Malware에 감염된 Endpoint환경에서 안전한 전자금융거래

이연재*, 이희조*
*고려대학교 컴퓨터정보통신대학원
discovelee@gmail.com, heejo@korea.ac.kr

A study on secure electronic financial transactions in the endpoint environment infected with malware

YeonJae Lee*, HeeJo Lee*
*Graduate School of Computer Information & Communication, Korea University

요 약

유무선 인터넷이 보편화되고 이용이 확산되면서 금융권에서는 고객의 편의성 증진을 위해 영업점의 상당한 업무를 인터넷뱅킹과 모바일뱅킹 등을 이용하여 처리할 수 있는 IT환경을 제공하고 있다. 이러한 Endpoint 환경의 변화는 점점 더 지능화되고 있는 사이버 공격 기술로 보안 위협이 증대되고 있는 실정이다. 이를 해결하기 위한 방법 중의 하나로 본 연구에서는 Reverse sandboxing 기술과 화이트리스트 기반의 보안 기술이 내장된 커널 수준의 TSX(Trusted Security eXtension)기술을 통하여 맬웨어가 감염된 상태에서도 안전하게 전자금융거래를 할 수 있는 Endpoint환경을 제공한다.

Keyword : 인터넷뱅킹, 모바일뱅킹, anti-virus, 피싱, 파밍, 메모리해킹, 샌드박스, trustzone, 가상화, 화이트리스트, 커널 보안

1. 서론

현재의 IT정보기술은 우리의 생활 전 부문에 걸쳐 없어서는 안 될 중요한 핵심 기술로 자리 잡았다. 특히 유무선 인터넷이 보편화되고 이용이 확산되면서 은행은 고객의 편의성 증진을 위해 은행에 가지 않고도 인터넷 뱅킹과 모바일 뱅킹 등을 이용하여 돈을 송금할 수 있고 금융정보 서비스를 제공 받을 수 있는 IT환경을 제공하게 되었다. 이러한 환경으로 컴퓨터와 인터넷을 연결한 온라인 기반의 인터넷 이용자수는 2014년 1/4분기중 인터넷뱅킹 이용건수는 6,369만건, 금액(일평균 기준)은 36조 1,394억원으로, 스마트폰뱅킹 이용건수 및 금액은 2,737만건, 1조 6,276억원으로 전분기대비 계속 증가하였다[1].

그러나 이와 같은 사이버 영역에 대한 활동들이 일상화되면서 최종 이용자의 매체(endpoint)에 대한 보안 침해 사고 및 공격으로 인한 피해 사례들도 지속적으로 발생하고 있으며, 2013년 국내의 연간 악성코드 감염 탐지는 242만건, 해킹사고 신고건수는 11천건으로 나타났다[2].

최근 들어 금융권의 사이버 공간은 고객 정보뿐만 아니라 금전적 이득을 목적으로 하는 새로운 공격의 대상으로 부상되었으며, 특히 인터넷 금융사기 수법인 피싱(phishing), 파밍(pharming)에서 한 단계 업그레이 된 새로운 해킹수법인 메모리 해킹이 등장했다. 이러한 현상은 인터넷뱅킹, 모바일뱅킹, 자동화기기(ATM), 판매시점시스템(POS) 등의 전자금융거래 이용수단의 발달로 금융 소비자들의 이용 편의성은 크게 높아졌지만, 아울러 사이버 공격 기법도 다양한 방식으로 은닉화, 지능화, 사회 공학적 범죄형 해킹이 증가하게 되었으며 앞으로 보안 침해 사고는 계속 늘어날 것이다. 그러나 Anti-virus 등과 같은 전통적인 보안 대응 기술로는 급속히 발전하는 Malware 공격에서 이용자나 금융기관을 보호하기에는 더 이상 충분하지 않은 실정이다.

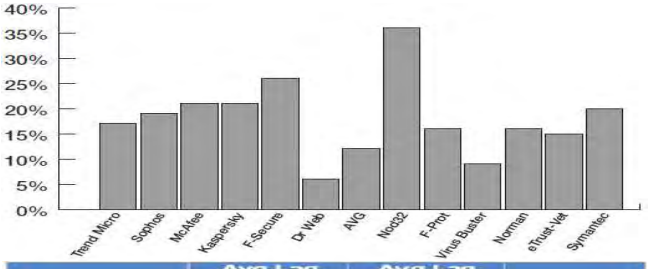
이에 본 논문은 Malware에 감염된 endpoint환경에서 안전한 전자금융거래를 할 수 있는 연구대상의 보안 기술을 제안하고, 기존 보안 기술의 유형에 대한 장단점과 비교분석하여 제안 기술의 차별성을 검증하고자 한다.

2. 문헌 연구

(1) 악성코드(Malware) 특성에 의한 분류

맬웨어는 악성 소프트웨어(malicious software)의 줄임말로, 유형은 다음과 같다. ①컴퓨터 바이러스(Virus)는 컴퓨터 시스템의 부트영역, 메모리영역, 파일영역 등에 기생하면서 자기 증식 및 복제가 가능하고 컴퓨터를 감염시킬 수 있는 악성 컴퓨터 프로그램을 말한다. ②웜(Worm)은 다른 프로그램을 감염시키지 않고 스스로 자신을 복제하여 네트워크상에 연결된 공격 대상을 찾아 시스템 및 네트워크를 마비시킨다. ③트로이 목마(Trojan horse)는 다른 프로그램 내에 숨어 있는 악성 소프트웨어

프로그램으로 합법적인 유틸리티 프로그램 내에 숨어서 컴퓨터에 침입하며 자기 복사 능력은 없다[5]. 이외에도 스팸발송이나 DoS공격 등의 원격작업을 수행하는 봇(Bot)과 이용자의 동의 없이 정보를 수집하는 스파이웨어(Spyware), 그리고 문서나 그림파일을 암호화하고 해독용 키 프로그램이 필요하다면 금품을 요구하는 랜섬웨어(Ransom ware) 등이 있다. 그러나 안티-바이러스 솔루션은 [그림2-1]과 같이 새로운 멀웨어 탐지 실패율이 60% 이상이며, 조치시간은 2~27일이 소요된다[12].



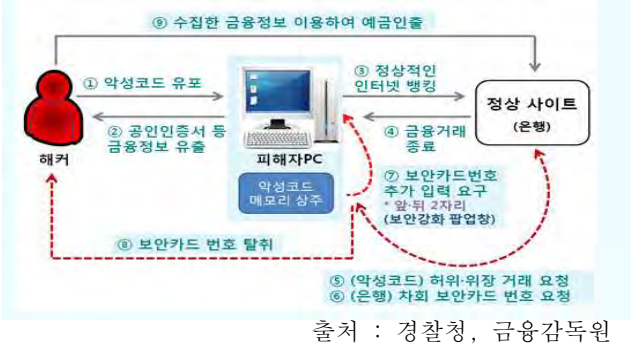
	Avg Lag Time In Hours	Avg Lag Time In Days	Ranking
Nod32	51.8	2.2	1
Kaspersky	90.8	3.8	2
AVG	124.5	5.2	3
Dr Web	131.8	5.5	4
Norman	152.7	6.4	5
Symantec	235.7	9.8	6
F-Secure	243.2	10.1	7
eTrust-Vet	273.5	11.4	8
McAfee	344.2	14.3	9
F-Prot	388.5	16.2	10
Trend Micro	390.3	16.3	11
Sophos	548.5	22.9	12
VirusBuster	653.2	27.2	13

[그림2-1] Anti-Virus 솔루션 탐지율과 조치시간[12]

(2) 전자금융 해킹에 의한 분류

①피싱(Phishing)은 금전취득의 목적을 위해 개인 정보를 불법적으로 획득하고자 하는 사람이 이메일, 메신저,URL 링크 등을 이용하여 불특정 다수에게 금융 기관임을 사칭하여 개인의 카드 혹은 계좌 정보를 빼내어 불법적으로 이용하는 방법이다. ②파밍(Pharming)은 이용자의 PC를 감염시켜 정상 금융사이트에 접속해도 가짜 사이트로 유도하여 금융정보를 탈취함으로서 해커의 대포통장으로 계좌 이체 시키는 행위이다[4,14].

③메모리 해킹은 정상적인 인터넷뱅킹 과정에서도 계좌를 임의로 변경하는 새로운 수법으로 메모리에 상주한 데이터를 위·변조하여 수취 계좌와 금액까지 변경 할 수 있는 해킹 방법이다. 메모리 해킹의 피해 흐름도는 [그림2-2]와 같다[3,4].



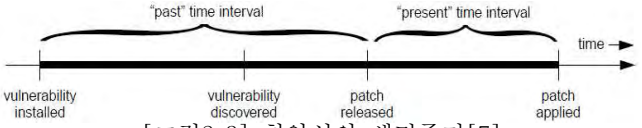
출처 : 경찰청, 금융감독원

[그림2-2] 메모리 해킹 피해 흐름도

(3) 메모리 해킹의 대응기술

① 전통적인 보안기술

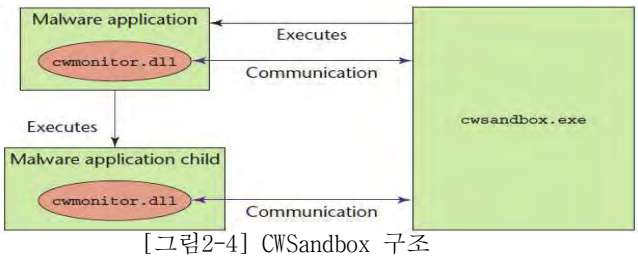
Anti-virus Updated, OS Patched, Anti-Virus Vaccine 등은 가장 널리 사용되고 있는 보안기술 중의 하나이지만, 특정 소프트웨어의 버그가 발생한 경우 [그림2-3]과 같이 패치가 배포 될 때까지 취약성을 모르거나 패치를 갱신하지 않아서 현재까지도 취약성이 계속 잠재하고 있다. 이는 맬웨어 탐지를 위한 정적 분석(Static Analysis)의 문제점이다[7].



[그림2-3] 취약성의 생명주기[7]

② Sandbox를 이용한 보안 기술

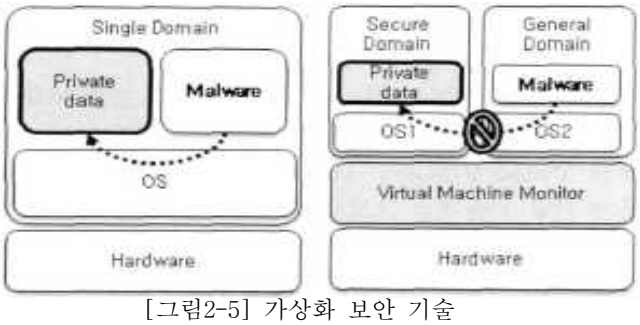
샌드박스는 통제된 환경에서 프로그램을 실행하고 그 프로세스와 쓰레드, 데이터 변경 및 시스템 트레이스를 부정하게 변경하는 것을 동적으로 분석하여 막아주는 보안 형태를 말한다. 이 기술의 예로는 CWSandbox와 Java Sandbox가 있다. CWSandbox는 [그림2-4]와 같이 실제 컴퓨터 시스템상에서 실행 파일(Executable File)을 실행하면 악성 코드를 위한 새로운 프로세스 이미지를 만든 후 대상 응용 프로그램의 주소 공간에 cwmonitor.dll을 인젝션 시킨다. 이후 해당 실행 파일의 모든 절차를 추적하여 해당 정보를 모두 CWSnadbox로 전달하게 되며, 이 과정에서 실행 파일의 악성코드 여부를 판단한다[8].



[그림2-4] CWSandbox 구조

(4) 가상화를 이용한 보안 기술

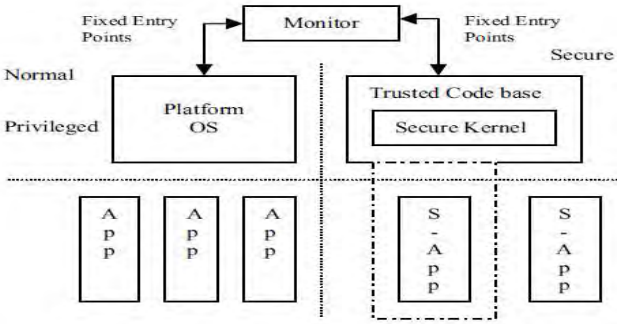
가상화는 물리적으로 다른 시스템을 논리적으로 통합하거나 또는 하나의 시스템을 논리적으로 분할해 자원을 효율적으로 사용하는 기술이다. 그러나 최근에는 [그림2-5]와 같이 악성코드 탐지나 컴퓨터 바이러스를 탐지하는 안티 바이러스 솔루션의 보안 영역으로 활용되고 있다[6].



[그림2-5] 가상화 보안 기술

(5) Trustzone Platform

트러스트존은 데이터 무결성을 보장하기 위해서 [그림 2-6]과 같이 프로세스 모드를 일반모드와 보안모드로 나누고 격리(isolation)된 보안모드에는 코어 아키텍처와 메모리 시스템을 관리하는 커널 보안 도메인을 제공하는 구조를 가지고 있기 때문에 메모리의 강력한 보호가 가능하다. 트러스트존은 실행 환경에서 시작해 시스템의 버스와 IP 블록 전체로 보안이 확장되어 시스템 전체를 고찰하는 접근법이다[9,10].



[그림2-6] TrustZone architecture[9]

(6) White list

화이트리스트는 특정 권한, 서비스, 이동성의 접근 또는 인식을 허용하는 목록이나 레지스터이다. 목록에 있는 사항들만 수락, 승인, 인식된다[11]. 즉, 안전이 증명된 것만을 허용하기 때문에 보안성은 블랙리스트 방식 보다 더 강력하게 유지할 수 있다. 최근 이란의 부세르 원자력발전소 시스템이 스턱스넷(Stuxnet) 웜 바이러스에 감염돼 장애를 일으키면서 본 기술이 주목을 받고 있다.

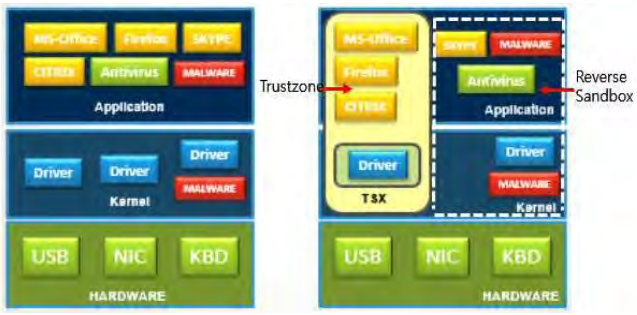
3. 제안 기술 SafeCentral

(1) 연구 방법

앞선 문헌연구에서 조사한 선행연구 작업들은 대부분 맬웨어를 예방, 진단, 치료하는 정적 분석기술과 맬웨어를 격리시켜 조치한 후 해당 거래를 수행시키는 동적 분석기술들을 병행 사용하지만, 새로운 맬웨어에 대한 안티-바이러스 탐지율은 40% 미만이고, 이를 조치하는 시간도 평균 2일이상 소요되고 있는 실정으로 endpoint의 보안 위협을 제거하지 못하고 있다. 따라서 본 연구는 최종 이용자의 컴퓨터(데스크 탑, 스마트폰, ATM, POS 등)에 빈번하게 발생하는 악성코드가 감염되어 있는 상태에서 전자금융거래를 안전하게 할 수 있는 보안 기술을 찾는데서 출발 하였다.

(2) SafeCentral Framework

인터넷(모바일)뱅킹거래의 온라인 세션 데이터를 가장 안전하게 보호하기 위하여 [그림3-1]과 같이 웹 세션 외부에 현재 컴퓨터에 존재하는 맬웨어는 Reverse Sandboxing 격리 기술로 원천적으로 차단하여 활동을 중지 시키고, Trustzone의 아키텍처를 기반으로 설계된 TSX(Trusted Security eXtensions)기술과 승인된 거래만 허용하는 Whitelist 방식이 적용된 보안 기술이 핵심이다[13].구조적으로 Secure Desktop(Mobile)과 Safe Browser가 보장되며 endpoint 보안에 적합하도록 설계되었다.



일반 Desktop [그림3-1] TSX가 설치된 Desktop

(3) SafeCentral 엔진의 동작 과정

[그림3-2]와 같이 1단계는 이용자의 컴퓨터가 맬웨어에 감염되었다고 가정하고, 2단계는 운영체계와 데스크톱을 주문형 잠금(on-demand lock-down)처리를 실시하여 커널 레이어에서 활동하는 멀웨어가 동작하지 못하도록 한다. 즉 Reverse Sandboxing 격리기술을 적용하여 온라인 세션과의 관계를 차단하고 커널상에 TSX의 기술로 OS기능과 프로세스들을 매핑하여 “Trusted” 영역을 정의한다. 3단계는 secure browser, secure desktop, secure session이 보장되는 환경에서 즉, 맬웨어가 존재하지 않는 안전한 환경에서 승인된 거래만 처리하는 Whitelist 방식으로 전자금융거래가 진행된다[13].

[그림3-2] SafeCentral 동작 과정

(4) 연구 분석 방법

①전자금융거래 영역별로 발생 가능한 보안 취약성을 조사하여 정리하고 이를 예방할 수 있는 보안 기술을 비교 분석하였다. ②화이트리스트 방식과 블랙리스트 방식, 그리고 전통적 또는 최신의 기술을 적용한 보안기술과 제안 기술을 비교 분석하여 그 차이점을 제시한다.

4. 연구 분석 결과

(1) 전자금융거래의 보안 취약성

전자금융거래는 각 거래 영역별로 발생 가능한 보안의 위협을 [그림4-1]과 같이 정의하였으며 현재는 실시간으

로 악의성 어플리케이션을 탐지하기 위해 샌드박스 또는 가상화 기술을 이용하여 동적으로 분석을 수행하는데 대부분 패턴 방식의 기술을 적용하고 있다.

[그림4-1] 전자금융거래의 보안 취약성

(2) 보안기술 비교 분석

가. Whitelist방식과 Blacklist방식

<표4-1>과 같이 화이트리스트 방식이 블랙리스트 방식보다 보안 수준이 높은 것으로 조사됐다.

<표4-1> Whitelist방식 vs Blacklist방식

구분	화이트리스트 방식	블랙리스트 방식
처리방식	사전예방(Proactive)	사후조치(Reactive)
애플리케이션 제어	승인된 것만 허용	승인된 것만 차단
업데이트/패치	정기적 점검	실시간 점검
적용 범위	제한적	범용적
엔진 크기	한정적	지속적 증가
리소스 점유율	낮음	높음
보안 수준	높음	낮음

나. 전통적 보안기술과 제안 기술의 비교

endpoint 환경에서는 보안 위협에 대한 원천적인 봉쇄로 전자금융거래로 인한 금전적 손실이 발생하지 않아야 한다. <표4-2>에서 ①전통적 보안기술은 시그내처라고 하는 패턴 DB와 블랙리스트 방식에 의하여 맬웨어의 예방, 진단, 치료가 수행됨에 따라 보안 위협이 부분적으로 남아 있거나, 상황에 따라 다른 솔루션의 추가 지원이 필요하기 때문에 보안 수준은 전반적으로 낮은 편이다.

②제안 기술은 Reverse Sandboxing 격리 기술과 Whitelist 방식, Trustzon의 아키텍쳐를 기반으로 설계된 커널 보안모드의 안전성으로 Endpoint상의 맬웨어는 온라인 거래가 수행하는 동안에 원천적으로 작동이 중단되며 별도의 하드웨어나 보안 솔루션이 필요하지 않으며 보안 수준이 높은 편으로 조사되었다.

<표4-2> 보안기술 비교

보안 솔루션 / 구분	전통적 또는 신기술 보안 솔루션 (Antivirus, Sandbox, 가상화)	제안기술 (SafeCentral: TSX, Reverse sandbox)
정의	악성코드 감염상태 제거(차단)로 깨끗한 컴퓨터 유지	악성코드의 활동상태를 중단시켜 안전한 브라우저 제공과 거래상태 유지
접근방식	Reactive	Proactive
예방/진단/치료	맬웨어 침입상황 분석하여 맬웨어 식별 룰과 시그네쳐 생성하여 실행시점 또는 시간 간격으로 점검(정적분석)	기존 컴퓨터 환경을 Reverse sandbox환경으로 전환하여 맬웨어의 활동을 중단시킴 (on-demand luck-down)
	맬웨어를 실시간으로 식별하기 위해 애플리케이션 및 데이터를 스캔하고 차단 (동적분석)	온라인 거래중 부당한 변경을 방지하기 위해 안전한 키보드와 브라우저 환경을 제공 (TSX)
기반 컨셉	Blacklist 방식	Whitelist 방식
패턴 DB 용량	지속적 증대	불필요
추가 자원	필요(백신관리 서버, 솔루션 등)	불필요
보안 수준	낮음	높음

(3)제안 기술의 보안 취약점 해결

일반 이용자가 본 기술을 직접 등록하여 사용할 경우 맬웨어가 감염된 소스를 화이트리스트에 포함시킬 수 있는 위험성이 있다. 그래서 본 기술의 도입은 기업이 담당하며 허용된 거래의 등록과 관리는 기업의 관련 시스템 담당자가 수행한다. 따라서 일반 이용자는 본 기술이 적용된 시스템을 활용만 하면 되기 때문에 직접 접근에 따른 보안 취약점은 해소 할 수 있다.

5. 결론과 향후 연구 방향

Endpoint의 사이버 공격 기술은 다양한 방식으로 점차 지능화 되어 최근에는 금전적 사기성 해킹까지 등장 했다. 그러나 기존 endpoint 보안 기술은 이용자 컴퓨터에서 악성코드를 완전히 제거할 수 없기 때문에 성능과 효과 측면에서 제한적이다. 본 연구의 제안 기술의 효과는 Reverse Sandboxing과 TSX 기술을 적용하여 개인의 컴퓨터에 감염되어 있는 맬웨어의 활동을 원천적으로 차단함으로써 피싱, 파밍, 메모리해킹 공격으로부터 고객의 데이터를 안전하게 보호할 수 있고 온라인 세션과 연계된 메인 시스템 운영에도 보안 수준을 한 단계 높일 수 있다.

앞으로 본 기술의 현장 검증 테스트를 마무리 하고 endpoint 환경을 포함한 광범위한 영역에 활용할 수 있도록 연구할 계획이다.

참고문헌

[1] 한국은행, 2014년 1/4분기 국내 인터넷뱅킹서비스 이용현황, 2014.5.15
[2] 한국인터넷진흥원, 2014년 5월 인터넷침해사고대응통계, 2014.7.22.
[3] 미래창조과학부, 신 변종 전자금융사기 합동 경보 발령, 2013. 8. 29
[4] 금융감독원, 신종 메모리해킹 전자금융사기 주의하세요, 2013. 9. 17
[5] 정태명, 엄정호, 한영주, 박선호, 사이버 공격과 보안기술, 2009. 1. 15
[6] 김정한,김지홍,신은환,엄영익, 가상화를 이용한 모바일 플랫폼 보안성 향상 기술, 정보보호학회, 2011.2
[7]Ashlesha Joshi, Samuel T. King, George W. Dunlap, and Peter M. Chen, Detecting Past and Present Intrusions through Vulnerability-Specific Predicates
[8] C. Willems, T. Holz, and F. Freiling. Toward automated dynamic malware analysis using cwsandbox. IEEE Security and Privacy, 5(2):32-39, 2007.
[9] Wan Huzaini Wan Hussin, Paul Coulton, and Reuben Edwards, Mobile Ticketing System Employing TrustZone Technology, 0-7695-2367-6/05,ⓒ 2005 IEEE
[10] Atul Verma, ARM 트러스트존 기술로 보안 시스템 구축, electronic science 2013. APR
[11] Ye Cao, Weili Han, Yueran Le, Anti-phishing Based on Automated Individual White-List, DIM' 08, October 31, 2008, Fairfax, Virginia, USA.
[12]Cyveillance, Malware Detection Rates for Leading AV Solutions, A Cyveillance Analysis August 2010
[13] Wontok, SafeCentral for Consumer, White Paper February 2012
[14] Chris K. Karlof, Umesh Shankar, Doug Tygar, David Wagner, Web authentication security against phishing, pharming, and active attacks, Technical Report No. UCB/EECS-2007-25, February 7, 2007