

Addressing Security Concerns in BYOD Through Sandboxing

Abhishek Mishra¹ Dhara Vyas² Bhishm Narula³ Dr Radha Shankarmani⁴

^{1,2,3,4}Department of Information Technology

^{1,2,3,4}Sardar Patel Institute of Technology, Mumbai, India

Abstract— A new trend of implementing Bring Your Own Device (BYOD) as an IT policy is being adopted by companies worldwide. It permits employees to bring their own portable devices like tablets, smartphones, etc to workplace and use them to access confidential corporate information while being both inside and outside their place of work. BYOD clearly raises serious security concerns since the device in question is not under the control of the enterprise and is vulnerable to a wide range of security threats. One of the major concerns in implementing a BYOD policy is data security and privacy. By allowing employees to access privileged corporate information on their personal devices, pertinent corporate data may be compromised. In this article, we address this problem and propose a solution that enhances the security in the BYOD scenario without compromising the usability and flexibility of the system. We suggest a sandbox which takes care of common connection, encryption and other security credentials for BYOD applications and helps monitor application usage on device for administrators.

Key words: BYOD(Bring Your Own Device), Virtualization, NAC(Network Access Control), MDM(Mobile Device Management), GCM, Mobile data security, Corporate security.

I. INTRODUCTION

Bring your own device (BYOD)—also called Bring your own technology (BYOT), Bring your own phone (BYOP), and Bring your own PC (BYOPC)—refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to office, and to use those devices for corporate usage through company-owned or independent applications[1]. It has now become a phenomenon and is commonly referred to as IT consumerisation.

Benefits of BYOD include increased productivity as the user is more comfortable with his personal device, in addition to being an expert and thus reducing device navigation time[2]. Additionally, personal devices are often more cutting edge as company technology does not refresh regularly. Job satisfaction improves with BYOD since it allows employees to use device of choice rather than one selected by the IT team. It also saves them from carrying separate devices for work and personal usage. Cost savings occur on the company end because they are not responsible for furnishing employee devices.

Although the ability to allow staff to work at anytime from anywhere and on any device provides real business benefits, it also brings significant risks. Corporate data security is one of the biggest concerns of corporate organizations in implementing a BYOD policy. Permitting employees to access the privileged corporate information and applications on their device can lead to pertinent corporate data being compromised. The problem of corporate data security becomes even more important in

cases when the employees lose their personal device or leave the company.

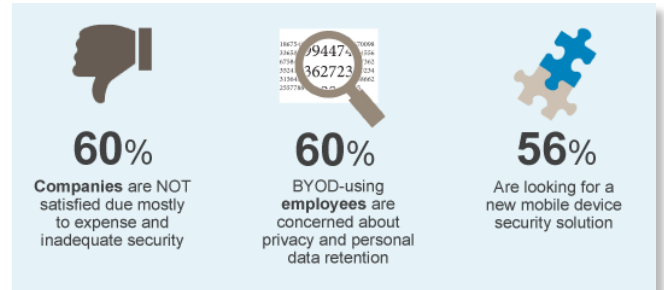


Fig.1: A study of BYOD related opinions

Source: survey.zixcorp.com

An important challenge for BYOD is employee apprehensiveness that companies may spy or track their activities and may have access to their personal passwords, websites and information on their personal device if used for both work and personal use[3].

In large corporate organizations it is almost impossible for the IT department to scale to thousands of employees with dozens of different types of devices, operating systems and platforms. A tough task of quickly analyzing problems and developing patches is associated with diverse devices on the network[4].

BYOD is the indispensable future of IT in any corporate organization because of the immense benefits it brings along with itself. Testimony to this fact is Gartner's recent prediction that by 2017, 50 % employers will require employees to use their own devices for work purpose. Thus it is imperative that we try and solve related security issues to stay on the safer side in future.

II. PROBLEM DEFINITION

Nowadays, there are a number of products in the market that are designed to support BYOD. Some of these are based on virtualization of the device, others offer specialized applications for specific business processes such as emails or VPNs. Furthermore, some products offer remote connections to the enterprise networks. Most of these solutions, however, exhibit the disadvantage that they either require a modification of the underlying operating system/kernel or a rooted device.

In the traditional case, the device being used by the employee is provided by the company and IT officials of the enterprise can make the necessary modifications to the device kernel and Operating System (OS), to enforce that the required enterprise policies cannot be bypassed by employees.

For instance, the enterprise could certify a certain OS configuration and guarantee the correct execution of binaries. But modifying the OS of an employee device is not an appealing solution since it prevents employees from installing updates on their devices, and it requires the

consent of the employee. Moreover, in BYOD scenarios, these solutions cannot be deployed. This stems from the fact that given the device does not belong to the enterprise, the latter does not have any justification in modifying the underlying kernel.

The problem seems complicated when considering possibly untrusted device owners or employees, who may (purposefully or accidentally) alter their device settings to bypass security policies.

For instance, enterprises might be interested in ensuring that sensitive information is always stored in encrypted form on the device, and is only communicated to trusted pre-approved entities, in spite of potential threats caused by malware, malicious applications, etc. Thus, there is a need to secure mobile devices in the context of BYOD without incurring significant changes in mobile device firmware.

III. EXISTING SYSTEMS

A. MDM:

Typical MDM (Mobile Device Management) solutions are client server models where employee's mobile device is a client and the corporate server represents the server for mobile device administration. This is a widely used method and provides complete control of the employee device. All communication between the device and any entity over the network happens through the company server. The primary disadvantage thus, is employee privacy breach[5].

B. Virtualization:

Virtualization solution provides the capability to run a fully virtualized copy of device operating system as a guest on a physical host's handset.

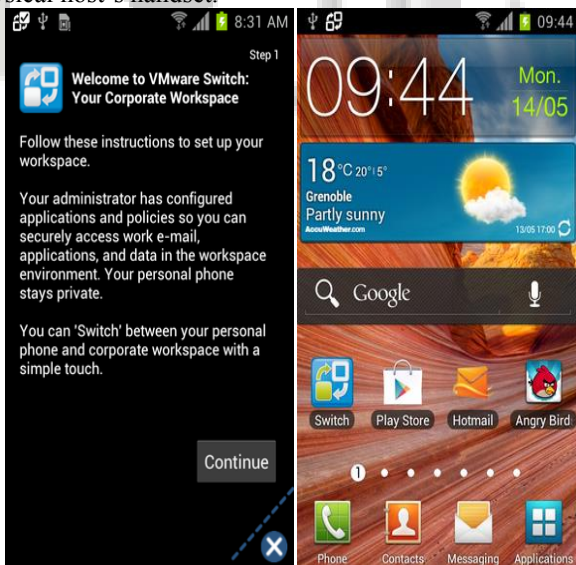


Fig. 2: VMWare virtualisation with a switch widget

Employees can enable their phones to have a handset hypervisor and run a virtual copy of Operating System that's fully managed by IT department of the organization. They fully control the virtual copy, its feel, the applications that can be installed on it, and the other policies.

The virtual machine is fully encrypted with AES 256 bit encryption, and it has a Virtual Private Network at the

backend. Even though concept of Virtualization looks appealing, it has some major drawbacks. Firstly, virtualization is heavy on device memory and leads to significant company costs. Virtualization may not be compatible on low end devices and if the organization decides to stick to a particular virtual copy of an OS, its proper working on different handsets may not be guaranteed.

C. NAC:

Typical NAC (Network Access Control) solutions ensure end point security through a corporate server tracking all network operations performed by devices. This type of solution examines the security status of the mobile device which is trying to connect to the corporate network and if the device meets the security compliance criteria, it authenticates the user to log into the network and determine what they can see and do. The primary disadvantage of NAC solution is that it fails to provide any security for the corporate data residing on the employee's mobile device when the device is not under the organization's vicinity and disconnected with the corporate network.

IV. PROPOSED SYSTEM

In contrast to existing systems in the market, we propose a solution that would enable the organization to achieve a balance between security of corporate data, device usage flexibility and privacy of employee's data. Our proposal does not penalize owners as it does not need a modification of the underlying OS of the employee device.

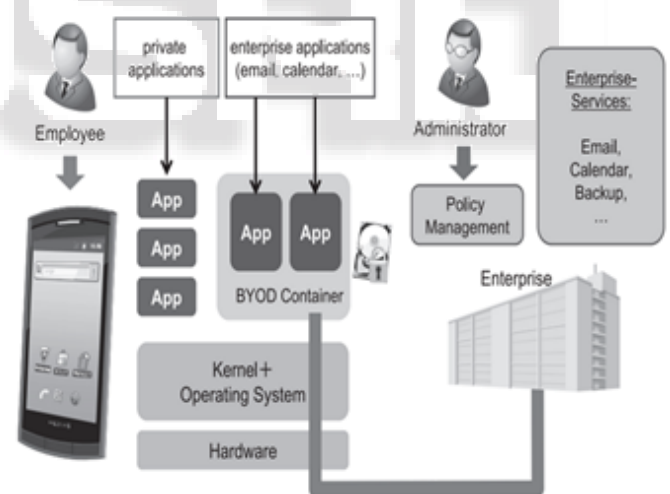


Fig. 2: Proposed architecture

A. Device platform:

The device hardware, kernel and operating system can be according to user's choice and no changes to these are needed. They shall provide to the proposed system, all functionality as in any other device not under corporate purview.

B. Applications:

Employees are free to download any application (or App in mobile terms) according to their need, for personal or corporate use. Private applications not registered at the server, shall be free to operate in any conditions and shall

not be a concern for the system under study. Employees will need to download a ‘starter’ BYOD application before they can use any of the applications developed by the company, that shall setup everything on the device, including device administration functionality and the proposed container.

C. Byod container:

Our solution consists of installing a background service within the user space that acts as a container for corporate applications within the android device. The background service will enclose and monitor all information that belongs to the organization. The service does not interact with data owned by other applications or employee’s personal data.

Fundamental advantage of being a service can be entailed by being persistent in memory even though the app may be closed. Important company circulars and BYOD messenger notifications can optionally be handled by the system. In addition, the system is quite scalable since any number of corporate applications may bind and unbind from the service as and when needed.

An important part of service functioning is reducing privacy concerns of employees. The system shall handle remote wipe commands from admin side and instead of wiping entire device memory and primary SD card (if present) as in the contemporary case, it shall wipe only part of system data that belongs to a specific BYOD application.

D. Enterprise server:

The controller service interacts with the corporate server for authentication of employee device. In case, there are multiple devices connected to the corporate network with the same profile, the proposed system will be responsible for communicating with the enterprise server and synchronizing application content over all of the registered devices.

After device and user credentials are verified by the server, the connection is authenticated and the background service initiates monitoring of the device. Any corporate data accessed by the employee is supervised and logged by the service as well as the corporate server.

E. Policy administration:

The background service shall handle remote policy change commands from remote administration application hosted on enterprise server and handle Android system and library calls for all corporate applications. Policy changes may be maximum allowed number of failed password attempts, setting minimum password length, etc.

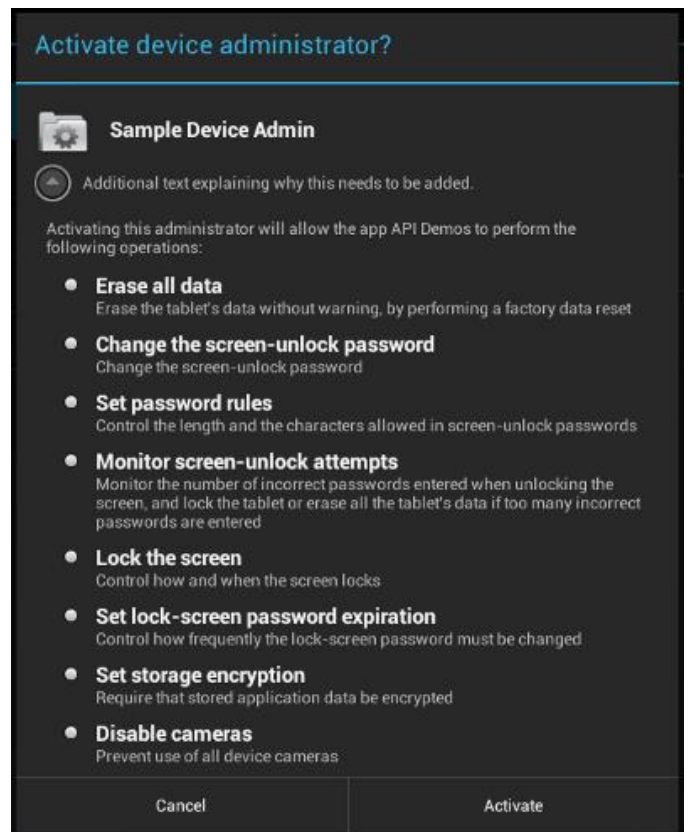


Fig.3: Android Device Admin API policy change permissions

Proposed system shall handle all common permanent and temporary session keys for BYOD applications and ensure all data transfer is encrypted and tamper-proof by adversaries at all times.

F. Communication:

The application server shall need a common means of communication with all devices and Google Cloud Messaging for Android comes to rescue. It allows sending data and commands from administration server to all registered Android devices.

The GCM server handles all aspects of queuing of messages and delivery to the target Android application running on the target device.



Fig. 4: App Registration on GCM server

When the employee device is authenticated, it receives a registration id from GCM server which can then be used to receive push notifications from the corporate application server.

G. Network security:

The service shall log accesses of sensitive data by inspecting all packets sent over HTTP and send a copy of the same to the enterprise server. The redundancy shall add a layer of security as these records could act as verifiers in case of system breach detection[6].

Considering the case where server knows there have been compromised/hacked accounts retrieving sensitive data from unknown devices over the network, the server could check if all accesses have been through registered devices by communicating with these services. If they do not have similar records, it can be concluded that the account being used on the device has been compromised and is being used on some other device as well.

V. CONCLUSION

Our proposed solution thus combines the use of one or more background services acting as a sandbox for only corporate applications on the device, making good use of storage facilities on the mobile device, along with specially-tailored cryptographic protocols that ensure the secrecy of long-term keys and sensitive materials in the mobile device. We show how this can be achieved simply by installing a single application (with controller service) within the user-level application space of the mobile device rather than on kernel/OS level as in most solutions available in the market.

Our findings show a good tradeoff between company costs, personal device load and flexibility of the system. Though device administration capability is not as strong on un-modified devices (with stock/original ROM), it is the way to go, if we want to promote BYOD among employees.

REFERENCES

- [1] "Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices", Gov Info Security, January 10, 2013.
- [2] UC Strategies. "BYOD's Productivity Gains Are 'Hard to Calculate' – Study Says", May 1, 2013.
- [3] Wiech, Dean, "The Benefits And Risks Of BYOD", Manufacturing Business Technology, 28 January 2013.
- [4] Kenneth C. Laudon, Jane P. Laudon, "Management of Information Systems"
- [5] Tom Kaneshige, CIO, "Attack of the BYOD-Killing MDM Software", February 4, 2014.
- [6] Jarrett, Marshall, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", Office of Legal Education, 15 May 2013.