International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.229-238
http://dx.doi.org/10.14257/ijsia.2014.8.4.20

Study on Enhancing Vulnerability Evaluations for BYOD Security

Kyong-jin Kim* and Seng-phil Hong**

Sungshin Women's University
{kyongjin, philhong}@sungshin.ac.kr

Abstract

As the mobile phone device is becoming the most indispensable devices user own, such device connecting to the corporate network is also rapidly changing. However there are many people using such Internet services from personal mobile devices with ignoring the basic concepts of information security. Especially in BYOD workplace, users as work tools can access sensitive corporate information from public areas. BYOD security challenges for corporate information are becoming more and more of a concern. In this paper, we are to focus on the private and confidential corporate information accessed from the attacker. We propose the network model applying multiplicative security to test using the simulator, and then prove the safety by attack scenarios in BYOD environments.

Keywords: *BYOD (Bring-your-own-devices), Mobile computing device, Corporate information, Personal information, Security vulnerability evaluation*

1. Introduction

These days the technology as regards the concepts of mobility and connectivity has been rapidly change, users using the Internet have become subordination of smart services such as mobile networking, social networking and cloud computing, whereupon there are many people using such services from personal mobile devices in global network while ignoring the basic concepts of information security. Mobile security is therefore becoming more and more of a concern. It raises the issue constantly in mobile environments; 79 percent of businesses have had a mobile security incident in the past year, according to the report in 2013 by Check Point Software Technologies Ltd [2], which is one of the most important venders in networking security, published the report related to mobility research security.

In particular, as the smart phone is becoming the most indispensable devices user own. By using this, their business is able to work through smart mobiles. The other word for such environments is BYOD that stands for a bring-your-own-devices [1, 3], and it is a growing trend in companies. As Gartner trend report [9], it predicts that personal mobile devices connecting to the corporate network were rapidly changing. It refers to the fact that users including employees and managers bring their own mobile computing devices such as smart phones, tablets to the workplace for work and connectivity on the business network, and then they access to business data without considering the information security. In a BYOD workplace, users using personal mobile devices as work tools can access sensitive or confidential information from public areas. Also unauthorized users like terminated employees can keep their own devices and even the data contained within. These factors can pose a serious threat because of working with sensitive corporate information [3, 5, 8].
[1]

[1] * First author, ** Corresponding author

ISSN: 1738-9976 IJSIA

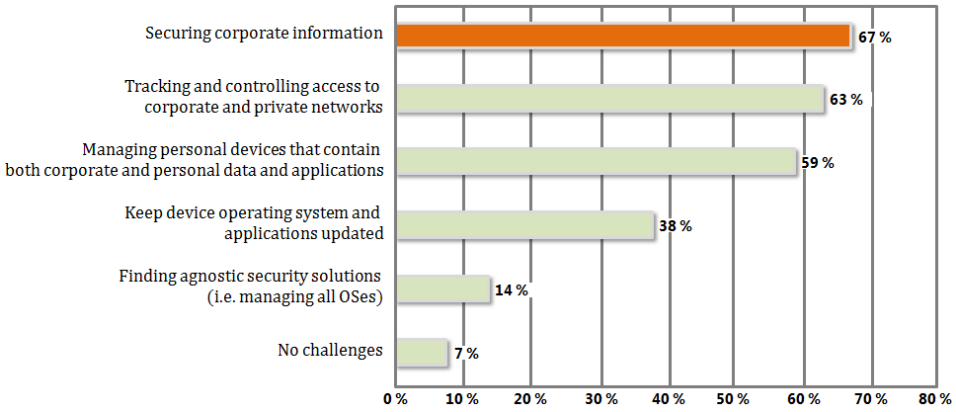

Figure 1. Challenges with BYOD [2]

According to the report [2], their main point is many companies have had costly BYOD mobile security incidents. Also the report found that BYOD brings security challenges for corporate information. As shown in Figure 1, 67 percent of companies said the most common challenge faced by organizations in adopting BYOD was securing corporate information.

In this paper, we are to focus on the private data and confidential corporate information accessed from the attacker in BYOD environments. To protect the sensitive data, we considered it necessary to develop the network architecture applying multiplicative security factors rather than traditional security technologies for potential threats. So we do need to be able to recognize what the impact on user's private is and what the impact of technological security innovation for business is.

The rest of this paper is organized as follows. In Section 2, we discuss various security threats related to mobile office environments, especially the BYOD, and suggest alternatives for security. Section 3 introduces our network model for security testing and we present an overall graph to attack paths by presenting a network model. Section 4 presents the simulation for security vulnerability evaluations that is proves the security risks of the vulnerability through performing tests. Finally, in Section 5, we state the conclusions.

2. Security Threats in BYOD Environment

Security threats on wireless networks are constantly increasing. Public or private wireless networking get heavy use because personal mobile devices have various functionalities such as Bluetooth, wireless LAN, and communication networks in general. Another reason trying to store service bills about wireless data, more and more mobile device users can utilize wireless access point that is retrieved by random. If a hacker has an intention of attacking and provides a wireless access point with a malicious code, mobile phone user can be catch a virus or a malware just accessing such an access point [1]. Thus wireless connection environments on a smart device can be attacked more easily than conventional computer environments that caught a malicious code when a harmful website was visited. There are several cases [5, 7] in which they collect the personal and location information in smart phones or tablets using the vulnerability of a wireless networking. And also the possibility is on the rise because personal information is exposed through fabricated wireless access points.

Although wireless environments pose these security threats to our environments, a mobile environment in companies, that is called BYOD, is becoming a new trend. In the following Figure, various threats that affects BYOD are to separate out, and then areas in a mobile environment based on this classification pose what each area needs.

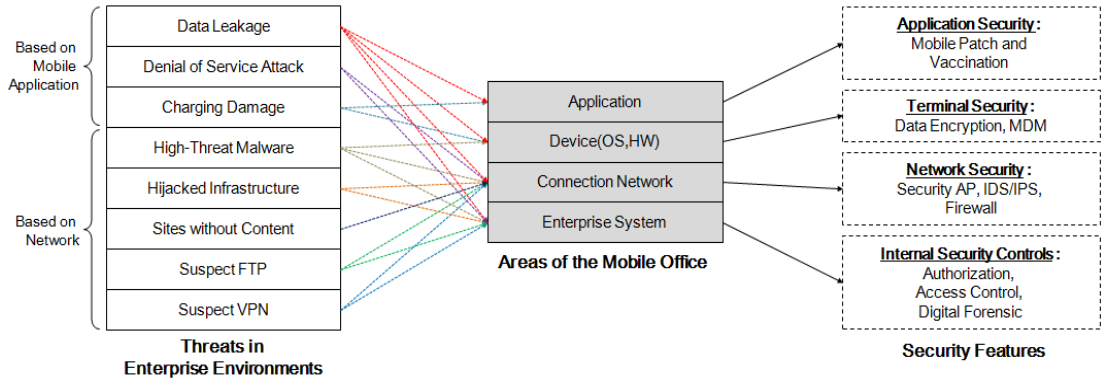

Figure 2. Alternatives for Each Area of Mobile Environments Related to Security

There are potential threats through the mobile application including data leakage, denial of service attack, charging damage [3, 7]. The risk of data leakage on mobile platforms is particularly acute. Mobile devices are designed to share data in the cloud and have no general purpose file system in business to share. And in an environmental sense mean that the service is used through open networks, the distributed denial of service (DDoS) attacks is to deny the enterprise service under attack to mobile device users. There are also inherent threat issues with the mobile computing devices that have personal information because most BYOD programs don't make a clear separation between personal and corporate data and applications. The charging damage is one of them.

There is another aspect to this inherent threats based on network. It is included [4]: high-threat malware, hijacked infrastructure, sites without content, suspect FTP, and suspect VPN. These threats are connections to malicious domains that are known malware threat site or hijacked infrastructure. Also in the same manner, VPN that gets the business dedicated line is connections from within an organization to suspicious VPN sites.

3. Network Model for Security Testing

3.1. Network Model based on Mobile Computing Environments

As shown in Figure 2, the network model based mobile computing and networking environments can be tested using a simulating methodology to defend latent security threats and vulnerabilities, which refers to Section 2. It can be composed of various entities; the terminal device such as smart phones and tablets, the application in mobile computing devices, the connection network, and the enterprise system related to business tasks (refer to Figure 3). In this paper, we assort it into five domains by connection devices and network environments.

- **Domain 1** : the terminal – *including a hardware, an operating system and an application*

This is the mobile computing device that users use for work, so this area includes various kinds such as a smart phone, a tablet, and a notepad. It is composed of two or more ingredients; but we are focused on a mobile operating system and a mobile application. A mobile operating system combines the features of a general computer operating system with other features related to mobile. It also operates the radio and other hardware, and manages various applications in mobile computing devices. A mobile application is software that can run on a mobile computing device, and then it will allow the device to perform specific tasks.

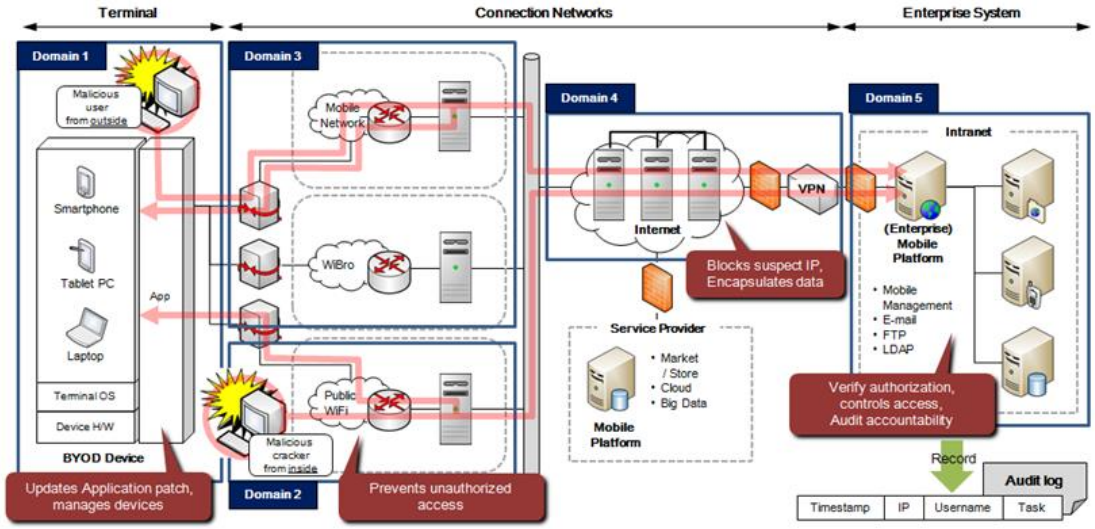

Figure 3. Network Model based on Mobile Networking Environments

- **Domain 2**: the public wireless networks

This is a technology that does the transmitting without using cables or fiber optics, and it includes a wireless LAN, Wi-Fi. It supports the environment of wireless local area networks, and then users can access to the network around supported anywhere by a wireless LAN. In particular, users have access to wireless network services at public areas, which they can use for personal business tasks.

- **Domain 3** : the mobile networks – *or the communication networks*

This is a technology to enable communication on the move, and it includes communication networks such as 3G, 4G and Wibro. Users are working at mobile area with own mobile device regardless of time or place, this technology provides mobile devices to network resources like video, audio, or data using a wireless network connect mode.

- **Domain 4** : the wired networks – *including DMZ and VPN*

Although a wireless network should provide mobile networking services with mobile devices, basically, each technology device can be connected to wire networks to use enterprise services. And thus mobile networking services are provided by wired connectivity that connects to the internal enterprise network or the task server. It should be composed of various security features such as a usage of authorized device and a traffic blocking; the infrastructure must be designed to protect for the enterprise that retained business-critical information.

- **Domain 5** : the enterprise system

The business internal system for the mobile networking service furnishes users who were working and requested it with business services. It must also manage historical logs about the system access, and it should record detailed task statements to carry out works.

Based on classified domains, attacker types are divided into two groups; the outside and the inside. If we are focused on the leaks of corporate information, it may be processed as follows; the outside attacker is in *Domain 1*, and points to *Domain 5* as a target for attacks. This way the attacker infringes on *Domain 5* – that there is the enterprise server – through *Domain 1*, *Domain 3* and *Domain 4*. The inside attacker is in *Domain 2*, this is also a target for attacks is the enterprise server in *Domain 5* to infringe business environments. So the attacker tries to access *Domain 5* via *Domain 2*, *Domain 3* and *Domain 4*. It may indicate a scenario from the other aspect like privacy; the outside attacker can infringe mobile devices for private in *Domain 1*, which means they are all connected to each other in mobile communication networks. It is how to attack, the access to privacy start at *Domain 1* and return to it through *Domain 3*. The inside attacker can also access mobile computing devices in *Domain 1* connecting to a wireless network from *Domain 2*.

3.2. Security Threats Evaluations by Attack Scenarios

In this section, we show results from security threats evaluations conducted by attack scenarios based on proposed network model in mobile networking environments. Figure 4 shows a graph that represents to grasp attack paths in our network model based on mobile computing and networking environments. It indicates several statuses that attack or infringe by network environments. By presenting a graph like this, we can grasp attack paths easily.

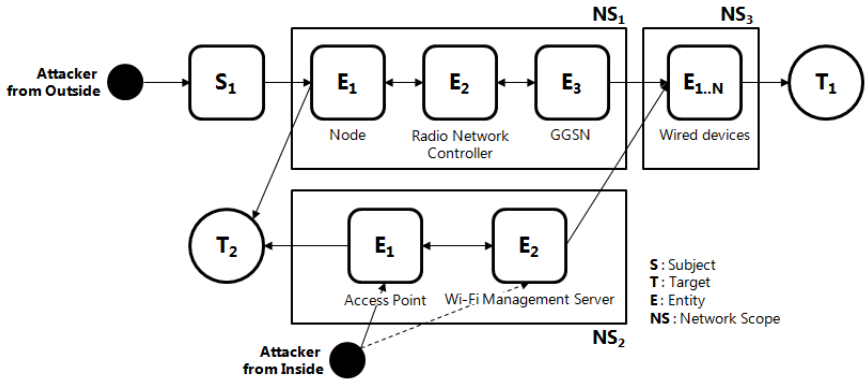

Figure 3. Graph for Path by Attack Cases

It is derived 4 attack paths for two targets including private and business from a graph based on network model to the below:

- Set *S, T, E,* and *NS* in a graph *G*,
  subject using mobile computing devices S_1; target to attack $T = (T_1, T_2)$;
  necessary equipments for networking $E = (E_1, E_2, E_3, \ldots, E_n)$; *NS* is set to the entity *E*;
- Access to *T* by attack paths. Then:
  - The outside attack is initiated from *Domain 1*.
    Case 1. $S_1 \rightarrow NS_1\{E_1 \rightarrow E_2 \rightarrow E_3\} \rightarrow NS_3\{E_{1..N}\} \rightarrow T_1$
    Case 2. $S_1 \rightarrow NS_1\{E_1\} \rightarrow T_2$
  - The inside attack is initiated from *Domain 2*.
    Case 3. $NS_2\{(E_1 \rightarrow E_2)_{or}\ E_2\} \rightarrow NS_3\{E_{1..N}\} \rightarrow T_1$
    Case 4. $NS_2\{(E_2 \rightarrow E_1)_{or}\ E_1\} \rightarrow T_2$

In such scenarios, there are several and various methods how to calculate quantification for security vulnerability, and we perform security threats evaluation of our network model based on CVSS[6] that is the best known method of them as shown in Table 1. First, we need to

capture three impact conditions, which are access to and impact on the target. **Access Vector(AV)**, that is whether or not the vulnerability is exploitable locally or remotely; **Access Complexity(AC)**, that is the complexity of attack required to exploit the vulnerability once an attacker has access to the target system; **Authentication (Au)**, that is whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability. The target system judges of the damage including **Confidential (C)**, **Integrity (I)** and **Availability (A)** by such three impact values.

Each case is calculated on the basis of CVSS that illustrated how changes in metric values influence the scores. It has simply the following expressions:

$\boldsymbol{TemporalScore}_i = case_i \times$ E(F:0.95) × RL(OF:0.87) × RC(C:0.9),

if $i \in$ number of cases, and then Round $\boldsymbol{TemporalScore}_i$ to one decimal.

And then, the environmental score of cases is calculated on each $\boldsymbol{TemporalScore}_i$ of $case_i$:

$\boldsymbol{EnvironmentalScore}_i$ = AT(about 1.589) + ((10-AT(about 1.589)) × CDP_x) × TD_y,

if $i \in$ number of cases, None:$0 \le x \le$ High:0.5 and None[0%] $\le y \le$ High[76-100%], and then Round $\boldsymbol{EnvironmentalScore}_i$ to one decimal

* AT is impacted by *Impact Sub score Modifiers* = {CR:H(1.51), IR:M(1.0), AR:M(1.0)}

Case 1: **AV** has '*Network* (*N*)' because it is possible to access far in the distance. This needs for the expertise like a socio technological method to access, and for that reason **AC** has '*Medium* (*M*)' about the complexity of attack. To access the enterprise interior system, **Au** sets up '*Single*(*S*)' since it is needed to use the login including password, single-sign-on, and certificates. For example, if this interior system was infected with the malware, it may be almost entirely exposed to the danger. Each of attack impact values has '*Complete*' to need to consider the most dangerous case scenario. A base score of case 1 is calculated by a temporal score including vulnerability values, and as a result it is a score of 8.5. The base vector of this vulnerability can be represented **AV**:*N*/**AC**:*M*/**Au**:*S*/**C**:*C*/**I**:*C*/**A**:*C*.

Case 2: To enable the attack of privacy from far away, **AV** sets up '*Network*(*N*)'. **AC** has '*Medium*(*M*)' because it needs for some expertise to access mobile devices. Case 2, what an attacker accesses the target device to the mobile networks using mobiles, cannot cause vulnerability to need to be authenticated, though it may lead to other problems, and for that reason Au has '*None*(*N*)'. Although an attacker accesses to a lot of methods and occurs many problems, this case is the most important in **C** from the individual perspective with regard to privacy, and then **C** has '*Complete*(*C*)'. And other attack impacts set up '*Partial*(*P*)' because mobiles have a restricted access and performance. A base score of case 2 is calculated by a temporal score related to vulnerability impact values, so that the result score is 8.3. The base vector of this vulnerability can be represented **AV**:*N*/**AC**:*M*/**Au**:*N*/**C**:*C*/**I**:*P*/**A**:*P*.

Case 3: **AV** sets up '*Adjacent Network*(*A*)' because it is possible to access and attack to be close. **AC** has '*Low*(*L*)' since the inside attacker can have a command of a penetration. To access the enterprise interior system, **Au**, like case 1 sets up '*Single*(*S*)' since it is needed to use the login. Also each of attack impact values has '*Complete*(*C*)' to need to consider the most dangerous case scenario in the same way as case 1. A base score of Case 3 is calculated by a temporal score including vulnerability values, and as a result it is a score of 7.7. If this attack is enable to access far in the distance using a public Wi-Fi, **AV** has '*Network*(*N*)'. So it is recalculated by a temporal score, and as a result it is a score of 9. Additionally, a base score has the highest score in attack options since an attacker accesses to a lot of methods and occurs many problems. Thus the base vector of this vulnerability can be represented **AV**:*N*/**AC**:*M*/**Au**:*S*/**C**:*C*/**I**:*C*/**A**:*C*.

Case 4: **AV** has '*Adjacent Network*(*A*)' and **AC** sets up '*Low*(*L*)' since the inside attacker can have a command of a penetration in the same way as Case 3. On the other hand, there is

no need to use the authentication for anyone in the Internet, which can access to it through a public Wi-Fi, so **Au** has '*None*(*N*)'. This, like case 2 focuses on the individual perspective about privacy, **C** has '*Complete*(*C*)' and other attack impacts set up '*Partial*(*P*)'. A base score of case 4 is calculated by a temporal score including vulnerability values, and as a result it is a score of 7.3. Also **AV** can have '*Network*(*N*)' in the same way as Case 3. So it is recalculated by a temporal score, and as a result it is a score of 9. Thus the base vector of this vulnerability can be represented **AV**:*N*/**AC**:*L*/**Au**:*N*/**C**:*C*/**I**:*P*/**A**:*P*.

Table 1. Analysis on a Case-by-Case Basis

		Case 1	Case 2	Case 3	Case 4
Base Multiple	*Access Vector (AV)*	***N*** : 1.0	***N*** : 1.0	***N*** : 1.0 (or ***A*** : 0.646)	***N*** : 1.0 (or ***A*** : 0.646)
	Access Complexity (AC)	***M*** : 0.61	***M*** : 0.61	***L*** : 0.71	***L*** : 0.71
	Authentication (Au)	***S*** : 0.56	***N*** : 0.704	***S*** : 0.56	***N*** : 0.704
	Confidentiality Impact (C)	***C*** : 0.66	***C*** : 0.66	***C*** : 0.66	***C*** : 0.66
	Integrity Impact (I)	***C*** : 0.66	***P*** : 0.275	***C*** : 0.66	***P*** : 0.275
	Availability Impact (A)	***C*** : 0.66	***P*** : 0.275	***C*** : 0.66	***P*** : 0.275
Base Score		8.5	9 (or 7.7)	8.3	9 (or 7.3)

On the basis of this, if a system model is applied from consolidated security functions complementing such threats and vulnerabilities, the vulnerability patch level of our system model that, if applied properly, is '*Official-Fix*', and the vulnerability reliability is of course '*Confirmed*'. Supposing the confidential in our system model is more important than that of general systems, and using environment values including the **Collateral Damage Potential** (Low:light loss≤**CDP**≤High:catastrophic loss) and the **Target Distribution** (Low[0-25%]≤**TD**≤High[76-100%]), the value or range of environment scores have from 1.8 to 8.5.

The details about calculation methods is completely beyond the pale, thus this paper represents nothing but a result. We tested the simulation to evaluate by defining a set of each value simply.

4. Simulation for Security Vulnerability Evaluations

In this section, we installed wired and wireless networks which can be connected to enterprise services, similar to BYOD environments. And the simulation is performed using each case how such environments impact with the security aspects of privacy and business.

We propose a test simulation, and do a performance using the simulator (OPNET++ tool) for experiment. It has also the ability to use the same packet to perform, and then evaluates performance on a vulnerability level from 0 to 10 since it can obtain the average value through a series of tests.

The Figure below shows graphs by attack path for purpose, this is shown with considering the impact on security, which is the horizontal axis on the graph, represents vulnerabilities of network model with a base score in the range 0.0-10.0. If the system with security functions applied is consolidated, it has the minimum value – almost zero. On the contrary, the maximum value means that the system model without security functions applied is vulnerable to attack. And the vertical axis, representing the average time taken that could have occurred in scenarios. We indicate that test simulation commonly consists of two graphs by attacker type of scenarios.

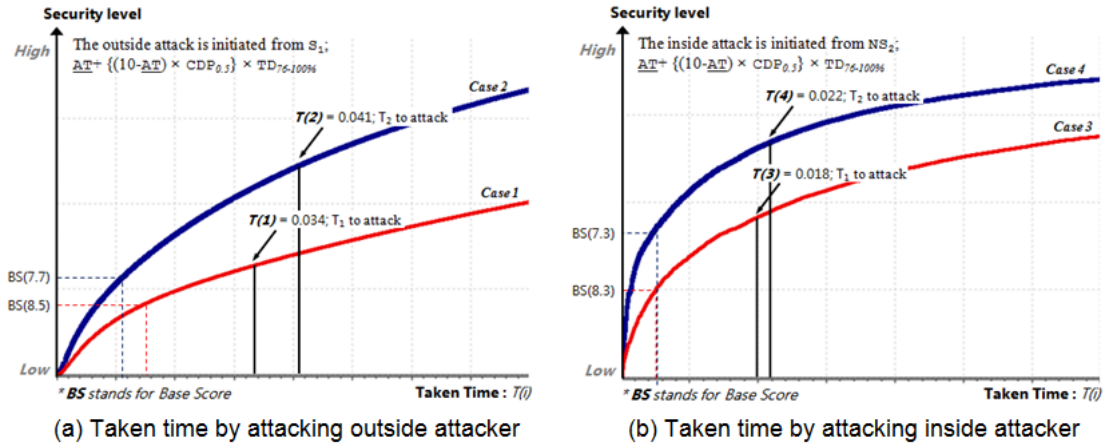

Figure 4. Impact of Applying Security Factors by Attacker Type

Case 1 and Case 2 are a way of attacking the outside attacker, as the security become stronger in system, this graph (a) represents that vulnerabilities are decreased and the access time for attack takes a long time. The graph (b) including Case 3 and Case 4 is a way of attacking the inside attacker, this is showing similar results as the security become stronger in the system model.

Based on these tests we performed, we can get quantitative information about the safety to be secure-effective since our suggested model is calculated by the vulnerability.

5. Conclusions and Future Research

Wireless environments on mobile computing devices can be attacked more easily than conventional computer environments, and also raising the possibility that personal information is exposed to danger in BYOD environments. Hence, we discuss various threats that affect BYOD and suggest the security function of each alternative based area of latent threats. We introduced our proposed network model to simulate using a wireless connect mode on condition that mobile computing devices have service for business's work. By presenting the network model, we represented that a graph indicates attack paths. We shows results from security threats evaluations conducted by attack scenarios based on proposed model, and then proved the security risks of the vulnerability in BYOD environments through performing tests using the simulator. These results met expectations; vulnerabilities are decreased and the access time for attack takes a long time.

This paper will help to get quantitative information about the safety to be secure-effective, and will consider the feasible possibility for changing enterprise environments.

Acknowledgements

This work was supported by the Sungshin Women's University Research Grant of 2014.

References

[1] "BYOD and Security", Info. Sec. Institute, TECH&GADGETS Articles, **(2013)** January, Available at http://www.business2community.com/tech-gadgets.

[2] "The Impact of Mobile Devices on Information Security: A Survey of It Professionals", Dimensional Research & Check Point Software Technologies Ltd., **(2013)** June, Available at http://www.dimensionalresearch.com.

[3] P. K. Gajar, A. Ghosh and S. Rai, "Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies", Journal of Global Research in Computer Science, vol. 4, no. 4, **(2013)** April.
[4] "Cisco 2014 Annual Security Report", Cisco systems Inc., **(2014)** January, Available at http://www.cisco.com.
[5] "Privacy trends 2014-Privacy protection in the age of technology", EYGM Ltd., Insights on governance: risk and compliance, **(2014)** January.
[6] "National Insitute of Standards and Technology", NVD Common Vulnerability Scoring System Support, vol. 2, Available at http://nvd.nist.gov/.
[7] D. Gessner, J. Girao, G. Karame and W. Li, "Towards a User-Friendly Security-Enhancing BYOD Solution", Nec Technical Journal, vol. 7, no. 3, **(2013)** March, pp. 113-116.
[8] M. Song and K. Lee, "Proposal of MDM Management Framework for BYOD Use of Large Companies", International Journal of Smart Home, vol. 8, no. 1, **(2014)** January, pp. 123-128.
[9] Gartner, "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes", Available at http://www.gartner.com/newsroom, **(2013)** May 1.

Authors

Kyong-jin Kim, she graduated with a B.S. in 2007, with a M.S. in 2009 and with a Ph.D. in 2013 from the Sungshin Women's University. She joined the Information Security lab as a postdoctoral fellow in March 2013. Her research interests focus on privacy protection, security framework, and access control.

Seng-phil Hong, he received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for Ph.D at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from KAIST University in Korea. He is actively involved in teach and research in information security at Sungshin Women's University, Korea. His research interests include access control, security architecture, Privacy, and e-business security.