International Journal of Networks and Communications 2018, 8(4): 106-114
DOI: 10.5923/j.ijnc.20180804.02

KANYI BYOD Security Framework: For Secure Access and Use of Mobile Devices in a BYOD Environment

David Kanyi*, Patrick Ogao

Faculty of Computing and Information Systems Management, KCA University, Nairobi, Kenya

Abstract Bring your own device (BYOD) is an IT policy where employees, students, and other people are allowed or encouraged to use their personal mobile devices—and, increasingly, notebook PCs—to access enterprise data and systems. BYOD has brought in a new dimension towards information security in enterprises. Hence new measurers to address the security concerns raised by BYOD implementation must be put in place. There are a number of frameworks developed in this domain of BYOD security. However these frameworks target to solve some security issues and leaves others unaddressed and hence this gap has to be filled by the proposed KANYI BYOD framework. The proposed framework was derived from reviewing existing frameworks and identifying their strengths and weaknesses. The proposed KANYI BYOD Framework borrows from BFS security Framework with a major difference in: advanced devices access to the campus network, Malware detection and prevention, Mobile devices users' categorization and access to servers and rogue access points by disabling Hotspots applications in mobile devices. Simulation methodology (using OPNET version 14.5) was used to test and validate the proposed framework by subjecting the framework network model to a mobile attacker node and putting preventive measures to address the attack and then comparing the simulation results of the various aspects of network performance tested as well as the campus server that was being targeted. We describe the structure and functioning of the framework, security vulnerability tests and discuss the results of the simulation test of the framework.

Keywords BYOD, BYOD Framework, MDM, Simulation

1. Introduction

BYOD was coined by marketers to describe the consumerization of IT as the growth of home computing and new mobile devices that include smart phones and tablets led businesses to demand for simple and easier computing to match those used at home. BYOD enables individuals to be in charge of their own devices in relation to the operating systems, management and maintenance of the devices.

There are some benefits brought about by adopting BYOD in organizations: Adopting BYOD reduces device investment costs for organizations by shifting the cost of procuring the devices to their employees [9, 12]. The other cost transferred to the employees by the organizations is that of replacing outdated equipment. [12] Notes that employees get satisfied by owning their own devices since they are able to maintain and replace the device at own will. BYOD adoption also enables employees to use cutting edge technology due to their ability of being able to constantly upgrade their devices [5]. Another benefit to organizations due to BYOD adoption is increased productivity by employees since by using their own devices they are able to work outside normal office hours [8]. Employees also appreciate more the IT support provided by their organizations since they perceive it as more personal I stead of just support to the devices [5].

Besides the benefits that are a number of issues and challenges associated with adoption of BYOD. These issues include challenges of delivering applications to multiple platforms, security issues and privacy issues [1]. According to [6] the issue of employees' privacy needs to be addressed because mobile devices contain a wealth of personal data which may mingle with employee data on the same device. [6] Classified threats due to BYOD as direct threats like loss/theft of devices and indirect threats which include interceptions of communications due to unsecured wireless network, malware attacks and location tracking. Other BYOD risks include; loss of control and visibility [1-3]. [12] Identifies malware attacks through rogue access points provided by an attacker as the major security threat in a BYOD environment. The aim of this project was to design the Framework and test the performance of the framework through simulation.

* Corresponding author:
daudikanyi@gmail.com (David Kanyi)
Published online at http://journal.sapub.org/ijnc

The paper is organized as follows: a review of current BYOD security Frameworks, introduction of the proposed framework, modelling of the proposed framework into a network topology diagram for simulation testing purposes, Security Threats Evaluations by Attack Scenarios, Quantification for Security Vulnerability Associated with the Proposed Framework, Simulation for Security Vulnerability Testing , Simulation Results and Discussion, Conclusion and Future Work.

2. A Review of Current BYOD Security Frameworks

To address BYOD security challenges and issues different BYOD frameworks and other solutions are proposed by various security experts to mitigate different issues. A BYOD framework is a systematic model and related processes to resolve each component issues holistically. In the BYOD security domain there exists other frameworks. The following existing frameworks will be reviewed:

- SSA Framework
- 2TAC Framework
- Cisco Framework
- BSF Framework
- RMS Framework

Security Service Architecture (SSA) Framework

This framework was proposed by [6] for checking the security status of smartphones by monitoring the applications that are downloaded from Application stores and checking smartphones for Malware, misbehaving applications and configurations. This is achieved by creating a virtual replica of the smartphone on the enterprise side and analysing it for security flaws. The noted weaknesses of the framework are as follows:

- Limitation to smartphones
- Lack of control of devices access to the enterprise network
- Mobile devices in connection are not accounted for.
- Space Isolation and protection of stored corporate data is not addressed.
- Access to enterprise network through Rogue access points (hotspots) is not addressed
- Controlled access of mobile devices into the enterprise internal network (servers).
- Spread of corporate data to personal emails

2 Tier Access Control (2TAC) Framework

This framework was proposed by [3] for controlling the access to enterprise information from mobile devices. This is achieved by implementing a double layer access control (one layer is at the device level and the other one is at the cloud level) along with device security profiles, anti-virus/malware scanners and social networking. The noted weaknesses of the framework are as follows:

- Mobile devices in connection are not accounted for.
- Access to enterprise network through Rogue access points (hotspots) is not addressed
- Controlled access of mobile devices into the enterprise internal network (servers).
- Space Isolation and protection of stored corporate data is not addressed.
- Spread of corporate data to personal emails

Cisco Framework

Cisco offers a BYOD smart solution that lay emphasis on infrastructure of the enterprise network and thus provides security policy management, mobile devices access and management, mobile applications management and further supports MDM from other parties. Mobile devices access and security management is very well addressed by this smart solution. It is strong BYOD security framework with the following notable weaknesses:

- Space Isolation and protection of stored corporate data is not addressed.
- Spread of corporate data to personal emails

Remote Mobile Screen (RMS) Framework

This framework was proposed by [8] and similarly modifies the BSF framework by moving the corporate space from the mobile device to the enterprise side hence providing true isolation. For access to the enterprise space from the mobile device a new element called Corporate Space Manager and VNC protocol are introduced. A VNC client installed in the mobile device aids the device to access the corporate space. When the user accesses the enterprise side he/she is presented with an interface designed for mobile devices. In other words a mobile device accesses a Mobile OS and not a desktop OS. This is a strong a framework which similarly modifies the BSF framework with the following notable weaknesses:

- Mobile devices in connection are not accounted for.
- Access to enterprise network through Rogue access points (hotspots) is not addressed
- Spread of Malware from mobile devices is not addressed.

BSF Framework

This framework has been modified by the RMS framework as well as the KANYI BYOD framework. It is covered in detail in section 2.1.

The above current BYOD frameworks were reviewed based on their existing literature and against the listed goals. In order to prevent BYOD threats and challenges, a BYOD solution must achieve the following goals: [8]

- Space isolation- this ensures that employee's space and corporates data spaces are isolated so that security policies can be implemented effectively.
- Corporate data protection-this comprises techniques such as encryption to ensure that corporate data is protected from unauthorized access.

- Security policy enforcement- this ensures that mobile devices are complaint with the existing security policies.
- True isolation- this ensures that corporate data cannot be stored in employee's devices.
- Non-intrusive- this ensures that any agent installed in employee's device does not infringe on the privacy of the mobile device user.
- Non-resource-intensive- this ensures that the solution to be implemented to handle security issues does not consume too much of the mobile devices computing resources.

[8] Categorized the various BYOD solutions into 5 categories as follows:

- Agent Based
- Cloud Based
- Mobile Virtual Machine (MVM)
- Framework
- Trusted Execution Environment (TEE)

We compared the current solutions to the desired goals above. The table 2 shows the comparison of the solutions that include the Proposed KANYI BYOD Framework.

We further compared the mentioned frameworks to how they address the listed key BYOD concerns as parameters of performance. The comparison is given in table 1.

Table 1. Comparison of BYOD Frameworks to BYOD concerns

BYOD Concerns	SSA	2TAC	CISCO Framework	BSF Framework	RMS Framework	KANYI BYOD Framework
Mobile devices access to the enterprise network	None	Double layer access control	NAC Server	NAC server	NAC server	NAC server, MDM Agent
Ensuring the devices OS and applications are updated and secure	None	none	none	none	none	MDM agent
Installation and spread of malwares through mobile devices	Replication of device Applications on enterprise side	none	none	None	none	MDM agent
Tracking and accountability of connected mobile devices	None	none	Third party MDM servers	MDM Server	none	MDM Server
Control of access to enterprise internal servers	none	Double layer access control	Cisco BYOD Firewall	SPD	SPD	Mobile Devices firewall
Unauthorized device access through rogue access points-hotspots	none	none	none	none	none	MDM agent
Corporate Data isolation , protection and spread to personal email addresses	none	none	Third party MDM	MVM and MDM agent	VNC agent and CSM	MDM agent

Table 2. Comparison between the Different Types of Solutions [8]

		DESIRED GOALS					
Solution	Type	Space Isolation	Security Policies	Corporate data protection	Non-intrusive	Non resource intensive	True Isolation
MDM/MAM	Agent based		**X**	**X**		**X**	
Cloud-based	Cloud Based			**X**	**X**	**X**	**X**
MOSES	MVM	**X**		**X**			
CELL	MVM	**X**		**X**			
SSA	Framework		**X**				
2TAC	Framework		**X**				
Cisco	Framework		X		X	X	
BSF	Framework	X	X	X			
TrustDroid	TEE	X	X				
KANYI BYOD Framework	Framework	X	X	X		X	X

2.1. BSF (A BYOD Security Framework)

BYOD Security Framework (BSF) was proposed by [12]. This framework addresses security issues from the perspective of the two sides:

Enterprise side: This is the enterprise network side that comprises of:

- Corporate's Resources
- Security Policy Database (SPD)
- MDM (Mobile Device Management)
- NAC (Network Access Control) - implements space isolation based on the SPD policies.

BYOD side: This is the mobile device side. Security on this side is enforced by MDM agent and MVM (Mobile Virtual Machine).

3. KANYI BYOD Framework

3.1. Architecture

This framework modifies the BSF Framework by [15] by eliminating the use of MVM. The isolation will instead be achieved by the MDM agent installed in mobile devices. Mobile devices access to the campus network will also be handled differently in our proposed framework. The proposed framework targets learning institutions simply because this is where BYOD is more pronounced. It can however be implemented in any other enterprise. The proposed framework addresses security issues from a perspective of the three sides:

BYOD Side: This is the device side. The BYOD side is entirely monitored by the installed MDM agent. The MDM agent is the key security implementing feature at the BYOD side. It scans the device to ensure that it is safe (complies with the SPD in the NAC server) to be granted access by the NAC server located on the perimeter side. The agent monitors applications to ensure that they do not introduce malwares into the campus network.

The MDM agent creates a secure container to temporary store campus data. This data is wiped out when the device is out of range of campus WI-FI. The agent disables Adhoc networking (tethering and hotspot applications) in mobile devices and other SSIDs while the active campus SSID is still active in order to avoid creation of rogue access points. It's a requirement for the MDM agent to be installed in the device before permission to access the campus network can be granted by the NAC server. The NAC server has to get permission granted confirmation from the agent before granting a device access to the campus network. MDM agent implements the policies stored in Security Policy Database. The database is stored and implemented from the NAC server.

Perimeter Network Side: this side resides from external firewall to the MDM firewall. Its components are:

- Network Access Control Server (NAC)-Grants or denies permission to the campus network based on communication received from MDM agent and MDM gateway server. Devices get blacklisted at NAC server. NAC has a got a security policy database (SPD). NAC server also checks for existence of an agent in the mobile device before connection can be granted. For the first time mobile device network access the NAC server has to prompt the MDM server to install an agent to the device. The user will be prompted to install the agent. If he/she accepts by clicking OK button then he/she will proceed to install the agent. If he/she clicks cancel button to deny the installation then NAC server denies him/her access to the campus network. NAC server is also connected and polls the authentication server. For a mobile device to be fully connected to the campus network, then the agent must be installed and have scanned the device based on the policy in the SPD and sent its confirmation to the NAC server. The agent becomes active and automatically scans the device once it detects and receives the campus WI-FI signal. If the agent detects an OS vulnerability, malware or outdated antivirus it will notify the user and informs the NAC server to deny access to the mobile device till corrections are done. The details are sent to MDM server for capturing. The agent captures all running applications as well as device hardware details and sends them for capturing to the MDM server only if the device is granted access to the network.
- MDM gateway server-resides in the DMZ zone to further filter traffic towards NAC server.
- Campus Firewall-filters the incoming traffic from a mobile device with an installed MDM agent.
- Mobile Devices Firewall- controls mobile devices access to the internal servers based on user's categorization found in the authentication server.

Enterprise Side: This is the side of the campus network consisting of the rest of the elements of the KANYI BYOD framework. The elements consist of:

- MDM server and Console (or mobile App)-all mobile device details and running applications are captured by the server as received from agents. This server installs agents into mobile devices and manages them.
- Authentication server- has got centralized log in system for the entire campus. All users' authentication and categorization is performed by this server.

The general outline of the proposed framework is as illustrated in Figure 1.

A flow chart of how devices access the enterprise network and are managed by the framework is illustrated by figure 2.

3.2. Network Topology Model of the KANYI BYOD Framework

KANYI BYOD Framework is implemented through a network topology diagram model as illustrated by figure 3. The topology model was evaluated using OPNET Modeler for security vulnerability test.

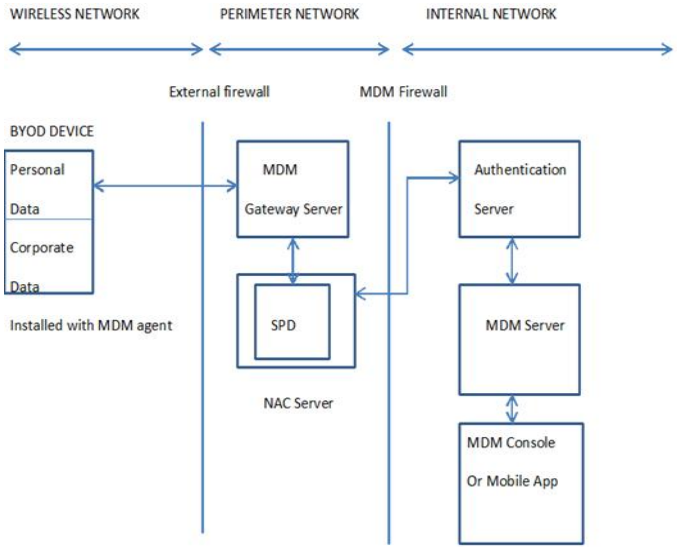

Figure 1. General Architecture of KANYI BYOD Security framework

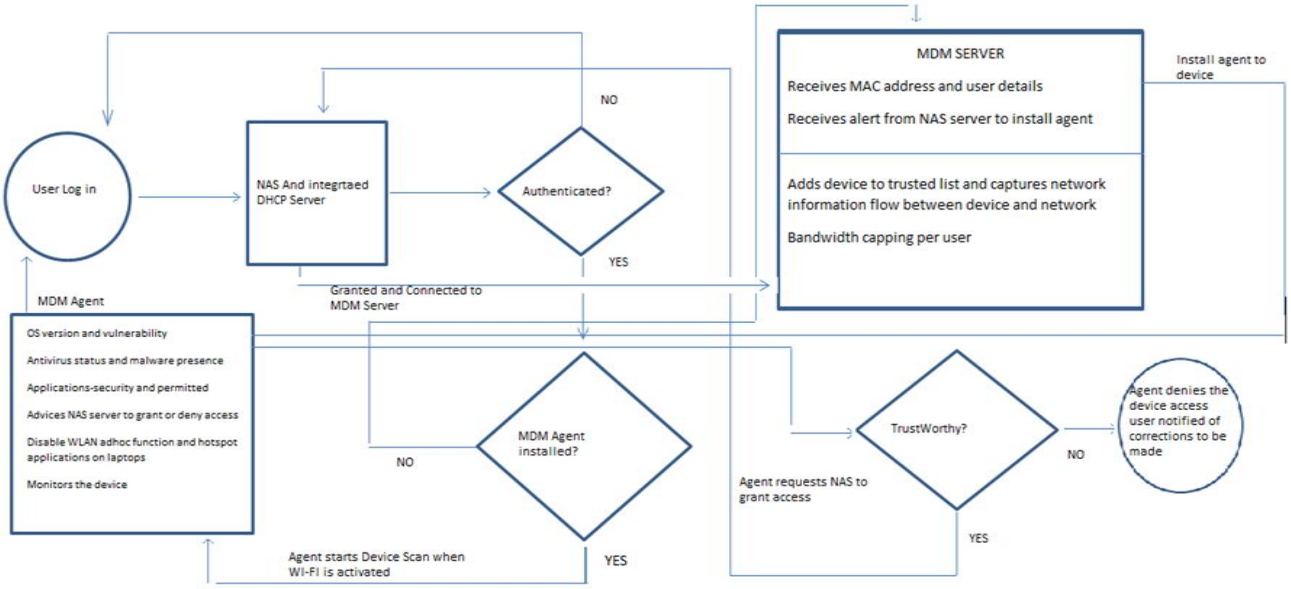

Figure 2. KANYI BYOD Security Framework Data Flow Diagram for devices access to the Campus network

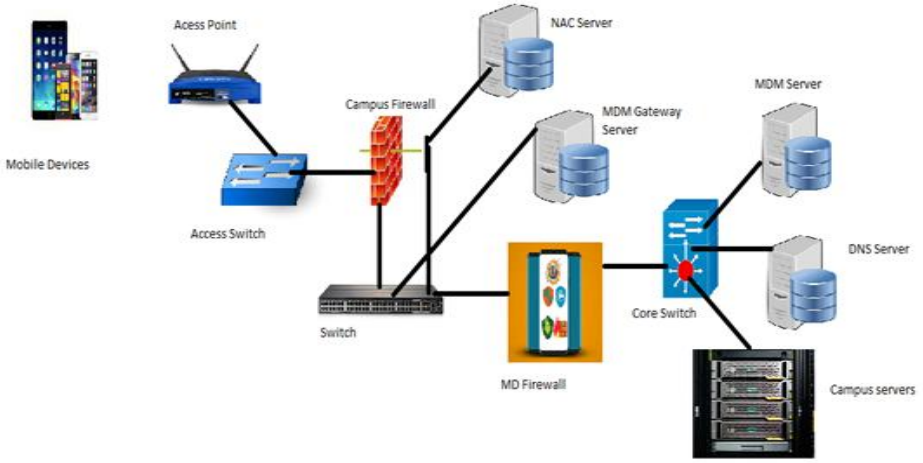

Figure 3. Proposed network Topology model to integrate KANYI BYOD framework to the Campus network

3.3. Security Threats Evaluations by Attack Scenarios

The network topology model was evaluated for security vulnerability as shown by figure 4. The threat evaluation is shown by a graph that represents the attack paths through the model.

The attack scenarios are elaborated into 4 cases: Outside attacker Scenario

Case 1

S1 → NS1 {E1 → E2 → E3 → E4} → NS2 {E1 → E2 → E3} → NS3 {E1..En} → T1

Case 2

S1 → NS1 {E1 → E2 → E3 → E4} → NS2 {E1} → T2

Inside attacker Scenario

Case 3

NS2 {E1 → E2 → E3} → NS3 → {E1..En} → T1

Case 4

NS2 {E1} → T2

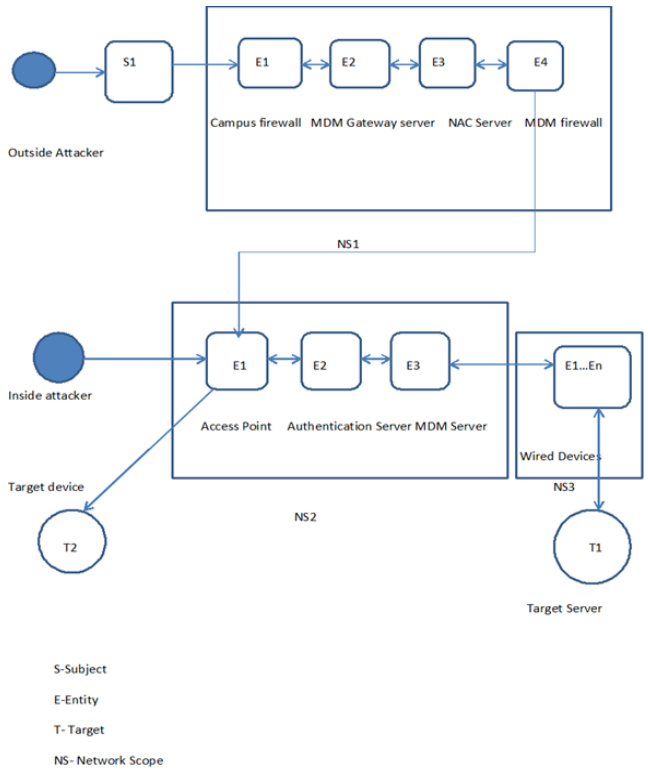

Figure 4. A graph of the Attack paths

3.4. Quantification for Security Vulnerability Associated with the Proposed Framework

Quantification for security vulnerability associated with the proposed framework was done based on the 4 cases. CVSS (Common Vulnerability Scoring System) Version 2 method which provides an open framework for communicating the characteristics and impact of ICT vulnerabilities was adopted. The base scores for the 4 cases were calculated and results captured in table 3.

Table 3. CVSS Analysis of the 4 cases

CVSS Metrics	Case 1	Case 2	Case 3	Case 4
Access Vector (AV)	N: 1.0	N: 1.0	A: 0.646	A: 0.646
Access Complexity (AV)	M: 0.61	M: 0.61	L: 0.71	L: 0.71
Authentication (Au)	S: 0.56	N: 0.704	S: 0.56	N: 0.704
Confidentiality Impact (C)	C: 0.66	C: 0.66	C: 0.66	C: 0.66
Integrity Impact (I)	C: 0.66	P: 0.275	C: 0.66	P: 0.275
Availability Impact (A)	C: 0.66	P: 0.275	C: 0.66	P: 0.275
Base Score	8.5	8.3	7.7	7.3

3.5. Simulation for Security Vulnerability Test

The proposed BYOD network model was setup using Opnet simulator version 14.5. Figure 5 is a screen shot of the designed model on the simulator.

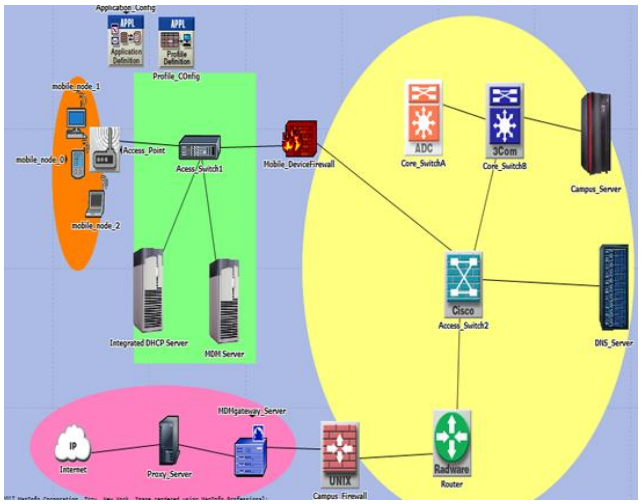

Figure 5. Screen Shot of KANYI BYOD network model design in Opnet Simulator

KANYI BYOD network model was subjected to an attacker launching ping flood attack as shown in Figure 6. The attacker was targeting the campus server with very large ping packets creating a huge congestion all over the network.

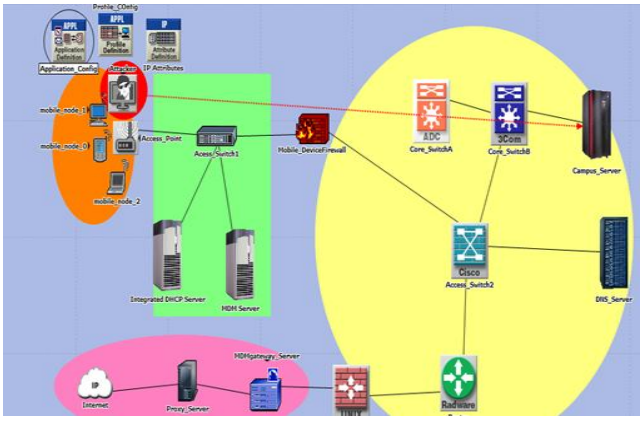

Figure 6. Screen shot of an attacker mobile node targeting the campus server

4. Simulation Results and Discussion

Three scenarios were created for the purpose of comparing the simulation results:

- Scenario 1- BYOD Simulation with no attack
- Scenario 2- BYOD simulation with an attacker mobile node
- Scenario 3- BYOD simulation with Preventive measures in place.

Various aspects of the performance of the network and its components based on the 3 scenarios were measured and the results were as follows:

a. Database application (entry) of the campus server

When there is not attack in the BYOD network the response rate of the database application (entry application) to the request made by the mobile_node 2 is less as compared to when there is an attacker scenario. When preventive measures are put in place the database application response rate reduces to normal rates.

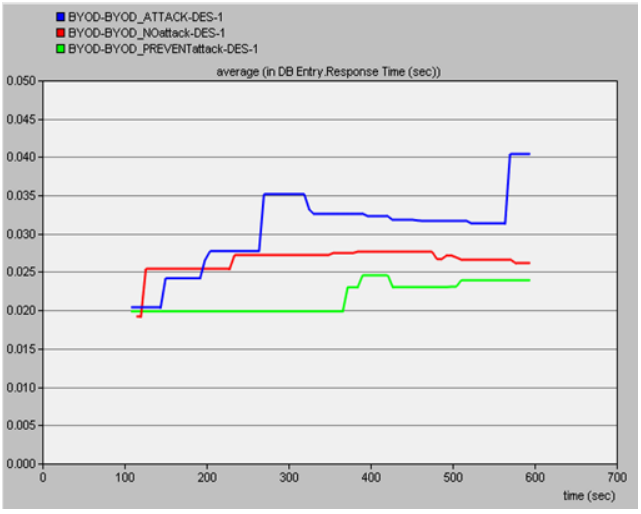

Figure 7. Screen shot of simulation results of the three scenarios in relation to the Database application (entry) of the target server

b. HTTP (web service) application of the Campus server

The web server response rate to the mobile node 2 was measured and the simulation results were captured in figure 8. It was noted that web service response rates went high when the DOS attacker was introduced. This was expected due to the fact that the network became congested by the ping flood packets from the attacker mobile node. When preventive measures were introduced (MDM firewall) to tackle the DOS attack the response rates go back to the expected levels.

c. DNS server CPU performance

The CPU performance of the Campus DNS server was analysed and the results of the utilization analyses simulation captured in figure 7. It was noted that DNS CPU utilization in percentage per second went high when the DOS attacker was introduced. This was expected due to the fact that the DNS was engaged by the ping flood packets from the attacker mobile node. When preventive measures were introduced (MDM firewall) to tackle the DOS attack the DNS CPU utilization rates went down to the expected levels.

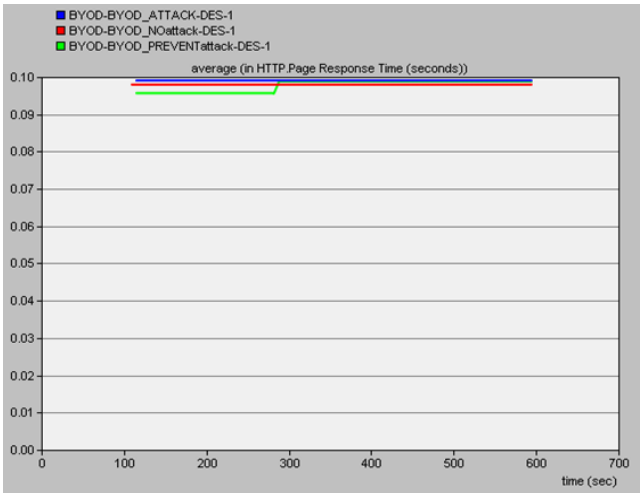

Figure 8. Screen shot of simulation results of the three scenarios in relation to the HTTP (web service) application of the target server

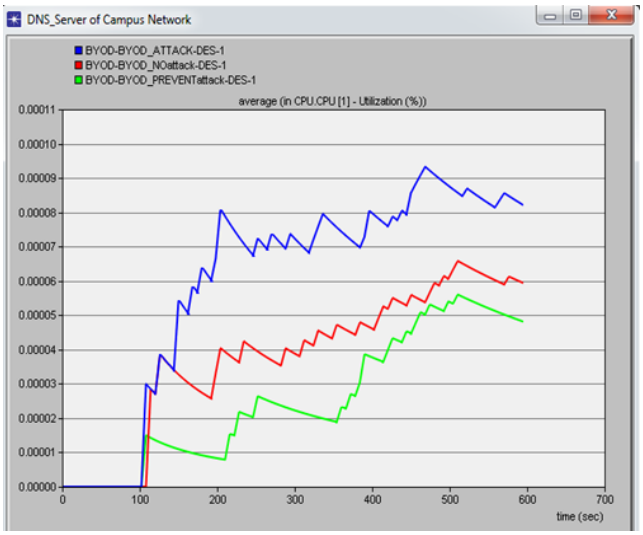

Figure 9. Screen shot of simulation results of the three scenarios in relation to the DNS server CPU performance

d. WLAN media access delay

The delay in accessing the WLAN media from mobile node 2 was measured and the simulation results captured in figure 10. It was noted that it took longer to access the WLAN media when the attacker node was introduced. This was as a result of the congestion of the network brought about by the ping flood packets from the attacker node. It was further noted that the WLAN media access delay was higher when MDM firewall was introduced as compared to when none was in existence because the firewall added to the delay of the WLAN media access as well.

e. Core Switch B traffic flow to and from Campus server

The flow of network traffic through core switch B to and from Campus server was measured for the three scenarios. The simulation results were as captured in figure 11. It was

noted that the switch was much busy-much network traffic when the DOS attacker node was introduced. This was expected due to ping flood packets from the attacker which increased the network traffic to high levels. When preventive measures were introduced to tackle the DOS attack the network traffic through the core switch reduced to become the least as shown in the figure due to few packets coming from the mobile nodes to the campus server.

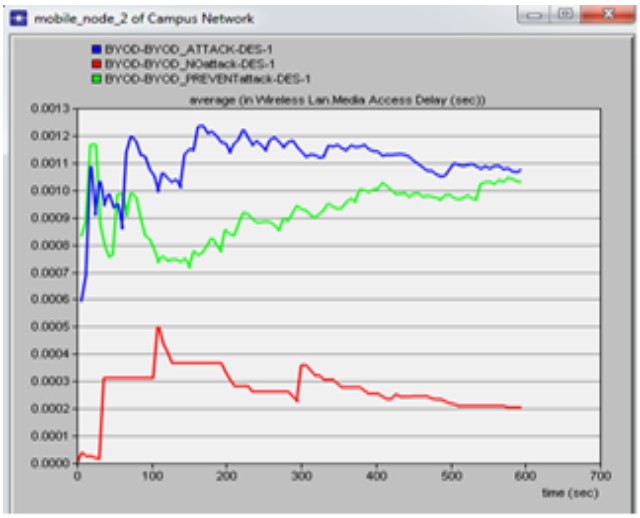

Figure 10. Screen shot of simulation results of the three scenarios in relation to mobile_ node 2 WLAN media access delay

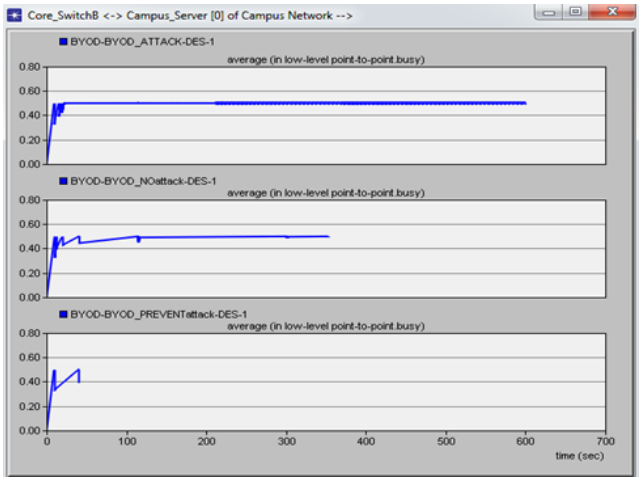

Figure 11. Screen shot of simulation results of the three scenarios in relation to Core Switch B traffic flow to and from Campus server

5. Conclusions

There are several frameworks and other solutions that have been developed by experts in this domain but each of them falls short of addressing some key security issues presented by adoption of BYOD. KANYI BYOD Framework was designed for a learning environment where BYOD is more pronounced and in extensive use. It can however be adopted in other enterprise where BYOD is in use. It strengths lie in how devices access the campus network, security of campus data in mobile devices (isolation and blockage from sending to personal email addresses), internal servers access and accountability of connected devices.

FUTURE WORK

A smartphone application console of this framework is the future way to go. This will enable ICT administrators to monitor and manage mobile devices while away from the enterprise.

ACKNOWLEDGEMENTS

I wish to acknowledge Prof. Ogao for his guidance to successful completion of this project and my wife Jane Muthoni Kanyi for her enormous moral support.

REFERENCES

[1] Ali, S., Qureshi, M.N. and Abbasi, A.G., 2015, December. Analysis of BYOD security frameworks. In Information Assurance and Cyber Security (CIACS), 2015 Conference on (pp. 56-61). IEEE.

[2] Boon, G.L. and Sulaiman, H., 2015. A review on understanding of byod issues, frameworks and policies. In 3rd National Graduate Conference (Nat Grad 2015), Universiti Tenaga Nasional, Putrajaya Campus. Retrieved from http://cogs.uniten.edu.my/portal/NatGrad2015/conference.html.

[3] Chung, S., Chung, S., Escrig, T., Bai, Y. and Endicott-Popovsky, B., 2012, December. 2TAC: Distributed access control architecture for "Bring Your Own Device" security. In BioMedical Computing (BioMedCom), 2012 ASE/IEEE International Conference on (pp. 123-126). IEEE.

[4] D. Titze, P. Stephanow, and J. Schutte, “A configurable and extensible security service architecture for smartphones,” in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th Int. Conf. on, 2013, pp. 1056–1062.

[5] Eslahi, M., Naseri, M.V., Hashim, H., Tahir, N.M. and Saad, E.H.M., 2014, April. BYOD: Current state and security challenges. In Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on (pp. 189-192). IEEE.

[6] Hernandez, A. and Choi, Y., 2014. Securing BYOD Networks: Inherent Vulnerabilities and Emerging Feasible Technologies.

[7] Hovav, A. and Putri, F.F., 2016. This is my device! Why should I follow your rules? Employees’ compliance with BYOD security policy. Pervasive and Mobile Computing, 32, pp.35-49.

[8] Ocano, S.G., Ramamurthy, B. and Wang, Y., 2015, February. Remote mobile screen (RMS): An approach for secure BYOD environments. In Computing, Networking and

Communications (ICNC), 2015 International Conference on (pp. 52-56). IEEE.

[9] Putri, F.F. and Hovav, A., 2014. Employees compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory.

[10] Russello, G., Conti, M., Crispo, B. and Fernandes, E., 2012, June. MOSES: supporting operation modes on smartphones. In Proceedings of the 17th ACM symposium on Access Control Models and Technologies (pp. 3-12). ACM.

[11] Vignesh, U. and Asha, S., 2015. Modifying security policies towards BYOD. Procedia Computer Science, 50, pp.511-516.

[12] Wang, Y., Wei, J. and Vangury, K., 2014, January. Bring your own device security issues and challenges. In Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th (pp. 80-85). IEEE.

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

[14] Zhao, Z. and Osono, F.C.C., 2012, October. "TrustDroid™": Preventing the use of Smart Phones for information leaking in corporate networks through the use of static analysis taint tracking. In Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on (pp. 135-143). IEEE.