International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 2 [ISSN : 2250-3757]
Publication Date : 30 October, 2015

A Study on Security Framework for BYOD Environment

Dongwan Kang, Changmin Jo, Taeeum Kim, Hwankuk Kim

***Abstract*—The term BYOD(Bring Your Own Device) collectively refers to the related technologies, concepts and policies, where employees do works by accessing corporate's IT resources, such as database and applications, using their personal mobile devices like smart phones, laptop computers and tablet PCs. However, with this trend serious security issues are emerging as a diversity of personal devices with unreliable security are increasingly accessing the typically closed intranets of conventional work environments. Corporations want to improve their productivity by taking advantage of the benefits of BYOD but it is difficult to handle an open BYOD work environment with current security technologies. As the access control policy of the NAC and MDM system is uniformly applied to users, however, they cannot be aggressive in implementing BYOD since there are security threats due to the frequent loss and theft of devices and low security. Accordingly, it is necessary to be able to flexibly set up policies and detect and control abnormal users by collecting personalized context information. In This study analyzes the BYOD environments, current threats to security and required security technologies, and presents a security framework for BYOD environments.**

***Keywords*—BYOD, Context, Access Control, Security Policy, Behavior Pattern**

I. Introduction

As the use of various mobile devices, such as smartphone and tablet PC, is increasing as a result of wireless communication technology advancement in recent times, the scope of mobile device use is expanding from simple personal communication to corporate work processing.

Accordingly, companies have introduced a working environment using mobile devices in order to improve their work productivity. They purchased and supplied devices in order to break away from closed working environment and, accordingly, to realize a working environment using mobile devices. However, it was not activated due to difficulties in device management and maintenance arising from device loss and changes as well as purchasing cost.

However, security issues are rising to be a priority concern as diverse personal de-vices with disparate operating systems and unreliable security are accessing typically closed and conventional intranets of work environments [1]. Current work environments typically operate a static security policy (rule), allocating IPs and verifying MAC (Media Access Control) on PCs. Also, additional agents like PMS (Patch Management System) are installed on PCs used at corporate offices, creating work areas with-in their control. On the other hand, it is not easy to place smart devices owned by individuals under control as they are highly portable and their managerial cycles are unpredictable. They are frequently replaced and prone to be lost or stolen, making it impossible to predict any change from a managerial perspective. Symantec Project Honeystick [2] for example, has proven that accessing the internal infrastructure of a corporation with a lost/stolen personal device happens quite frequently. In fact, 25% of employees in the US have had their personal devices used at work infected by malicious codes or hacked. Therefore, security is the top priority when considering the introduction of BYOD [3].

This study analyzed BYOD environments depending on user behavior patterns and presents a more comprehensive and flexible security framework. It is not corporations but users, devices and data that are central to any BYOD environment. This study addressed security policies through generalization of the behavior of each object and surrounding factors, which are applied as policy factors. Also, since individual behavior patterns are predictable based on various access environments and personalized device usage patterns, this study presents a security framework that detects loss, theft and malicious access of devices on the back of these patterns, and selectively finds malicious behaviors through multi-level control.

II. BYOD and Security Threats

Recently, an interest in working environments to use individuals' devices has increased and, accordingly, BYOD(Bring Your Own Device) is drawing attention as a new concept of corporate working environment[41]. BYOD is a concept where individuals bring in and use their own devices in business activities. Through BYOD, companies can anticipate improved productivity (efficiency) through the use of smart devices and also a reduction in the cost of purchasing devices.

However, as personal devices access internal infrastructures of a company, security issues, such as corporate data leaks, are generated. Personal devices are easy targets of hacker attack as a result of their frequent loss and theft as well as low security. Through Honey Stick project conducted by Symantec, it was found that access to a company's internal infrastructures through lost/ stolen personal devices is taking place frequently. According to a survey by OpenSignal in 2012, 3997 types of Android OS devices are being used and, for 70% of these devices, the respective manufacturers use the

*Dongwan Kang, Changmin Jo, Taeeum Kim, Hwankuk Kim
Korea Internet&Security Agency
Republic of Korea

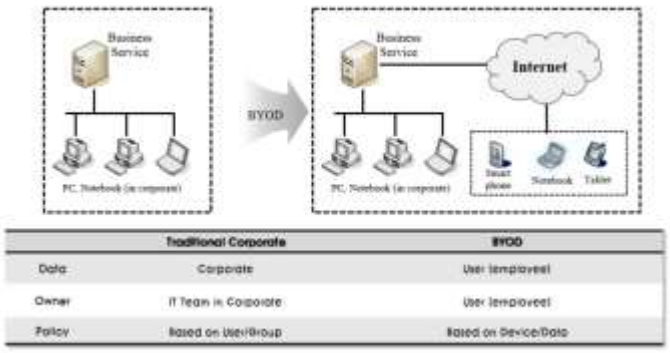

Figure 1. BYOD Environment

OS with variation. In addition to this issue concerning the device itself, the security is faced with a difficult situation since corporate confidential data can be easily leaked as a result of negligence in device management. And efficient control of personal devices can be difficult due to frequent device change. In fact, 25% of office workers in the U.S. experienced malicious code infection to or hacking of their devices used in BYOD system. Therefore, the top priority in introducing BYOD system is to establish security for the system.

BYOD environment is comprised of a number of access environments, such as through diverse devices or by wired/ wireless connection. Without considering characteristics of such diverse environments and individual user patterns, it is difficult to flexibly respond to BYOD environment with the existing network security equipment only.

NAC, a network access control security equipment, and MDM, a mobile device management method, are discussed as methods for BYOD security. The functions of NAC are to control accesses by identifying authenticated users or devices, to define access control policies and to force compliance with the security policies in switches or routers. As the release began in full scale in 2006, this solution has since been developed further in terms of the functions it offers. At present, NAC solution provides wired and wireless integrated security functions, such as a powerful IP-based control function, a function to authenticate mobile terminals and a function to verify terminal security and integrity [4].

MDM technology is taking the center stage as of late together with NAC. Displaying the fastest growth among corporate mobile software technologies, the global market scale of MDM expanded from $3.5 billion in 2011 to $5 billion in 2012 as a result of the increased necessity of mobile terminal device management [5]. Recently, MDM provides a comprehensively protective function for a variety of channels subject to data leaks, such as operating apps, camera, recorder and Wi-Fi, and, at the same time, a function to administer control on company-wide monitoring and user environment through the central management console.

However, they still have limitations in achieving an ultimate BYOD environment. NAC administers powerful authentication at the time of access. However, it does not engage in any behaviors after the access. In case of MDM, individual users tend to feel reluctant about installing this corporate security program in their personal devices. In addition, BYOD environment dependent on specific devices restricts users' right of selecting personal devices and this is not in conformance with the direction pursued by BYOD.

Unlike the existing intrusion detection system through network traffic analysis, this study proposes a method to model and patternize users' behavioral elements, and thus to identify whether the users' behaviors are normal or not.

III. Related Work

As BYOD has become a hot topic of the industry, many security companies have rushed to release solutions. BYOD related solutions typically emphasize control of the devices. Here, control implies many things; it expands controls mostly available in conventional work environments to personal devices (starting with the security of a device to authentication, registration and data input/output). Its ultimate goal is to secure control over personal devices' access to enterprise data, but its approach is different.

First, network-based technology traditionally handles control and authentication of accessing devices at a network level like an NAC (Network Access Control) [4]. Con-trolling a network can eliminate the dependency of personal devices but has limited control about post admission.

Second, there is device-based control technology such as MDM (Mobile Device Management) [5]. Centralized remote control of a device is enabled by installing a control agent.

Lastly, there is hybrid-type control technology that combines both network-based and device-based technologies. This enables corporations to take a more flexible ap-proach depending on their situation.

In point of behavior analysis, there are several studies.

In [6], a behavior-based NAC model was proposed. This model is classified into groups according to the roles of each network object. In case of a new object access, each group decides the degree of similarity through group voting and a decision for entry is made accordingly. In addition, after entry, it is examined whether or not behaviors of a new object are normal through group voting by the respective group members.

In [7], a method to detect current abnormalities based on network traffic characteristics, such as past packet count, in 3G mobile network environment was proposed. Unlike a wired network, a mobile network displays different traffic characteristics according to such environments as time and day of the week. Therefore, considering time and day of the week elements, this method performs comparative analysis for current behaviors against behavioral patterns of the past under a similar environment.

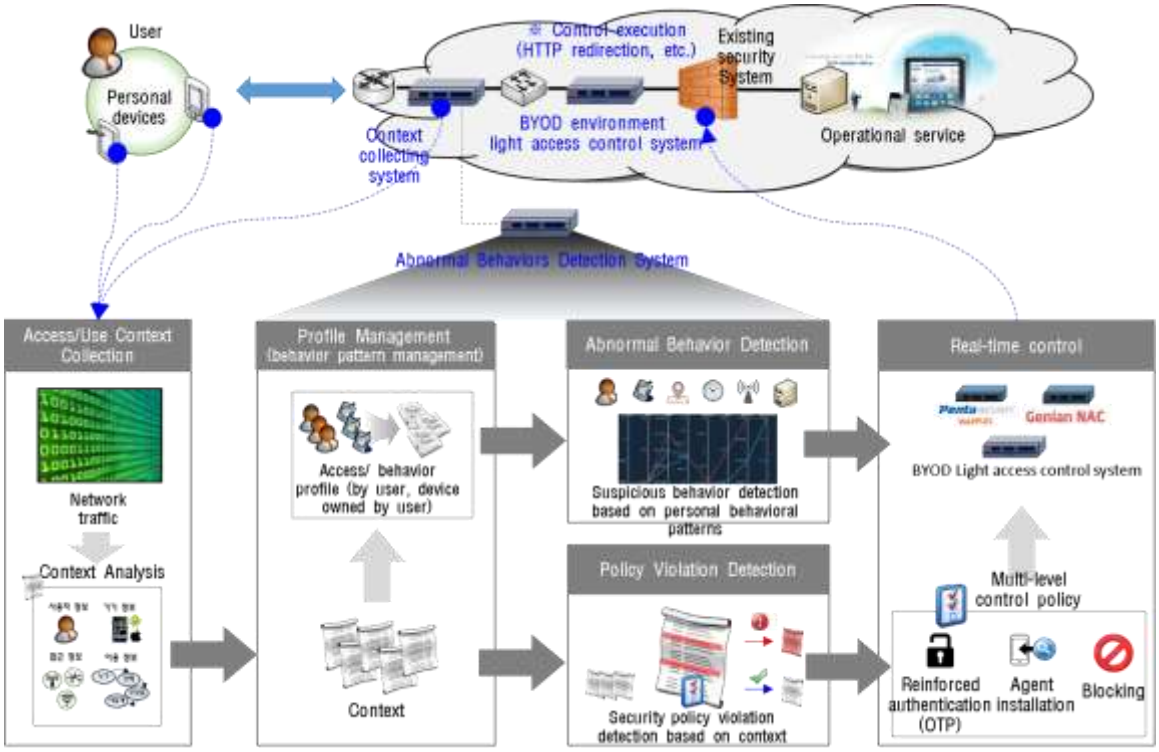

Figure 2. Security Framework on BYOD Environment

IV. Security Framework in BYOD

A corporation should be able to maintain its required levels of security depending on the roles and objectives of the employees and the value and types of information it owns. Also, it should ensure that its policies to maintain such levels of security are based on a sophisticated system that is manageable in an intuitive and flexible manner while incorporating many complex elements[8]. As such, we propose smart access control for BYOD environments, which defines context based on context.

Unlike conventional methods that rely on such components as TCP/IP or user groups, the proposed method is (1) more intuitive, (2) able to define behaviors and context available to be used as policies, (3) transform user behavior into a pattern, and (4) combine various environment factors to establish effective policies.

A. *Agent-less based personal device security control and automatic device identification/ registration technology*

- Resistance to enterprise security program installation in personal devices
- Realistically difficult to register all personal devices in advance
- Changes in personal device management, such as device loss, use of leased devices and device rental, occur continuously
- Therefore, a technology for personal device management and security control without an agent is necessary

B. *Security policy based on context of device access/service use*

- Security policies centering on user authentication are associated with difficulties in detecting corporate infrastructure access through lost devices
- In smart work environment, various access situations with different access environment, time, location and network(internet/mobile..) exist
- Even after device access, personal device access control is necessary in the level of internal corporate infrastructures, such as web server and DB
- Therefore, high-level security policies based on personal device access/ service use situation (behavior) information is necessary

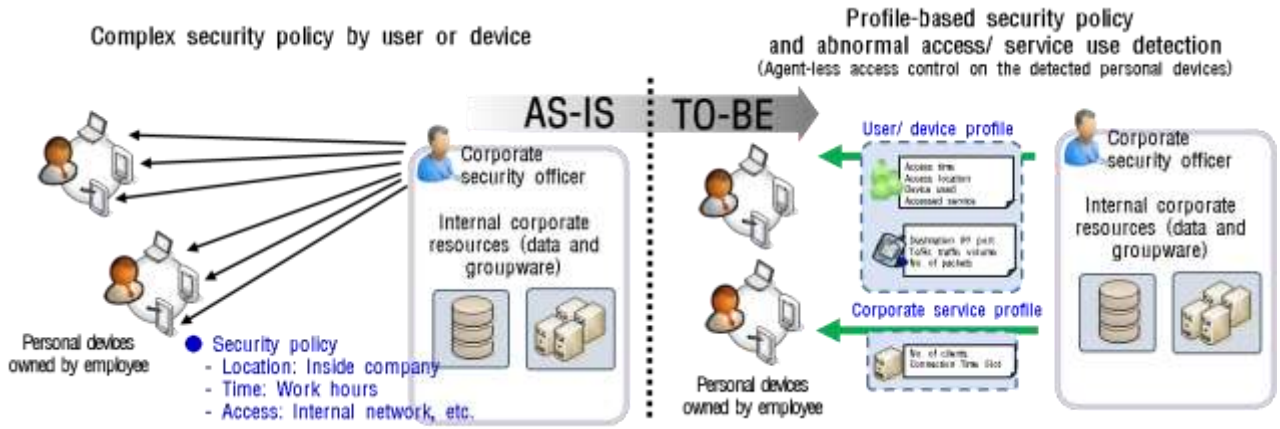

Figure 3. Profile based Security Management

C. *Profile-based security policy and abnormal access/ service use detection technology*

- Complexity of policy management increased as a result of various connection environments and the use of a large number of devices
- Security policy by user, device, server is realistically unattainable (black/whitelist-based security policy)
- Require a profile-based security policy and detection of abnormal activity

D. *Deep context collection and dynamic control for isolation device*

- Most NAC block device that violated policy when access a network
- However, to ensure work continuity using various devices, re-access permit required following the removal of causes for access blocking
- Therefore, a deep context collection and analysis, and allow re-access technology required by follow-up measures or remote control

v. Conclusion

As a result of BYOD and smart work system diffusion and distribution, a flexible security method has become necessary in an environment for business operation through internal corporate system access using personal mobile devices.

In BYOD environment, there is a variety of connection status like time, location device type, and etc. These various conditions due to the user's actions can have personalized characteristics.

And mobile devices, which have become diversified as of late, are producing various user patterns according to the environment characteristics of access time and locations rather than simply displaying differences in detailed functions.

Mobile devices, such as smart phones, are closely involved in the lives of individuals. Even if businesses reject mobile devices, user would find ways to use them at work. Therefore, we must embrace the fact that BYOD is a reality we face and need to make preparations for security technologies to be applied to the BYOD environment.

Acknowledgment

This work was supported by the IT R&D program of MSIP/KEIT. 10045109, The Development of Context-Awareness based Dynamic Access Control Technology for BYOD, Smartwork Environment]

References

[1] Johnson. K, Mobility/BYOD Security Survey. SANS Institute , 2012
[2] Symantec, Smartphone Honey Stick Project, http://www.symantec.com
[3] Miller. K.W., Voas. J., Hurlburt. G.F., BYOD: Security and Privacy Considerations, IT Professional 14(5), pp. 53–55, 2012
[4] Inverse, PacketFence, http://www.packetfence.org
[5] Henderson. T., How mobile device management works, IT WORLD , 2011
[6] V Frias-Martinez, Behavior-Based Network Access Control: A Proof-of-Concept, ISC 2008, pp. 175-190, 2008
[7] D'Alconzo. A, A Distribution-Based Approach to Anomaly Detection and Application to 3G Mobile Traffic, GLOBECOM, pp.1-8, Dec 2009
[8] Dongwan K, Joohyoung O, Chetae I, Context Based Smart Access Control on BYOD Enviroments, 15th International Workshop on Information Security Applications, LNCS Vol. 8909, August 2014