International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.87-98
http://dx.doi.org/10.14257/ijsia.2016.10.6.10

# A Study on Responding to DDoS Architecture in Smart Phone Environment

Mi-Ran Han[1], Young-Chul Oh[2] and Jong-Bae Kim[3*]

*[1,3*]Graduate School of Software, Soongsil University, Seoul 156-743, Korea*
*[2]Department of IT Policy and Management, Soongsil University, Seoul 156-743, Korea*
*Email: [1]agua1978@naver.com, [2]oyc@s3i.co.kr, [3*]kjb123@ssu.ac.kr*

## *Abstract*

*A smart phone is closely related to our lives throughout the world. It processes and stores various information from personal information to classified information of companies. As it is called as "a PC in my hand," it is similar to a PC so that it is likely to be misused, being exposed to many security threats such as hacking, malicious code, and loss, just like the DDoS attack on PC. A hacker can control a smart phone through a number of zombie smart phone instructions, even shutting down the service on the server. However, it is difficult to adapt the PC defense system to the smart phone environment as is because the attack methods on a PC and a smart phone are different. Therefore, this study aims to compare and analyze DDoS attacks on the smart phone environment and PC environment to predict DDoS attack scenario on the smart phone and establish a defense system to reduce the damage.*

***Keywords**: DDoS, smartphone DDoS, malicious code, Detection System*

## 1. Introduction

DDoS attack on March 4, 2011 demonstrated that the system to deal with DDoS is still imperfect. Moreover, there are increasing cases of personal information leakage and damage due to malicious codes planted by hackers. The smart phone has been getting more improvements than a PC, with a lot more portability and mobility. It makes it an easier target than a PC, and when the DDoS attack succeeds, the damage will be more severe. Chapter 2 shows and compares the tendency of DDoS attacks so far. Chapter 3 analyzes zombie smart phones and zombie PC environment, and explore the approach to detect malicious codes for mobile devices. Chapter 4 sets up the direction for further studies, concluding this study.

## 2. DDoS Attack and Smart Phone Attack Tendency

### 2.1. Existing DDoS Attack Tendency

DDoS attack is one of the hacking forms that many distributed attackers concentrating attacks on a target system. Most of the attacks use automatic tools because it means to break out in many places in a short time. Subjects are usually web services, but it can cause a bandwidth overload on organizations, companies, banks, and even government to decrease the network performance or shut down the service. Figure 1 shows the principles of DDoS attack. Due to DDoS attack, clients may not be able to access or be used as hosts without the system administrator's knowing.

[3*] Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 1738-9976 IJSIA

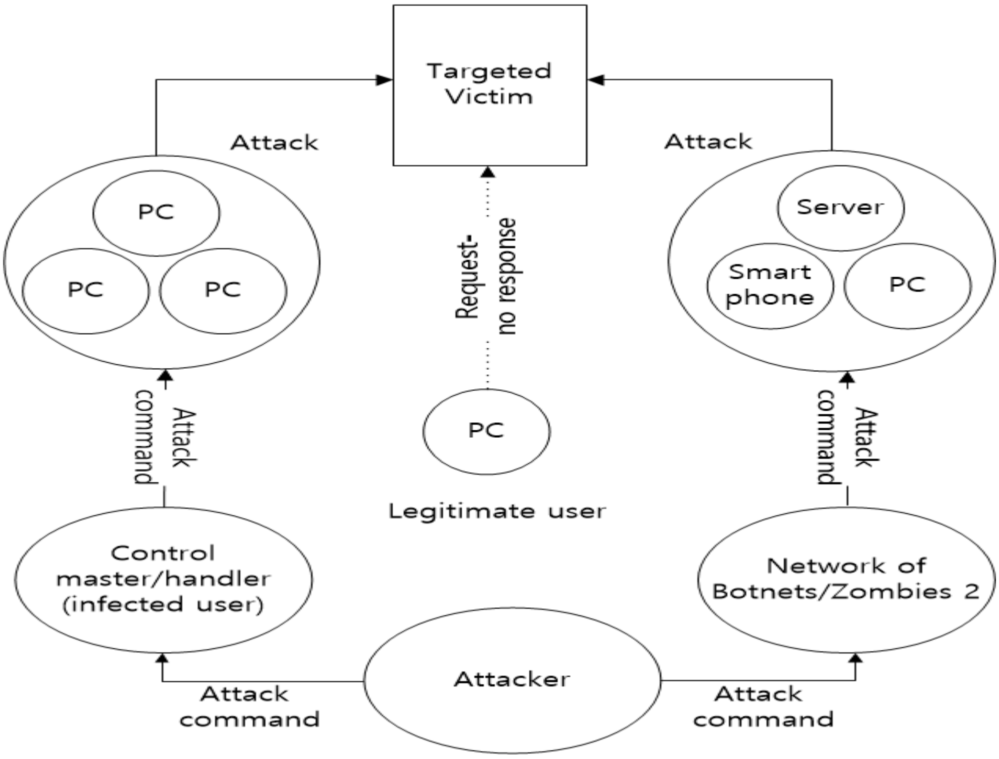

**Figure 1. 1 Diagram of DDoS Attack [1]**

**Table 1. DDOS Attack Type**

| | Bandwidth Encroachment | Server / Equipment load-induced Attack | Specific Denial of Service Attacks |
|---|---|---|---|
| Attack Methods | ICMP/UDP Flooding ,DNS Query Flooding DDoS | Syn Flooding Fragmented Packet Flooding | CC Attack<br>Get Flooding Slowloris |
| Attack Effect | N/W Excess Bandwidth Capacity | Causing the server load N/W Equipment, Security Equipment load-induced | Causing the Server load |
| Attack Type | Traffic Transmission to Surpass the Bandwidth | Backlog Queue ServerExcess | Sessions excess CPU Resource Depletion |

### 2.2. Tendency Threats to Smart Phones

Security threats to smart phone have steadily increased, along with the actual cases of smart phones damaged by malicious codes. Attack methods on smart phones can be classified as seen below in Table 2, by their subject resources.

**Table 2. Attack on Smart Phone and the Target**

| Level Classification | Server / Equipment load-induced Attack<br>Specific Denial of Service Attacks |
|---|---|
| Personal information and classified data leakage | Images, contacts, emails, document |
| Service misuse | Battery power, communication memory, processing power |
| Wasting terminal resources | Backlog Queue Server Excess<br>Sessions excess CPU Resource Depletion |
| Using hardware equipment illegal | Camera, external memory card |

**2.2.1. Private Information and Confidential Data Leakage:** The attacker installed a malicious application with intentional or unlawful purpose and it is a way to get an access to run a different program installed on your smartphone. These attacks have come through the misuse of the availability, confidentiality and integrity of information and it corresponds to the case that the attack can occur easily. There are following ways on such intrusion can be detected and prevented by firewall, an Application Certification, and selective authorization for protection.

**2.2.2. Misuse Service:** Unnecessary services waste of the resources and malicious applications attack the kernel of the smartphone application itself (kernel). The system library is to identify vulnerabilities in the smartphone text messaging, and expose it on your smartphone. These threats are less likely to occur due to its hardware platforms and security mechanisms (security mechanism) provided on the smartphone itself. If the actual result can be expected to seriously damage the entire system, prepare the desktop (Desktop) based on the computer's operating system vulnerabilities such as Rootkit (Rootkit) for research and to block the unauthorized access progressing from a smartphone at the same time.

**2.2.3. Terminal Wasted Resources:** Battery is wasted through the excessive iterative operations performed by malicious attackers. Or a case that caused a disruption in the application performance and operation and other functions to occupy the resources of mobile devices (Mobile device's resource). The goal and approaches for the limited resources, such as disk storage (diskstorage), memory (RAM), and CPU of the smartphone are resource management (Resource management), and intrusion detection / prevention system.

**2.2.4. Illegal Use of Hardware Devices:** The attacker's unauthorized use of external storage such as SD Card. Infected device to a computer, using the network as a network attack means the actual cross-platform, called Cardtrap (cross platform) for malicious code is reported in 2005 as a countermeasure for this intrusion detection / prevention system. Access control for the situation, with proposed method, such as a remote control (Remote management). Malware attacks by way of these smartphones will damage the system through malicious actions, Network Connections / economic damage through text messages sent, Users' confidential information and data on access to, commercial advertising and adware (Adware), distributed denial of service attacks (Distributed Denial of Service) or spam (Spam) the purpose of the botnet (botnet) composed appears. It simply appears to have the potential evolution of the threat that paralyzes society beyond the part of the individual.

**2.2.5. Research of Intrusion Detection based on Malware Detection:** In the PC environment security threats caused by viruses and malware is increasing, and these days, it's becoming worse, supported by a number of studies conducted by the security-related companies as well as academia. Although the environment of smart phones has similar experience that part of the PC software or app is running on the OS, PC. Limitations on the system resources of the smart phone itself (RAM, CPU, *etc*. Battery power) is due to the function provided by a wider variety of system interfaces (system interface) in connectivity. The PC of the various communication compared to the conventional PC environment represents a further aspect. As seen on research results in the PC environment, there are a number of problems. Due to this aspect, using Bluetooth, SMS, has infected smart phones and the PC environment. Studies on how these spread using different characteristics is underway. S. Toyssy [10] is the base technology for detecting malware that occur within the analysis of the propagation characteristics of the malicious code. A. Lot [11] *et. al.,* conducted a study in particular on the infection spread through the Bluetooth communication. Based on these data, L. Xie [12] and T.S. Yap [13], including a proposed malware detection techniques based on behavior. In addition, a lot of research were conducted for the plan to detect malicious code by analyzing the battery consumption pattern.

**2.2.6. Security Application Management Research through Certification:** Applications on the smart phone environment are deployed without any special certification and verification procedures by using the open market, it may be infected with malicious codes for users easily. To solve this problem, users can use a method that allows installing only authenticated software. W. Enck [8] is proposing to apply the technology in the field of Kirin Security Requirement Engineering in the smart phone's OS. This approach generates a Security Rule in each application before deployment. This approach is the pre-application. In terms of censorship and undermining the autonomy of the developers, they also have a lot of time needed for handling problems for numerous applications.

Since the structure of a smart phone is an open-source system, everyone can easily code and make an application. It means it is vulnerable to various attacks. Ever since the Cabir, the first smart phone virus, went out in 2004, many different viruses and malicious codes have been created.

**2.2.7. Security Technology Research Operating between the Limited Resources of a Smartphone:** Since a smartphone has limited resources of CPU, memory, and battery, there have been studies to detect malicious codes efficiently with the limited resources. Such studies aimed to reduce the resources consumed while analyzing an application to detect malicious codes. Some studies proposed a measure to get help from external servers to block malicious codes in the smartphone environment. Other studies suggested a method to collect behavioral patterns of many smartphones in the central detective server, and piece the information together to detect malicious codes. While such measures help a smartphone to be more true to its duties by reducing its roles, in case of the central server down, it may not provide the service. As the hardware resources for smartphones develop radically, moreover, measures to save resources have become meaningless.

**2.2.8. User Protection through the Access Control Technology in the Smartphone Environment:** In the Pervasive Computing Scenarios Mobile environment, the user becomes the system administrator at the same time. It means there is a need of a self-security control mechanism rather than an external security service. What is necessary in this situation is not the access control technology that were used by existing security managers but a new technology that can be easily understood by normal users without security consciousness. Existing studies were for meeting such demand, proposing access control technologies, in which the relationship between users and applications was considered. Other similar researches also suggested security models based on permission. They are effective to cope with issues such as personal information leakage in the PC environment. In the smartphone environment, however, they can barely protect against risks of malicious codes.

**2.2.9. Risk Analysis of Malicious Codes in the Smartphone Environment:** There has not been an effort to analyze specifically the risks of malicious codes in smartphone environment as this study intends to do. There are research cases that only show that it is possible to attack the cellular network and the base station with malicious codes in the smartphone environment.

**2.2.10. Mobile Botnet:** Recently, Botnet in the PC environment has been a big issue in many areas. Sending spam mails being controlled by Russian mafia and being applied to DDoS attacks, economic activities using zombie PCs have been spotted. The typical examples in Korea are the cases of Nonghyup DDoS attack and the National Election Commission website attack. This zombie PC may flow into the smartphone environment. A smartphone in which installed a malicious code corresponding to a zombie PC may be used as a zombie phone. These zombie PCs or phones have the C&C Channel (Command and Control), which enables a hacker to remotely control the device. Related studies have recently been started. Existing studies suggested a way to create the C&C channel in the mobile environment by using SMS. Other studies tested and confirmed a possibility to construct the C&C channel through Bluetooth communication. Such studies are not about detecting or preventing Botnet in the smartphone environment but are research cases showing the possibilities to construct Botnet in the smartphone environment.

**Table 3. Cases of Security Threats on Smart Phone**

| Mobile Malicious Code Name | Type | Electric Wave I/F | Subject | Description |
|---|---|---|---|---|
| **Palm/vapor** | Troy | WAP | PalmOS | Conceals every icon in the program when executed (files actually exist). Hot-Sync after Hard Reset to restore. |
| **Carbir** | Worm | Bluetooth | Nokia (Symbian) | The first worm targeting mobile devices |
| **Duts** | Virus | BlueTooth | Window Mobile 4.X | The first virus.<br>Proof of concept virus by 29A who created Cabir. |
| **Skulls** | Worm | Internet Download | Nokia (Symbian) | After being installed without the user’s consent, it changes files in the Nokia device to the files in Skulls.sis. Either applications are shown as skull icons or an skull image animation is displayed on the full screen. |

| | | | | |
|---|---|---|---|---|
| **Jailbroken** | Worm | WiFi | Apple (iPhone) | It sends an SMS, leading to doiop.com/iHacked. The installed hacking tool requests the user's personal information, mentioning that the iPhone's personal information can be acquired, so that it can delete it. |
| **Duh worm** | Worm | WiFi | Apple (iPhone) | It is infected in the same form of Ikee. In the wireless environment, the zombie smart phone is remotely controlled through the operation and common server in the form of botnet. Using Duh worm, it acquires the password of internet banking. |
| **Ikee worm** | Worm | WiFi | Apple (iPhone) | It spreads through SSh.<br>'Together Forever' of singer Rick Ashlee picture and The phrase appears 'ikee is never going to give you up' Attempts to spread to other iPhone |

### 2.3. Tendency of DDoS Attacks on PC and Smart Phone

As Table 2 shows, defense system against zombie PC is not enough to deal with zombie smart phone, because the two environments are different than each other. In short, the smart phone is carried and kept it turned on at all times. It means that durability is maintained, and it is reconnected whenever 3G/4G is on, irrelevant to the user's intention. Its environment cannot block external attacks because it is hard to trace the IP (it is changed at every connection) and the power is supplied at all times. Using the vulnerability of VM mobile, smart phone internet banking can be hacked. DDoS attack or terminal unit hacking watch for a chance that contents including a malicious code to be downloaded. Moreover, there is an increasing risk that the infected smart phone can be used to disable the network of the telecommunication company. For example, a smart phone is highly mobile and portable and the user can download any application through the app store. Such convenience increases the probability for the device to be infected with a malicious code and become a zombie smart phone while downloading an unverified application from a 3rd-party market. Lastly, unlike a zombie PC, which can be easily cured through a vaccine, smart phone vaccines are not prevalent. It is even difficult to assume the infection. It means the reaction to the DDoS attack against a smart phone must be different than that against a PC [12].

**Table 4. Environments of Zombie PC and Zombie Smart Phone DDoS [4]**

| **Classification** | | **Zombie PC DDoS** | **Zombie Smart Phone DDoS** |
|---|---|---|---|
| Hardware | CPU | More than 2Ghz (Dual/Quad core) | 1Ghz (Single/Dual core) |
| | Power | Power Cable (at all times) | - Battery use (1500mAh)<br>- When the screen is lit (about 4 hours) |

| | | |
|---|---|---|
| Network | Ethernet (100Mbps, 1Gbps) | - 802.11 b/g/n (54Mbps)<br>- 3G (2.4Mbps) |
| System Thread | Can make a lot of threads | Performance decreases and heat is generated when a lot of threads are made |
| How to infect and Spread malicious code | - Web browser weakness (IE)<br>- Web content<br>- E-mail, SNS, Messenger<br>- ARP Spoofing<br>- USB | - Official market, 3rd-party market<br>- SMS message, contact list<br>- QR Code<br>- Rogue AP<br>- Web browser weakness (Webkit)<br>- Web content<br>- E-mail, SNS, Messenger |
| Scope | - DDoS attacked server<br>- Backbone network | - DDoS attacked server<br>- Backbone network<br>- 3G network |
| Durability | - Until system shut down | - No more progress when the battery is discharged<br>- No more progress when using 3G/WIFI |
| Symptoms and Damages | Can attack the system without large loads | - Slowing down system and heating up the terminal<br>- Discharging the battery<br>- Billing for using 3G |

## 3. Approaches to Detect Malicious Codes Aimed at the Smart Phone

Viruses aimed at smart phones have drastically increased for the last several years that the amount is close to that of virus outbreaks targeting desktops for near twenty years. Common approaches for detecting malicious codes aimed at mobile devices include NIDS (Network Intrusion Detection System) and HIDS (Host-based Intrusion Detection System), while the representative methods to detect malicious codes are the Signature-based detection system and Anomaly detection system. Following the table below classifies and describes them further.

**Table 5. Categories of Directions of Detecting and Approaching to Malicious Code [2][6][8][9]**

| Category | System | Description |
|---|---|---|
| **Direction of Detecting and Approaching to Malicious Code** | Network Intrusion Detection System, NIDS | It detects any malicious activity such as a Dos or a computer crack by monitoring the traffic. NIDS reads every received packet and finds any suspicious pattern. For example, if it founds a very large number of TCP connection requests trying to connect through many different ports, it is assumable that an external attacker is trying to scan the ports. |

| | | |
|---|---|---|
| | Host-based Intrusion Detection System, HIDS | It is a special type of detection systems, which is focused on detecting and analyzing the inside of the computer system. Like the NIDS examines network packets, HIDS may detect the resource that the program is approaching so that the programs such as Word Processor cannot change the system password database. Similarly, HIDS confirms the system status to check if the contents of the RAM or the file systems are the ones expected by the status information. It works as an agent conducting surveillance of anything that bypasses the security policy of the OS. [8] |
| **Methods of Detecting Malicious Code** | Signature-base Detection System | It is also known as the Misuse detection system. It identifies an intrusion by monitoring traffic or the patterns of application data that are assumed to be malicious. Such types are considered to be able to detect known attacks only, but according to their rule sets, the signature-base IDS, sometimes, may detect new attacks that share distinctive features with known attacks such as the 'cmd.exe' approach through the HTTP GET request. The IDS analyzes the collected information and compares it through the huge database, in which attack signatures are saved. Essentially, it finds certain attacks that are already documented. Like a virus detection system, a misuse detection system is much the same as an attack signature database for just comparing the packets. [9] |
| | Anomaly detection system | It identifies an intrusion by reporting any traffic or an application content that is assumed to be different than the usual activity of the network or the host. The anomaly base IDS generally teaches itself. In anomaly detection, the system administrator defines the network traffic load, breakdown, protocol, the baseline for the general packet size, and the general state. A detector monitors the network segment to compare the status to the defined standard and find any anomaly. |

Still, new forms of attack continue to come out so that existing approaches and methods detecting malicious codes reach the limit. Therefore, the architecture this study suggests to deal with external attacks and intrusions and minimize the damage or loss is SCIT (Self-Cleansing Intrusion Tolerance).

## 4. SCIT Self-Cleansing Intrusion Tolerance

Existing intrusion detection systems ceaselessly monitor the system and report any abnormal intrusion. However, there is a problem that the attacks that cannot be classified by the signature in the system are not detected since the system generally uses known attack signatures. The SCIT method among the intrusion tolerance systems reactivates the machine in a short cycle of minutes to reset [12]. That is, the device is reactivated, provides services for a short period, and then be reactivated again. It can invalidate any intrusion because it resets the device before the intrusion leads to the security failure. Such system has to stop the machine while it is in service and make it to be in service again while it is standing by so that the virtualization technology is efficient [13].

**Table 6. Four Statuses of SCIT**

| Active | It is in service, being exposed to the internet. |
|---|---|
| **Grace period** | It provides the service of the request that has already been made, but it does not receive or respond to a new request. This period is necessary for the response to the user's request not to be ignored when the Active status is converted to the Grace Period. |
| **Live Space** | Reactivation is complete and the service can be provided anytime, only it is not active but standing by. |

In SCIT, each machine moves in the four states of above cycle. When it is in the Active state, it provides services. A while after, it moves to the Grace period to deal with leftover requests, and goes through the reactivation process in the Cleansing period. Lastly, it waits to be in service again in the Live Spare state. In general, the security of SCIT is dependent on the time it is exposed to the external network [2]. This time is calculated by summing up the lengths of two states; the Active and the Grace Period. The shorter the time is, the stronger the general system security is, since the attacker does not have much time to do something malicious in the system. Normally, the exposure time is within several minutes, and it may be restricted due to the number of spare machines and the time for cleansing. Systems that can adapt to the SCIT technology must not be changed much in the inside by an external input or request. Although such recovery technique that can reduce damage by external attacks runs effectively in the ITS, it is difficult to maintain the system with the recovery system in case a new type of attack comes into the system. Therefore, the proposed model inserts the Forensic period using SPT before the Cleansing period — between the Grace period and the Cleansing period. In the Forensic using SPT period, it records any forgery of file systems and memory areas of the machine before it restores the initial image during the cleansing process. These records may be used as symptoms of an intrusion. It can realize the machine learning, which uses the recorded data statistically. When the statistical distribution of the data shows an abnormality, it can be an important criteria to discern it as a new type of system attack. Even if a new type of attack does happen, it can secure availability and security of the system by resetting the machine. In addition, it acquires a large quantity of information about damage and traces of the intrusion while it is being restored to the initial image.

## 5. Conclusion

We have explored existing methods to detect malicious codes aimed at mobile devices. We suggest the SCIT system to be an effective method to detect new types of the attack, overcoming the limit of existing intrusion detection systems. As the use of smart phone increases, online e-commerce and banking have become active. Though the performance and services of smart phone provide convenience, they create an environment in which hackers can easily attack the smart phone. It is not easy to detect and deal with various infection routes and attack patterns which maliciously use weak points in the hardware and software configuring the system. Therefore, there have to be many experiments on services to construct safe and reliable smart phone network environment. Further studies are necessary to develop a core technology to build a safe network security environment.

## References

[1] P. Dzurenda and Z. Martinasek, ”Lukas MalinaNetwork Protection Against DDoS Attacks”, International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems, vol. 4, no. 1, **(2015)**.

[2] Yijongyeop, yunmiseon and H. Lee, “Monitoring and Investigation of DoS Attack”, KNOM Review, **(2004)**.

[3] Janggiheon, choesangmyeong and yeomheungyeol, “Smartphone DDoS attack trends”, KIISC vol. 21, no.5, **(2011)**, pp. 65-70.

[4] Choesangmyeong, “Zombie smartphones and DDoS attacks”, HAURI, **(2011)**.

[5] Gwakchanggyu, “Changes and prospects of DDoS attack techniques”, Financial Security Agency Issue Report **(2011)**.

[6] A. R. Kumar and P. and S. Selvakumar, “Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment A Survey on DDoS Attack Tools and Traceback Mechanisms”, IEEE International Advance Computing Conference, **(2009)**.

[7] Y. D. Sic, “Analysis & defence of detection technology in network Attacker”, Korea Information Assurance Society, Jouranl of Information and Security, ISSN: 1498-7329, **(2013)**, pp.155-163.

[8] L. Vokorokos and A. Baláž, “Host-based Intrusion Detection System”, Intelligent Engineering Systems (INES), 2010 14th International Conference on, DOI: 10.1109/INES.2010.5483815, **(2013)**.

[9] P. Chan, “Signature Based Intrusion Detection Systems”, CS 598 MCC, **(2013)**.

[10] S. Toyssy and M. Helenius, “About malicious software in smartphones”, Journal in Computer Virology, vol. 2, no. 2, **(2008)**, pp. 109-119.

[11] A. Loo, “Technical opinion security threats of smart phones and bluetooth”, Communication of the ACM, **(2009)**.

[12] L. Xie, X. Zhang, J. Seifert and S. Zhu, “pBMDS: a behavior-based malware detection system for cellphone devices”, WiSec'10, ACM, **(2010)**.

[13] T. S. Yap and H. T. Ewe, “A Mobile Phone Malicious Software Detection Model with Behavior Checker”, HIS, LNCS, vol. 3597, **(2005)**, pp. 57-65.

[14] K. Lee, R. S. Tolentino, G. Park and Y. Kim, “A study on architecture of malicious code blocking scheme with white list in smartphone environment”, Communication and networking, vol. 119, **(2010)**, pp. 155-163.

[15] A. Gupta, IIIT Delhi, New Delhi, India, T. Verma, S. Bali and S. Kaul, “Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks”, Communication Systems and Networks, E-ISBN:978-1-4673-5329-8, DOI: 10.1109/COMSNETS.2013.6465568.

[16] J. Sun, “Tendency of DDoS Attack Technology”, FSEC, **(2009)**.

[17] A. Bangalore and A. Sood, “Securing Web Servers Using Self Cleaning Intrusion Tolerance (SCIT)”, Second Internation Conference on Dependability, **(2009)**.

[18] K.-H. Kim, M.-r. Han and J.-B. Kim, “Design and Implementation of MQSPT Protocol for Establishing Financial Next-Generation Project PUSH Architecture, ASTL vol. 86, no 22, **(2015)**.

[19] X. Zhao, X. Song, X. Wang, Y. Chen, B. Deng and X. Li, “Analysis of Security Policy in Practical Internet Coordinates”, International Journal of Security and its Applications, vol. 3, no. 1, **(2009)**.

[20] Han Seong Sonand Soon Gohn Kim, “Architecture Design and Cyber Security Evaluation of a Festival Management System Server”, International Journal of Security and Its Applications, http://dx.doi.org/10.14257/ijsia.2014.8.3.24, vol. 8, no. 3 **(2014)**, pp. 235-240.

[21] P. E. Verissimo, N. F. Neves, C. Cachin, J. Poritz, D. Powell, Y. Deswarte, R. Stroud and I. Welch, “Intrusion-tolerant middleware: The road to automatic security”, Security & Privacy, IEEE, vol. 4, no. 4, **(2006)**, pp. 54-62.

[22] P. Pal, P. Rubel, M. Atighetchi, F. Webber, W. H. Sanders, M. Seri, H. Ramasamy, J. Lyons, T.,Courtney and A. Agbaria, “An architecture for adaptive intrusiontolerant applications”, Software: Practice and Experience, vol. 36, no. 1112, **(2006)**, pp. 1331-1354.

[23] M. Castro, and B. Liskov, “Practical Byzantine fault tolerance and proactive recovery”, ACM Transactions on Computer Systems (TOCS), vol. 20, no. 4, (**2002)**, pp. 398-461.

## Authors

**Mi-Ran Han,** received her Bachelor's Degree of Statistics in Dongguk University, Seoul (2002). And she is studying her Master's Degree in Software Engineering in Graduate School of Software, Soongsil University, Seoul. Her current research interests include pen source development and security.

**Young-Chul Oh** received his Bachelor`s Degree in Business Administration from Korea Maratime and Ocean University in Korea, (1991) and Master's Degree in Computer Science in Soongsil University, Korea (2009). He worked in the IT field as a system engineer over 20 years. Now he is CEO of S3I Co., LTD. since 2004.

**Jong-Bae Kim** received his Bachelor's Degree of Business Administration in University of Seoul, Seoul (1995) and Master's Degree (2002), Doctor’s Degree in Computer Science in Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.