# A Study on the Detection of Abnormal Behavior and Vulnerability Analysis in BYOD

Taeeun Kim(✉)

Korea Internet & Security Agency, Seoul, South Korea
tekim31@kisa.or.kr

**Abstract.** When many companies recently introduced BYOD (Bring Your Own Device), i.e. allowing employees to use personal mobile devices at work, they also adopted the NAC and MDM system for prevention of confidential information leakage, access control and efficient user management. 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. This paper proposes a behavior-based abnormality detection method that detects abnormal behavior by classifying vulnerabilities occurring in the BYOD environment and patterning various users' information use contexts.

**Keywords:** Mobile · BYOD · Security · Context information · Behavior pattern analysis

## 1 Introduction

As the use of employee-owned mobile devices is recently changing the working environment, the concept of BYOD (Bring Your Own Device) is drawing attention as a new corporate working environment. BYOD refers to the case of employees using their own mobile devices like notebooks, tablets and smartphones to access internal data and handle business. It can be expected to improve productivity and reduce costs.

As the appearance of new IT environments like BYOD increases convenience, there tends to be security problems like the leakage of enterprise data as personal devices are accessing the internal infrastructure of enterprises. A research found that personal devices can be easily attacked due to loss, theft and low security, and consequently the internal infrastructure of enterprises are accessed and attacked frequently [1].

For BYOD security, the NAC (Network Access Control) for network access control security and the MDM (Mobile Device Management) for mobile device control are proposed, but they certainly have limitations. The NAC controls users by authenticating users when they access the internal infrastructure of enterprises, but does not get involved in the user behavior after authentication [2]. As the MDM installs enterprise security programs in personal devices for monitoring and controlling, users may be repulsed by such programs. So it is thought to be far from the goal of BYOD [3]. Accordingly, it is necessary to detect and control abnormality by identifying the

B. Mandler et al. (Eds.): IoT 360° 2015, Part II, LNICST 170, pp. 162–167, 2016.
DOI: 10.1007/978-3-319-47075-7_20

information generated by devices and users in order to respond to various contexts occurring in the BYOD environment [4].

This paper proposes a method of using the scenarios of abnormal behavior occurring in the BYOD work environment to classify vulnerabilities, and capitalizing on the characteristics of users and devices and various service use elements to generate pattern data and detect abnormal use behavior. In the BYOD environment various elements, such as diverse devices and access environments, exist, and these characteristics make it possible to analyze personal access/use through patterning. The proposed method patterns service-level use contexts identical to users' corporate business environments, and predicts the probability of new use behavior occurrence based on patterned past data. It compares the probability of users' past behavior and the one of present behavior to detect abnormal behavior. Chapter 2 analyzes the technological trends in protection of internal resources of enterprises in the BYOD environment and the methods of collecting context information. Chapter 3 proposes the method of patterning service use behavior and detecting abnormal use behavior in the BYOD environment. Chapter 4 is the conclusion which discusses how to apply the proposed method to the BYOD environment and the direction of future researches.

## 2 Related Work

The NAC security technology targeting the BYOD environment checks whether user devices comply with the security policy before accessing the network and controls network access.

The NAC blocks infected PCs' access to the network to prevent the diffusion of malware on the enterprise network. Currently it provides wired and wireless integrated security functions, such as IP-based access control, authentication of mobile terminals, terminal security and integrity validation. As the primary purposes of the NAC itself are user authentication and access control, however, it is lacking in the ability to detect and respond to the abnormal behavior of users or devices after network access. Also, as it focuses on authentication of registered users, it is lacking in the function to authenticate/manage devices [3, 4].

Accordingly, the BYOD environment has distinctive security requirements, i.e. protecting enterprise data by isolating users engaged in abnormal behavior, as well as the utilization of various personal devices and the guaranteeing of business continuity. Therefore, the NAC solution alone cannot handle security issues in the BYOD environment.

The MDM technology uses the OTA (Over The Air) to remotely registers/manages mobile devices that are powered on through the administrator authority regardless of time and place, stop the use of lost devices and track devices [5].

The MDM system-based access control method, which can directly control personal devices in the BYOD environment, has problems. As the MDM is an application, it is difficult to control and monitor the access to other applications. Also, it is impossible to analyze mobile devices' behavior with regard to network data. More than anything else, due to demands for protection of privacy, users are reluctant to install the

MDM agent in their personal devices. So it is difficult to popularize and diffuse it. Furthermore, the cost of continuously managing the versions of various terminal devices will increase.

# 3 Proposed Method

This proposed method selects access/use behavior elements occurring in the process of using business service and uses them as user behavior patterns in order to detect abnormal use behavior. It selects not only the network traffic characteristics, but also atypical data, such as the user's device type, access time (during business hours, outside of business hours, etc.), access location (in the company, outside of the company, etc.) and use time, and uses them to pattern users' access. It also patterns the information generated while using business service and compares it with the existing identical access patterns to detect abnormal use behavior.

## 3.1 Definition of Security Vulnerabilities and Abnormal Behavior Scenarios in the BYOD Environment

### 3.1.1 Normal Users' Malicious Information Leaks

Normal users refer to users authorized to access the service of the enterprise. The normal user can maliciously access/download important information of the enterprise and leak it to the outside after authentication.

As existing security systems, i.e. the NAC and MDM, perceive them as employees who were normally authenticated and conduct business, they cannot detect abnormal behavior. As corporate information and personal information are leaked by internal users frequently, and such leaks cannot be detected, it is impossible to control abnormal behavior.

### 3.1.2 Theft of Devices by Malicious Users

Many users do not lock their personal devices in most cases, and store the ID/PW for accessing business service often. However, it is difficult to force security measures on personal devices, e.g. locking and cancelation of automatic access.

In this context, malicious users can steal normal users' devices and access corporate service very easily, and existing security systems do not have any method of perceiving them as abnormal behavior (Fig. 1).

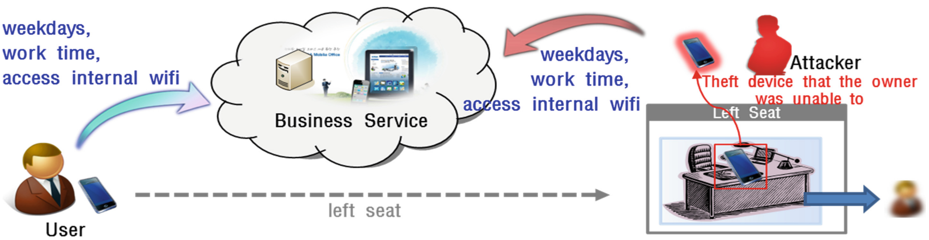
weekdays, work time, access internal wifi
Business Service
weekdays, work time, access internal wifi
Attacker
Theft device that the owner was unable to
Left Seat
User
left seat

**Fig. 1.** Device theft scenario

### 3.1.3 Attackers Using Devices Infected with Malware to Access Internal Resources

The attacker may attempt to access internal service by infecting the devices of employees with malware. As the attacker tries to access the business service using the devices of normal users in case of this attack, it is difficult to detect abnormal behavior.

Recently enterprise agents are installed to prevent device problems, e.g. infection with malware, by checking if vaccines are installed when business service is provided, but since it is impossible to detect all malware, it is impossible to defend against such attacks all the time.

## 3.2 Configuration of the Experimental Environment and Definition of Context Information

The structure of the corporate business environment and system is illustrated in Fig. 2. The context information is collected through the network traffic, collected during users' Captive Portal connection and use of business service. This patterned information will be used to detect users' abnormal behavior, and abnormal users or devices will be controlled in real time.

Meanings as user behavior will be imparted to the data generated by various devices of users and the access/use context, and this data will be processed into context information. The context information is defined as one of the set of attribute ranges for patterning behavior, and this defined information is used for comparison to detect abnormal behavior.

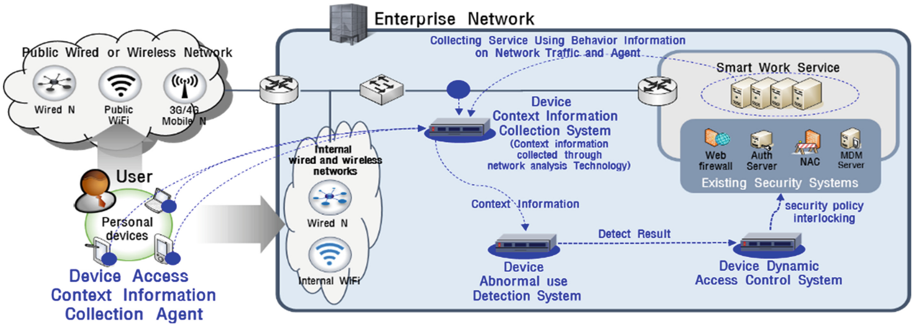
Enterprise Network
Public Wired or Wireless Network
Wired N
Public WiFi
3G/4G Mobile N
User
Personal devices
Device Access Context Information Collection Agent
Internal wired and wireless networks
Wired N
Internal WiFi
Collecting Service Using Behavior Information on Network Traffic and Agent
Device Context Information Collection System
(Context information collected through network analysis Technology)
Smart Work Service
Web firewall
Auth Server
NAC
MDM Server
Existing Security Systems
Context Information
security policy interlocking
Detect Result
Device Abnormal use Detection System
Device Dynamic Access Control System

**Fig. 2.** BYOD and the structure and security system of the smart work environment

## 3.3 How to Pattern Service Use Information

In the BYOD environment, users use their own devices to access the enterprise network and use services. The corporate business services provide users with the business environment through fixed services (bulletin board, e-mail, schedule management, etc.). The context information, generated when users use such business services, will be used to constitute generalized behavior models that users' behavior can represent.

To pattern the behavior of use context information, existing business service pages will be analyzed and structuralized using the web crawler. Each node (page) of this structuralized service will be connected to the behavior information used by users. In the context information, generated when users use services, the URL information will be connected to the node information of the structuralized service data and accumulated as service use behavior data.

## 3.4 Use Behavior Analysis and Abnormal Behavior Detection Method

The use behavior throughout the access cycle will be analyzed using users' accumulated service use behavior information, and compared with past use patterns to detect abnormal behavior.

### 3.4.1 Analysis of Use Behavior Throughout the Access Cycle

The behavior occurrence of each node of business service will be analyzed by accumulating the behavior information occurring when individual users use services throughout the access cycle.

### 3.4.2 Detection of Abnormal Use Behavior

The behavior information, collected and analyzed throughout the access cycle of users, will be compared with the past use behavior information that has the same access context information, and the overall behavior occurrence probability and the occurrence probability of each node will be compared to detect abnormal behavior.

To detect changes in overall behavior occurrence, as illustrated in Fig. 3, the error of the present and past behavior occurrence probability will be calculated.

$$Error = sqrt((present\,\#1 - past\,\#1)2) + \ldots + sqrt((present\,\#n - past\,\#n)2)$$

This error value will be compared to the normal permissible range of past behavior information. To supplement the false positive occurring when only the change in overall behavior occurrence (normal behavior range: error value < permissible range) is used to detect abnormal behavior, the change in individual items will be additionally

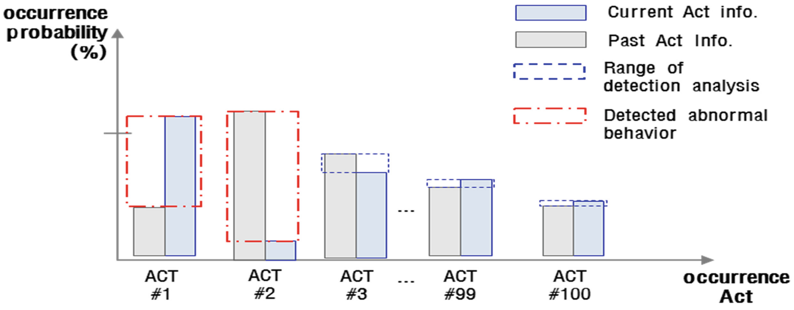

**Fig. 3.** Detection of abnormal behavior through analysis of use behavior

compared to the permissible range of normal behavior. (Normal behavior range: change in normal behavior of individual items is X% or lower).

## 4 Conclusions

Existing security systems, which manage access times, will have difficulties detecting users' abnormal use in the BYOD environment. Also, existing security technologies will have a hard time detecting the loss or theft of devices or theft of accounts, which is unknown to users, or normal users' malicious information leakage. This paper used various environmental factors to pattern and analyze user behavior in order to detect whether the behavior of business service users is abnormal. The authors will use stored user behavior to find additional methods of patterning user behavior, and minimize false positives by diversifying detection methods and applying commercial services.

**Acknowledgments.** This work was supported by the ICT R&D program of MSIP/IITP. [R0101-15-0026, The Development of Context-Awareness based Dynamic Access Control Technology for BYOD, Smartwork Environment].

## References

1. Miller, K.W.: BYOD: security and privacy considerations. IT Prof. **14**(5), 53–55 (2012)
2. Singh, M., Patterh, M.S.: Formal specification of common criteria based access control policy model. Int. J. Netw. Secur. **10**(3), 232–241 (2010)
3. Singh, M., Patterh, M.S.: Formal specification of common criteria based access control policy model. Int. J. Netw. Secur. **10**(3), 232–241 (2010)
4. Singh, M., Patterh, M.S., Kim, T.-H.: A formal policy oriented access control model for secure enterprise network environment. Int. J. Secur. Appl. **3**(2), 1–14 (2009)
5. Rhee, K., Jeon, W., Won, D.: Security requirements of a mobile device management system. Int. J. Secur. Appl. **6**(2), 353–358 (2012)