A Study on Context Information Collection for Personal Mobile Device Identification in BYOD and Smart Work Environment

Taeeun Kim(✉), MyoungSun Noh, Kyungho Chung, and Chaetae Im

IT Venture Tower, Jungdaero 135, Songpagu, Seoul, Korea
{tekim31, nmsnms, khc, chtim}@kisa.or.kr

Abstract. With the advent of BYOD (bring your own device) environment where personal mobile devices are used in work, companies began introducing NAC and MDM systems to prevent the leaks of, to access control and to efficiently manage confidential information. However, NAC and MDM access control policy is uniformly applied to users, and thus BYOD is not being actively introduced as of current where security threats exist as a result of frequent device loss and theft as well as low security level. Therefore, flexible policy setting and control method through personalized information collection are necessary. This study discusses the definition of context information and a method to collect the information to detect users' abnormal behaviors considering the diversity of devices used and connection environments for BYOD.

Keywords: BYOD · Security · Context information · Network management

1 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.

Recently, the concept of BYOD (bring your own device) is drawing attention as a new corporate working environment because of changes in working environment to use personally owned mobile devices [1]. BYOD environment is where individual employees work by accessing internal corporate data using their personal mobile devices, such as laptop computers, tablet PCs and smartphones. It is anticipated to produce work productivity improvement and cost reduction effects.

As convenience was improved as a result of the advent of BYOD, a new IT environment, the instances of personal devices accessing internal corporate

R. Giaffreda et al. (Eds.): IoT360 2014, Part II, LNICST 151, pp. 104–109, 2015.
DOI: 10.1007/978-3-319-19743-2_16

infrastructures increased and this led to such security issues as corporate data leaks. Personal devices are easily exposed to loss, theft and attacks as a result of their low security level and thus it has been investigated that accesses to and attacks on internal corporate infrastructures through personal devices are occurring frequently.

For BYOD security, NAC (network access control), a network access control security equipment, and MDM (mobile device management) for mobile device control are being proposed. However, these methods are subject to limitations. NAC controls users through authentication at the time of access to internal corporate infrastructures. However, it does not interfere with user behaviors after the authentication. In case of MDM, it is a method to install a corporate security program in personal devices, and thus to monitor and control the devices. It generates a sense of rejection among users, however, and thus does not conform to the direction pursued by BYOD.

Therefore, to respond to various situations that can occur in BYOD environment, methods for abnormal behavior detection and control through device and user identification are necessary.

In this paper proposed context information composition and collection method to create patterned information and detect abnormal behaviors based on user and device characteristics and diverse environmental elements. The proposed method is to organize captive portal for the existing corporate network access control, to administer user identification and context information collection/analysis through mirroring of traffic for service use and thus to pattern user behaviors. Using information created as such, abnormal behaviors are examined independently for individual users that display different patterns of use [5].

Technology trend for internal corporate infrastructure protection in BYOD and smart work environment and the method of context information collection are analyzed in Sect. 2 and the proposed method is described in Sect. 3. In Sect. 4, plans for applying the proposed method to BYOD environment and the direction of studies to be pursued in the future are discussed.

2 Related Work and Research

NAC security technology targeting BYOD environment controls network accesses by inspecting whether or not user's devices satisfy security policy standard before they access the network.

NAC blocks access to the network of infected PC in order to prevent the spreading of malicious code in corporate network. At present, wired and wireless integrated security functions, such as IP-based access control, authentication by mobile terminal, terminal security and integrity verification, are provided. However, as the main purpose of NAC is to control user authentication and access, it lacks the function to detect and respond to abnormal behaviors of users or devices after network access. In addition, it centers on the registered user authentication, and thus the functions for device authentication/management are insufficient [6, 7].

As such, BYOD environment is subject to a special security requirement to protect corporate data through isolation of users displaying abnormal behaviors in addition to the ensuring of work continuity and the use of various personal devices. Therefore, it is impossible to solve security issues in BYOD environment using NAC solution only.

MDM technology provides the functions for device registration/management, suspension of the use of lost devices and device tracking based on administrator authority in a remote location for powered-on mobile devices anytime, anywhere using OTA (over the air) [8].

There are also problems in MDM system-based access control, which provides a function to directly control personal devices in BYOD environment. MDM is an application in itself. Therefore, it is difficult to control and monitor accesses made by other applications. In addition, it is impossible to analyze behaviors in relation to network data of mobile devices. Most of all, users feel reluctant about MDM agent installation in their personal devices out of fear for violation of their privacy, and thus the system distribution and diffusion are difficult to achieve. At the same time, it is subject to an increase in the cost for continuous version management on various terminal devices.

3 Proposed Method

The proposed method is for context information that can be collected for abnormal behavior detection in BYOD and smart work environment and it outlines the structure and operating method of a system to collect the context information.

The overall system structure is as shown in Fig. 1. Context information is collected based on the user's captive portal connection and network traffic information, and thus the user's profile is created. The patterned information created as such is used in deciding users' abnormal behaviors. Users and devices detected of abnormalities are controlled real-time.

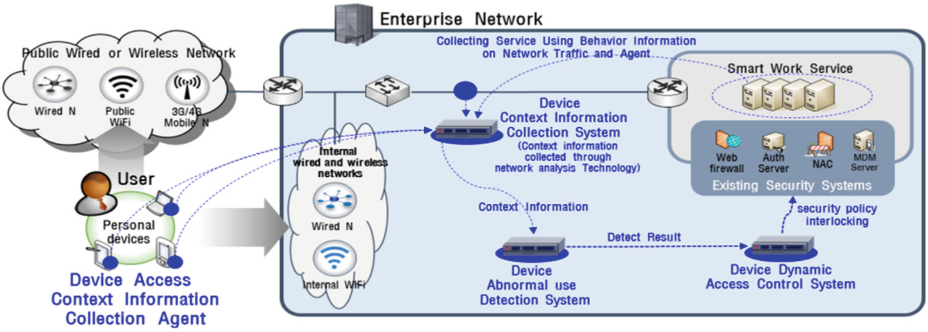
Enterprise Network
Public Wired or Wireless Network
Wired N
Public WiFi
3G/4G Mobile N
Collecting Service Using Behavior Information on Network Traffic and Agent
Smart Work Service
Device Context Information Collection System
(Context information collected through network analysis Technology)
Web firewall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

Fig. 1. Security system in BYOD and smart work environment

3.1 Context Information Collection System Structure and Operation

In BYOD environment, a technology to collect context information based on network independent of the types of users' devices is necessary. The proposed system is of a structure to administer mirroring on corporate network access traffic and categorizes users based on the connection IP. Context information is collected at the time of network access, use and termination separately. When user accesses corporate network using his or her personal mobile device, a captive portal linked to the company's authentication server is accessed. In this case, browser information and User_Agent in HTTP packet are analyzed, and thus the access context information is collected.

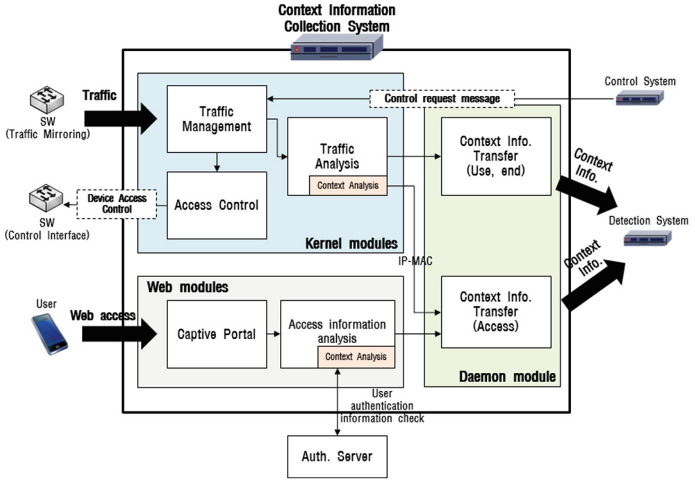

Fig. 2. Context information collection system configuration

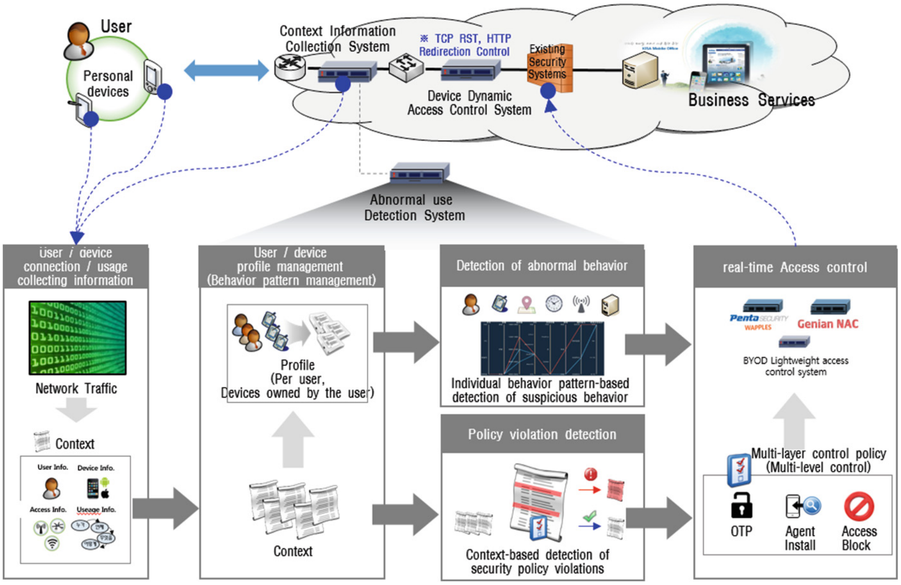
User
Personal devices
Context Information Collection System
※ TCP RST, HTTP Redirection Control
Existing Security Systems
Device Dynamic Access Control System
Business Services
Abnormal use Detection System
User / device connection / usage collecting information
Network Traffic
Context
User Info.
Device Info.
Access Info.
Useage Info.
User / device profile management (Behavior pattern management)
Profile (Per user, Devices owned by the user)
Context
Detection of abnormal behavior
Individual behavior pattern-based detection of suspicious behavior
Policy violation detection
Context-based detection of security policy violations
real-time Access control
Penta SECURITY WAPPLES
Genian NAC
BYOD Lightweight access control system
Multi-layer control policy (Multi-level control)
OTP
Agent Install
Access Block

Fig. 3. The data process of the proposed method

Following the access, context information is collected using periodic network traffic that occurs during the course of using company's internal service. If network use is not detected for a set period of time, context information for termination is created (Fig. 2).

3.2 Detailed Elements of Context Information

In BYOD environment, context information, such as user, device and connection environment information, is defined and the collected information is patterned to identify various personal devices used and the network access environments. User information includes user ID and authority, and device information consists of such information as MAC, OS, browser, device type and model name. As for connection environment information, it is divided into location of access, access time, access network and accessed service. The context information categorized as such is used in deciding abnormality following behavior patterning for each user in terms of who, when, where and what and also as data for policy application (Fig. 3).

4 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. It has become possible to create different behavior patterns by collecting meaningful information in user environment as well as mobile device information and user identification values. Through this, the establishment of various security policies rather than uniformed policy application has become possible. In this study, a system to compose and collect context information for user behavior patterning based on the collected information has been suggested by breaking away from the existing system, which is to apply security policies to the existing network traffic only. This system can be used in deducing the possibility of behavioral elements occurring in various environments, and thus in detecting abnormal behaviors.

The use of BYOD environment will continue to increase in the future and, accordingly, it is necessary to prepare the related security technologies. A further study will be conducted on the methods to enable more diverse information collection and user behavior element definition necessary for user identification.

Acknowledgments. This work was supported by the IT R&D program of MSIP/KEIT (Ministry of Science, ICT and Future Planning/Korea Evaluation Institute of Industrial Technology). [10045109, The Development of Context-Awareness based Dynamic Access Control Technology for BYOD, Smart work Environment].

References

1. Miller, K.W.: BYOD: security and privacy considerations. IT Prof. **14**(5), 53–55 (2012)
2. Electronic Frontier Foundation: Panopticlick(browser fingerprint). https://panopticlick.eff.org/index.php?action=log&js=yes

3. Fyodor: Remote OS detection via TCP/IP stack fingerprinting, October 1998. http://www.insecure.org/nmap/nmap-fingerprinting-article.html
4. Smart, M.: Defeating TCP/IP stack fingerprinting. In: Proceedings of the 9th USENIX Security Symposium, August 2000
5. Virvilis N., Gritzalis D., Trusted computing vs. advanced persistent threats: can a defender win this game? In: Proceedings. of 10th IEEE International Conference on Autonomic and Trusted Computing, pp. 396–403, IEEE. Press, Italy (2013)
6. Singh, M., Patterh, M.S.: Formal specification of common criteria based access control policy model. Int. J. Netw. Secur. **10**(3), 232–241 (2010)
7. 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)
8. Rhee, K., Jeon, W., Won, D.: Security requirements of a mobile device management system. Int. J. Secur. Appl. **6**(2), 353–358 (2012)