Secure Remote Mobile Screening (SRMS) Framework for Bring Your Own Device (BYOD)

Seham Alnefaie, Omar Batarfi

Information Technology Department
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia

***Abstract*- Bring Your Own Device (BYOD) refers to allowing the employee to bring his own device to the work place to use the company resources (e.g. network, software or data). Involving BYOD in corporates introduced many key benefits such as increasing the productivity and reducing the cost. On the other hand, BYOD poses many security risks ad it can lead to data leaking. Numerous solutions have been proposed in the literature to address the security of BYOD. In this paper, we provide an overview of BYOD including its advantages and the security issues that may faces BYOD enabled companies. Then, we proposed a Secure Remote Mobile Screening (SRMS)which enhances the security level of the original Remote Mobile Screening (RMS) framework by overcoming its limitation which resides on the ability of the employees to take screenshots of the corporate data.**

***Keywords*- Bring Your Own Device, BYOD, BYOD Security.**

I. INTRODUCTION

Nowadays, smartphones devices become ubiquitous due to the rapid evolution of functionality and computing capabilities of these devices. As a result, BYOD has emerged which is a new phenomenon that is receiving attention in the business environments. BYOD allows employees to use their own mobile devices for example smartphones, laptops, and tablets to access the corporate's data and network. BYOD have positively changed enterprise business environments by offering many advantages, but the most obvious benefit is reducing cost of providing devices and increasing employees' productivity [1]. However, the security level of employees' personal devices is less than the security level of corporate's devices. So, enabling BYOD caused many security issues related to the corporates data [2]. This paper addressed the advantages of applying BYOD, BYOD security issues including internal and external threats, and explains some of previous studies proposed by researcher to solve some of BYOD security issues. Then we proposed SRMS framework which enhances the Remote Mobile Screen (RMS) framework [6] by preventing the users from taking screenshots which leads to increase the level of security of this framework.

II. BACKGROUND

Implementing BYOD in working environments offers many advantages, these advantages include:

- Increasing employees' productivity and satisfaction.
- Reduce the cost of hardware, software, procurements, licenses, and insurance.
- Improve flexibility and mobility.
- Enhance the efficiency of the work because the employees are familiar with their own device which leads to reduce the training cost.
- Employees can utilize many smart apps that aims to facilitate the business work such as GotoMeeting which used to arrange virtual conferences in quick and easy manner.
- Employees will be careful in using their own devices rather than the corporates' ones.
- Facilitate sharing information and communication among employees [3].

A. BYOD Security issues:

BYOD enabled companies are subject to diverse security threats. Since the used devices are personally owned controlled by employees not by corporates. These threats are either external caused by cybercriminals (outsider) or by trustworthy employees (insiders). The following part will explain different examples about the mentioned threats types [2].

1) External Threats

Through implementing BYOD in organizations, employees access to more advanced technologies which make it easy for cybercriminals to steal corporates data and thieve financial profits especially when employees lack security awareness. The following part illustrates some of external threats that may face BYOD environments [2].

1. Malware:

As the fast growth in mobile devices technologies, there is an equivalent growth in malware software too. In BYOD environment, when a malware gets into an employee device it can spread its damages on the corporate for instance it may cause an interruption to the organization processes, thieves sensitive information, or attracting hackers by providing them with an entry point [1]. Therefore, malware threat is the most significant threat to the enterprise's data [2].

2. Social Engineering:

Due to the lack of security awareness among employees, social engineering become another dangerous threat to BYOD environments since attacker exploits social networks to spread malware. Hence, when a user uses his social networking accounts during breaks will rise the chance to infect the company network. Because it is difficult for the corporate to control and monitor the performed activities by employee personal devices [2].

3. Malicious Mobile Applications:

Through installing this kind of applications, the attackers may compromise and collect the company sensitive data [2].

4. Insecure Wireless Networks:

Outside the corporate, employees are daily accessing many external networks including home, public wi-fi and cellular networks. Normally, the security level of these external networks cannot be controlled by the corporate itself. Such insecure communication channels are subject to man-in-the-middle and eavesdropping attacks threats since the user and the attacker are using the same network [1].

2) Internal Threats

This type of threats caused by trustworthy employees (insiders) who could mistakenly or maliciously disclose organizations data. These threats include:

1. Mixing of the personal and company's Information.
2. Stolen, lost and unlinked Devices [2].

III. Literature Review

In this part we surveyed some recent solutions to provide security for BYOD-enabled companies and their employees. These solutions are varying between malware detection frameworks, general security frameworks and some propositions for detecting abnormal behavior.

A. Malware Detection Frameworks:

This section presents two previous studies that proposed solutions in the malware detection field which are:

- Spotmal : Ahybird malware detection framework with privacy protection for BYOD.
- A configurable and extensible security service architecture for smartphones.

Spotmal: a hybrid malware detection framework.

In [4], the authors proposed a hybrid malware detection framework that protect the (SpotMal) to detect malware in BYOD environments while maintaining the privacy and secrecy of personal data. The authors tried to produce an improvement in BYOD security solutions by providing a relevant solution that combines the advantages of externalized malware scanning and hybrid detection. Moreover, they showed that SpotMal offers many advantages such as: detecting and removing known and unknown malware. Further, it preserves the confidentiality of corporate's sensitive data. Also, they mentioned that the employees access the enterprise network without being afraid about infringement of personal privacy, since the employee's personal activities and data are anonymized before performing scanning process. However, to the best of our knowledge, anonymizing the personal data not enough to preserve the employee's privacy, for example personal photos will be disclosed even if it was from unknown source.

A configurable and extensible security service architecture for smartphones.

Titze.et.al. [5] proposed an extensible and configurable framework that allows BYOD enabled corporates to execute automatic security checks to inspect their employees' smartphones. This framework runs over a virtual replica of the physical device. It provides security services that can be replaced and configured based on the user security demands. The framework will check the virtual smartphone copy against any malware threat, if any threat is detected, then the framework will notify the affected device along with prescript about how to deal with this menace. On the other side, the framework will respond by preventing the outgoing and incoming traffic to the affected device. Moreover, the authors showed that their solution is sufficient for detecting malicious applications. Also, they mentioned that deploying the framework will not make deep changes in the employee's devices. However, it has a limitation regarding the emulation process which is not possible for all smartphone types. As a result, the number of supported devices is limited. Although I agree that this framework is powerful because of its ability to extend to add more security services and its ability to comply with the corporate security requirements, However, this solution leads to great overhead because of replicating and emulating each physical device.

B. BYOD security framework

This part presents a comprehensive framework for securing BYOD environment (RMS).

RMS (Remote Mobile Screening)

Ocano.et.al. suggested Remote Mobile Screen (RMS)[6] which is an approach that aims to provide secure BYOD environments. The researchers rely their solution on a previously proposed framework which is BYOD Security Framework (BSF). RMS adjusts BSF by transforming the corporate space into the enterprise network. As a result, BYOD side only contains the employee's personal data, applications along with VNC (Virtual Network Computing) client app which allow the employee to access to the enterprise network. Through accessing a virtual OS, the user can perform the asked tasks. RMS succeed to achieve its objective to protect BYOD environment. It provides a true isolation because it separates corporate space inside the enterprise network and the personal space in the employee device. Furthermore, ensue security policy enforcements because the company has the full control. Also, it preserves the data confidentiality because even in case of device loss the data will not be affected since the corporate data stored in the enterprise network. Although RMS is an efficient solution that overcome many BYOD security challenges, however, it suffers from some limitations in connectivity, latency, and the data secrecy is not totally preserved since it could be stolen through screen shots.

C. Detecting Abnormal Behavioral

This section presents two proposed solutions for securing BYOD enabled corporates based on detecting abnormal behavioral technique.

IFT - Intelligent Filtering Technique for Bring Your own device Network Access Control

In 2017, an Intelligent Filtering Technique (IFT) [7] proposed through the use of Artificial Intelligent (AI) Technique. Using the behavioral patterns of the device Packet Inter-Arrival-Time (IAT) features and using the header of network traffic flow packet, for example, TCP, UDP, and ICMP. This solution is an addition to the field of Artificial Intelligent (AI) which combines Device Behavior Profiling Technique and Filtering Techniques (FT) to detect Anomalies. The first stage of the process is Behavior Profiling stage that responsible for profiling the connected devices to BYOD environment using EMM and NAC. Then, the Intelligent Filtering Stage which in charge of abnormal behavior detection, reprocessing abnormal devices and forward the normal devices to ACSM. Moreover, the authors showed that K-Mean Clustering Algorithm is sufficient for profiling normal and abnormal devices and preventing the abnormal mobile devices from accessing BYOD environment. Through preliminary experiments on four cases of dataset gathered from GaTech, the researchers proved how powerful is their solution in profiling the devices according to the protocol type and in detecting normal and abnormal behavior. However, different IAT values not always be an indication for abnormal behavior.

A system for detecting abnormal behavioral in BYOD based Web Usage patterns.

In this study [8], the researchers proposed a method to detect abnormal use behaviors through patterning the information based on the characteristic of the users. This method aims to detect the abnormal use of service behavior after the employee access the corporate network normally. Then, they indicated that their solution applies agent-less method and Browser Fingerprint technology. They stated that their approach is composed of three systems the first for classifying the users, the second for detecting and patterning the third part for controlling the system. In addition, they clarified that to detect abnormal behavior they used the behavior analysis along with two patterning methods. By using the results of behavior analysis, the authors proved that detecting abnormal use behavior method is working properly as long as the analyzed data are from the same access condition.

IV. Proposed Solution

As discussed in the literature review (see section III), RMS Framework [6] is an approach that aims to provide secure BYOD environments. By isolating the enterprise side from the employee (BYOD) side, BYOD side only includes the employee's applications, personal data along with VNC client application which allows the employee to get access to the company's network. Through accessing a virtual OS, the user can perform the asked tasks. As a result of this isolation, RMS preserves the data confidentiality because even in case of device loss the data will not be affected since the corporate data stored in the enterprise network. However, the data are not totally preserved since it could be stolen through screen shots.

In this paper, we propose Secure Remote Mobile Screening (SRMS) framework which is an enhanced version of RMS that overcome the limitation of the ability of the employees to steal the corporate date through taking screenshots. Figure 1 shows the enterprise side, Figure 2 represents the employee side.

V. Implementation

A. The Enterprise Side:

For building the enterprise side as Figure 1 shows, we used: VirtualBox [9] to runs Linux operating system to host Android x-86[10] as guest MOS (Mobile Operating System). On the top of virtual android, we download VNC Server for android (Alpha VNC Light) remotely while keeping the employee's device free from any kind of corporate data. [11] this application allows the clients to access the corporate data and applications to perform the work.

B. . The Employee Side:

On the other hand, in the employee side as represented in Figure 2, we employ Android Studio [12] to modify Android VNC Viewer in order to enhance the security by adding some codes to prevent the users from taking screenshots to save the corporate's data. Moreover, to establish the direct connection, we add the following information to the viewer source code: add-on code from VNC developer account [13], the server public IP address, the TCP port number. Also, we configure the firewall of the VNC Server computer to give an exception for the VNC. Also, we configure the router of VNC Server to forward port 5900.

VI. Testing

For testing our framework, we used a Galaxy note4 (API 6) to run the employee side and we used windows 10 ASUS laptop to run the server (enterprise) side. We performed a usability test in order to identify if there is any problems or errors and to know how much the solution is efficient. Table 1 shows the usability test observations.

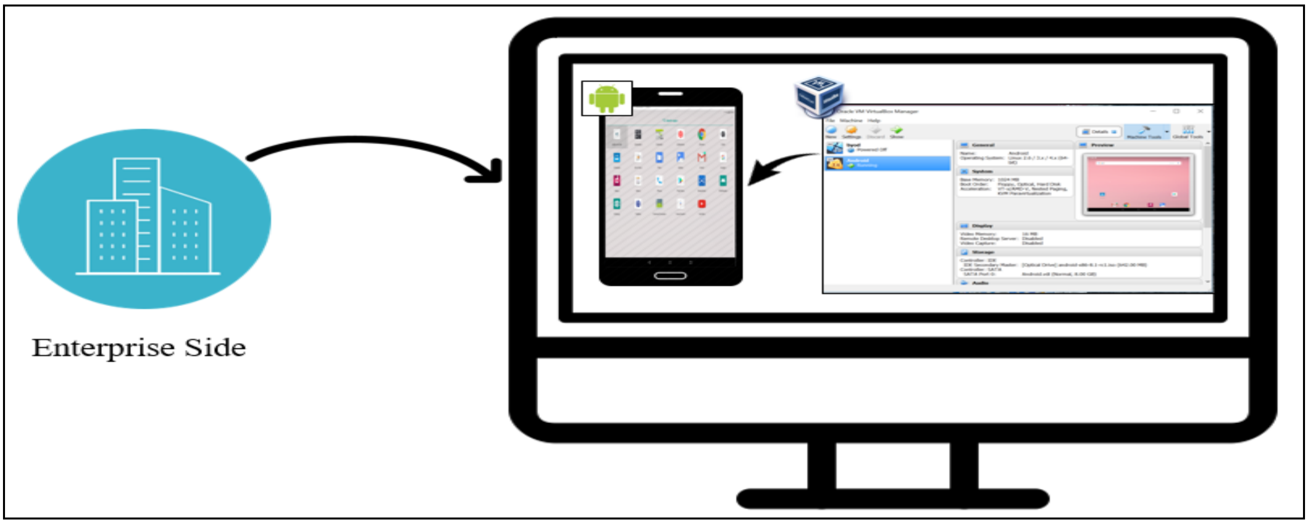

Figure 1 Enterprise Side

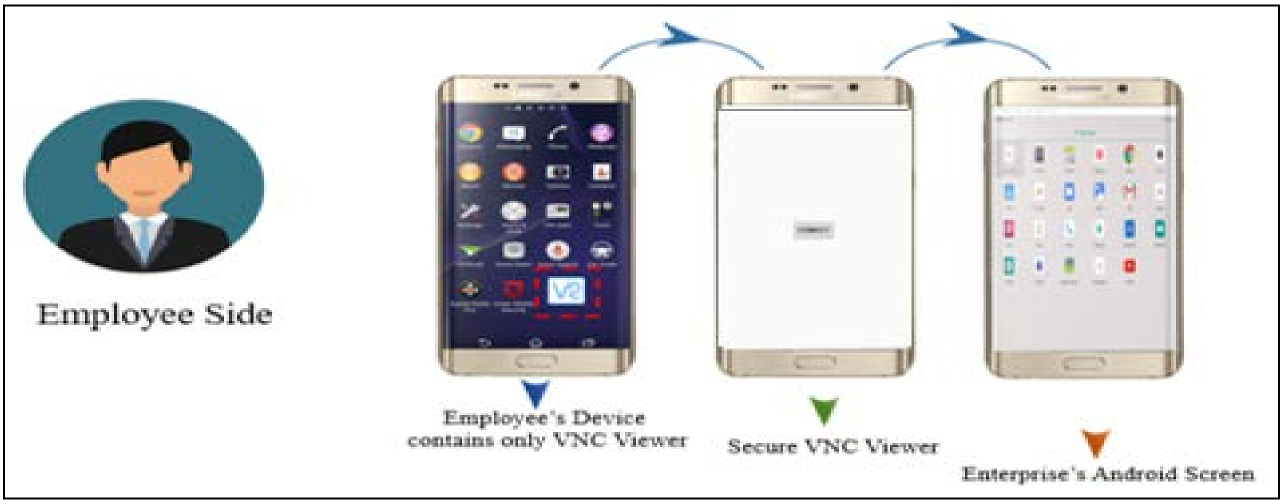
Employee Side
Employee's Device contains only VNC Viewer
Secure VNC Viewer
Enterprise's Android Screen

Figure 2 Employee Side

VII. Results

After implementing the framework, the new VNC client is blocking the user when he/she try to take a screenshot of the corporate data a warning message will be appear to the user that says:" Unable to capture screenshot. Prevented by security policy". Moreover, if the user tries to record his/her mobile screen using a screen recording application, the recording process works properly till the user open the new VNC Viewer, then the recorded screen become black empty screen. However, it suffers from some connectivity issues. Moreover, the proposed solution has some limitations for instance, VNC Viewer was developed only for android users, Also, it accepts only direct TCP connection by inserting the IP addresses and port numbers.

Table 1 Usability Test Observations

Tasks	Observations
1. Take a normal screenshot.	All the users failed to take a screenshot and received a warning message that says: " Unable to capture a screenshot, Prevented by security policy"
2. Take a screenshot using Mobizen application [14].	When pressing the capture button, a black empty screen will be saved in the phone screenshot photo folder.
3. Record the Screen using Mobizen application [14].	All the users could not record New VNC Viewer screen. When the user opened New VNC Viewer app, Mobizen is recording an empty black screen.
4. Use a DU recorder application [15] to record the screen.	When the users used DU recorder app, the app is recording only an empty black screen rather than New VNC Viewer.

VIII. Conclusion

In this research we have presented BYOD phenomena, its advantages and some of the security issues that may face BYOD enabled companies. Also, we provided a literature review for some of the previous research related to improving BYOD security. Then, we proposed a framework that adjust RMS [6] to provide the ability to block the user from stealing the corporate data through taking screenshots or recording the screen using recording application. The future work includes improving the connectivity between the viewer and the server, provide New VNC Viewer for IOS users.

References

[1] Ketel, M. and Shumate, T. (2015). Bring Your Own Device: Security technologies. SoutheastCon 2015. DOI: 10.1109/SECON.2015.7132981

[2] Flores, D., Qazi, F. and Jhumka, A. (2016). Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information. 2016 IEEE Trustcom/BigDataSE/ISPA. DOI: 10.1109/TrustCom.2016.0169

[3] Zahadat, N., Blessner, P., Blackburn, T. and Olson, B. (2015). BYOD security engineering: A framework and its analysis. Computers & Security, 55, pp.81-99. DOI:10.1016/j.cose.2015.06.011

[4] Gudo, M. and Padayachee, K. (2015). SpotMal. Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists - SAICSIT '15. DOI: 10.1145/2815782.2815812

[5] Titze, D., Stephanow, P. and Schutte, J. (2013). A Configurable and Extensible Security Service Architecture for Smartphones. 2013 27th International Conference on Advanced Information Networking and Applications Workshops. DOI: 10.1109/WAINA.2013.83

[6] Ocano, S., Ramamurthy, B. and Wang, Y. (2015). Remote mobile screen (RMS): An approach for secure BYOD environments. 2015 International Conference on Computing, Networking and Communications (ICNC). DOI: 10.1109/ICCNC.2015.7069314

[7] Muhammad, M., Ayesh, A. and Zadeh, P. (2017). Developing an Intelligent Filtering Technique for Bring Your Own Device Network Access Control. Proceedings of the International Conference on Future Networks and Distributed Systems - ICFNDS '17. DOI:10.1145/3102304.3105573

[8] Kim, T. and Kim, H. (2015). A system for detection of abnormal behavior in BYOD based on web usage patterns. 2015 International Conference on Information and Communication Technology Convergence (ICTC).DOI: 10.1109/ICTC.2015.7354798

[9] Oracle VM VirtualBox. Oracle. [Online]. Available at: https://www.virtualbox.orgAndroid x-86 [Online]. Available at: http://www.android-x86.org/

[10] Alpha VNC Lite [Online]. Available at: https://play.google.com/store/apps/details?id=de.abr.android.avnc&hl=ar

[11] Android Studio [Online]. Available at: https://developer.android.com/studio/

[12] VNC Developer [Online]. Available at: https://www.realvnc.com/en/developer/

[13] Mobizen Application [Online]. Available at: https://www.mobizen.com/

[14] DU Recorder [Online]. Available at: https://du-recorder.ar.uptodown.com/android