Journal of The Korea Society of Computer and Information
Vol. 20 No. 12, pp. 61-66, December 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.12.061

A Security Assessment on the Designated PC service

Kyungroul Lee*, Kangbin Yim**

Abstract

In this paper, we draw a security assessment by analyzing possible vulnerabilities of the designated PC service which is supposed for strengthening security of current online identification methods that provide various areas such as the online banking and a game and so on. There is a difference between the designated PC service and online identification methods. Online identification methods authenticate an user by the user's private information or the user's knowledge-based information, though the designated PC service authenticates a hardware-based unique information of the user's PC. For this reason, high task significance services employ with online identification methods and the designated PC service for improving security multiply. Nevertheless, the security assessment of the designated PC service has been absent and possible vulnerabilities of the designated PC service are counterfeiter and falsification when the hardware-based unique-information is extracted on the user's PC and sent an authentication server. Therefore, in this paper, we analyze possible vulnerabilities of the designated PC service and draw the security assessment.

▸ Keyword : the designated PC service, security assessment, device authentication, user authentication

I. Introduction

과거 아이디-패스워드 기반의 사용자 인증을 기반으로 공인인증서, 보안카드를 이용한 사용자 인증을 비롯하여 SSL(Secure Socket Layer), OTP(One Time Password), 그래픽 인증, 바이오 인증 등으로 발전하였다. 하지만 온라인을 이용한 본인확인수단이 이와 같이 많은 발전을 이루었음에도 불구하고, 온라인 본인확인수단 그 자체, 혹은 이용환경에 따른 취약점이 드러나기 시작하면서 온라인을 이용한 서비스들의 보안위협이 나타났다. 공인인증서와 보안카드의 경우, 사용자가 계좌번호나 보안카드번호 등을 소지하지 않고 이미지 파일을 안전하지 않은 공간에 업로드 함으로써 발생하는 문제점이 존재하였으며, 공인인증서의 복제 및 재발급을 통한 탈취 등의 문제점이 있었다[1]. 또한, 피싱이나 파밍을 통해 공인인증서를 탈취하는 공격, 공인인증서의 비밀번호를 GPU를 이용하여 복호화하는 공격 등[2]이 발생하면서 공인인증서의 안전성에 대한 우려가 증가하고 있다. SSL의 경우, 보안채널의 설정을 평문으로 전송하는 문제점, 보안성이 약한 버전으로의 변경[3] 등과 프록시 서버를 이용한 개인정보의 위/변조[4], 구현상의 취약점을 이용한 공격[5] 등이 존재하였으며, OTP의 경우, 중간자 공격을 통한 OTP 값 탈취[6], 리버스 엔지니어링을 이용한 OTP 값 탈취[7] 등의 공격이 존재하였다. 그래픽 인증에서는 네트워크 계층, 가상 키보드 모듈, 단말영역 환경에서의 보안위협이 존재하였으며[8], 그래픽 인증 시 출력되는 영상을 탈취하는 공격[9][10]도 존재하였다. 이와 같은 보안위협이 드러나면서 기존에 존재하는 온라인 본인확인수단을 보다 강화하기 위한 수단이 필요하였으며, 이에 이용 PC 지정 서비스가 제안되었다[11]. 이용 PC 지정 서비스란 기존 온라인 본인확인수단들이 사용자 인증을 하는 것과는 다르게 사용자가 사용하는 PC를 인증하는 일종의 디바이스 인증기술이다. 이를 위하여

• First Author: Kyungroul Lee, Corresponding Author: Kangbin Yim
*Kyungroul Lee (carpedm@sch.ac.kr), Post-doc. researcher, Soonchunhyang University
**Kangbin Yim (yim@sch.ac.kr), Dept. of Information Security Engineering, Soonchunhyang University
• Received: 2015. 08. 31, Revised: 2015. 09. 21, Accepted: 2015. 10. 05.
• This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1A6A3A01019717 and NRF-2015R1D1A1A01057300).

사용자는 업무 중요도가 높은 서비스를 사용할 사용자의 PC를 등록하는 과정이 선행되며, 이는 PC의 하드웨어 고유정보, 예를 들면 MAC 주소, CPU 아이디, 하드디스크 시리얼 넘버 등을 인증서버로 전송하여 등록하는 과정을 의미한다. 등록이 완료된 후, 사용자가 서비스를 이용하고자 할 경우, 사용자 PC의 하드웨어 고유정보를 인증서버로 전송하여 서버에 등록된 하드웨어 고유정보와 비교함으로써 인증을 완료한다.

현재 이용 PC 지정 서비스는 은행권을 비롯한 금융 사이트, 게임 사이트, 파일 보안 솔루션 등에서 제공한다. 하지만 현재 도입되어 서비스 중인 이용 PC 지정 서비스에 대한 보안위협에 대한 연구는 미흡한 실정이다. 따라서 본 논문에서는 이용 PC 지정 서비스에서 발생 가능한 보안위협을 도출하여 실제 위협임을 확인함으로써 그 안전성을 평가하고자 한다.

II. The Security Assessment of the designated PC solution

본 논문에서는 이용 PC 지정에서 발생 가능한 보안위협을 분석하고 실험을 통해 보안위협을 확인함으로써 그 안전성을 평가하고자 한다. 이용 PC 지정 서비스의 핵심은 사용자 PC의 하드웨어 고유정보이며, 이는 등록 및 인증 시점에 추출되어 전송되기 때문에 보안위협은 해당 시점에서 발생이 가능하다. 하드웨어 고유정보를 추출하는 시점에서는 메모리 해킹이나 리버스 엔지니어링, 하드웨어 직접 제어를 통한 위/변조, 하드웨어 고유정보를 전송하는 시점에서의 웹 브라우저 중간자 공격, 인터페이스 중간자 공격에 의한 위/변조가 있다.

메모리 해킹을 이용한 하드웨어 고유정보 위/변조는 사용자 PC에 설치되는 소프트웨어 모듈이 하드웨어 고유정보를 메모리상에 저장하는 취약점을 이용한 공격이다. 소프트웨어 모듈은 하드웨어 고유정보를 추출하여 메모리에 저장한 후, 필요하다면 연산을 통하여 PC의 고유정보를 생성한다. 이 과정에서 추출하거나 생성된 하드웨어 고유정보는 반드시 메모리상에 저장되어야만 하는데, 이 시점에서 하드웨어 고유정보를 탈취하거나 위/변조를 시도하는 공격이다. 리버스 엔지니어링을 이용한 하드웨어 고유정보 위/변조는 ollydbg, windbg 등의 특정 도구를 이용하여 소프트웨어 모듈 내의 하드웨어 고유정보를 탈취하거나 위/변조하는 공격[7]이며, 웹 브라우저 중간자 공격[6] 및 인터페이스 중간자 공격[14]은 웹 페이지 및 소프트웨어 모듈과 연관된 인터페이스들에 대한 중간자 공격을 이용하여 하드웨어 고유정보를 탈취하거나 위/변조하는 공격이다. 하드웨어를 직접 제어하여 하드웨어 고유정보를 위/변조하는 공격은 이용 PC 지정 서비스에서 등록되는 특정 하드웨어를 직접 제어하여 하드웨어 고유정보를 변경하거나 추출 시 위/변조를 시도하는 공격[12][15]이다.

이용 PC 지정 서비스에서는 상기와 같은 보안위협이 존재할 가능성이 있으며, 본 논문에서는 리버스 엔지니어링, 인터페이스 중간자 공격을 시도하여 이용 PC 지정 서비스의 인증을 우회하는 공격을 시도하였다. 실험에 앞서 이용 PC 지정 서비스에서 활용하는 하드웨어 고유정보를 하드디스크 시리얼 넘버, CPU 아이디로 가정하였으며, 지정된 PC와 공격자 PC의 하드디스크 시리얼 넘버, CPU 아이디를 그림 1, 그림 2, 그림 3, 그림 4에 나타내었다.

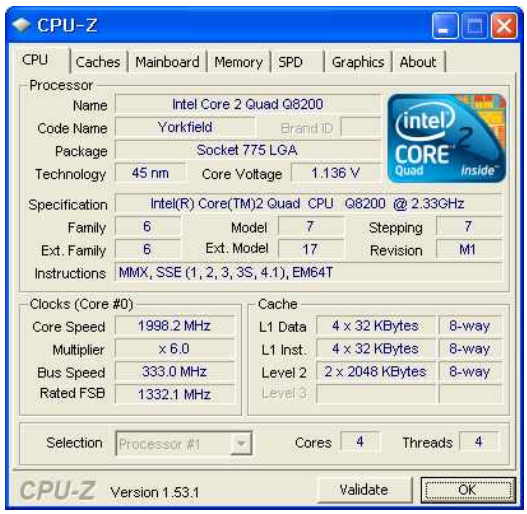

Fig. 1. Example of CPU ID on the designated PC

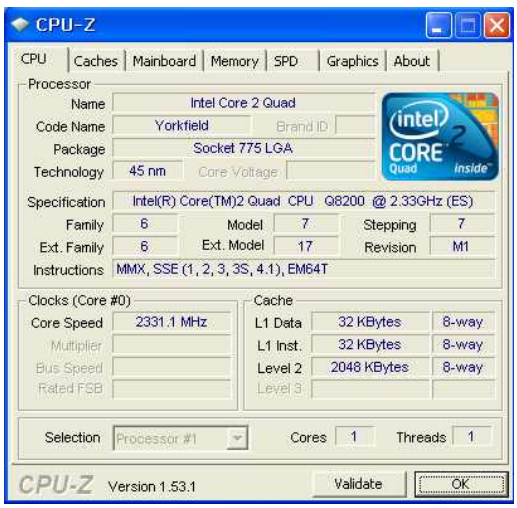

Fig. 2. Example of CPU ID on the attacker's PC

www.kci.go.kr

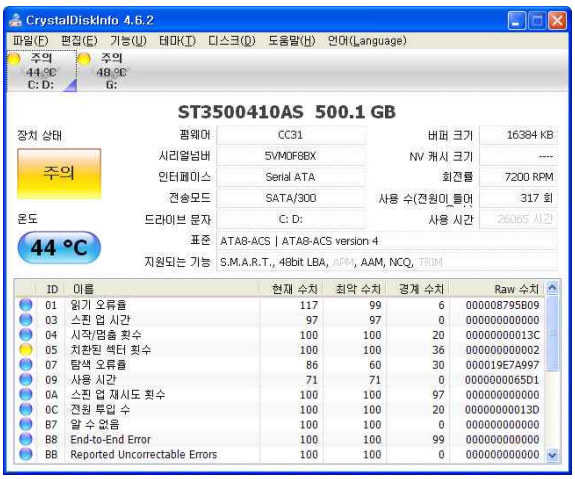

Fig. 3. Example of harddisk serial number on the designated PC

Fig. 4. Example of harddisk serial number on the attacker's PC

상기 두 하드웨어 고유정보를 이용하여 이용 PC 지정 서비스의 인증 시점에서 서버로 전송되는 정보를 패킷을 수집하는 방법, HttpSendReqest 함수의 후킹 및 리버스 엔지니어링을 이용하여 전송되는 데이터를 탈취하는 방법을 이용하여 해당 하드웨어 고유정보가 존재하는지 확인하였다. 확인결과 패킷을 수집하는 방법으로는 해당 하드웨어 고유정보가 노출되지 않았으나, HttpSendRequest 함수를 리버스 엔지니어링을 이용하는 방법에서는 하드웨어 고유정보가 노출되는 것을 확인하였으며, 그 결과를 그림 5에 나타내었다.

Fig. 5. Access information of the designated PC when authentication

상기와 같이 사용자의 아이디, 패스워드가 평문으로 드러나고, 사용자가 인증서버에 접속하기 위한 접속정보를 전송하며, mac2 필드를 통해 지정된 PC의 하드웨어 고유정보를 전송하는 것을 확인할 수 있다. 자세히 살펴보면 usrid 필드를 통해 사용자의 아이디(icon0001)를 전송하고, passwd 필드를 통해 사용자의 패스워드(LISASCH1)를 전송한다. Clientip 필드, macaddress 필드, gwmacaddress 필드를 통해 사용자 접속정보(220.69.200.145, 002354df697f, 00e0b1881440)를 전송하며, mac2 필드를 통해 지정된 PC의 고유정보(AA6DAC0DDFBD)를 전송한다. 따라서 공격자가 HttpSendRequest 함수를 후킹하여 탈취한 아이디와 패스워드를 토대로 지정된 PC의 고유정보를 변조하여 이용 PC 지정 서비스를 우회함으로써 사용자 인증의 우회가 가능하다. 해당 공격이 가능한 이유는 IP와 MAC 주소, 혹은 기타의 사용자 접속정보나 지정 PC의 고유정보가 서로 연관성이 없이 생성되었기 때문에 발생하는 문제점이라 할 수 있다. 이와 같은 이유로 공격자는 공격자 자신의 PC에 대한 고유정보를 사용자의 지정된 PC의 고유정보로 바꾸는 작업만으로도 이용 PC 지정 서비스를 우회하여 사용자 인증에 성공한다. 실험을 위해 아이디, 패스워드는 공격자가 이미 알고 있다고 가정하였으며, 공격자가 사용자 인증을 요청할 때의 접속정보를 그림 6에 나타내었다.

www.kci.go.kr

Fig. 6. Access information of attacker's PC when authentication

공격자가 HttpSendRequest 함수의 후킹을 통하여 탈취한 사용자의 아이디와 패스워드를 입력하면 공격자 PC의 고유정보(DE6281476564)를 생성하는 것을 확인할 수 있다. 하지만 공격자 PC의 고유정보는 지정된 PC의 고유정보(AA6DAC0DDFBD)와 다르기 때문에 이용 PC 지정 서비스 우회에 실패한다. 따라서 공격자 PC의 고유정보를 지정된 PC의 고유정보로 변경하여 이용 PC 지정 서비스의 우회를 시도하여 사용자 인증이 올바르게 이루어지는지 실험하였다. 그림 7에 수정된 쿼리를 나타내었으며, 탈취한 지정된 PC의 고유정보를 기반으로 공격자 PC에서 사용자 인증을 우회한 결과, 정상적으로 사용자 인증이 이루어지는 것을 확인하였다[16].

이와는 다르게 리버스 엔지니어링을 이용하여 인터넷 익스플로러와 같은 웹 브라우저에서 지정된 PC의 하드웨어 고유정보를 추출하는 과정을 분석함으로써 지정된 PC의 CPU 아이디, 하드디스크 시리얼 넘버를 탈취할 수 있으며, 분석결과를 통해 상기 하드웨어 고유정보들의 위/변조가 가능하다. 즉, 공격자가 배포한 악성코드가 지정된 PC의 CPU 아이디와 하드디스크 시리얼 넘버를 추출하여 공격자에게 전송하면, 공격자는 탈취한 CPU 아이디와 하드디스크 시리얼 넘버를 공격자 PC에서 하드웨어 고유정보를 생성할 때, 혹은 추출할 때의 출력인자로 변조하거나 생성이 완료된 고유정보를 추출한 후, 공격자에게 전송하여 분석한 처리과정을 통해 고유정보를 생성할 때 이를 변조하는 등의 공격을 통해 이용 PC 지정 서비스의 우회가 가능하다. 이 방법은 공격자의 능력에 따라 단기간에 이루어질 수도 있기 때문에 상기의 문제점보다 심각하다. CPU 아이디를 추출하는 과정을 그림 8, 하드디스크 시리얼 넘버를 추출하는 과정을 그림 9에 나타내었다.

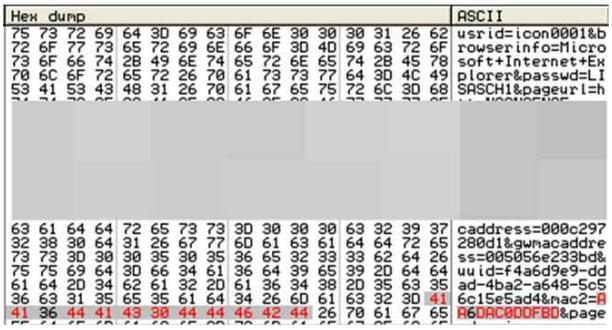

Fig. 7. Modification of hardware unique information for bypassing designated PC service on the attacker's PC

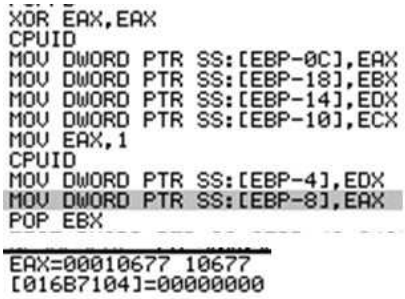

Fig. 8. Extracting process of CPU ID on the designated PC

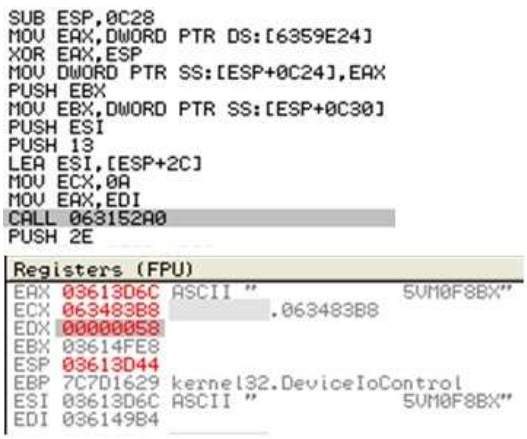

Fig. 9. Extracting process of harddisk serial number on the designated PC

상기 분석된 추출과정을 토대로 CPU 아이디와 하드디스크 시리얼 넘버를 추출할 시점에서 지정된 PC와 동일한 하드웨어 고유정보로 변조하는 방법을 이용하여 이용 PC 지정 서비스 우회를 시도하였으며, CPU 아이디와 하드디스크 시리얼 넘버를 수정하는 과정을 그림 10, 그림 11에 나타내었다[13]. 이와 같은 방법으로 인증을 우회한 결과, 올바르게 사용자 인증이 이루어지는 것을 확인하였다.

www.kci.go.kr

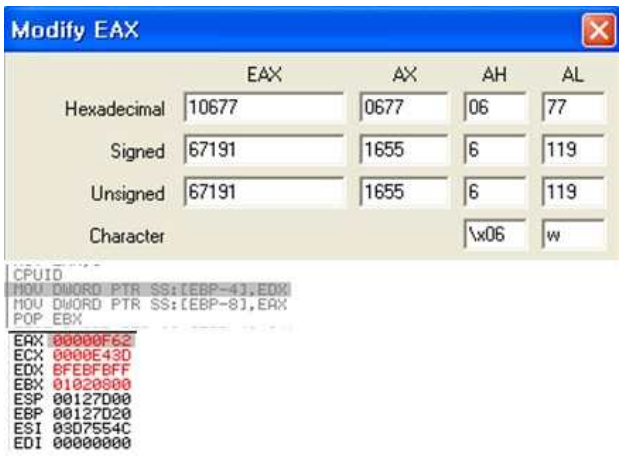

Fig. 10. Modifying process of CPU ID for bypassing designated PC service on the attacker's PC

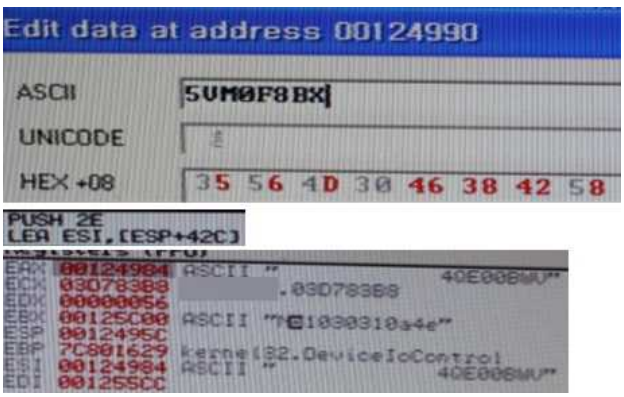

Fig. 11. Modifying process of harddisk serial number for bypassing designated PC service on the attacker's PC

상기와 같이 이용 PC 지정 서비스에서 핵심적인 요소인 하드웨어 고유정보를 추출하는 시점, 전송하는 시점에서 발생 가능한 취약점을 도출하고, 이에 대한 실험을 시도하였으며, 그 결과 위/변조된 하드웨어 고유정보로도 인증이 우회되는 것을 확인하였다.

III. Conclusions

본 논문은 기존의 온라인 본인확인수단의 문제점을 보완하고자 제안된 이용 PC 지정 서비스에 대해 살펴보았으며, 이용 PC 지정 서비스에서 발생 가능한 보안위협을 하드웨어 고유정보를 추출하는 시점, 전송하는 시점으로 분류하였고, 분류한 보안위협에 대한 세부사항을 도출함으로써 보안위협에 대한 시나리오를 도출하였다. 그 중 하드웨어 고유정보를 전송하는 함수를 후킹하여 위/변조하는 방법과 리버스 엔지니어링을 이용하여 하드웨어 고유정보를 위/변조하는 방법에 대해 실험을 통하여 인증 우회를 시도하였으며, 그 결과 인증 우회가 성공적으로 이루어지는 것을 확인하였다. 본 논문의 결과는 이용 PC 지정 서비스의 보안위협을 도출하고 이를 보완하기 위한 자료로 활용될 것이라 기대된다.

REFERENCE

[1] Su-Mi Lee, Jarmo Seung, "Domestic Electronic Financial Status and Classification of Security Threats", Review of Korea Institute of Information Security and Cryptology(KIISC), 21(7), pp. 53-61, Nov. 2011

[2] Kong Hoi Kim, Ji Min Ahn, Min Jae, Kim, and Yong Sik Joo, "Security threats and countermeasures of certificate password attack by performing SEED algorithm in GPU", Review of Korea Institute of Information Security and Cryptology(KIISC), 20(6), pp.43-50, Dec. 2010

[3] Yunyoung Lee, Soonhaeng Hur, Sangjoo Park, Donghwi Shin, Dongho Won, and Seungjoo Kim, "CipherSuite Setting Problem of SSL Protocol and It's Solutions", The KIPS Transactions: Part C, 15-C(5), pp.359-366, Oct. 2008

[4] Chasung Lim, Wookey Lee, and Tae-Chang Jo, "An Effective Protection Mechanism for SSL Man-in-the-Middle Proxy Attacks", Journal of the Korean Institute of Information Scientists and Engineers(KIISE), (16)6, pp.693-697, Jun, 2010

[5] Woo Hyun Ahn and Hyungsu Kim, "Attacking OpenSSL Shared Library Using Code Injection", Journal of the Korean Institute of Information Scientists and Engineers(KIISE), 37(4), pp.226-238, Aug. 2010

[6] Byung-Tak Kang and Huy Kang Kim, "A study on the vulnerability of OTP implementation by using MITM attack and reverse engineering", Journal of the Korea Institute of Information Security and Cryptology(KIISC), 21(6), pp.83-99, Dec. 2011

[7] Woochan Hong, Kwangwoo Lee, Seungjoo Kim, and Dongho Won, "Vulnerabilities Analysis of the OTP Implemented on a PC", The KIPS Transactions: Part C, 17-C(4), pp.361-370, Aug. 2010

[8] Telecommunications Technology Association(TTA), "Security Requirement for Virtual Keybord", TTAK.KO-12.0180, Dec. 2011

[9] Kyungroul Lee, Hyeungjun Yeuk, Youngtae Choi, Sitha Pho, and Kangbin Yim, "Security Vulnerability Analysis of Touchpad on Image-Based Login Method", Proceedings of the Winter Conference on Korean Society for Internet Information(KSII), pp.171-175, Dec. 2010

www.kci.go.kr

[10] Wan-soo Kim, Kyung-roul Lee, Pho Sitha, and Kangbin Yim, “Analysis on Ivasion of Privacy using Display Device Vulnerability”, Proceedings of the Winter Conference on Korean Society for Internet Information(KSII), 11(2), pp.81-82, Oct. 2010

[11] Neowiz games corporaion, “Internet connection blocking method through a fixed PC service using an IP address and hardware information”, G06F 21/20, Nov. 2011

[12] Kangwon Lee, Kyungroul Lee, Jaecheon Byun, Sunghoon Lee, Hyobeom Ahn, and Kangbin Yim, “Extraction of Platform-unique Information as an Identifie”, Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Application(JoWUA), 3(4), pp.85-99, Dec. 2012

[13] Kyungroul Lee, Hyeungjun Yeuk, Habin Yim, and Kangbin Yim, “Security Assessment of the Designated PC Solution”, Proceedings of the Spring Conference on Korean Institute of Smart Media(KISM), Apr. 2015

[14] Jonghoi Kim, Jinyoung Lee, and Seong-Je Cho, “A New Malware Propagation Technique based on the Send Function Hooking and Its Countermeasure”, Journal of Korean Institute of Information Scientists and Engineers(KIISE): System and theory, 38(4), pp. 178-185, Aug. 2011

[15] Kangwon Lee, Kyungroul Lee, Jaecheon Byun, Sunghoon Lee, Hyobeom Ahn, and Kangbin Yim, “Extraction of Platform-unique Information as an Identifie”, Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Application(JoWUA), 3(4), pp.85-99, Dec. 2012

[16] Hyeungjun Yeuk, Kyungroul Lee, Habin Yim, and Kangbin Yim, “An Analysis of the Vulnerability of the Designated PC solution”, Proceedings of the Spring Conference on Korean Institute of Smart Media(KISM), Apr. 2015

Authors

Kyungroul Lee received the B.S., M.S. and Ph.D. degrees in Dept. of Information Security Engineering from Soonchunhyang University, Asan, Korea, in 2008, 2010 and 2015, respectively.
Dr. Lee is currently a post-doc. researcher in Soonchunhyang University. He is interested in vulnerability analysis, system security, hardware security, platform security, user authentication, and device authentication. Related to these topics, he has worked on more than twenty research projects and published more than sixty research papers.

Kangbin Yim received his B.S., M.S., and Ph.D. degrees in Dept. of Electronics Engineering from Ajou University, Suwon, Korea in 1992, 1994 and 2001, respectively. Dr. Yim is currently a full professor in the Department of Information Security Engineering, Soonchunhyang University. He has served as an executive board member of Korea Institute of Information Security and Cryptology, Korean Society for Internet Information and The Institute of Electronics Engineers of Korea. He also has served as a committee chair of the international conferences and workshops and the guest editor of the journals such as JIT, MIS, JCPS, JISIS and JoWUA. His research interests include vulnerability assessment, code obfuscation, malware analysis, leakage prevention, secure platform architecture and mobile security. Related to these topics, he has worked on more than sixtyty research projects and published more than a hundred research papers.

www.kci.go.kr