Original Research Article

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

Abstract

Several systematic reviews on mobile device technologies have been undertaken mostly identifying mobile security threats and challenges to corporate organizations' sensitive private information. This paper surveyed the existing level of secure authentication achieved by various mobile device related frameworks against their listed goals. We compared the solutions and security level of the existing authentication approaches among these categories and improved on KANYI BYOND framework by introducing a Radius server with the 802.11 authentication supported feature that provide 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 was done with the help of riverbed modeler and 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 thought to overcome a self-reassuring by mobile device users on the network.

Keywords: Mobile device authentication, Framework, Dos Attacks, CVSS, Simulation.

1.0 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 due to their processing power, large storage capacity, and large memory, and form part of most

business corporate networks (Lutui, 2015). 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 (Farrell, 2015). 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 (Omori, 2017).

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 (Breitinger & Nickel, 2010). At the beginning of 2019, approximately 5 billion people around the globe were using smartphones (Taylor & Silver, 2019). Furthermore, with the current technological advancements in wireless telecommunications, we expect to have their number grow from 25 to 50 billion connected devices by 2020 (Silverio-Fernández et al., 2018). As of January 2021, Datareportal recorded a total of up to 5.22 billion unique mobile users (smartphone), making up 66.6% of the global population, with social media users increasing by more than 13 percent over the past 12 months (Chaffey, 2021).

A study conducted by Androulidakis (2016) 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 authorization of mobile devices onto corporate networks in the continent means new electronic attacks and malicious software (Aker et al., 2017, Jack et al., 2013). Moreover, without any proactive measures on authenticated and authorized, they are likely to cause a denial of service attack (Yan et al., 2016).

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 (Lane et al., 2010). As a result, corporate organizations consider adopting a Mobile Device Management (MDM) system to manage mobile devices' applications, data processing, and storage (Rhee et al., 2012).

In Uganda, the government, through National Information Technology Authority-Uganda (NITA-U), encourages corporate organizations 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 (NITA-U, 2014). A clear insight into mobile device authentication challenges in the corporate network requires organizations to implement regulations and frameworks as security design measures to overcome.

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 synchronization. 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. (2015) suggested that frameworks must achieve several goals including, space isolation separates 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 organization.

Wei et al. (2006) proposed a five-layer 'onion ring' framework to analyze mobile commerce security requirements and improve system security performance. Its primary aim was to assist m-commerce system experts in better analyzing, (re)design, 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. (2013) aiming 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. (2015b) 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 centered 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 proposed by NDENG'ERE (2017) 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'eres' 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

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 ring' framework	Wei J., et al. (2006)	✓	✓	X	✓	X	X	✓	Users' awareness No multiple authentication
Holistic Mobile Security Framework	Fidelis, et al. (2013)	✓	X	X	X	✓	X	X	Data is stored on device Users' awareness
Application Security framework	S. Chakraborti, et al. (2015)	✓	✓	X	X	✓	X	✓	Data is stored on device Developers intend No multiple authentication
KANYI BYOD framework	Ndeng'ere (2017)	✓	✓	✓	✓	✓	X	✓	No multiple authentication
MDA framework	Mboto P. (2020)	✓	✓	✓	✓	X	✓	✓	High device rejection rate

Much as all frameworks aim to protect corporate data, organizational 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 organization. According to ITU (2014), organization 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 authentication of mobile devices in a corporate network.

2. Methods and Materials

Design Science Methodology was adopted to guide the development of the proposed framework. According to Gregor & Hevner (2013), design Science Research is the research methodology used to create and evaluate artifacts for information models (abstractions, frameworks, conceptual systems) intended to solve an identified uncertain organizational problem using behavioral 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.

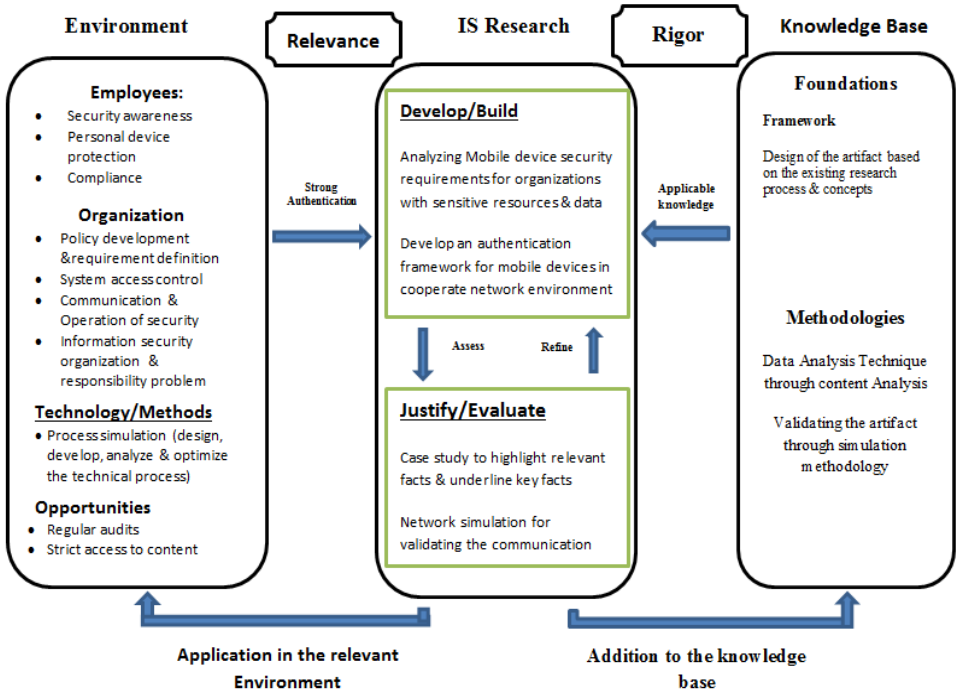


Figure 1. IS research framework. Adapted from Hevner et al. (2004)

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 that aimed to identify organizational requirements/needs and test the artifacts within the environment. Next is the Rigor Cycle that seeks to provide past knowledge to the research project to ensure its innovation. And lastly, the central Design Cycle that iterates between the core activities of building and evaluating the design artifacts and processes of the research. Artifacts must be built and evaluated thoroughly before releasing them to the relevant cycles and before the knowledge contribution is output into the rigor cycle.

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 (2004). Secondly, questionnaire methodology was adapted to target corporate IT administrators to establish the authentication challenges posed by mobile devices in corporate networks. A purposeful sampling technique was used to develop a sample size to choose corporate organization key internal systems. As a result, the researcher attained an excellent turnout of respondents from all the ten purposively sampled corporate organizations, indicated by a response rate of 100%.

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

A. 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 organizations had to tackle them. The discussion was, however, centered 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 below:

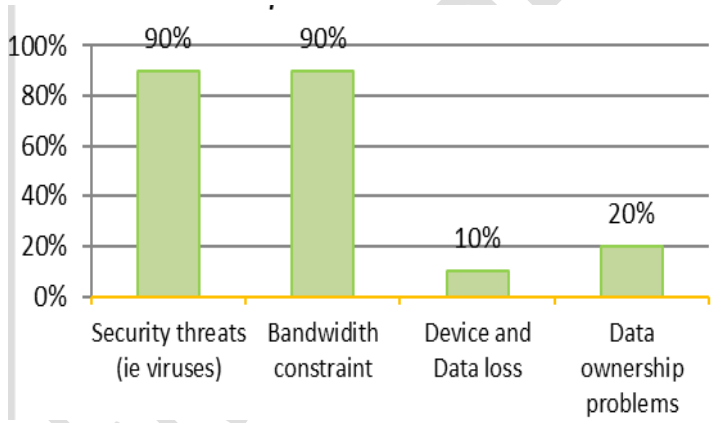


Figure 2: Negative Impacts Mobile device connection to corporate networks

The majority of respondents 90% both agreed that allowing mobile devices connected to a corporate network causes bandwidth constraints and exposes corporate networks to security threats; 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 organizations, it is notable that bandwidth constraint is the greatest worry of having mobile devices connected to their

corporate network. This is because corporate organizations 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 has the associated security impact of spreading malware/ viruses that was seriously reported by 9 corporate organizations, more so in all academic institutions. Lastly, the issue of data loss to data owners remains vital for corporate organizations, 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 organization. This was another challenge that the researcher ought to be addressed by the Mobile device authentication framework

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

The researchers aimed to determine whether the selected corporate organizations had measurer(s) in place to address security challenges brought about by mobile device connection on corporate networks. It was revealed that all the respondents acknowledged (YES), they have pre-existing measurer(s) to tackle security vulnerability challenges in their corporate organization. The most-reported was devices 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 organizations upon implementation.

iii) Security Attacks resulting from Mobile device connection in corporate networks

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

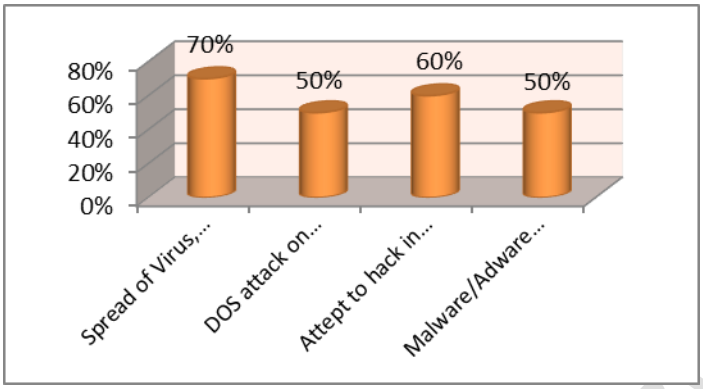


Figure 3: Security Attacks as a resulting from Mobile device connection in corporate networks

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

B. Determine matrices for existing mobile device security frameworks

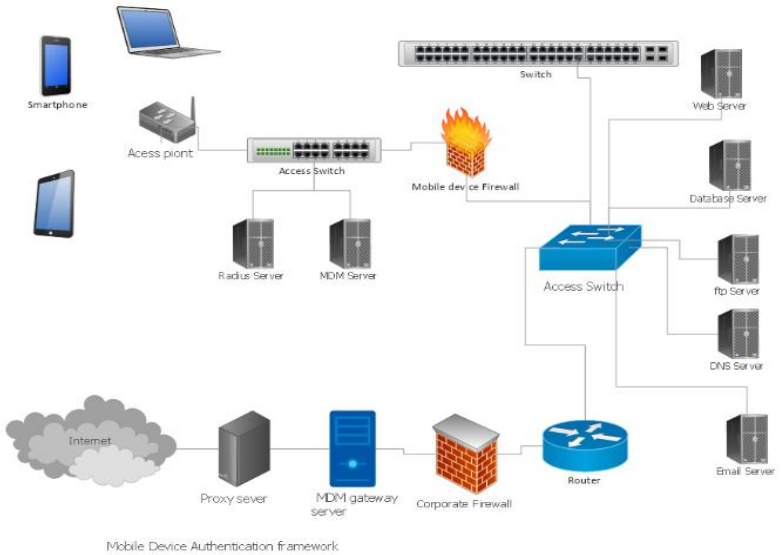
The reviewing of existing literature on Mobile device security frameworks and their solutions was done. Gimenez Ocano et al. (2015) suggested that frameworks development must be achieved based on five primary goals. The results of the review were captured in the matrix **Table 1**. Having reviewed all 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, authorization, 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

C. 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 a security vulnerability, as shown Fig 4 in below:



Mobile Device Authentication framework

Figure 4: Designed network Topology of the proposed framework

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

- Terminal devices- mobile devices such as a tablet, smartphone and laptop 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 organizational 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 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.

D. 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 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])

E. 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 figure below:

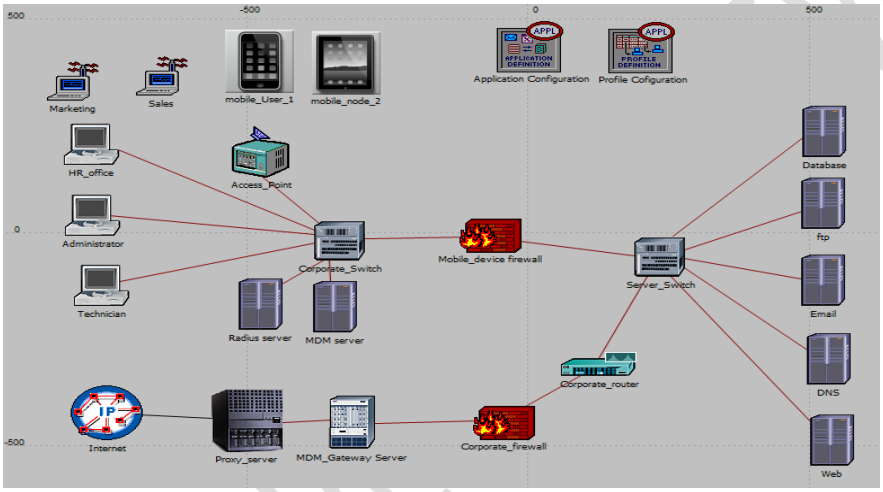


Fig 5: Screen shot of the proposed network model design in riverbed Simulator

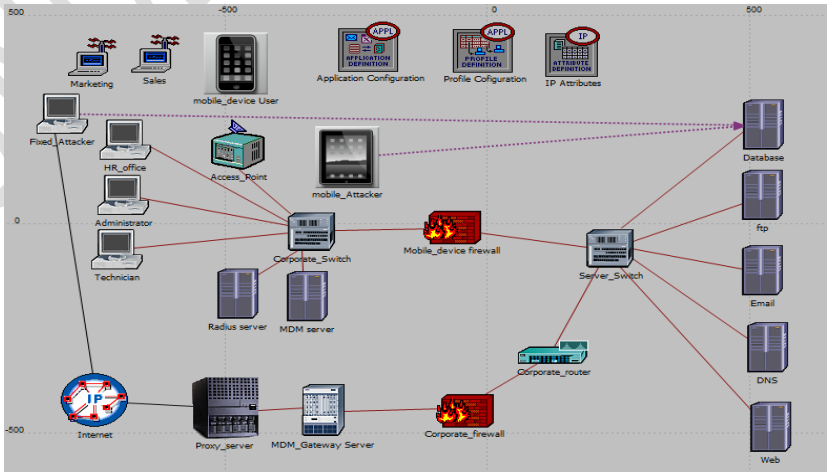


Figure 6: Screen shot of launching ping flood attack to a corporate server

The Attacks and preventive Scenarios

Simulation for the three scenarios was done, and the screenshots of the resulting graphs of the simulation are as shown below.

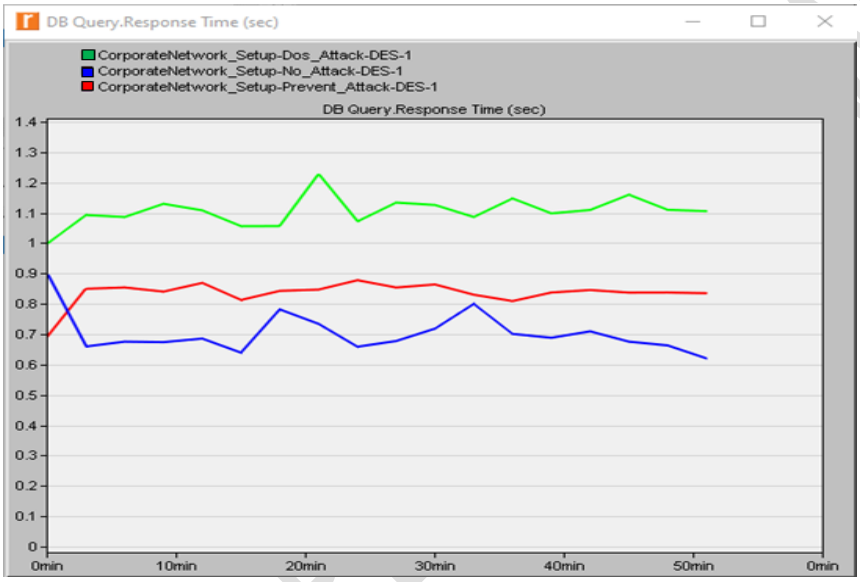


Figure 7: Screenshot of simulation results of the three scenarios in relation to the target server's database application (query)

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 on the DNS servers for orchestrating an amplification attack

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

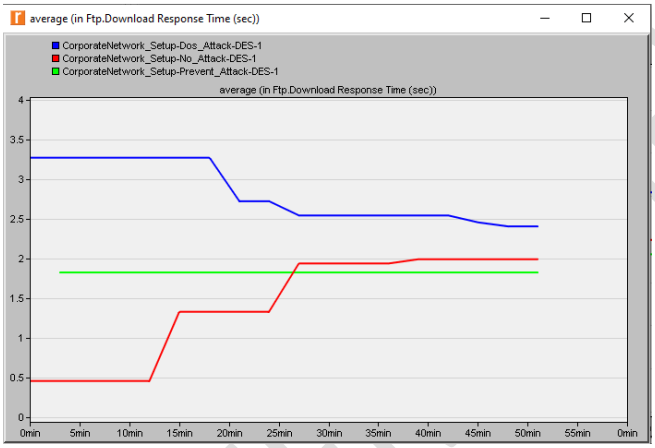


Figure 8. Screenshot of simulation results of the three scenarios in relation to the FTP download application of the target server.

On the same note, it was discovered that the CPU utilization 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 utilization returned to normal levels, having limited the number of authenticated mobile devices as shown below.

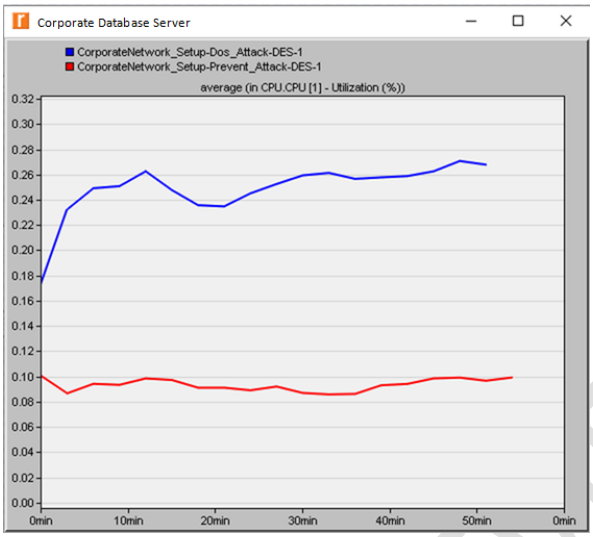


Figure 9: Screenshot of simulation results of the three scenarios in relation to the CPU utilization of the target server.

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.

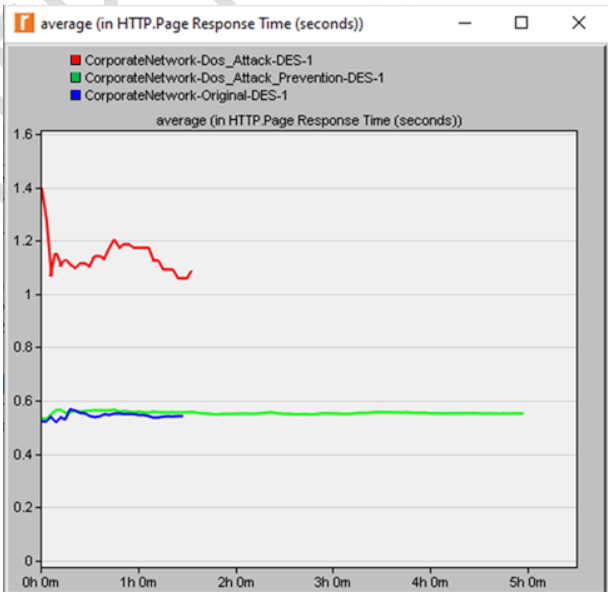


Figure 10: Screen shot of simulation results of the three scenarios in relation to the target server's HTTP (web service) application.

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 were 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 the simulation results. 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 analyzed, and the results of the utilization analyses simulation were captured. It was noted that CPU utilization 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 utilization 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 organizations were in existence. However, the study identified that little or no measures were adopted to address the foresaid challenges of increased mobile devices connected to their corporate network. The majority of corporate staff carry mobile devices at their workplaces, then allowed to freely connect to their corporate organizational network without strict measures to address mobile device-related challenges, and attacks are experienced. Findings from sampled corporate organizations (i.e. institutions of learning) revealed their lack of a mechanism to prevent attacks on their servers from the connected mobile devices that at a time causes denial of service problems, as highlighted by Davis et al. (2019). Therefore, the proposed framework is designed with clear mobile device attack preventive measures on how the challenge mentioned above can be solved with clear access to the network. Mobile devices from outside and connected to the corporate network were significant. They could not be overlooked since they are vulnerable to malware distribution, and data linkages of sensitive information, a challenge was foreseen by Jafari et al. (2016). The use of mobile devices could easily compromise both external and internal attackers. Therefore, all corporate organizations should institute security measures to shield themselves from evolving mobile device authentication-related threats and attacks, as earlier stated by (Marler, 2018).

This study, therefore, recommends that corporate organizations with more sensitive data and applications adopt the proposed framework to ensure that they rip its full benefit and keep themselves safe from mobile device-related threats and other authentication-related challenges.

References

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

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

Breitinger, F., & Nickel, C. (2010). User survey on phone security and usage. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI).

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

Chambers, E. A. (2004). An Introduction to meta-analysis with articles from The journal of Educational Research (1992-2002). The Journal of Educational Research, 98, 35-44.

Davis, M., Gilbert, M., Simon, K., Stephen, M., & Gilibrays Ocen, G. (2019). State of cyber security: the Ugandan perspective. International Journal of Scientific & Engineering Research.

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

Gimenez Ocano, S., Ramamurthy, B., Wang, Y., & Ocano, G. (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. https://doi.org/10.1109/ICCNC.2015.7069314

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

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly: Management Information Systems. https://doi.org/10.2307/25148625

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

Jack, W., Ray, A., & Suri, T. (2013). Transaction networks: Evidence from mobile money in Kenya. American Economic Review. https://doi.org/10.1257/aer.103.3.356

Jafari, N., Alsadoon, A., Withana, C. P., Beg, A., & Elchouemi, A. (2016). Designing a comprehensive security framework for smartphones and mobile devices. American Journal of Engineering and Applied Sciences, 9(3), 724–734. https://doi.org/10.3844/ajeassp.2016.724.734

Jeffrey, P. J. H., Leong, C. C., Huat, C. G., & Leng, L. S. (2016). CHALLENGES IN MOBILE SECURITY.

Lane, N. D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T., Campbell, A. T., & College, D. (2010). AD HOC AND SENSOR NETWORKS A Survey of Mobile Phone Sensing. IEEE Communications Magazine.

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

Majdi, E. B. (2013). Evaluation of mobile device management tools and analyzing integration models for mobility enterprise. http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-74017

Marler, W. (2018). Mobile phones and inequality: Findings, trends, and future directions. In New Media and Society. https://doi.org/10.1177/1461444818765154

Matovu, D., Gilbert, M. B., Authority of Kenya, C., Karume Simon, K., & Gilibrays Ocen, G. (2019). The Internet of Things: applications and security metrics with the Ugandan perspective. In International Journal of Advance Research. www.IJARIIT.com

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., Okoye, F. A., Mba, C. N., Asogwa, S. C., & Ozioko, F. E. (2013). A Holistic Mobile Security Framework for Nigeria. 3, 5–11.

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

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. International Journal of Security and Its Applications.

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? - a conceptualization within the paradigm of the internet of things. In Visualization in Engineering. https://doi.org/10.1186/s40327-018-0063-8

Taylor, K., & Silver, L. (2019). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally | Pew Research Center. In 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., & Koong, K. S. (2006). An onion ring framework for developing and

assessing mobile commerce security. International Journal of Mobile Communications, 4(2), 128–142. https://doi.org/10.1504/IJMC.2006.008605

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges. In IEEE Communications Surveys and Tutorials. https://doi.org/10.1109/COMST.2015.2487361