AN AUTHENTICATION FRAMEWORK FOR MOBILE DEVICE IN CORPORATE NETWORKS: The Case study of Eastern Uganda

Mboto Peter

BU/GS18/MCF/1

A DISSERTATION SUBMITTED TO THE DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND INNOVATION IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER IN COMPUTER FORENSICS DEGREE OF
BUSITEMA UNIVERSITY

BUSITEMA UNIVERSITY

MAY 2022

CERTIFICATION

The undersigned certify that they have read and hereby recommend for examination by Busitema University a dissertation titled: ***An Authentication Framework for Mobile Device in corporate networks, the case study of Eastern Uganda***, in partial fulfillment of the requirements for the award of Masters in computer forensics of Busitema University.

………………………………..………

DR. SAMSON RWAHWIRE

(MAIN SUPERVISOR)

Date: ………………………………………

…………………………………………

DR. GILBERT OCEN

(SUPERVISOR)

Date: ………………………………………

………………………………………………

DR. GODLIVER OWOMUGISHA

(SUPERVISOR)

Date: ………………………………………

DECLARATION AND COPYRIGHT

I **Mboto Peter,** declare that this dissertation is my original work and that it has not been presented and will not be presented to any other university for a similar or any other degree award.

Signature …………………………………

ABSTRACT

This study was envisioned to identify the evolving mobile security challenges, and threats brought about by Mobile device authentication onto corporate networks. The researcher preferred corporate networks because mobile devices are in extensive use by corporate employees together with clients and hence the challenges, threats, and attacks would be more pronounced and frequent requiring, outstanding attention, and solution. Most corporate organizations have their branches in Eastern Uganda, the reason why it was selected a case study to give a representative sample. The challenges, threats, and attacks were found using a questionnaire administered to 10 purposively selected corporate organizations with a reasonable number of employees and improved systems. Other existing frameworks were reviewed in order to find out how they tackled mobile device threats and authentication challenges in a corporate networked environment. A number of mobile device security frameworks were examined and improved to include additional security features such as advanced device access to the corporate network using Radius server security attributes available to offer multifactor authentication, malware detection and prevention, mobile device user categorization, and access control to servers, and rogue access points by disabling Hotspots applications in mobile devices. A Common Vulnerability Scoring System (CVSS) Version 3.1 was adapted to quantify, evaluate, and assess the severity of systems' security vulnerabilities in the performance of the MDA framework. The MDA framework was tested and validated using simulation techniques (Riverbed modeler version 17.5), which involved introducing the framework to a mobile Dos assault, putting preventive measures in place to handle the attack, and then comparing the simulation results. Various aspects of network performance were tested on corporate servers that would be targeted. The study findings from corporate organizations indicated that organizations had few (i.e. software antivirus and firewall protection) or no measures to address the evolving mobile device security challenges and attacks they experienced and hence MDA framework would be very useful if physically implemented.

ACKNOWLEDGMENT

I am grateful to my supervisors; Dr. Ocen Gilbert, Dr. Samson Rwahwire, and Dr. Godliver Owomugisha for your fruitful support and guidance in this project's completion and success. Your valuable contribution made it possible for me to achieve the objectives of this Project. May the Lord reward you for this wonderful service.

Special thanks to my mentor, the late Mr. Felix Bwire for his valued time, patience, and encouragement in walking me through this journey to achieve and complete this project. God bless you and may He rest you in eternal peace!

I thank my colleagues, MCF class 2018 for your collaboration. I value all your efforts.

Above all, I sincerely give thanks to you, O Lord for your strength, guidance, and capability to work on this project. My tongue will tell of your righteousness and praises forever.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

BYOD	Your Own Device
CVSS	Common Vulnerability Scoring System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOS	Denial of Service Attack
FTP	File Transfer Protocol
IP	Internet Protocol
IBM	International Business Machines
ISMS	Information Security Management Systems
MAC	Media Access Control
MAM	Mobile Applications Management
MDA	Mobile Device Authentication
MAUP	Multi Access User Policy
MDM	Mobile Device Management
NAC	Network Access Control
NITA-U	National Information Technology Authority-Uganda
OTP	One Time Password
SIM	Subscriber Identity Module
SPD	Security Policy Database
SSID	Service Set Identifier
VPN	Virtual private Network
WLAN	Wireless Local Area Network

CHAPTER ONE:
INTRODUCTION

1.0 Introduction

This chapter discusses the study's background, the problem statement, the study's purpose, the study objectives, and the research questions. It also covers the scope of the investigation, the motivation for the study, the significance of the study, the research framework, and the study's limitations.

1.1 Background of the Study

It has been over 25 years since mobile phones performed the roles of personal computers. In 1992, Simon's personal communicator, the first mobile device, was unveiled by International Business Machines (IBM) and made available to consumers in 1994. A survey conducted in 2010 by Breitinger Frank and Nickel Claudia revealed that mobile phone users worldwide exceeded 4 billion for the first time; indicating that mobile phones were used by two-thirds of the world's population (Breitinger, Nickel and Darmstadt, 2010) And approximately 5 billion people around the globe are using smartphones (Taylor and Silver, 2019). Furthermore, with the current improvement in wireless telecommunications, we are expected to have their number grow from 25 to 50 billion connected devices by 2020 (Silverio-Fernández, Renukappa and Suresh, 2018). Farrell (2015) pointed out that mobile devices nowadays come with improved functionality and increased storage of different sensitive data, making them more attractive to thieves.

Androulidakis (2016) conducted a study in 17 universities in 10 European countries to assess users' levels of security feeling and awareness regarding mobile device

REFERENCES

Abeka, S. O. (2012) 'Perceived Usefulness, Ease of Use, Organizational and Bank Support As Determinants of Adoption of Internet Banking in East Africa', *International Journal of Academic Research in Business and Social Sciences*, 2(10), pp. 2222–6990. Available at: https://www.mendeley.com/reference-manager/library/all-references.

Akbanov, M., Vassilakis, V. G. and Logothetis, M. D. (2019) 'WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms', *Journal of Telecommunications and Information Technology*, (1), pp. 113–124. doi: 10.26636/jtit.2019.130218.

Aker, J. C., Collier, P. and Vicente, P. C. (2017) 'Is information power? Using mobile phones and free newspapers during an election in Mozambique', *Review of Economics and Statistics*. doi: 10.1162/REST_a_00611.

Alhaidary, M. *et al.* (2018) 'Vulnerability Analysis for the Authentication Protocols in Trusted Computing Platforms and a Proposed Enhancement of the OffPAD Protocol', *IEEE Access*, 6(March), pp. 6071–6081. doi: 10.1109/ACCESS.2017.2789301.

Ambhire, V. R. and Teltumde, P. S. (2011) *Information Security in Banking and Financial Industry*, *IJCEM International Journal of Computational Engineering & Management*.

Amin, M. E. (2005) *Social Science Research Conception Methodology and Analysis.*, *Makerere University Printeryafd, Kampala.* Available at: https://scirp.org/reference/referencespapers.aspx?referenceid=2568178 (Accessed: 7 May 2022).

Androulidakis, I. I. (2016) *Mobile phone security and forensics: A practical approach, second edition*, *Mobile Phone Security and Forensics: A Practical Approach, Second Edition*. doi: 10.1007/978-3-319-29742-2.

Baffour, B., King, T. and Valente, P. (2013) 'The Modern Census: Evolution, Examples and Evaluation', *International Statistical Review*, 81(3), pp. 407–425.

Breitinger, F., Nickel, C. and Darmstadt, H. (2010) ‘User SurveyonPhone Security and Usage’.

Chakraborti, S., Acharjya, D. P. and Sanyal, S. (2015) ‘Application Security framework for Mobile App Development in Enterprise setup’, (March). Available at: http://arxiv.org/abs/1503.05992.

Clarke, P. (2013) ‘Tablets: Will They Replace PCs?’, *©Nemertes Research*, pp. 1–6. Available at: http://i.crn.com/custom/INTELBCCSITENEW/WhitePaper_Tablets_ReplacePCs.pdf.

Davis, M. *et al.* (2019) ‘State of cyber security: the Ugandan perspective’, *International Journal of Scientific & Engineering Research*.

Eddy, N. (2014) ‘Employees Slow to Report Stolen Mobile Devices’, *e-Week*. Available at: https://www.eweek.com/small-business/employees-slow-to-report-stolen-mobile-devices (Accessed: 7 October 2020).

Farrell, G. (2015) ‘Preventing phone theft and robbery: The need for government action and international coordination’, *Crime Science*. doi: 10.1186/s40163-014-0015-0.

Gadhiya, S., Bhavsar, K. and Student, P. D. (2013) ‘Techniques for Malware Analysis’, *International Journal of Advanced Research in Computer Science and Software Engineering*.

Gimenez Ocano, S. *et al.* (2015) ‘DigitalCommons@University of Nebraska-Lincoln Remote Mobile Screen (RMS): an approach for secure BYOD environments Remote Mobile Screen (RMS): an approach for secure BYOD environments’. doi: 10.1109/ICCNC.2015.7069314.

Gold, S. (2011) ‘Android insecurity’, *Network Security*. doi: 10.1016/S1353-4858(11)70104-0.

Gregor, S. and Hevner, A. R. (2013) ‘Positioning and presenting design science research for maximum impact’, *MIS Quarterly: Management Information Systems*. doi: 10.25300/MISQ/2013/37.2.01.

He, D., Chan, S. and Guizani, M. (2015) ‘Mobile application security: Malware threats and defenses’, *IEEE Wireless Communications*, 22(1), pp. 138–144. doi: 10.1109/MWC.2015.7054729.

Herenandez, A. B. and Choi, Y. B. (2014) ‘Securing BYOD Networks’, *International Journal of Computer and Information Technology*.

Hevner, A. R. *et al.* (2004) ‘Design science in information systems research’, *MIS Quarterly: Management Information Systems*. doi: 10.2307/25148625.

ITU (2014) *Understanding cybercrime: phenomena, challenges and legal response*, *Proceedings of the Annual Hawaii International Conference on System Sciences*.

Jack, W., Ray, A. and Suri, T. (2013) ‘Transaction networks: Evidence from mobile money in Kenya’, in *American Economic Review*. doi: 10.1257/aer.103.3.356.

Jafari, N. *et al.* (2016) ‘Designing a comprehensive security framework for smartphones and mobile devices’, *American Journal of Engineering and Applied Sciences*, 9(3), pp. 724–734. doi: 10.3844/ajeassp.2016.724.734.

Jayapandian N. (2019) ‘Threats and Security Issues in Smart City Devices’, in, pp. 220–250. doi: 10.4018/978-1-5225-7189-6.ch009.

Lane, N. D. *et al.* (2010) ‘Ad Hoc and Sensor Networks: A Survey of Mobile Phone Sensing’, *IEEE Communications Magazine*.

Lee, S. *et al.* (2018) ‘Game theory-based Security Vulnerability Quantification for Social Internet of Things’, *Future Generation Computer Systems*. doi: 10.1016/j.future.2017.09.032.

Lin, T. *et al.* (2019) *Over-the-air (ota) mobility services platform*.

Lutui, P. R. (2015) ‘Digital forensic process model for mobile business devices : Smart technologies’. Available at: http://aut.researchgateway.ac.nz/bitstream/handle/10292/9242/LutuiPR.pdf.

Majdi, E. B. (2013) *Evaluation of Mobile Device Management Tools and Analysing Integration Models for Mobility Enterprise*. Available at:

http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-74017.

Marler, W. (2018) ‘Mobile phones and inequality: Findings, trends, and future directions’, *New Media and Society*. doi: 10.1177/1461444818765154.

Matovu, D. *et al.* (2019) *The Internet of Things: applications and security metrics with the Ugandan perspective*, *International Journal of Advance Research*. Available at: www.IJARIIT.com.

Mohamad, M. M. *et al.* (2015) ‘Measuring the Validity and Reliability of Research Instruments’, *Procedia - Social and Behavioral Sciences*, 204, pp. 164–171. doi: 10.1016/J.SBSPRO.2015.08.129.

Ndeng’ere, D. K. (2017) ‘a Byod Framework for Secure Use of Mobile Devices in’.

NITA-U (2014) ‘National Information Security Policy (NITA-U)’, *Information Security*, (August).

Obodoeze, F. C. *et al.* (2013) ‘A Holistic Mobile Security Framework for Nigeria’, (3), pp. 5–11.

Okane, P., Sezer, S. and McLaughlin, K. (2011) ‘Obfuscation: The hidden malware’, *IEEE Security and Privacy*, 9(5), pp. 41–47. doi: 10.1109/MSP.2011.98.

Omori, S. (2017) ‘Information Security Report 2011’, pp. 1–32.

Peng, S., Yu, S. and Yang, A. (2014) ‘Smartphone malware and its propagation modeling: A survey’, *IEEE Communications Surveys and Tutorials*, 16(2), pp. 925–941. doi: 10.1109/SURV.2013.070813.00214.

POPESCUL, D. and RADU, L. D. (2016) ‘Data Security in Smart Cities: Challenges and Solutions’, *Informatica Economica*, 20(1/2016), pp. 29–38. doi: 10.12948/issn14531305/20.1.2016.03.

Rhee, K., Jeon, W. and Won, D. (2012) ‘Security requirements of a mobile device management system’, *International Journal of Security and its Applications*.

Roser, H. R. and Max (2017) ‘Technology Adoption’, *World Bank*.

Roungas, B., Meijer, S. and Verbraeck, A. (2017) ‘A framework for simulation validation & verification method selection’, *SIMUL 2017: The Ninth*

International Conference on Advances in System Simulation, pp. 35–40.

Schütz, P. *et al.* (2013) ‘Malware proof on mobile phone exhibits based on GSM/GPRS traces’. Available at: https://opus.bibliothek.fh-aachen.de/opus4/frontdoor/index/index/docId/5574.

Silverio-Fernández, M., Renukappa, S. and Suresh, S. (2018) ‘What is a smart device? - a conceptualisation within the paradigm of the internet of things’, *Visualization in Engineering*. doi: 10.1186/s40327-018-0063-8.

Suhail, N. A. (2017) *Exploring Mobile Phone Usage at Higher Education: A Case Study of Kampala University, Uganda*, *International Journal of Computer Applications*.

Taylor, K. and Silver, L. (2019) *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally | Pew Research Center, Https://Www.Pewresearch.Org/Global/2019/02/05/Smartphone-Ownership-Is-Growing-Rapidly-Around-the-World-But-Not-Always-Equally/.*

Wei, J., Liu, L. C. and Koong, K. S. (2006) ‘An onion ring framework for developing and assessing mobile commerce security’, *International Journal of Mobile Communications*, 4(2), pp. 128–142. doi: 10.1504/IJMC.2006.008605.

Wei, L., Liu, Y. and Cheung, S. C. (2019) ‘PIVOT: Learning API-Device Correlations to Facilitate Android Compatibility Issue Detection’, in *Proceedings - International Conference on Software Engineering*. doi: 10.1109/ICSE.2019.00094.

Yan, Q. *et al.* (2016) ‘Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges’, *IEEE Communications Surveys and Tutorials*. doi: 10.1109/COMST.2015.2487361.