Journal of The Korea Society of Computer and Information
Vol. 22 No. 5, pp. 29-39, May 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.05.029

An Analysis of Security Threats and Security Requirements on the Designated PC Solution

Kyungroul Lee*, Sun-Young Lee**, Kangbin Yim***

Abstract

In this paper, we analyse security threats and security requirements about the designated PC solution which restricts usable PCs that are only an user own PCs or a registered PC for online banking or very important services. Accordingly, causable threats of the designated PC solution are classified a process, a network layer, a software module, and an environment of platform, and we draw security requirements based on analysed security threats. Results of this research are considered utilization of criteria for improving security of the designated PC solution and standards for giving hint of imposition of the designated PC solution.

▸Keyword Designated PC solution, Security threat, Security requirement, Identification, Device authentication, User authentication

I. Introduction

온라인 뱅킹 및 전자상거래 규모가 급증하면서 인터넷을 통한 재화와 용역의 교환은 국가경제의 큰 부분이 되었다. 하지만 이와 같은 체제를 구축하는 과정에서 다양한 보안기술을 적용하였음에도 불구하고 2005년 5월 인터넷뱅킹 해킹사건이 발생하였으며, 이와 유사한 피해가 지속적으로 발생하였다[1].

일반적인 보안응용과 마찬가지로 온라인 금융거래에서도 보안기술은 기밀성, 무결성, 가용성, 진정성, 부인방지 등의 보안 요구사항의 확보가 필요하다. 이를 위하여 다양한 암호화 기반기술이 발전하였으며, 검증된 수학적 도구를 활용함으로써 그 효용성이 충분히 입증되었다. 그럼에도 불구하고 대부분 보안문제는 암호화 기반기술에서보다 보안응용을 위하여 이를 활용하는 과정이나 환경에서 발생하고 있다[2]. 따라서 이에 대한 취약점을 찾고 대응하기 위한 연구가 필요하다[22, 23, 24]. 이러한 보안 요구사항이 의미를 가지기 위해서는 보안의 주체에 대한 증명이 필수적이다. 주체에 대한 증명의 한 기술로 이용 PC 지정 기술이 연구되었다[3]. 이용 PC 지정 솔루션이란 사용자에 대한 인증뿐만 아니라 사용자의 PC만이 특정 서비스(게임, 파일보안, 금융거래 등)를 이용하는 인가방법이다. 사용자가 특정 서비스를 이용할 경우, 본인확인절차를 거친 후, 사용자 PC의 고유정보를 사전에 등록하고 이후 서비스 이용 시, 고유정보를 가진 PC만 서비스를 제공한다. 만약 사용자 PC가 아닌 다른 PC가 서비스를 요청하였다면, 이들 요청은 차단한다. 현재 국내의 은행 등을 비롯한 금융 사이트, 게임 사이트, 파일보안솔루션 등에서 이용 PC 지정 솔루션을 제공하고 있다.

이용 PC 지정 솔루션의 동작과정은 다음과 같다. 등록 단계에서는 이미 등록된 사용자가 아이디/비밀번호, 공인인증서, 핸드폰 인증 등의 본인확인을 통하여 사용자 인증을 수행하고 인증된 사용자 본인이 사용할 PC의 고유값을 생성하여 서비스 제공자에게 전달한다. 서비스 제공자는 수신한 정보를 데이터베이스에 저장하여 서비스 제공 시 검증하기 위한 정보로 활용한다. 인증 단계에서는 본인확인을 거친 사용자가 자신의 PC를 검증하기 위하여 고유의 값을 생성한 후, 서비스 제공자에게 전달하면, 서비스 제공자는 데이터베이스에서 수신한 정보를 확인함으로써 등록된 PC임을 인증한다. 따라서 이용 PC 지정 서비스는 등록된 PC가 아니면 서비스를 제공받지 못하기 때문에 사용자 인증에 대한 안전성을 보장한다[1].

• First Author: Kyungroul Lee, Corresponding Author: Kangbin Yim
*Kyungroul Lee (carpedm@sch.ac.kr), R&BD Center for Security and Safety Industries (SSI), Soonchunhyang University
**Sun-Young Lee (sunlee@sch.ac.kr), Dept. of Information Security Engineering, Soonchunhyang University
***Kangbin Yim (yim@sch.ac.kr), Dept. of Information Security Engineering, Soonchunhyang University
• Received: 2015. 08. 10, Revised: 2015. 10. 14, Accepted: 2017. 04. 25.
• This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) that is funded by the Ministry of Education (NRF-2015R1D1A1A01057300) and the Soonchunhyang University Research Fund

하지만 이와 같은 노력에도 불구하고 아직까지 이용 PC 지정의 보안위협 및 보안 요구사항에 대한 분석은 미흡한 실정이다. 따라서 본 논문에서는 이용 PC 지정에서 발생 가능한 보안위협을 프로세스에서의 보안위협, 네트워크 계층에서의 보안위협, 소프트웨어 모듈에서의 보안위협, 단말 영역 환경에서의 보안위협으로 분류하여[2], 이에 대한 취약점 및 보안위협을 분석하였으며, 분석한 보안위협을 토대로 보안 요구사항을 도출하였다.

II. Security Threats on the Designated PC Solution

본 논문에서는 이용 PC 지정에서 발생 가능한 보안위협을 프로세스에서의 보안위협, 네트워크 계층에서의 보안위협, 사용자 PC에 설치되어 실행되는 소프트웨어 모듈에서의 보안위협, 사용자 단말 영역 환경에서의 보안위협으로 분류하였으며, 이를 표 1에 나타내었다. 본 논문에서는 보안위협을 도출하기에 앞서 공인인증서, 보안카드 등 기존의 온라인 본인확인수단들이 취약점에 의한 보안위협이 발생함으로써 이용 PC 지정이 제안되었기 때문에 기존의 온라인 본인확인수단들이 가지는 취약점은 이미 존재한다고 가정하였다.

Table 1. Classification of security threats on the designated PC solution

Classification		Security Threats
Areas	Process	· Registration Process - Methods of Application and Registration - Output of Registration Result - Maximum Number of Registerable PCs · Authentication Process - Extraction Point of Hardware-unique Information · Addition Process - Method of Addition - Authentication Method when Addition · Termination Process - Method of Termination - Terminable End Terminal - Termination of Service
	Network Area	· Packet Sniffing · Session Hijacking · MITM(Man-In-The-Middle) Attack · Replay Attack · Phishing/Pharming Attack · Authentication Information Guessing Attack
	Software Module	· Web Browser MITM Attack · Reverse Engineering · Interface MITM Attack
	End Terminal Environment	· Memory Hacking · Direct Access of Hardware · Using Virtual Machine

2.1. Security Threats in the Process

프로세스에서 발생 가능한 보안위협은 등록 시 발생 가능한 보안위협, 인증 시 발생 가능한 보안위협, 추가 시 발생 가능한 보안위협, 해지 시 발생 가능한 보안위협으로 분류된다.

2.1.1. Registration Process

이용 PC 등록 시 발생 가능한 보안위협은 신청 및 등록방식, 등록결과 출력, 최대 등록 PC 개수로 분류된다.

● 신청 및 등록방식

이용 PC 지정은 기존의 온라인 본인확인수단들의 문제점을 보완하기 위하고자 제안된 인증방식이기 때문에 신청 및 등록 시 기존의 온라인 본인확인수단을 이용한다면 기존의 보안위협을 그대로 가질 뿐 아니라 안전성이 강화되기보다는 절차만 더욱 복잡하게 만드는 것이다. 또한, 신청과 등록 절차가 통합되어 있다면 한 번의 공격만으로 등록이 완료되므로 악의적인 행위가 가능하다는 문제점이 존재한다.

● 등록결과 출력

온라인 뱅킹에서의 메모리 해킹과 관련된 문제점으로 신청 및 등록 시 그 결과가 출력되지 않는다면 사용자의 지정 PC가 올바르게 등록되었는지, 변조되어 등록되었는지 확인할 수 없으므로 무결성을 증명할 수 없다. 만약 공격자가 지정 PC의 고유정보를 변조하여 등록하였다면 사용자의 지정 PC는 서비스를 이용할 수 없는 상태가 되며, 이를 통하여 공격자는 악의적인 행위를 수행하는 것이 가능하다.

● 최대 등록 PC 개수

이용 PC 지정은 서비스를 이용하는 단말을 제한하려는 것이 그 목적이다. 대부분의 사용자는 서비스를 이용하는 단말이 특정 단말, 즉, 집이나 직장, 휴대전화 등으로 제한되어 있기 때문에 이용 PC 지정 서비스의 활용이 가능하다. 하지만 지정하는 PC가 제한되지 않고 사용할 때마다 등록하여 서비스를 이용하는 것이 가능하다면, 그 목적을 상실할 뿐만 아니라 공격이 가능한 PC도 증가하게 되므로 그만큼 위협에 노출되는 문제점이 존재한다.

2.1.2. Authentication Process

이용 PC 인증 시 발생 가능한 보안위협은 하드웨어 고유정보 추출 시점이 존재한다.

● 하드웨어 고유정보 추출시점

하드웨어 고유정보를 추출하는 시점은 웹 페이지 접속 시점과 인증을 요청하는 시점이 있다. 만약 웹 페이지 접속 시점에서 하드웨어 고유정보를 추출하는 경우, 사용자가 인증이 되지 않은 상태에서 하드웨어 고유정보가 노출되므로 공격자가 사용자의 PC에서 웹 페이지에 접속하는 것만으로도 하드웨어 고유정보의 탈취가 가능하다.

2.1.3. Addition Process

이용 PC 추가 시 발생 가능한 보안위협은 추가방식, 추가 시 인증방식으로 분류된다.

● 추가방식

사용자가 지정한 PC 이외의 새로운 PC를 추가할 경우, 혹은 사용자가 지정한 PC의 네트워크 카드나 하드디스크, CPU 등의 내부 하드웨어를 교체하는 경우 추가 단계를 통하여 새로운 PC를 등록하여야 하는데, 이 과정 역시 등록 단계에서의 보안위협을 그대로 가진다.

● 추가 시 인증방식

사용자의 PC와 전화번호가 모두 바뀌었을 경우를 대비하여 전화번호를 변경하는 기능이 제공되기도 한다. 전화번호 변경은 최초 신청 시, 즉, 영업점을 방문하여 등록한 전화번호의 뒤네 자리와 새로운 전화번호를 입력함으로써 변경이 가능하다. 이와 같은 경우 공격자가 사용자의 전화번호를 알고 있다면, 새로운 PC(공격자 PC)를 추가할 수 있어 상기와 동일한 문제점이 존재한다. 전화번호를 변경하는 과정에 대한 일례를 그림 1, 그림 2에 나타내었다.

Fig. 1. Example of request web page for changing cell phone number

Fig. 2. Example of web page for changing cell phone number

상기와 같이 변경할 전화번호를 입력하고 인증번호 전송 버튼을 클릭하면 변경된 전화번호로 인증번호가 발송되며, 공격자는 이를 입력함으로써 인증을 완료한다. 이 과정은 등록된 전화번호와 변경될 전화번호가 어떠한 연관성을 가지는지 검증하지 않기 때문에 취약점이 발생한다.

2.1.4. Termination Process

이용 PC 해지 시 발생 가능한 보안위협은 해지방식, 해지 가능한 단말, 서비스 해지로 분류된다.

● 해지방식

등록된 PC를 해지할 경우에도 마찬가지로 기존의 온라인 본인확인수단만을 이용한다면 사용자가 인지하지 못한 상태에서 공격자가 PC를 등록하고 해지하는 것이 가능하므로 등록 단계에서의 보안위협을 동일하게 가진다. 또한 공격자가 등록된 사용자의 PC를 해지하는 것이 가능하므로 정상적으로 서비스를 받아야 하는 사용자임에도 불구하고 서비스를 받지 못하는 문제점이 발생한다.

● 해지 가능한 단말

사용자가 이용 PC를 해지할 경우, 접속한 PC가 아닌 등록된 다른 PC에서 해지가 가능하다면 상기와 동일한 문제점이 발생한다.

● 서비스 해지

이용 PC 지정은 지정된 PC에서만 서비스가 가능하기 때문에 이용 PC 지정 서비스를 해지할 경우 이용 PC 지정 서비스를 통하여 이용되던 서비스들이 기존의 온라인 본인확인수단으로 이용이 가능하다. 즉, 기존의 본인확인수단만으로 해지가 가능하다면 공격자는 사용자의 이용 PC 지정 서비스를 해지할 수 있으며, 해지가 되면 계좌이체 등 지정된 PC에서만 이용이 가능하였던 서비스를 이용할 수 있다는 문제점이 존재한다.

2.2. Security Threats in the Network Area

네트워크 계층에서의 보안위협은 사용자 단말과 인증 서버 간 네트워크를 통하여 정보를 전송하는 과정에서 발생 가능한 보안위협을 의미하며, 패킷 스니핑, 세션 하이재킹, 중간자 공격, 재전송 공격, 피싱/파밍 공격, 인증정보 추측 공격으로 구분된다.

● 패킷 스니핑[8]

패킷 스니핑은 네트워크상에서 전송되는 패킷을 스니핑하여 인증과 관련된 정보를 탈취한 후, 이를 악용하는 공격이다. 만약 사용자가 지정한 PC의 고유정보를 변형하지 않고 그대로 전송한다면 공격자는 이를 탈취하여 공격자 PC의 고유정보를 추출하거나 전송할 때 고유정보를 변조함으로써 인증을 우회하는 공격이 가능하다.

● 세션 하이재킹

사용자 단말과 인증 서버는 사용자 단말을 구분하기 위하여 각 세션별 아이디를 발급한다. 이와 같은 경우, 공격자가 세션 아이디를 탈취하여 자신의 세션 아이디를 탈취한 세션 아이디로 변조한다면 인증 서버는 해당 세션 아이디가 이미 인증을 완료한 사용자로 인식하기 때문에 인증을 우회하는 공격이 가능하다.

● 중간자 공격[9]

중간자 공격은 사용자 단말과 인증 서버 간 전송되는 정보를 위/변조하여 공격자가 정상적인 사용자로 위장하는 공격이다.

공격자는 사용자 단말과 인증 서버 간 전송되는 인증 및 연결과 관련된 정보 등을 위/변조하여 인증 서버가 공격자 단말을 사용자 단말로 인식하도록 하거나 사용자 단말이 공격자 단말을 인증 서버로 인식하도록 위장하는 공격이다.

● 재전송 공격[10]

재전송 공격은 사용자 단말에서 인증 서버로 전송하는 인증과 관련된 정보를 탈취하여 공격자 단말에서 인증 서버로 전송하는 정보를 탈취한 정보로 위/변조하여 전송함으로써 인증을 우회하는 공격이다.

● 피싱/파밍 공격[11][12]

피싱/파밍 공격은 공격자가 사용자가 접속하려는 인증 서버의 웹 페이지 등을 동일하게 만들거나 비슷하게 만들어서 실제로 사용자가 접속하는 인증 서버는 공격자의 인증 서버이지만 사용자가 인지하기에는 정상적인 인증 서버로 접속하는 것으로 속여 인증과 관련된 정보를 탈취하는 공격이다.

● 인증정보 추측 공격

인증 서버로 전송되는 인증과 관련된 정보가 단순하게 구성되었을 경우, 공격자는 탈취한 정보를 토대로 인증과 관련된 정보를 추측하여 인증을 시도함으로써 인증을 우회하는 공격이다.

2.3. Security Threats in the Software Module

소프트웨어 모듈에서의 보안위협은 지정된 PC를 인증하기 위하여 인증 서버로부터 사용자 단말에 설치되는 소프트웨어 모듈에서 발생 가능한 보안위협을 의미하며, 웹 브라우저 중간자 공격, 리버싱, 인터페이스 중간자 공격으로 구분된다.

● 웹 브라우저 중간자 공격[13]

웹 브라우저 중간자 공격은 사용자 단말의 웹 브라우저로 전송되는 웹 페이지를 위/변조하여 인증정보를 탈취하는 공격이다.

● 리버싱[14, 16, 3]

리버싱은 ollydbg, windbg 등의 특정 도구를 이용하여 소프트웨어 모듈 내의 인증정보를 추출하거나 위/변조하는 공격이며, 지정 PC의 고유정보를 추출한 후, 공격자 단말에서 실행되는 소프트웨어 모듈이 고유정보를 추출할 때 이를 위/변조하여 인증을 우회하는 등의 공격이다.

● 인터페이스 중간자 공격[15]

인터페이스 중간자 공격은 소프트웨어 모듈이 실행될 때 그와 연관된 인터페이스들에 대한 중간자 공격을 시도하는 것이며, 대표적인 공격방법으로 후킹이 있다. 소프트웨어 모듈 혹은 관련된 라이브러리 등에 대하여 후킹을 시도한 후, 사용자 PC의 고유정보와 같은 인증과 관련된 정보를 위/변조하는 공격이다.

2.4. Security Threats in the End Terminal Environment

단말영역 환경에서의 보안위협은 지정 PC의 환경에서 고유정보가 탈취되거나 위/변조를 통하여 인증을 우회하는 보안위협을 의미하며, 메모리 해킹, 하드웨어 직접 제어로 구분된다.

● 메모리 해킹

소프트웨어 모듈은 지정된 PC의 고유정보를 추출하여 이를 메모리상에 저장한 후, 필요하다면 연산을 통하여 고유정보를 생성한다. 이 과정에서 지정 PC의 하드웨어 고유정보 및 생성된 고유정보가 반드시 메모리상에 저장되는데, 현재 플랫폼은 메모리상에 저장된 정보에 접근하여 이를 탈취하거나 위/변조가 가능하도록 구성되어 있다. 따라서 메모리 해킹을 통한 고유정보 탈취 및 위/변조 공격이 가능하다.

● 하드웨어 직접 제어[3][4]

지정된 PC의 고유정보는 소프트웨어 모듈이 특정 하드웨어를 직접 제어하여 고유정보를 추출하기도 한다. 하지만, 이 방법은 방어자만이 사용할 수 있는 것이 아니라, 공격자 역시 사용할 수 있기 때문에 방어자와 공격자가 경쟁상태가 되므로 고유정보를 추출할 때의 접근제어는 불가능하다. 또한, 하드웨어를 직접 제어하여 고유정보를 위/변조하는 공격이 가능한데, 방어자 입장에서는 위/변조 사실을 확인할 수 없어 그 심각성은 더욱 크다. 이와는 다르게 하드웨어로 접근할 때의 주소에 트랩을 설정하여 고유정보를 탈취하거나 위/변조하는 공격도 존재한다.

이 중 MAC 주소에 대하여 살펴보면, MAC 주소를 추출하는 방법은 크게 레지스트리를 이용한 방법, API를 이용한 방법, I/O controller를 이용한 방법, NIC 내의 EEPROM을 이용한 방법이 있다. 레지스트리를 이용한 방법은 “내 컴퓨터₩HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Class₩{4D36E972-E325-11CEBFC1-08002bE10318₩0001“의 NetworkAddress 필드에 존재하는 MAC 주소를 레지스트리 관련 함수를 이용하여 추출하는 방법이며, 추출 결과의 일례를 그림 3에 나타내었다. 레지스트리를 이용한 방법은 레지스트리를 쓰는 작업만으로도 변경 가능성이 있다.

API를 이용한 방법은 마이크로소프트 윈도우즈에서 제공하는 API 함수인 UuidCreate, NetWkstaTransportEnum, GetAdaptersInfo, GetIfTable, Netbios 함수 등을 이용하여 추출 가능하며, 추출 결과의 일례를 그림 4에 나타내었다. 하지만 이 방법들 역시 해당 함수들의 후킹 등을 통하여 변경할 수 있는 가능성이 있다.

I/O controller를 이용한 방법은 PC에 I/O장치를 위한 controller가 별도로 준비되어 있으므로 이를 통하여 I/O장치들의 정보를 추출할 수 있다. I/O장치들은 일반적으로 PCI에 연결되어 있으므로 PCI에 연결된 NIC의 base address를 추출하여 MAC주소와 관련된 특정 레지스터를 읽음으로써 추출하며, 그 일례를 그림 5에 나타내었다. 이 방법은 하드웨어에 직접 접근하기 때문

에 매우 안전해 보이지만 NIC내의 MAC주소와 관련된 레지스터에 접근하여야 하기 때문에 특정 메모리에 접근하여야만 한다. 인텔의 경우 디버깅을 위한 목적으로 특정 메모리에 접근할 때 예외를 처리할 수 있도록 별도의 핸들러를 준비하고 있어 공격자와 방어자가 경쟁상태에 이르게 될 가능성이 존재한다.

Fig. 3. Example of extracting MAC address using registry

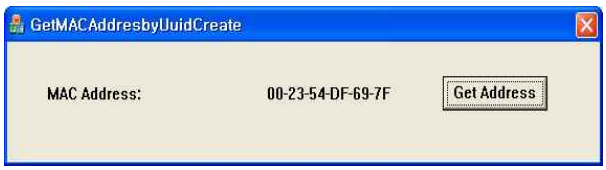

Fig. 4. Example of extracting MAC address UUIDCreate function

NIC 내의 EEPROM을 이용한 방법은 NIC내의 EEPROM과 관련 레지스터를 제어함으로써 MAC주소를 추출하며, 그 일례를 그림 6에 나타내었다. 상기와 마찬가지로 특정 메모리에 접근하여야 하는 문제점은 있지만, NIC의 MAC주소와 관련된 레지스터에 접근하는 것이 아니라 EEPROM내의 MAC주소와 관련된 메모리를 접근하는 것이기 때문에 보다 안전하다. 더구나 NIC의 MAC주소와 관련된 레지스터는 부팅 시 EEPROM내의 MAC주소와 관련된 메모리에서 복사되는 것이기 때문에 가장 낮은 레벨의 MAC 주소 추출방안이라 할 수 있다.

● 가상머신 이용

사용자가 가상머신을 이용할 경우에는 특정 하드웨어 고유정보들은 동일한 값을 가지게 되므로 가상머신을 탈취한다면 고유정보가 노출되는 문제점이 발생한다. 또한, 가상머신의 경우 소프트웨어로 구성되어 있기 때문에 호스트에서 가상머신의 구성정보의 변경이 가능하다. 따라서 가상머신의 구성정보를 변경함으로써 하드웨어 고유정보의 변경이 가능하므로 인증 우회가 가능하다.

III. Security Requirements on the Designated PC Solution

본 장에서는 제2장에서 분석된 보안위협을 토대로 이용 PC 지정에서의 보안 요구사항을 도출하였다. 도출된 보안 요구사항 역시 보안위협과 마찬가지로 프로세스에서의 보안 요구사항, 네트워크 계층에서의 보안 요구사항, 사용자 PC에 설치되어 실행되는 소프트웨어 모듈에서의 보안 요구사항, 사용자 단말 영역 환경에서의 보안 요구사항으로 분류하였다[20, 21].

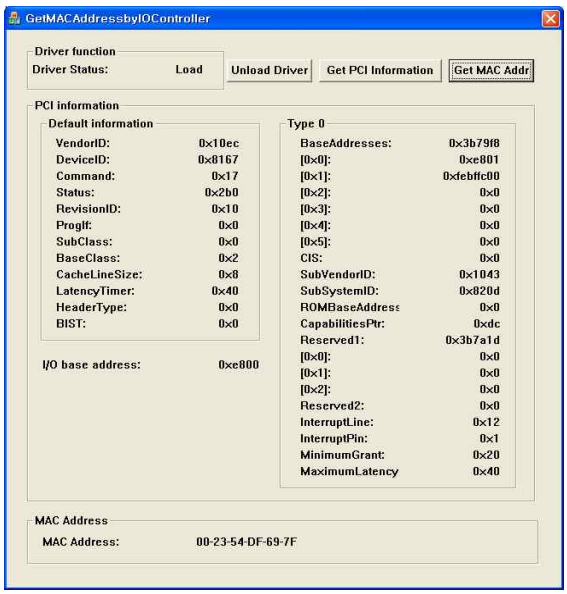

Fig 5. Example of extracting MAC address using I/O controller

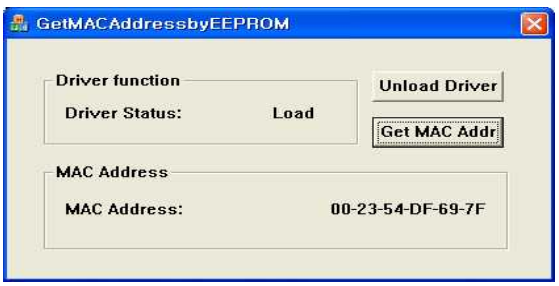

Fig. 6. Example of extracting MAC address using EEPROM

3.1. Security Requirements in the Process

프로세스에서의 보안 요구사항은 등록 시 보안 요구사항, 인증 시 보안 요구사항, 추가 시 보안 요구사항, 해지 시 보안요구사항으로 구분된다.

3.1.1. Registration Process

이용 PC 등록 시 보안 요구사항은 신청 및 등록방식, 등록결과 출력, 최대 등록 PC 개수, 히스토리 제공, 알림 서비스로 분류된다.

● 신청 및 등록방식

신청 및 등록방식은 기존의 온라인 본인확인수단을 이용한다면 기존의 보안위협을 그대로 가지기 때문에 결과적으로 절차만 더 복잡하게 만드는 것으로 반드시 오프라인이나 다른 2채널 인증방식을 통하여 이루어져야 한다. 또한, 신청과 등록 절차를 분리하여 한 번의 공격만으로 등록이 완료되지 않도록 한다.

● 등록결과 출력

사용자의 PC를 등록하면 그 결과를 사용자가 인지하도록 고

유정보 등과 함께 등록결과를 출력하여야 한다. 이는 온라인 뱅킹에서의 메모리 해킹과 관련된 것으로, 메모리 해킹을 이용하여 실제 사용자 PC가 아닌 공격자의 PC가 등록되는 것을 탐지하기 위함이다.

● 최대 등록 PC 개수

지정되는 PC가 무한대가 된다면 공격 대상이 증가되어 그만큼 공격 확률이 증가하게 되므로 등록 가능한 최대 PC의 개수를 제한하여야 하며, 일반적으로 3대 정도를 권장한다.

● 히스토리 제공

이용 PC 지정 서비스를 신청하거나 등록된 PC의 내역을 확인할 수 있도록 히스토리를 제공하여야 한다. 이는 사용자가 직접 자신의 신청 및 등록 내역을 확인할 수 있어 자신이 신청 및 등록하지 않은 PC를 확인하는데 활용되거나 차후 조사를 위하여 활용될 수 있다.

● 알림 서비스

이용 PC 지정 서비스를 신청하거나 등록이 완료되면 사용자가 자신의 요청이 올바르게 수행되었는지 인지하도록 메일 혹은 문자 등을 통하여 알려주어야 한다. 이는 공격자가 사용자 모르게 공격자의 PC를 등록하였을 경우, 사용자에게 이를 알려줌으로써 공격에 대비하는 역할을 한다.

3.1.2. Authentication Process

이용 PC 인증 시 보안 요구사항은 하드웨어 고유정보 추출 시점, 히스토리 제공 및 알림 서비스로 분류된다.

● 하드웨어 고유정보 추출 시점

하드웨어 고유정보를 웹 페이지 접속 시점에서 추출하게 된다면 사용자의 PC에서 인증되지 않은 상태의 웹 페이지에 접속하는 것만으로 고유정보가 노출된다. 이는 공격자가 원격 혹은 오프라인으로 PC들의 고유정보를 탈취할 수 있기 때문에 하드웨어 고유정보를 추출하는 시점은 반드시 인증을 요청하는 시점에서 이루어져야 하며, 인증 요청이 완료된 후에는 소프트웨어 모듈의 메모리에 저장된 하드웨어 고유정보를 반드시 삭제하여야 한다.

● 히스토리 제공 및 알림 서비스

신청 및 등록 시의 보안 요구사항과 마찬가지로 인증이 완료되어 계좌이체와 같은 특정 서비스를 이용한 후에는 서비스를 이용한 PC의 상세 내역과 서비스 내역에 대한 히스토리를 제공하여야 하며, 계좌이체와 같은 특정 서비스의 요청이 처리된 후에는 휴대전화 등과 같은 별도의 채널을 통하여 그 결과를 사용자에게 통지하여야 한다.

3.1.3. Addition Process

이용 PC 추가 시 보안 요구사항은 추가방식, 추가 시 인증방식, 히스토리 제공 및 알림 서비스로 분류된다.

● 추가방식

추가방식 역시 인증방식과 마찬가지로 반드시 2채널 인증방식을 통하여 이루어져야 한다.

● 추가 시 인증방식

이용 PC 추가 시 전화 승인을 통하여 인증할 경우, 사용자가 PC의 특정 하드웨어를 새로 구입하거나 새로운 PC를 구입하였다면 기존에 등록된 전화번호를 통하여 인증이 가능하다. 하지만 만약 사용자의 PC와 전화번호가 모두 변경된 경우에는 이와 같은 2채널 인증이 불가능하다. 따라서 이러한 경우, 전화번호 변경이 가능하도록 변경 서비스를 제공할 수 있지만, 기존 번호의 소유자에 대하여 검증할 수 없으므로 반드시 오프라인으로 전화번호를 변경한 후, PC를 등록하여야 한다.

● 히스토리 제공 및 알림 서비스

이전 보안 요구사항과 마찬가지로 사용자 PC의 추가가 완료되면 추가 내역에 대한 히스토리를 제공하여야 하며, 추가가 완료된 후에는 별도의 채널을 통하여 그 결과를 사용자에게 통지하여야 한다.

3.1.4. Termination Process

이용 PC 해지 시 보안 요구사항은 해지방식, 해지 가능한 단말, 서비스 해지, 히스토리 제공 및 알림 서비스로 분류된다.

● 해지방식

해지방식 역시 신청 및 등록방식과 마찬가지로 반드시 2채널 인증방식을 통하여 이루어져야 한다.

● 해지 가능한 단말

서비스 해지가 가능한 단말은 서비스가 신청된 단말이면 모두 가능하게 설정하는 것이 아니라 접속한 단말에 한해서만 해지가 가능하도록 하여야 한다. 그렇지 않을 경우, 공격자가 임의로 등록하여 등록된 모든 PC의 해지가 가능하며, 모든 PC가 해지된 후에는 정상적인 사용자도 서비스 받지 못하므로 반드시 접속한 PC만 해지되도록 하여야 한다.

● 서비스 해지

이용 PC 지정 서비스는 해지할 경우, 지정된 PC에서만 이용이 가능하였던 계좌이체와 같은 특정 서비스가 기존의 온라인 본인확인수단만으로도 이용이 가능하다. 따라서 사용자가 이용 PC 지정 서비스를 해지할 경우, 만약 하나의 PC만이 등록되어 있다면 오프라인을 통하여 해지하도록 하여야 한다.

● 히스토리 제공 및 알림 서비스

이전 보안 요구사항과 마찬가지로 사용자 PC의 해지가 완료되면 해지 내역에 대한 히스토리를 제공하여야 하며, 해지가 완료된 후에는 별도의 채널을 통하여 그 결과를 사용자에게 통지

하여야 한다.

3.2. Security Requirements in the Network Area

네트워크 계층에서의 보안 요구사항은 사용자 단말과 인증 서버 간 네트워크를 통하여 정보를 전송하는 과정에서의 보안 요구사항을 의미하며, 패킷 스니핑 방지, 세션 하이재킹 방지, 중간자 공격 방지, 재전송 공격 방지, 피싱/파밍 공격 방지, 인증정보 추측 공격 방지로 구분된다.

● 패킷 스니핑 방지

네트워크를 통하여 전송되는 모든 정보는 반드시 검증된 암호기법을 이용하여 전송함으로써 제3자에 의한 스니핑 공격 및 위/변조가 불가능하도록 하여 보안위협을 방지하도록 한다.

● 세션 하이재킹 방지

세션 하이재킹은 사용자와 인증 서버 간 연결된 세션을 제3자가 개입하여 정당한 사용자로 위장하는 행위를 말하며, 이를 방지하기 위하여 반드시 보안채널을 구성하여 제3자의 개입이 불가능하도록 하여야 한다.

● 중간자 공격 방지

사용자와 인증 서버 간 정보를 송/수신하기 이전에 보안채널을 구성함으로써 중간자 공격을 방지하여야 한다.

● 재전송 공격 방지

재전송 공격을 방지하기 위하여 사용자와 인증 서버는 송/수신하는 정보에 일회성 정보(난수 등)를 포함하여 제3자가 개입할 수 없도록 하여야 하며, 송/수신 시퀀스(타임스탬프 등을 활용)를 유지하여 제3자의 개입을 탐지할 수 있도록 구성하여야 한다.

● 피싱/파밍 공격 방지

피싱/파밍 공격을 방지하기 위하여 사용자와 인증 서버 간 송/수신되는 정보에 대하여 IP 블랙리스트나 URL 기반 필터, 베이지안 필터 등을 이용하여 정당하지 않은 서버에 대한 접근 제어를 수행하도록 하여야 하며, EV SSL과 같이 사용자가 시각적으로 확인할 수 있는 단서를 제공함으로써 접속하는 서버가 올바른 서버임을 사전에 탐지하거나 사용자가 인지할 수 있도록 하여야 한다.

● 인증정보 추측 공격 방지

사용자의 인증정보가 제3자에 의하여 쉽게 추측되지 않도록 일정길이 이상으로 구성하여야 하며, 네트워크상에서 전송되는 정보 또한 제3자에 의하여 쉽게 추측되거나 복원되지 않도록 일정길이 이상으로 구성하여야 한다.

3.3. Security Requirements in the Software Module

소프트웨어 모듈에서의 보안 요구사항은 지정된 PC를 인증하기 위하여 인증 서버로부터 사용자 단말에 설치되는 소프트웨어 모듈의 보안 요구사항을 의미하며, 웹 브라우저 중간자 공격 방지, 리버싱 방지, 인터페이스 중간자 공격 방지로 구분된다.

● 웹 브라우저 중간자 공격 방지

웹 브라우저 중간자 공격은 공격자가 사용자의 웹 브라우저에 악성코드를 삽입하거나 자바 스크립트 등을 이용하여 가짜 웹 페이지를 만들어 인증정보를 탈취하므로 웹 브라우저의 악성코드 감염여부를 확인하여야 하며, 사용자가 접속하는 웹 페이지가 실제 페이지인지 확인하기 위한 방안을 제공하여야 한다.

● 리버싱 방지

현재 플랫폼에서는 리버싱을 방지하기 위한 완벽한 해결책이 존재하지는 않지만, 코드 해독을 어렵게 함으로써 해독 시간을 지연시키는 난독화 기술 등이 연구되고 있다. 따라서 공격자가 리버싱을 시도하더라도 시간이 매우 오래 걸리도록 난독화 기술을 소프트웨어 모듈에 적용하여야 한다.

● 인터페이스 중간자 공격 방지

대표적인 인터페이스 중간자 공격으로는 후킹이 있다. 따라서 소프트웨어 모듈 내에서 핵심적으로 사용되는 함수들, 예를 들면 인증 서버로의 전송과 관련된 함수, 하드웨어 고유정보 추출과 관련된 함수 등에 대한 함수의 후킹을 탐지하는 방안이 마련되어야 하며, 후킹이 탐지되면 이를 복구하기 위한 대응방안 역시 마련되어 인증과 관련된 정보의 노출을 방지하여야 한다.

3.4. Security Requirements in the End Terminal Environment

단말영역 환경에서의 보안 요구사항은 지정 PC의 환경에서 고유정보 추출 및 인증정보와 관련된 보안 요구사항을 의미하며, 메모리 해킹 방지, 하드웨어 직접 제어 방지로 구분된다.

● 메모리 해킹 방지

소프트웨어 모듈은 지정된 PC의 고유정보를 추출하여 이를 메모리상에 저장한 후, 필요하다면 연산을 통하여 고유정보를 생성한다. 이렇게 생성된 고유정보는 인증을 위하여 인증 서버로 전송하게 되는데, 이 과정에서 메모리상에 존재하는 하드웨어 고유정보 및 인증정보의 변조가 가능하다. 따라서 추출한 하드웨어 고유정보 및 생성되는 고유정보를 저장할 때 메모리상에 분산하여 저장하는 등 메모리 해킹을 방지하기 위한 방안이 마련되어야 한다.

● 하드웨어 직접 제어 방지

하드웨어 고유정보를 추출하는 방법은 일반적으로 2장에서와 같은 방법이 활용된다. 따라서 하드웨어를 직접 제어하여 추출하는 방법이 가장 낮은 수준에서의 하드웨어 고유정보를 추출하는 방법이지만, 공격자 역시 하드웨어를 직접 제어하여 고유정보를 변경할 수 있다. 이와 같은 문제점을 해결하기 위하여 하드웨어에 접근할 때 디버거 핸들러 등을 이용하여 이와 같은

접근을 탐지하고 대응하여야 한다.

IV. Whole Model applying Security Requirements

현재의 이용 PC 지정 서비스를 기반으로 상기 도출한 보안 요구사항을 적용하였으며, 그 결과를 그림 7에 나타내었다. 등록단계부터 해지단계까지 상기에 도출한 프로세스에서의 요구사항이 적용되어야 하며, 각 단계의 전 구간에 걸쳐 상기에 도출한 네트워크 계층, 소프트웨어 모듈, 단말 영역 환경에서의 요구사항이 적용되어야 한다.

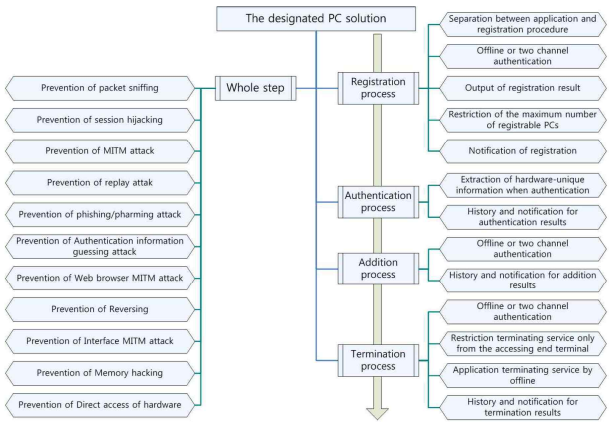

Fig. 7. Whole model applying security requirements

제안한 전체 모델 중 이용 PC 지정 서비스에서 발생이 가능한 보안위협으로는 하드웨어 고유정보 추출 시점, 리버싱, 메모리 해킹, 인터페이스 중간자 공격, 하드웨어 직접 제어인 5가지 위협이 있다. 하드웨어 고유정보 추출 시점의 경우에는 그림 8과 같이 웹 사이트에 접속하는 것만으로도 하드웨어 고유정보가 추출되기 때문에 공격자에 의하여 탈취가 가능하다. 따라서 추출 시점을 인증정보를 전송하는 시점이나 인증이 정상적으로 이루어진 후에 추출하여 고유정보를 검증하여야 보안성을 향상시킬 수 있다.

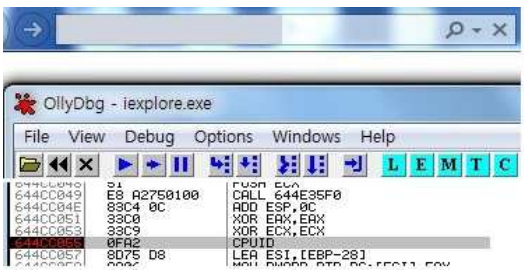

Fig. 8. Result of extraction point of hardware unique information

추출된 고유정보는 메모리 해킹과 리버싱을 통하여 탈취하거나 위/변조가 가능하다. 메모리 해킹의 경우에는 고유정보가 저장되는 소프트웨어 모듈 내의 메모리를 다른 프로세스에서 접근하는 것을 차단하는 방안을 적용하여야 한다. 이는 소프트웨어적인 다양한 방법이 존재하므로[17] 이러한 보안기술을 적용함으로써 고유정보의 탈취 및 위/변조를 방지하여 보안성을 향상시켜야 한다. 또한, 리버싱의 경우에는 다양한 난독화 기술을 적용함으로써 코드를 분석하지 못하도록 방지하여야 한다. 이러한 난독화 기술로는 배치 난독화, 자료 난독화, 제어 난독화, 방지 난독화 등이 있으며[18], 난독화 기법을 적용할 경우, 공격자는 소프트웨어 모듈의 코드를 분석하지 못하므로 고유정보를 위/변조하는 공격에 대응이 가능하여 보안성을 향상시킬 수 있다. 본 논문에서는 이에 대한 개념을 검증하기 위하여 IsDebuggerPresent 함수를 호출함으로써 디버거를 탐지하였으며, 그 결과를 그림 9에 나타내었다.

결과를 살펴보면, 디버거를 탐지하는 보안 모듈이 동작하는 동안 외부에서 디버거로 이용 PC 지정 서비스를 제공하는 프로세스인 인터넷 익스플로러로 디버깅을 시도하는 경우, 보안 모듈이 이를 탐지함으로써 리버싱을 통하여 발생하는 위협에 대응이 가능하다.

인터페이스 중간자 공격의 경우에는 인증정보와 하드웨어 고유정보를 전송하는 HttpSendRequest 함수를 후킹함으로써 아이디, 비밀번호, 고유정보의 탈취가 가능하다. 그림 10에 나타낸 바와 같이 비밀정보를 탈취함으로써 인증의 우회가 가능하므로 이러한 위협을 방지하기 위한 방안이 마련되어야 한다. 인터페이스 중간자 공격의 대부분은 후킹 기술을 이용하므로 후킹을 탐지하는 방안이 적용되어야 하며, 본 논문에서는 함수의 첫 다섯 바이트를 확인하는 방법으로 실험하였다. 따라서 프로세스가 동작할 때의 원본 다섯 바이트를 저장한 후, 소프트웨어 모듈이 동작하는 동안 해당 함수의 다섯 바이트가 변경되는지 확인함으로써 후킹을 탐지하였다. 그 결과, 그림 11과 같이 변경된 바이트가 0xE9이므로 JMP 명령어로 변경된 것을 확인할 수 있으며, 이는 다른 함수로의 분기를 의미하므로 후킹되었다는 것을 의미한다. 따라서 이러한 악의적인 행위를 탐지하여 대응함으로써 보안성을 향상시킬 수 있다.

마지막으로 하드웨어 직접 제어의 경우에는 대부분의 고유정보가 드라이버를 활용하여 커널레벨에서 추출하므로 응용 프로그램과 드라이버와의 통신을 담당하는 DeviceIoControl 함수를 통하여 전달한다. 따라서 이 함수를 감시하는 것만으로도 고유정보를 탈취할 수 있으며, 그 결과를 그림 12에 나타내었다.

결과를 살펴보면, DeviceIoControl 함수 호출 후, 고유정보를 전달받는 것을 확인할 수 있다. 따라서 공격자는 해당 함수를 감시함으로써 고유정보를 탈취할 수 있으며, 해쉬나 암호화되지 않은 평문으로 전송되기 때문에 그 위험성이 증가한다. 그림 13과 같이 전달받은 고유정보를 변경함으로써 우회가 가능하므로 이에 대한 대응방안이 필요하다.

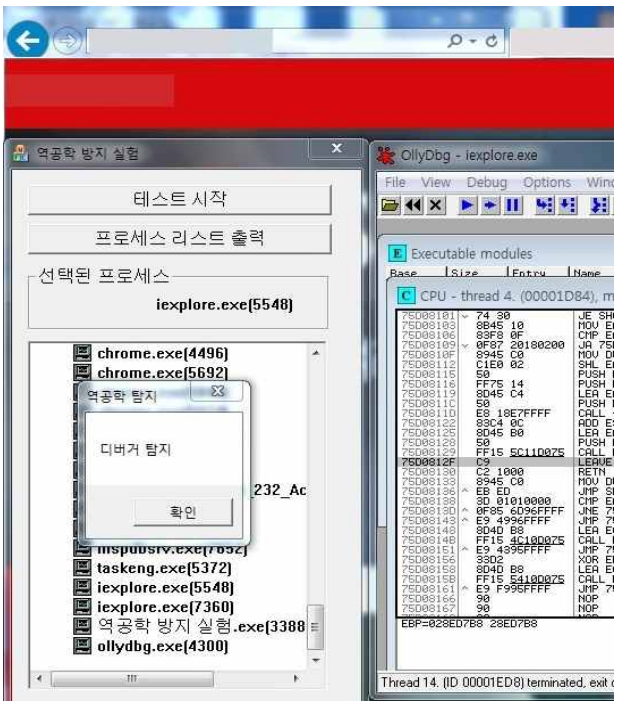

Fig. 9. Experiment result of preventing reverse engineering

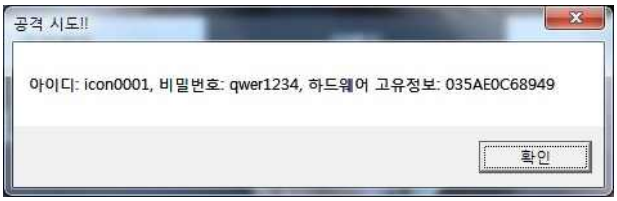

Fig. 10. Result of interface man-in-the middle attack

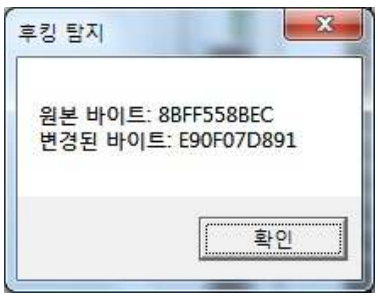

Fig. 11. Detection result of interface man-in-the middle attack

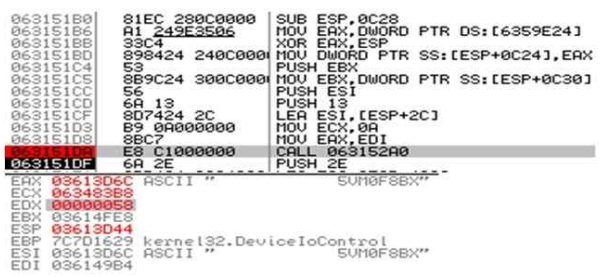

Fig. 12. Extraction result of hardware unique information

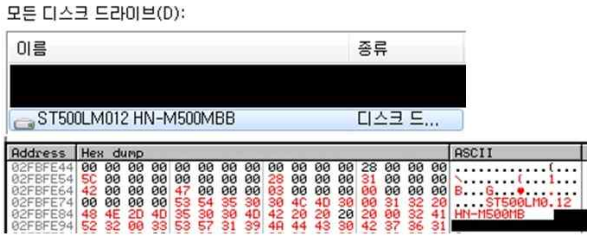

Fig. 13. Modification process of hardware unique information

이를 대응하기 위한 방안으로는 응용 프로그램과 디바이스 드라이버, 혹은 서버와 디바이스 드라이버 사이의 안전한 전송을 보장하고 재전송 공격을 방지하기 위하여 challenge/response 프로토콜이나[19] 다른 암호 기술을 적용하여야 한다.

Table 2. Analysis and comparison of security with existing technique

Evaluation Criteria	Existing Technique	Proposed Model
Bypassing authentication when changing	O	X
Analyzing code to extract hardware unique information	O	X
Detecting interface MITM attack	X	O
Extracting hardware unique information	O	X
Modifying hardware unique information	O	X
Bypassing authentication of designated PC solution	O	X

V. Conclusions

온라인 뱅킹 및 전자상거래 규모가 급증하면서 인터넷을 통한 금융시장은 더욱 성장하고 있지만, 이와는 대조적으로 인터넷 뱅킹 해킹사건이 지속적으로 발생함으로써 온라인 본인확인 수단의 평가방법에 대한 필요성이 대두되었다. 이에 본 논문에서는 행전안전부의 정보보호 수준 강화 사업과 관련하여 이용 PC 지정에서 발생 가능한 보안위협을 프로세스에서 발생 가능한 보안위협, 네트워크 계층에서 발생 가능한 보안위협, 소프트웨어 모듈에서 발생 가능한 보안위협, 단말 영역 환경에서 발생 가능한 보안위협으로 분류하여 분류된 각 보안위협에 대한 세부사항을 도출하였다. 또한 도출한 보안위협을 토대로 이용 PC 지정의 안전성을 확보하기 위한 보안 요구사항을 도출하였다. 본 논문의 결과를 토대로 도출한 보안위협과 보안 요구사항은 차후 이용 PC 지정 솔루션을 도입하는 입장에서 안전성을 더욱 확보하기 위한 자료로 활용될 것이라 기대된다.

REFERENCES

[1] Financial Security Agency(FSA), “Issue Report”, 2012(1), Jan. 2012

[2] Su-Mi Lee and 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

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

[4] Kyungroul Lee and Kangbin Yim, “A Guideline for the Fixed PC Solution”, In proceedings of Smart Convergence Technologies and Applications(SCTA), pp. 74-76, Aug. 2012

[5] Telecommunications Technology Association(TTA), “Security Requirement for Virtual Keyboard”, TTAK.KO-12.0180, Dec. 2011

[6] Mikro Tik, “Packet Sniffer”, Mikro Kifls SIA, 2004

[7] Jung-Yoon Kim and Hyoung-Kee Cho, “Weaknesses of the new design of wearable token system proposed by Sun et al.”, Journal of the Korea Institute of Information Security and Cryptology(KIISC), 20(5), pp. 81-88, Oct. 2010

[8] YoungJae Maeng and DaeHun Nyang, “An Analysis of Replay Attack Vulnerability on Single Sign-On Solutions”, Journal of the Korea Institute of Information Security and Cryptology(KIISC), 18(1), pp. 103-114, Feb. 2008

[9] Yang-Seo Choi and Dong-Il Seo, “Privacy information exposure techniques and countermeasures through Social engineering attacks”, Review of Korea Institute of Information Security and Cryptology(KIISC), 16(1), pp. 40-48, Feb. 2006

[10] Dong Hwi Lee, Kyong-ho Choi, Dong Chun Lee, Kuinam J. Kim, and Sang Min Park, “Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique”, Journal of Information and Security by Korea Information Assurance Society(KIAS), 6(4), pp. 171-177, Dec. 2006

[11] 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

[12] Woochan Hong, Kwangwoo Lee, Seungjoo Kim, and Dongho Won, “Vulnerabilities Analysis of the OTP Implemented on a PC”, Journal of the Korea Information Processing Society(KIPS) Transactions: Part C, 17-C(4), pp. 361-370, Aug. 2010

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

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

[15] 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

[16] 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

[17] Jong-Ik Shim, Tae-Kyou Park, and Jin-Tae Kim, “Protecting Memory of Process Using Mandatory Access Control”, Journal of the Korea Institute of Maritime Information & Communication Sciences, 15(9), pp. 1947-1954, Sep. 2011

[18] Kyung-Roul Lee and Kang-Bin Yim, “A New Analysis Method for Packed Malicious Codes”, Journal of the Korea Navigation Institute(KONI), 16(3), pp. 488-494, Jun. 2012

[19] Non Thiranant, Yvonne Tan Ying Hui, Taeyong Kim, and HoonJae Lee, “Challenge-Response Authentication with a Smartphone”, In Proceedings of the Korea Society of Computer & Information(KSCI), 20(2), pp. 187-190, Jul. 2012

[20] Woongryul Jeon, Jeeyeon Kim, Youngsook Lee, and Dongho Won, “Analysis of Threats and Countermeasures on Mobile Smartphone”, Journal of the Korea Society of Computer & Information(KSCI), 16(2), pp.153-163, Feb. 2011.

[21] Seong-Yoon Shin and Kang-Ho Lee, “A Study of Definition of Security Requirements on Encryption and Audit Logging”, Journal of the Korea Society of Computer & Information(KSCI), 19(9), pp.85-91, Sep. 2014.

[22] Jae-Chan Moon and Seong-Je Cho, “Vulnerability Analysis and Threat Mitigation for Secure Web Application Development”, Journal of the Korea Society of Computer & Information(KSCI), 17(2), pp.127-137, Feb. 2012.

[23] Mi-Og Park, “Weaknesses Cryptanalysis of Khan's

Scheme and Improved Authentication Scheme preserving User Anonymity", Journal of the Korea Society of Computer & Information(KSCI), 18(2), pp.87-94, Feb. 2013.

[24] Young-Back, Sung-Soo Kim, Kyung-Ho Chung, Soo-Yong Kim, Tae-Jin Yun, and Kwang-Seon Ahn, "A Vulnerability Analysis of Multi-Context RFID Mutual Authentication Protocol", Journal of the Korea Society of Computer & Information(KSCI), 18(10), pp.71-80, Oct. 2013.

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 research professor 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 eighty research papers.

Sun-Young Lee received the B.S. and M.S. degrees in Dept. of Computer Science from Pukyong National University, Busan, Korea, in 1993 and 1995, respectively. Dr. Lee received the Ph.D. degree in Dept. of Communication and Information Engineering from the University of Tokyo, in 2001. Dr. Lee is currently a professor in the Department of Information Security Engineering, Soonchunhyang University. She is interested in contents security, cryptography, information theory, and information security.

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 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 sixty research projects and published more than a hundred research papers.