International Journal of Engineering Innovation & Research
Volume 2, Issue 2, ISSN: 2277 – 5668

An Approach to Implement Bring Your Own Device (BYOD) Securely

Mr. Vishal Gupta, Deepak Sangroha, Lovekesh Dhiman

***Abstract* – BYOD (Bring Your Own Device) is a business policy to allow employees to bring their own devices at their work. The same device is used in and out of the corporate office and during outside use, it may be connected to insecure internet and critical corporate data become public. This can be a big threat to the office as well as business strategies and future policies are derived from this data.**

In this paper an approach is explained to guard against this type of threat and to secure the corporate data even outside the corporate premises.

***Keywords* – BYOD, Business Strategies, Security, Threat.**

I. INTRODUCTION

Vodafone techies say:

"The growing pace of consumerisation of IT means that employees are having a greater say in the technology that they use in the workplace, including their own devices. [1]"

Means, the fast growing IT world have a vast range of IT means that can provide better availability, accessibility, mobility and also cost saving to industry. Devices like smartphones; tablets etc. give the employee options to access their work tool or stuff anywhere in their organization. This is what BYOD is, bring your own personal devices and access your work utilities anywhere in office premises (i.e. wherever companies' wireless network available).

[4]Here we must understand the difference between accessing the wireless network as a guest and BYOD. In first one, the user use the wireless network to access the internet in general, but in second one, the employees use the wireless network to access their work tools which contain critical information about their organization, network infrastructure etc.

For example, BMC remedy is an IT management tools works with ARS (Action Request System) to perform tasks and troubleshoot Incidents regarding network devices, servers. In this way it contains a lot of sensitive information related to network infrastructure.

In today's world, we have a variety of mobile devices that can be used not only for entertainment but for work also. In that way they not only increase availability & mobility to employee but also cost saving & productivity for organization as the employee bring their own device and be available whenever business needs them [5]. Thus providing a win-win situation to both employee and the organization. IT means are strong enough to run heavy apps with good processing speed and huge primary storage.

II. SECURITY PROBLEM IN IMPLEMENTING BYOD

Security is the main concern whenever we move towards mobility as the environment changes and so as security policies. In BYOD, employee uses the organization's environment to access critical data and at that movement the data is safe as the organization has its own polices implemented on its security devices [7]. As everydevice have some kind of Operating system which operate on hardware and each OS create some kind of logs, temporary files, history or traces that are stored on the device. Now here is the issue begins, employee uses the corporate network to access internal data and some part of that data is stored in device as logs or in temporary files.

After that employee leaves the corporate network and goes home or any other place where he/she may uses the "Internet" which is highly insecure in nature and poses a huge risk. Every big attack or security breach start with internet by information leaks or some malware installation on devices. Anybody who is connected to internet is never safe. So, when that employee connects to internet, there is always possibility that some threats attack his/her device and get the precious data.

In this paper we have explained an approach to secure that corporate data while providing the flexibility and mobility to employee.

III. SOLUTIONS TO MAKE BYOD SECURE

A. First

First approach is to implement MDM (Mobile Device Management) [6], MDM software is used to secure, monitor, manage and support the mobile devices deployed in enterprises. These tools are becoming the basic need for the wireless networks as they do all operations from beginning to end.

For device enrollment it provides features like connection setup, device registration, and user authentication, restrictions based on platform or version. [9]For security it provides passcode, encryption, and compliance, restrictions based on the use of device features or applications. MDM is able to configure profiles, time-based profiles, certificates, accounts. For maintainability it can be used to monitor the policies, location, alerts, rules etc.

With all these above features, [8]MDM is first thing each organization want to implement, as it makes it a lot easy to handle BYOD concept. There are lots of MDM tools available in market like AirWatch, AmTel MDM,

FancyFon, MobileIron and a lot more [8]. Actually these tools basically focus on maintenance of BYOD devices and have some features of security but good maintenance is the first step for security.

Inspired from MDM a new approach called MAM (Mobile Application Management) has been introduced, which focuses on a particular application rather then whole device. This is much better way for security as the application accessing the corporate data remains in monitoring not the whole device. In this way employee also get some flexibility to use his other application which is not going to interfere with the corporate data as he will not be prompted for authentication each time any other application run.

B. Secondly,

With the same scenario we can use some utility to secure data in and out of the organization [2]. There must be a single way to access the business tools i.e. [9]All business tools must be accessed through this utility. This utility may have web browser like appearance and all the business tools must be assessed within this utility.

For understanding we take an example of Virtual machine which have characteristic to work like an operating system which itself is running on an operating system platform. We don't want our utility to work like a whole operating system but have characteristic to allow some application or business tool to run on it.

Now here is the complete process to work with this utility, first device must support the utility so that it can be installed on the mobile devices. Developer must keep this issue in mind that different devices work with different platform like Android, Windows, or any other proprietary platform. After utility installation the features come into play, this utility first authenticate itself to prove its authorization to access the business tools. Unauthorized user will be blocked to access business tools but may be allowed to continue with their access to wireless network [13]. Secondly, all the business tools are accessed through this utility i.e. instead of installing business tools on the OS; they are associated with this utility. To understand the concept we may use the example of portable browser which is useful in a scenario where temporary data, passwords, bookmarks etc. are stored and kept associated with browser not in the system memory. That's why portable browsers are considered as a secure thing to do Net Banking, Online Money Transactions etc. [11] on a non-personal PC. Now back to our concept, the connection between utility and the business server act like a tunnel which encrypts the data passing through this connection [10]. Another feature of utility is that it won't allow the OS of device to interfere with the data of this utility. In this way the data related to business remain accessible only to this utility and moreover OS or any application can't access the data neither creates logs or any type of temporary file or data, this thing makes it almost isolated from the system. This isolation will help to secure data when the user is outside the business environment and accessing the insecure internet. By doing this we are making our data confidential and in case of exposure encryption will help us to keep our data safe.

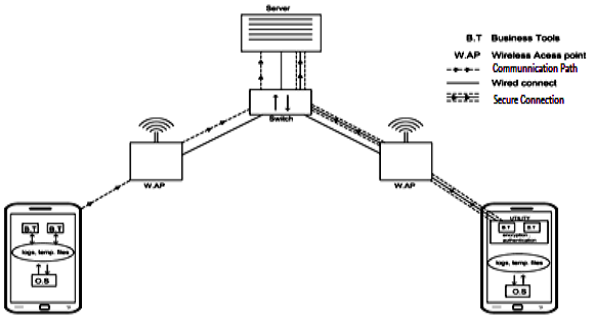

Fig.1. Showing secure access to business tools with utility in right side device.

C. Third

Moving further with 2nd step organization can use some proprietary encryption algorithm instead of Standard algorithm which is to be used in utility. [3]This idea of using proprietary algorithm is just to make it tougher for an attacker to get plain data as he/she needs to first get algorithm and then encrypted data to gain plain text. The algorithm needs not be the competitor of AES or DES, only a little complex algorithm will be enough and secondly it will help the device as lighter algorithm will run faster [6].

IV. Conclusion

BYOD technology is about accessing business data which may be highly sensitive. It's ok if we are using it within organization but the problem arises when data moves outside the organization.

The idea of using separate utility to access business tools gets a strong favor as big IT powers are moving towards web based tools like BMC Remedy. It is available in new web based version of it named BMC Remedy V3 and Service-Now, Summus, Bomgar are also web based tools for Infrastructure Management and Troubleshooting. These web based tools are easy to associate and customize with the utility.

For mobile device management and security here are three steps:

- For maintenance organization must use any MDM tool.
- Use a separate utility with security features and minimized interference with other applications.
- Use some proprietary encryption algorithm to increase complexity and to make it harder to get pain data [3].

REFERENCES

[1] http://enterprise.vodafone.com/insight_news/bring-your-own-device-a-considered-approach-white-paper.jsp
[2] Motorola: White paper BYOD: On-boarding and Securing Devices in Your Corporate network
[3] July 2012 University of Oregeon Factors for consideration when developing a bring your own device(BYOD)
[4] http://en.wikipedia.org/wiki/Bring_your_own_device
[5] http://en.wikipedia.org/wiki/Mobile_application_management
[6] http://www.cisco.com/web/solutions/trends/byod_smart_solution/index.html

[7] https://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf
[8] http://www.cadincweb.com/wp-content/uploads/2012/04/CAD_BRAD_Ten_Steps_to_Secure_BYOD.pdf
[9] http://www.computerworld.com/s/topic/227/Bring+Your+Own+Device+(BYOD)
[10] http://www.whitehouse.gov/digitalgov/bring-your-own-device
[11] http://finance.yahoo.com/news/gartner-says-bring-own-device-144200347.html
[12] http://news.yahoo.com/report-bring-own-device-byod-consumerimization-co-enterprise-103042270.html
[13] http://www.cnbc.com/id/47498441/Bring_Your_Own_Device_Smart_Move_For_Businesses

AUTHOR'S PROFILE

Mr. Vishal Gupta

Assistant Professor AIACTR. He had done his BE (CSE) from Rohilkhand University in 2001, and M-Tech (IT) from GGSPIU in 2006. He is pursuing Ph.D. (CSE) from JMI .His area of interest is Networking and Information security. He is working as Assistant Professor in AIACTR.

Mr. Deepak Sangroha

He Has Done B.Tech., Computer Science From Kurukshetra University, in 2007 and Currently Pursuing MTECH from Ambedkar Institute of Advanced Research & Technologies Guru Gobind Singh Indraprastha University M. Tech., in Information Security.

Mr. Lovekesh Dhiman

He had done his BTECH (IT) From Guru Gobind Singh Indraprastha University in 2008 And Currently Pursuing MTECH IN Information Security from Ambedkar Institute of Advanced Research & Technologies.