2019

Mitigating security implications of bringing your own device in an enterprise environment

Alfred Regerai Gono
Faculty of Information Technology (FIT)
Strathmore University

Recommended Citation

Gono, A. R. (2019). *Mitigating security implications of bringing your own device in an enterprise environment* [Thesis, Strathmore University]. http://su-plus.strathmore.edu/handle/11071/6754

MITIGATING SECURITY IMPLICATIONS OF BRINGING YOUR OWN DEVICE IN AN ENTERPRISE ENVIRONMENT

ALFRED REGERAI GONO

94800

Submitted in partial fulfilment of the requirements for the Degree of Master of Science in Information Systems Security at Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

June, 2019

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Student Name Alfred Regerai Gono
Student Number 094800

Signature
Date 01/03/2019

Approval

The dissertation of Alfred Regerai Gono was reviewed and approved *(for examination) by the following:

Supervisor Name Dr. Vitalis Ozianyi
Lecturer, Faculty of Information Technology
Strathmore University

Signature
Date 01/03/2019

Abstract

The rapid growth in the bring your own device (BYOD) phenomenon, has resulted in the introduction of personal mobile devices in the Enterprise environment. The benefit derived from embracing BYOD in organisations is enhanced mobility of employees and the reduced equipment cost to Enterprises. An effective BYOD management is required to protect company data as diverse mobile devices are finding their way into the enterprise. Available mobile device statistics revealed that 52% of these devices are either lost or stolen worldwide, this becomes a major security concern amid risk of exposure of sensitive and important corporate data.

The highlighted risks to the enterprises requires a solution to safeguard, reduce and attempt to mitigate security breaches. This research seeks to answer the following how intrusion detection is leading to increase in cybercrime? Rational look at security challenges for BYOD and how secure is BYOD?

The rapid application development (RAD) methodology was applied in this research to prototype a scanning and detection technique to prevent or mitigate threats from BYOD to the enterprise environment. The developed application is a scanner and firewall that will be able to scan, monitor and mitigate malicious attacks on BYOD and present results of scanned devices, ports and blocked devices with a 95% accuracy.

Keywords: BYOD, Mobile Devices, Wi-Fi, Android, NetScan, DDWRT, NAC

Table of Contents

Declaration ... ii

Abstract ... iii

Table of Contents ... iv

List of Figures ... vii

List of Tables ... viii

List of Abbreviations/Acronyms ... ix

Acknowledgements ... x

Dedication ... xi

Chapter 1: Introduction ... 1

1.1 Introduction ... 1

1.2 Problem Statement ... 2

1.3 Research Objectives ... 3

1.4 Research Questions ... 3

1.5 Scope and Limitations ... 3

1.6 Research Relevance ... 4

1.7 Summary ... 4

Chapter 2: Literature Review ... 5

2.1 Overview ... 5

2.2 Enterprise Organisations ... 6

2.3 Security Weakness and flaws in Mobile Devices ... 10

2.4 Security Approaches of BYOD ... 16

2.5 Conclusion ... 20

Chapter 3: Research Methodology ... 22

3.1 Overview ... 22

3.2 Software Methodology ... 23

3.2.1 Literature review 25

3.2.2 Observation and applications review 25

3.3 Design 25

3.4 Development 26

3.5 Testing 26

3.6 Deployment 27

3.7 Tool Validation 27

Chapter 4: Systems Design and Architecture 28

4.1 Overview 28

4.2 System Architecture 28

4.2.1 User Interface Design 29

4.2.2. Wireframe 30

4.3 System Analysis 33

4.3.1 Functional Specifications 33

4.4 System Design 35

4.4.1 Technical Specifications 35

4.4.2 Use Case Diagram 35

4.4.3 Class Diagram 36

4.4.4 Sequence Diagram 39

4.4.5 Data Flow Diagram 40

4.4.6 Activity Diagram 41

4.4.7 Database Design 42

Chapter 5: Implementation, Testing and Validation 43

5.1 Overview 43

5.2 Implementation 43

5.2.1 Development Environment 43

5.2.2 Mobile Application Development Tools ... 45
5.3 Testing ... 45
5.3.1 Mobile Device and Application Testing ... 45
5.3.2 System Testing ... 46
5.3.3 Usability Testing ... 46
5.3.4 Compatibility Testing ... 46
5.3.5 Functionality Testing ... 46
5.3.6 User Testing ... 47
5.4 System Validation ... 47
5.4.1 Tool Validation ... 47
Chapter 6: Discussions ... 48
6.1 Overview ... 48
6.2 Discussions of Findings ... 48
6.3 Testing and Validation ... 50
Chapter 7: Conclusion, Recommendations and Future Work ... 51
7.1 Conclusion ... 51
7.2 Recommendations ... 51
7.3 Future Work ... 52
References ... 53
Appendix A: Mobile Security Application Tool Screenshots ... 59
Appendix B: Net Scan Sample Designs ... 62
Appendix C: Turnitin Report ... 65

List of Figures

Figure 2.1 Android's Architecture (development.android.com, 2016) 6

Figure 2. 2 Android’s Architecture (development.android.com, 2016) 6

Figure 2.3 The BYOD Infographic (Logicalis, 2018) 8

Figure 2.4 The Need for BYOD Security (Burnham, 2014).. 13

Figure 2.5 Making BYOD Safe (Trend Micro, 2015) 18

Figure 3. 1 Phases Approach to RAD.. 23

Figure 4. 1 System Architecture 29

Figure 4. 2 Mobile Interface Design 30

Figure 4. 3 Home Login Screen... 31

Figure 4. 4 New Router/Device Screen 31

Figure 4. 5 Port Scanner... 32

Figure 4. 6 Node/Firewall Screen 32

Figure 4. 7 Use Case Diagram 36

Figure 4. 8 Class Diagram 38

Figure 4. 9 Sequence Diagram... 39

Figure 4. 10 Data Flow Diagram 40

Figure 4. 11 Activity Diagram... 41

Figure 4. 12 Entity Relationship Diagram 42

Figure 5. 1 Development Environment Hardware Specifications 44

List of Tables

Table 4. 1 Functional Specifications 34
Table 4. 2 Technical Specifications 35
Table 4. 3 Class Diagram 37

List of Abbreviations/Acronyms

BYOD - Bring Your Own Device

COPE – Corporate Owned Personally Enabled

DDWRT - DresDren Wireless Router

DOI – Digital Object Identifier

GSM – Global System for Mobile communication

IT – Information Technology

MAM – Mobile Application Management

MAM - Mobile Content Management

MDM - Mobile Device Management

MMS - Multimedia Messaging Service

PII – Personally Identifiable Information

SSH – Secure Socket Shell

Wi-Fi – Wireless Fidelity

2G – Second Generation

3G - Third Generation

4G – Fourth Generation

Acknowledgements

I extend my gratitude to my supervisor Dr. Vitalis Ozianyi, for the unwavering support, direction and feedback throughout the course of this dissertation.

I would also want to acknowledge my fellow students who enabled me to successfully complete this research project through encouragement and moral support.

Glory to the almighty

Dedication

This research is dedicated to my beloved wife Fungayi and our angels Ashley, Shantay, Armanda and Antoinette for their loving patience and exuberant fortitude during the entire MScISS study period. My greatest wish is they get inspiration to aim even higher in their future endeavors.

Chapter 1: Introduction

1.1 Introduction

The increase in the market availability of numerous personal electronic gadgets (smartphones, tablets, laptops) with vast processing power and storage capabilities finding their way into enterprises has seen the growth of the BYOD phenomena, many enterprises are now asking their employees to use their own personal devices to access and use enterprise resources, this is called bring your own device. In this research bring your own device (BYOD) means someone coming with their own device connecting to the corporate network and using it to conduct work. The term mobile device describes a handheld computer or tablet made for portability whilst others describe it as portable, wireless computing device that is small enough to be used while held in the hand. Globally the rapid adoption of mobile devices in particular smartphones has grown exponentially from 2.1 billion smartphones users in 2016 to around 2.5 billion by 2019 (Statista, 2019). A smartphone for the purpose of this research is a mobile phone with many functions of a computer. The number of mobile phone users in the world in 2018 was at 4.9 billion, making mobile devices usage outstrip computers three to one. The number of mobile devices at 7.22 billion entails that the growth has been quite exponential surpassing the world population and still growing making it the fastest growing phenomenon (Zachary D.B, 2014).

The identified research gap of mobile security weakness is being compounded due to the high adoption of mobile devices by employees. The bringing of personally owned devices (laptops, tablets and smartphones) to the workplace and using these devices to access privileged company applications and information exposes the enterprise to cyber-attack risk. As the world continues to be increasingly connected, enterprises have now found themselves vulnerable to security threats and breaches as the bring your own device phenomena has been embraced in the workplace, these mobile devices also connect to the internet widening the attack vector and becoming a futile ground for attacks from hackers plus other malicious users. According to Cybersecurity Insights Report, (2017), 40% of organisations have suffered due to employee’s mobile devices being compromised in the past twelve months. In the research gap it was also noted a serious vulnerability exists in that mobile devices handsets do not detect attacks by default, leaving the burden of this critical task to security aware users to install applications to detect and prevent attacks on mobile handsets. This points out to the fact that mobile manufacturers have a vital role to play in mitigating the proliferation and prevention of these vulnerabilities or create remedies on this click-driven interface.

The rising popularity of the bring your device (BYOD) has seen employees performing work-related tasks through their own mobile devices. The authorisation of employee-owned devices in the enterprise is a challenge to the IT administrator as there are many security risks, non-standard user settings, lack of anti-virus on the devices which leads to attacks. These attacks exploit weakness inherent in smartphones that can come from the communication mode short message service (SMS-text messaging), multimedia messaging service (MMS), Wi-Fi, Bluetooth and GSM. Security countermeasures for smartphones focus on different layers of software, to the dissemination of information to end users. These practices need to be observed at all levels from design to use, development of operating system, software layers and downloadable applications. From a mobile device security perspective, the research sort to prevent or mitigate the stealing of data be it personal or corporate sensitive information and the focus will be on Android the most widely-used operating system in the world created by Google. In this research android will be an open source operating system used for smartphones and tablet computers.

1.2 Problem Statement

This research is concerned with the following problem or issue. The embracing of ubiquitous computing has seen the increase and usage of personal mobile devices on enterprise systems to access corporate services, this has exposed the business to serious security risk as the enterprise security mechanisms are compromised by the personal mobile device (Sen, 2012). The number of mobile devices now connecting to network poses a great challenge for IT departments (Ismail, 2017) whose owners lack appreciation to security issues as humans are perceived to be the weakest link as technology has evolved to become more user centric, there is a tendency to over trust people in their usage of mobile devices this leads to poor decisions which exposes the enterprises to breaches. In this research paper we will review the security model of smartphones (android) to better understands the impact these devices will continue to have as their adoption and usage grows within enterprises. The solution offered for the described problem is to develop a networking scanning tool to be called NetScan that will scan, detect and disrupt unauthorised processes running on mobile devices. The tool should be able to display incidences and terminate identified breaches in real-time.

1.3 Research Objectives

The overall objective for this research is to create a mobile network scanning (NetScan) tool to detect and terminate unwanted processes on BYOD.

This research is concerned with the following:

i. To identify mobile security weaknesses that are exploited by cyber attackers.
ii. To identify and review the current security approaches used in mobile devices.
iii. To design, develop, test mobile based information security application tool to improve breaches detection.
iv. To validate the effectiveness of the developed information security application tool targeting mobile devices.

1.4 Research Questions

The research questions that will be addressed regarding this problem:

i. What mobile security weaknesses are being exploited and inherent in mobile devices?
ii. What are the current security approaches used in mobile devices?
iii. How can the proposed solution be designed, developed, tested?
iv. Does the developed tool detect and terminate unwanted processes on the enterprise network?

1.5 Scope and Limitations

This research will be limited to security of bring your own device (BYOD) focusing on the mobile device (smartphones) which use android software which is open source, thus this increase the risk of attacks. It seeks to develop a mobile device security application tool for detecting and terminating malicious activities. The research focused only on the android platform and android driven mobile applications. This can then be further developed for commercial use in the future and also to look at the other mobile operating systems.

1.6 Research Relevance

This research will seek to provide a mobile based application tool to scan and detect malicious activity on the mobile device to help organisations in better management of smartphones that now connect to the corporate enterprise network. In the process raise awareness of the dangers of downloading and installing software without authenticating. An overview of existing tools has established that these tools are limited to applications and a few address the identified research gap of security at operating system level while using android an open source software. This open source platform makes it an attractive attack environment for hackers as numerous developers are involved in producing numerous flavours of the operating system for use in mobile devices.

1.7 Summary

This chapter covered the introduction, problem statement, research objectives and research questions, research hypothesis, scope and limitations and research relevance. We cannot ignore that smart devices have become a business tool essentially, with the rise of BYOD. In the process they have become a target for malicious attacks and being used as a backdoor to gain access to critical enterprise systems. Chapter 2 will extensively cover the literature review, while Chapter 3 will cover the methodology. Systems Design and Architecture follows in Chapter 4, while Chapter 5 dwells on Testing and Validation. The Discussions are covered in Chapter 6. Finally, Chapter 7 deals with the Conclusion, Recommendations and Future Work.

Chapter 2: Literature Review

2.1 Overview

This research focuses on bring your own device (BYOD) a phenomenon which has redefined modern enterprise landscape business usage and behaviour (Kerner S.M., 2019). This chapter explores the literature review, with the purpose of identifying the need to enhance security monitoring and protecting the employee owned mobile devices as they are used in an organisation. The BYOD mobile device security has become increasingly important with personal and business information now stored on smartphones and tablets besides the BYOD being used for communication, they also plan and organise the user's work and private life. The use of these technologies have caused significant changes in organisations, whilst becoming a source of new security risks and a broad attack vector. The mobile phones are poised to be the world's most pervasive technology outnumbering landlines and personal computers (Karison, A.K, Bederson, B.B & Contreras-Vidal,J.L, 2008). Mobile devices applications and services have become integrated into the people daily livelihood and at professional level as they collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company (Karison, A.K, Bederson, B.B & Contreras-Vidal,J.L, 2008).

The employee owned mobile devices (BYOD) have security issues, according to (Ghosh, A., Gajar, P.K., and Rai, S., 2013) of these security issues 80% are on android as the most popular operating system due to it being open source. The BYOD devices using android are the most commonly used according to (Harris, M, A, Patten, K., and Regan, E., 2013) because of that we have people who are always looking for personal identifiable information (PII) (Schwartz, P., and Solove, D.J., 2014). Figure 2.1 below depicts the android's architecture for better understanding. As we can see, these BYOD mobile devices are now becoming a standard for employees in the enterprise industry, furthermore no one has studied how security flaws of these mobile devices is going to impact the enterprise industry. My research will explore how the BYOD personal mobile devices when used in an enterprise will result in security issues which in turn will impact the enterprise. Among the many security vulnerabilities that pestilence us can be traced back to software imperfections research has shown. From buffer overflows to SQL injection and cross-site scripting flaws, blunders or lack of caution by programmers continue to offer attackers a way into our systems.

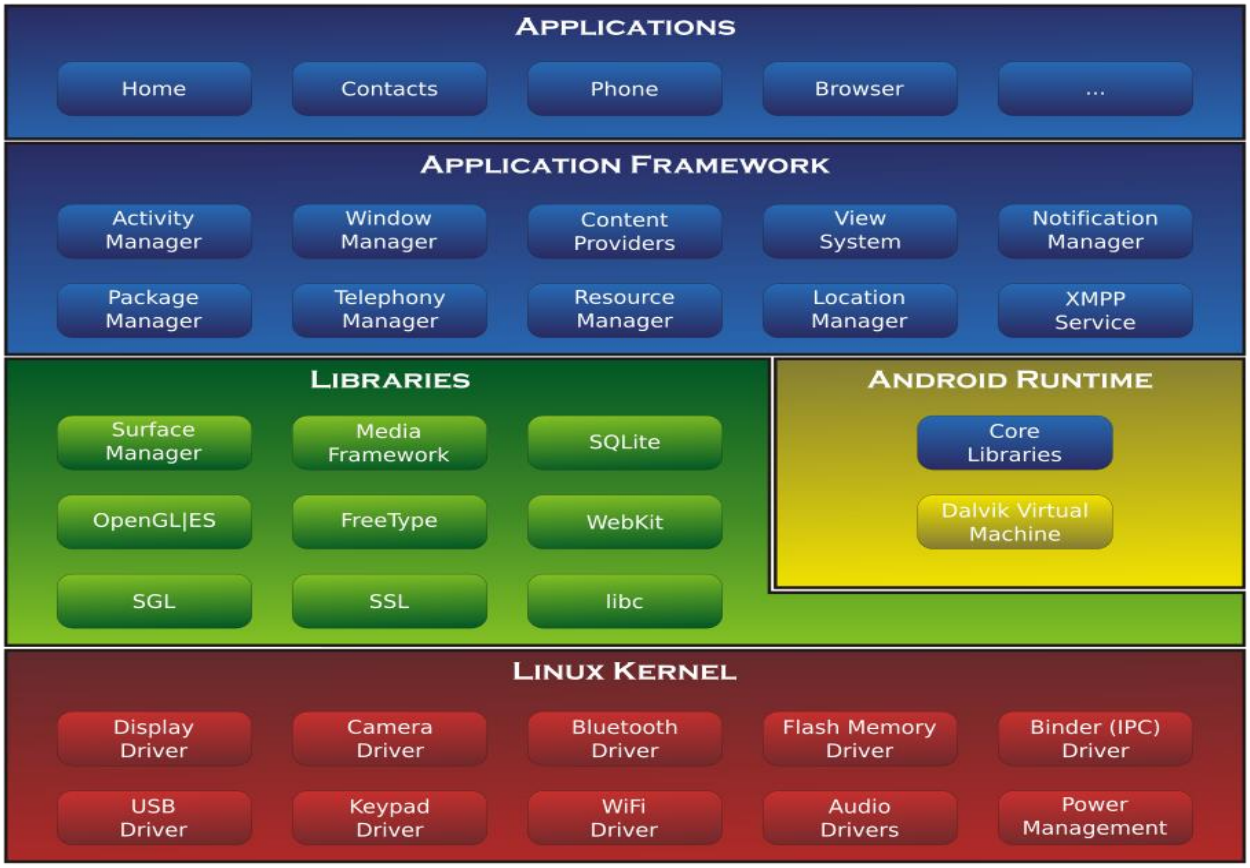


Figure 2.1 Android's Architecture (development.android.com, 2016)

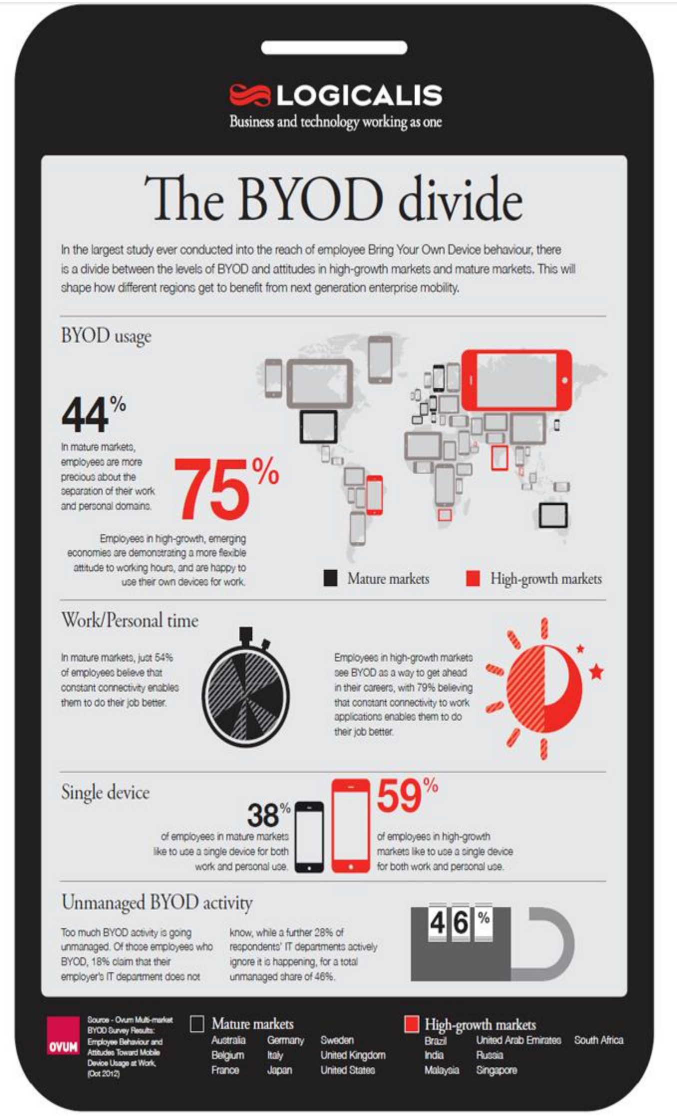
Figure 2. 2 Android’s Architecture (development.android.com, 2016)

2.2 Enterprise Organisations

The term enterprise depicts a company, business, organisation or other purposeful endeavour. For the purpose of this research an enterprise will mean all aspects of a business, particularly a business that has multiple departments or branches that focus on different activities. The focus will be on enterprise private sector, sometimes referred to as the citizen sector which is run by private individuals or groups for profit (Rouse, 2013). According to (Aurelie Leclercq - Vandelannoitte, 2015) consumerisation increase has led to investigation on how enterprise organisations react to employees’ adoption, adaption and use of personal devices at work. They conclude that this encourages innovative individuals and IT driven changes in enterprise practices (Aurelie Leclercq-Vandelannoitte, Henri Isaac., 2015). Other authors (Murdoch, M., Harris, J. and Devore, G., 2010) posit that there has been abandoning of enterprise IT hardware and software in favour of consumer technologies that offer greater freedom and fun. (Harris, Jeanne & Ives, Blake & Junglas, Iris., 2012) points out that IT consumerisation will be the greatest influential trend affecting the enterprise. (Ortbach, K., Bode, M. and Niehaves, B., 2013) points out that due to consumerisation employees establish, personalised setups which include privately owned and company provided Information Technology. This results in extending the end user computing phenomenon (Baskerville, 2011) (Ortbach, K., Bode, M. and Niehaves, B., 2013). In their contribution concludes that the proliferation of smartphones, home broadband internet access, mobile phone networks including wireless internet access have disrupted IT adoption in enterprises (Baskerville, 2011). Concurring with the assertion that due to the reduced costs, pervasiveness and availability of mobile devices many people now use mobile devices both for private and professional work (Crowston, Fitzgerald, Gloor, Schultze, & and Yoo, 2010).

The user behaviours in enterprises have changed, with employees becoming more technologically savvy, connecting to sophisticated devices with a willingness to use personal technologies in professional spheres thus bringing IT based changes to their enterprises (Kerner S.M., 2019). From the above scholarly review employee's resourcefulness to bring and use personal devices at work might initiate IT driven transformations that allow enterprises to evolve and rethink their processes (Harris, J.G., Ives, B. and Junglas, I., 2011). Reviewed literature on enterprise responses and acceptance of mobile personal devices have been studied mainly in practitioner studies from two main perspectives security and cost efficiency. The focus area has been security issues and risk emanating from these adopted mobile devices, which may inhibit enterprise acceptance of bring your own device (BYOD) while on the other hand reduction of technological costs remains an attraction to enterprises (Gens, F., Levitas, D. and Segal, R., 2011) This they further argue enables the enterprise to gain by employee creativity and innovativeness as they freely use their BYOD for work related activities they referred these employees as iWorkers (Gens, F., Levitas, D. and Segal, R., 2011). According to (Meske C., Stieglitz S., Brockmann T., Ross B., 2017) who state that the impact of mobile IT consumerisation in enterprises has seen an increased number of employees using personal mobile devices for work.

They concluded that digital object identifier (DOI) can efficaciously be applied to expound BYOD adoption behaviour, differentiated management strategies have to be applied to the whole workforce (Meske C., Stieglitz S., Brockmann T., Ross B., 2017). In their survey (Logicals, 2018) state that there is too much BYOD activity going on unmanaged, 18% claim IT Department does not know, while 28% state that IT departments actively ignore what's happening Figure 2.2 illustrating the employee BYOD behaviour.



LOGICALIS
Business and technology working as one

The BYOD divide

In the largest study ever conducted into the reach of employee Bring Your Own Device behaviour, there is a divide between the levels of BYOD and attitudes in high-growth markets and mature markets. This will shape how different regions get to benefit from next generation enterprise mobility.

BYOD usage

44%

In mature markets, employees are more precious about the separation of their work and personal domains.

75%

Employees in high-growth, emerging economies are demonstrating a more flexible attitude to working hours, and are happy to use their own devices for work.

Work/Personal time

In mature markets, just 54% of employees believe that constant connectivity enables them to do their job better.

Employees in high-growth markets see BYOD as a way to get ahead in their careers, with 79% believing that constant connectivity to work applications enables them to do their job better.

Single device

38% of employees in mature markets like to use a single device for both work and personal use.

59% of employees in high-growth markets like to use a single device for both work and personal use.

Unmanaged BYOD activity

Too much BYOD activity is going unmanaged. Of those employees who BYOD, 18% claim that their employer's IT department does not know, while a further 28% of respondents' IT departments actively ignore it is happening, for a total unmanaged share of 46%.

Source - Ovum Multi-market BYOD Survey Results: Employee Behaviour and Attitudes Toward Mobile Device Usage at Work, (Oct 2012)

Figure 2.3 The BYOD Infographic (Logicalis, 2018)

Concurring with the assertion that BYOD's are major trends that are impacting how enterprises perceive their own I.T (Donaldson S.E., Siegel S.G., Williams C.K., Aslam A. , 2015). They acknowledge the capability of the computing power on these mobile devices, from multiprocessing, graphical user interface and gigabytes of memory all this available at our finger tips the face of IT is changing almost daily (Donaldson S.E., Siegel S.G., Williams C.K., Aslam A. , 2015). The contribution of (Kim, 2016) agreeing to that many enterprises recently introduced BYOD and adopted the network access control (NAC) and mobile device management (MDM) system for the mitigation of confidential information leakage, access control and efficient user management. He further posits that safety of these mobile devices remains of great concern as there are security threats due to frequent loss, theft of these devices and low security (Kim, 2016). In their paper they propose behaviour based abnormality detection method in the BYOD environment and patterning various user's information use contexts (Kim, 2016). The other school of thought (Aenugu N.R., Butakov S., Zavarsky P., Aghili S., 2018) postulates that enterprises can adopt BYOD in two ways, contracting out to a vendor or build a custom made BYOD solution. In their research (Aenugu N.R., Butakov S., Zavarsky P., Aghili S., 2018) outlines residual risks to assist enterprises determine solution suitable for BYOD. Risk areas include lost and stolen devices, unauthorised third party applications that need to be analysed (Aenugu N.R., Butakov S., Zavarsky P., Aghili S., 2018). For the highlighted risk areas, risk mitigation techniques were outlined following the widely accepted industry standards. This research work adds additional source document to the knowledgebase of bring your own device (Aenugu N.R., Butakov S., Zavarsky P., Aghili S., 2018).

In their contribution (Balboni, F., Berman, S.J, Korsten, P. J., 2015) they state that mobile devices not only play an important role in collective consumption of information, but generate a growing proportion of new information with more than 2.5 quintillion bytes of data created each day. Data traffic is growing at 80% per year, however the understanding of the implications of the mobile devices in the enterprises is still to be understood (Balboni, F., Berman, S.J, Korsten, P. J., 2015). They argue that time has come for the enterprise to look beyond consumer applications and consideration be given to the transformational potential of mobile inside the enterprise. (Balboni, F., Berman, S.J, Korsten, P. J., 2015) posits that due to the ubiquity of mobile devices enterprises have opportunity to provide employees solutions to effectively work, tailoring workflows right information to the right employee. This they point out has seen the emergent of the individual enterprise resulting in engaged and appreciative customers. In conclusion they agree with the assertion that security is key and controls have to be employed for enterprise to cope with the fragmented device platforms driven by BYOD phenomenon (Balboni, F., Berman, S.J, Korsten, P. J., 2015). The enterprise perspective is still missing within the body of literature of the Bring Your Own Device as it a rapidly growing trend in enterprises (Downer, K., and Bhattacharya, M., 2015). BYOD presents a unique list of security concerns for enterprises implementing BYOD policies. (Downer, K., and Bhattacharya, M., 2015) points that while there is growing awareness of risk involved in incorporating BYOD in enterprises, it's still an underrated security concern. In their research they focused on specifically classifying BYOD security challenges alongside a comprehensive framework and solutions which were analysed to gauge limitations (Downer, K., and Bhattacharya, M., 2015).

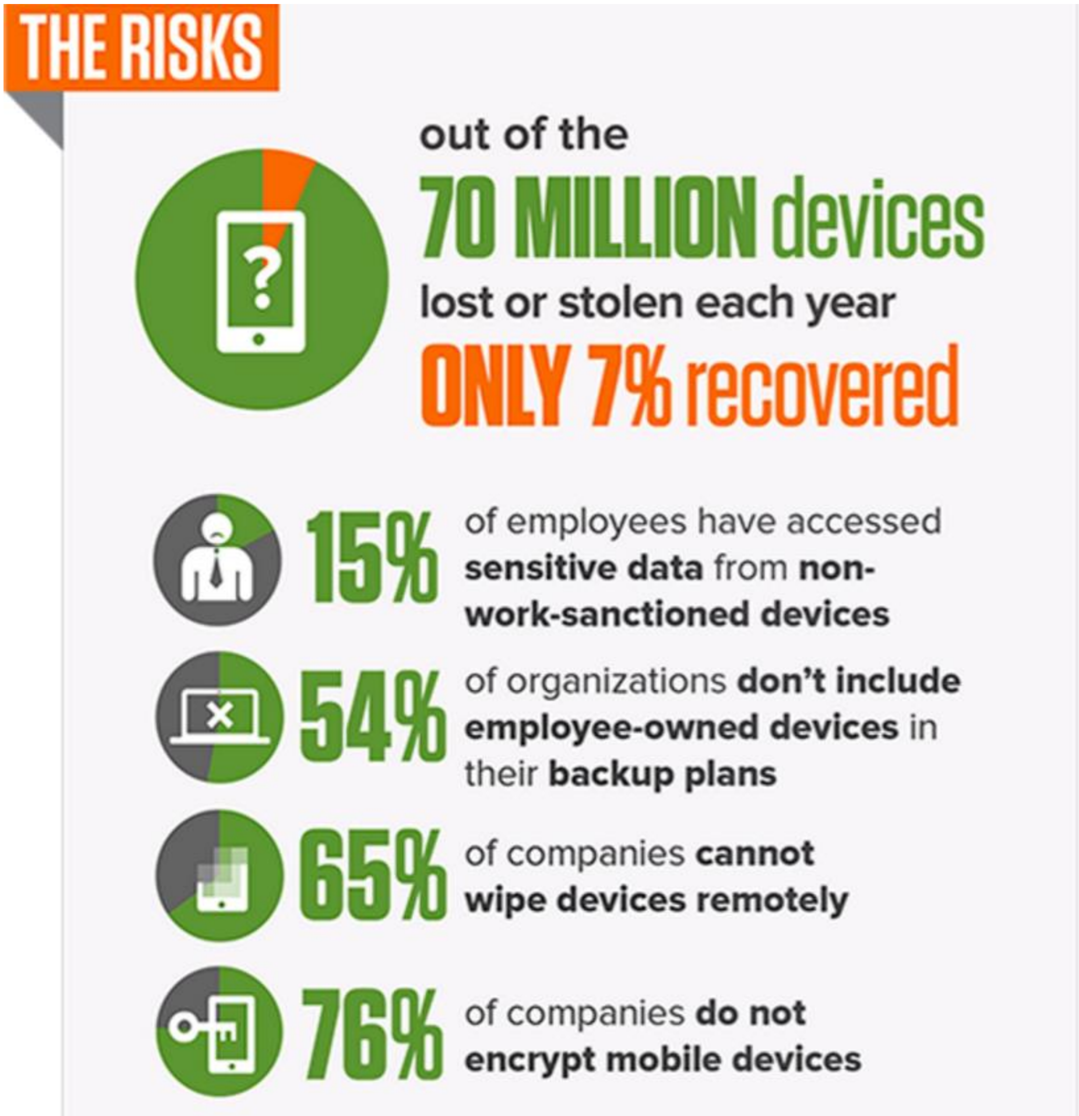
Looking at the Zimbabwean banking sector, (Musarurwa, Alfred & Flowerday, Stephen & Cilliers, Liezel., 2017) states that information security in this enterprise sector is heavily controlled, as banks store and mange client's private information. The BYOD phenomenon has enabled employees to connect to organisational network with their own devices. They further state that IT department fail to prescribe information security measures to mobile devices. This has compelled enterprises to entrust security of bank information assets with employees who become the de facto administrator (Musarurwa, Alfred & Flowerday, Stephen & Cilliers, Liezel., 2017). In their assertion they conclude that while technology solutions are being developed they have neglected the human aspect that implements these solutions. They studied 270 employees which lead to the conclusion that employee individual traits are significant for the BYOD information security culture (Musarurwa, Alfred & Flowerday, Stephen & Cilliers, Liezel., 2017)

2.3 Security Weakness and flaws in Mobile Devices

Contributing to the above (Mansfield-Devine, 2018) further asserts that while these problems are well implicit, concern or the question is why do they persevere? Attackers can also get more aggressive and turn to other forensic and penetration-testing tools such as Metasploit or Mimikatz that allow you to either inject code into system memory or read data stored in memory (Spring T, 2017). These open-source tools, along with others such as Lazagne, and Meterpreter, allow attackers to probe deeper into targeted systems, steal credentials and open reverse shells back to the adversary's control server. The other school of thought postulates that there will be advanced malware attacks, with more advanced obfuscation, polymorphism and injection techniques, that evade potential monitoring and detection software and techniques (Guri, M., Kedma, G., Kachlon, A., and Elovici, Y., 2014). (Abubakar Garba Bello, 2017) In their contribution concludes that during the last 10 years an unprecedented global adoption of technology has been experienced. This they further argue has helped usage of the internet explode from 15% by use to more than 40% of the world's population and companies of all sizes have built Internet connected networks to communicate with customers saving data that fuels their businesses. Collection and digitalisation of information combined with the vastness and reach of modern networks presents an enticing opportunity for thieves to steal data (Abubakar Garba Bello, 2017). Concurring with the assertion that security of transactions becomes paramount (Lewis, 2015) states that there is need for scientific study of critical infrastructures and their protection networks of nodes and links. There is critical need for analysis of the network to identify vulnerabilities and risks (Lewis, 2015).

The other school of thought (Josang A, Miralabe L, Dallot L, 2016) postulates that GSM network was designed in the 1980s and due to political pressure, the security of GSM was made weak to allow interception by law enforcement agencies. In their research (Josang A, Miralabe L, Dallot L, 2016) further elaborate that the subsequent network technologies of 3G and 4G where designed with security strengthened, but the weak link remains 2G limiting the security level of mobile networks in general as all the mobiles devices are being designed with the capability to connect to all the mobile networks 2G,3G and 4G. There are still security gaps most mobile handsets do not detect attacks by default stated (Josang A, Miralabe L, Dallot L, 2016).

Anecdotal evidence continues to support that in mobile application security, most users are unware of the security risks (Wang, Y., Wei, J., and Vangury, K., 2014). According to Symantec Report, (2017) 57% of adult users are still unware that security solutions exists for mobile devices. According to (Ogie, 2016) research should focus more on mobile platforms, analysis, detection and evaluation of malicious applications. According to (Kim, 2016) they posits that traditionally, stand-alone computers and small networks rely on user authentication and access control to provide security. These physical methods use system-based controls to verify the identity of a person or process, explicitly enabling or restricting the ability to use, change, or view a computer resource. However, these strategies are inadequate for the increased flexibility that distributed networks such as the Internet and pervasive computing environments require because such systems lack central control and their users are not all predetermined (Kim, 2016). Mobile users expect to access locally hosted resources and services anytime and anywhere, leading to serious security risks and access control problems (Kim, 2016). Other authors (Ismail, 2017) bring forward that security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wireline networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology (Ismail, 2017). These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance (Ismail, 2017). The contribution of (Cooper, W.T., and Thangamuthu, K., 2014) shows that we now have increased dependency on web applications through usage of mobile devices. Anecdotal evidence continues to support that malicious attack techniques have now shifted from the traditional web applications running on the desktop or laptop to mobile applications running on diverse mobile devices. They point out the use of touch-based interactions leading to a phenomenon now known as tap jacking which is an untapped threat in android (Cooper, W.T., and Thangamuthu, K., 2014). The risks statistics associated with BYOD are illustrated in Figure 2.3 to buttress the BYOD security need.



THE RISKS

out of the 70 MILLION devices lost or stolen each year ONLY 7% recovered

15% of employees have accessed **sensitive data** from **non-work-sanctioned devices**

54% of organizations **don't include employee-owned devices** in their **backup plans**

65% of companies **cannot wipe devices remotely**

76% of companies **do not encrypt mobile devices**

Figure 2.4 The Need for BYOD Security (Burnham, 2014)

Research has shown that mobile devices are the biggest security blind spot the power, ubiquity and capacity of smart phones present a security risk in organisations (Zimperium, 2017). Smartphones store critical personal and corporate data, whilst they can offer a backdoor to the more sensitive data. The other school of thought postulates that smartphones and other mobile devices have conquered every aspect of our lives (Totten, J., & Hammock, M., 2014). Security is an issue as they use wireless communications and the wide range of applications within a variety of platforms focusing on issues, trustees, reliabilities and accuracy providing knowledge to vital threats to users and enterprises (Totten, J., & Hammock, M., 2014).

Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from attacks, damage or unauthorised access (Craigen, D., Diakun-Thibault, N., & Purse, R. , 2014). Organisations with internet connectivity are prone to risk of attack. It has now evolved from what if you will be attacked, to when you will you be attacked. While the bulk of cyber-attacks are automated and indiscriminate, exploiting known vulnerabilities rather than targeting specific organisations (Craigen, D., Diakun-Thibault, N., & Purse, R. , 2014). The likelihood of an organisation being breached right now without being aware is high. They are two main attack vectors found in mobile networks, being any attack from the internet and the attack from the network. Today, attacks are bigger, faster, and deeper, ranging from blended (cyber-physical) attacks and malicious counterfeit hardware, to entire supply chain compromises and adaptive attacks on critical infrastructure (Craigen, D., Diakun-Thibault, N., & Purse, R. , 2014). The other school of thought (Garba, A.B., Armarego, J., Murray, D., 2015), highlights that BYOD is a growing trend in the enterprise environment. The factors that have given rise to this are work flexibility, increased productivity and efficiency of employees. The privacy and security are major concerns on these mobile devices BYOD allows access anywhere anytime, thus confidentiality and integrity of enterprise information resources and assets are at great risk (Garba, A.B., Armarego, J., Murray, D., 2015). In their research they focused on information and privacy in BYOD environments, in their case studies on organisational practises of BYOD concludes that enterprises need to use explicit policies and understanding risks is key (Garba, A.B., Armarego, J., Murray, D., 2015).Empirical evidence with regard to bring your own device (BYOD) has shown that it has emerged as the fastest growing phenomenon which IT divisions are having to deal with, this has introduced a boundless place where enterprise data is kept in various data locations (Oktavia, T., Tjong, Y., Prabowo, H., and Meyliana., 2016). They stress that problems associated with privacy and security in BYOD environment need to be identified. In their study they identified legal issues related to security and privacy challenge in BYOD as this is most important to any enterprise to ran their business (Oktavia, T., Tjong, Y., Prabowo, H., and Meyliana., 2016). The BYOD environment changes the operational processes and methods of organisation to operate their business, as this allows employees to work inside or outside their working place. (Oktavia, T., Tjong, Y., Prabowo, H., and Meyliana., 2016) argue that the security level of private network is lower than public networks.

While (Ogie, 2016) posits that BYOD collectively refers to related technologies, concepts and policies allowing employees access to internal enterprise IT resources using personal mobile devices. He points out that it's a side effect of consumerisation of IT, where technology emerge in the consumer market then spread to business and government enterprises. According to (Ogie, 2016) employees love the use of any device anywhere workstyle. He asserts that several risks are associated with BYOD and they are big gaps in BYOD policies adopted by today's organisations. He establishes the background of BYOD risks in the research having considered conditions that increase the occurrence of risks and consequences. The aim was to present the most commonly adopted BYOD solution, remedies and important policy considerations.

In their contribution (Ali, S., Qureshi, M.N., and Abbasi, A.G., 2015) they state that BYOD concept in enterprise environment is growing due to mutual benefits. They point out that BYOD deployment brings serious security and privacy concerns. (Ali, S., Qureshi, M.N., and Abbasi, A.G., 2015) posits that critical information can be leaked ruining the enterprise reputation and trust relationship. This research analysed threats associated with BYOD and presents security requirements and classification of security models discussed in literature. In conclusion the identified gaps provided a comprehensive design to meet the security requirement of the BYOD paradigm (Ali, S., Qureshi, M.N., and Abbasi, A.G., 2015). They proposed a framework which did not require modification to the underlying kernel and allowed IT remote administration to manage and control BYOD devices (Ali, S., Qureshi, M.N., and Abbasi, A.G., 2015). According to (Meske C., Stieglitz S., Brockmann T., Ross B., 2017) there are several important advantages for employees and employers when employees bring their own devices to work. They state that there are significant concerns about security privacy. In their research on handheld mobile devices are just the beginning of a generation of tools for on demand communication allowing enterprises to know everything an employee does, says, sees and be able to geo locate users (Meske C., Stieglitz S., Brockmann T., Ross B., 2017). They point out that it's now possible to record audio, video, health information due to the vast available capabilities on the mobile devices. Whilst embracing the mobile devices in the workplace has become the norm smartphones have become very popular due to their unique characteristics (Wang, Y., Streff, K., and Raman, S., 2012). Their adoption has presented challenges requiring new business models that offer countermeasures to ensure security. In smartphone threat model, malware is disguised as normal application through website or application store where users download the malware to the smartphone, which attempts to control resources, collects data and redirect the smartphone to malicious website or premium account (Wang, Y., Streff, K., and Raman, S., 2012).

2.4 Security Approaches of BYOD

The bring your own device in the corporate world has become increasingly popular, altering the way we work (Denys A. Flores, 2016). In a study of 3 000 I.T Managers and 1300 users (Intel, 2012) draws a conclusion that increased productivity is big benefit of BYOD (Intel, 2012). According to (Denys A. Flores, 2016) seamlessly allowing employees usage of personal devices in enterprise workspace reduces the need for multiple devices, however mixing personal and enterprise data presents security threats to proprietary information. Research has shown that these mobile devices had no additional security beside the default applications, and there is a tendency to choose usability over security highlighted (Denys A. Flores, 2016). Device security, malware and the enforcement becomes the major concern of BYOD. (Denys A. Flores, 2016) posits that BYOD security is a concern of many IT departments hence there is need for implementing a secure container to separate corporate and personal data on mobile devices to mitigate dangers brought by BYOD. The approach compared containers to Samsung Knox and IBM MaaS360 and concluded that these are promising solutions to BYOD security concerns (Moss, 2018).

Other authors (Rathnasekara, C., Athukorala, T., Dikwellage, L. and Wickramasuriya, U., 2017) point out that BYOD paved way allowing employees to use on mobile device for corporate work, however the downside is that it increased the risk of leaking sensitive corporate information from these devices to the outside. (Rathnasekara, C., Athukorala, T., Dikwellage, L. and Wickramasuriya, U., 2017) proposes Corporate Owned Personally Enabled (COPE) concept as a solution, where the company owned devices can be used for both corporate and personal use by employees. However, they are agreed that securing privacy or stopping leakage of corporate data to the outside is challenging. They also proposed a solution for Android mobile devices called Enterprise Secure Center (ESC) which is a secure environment for use of corporate data while keeping personal data intact (Rathnasekara, C., Athukorala, T., Dikwellage, L. and Wickramasuriya, U., 2017).

Consumerisation of mobile devices according to (Flores, D.A., Qazi, F., and Jhumka, A., 2016) has introduced the bring your own device trend to organisational context. These devices are perceived less secure compared to those supplied by the organisation. The issue of accessing corporate information from inside or outside the organisation perimeter has raised security concerns. In their findings (Flores, D.A., Qazi, F., and Jhumka, A., 2016) further asserts that it’s difficult to differentiate external malicious activity from reckless/naive employee behaviour. They proposed a STRIDE based threat model as a solution to analyse BYOD threat interactions from both inside and outside the corporate perimeter. Other authors (Tse, D., Wang, L., and Li, Y., 2016) concur that BYOD adoption has become more popular in the enterprise because of convenience and fantastic user experience. They assert that BYOD expose the enterprise to security risks, thus BYOD becomes an opportunity and a threat to enterprises. They propose to derive a secure mobility management solution from three contemporary BYOD solutions Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management (MCM). (Tse, D., Wang, L., and Li, Y., 2016) gives an enterprise a holistic view of the BYOD deployment so that they can choose appropriate solutions to secure own BYOD deployment. According to (Downer, K., and Bhattacharya, M., 2015)mobile devices are vulnerable to theft and loss due to their size and common usage environment, as they allow users mobility as they work away from the desks, while travelling and in public locations. This scenario brings high risk of loss of the mobile device. They propose a solution of using a wearable token that constantly attests to the user’s presence (Downer, K., and Bhattacharya, M., 2015). When token and device lose contact the devices automatically secures itself, this will require little effort from the user making it attractive to use. This they conclude relieves the tension between security and usability through the use of a wearable wireless hardware token (Downer, K., and Bhattacharya, M., 2015). Figure 2.4 illustrates making BYOD safe statistics.

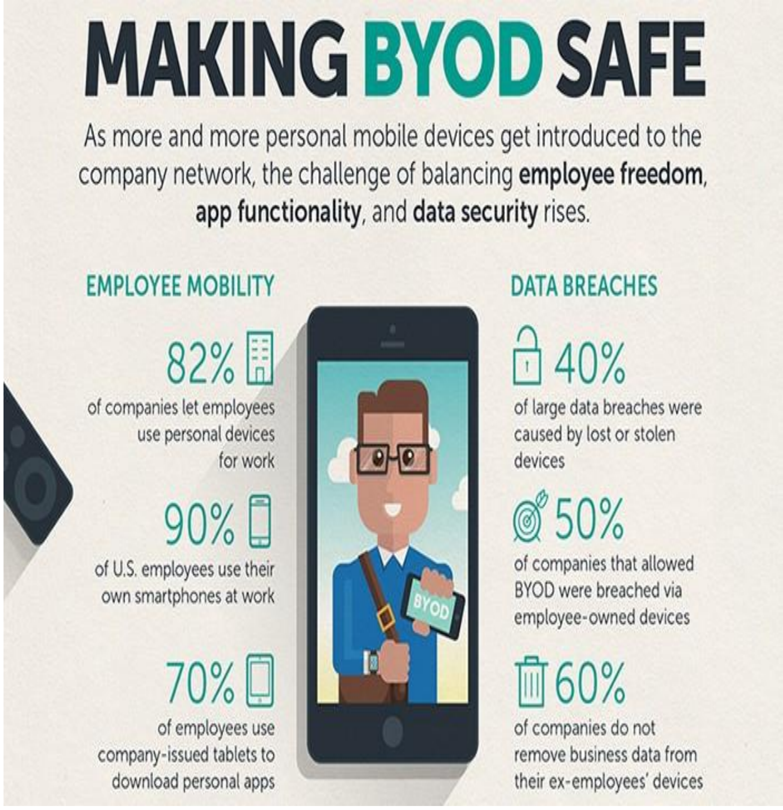

MAKING BYOD SAFE
As more and more personal mobile devices get introduced to the company network, the challenge of balancing employee freedom, app functionality, and data security rises.
EMPLOYEE MOBILITY
82%
of companies let employees use personal devices for work
90%
of U.S. employees use their own smartphones at work
70%
of employees use company-issued tablets to download personal apps
BYOD
DATA BREACHES
40%
of large data breaches were caused by lost or stolen devices
50%
of companies that allowed BYOD were breached via employee-owned devices
60%
of companies do not remove business data from their ex-employees' devices

Figure 2.5 Making BYOD Safe (Trend Micro, 2015)

These gaps that have been revealed in the literature have provided an opportunity for a research to be contributed to, in their assertion (Garba, A.B., Armarego, J., Murray, D., 2015) postulate various mobility strategies, defences and measures, control aspect, management and governance aspect in implementing BYOD strategy as an enterprise. They concur with that the rapid growth of mobile technology, availability of 3G/4G services and smartphones having created a new phenomenon for communication and data processing ability conduct business BYOD (Garba, A.B., Armarego, J., Murray, D., 2015). This phenomenon they conclude brings many risks to the enterprises and increases the attack vector for hackers to explore. In their contribution (Burnham, 2014) states that their different types of user interactions and deployment issues surrounding public displays, they used mobile devices to interact with large public displays. They discussed three application domains personal, semi-public and public. Personal allow a single user to visualise and process information at once, semi-public displays are situated in office building and public displays are locations that are open, usually with high pedestrian traffic like airports (Burnham, 2014). The other school of thought (Ocano, S.G., Ramamurthy, B., Wang, Y., 2015) posits that introduction of BYOD policy in the corporate world creates benefits for enterprise and employee.

However, this phenomenon creates security challenges as new vulnerabilities arise space isolation, data confidentiality and policy compliance. The handling of resource constraints of mobile devices and installed applications seeking to perform BYOD functions (Ocano, S.G., Ramamurthy, B., Wang, Y., 2015). The authors present Remote Mobile Screen (RMS), an approach for securing BYOD environments. This approach provides a trusted virtual machine running a mobile operating system on the enterprise network which then connects the BYOD (Ocano, S.G., Ramamurthy, B., Wang, Y., 2015). Agreeing with the notion that mobile devices are prevalent in workplaces and creates a unique environment (Wang, Y., Wei, J., and Vangury, K., 2014). The other school of thought postulates that bring your own device in enterprises are extensions of the corporate network thus it becomes essential to secure BYODs to protect enterprise networks. (Wang, Y., Wei, J., and Vangury, K., 2014) concurring with the assertion that security tools virus software, anti-spam software is widely used to protect corporate networks, similar tools are desirable to protect BYODs. Research has shown that BYODs have many advantages reducing enterprise cost, while increasing productivity. They also point out that their issues and challenges due to their unique security requirements, they presented a BYOD security framework that guides enterprises as they adopt BYODs (Wang, Y., Wei, J., and Vangury, K., 2014).

Anecdotal evidence continues to support that mobile malware has gained significant ground since the introduction of mobile devices smartphones, handheld devices (Penning, N., Hoffman, M., Nikolai, J., and Wang, Y., 2014). TrendLabs estimated 718,000 malicious and high risk android applications. Mobile devices malware malicious infections come through various techniques repackaged legitimate applications, updating current application that piggy back malicious variants. In their research (Penning, N., Hoffman, M., Nikolai, J., and Wang, Y., 2014) summarises that mobile malware threats and attacks, cybercriminal motivations behind malware, existing prevention methods and their limitations including the challenges encountered when preventing malware on mobile devices. The authors proposed cloud-based framework for mobile malware detection, the proposed framework requires a collaboration among mobile subscribers, application stores and IT security professional (Penning, N., Hoffman, M., Nikolai, J., and Wang, Y., 2014). They conclude that cloud-based malware detection is a promising approach towards mobile security. In their contribution (Fani, N., von Solms, R., and Gerber, M., 2016) states that information is a critical important asset, faces threats that can impact processes email retrieval and access to organisational system services. They point out that as a consequence of these threats enterprises should pay attention to security of information. BYOD adoption has benefits and introduces risks, and the authors (Fani, N., von Solms, R., and Gerber, M., 2016) discussed the small, medium and micro enterprises (SMMEs) context and challenges towards the governance of BYOD. They looked at the existing BYOD approaches and provided one suitable for SMMEs. They further evaluated and compared against the BYOD approaches in existence that where identified. In their approach (Fani, N., von Solms, R., and Gerber, M., 2016) utilised a cyclic approach. The other school of thought postulates that mobile devices are widely being used for personal and business purposes (Wang, Y., and Alshboul, Y., 2015). As they carry sensitive data they are easy target for cyber criminals. Mobile security testing targets to detect vulnerabilities and malicious applications on a mobile device. (Wang, Y., and Alshboul, Y., 2015) present for testing approaches for mobile security in their paper which are mobile forensic, penetration testing, static analysis and dynamic analysis. These gaps have been revealed in the body of literature have provided an opportunity for a research to be contributed to (Wang, Y., and Alshboul, Y., 2015) uses a mobile security testing network to further demonstrate in their paper how to evaluate the effectiveness of the four testing approaches. They conclude that mobile testing tools are still in their early development stages and meaningful efforts are desired to improve the existing tools. A summary of mobile testing challenges and future directions is given (Wang, Y., and Alshboul, Y., 2015).

2.5 Conclusion

The conclusion drawn from the literature reviewed is that while the enterprise private sector is in need of huge financial capital outlay to augment and support the growing requirements of mobile security breaches. The resultant implementations of technology entails that usage of BYOD becomes a requirement rather than a need (William P. Smith, 2017). As the processes and work done in this industry requires high mobility and real-time response to issues to better service the client’s (Aurelie Leclercq-Vandelannoitte, Henri Isaac., 2015). However, to remain relevant the uptake of technology systems has been huge in this enterprise industry. To further highlight the enterprise industry dilemma the mobile device security is lacking due to inherent vulnerabilities created in the earlier versions of the technology specifically 2G technology which mobile manufacturer’s colluded with political and government agencies as there was need to monitor and be able to intercept mobile data. While the BYOD phenomena cannot be ignored, we need a balance between personal and corporate data seriously considering the inherent vulnerabilities that exists on mobile devices by their mobility nature (Aurélie Leclercq - Vandelannoitte, 2015). A gap therefore, still exists in mobile device vulnerabilities which require intervention from the manufacturer ‘s perspective. Overaly the assertion from the reviewed literature shows there is no “one size fit all “solution, the enterprise has to look at the most appropriate, as a self-analysis is of great significance before getting a solution ((Harris, J.G., Ives, B. and Junglas, I., 2011). The application tool will be addressing the monitoring and detection of intrusions on the mobile devices and escalating the detected attacks for mitigation, while terminating the detected process from the enterprise perspective.

Chapter 3: Research Methodology

3.1 Overview

This chapter describes the methodology to be employed to address the objectives of this research which is to identify security weaknesses exploited by cyber attackers and secondly to identify and review the current security approaches used in mobile devices incorporated in the BYOD, which were covered in the Requirements Planning phase of the adopted RAD methodology. The third objective which was to design, develop and test an application that enforces the scanning of connected BYOD devices was addressed under the User Design and Construction phase. In the Cutover phase of RAD, the final objective was to validate the developed information security application tool for effectiveness.

The approach selected is partially theoretical in nature through literature review and the development of a mobile device application tool to validate the proposed solution. The relevant research documents on mobile security vulnerabilities were reviewed to identify the gap to be explored and mitigated while answering the first three objectives of the study. The theoretical research intention was to provide a deeper theoretical understanding of the research area, thus forming the basis for the development and validation of the proposed application development solution.

The developed tool is an android mobile security application that could be installed on any android device running version 6.0 (Marshmallow) or higher operating system. The developed mobile device security application tool will be named NetScan, and will target the mobile devices as they interact with their environment. The implementation on the mobile entails that the tool will always be readily available to the Administrator. The developed tool is a scanner and firewall, the purpose will be to detect connected devices and scan network vulnerabilities/threats, with functionality to block network devices deemed a threat on the network. The tool will be customisable to run new SSH commands as new threats are identified. The enterprise targeted network had a sample of devices connected on the Wi-Fi which was comprised of several network nodes.,

3.2 Software Methodology

Rapid application development (RAD) describes a method of software development which heavily emphasizes rapid prototyping and iterative delivery (Andrew Powell-Morse, 2016). The RAD model is, therefore, a sharp alternative to the typical waterfall development model, which often focuses largely on planning and sequential design practices (Waters, 2014). The rapid application development (RAD) model has become one of the most popular and powerful development methods in use.

The RAD development life cycle methodology was chosen for development of the NetScan tool because the objectives were clearly defined in the requirements planning phase. It's an iterative methodology that breaks the product developed into small increments to minimize the amount of upfront planning and design. This methodology will involve a continuous planning, continuous testing, and continuous integration to ensure the delivery of quality security tool (Jamsheer, 2017). The adaptive approach of Agile responds to changes very well, permitting direct communication to maintain transparency. This method allows to improve the quality of the software being developed by enabling detecting and fixing of defects in a timely manner (Jamsheer, 2017).

The selected methodology RAD uses four distinct steps aimed at assisting with software creation adapting short successive time frames known as iterations. The following key steps on RAD development life cycle methodology includes four basic steps Figure 3.1

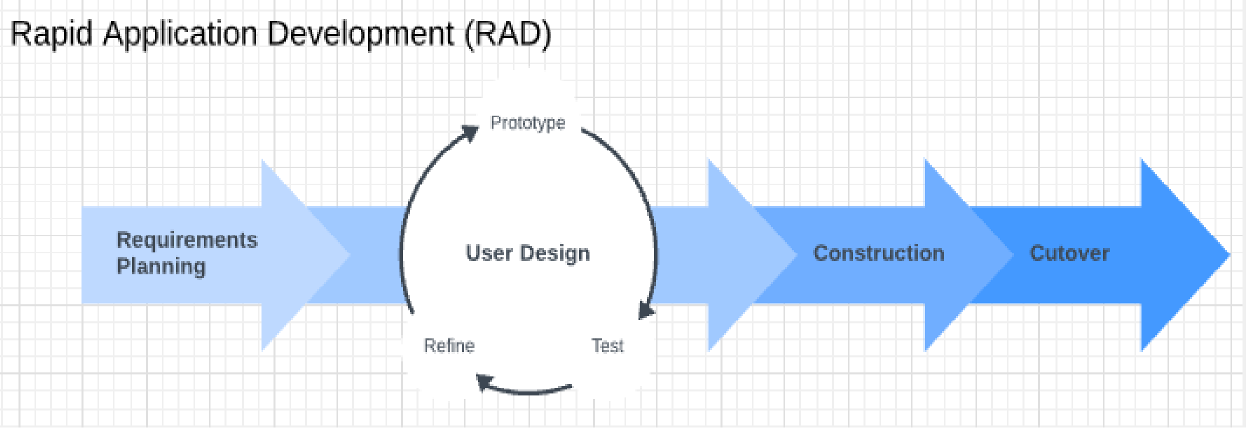


Figure 3.1 Phases Approach to RAD

Source (James Martin, 1991)

The phases in the rapid application development (RAD) model are

i. **Planning Requirements** - during this initial stage designers, developers, and users come to a rough agreement on project scope and application requirements, so that future stages with prototyping can begin.

ii. **User Design -** user feedback is gathered with heavy emphasis on determining the system architecture. This allows initial modeling and prototypes to be created. This step is repeated as often as necessary as the project evolves.

iii. **Rapid Construction** - Once basic user and system design has begun, the construction phase is where most of the actual application coding, testing, and integration takes place. Along with User Design, the Rapid Construction phase is repeated as often as necessary, as new components are required or alterations are made to meet the needs of the project.

iv. **Cutover** - The Final Cutover (or Transition) stage allows the development team time to move components to a live production environment, where any necessary full-scale testing or team training can take place.

3.2 Requirement Analysis

This will be the initial phase that will focus on gathering the requirements for the proposed NetScan tool. This phase gets to identify the requirements based on the analysis of the various gaps identified in the existing solutions during literature review. The requirement analysis for this research were obtained by through a critical analysis of the gaps that had been identified in the literature review, lack of software updates on mobile phones including those lost or stolen which go unreported but these expose enterprises to data breaches. The outcome of this phase will be to define the technical approaches that will be followed to successfully develop the tool. With each successive iterative, will be able to make changes to the requirements of the tool to achieve the specific objectives defined.

The various methods through which we can be able to achieve this will be through;

3.2.1 Literature review

This will involve reading a lot of literature about the development of similar systems and their operations. It will also involve doing research on the internet to read about such systems to be able to understand their working. This would be helpful in a way that:

- It helps in getting new ideas that one may not have thought about.
- It helps preview what security solutions others have used and derive their strengths and weaknesses.
- It helps give more insight on how similar systems had been developed previously and their various components.
- It eases the development process.

3.2.2 Observation and applications review

In this technique of requirement analysis. I will get to install existing tools that provide the solutions, and review their documentation with the intent of understanding their functionality, and discovering the areas where improvement is needed. The gaps identified include the need for enforced update of software on mobile devices and thus ultimately making the scanning process integrated in the operating system, this will eliminate user intervention in execution of the security solution. The prevalence of lost or stolen mobile devices which go unreported is also another identified gap facing the enterprise as this exposes the corporate data. The proposed scanning tool will use the secure socket shell (SSH) protocol in its execution.

3.3 Design

The design phase involves interpreting the requirements that have been identified in the requirement analysis stage. We will get to define the database schemas, and create a visual of the NetScan tool with use of diagrams (entity relationship, use case, sequence and wireframe diagrams). The identification of the appropriate system design to be used in this research was a step-by-step process whose aim was to establish the most appropriate system architecture meeting the identified requirements.

The tools that will be used for the analysis of the data and process will include the following;

i. Entity relationship diagrams – this will be used to show the relationships between the entities during database design and development
ii. Use Case diagrams – diagrams will be used to show the users interaction with the mobile security tool.
iii. Sequence diagrams – This diagram will get to show how object interact with one another and in the order of interaction.
iv. Wireframe diagrams – this is a visual tool that depict where different elements on an interactive page. Diagrams were used to ensure the system is built, showing the features of the application, how they work, usability.

3.4 Development

In this phase, we will start the actual development of the NetScan tool. The main concern here is to come up with small functional units each of which are iterative. The various system modules of the system will be developed. The proposal is to use the following tools

i. Android Studio 3.5 Canary 1 - for the development environment
ii. Java Programing language - for android mobile app development, though this will be open for addition of other languages if need arises.
iii. Android – for user interface (UI) designs

3.5 Testing

In this stage, system acceptance testing will be conducted to test the system functionality of the tool regarding the system requirements and objectives specified. Penetration testing on the tool will be carried out to test the security features of the proposed tool being implemented to ensure the objective of scanning and terminating unwanted malicious process is done successfully has been met. To this end a team of 10 users will be assembled to test the Android application tool. The Android application testing team will involve Android device users of varying ages, and preference in mobile application choices. The aim is to exhaustively ensure results of the scan cover numerous categories of mobile applications network ports.

The test will include installation testing - verifying installation process, updating, and uninstalling of the tool from the mobile devices, basic functionality testing – focusing on whether the application has meet the minimum requirements and usability testing – focusing on whether application has achieved set goals and performed optimally.

3.6 Deployment

To successfully implement this tool, the direct methodology will be used. This will involve installing the tool in the smartphone devices and getting feedback from the mobile users and incorporating the findings into each iterative development of the tool.

3.7 Tool Validation

To ensure accuracy, reliability, consistent performance the application system was validated by the performing the outlined functionality execution and results of each iteration reviewed and measured for accuracy and reliability.

Chapter 4: Systems Design and Architecture

4.1 Overview

This chapter discusses in detail the architecture and design of the Network Scanning Security Application, which satisfies the gathered requirements and those discovered while going through the requirement analysis and design phases. The mobile prototype to be developed will be called NetScan, and will enable the organisation to detect connected devices and scan network threats, with functionality to block network devices deemed a threat to the network.

The NetScan application will only work with wireless router since its installed on a mobile phone. This developed prototype relies on Secure Shell (SSH) a secure protocol for remote logins and specifically a DresDren Wireless RouTer (DDWRT) for its operation. The DDWRT is a firmware for specific network routers that are capable of running embedded Linux software. Some routers come with DDWRT pre-installed while others do not; in that case the Network Administrator is required to install the DDWRT router firmware on the network router. The developed prototype for the network scanning application allow Network Administrator in the organisation to scan for:

a) connected devices regardless of the type (whether it's a printer, laptop, mobile, tablet).
b) assess vulnerabilities on the connected devices.
c) manage firewall running in the network router.

Installing the application on a Local Area Network (LAN) capable android device would make it possible to administer LAN network directly. The mobile application was developed with the main aim of protecting an organization's network from malicious attacks from devices that connect to its network. This chapter will cover in detail the design and architecture of the system. The prototype was developed using RAD methodology.

4.2 System Architecture

The main components of the designed system are the user interface accessible from the front-end using the mobile application called NetScan. The designed system has the following a frontend client interface.

The main components that make up the system are:

i. DDWRT Router

ii. Network Nodes

iii. Net Scan Admin Device (which also falls under network nodes category)

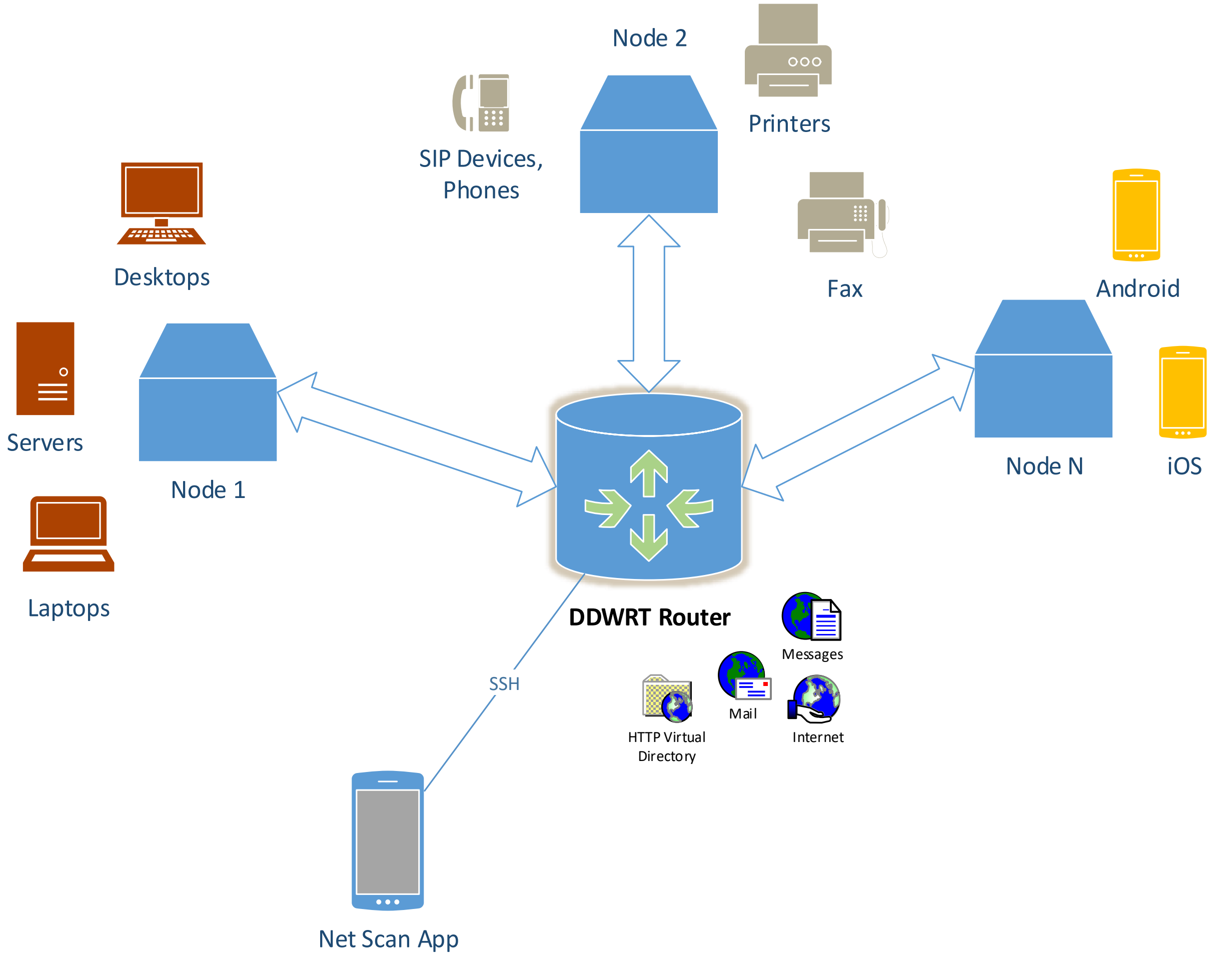


Figure 4. 1 System Architecture

4.2.1 User Interface Design

As the system is a prototype, the mobile application has interfaces that the user will interact with directly. These interfaces are as follows login, Main menu, Network Scan, Traffic Stats and Threat Detected. The design of the interface of the mobile security application was designed to be easy to use for the user while remaining intuitive.

4.2.2. Wireframe

A wireframe illustrates the hierarchical relationships between user interface elements. The user interface comprises:

i. Home Screen/ Log In
ii. New Router / Device Screen
iii. Device / Nodes Screen
iv. Port Scanner
v. Node / Firewall Screen
vi. Firewall Settings

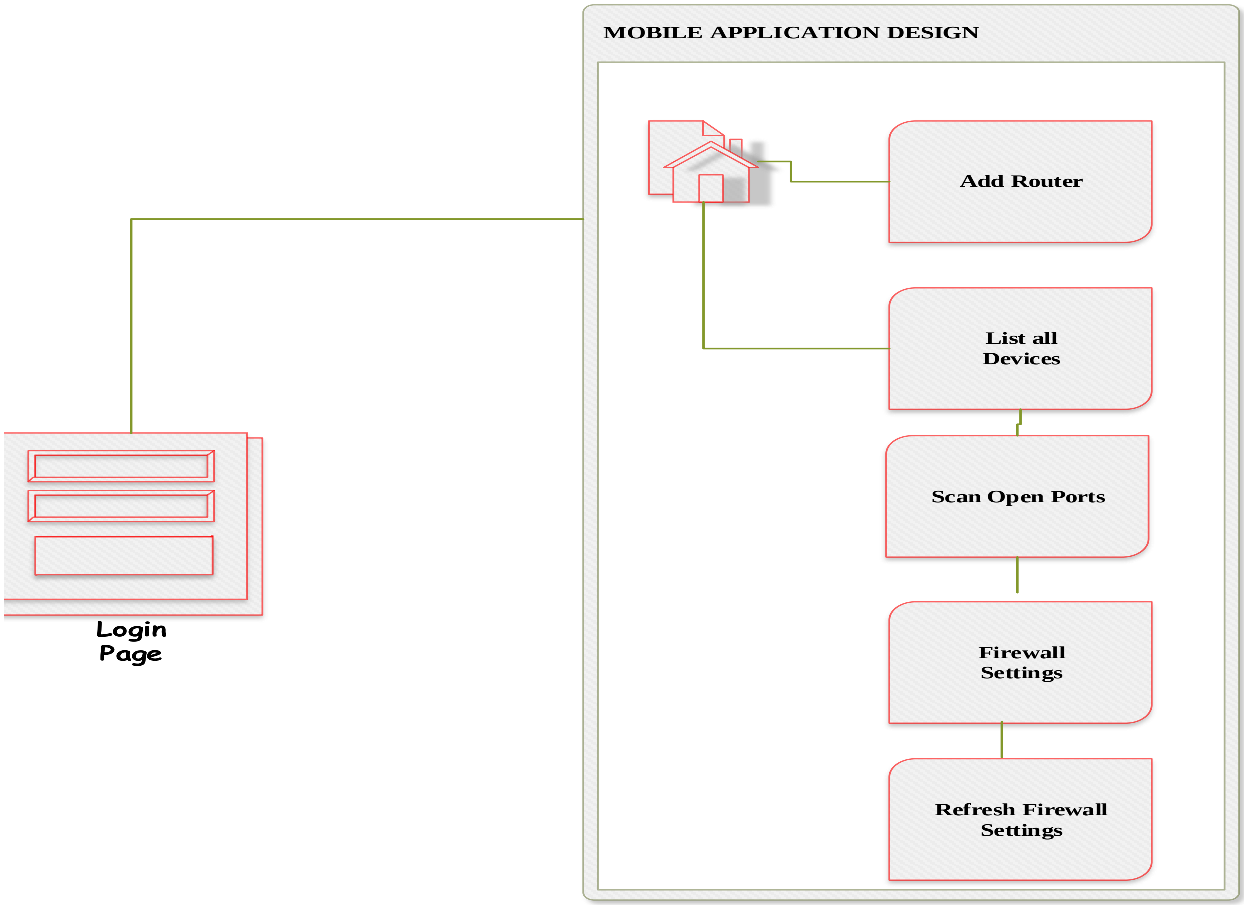


Figure 4. 2 Mobile Interface Design

The following wireframes depict the framework of the mobile application

i. Home Screen

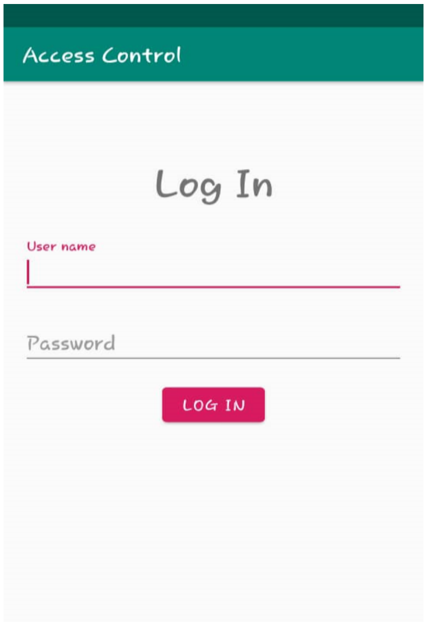
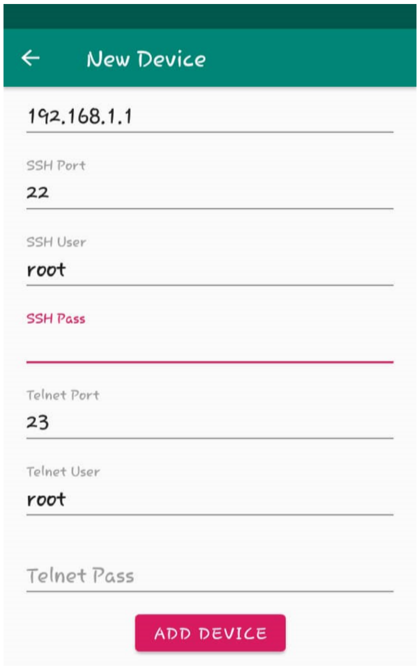


Figure 4. 3 Home Login Screen

ii. New Router / Device Screen



192.168.1.1

SSH Port
22

SSH User
root

SSH Pass

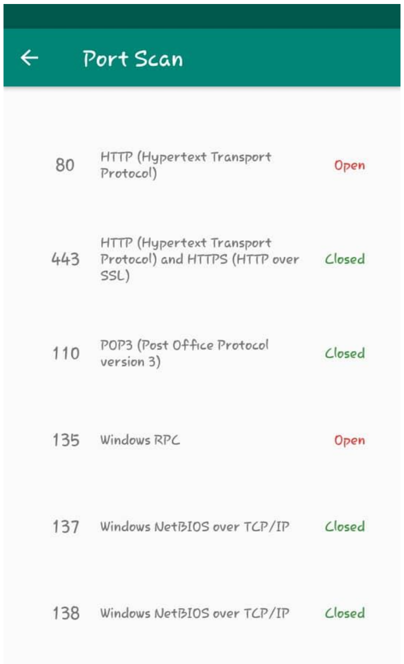
Telnet Port
23

Telnet User
root

Telnet Pass

Figure 4. 4 New Router/Device Screen

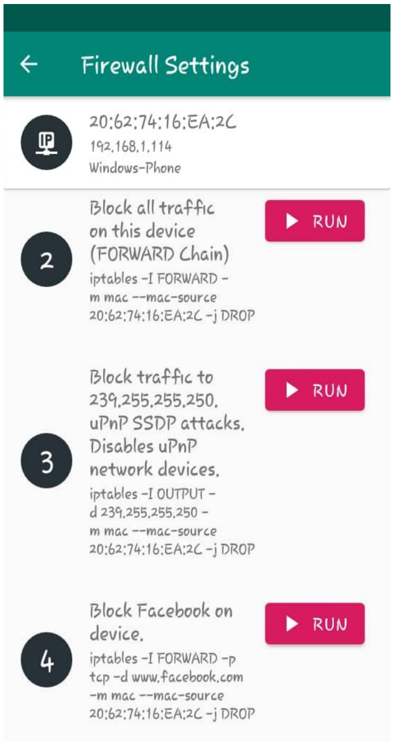
iii. Port Scanner



80	HTTP (Hypertext Transport Protocol)	Open
443	HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)	Closed
110	POP3 (Post Office Protocol version 3)	Closed
135	Windows RPC	Open
137	Windows NetBIOS over TCP/IP	Closed
138	Windows NetBIOS over TCP/IP	Closed

Figure 4. 5 Port Scanner

iv. Node / Firewall Screen



20:62:74:16:EA:2C
192.168.1.114
Windows-Phone

2 Block all traffic on this device (FORWARD Chain)

```
iptables -I FORWARD -m mac --mac-source 20:62:74:16:EA:2C -j DROP
```

3 Block traffic to 239.255.255.250. uPnP SSDP attacks. Disables uPnP network devices.

```
iptables -I OUTPUT -d 239.255.255.250 -m mac --mac-source 20:62:74:16:EA:2C -j DROP
```

4 Block Facebook on device.

```
iptables -I FORWARD -p tcp -d www.facebook.com -m mac --mac-source 20:62:74:16:EA:2C -j DROP
```

Figure 4. 6 Node/Firewall Screen

4.3 System Analysis

System analysis was done to better comprehend existing strengths and weakness of the mobile device security as covered in conclusions of the Literature Review chapter in order to come up with comprehensive requirements to facilitate in the design and subsequently development of prototype mobile application security tool. In most of the reviewed research papers, the different authors concur on that BYOD has brought about a new security headache to the enterprise environment which needs to be managed carefully otherwise data breaches in the enterprise will be commonplace. It was discovered that very few android mobile users regularly update their software to plug security flaws inherent in this software since it is open source and has many flavours available in the market and are being used on a variety of mobile phones. Other users actually turn off security applications that come preinstalled on the mobile devices for various reasons (data costs, space management). Reckless behaviour of the users also poses security threats to the enterprise lost/stolen devices that are not reported to the enterprise information technology department (Flores, D.A., Qazi, F., and Jhumka, A., 2016).

The highlighted limitations pose a significant challenge to the Systems Administrator in the enterprise as they have to secure and guard against potential or perceived security breaches to the enterprise data and network due to the usage of BYOD. This is further compounded by the fact that these mobile devices have capabilities for cloud connection which eliminates the enterprise IT involvement and control they are forced to rely on the good ethical behaviour of the user (Flores, D.A., Qazi, F., and Jhumka, A., 2016). The implementation of the tool consists of various components user interface where users interact with the system.

4.3.1 Functional Specifications

Android design principles were incorporated in making the design intuitive in nature. When launching the application, the user has to provide login details, after which a menu is displayed with various options to select and execute. As a result of system analysis the functional specifications derived includes functionality, usability, compatibility, navigation, supportability and security. The functional specifications identified for the tool are illustrated in Table 4.1.

Category	Functional Specifications
Functionality	Visualisation should be highly interactive
	Extract connected mobile device data from the network scan
	Analyse extracted connected mobile device data and traffic statistics
	Output a detailed visual report
Usability	Ease of use
	Independent on end user mobile platform
	Seamless installation
Compatibility	With Smartphones running Android software version 2.0 or higher
	Application to ran smoothly after installation
	Font and objects to be sized appropriately
Navigation	Accessible to users on demand
	Functions and features to work seamless
Supportability	Fully maintained by hosting entity
	Commercial development version in the future
Security	Secure coding standards followed in the application tool development (OWASP)
	Deploy tamper detection technology
	Test repeatedly

Table 4.1 Functional Specifications

4.4 System Design

In this section the design of the tool will elaborate on the use case diagram, use case diagram descriptions tables, sequence diagram, data flow diagram, activity diagram, class diagram, entity relationship diagram and the wireframes for the implementation of the functional and technical specifications. The proposed tool should be able to scan the network for all connected devices, run threat detection, block compromised devices~~,~~ extract, analyse and block compromised devices. A detailed report should be presented of the analysed data. The mobile application tool is therefore designed to have five main modules add network router, scan network, traffic statistics, detect connected devices, block network devices. A sub module will be incorporated for end user explanation detailing the tool and its functionality.

4.4.1 Technical Specifications

The technical specification explain how the functional specifications will be implemented Table 4.2.

Item	Technical Specifications
Platform	Android based system installed on Smartphone
Frontend Development	Android Studio 3.5 Canary 1, Android Smartphone, Android emulator
Backend Development	Java 8, OpenJDK 8, Gradle, DDWRT Firmware for LinkSys E900
Security	Secure coding standards OWASP

Table 4.2 Technical Specifications

4.4.2 Use Case Diagram

The illustrations of the major interactions that will take place in the developed prototype application between the various actors and the subsystems will be shown by use case diagram. The use case diagram illustrates the major interactions that take place between the various subsystems and actors in the developed prototype

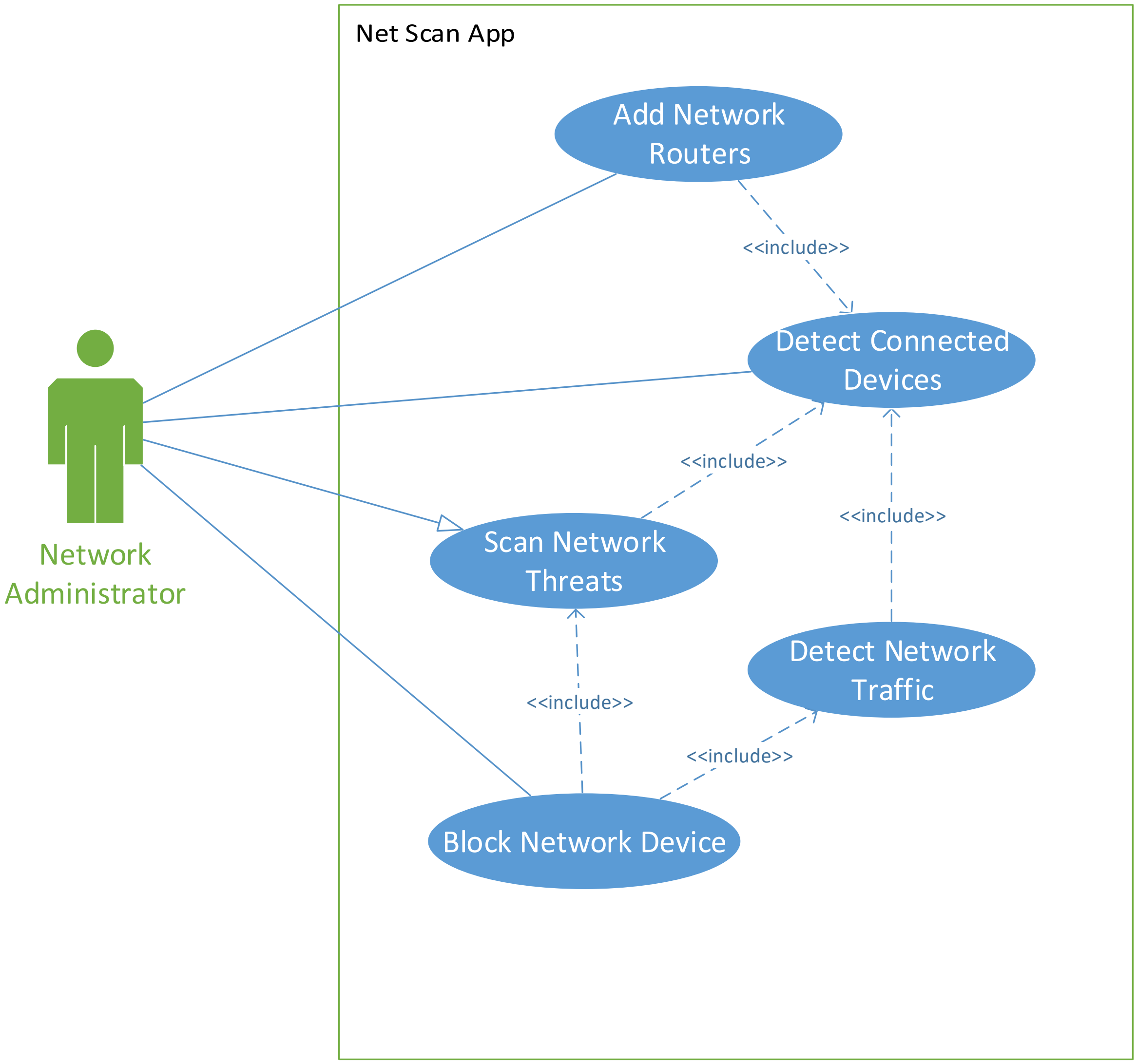


Figure 4. 7 Use Case Diagram

4.4.3 Class Diagram

A class diagram is a static summary of the interacting objects in a system (https://www.uml-diagrams.org) . It describes the attributes and operations of each class and the constraints imposed on the system. The system comprises of 9 main classes as illustrated below. The table below describes each of these classes and how they relate to the connected classes.

	CLASS	DESCRIPTION
1	Device	The system is centered on this one class. This class represents the source from which the router object is instantiated. Comprises attributes for describing the router in terms of: 1. Name, IP Address, and access credentials 2. Connectivity and availability 3. Memory usage 4. Nodes connected to the router (Printers, mobile devices, computers etc.)
2	DeviceStats	This class is a child class of the device class responsible for the connectivity status to the router. It comprises: 1. Availability of SSH connection to router 2. Number of nodes connected
3	MemoryUsage	This class is a child class of the device class and is responsible for the memory usage data of the router. Routers have internal ROM and RAM. It is this class's responsibility to keep track of RAM usage. This class keeps track of the following: 1. Total memory available 2. Currently used up memory 3. Currently available memory 4. Memory being shared by the different processes within the router
4	Host	Host class is a child class of device and is responsible for the publicly broadcasted details / host details as perceived by connected nodes. These details comprise: 1. WiFi SSID 2. WiFi BSSID or MAC address 3. Default router IP address on network
5	Node	Node class is responsible for the managing details relating to nodes connected to the router. The details comprise: 1. Node name, IP address, mac address and interface through which it is connected i.e. LAN or WLAN 2. Ports currently vulnerable on the node
6	Port	Port is a child class with 1-to-N relationship to Device. There will always be at least 1 node connected obviously because the app is always on a node connected to the router. Port class manages: 1. Port number 2. Port description i.e. purpose of port e.g. Port 80 is for HTTP whilst port 443 is for HTTPS 3. Whether port is vulnerable or not
7	IPTableRow	This class is related to node class and manages firewall information linked to the node. This information is about what features of the router and the network the node is permitted to access. By default there is no restriction to internet and network facilities for any new nodes.
8	SSHConnection	SSHConnection class is responsible for the actual connections to the SSH client inside the router. It does two things: 1. Connect and disconnect from SSH 2. Execute commands on SSH over TCP socket
9	SSHClient	SSHClient class manages the commands that can be run over SSH. The commands are defined as operations/methods within the class itself. It also allows for the execution of arbitrary SSH commands.

Table 4.3 Class Diagram

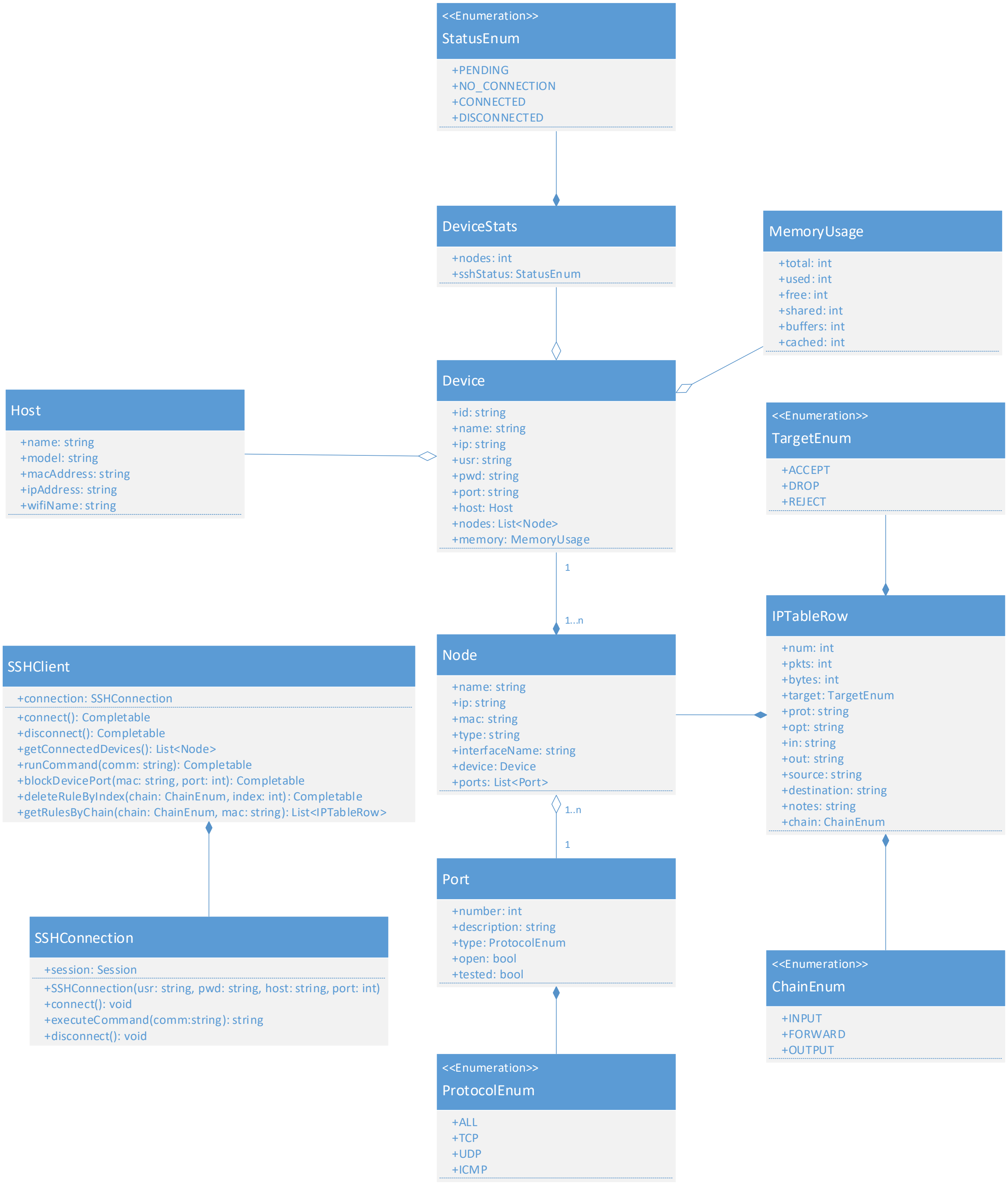


Figure 4. 8 Class Diagram

4.4.4 Sequence Diagram

The sequential flow of information passing through the key entities of the system is shown in the sequence diagram. The developed solution is shown in the Figure 4.9 depicting how a device is connected to the Organisation network. Sequence diagram is a UML illustration of event scenarios (Nikiforova, 2016). It does this by showing a series of parallel lines (lifelines), processes/objects during their lifetime and horizontal arrows to show messages being exchanged between the objects and actors of the system. Figure 4.9 is depicting the processes that will occur from the user, network scan and checking of the background process and blocking the threat.

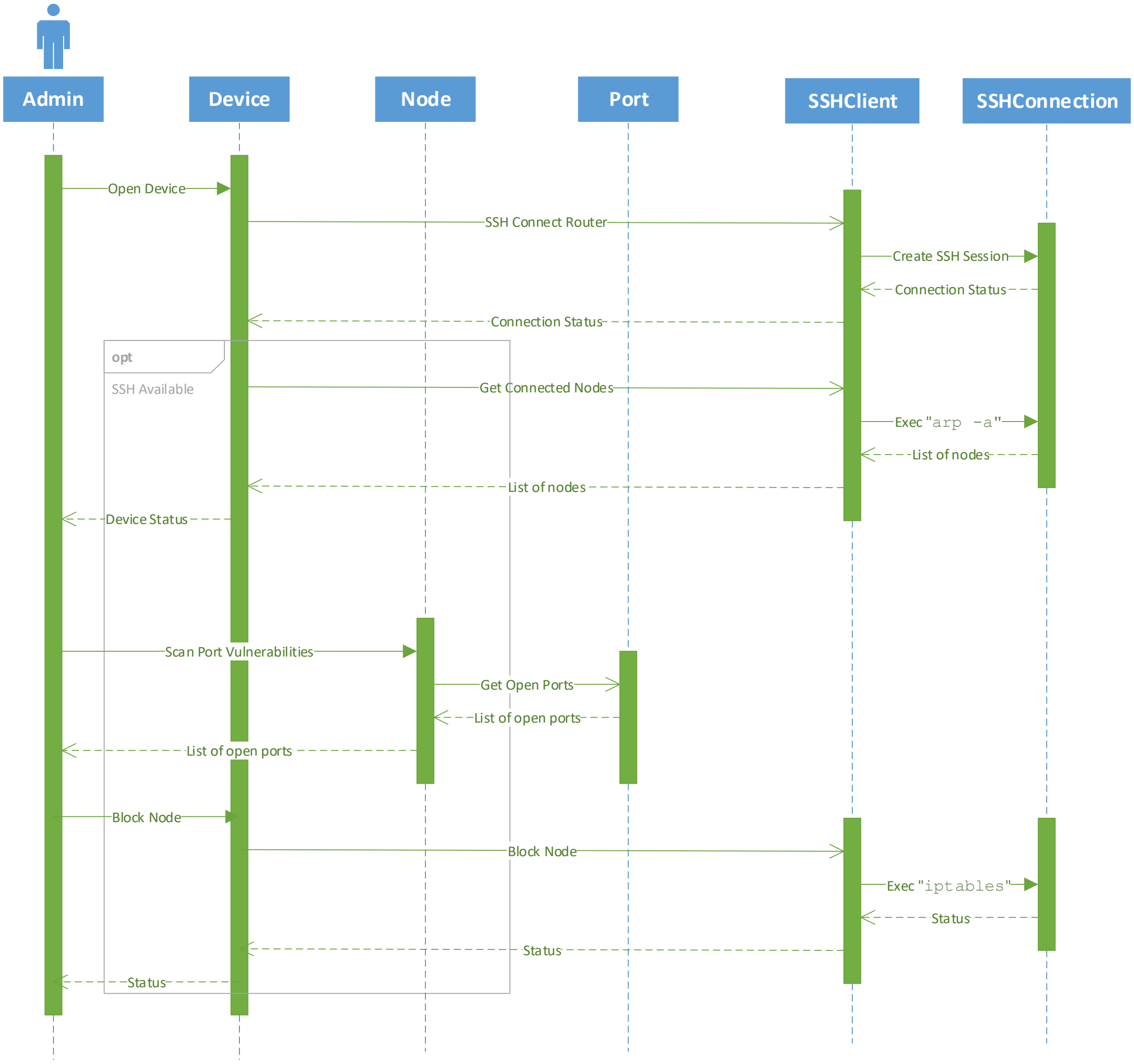


Figure 4. 9 Sequence Diagram

4.4.5 Data Flow Diagram

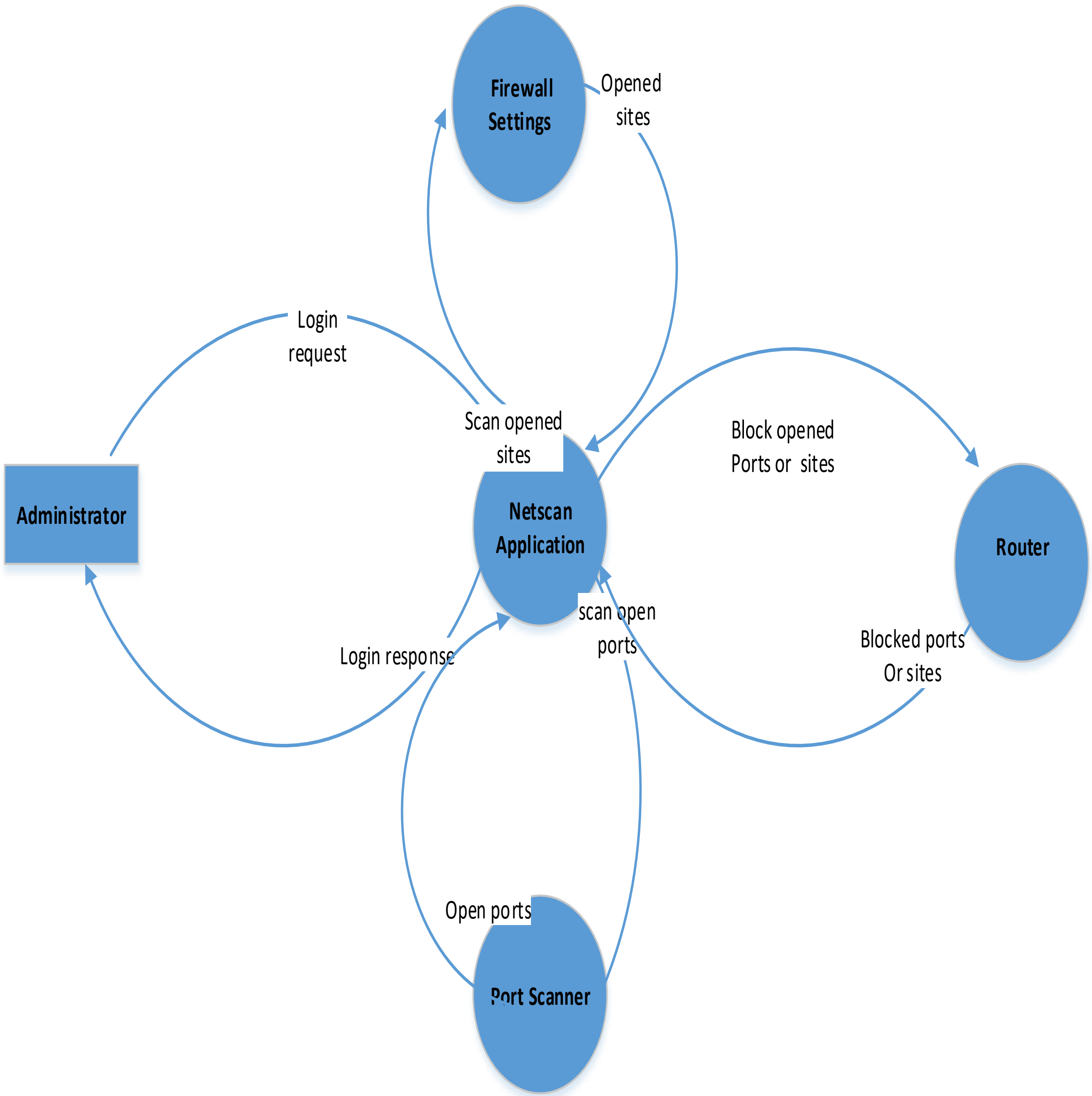


Figure 4. 10 Data Flow Diagram

4.4.6 Activity Diagram

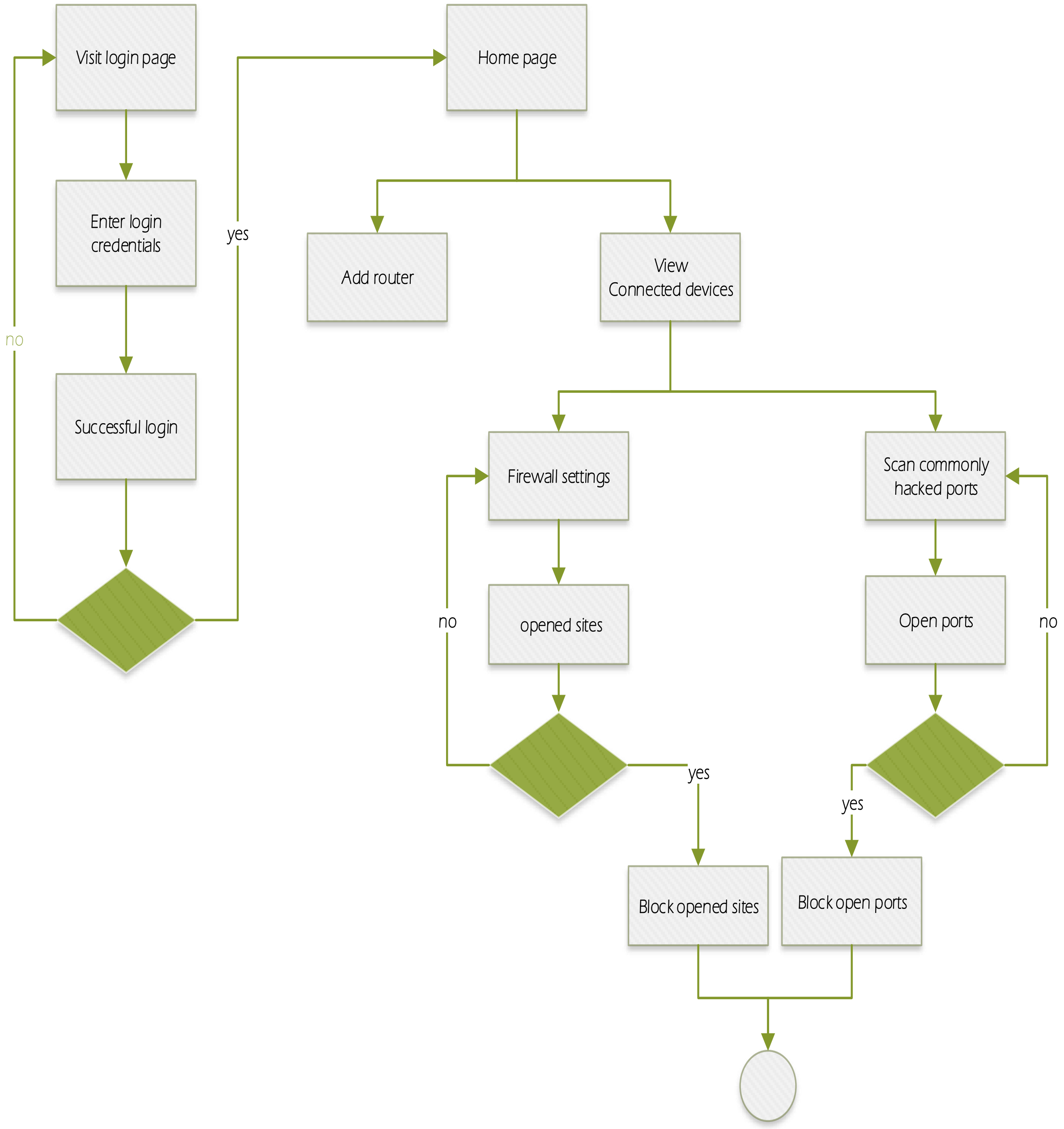


Figure 4. 11 Activity Diagram

4.4.7 Database Design

A database model shows the logical structure of a database, including the relationships and constraints that determine how data can be stored and accessed.

Entity Relationship Diagram

The database uses a number of entities to collect, save and retrieve data. An entity-relationship diagram *(*ERD*)* is a data modelling technique that graphically illustrates an information system's entities and the relationships between those entities. An ERD is a conceptual and representational model of data used to represent the entity framework infrastructure. The Figure 4.12 below illustrates the class relationships:

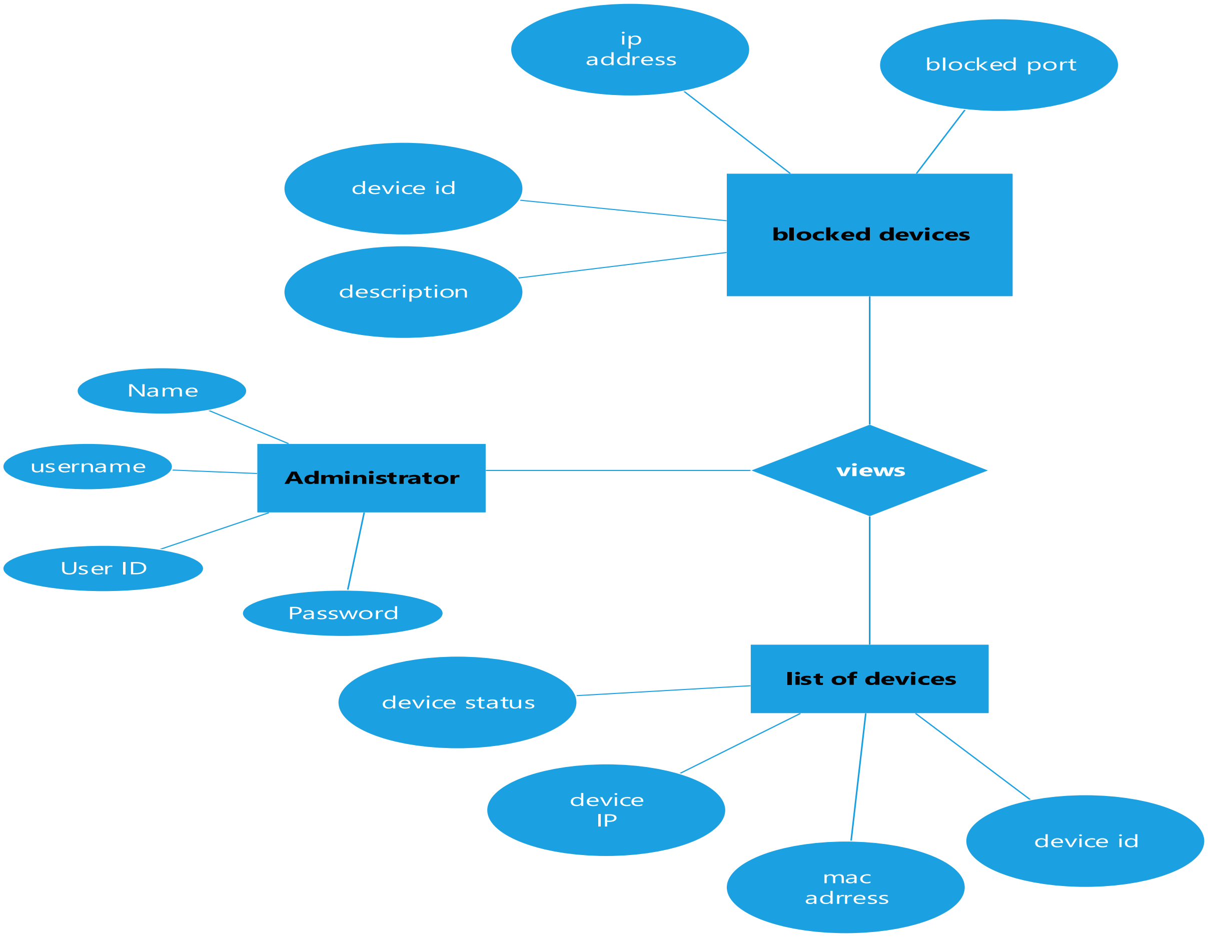


Figure 4. 12 Entity Relationship Diagram

Chapter 5: Implementation, Testing and Validation

5.1 Overview

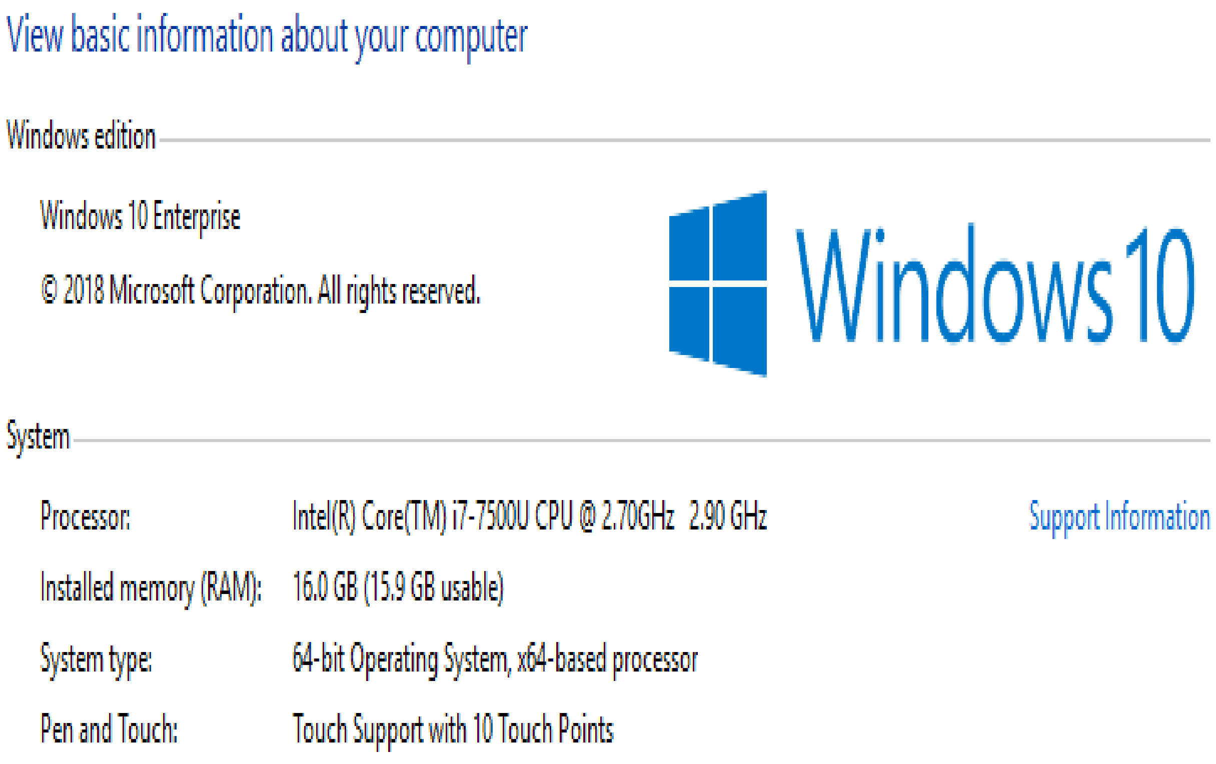
This chapter covers in detail the analysis done to better understand the existing challenges of BYOD specifications and identified requirements. It then aptly describes the implementation, testing and validation of the proposed application system tool and highlights the key features and results obtained. The implementation is carried out following the outlined methodology in Chapter 3 of this research. The testing and validation of the mobile application tool was carried out on a locally deployed version of the tool. The final deliverable is a working code and application.

5.2 Implementation

The system is built on android studio 3.5 canary 1. The developed application will have a graphical user interface. The generated output can be stored for further future analysis and review. The tool is downloaded from a secure application repository as an Android Package Kit (apk) file and installed on the mobile device. The frontend is implemented using the designed wireframes, while the backend is implemented using the use cases, class diagrams, in Java programming technology.

5.2.1 Development Environment

This was developed on a system running Windows 10 Enterprise Edition 64-bit version. The hardware specification's where Intel core i7-7500U, with CPU speed @ 2.70 GHz, 7th Generation, 16 GB Memory.



View basic information about your computer

Windows edition

Windows 10 Enterprise

© 2018 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz	Support Information
Installed memory (RAM):	16.0 GB (15.9 GB usable)	
System type:	64-bit Operating System, x64-based processor	
Pen and Touch:	Touch Support with 10 Touch Points	

Figure 5.1 Development Environment Hardware Specifications

The android studio ide-181.5-windows was used to install Android Studio 3.5 Canary 1 (2018). Android Studio is an integrated development environment (IDE) for Android application development a high performance software written in Java, Kotlin and C++ (Haslam, 2013). It is based on the Jetbrain's IntelliJ IDEA, a Java based integrated development environment for software which incorporates its code editing and developer tools.

5.2.2 Mobile Application Development Tools

i. Android Studio 3.5 Canary 1

ii. Has a built-in preview update mechanism. The IDE connects regularly to the update server and will present a popup at start-up when a new version is available. Android Studio categorizes updates using "channels", Canary, Dev, Beta and stable. For this development we will use the Canary channel.

iii. OpenJDK-10.0.2 windows x64

iv. OpenJDK (Open Java Development Kit) is a free and open-source implementation of the Java Platform, Standard Edition (Java SE). It is the result of an effort Sun Microsystems began in 2006. OpenJDK is the official reference implementation of Java SE.

v. Java 8

vi. This is a revolutionary release of the world’s number 1 development platform. It includes a huge upgrade to the Java programming model and a coordinated evolution of the JVM, Java language, and libraries. Java 8 includes features for productivity, ease of use, improved polyglot programming, security and improved performance. Welcome to the latest iteration of the largest, open, standards-based, community-driven platform.

vii. Gradle

viii. This comes integrated in the Android Studio and is used as the foundation for build system, which can be ran from the Android Studio menu and from command line. Gradle has flexibility

ix. DDWRT Firmware for Routers45

x. Is a Linux-based firmware project developed to enhance the performance and features of wireless Internet routers. This open-source firmware upgrade is developed for specific router models and used as a replacement for the inconsistent stock firmware.

5.3 Testing

5.3.1 Mobile Device and Application Testing

With the application installed on the mobile device and executed. The network scan was performed and the initial scan was able to pick all the connected devices on the router network. The test run detected and displayed 5 connected devices successfully.

5.3.2 System Testing

This is conducted to evaluate the system’s compliance with specified requirements. With the developed mobile application, system testing was conducted using randomly selected participants in the enterprise for the purpose of fully testing the mobile components of the system. The system testing was done with selected users in sessions where they fully tested the assigned components of the system security application tool.

5.3.3 Usability Testing

The user acceptance testing was done to rate, how difficult they perceived the mobile security application tool, from installation, launching the application and performing various available tasks in the menu (network scans, ports detection, firewall rules, device blocking). The various tasks on the NetScan application were tested and worked well.

5.3.4 Compatibility Testing

The developed NetScan application executes on smartphones running Android operating system version 6.0 or higher operating system. The test was done and the application executed successfully on a Samsung Duos and Windows smartphone.

5.3.5 Functionality Testing

The testers involved reported are 100% success rate in scanning their mobile devices after installation and launching the application. The initial network scan was able to list all the detected connected devices. On selecting the network scan option from the main menu, a scan is performed to check for connected devices on the network. The resultant data is displayed for the user to see on the screen then the button to scan for threats can be selected as shown below. The detected compromised devices where successfully blocked with a 100% success rate.

5.3.6 User Testing

This technique is used to evaluate a product, feature or prototype with real users. The tests were carried out with a selected group of ten users. The group included professionals from the Information Technology field with at least bachelor’s degree. The test done included accessibility test, checking the level of accessibility of the system to the user, mobile compatibility and router compatibility**.** The target Administrator’s group successful installed and executed the NetScan application and where satisfied with its functionality to scan, detect and block devices from the mobile device.

5.4 System Validation

For the validation of the system, an evaluation was carried out using an experienced expert in the field with certification CEH – (Certified Ethical Hacker). This gave the developer assurance that the findings will be acceptable. These actions were planned and carried out throughout he life cycle of the developed system

5.4.1 Tool Validation

The application tool was validated for ease to use user interface, to ensure that text was readable for all users. The app was checked for working in all the required mandatory fields. The application was also validated it was found to be working according to the requirements. Validated that the application performs according to requirements in all the versions of the Mobile 2G, 3G and 4G.

Chapter 6: Discussions

6.1 Overview

This chapter discuss the findings of this research focusing on the set objectives, research questions and scope. With explanations on the key areas covered. The main objective of the research was to review the existing security applications available to protect BYOD in their usage in the enterprise setup and develop a scanning application tool to scan for and stop malicious activities running on the user's mobile device without their knowledge. The literature review highlighted that BYOD is a phenomenon that will not go away and enterprises have to actively participate to protect their network environments.

6.2 Discussions of Findings

From the set objectives in Chapter 1 of this research, the identified key objectives where to identify the mobile security weaknesses exploited by cyber attackers, identify and review current mobile security approaches and design, develop and test mobile based information security application tool. From the literature review the research looked at the various mobile security weaknesses, smartphones now contain private and enterprise information which has become a rich attack vector for hackers, the fact that android platform is open source makes it susceptible to attacks. The software imperfections found in the android platform expose the mobile device to attacks, these are a result of blunders or lack of caution by programmers in the software development. In the operating environment there has been high theft or loss of these mobile devices creating a major security headache for IT Administrators. The growing incidences of information leakage, breaches in access control and user management has been rife and this has been further compounded by the usage of Wi-Fi both in Enterprise environment and public space which further exposes the mobile devices to attacks and including the reckless/naive behaviour of employees.

The research focused on the protection of the BYOD in the enterprise environment as they are used to carry out work activities while also using the private data on the same device. Therefore, due to some of the highlighted mobile security weaknesses it become imperative to develop a mobile security application which will assist in the network scan, threat scanning on the connected mobile devices as they interacted with the enterprise environment. Threat techniques identified include execution of malicious code attached to seemingly genuine software or connection session on the enterprise network. Unauthorised connection to the enterprise through wireless connection (Wi-Fi, Bluetooth). The threat detection module would mitigate these discussed attach vectors. The second objectives of the research focused on identifying and reviewing mobile security approaches that are in use on mobile devices. This research was able to identify the various methods been implemented to mitigate the inherent security flaws found in mobile devices and the vulnerabilities they bring as they get connected to the enterprise environment. The lack of security awareness of smartphone users as they rely on service providers to manage their security as they enjoy the usage of enterprise resources or free Wi-Fi access as the move around or travel. The use of a wearable token that constantly attests the user's presence, is one proposed approach revealed by literature review (Rakars, 2018). While others proposed remote mobile screen which provides a trusted virtual machine which connects the BYOD to the enterprise. In the research a cloud based framework for mobile malware detection is also proposed as an approach to address mobile security. The final objective of this research was to test the functionality of the developed mobile application tool. This was extensively covered in Chapter 5, with various tests done on the application tool. The tool proved to be ease to use and reduced malicious code from running on connected device on the enterprise network.

After launching the NetScan application, the following was successfully executed the scanning for devices on the connected and the application picked five connected devices android mobile phones, tablets and laptops. The execution of the firewall rules revealed that they were closed and open port on the devices. The ports displayed in the application are the commonly hacked ports which exposes the organisation to network vulnerabilities. The application successfully closed open ports, which the System Administrator selected, they were 100% success rate in the execution. The application also succeeded in blocking web sites i.e. Facebook from being accessed from the targeted device. From the test done on the selected 5 devices, the application performed according to the design with a good accuracy and consistent success rate. This tool assists the Administrator to configure devices which connect to the cooperate network to be secure and minimise, malicious attacks. This tool is easily customisable to ran new SSH commands as new threats are identified. For the test the targeted network was an organisation Wi-Fi which comprised of several network nodes. The application was developed for mobile to give the Administrator the flexibility to operate with high mobility, as the tool would be readily available.

6.3 Testing and Validation

The testing and validation of the proof of concept implementation revealed a functional prototype that was able to scan the network of connected devices, execute a threat detection scan, block compromised mobile devices detected, scan and display traffic statistics, analyse and show devices utilising more bandwidth beyond the set threshold and terminate and block the device from the network. The test also revealed that the tool can scan and analyse the connected devices on the network for vulnerabilities. The quality assurance carried out on the functionality, usability, compatibility, navigation, supportability and security revealed that the mobile application tool executes according to the functional requirements and specifications. The tool validation included checks for specifications, use cases, class diagrams, wireframes, source code review and functional completeness. Examination of the specification was done and discovered to in line with the end user requirements and the implementation of the specifications would achieve what the tool was designed to perform. Use cases, class diagrams and wireframes were scrutinised and revealed to be in sync and accurate according to the system specifications. The examination of the code review did not pick an errors or anything wrong in the source code. Validation for accuracy of results was carried out and the application tool extracts and analyses revealed accurate data and comprehensive systems reports.

Chapter 7: Conclusion, Recommendations and Future Work

7.1 Conclusion

This research focused on developing a mobile application tool that would scan the router (DDWRT) for connected mobile devices while checking for malicious activity on the mobile device. The developed tool was able to execute the intended duties successfully. Success was apparent in the ability to scan a selected device for malicious activity, that might have been deployed and the user was not aware of its existence. The tool was able to scan the user's mobile device for suspicious application activity, terminate the offending activity and block the activity. Additionally, the tool was linked to an antivirus software to compliment the scanning and enhance the security on the mobile device.

7.2 Recommendations

The findings of the research where a noticeable success rate securing of mobile device users by detecting and stopping malicious attacks, thus preventing theft of data. The tool was able to detect all the connected devices on the Wi-Fi network. It also succeeded in displaying the connected devices and the detected closed and open ports. The firewall refresh rules worked correctly. While the scanning and detection of the malicious activity was successfully executed and the disruptive activity terminated. The blocking of the open ports and selected open sites was also observed to have been done successfully. The tool managed to address the intended functionality scan, detect and block devices and ports. The research felt that more features and functionality could be added to the tool to improve efficiency and high detection rate with the following recommendations:

1) Further develop the alert functionality for execution and termination in realtime.
2) System Administrator's should have an interface to continually update and review incidences.
3) As this research focused on the android platform, there is need extend this mobile application to cover other operating systems including but not limited to Blackberry and iPhone IOS.
4) Analysis can be done using machine learning models that have been trained to classify network traffic
5) There is need to upload the mobile application to a reputable application store to boost confidence of users of the solution.

7.3 Future Work

Future improvements on the mobile device application security tool will include making it mandatory to download and install for anyone to use the enterprise information technology resources. Further work can be done from the user’s perspective on how to secure and protect private information as they interact with enterprise network.

References

Abubakar Garba Bello, D. M. (2017). "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments". *Information & Computer Security, Vol. 25 Issue: 4,*, pp.475-492, https://doi.org/10.1108/ICS-03-2016-0025.

Aenugu N.R., Butakov S., Zavarsky P., Aghili S. (2018). Security Perspective in Comparative Study of Platform-Based and Platform-Less BYOD Systems. *In: Kim K., Kim H., Baek N. (eds) IT Convergence and Security 2017*, Lecture Notes in Electrical Engineering, vol 450. Springer, Singapore.

Ali, S., Qureshi, M.N., and Abbasi, A.G. (2015). "Analysis of BYOD security frameworks,". *2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 2015,*, (pp. pp. 56-61.doi: 10.1109/CIACS.2015.7395567).

Aurelie Leclercq - Vandelannoitte. (2015). "Leaving employees to their own devices: new practices in the workplace". *Journal of Business Strategy, Vol. 36 Issue: 5*, pp.18-24, https://doi.org/10.1108/JBS-08-2014-0100.

Aurélie Leclercq - Vandelannoitte. (2015). "Managing BYOD: how do organizations incorporate user-driven IT innovations?". *Information Technology & People, Vol. 28 Issue: 1,*, pp.2- 33, https://doi.org/10.1108/ITP-11-2012-0129. Retrieved from https://doi.org/10.1108/ITP-11-2012-0129

Aurelie Leclercq-Vandelannoitte, Henri Isaac. (2015). “Managing BYOD: how do organisations incorporate user-driven IT innovations?”,. *Information Technology & People, Vol. 28 Issue: 1*, pp.2-33, https://doi.org/10.1108/ITP-11-2012-0129.

Balboni, F., Berman, S.J, Korsten, P. J. (2015). “The individual enterprise: all for one and one for all”. *Strategy & Leadership Leadership, Vol.43 Issue:4*, pp.3-10, https://doi.org/10.1108/SL-05-2015-0034.

Baskerville, R. (2011). “Individual information systems as a research arena”. *European Journal of Information Systems, Vol.20 No.3*, pp.251-254.

Burnham, J. D. (2014). *The Need for BYOD Security: “The Rise and Risk of BYOD”*. Retrieved from https://www.druva.com/blog/the-rise-and-risk-of-byod/

Cooper, W.T., and Thangamuthu, K. (2014). *System and Method for predicting future locations and of mobile communication devices using connection related data of a mobile access network.*

Craigen, D., Diakun-Thibault, N., & Purse, R. . (2014). *Defining Cybersecurity.* Retrieved from Technology Innovation Management Review, 4(10): 13-21.: http://timreview.ca/article/835 CSO. Retrieved 20 February 2017

Crowston, K., Fitzgerald, B., Gloor, P., Schultze, U., & and Yoo, Y. (2010). "SHIFTING BOUNDARIES: HOW SHOULD IS RESEARCHERS STUDY NON-ORGANIZATIONAL USES OF ICT?" (2010). *ICIS 2010 Proceedings. 119.*, https://aisel.aisnet.org/icis2010_submissions/119.

Denys A. Flores, F. Q. (2016). "Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information",. *Trustcom/BigDataSE/ISPA 2016 IEEE*, pp. 1008-1015, 2016, ISSN 2324-9013.

Donaldson S.E., Siegel S.G., Williams C.K., Aslam A. . (2015). *Enterprise Cybersecurity for Mobile and BYOD. In: Enterprise Cybersecurity.* Apress, Berkeley, CA.

Downer, K., and Bhattacharya, M. (2015). "BYOD Security: A New Business Challenge,". *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, 2015,*, pp. 1128-1133.doi: 10.1109/SmartCity.2015.221.

Fani, N., von Solms, R., and Gerber, M. (2016). "A framework towards governing “Bring Your Own Device in SMMEs”. *2016 Information Security for South Africa (ISSA), Johannesburg, 2016,*, pp. 1-8. doi: 10.1109/ISSA.2016.7802922.

Flores, D.A., Qazi, F., and Jhumka, A. (2016). “Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information”,. *Trustcom/BigDataSE/ISPA 2016 IEEE,*, pp. 1008-1015, 2016, ISSN 2324-9013.

Garba, A.B., Armarego, J., Murray, D. (2015). “Bring Your Own Device Organisational Information Security and Privacy”.

Gens, F., Levitas, D. and Segal, R. (2011). Consumerisation of IT Study: Closing the Consumerisation Gap,. IDC, Framingham, MA.

Ghosh, A., Gajar, P.K., and Rai, S. (2013). Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies.

Guri, M., Kedma, G., Kachlon, A., and Elovici, Y. (2014). "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies,". *2014 9th International Conference on Malicious and Unwanted Software:* (pp. pp. 58-67. doi: 10.1109/MALWARE.2014.6999418). The Americas (MALWARE), Fajardo, PR, 2014,.

Harris, J.G., Ives, B. and Junglas, I. (2011). The Genie is Out of the Bottle: Managing the Infiltration of Consumer IT into the Workforce. *Accenture Institute for High Performance,*, www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Managing-the-inflitration-of-Consumer-IT-into-the-workforce.pdf (accessed 25 February 2018).

Harris, Jeanne & Ives, Blake & Junglas, Iris. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive.* , 11. 99-112. .

Harris, M, A, Patten, K., and Regan, E. (2013). *The Need for BYOD Mobile Device Security Awareness and Training.*

Ismail, N. (2017). *Mobile in the enterprise - why traditional security tactics such as firewalls, IPS and anti-malwares are no longer enough.*

Jamsheer, K. (2017, March 3). *12 Best Software Methodologies with Pros and Cons. .* Retrieved from Best Software Methodologies with Pros and Cons. : https://acodez.in/12-best-software-development-methodologies-pros-cons/, Retrieved 27 February 2018.

Josang A, Miralabe L, Dallot L. (2016). *“Vulnerability by Design in Mobile Network Security”,.*

Karison, A.K, Bederson, B.B & Contreras-Vidal,J.L. (2008). *Handbook on User Interface Design and Evaluation for Mobile Technology.*

Kerner S.M., (. (2019, March 30). *BYOD Security: Understanding Bring Your Own Device Security Risks.* Retrieved from esecurityplanet.com: https://www.esecurityplanet.com/mobile-security/byod-bring-your-own-device.html,

Kim, T. (2016). A Study on the Detection of Abnormal Behaviour and Vulnerability Analysis in BYOD. *Internet of Things. IoT Infrastructures. IoT360 2015. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 170.* (p. In: Mandler B. et al. (eds)). Springer, Cham.

Logicals. (2018).

Mansfield-Devine, S. (. (2018, February 27). *“Interview: BYOD and the enterprise network”,*. Retrieved from doi.org: https://doi.org/10.1016/S1361-3723(12)70031-3.

Meske C., Stieglitz S., Brockmann T., Ross B. (2017). Impact of Mobile IT Consumerization on Organizations – An Empirical Study on the Adoption of BYOD Practices. *In: Nah FH., Tan CH. (eds) HCI in Business,*, Government and Organizations. Supporting Business. HCIBGO 2017. Lecture Notes in Computer Science, vol 10294. Springer, Cham.

Moss, C. (. (2018, February 27). *BYOD Part 1: Enterprise Strategy and Policy.* Retrieved from ravepubs,com: http://www.ravepubs.com/byod-part-1-enterprise-strategy-policy/.

Murdoch, M., Harris, J. and Devore, G. (2010). *Can Enterprise IT Survive the Meteor of Consumer technology?*

Musarurwa, Alfred & Flowerday, Stephen & Cilliers, Liezel. (2017). Individual traits that determine the Bring Your Own Device information security culture: A case study of the banking sector in Zimbabwe. .

Ocano, S.G., Ramamurthy, B., Wang, Y. (2015). “Remote mobile screen (RMS): An approach for secure BYOD environments,". *2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, 2015,*, pp. 52-56.doi: 10.1109/ICCNC.2015.7069314.

Ogie, R. (2016). "Bring Your Own Device: An overview of risk assessment,". *in IEEE Consumer Electronics Magazine, vol. 5, no. 1,*, pp. 114-119, Jan. 2016.doi: 10.1109/MCE.2015.2484858.

Oktavia, T., Tjong, Y., Prabowo, H., and Meyliana. (2016). "Security and privacy challenge in Bring Your Own Device environment: A Systematic Literature Review,". *2016 International Conference on Information Management and Technology (ICIMTech), Bandung, 2016,*, pp. 194-199.audiodoi: 10.1109/ICIMTech.2016.7930328.

Ortbach, K., Bode, M. and Niehaves, B. (2013). “What influences technological individualisation? – an analysis of antecedents to IT consumerisation behaviour”,. *Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago.*

Penning, N., Hoffman, M., Nikolai, J., and Wang, Y. (2014). "Mobile malware security challenges and cloud-based detection,". *2014 International Conference on Collaboration Technologies and Systems (CTS),* (pp. pp. 181-188.). Minneapolis, MN, 2014,: doi: 10.1109/CTS.2014.6867562.

Rakars, A. (2018, May 31). "How Wearables Influence the Future of Mobile Application Development?

Rathnasekara, C., Athukorala, T., Dikwellage, L. and Wickramasuriya, U. (2017). Securing Corporate Data in Mobile Devices in a COPE Environment.

Rouse, M. (2013). *"What is private sector? - Definition from WhatIs.com". Retrieved July 16, 2017.* Retrieved from Tech Target.

Schwartz, P., and Solove, D.J. (2014). *The PII Problem: Privacy and a New Concept of Personally Identifiable Information.*

Sen, J. (2012). Ubiquitous Computing: Applications, Challenges and Future Trends. *Book Chapter in "Embedded Systems and Wireless Technology: Theory and Practical Application",Editors: Raul Aquino Santos and Arthur Edwards Block* (pp. Chapter No. 1, Pp. 1-40,). University of Colia, Mexico: CRC Press, Taylor & Francis Group, USA.

Spring T. (2017, April 25). *Hard Target: Fileless Malware*. Retrieved from threatpost: https://threatpost.com/hard-target-fileless-malware/125054/

Statista. (2019). *Statista*. Retrieved from Statista.com: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

Totten, J., & Hammock, M. (2014). Personal Electronic Devices in the Workplace: Balancing Interests in a BYOD World. *ABA Journal of Labor & Employment Law, 30(1),*, 27-45,.

Tse, D., Wang, L., and Li, Y. (2016). *Mobility Management For Enterprises In BYOD Deployment.*

Wang, Y., and Alshboul, Y. (2015). "Mobile security testing approaches and challenges,". *2015 First Conference on Mobile and Secure Services (MOBISECSERV), Gainesville, FL, 2015,*, pp.1-5.doi: 10.1109/MOBISECSERV.2015.7072880.

Wang, Y., Streff, K., and Raman, S. (2012). "Smartphone Security Challenges,". *in Computer, vol. 45, no. 12,*, pp. 52-58, Dec. 2012.doi: 10.1109/MC.2012.288.

Wang, Y., Wei, J., and Vangury, K. (2014). “Bring your own device security issues and challenges,". *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2014,* (pp. pp. 80-85. doi:10.1109/CCNC.2014.6866552). IEEE.

Waters, K. (2014). *Agile Methodologies.* Retrieved from Agile Methodologies.: http://www.allaboutagile.com/agile-methodologies,

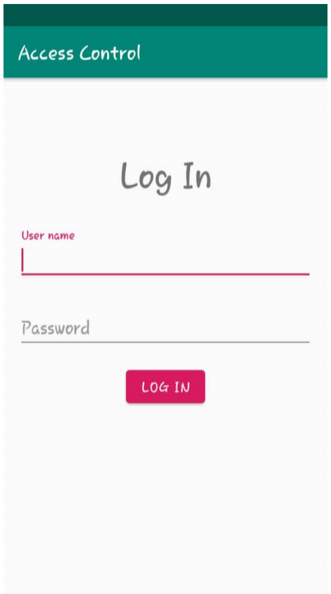
William P. Smith. (2017). "“Can we borrow your phone? Employee privacy in the BYOD era”",. *Journal of Information, Communication and Ethics in Society, Vol. 15 Issue: 4,*, pp.397-411, https://doi.org/10.1108/JICES-09-2015-0027 .

Zachary D.B. (2014, October 7). *Gadgets and Tech News*. Retrieved from independent.co.uk: https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

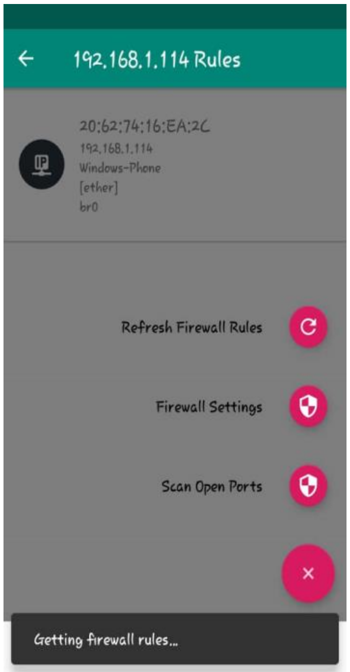
Zimperium. (2017). *Mobile Threat Defense*. Retrieved from The Leader in Mobile Security & Threat Defense: https://www.zimperium.com/

Appendix A: Mobile Security Application Tool Screenshots

Appendix A.1 Mobile Application Login Screen



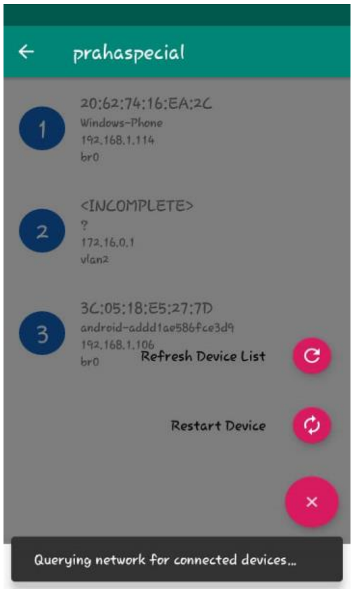
Appendix A.2 Mobile Application Main Menu



20:62:74:16:EA:2C
192.168.1.114
Windows-Phone
[ether]
br0

Getting firewall rules...

Appendix A.3 Mobile Application Network Scan Results



prahaspecial

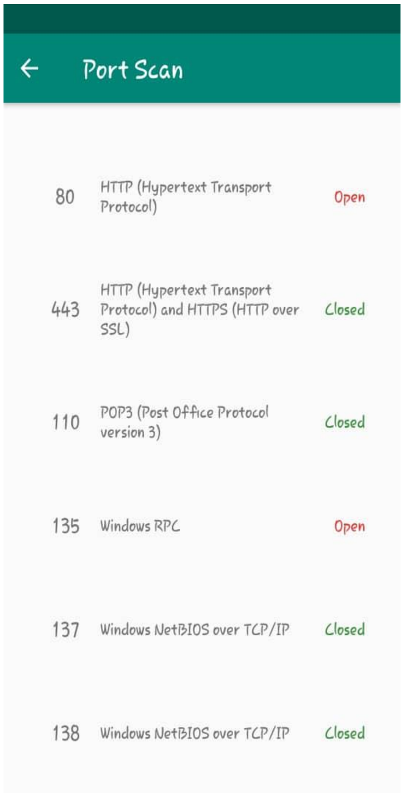
1 20:62:74:16:EA:2C
Windows-Phone
192.168.1.114
br0

2 <INCOMPLETE>
?
172.16.0.1
vlan2

3 3C:05:18:E5:27:7D
android-addd1ae586fce3d9
192.168.1.106
br0

Querying network for connected devices...

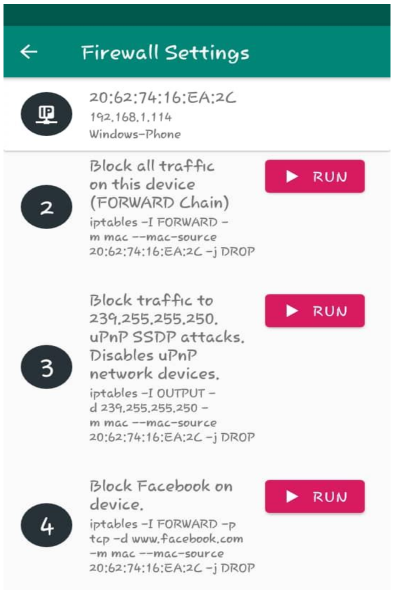
Appendix A.4 Mobile Application Port Threat Scan Results



Port Scan

80	HTTP (Hypertext Transport Protocol)	Open
443	HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)	Closed
110	POP3 (Post Office Protocol version 3)	Closed
135	Windows RPC	Open
137	Windows NetBIOS over TCP/IP	Closed
138	Windows NetBIOS over TCP/IP	Closed

Appendix A.5 Mobile Application Firewall Settings Scan Results



20:62:74:16:EA:2C
192.168.1.114
Windows-Phone

2 Block all traffic on this device (FORWARD Chain)

```
iptables -I FORWARD -
m mac --mac-source
20:62:74:16:EA:2C -j DROP
```

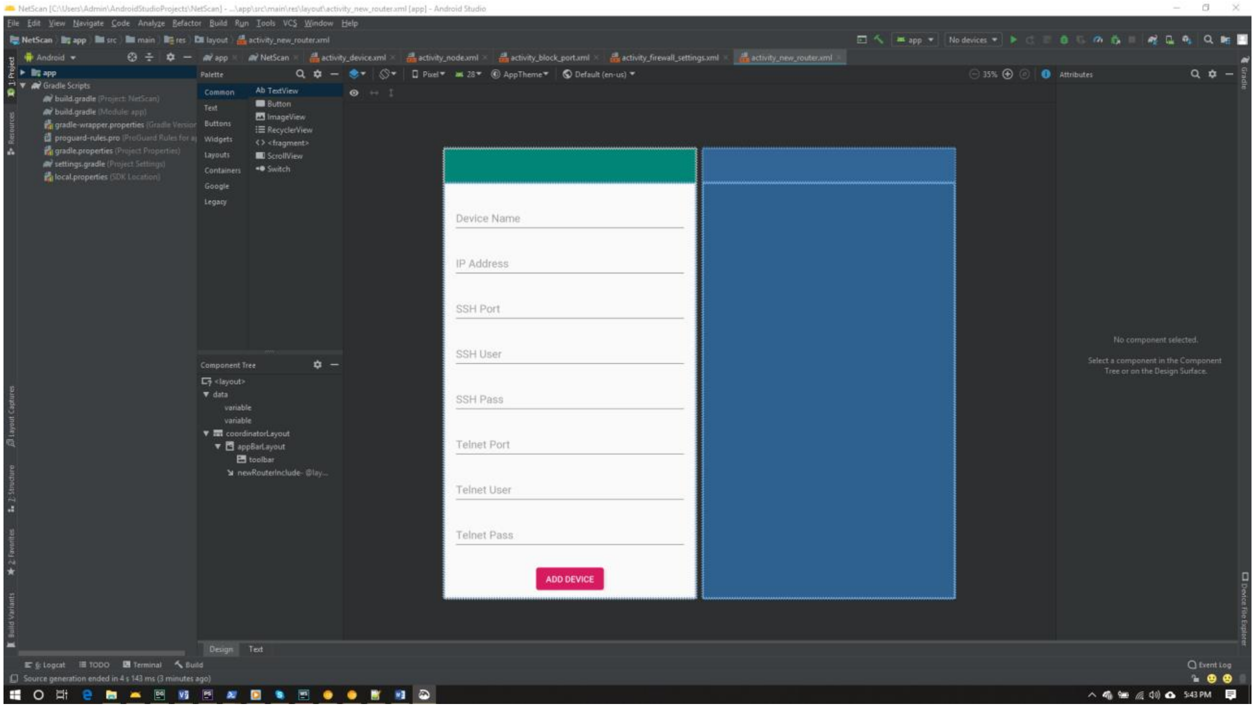
3 Block traffic to 239.255.255.250. uPnP SSDP attacks. Disables uPnP network devices.

```
iptables -I OUTPUT -
d 239.255.255.250 -
m mac --mac-source
20:62:74:16:EA:2C -j DROP
```

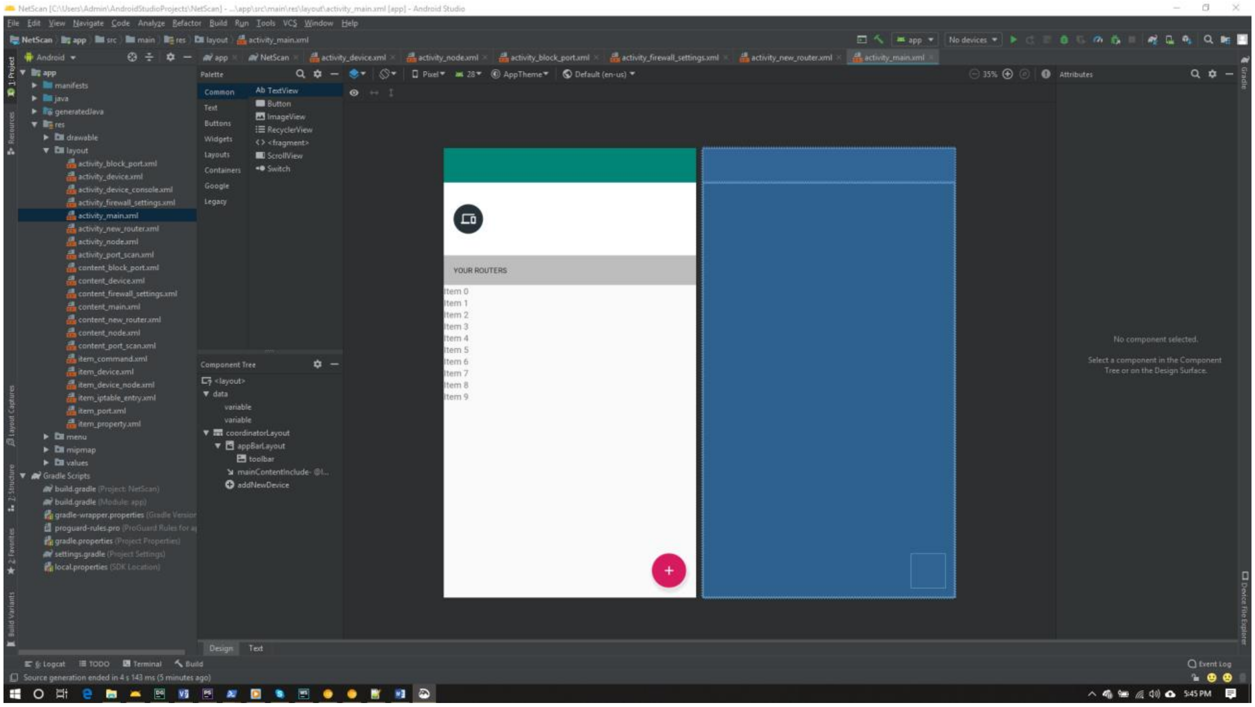
4 Block Facebook on device.

```
iptables -I FORWARD -p
tcp -d www.facebook.com
-m mac --mac-source
20:62:74:16:EA:2C -j DROP
```

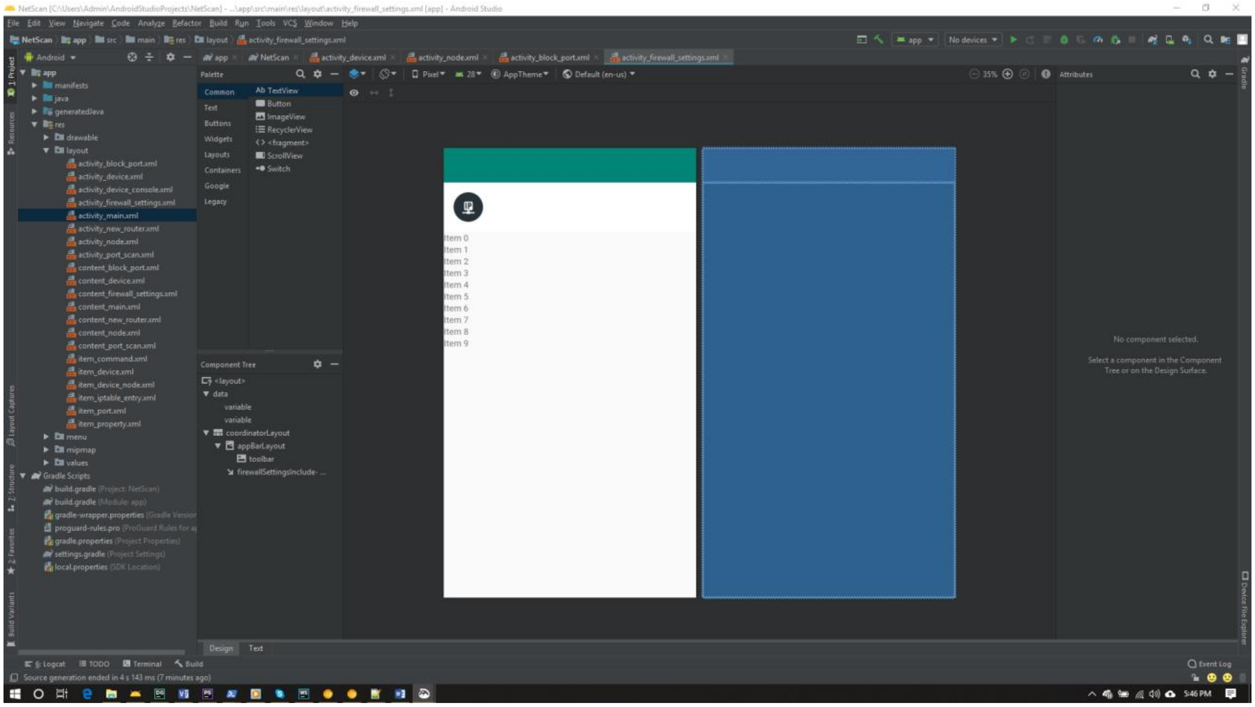
Appendix B: Net Scan Sample Designs


NetScan [C:\Users\Admin\AndroidStudioProjects\NetScan] - ...\app\src\main\res\layout\activity_new_router.xml [app] - Android Studio
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
activity_device.xml
activity_node.xml
activity_block_port.xml
activity_firewall_settings.xml
activity_new_router.xml
Palette
Common
Text
Buttons
Widgets
Layouts
Containers
Google
Legacy
Ab TextView
Button
ImageView
RecyclerView
<fragment>
ScrollView
Switch
Gradle Scripts
build.gradle (Project: NetScan)
build.gradle (Module: app)
gradle-wrapper.properties (Gradle Version)
proguard-rules.pro (ProGuard Rules for app)
gradle.properties (Project Properties)
settings.gradle (Project Settings)
local.properties (SDK Location)
Component Tree
<layout>
data
variable
variable
coordinatorLayout
appBarLayout
toolbar
newRouterInclude- @lay...
Device Name
IP Address
SSH Port
SSH User
SSH Pass
Telnet Port
Telnet User
Telnet Pass
ADD DEVICE
Attributes
No component selected.
Select a component in the Component Tree or on the Design Surface.
Design
Text
Logcat
TODO
Terminal
Build
Event Log
Source generation ended in 4 s 143 ms (3 minutes ago)
5:43 PM

New Router Activity Design



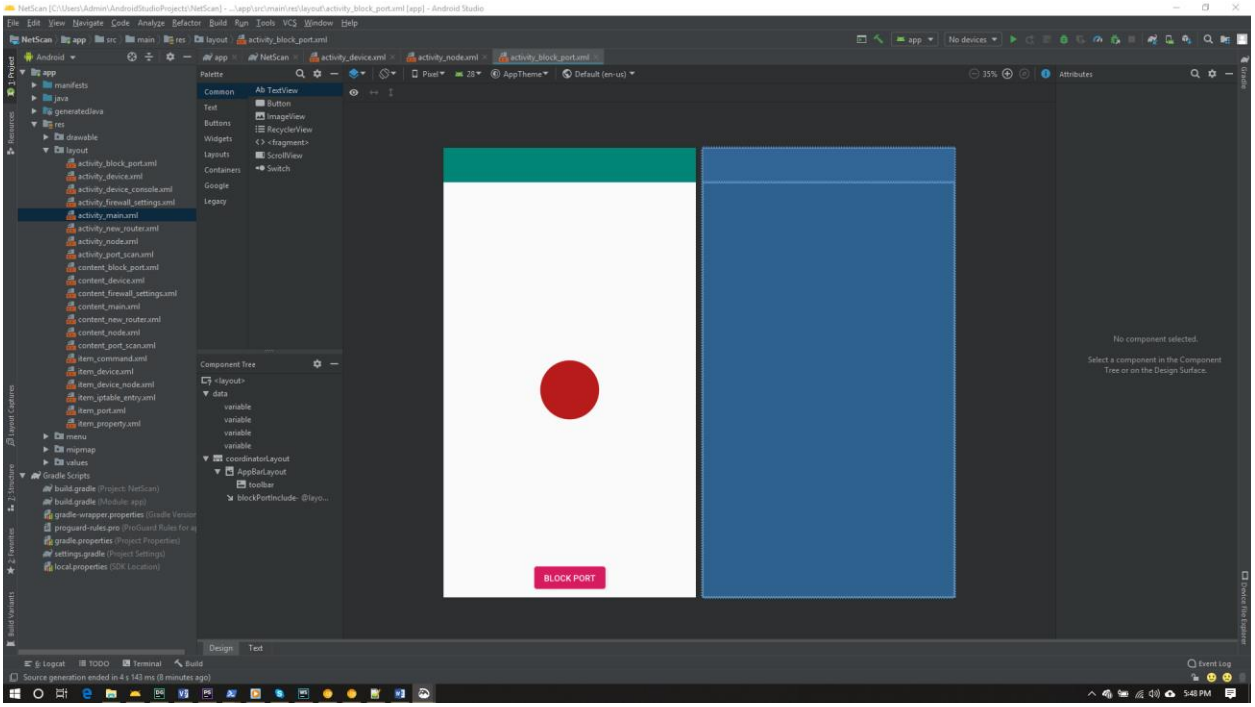
List of Routers Activity Design



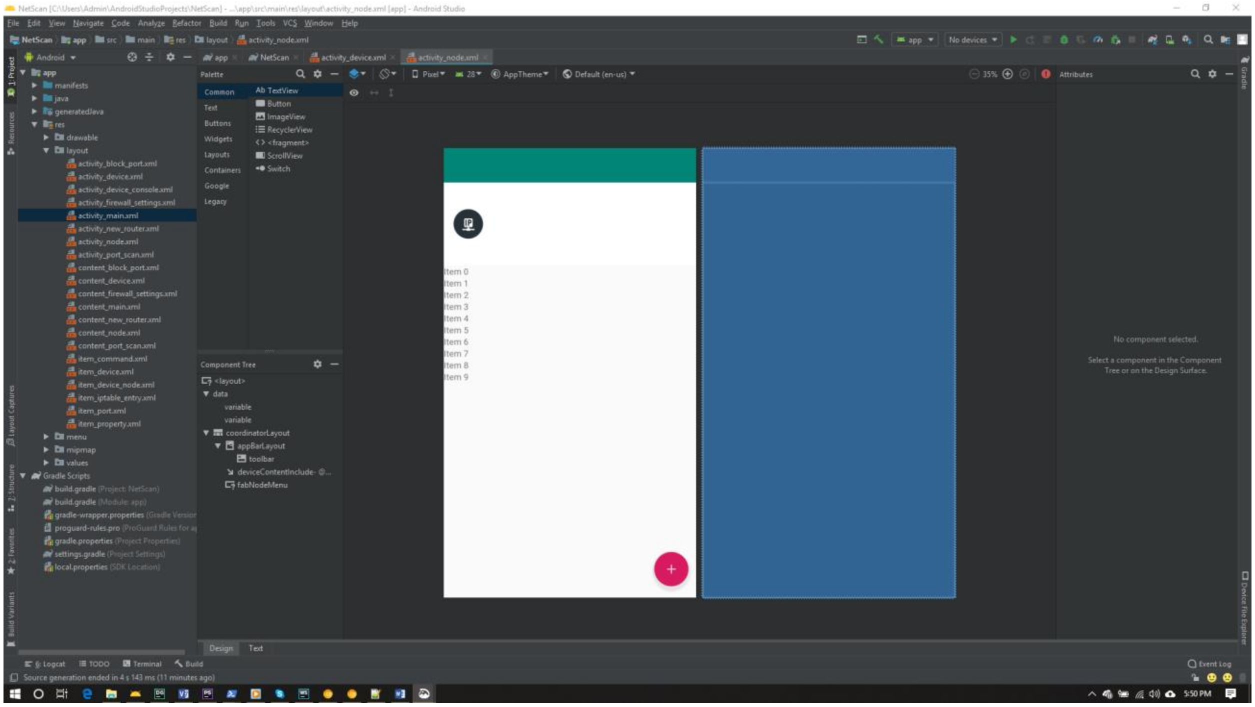
NetScan [C:\Users\Admin\AndroidStudioProjects\NetScan] - ...\app\src\main\res\layout\activity_firewall_settings.xml [app] - Android Studio

Source generation ended in 4 s 143 ms (7 minutes ago)

Firewall Activity Design

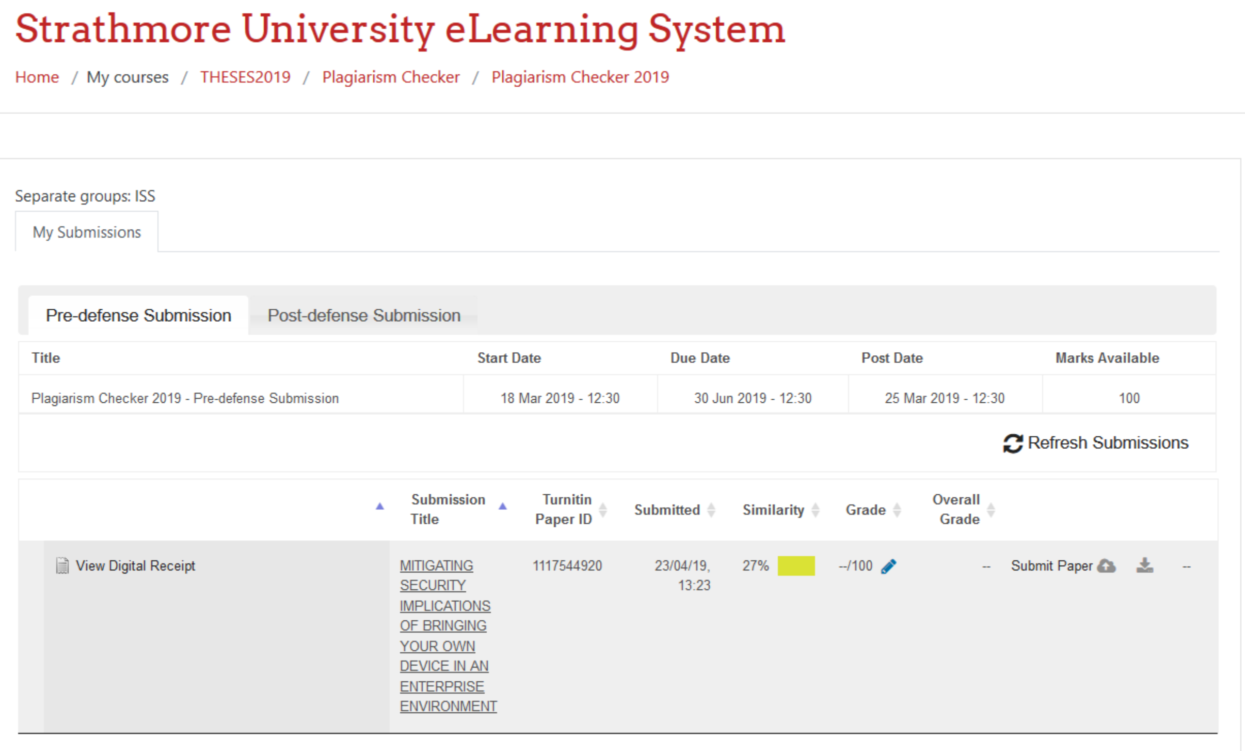

NetScan [C:\Users\Admin\AndroidStudioProjects\NetScan] - ...\app\src\main\res\layout\activity_block_port.xml [app] - Android Studio
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
NetScan app src main res layout activity_block_port.xml
app
manifests
java
generatedJava
res
drawable
layout
activity_block_port.xml
activity_device.xml
activity_device_console.xml
activity_firewall_settings.xml
activity_main.xml
activity_new_router.xml
activity_node.xml
activity_port_scan.xml
content_block_port.xml
content_device.xml
content_firewall_settings.xml
content_main.xml
content_new_router.xml
content_node.xml
content_port_scan.xml
item_command.xml
item_device.xml
item_device_node.xml
item_iptable_entry.xml
item_port.xml
item_property.xml
menu
mipmap
values
Gradle Scripts
build.gradle (Project: NetScan)
build.gradle (Module: app)
gradle-wrapper.properties (Gradle Version)
proguard-rules.pro (ProGuard Rules for app)
gradle.properties (Project Properties)
settings.gradle (Project Settings)
local.properties (SDK Location)
Palette
Common
Text
Buttons
Widgets
Layouts
Containers
Google
Legacy
Ab TextView
Button
ImageView
RecyclerView
<fragment>
ScrollView
Switch
Component Tree
<layout>
data
variable
variable
variable
variable
coordinatorLayout
AppBarLayout
toolbar
blockPortInclude- @layo...
BLOCK PORT
Attributes
No component selected.
Select a component in the Component Tree or on the Design Surface.
Design
Text
Logcat
TODO
Terminal
Build
Event Log
Source generation ended in 4 s 143 ms (8 minutes ago)
5:48 PM

Block Port Activity Design


NetScan [C:\Users\Admin\AndroidStudioProjects\NetScan] - ...\app\src\main\res\layout\activity_node.xml [app] - Android Studio
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
NetScan app src main res layout activity_node.xml
Palette
Component Tree
<layout>
data
variable
variable
coordinatorLayout
appBarLayout
toolbar
deviceContentInclude- @...
fabNodeMenu
Item 0
Item 1
Item 2
Item 3
Item 4
Item 5
Item 6
Item 7
Item 8
Item 9
+
Attributes
No component selected.
Select a component in the Component Tree or on the Design Surface.
Design
Text
Source generation ended in 4 s 143 ms (11 minutes ago)
5:50 PM

Node Activity Design

Appendix C: Turnitin Report



Strathmore University eLearning System

Home / My courses / THESES2019 / Plagiarism Checker / Plagiarism Checker 2019

Separate groups: ISS

Title	Start Date	Due Date	Post Date	Marks Available
Plagiarism Checker 2019 - Pre-defense Submission	18 Mar 2019 - 12:30	30 Jun 2019 - 12:30	25 Mar 2019 - 12:30	100

	Submission Title	Turnitin Paper ID	Submitted	Similarity	Grade	Overall Grade			
View Digital Receipt	MITIGATING SECURITY IMPLICATIONS OF BRINGING YOUR OWN DEVICE IN AN ENTERPRISE ENVIRONMENT	1117544920	23/04/19, 13:23	27% 🟨	--/100	--	Submit Paper		--