ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

사이버 방어를 위한 적응형 다중계층 보호체제☆

Adaptive Multi-Layer Security Approach for Cyber Defense

이 성 기1* 강 태 인1
Seong-kee Lee Tae-in Kang

요 약

사이버 공간에서 첨예화, 복잡화되고 있는 공격을 일대일 방식으로 방어하는데 한계가 있으므로 보다 효과적인 방어 방법이 필요하다. 본 고에서는 내외부의 공격에 대해 자산을 체계적 적응적으로 방어할 수 있는 다중계층 보안체제 구축 방안을 제시한다. 방어지역(Defense Zone)을 중심으로 한 다중계층 보안체제의 구조를 고안하고, 사이버 위협분석과 방어기술 자동할당 등 구현에 필요한 기술요소들에 대해 논의한다. 또한, 다중계층 보안체제에 대한 효과와 적용성을 보인다. 향후, 제시된 방안의 구체화를 위해 방어지역에 대한 상세구조설계, 최적 방어기술 자동선택방법, 위협 탐지를 위한 정상상태 모델링 기술 등에 대한 연구가 필요하다.

☞ 주제어 : 사이버 방어, 다중계층 보안모델, 적응형 보안체제

ABSTRACT

As attacks in cyber space become advanced and complex, monotonous defense approach of one-one matching manner between attack and defense may be limited to defend them. More efficient defense method is required. This paper proposes multi layers security scheme that can support to defend assets against diverse cyber attacks in systematical and adaptive. We model multi layers security scheme based on Defense Zone including several defense layers and also discuss essential technical elements necessary to realize multi layers security scheme such as cyber threats analysis and automated assignment of defense techniques. Also effects of multi layers security scheme and its applicability are explained. In future, for embodiment of multi layers security scheme, researches about detailed architecture design for Defense Zone, automated method to select the best defense technique against attack and modeling normal state of asset for attack detection are needed.

☞ keyword : Cyber Defense, Multi-Layer Security Model, Adaptive Security System

1. Introduction

Today computing environments become wide from hand-phone to internet, and computing services support diverse activities from individual to government. Using computer, we can buy books without going to the book store, transit money without going to the banks, send letter without going to the post office, reserve hotel with payment. The problem is that the more services we require, the more computers must be interconnected and the more information has to be opened and transferred over networks. If our information is leaked and misused by someone, then unwanted damages can be occurred in real life. In actual, many real damage cases have been reported and its trends are increasing. Nowadays many people are afraid about cyber threats such as service stop, information interception, modification which may result in economic loss[1,2,3]. However, unfortunately since they are concealed somewhere in stealth and occurred all at once in explosive, it is not easy to find threats or avoid attacks before real attacks come out and victims are suffered from them. In real case of distributed denial of services attack happened in recent, attack codes were covertly concealed in zombie for two years before attack. During thirty minutes after attack, hundreds of servers were corrupted and services were stopped.

Although many techniques and methods have been developed and deployed to defend these cyber threats or attacks, it is still not sufficient to securely keep our life from

[1] The 2nd R&D Institute-3, Agency for Defense Development, Seoul, 138-813, Korea.
* Corresponding author (seongkeel@hanmail.net)
☆ 본 논문은 2014년도 인터넷정보학회 추계학술발표대회우수논문 추천에 따라 확장 및 수정된 논문임
[Received 2 February 2015, Reviewed 9 February 2015(R2 17 April 2015, R3 11 June 2015), Accepted 21 July 2015]

cyber threats and attacks. Unknown attacks come out in continuous, and attack tricks become complicated and diverse. In practical, it is difficult to defend them by one defense technique or by one-to-one response manner. In order to cope with this situation, it is necessary to construct stronger defense system capable to use available defense techniques in maximum, to minimize or mitigate damages of attacks, to automatically response to attacks, to detect even unknown attacks if possible and so on[4,5,6,7].

As a method to realize such a cyber defense system, this paper proposes an adaptive multi-layer security scheme. The concept of this scheme is to enforce attacks go through multiple layers in which all available defense techniques are deployed. During going through layers, attacks can be cut off and damages can be mitigated. For this scheme, at first, this paper examines the overall security environments and its limitation in Section 2. Section 3 discusses the adaptive multi-layer security scheme. Here we model security environment into multi-layer security architecture based on defense zone and describe activities necessary to realize the architecture. Also we discuss applicability of our approach to mobile phone. Since this subject is not still matured, many techniques should be complemented. In Section 4, with the effect of multi layers security scheme, we address some technical issues needed to be studied further.

2. Related Works

In general, security environments include assets to be protected, attack to assets and defense against attacks.

Assets. Assets are computing resources which must be protected from attacks or threats. Assets provide many services for us, but may also have weaknesses which attackers can intrude into. The primary assets are systems, networks and data. Systems are diverse from host, server or PC to embedded system or devices. Networks include wired network and wireless network such as Bluetooth, Wi-Fi etc. Data includes information about assets themselves, sensitive individual information etc. As computing environments become wide, assets to be protected are increasing and their type become diverse.

Attack. Attacks intentionally intrude into assets with malicious purposes. These can steal, corrupt or modify assets. There are internal attacks and external attacks. While external attacks are primarily executed by hackers or the third parties in open computing environment such as internet, insider attacks are executed by insiders of organization in closed computing environment like classified network. Many attacks can be executed by diverse methods such as malicious code, and attacks are increasing in sharp.

Defense. Defense protects assets related to computing and services against attacks or threats. Defense activities include detecting attack, tolerating attack, recovering losses by attack, etc. How to defend can be dependent upon the importance level of assets or services. The essential services must be sustained in tolerant so that they can't be stopped. In order to defend threats or attacks, many defense techniques such as vaccines have been developed, but still are not sufficient.

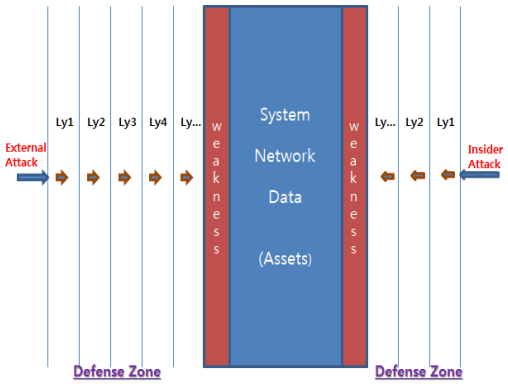
As we know, relation of attack and defense is like spear and shield. Keeping track of attacks, defense methods are evolving. However, since most defense techniques are treat-after-attack method, they have limitations for preventing attacks or damages[8,9]. In ideal, defense techniques of treat-before-attack type can be the best defense method, but it is difficult to find unknown threats or block attacks beforehand. In practical, since it is not easy to develop defense techniques of the treat-before-attack type, it may be a useful alternative to construct more solid defense system using currently available defense techniques in maximum. As alternatives, some issues like dynamic defense, layered defense has been studied. In particular, there are many studies on layered defense, in which they primarily focus on security within certain function layer of systems or networks[10,11,12]. However, since attacks target any vulnerabilities on overall computing environment rather than certain layer, in more wide view, it is necessary to examine security environment, design how to defend computing assets against cyber attacks or threats. That is, security architecture, cooperation among layers, application of defense techniques and so on must be considered in comprehensive.

3. Adaptive Multi-layer Security Scheme

3.1 Multi-Layer Security Architecture

When certain attack intrudes into asset, if several techniques rather than one technique try to block it, then the possibility to defend the attack or to mitigate damages would be more high. Also, if defense techniques are applied step by step rather than at random, then existing available defense techniques can be used to defend attack in systematical. Considering these viewpoints, this paper devises a multi-layer security scheme including several defense layers. Each layer in scheme applies defense techniques to block incoming attacks. When defense at the first layer is failed, techniques in next layer are fired towards the attacks which have just passed through the first layer. In this manner, defense techniques in each layer are applied to the intruding attacks until final layer. It can say that layers play a role of filtering attacks.

In order to design such multi-layer security scheme, this paper models typical security environment including assets, attack and defense into a multi-layer security architecture like Figure 1. As shown in the figure, defense part is composed of several layers which organize a kind of an area for defense. This paper calls the area by 'Defense Zone'.



(Figure 1) Multi-Layer Security Architecture

In the multi-layer security architecture of Figure 1, it is very important how to design the defense zone. Primary considerations on the design of defense zone are layers, techniques, strategies and organizations for defense.

Defense Layers. Layer plays a role as a kind of fence to block attacks or threats. The front side layers can usually be the layers related to defend access to assets such as authentication, authorization, etc. The rear side layers can be the layers related to defend contents of assets such as data encryption etc. The partition among layers is not stiff, but it is desirable to define partition criteria so that each layer can have unique role. Also number of layers will be dependent on partition criteria or security policy. Attacks can intrude to any layer or to multi layers in concurrent.

Defense Techniques. Each layer has defense techniques necessary to play its role. For example, when the role of the first layer is to defend access to assets, the techniques such as authentication or authorization must be deployed in the layer. According to features of techniques, it is necessary to classify the available defense techniques into the suitable layers. Also, new defense techniques must be developed in continuous and deployed in a layer of the defense zone. For example, if new strong authentication technique is developed, then it can be added in the first layer. In addition, when attacks are detected, method to select the most effective technique among available defense techniques in a layer is needed.

Defense Strategies. Strategies setup procedures, activities etc related to the operation of multi-layer security scheme. Strategies must be established so that defense techniques can effectively mitigate attacks[13]. For example, in order to enhance defense effectiveness, we can detail defense activities in layer into recognition, resistance and recovery step. Recognition detects attacks and assesses the resultant damage caused by attacks. Resistance tolerates with attacks so that services can be delivered continuously even under attacks. Recovery gets exploited assets or services back normal state after damages. Defense techniques must be also deployed according to the detail steps. These defense strategies may also be dependent on the security policy of organization responsible for the operation of defense system.

Defense Organization. Organization operates and manages multi-layer security scheme. It is necessary to establish work flow, information flow etc among organizations or departments related to the operation of multi-layer security scheme. Since late response to attacks may increases damages, organization must try to react to attacks as fast as possible and maximize defense effect. So, it is needed to promptly response to attacks

and automatically decide the best defense technique against attack. If defense techniques do not available or fail to defend, then organization must promote the development of new defense techniques and deploy the developed techniques into the proper layers of defense zone.

In order to realize the multi-layer security architecture described above, technical activities such as analysis of threats, classification of available defense techniques and assignment of defense techniques are required. The following sections describe these activities.

3.2 Assessment of Threat to Assets

The first activity to realize the multi-layer security architecture is to extract plausible cyber threats to assets. Since it is not easy to find threats before attacks occur in real, we can extract them from innate weaknesses of assets such as CWE and from attacks already known such as CVE. For each identified threat, it is necessary to analyze details such as the asset which threats occur, occurrence possibility, effects, severity, etc. Table 1 shows an example of threat analysis. Threat TH1 in the table means that although it does not happen frequently, since unauthorized user may access to system as system manager and make system unavailable, that threat is very dangerous to system availability. When new assets such as embedded system, mobile system or hand phone device are added in computing environments, new cyber threats caused by them must be also analyzed and listed up like Table 1.

(Table 1) Assessment of Threat Effect(example)

Asset	Threat	Probability	Effect	Severity
System	TH1: Unauthorized user access to system as system manager.	Low	Make system Unavailable	Serious
Data	TH2: Unauthorized user access to data as database user.	High	Steal critical information	Moderate

3.3 Classification of Defense Techniques

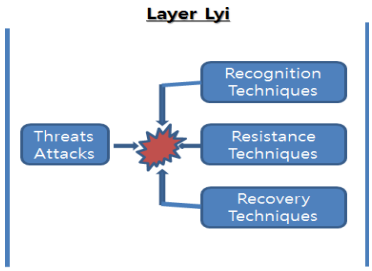
After threat analysis, it is necessary to identify defense techniques to prevent or defend threats identified in Table 1. As well as the existing defense techniques, the techniques needed to be newly developed future can be included. The identified defense techniques are deployed into layers of the defense zone. In deployment, defense strategies of organization must be reflected. As described in the defense strategy part of Section 3.1, when certain organization partitions defense activities into recognition, resistance and recovery step, defense techniques must be deployed into the these detailed steps. In result, for each threat, defense techniques are deployed by strategy, and defense zone layer able to react to the threat is designated. Table 2 shows an example of classification of defense techniques. As shown in table, in order to prevent or defend threat TH1, two defense techniques T1 and T2 for recognition, T5 for resistance and T7 for recovery can be used in the layer 1 of defense zone. Similarly, for threat TH2, techniques T3,4,6,8,9 can be used in the layer 2.

(Table 2) Classification of Defense Techniques(example)

Threats	Defense Strategies			Defense Zone Layer
	Recognition	Resistance	Recovery	
TH1: Unauthorized user access to system as system manager.	T1: Require hint related to password T2: Maintain and analyze access log	T5: Require system managers a stronger authorization mechanism	T7: Provide mechanism to automatically undo and recover system state	1
TH2: Unauthorized user access to data as database user.	T3: Monitor access Trials. T4: Compare user password	T6: Require privileged users a stronger authorization mechanism such as digital certificate	T8: Recover database from backup T9: Recreate records	2

3.4 Automated Assignment of Defense Techniques

When unexpected attack indications or situations are detected, defense techniques like Table 2 must be applied to recognize whether attacks really occur or not, resist to them if attacks occur, or recover losses if assets are already corrupted by attacks. Figure 2 shows situation that defense techniques are applied to defend attacks incoming into a layer Lyi.



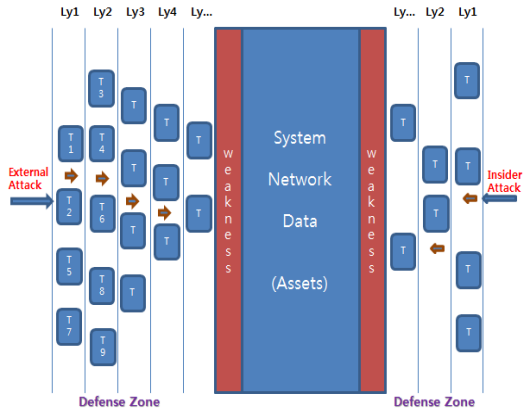
(Figure 2) Automated Assignment of Defense Techniques in Layer Lyi

If attacks pass through the layer Lyi, then defense techniques in the layer Lyi+1 are used to cope with attacks just coming into the layer Lyi+1. If the layer Lyi+1 is final layer and attacks pass through even the layer, then unfortunately assets such as system, network or data may be exploited.

There are some considerations about operation in layer. one is that when certain attack intrudes into a layer, it is needed to select the most appropriate defense technique in the layer to cope with the attack. For example, when threat TH1 of Table 2 is detected, we must decide either T1 or T2 to response to threat TH1. Another issue is time factor. In usual, because late response will increase misuse of assets or damages, defense techniques should be used in real time. To satisfy these technique selection and real time reaction problems, it is necessary to automatically select the best defense technique in layer and execute it without intervention of man[14,15]. For this, methods about automation of defense technique selection, real time attack situation awareness, triggering condition for certain technique to be selected and so on are required. Study on these methods is not included in this paper, they must be studied future.

3.5 Operation of Defense Zone

After multi-layer security architecture is constructed, defense techniques will be deployed and used in layers of the defense zone. In early period, existing available defense techniques are primarily deployed. Since their defense capabilities are known, and number of techniques is not sufficient, the defense zone may be frequently penetrated by modified or new attacks. However, as new defense techniques are accumulated on scheme continuously, defense capability will increase in gradual. Finally, they may have the capabilities affordable to defend even unknown attacks. Figure 3 shows an operational view of multi-layer security scheme in conceptual. As more defense techniques are deployed in layers, defense capabilities enhances in gradual. In view of cyberwar, the defense zone in multi-layer security scheme may play a role of the fighting line on cyberspace. How to operate the defense zone is very important issue in cyber defense organization.



(Figure 3) Operational View of Multi-layer Security Scheme

3.6 Applicability of Multi-layer Security Scheme

To show the applicability of multi-layer security scheme, this paper discusses about construction of multi-layer security scheme for mobile phone based on Android. At first, it is needed to analyze threats of mobile phone. Most threats on mobile phone can be identified as follows: maliciously using the permissions granted to installed application, exploiting a vulnerability in the Linux kernel or system libraries, draining resources, exposing private content, compromising internal network, etc[16,17]. For each threat identified above, by analyzing occurrence frequency, its effect and severity, threats on mobile phone can be listed as Table 3. Table 3 partially shows the analysis results about threats on mobile phone[18].

(Table 3) Assessment of Threat on Mobile phone

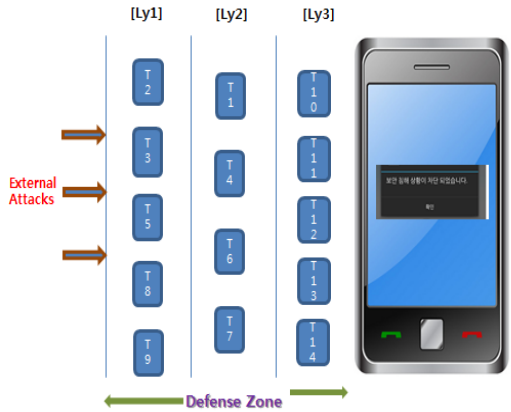
Asset	Threat	Probability	Effect	Severity
Mobile phone	TH1: Maliciously using the permission of application	Medium	Make application misused	Moderate
	TH2: Exploiting the vulnerability in Linux kernel	Low	Rooting Expoliting services and data	Serious
	TH3: Exploiting phone and privacy data	High	Flow out privacy data, Economic loss	Serious

After analysis, defense techniques to block the identified threats must be classified and deployed. It is necessary to choose defense techniques to react to each threat, and decide defense layers into which defense techniques are deployed. Like Table 2 before, when allocating defense techniques according to strategies and deploying them into layers in the defense zone, defense techniques to block threats of mobile phone can be classified like Table 4, which partially classifies defense techniques for threats TH1, TH2 and TH3 in Table 3. For example, in order to defend threat TH1, techniques T1 for recognition, T4 for resistance, T6 and T7 for recovery are deployed into layer 2 of the defense zone.

(Table 4) Classification of Defense Techniques for Mobile phone

Threats	Defense Strategies			Defense Zone Layer
	Recognition	Resistance	Recovery	
TH1: Maliciously using the permission of application	T1: Monitering malicious app. using vaccine	T4: access control for app. operations by security policy	T6: Reassign Permissions. T7: Notify intrusion and reaction result	2
TH2: Exploiting the vulnerability in Linux kernel	T2: Check kernel integrity T3: Compare input pattern with device pattern	T5: access control for resources by security policy	T8: Wipe data T9: Notify intrusion and reaction result	1
TH3: Exploiting phone and privacy data	T10: Monitoring processes	T11: access control to data by security poli. T12: Data Envryption	T13: Notify intrusion and reaction result T14: Wipe data, Disuse phone	3

To construct defense zone for mobile phone, it is necessary to establish defense layers. Using the results of threats analysis and techniques classification, we decide that at least 3 layers for defense zone must be needed as follows: the layer Ly1 to defend attacks on kernel, the layer Ly2 to defend attacks on mobile applications and the layer Ly3 defending attacks related to content stored in phone. In the layer Ly3, defense techniques such as data encryption can be deployed. Figure 4 shows multi-layer security scheme for mobile phone including 3 layers in the Defense Zone.



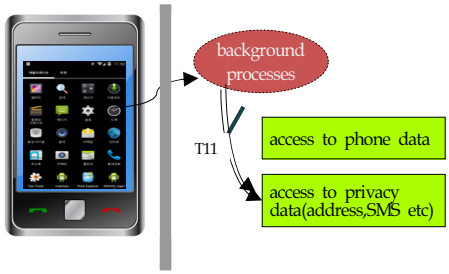
(Figure 4) Multi-Layer Security scheme for Mobile phone

In practical, when someone try to intrude into phone for rooting, if technique T3 at the layer Ly1 is selected to defend it, then T3 compares input pattern with authorized user pattern and blocks unauthorized patten, as shown in the left screen of Figure 5. However, if rooting is successful, and device is unlocked as the middle screen of Figure 5, then T5 can be used to defend exploitation. Since T5 limits the access to phone resources by the security policy of SEAndroid(Security Enhanced Android) which applies basically the denial policy at objects, T5 can block exploitation of phone resources even after rooting[19]. However, if even T5 fails to defend the attack, then since data on phone can be exploited, T8 wipes out all data on phone, or T9 notices intrusion fact to user like the right screen of Figure 5.

Device locked Before Rooting(T3) | Device Unlocked After Rooting(T5) | Notice Blocking Result(T9)

(Figure 5) Block Rooting on Mobile phone

Most threats or attacks on mobile phones may target phone or individual data. For example, as shown in Figure 6, when an user presses favorite applications in user view side, hidden malicious codes(processes) can be executed in background on phone. When such threat TH3 passes through the layer 1, 2 of defense zone and is not checked by monitoring(T10), the threat TH3 can try to access phone data or privacy data such as addresses, SMS data etc. In this time, T11 can be used to block TH3 based on access control policy. In result, although TH3 passes through layers 1 and 2, it is blocked by the access control technique T11 deployed in the layer 3.



[User View] [Background]

(Figure 6) Block Exploitation on Mobile phone

Like the case of mobile phone described above, the multi-layer security scheme may be also applied to defend assets such as system, network, etc.

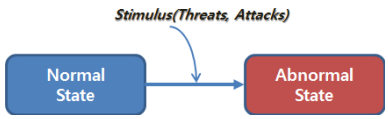
4. Benefits and Future Issues

This paper devises an adaptive multi-layer security scheme and shows its applicability by simple implementations on mobile phone. The features or benefits of the scheme are as followings.

- Multi-layer security scheme can mitigate exploitations by blocking attacks in layer by layer.
- Existing available defense techniques can be managed systematically and used in right purposes without keeping them idle.
- In managerial aspects, multi-layer security scheme helps that organization can well establish activities, policies and procedures for cyber defense.
- When analyzing the effectiveness of defense zone, we can identify weak layers. It is possible to identify techniques required to be newly developed with reason.
- After all, the most benefit is that the more defense techniques are accumulated in defense zone, the defense capability against threats or attacks can be enhanced in gradual. By reusing the existing techniques, new techniques can easily be developed.

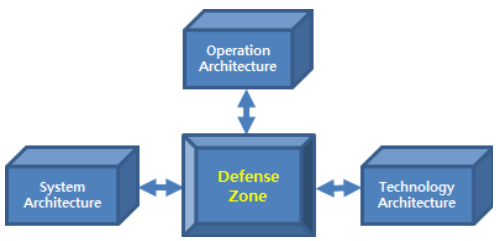
Although many benefits are expected, in order to realize adaptive multi-layer security scheme in practical, many issues must be studied. At first, it is needed to identify assets in more detail. Then, for detailed assets, analyzing threats and classifying defense techniques must be executed. Also, as described in Section 3.4, when certain threat is found or attack is detected, methods to automatically select the best defense technique in layer must be studied. In addition, it is considerable to develope multi-layer security scheme into a cyber defense framework in which individual defense technique is executed as a component. The study to reorganize many existing defense techniques deployed in organization into the defense zone will be valuable.

Another research issue is related to an advanced detecting method. In practical, it is difficult to know all possible threats or attacks including unknown threats or attacks before real attacks occur. Even though the defense zone is equipped by huge techniques, it is still not sufficient to completely prevent all threats or defend all attacks. In ideal, one of solutions to deal with this problem is to define the normal state of assets, and classifies every stimulus or events which make the normal state of assets fall in the abnormal state into threats or attacks. The more detail we represent the normal state of assets, the more accurate we can find threats or attacks[20,21,22]. Figure 7 simply shows the concept identifying threats or attacks from model of the normal state of assets.



(Figure 7) Modeling Normal State of Assets

In future, when an organization constructs multi-layer security scheme, it is important to establish how to run the defense zone in detail. Many aspects(views) about defense zone must be considered: layers, techniques, systems, organizations, their relationship and so on. For this, it will be useful to define architectures as follows: Operation Architecture(OA), System Architecture(SA), Technique Architecture(TA). These architectures must be interrelated with each other like Figure 8, and provide bases for establishment of security policy, development of defense techniques and construction of cyber defense system in organization[23].



(Figure 8) Architectures for Defense Zone

5. Conclusion

Today, cyber threats or attacks frequently appear around our life activities. Since it may be insufficient to defend them by one technique or one-to-one response, more systematic efficient defense solution is essential. As one of solutions, this paper proposes an adaptive multi-layer security scheme for cyber defense. To devise the scheme, we models a multi-layer security architecture focused on the defense zone and discusses activities such as assessment of threats, classification of defense techniques and automated assignment of defense technique. In particular, we show its applicability by simply implementing multi-layer security scheme for mobile phone. From this research result, we conclude that the multi-layer security scheme based on defense zone can be one of the systematic solutions to defend cyber attacks in effective.

This research about adaptive multi-layer security scheme is still ongoing, and many technical issues to realize the scheme are remained. As further researches solve the issues, adaptive multi-layer security scheme may be considered as an useful framework of future cyber defense system. More researches and concerns on this prospective cyber defense approach are needed.

References

[1] F. Yaqin, Z. Ge, L. Miao and Z. Xin, “The study found that the intelligent mobile phone technology of malicious code,” ICSEM-13, 2013, pp.1130-1133.

[2] US-CERT Technical Information Paper TIP-10-105- 01 Cyber Threats to Mobile Devices, US Dept. of Homeland Security, Apr. 15, 2010.

[3] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti and M. Rajarajan, “Android Security: A Survey of Issues, Malware Penetration and Defenses,” IEEE Communication Surveys and Tutorial, Jan. 2015.

[4] K. Kim, Development Prospects of Future Internet Security Technology, ppt material, Sep. 2010.

[5] National Science and Technology Council, Federal Plan for Cyber Security and Information Assurance Research and Development, Apr. 2006.

[6] R. Armstrong, J. Mayo and F. Siebenlist, Complexity Science Challenges in Cyber security, Sandia National Lab., Mar. 2009.

[7] P. Phister, “Cyberspace: The Ultimate Complex Adaptive System,” The International C2 Journal, vol.4, no.2, 2010-2011.

[8] C. Park, S. Lee, “A Study of the User Privacy Protection Behavior in Online Environment: Based on Protection Motivation Theory,” Journal of Internet Computing and Service(JICS), vol.15, no.2, Apr. 2014, pp.59-71. http://dx.doi.org/10.7472/jksii.2014.15.2.59

[9] Y. Ham, H. Lee, “Malicious Trojan Horse Application Discrimination Mechanism using Realtime Event Similarity on Android Mobile Devices,” Journal of Internet Computing and Service(JICS), vol.15, no.3, Jun. 2014, pp.31-43. http://dx.doi.org/10.7472/jksii.2014.15.3.31

[10] R. Lamb, R. Hayes and C. Ling, Dynamic Defense: Building Enterprise-wide Cybersecurity that Learns, Adapts, and Proactively Combats Rapidly Changing Cyber Threats, Booz Allen Hamilton Inc., 2012.
[11] K. Wilson and M. Kiy, “Some Fundamental Cybersecurity Concepts,” IEEE Access, vol.2 2014, pp.116-124.
[12] R. Goudar and P. More, “Multilayer Security Mechanism in Computer Networks,” Int. Jou. of Scientific and Research Pub., vol.2, Issue 1, Jan. 2012.
[13] J. Eom, “Cyber Defense Strategy for Information Superiority in Cyberspace,” Journal of Security Engineering, vol.9, no.5, Oct. 2012, pp.377-386.
[14] B. Benyo, P. Pal, R. Schantz, A. Paulos and D. Musliner, “Automated Self-Adaptation for Cyber Defense-Pushing Adaptive Perimeter Protection Inward”.
[15] D. Dasgupta. “Immuno-Inspired Autonomic System for Cyber Defense”.
[16] A. Shabtal, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev and C. Glezer, “Google Android:A Comprehensive Security Assessment,” IEEE Security & Privacy, Mar./Apr. 2010, pp.35-44.
[17] A. Shabtal, Y. Fledel and Y. Elovici, “Securing Android-Powered Mobile Devices Using SELinux,” IEEE Security & Privacy, May/Jun 2010, pp.36-44.
[18] A. Yuksel, A. Zaim and M. Aydin, “A Comprehensive Analysis of Android Security and Proposed Solutions,” I.J. Computer Network and Information Security, 2014, pp.9-20.
http://www.mecs-press.org/10.5815/ijcnis.2014.12.02
[19] S. Smalley and R. Craig, “Security Enhanced(SE) Android: Bringing Flexible MAC to Android”.
[20] D. Wagner and D. Dean, “Intrusion Detection via Static Analysis,” IEEE, 2001.
[21] O. Hofmann, A. Dunn, S. Kim, I. Roy and E. Witchel, “Ensuring Operating System Kernel Integrity with OSck,” ACM 2011.
[22] N. Petroni and M. Hicks, “Automated Detection of Persistent Kernel Control-Flow Attacks,” ACM 2007.
[23] B. Kang, S. Yang and J. Lee, “A Software Development Process for Mobile Applications,” Journal of Internet Computing and Service(JICS), vol.15, no.4, Aug. 2014, pp.135-140.
http://dx.doi.org/10.7472/jksii.2014.15.4.135

◐ 저 자 소 개 ◑

이 성 기 (Seong-kee Lee)
1984년 동국대학교 수학과(이학사)
1989년 연세대학교 공학대학원 전산학과(공학석사)
2003년 고려대학교 대학원 컴퓨터공학과(이학박사)
1984～1998 한국국방연구원 연구위원
1999～현재 국방과학연구소 수석연구원
관심분야 : 사이버보안, 소프트웨어공학, 인공지능
E-mail : seongkeel@hanmail.net

강 태 인 (Tae-in Kang)
1993년 홍익대학교 컴퓨터공학과(공학사)
1995년 홍익대학교 대학원 전산학과(공학석사)
1995～1998 국방정보체계연구소 연구원
1999～현재 국방과학연구소 책임연구원
관심분야 : 모바일 보안 기술
E-mail : tanekang@gmail.com