

## A Research on Security Awareness and Countermeasures for the Single Server

Hyuk-Jin Son<sup>1</sup> and Seungdo Jeong<sup>2,\*</sup>

<sup>1</sup> IT MBA, Graduate School of Business Administration,  
Hanyang Cyber University, Seoul, Korea

<sup>2</sup> Department of Information and Communication Engineering,  
Hanyang Cyber University, Seoul, Korea

\*Corresponding author, [sjeong@hycu.ac.kr](mailto:sjeong@hycu.ac.kr)

<sup>1</sup>[sonhj8@gmail.com](mailto:sonhj8@gmail.com)

### Abstract

*Accompanying to the growing utilization and dependency on the internet and the ICT (Information and Communication Technology), the threat by hacking, malicious code and virus are rising as serious problems. Especially, the single server which is hosted by professional hosting companies is exposed to diverse attack, and then abused as malicious server. Even though responsibility for the security problem on the single server is not to hosting company but to single server user, almost of users have little security awareness about the single server security. Thus, in this paper, we first survey the cause of increase of a single server, and then investigate reasons inducing vulnerable points of the single server. By inquiry with questionnaires about security awareness and necessity of security reinforcement for a single server, this paper suggests countermeasures for security of the single server including technical measures with low burden.*

**Keywords:** Server Security, Security Awareness, Single Server, Security Countermeasures, Server Intrusion

### 1. Introduction

Recently, growth of the informatization accelerates the utilization and dependency on the internet and the ICT (Information and Communication Technology) in almost all industries. And furthermore, huge supply of smart phone raises the usage rate of the internet more rapidly [1]. According to providing of diverse contents and services through the internet, the number of server has being increased steadily. Accompanying to the growing, as an adverse effect, the threat by hacking and malicious code has emerged as serious problems. It causes severe social and economic losses [2, 3]. Thus, thorough preparation is required to reduce an opposite effects caused by hacking, malicious codes, virus, and so on.

Most major companies with enough capital can maintain strong server security management by employed own experts or through entrustment to professional security company. However, the single servers operated by small companies or the private server by one user are exposed to many threats by intrusion with almost defenseless. The Korea Internet and Security Agency (KISA) offers establishing specification and its manual for the server security as well as self-inspection tools [4]. However, it is merely online guidance; furthermore, it is difficult to be accessed by inexpert users. Therefore, inexpert and general users cannot recognize recommended specification for the server security well. Even though they know that, most of users cannot apply those to their own server.

The recommended specification for the server security does not guarantee the perfect defense of all kinds of threats. However, the abuse of the single server as adverse effect is reduced through by establishing the key specifications. Thus, this paper investigates reasons for increasing single server and identifies weak points of the single server security, and then, suggests countermeasures according to the weak points.

This paper is organized as follows. We briefly review the trend of the single server including the risk and the state of the security for the single server in section 2. Section 3 explains current security awareness of the single server users. In Section 4, we suggest countermeasures about the single server including technical configurations. Finally, Section 5 summarizes and concludes this paper.

## 2. Recent Trend of the Single Server

### 2.1. The Risk of the Single Server

Most of small-scale companies use web service or server service hosted by the professional hosting company as shown in the Figure 1.

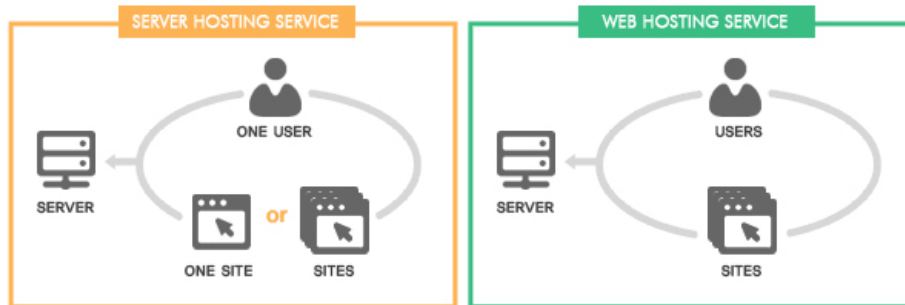
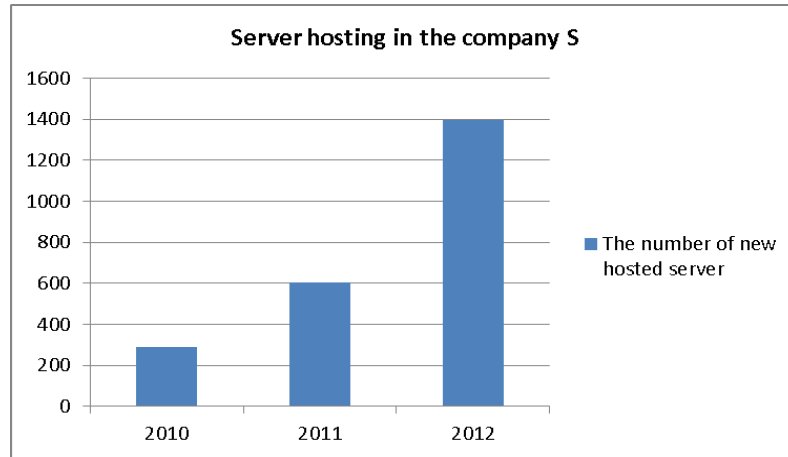


Figure 1. Concept of the Server and Web Hosting Service

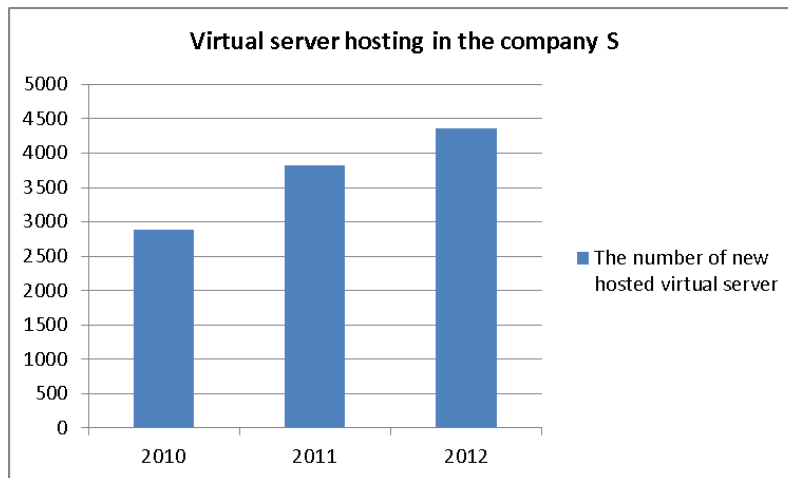
In the web hosting service, the professional hosting company assigns specified space for the requested user in the server. The hosting company has responsibility on managing the server, thus, establishes the server security with diverse specifications. In the contrast, the server hosting service offers only the server without any configuration about the server security. In this case, the user should manage the lent server. All responsibility related to the server security is up to the user. However, most of the users who have lent the server from the professional hosting company have almost no knowledge about the server security. These servers with weak security configuration have high possibility for intrusion. Thus, it could be easily abused as the server which may cause the DDoS attack and could induce secondary and tertiary damages.

### 2.2. The State of the Server Security in the Single Server

Due to spreading virtual server service through xen, hyper-v, and VMware as well as increasing cheap server hosting service as shown in the Figure 2 and Figure 3, the single server used by the individual increases rapidly. Another reason of the growing single server is owing to the restriction in the web hosting service. In the web hosting service, the user uses only restricted space in the server and shares one server with other users, thus, there are many restriction. For these reasons, many users prefer to use the single server freely. However it causes many problems associated with the server security.

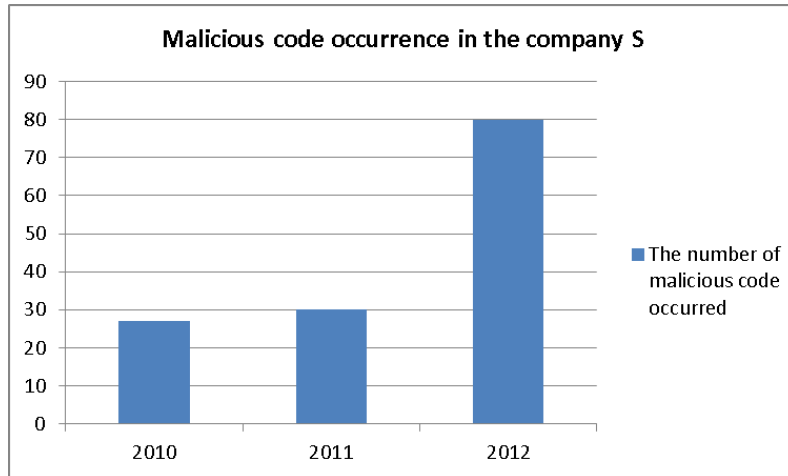


**Figure 2. The Trend of the Server Hosting Service**

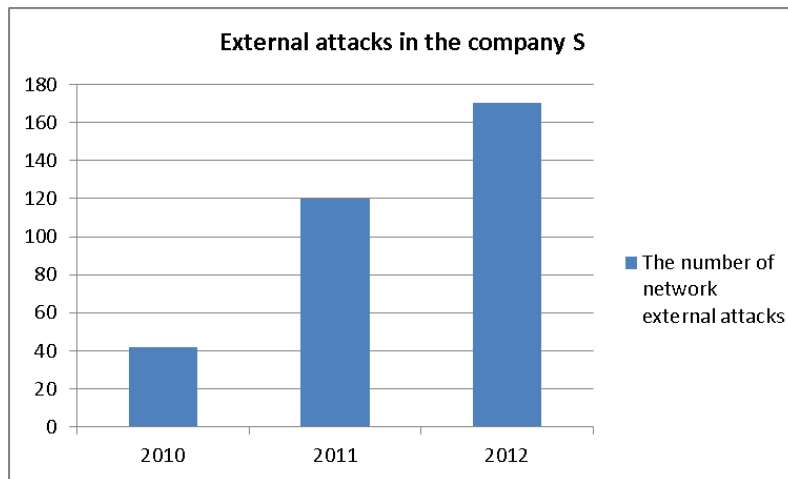


**Figure 3. The Trend of the Virtual Server Service**

The core of the problems is the growing single server with weak point related to the security because users who have little knowledge about the server security use the hosted server by themselves. Figure 4 and 5 show the number of server including malicious code and the external attacks occurred during recent 3 years, respectively, in the professional hosting company S. The target of this investigation includes the single server hosted by the company and the server of which OS managed by the user directly.



**Figure 4. The Trend of the Number of Malicious Code Occurrence**

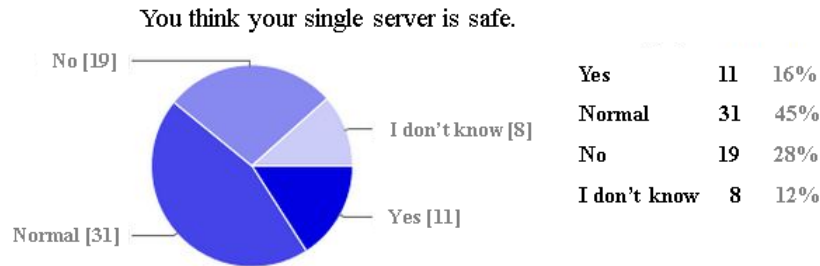


**Figure 5. The Trend of the External Attacks to the Single Server**

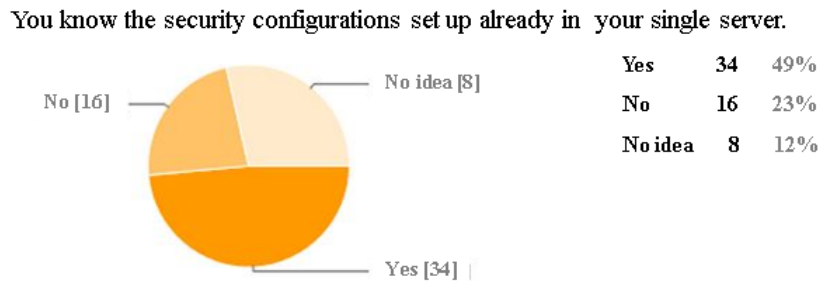
As shown in the figures, the seriousness related to the weakness of the single server security increases rapidly as time goes on. The fundamental reason is due to user's immaturity for the server security, thus, the server is exposed to the external attacks, and then, abused to spread a number of malicious codes. Many researchers suggest technical approaches with the general web firewalls such as mod\_security [5], webknight [6], and the network firewalls by configuring the operating system or by using diverse tools [7]. The methods for the server security proposed by these researches are very useful to the experts and related companies, however, inexpert users which manage the single server or the general users have difficulty to understand the content and then apply that to their own servers. Therefore, in order to cope with the problems caused by the growing single server with weak security configuration, researches for the countermeasures are required.

### 3. A Survey for the Security Awareness

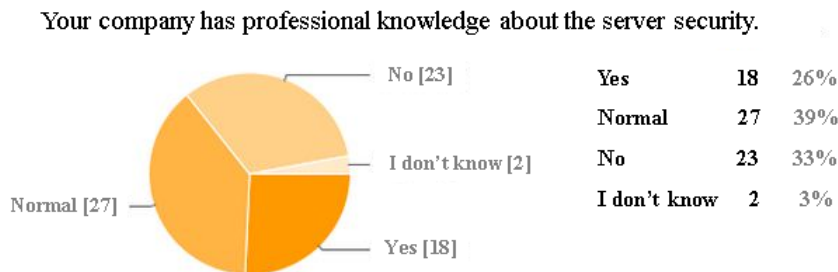
As increasing the single server, occurrence of dysfunction by intrusion also increase. Seriousness of the problems is tightly associated with the ignorance of the user about the security awareness. Most of users merely assume that the performance of the single server hosting might better than the one of web hosting service including the perspective of the cost and the degree of freedom, thus, they easily move the hosted service from the web to the server without any recognition about the server security. To identify these matters we survey the security awareness of the users by inquiring with questionnaires. First we put questions to the single server users related to management and security.



**Figure 6. Awareness for the Safety of the Single Server**

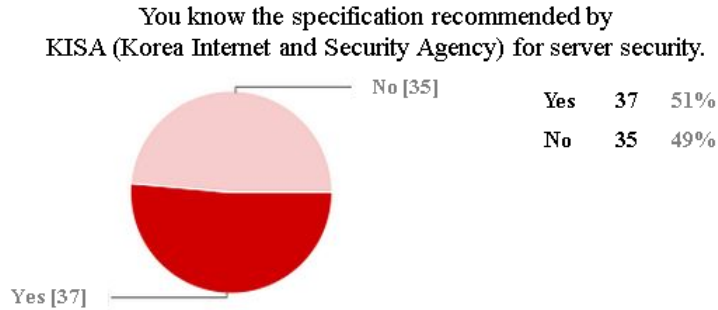


**Figure 7. Cognition for the Security Configuration in the Own Server**

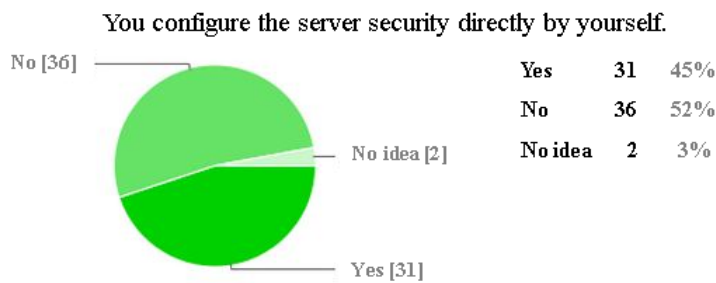


**Figure 8. Knowledge about the Server Security**

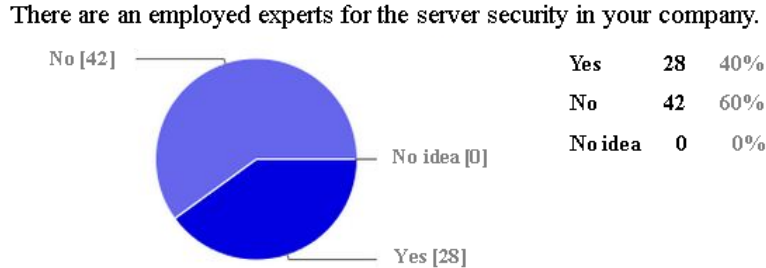
From Figures 6 to 8, we show the surveying result about the security awareness of the single server users. As shown in the Figure 6, more than half users consider their server might be safe. However, they have not enough knowledge about the server security as shown in the Figures 7 and 8. It means that there are many potential risks associated with the security.



**Figure 9. Cognition for the Specification by KISA**



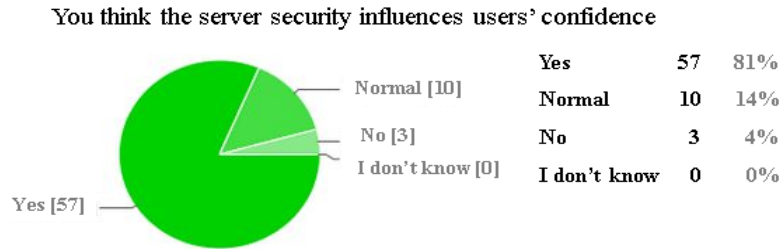
**Figure 10. Self-configuration Ratio for the Server**



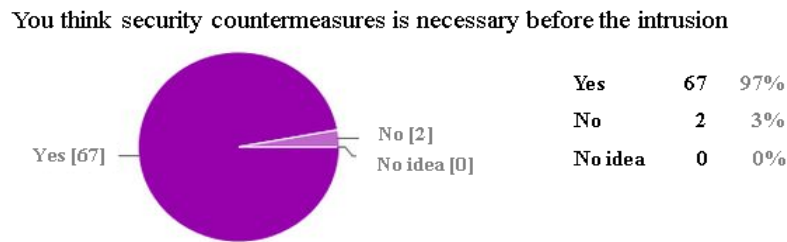
**Figure 11. The Presence of the Security Experts**

These tendencies are more definitely recognized from the results in Figures 9 to 11. Nevertheless nearly half of users don't know the security specification by recommended by KISA (Korea Internet and Security Agency), most of them configure their server by themselves, furthermore, ratio of the presence of the security experts in these companies is merely 40 percent. In these results, we surmise that most of the servers are exposed to diverse threats.

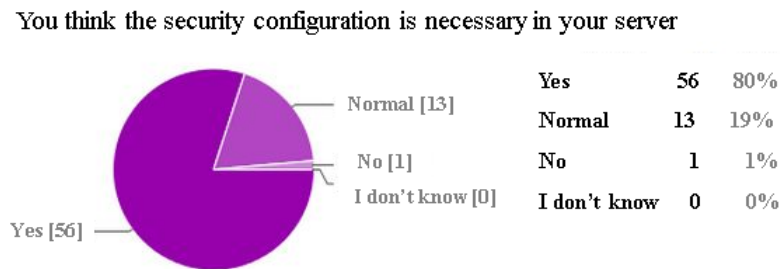
Next, we give several question to the users related to the security configuration and countermeasures to confirm necessity of the server security. The surveying results are shown in the Figures 12 to 14. More than 80% users reply that the server security is very important issues in their businesses and know that more robust configuration is required in the server.



**Figure 12. Relationship Between the Server Security with User's Confidence**

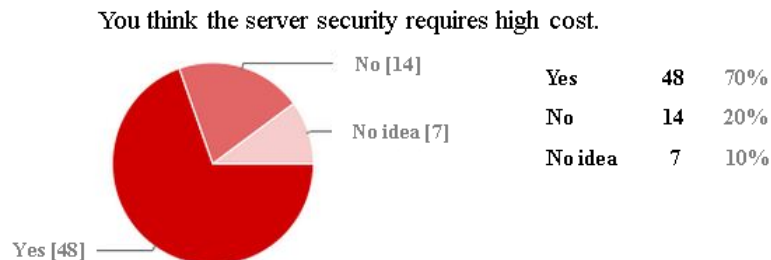


**Figure 13. Necessity of the Countermeasures**



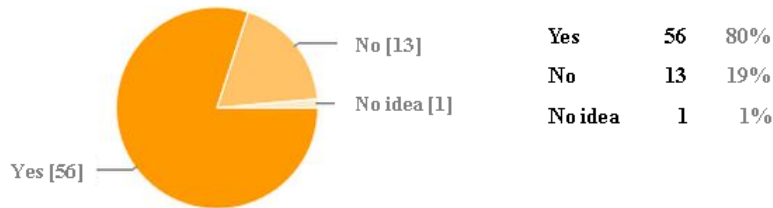
**Figure 14. Recognition of Weak Configuration about the Server**

As mentioned above, management of the server and knowledge for the users is insufficient even though most of users identify that more effort is required. It might be considered the problems with a viewpoint of the cost.



**Figure 15. A Viewpoint of the Cost of the Server Security**

You can give the request for the security to the professional company if the cost is cheap.



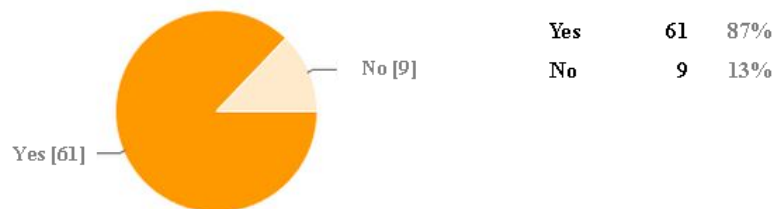
**Figure 16. Thought for the Professional Security According to the Cost**

As shown in the Figures 15 and 16, most of users have a burden of the cost associated with the server security. If the cost is cheap, however, they have enough intention to reinforce the server security.

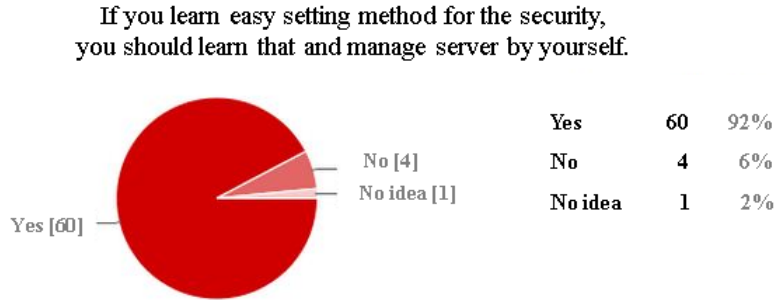
#### 4. The Countermeasures for the Single Server

Observing most of intrusion, servers with weak security are abused as foothold of DDoS attack or servers spreading malicious codes [8]. These abuses are sufficiently protected by only basic web firewall and network firewall. There are diverse technical measures to cope with intrusion to the server. In general, most of users who manage the single server do not know these kinds of establishment for the security. Even if they know that, users hesitate to apply those to their own server because it may be very difficult technique or accompanied with high burden of the cost. However, the server could have protection to many kinds of threats with basic establishment of the security which is opened to the public. For example, Window OS basically offer the local security policy. Webknight is also the free web firewall which will be installed to the window platform. For the server operated under Linux OS, there is iptables as a network firewall established in Linux itself and mod\_security which is the free web firewall for Linux. It can reduce damages by intrusion successfully; however, general users have difficulty to access or apply them because of lack of education for inexpert users. To solve these problems, we suggest two kinds of approaches. One is to reinforce education for inexpert users about the security. The other is mandatory of security configuration for the single server.

you will take the education for the security if the education is offered.

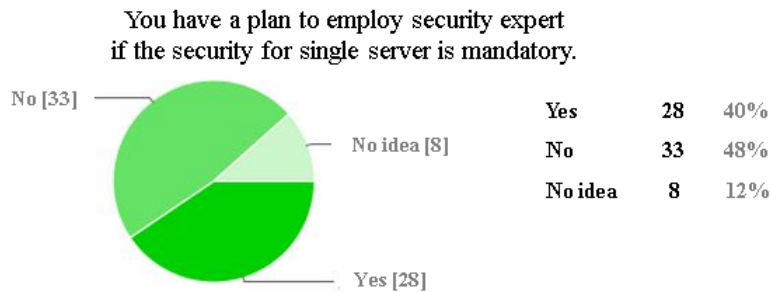


**Figure 17. Intension about the Security Education**

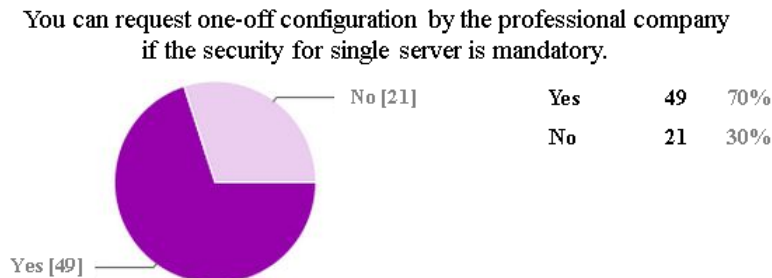


**Figure 18. Thought about the Security Education and Server Management**

The KISA already supports recommended security configurations and its manual [9]. However, there is insufficient announcement; thus, most of users don't know that. Moreover, most topics including cyber forensic, cryptography, and information security are fitted to the experts. Related to the education for the server security, we ask users a few questions. From answers in the Figures 17 and 18, we can easily identify that the single server users have positive intension to learn server security, but they don't know already existing education. Therefore the active promotion of the security education is desperately needed. In addition, more ease education course targeting to inexperienced single server user is also required.



**Figure 19. Plan to Hire Expert for the Single Server Security**



**Figure 20. Thought about One-off Configuration by the Professional Company**

Secondary suggestion by this paper is mandatory of the single server security. Now installing the security certification is mandatory in the company which deals with personal information. It bears many positive effects. Like the case of security certification, basic security configuration for the single server should be mandatory. They have much burden on

the cost such as hiring the expert. Nevertheless, most of the single server user agrees on the mandatory of the single server, and thus, they give positive answer about one-off configuration by the professional company, which can be done with low cost. From these inquiries, mandatory of the single server security should be firmly required for the single server security, and that should be closely connected to the low costing service by the professional company even if that is merely one-off configuration. It seems to be very helpful as proper countermeasures to the single server security, thus, damages by threat of intrusion and malicious codes could be reduced successfully.

## 5. Conclusions

Social and economic losses caused by intrusion and abuse of servers increase recently as increasing the single server. It is tightly associated with the ignorance of the security awareness. The responsibility related to the security of single server lies not in the hosting company but in the user. Nevertheless, most of users prefer to use the single server hosting service because of the performance including the perspective of the cost and the degree of freedom. By surveying with questionnaire, we can confirm that most of single server is exposed to many threats with almost defenseless due to little knowledge about the security of the single server. Most of abuse of the single server might be protected by basic configuration on the server security. However inexperienced users managing the single server do not know the configuration because of lack of education proper to inexperienced users. To reduce damages by the threats, we suggest two kinds of countermeasures; one is reinforcement and announcement for the education appropriate to inexperienced users, thus, single server users will get sufficient knowledge about the server security. The other is mandatory on the basic configuration for the server security. It might be burden of the cost to the small-scale company such as internet shopping mall. However, it could be effective countermeasure if cheap managing service even though one-off configuration by the professional company is supported and most of single server users agree and give active response on this kind of approach. Therefore, it is noted that expansion of education appropriate to inexperienced users and mandatory of the single server is very important and urgent matters.

## References

- [1] KISA (Korea Internet & Security Agency), "Survey on the Internet Usage", <http://isis.kisa.or.kr/board/index.jsp?pageId=040000&bbsId=7&itemId=792&pageIndex=1>, (2012).
- [2] H. J. Kim, "Online Social Media Networking and Assessing Its Security Risks", *International Journal of Security and Its Applications*, vol. 6, no. 3, (2012), pp. 11-18.
- [3] K. Lee, "Security Threats in Cloud Computing Environments", *International Journal of Security and Its Applications*, vol. 6, no. 4, (2012), pp. 25-32.
- [4] KISA (Korea Internet & Security Agency), Web Security Tool Box, <http://toolbox.krcert.or.kr/>.
- [5] Trustwave, ModSecurity, <http://www.modsecurity.org/>.
- [6] AQTRONix, webknight, <http://www.aqtronix.com/>.
- [7] S. H. Choi, "Defense Method against SQL Injection Attack by Hacking Tools", Master Thesis, Sogang University, Korea, (2011).
- [8] M. S. Kwak, A. B. Kim and Y. H. Kim, "Design and Implementation an Integrated Malicious Code Collection and Monitoring System", *Journal of the Korean Institute of Information Technology*, vol. 8, no. 2, pp. 117-125, (2010).
- [9] KISA Academy, Online Information Security e-Learning Center, <http://ww.sis.or.kr/>.

## Authors



**Hyuk-Jin Son**, graduated from Department of Management Information System in Keimyung University at 2010. He is currently candidate student of master at IT MBA, Graduate School of Business Administration, in Hanyang Cyber University. From 2009 to 2013, he worked the hosting specialist company, SimpleX Internet. He currently works at CDNetworks. He has certification of the RHCSA and Oracle OCP. His areas of interest include server security and network security analysis.



**Seungdo Jeong**, received his B.S. degree in Department of Electronic Engineering from Hanyang University at 1999 and earned the M.S. and Ph.D. degrees in the Department of Electrical and Computer Engineering from Hanyang University at 2001 and 2007, respectively. He is currently an Assistant Professor at Department of Information and Communication Engineering, Hanyang Cyber University. His research interests include multimedia information retrieval, computer vision, multimedia contents processing, tensor analysis, and network security.

