Asian Journal of Research in Computer Science

14(2): 33-46, 2022; Article no.AJRCOS.89366
ISSN: 2581-8260

Comparative Analysis and Development of Mobile Device Authentication Framework for Corporate Networks

Mboto Peter [a], Gilbert Gilibrays Ocen [a*], Godliver Owomugisha [a], Alunyu Andrew Egwar [a], Matovu Davis [a], Twaibu Semwogerere [a] and Rwahwire Samson [b]

[a] Department of Computer Engineering and Informatics, Faculty of Engineering, Busitema University, P.O.Box 236, Tororo, Uganda.
[b] Department of Polymer, Industrial and Textile Engineering, Faculty of Engineering, Busitema University, P.O.Box 236, Tororo, Uganda.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2022/v14i230335

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/89366

Original Research Article

Received 10 May 2022
Accepted 14 July 2022
Published 19 July 2022

ABSTRACT

Several systematic reviews on mobile device technologies have been undertaken mostly identifying mobile security threats and challenges to corporate organisations' sensitive private information. This paper surveyed the existing level of secure authentication achieved by various mobile device-related frameworks against their listed goals. The solutions and security level of the existing authentication approaches among these categories were compared and improved on the KANYI BYOND framework by introducing a Radius server with the 802.11 authentications supported feature that provides access control to wireless routers, access points, hotspots in EAP/WPA-Enterprise/WPA2-Enterprise modes as means to achieve multiple authentications to mobile device users in corporate networks. Testing and validation of the resulting framework were done with the help of a riverbed modeler and a Denial of Service attack was simulated on all mobile devices' nodes in the designed network. The results indicated that the resulting framework provides multiple authentications and is thought to overcome self-reassuring by mobile device users on the network.

**Corresponding author: E-mail: gocen@eng.busitema.ac.ug, gilbertocen@gmail.com;*

Keywords: Mobile device authentication; framework; DOS attacks; CVSS; simulation.

1. INTRODUCTION

In this current technologically dynamic world, mobile devices have been made to perform the role of personal computers. This increase in the role has been due to their processing power, large storage capacity and large memory and form part of most business corporate networks [1]. But, on the other hand, improved functionality, such as increased storage of different sensitive data, makes mobile devices more attractive to scammers and attackers of various forms [2]. Moreover, to our worry, Smartphones, tablets and personal digital assistants are increasingly performing complex tasks to replace the traditional option of computers and notebooks, which can digitally be investigated in case of damage [3].

Historically, Mobile phone users worldwide exceeded 4 billion for the first time by 1992, indicating that two-thirds of the world's population had mobile phones [4]. At the beginning of 2019, approximately 5 billion people around the globe were using smartphones [5]. Furthermore, with the current technological advancements in wireless telecommunications, the number is expected to grow from 25 to 50 billion connected devices by 2020 [6]. As of January 2021, Datareportal recorded a total of up to 5.22 billion unique mobile users (smartphones), making up 66.6% of the global population, with social media users increasing by more than 13 per cent over the past 12 months (Chaffey, 2021).

A study conducted by Androulidakis [7] revealed that mobile device users face more considerable security risks due to their self-reassuring sentimentality that such mobile devices are secure; a common challenge facing mobile device users in corporate networks, more so if they become less cautious in their security practices. Also, the ubiquitous connection, authentication and authorisation of mobile devices onto corporate networks in the continent means new electronic attacks and malicious software [8,9]. Moreover, without any proactive measures on authentication and authorisation, they are likely to cause a denial of service attack [10].

Application delivery channels such as the Apple App Store and Google Play stores have transformed mobile devices into application devices; downloading such applications come in with electronic attacks in the form of viruses [11]. As a result, corporate organisations consider adopting a Mobile Device Management (MDM) system to manage mobile devices' applications, data processing and storage [12].

In Uganda, the government, through National Information Technology Authority-Uganda (NITA-U), encourages corporate organisations to come up with Information Security Management Systems (ISMS) and also create information security programs or controls that are fully compliant with the requirements of US ISO/IEC 27001:2005 [13]. A clear insight into mobile device authentication challenges in the corporate network requires organisations to implement regulations and frameworks as security design measures to overcome.

1.1 Related Work

To address continuing mobile device authentication-related challenges and issues in corporate Information Technology enterprises, various security professionals have proposed different frameworks and solutions to alleviate the other problems. The mobile device authentication framework is a systematic model with additional system modules to related processes to aid and resolve each component issue. Additionally, an SMS-based mechanism is implemented as a backup tool for recovering the password and a possible means of synchronisation. Current Mobile device authentication frameworks were reviewed based on their existing literature and against the listed goals they achieved.

Mobile device security is an area where a lot of research has been conducted to develop frameworks and other solutions. For example, to prevent mobile device security-related threats and challenges, Gimenez Ocano et al. [14] suggested that frameworks must achieve several goals including, space isolation separating the corporate's space from the employee's space so that different security policies can be enforced; corporate data protection by employing encryption and rejecting unauthorized access; security policy enforcement, where the mobile device complies with the corporation's security policies; true isolation, where the corporate's data is not located on the mobile user device; non-intrusive, meaning that any software installed in the mobile device must not need any special privileges that might allow it to monitor the behaviour of the user on their device; and non-resource-intensive, as mobile devices are resource-constrained and do not have any spare resources for demanding applications. Four frameworks were reviewed because they aim to protect sensitive resources and applications in a mobile device-based corporate organisation.

Wei et al. [15] proposed a five-layer 'onion ring' framework to analyse mobile commerce security requirements and improve system security performance. Its primary aim was to assist m-commerce system experts in better analysing, (re) designing and implementing frameworks that increase security performance for specific mobile environments, thus estimating all aspects of security performance in mobile commerce. It consists of designing a context-aware mobile system (GSM part of the mobile phone) that supports users with location-specific information servers and applications. By doing so, the system uses the non-intrusive Push concept to deliver information to mobile users aided by cell-broadcast technology in either a spider diagram or a decision solution matrix. Furthermore, it demonstrates how the security level can be objectively measured and evaluated and the technical discussions on the framework's architecture.

Holistic Mobile Security Framework proposed by Obodoeze et al. [16] aims at combating mobile security challenges affecting the mobile telecommunication platforms such as hackers, the threats of malicious programs and the rampant theft of portable equipment that was identified to constitute the most significant security challenge. Building on the GSM security architecture, Fidelis discovered that networks were built but lacked the necessary features to curtail most mobile security insurgencies. And so, he identified the myriads of mobile security (physical, data and operational) challenges affecting the telecommunication industry and holistically suggested measures and guidelines mitigate and tackle them.

The application Security framework proposed by Chakraborti et al. [17] centres its discussion on the approach at the Mobile application layer during application design and coding by developers and thus Mobile Application Security standpoint. In Mobile App development, the focus was centred on four broad areas, i.e., data protection, intellectual property protection, secure authentication and code vulnerability. It provided a systemic approach to the developer, possible to mitigate these risks to a large extent and minimize them.

KANYI BYOD Framework was proposed by Ndeng'ere [18] after modifying the BSF Framework by eliminating the use of Mobile Virtual Machine (MVM) that he thought would instead be achieved by the Mobile device management (MDM) agent installed in mobile devices. Ndeng'ere's efforts were put on the physical implementation of BYOD to tackle threats and security challenges associated with Mobile devices' access to the network in higher institutions of learning that needed a burning need for unified endpoint management.

Much as all frameworks aim to protect corporate data, organisational security needs dictate the best model based on the solutions offered. The choice about which framework to choose and how to apply it is left to the implementing organisation. According to ITU [19], organisation heads struggle to implement effective policies to countermeasure possible threats associated with device mobility. Thus, no proper security control is offered just by policy implementation; preferably, a mobile device authentication framework is required to complete the authentication of mobile devices in a corporate network.

2. RESEARCH METHODOLOGY

Design Science Methodology was adopted to guide the development of the proposed framework. According to Gregor & Hevner [20], design Science Research is the research methodology used to create and evaluate artefacts for information models (abstractions, frameworks, conceptual systems) intended to solve an identified uncertain organisational problem using behavioural and design science paradigms. The researcher adopted this approach because of the creative knowledge within interactive cycles used to design solutions to identified field problems.

In Understanding and communicating the design science research process, three (3) distinct but interrelated design science research cycles were adopted, each with underlining activities. First was the Relevance Cycle, which aimed to identify organisational requirements/needs and test the artefacts within the environment. Next is the Rigor Cycle, which seeks to provide past knowledge to the research project to ensure its

Table 1. Comparative matrix of mobile authentication frameworks and their solutions in key corporate environments

Security frameworks	Publication year	Corporate Data protection	Non-intrusive	Space isolation	True isolation	Security policies	Multiple authentication	Non-resource-intensive	Gaps identified
Five-layer 'onion nng Framework me	Wel J. et al. [15]	✓	✓	×	✓	×	×	✓	Users awareness No multiple authentication
Holistic Mobile Security Framework	Fidelis, et al. (2013)	✓	×	×	×	✓	×	×	Data is stored on device Users' awareness
Application Security framework	S. Chakraborti, et al. [17]	✓	✓	×	×	✓	×	✓	Data is a on device Developers intend No multiple authentication
KANYI BYOD framework	Ndeng'ere [18]	✓	✓	✓	✓	✓	×	✓	No multiple authentication
MDA framework	Mboto P. (2020)	✓	✓	✓	✓	×	✓	✓	High device rejection rate

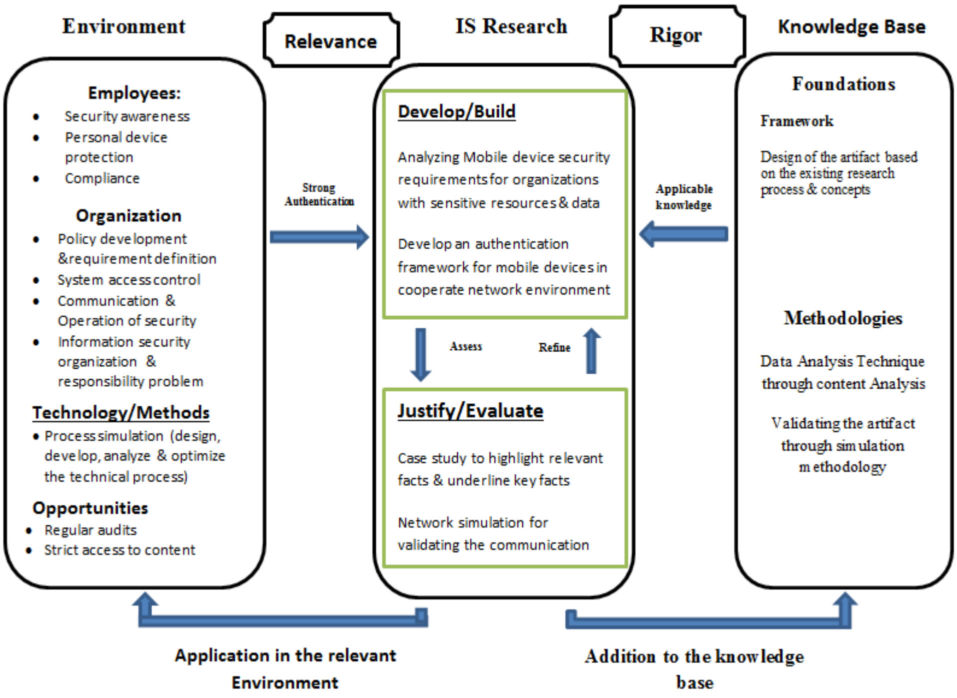
Environment
Relevance
IS Research
Rigor
Knowledge Base
Employees:
Security awareness
Personal device protection
Compliance
Organization
Policy development &requirement definition
System access control
Communication & Operation of security
Information security organization & responsibility problem
Technology/Methods
Process simulation (design, develop, analyze & optimize the technical process)
Opportunities
Regular audits
Strict access to content
Strong Authentication
Develop/Build
Analyzing Mobile device security requirements for organizations with sensitive resources & data
Develop an authentication framework for mobile devices in cooperate network environment
Assess
Refine
Justify/Evaluate
Case study to highlight relevant facts & underline key facts
Network simulation for validating the communication
Applicable knowledge
Foundations
Framework
Design of the artifact based on the existing research process & concepts
Methodologies
Data Analysis Technique through content Analysis
Validating the artifact through simulation methodology
Application in the relevant Environment
Addition to the knowledge base

Fig. 1. Information System (IS) research framework (Adapted from Hevner et al., [21])

innovation. And lastly, the central Design Cycle iterates between the core activities of building and evaluating the design artefacts and processes of the research. Artefacts must be built and evaluated thoroughly before releasing them to the relevant cycles and before the knowledge contribution is output into the rigour cycle.

2.1 Data Collection

This study adopted an extensive literature search using the World Cat search engine with key search terms relating to Mobile Device Security. First, the search was filtered for peer-reviewed journal articles and the returned results were assessed concerning their inclusion in this study following procedures employed by Chambers [22]. The researcher adopted the inductive approach used in Katherine Allen, Christine Kaestle, and Abbie Goldberg's study (2011) to collect data, analyze patterns in the data, and then theorize from the data. The researcher used this approach to analyze the written narratives of participants from 10 purposively selected corporate organizations in which participants described how mobile devices are authenticated on their network, the resulting security threats/challenges, and what they think can be done to mitigate them. Whereas the researcher targeted 63 corporate organizations in the Eastern Region-Uganda, only 10 met the criteria of inclusion. Establishing inclusion and exclusion criteria for study participants is a standard, required practice when designing high-quality research protocols (Patino & Ferreira, 2018). Out of the 63, only 13 organizations had corporate network infrastructure. Out of these 13, three (03) suggested that they cannot give such information to anyone who is not their IT Officer or management. They even suggested that even other staff of the organization were not allowed access to such information [23-28].

Therefore, being left with only 10 corporate organizations, the most appropriate sampling size was determined using a census enumeration, which is recommended for studies with very few participants (Baffour, King and Valente, 2013). The CVI for the research instrument used was 0.873. As per Kovacic's, (2018) view, a CVI of above 0.7 means the instrument is valid and therefore collected valid data.

2.2 Limitations

There was an unwillingness to disclose sensitive information more so with banks for fear of being pinned out. However, this was solved by making clarifications and assurance that the information was purely for academic purposes but no other interests. A time factor was a challenge since the majority claimed of having a busy schedule and datelines to meet. However, the researcher engaged research assistants who were trained to conduct interviews and also hand in, deliver and pick the questionnaires whenever completed within stipulated time. These limitations do not imply that the study did not meet the scientific demands of the objective. Rather, they helped the researcher to clearly explain and bring to attention insights addressed by the research problem of this study.

3. RESULTS AND DISCUSSION

The results were discussed based on each of the following study objectives:

a) To identify emerging security authentication challenges in a mobile device corporate network.
b) To determine matrices for existing mobile device authentication frameworks.
c) To develop a mobile device authentication framework to be adopted by corporate networks.
d) To test and validate the framework.

3.1 Emerging Authentication Challenges in a Mobile Device Corporate Environment and their Mitigation Strategy

The researcher used a questionnaire tool to discover various mobile device authentication challenges and mitigation strategies that corporate organisations had to tackle. The discussion was, however, centred on the following aspects:

i) Negative impacts of mobile device connection on corporate networks

The study finding revealed that mobile devices had a negative impact on the operation of corporate networks, illustrated by the graph in Fig. 2.

From Fig. 2, 90% of the respondents agreed that allowing mobile devices connected to a corporate network exposes corporate networks to security threats. Also, 90% agreed that allowing mobile devices connected to a corporate network exposes corporate networks to bandwidth constraints and; 10% indicated that it creates chances for both device and data loss. Whereas, 20% of the respondents indicated that data ownership was the problem associated with Mobile device connection to corporate networks.

Based on the responses obtained from all sampled organisations, it is notable that bandwidth constraint is the greatest worry of having mobile devices connected to their corporate network. This is because corporate organisations incur extra costs to provide bandwidth to the number of users on the network. Secondly, the view that mobile devices connected to any corporate network have the associated security impact of spreading malware/ viruses was seriously reported by 9 corporate organisations, more so in all academic institutions. Lastly, the issue of data loss to data owners remains vital for corporate organisations, especially banks; they value their sensitive information more than anything else. Once accessed by staff-owned devices, there is a possibility of data leakages that could cost the organisation. This was another challenge that the researcher ought to be addressed with the Mobile device authentication framework.

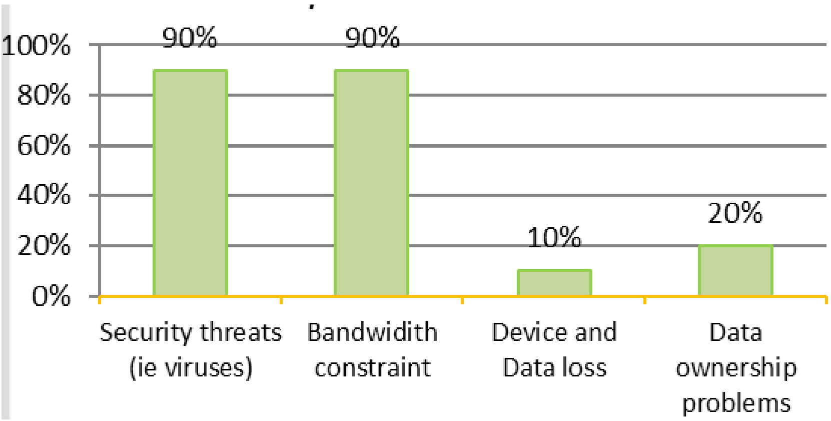

Fig. 2. Negative Impacts on mobile device connection to corporate networks

ii) Preventive Measures available to address the negative impacts brought by mobile device connection in corporate networks

The researchers aimed to determine whether the selected corporate organisations had measurer(s) in place to address security challenges brought about by mobile device connections on corporate networks. It was revealed that all the respondents acknowledged (YES) – that they have pre-existing measurer(s) to tackle security vulnerability challenges in their corporate organisation. The most reported was device access using WiFi authentication and antivirus scanners. However, these respondents further suggested that the available measures were inadequate to fight against the evolving mobile security. The proposed framework would therefore be of much help to corporate organisations upon implementation.

iii) Security attacks resulting from mobile device connections in corporate networks

The researchers intended to discover the actual attacks on their corporate systems due to mobile devices connected to their network. Therefore, all respondent views were summarized as illustrated in Fig. 3.

Respondents further highlighted that the spread of viruses, worms, Trojans and other malware to other devices; was the major security attack affecting most sampled corporate organisations. Attempts to hack into corporate servers were also another notable attack. In addition, DOS attacks and other malware were also reported in some corporate organisations. The attacks were attributed to the insecure use of mobile devices connected to corporate networks and weak security measures to tackle evolving threats.

3.2 Determine Matrices for Existing Mobile Device Security Frameworks

The reviewing of existing literature on Mobile device security frameworks and their solutions was done. Gimenez Ocano et al. [14] suggested that framework development must be achieved based on five primary goals. The results of the review were captured in the matrix Table 1. Having reviewed all the frameworks, the MDA framework was designed and developed to achieve the following specific goals in a corporate environment:

- Multifactor authentication attributes offered by the Radius server to the corporate network to achieve authentication, authorisation and accounting services.
- Solved the self-reassuring feeling concerning mobile devices by Device owners
- Solve corporate compliance problems with internal policies and procedures (management and internal controls).
- Mitigate malware invasion via installed applications: viruses, worms, Trojans and other harmful computer programs hackers use to wreak destruction.
- Deal with devices congestion problems in a corporate network causing Dos Attacks.
- Perform and schedule controlled mobile device OS and antivirus updates.
- Offer controlled Authentic access to internal systems and servers.

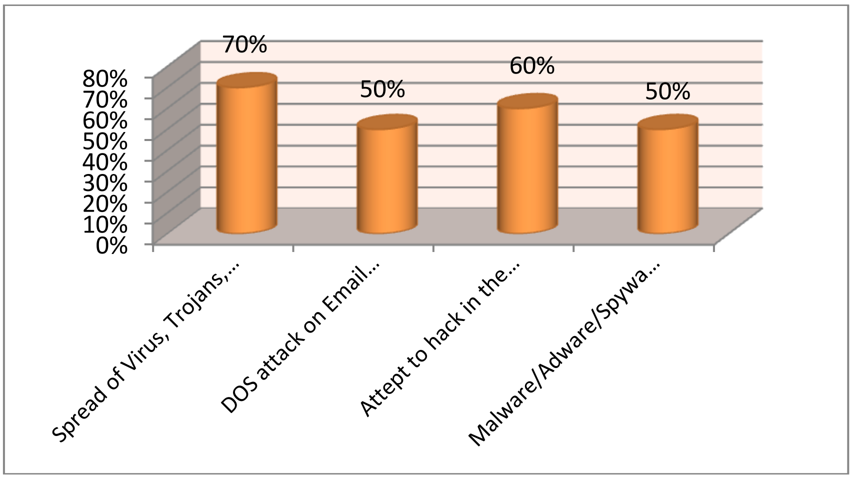

Fig. 3. Security attacks resulting from mobile device connections in corporate networks

3.3 Development of a Mobile Device Authentication Framework for Corporate Networks

The proposed framework was designed into a network topology that fits any corporate network design model. The designed network topology was evaluated using a riverbed modeler for security vulnerability, as shown in Fig. 4.

The network topology design model used to authenticate mobile devices in the corporate network environment shown in Fig. 5 will be tested using simulation methodology for security vulnerability. The topology comprises the following entities:

- **Terminal devices:** mobile devices such as a tablet, smartphones and laptops and applications running on the mobile devices.
- **The network access devices:** Access point, access switch, Radius server, MDM server and Mobile device Firewall are part of the connection network.
- **The corporate network access:** All corporate organisational internal network devices found in the server room such as switches, routers, firewalls, servers and proxy servers. Such internal network devices must be protected from threats brought about by mobile devices.
- **External network access:** A zone comprising of other security devices such as a corporate Firewall, MDM gateway server and Proxy server that ensure safe entry and exit of traffic from the corporate network and the internet, respectively. The designed network topology is further broken down and arranged in sectional domains:

Terminal devices domain (D1): This domain tackles the mobile operating system, device type and installed applications. The scanning of the terminal devices is done to determine their vulnerabilities. This is done by the MDM agent installed by the MDM server on all mobile devices.

Access network domain (D2): This domain will tackle secure access of mobile devices to the corporate network. Secure access is guaranteed by the MDM Server, Radius server and Mobile device Firewall.

Corporate network domain (D3): This section domain will tackle corporate internal network.

Devices comprising servers, core switches, switches and a router are also called the server room.

External network access domain (D4): this section domain will tackle the corporate network's security from mobile devices' internet activities. The domain comprises the corporate firewall, MDM gateway server and proxy server.

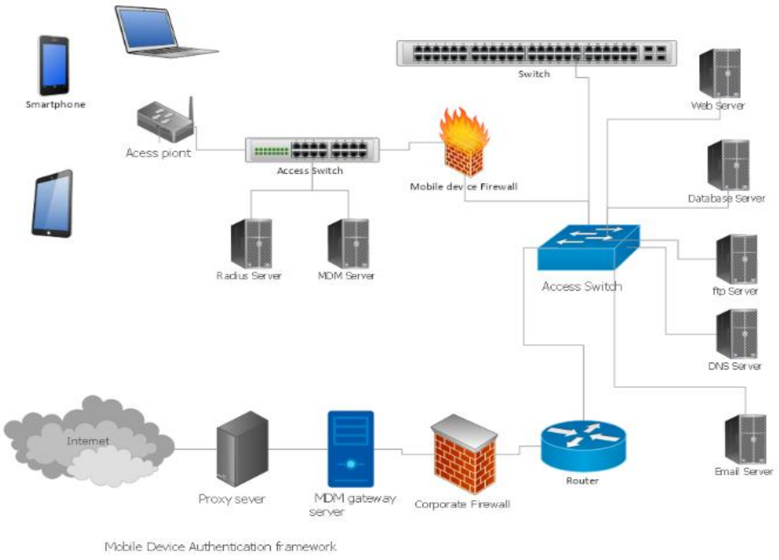

Fig. 4. Designed network topology of the proposed framework

3.4 Quantifying Security Vulnerability Associated with MDA Framework

According to (Lee et al., 2018) there are several methods to calculate the quantification of security vulnerability. However, the security threats evaluation performance for the MDA framework is done based on CVSS (Common Vulnerability Scoring System) Version 3.1. It attempts to establish a measure of how much concern vulnerability warrants, compared to other vulnerabilities so that efforts can be prioritized. The CVSS scores vulnerabilities on a scale of 0 – 10 (with 10 being the worst score relative to most severe vulnerabilities) to capture the principal technical characteristics of software, hardware and firmware vulnerabilities within a corporate network. Assuming the attacker had advanced knowledge of the weaknesses of the corporate target system, including general configuration and default defence mechanisms such as built-in firewalls, rate limits and traffic policing; it is possible to calculate the vulnerable component based on the exploitability matrices formula given below:

Impact Sub-Score (ISS) = 1 – [(1 – confidentiality) x (1 – integrity) x (1 – Availability)
Impact= 6.42 x ISS (if scope is unchanged)

Impact= 7.52 x (ISS – 0.029) – 3.25 x (ISS – 0.02) ^15 (if scope is changed)

Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges requirement x User interaction

If the scope is changed

Base Score = Roundup 1dp (Minimum [(Impact + Exploitability), 10])

If scope is unchanged

Base score = Roundup 1dp (Minimum [1.08 × (Impact + Exploitability), 10])

3.5 Framework Testing and Validation

The framework was designed in a riverbed modeler (a simulation tool) and an attacker node (mobile node) was introduced. The attacker node launched DOS (ping floods) attack on the corporate network, as shown in the Figs. 5 and 6.

3.5.1 The attacks and preventive scenarios

Simulation for the three scenarios was done and the screenshots of the resulting graphs of the simulation are shown Fig. 7.

When there is no attack on the corporate network, the response rate of the database application (query) was low as compared to when a mobile attacker was introduced. The high response rate indicates that the attacker orchestrated the attack prompting the server to send unsolicited responses to the victim network, which chokes down on the high volume of inbound packets, thus slowing down the server and eventually collapsing it. The database application response rate was reduced to normal when preventive measures were implemented due to limited traffic from all connected mobile devices. Limiting the Response Rate intends to prevent the abuse of the DNS servers for orchestrating an amplification attack.

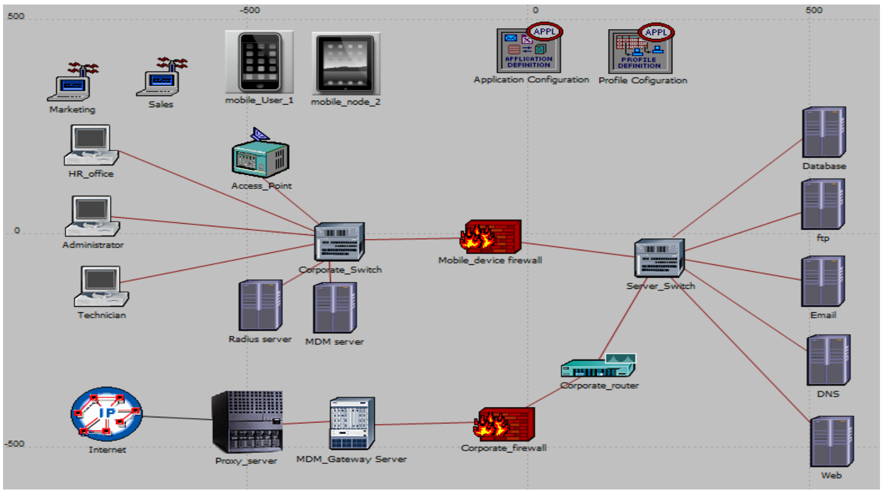

Fig. 5. Screen shot of the proposed network model design in riverbed Simulator

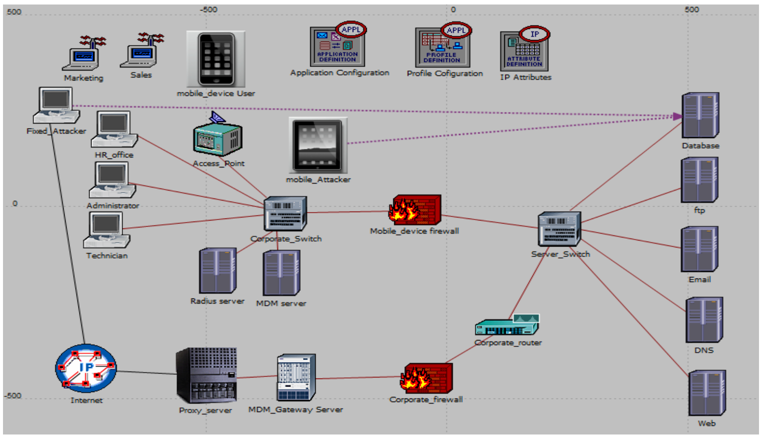

Fig. 6. Screenshot of launching a ping flood attack on a corporate server

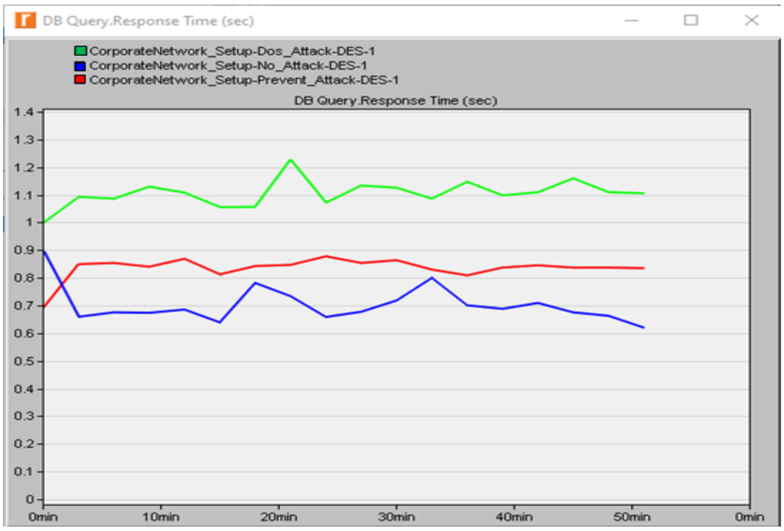

Fig. 7. Screenshot of simulation results of the three scenarios in relation to the target server's database application (query)

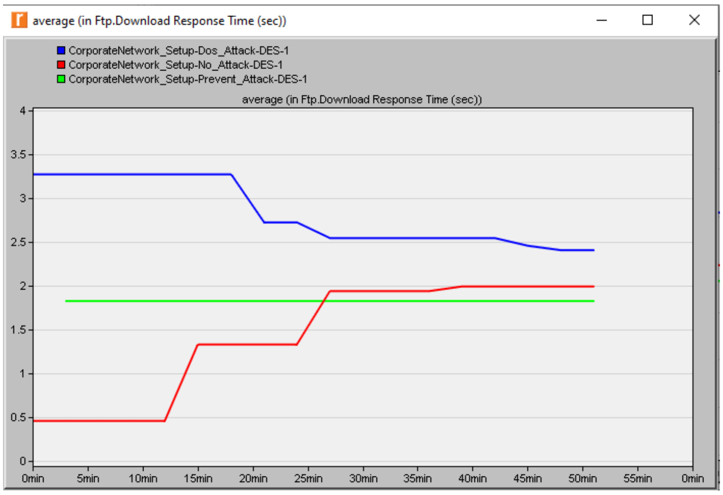

Fig. 8. Screenshot of simulation results of the three scenarios in relation to the FTP download application of the target server

Similarly, in the absence of an attacker on the corporate network, the average download response time increased exponentially to maximum rates. However, the download response time dropped drastically when a mobile device attacker was introduced. However, with preventive measures in place, the average download response time was maintained at constant rates. This is because preventive measures limit and regulate the no of authenticated devices on the corporate network.

On the same note, it was discovered that the CPU utilisation of the corporate server recorded during the moment the mobile attacker was introduced was much higher than the moment of no attack. However, when preventive measures were put in place, the level of CPU utilisation returned to normal levels, having limited the number of authenticated mobile devices as shown Fig. 9.

With no attacker on the corporate network, the response rate of the HTTP application from the target server to the request made by the mobile user is less than when there is an attacker scenario. Furthermore, the HTTP application response rate reduces to normal rates when preventive measures are implemented based on the number of mobile devices in connection.

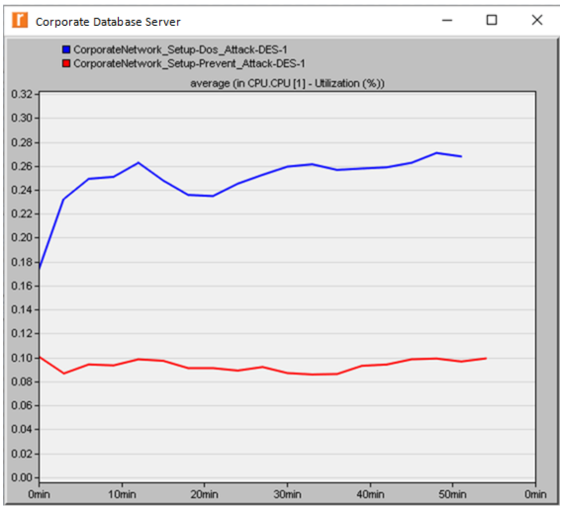

Fig. 9. Screenshot of simulation results of the three scenarios in relation to the CPU utilisation of the target server

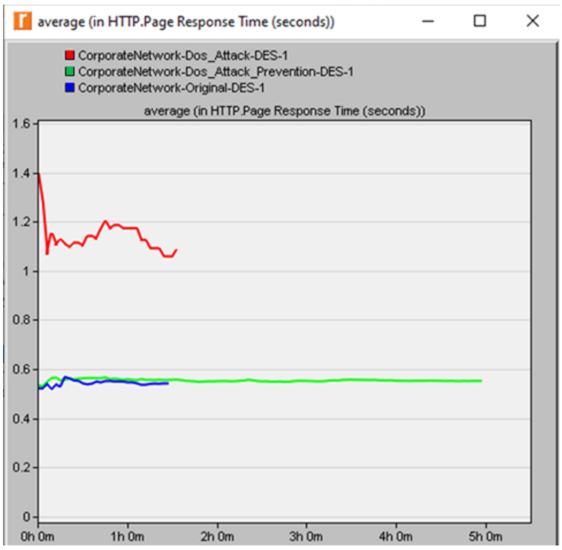

Fig. 10. Screenshot of simulation results of the three scenarios in relation to the target server's HTTP (web service) application

The simulation was done based on the three scenarios. Various aspects of the performance of the network and its components based on the 3 case scenarios were measured and the results were as follows:

The database server response rate from genuine mobile device users for the first case scenario was captured. The simulation of the response rate between the server and mobile users for the 3 case scenarios was captured. It was noted that database response rates went high when the DOS attacker was introduced. This was expected because the network became congested by the ping flood packets from the mobile attacker node. When preventive measures were introduced (managed through the Radius server and MDM firewall) to tackle the DOS attack, the response rates returned to the expected levels.

The download response rates of applications related to mobile users for the second case scenario were measured and it was noted that download response rates were high when the DOS attacker was introduced. This was expected because the network became congested by the ping flood packets from the mobile attacker node. However, the download response rates returned to the expected levels when preventive measures were introduced to tackle the DOS attack.

The web server response rates for mobile users for the last case scenario and the simulation results were measured. It was noted that web service response rates went high when the DOS attacker was introduced. This was expected because the network became congested by the ping flood packets from the mobile attacker node. However, when preventive measures were introduced to tackle the DOS attack, the response rates returned to the expected levels.

The CPU performance of the corporate server was analysed and the results of the utilisation analyses simulation were captured. It was noted that CPU utilisation in percentage per second went high when the DOS attacker was introduced. This was expected because the server was engaged by the ping flood packets from the mobile attacker node. However, when preventive measures were introduced (Radius server and MDM firewall) to tackle the DOS attack, the server CPU utilisation rates went down to the expected levels.

4. CONCLUSIONS AND RECOMMENDATIONS

The main goal of this study was to assert that mobile device security attacks and authentication challenges in various corporate organisations were in existence. It was concluded that despite mobile device security risks and threats, the majority of corporate staff carried mobile devices to their workplaces. The staff freely connected to their corporate organizational networks without strict measures to address mobile device-related challenges and attacks experienced as a result. This means that the corporate organizations were prone to threats and attacks. On comparing solutions advanced by the existing frameworks with the MDA framework, the researcher concluded that they fell short of achieving multifactor authentication. As a result, they left loopholes that could lead to the spread of malware to other corporate devices, which creates open doors for attackers. MDA framework was developed with its detailed functioning and components integration. The framework components can be integrated into the corporate network to achieve its intended purpose. The developed MDA framework contains multifactor authentication modules (using a Radius Server) that are necessary for attaining complete mobile device security for corporate networks.

Having performed simulation on the MDA framework, the researcher concludes that both internal and external security threats brought by mobile devices to corporate networks are detected and blocked. Therefore, the new MDA framework completely shields the corporate networks from attacks. All in all, the framework is effective in addressing vast corporate network mobile security-related threats if adopted and correctly implemented by the corporate organizations.

This study, therefore, recommends that the deployment of advanced device authentication frameworks within corporate networks. These advanced device authentication frameworks must use a Radius protocol to achieve multifactor authentication. The Radius protocol can control any part of RADIUS request processing, including tracking authentication status, authentication, verifying, and adding RADIUS attributes in requests and responses. Corporate network heads need to have plans concerning mobile device secure access, usage, and transfer of data to and from any insecure devices in any organizational network. Therefore, the sooner the corporate organizations embrace the proposed framework as a mobile device authentication measure, the better they deter themselves against evolving mobile device authentication threats.

Corporate organizations with more sensitive data and applications adopt the proposed framework not only to rip its full benefit but rather to keep themselves safe from mobile device-related threats and other authentication-related challenges. Further research should focus on the forensic capture and analysis of mobile device corporate server login attempt logs.

5. SUMMARY

The study attempts to address multiple gaps identified in the present frameworks and in doing so makes important contributions to academia. First, the study extends the limited research on the understanding of Mobile device authentication. This study is among the first to consider multiple authentications as an important antecedent of mobile device network security. It also explains the mechanism through which multiple authentications work.

Furthermore, the study represents an addition to the already existing practical models in the field of Mobile Authentication. Though there are already many other frameworks, no previous study to the best of the author's knowledge and through search in peer-reviewed databases embeds multiple authentications. This framework comes with an added advantage in terms of its ability to conduct Multiple Authentication, an area which other frameworks have not catered. This is done by integrating other prior models and adding more modules that did not exist in the other models. This, therefore, ensures that maximum security is guaranteed. This is also the first of the attempts in the country to establish such a framework that is very useful to the corporate world.

Also, this study contributes to the streamlining of Mobile device authentication processes, which can lead to decreased risks arising from an insecure mobile device network environment. The study contributes to knowledge by fronting the new MDA framework. The framework, unlike all others, offers a Multiple Authentication module that helps identify potential security-related threats and challenges. Once these threats are identified, they are blocked and denied access to the network systems. This is an important addition in the field of cyber security where emerging issues include security and protection of networks used in the corporate world.

Also, the study contributes to the knowledge of the IT professionals and forensic experts who have vested interests in network security and are either practicing in different corporate organizations or planning to start practice. The framework can also be studied in schools and can be put into real-life practice. This goes forward to widen the understanding of Mobile security and its related challenges.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Lutui PR. Digital forensic process model for mobile business devices: smart technologies; 2015. Available http://aut.researchgateway.ac.nz/bitstream/handle/10292/9242/LutuiPR.pdf.
2. Farrell G. Preventing phone theft and robbery: the need for government action and international coordination. Crime Sci. 2015;4(1).
   DOI: 10.1186/s40163-014-0015-0.
3. Omori S. Information security report. 2017;2011:1-32.
4. Breitinger F, Nickel C. User survey on phone security and usage. Lecture Notes in Informatics (LNI). Proceedings of the – series of the Gesellschaft fur informatik (GI); 2010.
5. Taylor K, Silver L 2019. Smartphone ownership is growing rapidly around the world, but not always equally | Pew Research Center. In. Available:https://www.Pewresearch.Org/Global/2019/02/05/Smartphone-Ownership-Is-Growing-Rapidly-Around-the-World-But-Not-Always-Equally/.
6. Silverio-Fernández M, Renukappa S, Suresh S. What is a smart device? - a conceptualisation within the paradigm of the internet of things. Vis Eng. 2018;6(1).
   DOI: 10.1186/s40327-018-0063-8.
7. Androulidakis II Mobile Phone Security and Forensics: A Practical Approach. Mobile phone security and forensics: A practical approach. 2nd ed; 2016.
   DOI: 10.1007/978-3-319-29742-2.

8. Aker JC, Collier P, Vicente PC. Is information power? Using mobile phones and free newspapers during an election in Mozambique. Rev Econ Stat. 2017;99(2):185-200.
DOI: 10.1162/REST_a_00611.
9. Jack W, Ray A, Suri T. Transaction networks: evidence from mobile money in Kenya. Am Econ Rev. 2013;103(3):356-61.
DOI: 10.1257/aer.103.3.356.
10. Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues and challenges. IEEE Commun Surv Tutorials. 2016;18(1):602-22.
DOI: 10.1109/COMST.2015.2487361.
11. Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT et al. A survey of mobile phone sensing. IEEE Commun Mag. 2010;48(9):140-50.
DOI: 10.1109/MCOM.2010.5560598.
12. Rhee K, Jeon W, Won D. Security requirements of a mobile device management system. Int J Sec Appl; 2012.
13. NITA U. National information security policy (NITA-U). J Inf Sec; 2014.
14. Gimenez Ocano S, Ramamurthy B, Wang Y, Ocano G. Digital Commons@University of Nebraska-Lincoln Remote Mobile Screen (RMS): an approach for secure BYOD environments Remote Mobile Screen (RMS): an approach for secure BYOD environments; 2015.
DOI: 10.1109/ICCNC.2015.7069314.
15. Wei J, Liu LC, Koong KS. An onion ring framework for developing and assessing mobile commerce security. Int J Mob Commun. 2006;4(2):128-42.
DOI: 10.1504/IJMC.2006.008605.
16. Obodoeze FC, Okoye FAN. Asogwa SC, Ozioko FE. A Holistic Mobile Security Framework for Nigeria. 2013;3:5-11.
17. Chakraborti S, Acharjya DP, Sanyal S. Application Security framework for Mobile App Development in Enterprise setup; 2015.
Available:http://arxiv.org/abs/1503.05992
18. Ndeng'ere DK. A BYOD framework for secure use of mobile devices in; 2017.
19. ITU. Understanding cybercrime: phenomena, challenges and legal response. In: Proceedings of the annual Hawaii international conference on system sciences; 2014.
20. Gregor S, Hevner AR. Positioning and presenting design science research for maximum impact. MIS Q Manag Inf Syst. 2013;37(2):337-55.
DOI: 10.25300/MISQ/2013/37.2.01.
21. Hevner AR, March ST, Park J, Ram S. Design science in information systems research. MIS Q Manag Inf Syst. 2004;28(1).
DOI: 10.2307/25148625.
22. Chambers EA. An Introduction to meta-analysis with articles from the Journal of Educational Research (1992-2002). J Educ Res. 2004;98(1):35-45.
DOI: 10.3200/JOER.98.1.35-45.
23. Davis M, Gilbert M, Simon K, Stephen M, Gilibrays Ocen G. State of cyber security: the Ugandan perspective. Int J Sci Eng Res; 2019.
24. Jafari N, Alsadoon A, Withana CP, Beg A, Elchouemi A. Designing a comprehensive security framework for smartphones and mobile devices. Am J Eng Appl Sci. 2016;9(3):724-34.
DOI: 10.3844/ajeassp.2016.724.734.
25. Jeffrey PJH, Leong CC, Huat CG, Leng LS. Challenges in mobile security; 2016.
26. Majdi EB. Evaluation of mobile device management tools and analysing integration models for mobility enterprise; 2013.
Available:http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-74017.
27. Marler W. Mobile phones and inequality: findings, trends and future directions. New Media Soc. 2018;20(9):3498-520.
DOI: 10.1177/1461444818765154.
28. Matovu D, Gilbert MB, Authority of Kenya, C, Karume Simon K, Gilibrays Ocen G. The Internet of Things: applications and security metrics with the Ugandan perspective. Int J Adv Res; 2019.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/89366