Context Based Smart Access Control on BYOD Environments

Dongwan Kang(✉), Joohyung Oh, and Chaetae Im

Korea Internet and Security Agency, Songpa-gu, Seoul, Korea
{lupin428, jhoh, chtim}@kisa.or.kr

Abstract. Recent mobile communication developments and the penetration of smartphones are spurring the increase of the number of smart devices owned by individuals. Mobile devices, because of the multitude of services they provide other than simple communication have become deeply rooted into each individual's life. This development has spread into the work environment spawning a new trend commonly known as BYOD (bring your own device). 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. This study analyzes the characteristics of BYOD environments, current threats to security and required security technologies, and presents a security framework suitable for BYOD environments. The framework presented here can manage a variety of devices despite their disparate operating systems and also control network factors according to the nature of the habits of BYOD users. As it is not based on IP or port-based analysis, which had been primarily used in the past, but on high quality, context information.

Keywords: BYOD · Context · Access control · Security policy · Behavior pattern

1 Introduction

The broad penetration of Internet infrastructure and mobile communication developments has brought huge changes to society. As the number of portable mobile devices like smartphones with their plethora of uses has surged, they have become deeply rooted into the social lives of their users, not merely a means of simple communication. Such a trend has spread into the work environment emerging as BYOD (bring your own device) [1]. BYOD is the concept of workers using their personal devices at work. It refers to the concept and policy of permitting employees to bring their own mobile devices (smartphones, laptops, tablets, etc.) to their workplace and use them to access the internal IT resources of their workplace such as databases and applications. From a corporate perspective, BYOD is expected to provide speed, efficiency and productivity by having work tasks completed more efficiently. In addition, using personal devices eliminates the cost burden of supplying additional devices for work. Therefore, many corporations are mulling whether to adopt BYOD even though many people are already using their personal devices at work without their employer being fully prepared.

K.-H. Rhee and J.H. Yi (Eds.): WISA 2014, LNCS 8909, pp. 165–176, 2015.
DOI: 10.1007/978-3-319-15087-1_13

However, security issues are rising to be a priority concern as diverse personal devices with disparate operating systems and unreliable security are accessing typically closed and conventional intranets of work environments [2]. Current work environments typically operate a static security policy, 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 within 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* [4] 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].

It is difficult for security technologies suitable for conventional, closed work environments to proactively address such a change. In particular, the reality is that, in order to protect corporate information, the areas to cover have significantly diversified and increased compared to the past, including changes in ownership of personal devices, establishing a security policy suitable for the deployed network environment (i.e. intranet, mobile), and monitoring personal behavior after access.

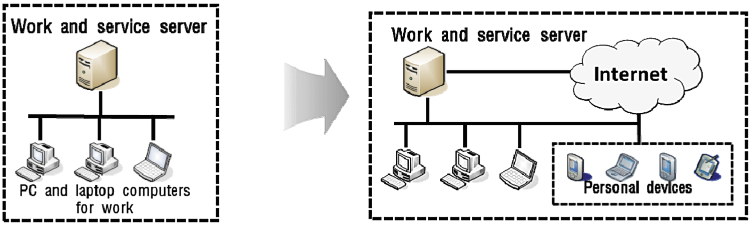
This study analyzed BYOD environments depending on user behavior patterns and presents a more comprehensive and flexible security framework. It is not corporations but users, devices and data that are central to any BYOD environment. This study addressed security policies through generalization of the 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.

2 BYOD Environments and Security Threats

2.1 BYOD Environments

BYOD (bring your own device) is the concept of using personal devices at work. It refers to the concept and policy of permitting employees to bring their own mobile devices (smartphones, laptops, tablets etc.) to their workplace and use them to access the internal IT resources of their work place such as databases and applications. BYOD implementation entails close scrutiny of the technologies and security measures involved.

The emergence of BYOD has transformed corporate internal infrastructure from being a closed environment to an open one. In other words, employees can now ac-cess work and service servers, which used to exist only in the corporate intranet, via the Internet with their personal smart device. Corporate data, which used to be processed



Classification	Enterprise Infrastructures (Closed Environment)	Enterprise Infrastructures (Open Environment)
Company Data	Processing: Devices owned by company, Store: Devices owned by company	Processing: Devices owned by individuals, Store: Devices owned by individuals
Device Ownership/ Management and Leadership	IT division in company	Individual users
Security Policy	User–centric security policy (user authentication)	Device/User–centric Security policy (device and user authentication)

Fig. 1. Change of enterprise workspace

and stored by corporate-owned equipment in a closed environment, can now be processed and stored by individually-owned devices in an open environment. Ownership, administration and control over devices have moved over to individual users from the IT departments of corporations as shown Fig. 1.

According to a *Cisco* survey of over 600 companies in 2012, 95 % had already permitted employees to use their personal smart devices at their workplace and decided that this enhanced employees' productivity. However, the emergence of a new IT environment like BYOD heightens security threats as much as it expands convenience. One of the causes that raise such security threats is the issue of how to control a system comprised of a wide variety of devices operating on a variety of operating systems and running a variety of apps. Currently countless manufacturers are making smart devices with a variety of operating systems. According to a research study conducted by *OpenSignal* in 2012, there were no fewer than 3,997 devices using An-droid, around 70 % of which used operating systems modified by their manufacturers. Problems lie not only in such devices themselves, but also in that important corporate information is leaked due to negligence in controlling the device, and the fact that it is difficult to efficiently control personal devices due to the frequency of their replacement.

There is no doubt that all users including individuals, corporations and institutions need to invest in information security in proportion to the benefit of convenience they bring. According to an IT World survey conducted in 2013 of over 1,192 corporate IT supervisors, it was found that the supervisors emphasized security as the top concern of introducing BYOD.

2.2 Security Threats

In conventional enterprise environments, devices that can access corporate infrastructure are fixed. Through IPs and MACs that are kept static, it is known which devices are currently accessing the corporate network. Also, it is easy to install data control programs in corporate-owned devices if necessary. That is, in conventional enterprise environments, the principal body that accesses the corporate network and the ways to control it are fixed, and it is possible to control them to some extent de-pending on the security policy of the corporation.

However, in a BYOD environment, personal devices of many different kinds access a variety of environments. Mobile devices, typically based either on iOS or An-droid, run on countless, fragmented operating systems and versions customized by their manufacturers. They can access via wired and wireless Internet or mobile networks. Access location can be expanded within local or from abroad, or from inside or outside one's company. Moreover, it is difficult to determine the security level of personal devices being maintained if at all.

Given such circumstances, the largest security threat is information leakage. It is assumable that someone can access corporate infrastructure via a personal device and send confidential corporate information to an external party via the same device. Malicious intent of a user, infection by a malicious code or a stolen/snatched device can cause such a situation.

For the purpose of analysis, security weaknesses that can cause information leaks can be categorized into users, devices and services. Users can be further classified according to the type of identity theft as either an unauthorized user or a user with malicious intent. Devices can be classified into those infected by a malicious code or those stolen/snatched. Identity theft occurring while the user is unawares is one of the most difficult situations for a corporation to control. From the service provider's side that has many access points, web hacking from both inside or outside must be considered.

3 Security Requirements for BYOD Environments and Limitations of Conventional Security Technologies

3.1 Security Requirements for BYOD Environments

BYOD has diversified work patterns that had previously been standardized and rather conventional in nature. However, these changes have brought with them a variety of inherent security weaknesses that can lead to information leakage. In this light, security requirements for enterprise security in BYOD environments were analyzed as follows.

When analyzing security requirements in BYOD environments, a primary consideration can be the security requirements of the principal body. First, users need a stricter and more flexible authentication technology. Unconditional adherence to a stricter authentication is not desirable to corporate productivity. A proper means should be devised factoring in the objects to be protected by each corporation and its level of security. The policy should not be fixed but rather a flexible one that is selectively applicable in many different environments. Second, it should be possible to efficiently control personal devices that tend to be frequently replaced. It is mandatory to track which devices are currently in use, those that have not been in use for a long time, and to register new devices. Third, on the services side, it is required to monitor which user uses which information and with which device. Monitoring users on their information usage should mean being able to not only watch user access but also do high-level monitoring on post-access behaviors, real-time inspection of potential violation of policies, and dynamic control. When it comes to control, in particular, flexible implementation of policies is needed such as applying a higher-grade security level to suspicious areas rather than just blocking access. Moreover, many environment factors and diverse devices in a BYOD environment make it highly likely to incur personalized characteristics such as access time, location and information of choice. Therefore, extracting such behavioral traits and turning them into a pattern can make it easier to analyze abnormal behaviors that are not a violation of policy. That is, it is necessary to ensure:

- automatic controls to respond to user/device changes
- control of personalized behaviors
- operation of security policies suitable to diverse environments
- establishment of high-level, flexible security policies

Factoring in such issues, technological requirements are defined as follows.

Smart Context Mining. In order to identify complex and rapidly changing environment easily, it need meaningful information to administrator. (Access environments of accessing devices/users from network-based and agent-based analysis).

Smart Behavior Insight. In order to analyze a personalized pattern of the various environmental factors, it need a high-level analysis function that able to inference behavior by analyzing the context during pre-admission and post-admission.

Smart Access Control (Context-based Security Policy Administration, Multi-level Dynamic Control). In order to keep as much as possible the availability in a variety of situations, it need flexible and differential management policy according to security level.

3.2 Limitations of Conventional Security Technologies

It is difficult to replace security technologies required by BYOD with conventional ones. Using a personal device at work itself is a new concept, so the closed working environment of the past has inadvertently transformed into an open one. Therefore, conventional static security technologies cannot satisfy security requirements of BYOD environments. The limitations of conventional security technologies are analyzed as follows:

Difficulties in Controlling Devices: Considering the static nature of conventional work environments, identifying a new device attempting to access and register it costs a lot as it incurs a change to the existing fixed structure that is systemized for conventional reception. However, in a BYOD environment, frequent changes in device control occur due to the characteristics of personal devices. This makes it challenging to address such changes.

Inflexible Security Policies (Control by Security Level): Conventional security policies are implemented based on individual, department and assignment criteria. In a BYOD environment, however, users who work on the same assignment within the same department are on different security levels, depending on whether they access from inside the organization or outside, whether they use a smartphone or a laptop, and whether they use an unreliable open wireless LAN or a mobile network. Such factors are crucial in judging the level of security of an accessing device. Still, with conventional security policies, it is challenging to control these diverse factors in a flexible manner.

Monitoring Post-access Behavior: The purpose of monitoring is to identify a behavior that is suspicious or violates policies from the perspective of security. Convention-al monitoring is based on the network, which depends on low-level information like traffic volume of two-way transmission. Given that the transmission format and users' behavioral patterns differ depending on the characteristics of each device, it is necessary to prepare measures for high-level monitoring that take these factors into account.

4 Related Works

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) [5]. Controlling 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) [6]. Centralized remote control of a device is enabled by installing a control agent. This can be a fault-proof way for control but installation of a control agent in personal devices may make users uncomfortable. In fact, corporations implement this type of control policy for strict control but challenges remain when distributing such an agent to personal devices. In addition, mobile devices are constantly evolving so it is necessary for corporations to continuously distribute agents to address this, which is not an easy decision to make considering the hefty costs involved.

Lastly, there is hybrid-type control technology that combines both network-based and device-based technologies. This enables corporations to take a more flexible approach depending on their situation. More efficient implementation can be achieved by opting for device-based control on the areas that require strict control, while performing network-based control on areas that need more flexibility. These are the technologies that are in place currently, but it is difficult to address the absence of implementation policies and the needs for higher-level monitoring on behavior.

In point of behavior analysis, a behavior-based NAC model was proposed at [7]. This model is classified into groups according to the roles of each network object as pre-defined. When new object access, each group decides the degree of similarity through group voting, then decision for entry. In addition, after entry, it is examined behaviors of a new object deciding whether or not through group voting by the respective group members. In [8], 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.

5 Security Framework in BYOD Environments

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. 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.

Also, it is constructed in a hybrid format, minimizing its dependency on agents and factors in a control framework that links analysis of the network with existing security equipment (Fig. 2).

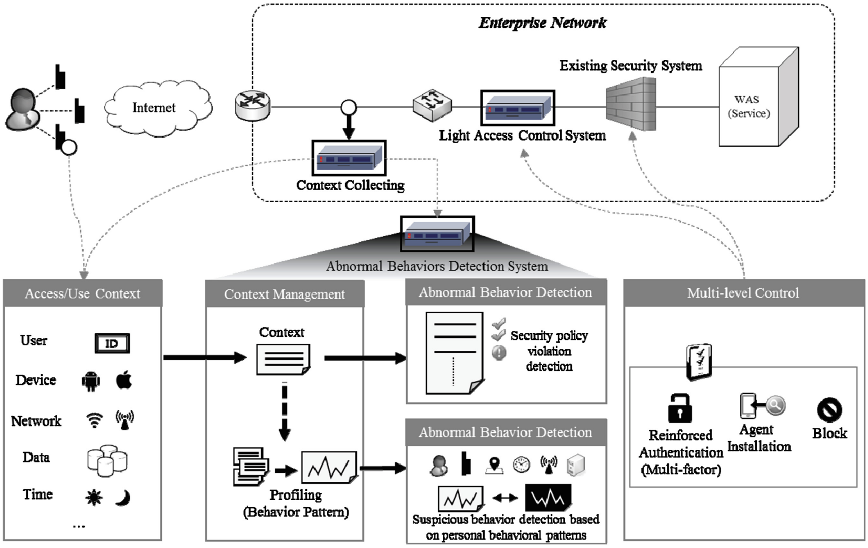

Enterprise Network
Existing Security System
Internet
WAS (Service)
Light Access Control System
Context Collecting
Abnormal Behaviors Detection System
Access/Use Context
User
ID
Device
Network
Data
Time
...
Context Management
Context
Profiling (Behavior Pattern)
Abnormal Behavior Detection
Security policy violation detection
Abnormal Behavior Detection
Suspicious behavior detection based on personal behavioral patterns
Multi-level Control
Reinforced Authentication (Multi-factor)
Agent Installation
Block

Fig. 2. Proposed BYOD security framework

5.1 Smart Context Mining

Context identifies subjects including users, devices and data, and defines access environment factors like time, location and network. It also includes actions like inquiry, registration, modification and deletion.

Device/User Context: Personal information data such as user identity or group information are objects to be identified. Device information consists of types, operating systems, browsers and installed programs. Usually, this information can be extracted from the User-Agent of HTTP header [9], Geo API [10], and analyzed using device fingerprinting methods like OS fingerprinting [11], browser fingerprinting [12], etc.

Access Environment Context. When, where and via which network a device accesses enterprise network. It does not simply state the time of access but generalizes such information into a meaningful context such as clock-in time and hours worked. Access locations are divided into domestic and overseas. Domestic locations are further divided into inside/outside the company, and GPS information is included when available.

Service Use Context. Objects of access like the URI and database table, and use behavior. Here, access resources are identified by analyzing the URI which includes information of the HTTP header such as the GET and POST. Furthermore, use behavior can be analyzed (inquiry, registration, modification and deletion) by mapping them with database usage on the back end of the WAS.

Context collecting requires various traffic analysis techniques. It basically needs device/OS fingerprinting and an agent that can be installed to collect authentication request/result information from the authentication system and GPS information of devices. However, the agent is not a must in this proposal. Depending on policy, it separately defines context that needs to be collected and requests installation of the agent.

Most contexts are collected in a network but some need analysis on access status. For example, when a user uses two devices at once, context cannot be collected on a device level. Instead, it can be identified whether a user is on multiple devices by controlling the access status activated in the collection system.

5.2 Smart Behavioral Insight

When a user or a device accesses the enterprise network, various environment components are collected through context. Once a certain amount of behaviors are ac-cumulated, a user's set of behaviors can be turned into a pattern. A profile is defined based on the users past behavioral pattern. By managing this profile, one can man-age the history of the user and his/her device.

Context needs to be specified in order to turn behaviors into a pattern. Depending on the characteristics of a corporation or department, behaviors can be generalized based on such components as devices used, access time and access day (i.e. weekday or weekend). Here, it must be configured that a user's behavior maps with one of the context components that are comprised as a discrete set. In this case, user behaviors can be described in a standardized format.

To create a discriminating behavioral pattern, it is important to select components that will comprise a behavior. A behavior has a set of behavioral components. A user has one behavioral component of each behavior. For instance, when Behavior A is "access time", its behavioral components can be set as {a_1: AM, a_2: PM} or {a_1:0H ~ 6H, a_2:6H ~ 18H, a_3:18H ~ 24H}. Then, when a set of behaviors by a user or a device is defined Behavior A = {a_1, a_2,…, a_i}, Behavior B = {b_1, b_2,…, b_j},…, Behavior N = {n_1, n_2,…, n_k}, the current behavior of a 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})* (Fig. 3).

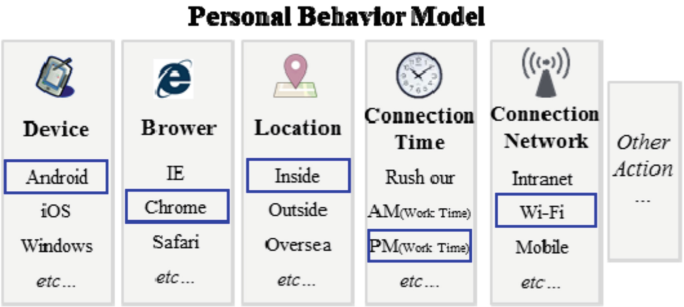


Fig. 3. User behavior model

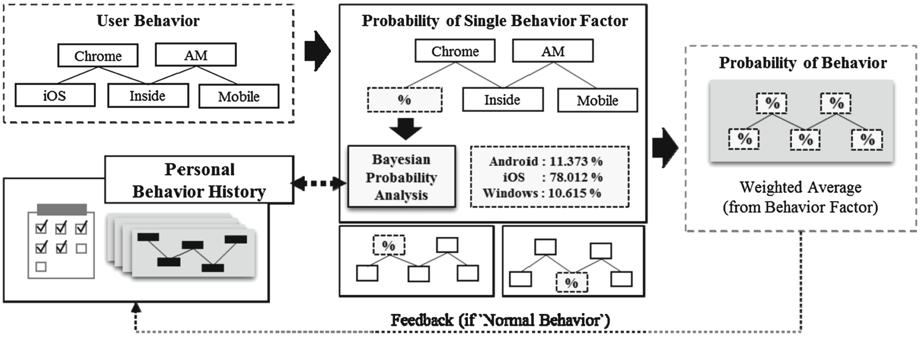

User Behavior
Chrome
AM
iOS
Inside
Mobile
Probability of Single Behavior Factor
Chrome
AM
%
Inside
Mobile
Bayesian Probability Analysis
Android : 11.373 %
iOS : 78.012 %
Windows : 10.615 %
Probability of Behavior
%
%
%
%
%
Weighted Average (from Behavior Factor)
Personal Behavior History
%
%
Feedback (if 'Normal Behavior')

Fig. 4. Possibility analysis of behavior with other factor by bayesian inference

Accumulating information on behaviors can analyze a user's access pattern in each context. Using *Bayesian Inference* [13], its likelihood can be estimated by analyzing how often each context component occurs and which behavioral component is highly likely to occur along with a specific behavioral component Fig. 4. Bayesian Probability theory generally used in SPAM classification based on frequency of a word in relation to word composition of a document [14]. In this study is not to decide a specific behavior pattern as abnormal, but to decide patterns different from the existing to be abnormal. Once the probability of each behavioral component is analyzed, overall probability can be derived by placing weightings on each behavioral component (which factors in work characteristics) and using the weighted average based on this. Weightings can be placed either across the board or per work unit. Discriminating behavioral components can get a higher weighting based on the analysis of the user's past behavioral data. As each individual differs in the way he/she uses a device at work and how much of his/her behavior has been turned into a pattern, weightings can be based on entropy analysis of an individual's behavioral components.

5.3 Context-Based Security Policy Administration

In order to maintain proper security levels per context, it should be possible to recognize a context and apply a dynamic policy accordingly. For instance, an access from a foreign country with a vulnerable Internet environment must go through a certain security app, while an access from a domestic location is only allowed to make inquiry into specific services. Environment components including user identity and device types should be factored in when determining enforcement of security policies.

As such, in a BYOD environment, each given situation should be identified with con-text and policies enforced based on it. A security policy must include at least one context and allow its administrator to configure the range and level of control with flexibility. An administrator-friendly GUI that can visually show the relations of sequence and inclusion is a must as policies need to utilize many components.

Determining which policy to apply can be based on users' access and use cycles. That is, there is a policy for when a device approaches an enterprise network, another one for real-time monitoring of violations after a device is connected, and yet another one for constant monitoring across the board. Also, once connected, the device should be monitored to detect any violation of the policy (that only includes constant context such as accessing user and device), and the operating system of the device within an activated session. A policy that includes changeable context such as location and type of services accessed needs to be continuously monitored for potential violation until the device is disconnected.

As the number of established policies increases, processing policies may hinder performance. This is because there is a policy to be enforced when a device approaches an enterprise network and another one for real-time monitoring after a device is connected. In such a situation, monitoring performance can be improved by structuring policies into a decision tree as policies are comprised of a limited number of context components.

5.4 Multi-level Dynamic Control

When a policy is violated or a suspicious access/use behavior occurs, no benefit of BYOD can be earned from simply cutting them off. Uniform ways of control are bound to lower usability no matter how diverse context-based policies are operated. As such, BYOD maintains continuity of work while keeping more robust authentication methods or stricter control over devices for more precise judgment when detecting a violation of policy or suspicious abnormal behavior. Extreme control such as immediate cut-off should be enforced for mission-critical areas of a corporation. However, a multi-level control policy is required to verify suspicious behaviors or violations of policy. Multi-factor authentication using OTP or installation of an agent to gain control over a device is an example of multi-level control policy. When an access deviates significantly from a user's usual access pattern, a strengthened multi-factor authentication verifies the user one more time before giving permission. A user who is on a business trip to a country with vulnerable security should install an agent in his access device to temporarily raise its level of security as required. In addition, if an unusual volume of information is requested or a scarcely used service is accessed, enforcing extra security controls can keep the level of security of a corporation in a dynamic and flexible manner.

Such control requires real-time collection of context and immediate control measures to detect any violation of policy or suspicious behavior. To ensure actual control, it must be coupled with authentication portals like the captive portal tech-nique or security equipment like NAC and the firewall (web firewall) already in place by corporations. Most couplings can be done through a standardized method like SNMP but also made available using a separate API. Another option is to couple with equipment like an MDM that controls data inside a device.

6 Conclusion

The practice of BYOD has diversified the previously standardized conventional work environment. Such diversification has made it difficult to control security with traditional security equipment. Security threats like information leaks, challenges in managing personal devices, and establishing effective security policies are major challenges hindering the spread of BYOD environments.

Given that users are already using their personal devices at work, however, corporations should utilize them to raise productivity rather than restrict them all. In order to achieve this, developing security technologies is required to analyze and address security threats in BYOD environments. This study defined smart access control as a security technology required for BYOD environments and proposed a security framework that satisfies such a requirement. The proposed security framework for BYOD environments can transform low-level information into an intuitively meaningful context. It also allows corporations to establish context-based, flexible security policies using accessing objects, access environments and use behaviors, and control policies for each level depending on context. In addition, by modeling user's behavioral patterns as a context, it creates profiles for personalized patterns, based on whether it can detect abnormal behaviors that were not previously recognizable, thereby enforcing stricter security policies to enlarge the possibility of behavior-based detection.

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

References

1. IDG Deep Dive: Guide to BYOD Strategy. IDG Korea (2012)
2. Johnson, K.: Mobility/BYOD Security Survey. SANS Institute (2012)
3. Miller, K.W., Voas, J., Hurlburt, G.F.: BYOD: security and privacy considerations. IT Prof. **14**(5), 53–55 (2012)
4. Symantec, Smartphone Honey Stick Project. http://www.symantec.com
5. Inverse, PacketFence. http://www.packetfence.org
6. Henderson, T.: How mobile device management works. IT WORLD (2011)
7. Frias-Martinez, V., Stolfo, S.J., Keromytis, A.D.: Behavior-based network access control: a proof-of-concept. In: Wu, T-C., Lei, C-L., Rijmen, V., Lee, D-T. (eds.) ISC 2008. LNCS, vol. 5222, pp. 175–190. Springer, Heidelberg (2008)
8. D'Alconzo, A.: A distribution-based approach to anomaly detection and application to 3G mobile traffic. In: GLOBECOM, pp. 1–8 (2009)
9. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Berners-Lee, T.: Hypertext Transfer Protocol-HTTP/1.1, RFC 2068 (1997)
10. W3C: Geolocation API. http://en.wikipedia.org/wiki/W3C_Geolocation_API
11. Nmap: Remote OS Detection. http://nmap.org
12. Kohno, T., Broido, A., Claffy, K.: Remote physical device fingerprinting. IEEE Trans. Dependable Secure Comput. **2**(2), 93–108 (2005)
13. Jose, M.B., Smith, A.F.M.: Bayesian Theory. Wiley, New York (1994)
14. Graham, P.: A Plan for Spam. http://www.paulgraham.com/spam.html