CHAPTER IV

RESULTS AND DISCUSSION

4.1 Introduction

In the previous chapter the methodology stages has been discussed to achieve the main aim of this research. This chapter presents the findings of this research. The purpose of this research is to propose BYOD security framework. The findings in this research include the proposed framework to secure BYOD and an interview findings which is conducted to evaluate the framework by number of experts from IT department.

4.2 BYOD Security Framework

Based on our evaluation of previous approaches on BYOD security, we are able to address the issue of BYOD security and create security framework by combining each concepts in the previous works into BYOD security framework consists of two layers. The idea of using two layers is to make the framework easier to manage and more reliable in the event of system failures.

BYOD security framework consists of two layers security control which is Device Control and BYOD Server as shown in Figure 7. Layer one is Device Control tier which located on the physical device itself. Device Control tier includes Device Profiles and Light Anti-Malware scanner. Layer two is BYOD Server tier, this tier consist of User Control and Applications

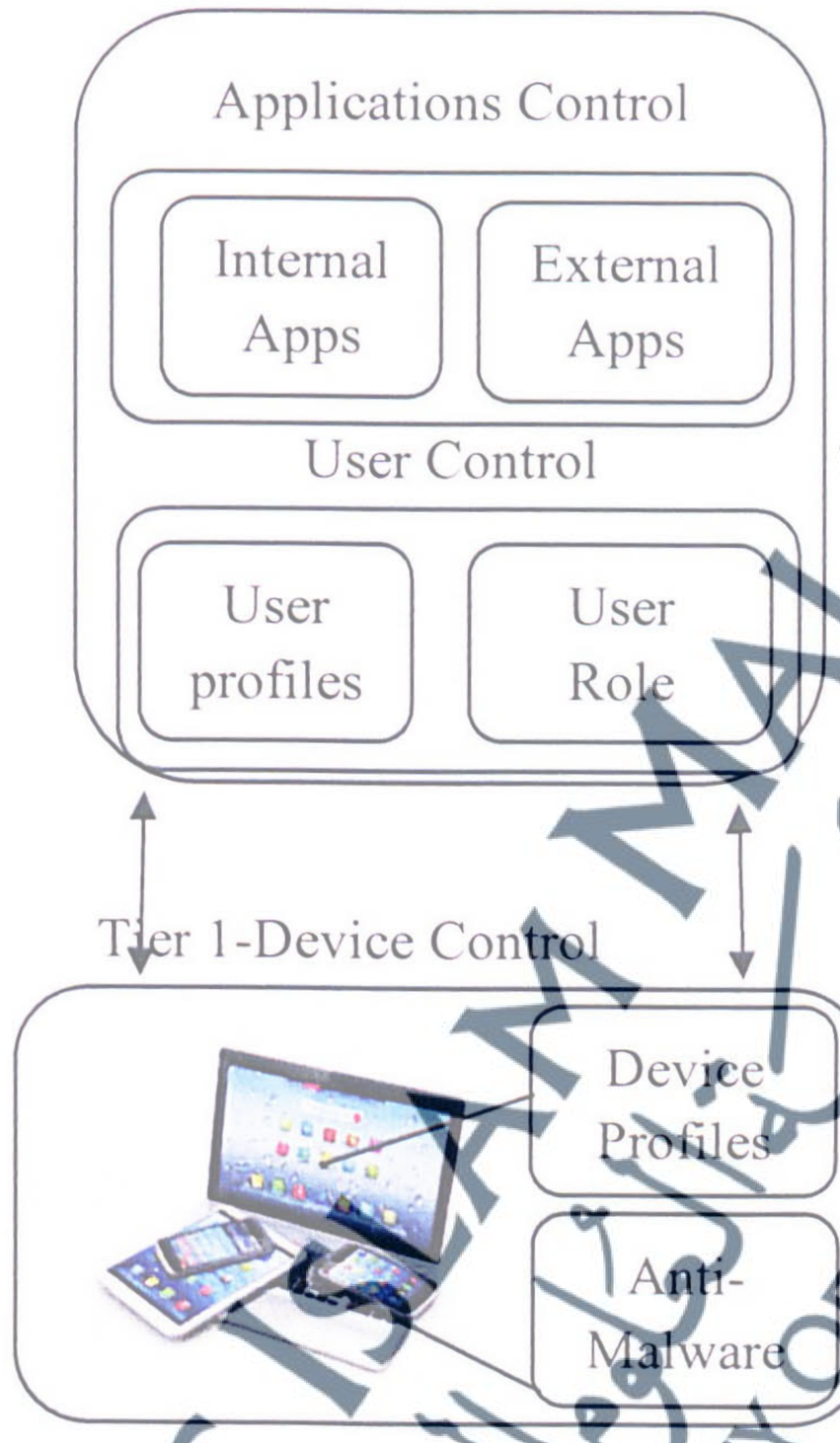

Figure 7: BYOD Security Framework

Control. Within User Control are User Profiles as well as User Role. Applications Control includes Internal Applications and External Applications.

- Tier 1 Device Control

The control mechanism of the device is located in this layer to promote the security. This layer contains of two main aspects: Device Profiles and Light Anti-Malware scanner.

1-Device Profiles: Each device has a set of profiles, each of their have specific set of permissions, setting, applications and resources. These profiles

cannot interact with each other in any case. The user also cannot adjust any of these setting without authorization. Each profile has special set of formulated rules to follow. These rules formulated based on current location of the device and the time of day. For example, a device should be in the "Work" profile whenever the current location is "ABC Building", or the current time is between 10am-6pm. Device profiles also dictate the regularity of device scans for malware or any other malicious activity. Device belonging to a more high-risk employee are scanned much more often than one with a lower risk.

2- Light Anti-Malware: Majority of personal computers and laptops come equipped with some type of anti-virus/malware software. In these devices, many resources are easily available; while it is not the case in smartphones. Although these devices have seen more powerful in recent years, they are still far compared with PCs in sides of processing power and battery life. For this reason, BYOD security framework performs a Lightweight anti-virus\malware scanner on each device. The function of this scanner is scans the vital parts of the device only, such as the kernel of the device or system files. The employee can activate the scanner if he feels his device has been compromised or is acting suspiciously, also when required by an administrator.

- Tier 2 BYOD Server

The management system for BYOD security framework is located in this tier. This tier contains of User Control and Applications Control. Within User

Control are User Profiles and User Role. For Applications Control are Internal Apps and External Apps.

1- User Control: This part controls the user access based on user condition and level of user authorizations in the organization. Each user has specific authorization level based on his role in the organization. User Control system includes User Profiles and User Role.

A) User Profiles: User profiles are directly dependent on the situation of the user inside organization. Where it is not possible for the user to change this situation. These profiles associated with some of the formal process of the organization such as issue and cancel the user permissions.

B) User Role: Access control should be restricted to the user based on his role and job description. There are different levels for the user authorizations can be used to classify the user. Depended on this classification, the organization can be imposed strict restrictions and severe control on the devices. This part provides several levels that can be used to classify the user category based on user role and his job description inside the organization :

1- Standard User: The standard user is an average employee who may have been in the organization for few times and understands the basics of security policies of the organization through training process. This employee would be subject to normal device scans via anti-malware scanner. For the access permission this employee

is given limited access to data and very limited access outside organization premises.

2- Advanced User: The advanced user is a trusted employee who may have been in the organization for an extended period of time and has at least basic to advanced security policies of the organization. This employee would be still subject to device scans. This user has more permission to access to the data than standard user and limited access to sensitive data.

3- Super User: The super user is a highly trusted employee and have advanced security knowledge towards security policies of the organization. The administrator of the organization fall into this category. This user has unrestricted administrative permission to access most if not all aspects of the BYOD Server center. The device of this user also has unrestricted access to sensitive data. For this reason, this user's device should monitor more than other devices, for instance, this device should have a pin number and smart card to access the device.

4- Untrusted User: An untrusted user is user who does not have any permission to access to the organization network using his device, and will be considered unauthorized user until a proper vetting of the device has occurred. This user level will be applied on any device that has been stolen and suspected devices as well.

2- Applications Control: The applications control system for BYOD framework is located in this part to promote the security level in the organization. This part contains of Internal Apps and External Apps control system.

A) Internal Apps: The idea of set up the internal apps comes from that the employee in the organization have only be doing specific tasks based on the place and the time when they are using their device. For instance, during work hours, an employee should only be accessing internal apps related to work. On the other hand, an employee should not be viewing confidential resources related to work at home.

B) External Apps: For external apps, also the permission to access is based on the place and the time when the employees used their device. During working hours, an employee should not be accessing unrelated materials online on their device such as playing games and chatting. Whereas it allow access to external apps during non-working hours.

4.3 Evaluation of BYOD Framework

In this section the evaluation conducted from interviews will be presented. After each section of evaluation, it will be analyzed and discussed in relation to the academic literature.

4.3.1 BYOD Usage

Using personal mobile devices for work purposes is very recommended and supported from all interviewees with the following findings:

1- Using BYOD for work can increase the productivity and efficiency.

2- BYOD policies must be set carefully to prevent any emerging attacks.

3- BYOD policies must be set by administrators only.

4.3.2 Device Profiles

Configuring mobile devices profiles is important for implementing BYOD at work place, the research finding about setting devices profiles are as following:

1- Setting up devices profiles could enhance the BYOD security.

2-All mobile devices must be registered and configured properly to be used at work place.

3- For more security levels, employees cannot change any profile settings without prior permission.

4- Profile setting should be set according to using rules based on location and time.

5-For privacy issues, devices profiles must be configured according to work environment only.

4.3.3 Anti-Malware Scanner

Installing and using anti-malware scanner on mobile devices is very important for implementing BYOD framework as the research results come with the following findings:

1- Mobile devices such as smart phone must install anti-malware scanner to prevent any mal-ware attacks.

2- Anti-malware scanner must be functioning at least the vital parts of the device.

3- BOYD admins must be sure about using the suitable anti-malware scanner in terms of price and performance.

4- BOYD admins must be sure about anti-malware scanner update.

5- Anti-malware must be configured to perform full scan of the devices periodically.

4.3.4 User Profiles

One of the user control variable is a user profile, which is located in BYOD server tier. The study results figure out the following findings:

1- Setting the users profiles is important to improve the BYOD security.

2- Users profiles can be used to define different levels of authentications.

3- Users profiles can provide specific authorization levels for specific users.

4- Only admins can set and configure the users' profiles.

5- Users' profiles must be set according to users' roles. Users' profiles can be used to monitor the users' activities for security and enhancement purposes.

4.3.5 User Role

User roles is the second variable of user control that can be used to classify the users in the organization in terms of implement BYOD framework, the results come out with the following findings:

1 -User roles must be used to specify the user activities.

2 -User roles must be set according to the user job descriptions.

3- Setting users' roles properly can help to increase the security level of BYOD system.

4- Four users classification can be defined as following table:

Standard user	**Advanced user**	**Super user**	**Untrusted user**
-This user should have limited access to organization data. -This user understands the basics of security policies. -This user should be subject to normal device scan by anti-malware scanner. -This user must have very limited access outside organization.	-This user is a trusted employee. -This user has at least basic to advanced security policies. -This user would be still subject to device scan of anti-malware scanner. -This user have more permission to access organization data. -This user may have limited access to sensitive data.	-Highly trusted user. -Has advanced security knowledge about security policies. -Can be the organization administrator. -Super user can be the admin of the BYOD server. -Can access all data and resources. -The super user's devices can monitor other users' devices.	-He/she does not have the permission to access the organization network using his/her device. -This user role normally apply to stolen and suspected sevices.

Table 10: User Classification

4.3.6 Internal Apps:

Internal apps is one of two variables of application control in the BYOD framework, they must be configure to apply more security to BYOD system. The following is the study results about using internal apps:

1- Using internal apps must be controlled.

2- Internal apps must not be used outside the organization unless right permission applied.

3- Using Visual Private Network (VPN) can be a good choice to allow using internal apps from outside the organization.

4- If necessary, the permission of using internal apps outside the organization should be given to trusted and super users only.

5- For more security, authorized user shouldn't access confidential data and resources outside the organization.

4.3.7 External Apps:

Internal apps are the second variable of the application control in the BYOD framework. The following is the study results about using external apps within the BYOD security framework:

1 -External apps must be controlled in terms of time and place.

2 -Apps such as games and chatting are forbidden.

3-Admins may allow specific apps if they safe and do not cause any security issues.

4-For necessary reasons, users may access safe and trusted external apps during working hours using their own internet connection, so this will not affect BYOD security.

4.4 Discussion

The main objective of this research is to propose a security framework for BYOD system in order to implement it within any organization within secure and safe environment in order to enhance and improve the productivity and efficiency of the organization.

In order to evaluate the BYOD security framework, interview method has been held in order to collect important data from IT experts and then analyzed using qualitative analysis methodology and the results come out with the following summary:

At the device control layer (tier 1), which is consists of two security elements (device profiles and anti-malware scanner), the control of devices' profiles will provide high level of security by defining the allowed devices to access the BYOD system. On the other hand, using anti-malware scanner will keep tracking the devices for any malicious apps or scripts.

So, at this point, the system insures that all devices that login to the system are authorized and clean devices.

At the BYOD Server layer (tier 2), which consists of four security elements (user profiles, user role, internal apps, and external apps), the proposed framework makes sure that user profiles will be set up carefully in order to prevent any misuse of any data or resources by any unauthorized user as the system admin configure each user profile according user role to define user level and allowed activities.

On the other hand, user role can be used to specify 4 different types of users (untrusted, standard, trusted, and super users) as each user type has different level of security which allow to access the resources according to users' permissions.

As a result, users' profiles and users' role will provide the required security to access the organization data and resources.

In addition, the use of internal and external apps is very important security challenge as the use of internal apps consider as main gates to the organization data and resources, also using external apps within the working hour could cause many security issues. Internal apps must be controlled to be used according to users' roles. Implementing of VPN and applying the right permission could be a good choice to provide the required security to access internal apps from outside the organization.

External apps must not be used within the organization to avoid and unexpected security issues.

4.5 Summary

This chapter presented the main findings of this research. First section presented in details the proposed framework which is the main aim of this research. The purpose of this framework is to present a solution to the "Bring Your Own Device" problem in businesses through control the user access coupled with device control, anti-malware scanners, user profiles, user role and applications control. Second section showed the interview findings which is conducted to evaluate the proposed framework.