A Systematic Approach to a Quantitative Vulnerability Assessment for BYOD System Variables through the Discovering of Threats

By

Priscilla Mateko Boadi

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of The University Of Portsmouth

School of Energy and Electronic Engineering

Faculty of Technology

University of Portsmouth

January 2019

ABSTRACT

As a result of the emergence of new technologies and application features in mobile devices. Personal own mobile devices have become part of one's daily life activity including accessing an organisation's network for resources, such as documents and applications. For this reason, security metrics should be used as a mechanism for investigating the security risk level of this system. The complexity in monitoring, identifying and evaluating the growing number of security risk on computing systems is on the increase. Hence, the potential of security evaluation inadequacy defies standard security risk measurement as organisations find it increasingly difficult to predict the security level of a system as well as to accomplish its security goals. Existing security measuring methods which are mainly centred on security analysis fails to address the systematic classification of security metrics for a BYOD employed network and its variables. Although security metrics use quantitative measurement there is often a lack of information on BYOD variable and existing BYOD security measurements are based on static qualitative methods. Another limitation is that they do not provide an inclusive knowledge about the degree of vulnerabilities associated with a particular BYOD variable according to their attack impact on the network and its users.

This research offers a novel systematic metrics approach used in scoring BYOD variables that match organisations and individual users need, by integrating appropriate available metrics input about known and unknown vulnerabilities in safeguarding a BYOD environment. This thesis is made up of three core contributions: firstly, it proposes a BYOD Absolute Score metrics (BASmetric) framework which focuses on quantitatively ranking the security risk level of both an organisation and its BYOD user by integrating probability theory and user induce severity rule with support from security attribute taxonomy. This metrics framework is for measuring vulnerabilities and aimed to quantify an organisation and its BYOD systems vulnerabilities through their security attributes, host-level (operating system) vulnerabilities.

Also, the proposed framework has been applied to different domains(known and unknown vulnerabilities) which resulted in the second and third contribution. The second contribution is the systematic classification of the framework used to measure a BYOD known vulnerability information on an employed organisation variable(security policy, technology and users).it also shows the vulnerability severity level of a present BYOD system by producing an absolute value. The final contribution is the BYOD Absolute Score framework principle being used in assessing the steps involved in measuring the unknown vulnerability level of a BYOD variable based on organisation security attributes and produce a practical understanding absolute value. In addition, using different network security metrics the overall results show that the proposed approach produces better outcomes compare to preceding ones that consider network security level in whole without measuring the BYOD systems variable. Furthermore, BAS metric calculation shows a practical way to label and evaluate vulnerabilities for improved systems performance.

DECLARATION

I declare that whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are original and the work of the named candidate and have not been submitted for any other academic award except for publications.

Name: Priscilla M Boadi

Signature: 

Date: 31/01/2019

ACKNOWLEDGEMENT

First and foremost, I give all glory, adoration and honour unto the giver of wisdom, most high and all-knowing God for sustaining me from the beginning to the end of this programme. To my Lord and my Saviour, Jesus Christ and my Comforter, Holy Spirit, I am grateful.

I would like to express my sincere gratitude to my first supervisor, Dr Shikun Zhou, for his guidance, counsels, constructive suggestions and timely responses during the period of this study. I equally appreciate my second supervisor, Dr Ioannis Kagalidis helpful ideas.

I would also like to acknowledge the School of Engineering in the Faculty of Technology at the University of Portsmouth for offering me a quality research environment. I am also grateful to my fellow students for their encouragement and friendship. My appreciation and thanks to all my colleagues Chinedu, Ismail, Mohammed and Gabriel. I say thank you for allowing me shared tears on your shoulder. And my Iraqi friends in room 2.04, Anglesea building for all the ideas, encouragement and laughter we shared as a family.

I would like to express my deep gratitude to my mother, for her constant support and encouragement and, more importantly, for giving me the foundation to seek knowledge and building faith in me all these years. Awoyo, I can never thank you enough for what you have done for me. To my husband Castro Boadi for his financial support throughout this study, my children, Kwaku Attaeffah, Yaa Boadiwaa, Nene Jornoboah, thank you for your encouragement, laughter, love and hugs even at my lowest moments. Also to Pastor and Mrs Ige and all members of Victory Chapel International, Portsmouth, for your prayers word of faith and inspiration.

DEDICATION

This Thesis is dedicated to all women who are raising children and never give up, in whatever life throws at them and welcome every achievement with a smile.

List of Publications

- Priscilla Mateko B, Shikun Zhou And Ioannis K "Current BYOD Security Evaluation System: Future Direction" Vol.8 No. 3 Doi: 10.4173/2165-7866.1000235 Journal Of Information Technology & Software Engineering 2018

- Priscilla M. Boadi, Shikun Zhou And Ioannis Kagalidis "Towards A Novel BOYD Vulnerability Metrics Taxonomy For Organisations" International Conferences on www/Internet And Applied Computing 2018

- Priscilla Mateko Boadi, Shikun Zhou And Ioannis Kagalidis "Analysis of Security Issues In Bringing Your Own Device (BYOD)" 19th International Conference On Cyber Defense And Information Engineering (Iccdie 2017), Rome, Italy, May 4-5, 2017

ABBREVIATIONS

BYOD	Bringing Your Own Device
CMDB	Configuration Management DataBase
CR	Confidentiality Requirement
IR	Integrity Requirement
AR	Availability Requirement
N	None
P	Partial
C	Complete
L	Low
M	Medium
H	High
VL	Very Low
Report Confidence	RC
Remediation Level	RL
Exploitability	E
CVSS	Common Vulnerability Scoring System
FIPS	Federal Information Processing Standards
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OWASP	Open Web Application Security Project
ISMS	Information Security Management System Standards
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CIA	Confidentiality, Integrity and Authentication
Pr	Payroll
Es	Estates
Admin	Administration
Comp	Computing
Fin	Finance
Ts	Temporal score
VPN	Virtual Private Network
Is	Impact score

S	severity
HTTP	Hyper_Text Transfer Protocol
IDS	Intrusion Detection System device
WLAN	Wireless local area networks
STEA	State-Time Estimation Algorithms
MTTC	Mean Time to Compromise
DOS	Denial of Service attack
BAS	BYOD absolute score metrics
NIPD	Network Intrusion Prevention Detection
P(Ω)	Probability of an event
FTP	FTP File Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
VSL	variable security level
Pd	Personal user device
Eqn	Equation

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1 INTRODUCTION

Information technology (IT) has transformed the present world and greatly affected the way information is traded, from the small priced and costly books to the newspapers and magazines, the innovation of computers and its internet technology simplifies and quicken up the process of procurement, publication, and ultimately the exchange of information. Additionally, the recent era presents a more flexible and effective communication means via modern digital transmission technologies. However, with this enormous growth in IT comes with its demons as there are also security issues (Jain & Shanbhag, 2012; Seigneur, Kölndorfer, Busch, & Hochleitner, 2013; Keyes, 2016), Such as information being at risk of maliciously accessed by unauthorised users (Garba, Armarego, & Murray, 2015a).

The Internet is advancing at a significant rate in all areas of society, especially with the penetration of smart devices affecting every aspect of a user's life, a study by Today in Tech reports approximately 1.3 million android devices are being activated globally every day (Burns, 2012). This is a significate outcome as both the internet and smart devices are considered a de-facto standard for data communication, particularly in schools (University), hospitals and agencies where there are a larger group of potential users (Tropmann-Frick, 2018). The prompt increment in organisations allowing personally owned mobile devices to access their network either on the premises or outside the premises (Inc., 2012), have given rise in internet traffic and it emerging complications in computer network exploits. Also, it could lead to an increase in attacks over the internet and putting a great impact on security requirements (Availability, Confidentiality, Integrity, Authorisation, Non-Repudiation, Privacy) in essential data information.

The phenomenon of Bringing Your Own Device (BYOD) is the use of personally owned devices within a working environment for professional purposes, this could be smart devices

such as smartphones, tablet, mobile devices, and laptops. Thus BYOD affects people's life, being in education, social and economy, whilst it has its many benefits so are it related disadvantages. BYOD can be attacked using exploiting vulnerabilities which may be present either in the application software, hardware (personal device or server) and an employed network (Weintraub, 2015), these exploitations can lead to attacks causing disruption to business processes and an increment in the information technology systems risk (Beale and Berris, 2018; Yan *et al.*, 2012). The Georgia Tech Information Security Centre (GTISC) and the Georgia Tech Research Institute (GTRI) released Emerging Cyber Threats Report for 2013 which stated vulnerable APIs, data loss, data compromise due to access to unencrypted data as a form of attacks against BYOD employed mobile devices (Hiller & Russell, 2013). Regardless of these attacks, smart devices need to perform their assign services.

Information Security (IS) is an important situation in any organisation especially as BYOD activity is evolving and increasing. Therefore routine check-up for related attacks in BYOD deployed network and their smart devices is performed by organisations. These could include infiltrating the network with intrusion detection systems, encryption, two-factor authentication, firewalls and antivirus as some of the preventive measures by organisations and users to check attack. Since an attacker achieves its objective by infiltrating the network of an organization, and they utilise on various vulnerabilities of a targeted host, therefore it becomes necessary for both users and organisations implementing BYOD to be aware of the risk posed by each vulnerability.

Classification of security level is influenced by network transmission, vulnerability, threats and up-to-date policy(Ahmed, Al-Shaer, & Khan, 2008), amid these influencers, an attack occurs when a vulnerability is exploited by an intruder since it considers it as an open door to enter a system, therefore vulnerability can be said to be a major influencer of network service exploitation. The bigger the organisations network the likelihood of a vast number of

vulnerabilities (L. Wang, Jajodia, Singhal, Cheng, & Noel, 2014). Also, quite a significate number of threats are actually vulnerabilities, such as in web browsers, email reader, document viewers and multimedia applications running on victim devices(Lippmann et al., 2007).

The quantitative evaluation of security level is a significant area to research since its final objective is to predict risks and threat, but it is extensive and exhausting working on a bigger organisation with much complex network structure in contrast to a small organisation with limited infrastructure. So, for the purpose of this research, a sub-organisation network is used as a case study. To effect this, a tool is required to measure the feasibility (probability) of vulnerabilities present in its network by deploying vulnerability scanning tools such as Nessus vulnerability scanning tool to detect any defects (Daud, Bakar, & Hasan, 2014). The outcomes of the vulnerability scanning tools merely display the ports which are likely to be exploited and the type of likely attack.

In network security engineering more effort is placed on safeguarding a network by tracing the steps of attackers in attaining their target and placing intrusion detection mechanism in the network. But for the security implication of an organisation offering a diversity of collective services (BYOD service), maximum effort should be put in measuring the general security level of the organisation's network quantitatively (Boyer *et al.*, 1986; Wang *et al.*, 2014; Homer *et al.*, 2013; Ou and Singhal, 2011). The concept of an attack tree is an important model used as a strategy by a security administrator to illustrate all the possible path of an attacker in breaching a security policy by exploiting the necessary vulnerability. Whereas this is a safe option, it is just a part of a holistic definition of a quantitative security risk evaluation, therefore a holistic quantitative security metrics in establishing the security risk level is deemed a useful approach. These metrics will aim to tackle the establish security goal of data confidentiality protection, uphold data availability to only authorised personals for authorised use and preservation of data integrity.

The following chapter examines the motivations which demonstrate how suitable this research is with regard to the problem it seeks to solve as well as the aims and objectives that the research intends to accomplish. Subsequently, the contributions of this thesis in terms of both knowledge and technical perspectives are emphasised. Finally, the overview of the contents of this thesis is explained.

1.1 Research Background

Theoretically, Smartphones and tablets are fast on the increase and employees (users) find it necessary and convenient to use them for official duties, thereby a BYOD. Yet, BYOD has no formal effective evaluating system and no continuous evaluating process for coping with changes which means that once a BYOD device is designated to a connected it remains connected with difficult for user's side security evaluation[20]. Significate amount of security continues to be the greatest factor in a BYOD environment, where there is a need for the protection of both the organisation network (data) and the personally own devices(Y. Wang, Wei, & Vangury, 2014). It is no longer a good security practice to stop security attack as and when they appear but to take initiative with attack prevention tools such as anti-virus, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). However, these attacks have also found new ways of exploiting a vulnerability.

Research shows organisations measure the risk of an attack statically by categorisation the many hardware and software policies and personal intuitions (MSRC, 2017). As a result, threats are tackled according to those that pose the greatest risk, however, an issue arises when these vulnerabilities/threats are too many to tackle and each is categorised by distinct scale (US-CERT, 2018), Currently, BYOD employed organisations and their users are prone to cyber-attack as their network is exposed to outside influences and so to reduce the impact of any vulnerability from being exploited. a quantitative measurement that scores BYOD variable security risk level promptly and clearly is a real challenge (Viehböck, 2011).

The development of security metrics by an organisation is a very challenging exercise as noted on the science of security report (Sanders & Nicol, 2018). Categorising the processes involved in its design, deployment, and evaluation is a tough challenge in cybersecurity. Particularly in the procedures used in identifying what should be covered in measuring a specific set of security policies and quantifying them efficiently. A security metrics level is centred on an Objectivity, answered by what required to be quantified its competence and control, also by the accuracy, authority and feedback of the created metrics. The main aim of the BAS metrics is in quantifying value (data) and measuring performance. Security metric is a problem-solving measure deployed in computing and information security engineering and its related field's. Many security metrics are currently available that can be used to analyse an organisations network; State Time Estimation Metrics (McQueen, Boyer, Flynn, & Beitel, 2005), Mean Time to Compromise (Leversage & Byres, 2013), Mean Time to Failure(Dacier, Deswarte, & Kaâniche, 1996) used to analyse the frequency of failure in a network. Despite the strong influence of current network security metrics and exactly how helpful they can be, there remain certain substantial limitations such as:

- Models based mainly on the main network but fail to address an individual BYOD network and its user's needs in the security metrics evaluation process. Authors (Zahadat, Blessner, Blackburn, & Olson, 2015; Ketel & Shumate, 2015) mentioned that a BYOD Security monitoring framework implemented for an organisation should reduce security breaches related to authentication, rogue mobile device access and the need to develop audit guidelines for BYOD (Brodin, 2015)
- Another deficiency in present BYOD security measurement is the classification of vulnerability solely on Mobile Device Security and ignoring the issue of network vulnerability. For example, Mobile device vulnerabilities such as inconsistent security policies within Different devices, Laptop Encryption discredited within a "Bypass Mode",

Unmanageable BYOD Laptops, Shared Media Leakage, Adhoc BYOD measurement, Readable Data carried on in a Disposed Of Devices, Inter application Data Leakage (Girard, 2013).

- Security and risk enforcement on BYOD system is challenging because of the variable classification into People (users), Technology (network, Operating Systems(devices) and applications) and Policy hence it is difficult for enterprise security administrators to audit its security policies (Yang et al., 2016). Resulting in limited Information on security risk of using the BYOD in terms of security attribute, trust and efficiency.

All these details offered the motivation towards the development of a new approach to overcome the measurement impracticality phenomenon and to achieve a comprehensive understanding of the BYOD variables. Two research problems are to be addressed. Firstly, by what means does all the organisational variables participate in the measurement, including the network configuration, personal device category and the users then create a relationship between the pertinent information. Secondly, with all the information incorporated, how to measure the security level of a system and references to establish policies relating to BYOD management.

1.2 Aim and Objective

To tackle the limitation of a security metrics, a framework is proposed centred on the techniques proposed in the research, which can have a true application with an impact in the scope of network security metrics system. The framework aids data integration and cyber-security measurement purposes. Affecting procedures enables the probable impact score to be produced as a result of data integrated from multiple network security tool. The essential aim is the ability to provide practical scoring metrics to rank vulnerabilities according to those that pose the greatest risk, focusing on organisations providing BYOD services on its network.

The aim of the research can be defined in these exact objectives:

1. To investigate the state-of-the-art techniques of security metrics and research gaps particularly in the area of computer network security. Also to examine tools available to employed BYOD users, and aid in decision making when evaluating the security risk level of their computer network.
2. To examine major BYOD security attacks and identify known and unidentified attacks which have been introduced onto an employed BYOD network thru the exploitation of known and unidentified vulnerabilities.
3. To develop a method to integrate data from individual metrics which allow for an employed BYOD network and its user's vulnerability level to be assessed. The approach should be able to calculate the identified known vulnerabilities and unidentified vulnerabilities based on probability rule and expressed as an absolute score, and launch towards the security requirement of users and the organisation as a whole.
4. To design an approach for BYOD security metrics. Then apply the proposed approached on a designated organisation's BYOD employed network
5. Evaluate the approach performance in comparison with state-of-the-art approaches

1.3 Major contributions

This research is focused on addressing the existing security measurement gap and investigates an approach by which to score the security risk level of an employed BYOD variable (Network, User device). this is done by using an extracted vulnerability information and categorising it accordingly. That is, the vulnerability type is classified into known and unidentified vulnerability. This is to ensure the practicality of the BYOD security metric. The aggregation of individual metrics into the computation process is one of the remedies that can overcome the limitation of establishing BYOD security measurement procedures. The BAS metrics are used to calculate the likelihood and impact of an attack on an employed BYOD variable and scored quantitative (absolute score).

The main contributions of this thesis are arranged in the following items:

1. It contributes towards the knowledge of present network quantitative security metrics by rising the understanding as to what ways current issues are usually tackled and why the weakness persists.
2. The representation of the extracted vulnerability is designed to integrate formula from individual metrics, this contributes to improving the consistency of measurement by overcoming the complexity and heterogeneous of interconnected computer networks.
3. It describes a novel BYOD Absolute Score(BAS) measurement framework. This is developed and evaluated and the metric shows an increase in its precision but also intensify in exact security level prediction.

1.4 Thesis Organisation

This thesis is structured as follows. It begins with chapter 1 where the general background of the thesis is presented followed by a brief description of the motivation and contributions of the research are offered.

Chapter 2 gives the theoretical background and related work highlighting different methods and approaches that are used in security risk assessment and mitigation in general and application of security metrics in particular.

Chapter 3 Introduces the BYOD Absolute Score framework and its modules in vast detail, this comprises the core of this work.

Chapter 4 Discusses the implementation of the proposed BYOD security metrics alongside the detail procedures that are used in calculating the score of the security level.

Chapter 5 Discusses the evaluation approaches. A comparison evaluation using a case-study to determine the system security requirements followed by result precision, accuracy and practicality of the security measures.

Chapter 6 presents the conclusion, in summary, the goal of the thesis is defined and the directions for future work are also presented.

Finally, the thesis includes the bibliographic references used for its elaboration and annexes that provide information relevant to the thesis.

CHAPTER 2 LITERATURE REVIEW

In order to describe the security metrics of any system, it is suitable to understand the objective behind the measurements of that system; for this particular study, the objective is the measurement of the security risk level of a BYOD system quantitatively. This chapter introduces the concepts employed by this research towards the realisation of that objective. First, a discussion on BYOD is presented in Section 2.1 in which a brief history of BYOD given, including the introduction, deployment, and its potential security risks. Followed by, Section 2.2 where an overview of BYOD Security Technologies is outlined such as features and schemes which employed metrics in information security risk prediction. Section 2.3; presents work on risk assessment models standards, which we will be later referring to in this thesis, the CVSS and the OWASP risk rating methodology. The former helps in characterising and calculating the effect of IT vulnerabilities while the latter methodology is to measure the security risk level of a BYOD invisible attack. Section 2.4 presents the Information Security Risk Management outline that is followed in the security requirement classification for this thesis. This section outlines the different sets of BYOD policy requirements that have been proposed together with the different approaches that are used in improving those questions. Section 2.5 describes the various security metrics used for the network evaluation. Section 2.6 illustrates intrusion detection and vulnerability assessment security tools. Finally, Section 2.7 summarizes the chapter and reports on the main observations obtained from preceding work that motivated the use of the quantitative measurement approach proposed in this thesis for BYOD security risk metrics.

2.1 Bringing Your Own Device (BYOD)

More organisations are introducing their networks and its data to the outside world, meaning they allow personally owned mobile devices to access their network either in the organisation or outside the organisation (Forrester Consulting, 2012). Nevertheless, it becomes even more interesting when employees are allowed to use these devices for work purposes such as

retrieving and storing of data, upload and download of files and any other official duties, this is done either in or outside the office premises, the phenomenon is known as BYOD (Ketel & Shumate, 2015). BYOD, as the name articulates is the use of personally owned devices within a working environment for professional purposes, the personally owned devices can be any smart devices such as smartphones, tablet, mobile devices, and laptops. The term BYOD became evident about 16 years ago by Information technology (IT) service provider Intel (Field, 2011), for reasons such as;

1) Allowance was allocated to employees to purchase devices of their choice for work purposes.

2) Using an employee's personal device to access corporate resources is allowed by the IT department of an organisation.

3) Most importantly, BYOD promotes mobility and flexibility, therefore users are drawn to them in their workplaces than the one that has been offered to them by their organization's IT department for the benefit productivity, increment in work efficiency and mobility (Bradley, et al., 2012; Twentyman, 2012; Sarker, et al., 2012).

Hence, an organisation is said to be practising BYOD only if the BYOD device user is allowed to use the BYOD device to access the organisation's resources without any hindrances.

The occurring security issues in terms of information security and its effective means of measuring these security threats when necessary is needed for safeguarding a BYOD employed network. Although most of the reviews are affected by consulting firms that mostly gives descriptive suggestions of the BYOD occurrences and normative advice for executives (Niehaves, Köffer, Ortbach, & Katschewitz, 2012). However, there are peer reviews and white papers on BYOD framework, some of these white papers recognised the risk associated with

BYOD and provided Policy-Based solutions. For example (EY, 2013), suggested the three areas of BYOD risk made up of mobile devices risk, application vulnerabilities, and inventory and platform management risks, but its white paper has a general explanation to BYOD risks and concluded by presenting eight steps to secure and improve BYOD programs. Other experts in the field of Information Technology such as (Leavitt, 2013; Morrow, 2012; Miller, et al., 2012; Thielens & Axway, 2013; Tokuyoshi, 2013; Olalere, et al., 2015). This showed the existence of BYOD by coming up with some information on its security concerns and how it can be handled administratively by an organisation. Nevertheless, they agreed on data security, malware, and network security as the main security challenges (Olalere, Abdullah, Mahmod, & Abdullah, 2015).

2.1.1 Evidence of Risk in BYOD Adoption

In the subsequent sub-sections, a review on BYOD security risk classification is presented with the different types of methods and techniques used in its assessment.

2.1.1.1 Features of Security Risk Management Approaches

Many different approaches have been used to rank computer security risk management; Static security management is one of the approaches that have been used by many organisations and researchers. (Morrow, 2012), ranks static security risk by scrutinising through an application or system to locate any malicious behaviour this includes software's or applications having conduct of maliciousness. In (Dawson, 2015; Chandramohan & Tan, 2012; Garba, Armarego, & Murray, 2015), the static mobile security risk is also defined based on threat towards the physical devices (Mobile devices). Likewise, authors like (Wang, Wei, & Vangury, 2016; Morrow, 2012; Jain & Shanbhag, 2012, Garba, Armarego, & Murray, 2015) also examines Static security policies as one of the main threat affecting data security in a Mobile device and its application environment with changing nature.

In (Eijndhoven, Iacob, & Ponisio, 2008; Hermosillo, Seinturier, & Duchien, 2010). Dynamicity is referred generally, as finding a decision point in a process and classifying them by their

business rules. Interestedly in the mobile security world, as explained by (Dawson, 2015), dynamic analysis happens when an investigator has access to a mobile application being executed in a remote environment, such as a virtual machine or using an emulator for monitoring. Authors in (Twentyman, 2012; French, Guo, & Shim, 2014; Morrow, 2012), Monitors security risk dynamically based on the computing system auditing policies of a security management system in real-time without major interaction from the environment (Chandramohan & Tan, 2012).

Furthermore, from the literatures both static and dynamic rankings are being affected by external factors and how they react to it makes it either dynamic or static, these factors include; (People (Users behaviour, Technology (physical devices), OS, applications) Organizational Policy (Management rules)) (Olalere, Abdullah, Mahmod, & Abdullah, 2015). Both static and dynamic security techniques have been highlighted in Table 2. 1, it also shows some advantages and disadvantages. Additionally, Table 2.2 to 2.3 characterises computing systems security vulnerabilities and their mitigation approaches.

Methodology	Advantages	Disadvantages
Static Security Monitoring System (Russo & Sabelfeld, 2010)	It examines program code and reasons over all possible behaviours that might arise at runtime manually	It is easy to manipulate since there is physical contact program any time there is a change in variable
Dynamic security Monitoring System (Wanniarachchi & Gamage, 2019)	Monitoring takes place at each stage of a BYOD program or operation, these observe the executions. Dynamic analysis should be exact with no estimation.	involves a great deal of calculation and may not always be relevant for later implementations

Table 2. 1 Static and Dynamic Security Monitoring System

Static Security Vulnerabilities	Mitigation Approaches
Physical threat and Exposure of confidential data from ; Stolen or loss and decommissioned of devices Malware, Hacking, Social Engineering	Personal device storage areas should be Encrypted Training users not to store sensitive dataon personal mobile devices Shutting down of devices remotely by administrators in the case of lost or stolen devices

(Dawson, 2015; Morrow, 2012; Lee & Shin, 2014; Garba, Armarego & Murray, 2015)	User education and awareness

Table 2. 2 Static Security vulnerabilities with their Mitigation Approaches

Dynamic Security Vulnerabilities	Mitigation Approaches
Risk of data insecurity or leakage(loss) from misuse of BYOD policy on access and insider threat. (Y. Wang et al., 2014; Morrow, 2012)	encryption of corporate data BYOD devices should be restricted Device integrity scanning application should be used
Storing an organization's data to an unsecured location (Jain & Shanbhag, 2012)	Regular user education and awareness System Monitoring
Insecure interface and APIs due to; Direction from Malicious QR codes (Quick Response Codes) Weak API(application programme interface). (Collett, 2015; Sharma, 2012; Thielens, 2013; Hashizume & Rosado, 2013).	Untrusted content downloaded on a BYOD device should be avoided Use secure web gateways, HTTP proxy servers, etc. to validate URLs Before allowing access Restrict peripheral use on mobile devices(e.g,disabling camera use) to prevent QR code reading strong authentication and access control mechanism
Untrusted Networks, application and mobile devices could result in the following; Eavesdropping Man-in-the-Middle attacks Malware attacks Downloading Malicious applications (Yang et al., 2016; Ketel & Shumate, 2015; Tokuyoshi, 2013).	Mutual authentication procedure should be used for verification from both endpoints InactiveNetwork interfaces disabled The third-party application should undergo a risk assessment before allowed to be used as a BYOD device forbid insecure Wi-Fi network connection

Insecurity in Virtual Machine Migration or creation. (Uehara, 2013; Tari, 2014)	Location services in mobile devices turn- off in sensitive areas or implement firewalls Use a separate browser within a secure sandbox for browser-based access related to organization monitoring through IDS (Instruction Detection System

Table 2. 3 Vulnerabilities Security vulnerabilities with their Mitigation Tactics

2.2 BYOD Security Technologies

Information security technology can be defined as the type of protection given to a piece of information to mitigate risk, these technologies can be used to secure information on the level application, host and network. Since the inception of the internet Information Security Administrators has tackled the issue of information security either by Proactive or reactive measures. Proactive technology measures are those information security technologies employed to keep data and its resources safe before a security breach can occur. Also, reactive technology measures are those security technologies being taken in the course of an information security breach so further damages are prevented and its related data and resources are kept secure. Furthermore, both proactive and reactive security technology measures are used at both the network, host or application levels which makes it an important field in measuring the BYOD security.

Presently, security risk evaluation is performed by an IT organisation to classify different vulnerabilities which threaten hardware and software policies. these vulnerabilities are tackled according to those that pose the greatest risk. However, an issue arises when these vulnerabilities are too many to tackle and each is scored by distinct scales.

A report on a BYOD security framework as published by the centre for internet security (CIS) (Zahadat, Blessner, Blackburn, & Olson, 2015).CIS confront the security concern of BYOD adoption using an authentication framework, The structure is made up of seven essential stages; (Plan, Identify, Protect, Detect, Respond, Recover, Assess and Monitor), surrounding the four

compulsory stages of the BYOD Security Lifecycle, the mentioned security framework is meant to fit in security policies of organisations and particularly acts as part of their risk management framework(Alberts & Dorofee, 2010). The proposed security framework stands as a static security strategic as it fails to dynamically monitor and update unknown devices and their risk associated. In the identity phase, users and their devices are registered on the organisation's network but only known devices are authenticated, but an error can occur where devices are newly registered and it is assumed it's following organisational security policy. The framework does not distinguish between visitors and regular. Nevertheless, there are peer reviews and white papers on BYOD framework, these white papers recognised the risk associated with BYOD and provide non-technical (policy-Based) solutions. For example, Insights on governance, risk and compliance report by Ernest and Young (EY, 2014), suggested the three areas of BYOD risk made up of securing mobile devices, addressing application risk, and managing the mobile environment it further concluded by presenting eight steps to secure and improve BYOD programs.from all studied literatures it could be noted that BYOD security program in specific is part of a larger security policy of most organisation.

In the following subsections, a detailed review on Vulnerability Scoring System is presented. This includes different methods of security risk scoring system being outlined in section 2.2.1 whiles previous work on security frameworks are outlined in subsection 2.2.2.

2.2.1 Vulnerability Scoring System

In the following sub-sections, a detailed review of vulnerability scoring approaches is presented with the different types of methods and techniques.

2.2.1.1 Security Risk Scoring Approaches

For the conversion of vulnerability data into an actionable material a Vulnerability Scoring System becomes necessary, there are several scoring systems used for grading vulnerability with each having its benefits. The Vulnerability Notes Database by CERT Coordination Center

(CERT/CC) (Viehböck, 2011)is used to generate vulnerabilities scores in the range of 0 to 180 and considers whether the Internet infrastructure is at risk and the category of security requirement a prone to exploitation. In (MSRC, 2017), which introduces the SANS vulnerability analysis scale consider where any form of weakness is located by deliberating on default configurations, client and server systems. Also, within (CWE, 2016) Microsoft's proprietary scoring system is introduced, which considers the difficulty of risk exploitation and the total impact of the vulnerability. While these scoring systems are useful, yet they are not made to suit the environment (individual and organisation) of a particular situation, therefore they can be term as an invariable solution.

2.2.1.2 Features for Evaluation and Predicting system's environment vulnerability

There are many different security risk management methods and models that have been proposed for smartphone usage. Some of these are dynamic security frameworks, which concentrate on system security policy and requirement. Authors in (Mell, Scarfone, & Romanosky, 2007; Scarfone, 2009) outline Security Management to include identifying, assessing and monitoring of all IT platforms for vulnerabilities. In spite of this, prioritizing and predicting these threats and vulnerabilities that pose the greatest risk is essential. Similarly, Authors (Mell et al., 2007), proposed a scoring system to translate the threats and vulnerabilities data into readily used information to prevent each different threat and vulnerability to be scored differently. Institutions such as (MSRC, 2017; NIST, 2018; Palmaers, 2013) classify vulnerabilities for scoring based on code, design, and architecture requirements. These systems reported in (CVE, 2019) and helps IT security managers to make decisions on activities to be performed in other to reduce the risk of Vulnerabilities and also encourage flexibility in the situation of BYOD users.

Modern security monitoring systems use vulnerabilities databases to predict the likelihood of an attack (Weintraub, 2016). These databases are frequently revised as new vulnerabilities are

detected and later using the scoring algorithm to predict the potential organisational losses, that is the returns on investment. Furthermore, these measures by assessing the database of published security vulnerabilities then compare it to real-time organisational vulnerabilities for present exposures (alert) and calculate the requirements which are confidentiality, integrity and availability. The impact measures for the organisation are also based on the environmental variables these are updated in the system's Configuration Management Data Base(CMDB) proposed by (Keller & Subramanian, 2009). This helps in making the scoring models proficient as prediction will be based on the organisational damages on a real environment rather than on the user's estimations. Figure 2. 1. Shows a Cluster-Based Monitoring system as an example used by the author (Weintraub, 2016) for its scoring system.

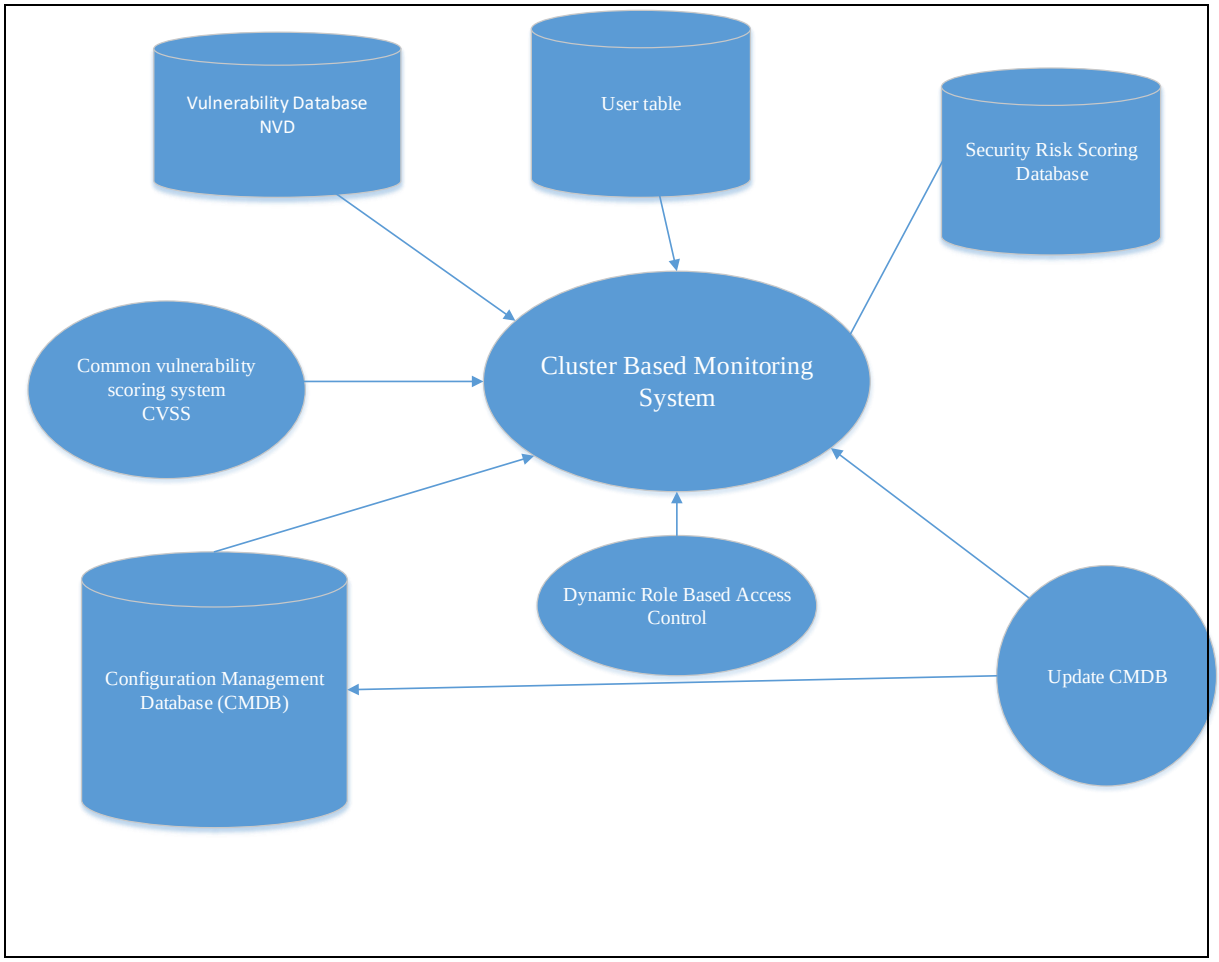

Figure 2. 1 Structure for Cluster-Based Monitoring Evaluation

The CMDB as presented in Table 2.4 below has configurations information of a system made up of the following entities: software, Application and system components, for instance, operating system, database management systems, utility programs and development components. The CMDB database is a corresponding database to the Cluster-Based Monitoring Evaluation system.

Column value	Column Name	Column Description	Value
Basic parameter	None, Partial, Complete	N, P, C	Unique
COMPONENT TYPE	Hardware Type (Smartphone, Tablet disk…), Software type(Microsoft, Apache), etc.	For example Database, Table,	Unique
CONFIDENTIALITY IMPACT (CI)			
CR	Confidentiality Requirement	The importance of the affected IT asset to a user's organization, measured in terms of confidentiality	L,M,H
IR	Integrity Requirement	Guarding against improper information modification or destruction.	L,M,H
AR	Availability Requirement	Ensuring timely and reliable access to and use of Information…	L,M,H

Table 2. 4 CMDB Database environmental Variables

2.2.2 Security Management Frameworks

In the following sub-sections, a review on security frameworks are presented in addition to other different types of scoring frameworks.

2.2.2.1 BYOD Security Lifecycle

This includes the security life cycle of the mobile device during its involvement in a BYOD program. The definition of each component, according to (Zahadat, Blessner, Blackburn, & Olson, 2015) is presented below, with their component also highlighted in Figure 2.2

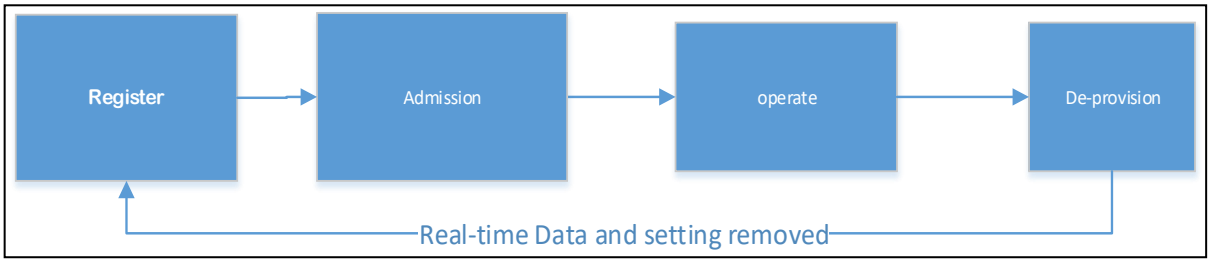

Figure 2. 2 BYOD security lifecycle

I. Register

The mobile device is listed onto the BYOD program. The device and its mobile operating system are scrutinized to certify they meet the basic requirement for its inclusion to the program.

II. Admission

This includes the Enrolment policy of the organisation where preparing and equipping the network are allowed for services and new users are admitted. During the process, the device is set-up with configurations settings, software, and certificates necessary to prepare the device for its admission into the BYOD program.

III. Operate

This involves granting access to BYOD users organisation resources. With all things being equal, the user continues to enjoy the benefits of BYOD while maintaining compliance with all organizational requirements for participation in the BYOD program.

IV. De-provision

In the cause of any tragedy factors such as theft or device loss, there is no longer a need for a device to stay connected to the BYOD program, therefore all the organizational data are removed dynamically(automatically) and in real-time that is immediately when the user resigns, report of the device stolen or any mishap.

Key de-provisioning activities:

- Real-Time access removal
- Real-Time Wiping of sensitive Data
- Real-Time removal of certification and configuration settings
- Real-Time removal of security Software

The device is returned to the user and is no longer able to access organizational resources.

2.2.2.2 Dynamic BYOD Security framework

Authors (Kearns, 2016). Classifies the security framework of an organisation BYOD program into seven (7) main stages which are in an iterative process and illustrated in Figure 2.3 below ;

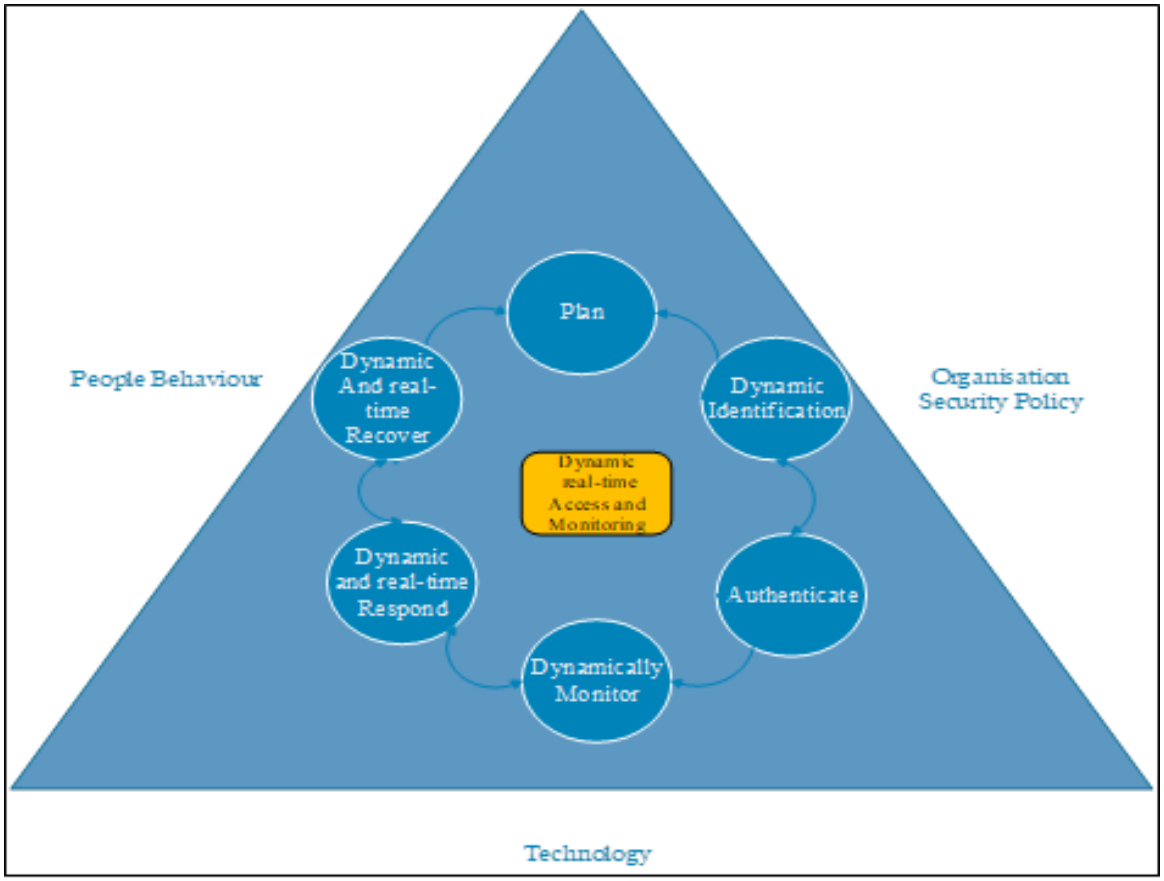

Figure 2. 3 Dynamic BYOD Security framework

Plan (Generating Security Policy)

In undergoing any major endeavour there is proper planning. In this section, we will highlight some of the key concepts that are critical during the planning process of a security program. The Plan phase requires close coordination across multiple disciplines and among all stakeholders. The planning process must be supported at the highest levels of management to ensure that appropriate time and human resources are allocated. It starts with understanding the business environment, this includes identifying who the users are and what resources they will be accessing. This also includes the standards needed in order to ensure that variables are capable of supporting functions and security requirements.

Some key planning item include:

a. Classify organisation information security policies with its security roles and responsibilities.
b. Identify regulatory and legal requirements.
c. Plan a business process model.

The Dynamic Identification phase

This begins the security lifecycle, and it includes registering of devices for participation in the BYOD program plus officially approved for use and provisioned with required security settings in accordance with the Plan phase. In the first step of the BYOD Security Lifecycle, the assigned department within the organisation will evaluate the variables to ensure it meets established hardware and operating system requirements for inclusion in the process. Some organisations may want to consider eligibility criteria for employees as well as devices. This extra check will ensure repeat violators of security policies are not placed in a position to cause additional harm. Prior to granting the user any access to organisational resources or data, the user should be trained on the policies and procedures as well as their individual role and responsibilities in carrying out the security controls associated with the said program. This initial training helps to clearly communicate the rules of behaviour expected of users(employees). Also, periodic training will reinforce security norms and build a culture of security responsibility and awareness surrounding a network. Next, the device should be provisioned in accordance with organisational policy. Provisioning is the act of implementing security configurations, settings, applications, device profiles, and software certificates necessary to fully realize all security controls established as part of the schedule. This can be done Over-the-air (OTA) or off-air, as approved by the organization during the Plan phase.

Authentication

It includes the organisation's variables being signed up to the network program. There is the need to ensure that devices and the information that resides on them are appropriately protected

throughout the BYOD Lifecycle. Subsequently, policies are adopted in the area of authentication and monitoring, and wireless and its related personal devices are protected from attacks such as man-in-the-middle and listening effect despite the best protections

Dynamically Monitor

New attacks may arise because of the dynamism in technology, people and organisational policy. Several different events such as new or updated operating system, behaviour change in users, patrons and guest and their frequency of stay etc. identified so as to immediately prevent, or respond to and recover from, intentional or unintentional threat events.

Dynamic and real-time Respond

Once a threat event has taken place, it immediately notified the organisation. The response will include applying vulnerability remedies that best suites the threat, Device account deactivation, remote wipes (malware and viruses) or removal incident response plan. However, these responses are based on the nature of the risk or threat event that has presented itself

Dynamic and real-time recovery

This phase is made up of the initial response in an event of a threat. In the event that this happens the organisation must be able to fully recover. Also, backups (organisation) and device tracking based on appropriate trust model are recommended. Organisation and Personal devices should be back up either by targeted directories or the specific sandboxed environment in real-time. Employee back up of personal devices will be part of the Dynamic security program

Dynamic and real-time Assess and monitor

The most important part of a security framework is the Assess and monitoring phase. This phase of a Security Framework can be achieved through clustering. For example;

a. user and device clusters

b. Security clusters

c. Trust and reputation based clusters.

Nevertheless, depending on the user's nature which can be identified as either customer or visitor and their security risk levels, grouping the attack priority as High, Medium, Low and very Low will provide insufficient information to create an effective framework. Finally, the various clusters must be updated dynamically so different policies will serve different clusters for easy management.

2.2.2.3 Other Dynamic security frameworks

Some other approaches have also been used for Dynamic security measurements, authors like (Reinfelder & Weishäupl, 2016) used a Security Success Model where the data item in question is the smartphone security policy of an organisation. But this proposed security model lack dynamicity which could be used with a BYOD policy in place, it needs to show individual outcomes with the effects of organisational variable, including the usage of a smartphone(personal devices) and its security issues. It's should also be able to store information on individual and organisational concerns on security events and processes to know the security trend aiming as a feedback loop. Furthermore establishing and maintaining dynamic trust in mobile devices have been embarked on by many researchers in an attempt to solve it, the Trust project by (Marsh, 1994) was one of the first attempts to formalize trust in computer science, the model introduced the concept widely used by other researchers such as security context and its condition of trust which constitute their Computational Dynamic Trust Model for User Authorisation framework. Also, The mutual authentication model from (Choudhury, Kumar, Sain, Lim, & Hoon, 2011; Zhong, Bhargava, Lu, & Angin, 2015) is established on dynamism as an information trust database to monitor risks and its probability

of occurrence, this database is built using the behaviour of users whose actions change based on certain patterns over time.

Works by (Das & Islam, 2011) presented a new architecture The Dynamic Trust Computation Model for Secured Communication in Multi-agent Systems this operates directly by integrating parameters like user feedback credibility, user similarity and historical trust into a trust computation technique. Other models by (Matt, Morge, & Toni, 2010), who also use a trust computation method technique for Multi-agent Systems combine statistical information regarding the past user behaviour to predict the expected future user behaviour that could cause security difficulty. This trust models prove challenging because it does not consider "context" that is the particular situations affecting the value of trust, thereby it accurate representation for real-life situations is argued.

According to (Zhu, Lv, Yu, & Zuo, 2010), the process of tackling information security of a grid computing system is determined by user authorization, where it operates by specifying the access rights to resources using the Dynamic role-based access control model to determine the role, task and the environment of a particular user. The authorization decision is updated dynamically by a monitoring component keeping track of user attributes, service attributes and the environment. A very similar model for grid computing was also proposed by (Fan, Liu, Li, Wu, & Guo, 2012) this also emphases on the dynamic change of roles of services. Though these approaches consider "context" into trust computation, their application is also limited to specific domains. Some ideas from this work can help in the development of the BYOD dynamic security model.

2.3 Risk Assessment Methodology

A performing computer and its associated network application security measurement is a challenging task since the application in question can have a complicated architecture. However, this assignment should be like any other software examination methodology such as

the use of valuable tools, skills and knowledge which has been explaining in some of the earlier works by (Aagedal, et al., 2002).

In the following sub-sections, a detailed review of risk and vulnerability assessment standards such as CVSS and OWASP is presented followed by the mentioning of other tools used in risk assessment.

2.3.1 The Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) (Mell et al., 2007), serves as an open framework for sharing the characteristics and effects of IT vulnerabilities. In the USA the exact CVSS scores for publicly recognised vulnerabilities are communicated by The National Vulnerability Database (NVD) (National Institute of Standards and Technology (NIST), 2016, 2018) and the Federal Information Processing Standards (FIPS) 199 (NIST, 2004). They use the security categorisation with the NVD and CVSS metrics to attain influential scores that are personalised to each agency's environment. According to the author (Allodi & Massacci, 2014), CVSS is the most widely used scoring system by industries to identify high-risk vulnerabilities with maximum priority. Yet, there are still doubt about the explanation of the CVSS regarding its absolute attacks, therefore a good scientific methodology is needed to compare different policies to assess the most effective policy. Finally, CVSS considers it metrics and scores in the range of 0-10 according to specific characteristics, and it is explained using the score calculator and its metrics interpretation shown in table 2.5.

CVSS Metrics	Characteristics

Base	Represent the intrinsic characteristics of the Vulnerabilities Considering the Exploitability of the following parameters **Access Vector**: access needed for the vulnerability to be exploited. The further distance an attacker is to the host, the greater the vulnerability score. **Access Complexity**: The complexity of an attacker to exploit the vulnerability **Authentication**; measures the level of authentication needed for an attacker to exploit a vulnerability. **Impacts**: the effect of exploiting the vulnerability on the three security factors; (Confidentiality, Integrity and Availability)(FIRST, 2018; Gallon, 2011; Gallon & Bascou, 2011; Mell et al., 2007).
Temporal:	Characteristics are based on the vulnerability that changes over time but remains constant to the user environments, these include **Exploitability(E):** represent the present exploitability level of techniques or code **Remediation Level (RL):** quantify the Ongoing facilities for mending vulnerabilities. **Report Confidence (RC):** This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details(Gallon, 2011; Keramati, 2017).
Environmental:	represents the characteristics of a vulnerability that are significant and dependent on a particular user's environment (FIRST, 2018)

Table 2. 5 CVSS Metric interpretation

2.3.1.1 Measurement characteristics

- The Base metrics are captured in a screenshot in Figure 2.4 whiles Figure 2.5 represents the CVSS base scoring calculator employed in determining the base score of the vulnerability below.

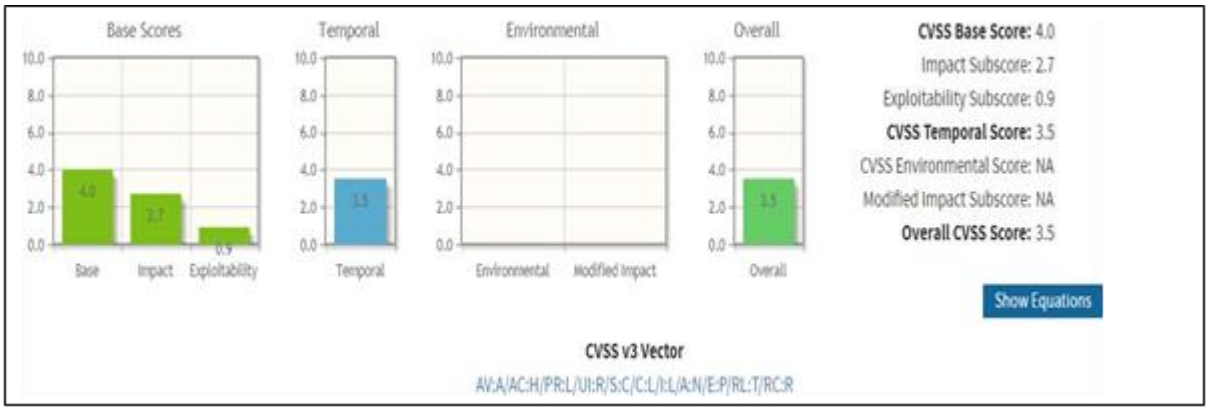

Figure 2. 4 CVSS Base score calculator vulnerability(CVE-2016-0051)

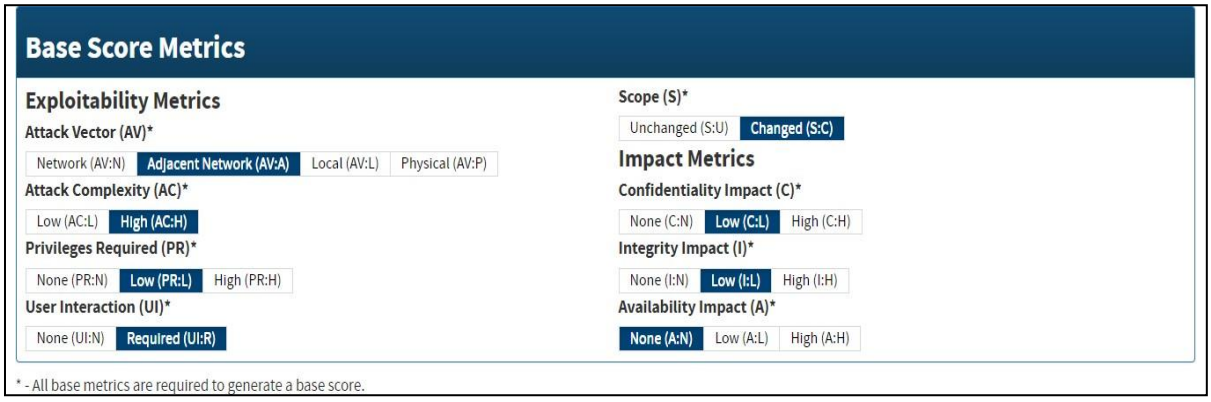

Figure 2. 5 CVSS base score metrics interpretation

- Environmental Metrics

shown in Figure 2.6 representing the CVSS environmental score calculator and Figure 2.7 the CVSS environmental metrics interpretations.

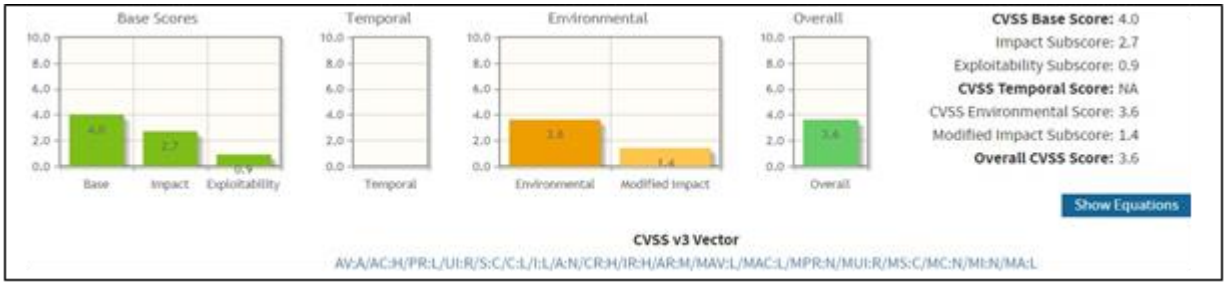

Figure 2. 6 CVSS environmental score calculator vulnerability (CVE-2016-0051)

Figure 2. 7 CVSS environmental metrics interpretation.

- Temporal Metrics

Temporal score calculator is shown in Figure 2. 8 whiles Figure 2. 9 shows the Temporal score interpretation.

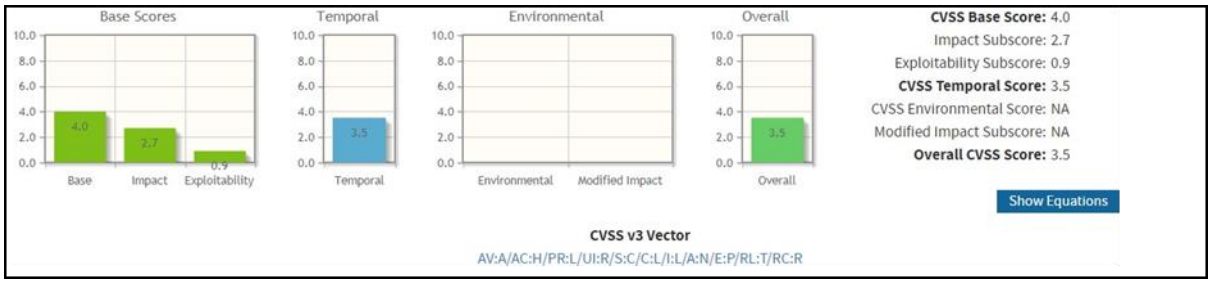

Figure 2. 8 Temporal score calculator vulnerability (CVE-2016-0051)

Figure 2. 9 CVSS Temporal metrics interpretation

However using the CVSS to score the security risk of a BYOD program have some deficiency, this is because only it's Base Score Group of Vulnerabilities is calculated by the CVSS calculator, leading to improper risk evaluation (Das & Islam, 2011.). Thus, systems vulnerabilities with its related situation are essential in the measurement calculation so as to obtain the correct score.

2.3.2 Open Web Application Security Project (OWASP)

OWASP risk rating methodology is said to be a straightforward technique used in calculating and scoring of an associated risk within a computer application or software (Open Web Application Security Project, 2018). The process of rating risk and its related impact is by gathering factors regarding the participating threat agent. These include the skillfulness of an attacker, the motivation, prospect, the scope of the attacker domain, and its vulnerability factors. The OWASP methodology quantifies risk in the scale of low, medium and high.

2.3.2.1 Definitions for OWASP Risk Rating

From the definition of OWASP, risk can is expressed as Risk = Likelihood * Impact

A. The Likelihood = Threat agent factor and Vulnerability factor.

Also, the definition from authors like (Rao & Pant) computes likelihood as the possibility of vulnerabilities being exploited by an attacker.

The two tables 2.6- 2.7, below explains the factors associated with the Likelihood calculation

Threat Factors	Definition
Skill level	This shows by what means is the threat agents technically skilled.

Motive	How motivated is the group of threat agents to find and exploit this vulnerability?
Opportunity	What means and chances are needed for this group of threat agents to find and exploit this vulnerability?
Size	How important is this group of threat agents?

Table 2. 6 Threat factors

Vulnerability Factors	Definition
Ease of discovery	How simple is it for this group of threat agents to uncover this vulnerability?
Ease of exploit	How simple is it for this category of threat agents to exploit this vulnerability in reality?
Awareness	In what way is this vulnerability known to this group of threat agents?
Intrusion detection	In what way possible is an exploit to be discovered?

Table 2. 7 Vulnerability factors

B. The Impact = Technical factors and Business factors

Again (Rao & Pant; OWASP, 2018) defines the Impact of an attack as the calculation of estimation on numerous factors that shows a successful attack on an application. Certain institutions have an asset catalogue and an impact reference guide to formalize the potential harm. The two tables 2.8 and 2.9 below explains the factors associated with the impact calculation.

Technical Factors	Definition
Loss of confidentiality	how sensitive is the data?

Loss of integrity	how much of the data can be damaged?
Loss of accountability	are threat agents activities traceable to a personality?
Loss of availability	how critical is this service?

Table 2. 8 Techincal impact factor.

Business factors	Definition
Financial damage	Not as much cost to fix the vulnerability?
Reputation damage	loss of important accounts?
Non-compliance	are threat agents activities able to be seen by an individual
Privacy violation:	how much personal info can be exposed?
Non-compliance:	how much exposure does non-compliance introduce? high-profile violation?

Table 2. 9 Business Impact Factor

The Likelihood and Impact Levels are rated as in table 2.11, this is to show the severity level

0 to <3 LOW
3 to <6 MEDIUM
6 to 9 HIGH

Table 2. 10 Rating of Severity level

2.4 Information Security Risk Management

Information Security Management (ISM) can be said to be a strategy that allows information technology administrators to protect their Information and Communications Technology (ICT) against different risks, vulnerabilities and threats. Hence it is vital for organisations to have a security standard with which they will manage their information risk asset, that is where an Information Security Management System Standards (ISMS) come into play with its

policies and procedures that can be implemented by an organisation to guarantee security requirements (confidentiality, availability and integrity) for its information resources from threat and vulnerabilities(Azuwa, Ahmad, Sahib, & Shamsuddin, 2012; Brodin, 2015). The ISO/IEC 27000 from (International Organization for Standardization, 2016) category is the most accepted and generally used ISMS, but the specific standard that is of relevance in BYOD security strategy is included in the ISO/IEC 27004 Information security measurements and ISO/IEC 27005 Information security risk management.

Table 2.11 below defines (ISMS) standard ISO/IEC 27000 with its categories as using definitions by (Almorsy, Grundy, & Ibrahim, 2011; International Organization for Standardization, 2016).

ISO/IEC standard	Purpose
ISO/IEC 27001 Information security management systems – Requirements	This provides the requirement inadequately executing the information security management systems (ISMS) , including information security risks within an organization's overall risks
ISO/IEC 27004 Information security measurements	It provides a framework letting an evaluation of ISMS efficiency to be measured and assessed in accordance with ISO/IEC 27001
ISO/IEC 27005 Information security risk management	Provides guidance on executing a process-oriented risk management method to help inadequately implement and achieve the information security risk management requirements of ISO/IEC 27001

Table 2. 11 ISO/IEC standards which are significate in BYOD security

Information security is the process where confidentiality, integrity and availability of sensitive information is observed, meaning sensitive information is protected from any alteration,

interference, destruction and scrutiny, observing security requirement for a BYOD system can best be managed if organisation and its employee (users) pays attention to their network in a BYOD situation. Authors in (Donald, 2004) define Framework as an outline structure supporting a system or approach, therefore using an information security framework serve as the outline for constructing an information security programme with an advantage of improving system recovery, encryption, and application security and to control risk and reduce vulnerabilities (Donald, 2004; Granneman, 2013).

The subsequent sub-sections show a detailed review of ICT security frameworks with its attributes. In addition, different security requirements are outlined in Section 2.4.1, while previous works on security attributes are outlined in Section 2.4.2.

2.4.1 Information and Telecommunication Security Framework

In the following sub-sections, a thorough review of ICT security outlines is presented in addition to the different types of security attributes.

2.4.1.1 Security Attributes

In a book by (Stallings, 1995), it describes network security as the most essential part in the information security risk management process since it's accountable for safeguarding entirely the flow of information in network computers their related devices, users and programs. Therefore designing and building a security risk metrics requires an understanding of the different standard, measures and model methods similarly used, this has been review through literature and discussed therein. The next portion clarifies these security attributes in relation to BYOD Risk, Threat and Vulnerabilities.

The concerns of any Information Technology Security (IT Security) according to SANS (Deck, 2018) is the process of applying measures and techniques to steadily protect and defend information (organisation and personal data) using any kind of technology develop to build, save and use from any unauthorized access, misapplication, failures, alteration, destruction, or wrongful disclosure, in so doing defending its security goal of confidentiality, integrity, Non-

repudiation and Authorisation and availability (Palmaers, 2013). The international standard (ISO/IEC 27002, 2005). also describes information security as the protection of confidentiality, integrity and availability of information, this could be in any form be it electronic or paper transcribe, other security goals such as authenticity, accountability, non-repudiation, and reliability are also involved. Similarly, description by authors (Arellano, 2015; IEC, 2018) on BYOD security goals is discussed beginning with Confidentiality, Integrity and Authentication (CIA) which is the generally accepted meaning of security.

2.4.1.2 Security Requirement Outline

- Confidentiality is the protection of information against disclosure to unauthorized groups.
- Integrity is the prevention of alteration of the information by an unauthorized group.
- Availability is the capability to offer information to authorized groups when necessary.
- Non-repudiation is the prevention of denial of a transaction by an interested individual.
- Access Control is the selective controls of access to a resource.
- Authentication is the technique of confirming the identity of a user or process.
- Authorization is an act of assigning permission to a specific user or process.

2.4.2 Goal-Focused Security requirements for a BYOD service

Authors like (Miller, Voas, & Hurlburt, 2012); Donald, 2004; Ketel & Shumate, 2015; Armando, Costa, Merlo, Verderame, & Wrona, 2016; Friedman, 2008) express security as an everyday thing thereby effecting a continuous process made up of the constant collaboration amongst policies execution and technical measures. In measuring the security goals of any introduce technology, authors (Arellano, 2015; International Organization for Standardization, 2016) examined starting with the traditional “CIA” (confidentiality, integrity and authentication) security goals, before specific arrangement such as BYOD can be examined with authenticity, accountability and non-repudiation.

The following sub-sections define the security goals which are relevant in measuring any BYOD technology.

2.4.2.1 Ensuring Confidentiality

Ensuring confidentiality relates to sensitive organisation data which is normally saved on users mobile devices. (Donald, 2004; Niehaves et al.,2017; Prashant Kumar Gajar, 2013). In (Bello Garba et al., 2015; Dawson, 2015), data is protected by being prevented from loss or leakages using encryption, implementing a user service agreement where personal devices are shut down remotely by IT administrators in the cases of lost or stolen devices and finally, authors (Morrow, 2012) suggested user education and awareness.

2.4.2.2 Integrity Checks during data communication

In (Y. Wang et al., 2014) Integrity goals is achieve when there are detection and prevention of any form of modification to data during transfer, previous work by (Morrow, 2012) in relation to the risk of Data integrity exploitation is the misuse of a policy or an Access control violation, Insider threat exploited or storing an organization's data to an unsecured location. Likewise authors(Jain & Shanbhag, 2012); Bello Garba et al., 2015) methods of ensuring confidentiality such as Regular User education and awareness, encryption of corporate data and BYOD devices restriction**,** also works for data integrity as well. Furthermore Mobile Virtual Private Network (VPN) and application controls must be used to hold information in transfer in its exact form throughout the communication period between BYOD devices and organisational system (Jain & Shanbhag, 2012)

2.4.1.3 Maintaining Availability

(Donald, 2004) defines maintaining availability as guaranteeing access to data when needed. this includes offering access to information to employees outside organisational control. limiting availability means a decrease in productivity and proficiency in ICT practices. Hence for preserve availability; Device data must be backup frequently either remotely via a wireless connection or by means of cable services. Desktop virtualisation can be employed to implement

applications and data storage, instead of on personal devices (Bello Garba et al., 2015; Dery & MacCormick, 2012).

2.4.1.4 Data Authentication

Data Authentication is the identification and verification of BYOD users and its devices .the authentication of BYOD users includes using factors such as username and passwords. The use of Digital Signature algorithm and a trusted Digital Certificates to sign in between BYOD devices and organisational environment upholds authentication. When there are weakness or flaws in the authentication process from the SESSION_ID and weak passwords, due to only one timed authentication process or identity impersonation, An attack is likely to happen (Wichers, 2013). A situation of broken authentication and session management is said to have occurred when; there is rogue mobile device access (Brodin, 2015), usage of a guessable session_ID, unable to detect frequent guessing trials while there is a mechanism in place, weak cryptography, limitation of HTTP, Insecure session handling methods and, weakness in the session management technique (Huluka & Popov, 2012). This difficulty can be overcome with a solution such as Mutual authentication procedure should be used for verification from both endpoints, If possible choose not to be connected to internet location services, a two-way authentication process and use of location services as suggested by (Huluka & Popov, 2012; Yuan, Yang, He, & Simpkins, 2016).

2.4.1.5 Securing Non-repudiation to Data

Non-repudiation is to accept acknowledgement of data from a third party without dispute over its content. It can also discourage a receiver from repudiating data it received(Donald, 2004). Noted that non-repudiation endeavours are made to keep a comprehensive transmission of data from being denied.

2.4.1.6 Access Control and Authorisation Regulation

An access control policy according to (Bello Garba et al., 2015) is meant to outline the practices and measures used in protecting computer and its network devices from unauthorised

admission. Garba et al suggested managing access control by changing the password on periodically, any ideal device should be logout automatically at a stipulated time(example 10minutes) without a repetition of the immediate password, limit the number of times failed password is repeated on organisational emails and applications. A dynamic access control system is created using information gathered on user devices behaviours (Koh, Oh, & Im, 2014). Therefore Broken authentication and session management occurs when there are weaknesses or flaws in the authentication and authorisation process, such as SESSION_ID and weak password, in a situation where there's only one timed authentication process stolen identity can be an attacking tool. There is also the issue of threat caused by insecure interface and APIs. Organisations currently send data via the Application Programming Interfaces (APIs) this is so because, when data is sent to a mobile device by an API it means the data does not need to reside on the device but instead it is retrieved by a mobile application running on the device (Wichers, 2013)**.** In a circumstance when there are flaws with the security of these interfaces, attackers can invade.

Furthermore, the general security threats of BYOD system include data loss and leakages, where the user's willingly authorised or unwillingly shares data with an unauthorized user, application or a third party this can jeopardize an organisations confidentiality and integrity.

Non-repudiation is said to be violated when Policies are misuse. That is the conflict between comfort, flexibility and productivity against security. A study by Cisco reveals 56% of workers don't mind going against their boss in the performance of their duties (Bradley, Loucks, Macaulay, Medcalf, & Buckalew, 2012).

2.4.2 Why Security Requirement?

Working on securing a system is a continuous process, this also applies to BYOD systems, therefore, it's better for the security monitors to take into consideration the security requirement (Lipner, 2004). There is a possibility of an amendment to the requirement during the

development stages, but in explaining the security requirements in the foundation stages prevent any requirement from being ignored. According to Firesmith (Donald, 2004).Thus, cases regarding loss in security requirements specifications in software development fall within three categories;

(i) Security is muted completely. That is, security is omitted at the development stages.

(ii) Plainly indicate unclear security goals. This point means a required security requirement is difficult to assess as a result of it being unstructured.

(iii) Generally handles used security processes as architectural limitations, because security requirement is induced very early on the architectural decision causing unsuitable security mechanisms.

Usually, security requirements are considered under non-functional requirements which represent how a system performs instead of what it achieves as a functional requirement, but Information security cannot be merely expressed by non-functional requirements, given that security objectives often inspire new functionality, for example, intrusion detection and access controls will also require functional requirements(Savola, 2007).

2.4.2.1 Identification of BYOD Security Objective

The first security objective to the service of a BYOD system is the physical defence of the mobile device used. Implying the threat of malicious application and the threat of unreliable and unguarded wireless communication network are most likely to be exploited by attackers. Importantly for BYOD to be successful there should be readily available internet which involves nodes and host systems on a network, and so Denial-of-service attack (DOS) could also become the main security threat towards BYOD operations. Denial-of-service (DoS) attacks occur when an attacker floods the resources (system, servers or network) of the authorised node connected to the internet with traffic rending it inaccessible. There is also the DoS activity where fabricated messages are sent for unauthorized nodes by an authorised node

via the flooding attack (Savola, 2007). Finally, since BYOD service is a process of a wireless communication system where users appreciate the safety of their information and resources from attacks and damage a vulnerability prediction score is crucial.

2.4.2.2 Risk

Authors such as (Singh et al., 2004) (Palmaers, 2013) reveals risk as the damage incurred from some intended or accidental occurrence and could negatively impact the information security process. Furthermore (Aven & Renn, 2009) define risk as occurrences where the result is unknown. Mathematically (Fernández-Muñiz, Montes-Peón, & José Vázquez-Ordás, 2012), express information security risk assessment as a representation of the attack impact and the likelihood of an information asset being the attack. This is express below

$$Risk = Attack\ likelihood \times Impact$$

Additionally, the impact of an information resource occurrence is equivalent to the output of asset vulnerability and asset value, represented mathematically as:

$$Risk = Attack\ Likehood\ \times Asset\ Value\ \times Vulnerability$$

(Vazquez, 2014) uses risk to signifies threat (likelihood of an Attack), asset value and Vulnerability. Amongst the three asset value (device, confidential data) is the simplest to score.whilst vulnerability and asset value are said to be the most essential factors considered in determining total security risk score.

2.4.2.3 Vulnerability

According to The International Organization for Standardization definition vulnerabilities are defects or weakness in system security procedures, design or implementation of internal controls that could be exploited (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy (International Organization for Standardization, 2016; ISO/IEC, 2018; (Azuwa et al., 2012). In principle, vulnerabilities occur

in organisations resources, which act as a gateway to attackers towards their computer systems(Mell et al., 2007). Author (Weidman, 2014) defines vulnerability as a weakness in a system (application and service) which lets an attacker evade security constraints and manoeuvre thru systems in a manner the developer never anticipated. Moreover, there is an increase in the number of services provided by computing devices (smartphones, Laptops and it related mobile devices) usage hence an increment in vulnerabilities as well (Viehböck, 2011) US-CERT, 2012.).

The factor of user Vulnerability as discussed by (Eskins & Sanders, 2011) illustrates how users are often left out of the BYOD security measurement design, for the reason of wrong perception based on security, privacy, usability and trust. Even with a familiar device. The BYOD user plays an important role in a BYOD induced network, but the traditional methods of cybersecurity evaluation seem to ignore the part played by the user in the system, though by design users have an influence on the cyber systems, they are not thoroughly considered by the organisation as it is mainly the network and its physical devices such as administration security policies, software and firewalls that take part in the evaluation. Then again humans (users) in BYOD evaluation situations are either clearly ignored or considered as a standalone system with static properties who will carry on their specified task complying with the organisation's administrative security policies and procedure. But, this is not always true as users are dynamic and their practice depends on usability, motivation, conditions of the system and user acceptability, etc. failure for IT security managers to recognise this can result in Vulnerabilities both to the organisation and the User (Human Participant).

2.4.2.4 Threat

The NIST Special Publication (SP) 800-30 (National Institute of Standards and Technology (NIST), 2016) defines threats as a series of occurrences within which a natural or intelligent invader may compromise the confidentiality, integrity, or availability of security system in an

illicit manner to cause harm (NIST, 2018). In the discipline of computer security, the threat is the likelihood of risk to computer resources with the intention of exploiting a vulnerability to breach security and cause harm (MSRC, 2017).

2.5 Metrics

Measurement is a process used in system identification for an environment with an extreme level of quantification accuracy. Lord Kelvin is quoted saying, “When you can measure what you are speaking about and express it in numbers, you know something about it”(C. Wang & Wulf, 1997). The development of security metrics by organisations is a very challenging exercise as noted on the science and security bulletin (Sanders & Nicol, 2018). Categorising the processes involved in design, development, evaluation, and deployment of security metrics is a tough challenge in cybersecurity, particularly in the procedures used in identifying what should be covered in measuring a specific set of security policies and quantifying them efficiently. Authors Vaughn, Henning, & Siraj, 2003; Villarrubia, Fernández-Medina, & Piattini, 2017) uses training and monitoring measures for its user security metrics. However, an effective way to tackle the security threats of a BYOD organisations network is to categorise the security metrics that quantify the security configuration characteristics dynamically. Saydjari defines metric as “a system of related measures enabling quantification of some characteristic” and with the measure as “a dimension compared against a standard.” (Saydjari, 2006). To help simplify the problem, the National Institute of Standards and Technology (NIST, 2016) through their security metrics manual on information technology system perceived that, security metrics must bring forth information that is quantified in keeping track of a system's performance, measures a repetitive activity and finally readily available data(O’Brien et al., 2015). Likewise, it should be measurable by using suitable procedures in collecting data of occurrences onto a pre-defined scale to represent appropriately the assign security requirements that meet an organisation’s environment. This work falls under the concept of situational awareness which gives a whole approach to understanding threat and

vulnerability analysis using predictive analytics to perform an evaluation of the current security situation and projects future security position. Similarly. situations awareness as defined by (Endsley, 1995; Dacier et al., 1996; NPFC, 1995) states that "the perception of an element in the environment with a volume of time and space, and the comprehension of their meaning shows the projection of their status in the near future".

Coming from the perspective of a defender in security analysis and auditing, one will have to be able to enforce Confidentiality, Integrity, and Availability security policies in a BYOD environment without compromising the performance of its network. However, having an attacker mindset is very effective because an attacker is inspired to attain a set goal continuously. Thus, investigations with such a background are more practical, as data can be gathered from simulated attacks (Jonsson & Olovsson, 1997).

NIST describes metrics as implementations made by organisations to help in policy-making through its data collection, evaluation, and reporting of significate performance-related data. Also, the author (Pendleton, Garcia-Lebron, Cho, & Xu, 2016) considers metrics as allocating value to an objective, many researchers and organisations have attempted to standardise security metrics, authors such as(Jansen,2010; Pendleton et al., 2016) explains security metrics on how a designated systems security objectives are met based on its quantitative attributes on certain scales such as nominal, interval, and ordinal. With the later moving on to subdivide it into sub-metrics namely Vulnerability, attack, defence, and situation respectively.

Basically, Metrics gives the organisation and their users (employee) a technique (quantitative or qualitative measurement) they can use in sorting and calculation their threat and vulnerability so that risk pose on information resources can be ranked quantitatively and qualitatively (NIST, 2016). Qualitative metrics define the evaluation process resulting in a non-numerical value which is difficult to analyse. Example ("high," "medium," and "low"), whiles

Quantitative is simple to understand and preferably meet a specific situation, It appropriate for decision making because it usually represented in numerical form.

Measurement-based security metrics by (Ramos, Lazar, Filho, & Rodrigues, 2017) is created from the examination of a system model where several parameters are entered (input). For instance, data from an Intrusion Detection System device (IDS), and then use suitable procedures in collecting the data of occurrences onto a pre-defined scale to represent appropriately the assign security requirements that meet an organisation's environment. (Almasizadeh & Azgomi, 2013) model-based security measures a repetitive activity and finally produces readily available mathematical output. Also, Analytical metrics by (Böhme & Freiling, 2008) which is a formal mathematical model is used as a Quantitative ranking metrics incorporating the human (User) in the policy of a workable BYOD security evaluation metrics. This is essential when it comes to balancing security and usability. A report from IBM's 2014 Cyber Security Intelligence Index (IBM, 2018.) indicates the anticipation from computer security officers and their designers about users mostly conforming to security rules and policies, as they are the weakest security link in an information security environment. The report thereby concluded on humans (user) errors such as default or weak passwords usage, loss of mobile devices, continuous opening of unsafe attachments or URL and deliberate by-passing security policies and procedure influences being 95% of all information security incidents.

According to (Ketel & Shumate, 2015; Inc., 2018), in recent times the use of personal devices for official duties both on-site and off-site has increased tremendously and so are its related security concerns. Yet, usable security measurements continue to be the greatest factor in a BYOD environment with security risk and vulnerabilities increasing each day. Consequently, a full security estimation should be considered. (Eskins & Sanders, 2011) also discussed how users are often being left out of the BYOD security measurement metrics design, for the reason

of the wrong perception related to security and privacy, usability and trust. Even with a familiar device. The BYOD user plays an important role in a BYOD induced network, but the traditional methods of cybersecurity evaluation seems to ignore the part played by the user in the system, though by design users have influence on the cyber systems they are not thoroughly considered by the organisation as it is mainly the network and its physical devices such as administration security policies, software's and firewalls that take part in the evaluation . Then again humans (users) in BYOD evaluation situations are either clearly ignored or considered as a standalone system with static properties who will carry on their specified task complying with the organisation's administrative security policies and procedure. But, this is not always true as users are dynamic and their practice depends on usability, motivation, conditions of the system and user acceptability, etc. failure for IT security managers to recognise this can result in Vulnerabilities both to the organisation and the User (Human Participant).

Authors in (IEC, 2016) make user security evaluation on a computing system to form part of the quantitative analysis (Measurement) step, for this to be productive the network of the organisation needs to be in the public space (internet) for the authorised users to be able to access it always. (ISO, 2015) categories the security metrics to indicate the level of security on Efficiency, Trustfulness, Accessibility, Confidentiality, Integrity, Availability and Accountability. Organizational Metrics as depicted by Authors (Ralston, Graham, & Hieb, 2007) in their Supervisory Control and Data Acquisition (SCADA) control systems to explain this form of metrics. Takes part in high-level security marking, for instance, the decision on the type of security initiatives available on an organisations data and their strength.

Finally, Threats agent's give rise to threats, which might exploit vulnerabilities to violate information security properties such as confidentiality, integrity, availability, etc. Security controls implement countermeasures to defend information technology systems (BYOD) by mitigating threats or plugging vulnerabilities, or both using policies, algorithms and metrics.

Hence achieving a precise measurement on the quality of the system results in a trustworthy BYOD realisation. This has been shown in Figure 2.11 below.

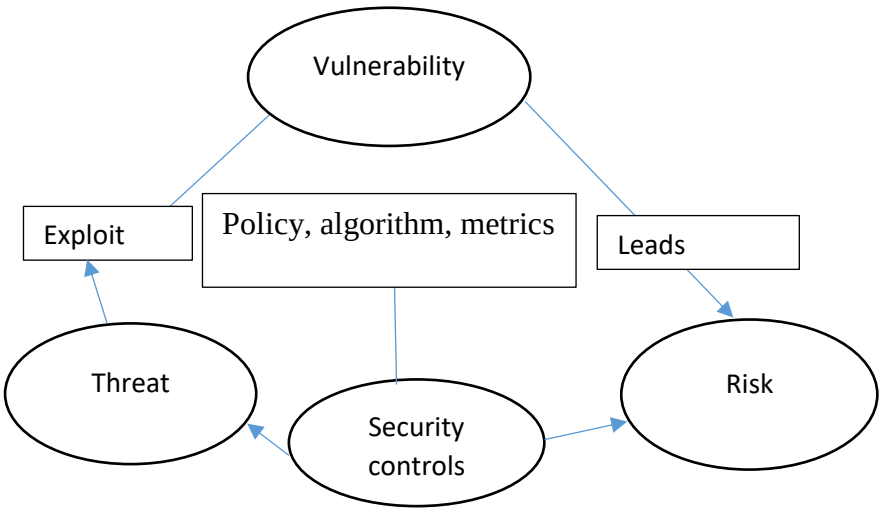

Figure 2. 11 Connections amongst Threats, vulnerabilities, risks and security controls

2.5.1 Categories of Metrics

This explains the various forms of Host-based Security Metrics used in the information system security measurement of an organisations network.

2.5.2 Host-based Security Metrics

These are metrics used to measure the security level of distinct hosts in a network. The host-based security metrics can be divided into two categories "with probability" and "without probability". This is done for the reason that: (i) in, instances locating a probability value for an attack happen to be infeasible, and (ii) Certain analysis and optimisation can be performed with or without probability concerns as explained in (Roy, Kim, & Trivedi, 2012).

2.5.2.1 With Probabilistic value

Publication on the measurement of belief by (Suppes, 1979) quantifies probability in the function of between 0 and 1. Probability Theory concepts have been adopted and used broadly

by disciplines such as artificial intelligence, machine learning and computer science etc.To measure the likelihood of prospective clustered attacks. Publication by (Denuit, Dhaene, Goovaerts, & Kaa, 2005) uses probability theory in modelling risk, this is based on the possible turn of event to take place. (Li & Wang, 2019) uses a probabilistic reasoning algorithm to develop precise navigation and integrated information system from existed wireless local area networks (WLAN) signals.

Conversely, the security metrics can also be measured based on their probability values, these include probability security metric (Wang, Islam, Long, Singhal, & Jajodia, 2008). Authors (J. A. Wang, Wang, Guo, & Xia, 2009) uses a Probabilistic metric known as the Attack Graph-Based Probabilistic metric, this combines numerous vulnerabilities from different network framework, the VEA_bility by (Tupper & Zincir-Heywood, 2008; McQueen et al., 2005)(Premaratne, Samarabandu, Sidhu, Beresh, & Tan, 2008) also uses the percentage of hosts with vulnerability on a network to measure its metrics.

2.5.2.2 Without Probability Value

This metric quantifies how fast BYOD induce network is likely to be compromised and the attractive of its different network topology to exploit, it measures the level of risk use in managing a system in an arranged environment. examples include State-Time Estimation Algorithms (STEA), Mean Time to Compromise(MTTC) respectively. The application of both the period based metrics can be said to be static but applying it in combination with a topological situation brings out the dynamic optimisation.

The Return on Attack metrics (Cremonini & Martini, 2005) is used to define the expected profit of an attacker upon a successful attack above the losses he suffers due to the security-measure implemented by the target. Hence for an organisation to calculate the efficiency of a security-measure specific type of intrusion attempts in opposed.

2.6 Intrusion Detection and Vulnerability Assessment Security Systems

Information and its communication mode continue to be an important business asset in all organizations. Therefore, it must be kept as safe as any other valuable asset. This can be said to be the objective of any information security program, not only in providing protection for its business information assets but for the protection of the business users as a whole.

The Internet and its computer networks are subjected to a rising amount of security threats on a daily basis, with different forms of attack appearing frequently. Yet, building a flexible and adaptive security-oriented methodology is still a challenge. The use of hi-tech tools for web services and remote access in-network communities comes with its own network security concerns, also these tools are needed to deliver a precise and consistent defence against malicious attack. That is where intrusion detection comes into play.

Network intrusion detection and prevention systems(NIDP) can be divided into two definite groups, namely; knowledge-based system (Signature-Based Detection) and Behaviour-based system (anomaly-based detection) (Alessandri, 2001). The knowledge-based system act as an audit trail system as it uses the data from system signatures to determine the known attack and or clearly defined outcome of interest. It then moves on further to compare the result with define attacks and vulnerabilities, a positive match indicates an intrusion. These type of intrusion detection tool are the most popular on the market and believe to be fairly accurate because it produces a low rate of false positives(Venayagamoorthy, Sharma, Gautam, & Ahmadi, 2016). However, it is constrained in the detection of unknown attacks that attacks with no known signature. OSSEC (OSSEC, 2019) is an example of knowledge-based intrusion detection systems, which is an open-source, supporting operating systems such as OpenBSD, Macintosh, Window and Solaris. Alternatively, Behaviour-based detectors go-ahead to label all unrecognised signatures as dangerous. To run, these systems compare the detected behaviour of the system against a model of expected behaviour. Anything different from the

standard system behaviour is labelled an intrusion(Jha, Sheyner, & Wing, 2002). Behaviour-based systems are thought to be complete, as it is able to catch all attacks. But, accuracy is said to be minimum. The NIDP approach is not always a perfect answer to system security as it is difficult to implement one that fit an organisation complete system requirement. Secondly, a highly functional intrusion detection system has the potential of sounding false alarms if it is not well studied to produce what is considered standard behaviour. Therefore an intrusion detection system can create an alarm only before the reason for an alarm occurs. In many lots of situations, this could by this instance be late.

In the following sub-sections, a detailed review of NIDP is provided. In addition, the architecture is outlined in Section 2.6.1, followed by computing vulnerability assessment methods in Section 2.6.2.

2.6.1 Snort NIDP Architecture

Snort is an open-source is a network intrusion detection and prevention (NIDP) developed on a rule-based expression joining signature, protocol and anomaly-based identification methods to identify hostile traffic. It was developed by Martin Roesch in 1998 (Roesch, Green, Sourcefire, Inc., & Cisco, 1998). Snort can be configured into a Network Intrusion Detection System (NIDS), this analyses the inward and outward traffic against a set of policies to expose any invasion in the network. Snort-based NIDS (S-NIDS) is designed to safeguard the networks from any form of likely intrusions and attacks, Snort examines packet header and executes protocol analysis. It also inspects a series of network threats by means of a content/signature pairing algorithms and records the traffic on the network by triggering an alarm against malicious events (Liao, Chun-Hung, Ying-Chih, & Kuang-Yuan, 2013). The architecture of a typical Snort NIDS involving the main parts; packet decoder, pre-processor, detection engine, logging and alerting system, and output modules are presented the Figure 2.10 below.

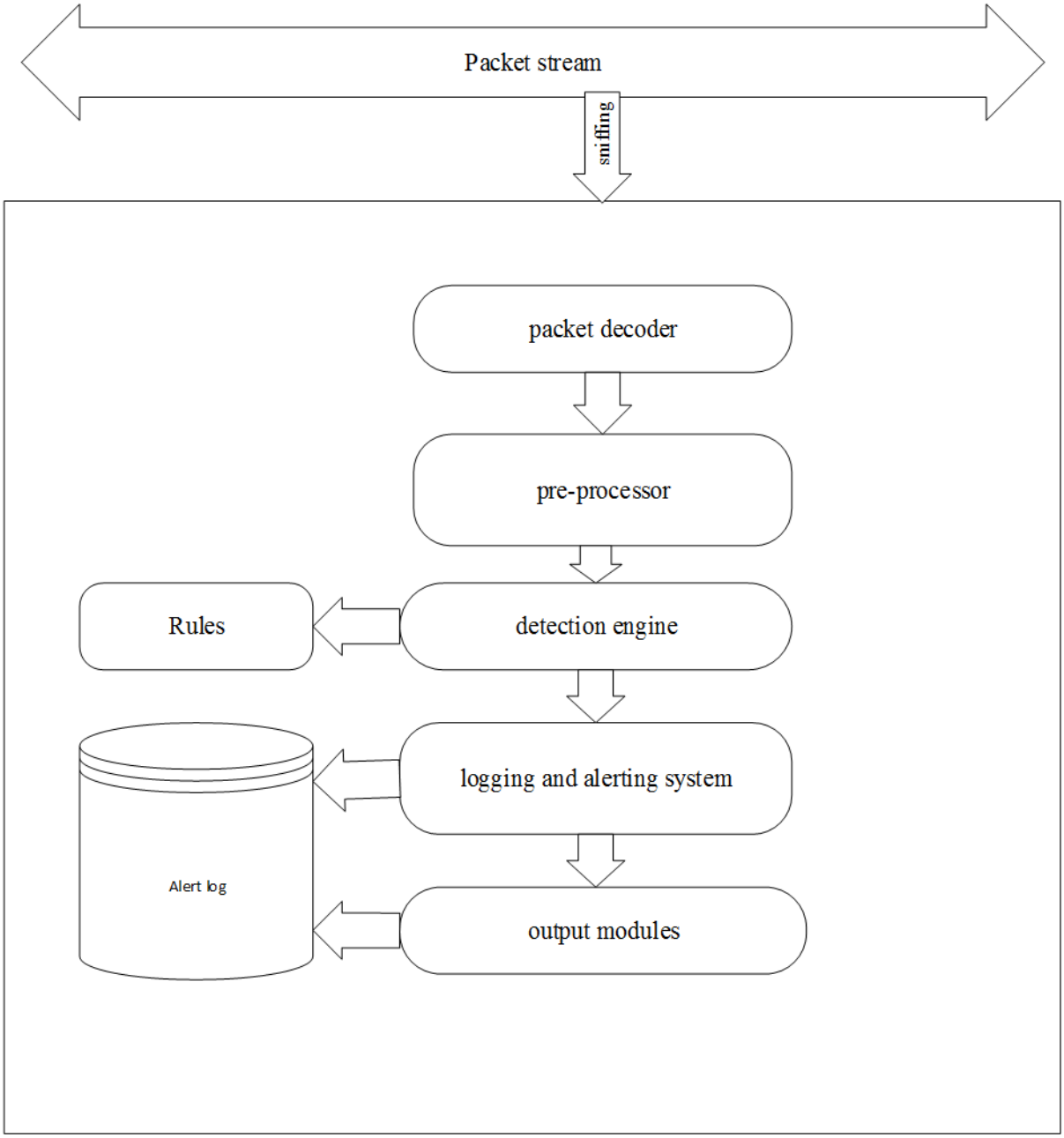

Figure 2. 10 The snort architecture

In a packet sniffing situation, the Snort gathers information from the network and presents it in its raw form on a monitor in a TCP dump mode. Its packet acquisition actually depends on libpcap and winpcap libraries, libpcap and winpcap are particular policies used in collecting traffic from the network. Packet acquisition scrutinises the packet incoming time and computes its total duration, it also checks the interface connection type on which the packet was captured.

When a packet stream goes around the network, the NIDS listens in then seizes the packets. The packet decoder takes packets from various network interfaces, for instance, point-to-point protocol, Ethernet, and Serial Link Internet Protocol, Token, Ring, Bus, etc and afterwards sort out the entire packets on behalf of pre-processing and detection engines. Snort assess the traffic on each link layer and when in doubt about any malicious packet, it starts to create a line up for that traffic (Karim, Vien, Tuan Anh Le, & Mapp, 2017). This process is a straightforward one specifically for an Ethernet link. The pre-processing perform numerous functions like analysing protocols and their activities for abnormality-based detection, the most important pre-processors inside a Snort are packet Defragmentation, Stateful Inspection session and application layer. The pre-processor is essentially a program operated to control the raw packets and limits them against abnormality-based behaviour, for example, HTTP plug-in administers the application at the time of traffic flow and also prevents processing undesirable traffic that can initiate an overload taking place in the network.

The detection engine is an essential part of Snort, which employs different times for different spans of packets, therefore time is a necessity. The main goal of the detection engine is to obtain data or packets from the pre-processor and harmonises the configuration of the collected packet using the database of a specified set of rules. When the configuration harmonises, it subsequently generates an alarm against the malicious packet then ceases to work on that particular packet. Else, Snort handles the packet as regular traffic and does not produce any alarm against it. The alerts or logs are generated subject to the prescribed rule, for example, if the rule is of little significance it will result in a low-level alarm. In the NIDP system mode, the greater the traffic level that Snort holds on to, the greater the number of packets abandon (Alserhani, et al., 2009).

2.6.2 Vulnerability Assessment

Recent studies on Vulnerability assessment define the process as a systematic technique of identifying security concerns (i.e., vulnerabilities) in a computing device, network, and their related communication infrastructures (Harrell, Patton, Chen, & Samtani, 2018). In definition related to this write-up, Vulnerability Assessment can be said to be the use of security test scanners to identify vulnerabilities, threat and its related risks posed, and the result of the scanners are presented in a vulnerability assessment report.

Currently, vendors such as Tenable (Tenable, 2019), Portswigger (PortSwiggers, 2018), and others offer organisations a variety of automated vulnerability assessment tools to support the position of their cybersecurity awareness through scanning and reporting of vulnerability status. Whereas competencies might differ between vendors, all vulnerability assessment tools are basically made up of two very functionalities that are scanning and reporting. The definition of each component, according to (Harrell, Patton, Chen, & Samtani, 2018) is presented below:
A **Scanner** is a software used to examine the architecture of a network, reports on the detected vulnerabilities, and in some cases give instructions on remediating the error

The **Report** presents a summary interpretation of the systems and their corresponding findings. Information on IP address, risk rankings, vulnerability description, and solutions are contained within the reports. Figure 2.13, below gives a representation of a network vulnerability assessment definitions

Figure 2. 11 Vulnerability scanning and Reporting representation.

The different type of known vulnerability assessment scans types include:

- Network-based scans; work to recognise possible network security attacks. This form of scan is able to detect weak systems on wired and wireless networks. (Tenable, 2019)
- Wireless network scans; usually scans an organization's Wi-Fi networks emphasising particularly on point of attack accessible to the wireless network infrastructure. (Kavado, 2019)
- Application scans; this is used to scan websites so as to detect known software vulnerabilities and any weak configurations within a network or web applications. (OWASP, 2018; Sanctum Inc, 2018)
- Database scans; is used to recognise the weak points in a database for the prevention of malicious attacks, for example, SQL injection attacks (Kaiyu, Xiao, Wei, & Dequan, 2019).

Below is a description of the universally accepted vulnerability assessment tools

2.6.2.1 Nexpose

This is said to be the most efficient vulnerability management tool used in giving consistent and timely results of findings according to (Rapid7, 2018). It aims to identify, measure and

mitigate the security risk level of networks revealed as exposure by vulnerabilities, misconfigurations and security policy violations, It can also be used to analyse malware in an IT environment which manages different operating systems, databases and web applications. It interacts with the user through a web browser and uses an attack generating tool known as Metasploit (Allodi & Massacci, 2014) to exploit vulnerabilities and calculate its criticality using CVSS(Keramati, 2017).

2.6.2.2 OpenVAS

OpenVAS is an open-source vulnerability assessment tools used in scanning and managing Vulnerabilities develop by Greenbone. Its definition according to (Greenbone Vulnerability Management (GVM) Solution, 2018; OpenVAS, 2018), is presented below;

- It supports different operating systems
- It can be term as an-inclusive vulnerability assessment tool recognising issues concerned to security in devices of a network
- Its engine is updated on a regular basis by the Network Vulnerability Tests, and it free of charge
- It mostly certified under GNU General Public License (GPL)

2.6.2.3 Wireshark

Wireshark is a comprehensive and powerful network protocol tool.

- It best used to analyze the networks at a minute level
- It picks up the problem online and the analysis is executed offline
- It can run on different programs such as Linux, macOS, Windows, Solaris (Beale & Berris, 2018).

2.6.2.4 Nessus Professional

Nessus tool is an exclusive and patented vulnerability scanner built by Tenable Network Security, The definition of its task according to (Tenable, 2019; Security, 2014), is presented below;

- It blocks the networks on or after the penetrations caused by hackers by evaluating the first vulnerabilities discovered.
- It is able to scan the vulnerabilities which allow remote hacking of sensitive data from a device.
- It supports almost all known operating systems, Databases, applications and a number of other devices among virtual and physical networks.
- It can be said to be the most widely used vulnerability assessment tool by users for both vulnerability assessment and configuration issues.

Nevertheless, the assessment of unidentified vulnerabilities is done by Identifying the visibility of a systems attack, this can be organised into categories such as Detectible attack, Detectible behaviour and host visibility then Using Invisible attack encounters such as Google Dorking.

2.7 Conclusion

In this chapter, a literature review of related works of Information Security scoring system has been discussed in this thesis. An information security vulnerability is measured using a series of events and the likelihood of it occurring alongside its consequence, therefore it provides a means of assessing the security requirement of both the organisation and its related BYOD user, based on the needs of each networks security administration, a series of specific suggestions will be generated. It highlighted the major security scoring metric approaches and explained the principles of arithmetical calculation of each approach.

Despite using measurement as a security analysis tool in detecting security vulnerability level and answering the questions associated with BYOD deployment, it has become very important for Network administrators to attain a quantitative score value(numerically) rather than qualitative results to establish the actual value of risk critically.

CHAPTER 3 A BYOD ABSOLUTE SCORE MEASUREMENT FRAMEWORK

3.1 Introduction

This chapter introduces the BAS Metrics for BYOD vulnerabilities in an organisation's variable. The BAS Metrics is a measurement framework that utilises the design science research knowledge, by proposing a novel approach to measure the security level of a BYOD system using the vulnerabilities information on a BYOD device and its network as an input. The model applies an evaluation process centred on mathematical analysis that generates quantifiable measurements to provide security risk level and provide recommendations. Thru this information, an organisation can make better decision to strengthen its network, data and mitigate the risks introduced whilst adopting BYODs. It begins with a brief introduction in section 3.1, followed by the description of the framework, in section 3.2, this includes the architecture design and the main components. Finally, section 3.3 summarises the chapter.

3.1.1 Framework For BYOD Security Level Measurement

With the significate development of network connectivity, has brought about an increment in the number of security attacks on institutions and organisation causing a distraction to their business operations. These institutions and organisation allow user-owned mobile devices to access their network either in the organisation or outside the organisation, thus BYOD affects various parts of people's life, being education, social or economic with it many benefits, as well as vulnerabilities. These Vulnerabilities may be present either in the operation system, application software, hardware (personal device or server), system authentication not properly setup, or users abuse of a targeted component. An attacker achieves its objective by infiltrating the network against both the user and the organization, they exploit on various vulnerabilities of the targeted host, therefore it becomes necessary for both users and organisations implementing BYOD to be aware of the risk posed by each vulnerability. When these attacks occur it can cause critical data loss, Denial of Service attack (DOS) etc., harming both the user

and the organisation. Therefore creating a secure environment for a BYOD system should include vulnerability scoring metrics to help identify high damaging vulnerabilities. The BYOD vulnerability scoring metrics is a ranking quantitative algorithm that is used to assess possible harm facing an organisation by evaluating the severity of the vulnerability and referencing it numerically for severity score of each vulnerability.

There are many networks and software such as firewalls, intrusion detection systems and CVSS metric which is being employed by organisations in the discovering and assessment of vulnerabilities. However, these approaches lack a better understanding by most computer security administrators as to their standard of measuring vulnerability in a BYOD facility. Moreover, dynamicity is not considered in a security measurement. This is because, essential security tasks, for example, responding to alerts, implementing network forensics, and searching mitigation techniques, require security administrator to gather and process a large volume of information that is outer the scope of a BYOD facility. These information's are located online, for instant vulnerability and exploit databases, vendor news, and security blogs, and could be unstructured text, therefore can be time-consuming to either patch up or setup exposed hardware and software appropriately. The scoring system is used to translate the threats and vulnerabilities data into readily used information. Hence, the BAS metrics is a security Metric that estimates the security level that a BYOD system is capable to grant.

This chapter introduces a novel vulnerability measurement scoring metric for the understanding of vulnerability information on BYOD facility. The proposed approach has developed a framework of a BYOD absolute score (BAS) metrics, the BAS metrics is an integration framework for the creation of assessment based measurement system that uses ratings as their source of knowledge. The motivation behind this approach is to not only tackle the limitation that security administrators sustain on the computation and representation of BYOD systems but as well as take into consideration the inconsistency in security policies used in managing

vulnerability posed on BYOD employed networks and its users. The BAS architecture takes into consideration the cybersecurity lifecycle of an admitted personal device to obtain information for its Risk Management. Additionally, to lessen the time taken in its vulnerability measurement, the BAS metrics make use of dynamic taxonomy in its security policies requirement classification. Its also does not go through all the stages in a security risk management framework but concentrates on the monitoring and assessment stages for better performance.

We begin with a quantitative ranking method of taxonomy described as Known attacks. The objective of the approach, first of all, is to extract necessary vulnerabilities using a vulnerability scanner based network traffic from the nodes of an operating system and integrate with information from numerous severity sources such as CVSS score, and user induces score from VEA_ability metrics. Integrating this information by means of taxonomy will obtain the ideal score.

Likewise, the second objective is to quantitatively measure the security risk level created from the taxonomy of the organisation's variables(Users, Technology and Policy). In order to offer appropriate quantitative metrics, two main probability principles approach, The law of total probability and inclusion-exclusion probability principle is used to compute the metrics on the said variables, that is, Individual users, employed network and department policy. This is to prevent the difficulty in vulnerability overload problem and to establish integrity and Efficiency.

On the other hand, NIPD is used to identify and categories unidentified vulnerability based on their visibility. Thus Google dorks (commands) is used as a taxonomy of unidentified vulnerabilities in reference to their attributes. The final objective is to put forward a set of rules in a Snort NIDPS signature database which is used to score the BYOD unidentified vulnerability. A case study involving a BYOD employed organisation have been used to

evaluate the system and to improve its accuracy, as is shown in greater detail in the evaluation chapter. The goal of this work is to increase the efficiency and conformity of the scoring metric by considering all variable (User, Organisation policy and Technology) in an employed BYOD system.

Figure. 3.1 below, shows the order for BYOD variable features, which consists of six classes: Variable class, Goal class, Composition class, Measurement reliability, Division and measurement Instant.

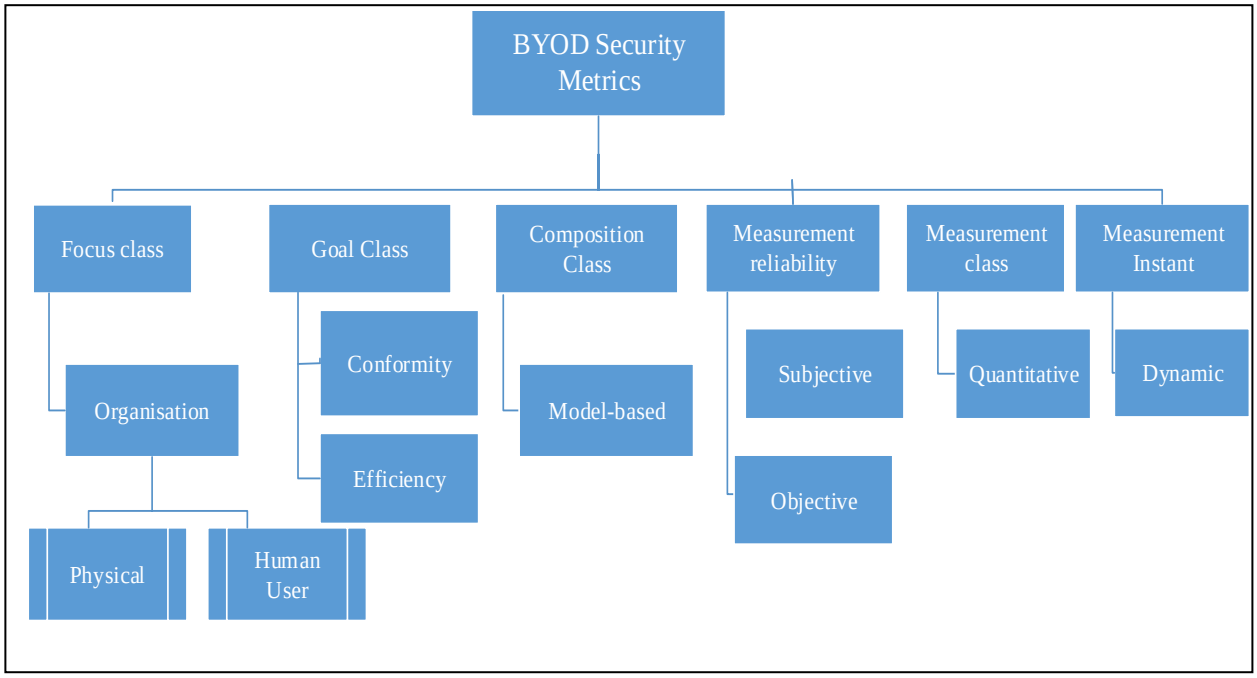

Figure 3. 1 BAS Metrics Identified Classes

I. Variable Class

The metrics calculation is done using an organisation variable this is done considering both the physical (technology) and user security.

a) The physical security includes the protection of an organisations assets such as information, hardware and software from threats

b) User security comprises the protections of BYOD engaged users.

II. Goal class.

The expectant result of this quantitative metrics is to measure:

a) Conformity of the security policies, procedures and standard of a BYOD employed organisational focus. An example is the metric sum of personnel with passwords in conformity with the password security policy.

b) Efficiency metrics quantify how well security solutions implemented are actually performing their assign task of responding to a security vulnerability.

III. Composition Class

It is the represented structure of the security metrics framework in question, this represents the organisation variable class being weighed thru a formal mathematical model. The metric is created from the examination of a system model. Parameters are entered (input) which include data from an Intrusion Detection System device (IDS) and vulnerability scanner and generate as output the required mathematical model based absolute value.

IV. Measurement Reliability

The BAS measurement reliability is Objective metrics. Thus, the extent to which data is unbiased, fair and impartial. That is, using the same method but different human users produced the same output

V. Division Class

The BYOD security is a quantitative metrics which is express as a cardinal number (counting just how much something there are) or percentage.

VI. Measurement Instant

The operations of a BAS metrics under the variable class performs in Dynamic or run-time, both its monitoring and access.

The BAS metrics framework has been built for situations where there is a need for personal devices and its user being assigned unto the BYOD platform are scrutinized to identify their

security risk levels. In its scope, the term security risk level is defined by the degree of severity and each vulnerability is scored by selecting appropriate factors that fit the BYOD organisations variables. The framework is adaptable as it can be personalised to any particular domain so far as it meets the measurement reliability class condition of having 'objectively' relevant items.

3.2 Outline Design

All these class mentioned in section 3.1. will impact on the score of each identified variable and the security requirement of each organisation. Hence this work has been presented with this relevant viewpoint. The proposed BYOD Absolute Score metrics (BASmetric) framework focuses on quantitatively ranking the security risk level of both an organisation and its BYOD user by integrating probability theory and period based metrics with support from security attribute taxonomy. This metrics is for measuring vulnerabilities and aimed to quantify an organisation and its BYOD systems vulnerabilities through their security attributes, host-level (operating system) vulnerabilities.

The framework BAS metric is consist of two-component, the first is constructed on known vulnerabilities and the second component is constructed on unidentified vulnerabilities. We begin the framework with an explanation of Data Gathering in section 3.3 and allocated into the first component (Known vulnerabilities), this is expressed in section 3.3.1, and in two layers. The first layer is the vulnerability scanning process, where vulnerabilities are identified and the second layer is the measurement layer, where the scoring procedure is finalised. The second component(Unknown vulnerabilities) is expressed in section 3.3.2 which look at the likelihood of BYOD variables being abused by an unidentified vulnerability leading to their exploitation. All the vulnerability data collected on a BYOD network are shown in Figure.3.2 below.

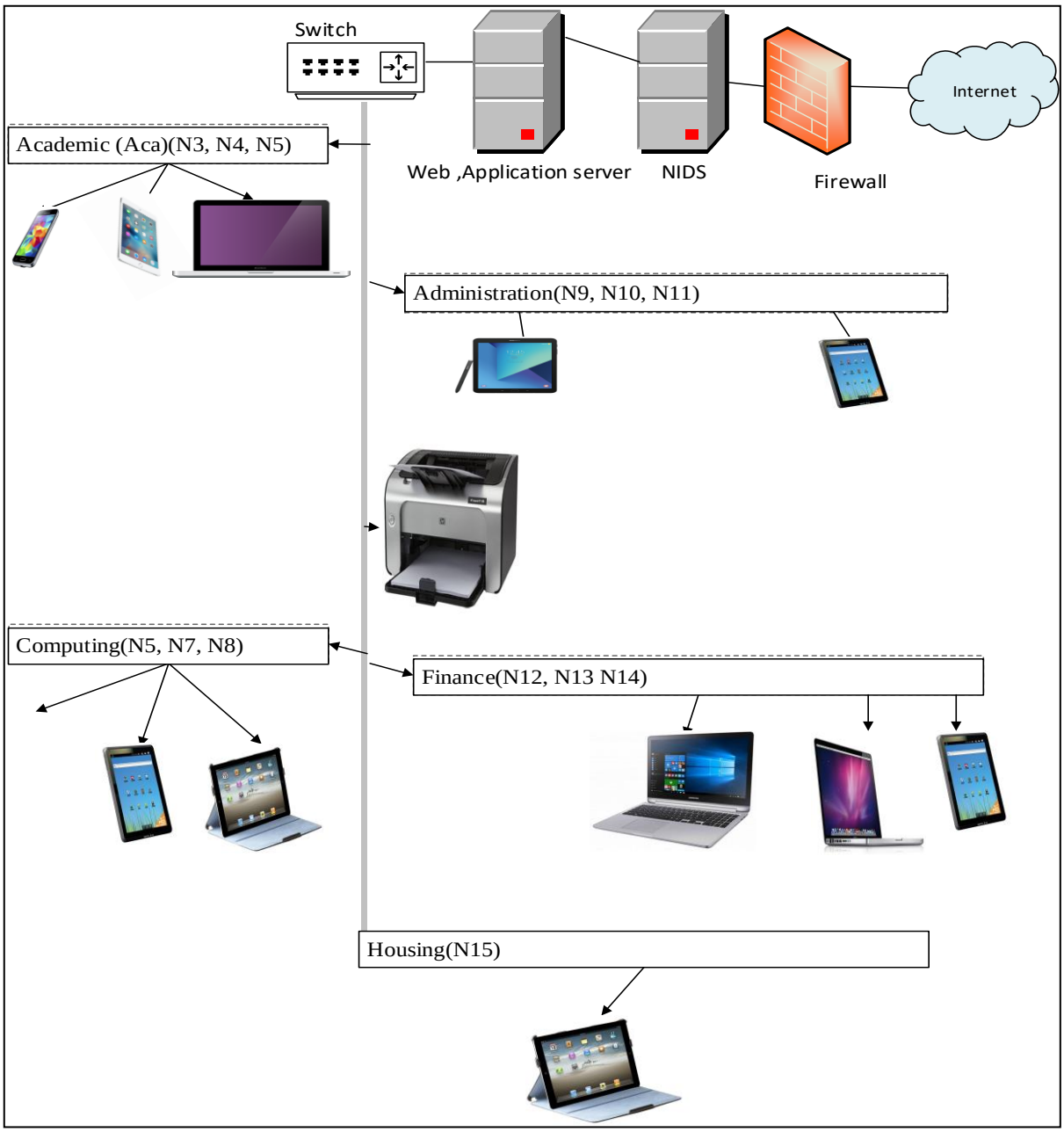

Figure 3. 2 A BYOD employed Network

As shown in Figure.3.2, above. The BYOD network is employed by five (5) departments that are part of a bigger organisation located in England (United Kingdom). These are further split into network nodes with each node representing an accessible BYOD host. This is for an easy measure of the security risk level scored as a result of discovered (known) vulnerabilities. Data were taken from February to September 2017 employing Nessus version 7.0.1. Also, the vulnerability description is defined based on Common Vulnerabilities and Exposures (CVE).

Calculations were done with Microsoft Office Excel 2016. The discovered vulnerabilities are appropriated into account. This is further elaborated in the experiment in chapter 4.0. Subsequently, calculated by means of two probabilistic principles, a metric is built with user induced rule of theVEA_ability metrics and the defined probability to produce a BAS metrics score.

3.2.1 BYOD Absolute Outline

A block diagram of the proposed BYOD Absolute Outline is displayed in Figure 3.3 below.

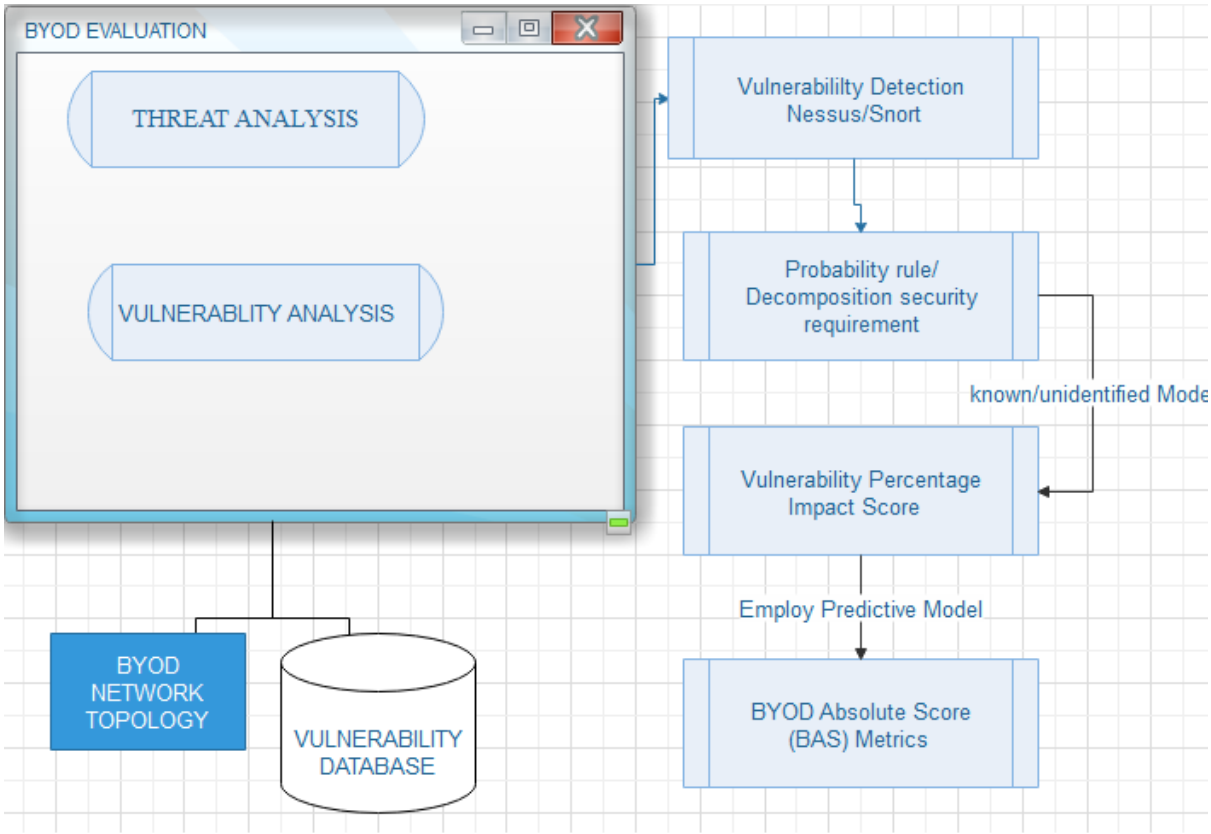

Figure 3. 3 BYOD Metrics Procedure

The process as illustrated in Figure 3. 3 above, displays all the participating processes that are involved in calculating the BAS metrics vulnerability score. The working architecture can be used for vulnerabilities identification, evaluation and response behaviour of a BYOD system without compromising its participating network. This method is applied here, for the calculation of vulnerability impact in the BYOD organisations variable and predicting the

likelihood of new threats and vulnerability level. Therefore the BYOD absolutes score which signifies the severity, for each variable is calculated using the average of the impact and temporal scores by the formula in Eqn. (3.10)

$$S = \frac{Is + Ts}{2} \tag{3.10}$$

BYOD absolutes value of the vulnerability represented by

The Temporal score(Ts) and Impact score(Is) are assigned by the CVSS value (Scarfone & Mell, 2009) value of the known vulnerability, which is then used to obtain the severity(S) of the vulnerability.

Temporal score(Ts) = the input of data by a user variable

Is = CVSS impact scores of related NESSUS data.

There the Vulnerability level is given by

$$BAS(Metrics) = S + \%\text{Impact value} \tag{3.11}$$

The configuration of the framework allows factors to be substituted without any additional amendments needed to other parts of the layers. For example, the security attribute of an organisation variable can be tailored to meet the security requirement and ranked appropriately, provided all the needed data needed in the measurement procedure is provided.

3.2.2 Probability Measure

In this phase, a practical statistical model is used in predicting the results of the experiments from the designated network occurrence if the subsequent two requirements are met. Firstly,

the applicable variables and their properties are reflected in the model. Secondly, the properties of the model should be mathematically reliable and generate a practicable evaluation.

Modelling of the statistical measure is described using three conceptual entities namely sample space, event, and probability measure (Kobayashi, Mark, & Turin, 2011).

1. Sample space: is the numerical collection of all likely experimental outcomes known as the sample space which is symbolised by (Ω). Additionally, entities which are within the (Ω) is referred to as sample point and symbolised in this research as (n). Thus, individual sample point corresponds to a probable outcome of the experiment. Example; three probable outcomes of an experiment is represented in a sample space as $\Omega = \{n_1, n_2, n_3\}$. Furthermore, to measure the likelihood of exploiting the vulnerability on a host(BYOD employed technology), ideally, the generated result can stand between zero and infinity. So, symbolised as $\Omega = \{n: 0 \leq n < \infty\}$.
2. Event: illustrates a set of sample points, this normally expressed in capital letters, such as B. Hence, Event $\Omega = B_n$(a set of outcome). Equally, $B_n = \{n: 0 \leq 0 < \infty\}$.
3. Probability measure: This is the apportioning of an actual number to an event described on Ω. The probability of an event B (a set of outcome) is symbolised by P(B).

3.2.2.1 Axiom of Probability

Two principles of probability were used in this approach, that is multiplication and Intersection principles.

a) Proof of Probability Principle

In this research, we are dealing with the collective set of experimental results. Although to determine the probability of event A, it is sometimes suitable to distinguish all possible occurrence leading to Event A**.** But, a probability involving a collective set of results A and B occurring simultaneously called joint event this is symbolised by P(A, B) (Kolmogorov, 1963) is used in treating a compound experiment. This is considered with one set having a possible

outcome of $\{A_{m:m=1,2,3,\dots}\}$ and the additional also with possible outcomes of $\{B_n : j = 1,2,3,\cdots\}$ and can be measured as a single experiment comprising the collection of possible outcomes $\{A_m, B_J\}$, Hence, applying the measure B_n to discrete random variables $\{B_n : j = 1,2,3,\cdots\}$ is accountable as $0 \leq P(B) \leq 1$. Also, the rule on joint probability can be generalised for event B that is $B_1, B_2 \dots, B_n$ thru the iterations of joint probability $P(A \cap B) = P(A|B) * P(B)$ to define the Multiplication principle and intersection principle, supposing $B_1 \cap B_2 \cap \dots, B_j \neq \emptyset, j = 1,2,..n$. This is shown in Table 3.1 of applied principles below.

Multiplication rule	**Intersection principle**
$\boldsymbol{P(A) = P[A\|B_1][B_1] + \cdots + P[A\|B_n][B_n]}$	$\boldsymbol{P(B_1 \cap A) + P(B_2 \cap A) + \cdots P(B_n \cap A)}$

Table 3. 1 Table of applied principles

3.3 Data Gathering

In the same manner, the data gathering is also in two phases, the first phase is captured for the known vulnerabilities whilst the second phase is captured for the unidentified Vulnerabilities. This is further elaborated in section 3.3.1 and 3.3.2 respectively.

3.3.1 Known Vulnerability

As it was decided that the known vulnerability variable class is made up of the organisation's user and technology, therefore the main formats of information that is needed to be gathered to support this metric are internally generated. Fortunately, all of this information can be captured through open-source applications that are publicly available. For example, the likelihood of a user leaving their device unattended, random application installation and access to open free Wi-Fi network, exposes the organisation to harm. However, using a vulnerability scanner to

capture this information is considered the first layer in a security assessment. Extracting precise information from the open-source application on a whole network is always a challenging task in network security management, so the network will be treated as a node whilst the connected mobile devices and its operating system are the host. The individual user and operating system in a department represent the variables connected to a BYOD network. These are scanned to identify vulnerabilities using the Nessus vulnerability scanner, the scanning process is shown below in Figure 3.4.

.

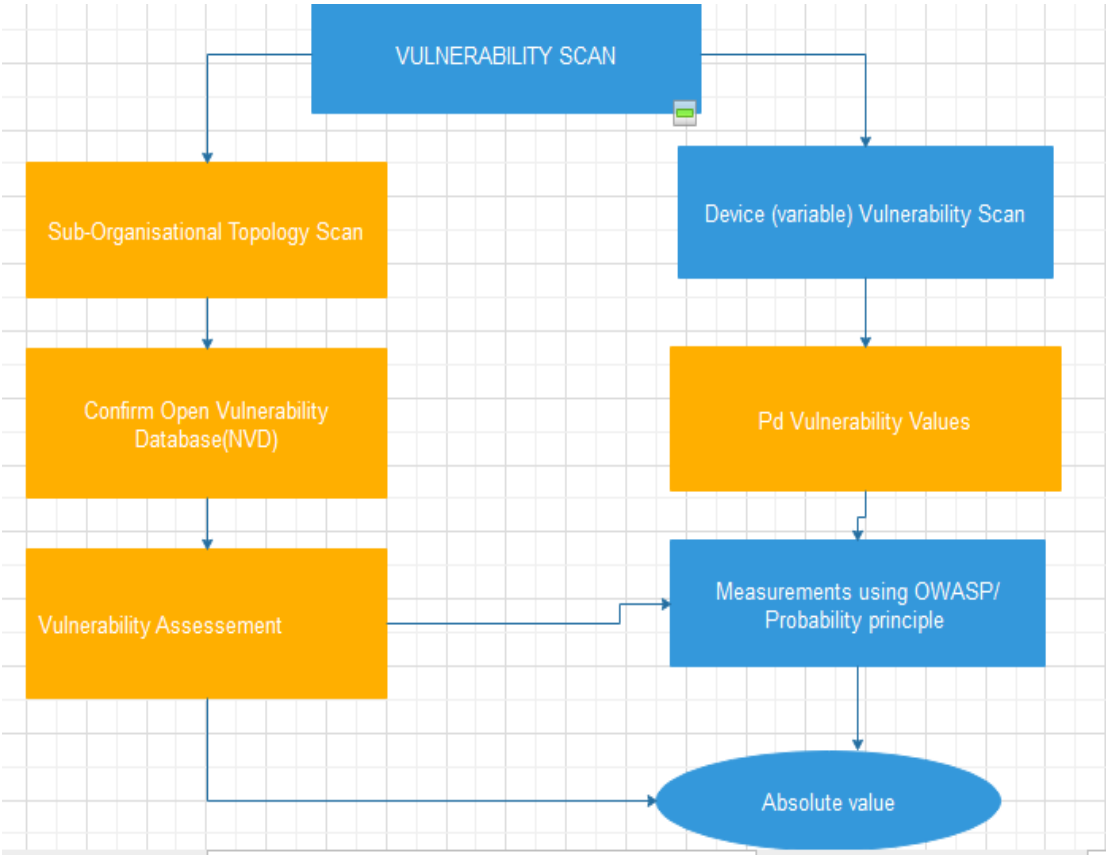

Figure 3. 4 Vulnerability scanning process

3.3.1.1 Probability of vulnerability exploited

First, we determine the severity of the host vulnerability by measuring the likelihood of exploiting an individual vulnerability on a host. This is achieved by using two probability

principles. For instance if, A is the subject of each individual node and B_n is the measurable event annotated by probability theory? For each theory $\{B_n : n = 1,2,3,\cdots\}$ is the countably infinite partition of a sample space in vulnerability situations. It can be computed using the law of total probability algorithm as shown in Eqn 3.12

$$P(A) = \sum_n P(A \cap B_n) \quad (3.12)$$

Where B_n = measurable vulnerability situation and $P(A)$ is the probability subject of Individual host on each department. With the same interpretation, the principle of inclusion and exclusion is used to compute the totality in the rank of the measurable event as shown in Eq.3.13

$$P(A) = \sum_{k=1}^{n}(-1)^{k+1}\left(\sum_{1\leq j1<\cdots<jk\leq n} P(B_{j_1} \cap B_{j_2\ldots} \cap B_{j_k})\right) \quad (3.13)$$

where K signifies the ith situation of a host in the department's network. The probability value of the metric serves as an input for computing the vulnerability score. The output of this phase is a percentage value term as the absolute score which will be used BAS metric. Additionally, it is used as a control to check the validity of the organisations variable (user, security attribute, operating system, etc). If it is authorised, it is parsed, thereby the user and its device continue to stay in the BYOD, otherwise, it will be blocked. Modelling a security framework that monitors individual department and ranks it numerically reduces the time taken to enforce the security solutions.

3.3.2 Unidentified vulnerability

This phase is used to measure the likelihood of BYOD variables being abused by an unidentified vulnerability leading to their exploitation. Network Intrusion Detection and Prevention System (NIDPS) is used to identify and categories unidentified vulnerability based on their visibility. Thus, Google dorks search operator list is used as a taxonomy of unidentified vulnerabilities in reference to their attributes. the detailed version of this component is

explained in chapter 4. This component is in three stages, the first examines the noted unidentified attacks, Stage two is to establish the risks of vulnerability in a BYOD variable by using the OWASP risk rating methodology and based on a security attribute. The final stage is the BAS metric referred to in Equation (3.10) and (3.11).

3.3.2.1 Unidentified Vulnerability(Instance)

Likewise, it was decided that the unidentified vulnerability class is made up of attacker activities which are generally presumed to be lawful. Thus, this attack has nothing to do with network security systems. For example, the transmission of information between two computing devices is completely an acceptable policy. However, sending data from one mobile device will be considered unlawful if the preceding operation is a brute force attack on the root passwords. Google dork is one of such well known invisible attacks. Fig 3.5 shows the interface of the google advance search which is used in the Google Dorking.

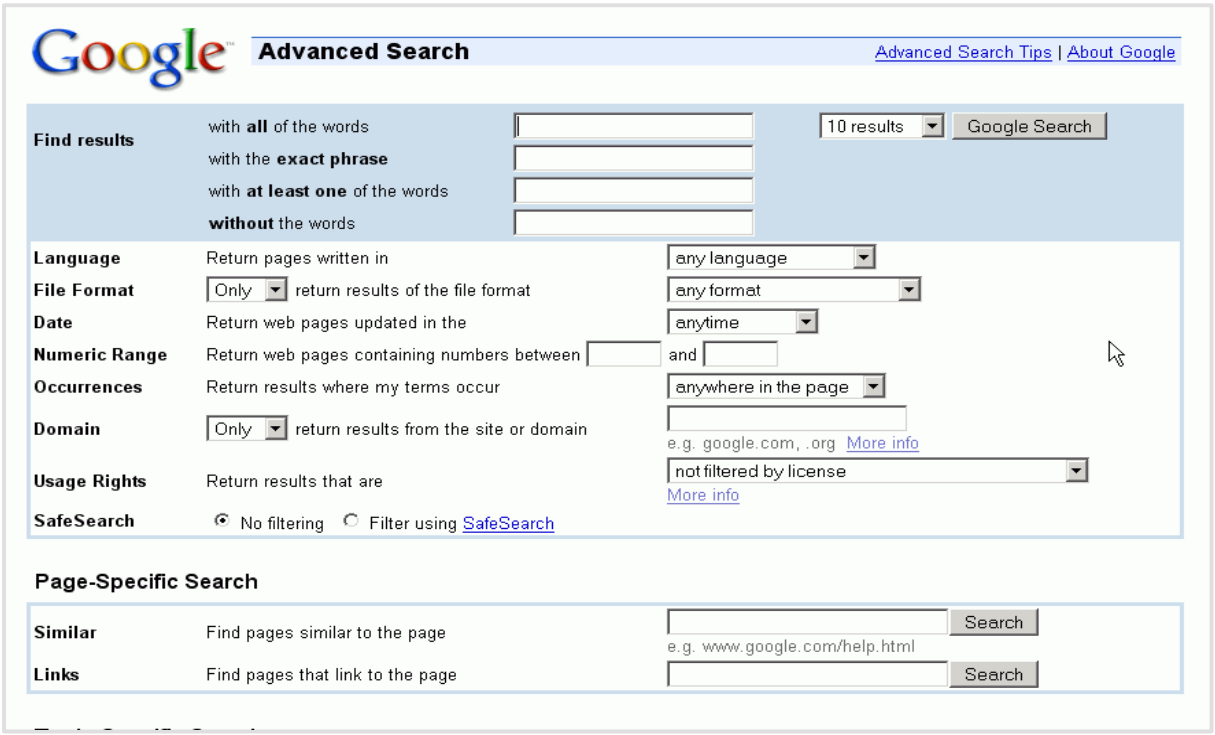

Figure 3. 5 Google advanced search interface

Google Dorking also referred to as Google hacking, involves using advance search command to locate the needed strings of text about a device connected to an organisations network (Wilhoit, 2013; Gupta & Dhami, 2015). In a social engineering situation where an intruder follows the activities of its victim and gathers sensitive information with the help of the Google advanced search. As a result of ineffective systems design, search engines can collect more information than necessary while moving thru the web with the help of a search operator to exploit insecure websites. Table 3.2 shows the records of likely operators for various search services used to create invisible Vulnerabilities.

Service	Search operator
Groups	intext, allintext, author, allintitle, intitle, insubject, group.
Web service	filetype, allinanchor, inanchor, site, intext, intext, inurl, related, allintext, allintitle, allinurl, cache, define, id, info, intitle, phonebook.
News service	intext, intitle, inurl, allintitle, allintext, source, allinurl, location.
Directory	filetype, ext, allintext, intext, inurl, intitle, allintitle, allinur
Image Search	site, allinurl, allintitle, intitle, filetype, inurl,
Product Search	allintitle, allintext

Table 3. 2 Likely Search Service Operators

The Google search engine has been used as a tool in exploiting vulnerability because a greater number of security countermeasures do not consider this form of attack. The procedure involved in data collection in the google hacking process is displayed in Table 3. 3, below.

	Google Advance Search
	↓
Results	Encrypted Username and User_ID
	↓
	Information decipher tool: Password decrypted
	↓
Results	Username and Password in plain text
	↓
	Access exposes system with complete right
	↓
Result	can Alter, steal or delete information

Table 3. 3 Google Hacking Process

Using the attack example illustrated in table 3.2 above indicates ways by which a well scripted and executed query in Google advanced search engine is used to fetch that sensitive information made up of usernames and passwords. Thus the attained information is decrypted quickly with the help of a decipher tool and further exploited in generating attacks. Though the user is unlawful it may seem lawful to the network, thus making the implemented security countermeasures on the network inadequate.this is captured by the BAS metrics as an unidentified vulnerability.

3.3.2.2 Unidentified attacks

There has been an increment in the Vulnerabilities uncovered by search engines rapidly, hence, it is necessary to analyse these attacks specifically. Using their characteristics, theses invisible attacks are categorised into ten (10) groups as shown given in Table 3. 4

Number	Attacks	Number of Commands
1	Pages contain login portal	129
2	Existing login websites	116
3	Blogs / Forums	37
4	Files having username and passwords in plain text	25
5	Error code message (Code 34)	8
6	Phishing emails	16
7	Files having username and passwords in encrypted form	32
8	Social attacks	5
9	Sensitive directories or files containing interesting information	134
10	Plug-ins	4

Table 3. 4 Taxonomy of invisible attack

Table 3.4 shows a taxonomy of invisible attacks which came by as a result of the vulnerability factors not identified. This attacks will be scrutinised further in chapter 4, to ascertain the vulnerability impact level and subsequently, the BAS metrics for the unidentified vulnerability scored.

3.4 Chapter Summary

This chapter presents details of the proposed BYOD absolute score metrics (BAS metrics). The BAS metrics framework is a combination of different component of an individual metric which are essential to achieve an effective working framework, these metrics are selected based on their network configuration and security requirements. The proposed framework supports the quantitative modelling of security risk levels of an employed BYOD network and its users. The defined approach is designed to provide monitoring references to the organisation and their users based on the numerical scoring profile of its variables for easy ranking and trustfulness. Two Probability theory is used to compute the absolute score for an individual department, individual users and the entire network as a solution for information overloading. Known vulnerabilities which were obtained from the network is the principal factor in this security risk metrics calculation. Factors influencing the source of a vulnerability such as Unknown vulnerabilities and human user factors are those vulnerabilities which permit an intruder to use them as access points to a network. For example, is possible for a web-services running on a host to be the exact targets for an intruder to compromise a network.

Also, BAS metrics is a novel, systematic classification model which support the solution to the quantitative scoring of vulnerability level of a BYOD system both an organisation and its users which relates to the problems of offering high-quality quantitative ranking measurement to BYOD security administrator. Therefore its foundation is built on quantitative representation, measurement and indexing of security situation information and presents integrated elements shared across metrics.

CHAPTER 4 TAXONOMY OF BYOD VULNERABILITY SEVERITY MODEL

4.1 Introduction

In a BYOD employed environment, every single mobile device happens to be locatable, addressable and accessible. While more organisations are accepting in the emergent of this phenomenon for various reasons as explained in chapter 2, The BYOD employed network is expected to contain a number of entities which will communicate amid each other as well as with other objects. These do not only consist of the physical device, that is mobile phones and laptops which are the means to the networks, but also variables such as organisations security attribute and users. The diversity of devices and technologies used in delivering these services has a huge impact on interoperability and security measurement. Finding the appropriate quantitative security measures for security analysis based on BYOD has become a challenging assignment. Security scoring metrics represent a likely approach by which to tackle vulnerability overload. Whiles security metrics have been used for the analysis of the security risk level in the same field, the various metrics may result in approximating the scale types of security risk analysis in BYOD. Therefore a predictive score which ranks each vulnerability based on the likelihood it will be leveraged in an attack is used to solve the approximation problem.

There are numerous influences trade-off struggle between security and efficiency in implementing an effective vulnerability monitoring system as mentioned in chapter 2 and efficient business operations practices could be equally omitted. The numerical representation improved security risk potential examining process, by using information from various metrics and integrated into attaining a comprehensive score with which to respond to a system's Variable (People, Technology and Organisational Policy). Likewise, modelling security metrics quantitatively is one of the main aims of applying the BYOD security risk level categorising. This chapter describes in detail both the comprehension of the categorisation

model and the vulnerability evaluation procedures that have been used in BAS metrics and exactly how the approach can tackle vulnerability overloading and numerical scoring problem experience by BYOD organisations and users. In the categorisation section, a new approach is presented to quantifies the percentage of hosts on a network using different probabilistic principles for both law of total probability (individual department) and inclusion-exclusion probability (entire network). Also, an algorithm is proposed to illustrate the concepts of comprehensive scoring metric. The recorded information is entered as an input in the vulnerability scoring metrics. BAS metrics attempt to solve the issue of security and efficiency experience by BYOD employed organisation and their users. In this thesis, two vulnerability taxonomy has been collected to support the proposed approach. Firstly, the known vulnerability and secondly the unidentified vulnerability

The second input support in this chapter discusses in depth the principle been proposed for assessing the stages involved in measuring the unidentified vulnerability level of a BYOD user based on security attributes. A file on Google dork commands is built from the NIDS filtering approach which recognises unidentified attacks. The OWASP mapping tools/ metrics are utilised to enhance the unidentified vulnerability algorithm. Furthermore, using OWASP classification metrics in the BYOD vulnerability scoring system helped to increase the security requirement made up of Confidentiality, Integrity and Availability(CIA) of an employed BYOD system to its users.

This chapter is organised as follows; The framework is introduced earlier in Section 4.1. Section 4.2 provides the experiment's operation and the result of the known vulnerabilities with a full description of its approach. Section 4.3.provides the experiment’s operation and result of the unidentified vulnerabilities structure with a full description of its approach. Section 4.4 summarises the chapter.

4.2 Known Vulnerability Analysis

The collection of known vulnerability into the absolute score process serves as one of the answers to overcome the limitations of established security risk metrics systems. A metrics is a measurement–based systems which are used to classify a particular process or activity quantitative or qualitatively. In technology, security metrics are used as a measure to assess the risk level of an organisations security goals and its users.

The systematic classification in a metrics is used to measure a BYOD known vulnerability information on an employed organisation variable(security policy, technology and users). The use of the vulnerability of a system to assess the security risk level of an organisation quantitatively helps in the distinctive evaluation procedure, example for example (Pendleton, Garcia-Lebron, Cho, & Xu, 2016), categorises security metrics for measuring the vulnerability of a system by quantifying the organisations and its computer systems vulnerabilities by means of user's password, software vulnerabilities, and the vulnerabilities of the use cryptographic keys. However, these are supposedly scored or rank according to the security level of distinct hosts in the network. By enabling an organisations network structure to be allocated into individual network resources help in easy measure of the security risk level produced as a result of known vulnerabilities(Homer et al., 2013; Issa-Salwe & Ahmed, 2011). Additionally, treating individual host on the network gives it an advantage of evaluating the likelihood of exploiting a particular vulnerability within the host by an attacker.

4.2.1 Principle of Known Vulnerability structure

Both commercial and non-commercial vulnerability scanning tools which have been looked at in the literature in chapter 2, help to identify network vulnerabilities and their related devices. However, these tools only do a fuzzy evaluation, classifying in terms of high, medium and low. So, it has become necessary for an absolute number to be achieved in the determination of the

security risk level of an employed BYOD organisation network and its users, hence this approach have been adopted and used in the design of this methodology.

All the useful information related to the BYOD network structure and how useful information are collected from the network has been described in chapter 3 section (3.2). These are presented as departments. There are 5 main departments dependent on the network with a further 15 classes of nodes connected to the departments. In addition, four distinct operating systems(host) are run on the identified nodes. Vulnerabilities are identified using the Nessus vulnerability scanner (security, 2014). This process defines an organisation variable that is technology(operating systems) which is further considered in the metrics. Moreover, the scanned results also show the services running on the network

The scanned data is collected from the network communication traffic both incoming and outgoing. A total number of 1567 different vulnerability is collected, this has been deliberated in table 4.1 below.

Hosts	Operating System	Low	Moderate	High
H1	Apple Mac OS X 10.3.9	0	1	0
H 2	Linux 2.6.18- 308.24.1.e15	12	9	37
H 3	Microsoft Lumia 950 windows 10	53	76	147
H4	Android 8.1 Oreo Moto G5 Plus	3	38	185
H5	Apple IOS 10 IPhone 8 Plus	0	0	30
H6	Android 8.0 Samsung galaxy s8 /s8 plus	0	10	37
H7	Apple IOS 10 IPhone 7 Plus	0	0	0
H8	Microsoft Lumia 950 widows 10	53	76	147
H9	Apple iPad IOS 9.3.5	0	0	1
H10	Apple iPad IOS 9.3.5	0	0	1
H11	Androids 7.0 Nougat Samsung Galaxy Note 5	9	14	205
H12	Apple IOS 12 Phone XS	0	0	0
H13	Android 8.1 Oreo Moto G5 Plus	3	38	185
H14	Apple Mac OS X 10.3.9	0	0	0
H15	Androids Android 7.0 Nougat Samsung Galaxy Note 5	14	9	205

Table 4. 1 Vulnerability Data Collected Base on Hosts

The rate of operating systems being affected most by the known vulnerability collected is taken notice of with Andriod having the most vulnerabilities made up of 955 vulnerabilities making it the mobile device operating system which is the most vulnerable to attacks. Using a small number of vulnerabilities from the Common Vulnerabilities and Exposures (CVE) metrics which we listed for some of the Andriod identified vulnerabilities, for example, The Android 1.0 through 9.0 has security concerns with score via CVE-2018-15835 and in all Android releases (Android for MSM, Firefox OS for MSM, QRD Android) via CVE-2018-10753, CVE-2018-11281, CVE-2018-11278, Android 9, Android ID: A-112661641 CVE-2018-9531 etc

We categorising the known vulnerabilities into the four distinct operating systems being discovered, this is distributed onto the nodes as follows; Apple macOS = Seven (7) nodes, Andriod =five (5), Windows = two (2) and Linux OS one (1). A bar chart representing the various distinct operating systems(host) and their distribution on the nodes are plotted as shown in Figure 4.1below

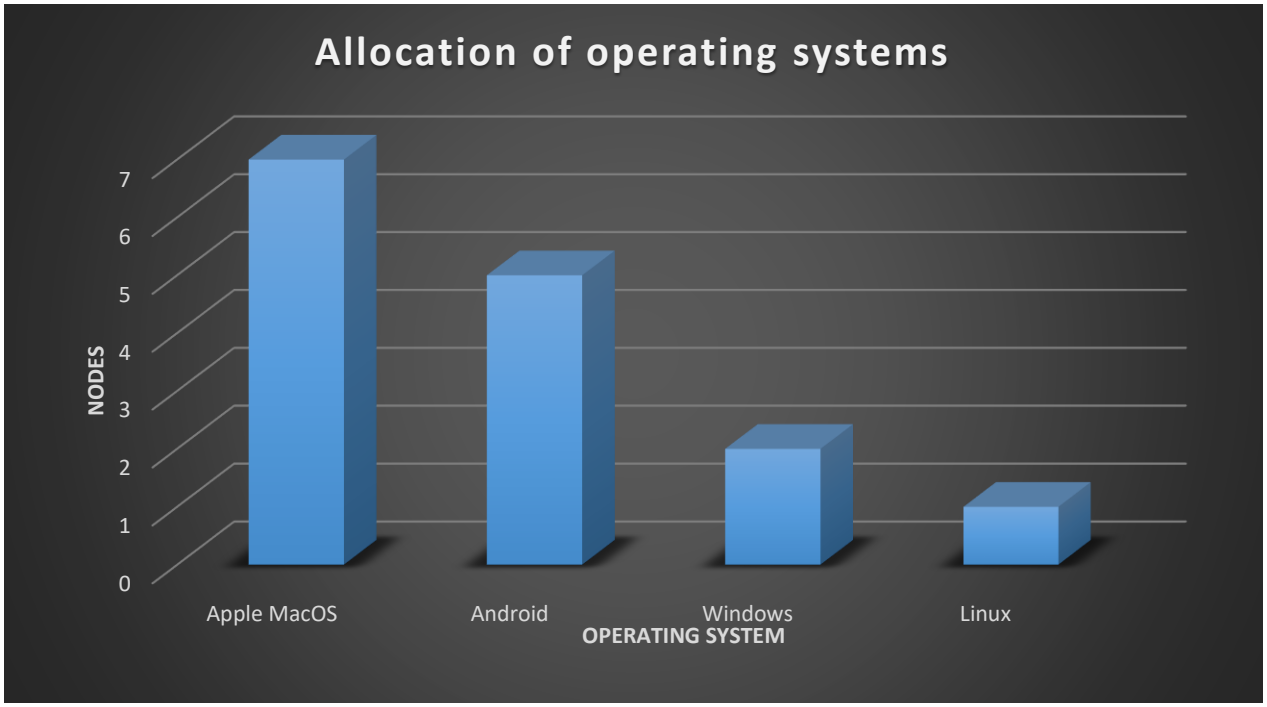

Figure 4. 1 Allocation of Operating System(host) against Nodes

Furthermore, thirty-six (36)services were discovered to be running on the nodes. The description of some of these services and their related nodes has been elaborated HTTPs services is running on all 15 nodes, Google Play services are running on 12 hosts and File Transfer Protocol (FTP) is on 10 nodes etc. A bar chart representing the various services and their distribution on the nodes is plotted as shown in Figure 4.2 below

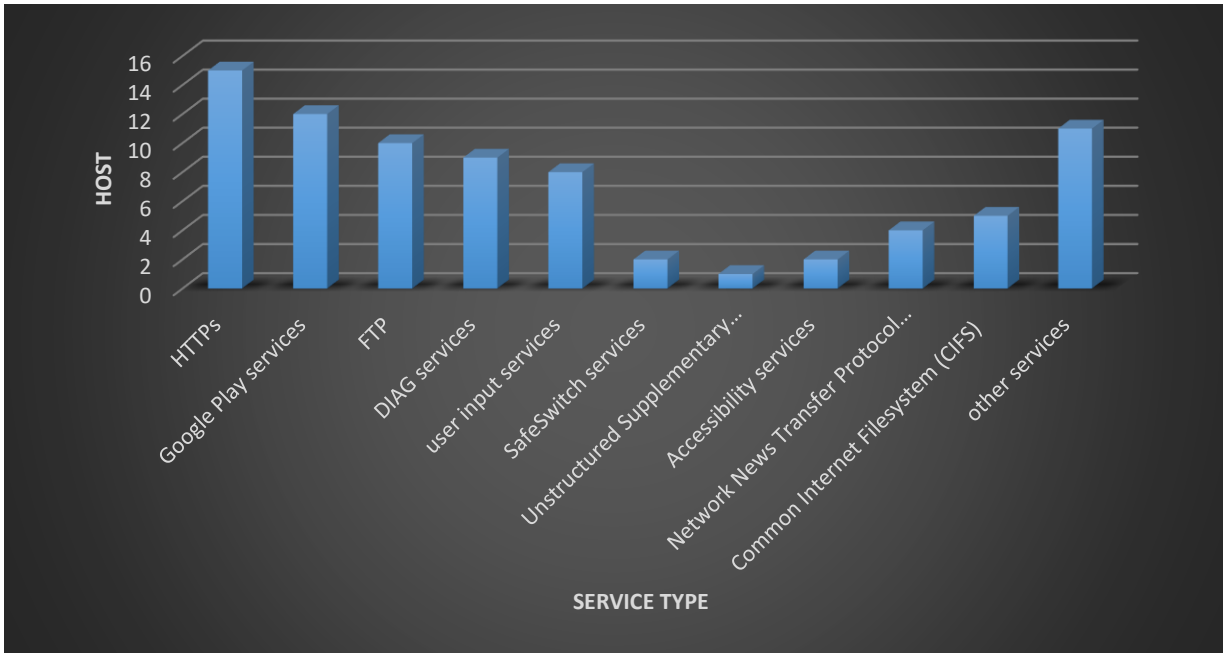

Figure 4. 2 Allocation Of Host Against Services Type

Additionally, to help understand the likelihood of the known vulnerability severity impact, an allocation of percentage severity impact against distinct nodes is shown by a pie chart based on the result from table 4.1. above. This is described in Figure 4.3 below.

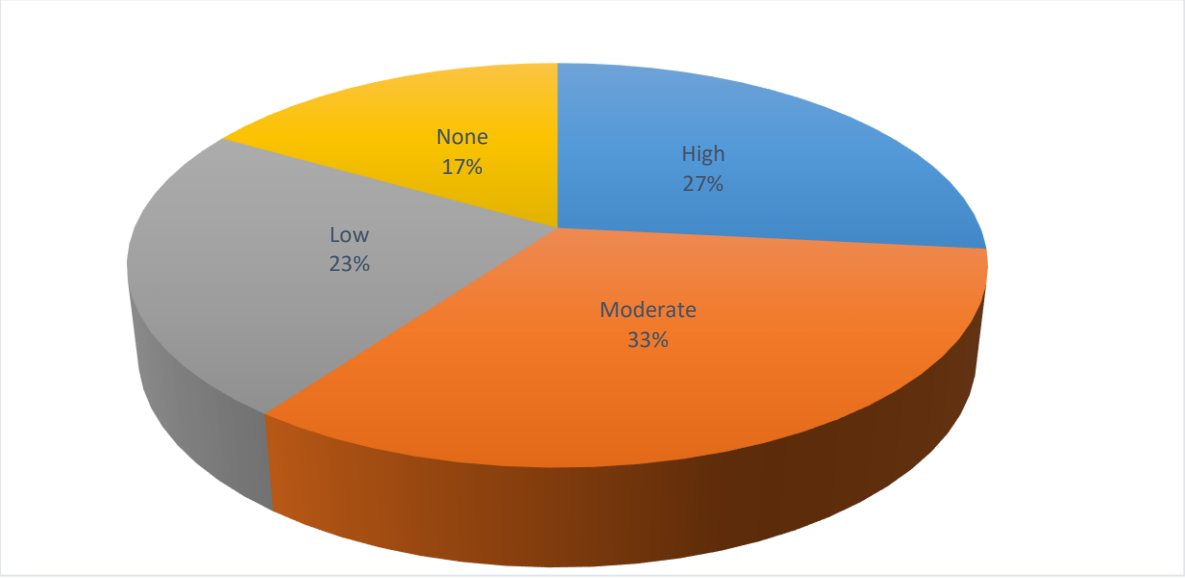

Figure 4. 3 Percentage likelihood Impact chart

Figure 4.3 above, presents the allocation of percentage vulnerabilities impact based on distinct nodes. This has been labelled as High, Moderate, Low and Non-likely, with the Moderate being the most likely severity of impact. This shows an initial estimate to survey the differences and similarities of the establish measurement. And in order to organise the models realistically the Nodes signify how personal devices(host) interact with the employed network.

4.2.2 Measurement of Known Vulnerability(Probability)

Three scenarios are designed to measure the severity level of vulnerability of a present BYOD employed organisation, created from real-time information of a system's variables(Users, Technology and Organisational Policy) quantitatively to produce an absolute value. we begin by using the letters L, M and H to represent the potential impact of Low, Moderate and High severity impact respectively. Although table 4.1 above shows some zero value in the scanned data. At this point, we scrub the data that has marked as zero(0).

Let say Hi stand for the ith Host in the network, then the security level of vulnerability in every single department on the assigned network and subsequently the entire network can be calculated to achieve an absolute value. The five identified department is labelled as Payroll, Administration, Computing, Finance and Estates and is represented by Pr, Admin, Cp, Fin, Es. Thereafter three techniques have been identified by which to model a BYOD security situation as follows;

Technique I: Describes the method used in calculating the probability of attack upon Individual users in the department and expressed as Low, Moderate and High.

Technique II: Describes the method used in calculating the probability of attack upon Individual user on a department network characterised by the total of known vulnerabilities.

Technique III: Describe the method used in calculating the probability of an attack on the entire BYOD employed network.

4.2.2.1 Technique I

The probability of an attack on Payroll (Ppr), Administration (PAdmin), Computing (Pcom), Finance (PFin) and Estates (PEs) departments is described by means of Low, Moderate and High values from table 4.1. These probabilities are ascertained using the law of total probability From the equation (3.12) the probability subject of Individual host on each department calculated and their results are shown in Table 4.2

Formular based on probability subject(Department)	Impact value		
	High	moderate	Low
$P_{Pr} = \sum_{n=3}^{5} P(A \cap B_n)$	0.2%	32.6%	0.5%
$P_{\text{Admin}} = \sum_{n=9}^{11} P(A \cap B_n)$	42%	7.76%	49.8%
$P_{\text{cp}} = \sum_{n=10}^{12} P(A \cap B_n)$	0	33%	0
$P_{\text{fin}} = \sum_{n=6}^{8} P(A \cap B_n)$	55.7%	0.38%	43%
$P_{\text{Es}} = \sum_{n=14}^{15} P(A \cap B_n)$	0	0	0

Table 4. 2 Probability Of Individual Host

The result as shown from table 4.2 saw that the Payroll department has a 0.2% High (H) and Low (L) vulnerability impact values came out (0.5%) which indicates the Payroll department is prone to some BYOD employed attacks. But, this is not always true for users in this department, as the security risk level with reference to moderate vulnerability impact values is 32.6%, meaning there is a likelihood for a successful attack against BYOD host on the Payroll department. On the other hand, Finance (PFin) department, has High vulnerability impact value of 55.7%, Low of 43% and Moderate impact value of 0.38%, indicating the utmost likelihood for a successful attack against BYOD host on the Finance department. Subsequently, the Computing department can be said to be secure in terms of High and low to known vulnerabilities as they both had (0) in the vulnerability impact value risk level but there is a Moderate vulnerability impact of 33% found meaning there a likelihood to attack. The Administration (PAdmin) department has an utmost vulnerability impact level because all the define impact levels of High, Moderates and Low has been fulfilled with percentage values 42%, 7.76% and 49.8% correspondingly. Additionally, the Estates (PEs) department from the result shows a zero vulnerability impact value, hence this will not be added in the evaluation of the BAS metric.

4.2.2.2 BAS Metrics Result

The BAS metrics is a combination of distinct metrics to create novel metrics for BYOD organisation variables (for instance, we combine host-based and network-based metrics to form Absolutes Percentage score. This is shown in Figure 3.2). Therefore the Absolutes Percentage score which signifies the severity impact for each department is calculated using the notion of average impact and temporal scores using equation (3.10) and the final layer that is BAS metric refers to equation (3.11). Table 4.3 below shows the result for the BAS metrics in Percentage.

Equation (3.11), for each defined Department	%BAS Metrics		
	High	moderate	Low
$BAS(Metrics) = S +$ %Impact value Payroll	7.6	*7.96*	5.25
$Administration$	7.6	7.72	5.74
Computing	12.6	7.33	2.0
Finance	8.61	7.33	4.43
Estate	7.75	7.15	5.05

Table 4. 3 BAS metric Result

4.2.2.2 Technique II

Describes the method used in calculating the probability of Vulnerability impact upon Individual users on a department network characterised by the total of known vulnerabilities.values from table 4.1. These probabilities are ascertained using the principle of inclusion and exclusion. From the Eqn 3.13, the probability subject of Individual host on each department based on the total of the known vulnerabilities. Table 4.4 shows the percentage impact value of total known Vulnerabilities on each host and subsequent BAS Metrics.

Formular based on probability subject (Departments)	%Impact value	BAS metrics using Equation. 3.11
$P(\text{pr}) = \sum_{k=3}^{5}(-1)^{k+1}\left(\sum_{3\leq i3<i4<i5\leq 5} P(N_{i_3} \cap N_{i_4} \cap N_{i_5})\right)$	0.1%	7.7%

P_{Admin}	24.7%	10%
P_{cp}	0.2%	7.8%
P_{fin}	24.3%	10%
P_{Es}	0	0

Table 4. 4 Probability of Impact Value and its BAS Metrics in Percentage

4.2.2.3 Technique III

Describe the inclusion-exclusion define in Eqn 3.13 in calculating the probability vulnerability impact on the entire BYOD employed network and subsequently the BAS metrics of an entire network.

This is identified by EN (BYOD employed network).

There $EN = \sum_{k=1}^{15}(-1)^{k+1}\left(\sum_{1\leq i1<i2\ldots<i_k\leq 15} \mathrm{P}(N_{i_1} \cap N_{i_2} \ldots\ldots \cap N_{i_k})\right)$

EN = 10% + (BAS Metric for entire network)

4.2.3 Discussion

The BAS Metrics calculation results of each building Pr, Admin, Fin, Com, and Es are shown in table 4.3 and table 4.4, whilst table 4.2- 4.3 shows the percentage impact value derived from the probability principles. Since the percentage value of BAS metrics is in the range [0], [10], therefore values beyond 10 are converted to 10. However, for the Percentage impact value, this

does not apply as it fellows the probability principle of a countably infinite partition.

For the %Impact values:

- The percentage score of 0 implies the best score since it has the lowest in low, moderate and high known vulnerability values
- The percentage score from 10 onwards indicates the worst security risk level in the low, moderate and high known vulnerability values

For % BAS metric

- 0 signifies the worst value since it has the lowest score of the BYOD variable security.
- 10 signifies the best value since it has the highest score of BYOD variable security.

4.3 Unidentified Vulnerability Analysis

This phase is used to measure the likelihood of BYOD variables being abused by an unidentified vulnerability leading to their exploitation, and it's in three stages, the first examines the noted unidentified attacks, a NIDPS rule is developed to monitor and safeguard the organisations BYOD network against vulnerabilities and it related invisible attacks, Stage two is to establish the risks of vulnerability in a BYOD variable by using the OWASP risk rating methodology and based on a security attribute. The final stage is the BAS metric referred to in Eqn 3.10 and 3.11.

Commercial NIDP tools which have been looked at in the literature in chapter 2, help to identify vulnerabilities and their related strategies. Also, All the useful information related to the BYOD network structure and how useful information are collected from the network has been describe in chapter 3 section 3.2. An attacking procedure has been illustrated in table 3.2 above, this indicates ways by which a well scripted and executed query in Google advanced search engine is used to fetch that sensitive information made up of usernames and passwords. Table

3.1 in chapter 3 shows the records of likely operators for various search services used to create invisible Vulnerabilities

4.3.1 Principle of Unidentified Vulnerability Structure

As indicated in chapter 3 section 3.2 the BYOD considers five departments on the network structure, namely Aca, Admin, Com, Fin and Hou departments. This has also been used for the known vulnerability. Also, information on an Individual department is limited to users within that department and specific webserver is employed to satisfy users webpage need. A network configuration based on user's devices policy is shown in Figure 4.4 below, this is used in the deliberation for identifying and quantifying the security vulnerability level against invisible attacks.

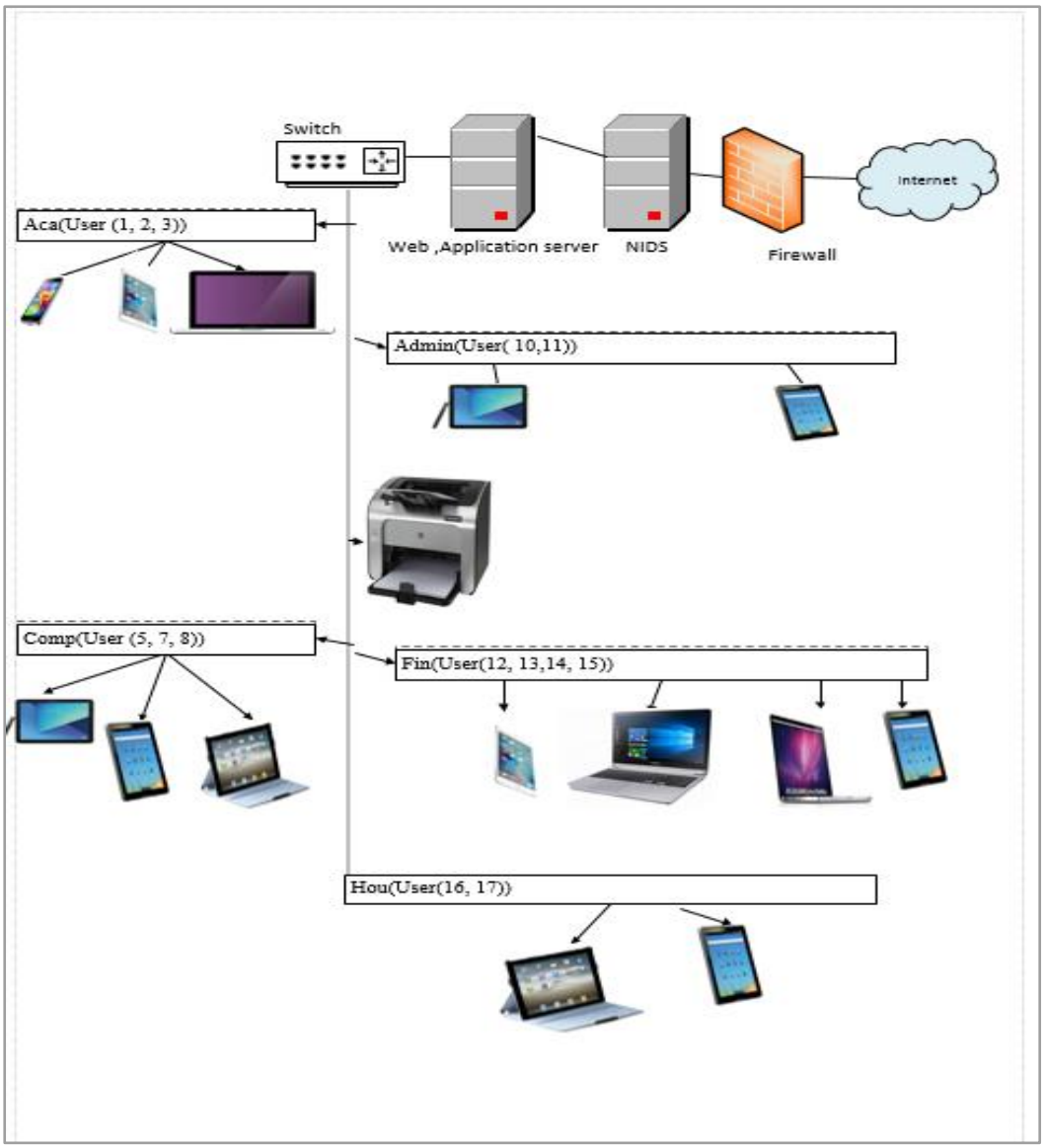

Figure 4. 4 User's Policy on a BYOD network Topology

Nevertheless, an essential factor to note is that the organisation is unaware of the invisible attacks because of the unidentified vulnerabilities. NIDP system is employed in between a firewall and the webserver to guard the networks sensitive information, The NIDP is used to detect and prohibit harmful intrusion by ensuring a deep examination of the incoming and outgoing data packets.

The introduced NIDP in the BYOD network topology is the Snort. The Snort is prefered because is a signature-based network intrusion and prevention system with adaptable rules that can be manipulated to fit any organisations business process. The network also consists of a

cisco catalyst series 3650 switch, a 1.0 Gigabit cables and 10 Gigabit cables are used in connecting the switch and various devices. A packets size of 128 byte signifying the aggregate of data is generated from source to destination. Figure 4.5 below highlights the NIDP object on the BYOD network design.

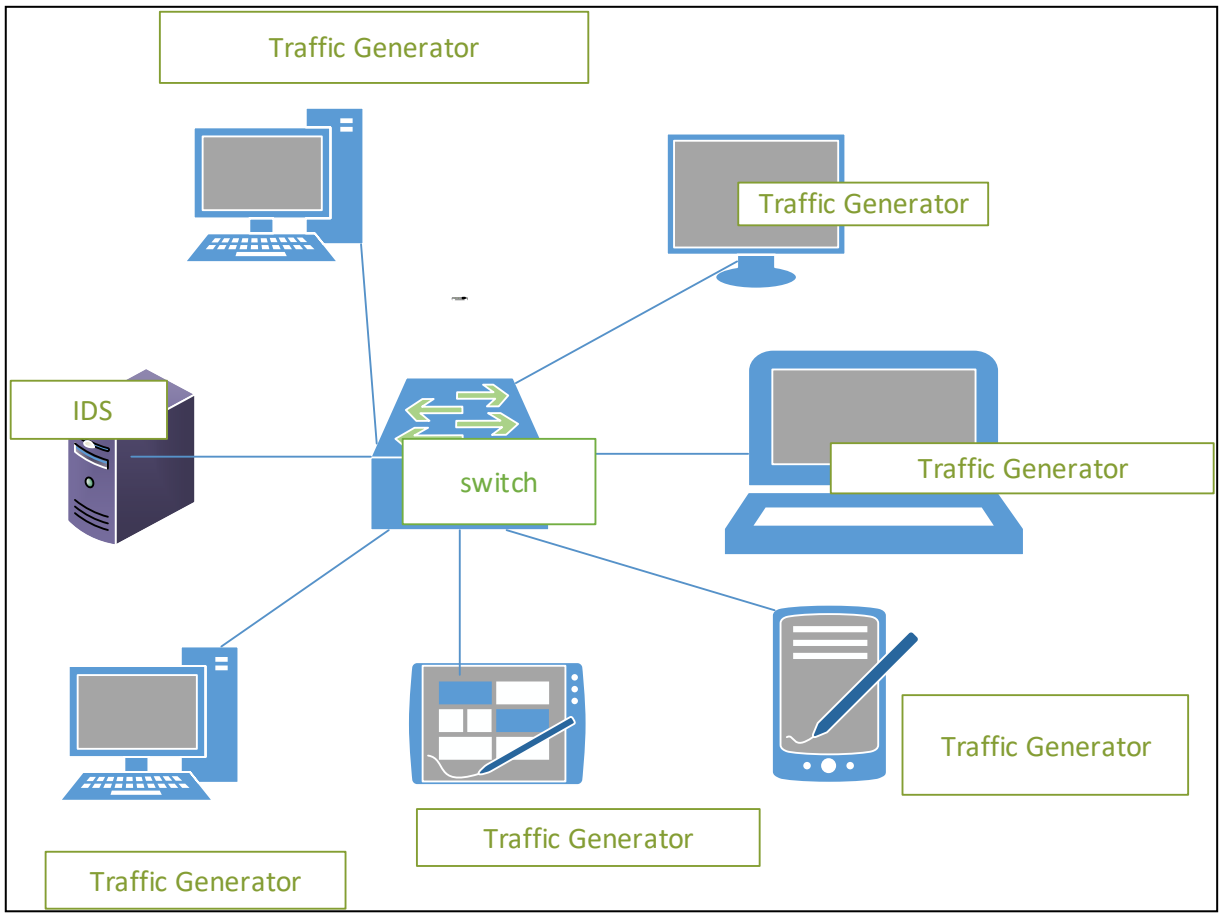

Figure 4. 5 NIDP Object on network Test bed

The NIDP as indicated in Figure 4.5 consist of built-in rules. Yet, the number of built-in rules do not determine its potency but the rule that is best in discovering attacks regardless of internal design or behaviour. Thus, Additional rules are implemented to capture malicious traffic and as a result capture attacks. Snort NIDP systems have a 7600 number of policies packed in its database.

4.3.2 Measurement Technique

The BAS metric is a novel scoring approach for a BYOD system develop by integrating available security methodologies. Hence, for the measurement of the unidentified vulnerabilities related to a BYOD system an OWASP risk rating methodology is first used to rate the likelihood of a vulnerability.

Furthermore, three Stages have been identified by which to model a BYOD scoring metrics for unidentified vulnerability situation as follows;

- The first stage, NIDPS rule is developed to monitor and safeguard the organisations BYOD network against vulnerabilities, this is used to examines unidentified attacks.
- Stage two is the establishment of the likelihood of vulnerability in a BYOD variable by using the OWASP risk rating methodology and based on a defined security attribute.
- The final stage is the BAS metric referred to in equation (3.10) and (3.11).

4.3.3 The first stage (Develop NIDPs rules to examine unidentified attacks)

In the case of the first stage, the identification and mitigation of the vulnerability of invisible attacks on the BYOD organisations network is examined. By means of Google advanced search engine, numerous Google dork commands are generated. During the cause of the study, confidential information such as Student ID, Password, Contact details and Exam score of the academic department is disclosed by Google dorks, to safeguard this information a signature-based NIDP system is positioned in between the firewall and web server as shown in the BYOD network topology in Figure 4.5 above. The essential objective of the firewalls is to deter access to particular services by operating as security personnel at the entrance of the network. Therefore, in the meanwhile, a NIDP system is adopted to Identify and register any effort of an unlawful intrusion attempt. It operates by conducting a profound scrutiny of data flow behind the firewalls. As mentioned in section 4.3.1, snort is the NIDP systems used for this research. Its flexibility and straightforward rule description language features make it a better

choice for this study, meaning Snort allows it, users to write down specific rules (policy) to filter the network traffic and mitigate invisible attacks. Figure 4.6, below shows the snort rule developed and tested and further stored in its database and applied as a rule

```
alert tcp $EXTERNAL_NET any → $HOME_NET 21 (msg: "Incoming FTP Connection! "; flags:S; sid: 60001;)
alert tcp $HOME_NET any → $ EXTERNAL_NET 80 (msg: "Vulnerability Information"; Content:" Unidentified Vulnerability "; NOCASE; sid: 60002;)
alert snmp $EXTERNAL_NET any → $HOME_NET any (msg: "Accepted information leak "; icode: 0; itype 8; sid: 60003;)
```

Figure 4. 6 Snort rules (policy)

As shown in Fig 4.6, a specific NIPD system rule policy can be divided into two sections:

1) Rule header; The section in the blue write-up represents the Rule header. The rule header essentially describes the packet's "who", "where" and "what", then offers the specifics regarding the packet response.

2) Rule options; The section surrounded in parenthesis is the rule options, whiles text ahead of the colons in the rule options part is dubbed option keywords.

The rule's action, protocol, source and destination IP address, and source and destination ports should be part of the rule header. The rule action, being the first field of the rule header directs the NIDP system towards the appropriate function upon locating a packet that meets its policy criteria. By default, five action rules are available in the chosen NIDP system. With every rule action explaining definite behaviour as follows;

Alert; causes an alert then logs the packet

Log; logs the packet

Pass; disregard the packet

Activate; alerts and triggers the dynamic rule

Dynamic; stays idle until activated by an activation rule, then functions as a log rule

In this first stage, the executed action is “Alert” this is very important because it is the objective of every network administrator to know the security condition of their network instantly for immediate action. The next field expressed in the rule header is protocol. Presently, the chosen NIDP system is able to scrutinise traffic for TCP, UDP and ICMP protocols for dubious descriptions. In the developed rule, the TCP protocol is used. It does not require the specification of source/destination IP and source/destination port numbers since the detail rule is in charge of monitoring traffic that is coming in and going out of any personal machine. The Alert messages and packet units being examined are illustrated in the rule options, this involves contents that the packet information would record for the packet to be highlighted as malicious. In this case, should a packet include some Google dork operators such as filetype, allintext and allintitle within the message contents, then NIDP system will signal the administrator via a generated message formed in the subsequent field of the rule options section? The additional fields in the rule option units are thresholds, which indicates interval alerts. Regarding the created rule, an alert is formed every two (2) minutes for the type limit. Figure 4.7, below shows the generated alert based on the specified rule for a Google dork operation on the network

Figure 4. 7 an illustrated alert obtained once as a test case

After adding the generated rule to the NIDP system rules database it assesses the Organisation's variable (Network and user) against invisible attacks, particular commands are produced, which are discovered by the implemented organisations NIDP system as shown in Figure 4.7, the results accomplished in stage one (1) indicates that by establishing a rule within the NIDP system, a network is able to be protected against invisible attacks. Chapter 3, Table 3.3 shows the taxonomy of the invisible attacks collected as a result

4.3.4 Stage Two; The Establishment of probable vulnerability in a BYOD environment

It is vital to establish the risks and facts of vulnerability in a BYOD system. However, it has become important to assess the attack associated with the organisation quantitatively. For this reason, the OWASP risk rating methodology is utilised to assess the vulnerability security level of the department of an organisation against invisible attacks. The OWASP tool has been chosen for this research because of its simplicity and capability towards the challenges being faced by web application. Thus, due to its features, numerous security administrators and security designers prefer using it.

In the BYOD situation, coming from the viewpoint of an attacker, an attacker takes advantage of an organisation's unidentified vulnerabilities by using the Google advanced search engine to develop invisible attacks which takes an organisation's confidential information. The BYOD risk methodology is made up of three (3) phases, and it’s illustrated as follows;

1. **Phase I Risk Identification**

The first phase of the risk model involves the identification requirement being rated. Because a system administrator gathers information concerning threat agents, vulnerabilities, attacks plus their impacts on an organisation. For the purpose of the BYOD employed department, the threat agents are the organisation variable (students and staff). This group use their mobile devices to access information from the organisation variable(Network). The vulnerabilities detected in this circumstance is the username and password, these can be exploited by the threat

agents to accomplish their goal. But, for the purpose of this study Google dorks is considered as a threat to BYOD service whilst the agent is the organisation variable (students and staff).

2. Phase II Features for assessing likelihood

Factors that influence the assessment of vulnerability likelihood are further categorised into two:

1) Threat agent features = Students and staff being BYOD users

2) Vulnerability features. For example, Aca (L) = the choice in the likelihood factors, where "P" = the specific attribute and "L" = likelihood of impact level

a. Threat agent features

Threat agents are identified as an individual attacker or a group of attackers that essentially produces incidence. Additionally, the factors(features) required in the framework of a threat agent to assess the probability of a fruitful attack are skills level, motivational level, opportunity and size of the threat. So, the vulnerability impact value related to each characterised threat agent features labelled A1 to A4 is deliberated below;

AI) Skill level

This indicates the attacker's ability to exploit the vulnerabilities of the system. Diverse selection on threat agent's skills are given below.

× No technical skills (1)

✓Some technical skills (2)

×Advanced computer user (5)

×Network and programming skills (6)

× Security penetration specific (8)

Featuring this specific scenario, “Some technical skills” is a better choice to weight on, since it does not necessitate any penetration, programming or advanced skill to retrieve vulnerability of the network.

A2) Motive

Motive signifies the level of interest of threat agents exploiting the weaknesses of the network system.

× Low or no reward (2)

✓Possible reward (3)

× High reward (9)

Selecting the “Possible reward (4)” option from the list is suitable because usually, threat agents ask questions about an organisations information during exploration. This is an information collection phase. Therefore, the documented information is used for assessing the value related to the possible attack on the company. Since the organisation under deliberated is not secure; therefore, the gathered information could be composed to access systems having company financial data and its resources.

A3) Opportunity

Opportunity summaries the resources needed for an attacker to control and exploit the vulnerable components of the network.

× Full access or expensive access required (0)

× Special access or resources (2)

✓Some access or resources required (8)

× No access or resources required (7)

“Some access or resources required (8)” is a better option to choose from the specified choices as the threat agent barely needs to access the invisible attacks by exploiting time, Internet and a suitable Google dork commands.

A4) Population size

The population size defines the number of people participating in causing the attack, in addition as exploiting the vulnerability of the system.

× Intranet users (3)

× Partners (5)

× Authenticated users (5)

✓ Anonymous Internet users (9)

“Anonymous Internet user (9)” is a better option to emphasis on since severity risk assessment is related to the Internet particularly from outside the network.

b. Vulnerability Factors

The aim of this feature is to predict the probability of detecting and exploiting particular system vulnerabilities. Let’s assume an attacker has adequate knowledge on the use of Google dork operators and understands how to develop a command from these operators so as to query particular vulnerabilities.

The factors that influence the detection, as well as exploitation of the system vulnerability, are labelled from B1 to B4 below.

B1) Ease of discovery

Different vulnerabilities come with different detection levels which is influenced by the attacker’s skill in addition to the tools essential in creating potions. The Following are the range of options used to establish how to discover a vulnerability.

× Not relevant (0)

× Practically impossible (1)

× Demanding (2)

✓ Easy (5)

× Automated tools available (8)

The appropriate option to select is the “Easy (5)” because it has become simple to detect vulnerability by Google dork operators and does not require any other device or sophisticated skills.

B2) Ease of Exploit

Having detected the vulnerability, it has become necessary to measure how easy to apply it in order to compromise the system.

× Not relevant (0)

× Theoretical (2)

× Demanding (4)

✓Easy (5)

× Automated tools available (9)

Because the information uncovered during the research is very sensitive and can be exploited by threat agents to gain entrance into different organisations network resources easily, therefore, “Easy (5)” is the appropriate option to select from the listed options.

B3) Awareness

This factor explains in what way the attacker knows the vulnerability.

× Not relevant (0)

× Unknown (2)

✓Hidden (4)

× Obvious (5)

× Public knowledge (8)

“Hidden (4)” option is the best choice among the selected vulnerability detected via Google dorks.

B4) Intrusion detection

This factor assesses intrusion based on the exploitation of vulnerability by the system Intrusion detection countermeasures.

× Not relevant (0)

× Active discovery in application (2)

× Logged and reviewed (2)

✓Logged without review (9)

× Not logged (8)

Table 4. 5 and Table 4. 6 shows the Threat agent factor and vulnerability factors with their selected options.

Threat agent factor	**Selected options**
Skill level	Some technical skills(2)
Motive	Possible reward (3)
Opportunity	some access or resource required(8)
Population size	Anonymous internet user(9)

Table 4. 6 Threat factors and their selected options

Vulnerability factors	Impact
Easy of discovery	Easy (5)
Ease of Exploit	Easy (5)
Awareness	Hidden (4)
Intrusion detection	Logged without review (9)

Table 4. 7 vulnerability factors and their selected options

3. Phase III Factors for Assessing Impact

Once vulnerabilities are exploited, the BYOD employed network with its resources is exposed to harmful factors, Therefore measuring the impact of an attack on the organisation or user level is necessary. These factors are discussed and measured based on the user level.

Using the expression P (L) to signify option in the impact factors.

Where P= specific feature,

L=describes the impact level

Hence, the impact value level is assessed based taxonomy below;

A) Technical Impact value Factors

This impact value factor defines the influence of the attack on the organisation variable. By means of a define security requirement attribute of both the employed BYOD organisation and the user. Based on the department define in this study, the impact factors(security attribute) are categorised into confidentiality, integrity, availability and accountability.

- **Decomposition of BYOD user Security Requirements**

The term decomposition is the break down into smaller segment a whole scheme. There are various discussions on the use of decomposition in security measurement, the requirements were started by (Wang & Wulf, 1997) and subsequently used by authors like Savola and Abie

in their Basic Measurable Components (BMCs) (Savola & Abie, 2009). So, BYOD security attribute(requirements), decomposes by

a. Find successive factors from each security requirement that impact at a level suitable to the security suitability, efficiency and flexible
b. Analyse the dependent factors to ascertain if further decomposition is necessary;
c. End decomposition once there is no need for any other leaf nodes to be decomposed.

Also, a target type must be defined. This includes the physical security that is protection of organisations assets such as information, hardware and software from threats. Whilst User security comprises the protections of BYOD engaged users (information. hardware, Education) (Ramos et al., 2017). Hence Figure 4. 8 below shows the scenario used in the decomposition of confidentiality security attribute

A1 Loss of Confidentiality

The loss of confidentiality impact assesses the sum of data that is likely released by invisible vulnerability.

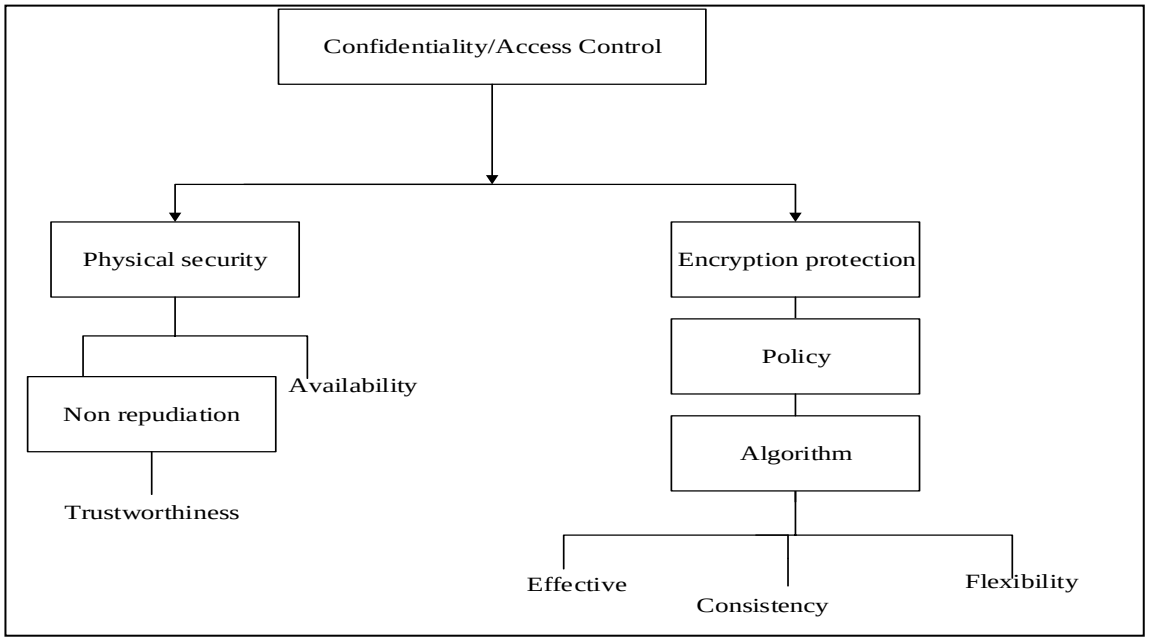

Figure 4. 8 Loss of confidentiality

× Not relevant (0)

× Insignificant non-sensitive data disclosed (3)

× Extensive non-sensitive data disclosed (7)

✓Extensive critical data disclosed (6)

× All data disclosed (8)

The data released in the case study includes confidential information example usernames and passwords which could be used to gain access to both user and organisations network .this is illustrated in Figure 4.9 requirements.

A2 Loss of integrity

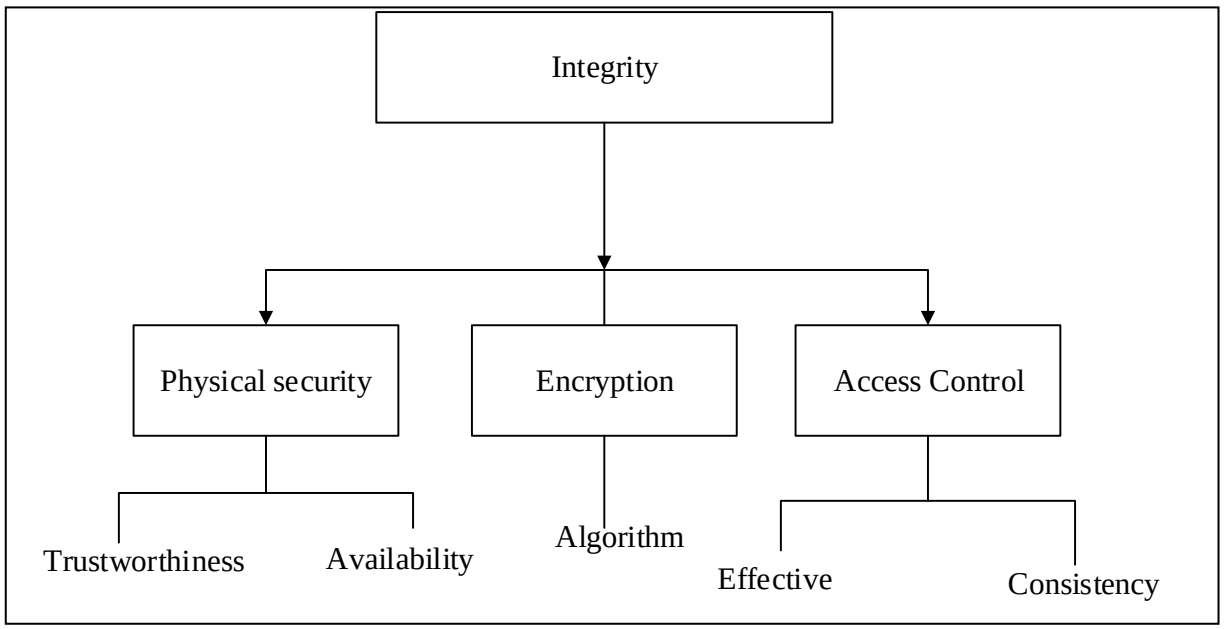

Figure 4. 9 Loss of integrity requirement

The loss of Integrity as illustrated in Figure 4.9, assesses the sum of data that is likely to be corrupted or damaged in the situation of a successful attack.

× Not relevant (0)

× Insignificantly slightly corrupt data (2)

× Insignificant seriously corrupt data (2)

× Extensive slightly corrupt data (6)

× Extensive seriously corrupt data (5)

✓ All data totally corrupt (8)

In the analysis process, it was discovered that the information that was store have

Login with maximum user privileges over several network resource in the academic department, and in addition causes an alteration in the entire organisation's data. This is because a modification in one instance affects a data in the other, thus, all other resources in the department can be modified.

A3 Loss of availability

This Figure 4. 10. below, which is availability requirement assesses ways a vulnerability being exploitation can impact the network BYOD services availability.

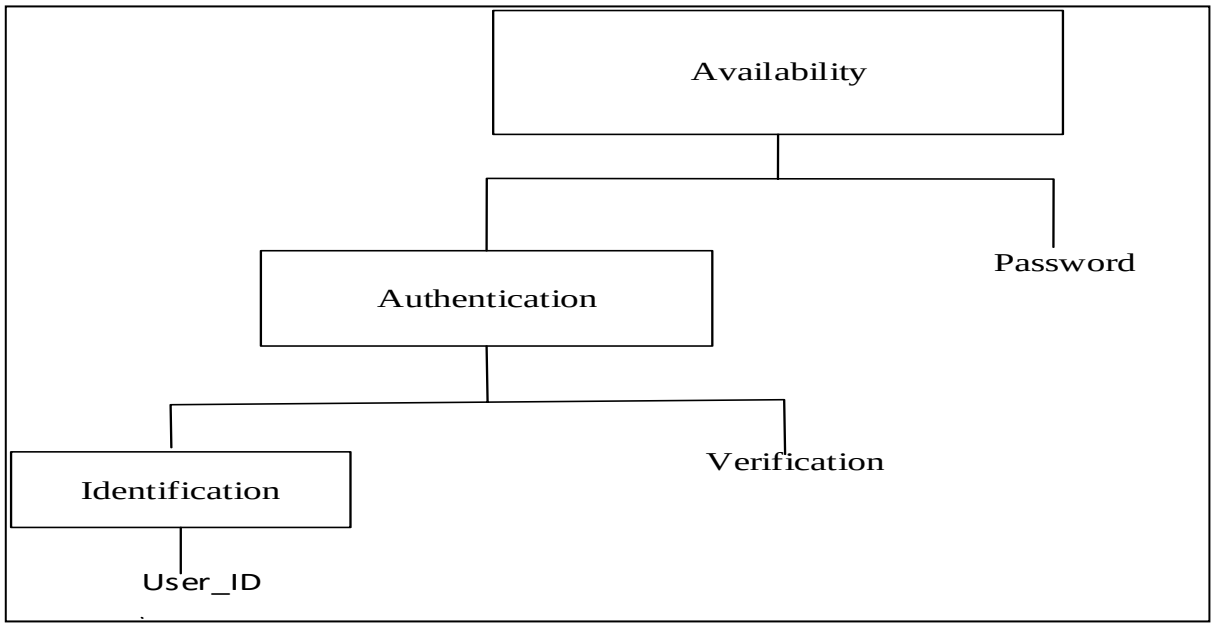

Figure 4. 10 Availability requirement

Using the scenario in a set of questions as follows;

- Will the attack causes the network to shut down?
- Will the attack cause any form of interference in the BYOD service?
- In what critical way will be the impact of services on the performance of the BYOD network and its users?

To respond to the above-stated issues, selecting from the itemised options can assist to quantify the impact of a loss of availability on the user.

✓ Not relevant (0)

× Insignificant secondary services interrupted (3)

× Insignificant primary services interrupted (6)

× Extensive secondary services interrupted (8)

× Entire services lost (9)

Not relevant is picked, because the information access is from the Estate department, hence login details will present no impact on the network services. But, this accepted information on the BYOD employed network and its user can be the basis for an attacker to disrupt services.

A4 Loss of accountability

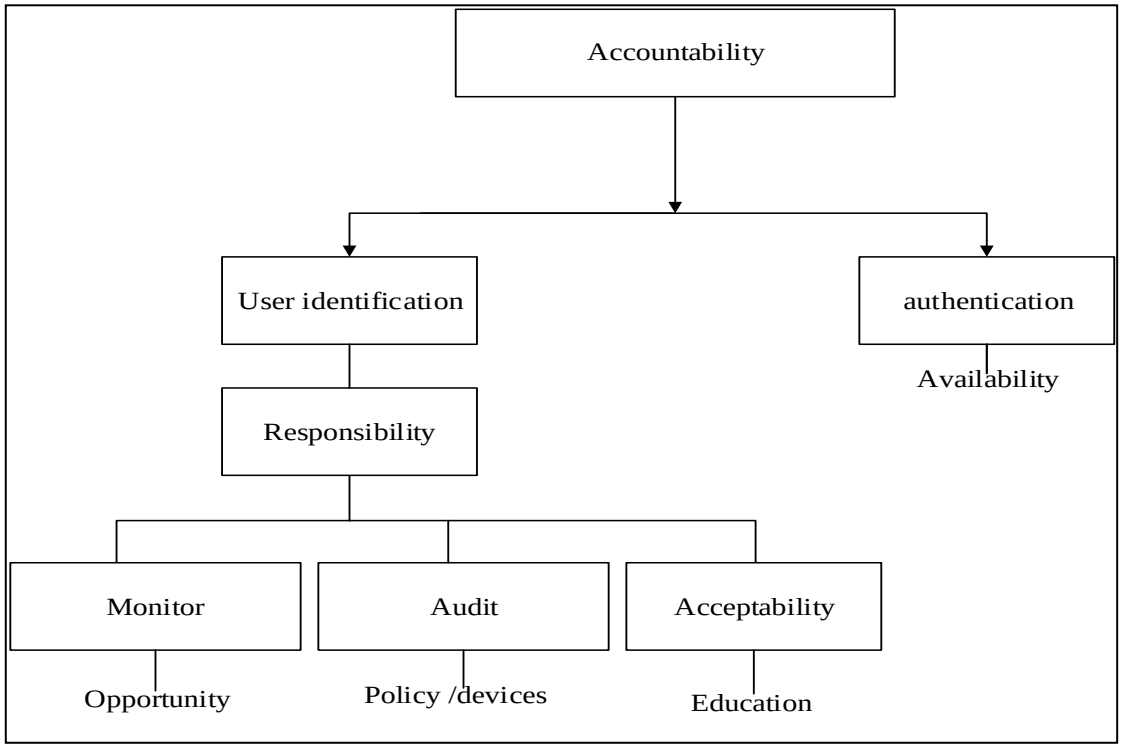

Figure 4. 11 Accountability requirement.

The accountability requirement illustrated in Figure 4.11 above, occurs once a system has been compromised, this factor aids in quantifying how security countermeasures are able to efficiently trace where the modification occurs and bring them towards the point of exploitation.

× Attack fully visible to individual (2)

✓Attack likely visible to individual (6)

× Attack fully unknown (8)

Selecting the text “attack likely visible to individual (6)” option in the itemised choice is a better choice since the security countermeasures make any form of system modification made

by the attacker such as alteration of user login to become visible. This does not in any way hold the lawful user accountable for abuse of its account. However, it is viable to get hold of the account but nearly impossible to reach the person producing the attack.

B Business Impact Factors

This deliberate on what is essential to the organisation and its users from an application approach. These impact factors are the regular fields (organisation business objective) for various organizations and are specifically unique to an organisation than the above-mentioned factors related to threat agent, vulnerability and technical impact. Some details of these factors along with their corresponding options are given below. In the case of BYOD metrics, the financial impact is not considered.

B1 Trust violation

This factor affects the way users view a BYOD service, thereby losing many important clients in addition to goodwill.

× Not relevant (0)

× Minimal damage (1),

× Loss of major accounts (5)

× Loss of goodwill (6)

✓trademark damage (9)

The preferred option is “trademark damage (9)” because once the organisation has been affirmed as compromised; it becomes a challenge for it to realise the client trust again.

B2 Non-repudiation violation

This seeks to answer, how much vulnerability expose does Non-repudiation introduce? The decomposition is illustrated in Figure 4.12 below.

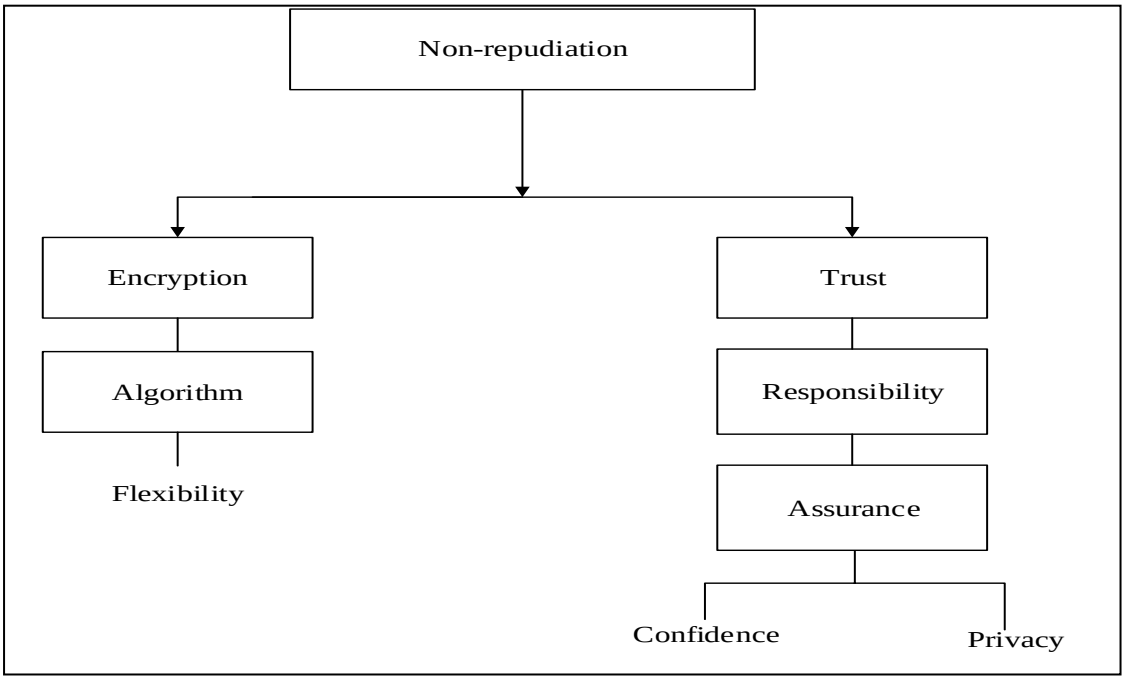

Figure 4. 12 Non-repudiation requirement

× Not relevant (0)

× Minor damage (3)

× Clear damage (6)

✓High profile damage (9)

High profile damage is a Preferred Choice to select for This Scenario.

B3 Privacy Violation

This factor holds a number of causes, for instance, loss of confidential data (Personal) could result in identity violation, and loss of confidential data (commercial) may result in legal liabilities. The decomposition is illustrated in Figure 4.13 below.

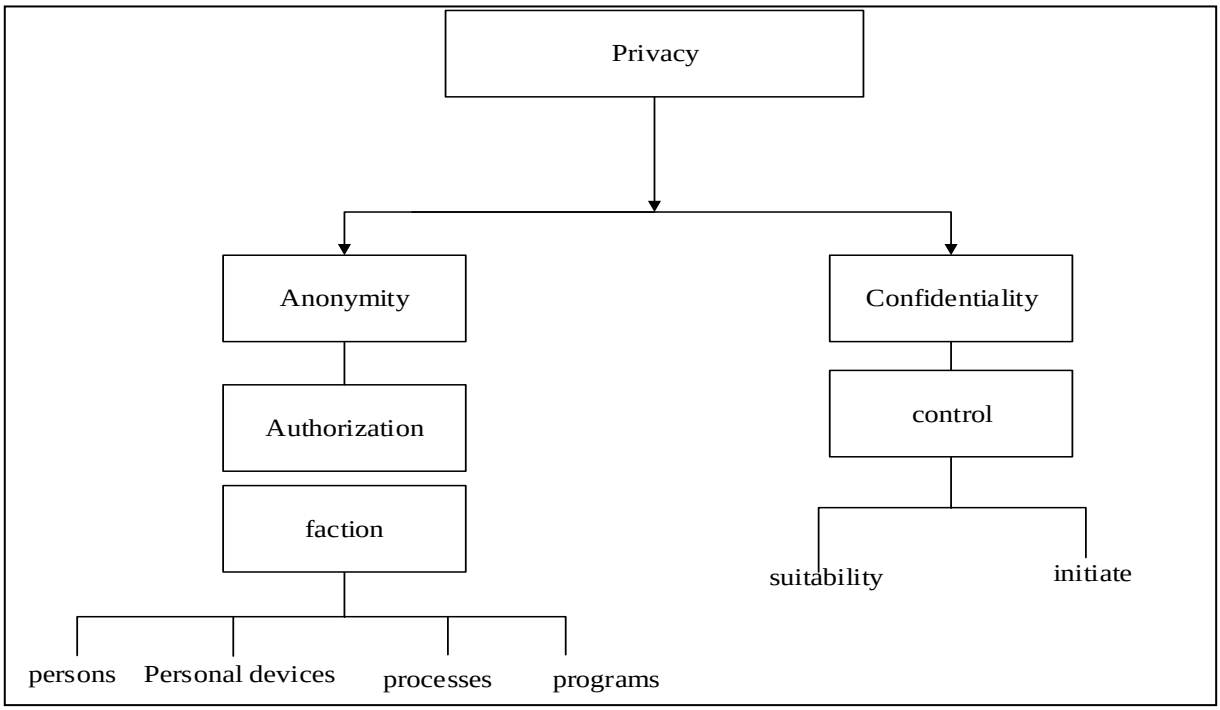

Figure 4. 13 Privacy Violation

× not relevant (0)

× One individual (5)

✓Hundreds of people (7)

× Thousands of people (8)

× Millions of people (9)

The sub-organisation under consideration is a small organisation, therefore, the “hundreds of people” is the preferred option of information disclosure, meaning the bigger organisation will effect bigger information disclosure exploitation. Table 4.8 and Table 4.9 shows the technical and business factors and their selected options respectively

Technical Impact Factor	Preferred Options
Loss of confidentiality	Extensive critical data disclosure(6)
Loss of Integrity	All data totally corrupt (8)
Loss of availability	Not relevant (0)
Loss of accountability	Attack likely visible to individual (6)

Table 4. 8 Summary of the selected preferred options for both technical impact factor

Business Impact Factor	Preferred Options
Trust violation	Trademark Damage(9)
Non-repudiation violation	High Profile Damage (9)
PRIVACY violation	Hundreds Of People(7)

Table 4. 9 Summary of the selected preferred options for both Business impact factor

Step-IV: Establishing the severity of the risk

The number of preferred options for the severity level is grouped from 0 to 9 and sublevel 0-3, 3-6 and 3-9 representing the impact level in the order of low, medium and high as shown in Table 4.10 below.

Security range	Severity level
(0, 3)	low
(3, 6)	medium
(6, 9)	high

Table 4. 10 severity level representation

The calculation of the overall severity risk level is based on the estimation of the likelihood and impact level of the security risk assessment. These are denoted by low, medium and high in Table 4. 11 below

	Severity level		
LIKELIHOOD	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

Table 4. 11 Estimation of the likelihood and impact level of the vulnerability assessment

Lastly, the total vulnerability impact level of the invisible attack on the Academic department is evaluated as follows,

nL = Total number of options chosen from the likelihood

nI= total number of Impact factors

LS= likelihood value and

IS= Impact factor value

ACA_L(L) = An individual value of the particular likelihood options being chosen.

ACA_I(L) = An individual value of the particular impact options being chosen.

$$LS = \frac{1}{n_l} \sum ACA_L \ (L) \qquad (4.1)$$

$$IS = \frac{1}{n_i} \sum ACA_I \ (I) \qquad (4.2)$$

Using the equation (4.2) and (4.2) the likelihood and impact value are calculated, this is shown in table Table 4. 12 below.

Equation	results
(4.1)	ACA_L(L) = 5.62 Likelihood factor score
(4.2)	ACA_I(I) = 6.62 impact factor score

Table 4. 12 likelihood and impact factor measure value

Since, the likelihood score falls within the severity risk impact level of (3, 6) meaning $LS \in$ (3, 6), making it a medium risk severity level, also the impact score falls within the severity risk impact level of (6, 9), meaning I$S \in$ (6, 9) making it a high-vulnerability severity level, in reference to the above description in table 4.9 and table 4.10 respectively. The noted corresponding risk severity level for {(medium, high), medium ∈ likelihood and high ∈ impact} is high. Consequently, the total impact level value for the academic department in the scenario affected by unidentified attack is high.

4.3.5 Stage three; BAS Metrics Results

The BAS metrics is a combination of distinct metrics to create novel metrics for BYOD organisation variables for unidentified vulnerabilities (for instance, we combine OWASP methodology value and probability-based metrics to form an Absolutes Percentage score. This is shown in Figure 3.2). Therefore the Absolutes Percentage score which signifies the severity impact for each department is calculated using the OWASP risk methodology of likelihood factor score and impact factor score average as applied in Eqn 3.10. Consequently, From Eqn 3.11, the BAS Metrics for the Unidentified Vulnerability is scored. Table 4.13 below shows the result for the BAS metrics in Percentage.

s = 8 (CVSS impact scores of related Unidentified vulnerability data)

ACA_L(L) = 5.62 (Likelihood factor score)

$ACA_I(\mathrm{I}) = 6.62$ (impact factor score)

Absolutes score	% BAS metric
6.12	0.14%

Table 4. 13 likelihood and impact factor measure value

In reference to Table 4. 3 the likelihood severity level is high representing the impact level Thus, within the scenario the BAS metrics of 0.14% as shown in table 4.13 above, signifies the fine value since it has the lowest score of the BYOD security level. Thereby the success rate for a BYOD organisation variable(user, network) to be exploited by an attacker is low.

4.4 Conclusion

This chapter explains the application of BAS metrics, It involves the application of each BAS section and stages which influence the activity of the measurement. Data collection using Google dorks commands and Nessus scanner have been used to prove the existence of both unidentified and known vulnerabilities. This model addresses the issue of achieving security goals quantitatively in a BYOD domain. The procedures of suggested %likelihood and impact level value have been tested. Results showed BAS metrics are capable of predicting vulnerability security level of a BYOD employed system numerically, thereby helps in achieving BYOD security goals. Chapter 5 describes in details the evaluation process for the measurement.

CHAPTER 5 EXPERIMENTAL EVALUATION

5.1 Experimental Study

The authors (O'Leary & O'Keefe, 1993), indicate the importance of an approach or metric is being “suitable” with regards to its proficiency since an unsuitable system has the potential of causing damaging errors. In Principle, a security metric is able to evaluate the absence of vulnerabilities (Wang A. A., 2005). But, in practice, the immense complexity of a systems problem indicates by no means can an approach details the absolute assurance that a system is safe (Bishop, 2003; Wang A. A., 2005). Thus, a model’s accuracy might although turn out sufficient by means of its estimates, as being inaccurate, points to the desirable conclusions (O'Leary & O'Keefe, 1993). Implying, the precise scores provided by BAS metrics may possibly not be extremely important. Instead, it is vital for the relative ranking in terms of vulnerability be reasonable. Again, (O'Leary & O'Keefe, 1993) discussed that a proficient system can be evaluated both on a component level and on a system level. Component level evaluation relates to analysing the distinct “segments” of the system and system-level evaluation involve analysing the entire operation of the system. All components in BASmetrics has been quantitatively evaluated by experiments and/or surveys. For instance, the effectiveness of vulnerability scanning tools was initially research within a literature review, then by an experiment, and finally by case studies. The main objective of this evaluation is to establish if the feasibility of the proposed measurement technique, which considers security metrics integration and individual attribute classification concepts for a BYOD situation, is better than the present BYOD network security methods, which does not consider individual attribute classification concepts for a BYOD situation. This chapter explains the experimental setup and reports the observed results.

To attain the objectives, we carried out the experiment by deploying the network of a sub-organisation that is a segment of a bigger organisation, with the sub-organisation made up

different departments and the network has a set of host Hs and vulnerability Vs. These notations are adopted for the evaluation.CVSS is also utilised as the basis for the system because it has extensive coverage of security expressions. The results presented by metrics are in numerical values and can be clearly understood by most users. The ranking of the metrics will depend on how convenient is to be applied to the participating BYOD employed network with lots of vulnerabilities. Calculations results were achieved via Microsoft Excel.

5.2 Experimental Description

The scope of this experiment is devoted to the Controller and Accountant Generals Department, located at Ministries which is a sub-organisation connected to a central organization in Accra by a wireless network. network management such as audit, monitoring and reporting are performed at the sub-organisation. Figure 5.1 shows the network topology of the assign organisation.

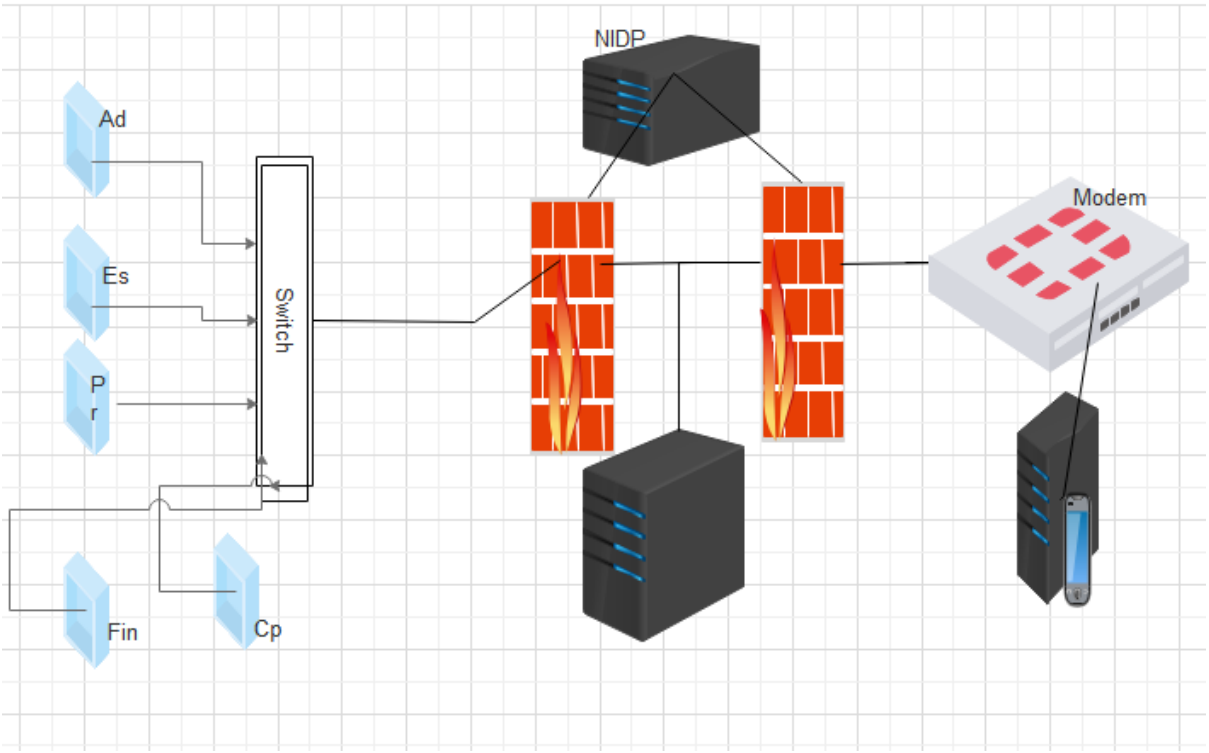

Figure 5. 1 Network topology of the Ministries Sub-Organisation

The network topology of the Ministries sub-organizations as shown in Fig.5.10 comprises 5 departments labelled (Ad, Es, Pr, Fin, Cp), with 2 servers namely network storage server(FTP) and web server (provides services to the mobile devices with different operating systems) respectively. The experiment lasted for a month that is from July-August 2018 in which data is collected on the number and characteristics of the identified vulnerabilities in the computer networks via Nessus version 7.1.1. There are two firewalls on the network and a network intrusion, Detection and prevention (NIDPS) device is placed in between them. Here, the inner firewall is used to safeguard the connections from the Internet to the network storage server while the outside firewall is used to allow secure connections to the web-server hosting the users, there are seven(7) host on the network, with a host in each department and the 2 servers also functioning as host, this has been labelled (h_i where i = 1, 2, 3…, n). The NIDP device placed between the firewalls allows for deep packet inspection technology, as shown in Figure 5.1, all packets that go towards and from the perimeter of the sub organisation is evaluated. With a Cisco Catalyst 2960X-24PD-L Switch and an IP service software as a wireless controller.

Each of the hosts are scanned using the Nessus vulnerability scanner, which shows details on open ports and vulnerabilities related to the host. Also, Common Vulnerabilities and Exposures (CVE) (MITRE, 2017) score on the relevant vulnerability of individual host as detected by Nessus, This is to allow simplicity in the evaluation. Table 5.1, below list the characteristics located in the host on the network. H_number signifies host number.

H_number	Open_Ports	Operating system	Known_Vulnerability			CVE-ID
			High	Medium	Low	
1	2	Apple IOS 12 Phone XS	1	1	9	CVE-2018-11281

2	4	Android 8.0 Samsung galaxy s8 /s8 plus	1	2	35	CVE-2018-14987
3	5	Apple Mac OS X 10.3.9	0	1	12	CVE-2018-14985
4	7	Android 7.0 Nougat Samsung Galaxy Note 5	0	3	18	CVE-2018-11259
5	5	Linux 2.6.18-308.24.1.e15	0	3	19	CVE-2017-8416
6	3	Microsoft Lumia 950 windows 10	1	2	24	CVE-2017-9831
7	3	Android 8.1 Oreo Moto G5 Plus	2	5	27	CVE-2016-6910

Table 5. 1 List of Vulnerability assigned Host

5.3 Evaluation Metrics

There are many procedures for evaluating security metrics systems. The evaluation involves the use of two analysis, one for the known vulnerability and the other the use of Snort as a security level experimental methods. The two evaluation methodologies will be discussed in detail in the following subsections.

5.3.1 **Security Analysis of the Example Network**

We use the exampled network in Figure 5.10 on existing security metrics such as MTTC and VEA_bility to execute security evaluation via the BYOD situation. Since the main organisation has a network Security management structure which is accessible. For efficacy, therefore, the

ministries sub-organisation security evaluation will focus primarily on BYOD monitor which is the scoring of the security risk level. vulnerability scanners such as Nessus is used to discover the network vulnerabilities (known). The objective of the study is;

- To compute MTTC and VEA_bility values of each sub- organisations network for department Ad, Es, Cp, Pr and Fin.
- To compare the security level of different network configurations for departments Ad, Es, Cp, Pr and Fin.
- To compute MTTC and VEA_bility, BAS score of the entire network. BAS score from chapter 4
- To compare the feasibility and ease of using BAS, MTTC and VEA_bility metrics in this study.

5.3.2 Mean Time-to-Compromise Metric (MTTC)

MTTC is the period assessment needed by an attacker to break into a system successfully in unit of days (McQueen, Boyer, Flynn, & Beitel, 2006). MTTC is a computation used for quantifying the risk established on system vulnerabilities and an attacker skill level. For example, the calculation is dependent on the attacker's level of skills and class of vulnerability. The higher value of MTTC score, the higher the level of network security and the lower the level of risk (Leversage & Byres, 2008). The actions of an attacker are divided into three statistical processes. However, the various equation from process 1 to 3 is realised from the master equation, which signified total time taken for the three processes to be compromise

$$T = t_1 P_1 + t_2 (1 - P_1)(1 - u) + t_3 u (1 - P_1) \qquad (5.10)$$

Where n indicates the nth day in time t ($t_1\ t_2 \ldots \ldots tn$).

- Process 1 (P1): this is when the attacker has discovered at least one known vulnerability and has at least one exploit accessible. The probability that the attacker is in process1is given as

$$P_1 = 1 - e^{-\left(\frac{\alpha VM}{K}\right)} \quad (5.11)$$

Where;

V= number of vulnerabilities found in the unit of concern

M= number of exploit accessible to an attacker

K= the number of vulnerabilities(Known) available in the National Vulnerabilities Database (NVD)

α = visibility factor

The values of k,v, m, and α and their features are given in Table 5.2.

Variable	Definition	Variable
K	Available total number of non-duplicate known vulnerability	9447
V	Total number of vulnerabilities per host	Low, medium, High
m	Possible number of exploit accessible to an attacker	150(beginner) 250(intermediate) 450 (expert)
α	Visibility reduction factor of vulnerabilities due to	1 (no review) 0.3 (semi-annual)

	boundary devices such as firewalls (depends on the number of security reviews conducted during a year)	0.12 (quarterly) 0.05 (monthly)
p	Likely value to quantify the attacker skills level	0.5(beginner) 0.9 (intermediate) 1 (expert)
$\frac{AN}{V}$	The ratio of the average number of vulnerabilities that can be exploited depending on the level of skills of the attacker to the total number of available vulnerabilities of unit concern	0,3(beginner) 0.55 (intermediate) 1 (expert)

Table 5. 2 Features and Constants For MTTC Calculations

Also, an attacker skills level is classified as;

- Beginner: signifies an attacker just able of applying existing code, tools and attack methods.
- Intermediate: signifies an attacker that is able to revise existing code, tools and attack methods.
- Expert: signifies an attacker able to developing new code, tools and attack methods

V = Total vulnerabilities for a host is obtained by the equation (5.15) below since V is equated by either Low, Medium and High

Therefore V= $0.1vl + 0.5vm + 1vh$ (5.12)

- Process 2 (P2): this is when the attacker has discovered at least one known vulnerability but has no accessible exploit, and with the assumption that the Process 1 and Process 2 cannot occur at the same instance. Thus, the probability of an attacker's presence in Process 2 is given by:

$$P_2 = e^{-V*M/K} = 1 - P_1 \quad (5.13)$$

Based on Average-Time-to-Compromise Metric (ATTC) (Leversage & Byres, 2007).The assumption of time is denoted by t_2. Likewise, this instance is also used by (McQueen, Boyer, Flynn, & Beitel, 2006; Turner, et al., 2004), to indicate the average time vulnerability is publicised on the accessibility of exploited code as;

$$t_2 = 5.8E \quad (5.14)$$

Where E = estimated number of tries by an attacker, t_2 being the estimated value of process 2

Therefore

$$E = \frac{AN}{V}\left(1 + \sum_{tries=2}^{V-AN+1}\left[tries \prod_{i=2}^{tries}\left(\frac{NM - i + 2}{V - i + 1}\right)\right]\right) \quad (5.15)$$

Where ;

AN= Average number of vulnerabilities that can be exploited depending on the level of skills of the attacker

NM = Number of vulnerabilities the attacker is unable to use irrespective of their skills level

V = Number of vulnerabilities on the unit of concern.

And V is found using

$$V = AN + NM \quad (5.16)$$

The ratio $\frac{AN}{V}$ value is specified in Table 5.I1.

- Process 3 (P3): this is when there is no data on known vulnerability and its exploit. That is an Unknown vulnerability (UV) is predicted in the next period (time) based on pass exploit. Hence this is dependent on the success of process 2.

Therefore;

Using the (Leversage & Byres, 2008) approach and introducing the proficiency level (P) of the attacker instead of AN/V from the Mcqueen approach, the probability of process 2 being unsuccessful is given by

$$U = (1 - P)^{\alpha V} \tag{5.17}$$

Where;

The values o P shows the attacker skills level, thus the possible value of P is provided in Table 5.12. The time employed in Process 3 is denoted by t_3,

$$t_3 = 30.42\left[\left(\frac{1}{P} - 0.5\right)\right] + 5.8 \tag{5.18}$$

Subsequently using the Mcqueen approach the equation (5.17) and (5.18) and becomes (5.19) and (5.20) respectively ;

$$U = \left(1 - \frac{AN}{V}\right)^{\alpha V} \tag{5.19}$$

$$t_3 = 30.42\left[\left(1 - \frac{AN}{V}\right)\right] + 5.8 \tag{5.20}$$

5.3.2.1 MTTC Evaluation Results

System backup and firewall updates are executed by the Network Administrators of the sub-organisation on a monthly basis, and so from Table 5.11 above the value of α = 0.05. the final score for the MTTC metrics is presented in Table 5.12, this indicates the MTTC scores for each

host located in the building of Ad, Es, Pr, Fin, Cp, as well as the total MTTC score this is the mean score of the entire network, related to the attacker level of skills. The MTTC is used to assess the time needed by an attacker to exploit a system successfully within days. Meaning the higher the MTTC score the higher the level of network security and the lower the level of risk.

HOST	DEPT	MTTC where α= 0.05		
		Beginner	Intermediate	Expert
1	Ad,FIN	74.46	28,62	0.00
2	Cp	76.18	30.25	5.78
3	Pr	70.29	28.89	3,39
4	Fin	72.69	30.06	2.64
5	Cp, Pr	73.36	29.66	13.88
6	Pr, Es	75,69	30,72	6,28
7	Es	71.36	29.40	20.48
Overall_MTTC(days)		73.43	29.50	4.98

Table 5. 3 MTTC score for Hosts in the departments

A chart comparing the MTTC score versus the number of vulnerabilities is illustrated in the Figure. 5. 2, the graph shows a declining pattern in the score for beginner and intermediate skills levels of attackers. This appears with the MTTC theory as the higher the MTTC score, the higher the security level of the recommended network and the lower the level of risk. But this is not noticed in the expert level of attackers as the graph shows an upward trend, therefore it is not consistent with the MTTC theory. This is because values for the number of vulnerabilities used in plotting the graph are treated general and not categorised into low, medium, high, or critical risk level. (use this in the comparison)

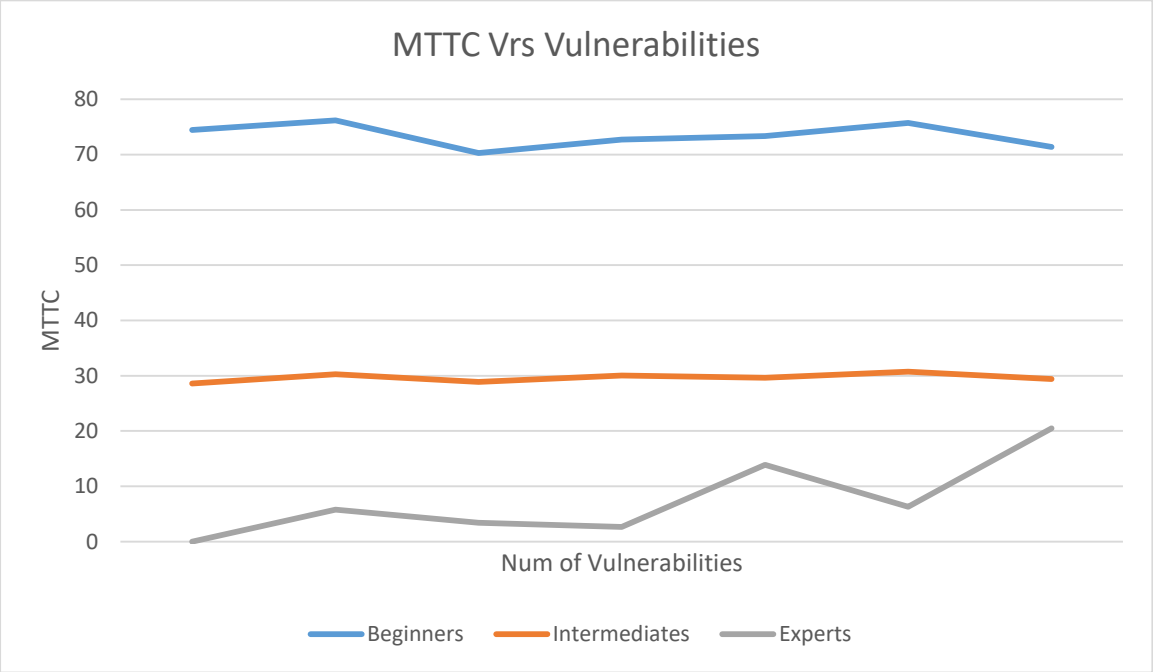

Figure 5. 2 Chart Of MTTC Vrs Vulnerability

5.3.3 Applying the VEA_bility metric to a network

The VEA_bility (Tupper & Zincir-Heywood, 2008) measures the security level of an organisations computer network and presents it scores quantitatively, it also established on the CVSS scoring system (Scarfone & Mell, 2009) and is expressed to acquire the various factors that impact the security of a network. Together with three elements Vulnerability, Exploitability and Attack ability expressed as V, E and A respectively its scored. Each of the three elements scored is a numeric value in the range [0,10].

- Host Dimension

The Temporal score(Ts), Impact score(Is) and Exploitability score(Es) assigned by the CVSS of a known vulnerability is used to obtain the severity(S) of the vulnerability. We define

severity(S) of the vulnerability to be the average of the Impact score(Is) and Exploitability score(Es). The severity(S) of the vulnerability is defined as

$$S = (I_S + T_S) \div 2 \quad (5.21)$$

For each of the Host located on the BYOD employed network, we then define the three dimensions based on the total number of known vulnerabilities

vulnerability on BYOD host Device is analysed as shown in Equations BYOD

V(ph) which represents the level of Vulnerability in BYOD Host

$$V(ph) = min\left(10, \ln\left[\sum e^{s(v)}\right]\right) \quad (5.22)$$

Exploitability(BYOD Host) $= E(ph)$

$$E(ph) = \frac{spd}{sn} min\left(10, \ln\left[\sum e^{Es(v)}\right]\right) \quad (5.23)$$

Attackerbility(BYOD Host) $= A(ph)$

$$A(ph) = 10nap/_{nnp} \quad (5.24)$$

Where spd = number of BYOD services on the host.

Sn = number of BYOD services on Network.

nap = number of attack paths

nnp = number of network path

- Network Vulnerability Dimensions

The vulnerability of the entire BYOD network depicts the degree to which an exploit is able to impact a system. The subsequent values for the entire network is gained from,

Vulnerability(BYOD employed network) $= V(n)$

$$V(n) = \min(10, \ln[\sum(e)\, V(ph)]) \quad (5.25)$$

Exploitability(BYOD employed network) = $E(n)$

$$E(n) = \sum E(ph) \quad (5.26)$$

Attackerbility(BYOD employed network) = $A(n)$

$$A_{n=\sum A(ph)} \quad (5.27)$$

Therefore the final VEA_bility score on an entire employed BYOD network is calculated by

$$BYOD(N) = 10 - ((V(n) + E(n) + A(n))/3) \quad (5.28)$$

5.3.3.1 VEA_bility Results

VEA_bility calculation results of each Host as per the building Ad, Es, Fin, Pr and Cp is shown in Figure 5.3. The value of VEA_bility is presented in the range [0,10], meaning the scores above the value 10 are recorded as 10. The final VEA_bility score is also presented in Table 5.4 below.

HOST	DEPT	V	E	A	VEA_bility
1	Ad,Fin	0 .00	0.00	0.00	0.00
2	Cp	10.00	10	0.00	3.33
3	Pr	10.00	5.47	0.00	8.56
4	Fin	10.00	10	0.00	3.33
5	Cp, Pr	6.54	10	0.00	4.52
6	Pr, Es	10.00	10.00	0.00	3.33
7	Es	10.00	10.00	10.00	3.33

Table 5. 4 Final VEA_bility Score on each Host

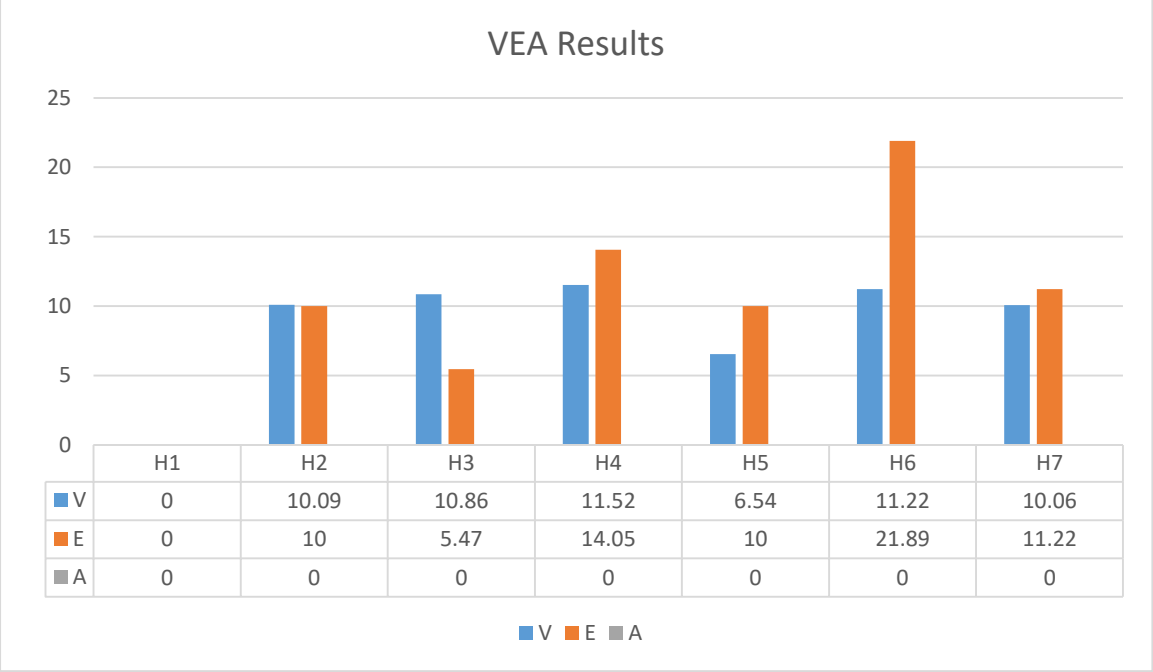

Figure 5. 3 VEA Final Score

The values in both VEA final score shows a high score for exploitability, this is due to the is the host having a lot of services. This is critical as once a service contains exploits, the other services related to the same host will likewise be exposed to attack. In this analysis, low attacka_bility score is due to network connectivity restriction by the two firewalls implemented

A. Interpretations of V, E, A Values:

- A score of 0 signifies the best value as the network can be said to have the lowest rate of vulnerability, exploitability, or attack ability. Again
- A score of 10 signifies the worst value as the network can be said to have the highest rate of vulnerability, exploitability, or attack ability

B. Interpretations of VEA_bility Values:

- A score of 0 signifies the worst value since the department network can be said to have the lowest level of security.
- A score of 10 signifies the best value since the department network can be said to have the highest level of security.

5.3.4 Experimental Results

The two security measure metrics mentioned in the evaluation section were used to evaluate the results obtained from participating sub-organisations network comparison between the established MTTC and VEA_bility metrics and the BAS metrics. The objective of this study is to evaluate the situation and how the BAS metrics enhanced with numerical information improve the performance of the BYOD system in terms of network security level and accuracy. To evaluate this, three measures have been used on the network configurations of the sub-organisation in fig 5.1

- The Bas Metrics, which is the BYOD situation measurements model developed in this work and presented in chapter 4;

- The MTTC measures the time estimation needed by an attacker to breach a system successfully in a unit of days. This is a calculation for quantifying the security risk based on system vulnerabilities and an attacker skill level.
- VEA_bility measures the level of security of a computer network configuration and shows its results with quantitative values. VEA_bility can also be used to evaluate numerous computer network configurations to establish which network is most secure.

In this experiment, an application of three security metrics to a BYOD network is compared. One is the BAS metrics presented in this work with all its components initiated, and the other two also gives a quantitative score based on known vulnerabilities, however, the MTTC is based on the weakest adversary that can compromise. The standard score for each metric are presented in Figure 5.4, this shows that the proposed approach metrics worked far more precisely than the traditional metrics. Table 5.5 below indicates the performance comparison between BAS, MTTC and VEA_bility metrics

	BAS_Metric	MTTC	VEA_bility
Calculation	More practical	Less practical	Less practical
Consistency	More consistent	Less consistent	consistent
Num of Vulnerability	Is able to measure a network with lots of BYOD related vulnerabilities	Can be applied to a network with various vulnerabilities	Less precision for a network with more vulnerabilities
Measurement Attributes	Level of Severity of BYOD system's variables	Adversary Skills level	Vulnerability, exploitability, attack_ability

Table 5. 5 Performance Comparison of BAS, MTTC and VEA_bility metrics

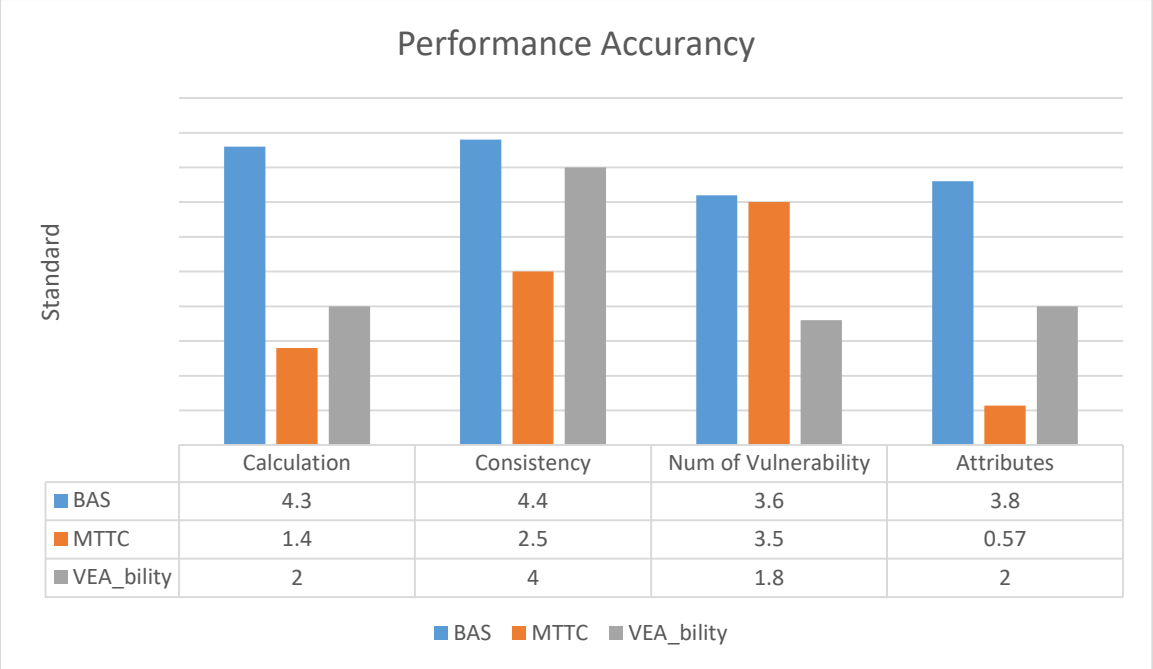

Figure 5. 4 Performance score of BAS, MTTC and VEA_bility metrics

Based on the performance scores in Fig 5.4 between the three metrics BAS metric, MTTC and VEA_biity, the security level of department Pr and Cp is the most secure when the BAS metrics were used for the measurement. Because it produced a higher percentage BAS score, the better the level of BYOD network security. Therefore it can be said security review is performed frequently, and the risk factor is minimum hence the security level of the network is also getting better. The MTTC for a given number of vulnerabilities can be calculated using either the Leverage-Byres method or the McQueen method with each method producing a different score for the same variable. Thereby this method is less feasible in its calculation of a BYOD employed system. Additionally, since the VEA_bility is affected by the vulnerability, exploitability, and attack_ability score, it appears more tedious to be applied on a BYOD system. Hence, it is less convenient to be used on a BYOD variable with lots of vulnerabilities. We use the exampled network in Figure 5.1 on existing security metrics such as MTTC and VEA_bility to execute security evaluation via the BYOD situation.

5.4 Description of the Unidentified Vulnerability Experiment

The exampled network in Figure 5.1 is used to conduct an experiment to test Snort NIDP performance in identifying and preventing harmful packets under high-speed traffic. A signature-based NIDP is preferred because of its popularity and its rules can be manipulated to fit the sub-organisations business process, the NIDP system is running a Snort and a Cisco Catalyst 2960X-24PD-L Switch as shown on the network design in Figure 5.1 above

The connection between the switch and PCs is achieved by using a 1.0 Gigabit cables and 10 Gigabit cables, the port linking the NIDP system to the network which sits on the switch acts as a spanning port. A packets size of 128 byte signifying the aggregate of data is generated from source to destination and is meant at the NIDP systems. The two types of packet considered are the TCP and UDP with a connection of 65536 bytes and 65507 bytes respectively. Additionally, the signature-based NIDP used in this work is made up of built-in policies. However, the amount of built-in policies does not determine its potency but the policy that is best in discovering attacks and prevent false positives regardless its internal design or behaviour, also policies simply implies the further possibility to capture malicious traffic. For 7600 number of policies are packed in the database.

The objective of this evaluation is to examine the number of packets accepted, analysed and dropped by the NIDP system. The performances were taken and recorded from the totality of the NIDP systems following executing for 1 minute, 3minutes, 6minutes and 10minutes. The systems task manager's record is used in calculating the application's usage (CPU usage)

The hardware description of the network elements is represented in Table 5.6 below.

Machine type	Hardware description
Network traffic generator/Attacking machines: . Windows 7 (64 bit)	

IDS Machine : Windows 7 (64 bit) . Windows Server 2012 (64 bit) . Linux (Fedora 3.5.3-1.fc17.i686)	Dell Optiplex 7010, Intel Core (TM) i5/i7 CPU, 16GB RAM, 1Gbps Full Duplex NIC (intel)
Android	"Nougat" 7.0
Switch	Cisco Catalyst 2960X-24PD-L Switch with 24x1 Gbps ports
Attacker machine Backtrack Linux Metasploit 4 Framework	Dell Precision, T3400, Intel Quadcore, Q6600,2GB Ram , 1Gbps network card
ESXi Server VMware ESXi Hypervisor Linux (Fedora 3.5.3-1.fc17.i686) Suricata, Snort	Dell Precision, T3400, Intel Quadcore, Q6600,4GB Ram, 1Gbps network card (for monitoring server), 10Gb for IDS Bandwidth monitor

Table 5. 6 The hardware description of the network elements

5.4.1 Data Source and Configuration

The NIDP system is implemented inside the sub-organisation restricted network area subject to security processes. Anyhow, the IDS is assigned, the sensor can give a meaningful assessment into traffic passing through the network and the completed results are tallied by checking the logs that display alerts of the intrusion attempts. On whichever day, the NIDP

system can give out thousands of alerts, this alerts can be a demanding task to analyse, that is why a form of measurement(metrics) comes in. Metrics are useful in quantifying value (data) and measuring performance in everyday decision making.

Defining the problem-solving metrics of the study depends on the factors specifying the security level of the BYOD employed organisation. So, the important questions linked to the BYOD user security will be, for example, is the network user security level increasing or decreasing? Is the NIDP system alarming schedule on the correct events. Thus, is this establishing metrics dependent on NIDP supposed functioning?

Presently Snort NIDP systems have the ability to categorise the alert generated based on the qualitative impact of an attack that is high, medium, low and very low via CVSS. But these fuzzy values are not very effective in assessing the security risk level of the organisation (network, user) especially in terms of the attack. Therefore, it is necessary for a NIDP system security risk metrics, with the requirement of expressing the network status as an absolute value using the alert produced by the NIDP systems constantly.

5.4.2 Metrics evaluation(Attack Exposure Rate)

In order to establish the usefulness of the snort performance on distinct traffic speed, a Metasploit tool is introduced to generate malicious traffic in the direction of the NIDP system. The generated traffic speeds are then analysed to determine the performance of the Snort. Thus identifying the number of packets dropped. The data is shown in Table 5. 7 below, this depicts the packet captured and analysed.

Traffic Speed (per second)	Packet Analysed (%)	Packet Dropped (%)	Alarm generated by Snort (%)
350Mb	100	0	100
400 Mb	100	0	100
750 Mb	100	0	100

1.5 Gb	100	0	100
2.0 Gb	86.4	13.6	99.7
2.5 Gb	82.6	17.4	99.2

Table 5. 7 Packet Captured and Analysed by Snort

It can be observed from Table 5. 7, the entire packet analysed by the snort exposed attacks until the traffic speed attains 2.0 Gbps. Then, it drops in the packet by 13.6% and an inadequate alert generated by 0.3%. Additionally, the traffic speed of 2.5 Gbps also dropped in a packet by 17.4% and an inadequate alert generated by 0.8%. Subsequently, the CVSS is used to classify the severity of the alert generated by snort NIDP in terms of high, medium, low and very low level. This is depicted in Table 5.8 below.

Number	Class-type	Description	Priority	Number of alert obtained
P1	attempted-admin	Attempted Administrator Privilege Gain	High	250
P2	attempted-user	Attempted User Privilege Gain	High	3
P3	inappropriate-content	Inappropriate Content was Detected	High	5
P4	policy-violation	Potential Corporate Privacy Violation	High	0
P5	shellcode-detect	Executable Code Was Detected	High	22
P6	successful-admin	Successful Administrator Privilege Gain	High	0
P7	successful-user	Successful User Privilege Gain	High	0
P8	trojan-activity	A Network Trojan Was Detected	High	2
P9	unsuccessful-user	Unsuccessful User Privilege Gain	High	0
P10	web-application-attack	Web Application Attack	High	52
P11	attempted-dos	Attempted Denial Of Service()	Medium	147
P12	attempted-recon	Attempted Information Leak	Medium	437
P13	bad-unknown	Potentially Bad Traffic	Medium	0
P14	default-login-attempt	Attempt To Login By A Default Username And Password	Medium	2
P16	misc-attack	Misc Attack	Medium	8

P17	non-standard-protocol	Detection of a Non-Standard Protocol or Event	Medium	1602
P18	rpc-portmap-decode	Decode Of An Rpc Query	Medium	0
P19	successful-dos	Denial Of Service	Medium	0
P20	successful-recon-largescale	Large Scale Information Leak	Medium	0
P21	successful-recon-limited	Information Leak	Medium	2204
P26	web-application-activity	Access To A Potentially Vulnerable Web Application	Medium	20
P27	icmp-event	Generic Icmp Event	Low	0
P28	misc-activity	Misc Activity	Low	25
P29	network-scan	Detection of a Network Scan	Low	0
P30	not-suspicious	Not Suspicious Traffic	Low	0
P31	protocol-command-decode	Generic Protocol Command Decode	Low	0
P32	string-detect	A suspicious string was detected	Low	0
P33	unknown	Unknown Traffic	Low	0
P34	TCP-connection	A TCP connection was detected	Very Low	0

Table 5. 8 CVSS classified the severity of alert generated by snort NIDP

To attain a numerical measurement of the security level for the sub-organization network, describe earlier in Figure 5.1 and producing metrics data from the alerts generated by the Snort. By means of the snort default classification, a taxonomy of attacks expressed in the Snort rule is generated and a total of 5113 alerts recorded against malicious traffic. This is used to plot a chart for Total number of alert establish on attack priority and expressed as high, low and medium, this is shown in Figure 5.5

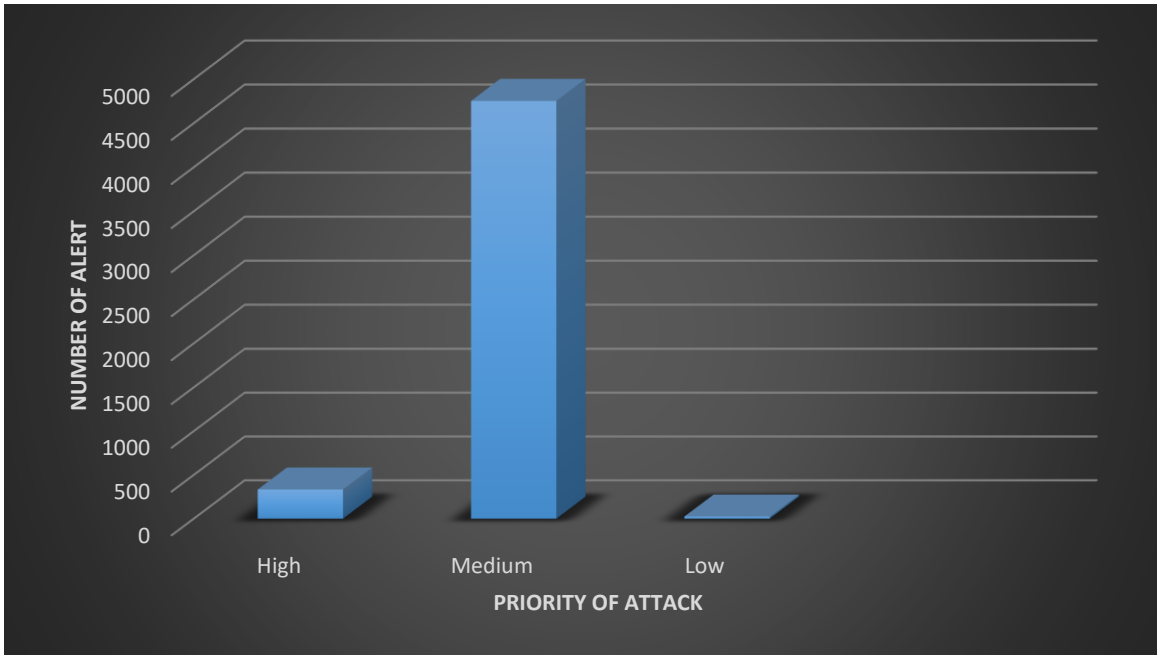

Figure 5. 5 Total number of alert establish on attack priority.

From the chart, 334 of alerts has a high priority of attack, the medium priority of 4754 alerts making it the most significate and the remaining 25 alerts are of low priority, no alert exists for the very low (For detail, please see Appendix). Using the information provided by the number of threat is not enough for an evaluation since this data is in a qualitative form so it does not provide an absolute score (numerical value) for one to deduce whether security level is improving or declining. Therefore, to best predict the security risk level quantitatively (Absolute score) a security metrics is also needed to give a better picture.

5.4.2.1 Evaluation Results

In the quantitative security risk level assessment, an investigation was conducted using the ministries sub-organisation network in Figure 5.1 above. The test was executed at a traffic speed up to 1.5 Gbps. Afterwards, the evaluation is organised using two calculated values and expressed also in two events from named factors, such as;

1) Categories of attack occurrences and

2) Impacts of attack

1) **Event-1:**

Network Security level (NSL) established on distinct types of attack instances, represented in Table 5.7 above stands as an attack taxonomy, hence, it has been ordered into 34 different classes beginning with the class types obtained from the snort rules and each identified class type detailed alongside its description. Also recorded in the table is the number of alert obtained versus each attack category. This is considered arithmetically, for instance, suppose the attack category P_d is d ∈ z and $1 \leq d < 34$ is the number of attacks generated against the variable (network). Therefore, VSL ($P_{d,}$) becomes the network security level of a personal device due to P_d attack. similarly, the security level of a personal device(service) based upon the class of attack is an expression as follows:

$$V SL\ (P_{d,}) = \left(\frac{\alpha i}{\sum \alpha}\right) \tag{5.29}$$

Where

αi = the number of alerts generated against ($_d$)

$\Sigma\ \alpha$ = total number of alerts collected against ($\forall\ P_d$)

Therefore from table 5.7, the network security level is calculated as

$$V SL\ (P_1) = \frac{250}{5113} = 4.87\% \tag{5.30}$$

$$V SL\ (P_2) = \frac{3}{5113} = 0.05\% \tag{5.31}$$

$$V SL\ (P_3) = \frac{5}{5113} = 0.09\% \tag{5. 32}$$

$$V SL\ (P_4) = \frac{0}{5113} = 0 \tag{5.33}$$

This is repeated for P4 through to P34 in, Table 5.9, below. The Security level (VSL) established on distinct types of attack instances.

$VSL\ (P_{d,}) = \left(\frac{\alpha i}{\sum \alpha}\right)$						
VSL (P1) = 4.87%	VSL (P6) =0.0%	VSL (P11) = 2.87%	VSL (P16) =0.0%	VSL (P21) =43.1%	VSL (P26) =0.39%	NSL (P31) =0.0%
VSL (P2) =0.05%	VSL (P7) =0.0%	VSL (P12) = 8.54%	VSL (P17) =31.3%	VSL (P22) =0.0%	VSL (P27) =0.0%	VSL (P32) =0.0%
VSL (P3) =0.09%	VSL (P8) =0.04%	VSL (P13) =0.0%	VSL (P18) =0.0%	VSL (P23) =0.0%	VSL (P28) =0.49%	VSL (P33) =0.0%
VSL (P4) =0	VSL (P9) =0.0%	VSL (P14) =0.0%	VSL (P19) =0.0%	VSL (P24) =0.0%	VSL (P29) =0.0%	VSL (P34) =0.0%
VSL (P5) =0.43%	VSL (P10) =1.01%	VSL (P15) =0.0%	VSL (P20) = 0.0%	VSL (P25) =0.0%	VSL (P30) =0.0%	

Table 5. 9 The network security level of a user device service (Pd)

The expression in Table 5.9 indicates the network security level of a user device (Pd) due to different attacks for P1is 4.87% meaning the user device on the network is 95.13% secure against an attack, also P2 is 0.05% prone to attack, which implies that the user device on the

network is 99.95% secure enough. But in a worst-case scenario, the likelihood of an attack level is highest at P21 with a score of 43.1%. This implies that the user device on the network is just secure at 56.9%, thus it necessary for appropriate countermeasures to be initiated to restraint the network and its users from potential attacks.

2) Event-3: Security level (BSL) established on the impact of attacks

Representing the values for priority of attack in the fig 5.15 above, that is, High, Medium, Low and Very Low with H, M, L and VL and scores of ΣH =334, ΣM = 4754, ΣL = 25 and ΣVL = 0, ΣH =334, ΣM = 4754, ΣL = 25 and ΣVL = 0, respectively.

Assuming, $\Sigma\ H + \Sigma\ M + \Sigma\ L + \Sigma\ V = \mathrm{C}$. therefore, the Variable (network) security level ($\mathrm{V}SL$) establish on impact is defined the equation:

$$\mathrm{B}SL\ (I\mathrm{c}) = \left(\frac{\Sigma\ Ic}{c}\right) \qquad (5.34)$$

Where;

Ic =individual impact type

ΣIc =Total alert of Ic type

C = the total alerts of all impact categories

Now, using the number of alerts obtained values in equation 5.34. Such as;

Ic =high impact =334,

medium impact =4754,

low = 25,

very low impact = 0

Therefore

$$\mathrm{V}SL\ (\mathrm{H}) = \left(\frac{334}{5113}\right) = 6.5\% \qquad (5.35)$$

$$V\mathit{SL}(\text{M}) = \left(\frac{4754}{5113}\right) = 92.9\% \quad (5.36)$$

$$V\mathit{SL}(\text{L}) = \left(\frac{25}{5113}\right) = 0.48\% \quad (5.37)$$

$$V\mathit{SL}(\text{VL}) = \left(\frac{0}{5113}\right) = 0 \quad (5.38)$$

Results from equations 5.35-5.38 gives a quantitative (absolute value) of the security risk impact on the network. With equation 5.35 showing a high impact ($V\mathit{SL}$(H)) score of 6.5%, meaning the secure rate of the network is 94.3%, which is adequately secure against attack. Subsequently, the security risk level of the network in regards to medium impact score ($V\mathit{SL}$(M)) of attack is 93% .meaning its secure rate stands just at 7%. Hence, an applicable countermeasure must be used to secure it. Likewise, assessing the network security level by means of medium impact ($V\mathit{SL}$(L)) came out with a result of 0.48% for equation 5.37 and expressed as (0.42% <1%), shows a network security impact level of 99.5%. Nevertheless, this cannot be defined as a fully secured network and so security measure is not far from it. Finally, equation 5.38 gives a value 0 for the very low impact of attack $V\mathit{SL}$(VL) =0. That is, the network is fully secured hence is free and subsequently not vulnerable to any threat, but this is not always true.

In this experiment, an application of two security metrics to an unidentified vulnerabilities of a BYOD network are compared. One is the metrics presented in this work with all its components initiated, and the other is the same process but with the categorisation of the different types of attack and their impacts being measured by limiting the evaluating to logs that indicate alerts of the intrusion attempts(Snort). The average values for each metric are presented in Figure.5.6, from the scores it can be concluded that the proposed approach worked far more precisely than the snort detection protection.

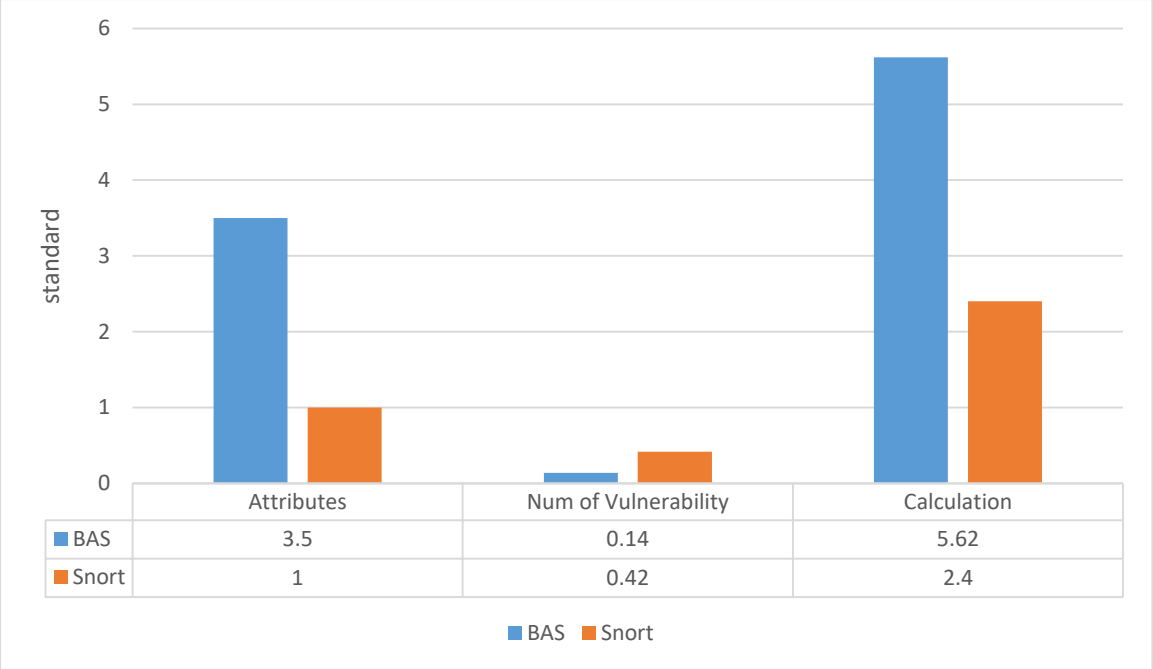

Figure 5. 6 performance Comparison Between BAS and Snort Process

From both metrics, it can be observed that the Snort drops packets in heavy and with high traffic speed. though there is Cisco Catalyst 2960X-24PD-L switch situated within the experimented network to improve performance such that packets are no longer dropped. But the Snort takes a longer period to run. Therefore using only the snort to assess the security risk level of a BYOD system is not advisable

5.5 Conclusion

This chapter describes the experimental evaluation composition and its information sources. Also, the principal measurement evaluation procedures have been categorised. These have been presented based on two items (Known and unidentified vulnerability). According to the application of security metrics to a BYOD system variable a quantitative security made up of the MTTC, VEA_bility were used for the known vulnerability evaluation, all the chosen metrics use the CVSS and the input data for them is obtained from Nessus scanning tool used on the sub-organisations network. These metrics were used because they are capable of clearly indicating critical vulnerabilities within an acceptable secure network. On the contrary, the

examination of system performance with unidentified vulnerabilities is according to the Snort NIDP. This has been employed to measure the security level of a network's personal device thru the examination of the alerts generated at different traffic speeds by means of the ministries sub-organisations network configuration. Data from the NIDP investigation made up of the different type of attacks and their impact is used in the evaluating process to obtain the security level of a network (metrics). The BAS scored security metric ranks the network in terms of absolute value, thus helps in quantifying the impact in addition to the risk related to each distinct attack category.

The evaluation results demonstrate the feasibility of the BAS metrics for a BYOD network. This is because it calculation process is easy with the known vulnerability data on the network extracted with a commonly available network security evaluation tools such as Nessus. Likewise, the results obtained from the BAS scores indicate the capability of the metrics signifying serious vulnerabilities in a rather secure network straightforwardly.

CHAPTER 6 CONCLUSION AND FUTURE WORK

This chapter represents the conclusion to the research path commenced in this thesis. A brief summary of the main topics that the thesis centres on and also summarises the main contributions offered by this thesis. Certainly, the study cannot be deemed as complete as much potential awaits and thus the last section outlines some recommended future work worth investigating.

6.1 Conclusion

Organizations employing BYOD on their network have a greater task to identify and evaluate vulnerabilities according to their risk and threat to the network this is due to the possibility of an increase in the number of personal devices and their complexity. Therefore this thesis deals with the issue of quantifiable means of security level measuring of a BYOD network. As has been discussed. Meanwhile, the introduction of personal devices onto an organization network means there is an incredible amount of network resources in the organisation environment which presents an immense pull for malicious attacks. Henceforth, for an attack to be successful on a depends on its capability to exploit a network's vulnerability, resulting in the compromise of the network resource. Also, a BYOD network can be set up to include firewalls that are used to monitor and block any intrusion. But, these scanning tools simply give an outline of the system design and vulnerabilities on one occasion. Thus the firewall may not always be the solution for measuring the security of a large scale BYOD organization's network. Therefore to achieve the task of detecting incoming traffic from BYOD users to the network, Intrusion Detection and Prevention (NIDP) systems are preferred in capturing the network vulnerability information. Additionally using data on the vulnerability of a system to provide a solution by measuring the total security level of the BYOD variable quantitatively has become a major challenge for network administrators currently.

This thesis emphasis on the following three main aspects:

- Create a novel scoring system framework that can be used as a recommendation for security evaluation and references to effect policies relating to BYOD network management
- Design and implement a composite BAS security metrics which combines individual host-based metrics with probability to give an absolute score
- A taxonomy designed to identify Network security attacks with their related threats and vulnerabilities which are broken down into smaller ranks that can be thoroughly investigated. These are first used to measure the security impact, then assigns a score to each risk related with each individual attack category

The main contribution of the thesis is that it offers a practical and convenient measurement system for the security risk level of BYOD an employed organisation variable(Network, User device) to tackle vulnerability overload problem through the developing of a composite framework which supports data accumulation and integration from multiple sources. However, BAS framework utilises quantitative security measures to enhance the security risk level and deal with approximating the scale types of security risk level in BYOD problem and to improve performance.

Specifically, this work has made the following contributions;

1. It contributes to the knowledge of existing network security metrics by increasing understanding as to how the issue is typically confronted and why limitation remains. From a scientific viewpoint, it makes relevant contributions to the emerging BYOD security metrics.
2. The systematic model structured to integrate data on a system vulnerability will contribute to improving the BYOD network security risk assessment by overcoming the consistency of Vulnerability information. Additionally, it presents properties, such as generality, which

allows it to be managed in different security matrics which change with the user's activity and the organisation's policy.

3. The creation of a novel BYOD security metrics framework that is designed around the case of invisible attacks, the framework is executed to reveal how these attacks were identified and mitigated. With the existence of different categories of invisible attacks, this work is centred specifically on the impact of Google dorks (hacking). A metrics design to specify in absolute value the total security risk level of a BYOD system.

Data was gathered for deliberated by using generated data on the system vulnerabilities to provide an absolute score of the BYOD network security risk assessment factor related to malicious cyber-attacks. The Vulnerability description is based on Common Vulnerabilities and Exposures (CVE), whilst Common Vulnerabilities Scoring System (CVSS) on the other-hand provides numeric scores to each vulnerability in the CVE database based on their characteristics and security impact.

The evaluation was done using data on individual departments in a BYOD employed Ghana, Ministries based organisation as a case study for both the known vulnerabilities and unidentified attacks. Using the results attained from known vulnerabilities in chapter 4, a BYOD security metrics framework is designed. In the situation of unidentified attacks, the study was executed to reveal how these attacks were identified and mitigated. With the existence of different categories of unidentified attacks, this work is centred specifically on the impact of Google dorks (hacking) and an unidentified risk to a BYOD variable. The effected results achieved from unidentified attacks is applied in designing a rule and afterwards engaged in the NIDP systems by way of a mitigation method. The BAS metrics can be used in any working BYOD environment in order to specify the absolute value of the total security risk assessment of the organization.

Finally, The experiment results show that the framework in this research can reduce security risk prediction complexity and provide a more practical measurement of BYOD variables based on known and Unidentified vulnerabilities. The results show that the BAS score for unidentified vulnerability calculation is 5.62% compare to the snort score of 2.4%. Also, the calculation for the BAS metrics scores on Known vulnerability shows 4.3% compare to the usual metric VEA_bility 2.0% and MTTC 1.3%. This indicates that the proposed framework is able to offer improved prediction accuracy and practical security metrics for a BYOD system. The higher the BAS score, the better the level of network security. The more often a security review performed, the lower the risk so the security level of the network is also getting better. This is true for a general network security performance.

6.2 Limitations

- The NIDP system used for intrusion detection is the snort, but it is essential for another NIDP system to be further employed and its performance compares to Snort to come out with the most suitable one for a network. Therefore, this study is biased towards the Snort NIDP system

- The definition and description of the BYOD security requirements assume a known understanding of the vulnerabilities involved, so if a particular threat or vulnerability is not a usually known issue it may not be acknowledged. This might lead to an unaccounted vulnerability, which will not be a proper reflection of the security requirement specification.

6.3 Future Work

- This research is limited to the Google dorks (hacking) established invisible attacks. However, the invisible attacks have the potential of being investigated further in order to build a generalised metrics involving a BYOD employed network. other forms of invisible

attacks such as phishing attack and zero base attacks can be explored further in a BYOD situation.

- The main security risk being access in this research is an outsider attack, thereby overlooking the insider attack, hence this should be included in the future BYOD scoring systems.

REFERENCES

Ahmed, M. S., Al-Shaer, E., & Khan, L. (2008). A novel quantitative approach for measuring network security. *Proceedings - IEEE INFOCOM*, 76–80. https://doi.org/10.1109/INFOCOM.2007.260

Alberts, C. J., & Dorofee, A. J. (2010). *Risk Management Framework*.

Alessandri, D. (2001). *Malicious-and Accidental-Fault Tolerance for Internet Applications Towards a Taxonomy of Intrusion Detection Systems and Attacks MAFTIA deliverable D3*.

Allodi, L., & Massacci, F. (2014). Comparing Vulnerability Severity and Exploits Using Case-Control Studies. *ACM Transactions on Information and System Security*, *17*(1), 1–20. https://doi.org/10.1145/2630069

Almasizadeh, J., & Azgomi, M. A. (2013). A stochastic model of attack process for the evaluation of security metrics. *Computer Networks*, *57*(10), 2159–2180. https://doi.org/10.1016/j.comnet.2013.03.011

Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011). Collaboration-based cloud computing security management framework. *Proceedings - 2011 IEEE 4th International Conference on Cloud Computing, CLOUD 2011*, 364–371. https://doi.org/10.1109/CLOUD.2011.9

Arellano Nestor E. (n.d.). Top 9 security threats to prepare for in 2015 | IT World Canada Slideshow.

Armando, A., Costa, G., Merlo, A., Verderame, L., & Wrona, K. (2016). Developing a NATO BYOD security policy. *2016 International Conference on Military Communications and Information Systems, ICMCIS 2016*, 1–6. https://doi.org/10.1109/ICMCIS.2016.7496587

Aven, T., & Renn, O. (n.d.). *On risk defined as an event where the outcome is uncertain*. https://doi.org/10.1080/13669870802488883

Azuwa, M. ., Ahmad, R., Sahib, S., & Shamsuddin, S. (2012). Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard. *International Journal of Cyber-Security and Digital Forensics*, *1*(4), 280–288.

Beale, S. S., & Berris, P. (2018). Hacking the Internet of Things : Vulnerabilities , Dangers , and Legal. *Duke Law & Technology Review*, *16*(1), 162–204.

Bello Garba, A., Armarego, J., & Murray, D. (2015). *BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION SECURITY AND PRIVACY*. *10*(3).

Böhme, R., & Freiling, F. C. (2008). On Metrics and Measurements. In *Dependability Metrics* (pp. 7–13). https://doi.org/10.1007/978-3-540-68947-8_2

Boyer, W. F., Mcqueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A. (1986). Quality of protection. *Anti-Corrosion Methods and Materials*, *33*(4), 7–8. https://doi.org/10.1108/eb020432

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., & Buckalew, L. (2012). Horizons BYOD : A Global Perspective Harnessing Employee-Led Innovation. *CISCO IBSG Horizons*, 1–21.

Brodin, M. (2015). Combining ISMS with Strategic Management: The case of BYOD. *IADIS International Conference Information Systems*, 161–168. https://doi.org/10.1016/j.dsr.2003.12.001

Burns, M. (2012). Eric Schmidt: ``There Are Now 1.3 Million Android Device Activations Per Day''. *TechCrunch*, *5*.

Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Hoon, J. L. (2011). A strong user authentication framework for cloud computing. *Proceedings - 2011 IEEE Asia-Pacific Services Computing Conference, APSCC 2011*, 110–115. https://doi.org/10.1109/APSCC.2011.14

Collett, S. (2015). API security leaves apps vulnerable: 5 ways to plug the leaks | CSO

Online.

CVE. (2019). CVE - Common Vulnerabilities and Exposures (CVE).

CWE. (n.d.). CWE - Common Weakness Enumeration.

Dacier, M., Deswarte, Y., & Kaâniche, M. (1996). Models and tools for quantitative assessment of operational security. In *12th International Information Security Conference (IFIP/SEC'96)*. https://doi.org/10.1007/978-1-5041-2919-0_15

Das, A., & Islam, M. M. (n.d.). *SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems*. https://doi.org/10.1109/TDSC.2011.57

Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014). A case study on web application vulnerability scanning tools. *Proceedings of 2014 Science and Information Conference, SAI 2014*, 595–600. https://doi.org/10.1109/SAI.2014.6918247

Dawson, P. (2015). *Hacking assessment*. 65–67.

Dery, K., & MacCormick, J. (2012). *Managing Mobile Technology: The Shift from Mobility to Connectivity*.

Donald, F. (2004). Specifying Reusable Security Requirements. *Journal of Object Technology*, *3*(1), 61–75.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Eskins, D., & Sanders, W. H. (2011). The multiple-asymmetric-utility system model: A framework for modeling cyber-human systems. *Proceedings of the 2011 8th International Conference on Quantitative Evaluation of Systems, QEST 2011*, 233–242. https://doi.org/10.1109/QEST.2011.38

EY. (2014). *Insights on governance, risk and complianc*. https://doi.org/https://www.ey.com/Publication/vwLUAssets/EY-internal-audit-

harnessing-the-power-of-analytics/$FILE/EY-internal-audit-harnessing-the-power-of-analytics.pdf

Fan, L., Liu, J., Li, G., Wu, Z., & Guo, J. (2012). A Grid Authorization Mechanism with Dynamic Role Based on Trust Model. In *Journal of Computational Information Systems* (Vol. 8).

Fernández-Muñiz, B., Montes-Peón, M., & José Vázquez-Ordás, C. (2012). Occupational risk management under the OHSAS 18001 standard: analysis of perceptions and attitudes of certified firms. *Journal of Cleaner Production*, *24*, 36–47. https://doi.org/10.1016/j.jclepro.2011.11.008

FIRST. (2018). FIRST - Improving Security Together.

Friedman, J. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, *7*(1/2), 159–180. https://doi.org/10.1016/j.is.2014.07.006

Gallon, L. (2011). Vulnerability discrimination using CVSS framework. *2011 4th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2011 - Proceedings*, 1–6. https://doi.org/10.1109/NTMS.2011.5720656

Gallon, L., & Bascou, J. J. (2011). Using CVSS in attack graphs. *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, 59–66. https://doi.org/10.1109/ARES.2011.18

Girard, J. (2013). Top Seven Failures in Mobile Device Security.

Granneman, J. (2013). IT security frameworks and standards: Choosing the right one.

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice*, *17*(1), 43–53. https://doi.org/10.1057/dddmp.2015.32

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector

cybersecurity: An international comparison. *Computer Law and Security Review*, *29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Homer, J., Zhang, S., Ou, X., Schmidt, D., Du, Y., Rajagopalan, S. R., & Singhal, A. (2013). Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, *21*(4), 561–597. https://doi.org/10.3233/JCS-130475

Huluka, D., & Popov, O. (2012). Root Cause Analysis of Session Management and Broken Authentication Vulnerabilities. *Internet Security (WorldCIS), 2012 World Congress On*, 82–86.

Ibm. (n.d.). *IBM Security Services 2014 Cyber Security Intelligence Index*.

Iec. (2016). *ISO/IEC Directives Part 1 Procedures for the technical work CONTAINS THE FINAL VERSION AND THE REDLINE VERSION colour inside*.

Inc., R. F. (2012). Key Strategies To Capture And Measure The Value Of Consumerization Of IT. *Trend Micro*, (May), 1–17.

International Organization for Standardization. (2016). ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://doi.org/10.1111/gbb.12061

ISO/IEC. (2018). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and*. *2018*, 38. https://doi.org/10.1177/0011128708322943

ISO. (2015). ISO - International Organization for Standardization.

Issa-Salwe, A. M., & Ahmed, M. (2011). Risk Management of an Information System by Assessing Threat , Vulnerability and Countermeasure. *International Journal of Research and Reviews in Computer Science*, *2*(1), 111–114.

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*(5), 28–33. https://doi.org/10.1109/MITP.2012.72

Jansen, W. (n.d.). *Directions in Security Metrics Research*.

Jha, S., Sheyner, O., & Wing, J. (2002). Two formal analyses of attack graphs. *Proceedings of the Computer Security Foundations Workshop*, *2002-Janua*, 49–63. https://doi.org/10.1109/CSFW.2002.1021806

Jonsson, E., & Olovsson, T. (1997). A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, *23*(4), 235–245. https://doi.org/10.1109/32.588541

Keramati, M. (2017). New Vulnerability Scoring System for dynamic security evaluation. *2016 8th International Symposium on Telecommunications, IST 2016*, 746–751. https://doi.org/10.1109/ISTEL.2016.7881922

Ketel, M., & Shumate, T. (2015). Bring Your Own Device: Security technologies. *Conference Proceedings - IEEE SOUTHEASTCON*, *2015-June*(June), 1–7. https://doi.org/10.1109/SECON.2015.7132981

Kobayashi, H., Mark, B. L., & Turin, W. (2011). Probability, random processes, and statistical analysis. In *Probability, Random Processes, and Statistical Analysis* (Vol. 9780521895446). https://doi.org/10.1017/CBO9780511977770

Koh, E. B., Oh, J., & Im, C. (2014). *Ii. Security Issues and New Dynamic Access Control System As a Solution*. *II*.

Lee, B.-C., & Shin, S.-J. (2014). The Study of Privacy Security in Mobile Traffic Control Environment. *International Journal of Security and Its Applications*, *8*(2), 173–182. https://doi.org/10.14257/ijsia.2014.8.2.18

Leversage, D. J., & Byres, E. J. (2013). Comparing electronic battlefields: Using mean time-to-compromise as a comparative security metric. *Communications in Computer and Information Science*, *374*(PART II), 213–227. https://doi.org/10.1007/978-3-540-73986-9-18

Lippmann, R., Ingols, K., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M., & Cunningham, R. (2007). Validating and restoring defense in depth using attack graphs. *Proceedings - IEEE Military Communications Conference MILCOM*. https://doi.org/10.1109/MILCOM.2006.302434

Marsh, S. P. (1994). Formalising Trust as a Computational Concept. *Department of Computing Science and Mathematics, University of Sterling*, (April), 184. https://doi.org/10.2165/00128413-199409230-00010

Matt, P.-A., Morge, M., & Toni, F. (n.d.). *Combining statistics and arguments to compute trust*.

McQueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A. (2005). Time-to-Compromise Model for Cyber Risk Reduction Estimation. In *Quality of Protection*. https://doi.org/10.1007/978-0-387-36584-8_5

Mell, P., Scarfone, K., & Romanosky, S. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, *14*(5), 53–55. https://doi.org/10.1109/MITP.2012.93

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8. https://doi.org/10.1016/S1353-4858(12)70111-3

MSRC. (2017). Microsoft security response center security bulletin severity rating system.

National Institute of Standards and Technology (NIST). (2016). National Vulnerability Database (NVD): Summary.

National Institute of Standards and Technology (NIST). (2018). National Vulnerability Database (NVD). https://doi.org/10.3928/23258160-20150422-03

Niehaves, B. ;, Köffer, S. ;, Ortbach, K. ;, Katschewitz, S., Becker, J., Backhaus, K., … Ortbach, K. (n.d.). *A Service of zbw Leibniz-Informationszentrum Wirtschaft Leibniz*

Information Centre for Economics Towards an IT consumerization theory: A theory and practice review Working Papers Towards an IT Consumerization Theory-A Theory and Practice Review.

NIST. (2004). Fips Pub 199. *FIPS Publication 199*, *199*(February 2004), 13. https://doi.org/10.6028/NIST.FIPS.199

NPFC. (1995). NPFC - MIL-HDBK-1785 - HANDBOOK FOR SYSTEM SECURITY ENGINEERING PROGRAM MANAGEMENT REQUIREMENTS | Engineering360.

O'Brien, G., Lesser, N., Pleasant, B., Wang, S., Zheng, K., Bowers, C., & Kamke, K. (2015). *Securing Electronic Health Records on Mobile Devices*.

Ou, X., & Singhal, A. (2011). *Quantitative Security Risk Assessment of Enterprise Networks*. https://doi.org/10.1007/978-1-4614-1860-3

Palmaers, T. (2013). *Implementing a vulnerability management process*.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A Survey on Systems Security Metrics. *ACM Computing Surveys*, *49*(4), 1–35. https://doi.org/10.1145/3005714

Prashant Kumar Gajar, 2*Arnab Ghosh and 3Shashikant Rai. (2013). Available Online at www.jgrcs.info BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING. *Journal of Global Research in Computer Science RESEARCH PAPER Available Online at Www.Jgrcs.Info BRING*, *4*(4), 62–70.

Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, B., & Tan, J. C. (2008). Application of security metrics in auditing computer network security: A case study. *Proceedings of the 2008 4th International Conference on Information and Automation for Sustainability, ICIAFS 2008*, (January 2009), 200–205. https://doi.org/10.1109/ICIAFS.2008.4783996

Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594.

https://doi.org/10.1016/j.isatra.2007.04.003

Ramos, A., Lazar, M., Filho, R. H., & Rodrigues, J. J. P. C. (2017). Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys and Tutorials*, *19*(4), 2704–2734. https://doi.org/10.1109/COMST.2017.2745505

Sanders, W. H., & Nicol, D. M. (2018). Science of Security (SoS) Lablet | Information Trust Institute.

Savola, R. (2007). Requirement centric security evaluation of software intensive systems. *Proceedings - International Conference on Dependability of Computer Systems, DepCoS - RELCOMEX 2007*, 135–142. https://doi.org/10.1109/DEPCOS-RELCOMEX.2007.41

Scarfone, K. (2009). *Third International Symposium on Empirical Software Engineering and Measurement An Analysis of CVSS Version 2 Vulnerability Scoring 1*.

Sharma, V. (2012). *A study of malicious qr codes*. *3*(5), 3–8.

Singh, S., Tu, H., Allanach, J., Areta, J., Willett, P., & Pattipati, K. (2004). Modeling threats. *IEEE Potentials*, *23*(3), 18–21. https://doi.org/10.1109/MP.2004.1341780

Tari, Z. (2014). Security and Privacy in Cloud Computing. *IEEE Cloud Computing*, *1*(1), 54–57. https://doi.org/10.1109/MCC.2014.20

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security*, *2013*(4), 12–13. https://doi.org/10.1016/S1353-4858(13)70050-3

Tropmann-Frick, M. (2018). Internet of things: Trends, challenges and opportunities. *Communications in Computer and Information Science*, *909*, 254–261. https://doi.org/10.1007/978-3-030-00063-9_24

Uehara, M. (2013). Proposal for BYOD based virtual PC classroom. *Proceedings - 16th International Conference on Network-Based Information Systems, NBiS 2013*, 377–382. https://doi.org/10.1109/NBiS.2013.60

US-CERT. (n.d.). Current Activity | US-CERT.

Vazquez, C. (2014). *Auditing using Vulnerability tools to identify today's threats Business Performance*.

Venayagamoorthy, G. K., Sharma, R. K., Gautam, P. K., & Ahmadi, A. (2016). Dynamic Energy Management System for a Smart Microgrid. *IEEE Transactions on Neural Networks and Learning Systems*, *27*(8), 1643–1656. https://doi.org/10.1109/TNNLS.2016.2514358

Viehböck, S. (2011). US-CERT Vulnerability Note VU#723755 - WiFi Protected Setup (WPS) PIN brute force vulnerability.

Villarrubia, C., Fernández-Medina, E., & Piattini, M. (n.d.). *Towards a Classification of Security Metrics*. https://doi.org/10.5220/0002688203410350

Wang, C., & Wulf, W. a. (1997). Towards a framework for security measurement. *20th National Information Systems Security Conference*, *Baltimore*, 1–15.

Wang, J. A., Wang, H., Guo, M., & Xia, M. (2009). Security metrics for software systems. *Proceedings of the 47th Annual Southeast Regional Conference on - ACM-SE 47*, 1. https://doi.org/10.1145/1566445.1566509

Wang, L., Jajodia, S., Singhal, A., Cheng, P., & Noel, S. (2014). K-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, *11*(1), 30–44. https://doi.org/10.1109/TDSC.2013.24

Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. *2014 IEEE 11th Consumer Communications and Networking Conference, CCNC 2014*, 80–85. https://doi.org/10.1109/CCNC.2014.6866552

Weintraub, E. (2015). *PMContinuous Monitoring System Based on Systems' Environment*. *4*, 20.

Wichers, D. (2013). *OWASP Top-10 2013 OWASP Top 10 Project Lead OWASP Board Member COO/Cofounder, Aspect Security*.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, *14*(4), 998–1010. https://doi.org/10.1109/SURV.2012.010912.00035

Yang, G., Wang, Y., Li, J., Liu, J., Ru, Y., Yuan, K., … Liu, K. (2016). An assessment method of vulnerabilities in electric CPS cyber space. *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, ICNC-FSKD 2016*, *1*(51377122), 397–402. https://doi.org/10.1109/FSKD.2016.7603206

Yuan, X., Yang, L., He, W., & Simpkins, L. (2016). *Teaching Security Management for Mobile Devices*. https://doi.org/10.1145/2978192.2978227

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81–99. https://doi.org/10.1016/j.cose.2015.06.011

Zhong, Y., Bhargava, B., Lu, Y., & Angin, P. (2015). A computational dynamic trust model for user authorization. *IEEE Transactions on Dependable and Secure Computing*, *12*(1), 1–15. https://doi.org/10.1109/TDSC.2014.2309126

Zhu, X., Lv, S., Yu, X., & Zuo, G.-P. (2010). Dynamic Authorization of Grid Based on Trust Mechanism. *2010 International Symposium on Intelligence Information Processing and Trusted Computing*, 417–421. https://doi.org/10.1109/IPTC.2010.113

APPENDICES

Appendix 1

CVE Vulnerabilities Based on Nessus Vulnerability

Reports Search Parameters:

Results Type: Overview

Search Type: Search All

Keyword (text search): oracle database server

There are 348 matching records.

Oracle Database Server

Vuln ID Summary CVSS Severity

CVE-2017-3567

Vulnerability in the OJVM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4 and 12.1.0.2. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise OJVM. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of OJVM. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

Published: April 24, 2017; 03:59:04 PM -04:00 V3: 5.3 MEDIUM

V2: 3.5 LOW

CVE-2017-3486

Vulnerability in the SQL*Plus component of Oracle Database Server. Supported versions that are affected are 11.2.0.4 and 12.1.0.2. Difficult to exploit vulnerability allows high privileged attacker having Local Logon privilege with logon to the infrastructure where SQL*Plus executes to compromise SQL*Plus. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in SQL*Plus, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in the takeover of SQL*Plus. Note: This score is for Windows platform version 11.2.0.4 of Database. For Windows platform version 12.1.0.2 and Linux, the score is 6.3 with scope Unchanged. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H).

Published: April 24, 2017; 03:59:02 PM -04:00 V3: 7.2 HIGH

V2: 3.7 LOW

CVE-2017-3310

Vulnerability in the OJVM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4 and 12.1.0.2. The easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise OJVM. Successful attacks require human interaction from a person other than the

attacker and while the vulnerability is in OJVM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in the takeover of OJVM. CVSS v3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts).

Published: January 27, 2017; 05:59:04 PM -05:00 V3: 9.0 CRITICAL

V2: 6.0 MEDIUM

CVE-2017-3240

Vulnerability in the RDBMS Security component of Oracle Database Server. The supported version that is affected is 12.1.0.2. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where RDBMS Security executes to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS Security accessible data. CVSS v3.0 Base Score 3.3 (Confidentiality impacts).

Published: January 27, 2017; 05:59:02 PM -05:00

Data handling

Vuln ID Summary CVSS Severity

CVE-2017-0131

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:03 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0094

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:02 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0071

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same

user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:01 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0070

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:01 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0067

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:01 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0035

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same

user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0032, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:01 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0032

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0015, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:00 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0015

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0010, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:00 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-0010

A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same

user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability is different from those described in CVE-2017-0015, CVE-2017-0032, CVE-2017-0035, CVE-2017-0067, CVE-2017-0070, CVE-2017-0071, CVE-2017-0094, CVE-2017-0131, CVE-2017-0132, CVE-2017-0133, CVE-2017-0134, CVE-2017-0136, CVE-2017-0137, CVE-2017-0138, CVE-2017-0141, CVE-2017-0150, and CVE-2017-0151.

Published: March 16, 2017; 08:59:00 PM -04:00 V3: 7.5 HIGH

V2: 7.6 HIGH

CVE-2017-6814

In WordPress before 4.7.3, there is authenticated Cross-Site Scripting (XSS) via Media File Metadata. This is demonstrated by both (1) mishandling of the playlist shortcode in the wp_playlist_shortcode function in wp-includes/media.php and (2) mishandling of meta information in the renderTracks function in wp-includes/js/mediaelement/wp-playlist.js.

Published: March 11, 2017; 08:59:00 PM -05:00 V3: 5.4 MEDIUM

V2: 3.5 LOW

CVE-2017-6800

An issue was discovered in ytnef before 1.9.2. An invalid memory access (heap-based buffer overread) can occur during handling of LONG data types, related to MAPIPrint() in libytnef.

Published: March 10, 2017; 05:59:00 AM -05:00 V3: 7.5 HIGH

V2: 5.0 MEDIUM

CVE-2016-5374

NetApp Data ONTAP 9.0 and 9.1 before 9.1P1 allows remote authenticated users that own SMBhosted data to bypass intended sharing restrictions by leveraging improper handling of the owner_rights ACL entry.

Published: March 01, 2017; 03:59:00 PM -05:00 V3: 8.8 HIGH

V2: 6.5 MEDIUM

CVE-2017-2791

JustSystems Ichitaro 2016 Trial contains a vulnerability that exists when trying to open a specially crafted PowerPoint file. Due to the application incorrectly handling the error case for a function's result, the application will use this result in a pointer calculation for reading file data into. Due to this, the application will read data from the file into an invalid address thus corrupting memory. Under the right conditions, this can lead to code execution under the context of the application.

Published: February 24, 2017; 05:59:00 PM -05:00 V3: 7.8 HIGH

V2: 6.8 MEDIUM

CVE-2016-3013

IBM WebSphere MQ 8.0 could allow an authenticated user to crash the MQ channel due to improper data conversion handling. IBM Reference #: 1998661.

Published: February 22, 2017; 02:59:00 PM -05:00 V3: 6.5 MEDIUM

V2: 4.0 MEDIUM

CVE-2016-9225

A vulnerability in the data plane IP fragment handler of the Cisco Adaptive Security Appliance (ASA) CX Context-Aware Security module could allow an unauthenticated, remote attacker to cause the CX module to be unable to process further traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to improper handling of IP fragments. An attacker could exploit this vulnerability by sending crafted fragmented IP traffic across the CX module. An exploit could allow the attacker to exhaust free packet buffers in shared memory (SHM), causing the CX module to be unable to process

further traffic, resulting in a DoS condition. This vulnerability affects all versions of the ASA CX Context-Aware Security module. Cisco has not released and will not release software updates that address this vulnerability. There are no workarounds that address this vulnerability. Cisco Bug IDs: CSCva62946.

Published: February 01, 2017; 02:59:00 PM -05:00 V3: 8.6 HIGH

V2: 7.8 HIGH

CVE-2017-3318

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).

Published: January 27, 2017; 05:59:04 PM -05:00 V3: 4.0 MEDIUM

V2: 1.0 LOW

CVE-2016-4323

A directory traversal exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in an overwrite of files. A malicious server or someone with access to the network traffic can provide an invalid filename for a splash image triggering the vulnerability.

Published: January 06, 2017; 04:59:01 PM -05:00 V3: 3.7 LOW

V2: 5.8 MEDIUM

CVE-2016-2380

An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent to the server could potentially result in an out-of-bounds read. A user could be convinced to enter a particular string which would then get converted incorrectly and could lead to a potential out-of-bounds read.

Published: January 06, 2017; 04:59:01 PM -05:00 V3: 3.1 LOW

V2: 4.3 MEDIUM

CVE-2016-2378

A buffer overflow vulnerability exists in the handling of the MXIT protocol Pidgin. Specially crafted data sent via the server could potentially result in a buffer overflow, potentially resulting in memory

corruption. A malicious server or an unfiltered malicious user can send negative length values to trigger this vulnerability.

Published: January 06, 2017; 04:59:01 PM -05:00 V3: 8.1 HIGH

V2: 6.8 MEDIUM

CVE-2016-2377

A buffer overflow vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent by the server could potentially result in an out-of-bounds write of one byte. A malicious server can send a negative content-length in response to an HTTP request triggering the vulnerability.

Published: January 06, 2017; 04:59:01 PM -05:00

Microsoft Application Server

Vuln ID Summary CVSS Severity

CVE-2017-3823

An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application

programming interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.

Published: February 01, 2017; 06:59:00 AM -05:00 V3: 8.8 HIGH

V2: 9.3 HIGH

CVE-2016-0051

The WebDAV client in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10

137

Gold and 1511 allows local users to gain privileges via a crafted application, aka "WebDAV Elevation of Privilege Vulnerability."

Published: February 10, 2016; 06:59:15 AM -05:00 V3: 7.8 HIGH

V2: 7.2 HIGH

CVE-2015-2359

Cross-site scripting (XSS) vulnerability in the web applications in Microsoft Exchange Server 2013 Cumulative Update 8 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Exchange HTML Injection Vulnerability."

Published: June 09, 2015; 09:59:38 PM -04:00 V2: 4.3 MEDIUM

CVE-2015-1771

Cross-site request forgery (CSRF) vulnerability in the web applications in Microsoft Exchange Server 2013 SP1 and Cumulative Update 8 allows remote attackers to hijack the authentication of arbitrary users, aka "Exchange Cross-Site Request Forgery Vulnerability."

Published: June 09, 2015; 09:59:37 PM -04:00 V2: 6.8 MEDIUM

CVE-2015-1764

The web applications in Microsoft Exchange Server 2013 SP1 and Cumulative Update 8 allow remote attackers to bypass the Same Origin Policy and send HTTP traffic to intranet servers via a crafted request, related to a Server-Side Request Forgery (SSRF) issue, aka "Exchange Server-Side Request Forgery Vulnerability."

Published: June 09, 2015; 09:59:33 PM -04:00 V2: 4.3 MEDIUM

CVE-2015-0086

Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 Gold and SP1, Word 2013 RT Gold and SP1, Word Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 Gold and SP1, Web Applications 2010 SP2, and Web Apps Server 2013 Gold and SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted RTF document, aka "Microsoft Office Memory Corruption Vulnerability."

Published: March 11, 2015; 06:59:13 AM -04:00 V2: 9.3 HIGH

CVE-2015-0085

Use-after-free vulnerability in Microsoft Office 2007 SP3, Excel 2007 SP3, PowerPoint 2007 SP3, Word 2007 SP3, Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013

Gold and SP1, Word 2013 Gold and SP1, Office 2013 RT Gold and SP1, Word 2013 RT Gold and SP1, Excel Viewer, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 Gold and SP1, Word Automation Services on SharePoint Server 2013 Gold and SP1, Web Applications 2010 SP2, Office Web Apps Server 2010 SP2, Web Apps Server 2013 Gold and SP1, SharePoint Server 2007 SP3, Windows SharePoint Services 3.0 SP3, SharePoint Foundation 2010 SP2, SharePoint Server 2010 SP2, SharePoint Foundation 2013 Gold and SP1, and SharePoint Server 2013 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Component Use After Free Vulnerability

Appendix 11

Google Hacking Database

2018-12-04	inurl:/help/lang/en/help	Various Online Devices	TheCrypticSailor
2018-12-04	inurl:public.php inurl:service ext:php	Various Online Devices	Rootkit_Pentester
2018-12-04	intitle:ProFTPD Admin - V1.04	Various Online Devices	XLOMBOX
2018-12-04	intitle: "VB Viewer"	Various Online Devices	Brain Reflow
2018-12-17	intitle: "Nexus Repository Manager"	Various Online Devices	Alfie

2019-01-17	inurl:/setup.cgi@next_file=	Various Online Devices	ManhNho
2019-01-21	"Please click here to download and install the latest plug-in. Close your browser before installation."	Various Online Devices	Sohaib E.B.
2019-01-30	intitle:QueryService Web Service	Various Online Devices	Miguel Santareno
2019-02-05	intitle:"Device(" AND intext:"Network Camera" AND "language:" AND "Password"	Various Online Devices	Brain Reflow
2019-02-05	intext:"Any time & Anywhere" AND "Customer Login"	Various Online Devices	Brain Reflow
2019-02-05	intitle: "Screenly OSE" intext:"Schedule Overview" AND "Active Assets" AND "Inactive Assets"	Various Online Devices	Brain Reflow
2019-02-05	inurl:"fhem.cfg" AND 'fhem.cfg' -github	Various Online Devices	Brain Reflow
2019-02-05	intitle:"webcam 7" inurl:'/gallery.html'	Various Online Devices	Brain Reflow
2019-02-05	intitle:"Login - Xfinity" AND "Gateway > Login"	Various Online Devices	Brain Reflow
2019-02-18	intitle:"Home-CUPS" intext:printers -mugs	Various Online Devices	Bruno Schmid
2019-02-19	inurl:/snap.cgi?&-getpic	Various Online Devices	Midori-SH
2019-02-20	allinurl:asdm.jnlp	Various Online Devices	Kevin Randall
2019-03-01	intitle:"NetcamSC IP Address"	Various Online Devices	Hussain Vohra

FORM UPR16

Research Ethics Review Checklist

Please include this completed form as an appendix to your thesis (see the Research Degrees Operational Handbook for more information

UNIVERSITY OF PORTSMOUTH

Postgraduate Research Student (PGRS) Information				**Student ID:**	795078
PGRS Name:	Priscilla M Boadi				
Department:	School of Computing	**First Supervisor:**	Dr Shikun Zhou		
Start Date: (or progression date for Prof Doc students)	**01/02/2016**				
Study Mode and Route:	Part-time ☐	MPhil ☐	MD ☐		
	Full-time ☒	PhD ☒	Professional Doctorate ☐		

Title of Thesis:	A Systematic Approach to a Quantitative Vulnerability Assessment for BYOD System Variables through the Discovering of Threats
Thesis Word Count: (excluding ancillary data)	33582

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study

Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

UKRIO Finished Research Checklist:
(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)

a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES ☒ NO ☐
b) Have all contributions to knowledge been acknowledged?	YES ☒ NO ☐
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES ☒ NO ☐
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES ☒ NO ☐
e) Does your research comply with all legal, ethical, and contractual requirements?	YES ☒ NO ☐

Candidate Statement:

I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)

Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):	C78F-68DE-6ED5-931F-3BC7-5799-AB27-3C9A

If you have *not* submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:

Signed *(PGRS)*:		**Date:** 08/09/2020