the majority of Smart cards found in the workplace are MIFARE classic cards. This type of Smart card have had known weaknesses since 2008, and are easy to duplicate or crack, often sharing security keys, meaning once one is broken all are. The authors further explain that the cards itself are often weak, with security keys printed on the side. Furthermore, these security keys are often sequential, meaning malicious hackers can guess other keys without much trouble.

The main issues present in Smart Cards is that they can be stolen, and have little to no way to prevent an unauthorised user getting access to restricted areas. Both Alazmi et al. (2018) and Büttner et al. (2020) discuss this problem, and seems to be an unsolvable issue unless more intrusive or bothersome controls are implemented into the cards, such pins or biometrics, which defeats the ease of use that Smart Cards provide. Büttner et al. (2020) research is more in-depth on the vulnerabilities present in this common form of access control, which provides a greater understanding of how this can affect the decisions made by SOC teams when implementing them into an organisations' security. However, the research fails to detail practical ways to counter common Smart card fraud.

Abellon et al. (2021) in [1] conduct a detailed risk assessment and methodology into how to duplicate MIFARE cards, aiming to display how weak this form of access control is. The researchers use several tools, such as the MIFARE Classic tool and the NFC mobile application, both of which can be used to duplicate and rewrite cards. The authors were successfully able to spoof an access card, and discussed how social engineering could be used to gain access to the Smart card in order to read the contents for duplication. This practical research is good, but it is a shame that the authors did not conduct further study into writing their own security keys in order to gain unauthorised access. It has already been previously discussed that cards can be sequential, or have identical keys, so it would have been interesting to see this topic delved into more.

Bhatt et al. (2021) in [10] agrees with the thoughts of previous researchers, stating that Smart Cards have become outdated with modern security systems. New flashy and attention grabbing technologies such as Internet of Things (IoT) devices have led to a lack of attention placed on Access Control. The authors go on to state that serious care and improvements must be conducted with traditional Access Controls, but fail to give any ideas or suggestions on what specifically could be done, making it only an average paper.

Smart Card data is rarely encrypted, as stated by Bozzato et al. (2015) in [11], with communication between the card to reader to server all being in plaintext. These makes it very easy to intercept the communication and use it for creating duplicate cards. The authors then go onto to analyse typical encryption methods and how they can be reversed engineered, a complex and frankly rarely useful process considering the negligence to use security standards on communication. This statement also seems to directly back up Benes et al. (2017) in [9] insistence on upgrading the encryption algorithms on Smart Cards to easily prevent Man in the Middle attacks.

Ahmad et al. (2016) in [2] focus their paper on the worrying failings found within EMV Smart Cards (as discussed earlier), as the researchers found that this colossus of payment options to be very vulnerable. Skimming of sensitive payment information was the main weakness that the authors brought up, where an external device intercepts data whilst the owner tries to use a trusted machine, such as on an ATM or even a fake pin pad, as seen in Figure 2.3. This malicious technique is difficult to prevent, as skimmers are almost identical to the trusted machine, and without regular checks on the payment interface they rarely get found. The researchers state that cloning is still an issue with these EMV cards as well, but do not go further into the problem and causes.

Figure 2.3: Card Skimmer found on a UK ATM (Cooper, 2014)

Ahmad et al. (2016) supply a decent paper on the insecurities within Smart Cards used for payment, and it is interesting how similar issues are present on cards used purely for Access Control. However, the paper is lacking in content and discussion, with their only being one real example of insecurity and a lack of practical discussion on how malicious threats exploit the cards, perhaps this is a good topic for future work. EMV Smart Cards dominate modern payment methods, especially with the Coronavirus causing businesses and members of the public to use cash less and switch to virtual payments to avoid contamination. This makes a proper audit of Smart payment Cards relevant now more than ever. The author's paper is older than others reviewed, which reveals some gaps in the technology covered, as ATM shimmers have outshone the skimmers discussed by Ahmad et al. (2016). A shimmer is forcefully inserted into the card slot of an ATM as seen in Figure 2.4,rather than an external attachment to the machine like traditional skimmers. This makes the shimmer very difficult to spot by an unsuspecting member of the public, and harder to remove from the machine.

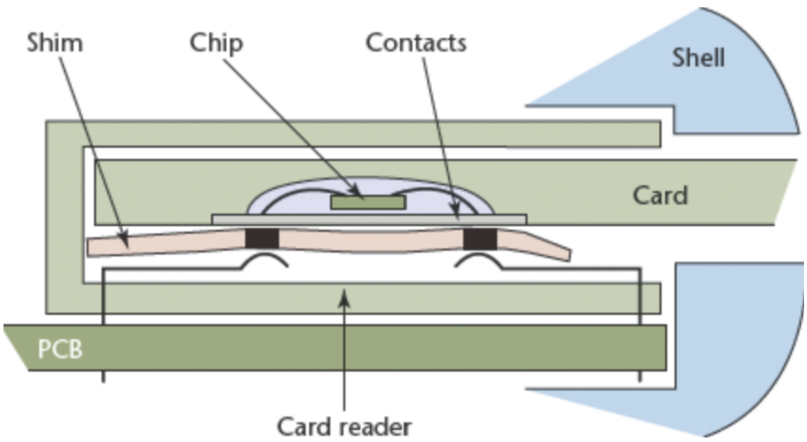


Figure 2.4: ATM shimmer diagram (Kamble & Zinjurde, 2020 in [18])

Kamble & Zinjurde (2020) in [18] cover the topic of how Banking Cards, like credit or debit, meet Multi-Factor Authentication standards. Banking has utilised smart cards for a long time, in the form of credit or debit cards used to access a clients' account and funds. A Personal Identification Number (PIN) is typically the primary form of security for these Smart Cards, where the owner inputs four digits after entering their card before access is granted to banking services. This fulfils two aspects of Multi-Factor Authentication (MFA)being the "something you know" through the PIN and "something you have" through the physical card.

The third pillar of MFA comes in the form of "something you are" such as biometrics data. Kamble & Zinjurde (2020) aimed to incorporate this into the traditional banking security through the use of facial recognition. The authors state that biometrics are more secure than other methods of Access Control and suggested that the feature would use a client's mobile device to verify their identity. It is not unprecedented for phones to be used for banking security, as many businesses utilise One Time Passwords (OTP) sent to the client's registered mobile number before granting access or allowing a payment to be made. OTPs serve as an additional, "Something you have" which was deemed by the authors to not increase security enough for the investment into this security feature.

The pair used standard python libraries such as OpenCV to enhance Smart Card security and gained an accuracy of 87% in recognising a client's face. The paper served as an interesting peek into the future of Smart Card Technology, and how facial recognition will likely be tied to it. As their research focused on development it did lack discussion into areas of interest such as ethics and issues with the technologies, but did prove that effective Facial Recognition can be achieved through simple and available resources.

This is not the only example of Facial Recognition being entwined in Smart Cards, as Benamara et al. (2021) in [8] show in their paper on improving traditional MIFARE cards. The researchers stated that Electronic Payment methods were too vulnerable to stolen cards, so suggested adding Facial Recognition to enhance security in not only payment cards but all Smart Cards. As shown in Figure 2.1, much of the storage on MIFARE cards is unused, so the researcher suggested also storing a face ID on the additional space, and built a Raspberry Pi scanner to first check the User ID of the card, and then use a camera to verify the face of the user. The project was very successful, and shows the growing trend of Facial Recognition Technology found throughout the majority of research.

This also shows the growing irrelevance of Smart Card Security, and how they will likely be tied to some other form of authentication in the future, with Facial recognition being first in line.

2.4 Facial Recognition

Ten of Thousands of years ago, Humans developed the innate ability to recognise faces. Originally, this evolution occurred so that early man could spot hostile faces amongst the dense jungle, and to understand the emotions through the expressions of fellow tribe members. This ability has served mankind throughout the ages and is an essential part of our being. Humans are excellent at spotting faces, even where none might be, such as the "Face on Mars" which was captures by Viking 1 orbiter in 1976, as seen in Figure 2.5. In reality this was simply a trick of the light, hitting the Martian landscape in just the right way, but nevertheless shows how potent our Facial Recognition Capabilities are. It was inevitable that mankind would one day gift this ability to machines, who would quickly outshine us in this area with ease.

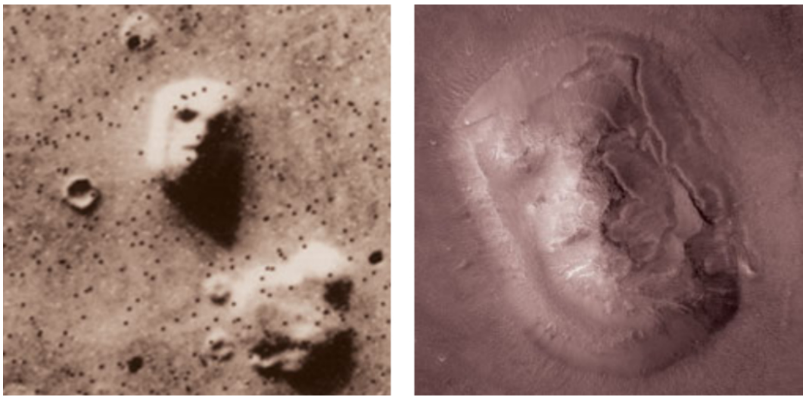


Figure 2.5: Face seen in Mars Versus the rock formation in reality (Bates, 2008)

Shen et al. (2020) in [26] discuss all this in their paper on the subject of Facial Recognition, and it's future, detailing how Charles Darwin, the creator of the theory of evolution, was fascinated by this ability and wrote at lengths about it. The researchers state that there are three stages to Facial recognition, which are:

1. **Detection -** Involves finding a face using Computer Vision and Artificial Intelligence, which identifies and extracts a face from media (image/video/3D graphic).

2. **Analysis -** The Facial Recognition algorithm then maps the face using specific "landmarks" to calculate the geometry of the subject. Features that differentiate one face from another could include eye gap, shape of face, the distance between lips and nose, eyebrow angle, and much more. This data is converted into a unique faceprint (like fingerprint or iris feature), essentially points that define the persons' face and can be used to reproduce it. This can be seen in Figure 2.6 from Jiang. (2020).

3. **Recognition -** The faceprint is then compared (and often added for future refinement) to a database of faces until a match is found.

Shen et al. (2020) provide an excellent discussion on the historic routes of Facial Recognition, and over how the technology specifically works in the modern day. The paper discusses far more about future possibilities in Facial Expression Recognition, attributing it as the next stage for the

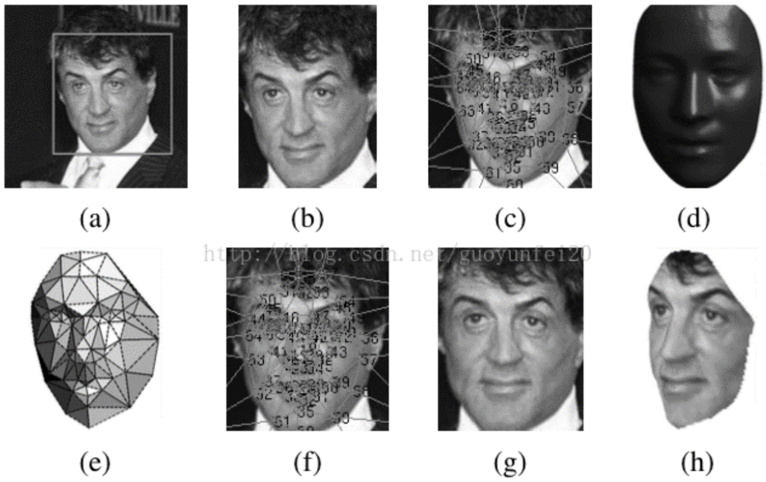


Figure 2.6: How Facial Recognition Technology create a faceprint from an Image, using Sylvester Stallone (Jiang, 2020 in [17])

technology, and propose an interesting framework. However, this research into expression recognition is out of scope for this literature review, and paper in general, as the focus is more on the security side of Facial Recognition. Regardless, the authors have written an excellent paper that contributes to the field of research.

Facial Recognition has seen a meteoric rise in usage over the last ten years, being widely adopted in a variety of technical solutions. It is standard for Smartphones to possess Face IDs to unlock the device, and for businesses to upgrade from standard access cards to a more secure form of authentication (Mao et al. 2020). The growing trend seems to be that biometrics, and especially facial recognition, will replace traditional Access Control and be integrated into every aspect of everyday life. Jiang. (2020) in [17] concurs with this prediction in their review of Facial Recognition methods. The author states the reason why Facial Recognition is preferred over other biometrics such as fingerprints, retina scans, and DNA is that it does not require any contact with the user to perform authentication or identification. This can be seen as a great positive through accessibility, making Access Control easier for people afflicted with disability.

Memiş. (2018) in [23] states that Facial Recognition uses Machine learning to authenticate users, by classifying if a user matches any faces in a database, giving the example of K-nearest neighbour(KNN) as a viable algorithm, an example of which can be seen in Figure 2.7. The researcher discusses the technology at length, stating how facial recognition can be highly accurate in a controlled setting with plenty of input data, like any Machine Learning algorithm, but struggles when data is limited. The paper gives good background on the subject of Facial Recognition but falls short on further research.

Mao et al. (2020) in [22] discuss the subject further, bringing up the point that facial changes can greatly affect the success rate of a Facial Recognition algorithm. Growing out facial hair, gaining or losing significant weight, ageing, facial disfigurement, or any other relevant factors can cause algorithms to fail at recognising an authorized face. This confers with Memiş. (2018) point about

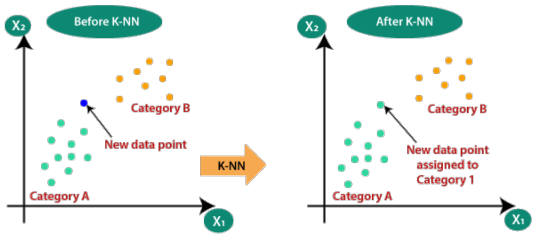


Figure 2.7: K-nearest neighbour example (Java T Point, N.D.)

the effectiveness of Facial Recognition algorithms, as to work properly a constant supply of up-to-date images are needed. This can be achieved by simply saving an image of the user's face each time a successful recognition occurs, therefore building a timeline of facial changes. This works for systems that have frequent occasions where the algorithm is working, like unlocking a phone, but struggles when there are greater lengths of time between recognition attempts. Mao et al. (2020) aimed to solve this through the use of Facial Expression Recognition, in a similar hope to Shen et al. (2020), which would counter any facial changing factors. This paper is not as relevant to the subject at hand, but shows the technological growth in Facial Recognition from multiple independent authors, which gives insight into what the future of this access control might look like.

Jiang. (2020) also brings up some downsides of the technology, stating that external factors can greatly affect the success rate of Facial Recognition, which is a much lesser concern for traditional Access Control that are more tactile. Factors could include lighting, camera quality, the users' expression, and the colour of the image (black and white CCTV). This data adds to the growing list of factors that can negatively effect recognition abilities, as discussed by Mao et al. (2020). Jiang. (2020) also states that facial alignment can cause noticeable dips in success rate. An aligned face has an accuracy rate of 97.5%, whilst an unaligned face dips to 87.9%.

This figure is interesting as it correlates with the data acquired by Kamble & Zinjurde (2020) in [18], with their success rate being 87%. This suggests that Facial Recognition algorithms tend to perform worse when using cheaper technology or if the user is avoiding the camera. An educated guess can be made that if these two factors were combined, then success rate would drop even further.

Kasthuriarachchi et al. (2021) did also find that wearing a face mask alone blocks Facial Recognition Cameras fifty percent of the time, with only covering the mouth and parts of the nose. More advanced (and expensive) cameras are required to properly recognise a user, and larger masks significantly increase the aforementioned percentage, showing the natural (but obvious) workarounds possible to avoid Facial Recognition detection.

Cornelis et al. (2008) in [15] touches further on the topic of Facial Recognition Accuracy in their paper on issues and ethics of the technology. The researchers definitively state that Facial Recognition services should not be considered capable of telling the "Objective Truth", only being able to tell the "Probable Truth". This statement, despite being old, still correlates with the recent data seen in Kamble & Zinjurde (2020) and Jiang (2020) papers, as Facial Recognition was shown to never be 100% accurate, even in closed testing environments. The authors then go onto bring up the ethical issues with the technology, which is a rather large aspect of Facial Recognition technology.

2.5 The Ethical Issues of Facial Recognition

The adoption of Facial Recognition has not come without criticism, which is natural for any burgeoning technology. The issues are vast, which are covered by several authors reviewed, such as Milossi (2021) in [25] research on the ethics of Facial Recognition. A core facet of Facial Recognition is the lack of consent from users, especially in cases of law enforcement or Governmental bodies using it, as previously existing pictures can be used to recognise a face. Naturally, users consent for images on personally uploaded to social media to exist online, the problem comes when external bodies use these images for other means. The author states that this naturally contradicts the General Data Protection Act (GDPR), which gives the public the right to know and prevent how their data is being handled.

Miller & Smith (2022) in [24] cover more of the legal issues regarding Facial Recognition Technology, covering much of the same ground but adding more valuable detail to flesh out the subject. As they state, Ethics and Politics are always linked, so any ethical issue should also be regarded as a legal issue, and vice versa.

The pair discuss the precedented legal trouble Facial Recognition has already caused authorities in the United Kingdom (UK) and United States of America (USA). Law enforcement had hired the use of Clearview AI, which scraped over three billion facial images from social media to build a database for future Facial Recognition. This was all done of course without the consent of tens of millions of victims, which seems to be a repeated pattern throughout the use of this technology. This information was used in part in CCTV feeds for real time identification of members of the public, and could be used in conjunction with other forms of collected data (like phone metadata, internet history, location tracking, etc.) to build a complete picture of an individual's moves, lifestyle, and personality. Clearview AI was served with cease and desists from Facebook and Twitter after it was proven the company had violated the privacy policies of the respective websites. Furthermore, a class action lawsuit has been underway against Clearview AI by the law firm Haeggquist and Eck, aiming to compensate all the victims of the company.

Figure 2.8: Facial Recognition incorporated into CCTV in China (Cardia et al. 2022)

Almeida et al. (2021) in [5] serves as a much lengthier paper on the ethics of facial recognition. The authors how Facial Recognition Technology (FRT) must balance an individuals' privacy rights versus the accuracy of the system. Governments are under constant pressure to keep the populace safe, which is often achieved through new technologies, such as CCTV, drones, automated systems, and now Facial Recognition. However, each of these technologies encroach on civilians' privacy, which can affect the public's relationship to the government. This boundary has been pushed further than ever before due to the Covid-19 Pandemic, which saw the public giving up much of their privacy and autonomy through widespread use of tracking applications such as the Malaysian "MySejahtera" or the United Kingdom's "NHS COVID-19 APP". This was done for the purpose of public safety and prevention of this deadly virus, however, has only added to the precedent of the removal of citizen's privacy. The authors state that this invasion will only continue, and that unconsenting Facial Recognition is likely to be a major part of the general public's life's from now on.

Almeida et al. (2021) also agree with the core issue other researchers brought up, being the lack of consent, going further to state that this breaks the General Data Protection Act (GDPR). This law gives the public the power to have control over how their data is processed and stored, which is ignored by Facial Recognition Technologies. The researchers add the fact that Article Nine of GDPR details how biometrics, like fingerprints/DNA/Facial Scans, are not to be used to identify someone unless explicit permission is given or with special exemptions (suspect is a criminal or terrorist).

Facial Recognition has also been known to have a racial bias, particularly towards women of colour, as found by the National Institute of Standards and Technology (NIST). A false positive recognition in the scenario of identifying criminals can lead to innocent people receiving unwarranted stress and negative attention, which would adversely affect already oppressed minority groups due to the racial bias. The author states that a success rate of 99.92% is considered perfect when in regard to Facial Recognition, yet in any large city this would lead to thousands of potential matches, showing the flaws in the technology when it comes to larger scales.

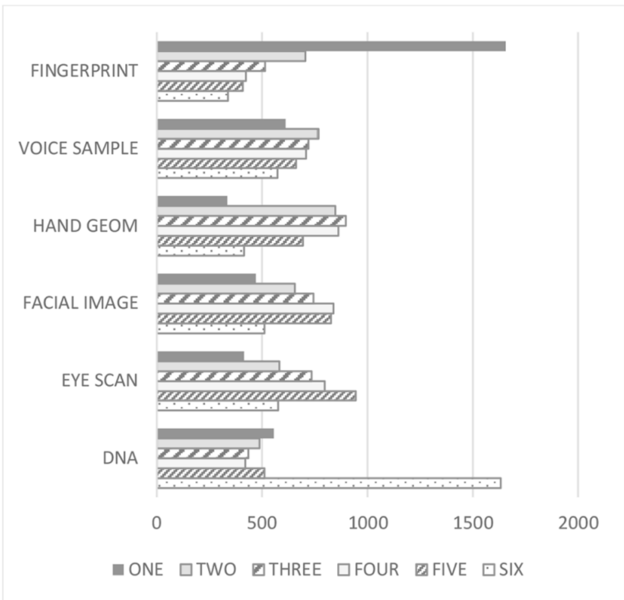


Figure 2.9: U.S. adults' ranking of comfort with six types of biometrics. One is the most comfortable ranking, and six is the least comfortable ranking. (Anderton et al. 2022 in [3])

Anderton et al. (2022) in [3] emphasises the importance of collaborators to researcher, having ten authors in total, and had the best paper on the subject of opinions towards Biometrics by conducting a survey of over four thousand adults. The authors agree on the racial discrimination that Facial Recognition is known to have, and state that minority groups also distrust this form of biometric identification more than others surveyed. Figure 2.9 shows the results of one of the survey questions, displaying the trust associated with each form biometric. The graph shows that facial recognition is right in the middle of trust or distrust, meaning that it is the most invasive form that Governmental bodies and Organisations can get away with, otherwise members of the public would likely protest.

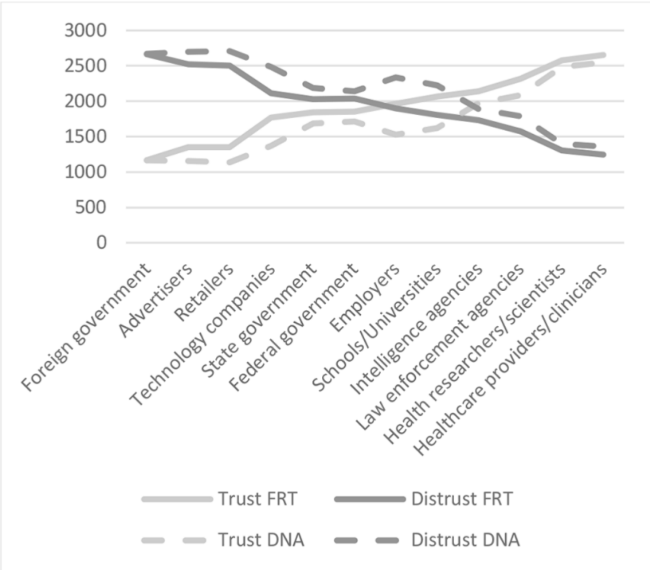


Figure 2.10: Trust of different social actors using Facial Recognition Technology and DNA, from the least trustworthy to most. (Anderton et al. 2022 in [3])

Figure 2.10 shows the trust associated with different social actors, which helps illuminate the public's disposition towards the technology in different hands. Further surveying from the researchers showed that the public were fine with Facial Recognition being used to assess security threats in public, such as potential terrorists or dangerous criminals. This does not solve the previously discussed issues associated with public Facial Recognition, making the trade-off between enhanced security versus privacy, fair treatment, and anonymity. The authors claim the findings are unremarkable, but this is far from the case, as it shows the general public opinion to this technology, whilst also highlighting the natural contradiction of its usage. It appears that the public are in favour of Facial Recognition, but not the organisations using it, such as large tech conglomerates or Governments. This paper is an excellent piece of research that has helped form the core questions of this project.

Almeida et al. (2022) in [5] brings up further the fact that Facial Recognition has a repeated racial bias throughout its history. This unfortunately correlates with law enforcement's infamous discrimination of minority groups, making one of the core use cases for Facial Recognition Technology unintentionally add to the deep-rooted issues seen in modern policing. Algorithms have no accountability when it comes to false positive recognition attempts, which could lead to more wrongful arrests of minority groups and to a greater loss of trust for the government. The researchers state that this problem generally arises due to White men dominating the field of tech, leading to a neglect of testing and building Facial Recognition algorithms to work better with minority groups.

The authors conclude their paper with a set of ten ethical questions regarding Facial Recognition Technology (FRT), which are:

1. Who should control the development, purchase, and testing of FRT systems, ensuring the proper management and processes to challenge bias?
2. For what purposes and in what contexts is it acceptable to use FRT to capture individuals' images?
3. What specific consents, notices and checks and balances should be in place for fairness and transparency for these purposes?
4. On what basis should facial data banks be built and used in relation to which purposes?
5. What specific consents, notices and checks and balances should be in place for fairness and transparency for data bank accrual and use, and what should not be allowable in terms of data scraping, etc.?
6. What are the limitations of FRT performance capabilities for different purposes, taking into consideration the design context?
7. What accountability should be in place for different usages?
8. How can this accountability be explicitly exercised, explained and audited for a range of stakeholder needs?
9. How are complaint and challenge processes enabled and afforded to all?
10. Can counter-AI initiatives be conducted to challenge and test law enforcement and audit systems?

Almeida et al. (2021) paper is an excellent overview of Facial Recognition Ethics, and really highlight how the issues with the technology has still not been resolved. The points addressed effectively give the reader the key issues whilst the series of ethical questions set the stage for future improvements to Facial Recognition when privacy laws catch up, that is if they ever do.

Unfortunately, the legal issues seen in the USA and UK are not the worst case example of Facial Recognition misuse, as the researchers go on to discuss further details surrounding China and their Social credit system. Facial Recognition is widespread through the state surveillance system, monitoring the populace at all times to keep them on best behaviour. Low level crimes such as jaywalking are caught and punished using the technology, and even harmless actions like wearing pyjamas outside can lead to public shaming. The key issue is that this technology is enabling the government to further oppress their population, as bad credit scores can lead to a number of restrictions. Civilians can lose access to private institutions like hospitals or well respected schools, be denied promotions, and can even be banned from leaving the country.

Miller & Smith paint a very dystopian view of Facial Recognition Technology, and how in the wrong hands can be greatly used to oppress innocent civilians. The authors give great detail on the topic compared to similar papers reviewed, with the added legal discussion really adding to the overall point of the document. The pair conclude on the question of whether it is acceptable to collect biometric data from civilians who have not committed any crime? as the technology becomes more widespread, what measures should be put in place to avoid an Orwellian nightmare.

Kasthuriarachchi et al. (2021) in [19] covers a very similar topic, with slightly more focus on the effect masks can have on facial recognition, covering some of the issues already discussed. A key point brought up by the researchers is the right to anonymity, which Facial Recognition stunts somewhat. Members of the public have the power to turn off location tracking, cookies, and other intrusive services on their devices, but cannot get rid of state mandated Facial Recognition, as employed by the Chinese Communist Party (CCP). Facial Recognition cameras have been erected all around mainland China, creating a surveillance state, much the panopticon, where prisoners can never tell if they are being watched by guards and so must always behave just in case. The researchers state that Law enforcement has repetitively mistaken innocent people for criminals through the use of facial recognition, and that the technology presents a significant risk of being a tool for oppressive regimes all around the world.

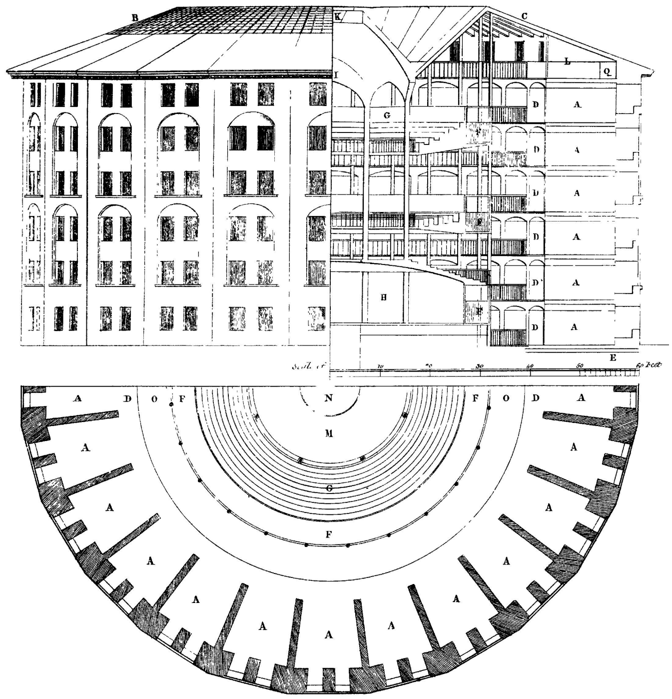


Figure 2.11: Panopticon Prison Design, similar to state wide Survielance seen in China (Shone, 2013)

Interestingly, Cornelis et al. (2008) bring up many of the same ethical issues of Facial Recognition as other more current papers did, primarily being the lack of consent from the user. User devices often have Facial Recognition built into the hardware itself, with little guarantee that images are being captured discreetly to be used as training data. Furthermore, there is never consent given for public Facial Recognition systems found in organisation's security system. The authors state that this will not change until laws are passed to protect the public's privacy regarding Facial Recognition.

This paper may be old, but as it regards ethics and issues it is more relevant to today's technology landscape than a paper simply discussing the general aspects of Facial Recognition. Additionally, the authors' suggestion that a law will pass regarding Facial Recognition privacy has not come to fruition, which makes the paper ever more relevant, as it shows the fundamental problems with the technology still have not been addressed correctly. Oddly, the paper ends on a happy note, suggesting that Facial Recognition "will improve the living standards of human beings", disregarding all the previous issues brought up in favour of the flawed optimism for the technology.

Overall, Facial Recognition looks like it is here to stay, and will only continue to get more advanced, as seen by the expression recognition in Mao et al. (2020). It is also likely that Facial Recognition will see larger incorporation into organisational security, replacing access cards and security cameras to better track employees and detect unauthorised intruders. This will likely take time, and cost a lot for the necessary upgrades, but still is a predictable future. Governmental bodies will likely also upgrade to Facial Recognition technology, firstly in important high risk areas (military compounds, Government buildings, National monuments) with further expansion later on to nationwide, as seen in China.

2.6 Additional Access Control Solutions

Chan et al. (2012) in [14] was discussed earlier in regard to the need for access controls in the first place. However, the researchers presented several alternatives to forms of Access Control, aiming to solve the issue of Tailgating, where a malicious actor will follow authorised users into restricted areas. This is an easy form of social engineering, as people will often hold doors open out of politeness, and will not risk denying entry to a potential authorised user. The researchers discuss a study where agents of the Federal Aviation Administration for the United States government were able to breach security of major airports by simply following airline and airport staff into restricted areas. The agents had a 68% success rate, which is incredibly worrying as US airports are notorious for their security, it is easily imaginable that standard businesses would have a much higher success rate.

Chan et al. (2012) discuss the use of turnstiles as a potential fix, where employees use Smart Cards or Biometric thumbprints to authenticate themselves. However, this is not achievable for all types of organisations, such as high speed environments like hospitals, where quick access to areas is needed in order to save lives, turnstiles would simply slow down essential workers. The researchers also present the use of cameras and machine learning to detect when too many people enter a restricted area without doing the proper authentication checks, showing the natural shift towards facial recognition as the new form of access control. Overall their research is excellent, with the team building a tailgate tracking system using a cheap IP camera, and backing it up with solid research into the field.

2.7 Physical Penetration Testing

It is not always the malicious actors wishing to exploit the Access Control measures of a business or organisation. Penetration testing is the art of simulating an attack to better evaluate the security of the target, normally in order to find and fix issues that could be exploited by a malicious party. This large area of Information security began from Military operations in the Cold War, where United States Governments would create and hire “Red Teams” to try and break into restricted facilities as the Soviets would.

Craft. (2017) in [16], in their paper on the future of Red teaming test, details how Red team Penetration tests incorporate many different tools and techniques to properly test the security of a client. The tester uses methods like Social Engineering, Digital Attacks (like phishing), and even through Access Control exploitation. The researcher states this can be as simple as using lock picking kits to hijacking security cards. Physical Security is a large part of Penetration tests, as once a malicious actor is within the network, it is a lot easier to launch attacks. Craft. (2017) presents an interesting history of the Art of Penetration Testing, and discusses how future technology like IoT devices will affect security. Although this is valuable research in its self, it was not deemed in scope for this project, and is disappointing that the author did not cover Smart Cards or Facial Recognition in any regard. This is an obvious gap in research, as other papers have stated how these forms of Access Control seem to be the go-to option for present and future security.

It is very important for an organisation to test and secure their Access Control methods, a point that Craft. (2017) and Carreira et al. (2020) both agree on. Carreira et al. (2020) present an excellent paper on practically exploiting the Smart Card system found at the researchers’ university in order to recommend fixes for the future. The authors presented several of the already discussed vulnerabilities of, such as skimming, but decide to take it a step further and build a model to harvest

Smart Card information. Using a Raspberry Pi Zero, the authors managed to intercept the User IDs from the Smart Card scanner and store them, which could be used later for cloning cards. The final product worked excellently, and was an excellent proof of concept of how cheap hardware can lead to organisation wide exploitation. This all shows how important Physical Penetration Testing is for a SOC team to incorporate, as insecure Access Control could be the Achilles Heel for their client.

2.8 Expanded Problem

From the research review, it is clear that Access controls are incredibly important to a functioning Cyber defence. Without adequate controls put in place, an organisation could suffer from serious damages that could cause massive losses or even bankruptcy. The research also shows the gradual shift from physical Smart cards to more biometric based authentication, such as thumbprints unlocking E-Wallets or Facial Recognition cameras. Only large organisations or Governments can afford this new technology at this time, but it is likely that over the next ten years these biometric access controls will become more common, as they become cheaper whilst providing better security.

The research also revealed a gap in literature, as no authors made significant attempts to bypass these Access controls in order to learn more about their limitations. The standard practise of Penetration testing is used to find vulnerabilities in a network before a Malicious Hacker can, so why is not the case that these industry experts aren't diving into physical security exploits to find weaknesses in this critical area of Cyber defence.

Sun Tzu said "Knowing the enemy is half the battle", which serves as the basis of this project. A malicious actor will use all their power to bypass Access Control Measures like Smart Card Scanners, knowing what methods they are likely to use and how they would be set up will serve as excellent research into how a SOC team can prevent this attack from occurring in the future. Testing Smart Card systems is the only way to understand them properly, aiming to gain illegitimate access and possibly even a skeleton key to a facility will effectively show the current state of Smart Card security and highlight the changes that need to be made.

Figure 2.12: Facial Paint to avoid Facial Recognition Technology (Ferrari, 2020)

As Facial Recognition grows and looks to be a market leader in Access Control, it is important that research be conducted into the various security concerns it raises. From the research, it is clear that the technology has a lot of issues regarding ethics and privacy, leading to many legal cases and protests against it. To a Malicious Actor, Facial Recognition serves as a thorn in their foot when trying to gain illegitimate access to a building. Many papers discussed that members of the public wish to avoid Facial Recognition Cameras, but none actually listed effective methods of doing so. There are already methods used in real life scenarios, such as protesters at the Hong Kong Riots using face paint to trick cameras or facial coverings (Ferrari, 2020). No papers mentioned these techniques, so it is an important area to research, alongside some other new methods.

Furthermore, a Malicious actor is likely to use facial coverings to avoid cameras without drawing suspicion. Knowing the most effective everyday solutions to prevent recognition is crucial for SOC teams to know and understand. Seeing a suspicious individual consistently wearing effective and subtle coverings (such as sunglasses/baseball cap/face mask combination) could aid Security teams in profiling a Malicious Actor before any harm can be done. It is interesting to find out what is the minimum covering can be used to prevent Recognition whilst drawing the least suspicion from the general public.

Therefore, this project will aim to cover these gaps in literature to find the flaws found in current and future Access Control so that SOC teams can better understand them and build them back up for stronger security in the future.

Chapter 3

Methodology

This section will cover the various aspects to the actual methodology of the project, covering how it will be designed, tested, resources needed, and any risks that might be faced.

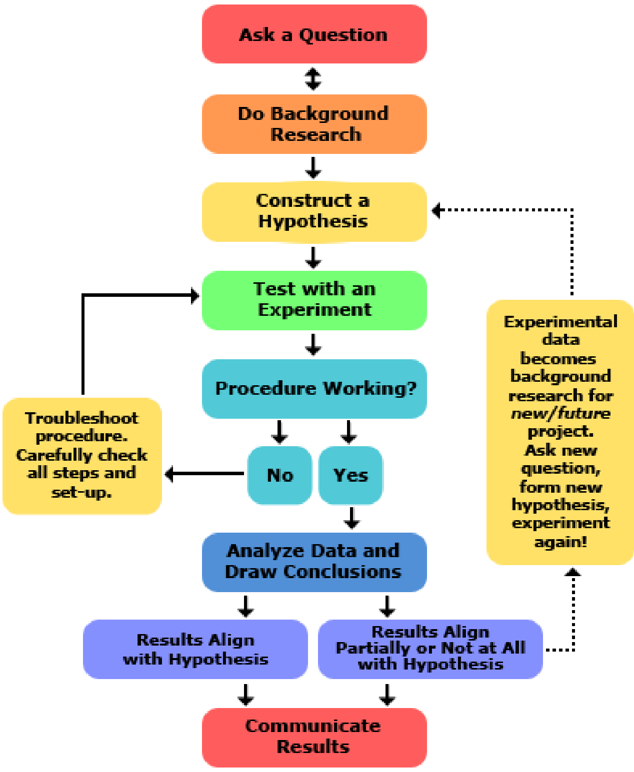


Figure 3.1: Scientific method used for the Propose Project (Science Buddies, 2013)

3.1 Design Approach

The nature of this project is more experimental than a traditional development project, so the typical design methodologies could not be used effectively (like Waterfall design). Instead, the Scientific method has been selected as the design approach for this project, as it focuses on asking questions to then test with experimentation. This is perfect for the chosen project, and the thorough flow chart seen in Figure 3.1 show each step of the design method. Furthermore, the Research Questions formulated make the perfect input for the Scientific method, allowing easy development suited to the requirements of the proposed project.

3.2 Resources

For resources, the main items needed will be various Smart Cards and readers to test with, as seen in Figure 3.2. These can both be bought for reasonable prices from various online stores (Alibaba, Shopee, EBay), and existing cards for real world use (i.e. apartment resident cards) that can be used as a guideline. Software to read the cards will also be required, luckily there are various options, such as ACS solutions and the smartcard linux tool (ACS, N.D.). Abellon et al. (2021) also discussed several tools that can be used for this purpose, showing the existing research into this topic.

Figure 3.2: Various Smart Card readers (GeniSoftware, N.D.)

Facial Recognition is much easier, as many commonly used items like mobile phones have the technology built in. Further testing can be done with Amazon Web Service's (AWS) Facial Rekognition, which is a multipurpose tool for the subject, and can give more accurate results. A final option could be the Facial Recognition resources found on campus, as Asia Pacific University used the technology for a time to authenticate students. It is reasonable to presume that this resource would be available for the planned experiments. Facial Recognition might require some more cosmetic resources in order to avoid detection, such as face paint and masks, but these are easy to acquire.

The final resource needed will be existing research, which will be primarily retrieved from Academic sources such as the Institute of Electrical and Electronics Engineers (IEEE) or the Association for Computing Machinery (ACM). Non-Academic articles will also be reviewed for finding more methods of exploitation and experimentation as well, so that the project has a broad scope of research behind it.

3.3 Testing Plan

The aim of this project is to find out whether these physical security methods that are entrusted are actually safe or not. The testing will aim to find Qualitative results, as it is more about finding key issues in the technology rather than a large amount of small ones. The research will also be far more action focused, as the aim is to improve the knowledge of the technology for the use of an SOC team, and therefore improve the field of Information security. As this is experimental research testing occurs throughout the entire project, however, the final products will be tested through two mediums.

At the end of experimentation, there will hopefully be a couple methods to bypass Smart Card access control, which then can be officially tested against various consenting security systems to see if the exploit is universal or not. This will aim to see how potent the Smart Card exploitation is, with variables like how the success rate and the complexity of the solution. The same will go for Facial Recognition, using the various prevention methods against various systems, such as Phone Face ID, Amazon Rekognition, and even official systems found on campus (if permitted). These tests will evaluate how effective a malicious actor would be using the found techniques in a real world scenario, thus showing the weakness or strength of physical security.

This testing was deemed sufficient for the actual exploits themselves, but a further test has been planned for the usability, aiming to get the public's insight on the research. An exploit could break past physical security mechanisms 100% of the time, but would not be usable if the Malicious actor would need to use a large device in place of a Smart Card or have to wear a something outrageous on their head to avoid Facial recognition cameras (like a bank robber using a Halloween mask). The various methods acquired would be presented to the reader, and asked if they would find it suspicious if someone was using it in a real world scenario. This would allow the methods found to be properly evaluated as to find the most viable threats to physical security. The grouped surveyed will not be exceptionally large, as the feasibility of doing this is not possible due to the researcher's lack of reach to gain large amounts of data. This means the analysis of the data collected from surveying will have to be Inferential analysis, applying the results from the sample size to the population.

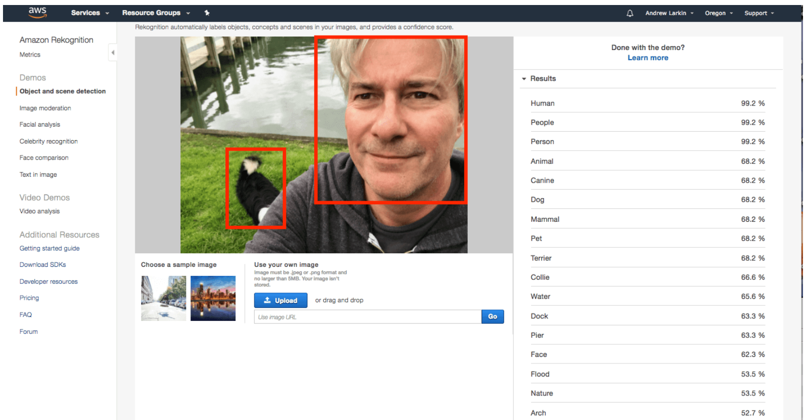


Figure 3.3: AWS facial Rekognition (Larkin, 2017)

3.4 Research Plan

To show the research plan for the project, a Gantt chart has been constructed, seen in Figure 3.4, showing the flow of research and experimentation planned for the project. The Gantt has also been categorised into three distinct sections to better manage the stages of the project life cycle, being "Research Stage", "Experimentation Stage", and finally a "Testing and Write up stage" to wrap up the project. The time allocated for each task has buffer time included to simplify the graph, but the rule followed is that for every five days dedicated to a task, an additional two is assigned as buffer (majority of tasks have ten days assigned and four days of buffer).

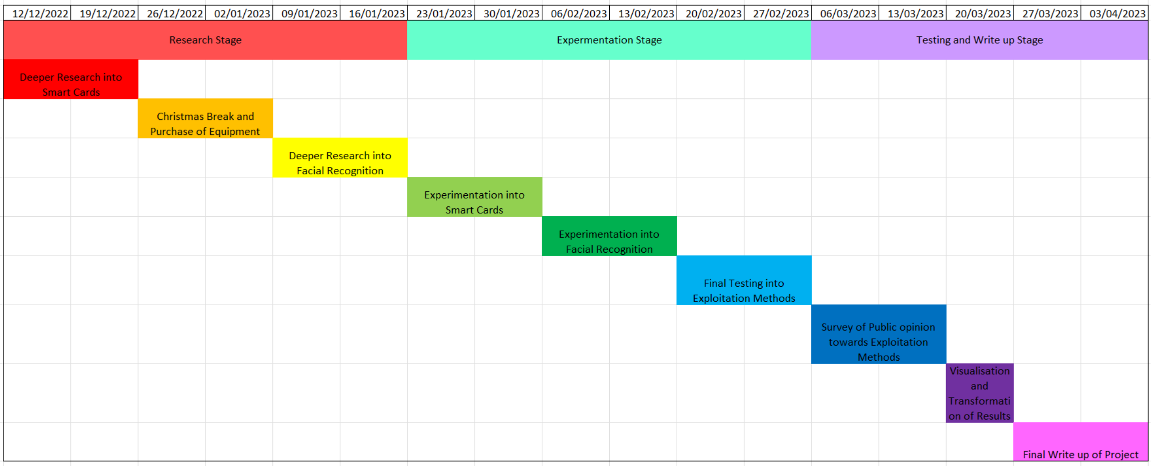


Figure 3.4: Gantt Chart for Project

An additional view of the Gantt was also constructed to give a better picture of each week's responsibilities to the project. This can be seen in Figure 3.5.

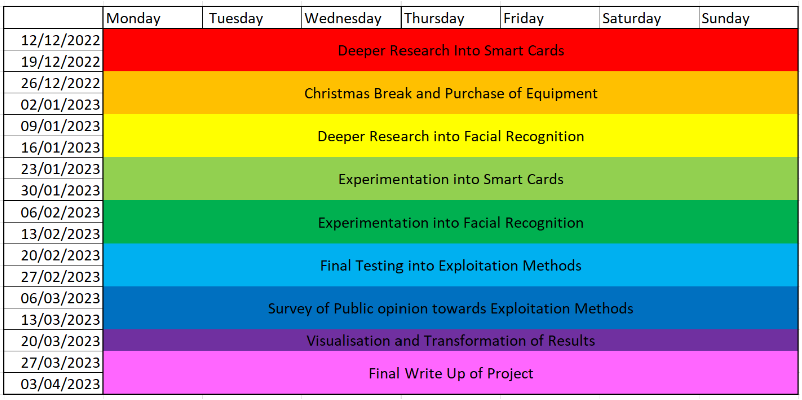


Figure 3.5: Gantt Chart for Project

3.5 Risks

This project does not come without its risk, and it is important to address and put forward mitigation plans now to avoid them causing issues later in the research. Several Risks have been identified, which could majorly interrupt the project if mitigation plans are not followed.

- **R1: Unrealistic Time Estimates**
  - The Risk of unrealistic time estimates being allocated to each task discussed in the Gantt chart, leading to areas lacking in research and experimentation due to the delivery date shifting.
  - This is mitigated through the Gantt chart, as plenty of time has been given to tasks with buffer periods as well. The researcher will also organise bi-monthly meetings (which will transition to weekly as the delivery date draws nearer) with the project supervisor to motivate giving regular updates and avoiding procrastination.
- **R2: Hardware/Software Failure**
  - The main tools of research will be physical scanners, Facial recognition cameras, and of course a laptop to use for exploitation and to record results. There is the risk that any of these pieces of hardware fails, causing loss of progress and possible delays to the Gantt chart. Additionally, there is the risk that software used stops working, which is much harder to remediate, leaving experimentation unable to continue.
  - This can be mitigated through the use of backups, that will be stored in various places, such as a Google Drive folder and an external hard drive. The software mitigation is harder, but can be remediated through third party or competitor options if the primary option stops working. There are also many computational resources in the University Campus that the researcher has access to if the laptop used for the project abruptly stops working. The project is also being written up in Overleaf, which is an online TEX editor, meaning if hardware failure occurs there will be no loss to any written progress.
- **R3: Act of God**
  - There is always the risk in any project that an event outside the researcher's control occurs which might cause progress to slow down or even cease completely. An Act of God could take the form of a natural disaster, Governmental issues, or a global pandemic.
  - There is very little ways to mitigate this risk in any practical way, other than having a stable working environment and a backup plan. The researcher for this project is an international student, meaning there is always the potential to move away if this risk occurs, so work can continue in a new setting. As shown by the risk matrix, this risk is far less likely than others, so does not need drastic measures to mitigate it (such as building a bunker for protection).
- **R4: Ethical Issues**
  - As the project relates to the exploitation of physical security mechanisms, there is the risk that research and experimentation could breach ethical concerns. Testing solutions on systems without consent could see the project thrown out.
  - This is mitigated through the primary research being conducted on scanners and virtual systems owned by the researcher, and any further research being only on consenting systems, thus avoiding any ethical issues.

- **R5: Failure to Produce Results**
  - There is a concern that the researcher will not produce any interesting results, failing to exploit either form of access control and finding no weakness. This could lead to a rather disappointing final product.
  - This is hard to mitigate, however, significant time has been dedicated to each section of experimentation, giving the researcher the best chance to fully explore the subject without concern. Additionally, as this project relates to security it would not be a terrible outcome if these Access controls are found to be too secure to break, as it would prove that any concern for physical security is unfounded, making the research still valuable.
- **R6: Malicious use of Project Research**
  - Similar to R4, there is the risk that the project results could be used by a Malicious Individual to exploit real businesses, which would only worsen the problem that this project is trying to address.
  - To mitigate this risk, all project sensitive details and research will be kept private, through use of locked storage. Additionally, research is only being conducted in an educational sense, and will not be published to a wide market where it could be used by a Malicious actor.

These risks have been visualised in the form of a Risk Matrix, as seen in Figure 3.6. This shows the main issue to be mindful of throughout the project will be time estimates, so particular attention will be focused on avoiding procrastination.

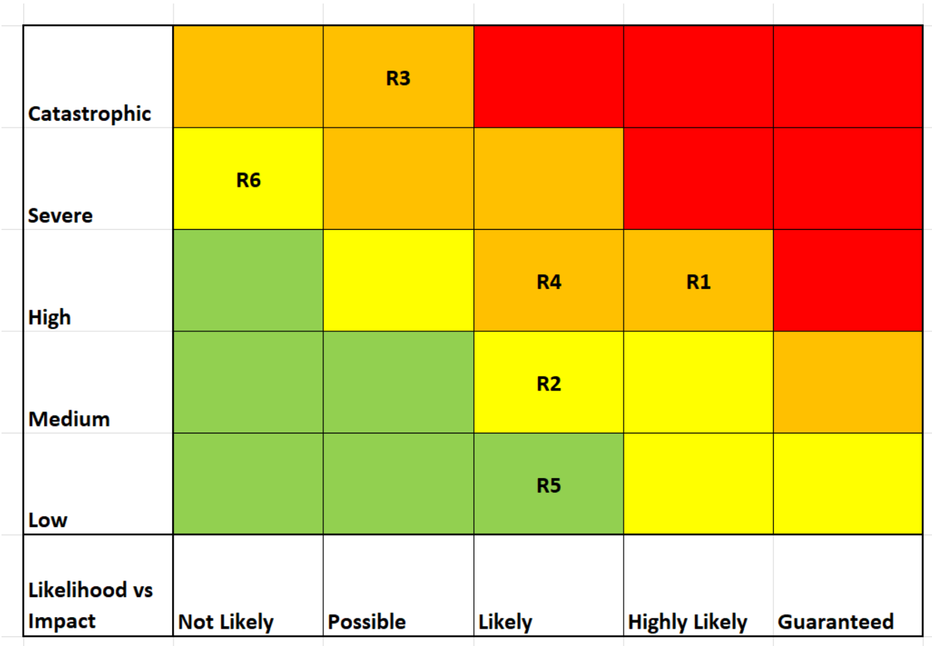


Figure 3.6: Risk Matrix for Proposed Project

Chapter 4

Procedure

This chapter covers the

4.1 Building of Experimentation Environment

Several testing grounds were needed to properly research Smart Cards and Facial Recognition Technology, otherwise this project would only result in hypothetical answers. Three different environments were utilised as part of this research, which are as follows.

4.1.1 Arduino Environment

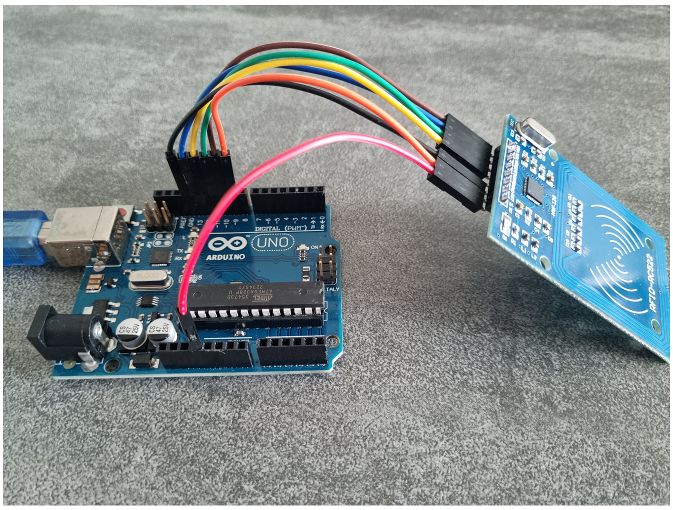


Figure 4.1: Arduino wiring to RC522 reader

A home system was always intended to be built for the sake of research and learning the intricacies of Smart Card technology. Arduino was the leading choice for an at-home system, as kits have everything needed to create RFID scanners at an affordable price. Additionally, as the environment was primarily hardware based the advantages that Raspberry Pi boards present (faster processing, independent Operating System) were not relevant to the rather simple nature of RFID technology.

The MFRC522 library is specially designed to work with Arduino boards and RFID technology, and was used to build the at-home system. The kit purchased contained an Arduino Mega 2560 board (which was later changed to Arduino Uno board due to hardware failure), all the wires necessary, and the RC522 RFID based reader, as well as all the Smart Cards required. The RC522 reader first needed to be soldered before use, using the documentation (Balboa, 2021) the circuit was constructed as seen in Figure 4.2.

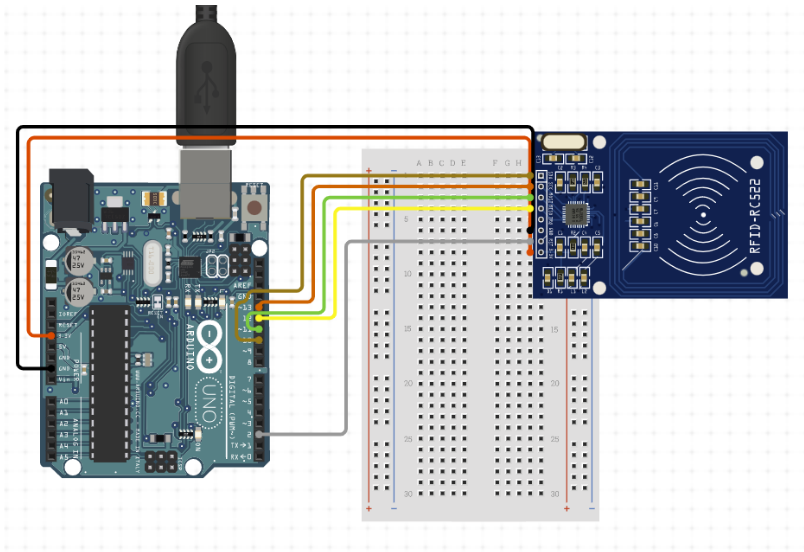


Figure 4.2: Arduino Circuit Diagram

A simple RFID scanning program was then written in the Arduino editor, the full code can be found in Appendix A. Once the various components are initialised the board will wait until a card is scanned, before sanitising any input (as only the User ID is needed from the card) and normalising it for verification.

```
//Contantly checks for a card to read
void loop() {
  if ( ! mfrc522.PICC_IsNewCardPresent()) {
    return;
  }
  if ( ! mfrc522.PICC_ReadCardSerial()) {
    return;
    }

  //prints once a card is read
  Serial.println(F("Scanned UID:"));

   String content= "";
   byte letter;

   //Input from reader needs to be sanitised before use
   for (byte i = 0; i < mfrc522.uid.size; i++)
  {
     Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
     Serial.print(mfrc522.uid.uidByte[i], HEX);
     content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
     content.concat(String(mfrc522.uid.uidByte[i], HEX));
  }
```

Figure 4.3: Arduino Code showing

The input is then compared to all the authorised User IDs, which at this stage were stored through a simple array of data. The program would display if the attempt was successful or not, before resetting for the next user, as seen in Figure 4.3.

```
  Serial.println();
  content.toUpperCase(); //More sanitisation
  int approved = 0; //To indicate if they are allowed access

  //Cleaned variable is compared against an array of User IDs
  for (int i = 0; i < 2; i++){
    if (content.substring(1) == UIDs[i]){
       Serial.println("Authorized access");
       Serial.println();
       approved = 1;
      }
     }

  if (approved == 0) {
    Serial.println("Accessed Denied");
    Serial.println();
    }

  //Cleanup, resets the reader for new entry request
  Serial.println("");
  mfrc522.PICC_HaltA();
  return 1;
}
```

Figure 4.4: Arduino Circuit Diagram

4.1.2 Real Life System

Originally the Real Life systems were planned to be through the Smart Card systems found in Asia Pacific University and the researcher's Residential building, this was to provide validity to results found on home systems. Unfortunately, access was reasonably denied to both options, leading to no way to verify results on a real system. This was rather limiting to the overall project, so to mitigate this somewhat, the components to a real life system were purchased and constructed independently.

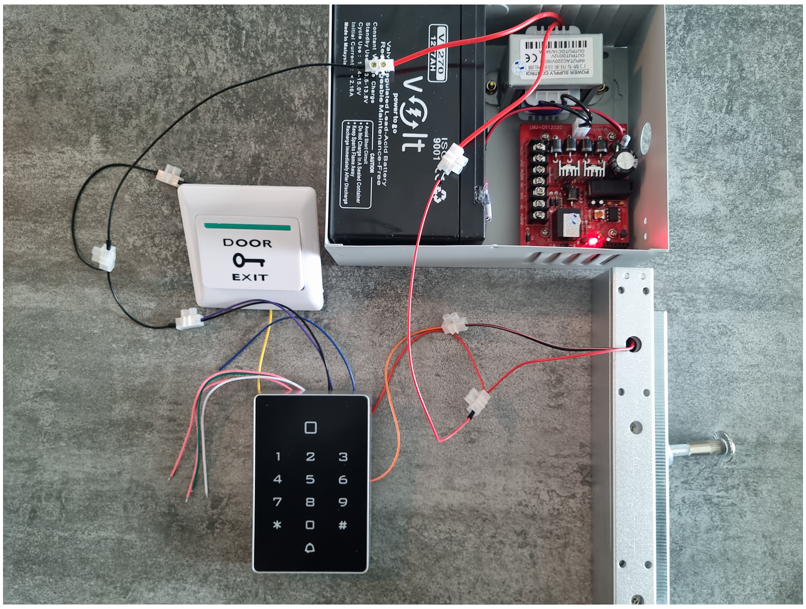


Figure 4.5: Wiring of Physical System, with all components of a typical door Access Control

The items purchased were of the same make and model as ones found in typical residential buildings to have as realistic of an environment as possible. The physical system can be seen in Figure 4.5, fully operation (as indicated by the red LED) after wire stripping and connect with chocolate blocks. The items purchased were:

- **RFID keypad -** This keypad featured the standard RFID technology necessary for Smart Cards (of a 13.56 MHz frequency) Access Control. This option was also selected as the entire database of user IDs are actually stored within the board itself rather than a back-end server. This decentralised system is rather popular in scenarios where security is not as tight and is more important for the system to work out of the box, such as residential buildings, whilst centralised systems are often seen in large businesses.

- **Exit Button -** A Standard Exit Button was also purchased to be added to the system, firstly to test if other components worked, and secondly to complete the circuit as per the keypad's instructions.

- **Magnetic Door Lock -** A Magnetic Door Lock was also needed for the circuit, and is an effective tool for visualising successful entry attempts.

- **Power Supply -** Finally, a 12 Volt power supply was needed to power the entire circuit. It is likely that in a Real Life System the power would come from the electrical mains, but this also served as a good option.

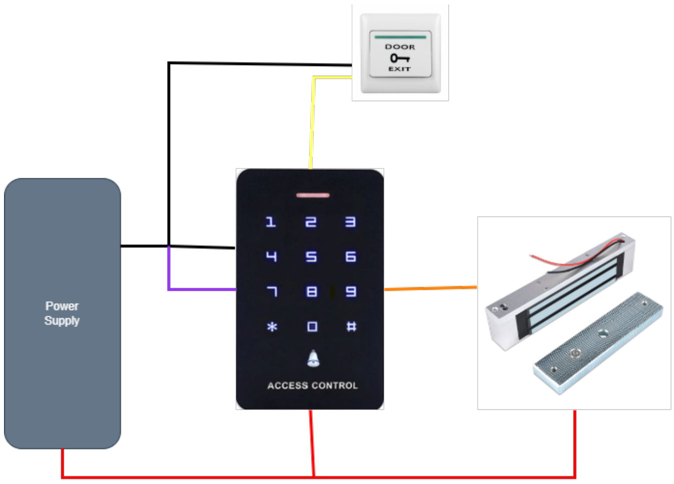


Figure 4.6: Circuit Diagram for Real Life System

The circuit was built using manufacturer's instructions, connecting all the wires correctly using chocolate block connectors. The full circuit diagram can be seen in Figure 4.6, showing that the majority of Real Systems are rather simple when it comes to hardware, the only unknown complexity could come from back-end server connection.

4.1.3 SQL system

Later in experimentation it became clear that a more advanced form of Smart Card scanning system was needed, not only for specific tests but also for replicating how a real system would work. The basic Arduino solution stores card entries in code, which goes against security standards, as any new users or edits to credentials requires redeploying source code with changes. Additionally, anything in source code is seen as public and plaintext, which is not the worst case for Smart Cards, but when it comes to more sensitive data like passwords it is far better to store it somewhere else.

```
MariaDB [rfid]> insert into cardID(cardNumber) values('73f60c0e');
Query OK, 1 row affected (0.001 sec)

MariaDB [rfid]> select * from cardID;
+----+------------+
| ID | cardNumber |
+----+------------+
|  2 | 73f60c0e   |
+----+------------+
1 row in set (0.000 sec)

MariaDB [rfid]> 
```

Figure 4.7: Final Database for RFID scanning

This led to the creation of a simple secure Python3 program using MariaDB as the database, all built and run within a Kali Linux Virtual Machine. The database was set up with one table named “cardID”, which had two columns, being “ID” and “cardNumber”. The value for the testing card was then added to the Database as seen in Figure 4.7 with the ID automatically incrementing.

```python
from time import sleep
import string
import mariadb
import sys
import textwrap


#Connecting to Database
try:
    conn = mariadb.connect(
        user="your-username-here",
        password="your-password-here",
        host="127.0.0.1",
        port=3306,
        database="your-database-here"
        )
except mariadb.Error as e: #Catching Errors
    print(f"Error connecting to MariaDB Plaftform: {e}")

#Connection to use later
cur = conn.cursor()
```

Figure 4.8: Setting up Database Connection in Python

The python code was then written, which firstly had to connect to the database using the `mariadb` library. All the data needed, including username, password, and database name was used to connect to the database, whilst catching any errors with a `try except` block, as seen in Figure 4.8.

The code then constantly waits for a card to be scanned from the user, and converts the value given from the reader to the proper hex value (due to a quirk of the reader that will be discussed later). The database is queried for any matches relating to the card's User ID, returning a result if there was, and nothing if it wasn't found, as seen in Figure 4.9.

```
#Main Code runs continously
while True:
    #Takes in Decimal Card Number from Scanner
    scannedCard = input("Scan Card to Begin: ")

    #Verifying that card has scanned
    if scannedCard != None:
        #Convert from Decimal to Hex
        hexValue = hex(int(scannedCard))
        correctHex = hexValue.replace('x', '') #Remove
        splitValues = textwrap.wrap(correctHex, 2)#Split Hex into pairs
        #Rearrange Hex pairs to true value(e.g. OE OC F6 73 to 73F60C0E)
        orderHex = splitValues[3] + splitValues[2] + splitValues[1] + splitValues[0]

        #Query Database using new value
        cur.execute(
            """SELECT ID from cardID WHERE cardNumber = '%s'""" % orderHex
            )
        #Returning any matches
        foundInDB = cur.fetchone()
        if foundInDB != None: #If there was a match
            print("Access Granted")
        else: #If no matches were returned
            print("Access Denied")

        print("Finished Operation")


    sleep(0.5)
```

Figure 4.9: Repeating Code for Scanning and Verifying Cards

Figure 4.10 shows the program in operation, successfully authentication a card found in the database, and denying an unknown card. This program is an effective form of Access Control whilst maintaining secure coding practises.

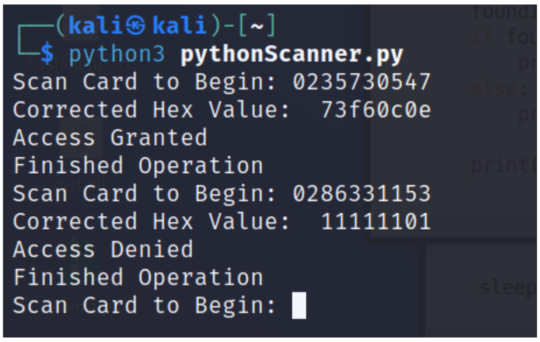


Figure 4.10: Code successfully working, allowing access to approved card whilst denying other cards

4.1.4 Facial Recognition using Python

There are many options for Facial Recognition available in the modern technological landscape, varying in effectiveness and ability. For this research it was deemed that three unique Facial Recognition Algorithms should be used, each varying in scope and ability, to give a clearer picture when it comes to testing. Commercial grade Facial Recognition would not fit the scope of a "Low-Level Algorithm", so instead one was written for this project. The code was written in Python 3 in the text editor PyCharm(Due to developer preferences), primarily using the OpenCV library, which focuses on computer vision and has options for Facial Recognition.

```
import cv2
import pickle

#Setting up
video = cv2.VideoCapture(0)
box = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")
recognise = cv2.face.LBPHFaceRecognizer_create() #Face Recogniser Setup
recognise.read("faceLabels.yml") #Loading labels

# Creating the Label Array
labels = {}
with open("labels.pickle", 'rb') as f:
    og_label = pickle.load(f)  ##
    labels = {v: k for k, v in og_label.items()}  ##
    print(labels)
```

Figure 4.11: Circuit Diagram for Real Life System

The full code for both programs can be found in Appendix A, initially the Webcam for the device is set up, before loading an external file that displays a box around any face found on screen. The recognition functions of OpenCV are loaded, as well as the labels for each authorised face (which will be created later).

```
# Main Operation
while True:
    check, frame = video.read()
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY) # Switch frames to Grayscale for easier computation
    face = box.detectMultiScale(gray, scaleFactor=1.2, minNeighbors=5) # Placing a box around any Face found

    for x, y, w, h in face:
        face_save = gray[y:y + h, x:x + w]

        # Taking the face and seeing if it matches any saved
        ID, conf = recognise.predict(face_save)

        # If the confidence is high enough then identify them
        if conf >= 50:
            print("Face Recognised as ", labels[ID])
            # Display user name and a green box
            cv2.putText(frame, labels[ID], (x - 10, y - 10), cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2, cv2.LINE_AA)
            frame = cv2.rectangle(frame, (x, y), (x + w, y + h), (0, 255, 0), 4)
        else:
            print("Not Recognised")
```

Figure 4.12: Circuit Diagram for Real Life System

The video is constantly monitored in greyscale, as it easier to compute and better for 3D mapping when it comes to recognition. Once a face is detected, the `predict` function is used to see if it matches any authorised users. The confidence is then used to determine if it is a match, if successful the user's name will appear above the box highlighting their face, as seen in Figure 4.13.

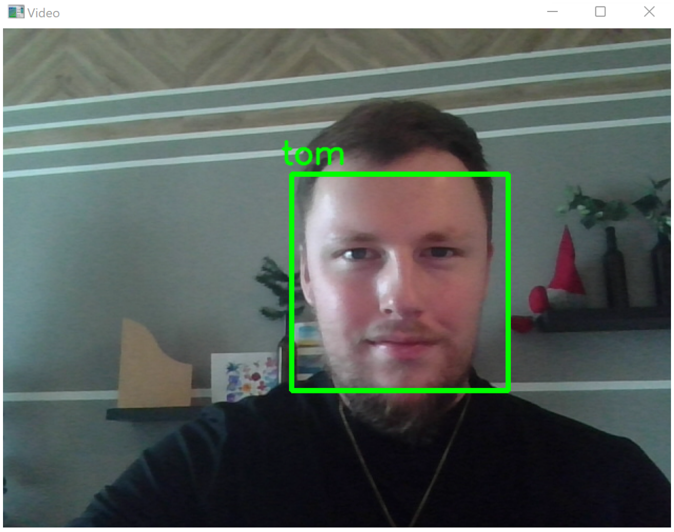


Figure 4.13: Python code successfully recognising a user

The labels used to identify a user were created with a different Python program, still using OpenCV, but first images were needed of any user wishing to be identified by the program. Twenty-five were collated and added to a folder in the program files, as seen in Figure 4.14. The code was also written to be able to expand for multiple users, all that would be needed is a similar amount of pictures in a separate folder.

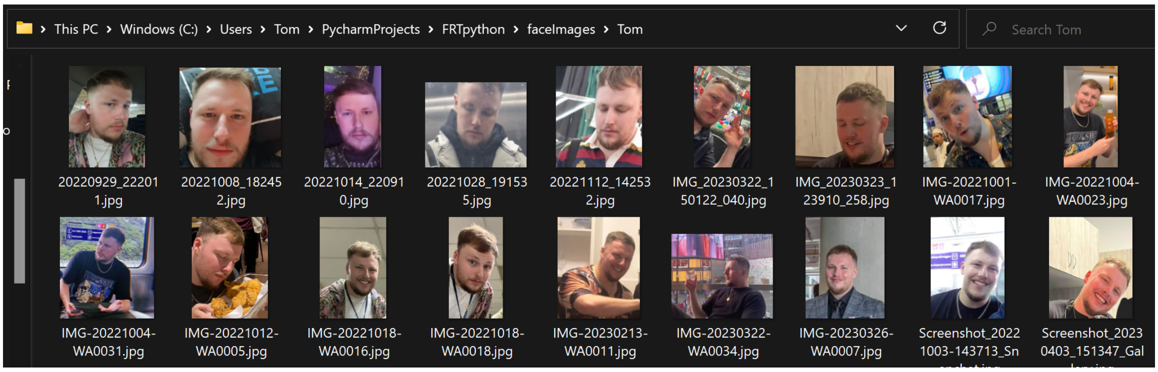


Figure 4.14: Images needed to build labels

The code was developed using the OpenCV documentation (OpenCV, N.D.), which would take each image, turn it grayscale, and find all the key features to use for labels. The labels would all be collected and added to two different files, being "faceLabels.yml" and "labels.pickle", which completes the program. This provides an effective solution to low-level Facial Recognition that would not be available otherwise.

```python
# A loop for creating labels for multiple users
for root, dirs, files in os.walk(my_face_dir):
    for file in files:
        # Verifying the file type (png or jpg)
        if file.endswith("png") or file.endswith("jpg"):
            path = os.path.join(root, file) # Setting Image path

            # Folder name becomes the user ID
            label = os.path.basename(root).lower()
            if not label in label_id: # changing the ID number for each subsequent user
                label_id[label] = current_id
                current_id += 1
            ID = label_id[label]
            pil_image = Image.open(path).convert("L") # Changing to grayscale for computation

            # converting the image data into numpy array
            image_array = np.array(pil_image, "uint8")
            face = cascade.detectMultiScale(image_array)

            # Identifying key features to create labels for
            for x,y,w,h in face:
                img = image_array[y:y+h, x:x+w]
                cv2.imshow("Test",img)
                cv2.waitKey(1)
```

Figure 4.15: Labelling faces code

4.1.5 Medium level Facial Recognition Environment

A middle-ground for Facial Recognition Testing was needed to properly evaluate the effectiveness of the strategies found, the perfect choice being Face ID security feature found in modern Smartphones. Facial Recognition has been a part of Mobile Security since 2011 with Android 4.0, and become a standard method of unlocking devices. The technology had shaky beginnings, with a picture of the device's owner being able to fool the algorithm into unlocking (Wankhede, 2022). However, Mobile Facial Recognition has come a long way in the last decade, fixing the issues present and advancing further. Infrared lens and lighting have been included in newer, higher-end, mobile phones as seen in Figure 4.16, being able to recognise faces even in low lighting. Infrared has several notable features that make it more secure than traditional cameras, one being that images are not picked up at all by the lens, thus completely avoiding the issues found in earlier versions.

Figure 4.16: Infrared lens being incorporated into Mobile Phone (Wankhede, 2022)

As Mobile Devices are found everywhere in modern society, it makes sense that this medium of technology be included in this project. The phone selected for experimentation was a Samsung Galaxy 21+ 5g (S21+), as it was the most convenient for the purposes of the project. Unfortunately this phone does not possess an Infrared lens, but as this is a new development in the field it still serves as a suitable middle-ground for valuable testing data.

Figure 4.17: Samsung Galaxy S21+, which will be used for testing (Mobile2go, N.D.)

4.1.6 AWS Rekognition Testing Environment

Amazon Web Service (AWS) provides many different cloud computing services for clients in numerous different fields, from basic storage to managing complex web applications. AWS also offers one of the best Facial Recognition services out there, being AWS Rekognition, which has been so successful that Amazon have even started to sell the service to World Governments, under the vague condition that it is used legally (Reuters, 2019). Rekognition offers numerous features just in this one service alone, such as emotion recognition, text analysis, and even the ability to detect inappropriate content to hide from children (AWS, N.D.).

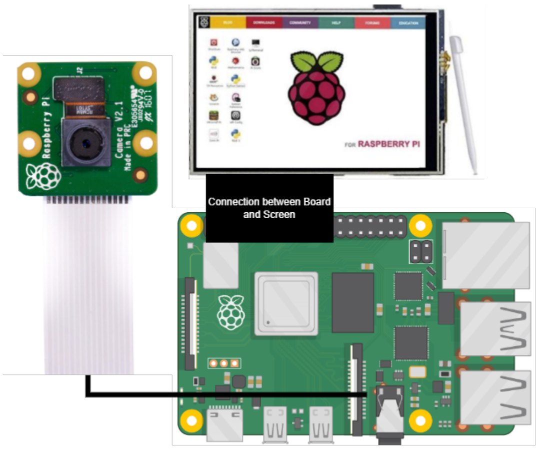


Figure 4.18: Circuit Diagram for board

This serves as an excellent option for high-end Facial Recognition for this project, as if bypass strategies work even on the high-end services that governments use, it truly shows their effectiveness. AWS does offer a free tier as well, meaning it can be easily used as part of this project. The AWS program was written again in Python3, this time using a Raspberry Pi 4 model B to compliment the Arduino solution earlier and potentially use the RC522 scanner.

Figure 4.19: Raspberry Pi with Camera attached

The board was using a small screen connected through GPIO pins as a display, whilst having the mouse and keyboard connected through the USB ports. The Camera was attached to the CSI connector with its ribbon wire, which completed this system, as seen in Figure 4.19.

Figure 4.20: Adding photos to AWS collection of faces, automatically creating face print in the process

A collection of faces was created using the AWS command line interface, adding a couple photos collected for the OpenCV option to a S3 bucket. AWS Rekognition automatically created a face-print to be later used in authentication attempts, as seen in Figure 4.20. Figure 4.21 shows how data is processed in the project, first the camera acts as the input, which is converted and sent through Python to AWS, which compares the face-print and sends back a result to Python.

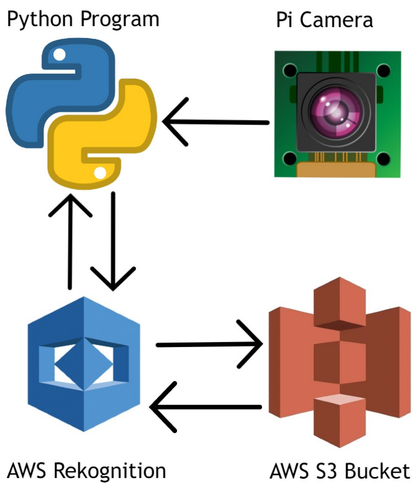


Figure 4.21: How data is processed

The code follows the same format from previous programs, waiting constantly for user input, once Enter is pressed the `os` library is used to take a picture using the Pi camera, which is then converted to bytes. This so it can be sent in a request to AWS to see if it matches any face in the collection, with a threshold of 95%. This figure was chosen after experimentation with the program to find the right threshold, as the Pi camera is not the best, so was found to be negatively effecting the threshold. This can all be seen in Figure 4.22

```
#Main code that runs constantly
while True:
    beginProgram = input("Hit Enter to begin")
    if beginProgram != None:
        #Takes a picture using Raspberry Pi camera
        os.system("raspistill -o image.jpg")
        image = "image.jpg"

        #Connect to rekognition and convert image to bytes
        client = boto3.client(service_name="rekognition")
        with open(image, "rb") as sourceImage:
            sourceBytes = sourceImage.read()
        #Send image to AWS to compare against collection of faces
        response = client.search_faces_by_image(Image={'Bytes': sourceBytes}, CollectionId='faces',
                                                FaceMatchThreshold=95) #95% confidence or higher
        matches = response['FaceMatches']

        print("-------------------------------")
```

Figure 4.22: Taking picture and sending to AWS rekognition

AWS returns a result very quickly, which is then verified to see if there were any matches, showing the user is found in the S3 bucket collection, as seen in Figure 4.23. The various bits of data, such as the user's name (which is taken from the Image originally uploaded to the bucket), similarity, and confidence are then extracted and printed to the display, showing the all the values to the hypothetical SOC team.

```
        print("-------------------------------")

        #If a match was found
        if len(matches) > 0:
            face = matches[0]
            specificface = face['Face']
            #Cleaning Output
            rawName = format(specificface['ExternalImageId'])
            removeDigits = str.maketrans('', '', string.digits)
            noNumberName = rawName.translate(removeDigits)
            faceName = noNumberName.translate( { ord("-"): None } ) #Retrieving Name from image
            #Shows users name, similarity percentage and confidence
            print("Matched with", faceName,": {}""%"" Similarity.".format(face['Similarity']))
            print("With Confidence of: {}".format(specificface['Confidence']))

        else:
            print("Access Denied: Face does not match records.")


        print("Finished Operation")

    sleep(0.5)
```

Figure 4.23: Rekognition checking for matches and printing similarity

The code was then run, which was successfully able to recognise a user and deny entry to a stranger, as seen in Figure 4.24. This image is notably running in Kali Linux, which was due to a hardware fault in the Raspberry Pi when it came time to document code.

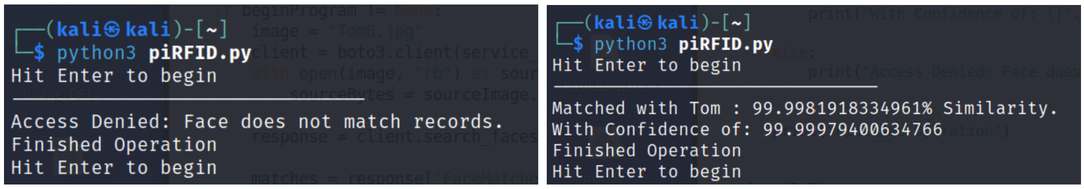


Figure 4.24: AWS rekognition being Successful at Authorising/Denying users

An edit to the program was required when moving it to the development laptop, simply using OpenCV to take a picture of the user using the webcam, as seen in Figure 4.25. The Raspberry Pi board was still used for testing and experimentation, as it only failed near the end of the project's lifecycle. The edit also included a `try/except` block to catch if no face was found within the picture to prevent errors, as seen in Figure 4.26, the full code can be found in Appendix A.

```
#Take Picture using CV2
cam = cv2.VideoCapture(0)
check, frame = cam.read()
cv2.imwrite("image.jpg", frame)
image = "image.jpg"

#Connect to rekognition and convert image to bytes
client = boto3.client(service_name="rekognition")
with open(image, "rb") as sourceImage:
    sourceBytes = sourceImage.read()

#Error Catching incase no face is in picture
try: #If a face is found
    #Send image to AWS to compare against collection of faces
```

Figure 4.25: OpenCV edits for code with try block for error catching

```
    except: #If no Face was found
        print("No Face Found in Frame")


    print("Finished Operation")
    #Cleanup, removing image and resetting camera
    os.remove("image.jpg")
    cam.release()
    cv2.destroyAllWindows()
sleep(0.5)
```

Figure 4.26: OpenCV edits for code with except block and cleanup

4.2 Smart Card tools and Scanners

There are a multitude of tools and devices for Smart Card Technologies that offer functionality to this form of Access Control or ways to exploit it. Many of these tools were purchased to see the true effectiveness or to be added to testing systems, which are covered in detail in the following sections.

4.2.1 MIFARE Classic Tool

The MIFARE Classic Tool is a Mobile Application found on Android devices, which offers users the ability to read/write/save Smart Cards from their phone (GitHub, 2021). The user's phone obviously has to have a scanner built in, which is not unusual in the age of Smart Wallets like Apple Pay. The App was recommended from Literature, and is a very effective tool for Smart Card experimentation, notably allowing for manual editing of card data blocks.

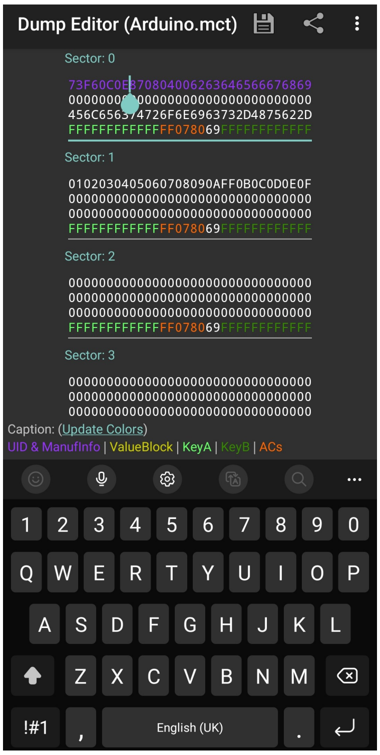


Figure 4.27: MIFARE Classic Tool, allowing for manual editing of Data on saved Cards

This feature comes in handy when crafting unique exploits, but also give reassurance to any users, as there is always backups of the original card contents whilst editing a saved cards' data, as seen in Figure 4.27. This App is not only handy but also subtle, as many other scanners are bulky devices with loud noises whenever any button is pressed. A Malicious Actor wishing to be subtle would most likely prefer using their phone and the MIFARE Classic tool to clone cards. This leads to the MIFARE Classic tool to be included in the survey, to understand if the public would find someone using this suspicious compared to traditional cloners.

4.2.2 Flipper Zero

The Flipper Zero is the latest craze device in the Information Security community, being described as a multipurpose tool for all sorts of hacking. The tool was inspired by a Pwnagotchi, an open sourced Wi-Fi hacking gadget that uses machine learning to get better at cracking network passwords. Flipper Zero takes much of the stylistic choices made by Pwnagotchi (which intentionally resembles Tamagotchis of the 1990s), with a simple appealing casing and dolphin mascot. The tool was designed to friendly to younger researchers, as it comes ready inbox (only lacking a Wi-Fi card) unlike its predecessor, with the goal of being used as a teaching tool.

Figure 4.28: Flipper Zero being used on Access Control (FlipperZero, N.D.)

The tool features a 433 MHz antenna with a fifty-meter range (depending on region), GPIO pins for physical connections, an infrared transciever, and even Bluetooth. These all contribute to an incredibly versatile tool, able to send requests to television sets through infrared and famously open up Telsa car charging ports through cloned frequencies (FlipperZero, N.D.). The relevant aspect to this project is through the Flipper Zero's ability to clone and replay RFid signals, supporting most commonly used Smart Cards. The tool can be seen demonstrating this in Figure 4.28, showing it potential to be used by a malicious actor to gain illegitimate access to a building.

The Flipper Zero has gone viral after several TikTok videos demonstrating the more unethical side of the tool, resulting in the product being sold out the majority of the time. The legal side is also of issue, as the tool falls into the same category as bolt cutters or lock-picking sets, which can be used for good or bad depending on the owner's morals. This has led to many shipped product being held in customs (Person, 2022), meaning that use of the Flipper Zero within this project is near to impossible. In-fact, a recent development has sene Amazon remove the product from its storefront, with bans for any users caught selling it, as they deem Flipper Zero to be a tool capable of card skimming. Amazon obviously does not wish to be seen selling illegal tools, but this does demonstrate how the line is not clear when it comes to using this sort of devices legally.

As no physical testing can be conducted with the device, only hypothetical discussion can be had regarding the capabilities in the hands of a malicious actor. Flipper Zero could very easily be used in a replay attack, as the device can clone RFid signals from a fair distance. To acquire a skeleton key, all that would need to be done is to intercept the signal once an individual with access rights (i.e. a guard) is trying to get into restricted areas. The relative small size of the device would make this not the most challenging of tasks, but whether it would be a reliable method cannot be researched at this time. What can be ascertained is whether the Flipper Zero would arouse suspicion in staff, as the casing has a white/orange palette, and would stand out compared to traditional Smart Cards. Despite not being used for practical purposes, the hypothetical uses can still be researched through surveying the public's opinion.

4.2.3 Additional Smart Card Scanners

Several other Smart Card tools were purchased to see what was available for a Malicious Actor to use against Access Control security systems. One of the key products advertised was these cheap unbranded cloners as seen in Figure 4.29, which were heavily featured in non-academic literature on the subject. These tools claim to be able to read and then write card contents, making for easy cloning, using only two AA batteries for power.

Figure 4.29: Unbranded RFID writer ()

Experimentation with this product revealed the real capability of the tool in the hands of a Malicious Actor. The cloner was only able to read/write to Smart Cards of 125 kHz, a fact that was not advertised anywhere. Additionally, existing academic research failed to mention the difference between frequency bands for RFID. When it comes to RFID frequencies there are several options, but only two are used in reality, being:

- **125 kHz -** Used primarily for animal tagging and cargo identification. This is due to its longer range, ability to bypass environmental conditions (rain/dirt on tag), and the relative cheapness of the product. Usually in the form of a key-fob rather than card.

- **13.56 MHz -** Standard for Smart Cards and Access Control, as it has less range (being less than a meter) to enhance security. Does not transfer data as fast as the previous frequency, but can transfer more with additional security through encryption (RFID4u, N.D.).
- **Very High frequencies (433MHz, 960MHz, 5.4GHz) -** Anything higher tends to be used for purposes like Container tracking of many sorts, from pallets to cargo trains.

Higher frequencies are not necessary for RFID technology, as the 13.56 MHz standard is adequate. A nondescript scanner was also purchased, advertised for use in management offices, to set up cards in the first place. This was deemed a valuable tool for researching standard methods for setting this critical Access Control method.

The tool was a simple read/writer, that would output a Smart Card's data to any text box selected on the connected machine, meaning it could be used with any RFID software or command terminal. Interestingly, this scanner was found to have a strange quirk when compared to the RC522 chip, as both produced different results from the same card. The testing card had a UID of "73F60C0E", which was verified using the Arduino system and MIFARE Classic tool, whilst the basic scanner returned "0235730547", as seen in Figure 4.30. This was found to be a poor conversion from the Hex UID to decimal, despite the decimal value of the testing card being "1945504782".

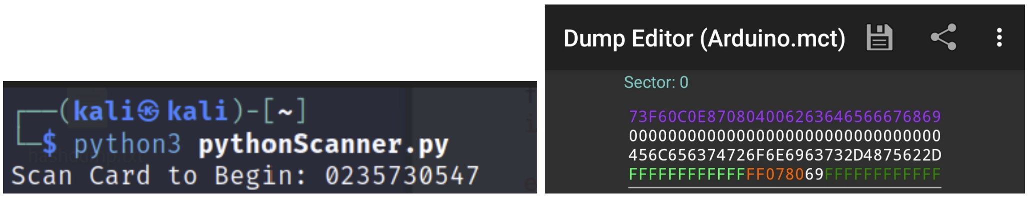


Figure 4.30: Mismatching Data from scanner to MIFARE Classic Tool

This was actually due to scanner sending two bits at a time working from the back to the start of the UID, meaning "73 F6 0C 0E" became "0E 0C F6 73" before conversion to decimal. This quirk meant that all values from this scanner had to be rearranged before use, which was achieved with the code seen in Figure 4.31. This takes the incorrect decimal value and converts it back to hex, before splitting it into two bit segments. The segments are then rearranged to be queried against the database, opting to have uniform storage method of hex throughout the project.

```
#Convert from Decimal to Hex
hexValue = hex(int(scannedCard))
correctHex = hexValue.replace('x', '') #Remove
splitValues = textwrap.wrap(correctHex, 2)#Split Hex into pairs
#Rearrange Hex pairs to true value(e.g. OE OC F6 73 to 73F60C0E)
orderHex = splitValues[3] + splitValues[2] + splitValues[1] + splitValues[0]
```

Figure 4.31: Code to fix hex values

4.2.4 Cloning Device

Many locksmiths offer card cloning services, using tools to quickly copy and write a customer's new cards. Due to the previous option only supporting low frequencies, a more advanced cloner was purchased, being far more versatile not only in frequencies but also in setting the UIDs through a keypad. The device would display a legality warning once ran, as seen in Figure 4.32, showing the legal grey zone that this (and many other hacking tools) fall into.

Figure 4.32: Cloner Legality warning

The cloner could then be used by slotting in a card at the back and pressing one of the option buttons, as seen in Figure 4.33 for this the read option was chosen. This like the scanner had its own quirks when converting to decimal (poorly again), but as this device had no interaction with code or databases it was not necessary to fix these values.

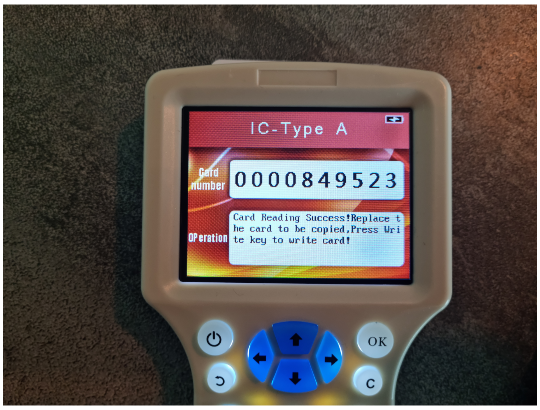


Figure 4.33: Cloner successfully reading card

4.2.5 ESP Key

Figure 4.34: ESP Key chip (Red Team Tools, N.D.)

An ESP Key is a tool specifically designed to attack Smart Card technology, through intercepting communication between a reader and the back-end server. An ESP Key takes the form of a small chip, as seen in Figure 4.34, and can be hidden easily in standard RFID scanners. A Malicious Actor would covertly wire the ESP Key into the RFID reader and perform a man-in-the-middle attack, which can gather up to 80,000 credentials. These credentials can be viewed and even replayed through a Wireless Interface to make the attackers' life all the easier, as seen by Figure 4.35. The tools can be used further in an offensive manner by Denial of Service of RFID scanners, preventing and authorisation attempt making it to the backend server. This could prevent any employees entering the building or restricted are (like a server room) causing mass confusion and potentially giving a Malicious Actor a window of opportunity.

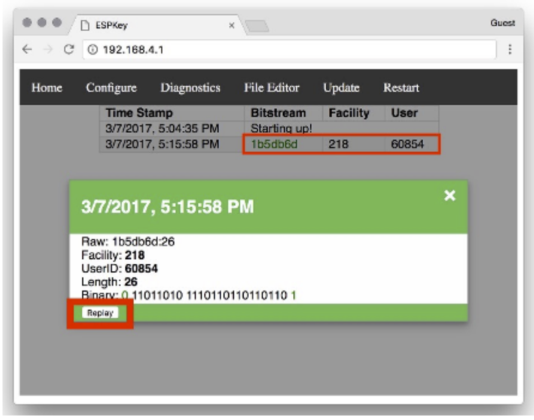


Figure 4.35: ESP Key's web interface, allowing for viewing and replay of attacks (Beard, 2020)

The ESP Key is fairly easy to set up, as it literally just hijacks onto the wires already used in standard RFID scanners using punch-down connections, allowing for no drop in availability to occur (which could be suspicious to Security staff). The wires must be connected in a specific order to avoid damaging the device, as seen in Figure 4.45, and the manufacturer recommends that a nine volt battery is a good option instead of using the scanners power, as the tool cannot exceed a voltage of eighteen volts. The ESP Key web interface is then available and can be customised to prevent unauthorised access.

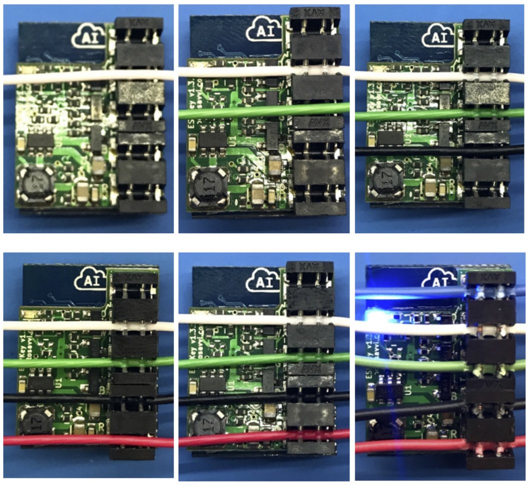


Figure 4.36: ESP Key connecting to Scanner through punch-down pins (Red Team Tools, N.D.)

This tool was purchased in order to test against the physical system and see if it could be incorporated into the Arduino system too. This was deemed as a valuable area of research, as the tool's potential in the given scenario was great. Unfortunately, the device was destroyed by Malaysian Customs, meaning no research could be conducted on this tool.

An ESP Key could feasibly make a skeleton key with ease, as the Malicious Actor would have enough entries to discern any patterns in User ID setup, allowing for an educated guess of admin keys. Another method could be through observing guards routines, if the web interface is detecting a User visiting every floor of a building at anti-social hours then it is likely that it is a security staff member performing an inspection. With an ESP Key, a Malicious Actor simply has to wait patiently until a skeleton key is given freely to them. This tool has great potential and should be highlighted as a key risk to any SOC team, with a countermeasure put in place to prevent this form of attack.

4.3 Smart Card Experimentation

Now that the testing environments are set up and the tools have been acquired, it is time for testing and experimentation of Smart Card technology. This section aims to start with the basics and, following the scientific method, find more exploits to inflict through Smart Cards.

4.3.1 Basic Cloning

The vast majority of Academic and general discussion regarding Smart Card exploiting is around the topic of Cloning. This is understandable, as this technique has been effective since the late 1990s, whilst remaining incredibly simple to perform. A cloner, as demonstrated by the previous section, comes in many forms, but all perform the same base function. Once a Smart Card is in contact with the device, the Cloner simply acts as a reader would, supplying power to the chip which then transmits the data through RFID. The Cloner then saves that to Volatile memory (or to non-volatile in the case of MIFARE Classic Tool) to then be written to as many cards as the user wishes.

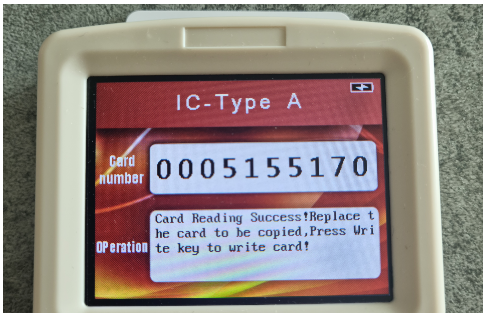


Figure 4.37: Successfully Reading and Writing cards with Cloner

Figure 4.37 shows the Cloner successfully reading card contents to then write to a new card, which can be done with a simple button press. The new card now has the testing User ID, showing that cloners do not copy the entire card contents, only the important section. Figure 4.38 shows the card contents before and after cloning, highlighting the change in User ID. The cloned card worked against all three systems, showing the effectiveness of this technique. The issue with Cloning from an experimental standpoint is that not much more can be done from here, the technique is simple and works well, meaning nothing further was done with cloning.

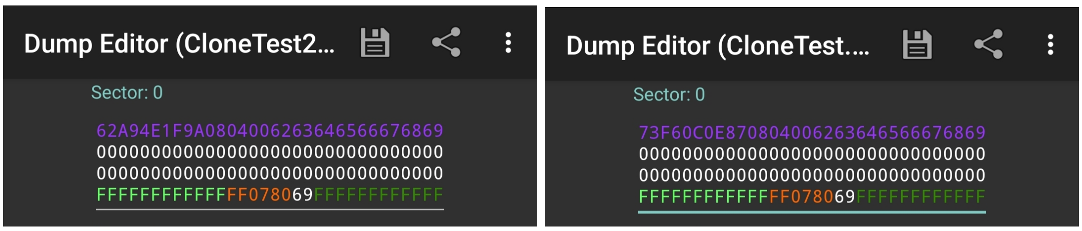


Figure 4.38: Card Data before and After cloning

4.3.2 SQL Injection

SQL Injection is the process of injecting code into an SQL query through an input form to do a variety of requests that the developer never intended for. This could include retrieving sensitive data (like user passwords), to modifying or deleting database tables. Figure 4.39 shows an example of SQL Injection, where a Malicious Hacker injects a request for all the usernames and passwords from the server.

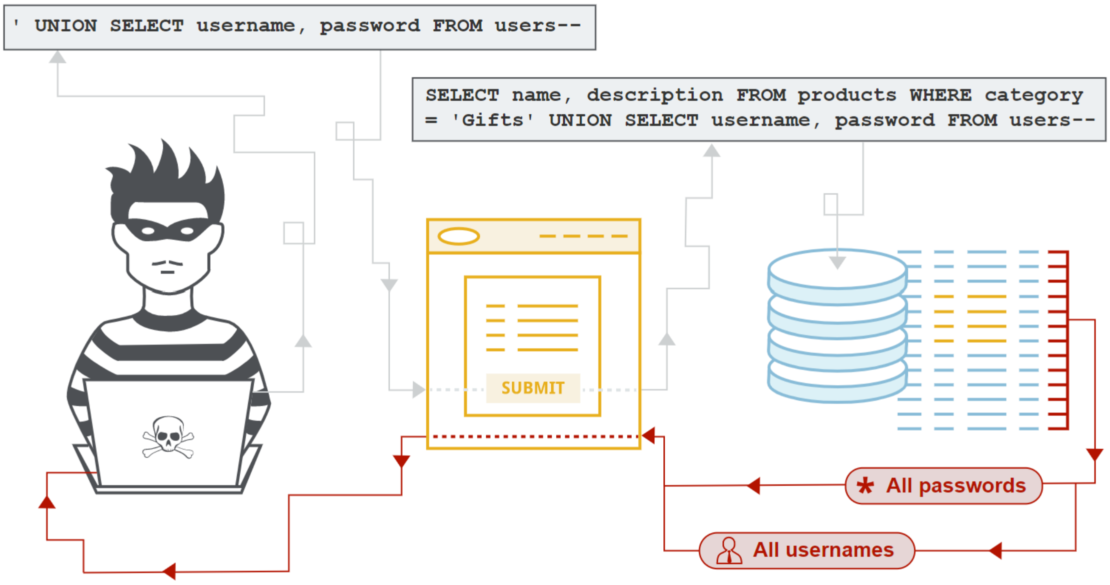


Figure 4.39: SQL Injection Example, where a Malicious Hacker retrieves all usernames and passwords from Database (PortSwigger, N.D.)

In many Smart Card systems, SQL is used as a more secure and global manner of storing permissions, as storage in code or on the physical scanner are not the best security practises. As RFID is essentially an input form it is not inconceivable for Smart Cards to be used as part of an SQL injection attack, so with this hypothesis experimentation began.

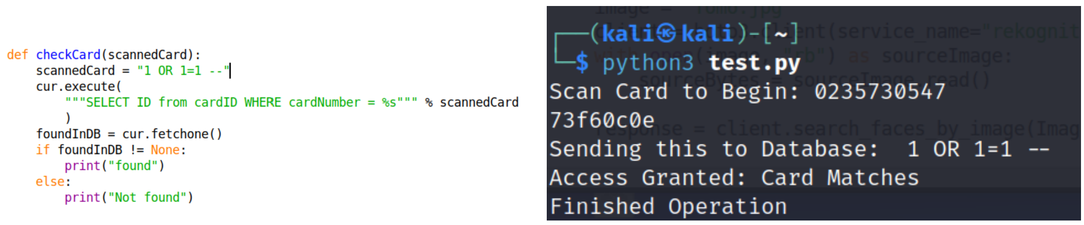


Figure 4.40: SQL injection test against Database working

The first part of this experiment was to test if the database would accept the SQL Injection commands in the first place, which was tested through submitting the malicious string rather than the card number in the code itself. This proved successful after multiple attempts to find the right syntax, allowing access despite the card contents never making it to the server, as seen in Figure 4.40. Next the working Injection value was converted to Hex, which is the standard storage on MIFARE cards, using an online converter. This was then manually written to a card using the MIFARE Classic Tool, as seen in Figure 4.41

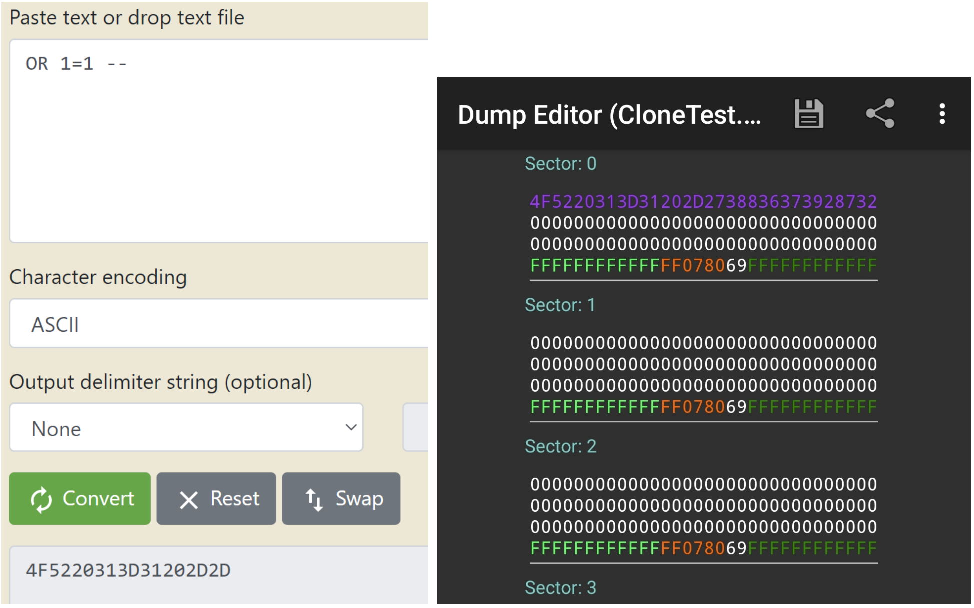


Figure 4.41: Converting SQL Injection to Hex and writing to card

The code was edited slightly for experimentation purposes, as after sanitisation it would send a Hex value to the Database, which would not work with this attack, so a string was sent instead. However, as Figure 4.42 shows, this test did not work at all. This was due to the inbuilt sanitisation from the scanner, as it only sent the first eight bits of the User ID, meaning only “1 OR ” managed to get through. This is not a fault of the scanner, as all devices relating to reading cards would only send eight bits, meaning it seems to be industry standard. This means that SQL injection would never work against a real system, even with ignoring the mismatching conversions, as it is highly unlikely that a database would use text to store User IDs. This concluded the SQL Injection testing, as it was deemed not possible.

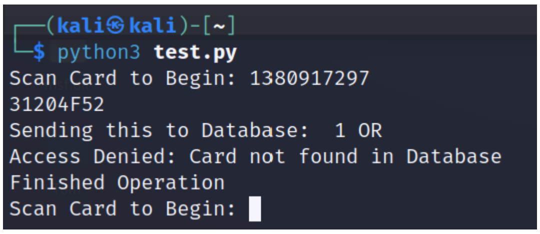


Figure 4.42: SQL Injection Failing through character limit

4.3.3 Shellcode

Shellcode operates similarly to SQL injection, but allows for a wider variety of target systems. A shellcode is essentially a series of executable instructions that hijack a program through injecting into memory, resulting in a “shell” to run further commands out of, often malicious in nature (SentinelOne, 2019). Shellcodes have long been used as the final nail in a security system for professionals like Penetration Testers, showing that a hacker was able to gain full control of a system and could have potentially caused havoc.

Naturally, this leads to further experimentation to see if it is possible to include shellcode onto MIFARE Classic cards, and for them to grant a remote shell on the target system. This experiment arose from a blog from 2009, documenting how a shellcode could run on the researcher’s personal RFID scanner (Stevens, 2009), as seen in Figure 4.43. This experimentation was planned to see if this was still possible on the modern systems built for this project.

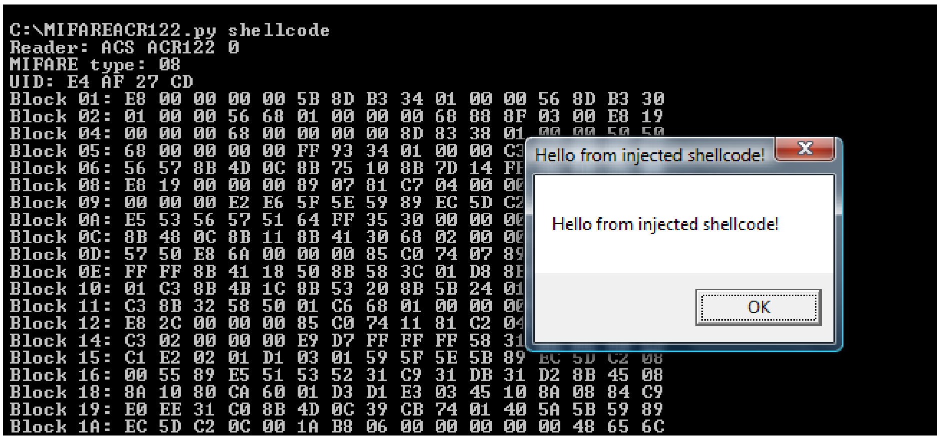


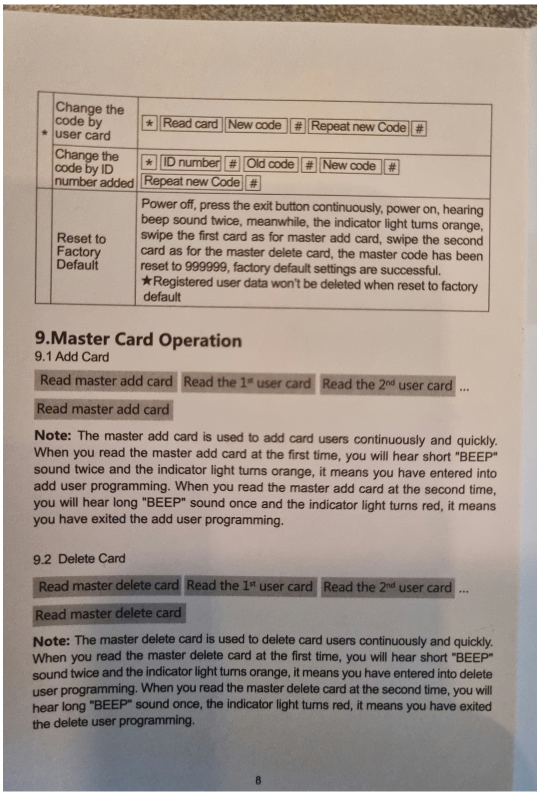
Figure 4.43: Shellcode running on a homemade RFID system (Stevens, 2009)

The results from the SQL injection experiments made it apparent that this was not going to work at all on the systems, as the previous researcher had used the unused blocks of memory to store shellcode. As scanners and software only care about the first eight bits of the UID, it is not possible for shellcode to be transferred to the target system through RFID, at least not without heavy editing.

Stevens built their scanning software to read the entire contents, which is why it worked on their system. Naturally, the same could be done for the testing environments, but this then means that these environments are no longer similar to the real life systems they were built to replicate. As shellcode would not work on any system without compromising the aim of the project it was struck from experimentation, as no Malicious Actor would be able to use it, and therefore is no threat to any SOC team.

4.3.4 Manufacturers Instructions

Default Credentials have long been a thorn in modern security systems, making an otherwise effective products useless due to user negligence. The majority of systems come with Default Usernames/-Passwords simply to get the product up and running, with it highly recommended that these are changed as soon as possible to avoid an illegitimate party using these publicly available details. This was found to be also applicable to Smart Card systems when constructing the physical system.



*	Change the code by user card	* Read card New code # Repeat new Code #
	Change the code by ID number added	* ID number # Old code # New code # Repeat new Code #
	Reset to Factory Default	Power off, press the exit button continuously, power on, hearing beep sound twice, meanwhile, the indicator light turns orange, swipe the first card as for master add card, swipe the second card as for the master delete card, the master code has been reset to 999999, factory default settings are successful. ★Registered user data won't be deleted when reset to factory default

9.Master Card Operation

9.1 Add Card

Read master add card Read the 1st user card Read the 2nd user card ...

Read master add card

Note: The master add card is used to add card users continuously and quickly. When you read the master add card at the first time, you will hear short "BEEP" sound twice and the indicator light turns orange, it means you have entered into add user programming. When you read the master add card at the second time, you will hear long "BEEP" sound once and the indicator light turns red, it means you have exited the add user programming.

9.2 Delete Card

Read master delete card Read the 1st user card Read the 2nd user card ...

Read master delete card

Note: The master delete card is used to delete card users continuously and quickly. When you read the master delete card at the first time, you will hear short "BEEP" sound twice and the indicator light turns orange, it means you have entered into delete user programming. When you read the master delete card at the second time, you will hear long "BEEP" sound once, the indicator light turns red, it means you have exited the delete user programming.

8

Figure 4.44: Example Manufacturer's Instructions, showing how to factory reset

The instructions for setting up the system included details for the default master card(or skeleton key), which was `999999`. Any Malicious Actor conducting recognisance on a target building would take notes on what RFID readers are being used, and then would easily be able to find the default master card value from online manuals. Even if these credentials have been changed the Instructions still offer valuable methods for exploitation, as the physical system had easily repeatable steps to factory reset the scanner, as seen in Figure 4.44, which in turn would reset the master passcode to `999999`. This is a very effective technique againsts purchased systems, and SOC teams should put steps in place to prevent it, but would be ineffective against custom or private software. This is the reason why this test could not be performed against the Arduino or Python systems. However, when tested against the physical system, it resulted in easy fraudulent access.

4.4 Facial Recognition Experimentation

Facial Recognition cannot be tackled in the same way that RFID can be, the mediums of Access Control are very different. A Malicious Actor would take a drastically different approach to dealing with Facial Recognition cameras than to Smart Card scanners, for being that there cannot be any tangible interaction with the devices or any transfer of manipulated data (as in the case of sending a shellcode through RFID). A Malicious Actor is limited mainly to methods of obfuscation to prevent cameras from recognising them, whilst minimizing suspicion from onlookers. Several methods of avoiding Recognition Algorithms were researched to be used in experimentation against the setup testing environments later.

4.4.1 Facial Recognition Avoidance using everyday items

A key way to prevent Facial Recognition Cameras from working is to obscure or cover the user's face, which saw some attention in Literature, such as Kasthuriarachchi et al. (2021) stating that masks prevent recognition 50% of the time. The research was found to limited, as a Malicious Actor would likely use everyday items to cover their face, not only from Facial Recognition cameras but also CCTV.

This section of the Procedure aims to research and then test what are the best options for covering a face to prevent recognition, whilst drawing the least suspicion. There would likely be a combination of everyday items that make the optimal "disguise" that a Malicious Actor would use to fool cameras, whilst not fooling guards. Researching this topic aids SOC teams by identifying what a Malicious Actor would likely wear, so that they can be better spotted in the future.

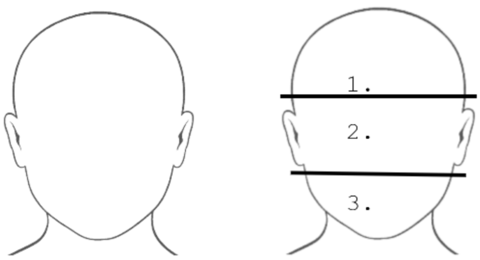


Figure 4.45: Segmenting a face into three sections

Different items cover different parts of a person's face, so items were placed into three categories, being:

1. **Head-ware -** Any item that is worn above the eyebrows, such as hats.
2. **Eye-ware -** Any item was placed around or covers the eyes, such as glasses.
3. **Mouth coverings -** Any item that is place below the nose, such as a scarf.

Figure 4.46: Typical array of items for testing, featuring an item for each section of the face

Each section was designated as 33.33% of the overall face, even though the Eye-wear section in smaller in size it is of greater importance when it comes to recognition, hence the equal distribution. Three items were chosen for each category, aiming to vary in area cover from low to high, whilst not over complicating the experimentation with an unnecessary number of items. An example of the items selected for testing can be seen in Figure 4.46, showing an item for each section of the face. Table 4.1 shows each item selected for each facial area, as well as their percentage coverage.

Face Section	Item	Percentage covering	Total Facial Covering
Head-ware	Bandana	33%	11%
	Beanie	66%	22%
	Hard Hat	100%	33%
Eye-ware	Glasess	33%	11%
	Sunglasses	66%	22%
	Blindfold	100%	33%
Mouth covering	Loose Scarf	33%	11%
	Face Mask	66%	22%
	Full Scarf	100%	33%

Table 4.1: Everyday Items with estimated percentage of covering

These items will each be individually tested later on, initially individually and then in combinations, to find the most effective strategies.

Hypothesis: This Technique will be effective as coverage of the face increases, with all recognition struggling in the upper percentiles of coverage.

4.4.2 Facial Recognition Avoidance using Painting Technique

As mentioned in the Literature Review, Facial Painting has seen use as a method to obfuscate Facial Recognition cameras, by masking the areas of a face that Algorithms use for recognition. There has been no academic research on this subject, so using the testing environments constructed different painting methods discussed in various articles, such as the examples in Figure 4.47, will be applied to see if recognition fails or not.

Figure 4.47: Examples of Facial Painting to avoid recognition (Tapper, 2020)

Articles do not mention any specific patterns that fools recognition cameras, so the scientific method will come into play, experimenting with the various applications of the paint. The logic is to blend identifying features together, lighten dark areas of the face, and create general confusion for algorithms (Getahun, 2022). Obviously, this is a very suspicious form of obfuscation that any security guard would notice, but it is still valuable to get the public's opinion on whether or not they would find it suspicious. This adds another series of questions to the survey to add further to this research.

Hypothesis: This technique will work well against low level systems, encountering some pushback on medium level recognition algorithms, and be ineffective against complex solutions to Facial Recognition.

4.4.3 Anti-Facial Recognition Glasses

Strategies to avoid Facial Recognition have seen the gradual incorporation into Hollywood movies, a notable example being the 2017 film "Baby Driver". As with any film regarding bank robberies, one of the core challenges the characters have to overcome is to avoid being caught by cameras, which is particularly difficult in the age of Facial Recognition. Rather than the classic choices of the genre like ski masks, the cast opt for anti security camera glasses, that use high power Infrared Light Emitting Diodes (IR LED) to block any cameras from catching their faces. Jon Hamm's character can be seen wearing the anti recognition glasses in Figure 4.49, as well as the real life prop.

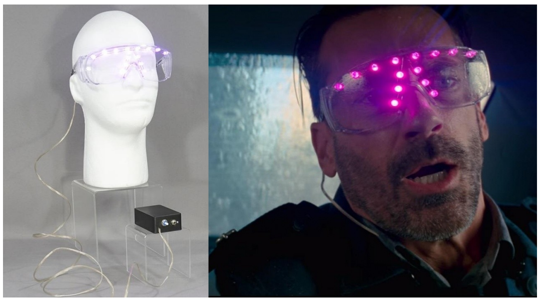


Figure 4.48: Anti Recognition Glasses used in the movie "Baby Driver" (2017) (Your Props, N.D.)

This strategy is not a work of fiction, but lifted directly from reality, as the concept was introduced by the National Institute of Informatics four years prior to the release of the film. IR LEDs are rather easy to acquire, making this a cheap "Do It Yourself (DIY)" tool for blocking Facial Recognition Cameras. The researchers state that the IR LEDs mask the darker areas of a human face that are used for Facial Recognition, but a subject's face can still be made out by a human eye, especially if the camera is not directly facing the user (as is often the case with cctv cameras). The glasses are obviously effective at tricking algorithms, but unlikely to fool any manual review of camera footage or physical guards, who would likely find the device to be suspicious.

Figure 4.49: Privacy Visor Glasses being used to block Facial Recognition (Ikinamo, 2013)

This is not the only development in Facial Recognition blocking glasses, as designer Scott Urban has led to a more marketable and stylish solution to the key ethical issue with the technology. Urban designed several models of glasses to protect customer's privacy, operating under the philosophy of creating “an opt-out because the system is not an opt-in” (Morse, 2019). Original designing glasses to reflect natural light to ruin any flash photos (marketing towards celebrities wishing to mitigate paparazzi harassment) Urban made the natural leap to frames that could also reflect Infrared flight, thus preventing any 3D dot mapping algorithms to perform Facial Recognition. The “Phantoms” Reflectables look like any run-of-the-mill glasses, and can even be fitted with prescription lens, allowing for a subtle reclaiming of privacy that is highly unlikely to look out of place. Figure 4.50 shows the product, with the reflective components only being partially visible on the white pair, showing how inconspicuous the glasses are.

Figure 4.50: Phantom Glasses by Scott Urban (Reflectables, N.D.)

The glasses only are noticeable to Infrared cameras, causing the glowing eye effect seen in Figure 4.51, so will not look suspicious to any guard monitoring standard CCTV cameras. Privacy does come at a cost, however, as the glasses retail $168 dollars for a base model.

Figure 4.51: Phantom Glasses successfully blocking Facial Recognition Camera (Morse, 2019)

These glasses are very effective for any Malicious Actor wishing to remain anonymous whilst in the presence of Facial Recognition Cameras, as well as having the notable advantage of not being suspicious. The only downside, which is also faced by the LED option, is that manual review of footage can still be done to identify them. As both of these privacy glasses have been tested and proved to work against Facial Recognition Technology, it was deemed irrelevant to this project. However, it is also valuable to survey the public to see if any suspicion would be aroused from the use of these products, and find the viability in the hands of a Malicious Actor.

Chapter 5

Results and Testing

This chapter will cover the various tests conducted to discover how effective avoidance methods are for Facial Recognition Technologies, through use of the testing environments built in the previous chapter. The tests aim to find the best methods that a Malicious Actor would likely use to bypass security mechanisms. The public will also be surveyed, not only on Facial Recognition, but also querying them about Smart Cards as an Access Control, aiming to find the general disposition to this form of technology. These results will be collected and discussed at length in the Chapter 5: Discussion.

5.1 Test Plan

The testing for this project was split into two sections, being the tangible tests and the survey, which will only be conducted through digital mediums. The testing focuses more on the Facial Recognition portion of this project (with tangible tests being exclusively Facial Recognition), whilst Smart Cards will only be discussed in the Survey. This was an intentional choice, as Smart Cards received the bulk of testing and experimentation throughout Chapter 4: Procedure. The Scientific method meant that with Smart Cards the only real result from experimentation was either success or failure, which would then lead to further hypothesis and experiments, and therefore would not be appropriate for this chapter (as it fits much more with the rest of the Procedure).

The experimentation on Smart Cards from the Chapter 4 would classify as Qualitative data, and so a focus was put on acquiring a similar class of data for Facial Recognition. The testing of the technology aims to acquire key trends and research in the effectiveness of avoidance techniques against a myriad of systems. The Survey on the other hand will focus on collecting Quantitative results, through as many user responses to the questions, to gather the common consensus regarding Access Control. The Survey also aims to research how suspicious various avoidance strategies or hacking tools (like the FlipperZero) are to a normal person, and how likely they would be to a normal person, gageing how truly effective they would be in reality.

These tests will acquire results in various forms, all in the goal of researching Access Control technologies to the fullest extent of the project's scope.

5.2 Facial Recognition Avoidance Through Everyday Items Tests

The items mentioned in the Procedure, were acquired, as seen in Figure 5.1, and once the testing environments were built the official tests were good to go. Each item and every potential combination was added to a results table, containing sixty-three unique coverings, to attempt to avoid Facial recognition. Additionally, the percentage of coverage of the items was also included to find the correlation and sweet spot for maximum avoid whilst having minimum facial coverage.

Figure 5.1: Everyday Items with estimated percentage of covering

The tests are rather quick to perform but numerous, so each "disguise" will be tested five times against each environment, which will then be converted to a percentage of success rate, with a total percentage as well (from all three environments). Additionally, the Effectiveness was calculated to show the relationship between coverage and success rate, which was worked out with the equation seen in 5.1. In this, E is the Effectiveness of the disguise, whilst Sr is the Success rate multiplied by the Percentage Covering.

$$E = 1 - (Pc \times Sr) \tag{5.1}$$

Figure 5.2: Collection of item combinations tested against environments

The test were all conducted, with several examples of item combinations visible in Figure 5.2. The raw results for individual tests can be seen in Figure 5.3, whilst the other results for more complex combinations can be found in Appendix C.

Face Section	Item	Percentage Coverage	Enviroment 1	Enviroment 2	Enviroment 3	Overall Pass Rate	Effectiveness	Comment
Individual Tests	Bandana	11.00%	100.00%	0.00%	100.00%	66.67%	92.67%	
	Beanie	22.00%	100.00%	60.00%	100.00%	86.67%	80.93%	eye contact matters with cv2
	Hard Hat	33.00%	100.00%	0.00%	100.00%	66.67%	78.00%	
	Glasess	11.00%	100.00%	0.00%	100.00%	66.67%	92.67%	
	Sunglasses	22.00%	100.00%	0.00%	100.00%	66.67%	85.33%	
	Blindfold	33.00%	0.00%	0.00%	100.00%	33.33%	89.00%	
	Loose Scarf	11.00%	100.00%	100.00%	100.00%	100.00%	89.00%	
	Face Mask	22.00%	0.00%	0.00%	100.00%	33.33%	92.67%	
	Full Scarf	33.00%	0.00%	0.00%	100.00%	33.33%	89.00%	

Figure 5.3: Raw Results for Individual Items

5.3 Facial Recognition Through Painting Technique Tests

Testing for the Painting Technique will use a very similar methodology to Everyday items, except only having five options instead of the previous sixty-three, which can be seen in Figure 5.4. This is due to the Painting technique being more subjective and taking longer to apply, whilst having a more limited range of data that could be acquired. This experiment is meant to simply prove if this is truly possible or effective, rather than get coverage data like the Item experiments. Yet again, five tests will be done for each painted face on each testing environments, which will then be turned into a success rate percentage.

Figure 5.4: Painted faces used for testing Facial Recognition (Top: #1,#2,#3. Bottom: #4,#5.)

After a lengthy testing time, the results were gathered, as seen in Figure 5.5, which concluded the painting experimentation of Facial Recognition.

Painted Face #	Enviroment 1	Enviroment 2	Enviroment 3	Overall Pass Rate
1	0.00%	0.00%	80.00%	26.67%
2	0.00%	0.00%	100.00%	33.33%
3	100.00%	0.00%	100.00%	66.67%
4	60.00%	0.00%	100.00%	53.33%
5	0.00%	0.00%	100.00%	33.33%

Figure 5.5: Raw Results for Painted Faces

5.4 Surveying the Public

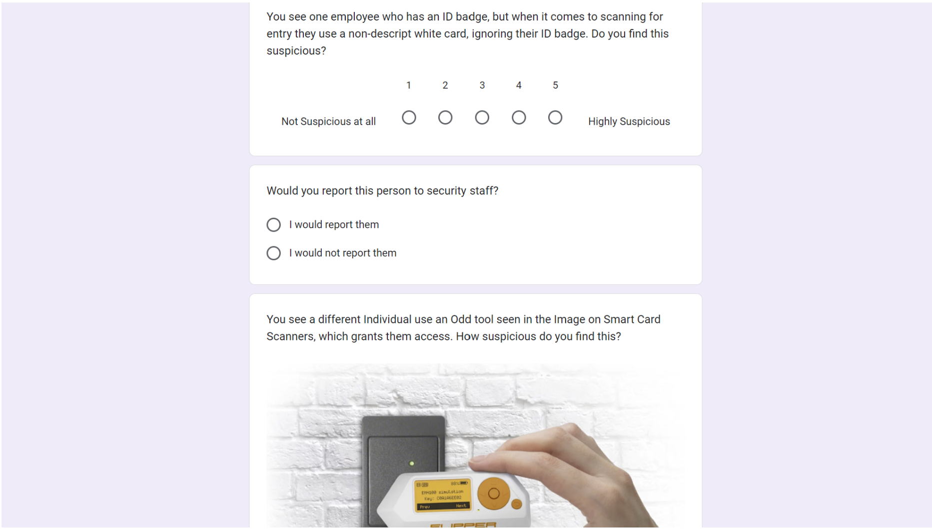


Figure 5.6: Survey Example, sent to the Public aiming to get their perspective

The Survey will be conducted through Google Forms, as it the platform with best ease of use, which is important when wanting to collect as many results as possible. This is a design philosophy followed throughout the entire survey, as the aim is to gather a large quantity of data rather than long quality answers. Short effective questions were selected to make responses easier for users, with a series of options for them to select from to each question, being "Strongly Disagree/Disagree/Neutral/Agree/Strongly Agree", or binary answers like simple "Yes/No", as seen in Figure 5.6. The survey was also segmented into distinct sections to tackle each topic of this project and avoid confusion. An introduction page was also added to inform the user of the project, what their answers will be used for, and how their data will be protected (to comply with GDPR and right of anonymity), as seen in Figure 5.7. Additionally, a little informative paragraph was included on each page, so there would be no confusion for any user of any technical ability.

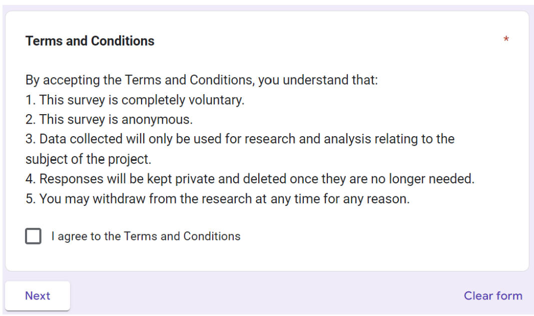


Figure 5.7: Terms and Conditions for the Survey

The Survey consisted of the following questions:

- **Smart Cards Questions**
  1. Have you used Smart Cards before for Access Control? (i.e. opening a locked hotel door)
  2. How often do you use Smart Cards?
  3. How secure do you think smart cards are?
  4. Do you think Smart Cards will continue to be used or replaced with other technologies? (i.e. Facial Recognition, fingerprint)
  5. Do you think it is possible to Clone a Smart card?
  6. Would you trust a Smart Card system as the only form of Access Control to a building/business/organisation?
- **Facial Recognition Questions**
  1. Have you used Facial Recognition before? (i.e. Face unlock on phones)
  2. Do you prefer using Facial Recognition to other forms of Access Control? (i.e. password, fingerprint scanning)
  3. Do you think Facial Recognition will replace other forms of Access Control? (i.e. Smart Cards, physical keys)
  4. Are you worried that Facial Recognition could be used to track you?
  5. Do you think it is ethical for governments/businesses to use Facial Recognition without your consent?
  6. How important is consent for you when dealing with Facial Recognition Technologies?
  7. Would you trust Facial Recognition as the only form of Access Control to a building/business/organisation?
- **Scenario Questions**
  1. You see one employee who has an ID badge, but when it comes to scanning for entry they use a nondescript white card, ignoring their ID badge. Do you find this suspicious?
  2. Would you report this person to security staff?
  3. You see a different Individual use an Odd tool seen in the Image (a Flipper zero) on Smart Card Scanners, which grants them access. How suspicious do you find this?
  4. Would you report this person to security staff?
  5. You see someone opening up a Smart Card reader and messing around with the wires before putting it back together. How suspicious do you find this?
  6. Would you report this person to security staff?
  7. A member of staff seemingly never uses their ID card, instead pressing a button on their phone which unlocks doors. How suspicious do you find this?
  8. Would you report this person to security staff?
  9. A member of staff wears these glasses (Phantom Reflectables). Do you find this suspicious?
  10. Would you report this person to security staff?

11. Someone enters the building fearing facial paint like in the image. Do you find this suspicious?
12. Would you report this person to security staff?

Two weeks were allocated to gather results from the survey, eighty-nine responses were gained from willing participants which can be seen in 5.8, which helped gain a good understanding of the public's opinions towards access control. Full results can be found in Appendix C, whilst the full survey can be seen in Appendix B.

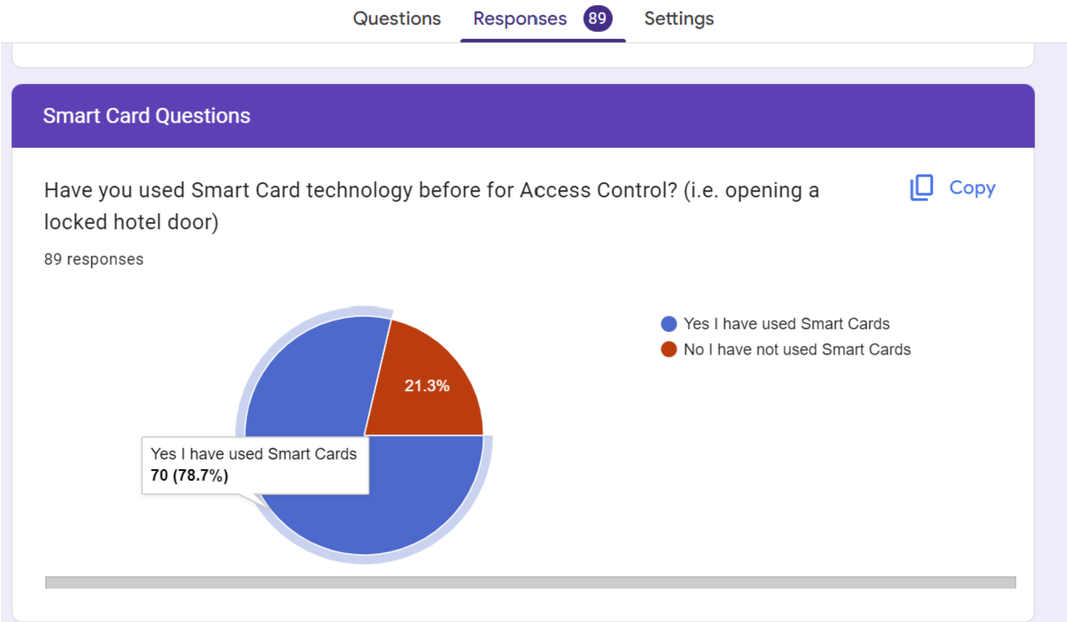


Figure 5.8: Example Results from the Survey

Chapter 6

Discussion

This chapter will cover the general Discussion of the project, aiming to give details on every aspect of completing this white paper. This will be done through delving into how the proposed plan compared to reality, details into how development and experimentation was, what the results of the testing mean, and a final evaluation of the project's success.

6.1 Proposal versus Development Discussion

The original Proposal for the project set out a lot of ideas, expectations, and discussion regarding how the research will be conducted and factors that will come into play. Of course, this was all done from a hypothetical point of view, with only educated guesses to how the project would turn out. The reality is a very different story, with many changes from the original plans due to unforeseen circumstances. Nevertheless, it is a good learning opportunity to discuss the differences between the Proposal and reality, aiming to uncover root causes of problems and issues so that they can be better mitigated in future research.

6.1.1 Design Approach

The Scientific method proved to be the perfect fit for the nature of the project and the developer's working style. The design approach allowed for easy intuitive experimentation without any constraints, whilst providing a backbone to guide research during the project life-cycle. The methodology was forgiving when risks became reality and effective when development was running smoothly, showing the versatility of the selected approach. The Scientific Method can be seen in Figure 6.1, with an example input from this project.

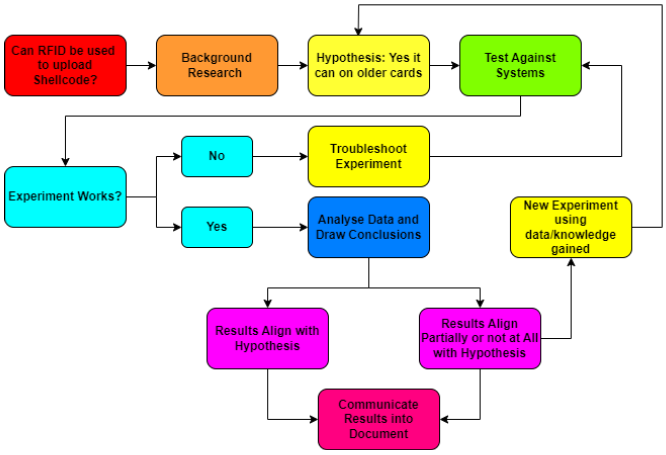


Figure 6.1: An example use of the Scientific Method, using the Question of if Shellcode can be communicated through RFID

6.1.2 Gantt Comparison

Gantt charts are a common tool used in any project, aiding greatly in time management and avoiding issues like feature bloating. A Gantt chart was constructed as part of the proposal for this project, showing an idealised plan for how research and experimentation would be carried out. The reality of project management is never as tidy and organised as originally intended, and this project was no different. Figure 6.2 and Figure 6.3 show the original Gantt charts versus the real timeline of the project.

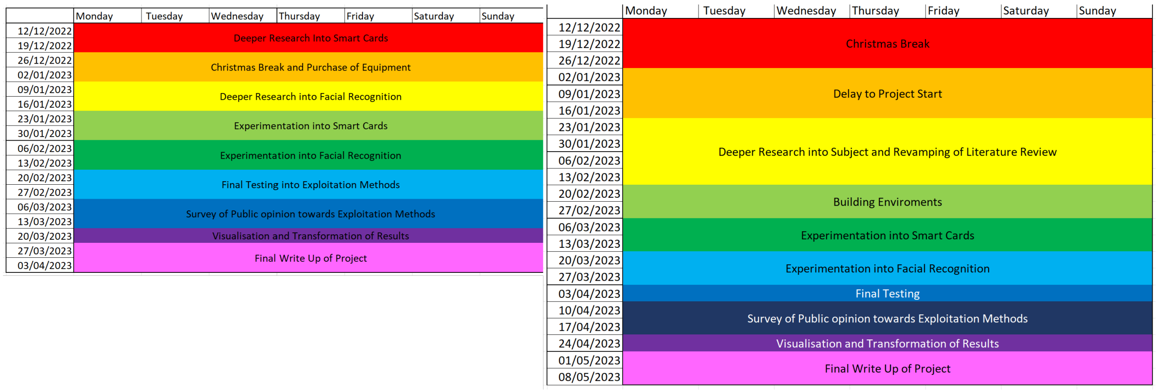


Figure 6.2: Original Gantt chart (Left) versus actual Gantt Chart (Right)

There is a noticeable difference between the original graphs and reality, being the extension of the deadline by a month (from April 7th to May 10th). This was due to a delay in starting the project from the original timeline, due to developer burnout and personal reasons. This project is obviously large and needed quality time to properly execute each planned stage of research, and so an extension request was submitted for an additional month to make up for lost time, which was approved by Asia Pacific University and the Supervising Lecturer.

Another notable change can be seen in the “Deep Research” sections of the original, which were merged together and used to significantly improve the Literature Review chapter of this document. The original Draft of the chapter was deemed mediocre, so serious research was conducted to improve the knowledge on the topic, providing a better basis of understanding for experimentation and affirming the need for this project.

A key issue in the project life-cycle and caused a change to the Gantt chart was the failure to acquire a real life testing environment to experiment in. The project proposal profusely stated that testing in a real life environment would be the ultimate indicator of success, and the potential issues present in Access Control methods. Permission was asked of Asia Pacific University and the place of residence of the author, with both parties denying the request. This is understandable, as experimentation on a real life system could cause real life damages, affecting all other students or residents in the respective buildings. Despite this Asia Pacific University generously offered to cover costs for purchase of door lock systems found in standard buildings for research, which lead to the testing environment present in the project. This was a good compromise, as it resulted in valuable research on how traditional real life systems are constructed. However, it would have been very insightful to uncover how the respective organisations manage Smart Card system and what security mechanisms are in place.

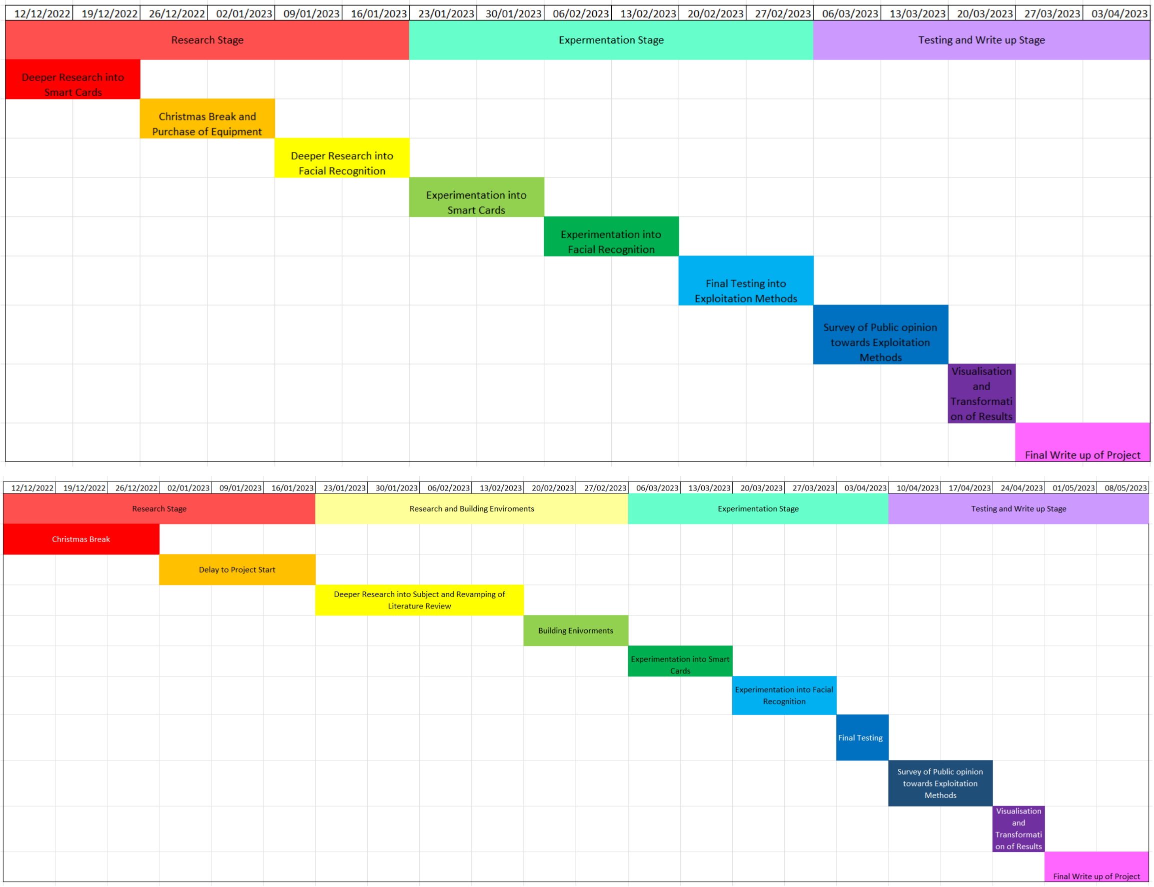


Figure 6.3: Original Gantt chart (top) versus actual Gantt Chart (Bottom)

Asia Pacific University also denied access to the Facial Recognition Cameras and system used in the Campus authentication system for similar understandable reasons. This resource would have also been very valuable to the project, as the cameras were able to perform recognition with the user wearing a mask, which could have shown how methods worked against a more advanced system. Still, issues like these lead to innovations and workarounds, which is a core principle of scientific research. This led to the new task being added to the Gantt chart of building the testing Environments for the project, which obviously required time and effort to complete properly.

There are not any other significant changes to the Gantt chart, the only thing to mention is that the write-up of research occurred concurrently with experimentation, lightening the load for later on and avoiding any lost work. The lengthy times dedicated to each task and included buffer allowed for a more relaxed and free flowing process to development, which greatly aided keeping the project interesting and experimenting independently. These vague task allocations allowed for unplanned or spur of the moment research to be conducted, which would not have occurred in a more strict itinerary. Overall, the Gantt chart served as a good guideline to project development, helping keep tasks on track, but also allowing for the normal disruption of life to not cause the any major issue.

6.1.3 Risks

Several risks were discussed as part of the proposal for this project, resulting in the creation of a risk matrix and plans of mitigation. Unfortunately, some of these risk came to fruition leading to delays and issues with the project. These risks are:

- **R1: Unrealistic Time Estimates**
  - As mentioned, the original timeline of the project did not fit the real scenario and conditions that were faced. The Gantt chart had made no break in work from one busy Semester to the start of the project, an error in hindsight which led to severe developer burnout. A beginning of any project is a critical time, starting on the right footing is necessary to see the project meet all of its goals and objectives. This led to a length break period as to start the project with a fresh mind and a more optimistic attitude, but also consequently led to severe knock-backs in planned work.
  - This risk was resolved through a series of actions, the main being an extension to the project deadline to make up for the lost time. Additionally, similar tasks were grouped together to simplify workload, whilst writing of the document was done in conjunction with research, allowing for more time.
- **R2: Hardware/Software Failure**
  - As this project deals with a lot of hardware components, it was understood that there was a risk of these parts failing, leading to delays. This risk did occur throughout the project, with items like the Power Supply Unit being ineffective in the physical system, to the Arduino Board originally used (Arduino Mega 2560) breaking, causing it to be quickly replaced with another board (Arduino Uno, which served much better than the original). However, these do not compare to the biggest blow-back of being denied access to real life systems, which caused significant issues to the project, as discussed earlier.
  - This issue was resolved by having all the hardware components be purchased and used near the start of the project timeline, meaning plenty of time was available for seeking replacements. Additionally, the denial of real life systems may have been a blow at first but did allow for more in-depth development into how these Access Control system are constructed and work, aiding in knowledge and practical research at the cost of more time

6.1.4 Smart Cards Experimentation

A key loss to the project was the destruction of the purchased ESP Key by the Malaysian Customs Authority. The ESP Key had potential to be one of the most effective and efficient tools for a Malicious Actor to use, the ability to easily view/clone/replay tens of thousands of User IDs. No Academic Research had mentioned this tool, so it was deemed to be a topic of interest for research and experimentation. Furthermore, the tool was expensive (around $100 or 500rm with shipping) and had a lengthy shipping period from the United States. The notice from Customs came at a point in the project life-cycle where it was no longer viable to reorder the product from a different supplier (in the vain hope this new purchase would make it through), meaning the ESP Key's part of this project had to be severely downsized to only a hypothetical discussion.

Although this is a loss for the project it is an overall good sign of the growing awareness of security issues. Clearly Customs officers are aware of ESP Keys, and how dangerous they can be in the wrong hands, and made the reasonable decision to destroy the device. Perhaps if the address had been set to a business rather than a residential the parcel would have got through, as it would be clearly used for professional use rather than suspected as malicious. Still, the product was discussed in detail, how it could be used to create a skeleton key, and later on how as a SOC team could counter it, so not a complete loss. If one destroyed ESP key meant for educational uses prevents many from malicious uses, then it is a fair trade-off in the greater good of the security scene.

The other issues with the Smart Cards are trivial compared to this, with only minor problems like differences of output from scanners, which was corrected through code. The RC522 did not come with its connections attached, meaning the board had to be soldered before use in this project. Soldering was not too difficult to learn (aided by trial attempts and a backup RC522 scanner), which led to the soldered board seen in Figure 6.4, but still caused delays through learning the technique and waiting for a soldering kit to be delivered.

Figure 6.4: Soldered RC522 board

6.1.5 Facial Recognition Experimentation

The Facial Recognition Experimentation went relatively smoothly, with the only real issue coming from the Raspberry Pi's camera failing rather late into the project lifecycle. This led to a sudden switch over to Kali Linux for the code and a later secure environment developed, leading to compatibility issues to work out, such as switching to Open CV to use the webcam. This only caused minor delays to the project, but still irritating as the Raspberry Pi was planned to be used for demonstration purposes.

6.2 Results Discussion

This section details the various results gathered from the project from various stages, taking the raw results and transforming them through visualisation. The results gathered helped prove or disprove hypothesis, whilst also gaining unknown information that would not have been considered beforehand.

6.2.1 Smart Cards Results

The results for Smart Cards were rather disappointing when compared to the original optimism for discovering different exploits. From the results, it is clear that Smart Cards are a very simple technology, which is why simple experiments like Cloning cards is so effective. Cloning takes the main feature of Smart Cards and uses it against the technology, which is why it was discussed in many of the Academic papers reviewed. More advanced exploits like insertion of Shellcode or SQL Injection were not even hinted at in Literature, which should have been an early indicator to the success of these experiments. The hard truth is that Smart Cards are too limited for sophisticated attacks, with issues from converting malicious card contents to industry standard limiting of RFID transmission. These two factors prevented any of the planned experiments(asides from cloning) from working, and preventing any future exploits that were to be attempted after.

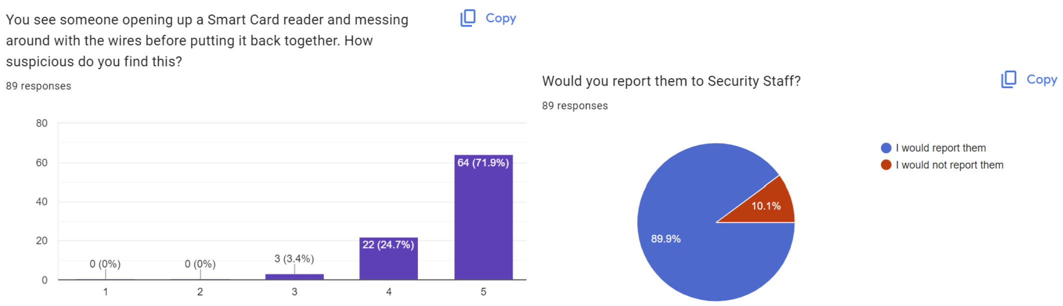


Figure 6.5: Survey Results relating to ESP keys

This is disappointing from a research project perspective, but very reassuring for SOC teams, as it shows that Malicious Actors are fairly limited when it comes to Smart Card Exploitation. However, ESP keys present a whole other level of danger to SOC teams, as this little chip perfects the concept of Cloning. Of all the tools researched and purchased, this has to be the one with most potential threat to a business. Members of the public were asked if they would find someone interfering with scanners suspicious, and if they would report them to security, essentially asking what they would think of a Malicious Actor installing an ESP Key. Users agreed they would find it suspicious, with 90% claiming they would report it to security, showing that installation of ESP keys is the tricky part. However, once installed there would be little to no suspicion from employees that their Smart Card Values are being harvested. This is backed up by the following question, which asked participants if they would find it suspicious if a person was using their phone at scanners to unlock doors (essentially using the ESP key Wi-Fi interface or MIFARE Classic App to replay stolen card details). Figure 6.6 shows the result of this, with the majority of users being neutral or not finding it suspicious. This makes it critical for SOC team to put the steps in place to prevent this from happening in the first place.

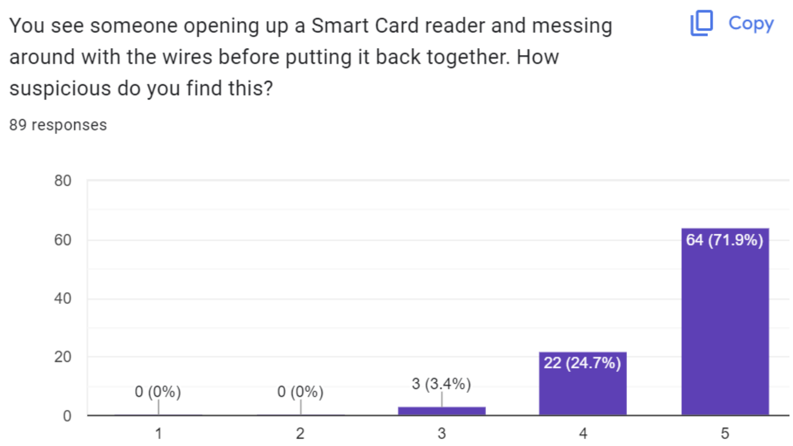


Figure 6.6: If members of the Public would find the ESP Key Wi-Fi interface suspicious

Less subtle tools like the Flipperzero(with its neon orange casing) proved to be far more suspicious to the general public, with 90% saying they would report anyone using it to security. This is a conclusive fact that any exploit that a Malicious Actor plans to use has to be subtle, which means SOC team do not need to worry about trendy hacking devices. Participants were also asked if they would find a person using a clearly cloned card suspicious, with most users saying they would feel neutral about it, and 62% saying they would report it to security, as seen in Figure 6.7. Having 38% of the participants saying they would report the cloned card is rather high compared to other results, but this is likely due to the wording of the scenario, which specified the exact type of employee ID smart card that would contrast greatly against a plain MIFARE card. This result does show that cloning is not only the simplest but also the subtlest form of exploit in a Malicious Actor's toolkit.

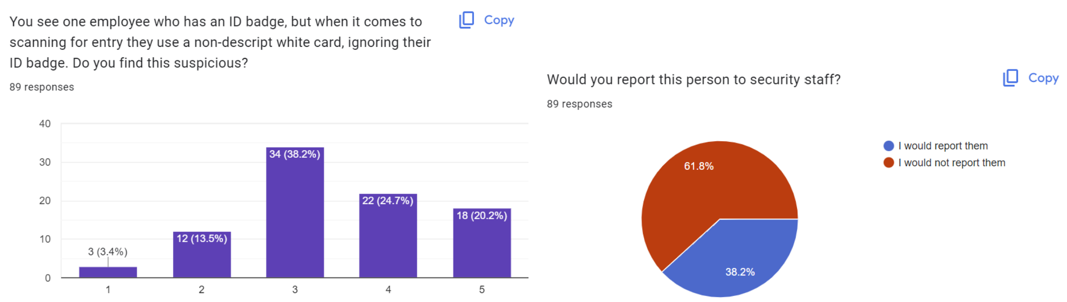


Figure 6.7: How subtle are cloned cards?

Overall, Smart Cards proved to be insecure but not the biggest concern to an SOC team, as their limited nature prevents more complex and damaging attacks. The key takeaway is that the subtle forms of exploitation, through cloned cards and ESP keys, should be taken incredibly seriously, with prevention methods put in place.

6.2.2 Facial Recognition Everyday Items Results

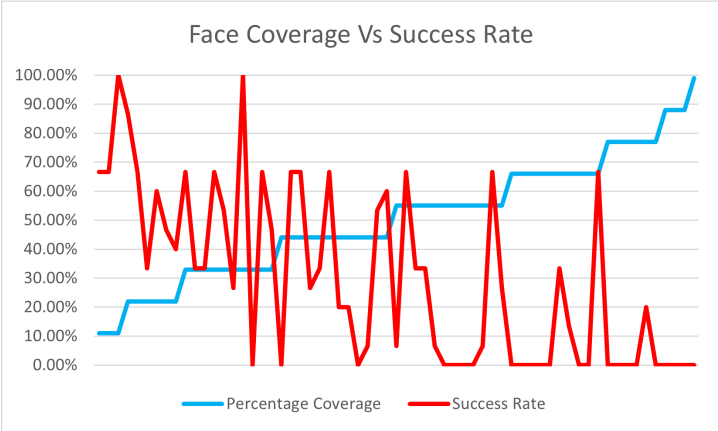


Figure 6.8: Percentage coverage of face versus Success Rate of Facial Recognition environments

The tests for Everyday items stayed very close to the original hypothesis, that with more coverage, the less effective an environment would become. Figure 6.8 shows this in full effect, as Percentage of a face increases the Success Rate decreases, with a drastic decline after 50% of a face is covered. This is predictable, as the defining features extracted to make a face-print are masked by these items, the interesting point that was revealed during experimentation were the different weak points for each solution. The python program using CV2 struggle when a user's mouth was obscured in any way, particularly from use of a face mask, whilst AWS could not handle heavy coverage of the eyes. These quirks can be seen in Figure 6.9, where sudden spikes in Success Rate are caused by these critical areas having less coverage.

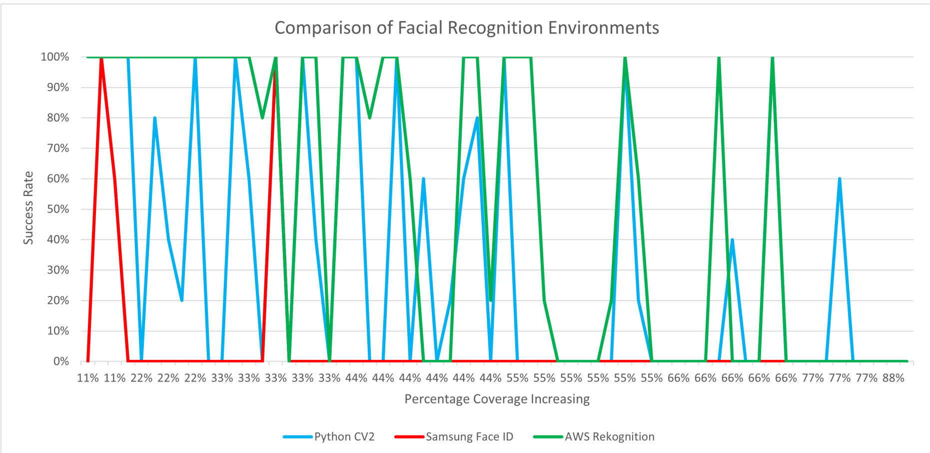


Figure 6.9: Line Graph of Success Rate for each Facial Recognition Environments as Face Coverage increase

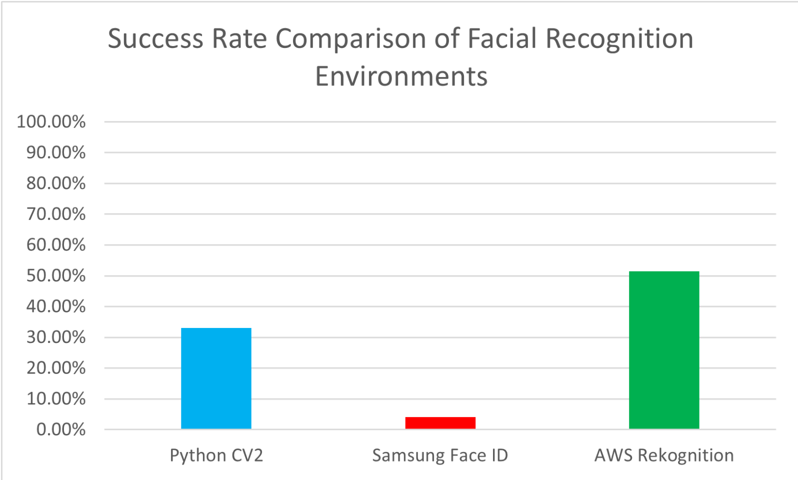


Figure 6.10: Bar chart of Success Rate between Facial Recognition Environments

Figure 6.10 shows a comparison of the three testing Environments, with AWS having the highest success rate, followed by Python CV2 and then the Samsung's Face ID. The Success rate results may seem a bit low, but it has to be understood that over half of tests featured the majority of the testers face covered, so AWS being able to recognise users through 50% is impressive.

Figure 6.8 reveals the minimum percentage of face coverage needed to stop Facial Recognition Algorithms, being anything greater than 55%. After this value, each solution failed to recognise the tester, with only outlier cases.

The items select for face coverage did not matter other than the inherent facial coverage, the only exception being the glasses with a coverage of 11%. Although meant to be the least effective eyewear option, the glasses actually surpassed the sunglasses on many of the tests, especially with the Python CV2. The individual tests showed that the sunglasses had an Effectiveness of 85%, whilst the glasses had 93%, which was true for the majority of the tests for these two items. This was actually due to the glasses reflecting light back into the cameras, obfuscating the critical eye area for face-print creating. This is interesting because these cheap non-prescription glasses offer some of the same functionality as the Reflectables glasses, notably missing the infrared blocking ability. This reaffirms the notion that coverage is not the only factor, and that reflective abilities should be also considered when trying to mitigate Facial Recognition. Perhaps if the sunglasses had more of a reflective tint to them, then they would have proved more effective in testing. The Reflectables glasses were included in the survey to see if any participants found them suspicious, with 90% of answers giving the lowest suspicion value for the product, and a unanimous consensus that they would not alert security to anyone wearing them. This shows that Reflectables are an incredibly effective form of blocking Facial Recognition, with little downsides other than the price.

The survey also asked users how suspicious they are of a couple item combinations from testing, being the ones seen in Figure 6.11. Members of the public did not find these options to be suspicious at all, despite the effectiveness at blocking Facial Recognition, with a majority of selecting the lowest option on the linear scale. The only outlier was disguise 3, which users found slightly more suspicious than others, which is likely due to it having more facial coverage than the other options, being 66%

versus disguise 5's 44% and disguise 2's 33%. This suggests that anything greater in coverage would draw too much suspicion, meaning that the sweet spot for Facial Coverage is between 55% and 65%, falling in line with the hypothesis of 50% to 70%.

Figure 6.11: Disguise 5, 2, and 3 respectively

Likely the best combination of items to avoid Facial Recognition and remain inconspicuous is any form of head-wear (applicable to the environment), paired with Reflectables glasses and a face mask. COVID-19 has normalised the use of medical masks in public throughout the entire globe (which would have been odd to wear in Western Countries before the Pandemic), which is amazing for anyone wishing to maintain their privacy from Facial Recognition Cameras, as even in the individual tests they had an impressive Effectiveness score of 93% (which was tied the highest value out of this round of testing, with only AWS succeeding to recognise the user). This testing provides valuable research into what a Malicious Actor would likely use to conceal their face, and how effective these disguises would be against a series of Facial Recognition Algorithms.

6.2.3 Facial Recognition Paint Results

The painting experiment provided interesting results, as before testing it was hypothesised that this technique would only be mildly effective against lower end environments, and have no effect on the advanced AWS system. This is partly true, as AWS Rekognition was able to recognise the painted face 100% of the time, as seen by Figure 6.12, but surprisingly Samsung's Face ID failed to recognise a single one. This is consistent with results gathered from the Everyday Items tests, highlighting that this Facial Recognition Algorithm is very strict.

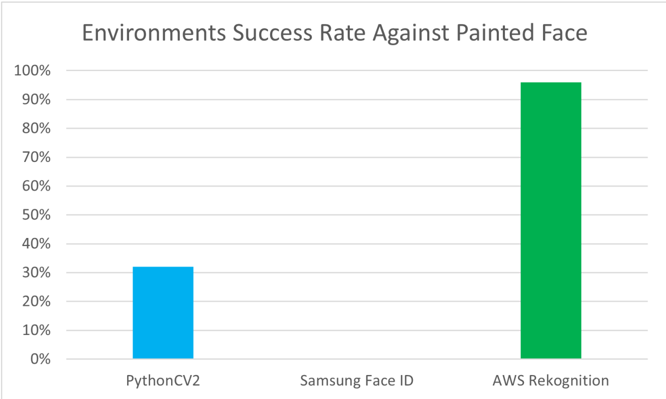


Figure 6.12: Comparison of Facial Recognition Environments against Painting Technique

Initially, the Python CV2 environment struggled as well to detect faces, as seen in Figure 6.13, which shows the open window created by the program with no face detected. Later CV2 was able to recognise some faces, averaging around a third of tests, but on reflection these tests succeeded due to less paint being applied, as seen in Figure 6.14. The python program also required a smaller threshold to make recognition possible, being only 50% otherwise causing failure. This could have led to the higher success rate when compared to Samsung's Face ID, which as testing proves likely has a high threshold.

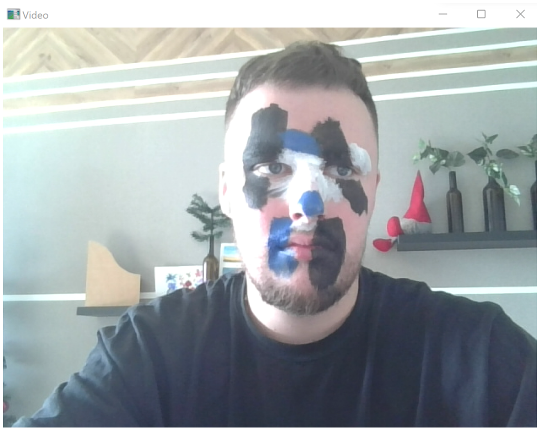


Figure 6.13: Python Facial Recognition Failing to Recognise Face

AWS Rekognition is the clear winner when it comes to Facial Recognition Environments, which is understandable considering the scope of the solution and the governmental usage of it. AWS has to provide the most effective and reliable option for Facial Recognition in order to compete in the software marketplace, which is evident from its ability to recognise users far more than other solutions. From testing, it is clear that even if a Facial Recognition solution works well it simply cannot compete with what AWS is offering, so any SOC team should look into upgrading to this option.

Figure 6.14: Different Paint applications covering different areas of the Face

The painting technique was found to be effective, proving its technical use against Facial Recognition Algorithms. Notably, it was found that darkening the eyebrows and mouth produced the best result, and the more of the face that was covered the less likely it is to be detected. This testing shows that the painting technique is highly effective against systems with either a high threshold or low-level analysis, but fails against higher end options. The practical use of the paint technique was asked in the survey, as seen in Figure 6.15, showing that members of the general public found it to be suspicious. Additionally, 83% of users claimed they would report to security anyone who used this technique, showing that even if it is effective, it could not be used by a Malicious Actor to counteract Facial Recognition. The previous usage of this technique was seen at riots or football matches, which would mitigate any suspicion and make facial painting effective, but otherwise SOC teams should not need to worry about it.

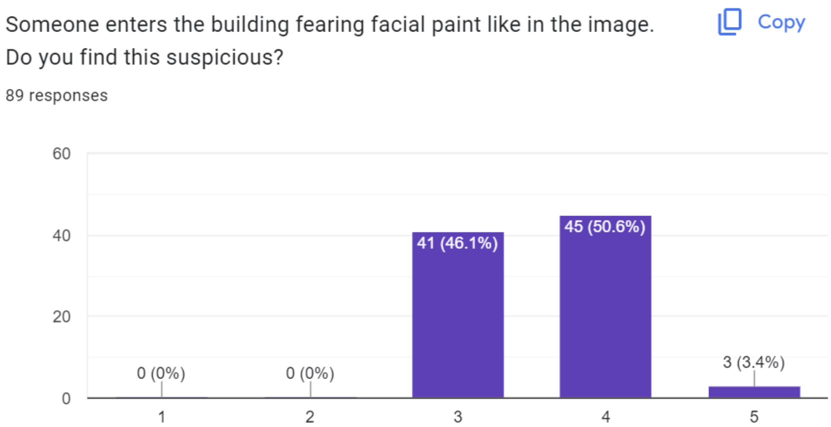


Figure 6.15: Result from Survey asking users if they would find Facial Painting technique suspicious

6.2.4 Survey Results

Much of the results of the survey have already been detailed in the relevant areas of discussion, however, participants were asked some more general questions relating to Smart Cards and Facial Recognition. This section will cover some of the more miscellaneous pieces of data retrieved from the survey.

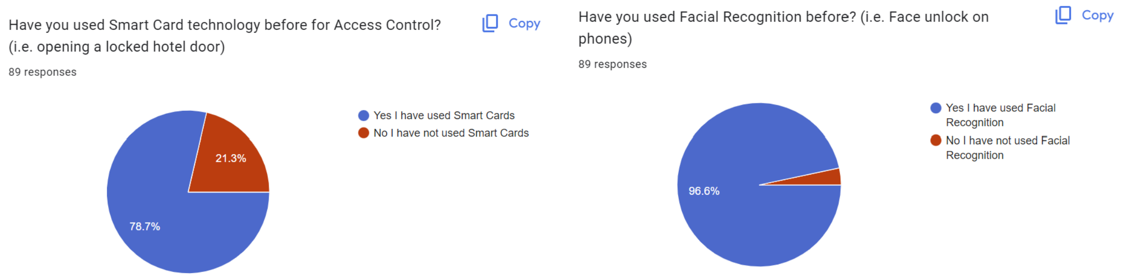


Figure 6.16: Smart Card Usage Vs Facial Recognition Usage

The first question of each section asked participants if they had used the respective technologies before, which resulted in the pie charts seen in Figure 6.16. The vast majority of users had used Facial Recognition before, likely from Face ID features on their mobile devices, but a noticeable 21% of people had not used Smart Card technology, which is surprising. This is likely due to the backgrounds of people involved in the survey, as a significant proportion of potential participants live in the United Kingdom (due to developer background). The U.K. does have Smart Cards in more modern workplaces and hotels, but opt for the key fob alternative when it comes to residential security. This likely contributed to the higher number of users who hadn't used Smart Cards before. A similar reason can be put forward for participants who have not used Facial Recognition before, this time from old age rather than background. The survey intentionally did not ask users any details about their background, identity, or any other facts about themselves to comply with GDPR and focus purely on the Quantitative results. Perhaps in a more general project on Access Control these questions should be asked to reach new conclusions

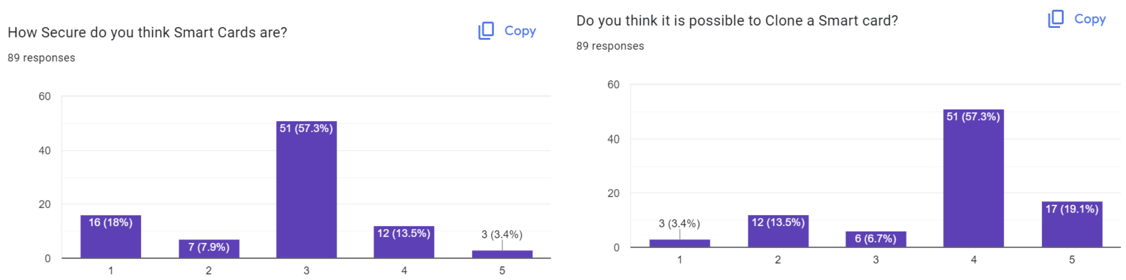


Figure 6.17: Smart Card Security Results

Participants were asked if they thought Smart Cards were insecure, and if it was possible to clone a card, as seen in Figure 6.17. These results reveal that over 50% of the population feel that Smart

Cards are neither Insecure nor Secure, with a similar percentage of people thinking that it is possible to clone cards. This is likely due to the common practise of commercial cloning (at locksmiths or other handyman type businesses), with users not giving much thought to how weak their Smart Cards actually are. This naivety to insecurity was reflected throughout literature, as these Cards have been weak for a long time with much more secure options available.

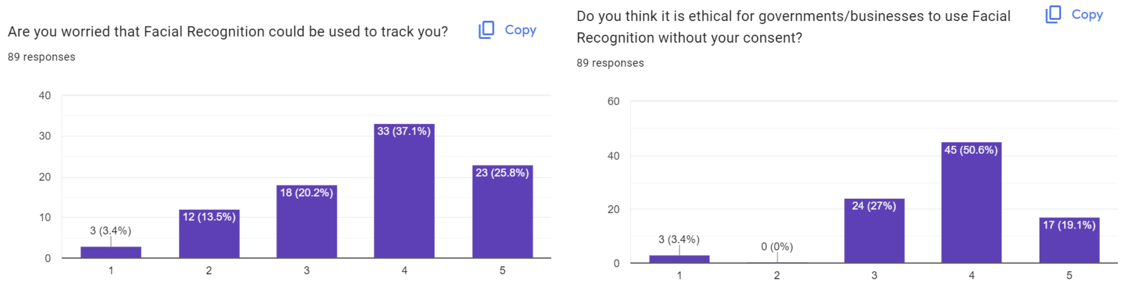


Figure 6.18: Facial Recognition Ethical Questions

On a similar vein, participants were asked about the key issues with Facial Recognition, with questions about tracking and governmental use of the technology, as seen in Figure 6.18. Users predictably responded negatively to the ethic issues of the technology, reaffirming that privacy policies need to be introduced to Facial Recognition in order to make it better for everyone.

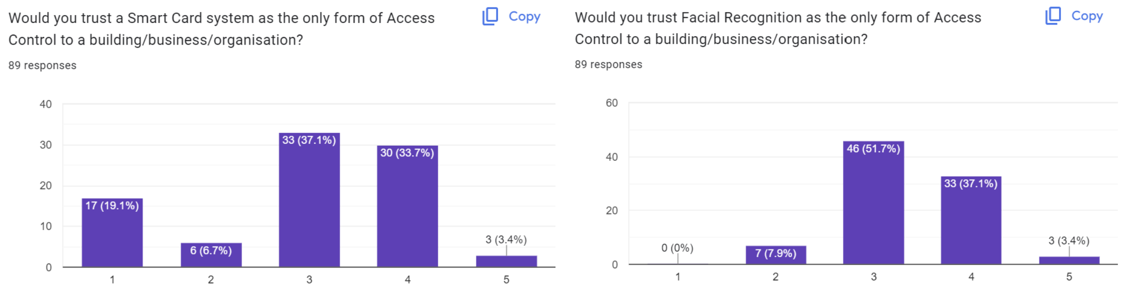


Figure 6.19: Trust in Access Control Results

The concluding question to each section asked participants whether they would trust the respective form of Access Control as the sole form of security for a building, business, or organisation, the results of which can be seen in Figure 6.19. This question was written with the notion that users would not place trust in a single Access Control system, with only marginally higher trust for Facial Recognition. Although Facial Recognition has a higher trust rating than Smart Cards, it was still surprising that the general public would trust these systems so much. This highlights that non-security staff do not consider the security systems in play, and so it is purely on the SOC team to make the necessary changes. Figure 6.20 shows another question, where participants were asked if they though either technology would replace the other. Facial Recognition did have higher results again, but the general consensus was that both technologies are here to stay. This suggests that the likely future is a hybrid of Smart Cards with Facial Recognition, creating a Multi-factor

Authentication scheme to improve security. Naturally, this concept is not perfect by itself, as each technology comes with their own issues and vulnerabilities that would have to be resolved.

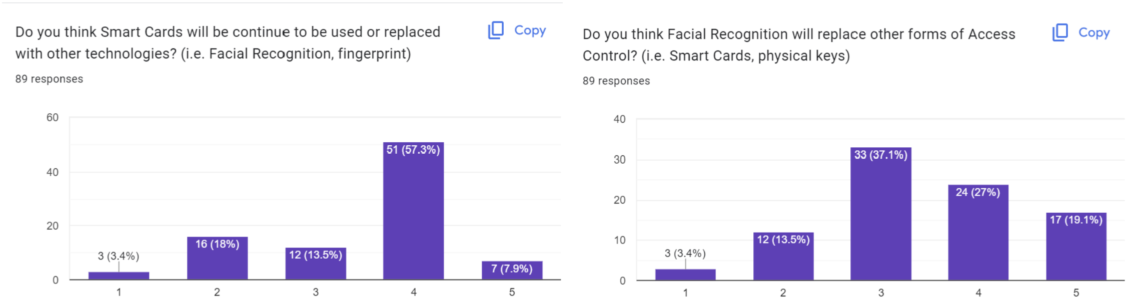


Figure 6.20: Future of Access Control Results from Survey

6.3 Solutions to Issues found

This entire project has revolved around finding these issues in Access Control before a Malicious Actor can, and resolving them for the future. To any SOC team the research found reveals the shocking truth that Smart Cards, like traditional locks, are merely the illusion of security, whilst Facial Recognition has several problems that could be exploited. After uncovering these issues, research and experimentation was done to find solutions that could be implemented to better protect businesses from Malicious Actors.

6.3.1 Cloning

Throughout research in Literature and Experimentation, Cloning was the key issue with Smart Cards that was consistently brought up, as this simple act has the potential to completely bypass any security mechanisms designed for Access Control. The act of cloning is rather simple, with cheap tools being able to effectively replicate cards. The interesting fact is that like the nature of Cloning the solution is also rather simple, and was discussed in Literature by several authors.

The MIFARE Classic card is by far the most common found in the businesses across the globe, mainly due to how inexpensive it is. A basic MIFARE Classic card with 1 Kilobyte(1k) of storage costs $0.83 for one card (BSC, N.D), with it becoming drastically cheaper if bought in bulk (dependent on the vendor). More Advanced options from MIFARE, such as MIFARE DESFire EV1 8K Card(with better memory and security options) costs $2.70 for a single card (CardLogic, N.D.), an increase of 225%. This fact only dissuades many businesses from upgrading to the more secure cards, opting to instead save the money for other purposes. Even if the savings are going to other security upgrades, it still leaves the fact that the primary form of Access Control is insecure, making the majority of other mechanisms irrelevant(such as external Firewalls) to any Malicious Actor. The MIFARE DESFire card has to this date not been cloned, showing how effective a simple upgrade could be for any business (Digital ID, 2022).

Figure 6.21: A Smart Card scanner with added Facial Recognition (Alibaba, N.D.)

Another recommendation that several authors suggested was the use of Multi-factor Authentication to enhance Smart Card security, often suggesting Facial Recognition. This would require significant upgrade to the scanners found throughout the premises with large cost, like the scanner seen in Figure 6.21, but would also mitigate cloning incredibly effectively. There is precedent for use of Facial Recognition to enhance Smart Card security, as during the COVID-19 Pandemic, many businesses and organisations began using Cameras to Identify and detect the temperature of staff to catch early signs of the virus. The worst of the Coronavirus is behind us, but insecure Access Control is still a pressing issue, so investing in this technology is highly recommended.

Additionally, physical RFID technologies have had a gradual decline as more vendors opt to digitise their cards into mobile applications. A Smart Card could easily be misplaced for a short period of time without a staff member noticing, allowing for quick cloning. Mobile apps mitigate this issue, whilst providing a large variety of improvements, as it is easy to securely store credentials with encryption, and credentials can be updated remotely at any time to save staff time. Advanced security features can also be added to the RFID application, requiring a form of biometrics before the Card can be used.

These methods individually counteract Smart Card Cloning, whilst together could form an impassible barrier to any Malicious Actor wishing to exploit Access Controls.

6.3.2 Encryption and non-sequential ID numbering

Encryption should be a standard practise for any Smart Card system, as it often comes with options on even the most basic of cards. Encryption found on the MIFARE Classic is decent, but not acceptable for a modern system. SOC teams should take the steps to use non-standard encryption methods to keep sensitive User IDs secure.

A key aspect found in research was that several companies use sequential allocation for User IDs, and in-fact the instructions for the physical system had this as the default recommendation for customers. The Skeleton code for the particular model used in this project was "999999", a value that any Malicious Actor could easily look up online and write to their own card. Having sequential card numbering allows for educated guesses at other staff member's details, which should not be the case in any secure system

It is highly recommended that any SOC team ignore the default settings for card numbers, and instead uses random encrypted values, which are then authorised through a back-end server rather than the actual scanner itself (as seen with the physical system).

These two security features can be achieved independently with the MIFARE Classic cards, however, it recommended that better programmable cards mentioned are used instead.

6.3.3 Shellcode and SQL Injection

Although Shellcode and SQL Injection were found to be not possible, it is still important to prevent users from entering anything unexpected into the Database, as it could cause issues. Data sanitisation is the solution to this, as it prevents anything but expected values executing, thus preventing shellcode and SQL injection (Pollack, 2017). Before comparing to the database the value retrieved from RFID is sanitised, with checking for empty values, special characters, and validating there is no SQL code inside, as seen in Figure 6.22. This sanitation process prevents anything unexpected running and executing, mitigating effectively another issues found with Smart Cards.

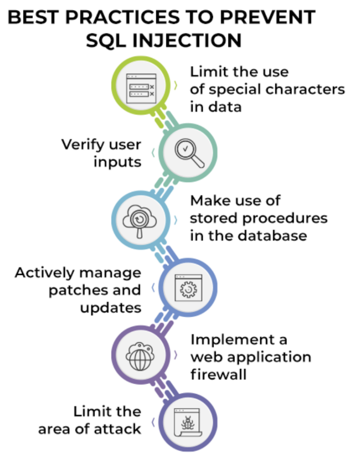


Figure 6.22: How to prevent SQL Injection, and using the same practised shellcode injection (BasuMallick, 2022)

6.3.4 ESP Key

Although never tested physically as part of the project, this tool was still deemed dangerous enough that solutions were researched for SOC teams to implement to prevent this form of attack. ESP Keys are ridiculously easy to install if RFID scanners are not mounted properly, with a Malicious Actor being able to attach the device within a minute due to the punch-down connections.

Figure 6.23: Example of a tamper alarm, using a spring to detect interference (Delta, N.D.)

Tamper alarms are an effective way to alert SOC teams to potential malicious activity, as once an RFID scanner's casing is opened an alert is sent to the output destination, an example can be seen in Figure 6.23. In-fact, many scanners come equipped with such alarms, however, the majority are not connected to anything. Connecting a tamper alarm to standard SOC tools such as a Security Information and Event Management(SIEM) software, which manages log alerts, would be a valuable way to detect any future attempts to install an ESP Key. It should also be mentioned that tamper alarms are not perfect, as there are different ways to exploit them depending on the manufacturer. Tamper alarms use different methods, such as:

- **Motion Detectors -** Which can be bypassed through keeping the detector covered with a slip of paper or card (which would work on the spring example in Figure 6.23).

- **Magnetisation -** Which can be bypassed through using an additional magnet to prevent the alarm going off.
- **Circuitry -** Which can be bypassed by using wire to prevent the circuit from breaking.

To prevent an attacker using one of these methods, it is recommended to use an independent tamper alarm (that is placed in a different location and uses a different strategy) to the one provided with the RFID scanner. A Malicious Actor is very likely to scout the physical location before an attack is launched, and will be taking note of what scanners are being used to research how to exploit them. Using a series of different strategies will greatly minimize the success rate of tampering, mitigating the likelihood of an ESP Key being used. Additionally, it is recommended that security cameras be positioned to have all scanners in view, so if any tamper alarms are set off the culprit can be identified. Any alarms raised should be dealt with by a Security engineer so that they can properly identify if an ESP key has been added.

6.3.5 Facial Recognition Versus Gait Recognition

This paper has discussed the various issues of Facial Recognition, from ethical to technological, and experimented in the various ways a Malicious Actor could bypass Algorithms through covering or obscuring their face. Facial Recognition clearly has its faults, which is not a good sign for a potential market leader of Access Control. There is a different biometric option, which surpasses Facial Recognition whilst mitigating its faults, being Gait Recognition.

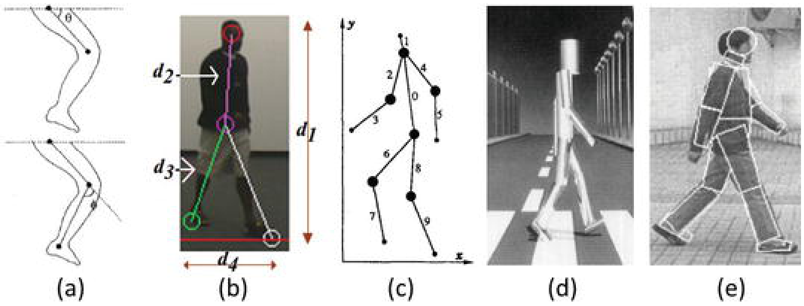


Figure 6.24: Gait Recognition (Almaadeed et al., 2018)

A Gait is the manner in which a person walks, through analysis of their stride, body shape, and speed (Nash, 2022). Gaits can be used as unique identifiers for an individual, and unlike Facial Recognition, cannot be easily covered. In-fact, to mask a person's gait, deliberate thought must be taken into each step (which would make them look unnatural to any onlooker) the entire time they are on camera. Kevin Mitnick, an infamous computer hacker, avoided gait recognition through putting rocks in his shoes whilst on the run from the police, showing the great effort it takes to have avoided the technology (Almaadeed et al. 2018). Figure 6.24 shows how gait recognition works, by emulating the movements to a skeletal structure, and comparing them versus a database of individual's gaits.

Gait recognition comes with obvious downsides, the key one being the time taken to initially add an individual to the database. Facial Recognition only needs a quick scan of a face to begin working, whilst Gait Recognition Technologies need a large sample of walking to become accurate. This technology also does not address the key ethical issues of Facial Recognition, rather it makes it harder to avoid with traditional methods like the Infrared Reflecting Glasses.

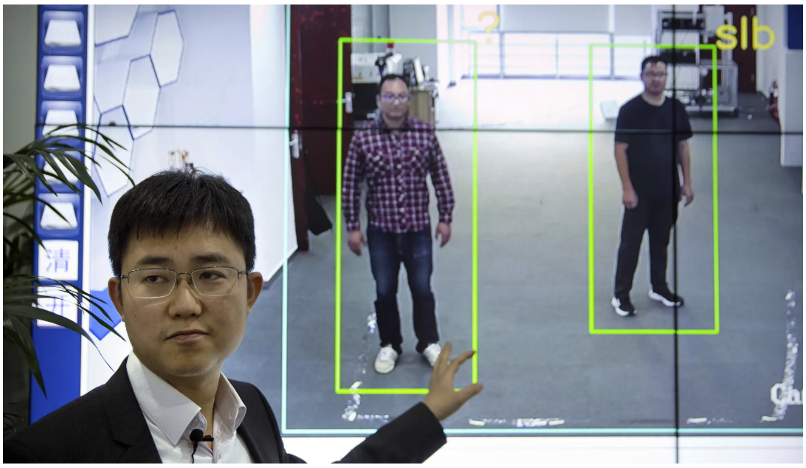


Figure 6.25: Gait Recognition example (NY Post, 2018)

From a SOC perspective this technology is still feasible, as Gait Recognition could be used consensually with employees, allowing the business to track staff movements, whilst any outsiders are left alone. This would aid in catching any Malicious Actor from pretending to be a staff member, as even if they have fraudulent Identification (through cloning or theft) they still would be highlighted as an outsider from the Gait Recognition Algorithm. Figure 6.25 shows Gait Recognition software working, with recognised individuals highlighted in green, whilst outsiders could be highlighted in red so security teams can keep an eye on them.

Overall, Gait Recognition seems like a much more effective and potentially ethical (through employee consent) form of biometric authentication. Facial Recognition is seen as the technology for the future of Access Control, but any SOC team should look into developing Gait technologies for a more secure workplace.

6.3.6 Facial Recognition Avoidance Methods

Gait recognition works in the long term, but any SOC team would want practical fixes to implement in the short term to prevent Malicious Actors using the avoidance methods found. An easy short term fix is to use security guards to enforce mandatory Facial Recognition scans when entering facilities, as part of the security policy for staff to follow. Guards if trained correctly have the ability to mitigate any avoidance method, easily spotting any facial painting or high facial coverage, whilst also being able to ask users to remove items until they get a successful recognition attempt, thus preventing the Reflectables sunglasses and less obtrusive coverings.

Physical security has far more value to an SOC team than most probably realise, when dealing with the tricky subject of Facial Recognition (which is often exploited through non-digital means) it is best to deal with it in person. Furthermore, having mandatory Facial Recognition as part of staff Access Control lessens the ethical concerns raised by the technology. Staff would have to consent to use of Facial Recognition as part of their terms of employment, with the face IDs only being used internally and deleted once they leave the organisation, making the data GDPR-compliant. This gives back power to the user, allow them to know exactly how their facial information is being used and processed, and giving them an option to remove it (which doesn't exist on much of the Facial Recognition systems found today).

6.4 Putting Solutions into Practise

These solutions help to prevent the issues found throughout the project, but to demonstrate this further, a final secure testing environment was created, which was inspired from the concluding questions of the survey. The program was written in Python 3, and took aspects from previous environments to create a better method of Access Control, also showing to SOC teams that security can be quickly improved when fixes are implemented. The system used the nondescript scanner previously used in the Python SQL environment, and initially was run on the Raspberry Pi board but was switched over to a Kali Linux virtual machine (after the Pi Camera stopped working). The program used AWS Rekognition to authenticate users, as from testing it was proved to be the best option for Facial Recognition. A flowchart of the program's functions can be seen in Figure 6.26, showing the process it takes to authenticate users.

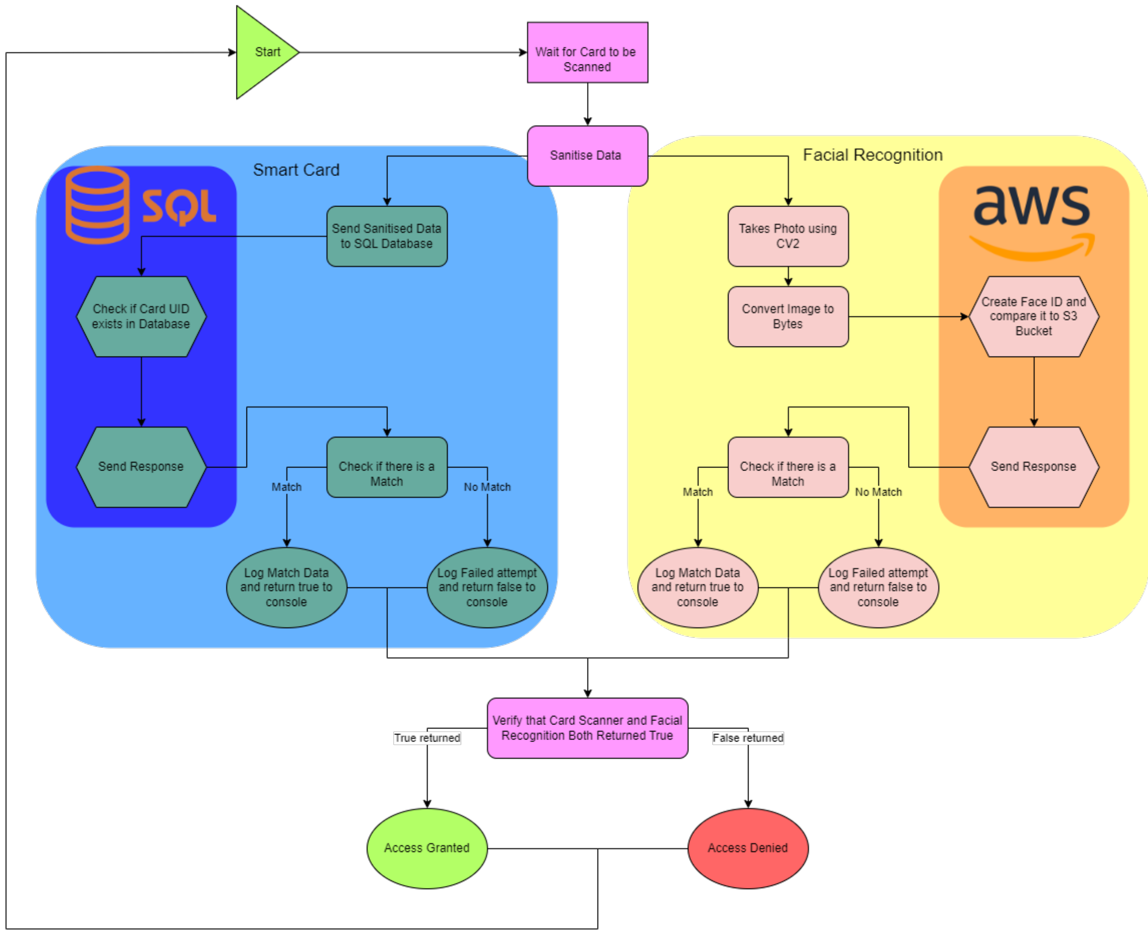


Figure 6.26: Secure Environment Flowchart

Much of the code was reused to form the combined environment, however, there were some changed to improve security. Notably went through a Sanitisation process, and the Query sent to the SQL Database was altered to prevent SQL Injection. This can be seen in Figure 6.27, specifically in the Query line.

```
#Checks Clean value against Database
def checkCard(sanitisedValue):
    cur.execute( #SQL Injection safe Query
        """SELECT ID from cardID WHERE cardNumber = '%(cardNumber)s'""" % {'cardNumber': sanitisedValue}
        )
    foundInDB = cur.fetchone()
    #If a match was found
    if foundInDB != None:
        print("SQL: Card Matches")
        return True
    else: #If nothing was found
        print("SQL: Card not found in Database")
        return False
```

Figure 6.27: Code for checking Card against SQL Database, including a safe Query

The main operation code was also changed somewhat, this time to be cleaner and less verbose to the operating user. The program will only inform the user if Access has been granted or not, without revealing if the issue is with their face or card if they fail to gain entry. This was originally achieved through an LED screen attached to the Raspberry Pi, but had to be converted to just sending to the running terminal. Of course the actual success messages would be hypothetically sent to SOC team most likely through logs, so that they can verify any issues. These are the things of note when making this secure Multi-factor Authentication system, the full code can be found in Appendix A.

```
#Constantly running code
while True:
    print("--------------------------------")
    scannedCard = input("Scan Card and Look into Camera to Begin: ")

    #Verify if something has been entered
    if scannedCard != None:
        sanitisedValue = dataSanitisation(scannedCard)
        isRecognised = checkFace()
        processedCard = checkCard(sanitisedValue)

        #Checking if both the Card and Face matches to gran access
        if (isRecognised == True and processedCard == True):
            print("Access Granted")
        else:
            print("Access Denied")
        #Finishes program with non-descript answer to users
        print("Finished Operation")
        print("--------------------------------")

    sleep(0.5)
```

Figure 6.28: Main Function of the Secure Environment

The running code can be seen in Figure 6.29, showing the program allowing entry after the card is first sanitised, followed by the face matching, and finally with the sanitised value matching the SQL database. The figure also shows the result of several denied request, such as when a card is not found in the database, when the face does not match, or when no face is found in the frame.

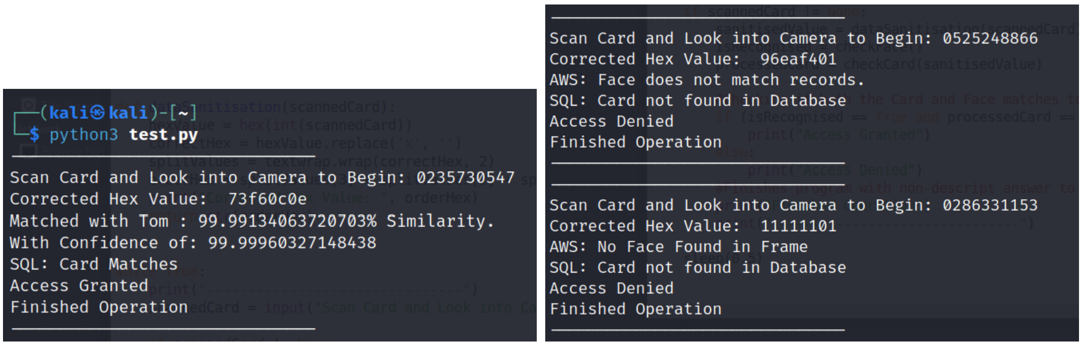


Figure 6.29: Secure Program Successfully Authenticating a User, whilst also denying entry to another

This Access Control environment mitigates much of the issues found throughout the project, and can be implemented by any competent SOC team to improve security mechanisms. This program alone fills two thirds of the MFA triad, with "Something you have" through the Smart Card, and "Something you are" through Facial Recognition. It can be safely assumed that Employee workstations have passwords on them, completing the last third of "Something you know", meaning that this system can easily be classes as having full Multi-factor Authentication.

6.5 Evaluation of Success

This section will round off the discussion with an overall evaluation of success, using the Research Questions, Objectives, and Problem statement from the Introduction of this document. These will be the best indicators of whether the research, experimentation, and testing met the original goals or not.

6.5.1 Research Questions

A series of research questions were written at the start of the project to contrast against the reality once all the testing and experimentation had concluded. The results of this are:

1. **How effective is Facial Recognition as a security mechanism?**
   - **Hypothesis -** Facial recognition is a very effective tool for security, with little methods to exploit it.
   - **Reality -** Facial Recognition is a very effective tool for security, with a couple of methods to exploit it to varying success, such as Face covering, Facial Painting, and Reflective Glasses.
2. **How secure are Smart cards as a form of access control?**
   - **Hypothesis -** Smart Cards are an insecure form of access control, with many ways to exploit the technology to gain illegitimate access.
   - **Reality -** Smart Cards are an insecure form of access control, with a few highly effective ways to exploit the technology to gain illegitimate access. The simple nature of Smart Cards is a double-edged sword, providing easy ways to clone or intercept Card UIDs, whilst being too simple to before more complicated and potentially damaging attacks.
3. **How successful would a malicious actor exploiting these technologies be against a business?**
   - **Hypothesis -** A Malicious Actor would not be able to use Facial Recognition exploits to their advantage, as it is hypothesised that any usable exploit will either be impracticable or obvious to any security staff. Exploited Smart cards on the other hand will be an incredibly useful tool in any Malicious Actor's arsenal, and prove to be a key concern to any business using it as a form of security.
   - **Reality -** A Malicious Actor would be able to use Facial Recognition exploits to their advantage, particularly methods that were more subtle, effectively avoid recognition. Exploited Smart Cards are a reasonably effective tool in a Malicious Actor's arsenal, through ESP Keys, cloning, and various tools, making this a key concern to any SOC team.

6.5.2 Aim and Objectives

The Aim of this project was to "demonstrate the risks and inherent weaknesses in standard physical security mechanisms", which was done through the use of "Experimentation and Exploit Development". The research presented in this project has definitely met this aim, showing all the issues found in Smart Cards and Facial Recognition, not only through literature but also through practical experimentation that extensively targeted testing environments in the same manner a Malicious Actor would, proving the suspected weakness found in standard Access Control. The only part of the Aim that may not have been fulfilled by the project was "Exploit Development", which was attempted through SQL Injection and Shellcode, but later found to be not possible. Although this part of the project resulted in failure, it still contributed to the final conclusions, whilst providing valuable research to any SOC team.

The objectives were set at the start of the project, before any testing, experimentation, or any significant research. The original goal was to achieved all these objectives, with the reality being different to hypothetical plans. The objectives were:

- **Find a way to prevent facial recognition without just covering the subject's face -** This was achieved practically through the painting technique demonstrated in this project, being able to avoid recognition on the low and medium level Facial Recognition Environments. This was also theoretically achieved through research into avoidance techniques, such as the Reflectables glasses or the LED obfuscating method.

- **Discover if security will stop a subject who is deliberately trying to hide their face -** This was achieved through the survey, where it was found that Security would be called to any users using the painting technique. Additionally, the likelihood of being reported to Security increases as Face Coverage increases, having a total face coverage between 55% and 65% was the sweet spot for maximum effectiveness and minimum suspicion. Finally, the aforementioned Reflectables were found to draw the least suspicion from Security and the General Public. These all contribute to successfully meeting this objective.

- **Develop a Skeleton key for a Smart card system -** This objective was achieved in part, as a Skeleton key simply refers to the master key for a system. This objective was written when a Real Life environment was planned to be used for testing, after being denied access it was no longer possible to make a skeleton key in the planned way. However, many different methods were discussed on how to make a Skeleton key, from simply cloning using scanners or more advanced tools like the Flipper Zero, to devastating items like the ESP Key which was discussed at length on how it could be used to create a skeleton key.

- **Replicate another Smart Card without the use of simply cloning the card -** This objective was not achieved as planned, as it was written again with the notion of using a Real Life testing environment. It was planned to find patterns in UIDs to be able to recreate card details, presuming that systems had been set up with sequential card number or something similar. This objective was achieved theoretically through the ESP key, which instead of cloning intercepted Card UIDs to then be replayed later, essentially stealing card contents without cloning.

To discuss further, a core objective of the project was to create a skeleton key, able to access all the restricted areas of a real life system. This was to be achieved through learning how organisations tend to store user IDs, such as sequential numbers, or specific designations. It was predicted that sequential cards might have admin access if the user ID was changed to a low value (0 or 1), or if there were specific designators like residents of block B floor 40 having a user ID of B40, whilst guards having a universal value like an asterisk to note access to all floors. Alas, this was simply not feasible for this project, but does not devalue the work conducted despite these limitations.

6.5.3 Scope

The original Scope of the project was stuck to throughout, with experimentation into Smart Cards and tangible avoidance of Facial Recognition cameras. The security reality of these Access Control methods has already been discussed in the Research Question section. The only section not mentioned in the scope was the construction of the Secure solution, as it was never planned and a last minute addition to the document. This was due to the rather disappointing results from Smart Cards, being too limited to perform any interesting exploits. Spare time from efficiency and the updated Gantt chart allowed for this development, demonstrating how with relative ease security can be increased in a business.

6.5.4 Problem Statement

A Problem Statement was written as part of the Introduction after conducting background research on the subject of Access Control. This Statement discussed that no significant research had been done on the effectiveness of Access Control as a whole, testing the physical security mechanisms to their limits. Smart Cards were the go-to choice from background literature, with authors hinting Facial Recognition would be the likely replacement. Authors discussed vaguely the issues found in these technologies, notably the ethical problems of Facial Recognition and the cloning of Smart Cards

This Problem Statement was expanded on by the Literature Review, using background papers to guide the course of past Academic research. The discussed the ease of cloning cards further, but neglected any other exploitation through Smart Cards. At the time, this was presumed to be a gap in literature, but was proven to simply be not possible through experimenting with the technology.

A real gap in literature was found when researching Facial Recognition, as no authors had discussed the various ways to avoid detection. This was thoroughly experimented on, both physical tests and hypothetical discussion on the various methods found that work. The testing was done with the foresight that not all obfuscation methods would be successful in avoiding security and staff suspicion, which was tested using the survey on the general public. The results from this portion of testing and experimentation successfully filled the gap in Literature, allowing SOC teams to know what a Malicious Actor would likely use to avoid recognition.

The Problem Statement really focuses around the quote "Knowing the enemy is half the battle" by Sun Tzu, which served as the entire philosophy of this project. The "Malicious Actor" is well understood as this project concludes, with the various ways they could exploit Access Control for illegitimate entry. Furthermore, the Solutions discussed would mitigate any technique presented in this paper, allowing SOC teams to ensure the safety of their workplace and fellow employees.

Chapter 7

Conclusion

In Conclusion, this project explored the security of common Access Control thoroughly, through deep dives into Academic Literature to practical testing and experimentation. The research conducted illuminated any SOC team on the true insecurities found in physical security, and how a Malicious Actor would likely exploit them. The two areas of research were both found to be vulnerable through easily replicable methods, often with very damaging consequence.

Smart Cards were found to be a very insecure as a common form of Access Control, with it being incredibly easy to clone card contents through a variety of tools. Additionally, with devices like ESP Keys this flawed security mechanism could be exploited to devastating effects, with the ability to harvest all cards used on a scanner. Smart Cards are a very simple technology, meaning that they could not be used for more sophisticated attacks, but this does not lessen the inherent risk they bring to security systems.

Facial Recognition was found to be more exploitable than previously thought, with many different methods of obfuscating cameras. The various methods were effective in their own capacity, such as the painting technique working well against low level systems. The interesting results came from practical methods to avoid recognition, such the Reflectables glasses or the most effective level of facial coverage to avoid detection whilst minimizing suspicion.

The extensive experimentation and testing revealed one key fact about Access Control exploitation, and that is the simplest options are often the most effective. Cloning, covering a large portion of the face, or reflecting light into cameras were all found to be very effective and easy ways to disrupt Access Control mechanisms.

This project not only explored the true security of Access Control, but also provided effective fixes to be implemented by SOC teams in order to prevent exploiting from a Malicious Actor. The solutions effectively mitigate the vulnerabilities and dangerous devices found in research, and were demonstrated by construction of a secure system using Multi-Factor Authentication.

Overall, this project was a success, contributing to the field of security by filling gaps in literature, pushing common technologies to their limits, and effectively presenting solutions for a safer tomorrow. Access Control is critical not only to protecting a businesses resources, but also for protecting people from outside threats. Physical Security is a market that will only keep growing, if the foundations are weak how can it ever be secure. Hopefully with the research presented the right steps towards more effective security can be taken, transforming Access Control technologies to be more than the illusion of security they currently are into something that an SOC team can truly be proud of.

7.1 Future Work

Although this project was extensive in its research, experimentation, and testing, there is still room for future research to be conducted. If given more time, or if the project was later expanded upon, then these would be areas that would see further research.

Several items were either unavailable or out of budget when it came to this project, such as the Flipper Zero and the Reflectables glasses. These would have provided more depth to the resources available to a Malicious Actor, and would have been interesting to research to understand what threat they pose to a buildings' security. Additionally, one of the key items present through this project was unfortunately destroyed by customs, preventing any real use in the project. This was a key loss to research, as the ESP Key presented the most threat to SOC teams when discussing Smart Card Exploitation. If conditions were better, these items would have been purchased and used to create a fuller image of Access Control exploitation.

On a similar vein, better testing environments would have allowed for much better and more realistic results. The testing environments constructed were effective throughout the experimentation, and led to good research that would not have been acquired if access to real systems had been granted. However, the most effective way to testing various exploitation methods would have been through testing on a real life system that is used in a business or organisation. Infrared cameras would have also greatly benefitted the testing of Facial Recognition solutions, as real system are far more likely to use this superior way to capture user faces. If resources allowed, these environments would have been acquired, leading to more rounded and overall realistic research.

The secure solutions provided an effective groundwork for what Access Control should evolve to become, but due to be a late addition, lacked the time needed to construct an environment with all the solutions discussed. The secure solution can be improved in numerous ways, such as usage of more secure MIFARE cards, to constructing a CCTV based Facial Recognition solution to identify strangers to SOC teams. Literature pointed in the direction of Mobile Applications replacing both Smart Cards and Facial Recognition Cameras. In a larger project, significant time and effort could have been allocated to building a secure Access Control application for SOC teams to deploy to increase security.

Chapter 8

References

Academic References:

1. Abellon, A.P., Ariola, C.J., Blancaflor, E., Danao, A.K., Medel, D., Santos, M.Z. 2021. Risk Assessments of Unattended Smart Contactless Cards. *2021 IEEE 8th International Conference on Industrial Engineering and Applications.* pp. 338-341.

2. Ahmad, Z., Olowolayemo, A., Zeki, A.M. 2016. Security Failures in EMV Smart Card Payment Systems. *2016 6th International Conference on Information and Communication Technology for The Muslim World.* pp. 240-243.

3. Anderton, J., Claes, P., Cook-Deegan, R., Doerr, M., Evans, B.J., Katsanis, S.H., Lee, M.K., Tenenbaum, J.D., Wagner, J.K., Weinberg, S.M. 2022. 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). *IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, VOL. 3, NO. 1, MARCH 2022.* pp. 9-15.

4. Alazmi, S., Khan, A.R., Yu, Q. 2018. A Comprehensively Secure Smart card access controls. *2018 21st Saudi Computer Society National Computer Conference (NCC).* pp. 1-4.

5. Almeida, D., Lomas, E., Shmarko, K. 2021. The ethics of facial recognition technologies, surveillance, and accountability in an age of artifcial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics (2022).* pp. 377-387.

6. Altawy, R., Youssef, A.M. 2016. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Acces, Vol. 4.* pp. 959-979.

7. Attoh-Okine, N.O., Shen, L.D. 1995. Security Issues of Emerging Smart Cards Fare Collection Application in Mass Transit. *Pacific Rim TransTech Conference. 1995 Vehicle Navigation and Information Systems Conference Proceedings. 6th International VNIS. A Ride into the Future.* pp. 523-526.

8. Benamara, N.K., Keche, M., Munyaradzi, Z., Wellington, M. 2021. Securing E-payment

Systems by RFID and Deep Facial Biometry. *2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA).* pp. 151-157.

9. Benes, V., Dzurenda, P., Hajny, J., Malina, L. 2017. Efficient and Secure Access Control System Based on Programmable Smart Cards. *2017 40th International Conference on Telecommunications and Signal Processing (TSP).* pp. 32-36.

10. Bhatt, S., Gupta, M., Park, J. Sandhu, R. 2021. Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems. *IEEE Access, vol. 9.* pp. 1510004-151022.

11. Bozzato, C., Bundy, A., Focardi, R., Gkaniatsou, A., McNeil, F., Steel, G. 2015. Getting to know your Card: Reverse-Engineering the Smart-Card Application Protocol Data Unit. *ACSAC '15: Proceedings of the 31st Annual Computer Security Applications.* pp. 441-450.

12. Büttner, V., Hensel, M.F., Melgaard, M., Olsen, R.L., Sørensen, J.V., Teule, J.J. 2020. Examining the Cyber Security of a Real World Access Control Implementation. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).* pp. 1-3.

13. Carreira, R., Lopes, S.I., Pereira, H., Pinto, P. 2020. Hacking the RFID-based Authentication System of a University Campus on a Budget. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI).* pp. 1-5.

14. Chan, T.W., Soh, C.S., Yap, V.V. 2012. Embedded based tailgating/piggybacking detection security system. *2012 IEEE Colloquium on Humanities, Science and Engineering (CHUSER).* pp. 277-282.

15. Cornélis, M., Grandjean, N., Lobet-Maris, C. 2008. Sociological and Ethical Issues in Facial Recognition Systems: Exploring the Possibilities for Improved Critical Assessments of Technologies?. *Tenth IEEE International Symposium on Multimedia.* pp. 602-606.

16. Craft, R.L. 2017. Red Teaming in the Age of IOT. *2017 12th System of Systems Engineering Conference (SoSE).* pp. 1-6.

17. Jiang, E. 2020. A review of the comparative studies on traditional and intelligent face recognition methods. *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL).* pp. 11-15.

18. Kamble, V.B. & Zinjurde, A.M. 2020. Credit Card Fraud Detection and Prevention By Face Recognition. *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC).* pp. 86-90.

19. Kasthuriarachchi, N., Rasnayaka, S., Seneviratne, S., Vidanaarachchi, R., Wijnands, J.S. 2021. Imagery, Privacy and Ethics: An Overview of Partially Occluded Facial Biometric Analysis in the Era of Face Masks. *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET).* pp. 1-8.

20. Kim, Y.G., Kim, Y., Yu, J.Y. 2021. Intelligent Video Data Security: A Survey and Open Challenges. *IEEE Access Rapid Review, VOLUME 9, 2021.* pp. 26948-26967.

21. Khan, M.F.F. & Sakamura, K. 2016. A Secure and Flexible e-Health Access Control System with Provisions for Emergency Access Overrides and Delegation of Access Privileges. *2016 18th International Conference on Advanced Communication Technology (ICACT).* pp. 541-546.

22. Mao, Q., Xu, C., Zhang, F., Zhang, T. 2020. Geometry Guided Pose-Invariant Facial Expression Recognition. *IEEE Transactions on Image Processing, vol. 29.* pp. 4445-4460.

23. Memiş, A. 2018. Facial feature representation and face recognition with Neighborhood-based Binary Patterns. *2018 26th Signal Processing and Communications Applications Conference (SIU).* pp. 1-4.

24. Miller, S. & Smith, M. 2022. The ethical application of biometric facial recognition technology. *AI & SOCIETY (2022).* pp. 167-175.

25. Milossi, M. 2021. Remote biometric identification systems and ethical challenges: The case of facial recognition. *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM).* pp. 1-6.

26. Shen, J., Xu, J., Zhang, R., Zhang, Z. 2020. Two-stage Recognition and Beyond for Compound Facial Recognition. *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020).* pp. 900-904.

Other References:

ACS. N.D. Utility tools. [online] Advanced Card Systems Ltd. Available at: https://www.acs.com.hk/en/utility-tools/ [Accessed 28/11/2022]

Akati, J. & Conrad, M. 2021. Anti-Tailgating Solution Using Biometric Authentication, Motion Sensors and Image Recognition. *021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech).* pp. 825-830.

Alibaba. N.D. Biometric Fingerprint and Face Recognition and RFID Card Reader Time Attendance and Access Control Device. [online] Alibaba. Available at: https://www.alibaba.com/product-detail/Biometric-Fingerprint-and-Face-Recognition-and_817120972.html [Accessed 16/04/2023]

Almaadeed, N., Almaadeed, S., Rida, I. 2018. Robust gait recognition: a comprehensive survey. *The Institution of Engineering and Technology, Volume 8, Issue 1.* pp. 14-28.

AWS. N.D. Amazon Rekognition. [online] AWS. Available at: https://aws.amazon.com/rekognition/ [Accessed 11/04/2023]

Balboa, M. 2021. MFRC522. [online] GitHub. Available at:
https://github.com/miguelbalboa/rfid [Accessed 15/04/2023]

Baran, G. Amazon Banned Flipper Zero Pentesting Tool. [online] GB Hackers. Available at:
https://gbhackers.com/flipper-zero-pentesting/amp/ [Accessed 13/04/2023]

BasuMallick, C. 2022. What Is an SQL Injection? Meaning, Cheatsheet, Examples, and Prevention Best Practices for 2022. [online] SpiceWorks. Available at:
https://www.spiceworks.com/it-security/application-security/articles/what-is-sql-injection/ [Accessed 20/04/2023]

Beard, M. 2020. How Your Red Team "HID" in Your Readers - ESPKey Attacks. [online] Direct Defense. Available at:
https://www.directdefense.com/how-your-red-team-hid-in-your-readers-espkey-attacks/ [Accessed 04/04/2023]

Bates, G. 2008. The "face" on Mars. [online] Creation. Available at:
https://creation.com/face-on-mars [Accessed 22/02/2023]

BSC. N.D. NXP Mifare® Classic 1K (Blank Card). [online] Buy Smart Card. Available at:
https://buysmartcard.com/product/mifare-classic-1k-blank-card/ [Accessed 16/04/2023]

Cardia, A., Mozur, P., Qian, I., Xiao, M. 2022. China's Surveillance State is Growing. These Documents Reveal How. [online] The New York Times. Available at:
https://www.nytimes.com/video/world/asia/100000008314175/china-government-surveillance-data.html [Accessed 22/02/2023]

Card Logix. N.D. NXP MIFARE® DESFire® EV1 8K Card. [online] Card Logix. Available at:
https://www.cardlogix.com/product/mifare-desfire-ev1-8k/ [Accessed 16/04/2023]

Cooper, S. 2014. What you need to know about card skimming. [online] EnGadget. Available at:
https://www.engadget.com/2014-07-28-credit-card-skimming-explainer.html [Acccessed 22/02/2023]

Delta. N.D. Tamper contact (anti-tamper). [online] Delta Shop. Available at:
https://shopdelta.eu/tamper-contact-anti-tamper_l2_aid892.html [Accessed 07/04/2023]

Digital ID. 2022. How To Prevent Access Control Card Cloning. [online] Digital ID. Available at:
https://www.digitalid.co.uk/blog/prevent-access-control-card-cloning [Accessed 16/04/2023]

Ferrari, P. 2020. Activists are fighting facial recognition AI with face paint. They use cubist-inspired designs to foil algorithms. [online] CapStan. Available at:
https://www.capstan.be/activists-are-fighting-facial-recognition-ai-with-face-paint-they-use-cubist-inspired-designs-to-foil-algorithms/
[Acccessed 22/02/2023]

FlipperZero. N.D. Multi-tool Device for Geeks. [online] FlipperZero. Available at: https://flipperzero.one/ [Accessed 22/02/2023]

GeniSoftware. N.D. Smart Card Reader. [online] GeniSoftware. Available at: https://genisoftware.net/smart-card-reader/ [Accessed 28/11/2022]

Getahun, H. 2022. AI-designed face paint inspired by Juggalos could potentially fool the 15,000 facial recognition cameras at the Qatar World Cup. [online] Insider. Available at: https://www.businessinsider.com/ai-face-paint-camera-qatar-world-cup-facial-recognition-2022-12 [Accessed 12/04/2023]

GitHub. 2021. MIFARE Classic Tool (MCT). [online] GitHub. Available at: https://github.com/ikarus23/MifareClassicTool [Accessed 27/04/2023]

Hopkins, J. 2018. Locked doors: an illusion of security. [online] The Patriot Press. Available at: https://lhspatriotpress.com/opinion/2018/09/26/locked-doors-an-illusion-of-security/ [Accessed 28/11/2022]

Ikinamo. 2013. Privacy visor glasses jam facial recognition systems to protect your privacy. [online] YouTube. Available at: https://www.youtube.com/watch?v=LRj8whKmN1M [Accessed 08/04/2023]

Java T Point. N.D. K-Nearest Neighbor(KNN) Algorithm for Machine Learning. [online] Java T Point. Available at: https://www.javatpoint.com/k-nearest-neighbor-algorithm-for-machine-learning [Accessed 22/02/2023]

Larkin, A. 2017. AWS re:Invent 2017 Day 3. Amazon Rekognition Video Enables Object and Face Recognition. [online] Cloud Academy. Available at: https://cloudacademy.com/blog/amazon-rekognition-video-feature-announcement/ [Accessed 28/11/2022]

Mobile2go. N.D. Samsung Galaxy S21 5G [8GB RAM + 256GB ROM] - Original Samsung Malaysia. [online] Mobile2go. Available at: https://www.mobile2go.com.my/galaxy-s21-5g [Accessed 09/04/2023]

Morse, J. 2019. Fight facial-recognition technology with Phantom glasses. [online] Mashable. Available at: https://mashable.com/review/review-reflectacles-phantom-anti-facial-recognition-technology-glasses-frames [Accessed 08/04/2023]

Nash, J. 2022. Gait recognition could be better than face biometrics to ID coboting workers. [online] Biometric Update. Available at: https://www.biometricupdate.com/202208/gait-recognition-could-be-better-than-face-biometrics-to-id-coboting-workers [Accessed

13/04/2023]

NY Post. 2018. China's new recognition tech can ID people by how they walk. [online] New York Post. Available at:
https:
//nypost.com/2018/11/06/chinas-latest-recognition-technology-can-id-people-by-how-they-walk/
[Accessed 13/04/2023]

OpenCV. N.D. OpenCV modules Documentation. [online] OpenCV. Available at:
https://docs.opencv.org/4.x/ [Accessed 15/04/2023]

Person, C. 2022. The Flipper Zero is a Swiss Army knife of antennas. [online] The Verge.
Available at: https://www.theverge.com/23433594/
flipper-zero-hacking-gadget-wireless-pentesting-open-source-antenna [Accessed 22/02/2023]

Pollack, E. 2017. Sanitizing Inputs: Avoiding Security and Usability Disasters. [online] SQLShack.
Available at:
https://www.sqlshack.com/sanitizing-inputs-avoiding-security-usability-disasters/ [Accessed 20/04/2023]

PortSwigger. N.D. SQL Injection. [online] PortSwigger. Available at:
https://portswigger.net/web-security/sql-injection [Accessed 20/04/2023]

PurpleSec. 2022. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022.
[online] PurpleSec. Available at:
https://purplesec.us/resources/cyber-security-statistics/ [Accessed 28/11/2022]

Recfaces. 2021. Gait Recognition System: Deep Dive into This Future Tech. [online] Recfaces.
Available at:
https://recfaces.com/articles/what-is-gait-recognition [Accessed 13/04/2023]

Red Team Tools. N.D. ESPKey Wiegand Interception Tool. [online] Red Team Tools. Available at:
https://www.redteamtools.com/espkey [Accessed 04/04/2023]

Reflectables. N.D. Phatom. [online] Reflectables. Available at:
https://www.reflectacles.com/order/phantom [Accessed 08/04/2023]

Reuters. 2019. Amazon will serve any government agency with facial recognition technology, so long as it's legal. [online] VentureBeat. Available at:
https://venturebeat.com/ai/
amazon-will-serve-any-government-agency-with-facial-recognition-technology-so-long-as-its-legal/
[Accessed 11/04/2023]
RFID4u. N.D. How to Select a Correct Tag - Frequency. [online] RFID 4 u. Available at:
https://rfid4u.com/rfid-frequency/ [Accessed 04/04/2023]

Science Buddies. 2013. Steps of the Scientific Method. [online] Science Buddies. Available at:

https://www.sciencebuddies.org/science-fair-projects/science-fair/steps-of-the-scientific-method [Accessed 28/11/2022]

SentinelOne. 2019. Malicious Input: How Hackers Use Shellcode. [online] SentinelOne. Available at:
https://www.sentinelone.com/blog/malicious-input-how-hackers-use-shellcode/ [Accessed 20/04/2023]

Shone, T. 2013. Surveillance State. [online] The New York Times. Avaialable at:
https://www.nytimes.com/2013/07/21/books/review/the-panopticon-by-jenni-fagan.html [Acccessed 22/02/2023]

Stevens, D. 2009. Shellcode On a MIFARE RFID Tag. [online] Didier Stevens blog. Avaible at:
https://blog.didierstevens.com/2009/02/23/shellcode-on-a-mifare-rfid-tag/ [Accessed 27/04/2023]

Tapper, J. 2020. Hiding in plain sight: activists don camouflage to beat Met surveillance. [online] The Guardian. Available at:
https://www.theguardian.com/world/2020/feb/01/privacy-campaigners-dazzle-camouflage-met-police-surveillance [Accessed 12/04/2023]

Wankhede, C. 2022. Facial recognition on smartphones: Is it secure and should you use it?. [online] Android Authority. Available at:
https://www.androidauthority.com/face-unlock-smartphones-3043993/ [Accessed 09/04/2023]

YourProps. N.D. Baby Driver, Jon Hamm's Screen Used LED Glasses. [online] Your Props. Available at:
https://www.yourprops.com/Jon-Hamm-s-Screen-Used-LED-original-movie-costume-Baby-Driver-2017-YP809508.html [Accessed 08/04/2023]

Chapter 9

Appendix

9.1 Appendix A - Code

9.1.1 Arduino RFID Scanner

```
    #include <SPI.h>
#include <MFRC522.h>

#define RST_PIN          9
#define SS_PIN           10
#define userNumber 3
MFRC522 mfrc522(SS_PIN, RST_PIN);

//Array of approved Users
char* UIDs[2] = {"73 F6 0C 0E", "B3 14 16 9A"};


//Sets up board and reader
void setup() {
  Serial.begin(9600);
  while (!Serial);
  SPI.begin();
  mfrc522.PCD_Init();
  delay(4);
  mfrc522.PCD_DumpVersionToSerial();
  Serial.println(F("Scan card to enter:"));
}

//Contantly checks for a card to read
void loop() {
  if ( ! mfrc522.PICC_IsNewCardPresent()) {
    return;
  }
  if ( ! mfrc522.PICC_ReadCardSerial()) {
    return;
```

```
    }

  //prints once a card is read
  Serial.println(F("Scanned UID:"));

   String content= "";
   byte letter;

   //Input from reader needs to be sanitised before use
   for (byte i = 0; i < mfrc522.uid.size; i++)
  {
     Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
     Serial.print(mfrc522.uid.uidByte[i], HEX);
     content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
     content.concat(String(mfrc522.uid.uidByte[i], HEX));
  }


  Serial.println();
  content.toUpperCase(); //More sanitisation
  int approved = 0; //To indicate if they are allowed access

  //Cleaned variable is compared against an array of User IDs
  for (int i = 0; i < 2; i++){
    if (content.substring(1) == UIDs[i]){
       Serial.println("Authorized access");
       Serial.println();
       approved = 1;
      }
     }

  if (approved == 0) {
    Serial.println("Accessed Denied");
    Serial.println();
    }

  //Cleanup, resets the reader for new entry request
  Serial.println("");
  mfrc522.PICC_HaltA();
  return 1;
}
```

9.1.2 Python SQL Scanner

```
    from time import sleep
import string
import mariadb
import sys
import textwrap


#Connecting to Database
try:
    conn = mariadb.connect(
        user="your-username-here",
        password="your-password-here",
        host="127.0.0.1",
        port=3306,
        database="your-database-here"
        )
except mariadb.Error as e: #Catching Errors
    print(f"Error connecting to MariaDB Plaftform: {e}")

#Connection to use later
cur = conn.cursor()


#Main Code runs continously
while True:
    #Takes in Decimal Card Number from Scanner
    scannedCard = input("Scan Card to Begin: ")

    #Verifying that card has scanned
    if scannedCard != None:
        #Convert from Decimal to Hex
        hexValue = hex(int(scannedCard))
        correctHex = hexValue.replace('x', '') #Remove
        splitValues = textwrap.wrap(correctHex, 2)#Split Hex into pairs
        #Rearrange Hex pairs to true value(e.g. OE OC F6 73 to 73F60C0E)
        orderHex = splitValues[3] + splitValues[2] + splitValues[1] + splitValues[0]

        #Query Database using new value
        cur.execute(
            """SELECT ID from cardID WHERE cardNumber = '%s'""" % orderHex
            )
        #Returning any matches
        foundInDB = cur.fetchone()
        if foundInDB != None: #If there was a match
            print("Access Granted")
        else: #If no matches were returned
```

```
            print("Access Denied")
        print("Finished Operation")

    sleep(0.5)
```

9.1.3 Python Facial Recognition

main.py

```
#Imports
import cv2
import pickle

#Setting up
video = cv2.VideoCapture(0)
box = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")
recognise = cv2.face.LBPHFaceRecognizer_create() #Face Recogniser Setup
recognise.read("faceLabels.yml") #Loading labels

# Creating the Label Array
labels = {}
with open("labels.pickle", 'rb') as f:
    og_label = pickle.load(f)  ##
    labels = {v: k for k, v in og_label.items()}  ##
    print(labels)

# Main Operation
while True:
    check, frame = video.read()
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    # Switch frames to Grayscale for easier computation
    face = box.detectMultiScale(gray, scaleFactor=1.2, minNeighbors=5)
    # Placing a box around any Face found

    for x, y, w, h in face:
        face_save = gray[y:y + h, x:x + w]

        # Taking the face and seeing if it matches any saved
        ID, conf = recognise.predict(face_save)

        # If the confidence is high enough then identify them
        if conf >= 50:
            print("Face Recognised as ", labels[ID])
            # Display user name and a green box
            cv2.putText(frame, labels[ID], (x - 10, y - 10), cv2.FONT_HERSHEY_SIMPLEX,
            frame = cv2.rectangle(frame, (x, y), (x + w, y + h), (0, 255, 0), 4)
        else:
            print("Not Recognised")




    # Showing the video on screen
```

```
    cv2.imshow("Video", frame)
    key = cv2.waitKey(1)
    #Key for clean Keyboard Interrupts
    if (key == ord('q')):
        break

#Final Cleanup
video.release()
cv2.destroyAllWindows()
```

labelMaker.py

```
# import the required libraries
import cv2
import os
import numpy as np
from PIL import Image
import pickle


#Setting up
cascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")
recognise = cv2.face.LBPHFaceRecognizer_create()
BASE_DIR = os.path.dirname(os.path.abspath(__file__))# Setting the directory
my_face_dir = os.path.join(BASE_DIR,'faceImages')

# Created a function
def getdata():

    #Arrays for data
    current_id = 0
    label_id = {}
    face_train = []
    face_label = []


    # A loop for creating labels for multiple users
    for root, dirs, files in os.walk(my_face_dir):
        for file in files:
            # Verifying the file type (png or jpg)
            if file.endswith("png") or file.endswith("jpg"):
                path = os.path.join(root, file) # Setting Image path

                # Folder name becomes the user ID
                label = os.path.basename(root).lower()
                if not label in label_id:
                # changing the ID number for each subsequent user
                    label_id[label] = current_id
```

```
                current_id += 1
            ID = label_id[label]
            pil_image = Image.open(path).convert("L")
            # Changing to grayscale for computation

            # converting the image data into numpy array
            image_array = np.array(pil_image, "uint8")
            face = cascade.detectMultiScale(image_array)

            # Identifying key features to create labels for
            for x,y,w,h in face:
                img = image_array[y:y+h, x:x+w]
                cv2.imshow("Test",img)
                cv2.waitKey(1)
                face_train.append(img)
                face_label.append(ID)

    # Adding all the labels to the pickle file
    with open("labels.pickle", 'wb') as f:
        pickle.dump(label_id, f)
    return face_train,face_label

# Creating final file of labels
face,ids = getdata()
recognise.train(face, np.array(ids))
recognise.save("faceLabels.yml")
```

9.1.4 Python AWS

```
    from time import sleep
import os
import boto3
import string


#Main code that runs constantly
while True:
    beginProgram = input("Hit Enter to begin")
    if beginProgram != None:
        #Takes a picture using Raspberry Pi camera
        os.system("raspistill -o image.jpg")
        image = "image.jpg"

        #Connect to rekognition and convert image to bytes
        client = boto3.client(service_name="rekognition")
        with open(image, "rb") as sourceImage:
            sourceBytes = sourceImage.read()
        #Send image to AWS to compare against collection of faces
        response = client.search_faces_by_image(Image={'Bytes': sourceBytes},
        CollectionId='faces',
                                                FaceMatchThreshold=95)
                                                #95% confidence or higher
        matches = response['FaceMatches']

        print("--------------------------------------------")

        #If a match was found
        if len(matches) > 0:
            face = matches[0]
            specificface = face['Face']
            #Cleaning Output
            rawName = format(specificface['ExternalImageId'])
            removeDigits = str.maketrans('', '', string.digits)
            noNumberName = rawName.translate(removeDigits)
            faceName = noNumberName.translate( { ord("-"): None } )
            #Retrieving Name from image
            #Shows users name, similarity percentage and confidence
            print("Matched with", faceName,": {}""%"" Similarity.".
            format(face['Similarity']))
            print("With Confidence of: {}".format(specificface['Confidence']))

        else:
            print("Access Denied: Face does not match records.")
```

```
    print("Finished Operation")

sleep(0.5)
```

9.1.5 Secure Solution

```
    from time import sleep
import os
import boto3
import string
import mariadb
import sys
import textwrap
import cv2


#Creating Connection to the Database
try:
    conn = mariadb.connect(
        user="your-username-here",
        password="your-password-here",
        host="127.0.0.1",
        port=3306,
        database="your-database-name-here"
        )
except mariadb.Error as e: #Error message if connection failed
    print(f"Error connecting to MariaDB Plaftform: {e}")

cur = conn.cursor()


#Checks Clean value against Database
def checkCard(sanitisedValue):
    cur.execute( #SQL Injection safe Query
        """SELECT ID from cardID WHERE cardNumber =
        '%(cardNumber)s'""" % {'cardNumber': sanitisedValue}
        )
    foundInDB = cur.fetchone()
    #If a match was found
    if foundInDB != None:
        print("SQL: Card Matches")
        return True
    else: #If nothing was found
        print("SQL: Card not found in Database")
        return False


def checkFace():

    #Takes Image with Webcam
    cam = cv2.VideoCapture(0)
    check, frame = cam.read()
```

```
    cv2.imwrite("image.jpg", frame)
    image = "image.jpg"

    #Connection to AWS Rekognition
    client = boto3.client(service_name="rekognition")
    with open(image, "rb") as sourceImage:
        sourceBytes = sourceImage.read()


    #Error Catching incase no face is in picture
    try: #If a face is found
        #Send image to AWS to compare against collection of faces
        response = client.search_faces_by_image(Image={'Bytes': sourceBytes},
        CollectionId='faces',
                                                FaceMatchThreshold=95)
                                                #95% confidence or higher
        matches = response['FaceMatches']


        #If a match was found
        if len(matches) > 0:
            face = matches[0]
            specificface = face['Face']
            #Cleaning Output
            rawName = format(specificface['ExternalImageId'])
            removeDigits = str.maketrans('', '', string.digits)
            noNumberName = rawName.translate(removeDigits)
            faceName = noNumberName.translate( { ord("-"): None } )
            #Retrieving Name from image
            #Shows users name, similarity percentage and confidence
            print("Matched with", faceName,": {}""%"" Similarity."
            .format(face['Similarity']))
            print("With Confidence of: {}".format(specificface['Confidence']))
            return True

        else:
            print("AWS: Face does not match records.")
            return False
    except: #If no Face was found
        print("AWS: No Face Found in Frame")
        return False


def dataSanitisation(scannedCard):
    #Taking incorrect Decimal value and changing to correct Hex
    hexValue = hex(int(scannedCard))
    correctHex = hexValue.replace('x', '')
    splitValues = textwrap.wrap(correctHex, 2)
```

```
    #Reordering Hex Value
    orderHex = splitValues[3] + splitValues[2] + splitValues[1] + splitValues[0]
    print("Corrected Hex Value: ", orderHex)
    return str(orderHex)


#Constantly running code
while True:
    print("————————————————————————————")
    scannedCard = input("Scan Card and Look into Camera to Begin: ")

    #Verify if something has been entered
    if scannedCard != None:
        sanitisedValue = dataSanitisation(scannedCard)
        isRecognised = checkFace()
        processedCard = checkCard(sanitisedValue)

        #Checking if both the Card and Face matches to gran access
        if (isRecognised == True and processedCard == True):
            print("Access Granted")
        else:
            print("Access Denied")
        #Finishes program with non-descript answer to users
        print("Finished Operation")
        print("————————————————————————————")

    sleep(0.5)
```

9.2 Appendix B - Survey

Masters Thesis: A Survey on Access Controls

Dear Participants,

My name is Thomas Augustine MacKinnon and I am a Masters of Cyber Security Student at Asia Pacific University of Technology and Innovation. This survey aims to gain the perspective of the public towards Access Control methods, specifically of Smart Cards and Facial Recognition. This survey also wishes to see how suspicious various methods of exploiting Access Control, aiming to see if these techniques would actually be usable in real world scenarios. This survey is open to anyone of any technological knowledge, as the subject matter is applicable to the a large portion of the population.

This survey follows GDPR regulations, so is completely **anonymous** with only your answers to questions being saved to be used for research and analytical study of Access Control. All records will be **stored securely**, kept confidential, and will be deleted once the project concludes and is no longer needed.

Thank you for participating and contributing to my research, if you have any questions or inquiries please do not hesitate to contact me via email: tp066728@mail.apu.edu.my

Yours Sincerely,
Thomas Augustine MacKinnon.

* Indicates required question

1. **Terms and Conditions** *

By accepting the Terms and Conditions, you understand that:
1. This survey is completely voluntary.
2. This survey is anonymous.
3. Data collected will only be used for research and analysis relating to the subject of the project.
4. Responses will be kept private and deleted once they are no longer needed.
5. You may withdraw from the research at any time for any reason.

Check all that apply.

☐ I agree to the Terms and Conditions

Smart Card Questions

Smart Cards are a common tool used in Access Control, seen in many establishments to prevent illegitimate access to restricted areas, such as preventing strangers from entering your Apartment Block, or members of the public into business premises. Smart Cards provide an easy and efficient method of security, that is heavily favoured in the modern day Information Security Landscape.

Smart Cards work by sending a Unique Value through a scanner using Radio-Frequency Identification (RFID), which is then checked against a back-end database to see if the operator is allowed access.

These questions aim to show the general understanding of the technology, and what the future might bring for it.

2. Have you used Smart Card technology before for Access Control? (i.e. opening a locked hotel door) *

Mark only one oval.

- Yes I have used Smart Cards
- No I have not used Smart Cards

3. How often do you use Smart Cards? *

Mark only one oval.

Rarely Use Smart Cards
1 ◯
2 ◯
3 ◯
4 ◯
5 ◯
Frequently Use Smart Cards

4. How Secure do you think Smart Cards are? *

Mark only one oval.

Very Insecure
1 ◯
2 ◯
3 ◯
4 ◯
5 ◯
Very Secure

5. Do you think Smart Cards will be continue to be used or replaced with other technologies? (i.e. Facial Recognition, fingerprint)

Mark only one oval.

Here to stay
1 ⬭
2 ⬭
3 ⬭
4 ⬭
5 ⬭
Likely be replaced

6. Do you think it is possible to Clone a Smart card?

Mark only one oval.

Not possible
1 ⬭
2 ⬭
3 ⬭
4 ⬭
5 ⬭
Easy to do

7. Would you trust a Smart Card system as the only form of Access Control to a building/business/organisation?

Mark only one oval.

	I would not trust it at all
1	⬭
2	⬭
3	⬭
4	⬭
5	⬭
	I would completely trust it

Facial Recognition Questions

Facial Recognition is the process of comparing a person's face against a dataset of faceprints to see if there are any matches and identify the operator. This form of authentication has seen a huge rise through Mobile Phone Face unlocks, and is gradually being incorporated into everyday security surveillance, such as public CCTV feeds.

These questions aim to grasp your understanding and opinions towards Facial Recognition and its future in Access Control systems.

8. Have you used Facial Recognition before? (i.e. Face unlock on phones)

Mark only one oval.

⬭ Yes I have used Facial Recognition

⬭ No I have not used Facial Recognition

9. Do you prefer using Facial Recognition to other forms of Access Control? (i.e. password, fingerprint scanning)

Mark only one oval.

Heavily Prefer other options
1
2
3
4
5
Heavily Prefer Facial Recognition

10. Do you think Facial Recognition will replace other forms of Access Control? (i.e. Smart Cards, physical keys)

Mark only one oval.

Not Likely at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Highly Likely

11. Are you worried that Facial Recognition could be used to track you?

Mark only one oval.

Not worried at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Very Worried

12. Do you think it is ethical for governments/businesses to use Facial Recognition without your consent?

Mark only one oval.

Perfectly Ethical
1
2
3
4
5
Highly Unethical

13. How important is consent for you when dealing with Facial Recognition Technologies?

Mark only one oval.

Not Important

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Very Important

14. Would you trust Facial Recognition as the only form of Access Control to a building/business/organisation?

Mark only one oval.

I would not trust it at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

I would trust it completely

Scenario Questions

You work for a large company that uses a mix of Smart Cards and Facial Recognition as Access Control within the business premises.

Employees use ID badges, with employee details printed on them, such as their name, email address, department, and a picture of their face. These cards are used to get through the turnstiles at the entrance, to select a floor in elevators, and to unlock various doors around the building. Some employees have more access to restricted areas than others (such as IT staff having access to Server rooms), whilst some have very limited access.

The CCTV in the building also uses Facial Recognition Technology to identify Employees and highlight any unknown Individuals. The database of faceprints also include known criminals from a Police dataset to alert security to their presence.

15. You see one employee who has an ID badge, but when it comes to scanning for entry they use a non-descript white card, ignoring their ID badge. Do you find this suspicious?

Mark only one oval.

Not Suspicious at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Highly Suspicious

16. Would you report this person to security staff?

Mark only one oval.

◯ I would report them

◯ I would not report them

17. You see a different Individual use an Odd tool seen in the Image on Smart Card Scanners, which grants them access. How suspicious do you find this?

Mark only one oval.

Not Suspicious at all

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Highly Suspicious

18. Would you report them to Security Staff? *

Mark only one oval.

- I would report them
- I would not report them

19. You see someone opening up a Smart Card reader and messing around with the wires before putting it back together. How suspicious do you find this?

Mark only one oval.

Not Suspicious at all

1
2
3
4
5

Highly Suspicious

20. Would you report them to Security Staff? *

Mark only one oval.

- I would report them
- I would not report them

21. A member of staff seemingly never uses their ID card, instead pressing a button on their phone which unlocks doors. How suspicious do you find this?

Mark only one oval.

Not Suspicious at all

1 ⬭

2 ⬭

3 ⬭

4 ⬭

5 ⬭

Highly Suspicious

22. Would you report them to Security Staff? *

Mark only one oval.

⬭ I would report them

⬭ I would not report them

23. A member of staff wears these glasses. Do you find this suspicious?

Mark only one oval.

	Not Suspicious at all
1	⬭
2	⬭
3	⬭
4	⬭
5	⬭
	Highly Suspicious

24. Would you report them to Security Staff? *

Mark only one oval.

- I would report them
- I would not report them

25. Someone enters the building fearing facial paint like in the image. Do you find this suspicious?

Mark only one oval.

	Not Suspicious at all
1	⬭
2	⬭
3	⬭
4	⬭
5	⬭

Highly Suspicious

26. Would you report them to Security Staff? *

Mark only one oval.

- I would report them
- I would not report them

27. Would you be suspicious that this individual is trying to avoid Facial Recognition through everyday items?

Mark only one oval.

Not Suspicious at all

1

2

3

4

5

Highly Suspicious

28. Would you be suspicious that this individual is trying to avoid Facial Recognition through everyday items?

Mark only one oval.

Not Suspicious at all

1 ◯

2

3

4

5

Highly Suspicious

29. Would you be suspicious that this individual is trying to avoid Facial Recognition through everyday items?

Mark only one oval.

Not Suspicious at all

1 ⬭

2

3

4

5

Highly Suspicious

9.3 Appendix C - Results

9.3.1 Everyday Items Results

Face Section	Item	Percentage Coverage	Enviroment 1	Enviroment 2	Enviroment 3	Overall Pass Rate	Effectiveness	Comment
Individual Tests	Bandana	11.00%	100.00%	0.00%	100.00%	66.67%	92.67%	
	Beanie	22.00%	100.00%	60.00%	100.00%	86.67%	80.93%	eye contact matters with cv2
	Hard Hat	33.00%	100.00%	0.00%	100.00%	66.67%	78.00%	
	Glasess	11.00%	100.00%	0.00%	100.00%	66.67%	92.67%	
	Sunglasses	22.00%	100.00%	0.00%	100.00%	66.67%	85.33%	
	Blindfold	33.00%	0.00%	0.00%	100.00%	33.33%	89.00%	
	Loose Scarf	11.00%	100.00%	100.00%	100.00%	100.00%	89.00%	
	Face Mask	22.00%	0.00%	0.00%	100.00%	33.33%	92.67%	
	Full Scarf	33.00%	0.00%	0.00%	100.00%	33.33%	89.00%	

Face Section	Item	Percentage Coverage	Enviroment 1	Enviroment 2	Enviroment 3	Overall Pass Rate	Effectiveness	Comment
Dual Item Tests	Bandana + Glasses	22.00%	80.00%	0.00%	100.00%	60.00%	2.73	
	Bandana + Sunglasses	33.00%	100.00%	0.00%	100.00%	66.67%	2.03	
	Bandana + Blindfold	44.00%	0.00%	0.00%	0.00%	0.00%	0	
	Beanie + Glasses	33.00%	60.00%	0.00%	100.00%	53.33%	1.62	
	Beanie + Sunglasses	44.00%	100.00%	0.00%	100.00%	66.67%	1.52	
	Beanie + Blindfold	55.00%	0.00%	0.00%	20.00%	6.67%	0.13	
	Hard Hat + Glasses	44.00%	100.00%	0.00%	100.00%	66.67%	1.52	
	Hard Hat + Sunglasses	55.00%	100.00%	0.00%	100.00%	66.67%	1.22	
	Hard Hat + Blindfold	66.00%	0.00%	0.00%	0.00%	0.00%	0	
	Bandana + Loose Scarf	22.00%	40.00%	0.00%	100.00%	46.67%	2.13	
	Bandana + Face Mask	33.00%	0.00%	0.00%	80.00%	26.67%	0.81	Dip in Similarity
	Bandana + Full Scarf	44.00%	0.00%	0.00%	80.00%	26.67%	0.61	Face Does not Match in AWS
	Beanie + Loose Scarf	33.00%	100.00%	100.00%	100.00%	100.00%	3.04	
	Beanie + Face Mask	44.00%	0.00%	0.00%	100.00%	33.33%	0.76	
	Beanie + Full Scarf	55.00%	0.00%	0.00%	100.00%	33.33%	0.61	
	Hard Hat + Loose Scarf	44.00%	100.00%	0.00%	100.00%	66.67%	1.52	
	Hard Hat + Face Mask	55.00%	0.00%	0.00%	100.00%	33.33%	0.61	
	Hard Hat + Full Scarf	66.00%	0.00%	0.00%	0.00%	0.00%	0	
	Glasses + Loose Scarf	22.00%	20.00%	0.00%	100.00%	40.00%	1.82	
	Glasses + Face Mask	33.00%	0.00%	0.00%	0.00%	0.00%	0	no match but face detect
	Glasses + Full Scarf	44.00%	0.00%	0.00%	60.00%	20.00%	0.46	
	Sunglasses + Loose Scarf	33.00%	100.00%	0.00%	100.00%	66.67%	2.03	
	Sunglasses + Face Mask	44.00%	60.00%	0.00%	0.00%	20.00%	0.46	
	Sunglasses + Full Scarf	55.00%	0.00%	0.00%	20.00%	6.67%	0.13	
	Blindfold + Loose Scarf	44.00%	0.00%	0.00%	0.00%	0.00%	0	
	Blindfold + Face Mask	55.00%	0.00%	0.00%	0.00%	0.00%	0	
	Blindfold + Full Scarf	66.00%	0.00%	0.00%	0.00%	0.00%	0	

Face Section	Item	Percentage Coverage	Enviroment 1	Enviroment 2	Enviroment 3	Overall Pass Rate	Effectiveness	comments
Combination Item Tests	Bandana + Glasses + Loose Scarf	33.00%	40.00%	0.00%	100.00%	46.67%	85%	
	Bandana + Glasses + Face Mask	44.00%	20.00%	0.00%	0.00%	6.67%	97%	
	Bandana + Glasses + Full Scarf	55.00%	0.00%	0.00%	0.00%	0.00%	100%	AWS half face no match
	Bandana + Sunglasses + Loose Scarf	44.00%	60.00%	0.00%	100.00%	53.33%	77%	
	Bandana + Sunglasses + Face Mask	55.00%	0.00%	0.00%	0.00%	0.00%	100%	face detected
	Bandana + Sunglasses + Full Scarf	66.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Bandana + Blindfold + Loose Scarf	55.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Bandana + Blindfold + Face Mask	66.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Bandana + Blindfold + Full Scarf	77.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Beanie + Glasses + Loose Scarf	44.00%	80.00%	0.00%	100.00%	60.00%	74%	
	Beanie + Glasses + Face Mask	55.00%	0.00%	0.00%	20.00%	6.67%	96%	
	Beanie + Glasses + Full Scarf	66.00%	0.00%	0.00%	100.00%	33.33%	78%	
	Beanie + Sunglasses + Loose Scarf	55.00%	100.00%	0.00%	100.00%	66.67%	63%	cv2 focus on nose and bad with reflective
	Beanie + Sunglasses + Face Mask	66.00%	40.00%	0.00%	0.00%	13.33%	91%	
	Beanie + Sunglasses + Full Scarf	77.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Beanie + Blindfold + Loose Scarf	66.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Beanie + Blindfold + Face Mask	77.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Beanie + Blindfold + Full Scarf	88.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Hard Hat + Glasses + Loose Scarf	55.00%	20.00%	0.00%	60.00%	26.67%	85%	
	Hard Hat + Glasses + Face Mask	66.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Hard Hat + Glasses + Full Scarf	77.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Hard Hat + Sunglasses + Loose Scarf	66.00%	100.00%	0.00%	100.00%	66.67%	56%	
	Hard Hat + Sunglasses + Face Mask	77.00%	60.00%	0.00%	0.00%	20.00%	85%	relection is a big factor
	Hard Hat + Sunglasses + Full Scarf	88.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Hard Hat + Blindfold + Loose Scarf	77.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Hard Hat + Blindfold + Face Mask	88.00%	0.00%	0.00%	0.00%	0.00%	100%	
	Hard Hat + Blindfold + Full Scarf	99.00%	0.00%	0.00%	0.00%	0.00%	100%	

9.3.2 Paint Results

Painted Face #	Enviroment 1	Enviroment 2	Enviroment 3	Overall Pass Rate
1	0.00%	0.00%	80.00%	26.67%
2	0.00%	0.00%	100.00%	33.33%
3	100.00%	0.00%	100.00%	66.67%
4	60.00%	0.00%	100.00%	53.33%
5	0.00%	0.00%	100.00%	33.33%

9.3.3 Survey Results

Masters Thesis: A Survey on Access Controls

89 responses

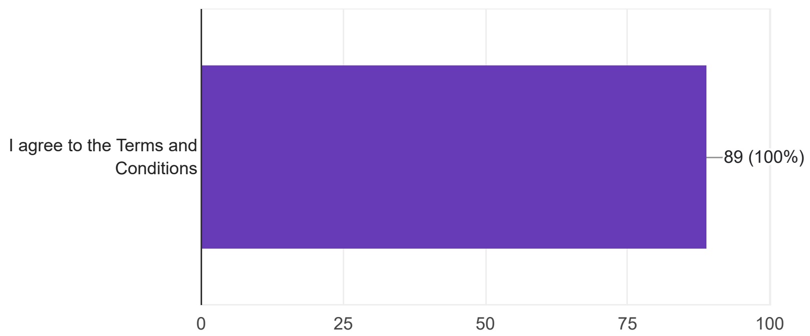
Publish analytics

Terms and Conditions

Copy

By accepting the Terms and Conditions, you understand that:
1. This survey is completely voluntary.
2. This survey is anonymous.
3. Data collected will only be used for research and analysis relating to the subject of the project.
4. Responses will be kept private and deleted once they are no longer needed.
5. You may withdraw from the research at any time for any reason.

89 responses

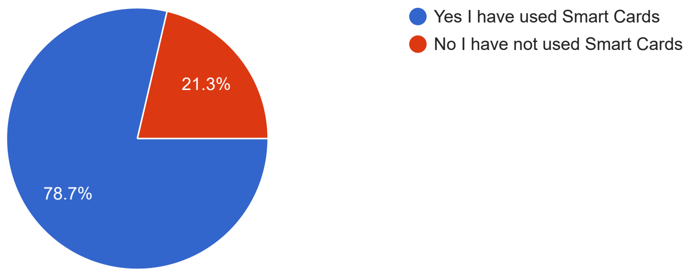


Smart Card Questions

Have you used Smart Card technology before for Access Control? (i.e. opening a locked hotel door)

Copy

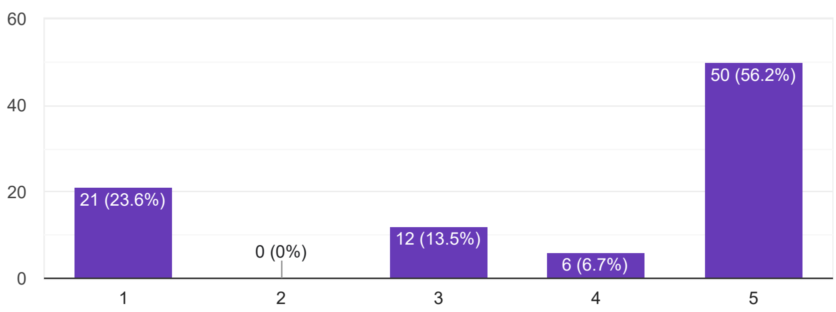
89 responses



How often do you use Smart Cards?

Copy

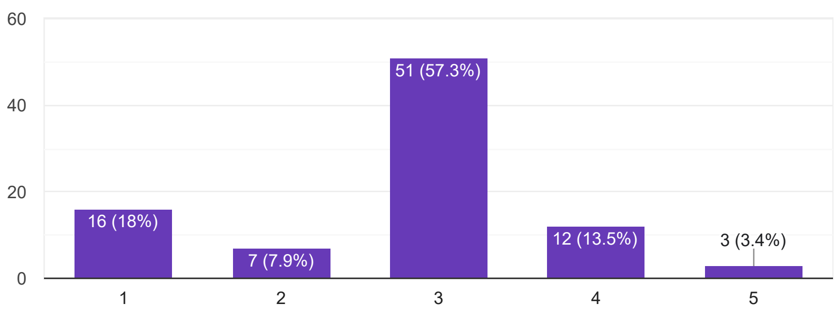
89 responses



How Secure do you think Smart Cards are?

Copy

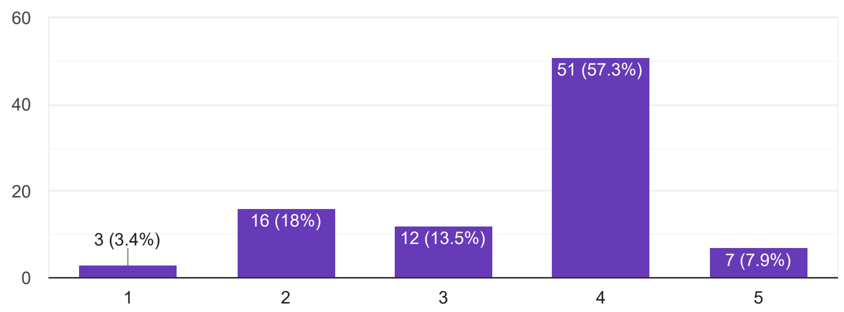
89 responses



Do you think Smart Cards will be continue to be used or replaced with other technologies? (i.e. Facial Recognition, fingerprint)

Copy

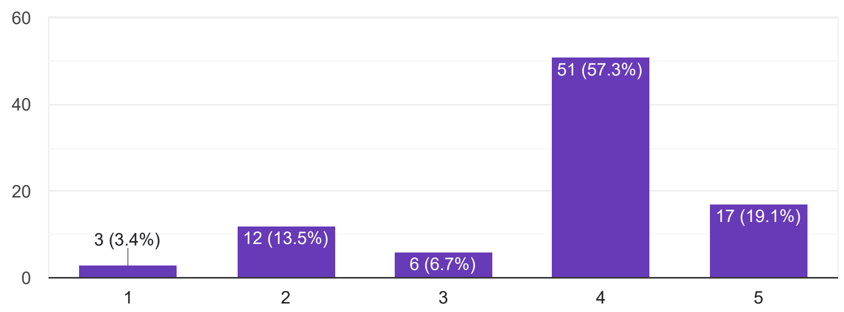
89 responses



Do you think it is possible to Clone a Smart card?

Copy

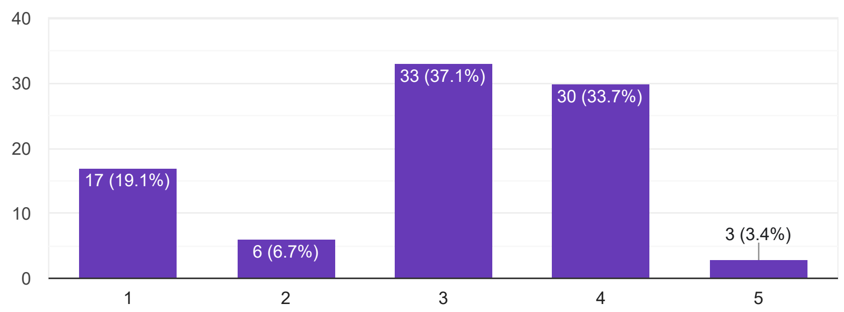
89 responses



Would you trust a Smart Card system as the only form of Access Control to a building/business/organisation?

Copy

89 responses

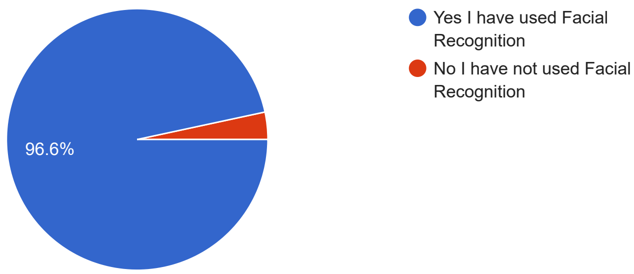


Facial Recognition Questions

Have you used Facial Recognition before? (i.e. Face unlock on phones)

Copy

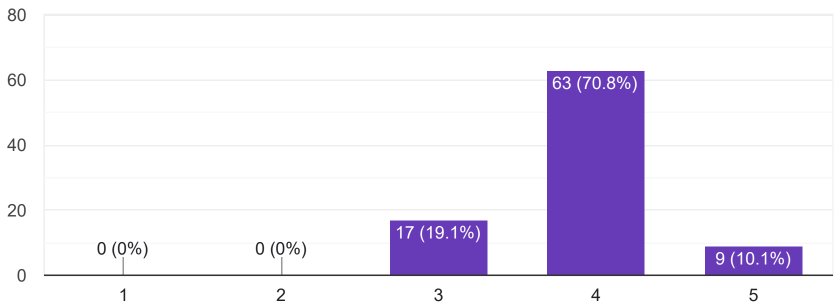
89 responses



Do you prefer using Facial Recognition to other forms of Access Control? (i.e. password, fingerprint scanning)

Copy

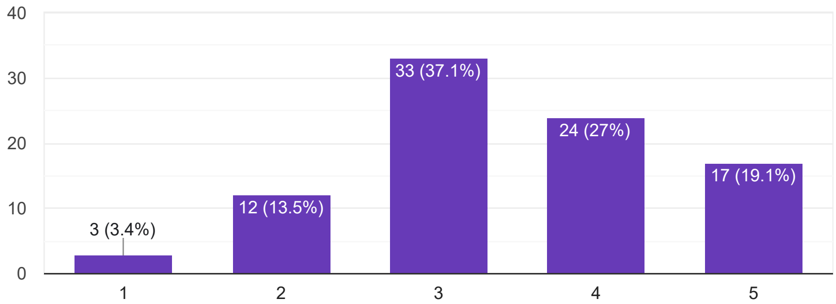
89 responses



Do you think Facial Recognition will replace other forms of Access Control? (i.e. Smart Cards, physical keys)

Copy

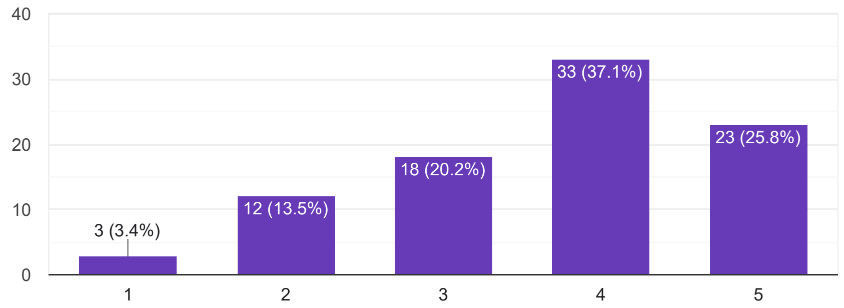
89 responses



Are you worried that Facial Recognition could be used to track you?

Copy

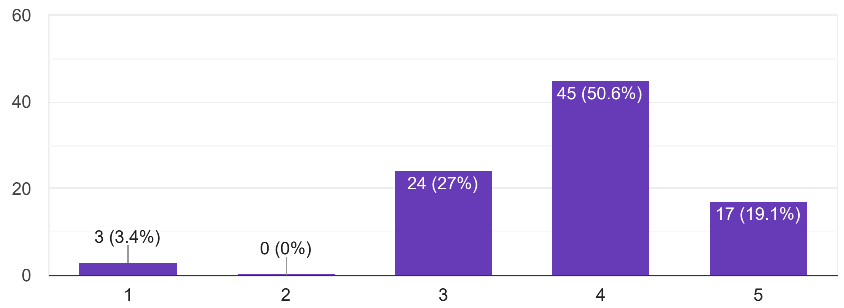
89 responses



Do you think it is ethical for governments/businesses to use Facial Recognition without your consent?

Copy

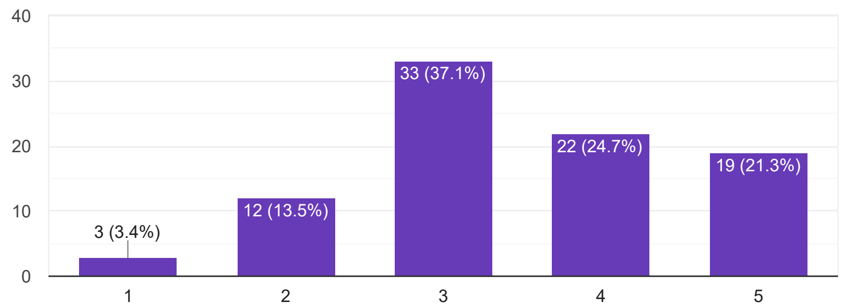
89 responses



How important is consent for you when dealing with Facial Recognition Technologies?

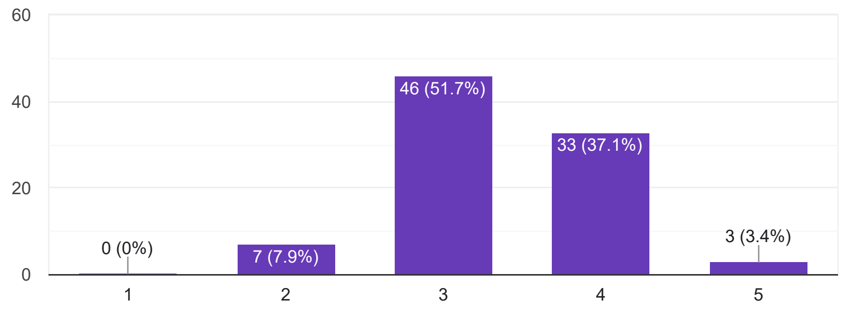
Copy

89 responses



Would you trust Facial Recognition as the only form of Access Control to a building/business/organisation?

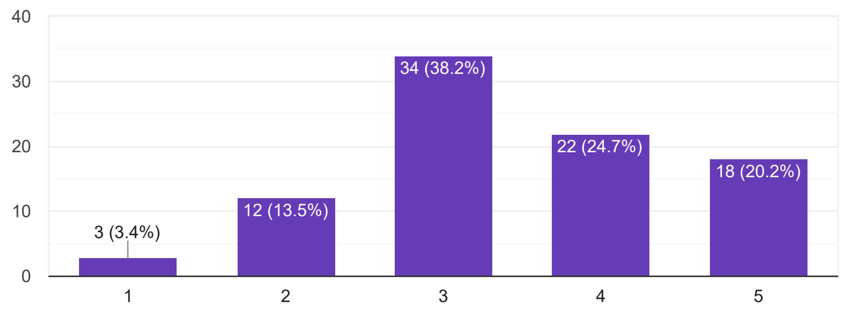
89 responses



Scenario Questions

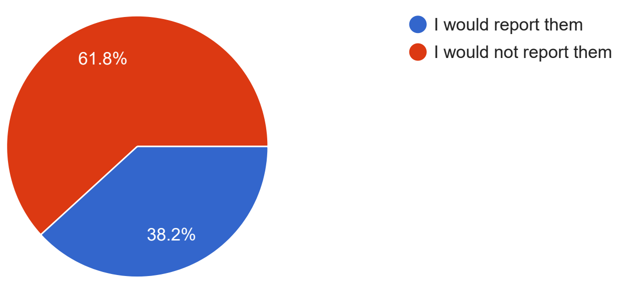
You see one employee who has an ID badge, but when it comes to scanning for entry they use a non-descript white card, ignoring their ID badge. Do you find this suspicious?

89 responses



Would you report this person to security staff?

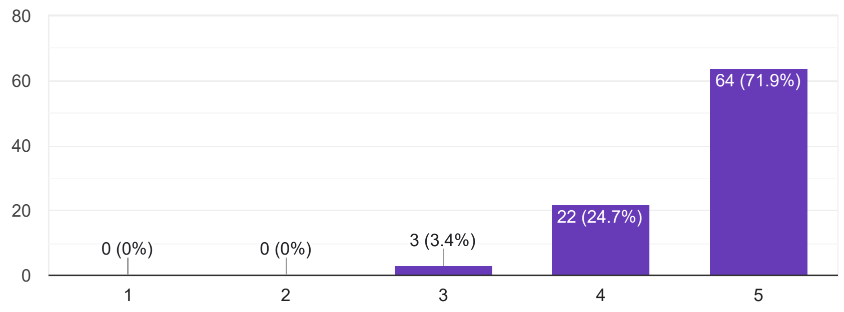
89 responses



You see a different Individual use an Odd tool seen in the Image on Smart Card Scanners, which grants them access. How suspicious do you find this?

Copy

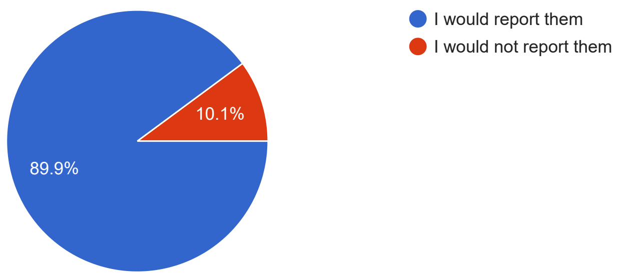
89 responses



Would you report them to Security Staff?

Copy

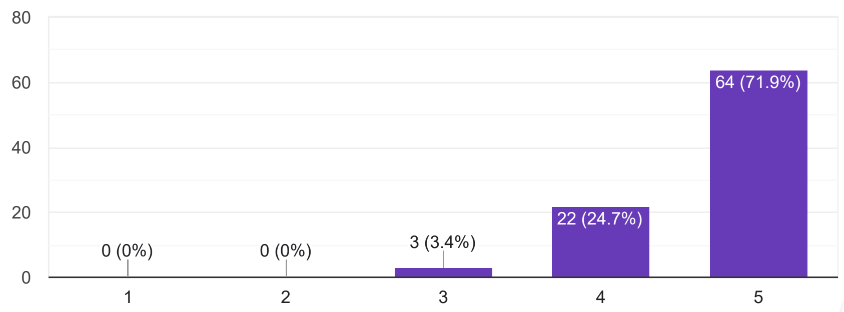
89 responses



You see someone opening up a Smart Card reader and messing around with the wires before putting it back together. How suspicious do you find this?

Copy

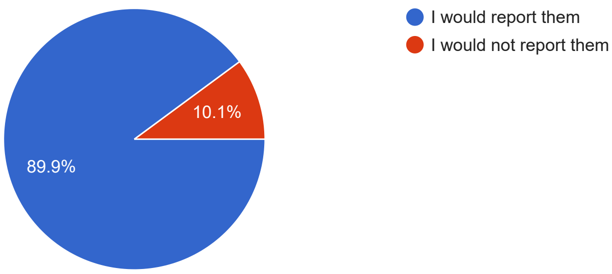
89 responses



Would you report them to Security Staff?

Copy

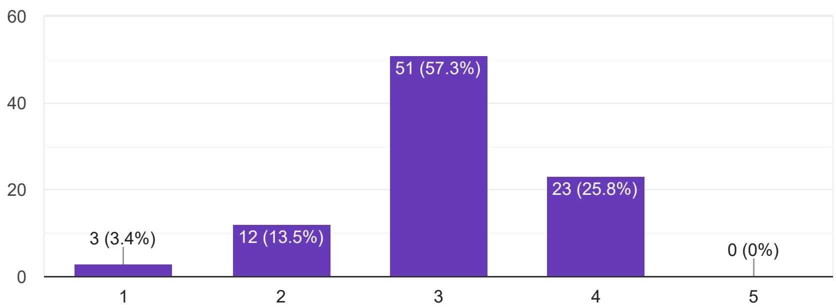
89 responses



A member of staff seemingly never uses their ID card, instead pressing a button on their phone which unlocks doors. How suspicious do you find this?

Copy

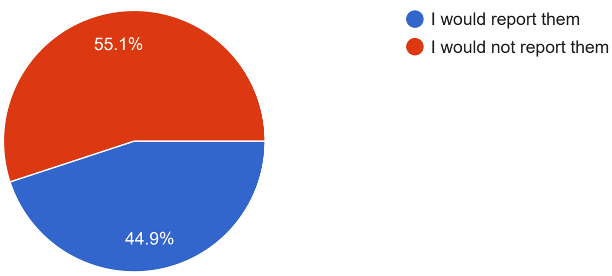
89 responses



Would you report them to Security Staff?

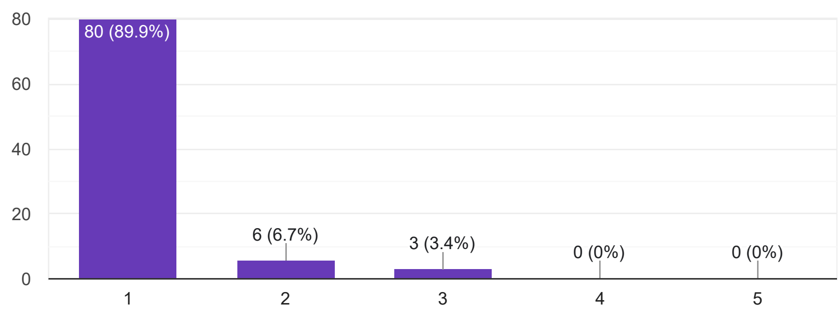
Copy

89 responses



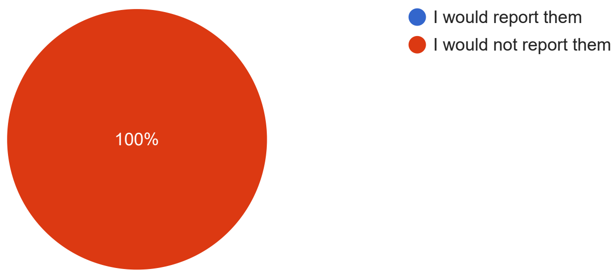
A member of staff wears these glasses. Do you find this suspicious? Copy

89 responses



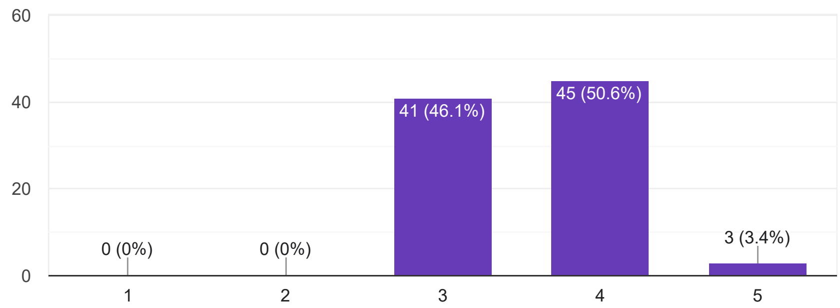
Would you report them to Security Staff? Copy

89 responses



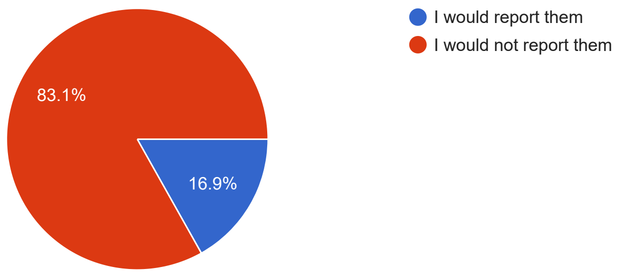
Someone enters the building fearing facial paint like in the image. Do you find this suspicious? Copy

89 responses



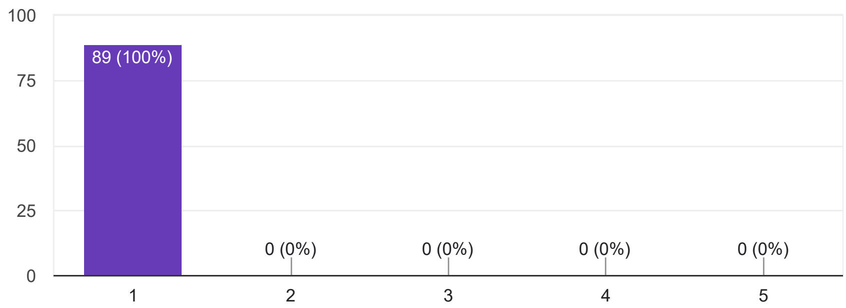
Would you report them to Security Staff?

89 responses



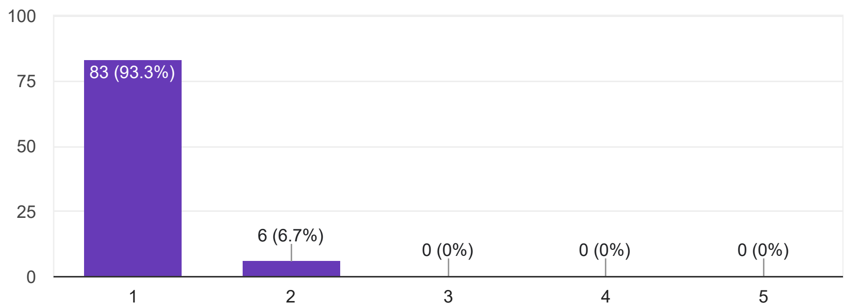
Would you be suspicious that this individual is trying to avoid Facial Recognition through everyday items?

89 responses



Would you be suspicious that this individual is trying to avoid Facial Recognition through everyday items?

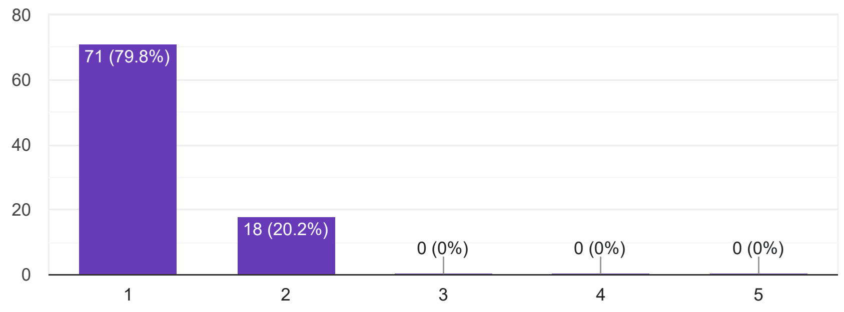
89 responses



Would you be suspicious that this individual is trying to avoid Facial Recognition through everyday items?

Copy

89 responses



9.4 Appendix D - Ethics Form

Office Record	Receipt – APU Fast-Track Ethical Approval
Date Received: Received by:	Student name: Student number: Received by: Date:

APU/APIIT FAST-TRACK ETHICAL APPROVAL FORM (STUDENTS)

Tick one box (level of study):
- ☑ POSTGRADUATE (PhD / MPhil / Masters)
- ☐ UNDERGRADUATE (Bachelors degree)
- ☐ FOUNDATION / DIPLOMA / Other categories

Tick one box (purpose of approval):
- ☑ Thesis / Dissertation / FYP project
- ☐ Module assignment
- ☐ Other: ____________________

Title of Programme on which enrolled … M.Sc in Cyber Security… … … … … … … … … … … … …

Tick one box: ☑ Full-Time Study or ☐ Part-Time Study

Title of project / assignment Utilization of Blockchain and Artificial Intelligence Solutions for Smart and Secure Healthcare Management System

Name of student researcher …Thomas Augustine MacKinnon … … … … … … … … … … … … … …

Name of supervisor / lecturer… … …Dr. Julia Juremi … … … … … … … … … … … … … … … …

Student Researchers- please note that certain professional organisations have ethical guidelines that you may need to consult when completing this form.

Supervisors/Module Lecturers - please seek guidance from the Chair of the School Research Ethics Committee if you are uncertain about any ethical issue arising from this application.

		YES	NO	N/A
1	Will you describe the main procedures to participants in advance, so that they are informed about what to expect?	✓		
2	Will you tell participants that their participation is voluntary?	✓		
3	Will you obtain written consent for participation?	✓		
4	If the research is observational, will you ask participants for their consent to being observed?	✓		
5	Will you tell participants that they may withdraw from the research at any time and for any reason?	✓		
6	With questionnaires and interviews will you give participants the option of omitting questions they do not want to answer?	✓		
7	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	✓		
8	Will you give participants the opportunity to be debriefed i.e. to find out more about the study and its results?	✓		

If you have ticked No to any of Q1-8**,** you should complete the full Ethics Approval Form.

		YES	NO	N/A
9	Will your project/assignment deliberately mislead participants in any way?		✓	
10	Is there any realistic risk of any participants experiencing either physical or psychological distress or discomfort?		✓	
11	Is the nature of the research such that contentious or sensitive issues might be involved? This includes research which could induce psychological stress, anxiety or humiliation, or cause more than minimal pain.		✓	
12	Does your research involve the use of sensitive materials? Eg, records of personal or sensitive confidential information,		✓	

13	Does your research require external agency approval?		✓	
14	Does your research use hazardous or controlled substance?		✓	
15	Does your research require you to visit participants in their home or non-public space?		✓	
16	Does your research use genetically modified organisms?		✓	
17	Does your research investigate illegal activities or behaviours?		✓	
18	Does your research involve discussion or collection of information on potentially sensitive, embarrassing or distressing topics, administrative or secure data? This includes research involving respondents through internet where visual images are used, and where sensitive issues are discussed		✓	
19	Does your research involve invasive or potentially intrusive procedures?		✓	
20	Does your research involve administration of substances?		✓	
21	Will your research be involved in the collection/ processing of human tissue samples		✓	
22	Will your participants be receiving financial compensation for participating in your research?		✓	
23	Will your research data be used in the future after the conclusion of your project?		✓	
24	Will your research involve in processing sensitive data belonging to an organisation/persons?		✓	
25	Will your research be collecting photographs, videos, and audio recordings of the participants?		✓	
26	Will the participants' personal particulars be known to any third party?		✓	
27	Will the participants' data confidentiality be made known to the public?		✓	
28	Will the research be conducted where the safety of the researchers maybe in question?		✓	
29	Will be the research be conducted outside of the UK and/or Malaysia?		✓	
30	Will your research involve human participants at premises other than those of the University?		✓	

If you have ticked Yes to any of Q9 – 30**,** you should complete the full Ethics Approval Form. In relation to question 10 this should include details of what you will tell participants to do if they should experience any problems (e.g. who they can contact for help). You may also need to consider risk assessment issues.

			YES	NO	N/A
31	Does your project/assignment involve work with animals?			✓	
32	Do participants fall into any of the following special groups? **Note that you may also need to obtain satisfactory**	Children (under 18 years of age)		✓	
		People with communication or learning difficulties			
		Patients			
		People in custody			
		People who could be regarded as vulnerable or lack capacity to make decision for themselves			
		People engaged in illegal activities (eg drug taking)			
		Groups of people whose relationship among each other allow one to have influence over the other such as:			

	clearance from the relevant authorities	Carers and patients with chronic conditions; teachers and their students; prison authorities and prisoners; employers and employees			
		Deceased person’s body parts or other human tissues including bodily fluids (e.g. blood, saliva).			
		groups where permission of a gatekeeper is normally required for initial access to members.			
		Human participants who are off-campus APU staff or students who wish to carry out investigations involving human participants at premises other than those of the University			
33	Does the project/assignment involve external funding or external collaboration where the funding body or external collaborative partner requires the University to provide evidence that the project/assignment had been subject to ethical scrutiny?			✓	

If you have ticked Yes to any Q31-33**,** you should complete the full Ethics Approval Form. There is an obligation on student and supervisor to bring to the attention of the APU School Research Ethics Committee any issues with ethical implications not clearly covered by the above checklist.

STUDENT RESEARCHER
Provide in the boxes below (plus any other appended details) information required in support of your application. THEN SIGN THE FORM.

Please Tick Boxes

I consider that this project/assignment has no significant ethical implications requiring a full ethics submission to the APU School Research Ethics Committee.	✓
I am aware of APU liability policy and will make the necessary arrangement for insurance coverage of all researchers and participants of the project/assignment.	✓
Give a brief description of participants, procedure of recruitment and procedure of data collection (methods, tests used etc) in up to 150 words. A Google Form requiring willing participants to choose a value that represents their opinion on a linear scale (from 1 to 5, Strongly Disagree to Strongly Agree) or Binary Answers (Yes or No). The Form will be sent to people known by the researcher through social media and messaging.	
I also confirm that: i) All key documents e.g. consent form, information sheet, questionnaire/interview, and all material such as emails and posters for the purpose of recruitment of participants are appended to this application.	
Or ii) Any key documents e.g. consent form, information sheet, questionnaire/interview schedules which need to be finalised following initial investigations will be submitted for approval by the project/assignment supervisor/module lecturer before they are used in primary data collection.	✓

Signed… … … … … … … Print Name… Thomas Augustine MacKinnon… …
Date… 02/05/2023…
(Student Researcher)

Within this document, any variation to the items considered which affects ethical issues of the stated research will require submission of a revised research plan and research methodology details; as a consequence, new ethical consent may need to be sought.
The completed form (and any attachments) should be submitted for consideration by your Supervisor/Module Lecturer

SUPERVISOR/MODULE LECTURER
PLEASE CONFIRM THE FOLLOWING:

Please Tick Box

I consider that this project/assignment has no significant ethical implications requiring a full ethics submission to the APU School Research Ethics Committee	/
I have checked and approved the key documents required for this proposal (e.g. consent form, information sheet, questionnaire, interview schedule)	/

SUPERVISOR AND SECOND ACADEMIC SIGNATORY

STATEMENT OF ETHICAL APPROVAL (please delete as appropriate)

1) **THIS PROJECT/ASSIGNMENT HAS BEEN CONSIDERED USING AGREED APU PROCEDURES AND IS NOW APPROVED**

2) **THIS PROJECT/ASSIGNMENT HAS BEEN APPROVED IN PRINCIPLE AS INVOLVING NO SIGNIFICANT ETHICAL IMPLICATIONS, BUT FINAL APPROVAL FOR DATA COLLECTION IS SUBJECT TO THE SUBMISSION OF KEY DOCUMENTS FOR APPROVAL BY SUPERVISOR (see Appendix A)**

Signed… … … … … … … … … … … Print Name… … … … … … … … … … … Dr. Julia Juremi Date… … … … 2.05.23
(Supervisor/Lecturer)

Signed… … … … … … … … … … … Print Name… … … … … … … … … … … Date… … … …
(Second Academic Signatory)

Office Record Date Received: Received by:	Receipt – Appendix A (APU Fast-Track Ethics Form) Student name: Student number: Received by: Date:

APPENDIX A
AUTHORISATION FOR USE OF KEY DOCUMENTS

Completion of Appendix A is required when for good reasons key documents are not available when a fast track application is approved by the supervisor/module lecturer and second academic signatory.

I have now checked and approved all the key documents associated with this proposal e.g. consent form, information sheet, questionnaire, interview schedule

Title of project/assignment… …

… ....

Name of student researcher … ....

Student ID: ………………………………   Intake: … … … … … … … … … … … … … … … … … ……..

Signed… … … … … … … … … … … … Print Name… … … … … … … … … … … … Date… … ……... ……..
(Supervisor/Lecturer)

9.5 Appendix E - Front cover and Spine

ACCESS CONTROL EVALUATION AND IMPROVEMENT OF SMART CARD AND FACIAL RECOGNITION TECHNOLOGY TO CREATE A SECURE WORKPLACE

THOMAS AUGUSTINE MACKINNON

ASIA PACIFIC UNIVERSITY OF TECHNOLOGY AND INNOVATION
(APU)

Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Thomas Augustine MacKinnon

APU

2023

9.6 Appendix F - Meeting Logs

Project Log Sheet – Supervisory Session

Student's name: Thomas Augustine MacKinnon **Date:** 02.09.2022 **Meeting No:** 1

Project title: Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Intake: APDMF2204CYS(PR)

Supervisor's name: Dr. Julia Juremi **Supervisor's signature:** ……………

Items for discussion (noted by student before mandatory supervisory meeting):

1. **Master thesis title**
2. **Processes that need to be taken**
3. **Literature review**
4.

Record of discussion (noted by student during mandatory supervisory meeting):

1. **Finalizing the thesis title**
2. **Explaining about the processes that has to be taken afterwards**
3. **Discussion on the literature review components**
4.

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1. **Finishing the Literature review**
2. **Understanding the project proposal requirements**
3.

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.

Project Log Sheet – Supervisory Session

Student's name: Thomas Augustine MacKinnon **Date:** 20.10.2022 **Meeting No: 2**

Project title: Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Intake: APDMF2204CYS(PR)

Supervisor's name: Dr. Julia Juremi **Supervisor's signature:** …… ……..

Items for discussion (noted by student before mandatory supervisory meeting):

1. Feedback on Literature Review

2. Discussion on Introductory Chapter

3. Discussion on Methodology for project

Record of discussion (noted by student during mandatory supervisory meeting):

1. Going through the Literature Review and highlighting areas for improvement

2. What items are required for Introduction

3. Choosing the right design approach and identifying risk

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1. Make necessary corrections to Literature Review

2. Begin Work on Introductory Chapter

3. Begin Work on Methodology

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.

PLS V1.0

Project Log Sheet – Supervisory Session

Student's name: Thomas Augustine MacKinnon **Date:** 15.11.2023 **Meeting No:** 3

Project title: Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Intake: APDMF2204CYS(PR)

Supervisor's name: Dr. Julia Juremi **Supervisor's signature:** ……………

Items for discussion (noted by student before mandatory supervisory meeting):

1. Notes on Introductory Chapter

2. Notes on Methodology

3. Final Draft of Literature Review

Record of discussion (noted by student during mandatory supervisory meeting):

1. Changes to be made to Scope and Research Questions

2. Inclusion of more graphs

3. Scientific Method being the best choice for the project

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1. Finishing the project proposal

2. Develop Presentation

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.

Project Log Sheet – Supervisory Session

Student's name: Thomas Augustine MacKinnon **Date:** 02.02.2023 **Meeting No: 4**

Project title: Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Intake: APDMF2204CYS(PR)

Supervisor's name: Dr. Julia Juremi **Supervisor's signature:** ………………

Items for discussion (noted by student before mandatory supervisory meeting):

1. **Extension Request**
2. **Revisions to Proposal Chapters**
3. **Discussion on Testing and Experimentation**

Record of discussion (noted by student during mandatory supervisory meeting):

1. **Approval of Extension Request**
2. **Areas to fix for Proposal Chapters**
3. **Begin Testing and Experimentation**

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1. **Follow Procedure for Extension**
2. **Make changes to Proposal Chapters**
3. **Begin Procedure Chapter**

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.

Project Log Sheet – Supervisory Session

Student's name: Thomas Augustine MacKinnon **Date:** 03.03.2023 **Meeting No: 5**

Project title: Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Intake: APDMF2204CYS(PR)

Supervisor's name: Dr. Julia Juremi **Supervisor's signature: …… ……..**

Items for discussion (noted by student before mandatory supervisory meeting):

1. Review of Procedure

2. Discussion on Testing

3. Notes on Update Literature Review

Record of discussion (noted by student during mandatory supervisory meeting):

1. Develop own testing environments as part of project

2. Testing through physical tests and surveying

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1. Build testing Environments

2. Layout Test plan

3. Draft of Survey

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.

Project Log Sheet – Supervisory Session

Student's name: Thomas Augustine MacKinnon **Date:** 14.04.2023 **Meeting No: 6**

Project title: Access Control Evaluation and Improvement of Smart Card and Facial Recognition Technology to Create a Secure Workplace

Intake: APDMF2204CYS(PR)

Supervisor's name: Dr. Julia Juremi **Supervisor's signature: ……………**

Items for discussion (noted by student before mandatory supervisory meeting):

1. Review of Procedure

2. Review of Testing and Results

3. Discussion Chapter format

Record of discussion (noted by student during mandatory supervisory meeting):

1. Finalise Procedure

2. Save visualisation and discussion for relevant chapter

3. Discussion format examples

Action List (to be attempted or completed by student by the next mandatory supervisory meeting):

1. Finishing Procedure and Testing

2. Complete Discussion Chapter

Note: A student should make an appointment to meet his or her supervisor (via the consultation system) at least ONE (1) week prior to a mandatory supervisor session – please see document on project timelines. In the event a supervisor could not be booked for consultation, the project manager should be informed ONE (1) week prior to the session so that a meeting can be subsequently arranged.