한국사물인터넷학회논문지 Vol. 5, No. 2, pp. 95-101, 2019 https://doi.org/10.20465/KIOTS.2019.5.2.095

사물인터넷 환경에서 시스템에 대한 비정상행위 방지 기법

이근호*
백석대학교 ICT학부 교수

A Scheme on Anomaly Prevention for Systems in IoT Environment

Keun-Ho Lee*
Professor, Div. of Information Communication Technology, BaekSeok University

요 약 4차 산업혁명시대와 사물인터넷의 시대로 접어들면서 다양한 서비스가 빠르게 성장하고 있으며 관련된 다양한 연구가 활발히 진행중에 있다. 그중에서도 사물인터넷에서 사용이 되고 있는 다양한 디바이스에 대한 비정상행위에 대한 연구도 진행이 되고 있다. 초연결의 사회에서 하나의 잘못된 디바이스로 인한 피해가 발생하면 다양하게 연결되어 있는 시스템에 심각한 영향을 줄 수 밖에 없다. 본 논문에서는 이러한 사물인터넷 환경에서 디바이스에 대한 안전성을 높일 수 있는 방법과 안전하게 디바이스와 서비스를 이용하 수 있는 방법에 대하여 안티디버깅 기법, 이상 프로세스 탐지 기법, 백도어 탐지 기법 등 여러 가지 비정상적인 행위로 인한 위협요소에 대응하기 위한 기법을 제안한다.

주제어 : 사물인터넷, 시스템, 비정상행위, 디바이스, 위협, 안티디버깅, 악성코드

Abstract Entering the era of the 4th Industrial Revolution and the Internet of Things, various services are growing rapidly, and various researches are actively underway. Among them, research on abnormal behaviors on various devices that are being used in the IoT is being conducted. In a hyper-connected society, the damage caused by one wrong device can have a serious impact on the various connected systems. In this paper, We propose a technique to cope with the problem that the threats caused by various abnormal behaviors such as anti-debugging scheme, anomalous process detection method and back door detection method on how to increase the safety of the device and how to use the device and service safely in such IoT environment.

Key Words : Internet of Things, System, Anomaly, Device, Threat, Anti-Debugging, Malware

1. 서론

최근에 가장 많은 연구가 이루어지고 있는 분야가 사물이터넷과 4차 산업혁명에 대한 연구일 것이다. 그중에서도 AI, 블록체인, AR/VR, 빅데이터, 클라우드, 드론 등 사물인터넷 시대로 접어들면서 다양한 디바이스를 통한 서비스가 활발히 개발이 되면서 새로운 서비스가 제공이 되고 있다. 이러한 시대적 변화에 따라서 사물인터넷 기반에서 제공이 되고 있는 다양한 시스템에 대한 안전성을 위한 연구가 비정상적인 행위에 대한 탐지 및 방어기술에 대한 연구가 중요한 기술로 자리매김하고 있다. 이러한 기술을 해결하기 위한 방법으로 윈도우 환경에서 안티디버깅(Anti-Debugging) 기술은 널리 사용되고 있으며, 최근 사물인터넷 기술과 다양한 서비스가 빠르게

본 논문은 2019년 백석대학교 학술연구에 의하여 지원되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2019년 10월 22일 수정일 2019년 12월 10일 심사완료일 2019년 12월 17일

성장하고 있다.

또한 블록체인 기술 및 이슈에 대한 관심도 높아지고 있다. 블록체인은 보안성과 신뢰성이 필요한 다양한 기술에 블록체인을 적용하고 있다. 블록체인의 구조 및 다양한 응용분야와 블록체인 기술을 활용하는 사물인터넷에 활용이 되도록 많은 연구가 진행이 되고 있다. 사물인터넷으로 발전하면서 안티디버깅의 기술을 통한 사물인터넷관련 프로그램에 적용하기 위한 노력들이 진행이 되고 있다. 안티디버깅이란 디버깅을 할 수 없게 만드는 것 인데 바이러스 파일에서도 많이 사용되어지고 있다. 왜냐하면 바이러스 파일을 분석하지 못하게 하기 위해 백신에서 뿐 만 아니라 바이러스 파일에서도 많이 사용되는 방법이다[1,2]. 또한 자신이 개발한 프로그램들을 분석하지 못하도록 안티디버깅 기법들을 많이 사용한다. 안티디버깅을 통한 방법과 그동안의 악성코드는 불특정 다수를 위한 악성코드로 한번 제작되면 최대한 많은 피해자를 만들어 금전적 이득과 개인정보 등의 데이터 획득에 목적이 있었다. 사물인터넷으로 확장시에도 이러한 악성코드는 다수의 사물인터넷을 구성하고 있는 각 디바이스에 피해를 주기 때문에 백신제작 업체도 해당 악성코드를 파악하고 빠르게 백신 룰(시그니처)에 추가하여 추가적인 피해를 차단하는 형식으로 진행하고 있다. 이러한 악성코드는 비교적 빠른 시일 내에 백신 룰이 만들어져 백신 솔루션을 사용하고 있는 기업은 피해를 빠르게 막을 수 있지만 최근에 진행되고 있는 APT 악성코드는 특정 목표를 달성하기 위해 만들어졌으며 불특정 다수가 아닌 특정 목표에게 악성코드 감염을 시도하고 공격자는 목표를 달성하기 위해 지속적으로 보안 솔루션 우회방법을 찾고 공격을 시도하기 때문에 APT악성코드는 백신 솔루션에서 탐지하기 힘들다. 이에 사물인터넷 환경에서의 악성코드의 특징을 이용해 기존 악성코드 및 APT악성코드를 빠르게 탐지 할 수 있는 연구도 필요하다. 본 연구에서는 사물인터넷의 비정상행위에 대한 연구를 위하여 안티디버깅과 악성코드에 대한 관련연구를 진행하고, 그에 따른 비정상행위에 대처하기 위한 방법으로 안티디버깅 기법, 이상행위 프로세스, 백도에 대한 탐지와 블록체인을 통한 대응기법에 대하여 제안한다.

2. 관련연구

2.1 안티 디버깅

- 안티 디버깅

안티 디버깅 기술은 분석하는 대상에 대한 프로그램을 디버깅을 하지 못하게 디버거를 강제로 종료하거나 에러를 발생하게 하는 방법을 이용하여 분석을 못하게 한다. 그렇기 때문에 이러한 기술이 적용되어진 악성코드 및 기타 프로그램들의 경우 분석가들에게 있어서 분석을 하기 어렵게 만든다. 때문에 매우 빠르게 분석을 하게 하기 위해서는 분석을 하려는 프로그램의 안티 디버깅 기술 적용 여부 및 해당 패턴을 자동으로 탐지하는 기술이 요구된다[1,2]. 또한 안티 디버깅의 종류에는 크게 Static 안티 디버깅과, Dynamic 안티 디버깅 기법이 존재한다.

- Static 안티 디버깅

Static 안티디버깅의 특징은 프로그램의 첫 실행에서 디버거를 탐지하는 것이다. 그 후에는 더이상 탐지하지 않는다. 즉, 안티 디버깅을 수행하는 함수가 호출 되는 시점에서만 디버거의 존재를 확인하고 그 뒤에는 탐지하지 않는다. 목적은 대부분 디버거의 탐지이다[3].

- Dyanmic 안티 디버깅

프로그램이 실행되는 중간중간 계속해서 디버거를 탐지하는 것이다. 프로그램의 실행과 함께 계속해서 실행되며, 중간중간 디버거의 유무를 확인하기 때문에 해제의 경우에도 지속적으로 해제가 필요하다. 목적은 내부 코드와 데이터를 숨기는 것 디버거를 탐지하는 것에 있다[3].

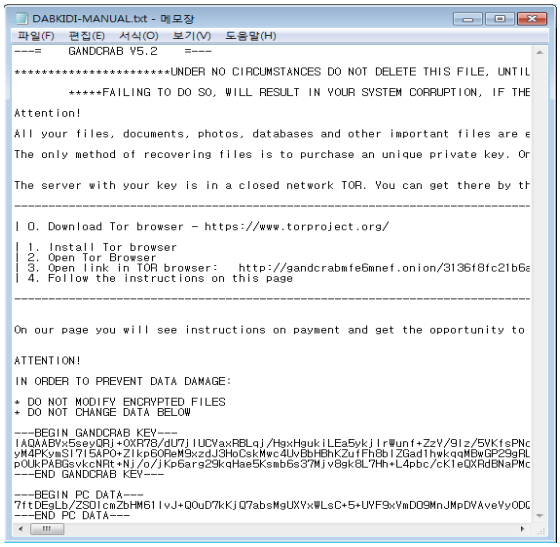
2.2 악성코드 관련

- APT 공격

APT(Advanced Persistent Threats)란 지능적 지속 위협공격으로 공격자가 특정 대상을 목표로 하나의 공격이 아닌 다양한 해킹 공격을 지속해서 시도해 피해를 주는 공격이다. 최근 APT 공격은 국가의 지원을 받으며 정교한 공격이 이루어지는 만큼 탐지하기 더욱 어려워지고 있다[4,5].

- 악성코드

악성 코드는 사용자의 의사와 관계없이 컴퓨터를 파괴하거나 정보유출, 금전탈취 최근에는 비트코인 탈취 등 악의적인 행위를 목적으로 만들어진 프로그램으로 종류에는 대표적으로 문서형 악성코드, 실행파일 악성코드 트로이 목마, 랜섬웨어 등 이 존재하고 사용자에게 금전을 갈취하기 위해 Fig 1과 같이 사용자에게 돈을 요구하는 메시지를 보내는 경우가 있다[4,5]. 이러한 프로그램들을 악성코드라 부를 수 있다.



[Fig. 1] Screen asking for money from user

2.3 블록체인

블록체인은 기존의 네트워크 방식이었던 P2P방식을 기반으로 데이터들이 해쉬암호화를 통한 체인형태의 연결고리 기반으로 분산 저장되어 있다. 블록체인은 기존의 중앙집중 방식인 데이터를 지속적으로 서비스 참여자들에게 모두 전송하고 데이터 내역을 중앙에서 관리하는 것이 아닌 각 이용자들이 보관하는 형태로 저장하는 탈중앙화 기술이다[6,7]. 블록체인은 변조를 판단하기 위하여 정보들을 모은 블록의 방법으로 해쉬를 만드는데 해쉬를 만들 때마다 이전 블록의 해쉬값을 입력하여 현재 블록의 해쉬를 만들어 영향을 끼치게 한다. 블록체인은 중앙관리체제로 운영되는 클라우드와 비교되는 네트워크의 구조이고 분산형 구조 형태로 모든 데이터 정보를 가지고 있다. 또한 중앙 서버에 모든 정보를 처리하는 클라우드 방식과는 다른 네트워크 방식으로 동작한다. 블록체인은 데이터 정보를 하나에만 저장하지 않고 여러 곳으로 분산하여 분산된 형태로 배치되기 때문에 데이터가 변조될 가능성은 매주 낮으며 중앙서버에서 관리하는 형태가 아니기 때문에 사용자의 모든 데이터 정보를 가지고 있으며, 중앙체제에서는 서버에 저장한 정보를 보호하기 위하여 시스템들을 보안하여 운영한다. 그러므로 정보를 서버에 저장하는 방식 및 보안에 필요한 인력의 유지비용으로 소모하게 된다. 블록체인의 방식은 중앙관리체제가 필요하지 않은 방식이라서 중앙서버에서 소모되는 유지비용이 적게 든다[10-12].

2.4 사물인터넷 시스템 관리의 보안성

블록체인에서 각 사용자에게 해쉬 값 기반의 공공키가 아이디로 부여되며 트랜잭션에 사용된다. 익명성을 사용해 기기 소유자의 프라이버시를 보호한다는 장점이 있다. 또한 사물인터넷 기기 관리의 보안성에 블록체인을 적용한 방식들은 각 사물인터넷 시스템이 주기적으로 블록체인에 트랜잭션을 생성한다는 공통점이 있다. 하지만 블록체인은 한 블록에 저장될 수 있는 트랜잭션 데이터의 양이 제한되어있다. 트랜잭션 처리량을 늘리기 위해 블록을 크게 만들면 블록을 브로드캐스팅하기 때문에 네트워크 트래픽이 증가한다. 따라서 사물인터넷 시스템이 생성하는 트랜잭션을 효율적으로 수용할 수 있는 연구가 필요하다[11,12].

2.5 백도어

백도어란 시스템에 비인가 접근 시도 프로그램을 의미한다. 일반적으로 공격으로 루트권한을 얻은 후 차후 접근 용이를 위해 설치하는 프로그램이다.

최근에는 미국 NSA, 삼성전자, 샤오미, 애플 등 특정 국가 및 해당 국가의 기업에서 악의적 목적으로 백도어를 사용한다는 의심 사례들이 있다. 대표적인 백도어의 종류는 아래와 같다[13-16].

- 로컬 백도어

서버의 셀을 얻어낸 뒤에 관리로 권한 상승을 할 때 사용하는 백도어이다.

- 원격 백도어

원격에서 관리자로 계정과 패스워드를 입력하고 로그인한 것처럼 바로 시스템의 관리자 계정을 할 수 있는 백도어이다.

- 패스워드 크래킹 백도어

인증을 회피 한다기 보다는 인증에 필요한 패스워드를 원격지의 공격자에게 보내주는 역할을 하는 백도어이다.

- 트로이 목마형

처음부터 백도어를 목적으로 만들어진 프로그램이 아닌데도 백도어로 동작하는 경우 윈도우에서는 웹 브라우저나 명령창, 간단한 게임등도 백도어와 섞을 수 있다.

3. 사물인터넷에서 비정상행위 방지기법

3.1 안티디버깅 적용 기법

Fig 2는 사물인터넷에서 비정상행위를 하지 못하도록 하는 방법을 구현한 결과이다. 안티디버깅을 적용하여 각 사물인터넷 관련 프로그램마다 안티디버깅을 적용하는 방법이다. 사물인터넷에서 프로그램마다 안티디버깅 적용은 PEB, NtQueryInformationProcess(), FindWindow() NtQueryObject(), ZwSetInformationThread()을 이용하여 제안하여 적용하는 기법이다.

- PEB(Process Environment Block)

현재 프로세스의 디버깅 여부를 알기위해 PEB 정보를 이용한다. 정보를 신용할 수 있으며 사용하기 편하기 때문에 가장 널리 사용되는 안티 디버깅 기법이다. 안티 디버깅 기법에서 사용되는 PEB구조체에서 멤버는 BeingDebugged, Ldr, Proess Heap, NtgloblFlag을 이용하는 기법을 제안한다.

· BeingDebugged

PEB.BeingDebugged 멤버의 값은 디버깅 중일 때 1로 세팅 되고 일반 실행인 경우 0으로 세팅 되는 점을 이용하여 디버깅 탐지 및 회피를 할 수 있다.

· Ldr

디버깅 프로세스는 힙 메모리 영역에 디버깅 당하는 프로세스라는 표시를 한다. 힙 메모리에 사용하지 않는 영역을 0xFEEEFEEE 라는 값으로 채운다는 점을 이용하여 탐지 및 회피를 할 수 있다.

(window XP 이상에서는 사용할 수 없다.)

· Process Heap

PEB.ProcessHeap 멤버는 HEAP 정보를 가리키는 포인터이다. HEAP 구조체중 Flags 멤버와 ForceFlags 멤버는 디버깅 중에 특정한 (Flags = 2, ForceFlags = 0이 아닌값) 값으로 설정 되기 때문에 이를 이용하여 탐지 및 회피를 할 수 있다.

(window XP 이상에서는 사용할 수 없다.)

· NtglobalFlag

프로세스가 디버깅 중일 경우 PEB.NtGlobalFlag 멤버의 값은 0x70으로 세팅이 되는데 이 값을 이용하여 디버깅 여부를 판단한다.

- NtQueryInformationProcess()

ntdll!NtQueryInformationProcess() API를 사용하면 프로세스의 디버깅 관련 정보를 비롯하여 다양한 정보를 얻을 수 있다. 디버거 탐지에 사용되는 것은 아래와 같다.

· ProcessDebugPort

프로세스가 디버깅 중일 경우 Debug Port가 할당되는데 이 값을 이용하여 디버거 탐지에 사용할 수 있다.

· ProcessDebugObjectHandle

디버깅 여부를 판별해 주는 함수이다. 이 함수를 이용하여 디버깅을 판별 할 수 있으며 함수를 분석하여 변경함으로써 회피를 할 수 있다.

· ProcessDebugFlags

프로세스가 디버깅 될 때 Debug Object가 생성되는데 이것을 이용하여 디버깅 여부를 판단하고 응용하여 회피를 한다.

- NtQueryObject()

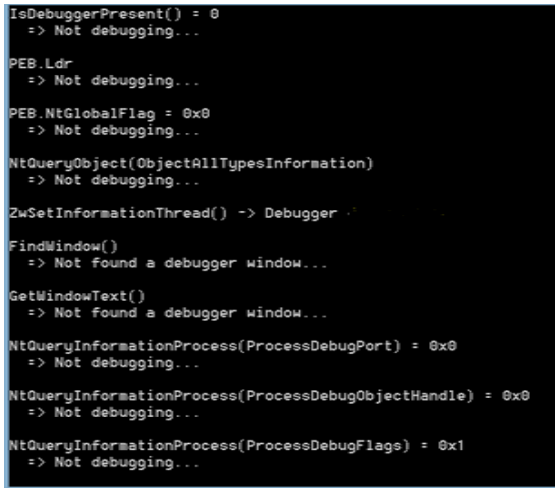
시스템에 디버거가 다른 프로세스를 디버깅 중이면 그 때 DebugObject 타입의 커널 객체가 생성이된다. 이때 그 DebugObject의 여부를 확인하는 것이다. ntdll!NtQueryObject() API 는 시스템 환경의 다양한 커널 객체 정보를 가져오는 함수이다.

- ZwSetInformationThread()

디버깅 당하는 쪽(디버거)에서 강제로 디버거를 떼어내는 방법에 대한 설명이다. ZwSetInformationThread() API를 이용하여 자신을 디버깅하는 디버거를 떼어낼 수 있다. (window XP 이상에서는 사용할 수 없다)

- FindWindow()

FindWindow()를 이용하여 대표적인 디버깅 프로그램 이름들을 검색하여 확인할 수 있는 방법이다.

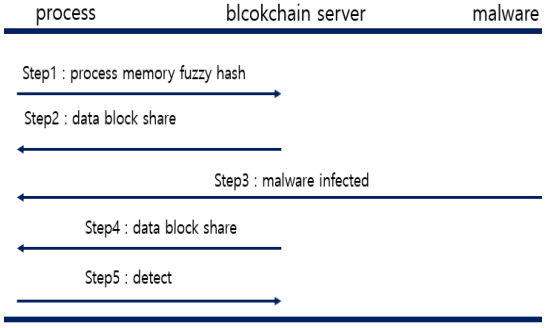


[Fig. 2] result of implementing anti-debugging

3.2 블록체인을 적용한 악성프로세스 탐지 기법

Fig 3은 블록체인을 적용하여 악성코드를 탐지하는 기법으로서 퍼지해쉬를 이용하여 해쉬를 통한 데이터에 대한 블록체인화를 하는 기법으로 블록체인의 투명성에 기반을 한 탐지 기법을 제안한다. 사물인터넷에서의 프로

세스란 사물인터넷의 프로그램이 저장장치에 저장되고 프로그램을 실행할 때 실질적으로 메모리에 올라가 CPU에서 처리할 수 있는 상태를 말하는데 프로그램이 실행될 때 프로세스로 올라가 실행되는 것이 특징이다. 이는 악성코드도 프로그램으로 작동함으로 프로세스에 올라가 실행됨을 의미하는데 악성코드는 프로세스에 올라가야 실질적인 악성 행위를 진행한다. 또한 악성프로그램이 실행된 이후 대부분의 악성코드들은 프로세스에 지속적으로 상주하는 경우가 많다. 이를 탐지하기 위해 블록체인 기술을 이용한 이상 프로세스 탐지기법을 제안한다.



[Fig. 3] malicious process detection using blockchain

Step1 : 프로세스 덤프를 퍼지 해쉬를 이용하여 해쉬화 이후 데이터 블록을 전송한다.

Step2 : 각각의 블록체인 서버에서 블록을 공유하여 프로세스 덤프 유사도 비교를 진행한다.

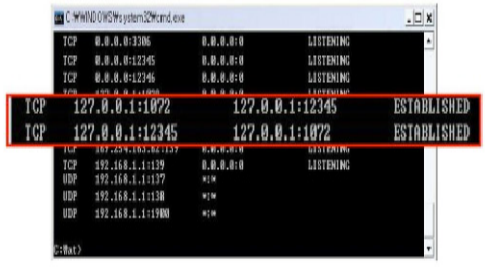
Step3 : 악성코드가 컴퓨터 메모리에 악성코드를 실행 한다.

Step4 : 지속적으로 블록체인 서버에서 공유된 데이터를 이용하여 이상프로세스 존재 유무를 검사 한다.

Step5 : 이상프로세스가 존재하면 즉시 블록체인 서버에 이상프로세스가 탐지되었다는 데이터를 보내고 보안 담당자 또는 CERT팀에서 탐지한다.

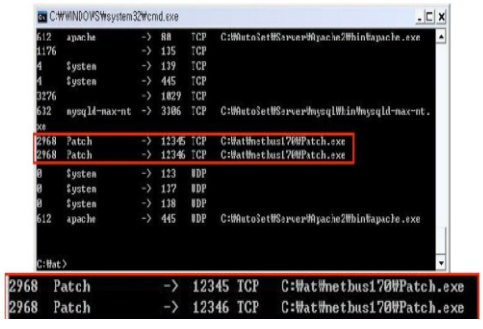
3.3 백도어 탐지 기법

백도어의 다양한 공격에 맞추어 다양한 기능을 수행할 수 있는 백도어 탐지기법을 제안한다. 제안 기법은 사물인터넷 프로그램에서 열린 포트 확인 및 닫기, SetUID파일 검사, 바이러스 및 백도어 탐지툴 검사, 파일에 대한 무경성 검사, 로그분석을 통해 일반유저가 접근하기 힘든 시스템 분석을 사용자 인터페이스에 맞춰 쉽게 접할 수 있도록 구성하는 방법이다. 적용하는 기법에서 기능효과로는 열린 포트를 확인하기 기능을 통해 현재 내 PC에 열려 있는 포트를 Fig 4와 같이 확인할 수 있고 Fig 5에서 응용프로그램이 사용하는 포트를 제외한 나머지 포트를 확인하여 사물인터넷에서의 소유한 디바이스가 백도어 공격에 노출되어 있는지 확인할 수 있고 열린 포트 닫기 기능을 제공하여 백도어의 노출 위험이 있는 포트를 닫아 공격의 위험성을 줄일 수 있는 기법이다.



[Fig. 4] check open ports

SetUID는 일시적 권한 상승을 통해 root 권한을 획득하는 방법으로 SetUID파일 검사를 통해 위험성 있는 파일을 검사하여 삭제함으로써 위험을 줄일 수 있다.



[Fig. 5] check the port used by the application

제안하는 기법은 사물인터넷에서 주로 이용이 되고 있는 컴퓨터, 노트북, 스마트폰 등 전자기기에서 개인정보뿐만 아니라 다양한 정보들이 많이 포함되어 있는데 이러한 정보들이 해킹으로 인해 유출이 될 수 있다. 해킹 공격은 시간이 지날수록 어려운 공격들이 생겨나고 있기 때문에 보안에 문제점이 많이 생기고 있다. 하지만 해킹에 대한 위험성은 인지하고 보안의 중요성을 깨닫게 되면 개인이 해킹의 대해 조심성이 생기고 보안의 유지를 할 수 있게 된다. 또한 현재 이메일로도 해킹이 되고 있는데 발신자가 명확하지 않는 경우와 확인이 되지 않은

URL를 조심해야 되며 주기적으로 백업을 진행함으로써 다양한 정보를 지키고 주기적으로 백신프로그램의 보완이 필요하다.

4. 제안 기법에 대한 안전성 분석

본 논문에서 제안하는 사물인터넷 기반에서의 비정상행위를 방지하기 위한 방법으로 제안하고 있는 안티디버깅, 블록체인 적용 이상프로세스 탐지, 백도어 탐지 기법을 통한 각 탐지 기법에 대한 사물인터넷 환경에서의 안전성에 대한 부분을 살펴본다.

- 안티디버깅 관련 안전성

사물인터넷에서 비정상행위를 하지 못하도록 하는 방법으로 구현이 되어 각 사물인터넷 관련 프로그램마다 안티디버깅을 적용시에 사용되는 하는 방법 PEB, NtQueryInformationProcess(), FindWindow() NtQueryObject(), ZwSetInformationThread()을 이용하여 프로그램에 대한 변경이 이루어지지 않으므로서 사물인터넷에서의 안전성을 높일 수 있다.

- 블록체인을 적용한 악성코드 관련 안전성

악성코드에 대한 행위를 탐지하거나 악성코드를 대응하기 위한 기법으로 제시한 프로세스 덤프를 퍼지 해쉬를 이용하여 해쉬화 이후 데이터 블록으로 처리하고, 각각의 블록체인 서버에서 블록을 공유하여 프로세스 덤프 유사도 비교를 진행하면서 악성코드가 컴퓨터 메모리에 악성코드를 실행하는 과정에 대해서 지속적으로 블록체인 서버에서 공유된 데이터를 이용하여 이상프로세스 존재 유무를 검사하여 이상프로세스가 존재하면 즉시 블록체인 서버에 이상프로세스가 탐지하는 과정을 통하여 무결성과 기밀성을 보장하고 있다.

- 백도어 탐지 관련 안전성

사물인터넷 프로그램은 열린 포트 확인 및 닫기, SetUID파일 검사, 바이러스 및 백도어 탐지툴 검사, 파일에 대한 무결성 검사, 로그분석을 통해 백도어 공격에 노출되어 있는지 확인할 수 있고 열린 포트 닫기 기능을 제공하여 백도어의 노출 위험이 있는 포트를 닫아 공격의 위험성을 줄일 수 있는 기법을 제안하여 사물인터넷 환경으로 변화에서 안전성을 높여준다.

5. 결론

사물인터넷 시대에 모든 IT관련 분야의 안전성에 대한 전망을 100% 예측하는 것이 어렵지만 사회적인 측면을 보면 웜, 바이러스 같은 악성코드가 증가하고 있으며, 한국의 사물인터넷 관련 서비스의 확대로 인해 보안의 중요성이 증가 하고 있다. 이에 사물인터넷 환경에서의 악성코드의 특징을 이용해 기존 악성코드 및 APT악성코드를 빠르게 탐지 하는 방법과 사물인터넷환경에서 디바이스를 통한 서비스에서 비정상행위에 대한 연구도 필요하다. 본 연구에서는 사물인터넷의 비정상행위에 대한 연구를 위하여 안티디버깅과 악성코드에 대한 관련연구를 진행하고, 그에 따른 비정상행위에 대처하기 위한 방법으로 안티디버깅 기법, 이상행위 프로세스, 백도에 대한 탐지와 블록체인을 통한 대응기법에 대하여 제안하였다.

REFERENCES

[1] J.W.Park and Y.S,Park, “An automatic detection scheme of anti-debugging routines to the environment for analysis,” Proc. Control Conference, p.2, 2014.

[2] H.M.Kwak, T.H.Lee, G.N.Kim, J.W.Cho and K.H.Lee, “A Scheme for Avoidance through Anti-debugging Program”, The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.55-57, 2019.

[3] p3ngdump's study blog. p3ngdump, June. 15. 2016, "https://p3ngdump.tistory.com/56".

[4] H.N.Kim, “Real-time hybrid analysis based on multiple profile for prevention of malware,”Hongik University Graduate School: Department of Information Security, 2014.

[5] JH.Choi, K.H.Lee and S.H.Yun, “Abnormal Process Detection Using Blockchain”, The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.67-68, 2019.

[6] E.G.Hong, S.J.Lee and S.H.Seo, “Blockchain Technology Trends for the Internet of Things“, Journal of Information Security, Vol.9, No.1, pp.38-46, 2018.

[7] J.H.Choi, K.H.Lee and S.H.Yun, “Abnormal Process Detection Using Blockchain”, The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.67-68, 2019.

[8] H.Y.Kim, “Analysis of Security Threats and Countermeasures on Blockchain Platforms,” Korean Institute of Information Technology, Vol.16, No.5, pp.103-112, 2018.

[9] H.J.Chu, I.H.Song and B.G.Choi, “A Decentralized Test Management Tool Based on Blockchain Technique,” The Korean Institute of Information Scientists and

Engineers, Vol.25, No.7, pp.321-328, 2019.

[10] J.H.Hong, K.H.Lee and S.H.Yun, "A Scheme for ECU Application Technique using Blockchain", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.34-35, 2019.

[11] T.Hardjono and N.Smith. "Cloud-based commissioning of constrained devices using permissioned blockchains." IoTPTS '16 Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 2016.

[12] J.H.Yang and K.H.Lee, "A Scheme for Application of Internet of Things and Blockchain Technology", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.75-76, 2019.

[13] J.T.Kim, J.H.Kho, M.S.Hong, C.W Son, B.Park, D.W.Lee and G.Lee "A Study on Intrusion Protection Techniques against Linux Kernel Backdoor", The Journal of The Institute of Webcasting, Internet Television and Telecommunication, Vol.9, No.3, pp.201-207, 2009.

[14] S.J.Park, G.S.Go, J.H.Cho and, K.H.Lee, "A Scheme for Anomaly Process Detection Using Blockchain", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.24-25, 2019.

[15] Wikipedia, "chkrootkit", https://ko.wikipedia.org/wIki/Chkrootkit

[16] J.H.Hong, J.W.Kim, C.J.Kim and, K.H.Lee, "Security Techniques for Various Hacking Using Kali-Linux", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.61-62, 2019.

이 근 호(Lee, Keun Ho) [종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 ICT학부 부교수

〈관심분야〉

이동통신 보안, 융합보안, 개인정보보호