J Inf Process Syst, Vol.12, No.3, pp.489~501, September 2016
http://dx.doi.org/10.3745/JIPS.01.0009

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

HB-DIPM: Human Behavior Analysis-Based Malware Detection and Intrusion Prevention Model in the Future Internet

Jeong Kyu Lee*, Seo Yeon Moon*, and Jong Hyuk Park*

Abstract

As interest in the Internet increases, related technologies are also quickly progressing. As smart devices become more widely used, interest is growing in words are missing here like “improving the” or “figuring out how to use the” future Internet to resolve the fundamental issues of transmission quality and security. The future Internet is being studied to improve the limits of existing Internet structures and to reflect new requirements. In particular, research on words are missing here like “finding new forms of” or “applying new forms of” or “studying various types of” or “finding ways to provide more” reliable communication to connect the Internet to various services is in demand. In this paper, we analyze the security threats caused by malicious activities in the future Internet and propose a human behavior analysis-based security service model for malware detection and intrusion prevention to provide more reliable communication. Our proposed service model provides high reliability services by responding to security threats by detecting various malware intrusions and protocol authentications based on human behavior.

Keywords

Future Internet, Human Behavior, Intrusion Prevention, Malware Detection

1. Introduction

Recently, most research has focused on establishing an efficient Internet environment that overcomes the structural constraints of existing Internet technology, as all the activities of people today are connected on a network [1]. In particular, with the widespread use of devices with access capabilities and progresses in Internet technology, various Internet-based services have appeared. This has led to a higher demand for a more pleasant and stable Internet connection. In addition, research is being conducted on tailored services for users. To provide such tailored services, device agents that can judge for themselves and act on this judgment are required. However, when the Internet was first conceived, the aspects of mobility, wireless, and security were not taken into account, which resulted in many limitations. Mutual communications between various devices are not smooth enough at the moment to realize the future Internet to make the dure Internet possible. Furthermore, there are many inconveniences and constraints when using large amount of contents. Although transferring data to

Manuscript received February 3, 2016; accepted August 12, 2016
Corresponding Author: Jong Hyuk Park (jhpark1@seoultech.ac.kr)
* Dept. of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, Korea ({jungkyu21, moon.sy0621, jhpark1}@seoultech.ac.kr)

various media over the Internet is possible, with the constant increase in the types of communication media and data amounts, limits inevitably occur in transmission over the wireless Internet [2].

The future Internet, as with the existing Internet, is faced with security threats, such as data counterfeiting, eavesdropping, stealing, and other malicious behavior [3]. To address such security threats, the United States, European Union, Japan, Korea, and other major advanced countries have undertaken research and development projects on the future Internet that can overcome the constraints of the existing Internet, guarantee transmission quality and mobility, and complete security so that it can be applied to new convergence services [4-6].

This paper proposes HB-DIPM as a human behavior-based detection of malware intrusion to better respond to security threats. The proposed method is human behavior-based, in order to constantly detect malicious activity and comparatively analyze the characteristics of viruses and malicious codes to detect and respond to. Moreover, to address the security threats to future Internet, it provides highly reliable services through authentication of the protocol.

This paper is organized as follows: in Section 2, we discuss related works, such as case studies on the future Internet, and explain the analysis and detection technologies for malicious behavior. Next, security threat factors in future Internet environments are reviewed and the existing studies on it are described. In Section 3, we conduct a comparative analysis of the architecture and scenario that we used in our proposed service model. In Section 4, we conclude our research and follow-up the researches.

2. Related Work

This chapter discusses the research trends and core technologies that have been applied to proposed services, as well as threats, responses to threats, requirements, and existing studies.

2.1 Case Studies on the Future Internet

This section defines the future Internet and discusses the case studies that are currently underway in the United States, Europe, Japan, and other countries.

The future Internet refers to the Internet itself as being one large smart computer. Different service networks are connected to each other to provide services to meet user needs. For convergence, smart services to be provided in an Internet environment; quality improvement of the service environment, such as cloud computing, smart media, personalization, virtual services, convergence of wired and wireless, the Internet of things, and strengthened information security are discussed [7].

2.1.1 United States

The United States has been undertaking the Global Environment for Network Innovations (GENI) project, which is an innovative Internet architecture-based test bed environment establishment project to conduct various experiments and prepare for the future Internet. The GENI project has the National Science Foundation (NSF) at the center of operations with organizations from around the world taking part in presenting innovative Internet structures, verifying the experiment infrastructure, and developing technology so that these areas can be adopted in the actual network. The projects undertaken by NSF are

the Networking Technology and Systems (NeTs), under which sub-tasks of Programmable Wireless Networks (ProWins), new Wireless Networks (WNs), Future Internet Design (FIND), the Networking of Sensor Systems (NOSSs), and Networking Broadly Defined (NBD) are carried out. Among them, FIND completely excludes existing Internet technologies to develop completely different innovative Internet architecture [8,9].

2.1.2 Europe

Europe, with the European Union (EU) at its center, took upon a large-scale project called the 7th Framework Programme (FP7) as part of Information and Communications Technology (ICT) to conduct studies that focus on the future Internet. The Future Internet Research & Experimentation (FIRE) project is part of FP7's ICT support sector and is a project that aims to establish a research environment for future Internet technologies. Moreover, future Internet studies include Advanced Research & Technology for Embedded Intelligence and Systems (ARTEMIS), eMobility, Networked and Electronic Media (NEM), the Networked European Software and Services Initiative (NESSI), the European Nanoelectronics Initiative Advisory Council (ENIAC), and the Integral Satcom Initiative (ISI). By conducting short studies in the networking field consisting of actual experiment equipment, they are linked with large-scale test beds for mutual connected authentication to provide an environment where experiments are possible [9,10].

2.1.3 Japan

Japan has a project led by the National Institute of Information and Communications Technology (NICT) called the AKARI Architecture Design Project to establish the next generation network architecture establishment project. The direction for the future Internet as announced by the Japanese government defines the three stages of JGN as a Next Generation Network (NXGN) that considers an IP basis. The goal is to provide quadruple-play services. Starting in 2015, all research that has been conducted in this field has had the aim of achieving progress into an IP+a or post-IP form of a new network, known as the New Generation Network (NWGN). The New Paradigm Network (NPN22) defines the characteristics of this network. The sub-infrastructure of the NWGN will be a light, mobile, sensor network, and various studies are being undertaken on this topic. MIRAI, which studies the sensor network-based ubiquitous network structure, is a leading project [9,11].

2.1.4 Korea

Researches on the future Internet of Korea are being conducted as part of a preliminary stage, which was started by the government. A future Internet forum where industry, academia, and research communities take part has also been established. With the goal of building a ubiquitous Korea, the country has developed next-generation wireless communication methods, such as WiBro and DMB. Moreover, IP-USN technology that uses IP networks to integrate, operate, and manage USN sensor networks was used to establish a broadband integrated research development network called KOREN. Various studies, experiments, and trial services are being implemented to further R&D in the field of the future Internet [9].

2.2 Technologies for the Analysis and Detection of Malicious Behavior

This section discusses the technologies for analyzing and detecting malicious codes. Analysis methods can be categorized into static analysis and dynamic analysis. By analyzing malicious codes, the information they seek to acquire, their targets, the operation process within the system, the purpose of these codes, and their dissemination channel can be identified. Later this information can help to better address issues of the same malicious code and its mutants [12].

Static analysis does not implement the program and is used to verify the characteristics of dynamic execution by analyzing the code of the program. That is, by analyzing the correlation or calling relationship of malicious codes' components, the overall structure and flow of the malicious code are analyzed. Since static analysis does not directly execute the malicious code, it is secure and is not limited to certain execution conditions when analyzing the structure and operation flow. However, automation is difficult and it requires much effort and time. In addition, if binary files are packed by methods such as encryption analysis is difficult [13,14].

Dynamic analysis examines the content that is carried out when the malicious code is actually executed. It is a way to analyze in real time the registry generation and revision in the emulator or the virtual machine, network usage behavior, and Application Programming Interface (API) calling dynamic analysis allows for conducting a relatively accurate analysis of malicious behavior, but when certain environments or conditions are not met, the analysis of the function of malicious codes can be difficult and only a handful of execution pathways among numerous pathways can be analyzed [12,15,16].

The host-behavior-based malicious code detection method observes the behavior occurring within the system to detect files that are suspected of having a malicious code. By monitoring the execution of programs, such as dynamic analysis tools and sandbox, the analysis methods are included in the host-behavior-based detection methods. Unlike the traditional signature-based malicious code detection method, this allows for the detection of a malicious code that is newly emerging and that takes a detour around the detection method. However, there is the possibility of a false-positive where normal files are mistaken for being malicious codes [17].

The network-behavior-based malicious code detection method monitors the network packet and sees traffic that derails from the already defined rule set or normal behavior as an attack. This technology enables real-time packet processing and the detection of transformed attacks in real time. It also learns to distinguish between normal and abnormal behaviors. However, thus far, this detection rate is low, making the false-positive rate very high [18].

2.3 Threat Analysis and Considerations for the Future Internet

This section discusses the various malicious code and authentication issues that pose a threat to the current Internet. However, these issues can also appear as a threat in future Internet. These threats are discussed by each issue.

The most widely used user authentication method is an ID and password system. But as users have an increasing number of IDs and passwords, they experience difficulty in memorizing all of them. Various technical methods are emerging to address this issue even in the existing Internet environment. However, to provide information security that lives up to the standards of the future Internet, such

simple authentication methods fall short. A new user authentication mechanism is required. Also, threats from malicious codes will continue to increase in the future. In recent years, hackers have been interested in monetary gain. The attacks that are most commonly used in such crimes rely on malicious codes [19]. Moreover, Internet fraud is also going beyond simply using personal information and is reaching a very sophisticated level by turning to automated mechanisms. By snatching the packet that is transmitted over the network, they pose security threats, such as spam or service denial attacks. Moreover, since the original address of the packet can be disguised, the security threat levels are very high. Mechanisms to address these issues will also be in demand in the future Internet.

One of the most basic Internet services today is Domain Name Service (DNS), but it is still not secure. In the future Internet, a new protocol to replace this or a mechanism that strengthens DNS against security threats would have to be provided. One of the leading devices to be used in the future Internet is the smartphone. In particular, smartphones not only support the basic functions of serving as a phone and access to wireless Internet, they also provide various functions in a mobile environment [20]. However, all of the security threats that can occur on a PC can also occur on smartphones. Moreover, important personal information is stored on smartphones and an open development environment means that the production and dissemination of malicious codes can easily occur [21]. Therefore, in the future Internet environment, mechanisms and security methods to prevent such issues are required.

The future Internet is operated by important systems and networks. The importance of the system is greater than the security threat. Therefore, security threats posed against systems also need to be considered in the future Internet. One of the ways to address security threats in the future Internet is to apply an authentication method to all of the protocols that will be used.

2.4 Security Requirements for the Future Internet

This section describes the threat factors related to the future Internet and security requirements for information protection, as mentioned in Subsection 2.3.

Confidentiality: Confidentiality of the security system that blocks malicious behavior is one of its most important aspects. The following items need to be considered in terms of confidentiality. First, the internal information of the user must not be accessible by outsiders. If this occurs, it must be possible to detect and trace it. Second, it must be possible to detect and prevent malicious activity that occurs through various sways. Third, it must be possible to prevent the malicious code from being executed or redirected through network services.

Integrity: Along with confidentiality, integrity is also an important aspect. To that end, the security system must consider the following. First, it must be possible to monitor the internal system information. Second, it must not be possible to make arbitrary changes to the internal system files, processes, registry, or network through the execution or redirection of malicious codes. Third, it must be impossible to revise or delete the system's internal resources that are not authorized by the user.

Accuracy: One of the most important issues of the intrusion detection system is the numerous errors that occur. While this is a serious issue if it is an intrusion detection system, it cannot be allowed in an intrusion blocking system. Inaccurate detection implements a response mechanism that affects legitimate traffic, which in turn creates unnecessary traffic, leading to disruptions in the user's work. Therefore, accuracy is an important aspect to consider in an intrusion blocking system.

Reliability: Reliability does not disrupt the other systems in the network, and it must be able to implement the unique functions of the service model. That is, the service model itself must not affect the system. Moreover, even if a malicious code is executed, the files, process, registry, and network of the system should not be arbitrarily changed. Lastly, it must not be possible to revise or delete the system's internal resources from an unauthenticated user.

Usability: For a normal operation as a security system, usability, confidentiality, integrity, accuracy, and reliability must also be considered. Delays cannot occur for the user who is using the desired function. Also, in order for usability to be made possible, it must be verified by designing the monitoring of the software and the system itself. Moreover, logging information related to the system must be independent from the system DB so that usability against an attack on or disorder in the DB is secured.

2.5 Existing Studies

Wang and Wang [22] developed an automatic malware detection system that is based on behavior signatures to use the Support Vector Machine (SVM) categorizer. The cross validation scheme was used to resolve the accuracy issue by using 60 malwares. Their proposed system consists of three modules of system backup, system monitoring, and system recovery. System backup offers backups for important files in the client and server. System monitoring restores the operating system and user data using the previous backup data. The system restoration module uses reversing engineering technology to restore the process infected by malicious software.

Dewan et al. [23] proposed a model that detects malicious email using social information. In this model, various machine-learning algorithms are applied to combine information that can be gained from the profiles of social services or from the title, contents, or attached file of the email. This research concluded that recognizing a malicious email via LinkedIn was not helpful, but it is meaningful in that it was one of the first attempts to detect malicious email by combining characteristics of email and social media.

Mohaisen et al. [24] proposed a labeling system that resolved the existing shortcomings and malware software analysis based on automated behavior called AMAL. AMAL consists of the two sub-systems of AutoMal and MaLabel. AutoMal is a tool that can collect the behavior artifacts of memory, the network, registry, and file system. MaLabel generates a feature using the collected artifact, and based on the learned data categorizes the data.

Nissim et al. [25] proposed a new machine learning method designed to acquire a malware framework based on exploitation and combination. It uses a static analysis method to express the benign and malicious execution files by taking the idea from text categorization.

Alam et al. [26] proposed a framework that allows for the real-time generation of a behavior signature and the detection of metamorphic malware. They proposed a new technology called an Annotated Control Flow Graph (ACFG) and Sliding Window of Difference and Control Flow Weight (SWOD-CFWeight). Unlike other technologies, ACFG offers a quick comparison of CFG without changing detection accuracy. SWOD-CFWeight eases current issues related to the changes of the opcodes' cycle,

such as the use of other compilers, the optimization of compilers, and code obfuscation. The proposed framework improves the detection time to optimize the malware detection time.

3. HB-DIPM

This paper proposes a Human Behavior Analysis-Based Malware Detection and Intrusion Prevention Model (HB-DIPM), which we will describe in terms of its architecture, service scenario, and analysis of comparisons against other existing studies.

3.1 Architecture

Our proposed HB-DIPM consists of a future Internet time synchronizer, host-based behavior monitor, network-based behavior monitor, analyzer, inspector, authenticator, audit trailer, logger, and DB, as shown in Fig. 1.

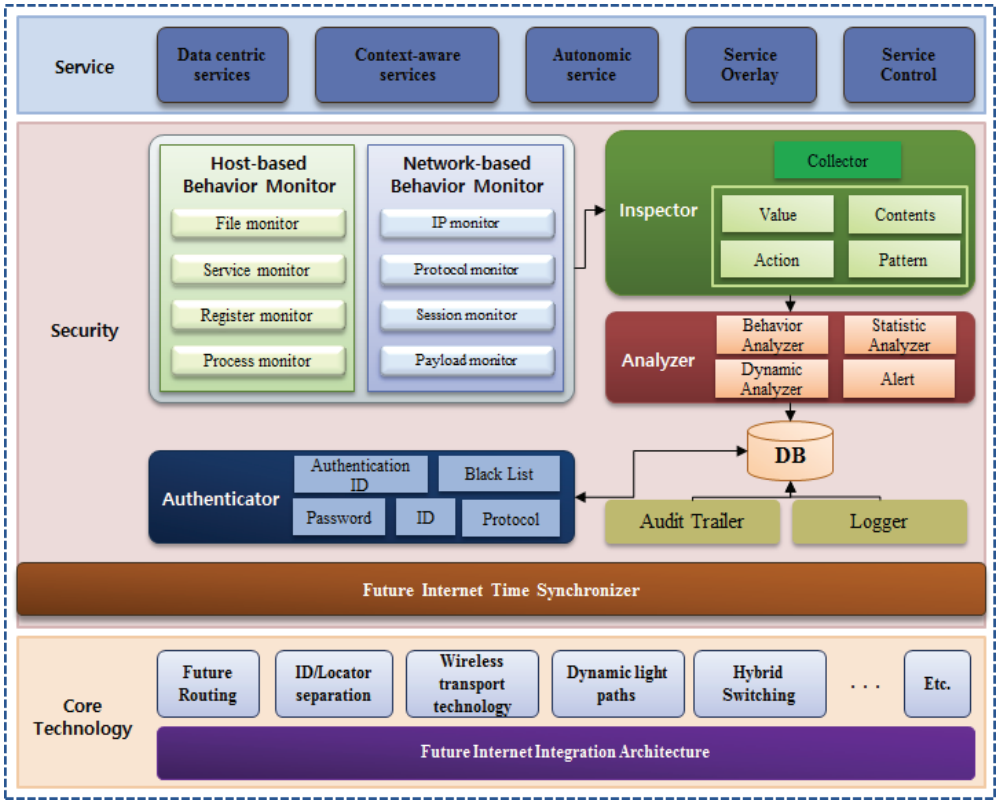

Fig. 1. Architecture of HB-DIPM.

It monitors authority, file, services, registry, process, and network information. The collected information is analyzed statically or dynamically. In addition, the degree of risk is categorized and blocks are carried out based on the analyzed information. At the same time, an alarm is triggered by the

user. The proposed HB-DIPM is categorized into three layers of security, core technology, and service.

The service layer creates an environment where various services can be provided, such as data-oriented services, situation recognition services, automated services, service overlay, and service control. Such services can only be used by authorized users.

The security layer is where security technologies for highly reliable and secure future Internet services are used. By linking with human behavior-based technologies, services are provided. The future Internet time synchronizer module synchronizes time with other modules to offer reliability to the log data. The analyzer consists of a behavior analyzer, static analyzer, and dynamic analyzer, in addition to an alert function. Static analysis includes analysis via the file's signature and hash value, while dynamic analysis include sandbox or hash value analysis. This module is where secondary analysis on the file and traffic takes place. Once analysis is complete, the information is sent to the DB. The host-based behavior monitor includes the following functions: the process monitor manages malicious behavior in the process; the register monitor monitors change by managing malicious behavior on the registry; the file monitor manages malicious behavior to observe changes in the file; and the service monitor manages malicious behavior in the service process and monitors change. The network-based behavior monitor exists in the behavior layer and carries out the following functions: the session monitor manages the sessions generated in the network; the IP monitor manages the information on the departure point and destination point of the IP address; the protocol monitor constantly oversees the information about unknown protocols; and the payload monitor manages the information that is sent out through the network. The inspector monitors the user's activities and collects the artifacts of authority, files, processes, and network. The collector gathers information on system malware. The analyzer analyzes the file forwarded from sub-components, processes, memory, authentication, and malware information on a comprehensive level. Dynamic analysis analyzes behavior, while static analysis analyzes based on the artifacts of authority, file, processes, and the network. The authenticator is a component that is in charge of the authentication of the file and process. It handles the authentication information and access information and takes care of the authentication of the protocol. The database stores the collected data and the analysis information and results to provide them during monitoring and tracking. The audit trailer is a module that monitors and tracks the system's activity or issues using the DB information. The logger independently records the information on the execution or stopping of the service model.

Core technology is the layer where various technologies are linked to provide services. Future routing technology, the separation of the ID/locator, wireless transmission technology, the dynamic light pathway, and hybrid switching are such examples.

3.2 Service Scenarios

This section discusses the operation procedure and service scenarios in HB-DIPM. Fig. 2 is a dynamic procedure where the user's activity is collected and constantly monitored. When malware is detected, a secondary test is conducted through dynamic and static analysis. The inspector does testing and analysis and the findings are stored in the DB. If malware is detected, it is immediately blocked. If it is not malware, authentication is carried out to check whether it has approved access or not. Unauthorized access is blocked, while authorized accesses are offered normal services.

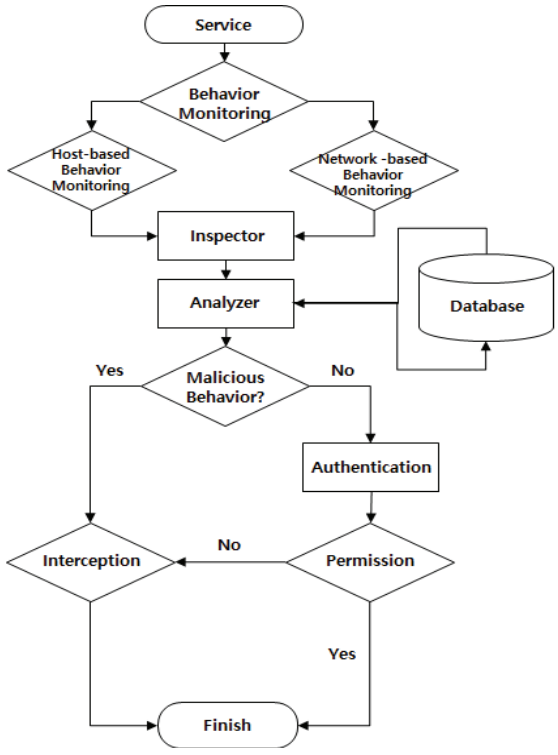

Fig. 2. Operation procedure of HB-DIPM.

The marking used in the proposed service scenario is as shown in Table 1, and Fig. 3 shows the service scenario.

Table 1. Definition of acronyms

Term	Explanation
AN	Analyzer
DB	Database
AU	Authenticator
AT	Audit trailer
LOG	Logger
ND	Audit trailer
NB-Info	Normal behavior information
MB-Info	Malicious behavior information
Req_()	Request
Res_()	Response

The DB has the information on all protocols. The analyzer reports the protocol authentication information to the authenticator. It then receives whether the authentication was a success or not. Information on each activity is stored in the DB. Inquiries for auditing and monitoring are sent to the DB, and the response to this is received. LOG exists independently of the DB and stores the activity information of all modules.

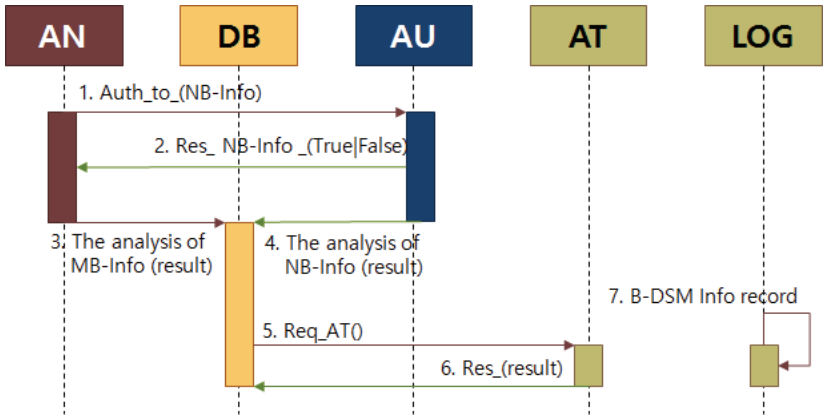

Fig. 3. Service scenario of HB-DIPM.

3.3 Analysis of HB-DIPM

In this section, we analyze the HB-DIPM by comparing it with other existing studies based on the major components of security requirements, as discussed in Section 2.

Table 2. Comparison among the exiting researches and our HB-DIPM

Characteristic	Wang and Wang [22]	Dewan et al. [23]	Mohaisen et al. [24]	Nissim et al. [25]	Alam et al. [26]	HB-DIPM
Confidentiality	△	△	△	○	△	○
Integrity	○	△	○	○	○	◎
Accuracy	○	△	○	△	○	◎
Reliability	○	△	○	△	◎	◎
Availability	○	△	△	△	○	◎

◎=good, ○=middle, △=weak.

Table 2 shows the comparison among the exiting researches and our HB-DIPM. The method used in [22,26] is a way to detect malware and is excellent in preventing execution, but it falls short in terms of integrity and usability studies [23,24]. If the malware is designed to not operate in a specific environment, that is, in a virtualized environment, it is difficult to acquire quality analysis information, and, thus, reliability is hard to secure. The research in [25,26] are excellent in detecting or preventing the intrusion of malware, malware execution, and redirection, but integrity and usability are not considered and are limited in securing reliability. Only using social information to analyze is not enough to prevent already known intrusions. By preventing a malicious act over an existing static or dynamic analysis detection method, the proposed HB-DIPM provides confidentiality. In addition, accuracy is strong while dealing with host-based behavior-monitoring; monitoring network-based actions; user-selected service; and usage patterns, such as the number of times; and can perform detection and response comparisons. It also includes monitoring and certification management, which can guarantee integrity. It has credibility through audit trails and by logging information independent of management can also ensure the availability of the DB failure in targeted attacks via a separate configuration DB.

4. Conclusion

We reviewed the causes that led to the emergence of the future Internet and described the requirements for information security in the future Internet in order to address security threats. The approach to the future Internet can be categorized into an evolutionary approach where we gradually improve existing technologies and a revolutionary approach that champions a clean slate from which we should seek a fundamentally innovative way without considering the compatibility of the existing Internet. The most important issue in the future Internet is the issue of security. The Internet as it currently exists has many counterproductive features, such as the threat to network security posed by malware, online fraud, the denial of service attacks, and spam mail. To address existing and future threats, the detection of and response to malware that meets the security requirements are needed.

In this paper, we have proposed HB-DIPM in which the service model detects malware through host-based behavior monitoring and network-based monitoring to reinforce security. Only authorized users can use the services and reliability is secured through protocol authentication. Moreover, the auditing and monitoring functions and logging of information are independently managed to guarantee usability.

In the future, additional research on information security threats and protocols, mechanisms, and functions to resolve these issues through an evolutionary or a revolutionary approach must be carried out.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the government of Korea (MSIP) (No. 2016R1A2B4011069).

References

[1] S. Ata, D. Huang, X. Liu, A. Wada, T. Xing, P. Juluri, C. J. Chung, Y. Sato, and D. Medhi, "SeRViTR: a framework, implementation, and a testbed for a trustworthy future Internet," *Computer Networks*, vol. 63, pp. 128-146, 2014.

[2] A. Ghezzi and M. Dramitinos, "Towards a Future Internet infrastructure: analyzing the multidimensional impacts of assured quality Internet interconnection," *Telematics and Informatics*, vol. 33, no. 2, pp. 613-630, 2016.

[3] P. Jappinen, R. Guarneri, and L. M. Correia, "An applications perspective into the Future Internet," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 249-254, 2013.

[4] K. C. Wang, M. Brinn, and J. Mambretti, "From federated software defined infrastructure to future Internet architecture," in *Proceedings of International Science and Technology Conference Modern Networking Technologies (MoNeTeC)*, Moscow, Russia, 2014, pp. 1-6.

[5] M. Berman, J. S. Chase, L. Landweber, A. Nakao, M. Ott, D. Raychaudhuri, R. Ricci, and I. Seskar, "GENI: a federated testbed for innovative network experiments," *Computer Networks*, vol. 61, pp. 5-23, 2014.

[6] A. Hakiria, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud "Software-defined networking: challenges and research opportunities for Future Internet," *Computer Networks*, vol. 75, pp. 453-471, 2014.

[7] C. Granell, D. Havlik, S. Schade, Z. Sabeur, C. Delaney, J. Pielorz, et al., "Future Internet technologies for environmental applications," *Environmental Modelling & Software*, vol. 78, pp. 1-15, 2016.

[8] The Global Environment for Network Innovations (GENI) [Online]. Available: http://groups.geni.net.

[9] J. Kim and D. Kim, "A Future Internet testbed in Korea," in *Proceedings of the 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing (WorldComp*), Las Vegas, NV, 2011 [Online]. Available: http://weblidi.info.unlp.edu.ar/worldcomp2011-mirror/ICM.htm.

[10] A. Lanna, F. Liberati, L. Zuccaro, and A. Di Giorgio, "Electric vehicles charging control based on Future Internet generic enablers," in *Proceedings of 2014 IEEE International Electric Vehicle Conference (IEVC)*, Florence, Italy, 2014, pp. 1-5.

[11] W. Tsai, C. F. Lai, and A. V. Vasilakos, "Future Internet of Things: open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201-2217, 2014.

[12] Y. Park, D. S. Reeves, and M. Stamp, "Deriving common malware behavior through graph clustering," *Computers & Security*, vol. 39, pp. 419-430, 2013.

[13] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42-57, 2013.

[14] S. J. Hashim, A. R. Ramli, F. Hashim, K. Samsudin, R. Abdullah, A. R. Azmir, L. B. Osamah, I. A. Al-Baltah, and M. M. Al-Habshi, "SCARECROW: scalable malware reporting, detection and analysis," *Journal of Convergence Information Technology*, vol. 8, no. 14, pp. 1-12, 2013.

[15] Y. Qiao, Y, Yabg, L. Ji, and J. He, "Analyzing malware by abstracting the frequent itemsets in API call sequences," in *Proceedings of 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Melbourne, Australia, 2013, pp. 265-270.

[16] R. Islam, R. Tian, L. M. Batten, and S. Versteeg, "Classification of malware based on integrated static and dynamic features," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 646-656, 2013.

[17] L. Feng, X. Liao, Q. Han, and H. Li, "Dynamical analysis and control strategies on malware propagation model," *Applied Mathematical Modelling*, vol. 37, no. 16, pp. 8225-8236, 2013.

[18] D. DeBarr, V. Ramanathan, and H. Wechsler, "Phishing detection using traffic behavior spectral clustering and random forests," in *Proceedings of 2013 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Seattle, WA, 2013, pp. 67-72.

[19] B. Prelipcean, A. S. Popescu, and D. T. Gavrilut, "Improving malware detection response time with behavior-based statistical analysis," in *Proceedings of 2015 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, Timisoara, Romania, 2015, pp. 232-239.

[20] G. Aloi, M. Di Felice, V. Loscri, P. Pace, and G. Ruggeri, "Spontaneous smartphone networks as a user-centric solution for the Future Internet," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 26-33, 2014.

[21] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart device," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 961-987, 2014.

[22] P. Wang and Y. S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier," *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 1012-1026, 2015.

[23] P. Dewan, A. Kashyap, and P. Kumaraguru, "Analyzing social and stylometric features to identify spear phishing emails," in *Proceedings of 2014 APWG Symposium on Electronic Crime Research (eCrime)*, Birmingham, AL, 2014, pp. 1-13.

[24] A. Mohaisen, O. Alrawi, and M. Mohaisen, "Amal: high-fidelity, behavior-based automated malware analysis and classification," *Computer & Security*, vol. 52, pp. 251-266, 2015.

[25] N. Nissim, R. Moskovitch, L. Rokach, and Y. Elovici, "Novel active learning methods for enhanced PC malware detection in windows OS," *Expert Systems with Applications*, vol. 41, no. 13, pp. 5843-5857, 2014.

[26] S. Alam, R. N. Horspool, I. Traore, and I. Sogukpinar, "A framework for metamorphic malware analysis and real-time detection," *Computers & Security*, vol. 48, pp. 212-233, 2015.

Jeong Kyu Lee

He received B.S. in Mokwon University in 2014, and M.S. degrees in Department Computer Science and Engineering from Seoul National University of Science and Technology in 2016. His current research interests include e-healthcare, mobile communication and computer security.

Seo Yeon Moon

He received B.S. in School of Computer Engineering from Kumoh National Institute of Technology, and Master Course in Department Computer Science and Engineering from Seoul National University of Science and Technology in 2016. His current research interests include Internet of things, network security and quantum computer.

Jong Hyuk Park

He received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December 2002 to July 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co. Ltd. in Korea. From September 2007 to August 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology, Korea.