중소기업융합학회 논문지 제3권 제1호 pp. 43-48, 2013

금융 hacking 방지 대응방안

홍성혁*
백석대학교 정보통신학부

Countermeasure for Anti-financial hacking

Sunghyuck Hong*
Baekseok University, Divsion of Information and Communication

요 약 컴퓨터 기술이 발전함에 따라 시스템 공격 기술이 점점 더 진화하고 다양화 되고 있다. 컴퓨터의 하드웨어와 소프트웨어는 점점 진화하고 성능이 향상되고 있지만 기본 동작 원리는 거의 변화하지 않고 있어 문제 대두되고 있다. 일반적으로 응용프로그램들이 실행상태에 놓이면 프로그램의 데이터들이 메모리에 놓이게 된다. 이러한 데이터들은 운영체제 동작의 효율성 때문에 메모리에 남아있게 되어 메모리 해킹이나 메모리 분석을 통하여 데이터들에 접근할 수 있게 된다. 그로 인하여 사용자의 개인정보, 암호화된 키, 인증서 등이 유출되어 큰 피해가 발생하기 때문에 대응 방안이 마련 되어야 한다. 본 논문으로 메모리 해킹에 대한 문제점과 그에 대한 대응책을 제안한다.

Abstract With the development of computer technology, and have diversified technical system attacks evolve more. Computer hardware and software has evolved more and more, performance is improved, but the basic principle of operation does not change much, it is a problem. In general, the application is placed in a running state, the program data is placed in memory. Remains in memory for efficiency of operation of the operating system, we analyze memory and memory hacking, these data will have access to data. Since a large damage occurs key, such as certificates personal information, encrypted flows out, measures should be provided by it. In this content, I want to discuss the issues and work around memory hacking.

Key Words : System Attack Technique, Data, Memory, Hacking, Personal Information

1. 서론

컴퓨터 시스템의 향상 및 응용프로그램이 발달함에 따라 시스템을 공격하는 공격 기술이 점점 더 다양화 되고 있으며 이러한 공격 기술들을 방어하는 방어 기술 또한 다양하게 연구되고 있다. 특히 안티 바이러스 및 침입 탐지 기술의 발달로 기존에 있던 여러 가지의 악성 코드 및 악의적인 공격은 충분히 예방되고 있으며 여러 공격 방어 기술이 발달되고 있지만 아직 부족한 부분이 많아 공격에 취약하다. 시스템 내부의 악성 코드 혹은 직/간접적인 해킹을 통하여 사용자의 데이터나 키보드 사용에 따라 키 로그 정보를 메모리 접근을 통해 도출 하는 공격이 문제 되고 있어 메모리 내의 개인 정보의 유출에 대한 위협에 대한 대응은 미흡하다.

일반적으로 프로세스가 실행중인 메모리에 접근하는 것은 운영체제에서 접근권한이 벗어나는 일이지만 윈도우 운영체제에서는 메모리내의 데이터를 볼 수 있는 방법이 존재 한다. 이로 인하여 금융권 등에서 피해자가 급증하고 있어 문제가 대두 되고 있다.

접수일 : 2013년 3월 23일 수정일 : 2013년 4월 28일 게재확정일 : 2013년 5월 7일
*교신저자 : 홍성혁(shong@bu.ac.kr)

2. 본론

2.1 메모리 해킹 정의

최근 금융범죄 수법이 사용자가 이용하고 자 하는 정상적인 사이트주소를 악성코드가 담긴 가짜 사이트로 우회하여 사용자가 자신의 개인정보를 입력하게 한 후 사용자의 예금을 인출해가는 '파밍'에서 게임 보안 모듈 공격에 악용되었던 '메모리 해킹'이라는 신종 수법으로 점차 진화하고 있다.[1]

메모리 해킹이란 정상 인터넷 뱅킹 사이트를 이용하는 인터넷 뱅킹 서비스를 이용하는 사용자를 대상으로 하는 신종 해킹방법으로 사용자들에게 보안강화를 가장한 팝업 창을 이용하여 고정적인 패스워드인 보안카드 번호를 입력하게 하고 일정시간이 지난 후 사용자 예금이 부당으로 인출되며 사용자의 여러 정보가 유출되는 피해를 말한다.[1-5]

이 메모리해킹은 금융권과 사용자 자신이 모르는 사이에 계좌에서 인출되는 방식으로 최근 문제가 대두되고 있으며 그로인한 피해를 줄이기 위한 방법이 필요하다.

2.2 메모리 해킹 사례 및 공격 방법

Fig. 1은 정상적인 이체 거래 페이지에서 입금 계좌번호를 입력하면 공격자는 사용자의 메모리를 해킹하여 입금정보에 공격자의 정보를 입력하는 방법으로 사용자의 예금을 부당 인출 할 수 있다는 것을 보여주는 사진이다. 구체적인 사례를 보자면 최근 한 사용자는 자신의 공인인증서를 통하여 은행 홈페이지에 접속하고 정상적인 서비스를 이용한 후 계좌번호와 Fig. 2 와 같은 팝업창에 보안카드 숫자 2글자만 입력하였다. 하지만 평소와 다르게 컴퓨터 화면이 다음 단계로 넘어가지 않았는데 일시적인 오류라 생각하여 대수롭지 않게 넘어갔다. 시간이 지난 뒤 입출금 내역을 확인하니 자신의 계좌가 여러 계좌로 분산되어 인출 되는 경우가 발생하였다.[2-5]

Fig. 1. 계좌번호 변조

Fig. 2. 개인정보 입력 창

이 사례를 통해 알 수 있는 '메모리 해킹'에 대한 공격 방법은 다음과 같다. Fig 3[5]는 이 메모리 해킹의 공격 방법에 대한 사진이다.

인터넷 뱅킹을 사용하는 사용자가 취약 금융 사이트에 방문 시 악성코드에 감염 된 후 사용자가 금융 사이트를 재방문하면 악성코드가 해당 사실을 감지하고 사용자의 금융 사이트 방문 시 구동되는 보안 모듈인 키보드 보안 솔루션, 공인 인증서 등 금융 사이트에서 구동 시에 사용자의 보안을 위해 자동으로 구동되는 보안 솔루션에 메모리 해킹 공격을 시작한다. 악성코드는 평소에는 사용자의 일반 인터넷 이용 시에는 반응을 하지 않지만 금융 기관의 금융 거래 서비스 이용 시에 자동으로 동작하는 보안 모듈이 구동되면 이를 감지하여 보안 모듈의 메모리 해킹을 시작한다. 만약 보안 모듈이 동작하지 않을 경우에는 금융기관에서 이를 파악하고 공격을 차단 할 수 있으므로 메모리 해킹 방식은 보안 모듈은 동작을 유지하되 모듈을 무력화시키고 악성 코드가 원하는 사용자 개인 금융 정보 유출을 먼저 수행하도록 조치한다. 그 후 악성 코드로 얻은 개인 금융 정보를 이용하여 사용자의 예금 인출을 시도하고 탈취한 보안카드 정보는 공격자의 에러처리로 은행에 인출한 사실이 전달되지 않았으므로 그대로 재사용 할 수 있다.[7,8]

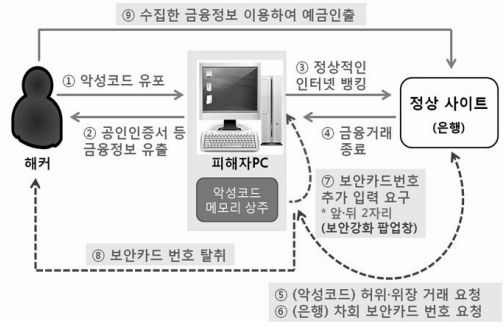

Fig. 3. Attack Method

fig.4[3]는 공격자가 심어놓은 악성 코드에 감염된 개인 PC가 금융 사이트의 서비스를 이용할 때 나타나는 모습이며 사용자가 정상적인 이체 페이지를 통하여 입력한 정도를 토대로 정보를 입수하고 계좌번호 변조를 통하여 공격자의 계좌번호로 변조 하는 방법을 소스로 보여주는 그림이다.

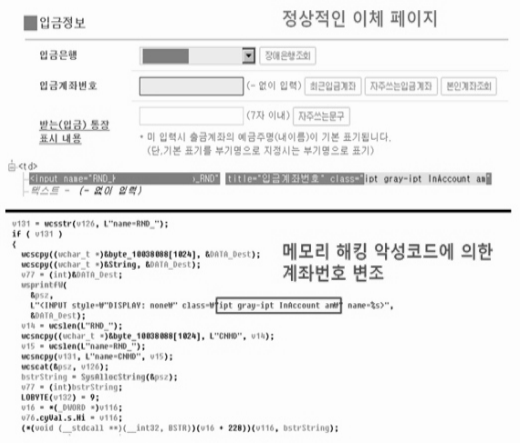

Fig. 4. 정상적인 이체 페이지에서의 정보 변조

2.2.1 사용자 정보 유출

Fig. [5],[6]는 사용자가 인증서 암호를 이용하여 로그인 한 것을 16진수와 ASCII코드로 보여주는 그림이며 Fig. 6[6]은 이러한 로그인 정보와 더불어 사용자의 정보까지 공격자의 PC에서 보여 지는 것을 나타낸 그림이다. 이와 같이 금융 서비스를 이용했을 때 메모리 해킹을 이용하여 공격자가 사용자의 개인정보를 쉽게 알 수 있다는 것을 실습해본 그림이다.

그림에서는 사용자 인증서 암호로 memorydump61을 이용하여 은행에 사용자 로그인을 하였다. 공격자는 이러한 사용자 로그인 정보를 메모리 해킹을 통하여 이러한 인증서 정보와 더불어 사용자의 식별번호인 주민등록번호, ID까지 노출이 되는 것을 확인 할 수 있다.

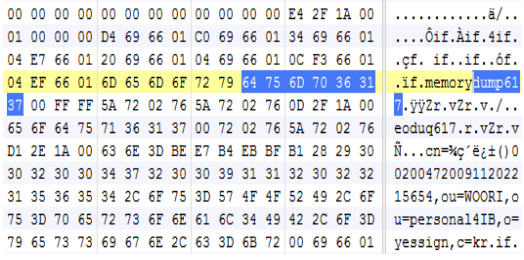

Fig. 5 인증서 암호 로그인

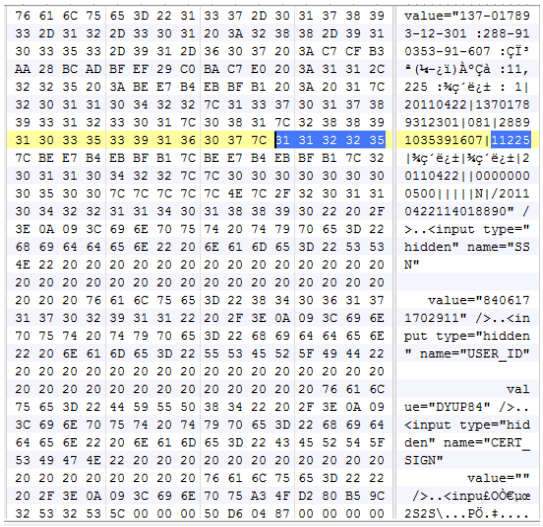

Fig. 6. 사용자의 정보 노출

2.3 메모리 해킹 악성 코드 분석

악성 코드를 분석한 결과 %TEMP%경로에 3개, %SYSTEMROOT%\system.32와 %SYSTEMROOT%\system32\drivers에 각 2개, 1개가 있었다. 악성코드 파일의 타입은 DLL이였고 파일의 크기는 제각각 이였다. 이중 %TEMP% Directory의 악성 코드 qBr.dll를 분석해 보면 다음과 같다.

qBr.dll이 상주하고 있는 프로세스 명이 각 보안업체의 프로세스 명일 경우 종료하며 iexplore.exe가 아닐 경우 종료하며 iexplore.exe일 경우 6개의 쓰레드를 생성하고 종료한다.

Fig. 7 [7] 그림은 쓰레드 1에 대한 설명으로 V3, 알약 제품 등의 보안 기능을 무력화 시키고 Fig 8[7] 그림인 쓰레드 2의 경우 보안 프로그램이 있는지 조사 한 후 보안 프로그램의 자동 실행을 막기 위하여 레지스트리를 삭제한다. Fig. 9[7] 사진은 쓰레드 3이 다른 쓰레드가 실행 가능한지 탐색하고 idle상태의 쓰레드를 실행 가능한 상태로 만들기 위해 사용 된다. Fig 10.[7] 은 쓰레드 4와 5의 역할에 대해 보여주는 사진인데 다른 URL로부터 악성코드를 %TEMP% 경로에 다운로드 받은 후 실행하는 역할을 한다. 마지막으로 Fig. 11[7]의 쓰레드6의 경우 현재 실행중인 프로세스의 목록을 조사하여, 여러 제품 관련 보안 프로그램을 강제 종료한다.[7,10]

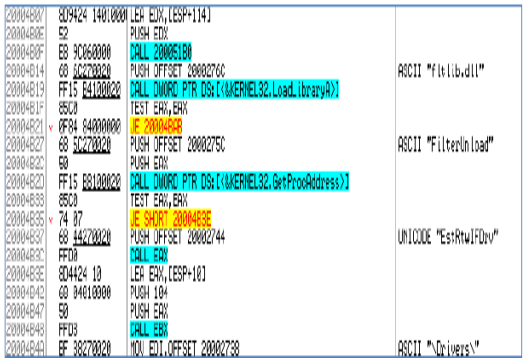

Fig. 7. thread 1

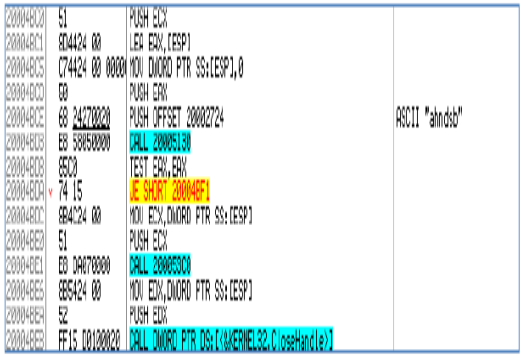

Fig. 8. thread 2

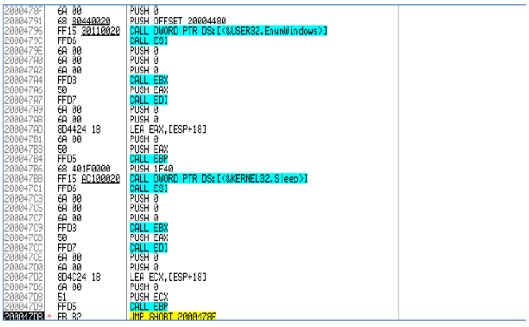

Fig. 9. thread 3

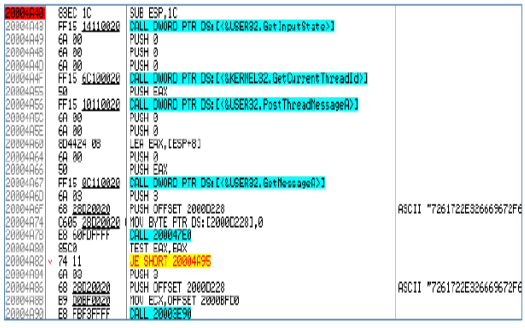

Fig. 10. thread 4, 5

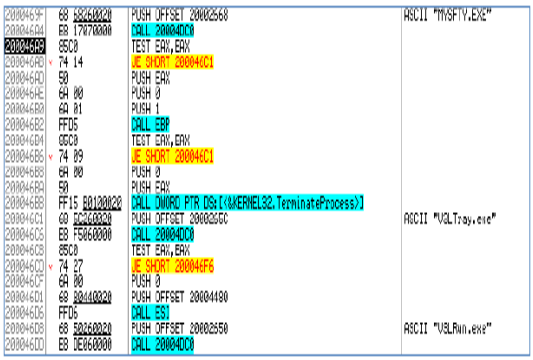

Fig. 11. thread 6

2.4 메모리 해킹의 심각성

메모리 해킹의 심각성은 피해사례에서 생각해볼 수 있다. 클라이언트 보안 제품에 대한 직접적인 해킹으로 정상적으로 금융 사이트에 접속이 가능하며 정상적으로 보안 모듈 구동을 유지하면서 수행되는 공격이므로 해당 금융기관 서버에서는 이를 감지하기 힘들다. 특정 공격 방식의 경우 사용자 입장에서 보안카드 번호 입력 시에 계속 에러가 나는 것 외에는 별다른 이상 징후를 파악하기 어려워 뒤늦게 피해를 인지할 가능성이 높다. 또한 이 메모리 해킹 방법이 은행 사이트를 이용 시 자동으로 구동되는 키보드 보안 솔루션이나 공인 인증서 등 보안 모듈의 메모리를 해킹하여 무력화하고 악성코드가 원하는 개인정보 유출을 먼저 수행한다. 그러므로 사용자는 이러한 메모리 해킹이 일어나는 것을 전혀 인지 할 수 없으며 만약 알았다고 하더라도 이미 자신의 개인정보를 유출을 당하고 금전적인 피해를 입은 후라 대응하기 어려워 피해가 점점 커지게 된다. 또한 각각의 악성 코드들이 여러 은행들을 Target으로 삼아 해당 금융기관만 특화되어 제작되어 있으므로 예방하거나 대처하기 더욱 더 어려워지고 있는 실정이다. 이러한 문제들로 인하여 메모리 해킹으로 점점 더 큰 피해를 입을 수 있다. [8]

2.5 예방책과 대응책

메모리 해킹의 전형적 수법은 금융 서비스 이용 중 컴퓨터가 갑자기 꺼지거나 서비스를 정상적으로 이용한 후에 추가로 팝업창이 떠 개인정보를 묻는 방법으로 그 예방방법은 다음과 같다.

몇몇 은행에서는 금융서비스를 이용하는 PC를 지정하는 서비스를 제공하고 있는데 이 서비스는 휴대폰 인증을 통해 사용할 PC를 등록하는 방법으로 이용자 시스

템의 MAC주소(물리적 주소)를 이용하여 인증한 컴퓨터만 금융 서비스를 이용할 수 있도록 하는 방법이 있으며 공인인증서, 보안 카드 사진 등 개인정보를 PC나 이메일에 저장하지 않으며 무분별한 웹 서핑, 출처 불분명한 파일을 다운로드 하지 않는 것이 좋다. [3,5]

더욱 더 확실한 방법으로는 금융 기관에서 발급받은 보안카드 대신에 OTP(One Pass Time : 일회용 비밀번호 생성기) 를 이용하는 방법으로 고정된 패스워드 대신 각 사용자에게만 할당된 비밀 키를 이용해 값을 생성한다. 비밀 키는 초기에 OTP생성기를 제작할 때에 함께 생성되며 인증 서버에 저장하여 인증정보를 OTP가 생성될 때에 비밀 키와 동시에 연산되도록 하는 방법으로 무작위로 패스워드를 생성하는 일회용성 패스워드를 이용하는 사용자 인증 방식 이다. [4,5,8,11]

Fig. 12[11]는 OTP 원리에 대한 설명을 그림으로 간략화 한 모습이다. OTP도 PC등록과 마찬가지로 서버와 클라이언트가 미리 약속한 방식을 통하여 MAC을 생성하여 서버에게 전달함으로써 생성한 MAC의 무결성을 검증하여 인증을 받게 되는 방식이다. 또한 서버와 클라이언트 또는 토큰 사이에 미리 약속된 룰에 의해서 클라이언트 쪽에서 생성한 일회성 암호를 서버 측에 보내게 되면 서버 측에서는 같은 룰을 이용하여 데이터가 들어있는 데이터베이스에서 비밀 값을 가져온 후 일회성 암호를 생성하여 클라이언트가 보낸 값과 서버 측의 암호를 비교 하는 형식이다. 이 때 양 측의 암호를 동기화 시키는 것이 OTP 원리의 가장 핵심이다. 동기화 시키는 방법은 서버 측에서 난수 발생기를 사용해 일정한 자릿수의 질의 값을 클라이언트 측으로 보내면 그 질의 값을 토큰에 입력하여 응답 값을 생성해 낸다. 이 토큰은 서버에서 보내온 질의 값과 토큰 자체의 비밀 값 등을 가지고 해쉬 함수를 이용하여 적당한 처리를 하여 응답 값을 생성하며 생성된 값을 서버 측으로 보내어 인증을 받는 Challenge/Response방식이 대표적이다. [11,12]

3. 제안하는 메모리 해킹 방지 방안

메모리 해킹은 개인 혹은 금융권에서 각자 예방방법을 가지고 사전에 방어 한다고 하더라도 모든 공격을 방어할 수 있는 공격이 아니라고 생각한다. 그래서 생각한 새로운 방안을 제안하고자 한다.

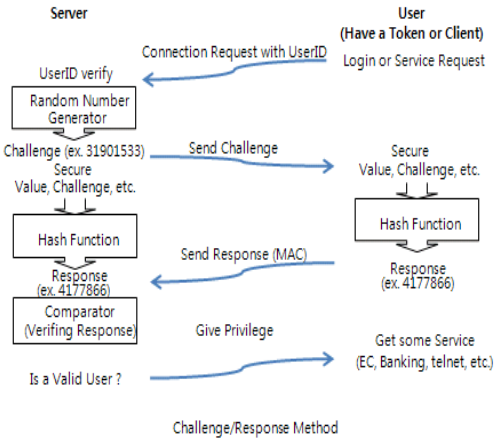

Fig. 12. OTP 원리

신종 공격인 메모리 해킹을 방어하기 위하여 기존의 존재하는 OTP 생성기와 공인인증서를 가지고 암호화 하는 방법을 생각해 보았다. 그 방법은 다음과 같다. 사용자와 금융권인 은행에서는 사용자의 공인인증서 생성 시에 해당 공인인증서의 정보가 들어있는 OTP생성기를 발급한다. 발급 받은 OTP생성기에는 사용자의 공인 인증서 정보가 입력되어 있으므로 공인 인증서와 임의의 값이 알고리즘으로 연산되어 암호화 된 값으로 값을 출력한다. 그렇게 연산되어 암호화 된 값은 기존의 금융권과 사용자 사이에서 나타나는 OTP 값과 비슷한 방법으로 사용자가 암호화 된 값을 금융 서비스를 이용할 시에 입력하게 되면 금융권에서는 해당 값을 복호화하여 사용자의 금융 공인 인증서 값을 알아내는 방법이다.

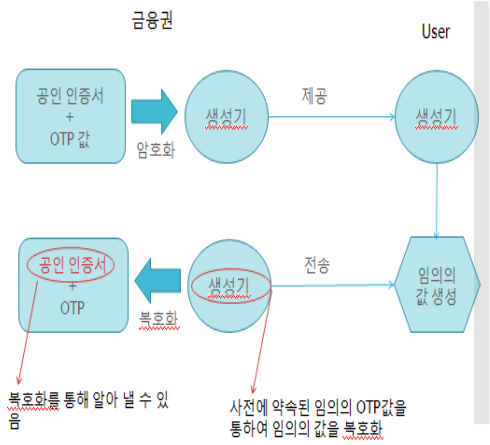

Fig. 13. OTP와 공인인증서를 통한 새로운 방안

4. 결론

본 내용에서는 메모리 접근을 통하여 발생할 수 있는 정보 유출의 가능성에 대하여 논하고 대응과 예방할 수 있는 방법에 대해 소개하였다. 메모리 공격 방법이 다른 여러 해킹 방법들에 비해 덜 알려져 있으며 대응할 수 있는 방법이 적으므로 메모리 해킹에 대한 위험성에 대한 인식이 아직 부족하다. [11]

메모리 접근을 통해 중요한 시스템이나 컴퓨터에 대한 공격이 이루어질 경우 컴퓨터에 대한 여러 정보와 사용자 개인의 개인 정보 등 해커들이 얻을 수 있는 정보가 방대하기 때문에 위험하다. 메모리에 프로세스가 남아있는 이유는 사용자가 해당 프로그램을 다시 실행시킬 경우 보다 빠른 실행이 가능하므로 메모리에 남아있는 것이 효율적이다. 그러나 해커들은 이 부분을 악용하기 때문에 주의하고 예방할 필요가 있다. 본 내용에서는 이러한 위험성을 이야기 하고 실 생활에서 사용자 스스로 예방할 수 있는 방법을 제시 하였다.

참 고 문 헌

[1] POL/폴인러브는 순찰 중. “전자금융사기(스미싱, 메모리해킹)의 모든 것”. POLINLOVE. September 24, 2013, 경찰청 대변인실. October 10, 2013, <http://polinlove.tistory.com/6521>

[2] 경북북부 인터넷뉴스. 2013. “이체정보 가로채는 신종 메모리해킹 수법”, 9월19일

[3] 보안뉴스. 2013 “7개 은행을 타깃 메모리 해킹 공격 실태 분석해보니.” 10월 7일

[4] 디지털엔젤. “신종 인터넷 금융사기 메모리해킹 수법과 대처법”, August 16, 2013, DiskShot. October 11, 2013, <http://www.diskool.com/2370217>

[5] news1 korea. 2013. “메모리 해킹 등 신종 금융범죄 '주의보'”, 8월 27일.

[6] Daeyeop Yang, Manhyun Chung, Jaeik Cho, Taeshik Shon, and Jongsub Moon. 2012. “메모리 초기화를 이용한 사용자 데이터 유출 방지에 관한 연구”, 전자 공학회 논문지, 49권 7호:74

[7] Red Alert. 2013. “악성코드 분석 보고서”, 13-15,

[8] POL/폴인러브는 순찰 중. “신종 금융범죄 수법”. August 22, 2013, 경찰청 대변인실. October 11, 2013, <http://polinlove.tistory.com/6487>

[9] 보안라이프/이슈&이슈. “메모리 해킹(수정)”으로 금융정보 및 금전 유출 시도하는 악성코드 분석. July 3, 2013, AhnLab보안세상. October 12, 2013, <http://blogsabo.ahnlab.com/1512>

[10] Minul. “OTP 시스템의 구현방안“. August 31, 2007, October 12, 2013. <http://mimul.com/pebble/default/2007/08/31/1188572280000.html>

[11] Seungki Kim, Jungjoo Seo, Hyunmok Song,Hyunsang Park, Sungjin Lee, Seungjoo Kim, Dongho Won. “A secure OTP system using key input devices for financial service”. 5page. 2008

저 자 소 개

홍 성 혁(Sunghyuck Hong) [정회원]

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

- E-Mail : shong@bu.ac.kr

<관심분야> : 네트워크 보안, 해킹, 센서네트워크 보안