UNIVERSITI PUTRA MALAYSIA

ACCESS CONTROL FRAMEWORK IN A BRING YOUR OWN DEVICE ENVIRONMENT

OLALERE MORUFU

FSKTM 2016 43

ACCESS CONTROL FRAMEWORK IN A BRING YOUR OWN DEVICE ENVIRONMENT

By

OLALERE MORUFU

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

November 2016

DEDICATIONS

To my late daughter (Muzeenat Apeke Olalere)

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

ACCESS CONTROL FRAMEWORK IN A BRING YOUR OWN DEVICE ENVIRONMENT

By

OLALERE MORUFU

November 2016

Chairman : Mohd Taufik Abdullah, PhD
Faculty : Computer Science and Information Technology

As a result of several attractive features of mobile devices (portability and access to voice and data services), people have started to take their mobile devices to their work place and connect to the company network to do their daily job. This has given rise to a policy called "Bring Your Own Devices" or BYOD. However, to determine who is allowed to access enterprise resources poses a serious security concern as both the knowledge and ownership means of authentication in a traditional enterprise network are insufficient in a BYOD environment. Unauthorised access to sensitive information of an enterprise through a lost mobile device of an employee, by shoulder surfing password attacks and password guessing attacks can all lead to data leakage. Also, unmonitored employee mobile devices when connected to enterprise resources can inadvertently causes malware infection into the enterprise network. In a traditional enterprise network, Uniform Resource Locators (URLs) blacklisting is a common approach many enterprises employ to address this problem. Apart from the fact that the blacklisting approach is faced with different challenges (such as wrong classification due to human error and unavailability of newly created malware URLs), employing the blacklisting approach in a BYOD environment is not sufficient to monitor employee mobile devices.

For proper implementation of BYOD policy, the security challenges confronting BYOD need to be addressed. The need for addressing these challenges make this study significant. Consequently, this study proposes access control framework for authenticating and monitoring employee mobile devices in a BYOD environment. The proposed framework will not only authenticate employee mobile devices at the point of login to enterprise resources, but also monitor the interaction of the employee mobile device when connected to the enterprise resources. Consequently, the proposed access control framework consists of a two-factor authentication framework and monitoring framework. The proposition of these two novel frameworks for access control in a BYOD environment form the major contributions of the study.

The first framework which serves as the first layer of the proposed access control framework is a two-factor authentication framework that combines both knowledge-based and biometric-based authentication techniques to form an unobtrusive authentication technique for an employee's mobile device in a BYOD environment. This framework addresses the data leakage problem that may arise as a result of the present authentication technique being too weak. The second novel framework which serves as the second layer of the proposed access control framework is a real-time employee's mobile device monitoring framework. This framework addresses the possibility of a malware infection that may occur as a result of unmonitored interaction of an employee's mobile device with third party cloud applications.

Based on the second layer, another main contribution of this study is the proposition of a predictive trust model for computation of the trust value of a third party cloud application. For proper monitoring of the employee's mobile device against malware infection on the enterprise network, this study proposes classification of third party cloud application URLs that relies on a predictive trust model. The purpose of the trust value computation is to determine whether a trusted cloud application in terms of malware infection. Another major contribution under this layer is proposition of the novel discriminative lexical features that distinguish malware URL from benign URL.

To validate and test the performance of the model, a dataset comprising of benign and malware URLs was built. The dataset was trained and labelled. Application of the WEKA data mining tool on the trained dataset gave rise to computation of the performance evaluation parameters of the predictive trust model. Prediction performance was evaluated based on True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), accuracy, True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR), and the time to build the model. With a very short time to build the predictive trust model, the model achieved 97.31 % accuracy with a moderate FPR of 0.04 and a FNR of 0.018. The overall output of this study is the proposition of an implementable access control framework for a BYOD environment thereby serving as a potential application for authenticating and monitoring employee mobile devices in a BYOD environment.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

RANGKA KERJA KAWALAN CAPAIAN DALAM PERSEKITARAN BAWA PERANTI ANDA SENDIRI

Oleh

OLALERE MORUFU

November 2016

Pengerusi : Mohd Taufik Abdullah, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Hasil daripada beberapa ciri menarik peranti mudah alih (kemudahalihan dan capaian kepada perkhidmatan suara dan data), orang telah mula membawa peranti mudah alih mereka ke tempat kerja dan disambung kepada rangkaian syarikat untuk melakukan kerja harian mereka. Ini telah menerbitkan dasar yang dipanggil "Bawa Peranti Anda Sendiri" atau BPAS. Namun begitu, untuk menentukan siapa yang dibenarkan untuk mencapai sumber syarikat menimbulkan kebimbangan keselamatan yang serius kerana cara pengesahan kedua-dua pengetahuan dan pemilikan dalam jaringan perniagaan tradisional tidak mencukupi dalam persekitaran BPAS. Capaian tanpa kebenaran kepada maklumat perniagaan yang sensitif melalui peranti mudah alih seorang pekerja yang hilang, melalui serangan kata laluan intip bahu dan serangan penekaan kata laluan semuanya boleh membawa kepada kebocoran data. Juga, peranti mudah alih pekerja yang tidak diawasi apabila disambung kepada sumber perniagaan boleh menyebabkan jangkitan perisian hasad secara tidak sengaja ke dalam rangkaian perniagaan. Dalam rangkaian perniagaan tradisional, senarai hitam Pelokasi Sumber Seragam (PSS) adalah pendekatan kebiasaannya digunakan oleh kebanyakan syarikat untuk menangani masalah ini. Selain daripada fakta yang pendekatan senarai hitam hadapi berbagai cabaran (seperti pengelasan yang salah kerana kesilapan manusia dan tidak terdapatnya PSS perisian hasad yang terbaharu), menggunakan pendekatan senarai hitam dalam persekitaran BPAS tidak cukup untuk memantau peranti mudah alih pekerja.

Untuk pelaksanaan yang betul dasar BPAS, cabaran keselamatan yang dihadapi BPAS perlu ditangani. Keperluan untuk menangani cabaran-cabaran ini membuat kajian ini penting. Oleh itu, kajian ini mencadangkan rangka kerja kawalan capaian untuk mengesah dan memantau peranti mudah alih pekerja dalam persekitaran BPAS. Rangka kerja yang dicadangkan tidak hanya akan mengesahkan peranti mudah alih pekerja semasa log masuk ke dalam sumber perniagaan, tetapi juga memantau interaksi peranti mudah alih pekerja apabila disambung kepada sumber perniagaan. Oleh itu, rangka kerja kawalan capaian yang dicadangkan terdiri daripada rangka kerja pengesahan dua faktor dan rangka kerja pemantauan.

Cadangan kedua-dua rangka kerja baharu untuk kawalan capaian dalam persekitaran BPAS membentuk sumbangan utama kajian.

Rangka kerja pertama berperanan sebagai lapisan pertama rangka kerja kawalan capaian yang dicadangkan adalah rangka kerja pengesahan dua faktor yang menggabungkan kedua-dua teknik pengesahan berasaskan pengetahuan dan berasaskan biometrik untuk membentuk satu teknik pengesahan tanpa ganggu peranti mudah alih pekerja dalam persekitaran BPAS. Rangka kerja ini menangani masalah kebocoran data yang mungkin timbul akibat daripada teknik pengesahan yang terlalu lemah. Rangka kerja baharu kedua berfungsi sebagai lapisan kedua rangka kerja kawalan capaian yang dicadangkan adalah rangka kerja pemantauan peranti mudah alih pekerja pada masa nyata. Rangka kerja ini menangani kemungkinan jangkitan perisian hasad berlaku akibat daripada interaksi peranti mudah alih pekerja yang tidak diawasi dengan aplikasi awan pihak ketiga.

Berdasarkan lapisan kedua, satu lagi sumbangan utama kajian ini adalah cadangan model kepercayaan ramalan untuk pengiraan nilai kepercayaan aplikasi awan pihak ketiga. Untuk pemantauan peranti mudah alih pekerja daripada jangkitan perisian hasad pada rangkaian perniagaan, kajian ini mencadangkan pengelasan PSS aplikasi awan pihak ketiga yang berdasarkan model kepercayaan ramalan. Tujuan pengiraan nilai kepercayaan adalah untuk menentukan sama ada aplikasi awan dipercayai dari segi jangkitan perisian hasad. Satu lagi sumbangan utama yang terdapat di lapisan ini adalah cadangan ciri leksikal diskriminatif baharu yang membezakan PSS perisian hasad dengan PSS tidak berbahaya.

Untuk mengesahkan dan menguji prestasi model, satu set data yang terdiri daripada PSS tidak merbahaya dan PSS perisian hasad telah dibina. Set data telah dilatih dan dilabel. Pemakaian alatan perlombongan data WEKA pada set data terlatih menentukan pengiraan parameter penilaian prestasi model kepercayaan ramalan. Prestasi ramalan dinilai berdasarkan Positif Benar (PB), Negatif Benar (NB), Positif Palsu (PP), Negatif Palsu (NP), ketepatan, Kadar Positif Benar (KPB), Kadar Negatif Benar (KNB), Kadar Positif Palsu (KPP), Kadar Negatif Palsu (KNP) dan masa di ambil untuk membina model. Dengan masa yang singkat untuk membina model kepercayaan ramalan, ketepatan model adalah 97.31% sederhana dengan KPP iaitu 0.04 manakala KNP adalah 0.018. Output keseluruhan kajian ini adalah cadangan rangka kerja kawalan capaian yang dilaksanakan untuk persekitaran BPAS dan dengan itu dapat menjadi satu aplikasi yang berpotensi bagi mengesah dan memantau peranti mudah alih pekerja dalam persekitaran BPAS.

ACKNOWLEDGEMENTS

After Allah is Allah, all praise and adoration is due to the Almighty Allah, the giver and the taker of life, the cherisher and the sustainer of the world who is full of mercy and compassion for given me strength and good health during the period of my study at UPM.

I cannot but express my unreserved appreciation to my supervisory committee chair Dr. Mohd Taufik Abdullah for his valuable time, nice ideas, support, direction and guidance, “see me anytime policy” provided from the beginning of my study to the end. My deepest gratitude goes to my supervisory committee members, Professor Ramlan Mahmod and Dr. Azizol Abdullah for their time, support, suggestion, and constructive criticism that has impacted this study positively. I pray to Allah to reward you abundantly.

I am indebted to my late father Mr. Yusuf Olalere Alabata, for setting my feet in the education line. I prayed that almighty Allah count you among the inmate of paradise (amen). I will not forget to express my sincere gratitude to my mother Mrs. Serifat Olalere not only for given birth to me but also for her spiritual support. To my mother I say long life and prosperity. My sincere gratitude also goes to the sons and daughters of my late father for their support in one way or the other. I love you all my brothers and sisters.

My sincere appreciation goes to the following for their support during the period of my study, Dr. Richard Adesiji, Dr. Peter Adeoye, Engr. Segun Adebayo, and Mr. Abayomi Jegede. I appreciate the friendship and support I got from the Information Security Lab mates. I pray to Allah to reward you. I appreciate management of Federal University of Technology, Minna for sponsoring me. My appreciation also goes to my colleagues in the Department of Cyber Security Science for their support and cooperation. My sincere appreciation will not be completed if I fail to mention my one and only friend in Malaysia who stood by me throughout my study in UPM. Habibah binti Mohd Yusah I say thank you so much.

My wife, Zainab Maruf Olalere and my sons and daughter, Yusuf, Yunus and Zeenat. I appreciate you for your love, care, courage, patience, moral support, understanding, encouragement and above all your spiritual support endowed me with throughout my study period. I pray to Allah to admit our late daughter (Muzeenat) who died during the period of my study into paradise. Alhamdulillah Rabbil Alameen.

I certify that a Thesis Examination Committee has met on 3 November 2016 to conduct the final examination of Olalere Morufu on his thesis entitled "Access Control Framework in a Bring your Own Device Environment" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Shamala a/p K Subramaniam, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati binti Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Nur Izura binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Jemal Abawajy, PhD
Professor
Deakin University
Australia
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 26 January 2017

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Mohd Taufik Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Ramlan Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Azizol Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully -owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ________________________ Date: ___________________

Name and Matric No.: Olalere Morufu, GS38714

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ______________________
Name of Chairman of Supervisory Committee: Dr. Mohd Taufik Abdullahi

Signature: ______________________
Name of Member of Supervisory Committee: Professor Dr. Ramlan Mahmod

Signature: ______________________
Name of Member of Supervisory Committee: Dr. Azizol Abdullah

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

2TAC	2-Tier Access Control
APUFs	All Proposed Features
BBM	Black Berry Messenger
BL	Blacklist
BYOD	Bring Your Own Device
CA	Cloud Application
DDoS	Distributed Denial of Service
DNS	Domain Name System
eBC	Enterprise Business Context
ED	Employee Device
EMD	Employee Mobile Device
EDB	Enterprise Database
EMS	Enterprise Monitoring Server
FN	False Negative
FP	False Positive
FNR	False Negative Rate
FPR	False Positive Rate
iOS	iPhone Operating System
IP	Internet Protocol
IT	Information Technology
NB	Naïve Bayes
NPUFs	Not Previously Used Features
NPV	Negative Predictive Value
PA	Predictive Accuracy
PC	Personal Computer
PIN	Personal Identity Number
PPV	Positive Predictive Value
PriPARD	Privacy-Preserving Accountability for Personal Devices
PUFs	Previously Used Features
SLD	Second Level Domain
SVM	Support Vector Machine
TLD	Third Level Domain
TN	True Negative
TP	True Positive
TNR	True Negative Rate
TPR	True Positive Rate

TV	Set of Trust Values
tV	Trust Value
UK	United Kingdom
URL	Uniform Resource Locator
US	United States
Wi-Fi	Wireless Fidelity
WL	Whitelist
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

1.1 Background

Electronic computing has undergone several notable transitions since its birth in the 1940s. The journey started with mainframe computing followed by minicomputers then to client-server driven personal computing (PC). The PC era lead the information technology (IT) world to Internet computing. Mobile computing has classically supplanted Internet computing because of cloud based applications and the proliferation of mobile devices (such as smartphones, laptops, palmtops and tablets). People can experience high quality computing in their palm through cloud based applications and mobile devices. Mobile devices like smartphones and tablets combine several attractive features as they are easy to carry and provide access to voice and data services, thereby opening up a wide variety of potential mobile applications, “anytime and anywhere” (Disterer and Kleiner, 2013). People started going to their work place with mobile devices and getting connected to their company network so as to get their daily job done and to connect to their various social network platforms such as Facebook, WhatsApp, and Black Berry Messenger (BBM).

Using personal mobile devices for work gave rise to a trend called “bring your own device” or BYOD (Gheorghe and Neuhaus, 2013). Bring Your Own Device is an enterprise IT policy that encourages employees to use their own devices to access sensitive corporate data at work through an enterprise IT infrastructure (Li et al., 2013). The BYOD policy does not only allow employees to gain access to enterprise data when at the work place but also allows them to gain access to enterprise data outside the enterprise environment. This implies that employees can obtain access to the database of the enterprise remotely. Meanwhile, there are many security challenges associated with this advantage of BYOD. When employee’s access enterprise resources without appropriate control, there will be room for many possible information breaches such as data leakage that can lead to data theft. Moreover, employee mobile devices can be infected with malware, due to unmonitored interaction with cloud based applications. Many mobile device users rely on security measures offered by mobile device manufacturers. Security measures such as a four digit password for authentication and antivirus that maybe too weak are common forms of protection offered by most mobile device manufacturers.

Meanwhile, the security mechanisms offered by most popular mobile operating systems offer only limited protection to the threats posed by malicious applications that may be inadvertently installed by the users and therefore they do not meet the security standards required in corporate environments (Armando et al., 2013). There is need for organisations to make security a top priority when deploying BYOD. Organisations must compartmentalise access to sensitive information, employ better audit logging and log analysis, and deploy security solutions that are designed to support current BYOD strategies (Morrow, 2012). Therefore, the BYOD environment needs a new comprehensive security framework to address the problem of data leakage that may occur as a result of unauthorised access to the enterprise resources and the problem of malware infection that may occur as a result of unmonitored interactions of mobile devices with third party web based applications when connected to the enterprise resources.

1.2 Motivation

Growing pressures to enable and support the use of smartphones, tablets and other personal devices in the workplace means that ignoring the need to put in place some form of BYOD policy is no longer an option for today's businesses (Millard, 2013). A survey by Cisco (2012) to determine whether BYOD is growing only in United States or in large enterprises revealed that BYOD is a global phenomenon. Cisco carried out this survey across eight countries in three regions (Latin America, Asia, and Europe) including both enterprises (1000 or more employees) and midsize companies (500-999 employees). This survey was an expansion of an earlier survey conducted in the United States with 600 IT leaders from 18 industries.

A survey by Ovum (2012) of 3796 consumers in 17 countries in both emerging economies and developed economies, revealed that 75% of users in countries with emerging high-growth economies such as Malaysia, Singapore, Brazil, India and Russia use their own mobile devices at work, while 40% of workers in countries with developed economies such as the US, UK, Sweden, Italy and Japan use their own mobile devices at work. Gartner (2012) predicts that by 2018 seventy percent of mobile users will conduct all their work on personal smart devices. These surveys reports show that BYOD has come to stay in both emerging economies and developed countries. With this level of BYOD policy deployment and with future prediction of increasing deployment, the security challenges confronting BYOD need to be addressed. Consequently, this study is taking a step in addressing the top most security challenges confronting the BYOD policy. The need to address these challenges motivated this study.

1.3 Problem Statement

As both the organisations and their employees are reaping the benefits of BYOD, they are also worried about the challenges of the BYOD policy. The real security challenge of the BYOD environment is not actually about the devices, it is about controlling access from the device to the corporate data (Thielens, 2013) and the increased exposure of the enterprise network to malware due to the lack of control and visibility of the mobile devices of the employees (Pao, 2016). Throne (2016) pointed out that the enterprise must make sure that an employee mobile device connected to the sensitive data of the enterprise meets some standard of authentication as well as prevention and protection against viruses, malware and spyware.

Alharthy and Shawkat (2013), Camejo (2016), Liu (2016) claimed that the loss or theft of mobile devices is the biggest risk that businesses could face by implementing BYOD, because it leads to loss of data to unknown users. This implies that when an employee’s mobile device is in the hands of an unauthorised user or attacker, enterprise resources can be accessed through the mobile device if a strong authentication mechanism is not in place. A 2014 Verizon study revealed that 76% of breaches of corporate networks were due to weak employee passwords (Guccione, 2016). Perhaps, some authentication techniques are too restrictive that staff prefer to rely on a password or Personal Identity Number (PIN) which suffers from shoulder surfing attacks, brute force, and password guessing attacks to gain unauthorised access to enterprise resources through the lost mobile device. Therefore, a secure and scalable BYOD strategy is required to manage the risks introduced by employee owned devices as a result of the loss of a mobile device or the device being stolen by an attacker (Thielens, 2013). There should be a way in which the employee unique identity can be linked to the mobile device of the employee, such that when an attacker possesses the employee’s mobile device as a result of loss or theft, it will be difficult for the attacker to access enterprise resources through the misappropriated mobile device. Linking employee identity with the employee mobile device will result in strong authentication required for a BYOD environment.

Gone are the days when malware infection on an enterprise network only occurred through external storage devices such as an external hard disk or flash drive. With the rapid proliferation of Internet technologies and web applications, attackers can now use the web as a means of introducing malware into an enterprise network. In a traditional enterprise network (a desktop setting), this change in attack vector has forced many enterprises to subscribe to services that provide blacklisting of malware URLs which are provided by a range of techniques including manual submission of suspected malware URL and honeypots. The malware URL blacklist is used to monitor the interaction of members of an enterprise network with third party cloud applications. With 571 new websites available on the Internet per minute (CoNet, 2016), the blacklist approach to detect malware URLs is inadequate as many new malware URLs are not blacklisted immediately they are launched on the Internet. Moreover, since the blacklist is created by volunteer experts, human error in classification is unavoidable. Exact matching in blacklisting also renders it easy to be evaded (Choi, Zhu and Lee, 2011). Apart from the fact that this approach is faced with many challenges, the blacklist approach is not practically possible for the BYOD environment.

In a BYOD environment, the employee mobile device is used to access the enterprise network and interact with third party cloud applications through the Internet either by typing a URL on the web browser or by clicking a URL link to the web application. In any case, the URL serves as a means of getting access to third party cloud applications. Thus, this makes the URL an exploitable tool for attackers to infect malware into their victims’ devices. Meanwhile, the security mechanisms offered by most popular mobile operating system offer only limited protection against the threats posed by malicious applications that may be inadvertently installed by the users and they do not meet the security standards required in corporate environments (Armando et al., 2013). Also, many mobile devices do not have the resources to accommodate strong anti-malware. Meanwhile, malware infection of an employee mobile device through interaction with third party cloud applications can lead to malware infection of the enterprise network if the required security measures to prevent this are not in place.

Employee mobile device authentication and monitoring are among the key security concerns described by (Zahadat et al., 2015). Though their study does not offer any solution to this security issues, the need to address this security issues was emphasized. In essence, the two problems highlighted above can result in data leakage that may occur as a result of an authentication technique that is too weak which can lead to unauthorised access to enterprise resources and malware infection on the enterprise network due to a lack of proper monitoring of the interaction of the employee mobile device with third party applications. For better security, implementation, and management of the BYOD policy, strong authentication and proper monitoring of the employee's mobile device with third party cloud applications when connected to an enterprise network becomes necessary.

Consequently, this study proposes an access control framework for prevention of data leakage (that may occur as a result of an unauthorised user gaining access to an enterprise network) and for real-time malware detection (that may occur as a result of an employee mobile device interaction with third party application). The proposed access control does not only authenticate legitimate users of an employee mobile device at the point of login to the enterprise network, but also monitors the interaction of the employee mobile device when connected to enterprise resources with a view to detect third party web applications that can cause malware infection.

1.4 Objectives of the Research

The general objective of this study is to propose an access control framework for data leakage and malware detection for mobile devices in a BYOD environment, thereby offering potential future applications for better security, implementation, and management of the BYOD policy. To achieve this objective, the study will be guided by the following specific objectives:

1. To propose a two-factor authentication technique that maps the unique identity of employees with their mobile devices in order to prevent data leakage that may occur as a result of unauthorised access to enterprise resources.
2. To propose a novel framework for monitoring the interaction of the employee's mobile device with third party cloud applications for malware detection when connected to the enterprise network.
3. To propose a predictive trust model for computation of the trustworthiness of third party cloud applications for real-time malware URL detection that can lead to malware infection on an enterprise network through the employee's mobile device.

4. To propose novel discriminative features of malware URL for the proposed predictive trust model.

1.5 Scope of Research

The BYOD policy is faced with different challenges (see Chapter 2). However, the security challenge has been identified as the topmost challenge facing BYOD. According to the literature, data leakage and malware are the most challenging security threats to the BYOD policy (Morrow, 2012). The security issue in a BYOD environment has been of major concern of academic researchers, although not many contributions have been made in addressing these security challenges. In fact, very little has been done by researchers in addressing these challenges (both security challenges and others) facing BYOD. Niehaves et al. (2012) claimed that from the information system research perspective, a rigorous application of methods and theory to help practitioners understand the phenomenon of BYOD in general, and its implications for employee performance in particular, remains lacking.

However, this study does not address all the challenges confronting the BYOD policy. The study is focused on addressing the problem of access control that is lacking in both the literature and industries, which aims to prevent data leakage and malware infection of an enterprise network. The data leakage problem is addressed in this study by proposing a two-factor authentication technique that combines the unique identity of an employee with the traditional password system user authentication. It is important to note that only the theoretical details of the proposed two-factor authentication is within the scope of this study. Hence, the proposed two-factor authentication technique is not validated by any means. Also, this study addresses the BYOD malware challenge by proposing a monitoring framework that prevents the mobile device of the employee from introducing malware into an enterprise network through interaction with third party cloud applications. This framework can only monitor the employee mobile device when connected to the enterprise network. It is important to state clearly here that the monitor framework does not monitor the employee's mobile device when outside the enterprise network as this constitutes an infringement of employee privacy. However, for the case of an employee mobile device that might have been infected before establishing connection with the enterprise network, scanning before connection as proposed by (Beyondtrust, 2013) and (Chung, Chung, Escrig, Bai, and Endicott-Popovsky, 2012) becomes necessary.

1.6 Contributions of the Research

The main contribution of this thesis is the provision of an implementable access control framework for authenticating and monitoring the mobile devices of employees in a BYOD environment. The first part of the proposed access control framework authenticates the employee's mobile device at the point of connection to enterprise resources while the second part monitors the interaction of the employee's mobile device with third party cloud applications with a view to detect suspicious malware URL that can introduce malware into the enterprise network. The proposed access control has led to the following contributions:

a. Proposition of a two-factor authentication technique that combines two methods of authentication to form a strong authentication technique. This is to prevent an attacker who maybe is in possession of an employee's mobile device from gaining illegal access to the enterprise data as a result of a weak password that can suffer a series of attacks, including guessing.
b. Proposition of a monitoring framework that monitors the interaction of an employee's mobile device with third party cloud applications. This framework does not only monitor the employee's mobile device against interaction with malware URL but also creates a malware URL blacklist that can serve as a tool for security decisions or policy making. This framework is novel in the arena of BYOD.
c. Proposing a predictive trust model that computes trustworthiness of third party cloud applications. The essence of this model is to compute the trustworthiness of third party cloud applications that the employee may attempt to visit using his/her mobile device. If a third party cloud application is not trusted based on the value of computed trustworthiness, then the employee's mobile device will not be allowed to visit such web applications. The proposed predictive trust model was validated and evaluated accordingly.
d. Proposition of novel discriminative features of malware URL for the proposed predictive trust model. The predictive trust model uses discriminative features of malware URL to compute the trustworthiness of third party cloud applications. This study has identified a new set of discriminative features of malware URL. Experimentation with these sets of discriminative features shows good performance in terms of accuracy and effectiveness.

1.7 Organisation of Thesis

This chapter has provided a general overview of the entire thesis. The remainder of the thesis is structured as follows:

Chapter 2: Literature Review. This chapter reviews related work on BYOD. The chapter starts a with general discussion of BYOD including the BYOD environment network architecture, BYOD deployment level, BYOD benefits, BYOD challenges, security threats to BYOD, and BYOD and Mobile Device Management Applications. This chapter also reviews existing works concerning BYOD. The last part of this chapter presents an overview of different types of authentication techniques vis-à-vis the way each type of authentication technique works. The strengths and weaknesses of each type of authentication technique are also presented.

Chapter 3: Research Methodology. In this chapter, the Research Methodology is presented and this gives an overview of the whole process involved in this study. The chapter begins with a presentation of the input and output of this study. Also presented in this chapter are the components of the proposed access control framework. Also discussed in this chapter are the design, data collection, and experimentation processes. The last part of the chapter discusses the performance evaluation parameters used for this study.

Chapter 4: Proposed two-factor authentication: This chapter presents the proposed two-factor authentication technique. The proposed two-factor authentication technique framework is also described in this chapter. How each of the components of the framework works is also detailed. Finally, the chapter is concluded by a review of previous studies on keystroke dynamics.

Chapter 5: Proposed monitoring framework. The proposed monitoring framework is presented in this chapter. The chapter begins with an overview of the proposed framework. This is followed by a description of the proposed monitoring framework. The components of the proposed monitoring framework are also discussed in this chapter. A description of the predictive trust model is presented in this chapter. A description is given of how a whitelist and blacklist are created. Further discussion focuses on the proposed discriminative lexical features. Categories of the proposed features are also presented in this chapter.

Chapter 6: Results and Discussion. This chapter focuses on the results of all the experiments performed in this study. The chapter starts with the results of the preliminary experiments for validating the predictive trust model. Performance evaluation of the results of the experiments with different categories of the proposed discriminative lexicon are also presented in this chapter. A performance evaluation comparing the categories of the proposed discriminative lexical features is given. This chapter is concluded with a comparison of this study with previous studies.

Chapter 7: Conclusion. Chapter 7 is the final chapter of the thesis. The chapter presents the conclusion of the study. The chapter discusses the contributions of this study and future works that can improve or serve as extension to this study.

REFERENCES

Airwatch. (2012). Enabling bring your own devices (BYOD) in the enterprise. Retrieved from http://www.ciosummits.com/media/solution_spotlight/byod-whitepaper.pdf

AlHarthy, K., & Shawkat, W. (2013). Implement network security control solution in BYOD environment. *IEEE International Conference on Control System, Computing and Engineering*, Penang, Malaysia, pp. 7- 11.

Armando, A., Costa, G., & Merlo, A. (2013). Bring your own device, securely. *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, Coimbra, Portugal, pp. 1852-1858.

Babaeizadeh, M., Bakhtiari, M., and Maarof, M. A. (2014). Keystroke dynamic authentication in mobile cloud computing. International Journal of Computer Application. (90)1: 29-36.

Basnet, R.B. & Sung, A.H. (2014). Learning to detect phishing webpages. Journal of Internet Services and Information Security (JISIS). (4)3, pp. 21-39

Bell Technogix. (2013). The real benefits of BYOD. White paper. Retreived from http://belltech.wpengine.com/wpcontent/uploads/2015/07/BellTechlogix_RealBenefitsOfBYOD2.pdf

BeyondTrust. (2013). Best Practices for Securing Remote and Mobile Devices. Retrieved from http://www.beyondtrust.com/Content/whitepapers/BestPractices-for-Securing-Remote-and-Mobile-DevicesWP.pdf.

Bleha, S., Silvinsky, C., and Hussien, B. (1990). Computer-access security systems using keystroke dynamics. IEEE Transactions on Pattern Analysis and Machine Intelligence. (12)12: 1217–1222.

Blum, A., Wardman, B., Solorio, T., Warner, G. (2010). Lexical feature based phishing URL detection using online learning. Proceedings of the 3rd ACM workshop on Artificial Intelligence and Security; 2010 October 04 – 08; Chicago, Illinois, USA. ACM; 2010. p. 54-60.

Camejo, C. (2016). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. *Digital guardian*. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Campisi, P., Maiorana, E., Bosco, M. L., and Neri, A. (2009). User authentication using keystroke dynamics for cellular phones. IET Signal Process. (3)4: 333-341. Retrieved December 10, 2014 from http://www.ietdl.org.

Choi, HS., Zhu, BB., Lee, H. (2011). Detecting malicious web links and identifying their attack types. Proceedings of the 2nd USENIX Conference on Web Application Development; 2011 USENIX Association Berkeley, CA, USA.

ACM Digital Library; 2011. p. 1-11.

Chung, S., Chung, S., Escrig, T., Bai, Y., & Endicott-Popovsky, B. (2012). 2TAC: Distributed access control architecture for “bring your own device” security. *ASE/IEEE International Conference on Biomedical Computing*. Washington, DC, pp. 123-126.

Cisco. (2012). BYOD: A global perspective. Survey report. Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf.

Clarke, N. L., and Furnell, S. M. (2007). Advance User authentication for mobile devices. Computer and Security. (26)2: 109-119.

Clarke, N. L., Furnell, S. M., and Reynolds, P. L. (2002). Subscriber authentication for mobile phone using keystroke dynamics. Proceedings of the Third International Network Conference (INC 2002). Plymouth, UK: 347-455.

CoNet. (2016). Ever wondered how many websites are created every minut? [Internet] 2014 June 11 [updated 2016 Jan 1; cited 2016 Apr 5]. Available from http://www.designbyconet.com/2014/06/ever-wondered-how-many-websites-are-created-every-minute/.

Copeland, R., & Crespi, N. (2012). Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules. *IEEE 16th International Conference on Intelligent in Next Generation Networks*, Berlin, Germany.

Crawford, H. (2010). Keystroke dynamics: characteristics and opportunities. Eighth Annual International Conference on Privacy, Security and Trust. 17-19 August 2010, Ottawa: 205-212.

De las Cuevas, P., Mora, A.M, Merelo, J.J, Castillo, P.A., García-Sánchez, P., & Fernández-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer communications*. Vol. 68, pp. 83-95.

Deloitte. (2013). Understanding the bring-your-own-device landscape. *A Deloitte research report*. Retrieved from http://www.deloitte.com/assets/Dcom-Guam/Local%20Assets/Documents/Technology,%20 Media%20and%20Telecommunications/Understanding%20the%20bring-your-own-device%20 landscape.pdf.

Denman, S. (2012). Why multi-layered security is still the best defence. *Network Security, 2012*, 5-7. doi:10.1016/S1353-4858(12)70043-0.

Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology, 9*, 43-53. doi:10.1016/j.protcy.2013.12.005.

Dmoz. (2015). Open directory project. Retrieved from http://www.dmoz.org.

Edwards, C. (2013). Identity - The new security perimeter. *Computer Fraud & Security, 2013*, 18-19. doi:10.1016/S1361-3723(13)70082-4.

Engle, M. (2009). The seven steps of the research process. *Oline Library Reference Research and Learning Services, Olin and Uris Libraries, Ithaca, NY: Cornell University Library*. Retrieved from www.library.cornell.edu/olinuris/ref/research/skill1.htm.

Eshete, B., Villafiorita, A., Weldemariam, K. (2012). BINSPECT: Holistic analysis and detection of malicious web pages. *Proceedings of 8th International ICST Conference, SecureComm 2012; 2012 Sep. 3–5; Padua, Italy. Berlin*: Springer; 2013. p. 149-166.

Ernst & Young. (2013). Bring your own device: Security and risk considerations for your mobile device program. Insights on governance, risk and compliance. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf.

Flior, E. and Kowalski, K. (2010). Continuous biometric user authentication in online examination. Seventh International Conference on Information Technology. IEEE Computer Society. 12-14 April, 2010, Las Vegas: 488-492.

Forrester. (2012). Key strategies to capture and measure the value of consumerization of IT. *Cambridge, MA: Forrester Consulting*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf.

Gaines, R., Lisowski, W., Press, S., & Shapiro, N. (1980). Authentication by keystroke timing: some preliminary results. Technical Report Rand Rep. R-2560-NSF, RAND Corporation, 1980. Retrieved from https://www.rand.org/content/dam/rand/pubs/reports/2006/R2526.pdf.

Garcia, J. (1986). Personal identification apparatus. U.S. Patent Number 4,621,334, November 4, 1986. Retrieved November 3, 2014, from http://www.google.com/patents/US4621334.

Gartner. (2014). Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018. *Gartner Newsroom*. Retrieved from http://www.gartner.com/newsroom/id/2648515.

Gheorghe, G., & Neuhaus, S. (2013). Poster: Preserving privacy and accountanbility for personal devices. *Presented at the Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS' 13)*, Berlin, Germany, pp. 1359-1361.

Grover J. (2013). Android forensics: Automated data collection and reporting from a mobile device. *Rochester Institute of Technology, RIT Scholar Works*. Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=5389&context=theses.

Guccione, D. (2010). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. Digital guardian. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Guven, A., and Sogukpinar, I. (2003). Understanding users' keystroke patterns for computer access security. Computer and Security. (22)8: 695-706.

Ho, G. (2013). Tapdynamics: strengthening user authentication on mobile phones with keystroke dynamics. Technical report, Stanford University. Retrieved from http://cs229.stanford.edu/proj2013/Ho-TapDynamics.pdf

Howard, D. (2016). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. *Digital guardian*. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Hwang, S., Cho, S.-s., and Park, S. (2009). Keystroke dynamics-based authentication for mobile devices. ScienceDirect Computer and Security. (28)1-2: 85-93.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Trans. Circuits and Systems for Video Technology*. (14)1: pp. 4-20.

Jaramillo, D., Newhook, R., & Smart, R. (2013, April). Cross-platform, secure message delivery for mobile devices. *Proceedings of IEEE*, Southeastcon, Jacksonville, FL, pp. 1-5.

Johnson, K. (2012). BYOD security survey. *A SANS Whitepaper*. Retrieved from http://www.sans.org/reading-room/analysts-program/mobility-sec-survey.

Kalafut, AJ., Shue, CA., Gupta, M. (2010). Malicious hubs: detecting abnormally malicious autonomous systems. Proceedings of IEEE INFOCOM, 2010 Conference. 2010 March 14-19; San Diego, CA, USA. IEEE; 2010. p. 1-5.

Karnan, M., Akila, M., and Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamic: a review. Applied Soft Computing. (11)2: 1565-1573.

Kerravala, Z. (2012). Bring-your-own-device requires new network strategies. *ZK Research.* Retrieved from http://www.xirrus.com/cdn/pdf/zeusk_byod_requires_new_network_strategies.

Kim, D. H., Gong, J. H., Park, W. H., & Park, N. (2013). Vulnerability of information disclosure in data transfer section for safe Smartwork infrastructure. *2013 International Conference on Information Science and Applications (ICISA),* Suwon, South Korea, pp. 1-3.

Kodeswaran, P., Chakraborty, D., Sharma, P., Mukherjea, S., & Joshi, A. (2013). Combining smart phone and infrastructure sensors to improve security in enterprise settings. *1st International Workshop on Pervasive Urban Crowdsensing Architecture and Applications*, Zurich, Switzerland, pp. 1151-1158.

Krcma, P. (2016). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. *Digital guardian*. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Le, A., Markopoulou, A., Faloutsos, M. (2010). PhishDef: URL names say it all. Proceedings of IEEE INFOCOM, 2011; 2011 April 10-15; Shanghai, China. IEEE; 2011.p. 191–195.

Leavitt, N. (2013). Today’s mobile security requires a new approach. *IEEE Computer Society, 46*, 16-19.

Lee, J., Lee, Y., & Kim, S. (2013). A white-list based security architecture (WLSA) for the safe mobile office in the BYOD era. In *Grid and pervasive computing* (vol. 7861, pp. 860-865). Berlin, Germany: Springer.

Li, F., Peng, W., Huang, C., & Zou, X. (2013, June). Smartphone strategic sampling in defending enterprise network security. *IEEE International Conference on Communications*, Budapest, Hungary, pp, 2155-2159.

Link klipper. (2015). Retrieved from https://chrome.google.com/webstore/category/apps?hl=en.

Liu, S. (2016). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. *Digital guardian*. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Mahesh, S., & Hooter, A. (2013). Managing and securing business networks in the smartphone era. *Management Faculty Publications*. Paper 5. Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5.

Maiorana, E., Campisi, P., Gonzalez-Carballo, N., and Neri, A. (2011). Keystroke dynamics authentication for mobile phone. Proceedings of the 2011 ACM Symposium on Applied Computing. 21-25 march, 2011 Taichung, Taiwan: 21-26.

MalwarePatrol. (2015). Retrieved from http://www.malwarepatrol.net.

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security, 2012*, 14-17. doi:10.1016/S1361-3723(12)70031-3.

Millard, A. (2013). Ensuring mobility is not at the expense of security. *Computer Fraud & Security, 2013*, 11-13. doi:10.1016/S1361-3723(13)70080-0.

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

Monrose, F., and Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems. (16)2000: 351–359.

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

MTI Technology. (2014). Bring your own device. The future of corporate computing. *MTI white paper*. Retrieved from https://mti.com/Portals/0/Documents/White%20Paper/MTI_BYOD_WP_UK.pdf.

Nauman, M., and Ali, T. (2010). Token: trustable keystroke-based authentication for web-based applications on smartphones. Informationa Security and Assurance. (76)2010: 286-297.

Niehaves, B., Koffer, S., Ortbatch, K., & Katschewitz, S. (2012). Towards an IT consumerization theory: A theory and practice review. *Working papers*, *ERCIS – European Research Center for Information Systems*, no 13. Retrieved from htt://hdl.handle.net/10419/60246.

Ovum. (2012). An emerging market trend in more ways than one. *Consumer impact technology*. Retrieved from http://www.us.logicalis.com/global/united%20states/whitepapers/logicalisbyodwhitepaperovum.pdf.

Pao, S. (2016). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. Digital guardian. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Peacock, A., Ke, X., and Wilkerson, M. (2004). Typing patterns: A key to user identification. IEEE on Security and Privacy. (2)5: 40-47.

Peng, W., Li, F., Han, K. J., Zou, X., & Wu, J. (2013, October). T-dominance: Prioritized defense deployment for BYOD security. *IEEE Conference on Communication and Network Security (CNS)*, National Harbor, MD, pp. 37-45.

Polla, M. L., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE Communications Surveys & Tutorials, 15*, 446-470.

Potts, M. (2012). The state of information security. *Network Security, 2012*, 9-11. doi:10.1016/S1353-4858(12)70064-8.

Ramu, T. and Arivoli T. (2013). A framework of secure biometric based online exam authentication: an alternative to traditional exam. International Journal of Scientific and Engineering Research. (4)11: 52-60. Retrieved November, 20 2014 from http://www.ijser.org.

Sayamber A. B., Dixit A. M. (2014). Malicious URL detection and identification. International Journal of Computer Applications. 2014 August; 99(17):17-23

Scarfo, A. (2012). New security perspectives around BYOD. *Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, Victoria, BC, pp. 446-451.

Shanmugapriya, D., and Padmavathi, G. (2009). A survey of biometric keystroke dynamics: approaches, security and challenges. International Journal of computer Science and Information Security. (5)1: 115-119.

Shepherd, S. J. (1995). Continuous authentication by analysis of keyboard typing characteristics. European Convention on Security and Detection. 16 May-18

May, 1995. Brighton, UK: 111-114.

Soghoian, C., & Stamm, S. (2010). Certified lies: detecting and defeating government interception attacks against SSL. Retreived from http://files.cloudprivacy.net/ssl-mitm.pdf

Spillane, R. (1975). Keyboard apparatus for personal identification. Technical report. IBM Technical Disclosure Bulletin. (17)11: 3346-3346.

SSLShopper. (2008). When are self-signed certificates acceptable? Retreived from https://www.sslshopper.com/article-when-are-self-signed-certificates-acceptable.html.

Stewart, J. C., Monaco, J. V., Cha, S.-H., and Tappert, C. C. (2011). An investigation of keystroke and stylometry traits for authenticating online test takers. Proceeding of the International Joint Conference on Biometrics (IJCB `11). Washington, DC. 11-13 October, 2011: 1-7.

Tasia, CJ., Chang, TY., Cheng, PC., Lin, JH. (2013). Two novel biometric feature in keystroke dynamics authentication system for touch screen devices. Security Comm. Networks 2014(7): 750-758.

Teh, P. S., Teoh, A. B. J., and Yue, S. (2013). A survey of keystroke dynamics biometrics. The Scientific World Journal. 2013: 1-24.

Teh, P. S., Teoh, A. B. J., Tee, C., and Ong, T. S. (2010). Keystroke dynamics in password authentication enhancement. Expert System with Applications. (37)12: 8618-8627.

Thielens, J. (2013). Why API are central to a BYOD security strategy. *Network Security, 2013,* 5-6. doi:10.1016/S1353-4858(13)70091-6.

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security, 2012*, 5-8. doi:10.1016/S1353-4858(12)70013-2.

Thorne, M. (2016). BYOD Security: Expert Tips on Policy, Mitigating Risks, & Preventing a Breach. Digital guardian. Retreived from https://digitalguardian.com/blog/byod-security-expert-tips-policy-mitigating-risks-preventing-breach.

Titze, D., Stephanow, P., & Schutte, J. (2013, March). A configurable and extensible security service architecture for smartphones. *27th International Conference on Advance Information Networking and Applications Workshops*, Barcelona, Spain, pp. 1056-1062.

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

Trojahn, M., Arndt, F., and Ortmeier, F. (2013). Authentication with keystroke dynamics on Touchscreen kaypads-effect of different n-graph combinations. MOBILITY 2013: The Third International Conference on Mobile Services, Resources, and User. 17 – 22 November, 2013, Lisbon, Portugal: 114-119.

Wang, W., & Shirley, K. E. (2015). Breaking bad: detection malicious domain using word segmentation. Proceedings of the 9th Workshop on Web 2.0 Security and Privacy (W2SP) 2015.

Werthmann, T., Hund, R., & Davi, L. (2013). PSiOS: Bring your own privacy & security to iOS devices. *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, Hangzhou, China, pp. 13-24.

Wikipedia. (2016). Logistic regression. Retreived from https://en.wikipedia.org/wiki/Logistic_regression

Young, J. R. and Hammond, R. W. (1989). Method and apparatus for verifying an individual's identity. U.S. Patent Number 4,805,222. Retrieved November 5, 2014, from http://www.google.com/patents/US4805222A.

Zahadat, N., Blessner, P., Blackburn, T. & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*. Vol. 55: pp. 81-99.

Zahid, S., Shahzad, M., Khayam, S. A., and Farooq, M. (2009). Keystroke-based user identification on smart phones. Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID). Semptember, 2009, Berlin, Heidelberg: 224-243.

Zhao, Z., & Osorio, F. C. (2012). "TrustDroid^{TM}: Preventing the use of smartphones for information leaking in corporate networks through the use of static analysis taint tracking. *7th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, pp. 135-143.