Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 511 – 516

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Modifying security policies towards BYOD

Vignesh.U, Asha.S

* *Vignesh.U, VIT UNIVERISITY-CHENNAI,INDIA*
**Asha.S, VIT UNIVERISITY-CHENNAI,INDIA*

Abstract

In the IT Consumerization phase, the organizations permit their employees to bring their personally owned device to workplace. This is achieved through enforcing policy or agreement - Bring Your Own Device. The BYOD policies adopted in numerous organizations are vague and generally immature. The prevailing security policies in BYOD are no more supportive for mobile devices like smartphones, tablets and laptops. The security policies must be modified to suit these devices. To mitigate this downside, 3-tier enhanced policy architecture is proposed which specifies the policies to be followed by the device, applications and organizations.

Keywords: Bring Your Own Device (BYOD), security policies, IT Consumerization, mobile device.

1. Introduction

The BYOD refers to Bring Your Own Device to workplace for official use. This was developed due to consumerization in IT. The term Consumerization refers to growing rate of Information Technology which was initially in the consumer market and later shifted to business and educational institutions. The purpose of this policy is to use the device for both office and personal use. The employee owns the device and supported financially and technically by the organization. The devices can be smartphones, tablets and laptops. However, there are issues in securing devices from network related attacks. Since sensitive data on organization and personal data are present, the device must be secured from such attacks. The BYOD policies are developed to protect the sensitive data in the devices.

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.023

2. WHY BYOD?

BYOD is now a growing trend according to surveys made by different organization and IT companies. The employees prefer working with their own device rather than the company's device. They feel comfortable to work with their devices which increase their efficiency and productivity. BYOD increase the mobility of devices and work can be completed from any geographic point. This will make the organization to extract work from the employees irrespective of their locations. Simplified infrastructure is required for wireless devices which save cost for the organization. It is now an easy task to establish a workplace using BYOD policy. The organization can cut cost in providing machines to the employees. This will reduce the IT management troubleshooting and support costs.

A recent survey [1] by Intel performed on many organizations about benefits of BYOD for IT and as follows.

- 28% improved efficiency and productivity
- 22% improved worker mobility
- 17% saving on inventing in new machines
- 9% job satisfaction and retention
- 6% reduce IT management/troubleshooting

The survey reveals the reason for IT and other organization shifting towards BYOD.

3. Security Concern

Many queries arise once it involves security. What if the device is stolen? The device containing the sensitive information about the company may be lost or stolen which is a serious issue. What if the worker leaves the organization? The employee signed up for BYOD policies have device supported by company financially and technically may leave the company for different reason. This will raise the question about the device ownership. Who owns the data in the mobile devices? There may be information about the company in the personal device. The data ownership problem arises when the data is been stored in the mobile device. What devices can BYOD policies support? The employees may prefer bringing different products running on different operating system. These heterogeneous devices may or may not be compatible to the organization. What if data are accessed in public/untrusted network? The data will remain safe when accessed from the home network. There are chances of network attacks like eavesdropping, man in the middle attack when accessed from public networks or mobile networks.

A recent survey [2] by SAANS Analyst Program performed on many enterprise organizations (i.e. more than 1,000 employees) about criticality of Mobile Security Policy have identified 97% of organization feels BYOD policies are important.

- 37.1% believe critical
- 40.0% believe extremely important
- 19.7% believe important
- 0.7% feel unimportant
- 2.6% don't know

But the question is do they actually follow the BYOD policy. According to the survey by SAANS Analyst Program, 36% of the organization has no formal BYOD policy. 23% of the companies do not permit personal devices and 14% of organization informs their employees to secure and monitor their own devices.

The rooting or jailbreak devices are capable of using operating system with administrator permission. These types of devices are not so wide and it is lesser than 2% available in the industry but this must be looked seriously. The rooted devices are capable of installing unauthorized application which may display spam and send anonymous

data about the device. The mobile number used in the device must be verified so as to confirm that the employee is the owner of the number. The smartphone devices may be password protected and secured. This will make the smartphone secured physically. Memory slots are available in these phones containing memory cards. The external memory cards may be stolen which results in data breach easily. There are some compatibility issues when devices working on different operating system. This issue must be solved to make the choice of devices flexible.

There are many trivial and unorganized solutions for the security issues. Strong passwords are recommended to lock the devices which provide to the security. Virtual desktops are replaced to stop the device saving the data in the device. This will make employee to work only online. Offline work is not possible when virtual desktops are used. Mobile Device Management that assist the device owner to change the passwords periodically and remote wipe when entered passwords incorrectly. The productivity of the employee decrease with the increase of security constraints.

4. Model

There exist different security solutions for BYOD in various organization which deals only for specific domains in the companies. The policies followed by different organizations are vague and unorganized. The BYOD security policies proposed is a multilevel security policy. Increase in the security should not reduce the security. This model is designed to include the policies required for implementing effective BYOD without compromising the productivity. Figure 1 shows the multilevel security policy in BYOD. The multilevel security policy is made up of three levels – Organizational level, Application level and Device level policies.

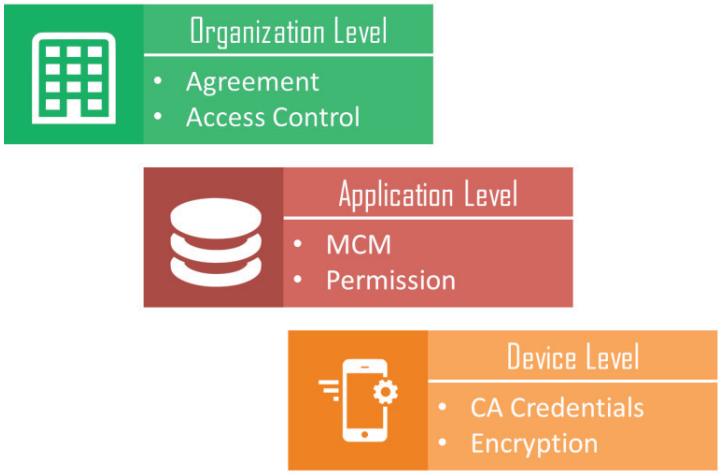

Fig 1: Multilevel Security Policy

Level 1 – Organizational Level

The organization should consider this level before signing an employee in BYOD policy. The organizational level policies are a checklist to see before implementing BYOD in the organization. A BYOD agreement recommended checklist: Clarify the responsibility for device support, maintenance and costs; Make sure the users are responsible for backing up their personal data; the employees must remove apps in the device on the request of the organization; The Employee should not use the rooted or jail-broken devices; And explain the consequences for any violations to the policy.

Access Control must be restricted to the employee based on their grade and job description. The fingerprint mechanism is used to register the devices and the devices not registered won't gain to the company's network and information. All the employees in the organization don't need to bring their personal device for work. This part provides a few suggested profiles that can be used to classify the employees.

1. Standard User: The Standard User would be a basic employee who may have been with the organization for a

minimum amount of time and understands the basics of security as defined by an organization in the training process. This employee would be subject to bring the device to work and can gain access to company in his company networks. The company may limit the access outside the company premises.

2. Advanced User: The Advanced User is a trusted employee who requires device to be used in the workplace and home. The employee can access the company information from the public networks but access to sensitive data is denied to this user. His device profile will allow similar access at work and home in terms of capabilities and privileges.

3. Professional User: A Professional User is one who has advanced security knowledge and is a highly trusted employee. A system administrator or the head of the company fall into this category. They have privileges to access any information in the company from the home network or untrusted network. VPN and cloud services are used to access sensitive information of the company. This user's device should be monitored more closely because of its high privilege.

4. Guest User: the Guest User is a new user to the network. These devices won't have any access to the organizations network using their device until it is registered to the company's network. The device cannot used to access the company's information until the device is fingerprinted and verified.

Level 2 – Application Level

This level provides security in the form of mobile applications. The smartphones are monitored by application and assist the user in securing the devices. Such an application in the mobile device is known to be Mobile Device Management. There are many vendors like AirWatch, Codeproof, dell and lookout which provides mobile Device management. The MDM security approach is based on three basic actions: control, monitor and protect [3]. The Company's server can be configured and accessed from these applications. The Mobile Device Management supports full device control like lock down, control, SSL connection to the server, remote wipe, siren, signal flare and personal data backup and enforces policies even on mobile devices. MAM Mobile Application Management similar to Mobile Device Management is use to control specific application in the device. The applications monitored are enterprise applications which can be monitored closely and locked down. The Mobile Application Management is not reliable since it doesn't provide complete protection to the mobile devices. The MDM should include MCM Mobile Content Management which is most important when handling sensitive information in the devices. The Mobile Content management is used to secure the data present in the smartphones, Tablets and PDA'S. The data can be encrypted and stored in device. If I device is stolen, the data cannot be retrieved. Location based lock can be applied using GPS. The data can be decrypted and accessed only at a specific geographic point like workplace and at home. 2-step verification can be done to access the data. First step to prompt for a password and second step to prompt for a token number sent to the mobile number owned by the user. This will increase the security and solve the number ownership problem.

There should be external encryption software to encrypt the external memory card. Whenever a user install an application from marketplace or app store, the application request permission to access some features in mobile such as

- Account details
- Application Information
- Phone calls
- Network Communication
- Sync Settings
- System Tools
- Location
- Camera
- Bookmark and Web history
- Storage

The above credentials are sensitive and some applications request access to these credentials which makes the device highly vulnerable to attack and the details about the device can be leaked without the user's knowledge. The Mobile Device Management should monitor and restrict the application to be installed. These applications can be

malware and the data can be stolen from the devices through the network. The Mobile Device Management must warn the user before installing such applications on the mobile devices.

Level 3– Device Level

Most of the organizations leave the device level security policies and assume that it is dependent on the owner and the manufacturer of the device. Some device level policies are Certificate authority, data encryption, multiuser and rooting issue. Now, every smartphone comes with preloaded trusted Certificate authority credentials such as American online, COMODO, thawte, verisign, VISA and much more. These credentials were hidden in earlier versions of smart phone. In the latest smart phone these credentials can be managed. The user can add new certificates and remove existing certificates. Removing a certificate will make the user work online in untrusted network. There are chances of adding fake Certificate Authority to the smartphones which get the details of the user and data breach occurs. If the Certificate is hacked, there are chances of accessing the device and if the company uses the same certificate, then the hacker can gain access to the server. So, the device has to monitor the CA credentials. The latest smartphone comes with inbuilt encryption application. This will encrypt the data like accounts, settings and apps. But the user doesn't bother to see that option and also it takes several hours to complete based on storage capacity of the device. There are options available to encrypt sd card inserted in it in some smartphones. The jail-break or rooted devices are unnoticed in several organizations. Jail-break or rooting refers to gaining administrative privilege in the smartphones. Similar to Linux, root users are administrators and have privilege to modify the operating system and install any application in the system. If the smartphones are rooted, then the user can install unauthorized application which tamper or leak the sensitive data in the mobile phone. The iphones and android phones are rooted generally. The rooting is made legal in Australia, USA and UK. The organization should prevent the rooted devices to be used in the company as a part of BYOD.

5. Conclusion

In this paper, the solution for "Bring Your Own Device" problem is modifying modified security to adopt for mobile devices. The modified security policy is the integration of necessary security policies for Bring Your Own Device with enhanced features to increase the security level without compromising the productivity. By adopting the three levels of security policy: Device level, Application level and Organization level; the level of security has increased and the organizations are in the safe zone while using BYOD. The devices are upgrading every period of time and different features are made available in the smartphones. The organization should change their trivial security policies and adopt the enhanced security policies to suit the mobile devices.

REFERENCES

[1] http://www.intel.com/content/www/us/en/mobile-computing/consumerization-enterprise-byod-peer-research-paper.html

[2] Kevin Johnson and Tony DeLaGrabge; "**SANS Survey on Mobility/BYOD Security Policies and Practices",** SANS Analyst Program.

[3] Scarfo, A; "**New Security Perspectives around BYOD**", Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International, Page(s): 446 – 451.

[4] http://www3.hp.com/t5/Following-the-Wh1t3-Rabbit/Hacked-Certificate-Authorities-When-there-is-Nothing-Left-to/ba-p/5323869#.UoLdrbTtfsQ

[5] Sean Chung, Sam Chung, Escrig, T, Yan Bai and Endicott-Popovsky,B.; **"2TAC: Distributed Access Control Architecture for "Bring Your Own Device" Security**" BioMedical Computing (BioMedCom), 2012 ASE/IEEE International Conference, 2012, Page(s): 123 – 126.

[6] Lennon, R.G.; "**Changing User Attitudes to Security in Bring Your Own Device (BYOD) & the Cloud**" Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania, 2012 , Page(s): 49 – 52.

[7] Miller, K.W., Voas, J. and Hurlburt, G.F.; "**BYOD: Security and Privacy Consideration**" IT Professional, Volume 14, Issue: 5, 2012 , Page(s): 53 – 55.

[8] Benedikt Lebek, Kenan Degirmenci, Michael H. Breitner.; "Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices" AIS Electronic Library (AISeL).

[9] Kendall, R. A., Sosonkina, M., Gropp, W. D., Numrich, R. W., & Sterling, T. (n.d.). Parallel Programming Models Applicable to Cluster Computing and Beyond.

[10] Moscovich, E. (2012). Big Data for Conventional Programmers. Retrieved From http://www.ca.com/~/media/Files/About%20Us/CATX/big-data- forconventional-programmers-moscovich.pdf

[11] Nieuwpoort, R. V., Wrzesinska, G., Jaacobs, C. J., & Bal, H. E. (n.d.). Satin: A High-Level and Efficient Grid Programming Model. *ACM Transactions on Programming Languages and Systems*, *10*(10), 1-40. Retrieved from ACM 0164-0925/20x/0500-0001

[12] Simonet, A., Fedak, G., & Ripeanu, M. (2012). *Active Data: A Programming Model for Managing Big Data Life Cycle* (1). Retrieved from informatics mathematics website:http://hal.inria.fr/docs/00/72/90/02/PDF/RR-8062.pdf

[13] Thusoo, A., Sarma, J. S., Jain, N., Shao, Z., Chakka, P., Zhang, N., Antony, S., Liu, H., & Murthy, R. (2010). Hive? A Petabyte Scale Data Warehouse Using Hadoop. *IEEE*, 996-1005. Retrieved from 978-1-4244- 5446-4/10

[14] Tomasic, I., Ugovsek, J., Rashkovska, A., & Trobec, R. (2012). Multicluster Hadoop Distributed File System. *Mipro Croatian society*, 301-305.

[15] Yang, X., Liu, Z., & Fu, Y. (2011). MapReduce as a Programming Model for Association Rules Algorithm on Hadoop.

[16] Yang, G. (2011). The Application of MapReduce in Cloud Computing. *International Symposium on Intelligence Information Processing and Trusted Computing*, 154-156. doi:10.1109/IPTC.2011.46