International Journal of Earth, Energy and Environmental Sciences
ISSN: 2517-942X
Vol:7, No:12, 2013

# A Study on Abnormal Behavior Detection in BYOD Environment

Dongwan Kang, Joohyung Oh, Chaetae Im

***Abstract*—**Advancement of communication technologies and smart devices in the recent times is leading to changes into the integrated wired and wireless communication environments. Since early days, businesses had started introducing environments for mobile device application to their operations in order to improve productivity (efficiency) and the closed corporate environment gradually shifted to an open structure. Recently, individual user's interest in working environment using mobile devices has increased and a new corporate working environment under the concept of BYOD is drawing attention. BYOD (bring your own device) is a concept where individuals bring in and use their own devices in business activities. Through BYOD, businesses can anticipate improved productivity (efficiency) and also a reduction in the cost of purchasing devices. However, as a result of security threats caused by frequent loss and theft of personal devices and corporate data leaks due to low security, companies are reluctant about adopting BYOD system. In addition, without considerations to diverse devices and connection environments, there are limitations in detecting abnormal behaviors, such as information leaks, using the existing network-based security equipment. This study suggests a method to detect abnormal behaviors according to individual behavioral patterns, rather than the existing signature-based malicious behavior detection, and discusses applications of this method in BYOD environment.

***Keywords*—**BYOD, Security, Anomaly Behavior Detection.

## I. Introduction

ADVANCEMENT of communication technologies in the recent times is changing user's communication environment from wired to wireless and, moreover, to wired and wireless integrated environment. In addition, the increase and spread of diverse mobile devices offering portability, such as laptops, smart phone and tablet PCs, are resulting in the functions of these devices to become expanded from simple personal communication means to devices applied to all aspects of human life including working environment.

Since early days, businesses had started introducing environments for mobile device application to their operations in order to improve productivity (efficiency) and the closed corporate environment gradually shifted to an open structure. Companies purchased and supplied internally controllable devices in order to apply smart devices to their operations. However, these devices are not spreading widely as a result of difficulty in management caused by loss and change of the devices and economic aspects concerning the device purchase.

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 [1]. 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.

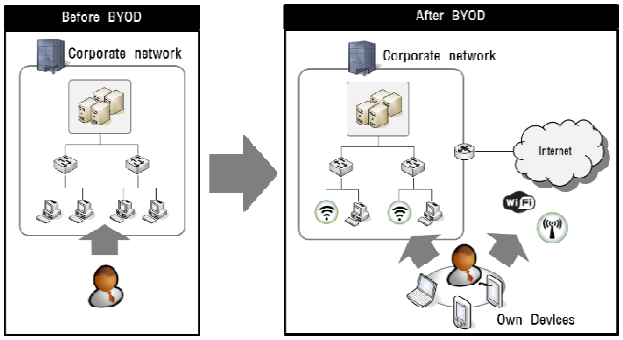


Fig. 1 BYOD Environment

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. 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.

In this paper, a method to detect abnormal behaviors based on diverse environmental elements, such as user/device characteristics and user environments, is proposed. The proposed method does not use the existing network traffic volume and specific packet's payload data. Instead, it patternizes users' behaviors based on elements, such as time slot of access and types of the devices used, and, based on the pattern data, it distinguishes abnormality of new behaviors. Through this process, the status of abnormal behaviors can be independently distinguished in relation to individual users displaying different use patterns.

Dongwan Kang, Joohyung Oh, and Chaetae Im are with the Korea Internet & Security Agency, Seoul, Korea (South) (e-mail: lupin428@kisa.or.kr, jhoh@kisa.or.kr, chtim@kisa.or.kr).

## II. Related Work and Research

A number of security products targeting NAC and BYOD detect abnormal behaviors mostly based on network traffic characteristics. The focus is on detecting malicious intrusion attempts or attacks using malicious codes. Therefore, these products are not very much different from the conventional intrusion detection systems.

PacketFence [2], an open source NAC developed by Inverse, isolates access of a new device into registration VLAN for authentication and administers forced authentication through captive portal. In addition, through link with vulnerability inspection tools, such as Nexus, it checks security of an object prior to access. In relation to behavior monitoring, PacketFence has a structure to monitor behaviors of network use (network traffic) through a link with Snort following authentication.

In [3], 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 [4], 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.

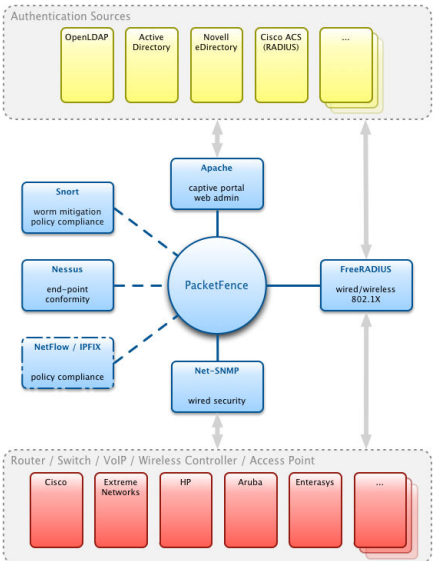


Fig. 2 PacketFence (Open source NAC) [2]

## III. Proposed Scheme

In a BYOD environment, personal access characteristics and characteristics of device use are different. As much as so, detecting abnormal behaviors based on consistent standards is highly likely to produce false or erroneous results. Therefore, to detect abnormal behaviors, a method with which to patternize previous normal behaviors of each object, and thus to dynamically manage the patterns is necessary. This study proposes a method to detect abnormal behaviors by patternizing behaviors based on a variety of behavioral elements, such as time/ location of target object, accessed network and devices used, unlike the conventional network-based security equipment conducting detection through network traffic analysis.

For abnormal access/ use behavior detection, the proposed method sorts behavioral elements possible to occur in a work scenario and uses them in patternizing the users' behaviors. In addition to network traffic characteristics, unstructured data, such as types of devices used, access time (working hours, non-working hours), access locations (inside or outside company) and time of use, are used as elements in patternizing users' access/ use behaviors.

### *A. Overview*

The proposed abnormal behavior detection method is implemented mainly in three stages. The first is to model elements concerning the respective behavior, the second is to patternize the behavior and the third is to detect abnormalities for the entered behavior as shown Fig. 3.

The proposed algorithm is based on Bayesian theory, which is applied to SPAM filtering. However, for abnormal behavior detection, patterning (occurrence frequencies of words in SPAM and normal e-mail) used in the existing SPAM filtering has been changed. In case of SPAM detection, the division of groups (SPAM or normal e-mail) is clear. In addition, the count of SPAM occurrence is the same or larger than the count of normal e-mails. Therefore, learning the difference of the two groups can be sufficiently achieved [5]. However, in case of an abnormal detection, it is difficult to directly apply normal and abnormal classifications because abnormal behavior occurrence cannot be predicted. Therefore, the proposed algorithm uses each behavioral element as classification criterion and classifies a single behavior element by patternizing occurrence information of other behavioral elements. That is, when a user's behavior is $\{a_3, b_2, c_4\}$, it does not classify the behavior as a whole (normal/ abnormal). Rather, it identifies first the occurrence possibility of each behavioral element, $a_3$, $b_2$ and $c_3$. The occurrence possibility of a3, in case of a behavior corresponding to a3, can be calculated as follows using occurrence possibilities of $b_2$ and $c_4$.

By applying this to each behavioral element, occurrence probability of each behavioral element considering other behavioral elements can be obtained. Then, with occurrence possibility of each behavioral element as an average, overall behavior occurrence possibility is estimated.

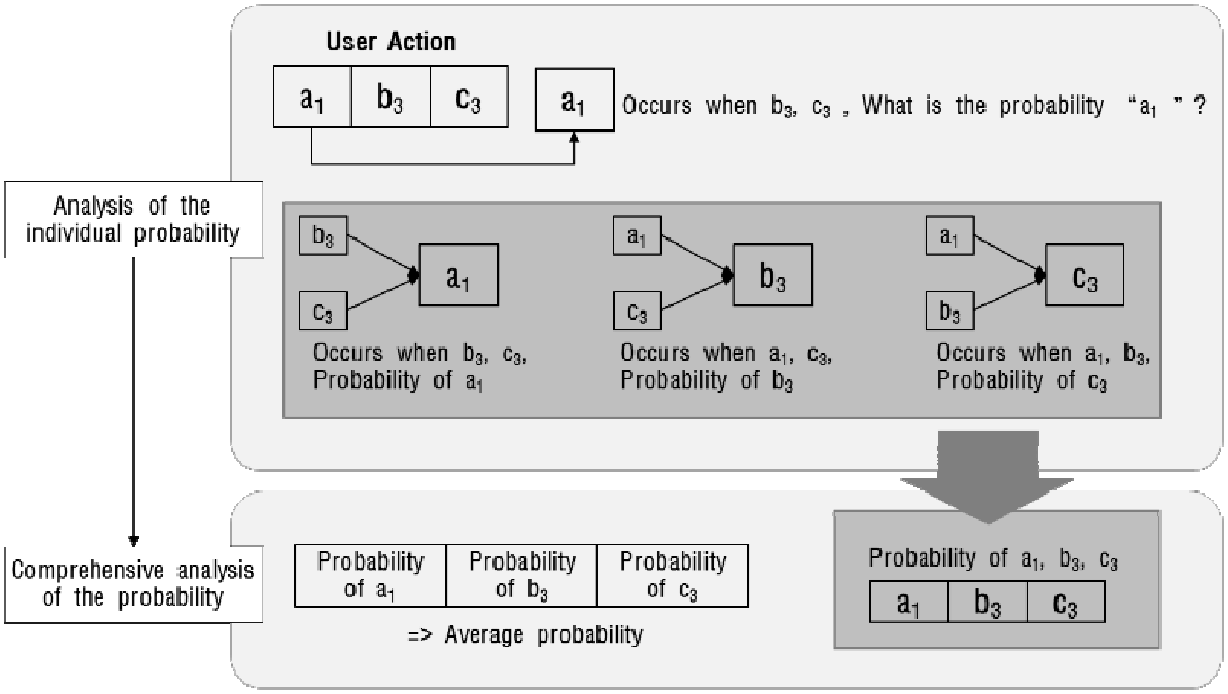


Fig. 3 Main Flow of Anomaly Behavior Detection

*B. Step 1: Patternize of Service Access/Use*

In a BYOD environment, people can use their own devices. In addition, access time, time of use, devices used and services used may vary according to users' commuting routes and personal characteristics. Characteristic elements displayed by users' behaviors are categorized, and thus a generalized behavioral model is formulated.

Behavior modeling requires selection of behavioral elements with which each behavior can be distinctly classified. A behavior holds a group of behavioral elements and a user holds one of the respective behavioral elements in relation to each behavior. For example, assuming that behavior A is "access time," behavioral elements can be set as {$a_1$:AM, $a_2$:PM} or {$a_1$:0H~6H, $a_2$:6H~18H, $a_3$:18H~24H}. If so, when defining the group of behaviors of a user or a device as behavior A={$a_1$, $a_2$, ..., $a_i$}, behavior B={$b_1$, $b_2$, ..., $b_j$}, ...,behavior N={$n_1$, $n_2$, ..., $n_k$}, behaviors of a current user can be modeled as {$a_x$, $b_y$, ..., $n_z$}.

$$User\ Behavior = \{a_x, b_y, ..., n_z\}\ (A=\{a_1, a_2, ..., a_i\})$$

Behavior pattern information can be managed with matrix according to the composition of behavioral elements. The 'behavioral pattern matrix' provides behavior pattern information of each user. It holds data on the occurrence frequencies of different behavioral elements based on individual behavioral elements.

The following Fig. 4 shows that a patterned user behavior based on behavior model.

Through this matrix, relevance of the occurrence of other behaviors to the occurrence of a base behavior can be analyzed. On the other hand, based on other behavioral elements generated on the basis of Bayesian statistics theory, it can be analyzed as to which elements of the base behavior have high possibilities of occurrence.

*C. Step 2: Detection of Abnormal Behavior*

Abnormal behavior detection requires user behavior information of a certain level. When a user's "behavior pattern matrix" is completed as data about specific counts or time limits are accumulated, the user's behavioral pattern can be analyzed using the matrix. Abnormal behavior detection is largely divided into two stages. The first is to analyze occurrence possibilities of individual behavioral elements and the second is to analyze overall behavior occurrence possibility.

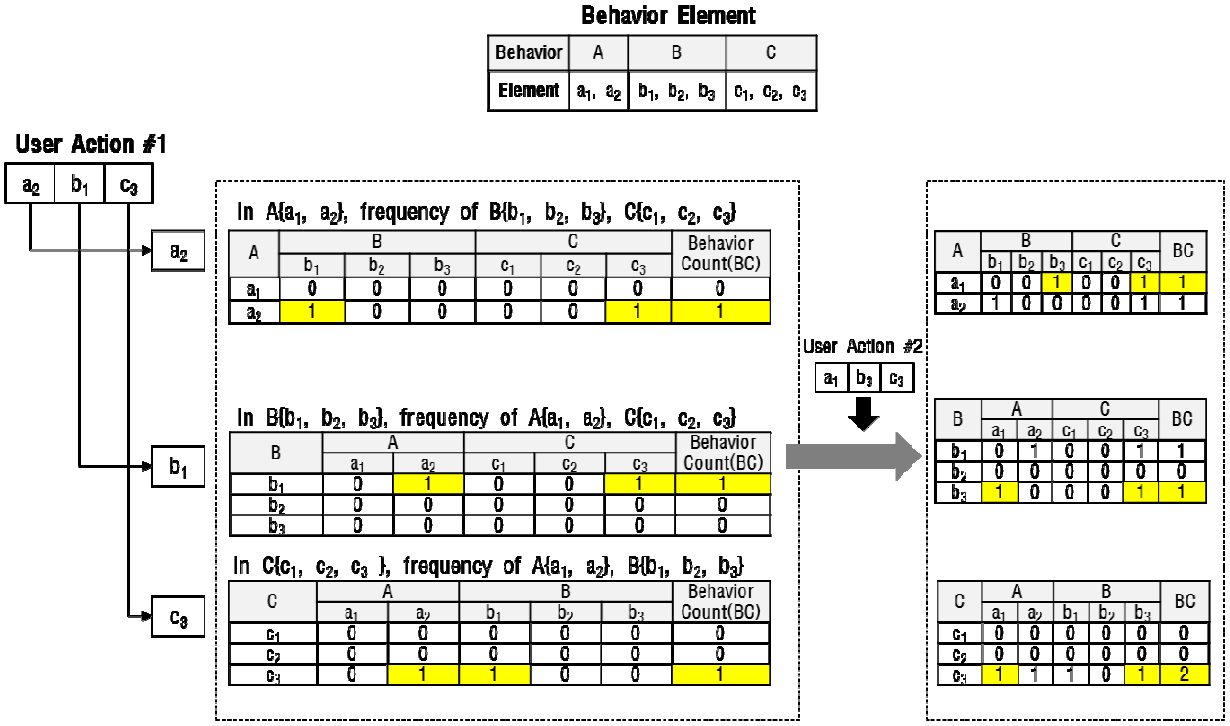


Fig. 4 Patternize of User Behavior

Bayesian Probability theory generally used in SPAM distinguishes SPAM based on frequency of a word in relation to word composition of a document. The reason such an application is possible is because it is relatively easier to obtain data about SPAM. However, the problem of solving abnormal behaviors as discussed in this study is not to decide a specific behavior pattern as abnormal, but to decide patterns different from the existing to be abnormal. Therefore, in order to analyze occurrence frequencies of all behavioral elements, it is necessary to analyze occurrence possibility of each behavioral element and, based on the results, to analyze overall behavior occurrence possibility. For analysis of the occurrence probability of individual behavioral elements, the probability is calculated based on probabilities of other behavioral elements in relation to each behavioral element through reference to the behavioral pattern matrix. Once probabilities of individual behavioral elements are calculated, detailed overall occurrence probability can be estimated based on weighted values of each behavioral pattern.

## IV. Conclusion

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. This study modeled users' behaviors going beyond the existing network traffic characteristics and, based on the behavioral models, proposed a method to analyze abnormal behaviors according to individualized characteristics. Using this method, occurrence possibilities of behavioral elements generated under diverse environments can be deduced, and, based on the deduction; abnormal behavioral elements can be detected.

Mobile devices, such as smart phones, are closely involved in the lives of individuals. Even if businesses reject mobile devices, individuals 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. In the future, methods to define and collect detailed user behavioral elements and also to patternize the collected information will be studied. In addition, by designing detailed functions, a system for abnormal behavior detection will be established.

## 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] Miller, K.W. “BYOD: Security and Privacy Considerations,” IT Professional, Vol 14, No 5, Oct, 2012, pp. 53-55.
[2] Inverse, "PacketFence," 2013, (http://www.packetfence.org/).
[3] V Frias-Martinez, "Behavior-Based Network Access Control: A Proof-of-Concept," ISC, 2008, pp. 175-190.
[4] D'Alconzo, A. "A Distribution-Based Approach to Anomaly Detection and Application to 3G Mobile Traffic," GLOBECOM, Dec. 2009, pp. 1-8.
[5] P. Graham, "A Plan for Spam," http://www.paulgraham.com/spam.html, 2002.