Journal of The Korea Society of Computer and Information
Vol. 24 No. 4, pp. 65-71, April 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.04.065

A Study on Privilege Elevation Attack Management for Smart Transaction Security on BlockChain Etherium Based System

Youn-A Min*

Abstract

IAs smart device penetration rate is more than 90%, mobile transaction ratio using smart device is increasing. Smart contracts are used in various areas of real life including smart trading.

By applying smart contracts to the platform for smart transactions through block-chain technology, the threat of hacking or forgery can be reduced.

However, various threats to devices in smart transactions can pose a threat to the use of block chain Etherium, an important element in privilege and personal information management.

Smart contract used in block chain Ethereum includes important information or transaction details of users. Therefore, in case of an attack of privilege elevation, it is very likely to exploit transaction details or forge or tamper with personal information inquiry.

In this paper, we propose a detection and countermeasure method for privilege escalation attack, which is especially important for block chain for secure smart transaction using block chain Ethereum.

When comparing the results of this study with the results of similar applications and researches, we showed about 12~13% improvement in performance and suggested the future countermeasures through packet analysis.

▸Keyword: Blockchain, Ethereum, privilege elevation

I. Introduction

스마트 디바이스의 확산에 따라 스마트 거래의 비율이 점차 증가하고 있다. 2018년 통계청에 의해 발표된 온라인쇼핑동향 보고서에 의하면 전체 전자상거래 금액은 10조 6,293억이고 그중 스마트 거래는 6조 5,967억이다. 이는 전체 거래의 62.1%에 해당한다[1].

스마트 디바이스를 이용한 스마트 거래의 비율이 증가하면서 개인정보 보호와 거래의 투명성 등에 대한 관심이 높아지고 있다. 지난 2008년부터 블록체인 기술이 적용되기 시작하여 스마트 거래 등 다양한 거래 트랜잭션에 대한 투명하고 정확함을 높이고 있다. 블록체인 기술은 분산 시스템을 활용하여 공유하고 있는 모든 사용자에게 분산원장을 보유하게 하고 확인토록 하는 기술이다[2]. 블록체인 기술은 관리주체와 데이터 접근 및 거래증명에 따라 Public, Private, Consortium 블록체인의 형태로 분류되며 블록체인 기술의 투명성 등을 실생활에 활용하기 위하여 금융, 무역, 투표 등 여러 분야에 해당기술을 적용하고 있다[2]. 국내에서는 2018년에 공공 블록체인 시범사업 6개가 지정되어 관세청, 농림수산부 등에서 데이터를 블록체인 기술로 처리하는 기술을 개발하기 시작하였다[3].

본 논문에서는 블록체인 Ethereum 기반 안전한 스마트 거래를 위하여 거래 트랜잭션의 투명성과 개인정보 보호를 위한 방법으로 스마트 디바이스의 권한상승 공격에 대한 효과적인 탐지 및 대응방법을 제안하였다.

• First Author: Youn-A Min, Corresponding Author: Youn-A Min
*Youn-A Min (yah0612@gachon.ac.kr), Dept. of software, Gachon University
• Received: 2019. 02. 20, Revised: 2019. 03. 26, Accepted: 2019. 04. 11.

II. Preliminaries

1. Related works

1.1 Smart trading

2018년 통계청을 통하여 발표된 '2018 온라인 쇼핑동향'에 의하면 2018년 온라인 쇼핑 전체 거래액은 10조 6,293억 원이고 그 중 스마트 거래는 2017년 대비 28% 증가한 6조 5,967억으로 보고되었다[1]. 스마트 거래의 대부분은 스마트 디바이스를 통한 서비스, 생활 등에 대한 것이며 간편한 결제와 스마트 디바이스의 확산에 따라 점유비율이 높아지고 있다.

Table 1은 2018년 정보통신정책연구원에서 발표한 국내 스마트 거래 시장규모를 나타낸 것이다.

Table 1. Smart trading market growth rate forecast[4]
(unit : 100 Million won)

Year	amount	growth rate
2017	782,000	-
2018	934,000	19.44%
2019(e)	1,115,000	19.38%
2020(e)	1,331,000	19.37%
2021(e)	1,590,000	19.46%
2022(e)	1,898,000	19.37%

Table 1에 따르면 평균 19% 이상의 시장규모 증가를 예측할 수 있다[4]. 이에 따라 스마트 거래 시 발생하는 트랜잭션의 무결성과 투명성의 보장에 대한 사용자의 요구는 증가하고 있다.

1.2 Blockchain Etherium and Use case

Blockchain은 여러 개의 트랜잭션을 일정시간마다 하나의 블록으로 구성하여 여러 개의 블록을 체인으로 연결하는 데이터 구조이다[5].

Blockchain 기술은 암호화폐의 역할을 하는 비트코인을 시작으로 Smart Contract가 가능한 Etherium 기술 등으로 발전하고 있다. Blockchain은 분산과 독립, 개방이라는 큰 특징을 가지고 있으며 이러한 특징은 해시함수, public key와 private key를 통한 전자서명과 암호화 등의 기술을 통하여 구성 된다. Blockchain은 분산형 인프라를 구축하고 PC와 스마트 디바이스를 통하여 다양한 분야로 사용되는 분산 장부를 가진다. Blockchain을 승인범위에 따라 세 가지 형태로 나눌 수 있다. 누구나 참여가능하고 승인해야하는 Public 형태와 중앙기관이 모든 권한을 보유하고 허가받은 일부의 승인이 필요한 Private 형태, 소수 기업이 컨소시엄을 운영하고 컨소시엄에 소속된 참여자에 의해 관리되는 Consortium 형태이다[3].

최근 스마트 거래에 Blockchain 기술이 적용되면서 Pubic 형태부터Consortium 형태까지 다양한 형태로 기 적용되고 있다.Blockchain 기술의 특징인 익명성, p2p, 확장성, 투명성, 보안성, 시스템 안정성에 대한 활용 범위 스마트거래에 적용되면서 거래의 투명성과 정확성에 대한 신뢰도 높아졌다[6].

Table 2는 2018년 정보통신산업진흥원에서 발표한 Blockchain 기술 특징과 기존 기술 대비 장.단점을 정리한 것이다.

Table 2. Characteristics of Blockchain[6]

Divide	Merits	Demerits
Anonymity	No personal information required / Provides high anonymity compared to payment methods such as bank account and credit card	Possible to settle illegal transaction price
p2p	p2p deals without authorized third parties	Accountability obscurity
Scalability	Easily build and connect by open source	Actual size of transactions in the economy
Transparency	Disclosure and access to all transaction records / Cultivating transactions	Track all transactions
Security	Joint ownership of the book / Reduced security related costs	Hacking of private keys, no solution when lost
System stability	Single point of failure does not exist	Real-time, large capacity difficulty

핀테크, 관세청의 전자상거래계획, 투표 등 실생활의 Blockchain 기술의 활용분야는 매우 다양하다.

Blockchain기술을 핀테크 등에 적용하면서 기존 공인인증서 등으로 관리되었던 온라인 금융거래가 보다 투명하고 보안이 강화된 형태로 관리 가능하였다. Blockchain을 활용하여 2018년 12월 관세청은 Blockchain 전자상거래를 구축하였고 전자상거래업체와 배송업체간의 데이터를 Blockchain 장부를 만들었다. Blockchain을 통한 분산 장부를 통하여 거래 내역을 동시에 확인하는 작업이 가능하여 기존에 여러 차례 통관절차를 거쳤던 거래 프로세스가 간소화, 투명화 되었다. 전자상거래분야에 적용된 Blockchain기술을 통하여 일평균 36000건이었던 통관처리량이 3.5배 이상 늘어날 것으로 전망하고 있으며 1건 처리 당 5일 이상 걸렸던 절차가 2일 이내로 줄어들 수 있다[7]. 이 외에도 농축산물 생산 이력 등의 조회도 Blockchain을 통하여 확인가능하다.

Table 3은 2016년 세계적인 회계법인 언스트앤영에서 조사한 Blockchain 적용 시나리오의 일부이다. 아래 표를 살펴보면 금융, 자동차, 의료정보, 디지털콘텐츠 등 방대한 분야에 대한 Blockchain 기술의 활용 시나리오를 예측할 수 있다[8].

Table 3. Scenario using Blockchain technology[8]

Application field	Utilization plan
Financial Services	Fast settlement of stocks, bonds, etc. and low transaction costs
Medical information ecosystem	All medical information connected to patient, hospital, etc.
Digital copyright protection	Record the usage history of music files in a public Blockchain, etc.

Blockchain을 사용한 스마트거래 활용사례 중 대표적인 것으로 5Miles의 사이버마일즈(CyberMiles)를 들 수 있다.

5Miles는 위임지분증명(DPos) 기반 사이버마일즈 암호화폐를 활용하여 2019년부터 Etherium Smart Contract 기반의 전자상거래 시스템 구축 계획을 세우고 2018년 10월 메인넷을 시작하였으며 총 7억 6,500만개의 유통량을 계획하고 있다[9].

Smart Contract를 기반으로 일정 코인을 사이버마이즈에 예치하면 마스터노드로써 권한을 가지고 거래의 투명성과 거래확인에 참여할 수 있다[10].

이 외에도 Blockchain Etherium 기술을 활용한 다양한 스마트 거래에 대한 시도가 각 지자체단위로 계획되고 있다.

Blockchain 기술 자체는 합의와 해시 등의 기술로 해킹이 쉽지 않다. 하지만 거래 플랫폼이 되는 스마트 디바이스에 대한 다양한 공격에 대한 위협은 다양화되고 증가하고 있다

다음 절 에서는 스마트 디바이스에서 발생 가능한 다양한 위협과 연구사례에 대하여 알아본다.

1.3. Smart Device Threat Factors

가트너의 2018년 android's rise to smartphone dominance 발표에 의하면 전체 스마트 디바이스 중 86%가 안드로이드 OS기반이다[11].

보안 솔루션 기업인 맥아피(Mcaffe)가 발표한 악성코드 위협 보고서의 내용 중 2015-2017까지의 악성코드 증가 추이부분을 살펴보면 2017년 3분기 기준 악성코드는 21,000,000개 이상으로 이 중 감염 기종의 81%는 안드로이드 OS 기반인 것으로 나타났다[12].

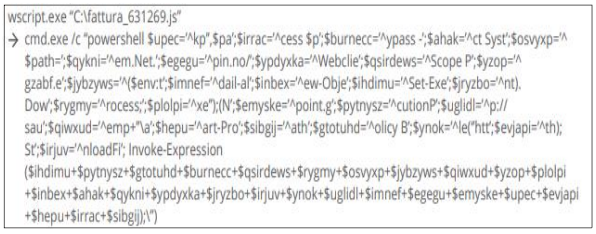

Fig. 1. Infection code through packing file[12]

안드로이드 OS는 개인정보 수집 및 유출, 권한상승 등의 위협이 있으며 그 중 권한상승 공격은 사용하는 프로그램의 코드 취약점을 이용하여 중요 권한을 획득하는 유형이다.

권한상승 공격을 통하여 악의를 가진 사용자는 파일시스템 내의 중요 정보에 접근하여 개인의 주요정보를 유출하고 원격제어를 통하여 또 다른 권한에 대한 접근을 시도할 수 있다.

Blockchain Etherium 기술을 사용하여 각 사용자가 각각의 합의 및 허용 권한을 가지고 Smart Contract를 할 경우 권한상승으로 인한 개인정보공격 및 위변조는 거래의 신뢰성과 무결성 유지에 큰 이슈가 될 수 있다.

Table 4는 Jiang의 연구에서 정리한 안드로이드 악성코드 유형의 분류이다[13,14].

Table 4. Malicious code type classification[13,14]

Division	Attack means
Elevation attack	Gingerbreak, Asroot etc
Charge	Phone call, SMS etc
Remote control	SMS, Net etc
Personal Information extrusion	Number, User Account etc

Fig.2는 스마트 디바이스 다양한 악성코드 공격에 대한 TraintDroid, Aurasium의 대응사례를 보여준다.

권한상승 공격의 대응방법에 대한 기존 연구 중 TraintDroid 는 다양한 Layer에 대한 공격 시 file level과 method level 및 variable level의 tracking이 가능하다[15].

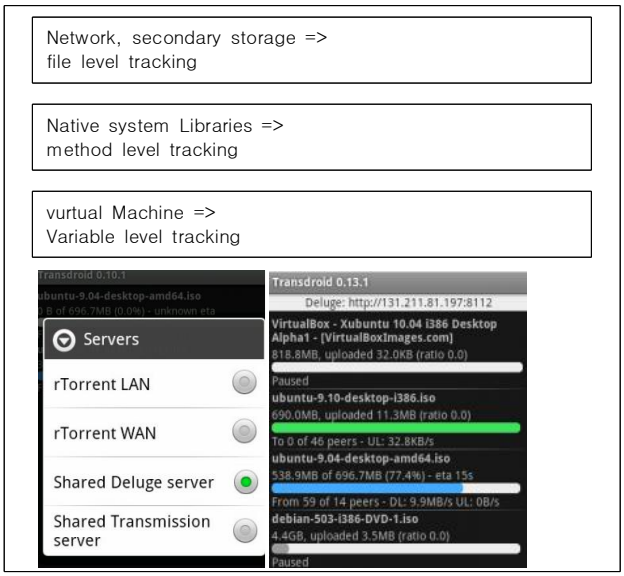

Fig. 2. TraintDroid layer correspondence[15]

Fig.2와 같이 TraintDroid는 개인정보추적을 위한 단계별 architecture 구조를 제시하지만 권한상승 공격 등에 대한 tracking 및 대응은 불가하다.

Aurasium 역시 스마트 디바이스를 통한 RPC request 시 IPC를 통한 answer를 처리하는데 해당 과정 중 발생 가능한 악성행위를 Fig.3과 같이 대응할 수 있다. 하지만 Aurasium은 스마트 디바이스에서 발생하는 악성행위에 대하여 모니터링하고 대응하기 위한 방법이나 유저 레벨의 모니터링 기법을 사용하기에 재패키징 및 권한상승 공격 등에 대해서는 적절하게 대응하기 힘들다[16].

Fig. 3. Aurasium layer correspondence[16]

이 외에도 시스템함수 후킹 등을 통하여 시스템 함수를 통한 동작여부파악 후 대처 방법 등이 있으나 read/write 시간에 대한 오버헤드가 크고 대응에 대한 방법이 시스템 콜 확인 등으로 국한하고 있다.

본 논문에서는 Blockchain Etherium 기반의 스마트 거래 시 요청되는 권한 관련, 권한상승공격에 대한 위협을 가진 코드인지 사전 탐지하고 의심되는 코드에 대한 시스템 내,외부적 대응을 연구하였다. 이를 위하여 안드로이드 바인더 드라이브의 ioctl() 함수의 메타데이터를 관리하여 권한상승공격을 탐지하고 의심코드에 대한 패킷 분석을 통하여 중요정보와 트랜잭션을 보호하고 거래의 투명성과 무결성을 보장하고자 한다.

III. Privilege Elevation Attack Management for Smart Transaction Security on Block Chain Etherium Based System Scheme

본 논문에서는 Blockchain Etherium을 사용한 스마트 거래를 가정하고 거래 시 발생 가능한 다양한 위협 요소 중 권한상승 공격을 중심으로 바인더 드라이브를 활용하여 악성코드를 미리 탐지하고 대응할 수 있는 방법을 제안하였다.

또한 의심 코드에 대한 대응을 위하여 패킷분석을 실시하였다.

1) 스마트 트랜잭션 처리를 위한 권한상승공격 관리방법

본 연구를 위하여 Blockchain 구축 후 샘플 트랜잭션에 대한 smart contract를 작성하고 스마트 거래 시 발생 가능한 권한상승 공격에 대한 샘플 코드를 삽입한 후 제안한 연구 내용을 토대로 처리하는 과정을 Fig.4와 같이 정리하였다. Blockchain private system을 구축한 후 Sample malware를 추가하여 escalation attack이 발생된 상황을 예측하고 function call을 통한 ioctl()수정과 모니터링을 통하여 malware를 checking 하는 과정이다.

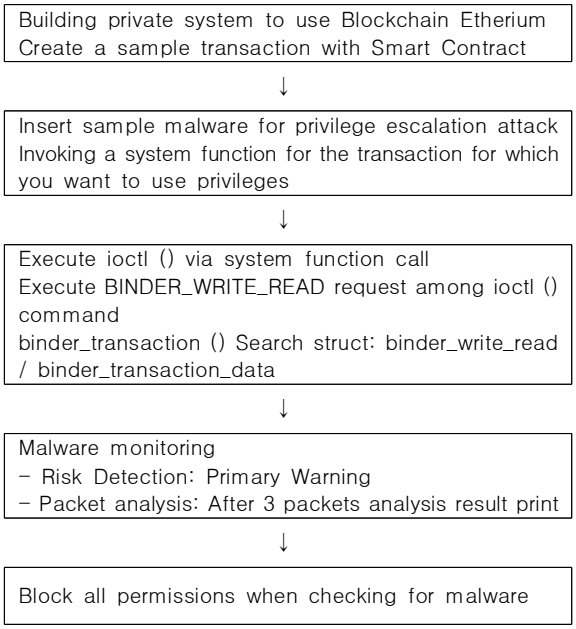

Fig. 4. processing process

해당 과정 중 binder_transaction()의 buffer처리를 위하여 target_handle과 BR_REPLAY를 검색하고 모듈을 추가하여 위협적인 요소를 처리한다. 해당 내용에 대한 세부처리 과정은 Fig.5와 같다. 해당과정을 통하여 write_buffer안의 BC_REPLAY를 세팅하고 taget_handle과 BR_REPLAY를 검색한 후 module을 추하여 malicious code에 대하여 판단하게 된다.

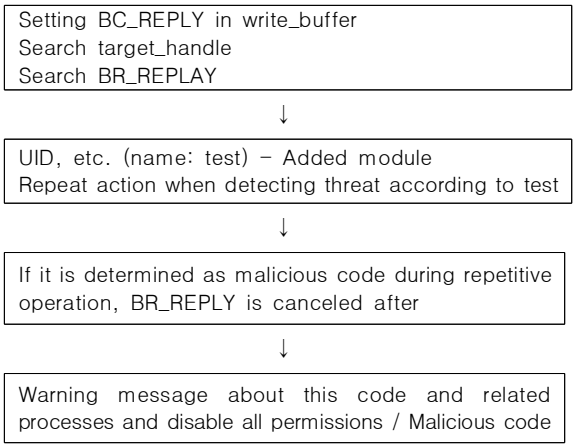

Fig. 5. binder_transaction detail processing

위의 Processing 중 read와 write의 buffer에 대한 struct 구조에 다음과 같이 UID 및 경로 확인을 위한 Member를 추가하고 해당 Member에 대한 지속적인 감시와 탐지를 실시한다.

Table 5은 권한상승공격에 대한 탐지를 위한 struct 일부를 나타낸 것이다.

Table 5. part of Struct for detection code

```
struct binder_transaction_data {
    union {
        size_t handle;    ....
    pid_t sender_pid;
    uid_t sender_euid;
    size_t data_size;
    unsigned int test;
    size_t offsets_size;
    union {
        struct {
            const void *buffer; ...
```

해당 과정에서 struct binder_transaction_data를 통하여 서비스 핸들에 대한 처리와 RPC code 및 RPC data의 정보를 저장할 수 있다.

또한 위의 struct에서 추가한 test Member를 통하여 uid의 접근경로와 위협경로에 대한 탐지 및 확인을 위한 패킷 수집이 시작된다.

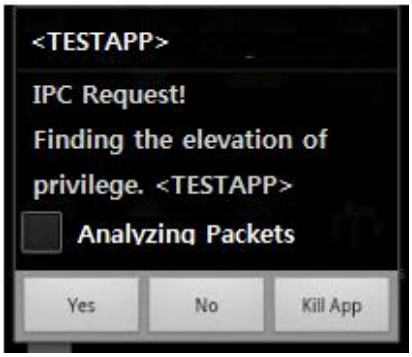

Fig. 6. Warning screen

위에서 제시한 탐지과정에 대하여 데이터의 처리과정과 physical page의 공유 및 확인 과정이 필요하다. 제안한 IPC 전달과정을 Fig.7과 같이 정리할 수 있다. Write buffer와 Read Buffer를 통한 BC,BR Transaction_data를 통하여 Physical pages를 공유하고 검증을 통하여 attack 여부를 판단하는 과정이다.

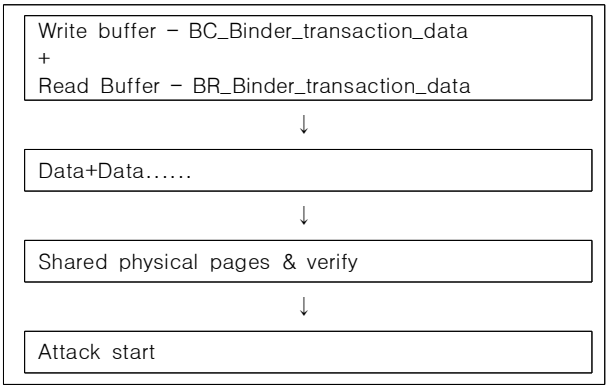

Fig. 7. IPC delivery process

악성코드를 통한 권한상승이 요청되면 요청자와 응답자 간 target_handled을 통하여 응답하고 read buffer를 통하여 실행되는 BR_TRANSACTION을 통하여 BR_REPLY Command로 answer 할 수 있다.

본 연구에서는 전달받은 BR_TRANSACTION을 통하여 target 및 code에 대한 구분을 하고 안전한 상태와 의심상태를 구분하여 안전한 상태일 경우 Read_buffer를 통하여 IPC data를 전달하고 그렇지 않을 경우 지속적인 패킷 분석을 통하여 위협 경로를 통한 접근인지를 판단하게 된다.

최종적으로 위협경로를 포함한 악성코드에 의하여 권한상승 공격을 받은 것으로 인지하게 되면 해당 요청을 한 모든 프로세스에 대한 권한을 중지한다.

2)성능평가

본 연구에 대한 성능측정을 위하여 악성코드가 포함된 샘플 코드를 동작 시키어 샘플 프로세스 동작과정과 탐지 및 대응과정에 대한 오버헤드를 측정한다.

본 실험을 위하여 PoA 기반 Blockchain Etherium Private system을 구축하고 간단한 거래가 가능하도록 작성하였다.

Solidity 기반 Smart Contract의 샘플을 3개 준비하였다.

① Blockchain Etherium Private system 구축

Blockchain Etherium은 PoA 기반 Puppeth를 활용한 Private system으로 간단한 거래가 가능하도록 작성하였다.

Solidity 기반 Smart Contract의 샘플을 3개 준비하였다.

본 연구는 스마트 거래에 대한 권한상승 공격 탐지 및 대응 방법에 대하여 중점을 두므로 기타 실험에 필요한 과정은 간단히 설명토록 한다.

Table 6은 실험을 위한 환경이다.

Table 6. Experiment environment

- Blockchain version : Blockchain Etherium private system
  - sample instance : AWS
  - OS : ubuntu server 16.04 (HVM)
  - sample : 3 (geth2, geth2, heth3)
  - agreement method : PoA
  - Smart Contract language : solidity
  - Smart Contract connect tool : Mist
- Memory : 2GB
- test tool : wireshark
- packet format : pcapng
- result format : xml

Blockchain의 private system 구축을 위한 기본 노드 구성은 faucet와 wallet 및 sealnode가 boot_node를 향하도록 한다. 또한 dashboard가 faucet와 wallet, ethstat를 가리키도록 앱을 구성한다.

Docker compose를 위하여 Fig.8과 같이 구성한다.

```
$ sudo apt-get install docker.io


$ sudo usermod -aG docker $(whoami)
$ sudo curl -L "https://github.com/do...ompose
 $ sudo chmod +x /usr/local/bin/docker-compose
```

Fig. 8. Docker compose configuration

② 권한상승공격을 탐지하기 위한 악성코드 프로그램 작성 및 분석

Fig.9는 권한상승공격을 위한 악성코드를 포함한 샘플 프로그램의 일부이다.

```
private void test_sampleHook{
int test;
_you_enter(this);
try{
    List sampleTasks *this.getApplicationContext().
    getSystestService();
    ...
    if(verify<conf_owner_lisr.lenght)    ...
```

Fig. 9. Part of sample programs

악성코드로 의심되는 프로세스의 경우 해당 프로세스에 대한 패킷을 wireshark로 3차례 분석한다.

Fig.10과 11은 샘플로 제작한 악성코드에 대한 패킷 일부를 샘플로 저장하여 xml로 나타낸 후 캡쳐한 화면이다.

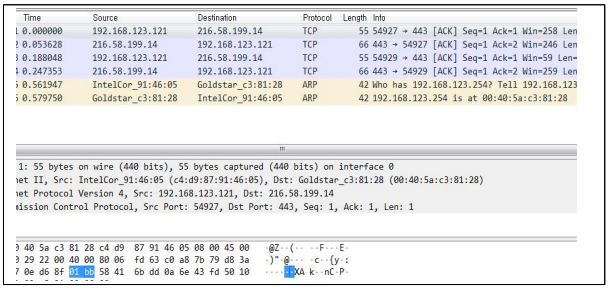

Fig. 10. Packet analysis capture screen via wirewhark

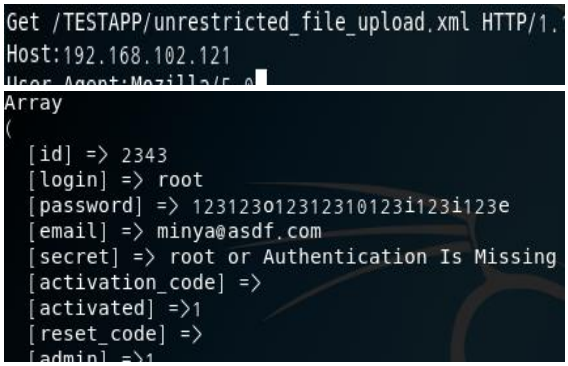

Fig. 11. xml screenshot for results

Fig.12의 화면에서와 같이 중요정보에 대한 사항이 요청되고 아직 권한을 중지하지 않은 상태로 중요정보를 탐지하고 있음을 확인할 수 있다.

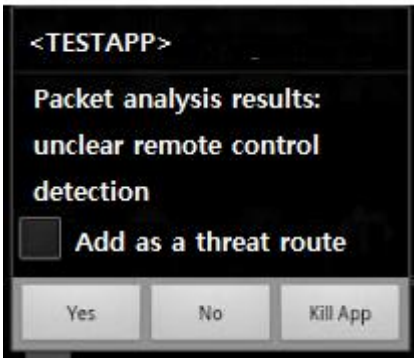

Fig. 12. Check for malware detection and screen for route confirmation

해당 실험에 대한 read / write에 대한 성능측정을 위하여 바인더드라이브 실행부터 악성코드 탐지까지의 시간을 세 가지 방법으로 측정하였다.

③ read/write 성능 평가

본 논문에서는 Blockchain Etherium 기반 스마트 거래를 위하여 권한상승공격을 탐지하고 대응하기 위한 방법을 제시하였다. 해당 연구내용의 결과 속도를 측정하기 위하여 기존 유사연구와 본 연구내용의 read/write의 속도를 측정하였다.

Table 7은 제안하는 방법(A)과 기존 발표된 유사 연구 방법(B),(C)의 read/write time에 대한 비교를 위하여 총 5회 실험한 결과의 평균값이다.

Table 7. Performance evaluation

Division	Case A	Case B	Case C
read time	549ms	602ms	622ms
write time	1003ms	1108ms	1151ms

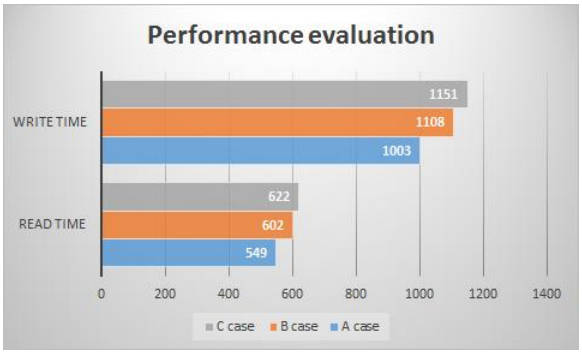

Fig. 13. Performance evaluation graph

Fig.13과 같이 실험 결과 제안하는 방법과 기존 유사 연구방법의 성능을 측정한 결과 읽기속도는 평균 12%, 쓰기 속도는 평균 13% 향상된 것을 알 수 있다.

측정된 read/write 속도는 악성코드 탐지를 위한 조처를 전혀 취하지 않은 상태와 비교하여 약1초 정도 속도가 저하되는 것을 알 수 있다. 이러한 속도 저하와 시스템 보안은 tradeoff

를 고려할 만한 수치이다. 하지만 많은 트랜잭션 처리시를 고려하여 더욱 빠르게 악성코드를 감지할 수 있는 향후 추가 연구가 필요하다.

Ⅳ. Conclusions

스마트디바이스 보급이 90%가 넘고 있으며 이를 반영하듯 스마트 디바이스를 사용한 스마트 거래율이 점점 높아지고 있다. 스마트 거래 포함 실생활의 다양한분 야에서 Blockchain Etherium Smart Contract를 적용하고 있으며 이를 통하여 거래 내역에 대한 해킹이나 위변조에 대한 위협을 감소할 수 있다. 하지만 스마트 거래 시 디바이스에 대한 다양한 위협이 발생하고 있다. Blockchain의 경우 권한과 인증이 중요한 요소이다. Blockchain Etherium에서 사용하는 Smart Contract의 경우 사용자의 중요정보나 거래내역에 대한 조회가 가능하고 권한을 공격받았을 경우 개인정보 조회는 물론 거래내역을 악용하거나 위변조의 가능성이 매우 크다. 본 논문에서는 Blockchain Etherium을 사용한 안전한 스마트 거래를 위하여 Blockchain에 특히 중요한 권한상승공격에 대한 탐지 및 대응방법을 연구하였다. 본 연구를 통하여 불가피한 선공격에 대한 대응 방법을 추가하여 사후 상황을 대비하였다. 악성코드를 통한 권한상승 공격이 매우 빠르게 시스템함수를 작동시키고 원격제어에 들어갈 경우 위험 프로세스에 대한 패킷 분석을 통한 차후 대처가 이루어지므로 보다 안전한 트랜잭션 관리가 가능하다.

본 연구와 기존 유사 어플리케이션의 read/write 속도를 비교한 결과 약 12~13% 정도 속도가 개선되었다.

하지만 모듈 설치 및 대응을 위한 프로그램 가동으로 추가 처리시간이 추가되어 기존 대비 1초 정도의 성능 차이를 보인다.

향후 많은 트랜잭션 처리를 고려하여 Blockchain 사이드 체인 기반의 권한상승에 대한 연구와 보다 빠른 악성코드를 감지를 통한 read/write 속도 향상을 위한 연구가 필요하다.

REFERENCES

[1] Min.K.S, "Online shopping trend survey," National Statistical Office, 2019.
[2] Lee.S.H, "Device Authentication for Smart Grid System Using Block Chain," KAIST, 2016.
[3] The Cointelegraph, A Brief History of Ethereum From Vitalik Buterin's Idea to Release, https://cointelegraph.com/news/ethereum-101-from-idea-to-release
[4] Information and Communication Policy Institute, "Online marketing trend, " 2018
[5] Lim.M.H, "Impacts and Implications of Block Chain Technology," Information and Communication Technology Promotion Center, 2017.
[6] Kang.S.J, "Understanding and Development Status of Block Chain Technology and Implications," The 4th Industrial Revolution and Soft Power Issue Report by the Information and Communication Industry Promotion Agency, No.13, 2018.
[7] Block Chain & PinTech leads 'smart finance,' http://www.etnews.com/20180816000425
[8] Ernst & Young Global Limited, https://www.ey.com/kr/ko/home
[9] 5Miles, https://www.5mils.com
[10] Block Chain - Fancy or Innovative, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201902070600055&code=940100
[11] Gartner, https://www.gartner.com/en
[12] Mcafee, https://www.mcafee.com/ko-kr/index.html
[13] Zhou,Y.,& Jiang,X, "Dissecting android malware:Characterizationand evolution.InSecurityandPrivacy," 2012 IEEE Symposium pp.95-109, 2012.
[14] JIANG. X, "Gingermaster: First andorid malware utilzing a root exploit on android 2.3," NC State University,2011.
[15] William Enck & Peter Gilbert & Byung-Gon Chun, "TaintDroid:aninformation-flow trackingsystem forrealtimeprivacy monitoring on smartphones, " InProceeding sof the 9th USENIX conference on Operating systems design and implementation, pp.1-6, 2014.
[16] Xu.R. & Saidi.H & Anderson.R, "Aurasium:Practical policy enforcement for android applications," InProceeding sof the 21st USENIX conferenceon Security symposium, pp.27-27, 2012.

Authors

Youn-A Min received computer architecture and embedded system security Ph.D. degrees in Computer Engineering from Dongguk University, Korea, in 2008 and 2013, respectively Dr. Min Youn-A interested in the security of embedded systems and smart devices. Recently, she is interested in on chain, off-chain block chain and hash algorithm.