Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1067

모바일 게임 보안을 위한 안드로이드 에뮬레이터 탐지방법에 관한 연구*

윤 종 성,† 이 상 진‡
고려대학교 정보보호대학원

A Study on android emulator detection for mobile game security*

Jongseong Yoon,† Sangjin Lee‡
Center for Information Security Technologies(CIST), Korea University

요 약

최근 모바일 게임 사용자가 증가하면서 점수 및 레벨 조작, 게임 속도 조작, 결재부정과 같은 부작용이 발생하고 있다. 특히, PC에서 모바일앱을 구동할 수 있도록 해주는 에뮬레이터를 사용하면 게임 앱을 디버깅을 하거나 게임 조작을 자동화하기 쉬워지기 때문에 모바일 게임 보안관점에서 커다란 위협이 되고 있다. 따라서 본 논문에서는 모바일 게임 보안 위협 완화를 위해 최근 많이 사용되는 안드로이드 에뮬레이터인 BlueStacks, GenyMotion, Andy, YouWave와 구글 크롬에서 안드로이드를 동작 시킬 수 있는 ARC Welder 확장 프로그램을 클라이언트(앱), 게임서버 및 네트워크 관점에서 효과적으로 탐지할 수 있는 방법에 대해 연구하였다.

ABSTRACT

With the recent increase of the number of mobile game users, the side effects such as the manipulation of game points, levels and game speed and payment fraud are emerging. Especially, the emulators which make it possible for mobile applications to run on PC is a great threat to mobile game security since debugging specific game application or automating the game playing can be done easier with them. Therefore, we research the efficient ways to detect widely used Android Emulators such as BlueStacks, GenyMotion, Andy, YouWave and ARC Welder from the perspective of client(app), game server and network to reduce threat to mobile game security.

Keywords: Mobile game security, Android emulator detection

I. 서 론

2009년 세계 게임시장에서 모바일 게임의 비중은 10.1%에 불과하였지만 스마트폰, 태블릿과 같은 모바일 기기의 급속한 보급으로 2013년도에는 14.4%까지 비중이 급격히 늘어났으며 2018년에는 16.8%까지 올라 지속적으로 성장할 것으로 예상되고 있다[1]. 모바일 게임 초기에는 간단한 퍼즐게임이 주류를 이루었으나 스마트폰, 태블릿 등 모바일 기기의 성능이 발전하면서 MMORPG, FPS, 액션과 같이 기존 PC 환경에서 인기를 끌던 장르의 게임들이 등장하고 있다.

모바일 게임은 소셜 네트워크 서비스와 결합하여 게이머간의 경쟁을 유도하고 인앱 결제 방식을 통해 손쉽게 아이템을 구매할 수 있어 온라인 게임에 이어 금전적 이익을 노리는 공격자들의 위협에 노출될 가

접수일(2015년 6월 22일), 수정일(2015년 9월 1일), 게재 확정일(2015년 9월 11일)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터 육성 지원사업의 연구결과로 수행되었음(IITP-2015-H8501-15-1003)
† 주저자, yoonjs53@naver.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

능성이 점점 높아지고 있다. 실제로 2012년 게임 아이템 거래 사이트에서 모바일 게임들이 거래 시장에 등장하였으며 아이템 거래가 점점 증가하고 있다. 인기 모바일 게임인 룰더스카이는 일간 거래액이 약 2500만원 수준(2012년 10월 기준)을 기록하였으며[2] 몬스터 길들이기의 경우 아이템의 일평균 거래량이 800만원 수준이고 월 거래량은 2억원(2014년 2월 기준)에 달하였다[3].

모바일 게임의 증가하는 보안 위협에 비해 짧은 인기주기, 개발사의 작은 규모, 개발자의 보안의식 결여 등과 같은 이유로 보안성은 향상되지 못하고 있는 실정이다. 모바일 게임은 PC용 게임과 다르게 클라이언트에 적용할 수 있는 보안대책이 매우 제한적이며 안드로이드의 경우 간단한 방법으로 디컴파일이 가능하여 공격자로부터 앱을 보호하기 어렵다. 특히 모바일 앱을 구동할 수 있는 에뮬레이터는 모바일 게임의 조작을 자동화하거나 디버깅 쉽도록 만드는 역할을 할 수 있어 보안 관점에서 위협이 될 가능성이 높다. 에뮬레이터는 앱 개발시 테스트를 위해 사용할 목적으로 활용되었으나 최근에는 PC에서 선호하는 앱을 사용하거나 게임을 즐기기 위해 일반 사용자까지 확산되고 있는 추세여서 게이머나 공격자가 에뮬레이터를 사용하여 악의적인 게임 조작을 할 가능성이 증가하고 있다.

과거 인기를 끌었던 애니팡 게임의 경우 PC 에뮬레이터에서 구동하고 조작을 자동화하여 고득점을 올리는 프로그램이 개발되어 사용되기도 하였으며, 최근에는 안드로이드 에뮬레이터를 기반으로 제작한 모바일 게임 자동화 프로그램을 판매하여 금전적인 수익을 얻으려는 사례도 발생하고 있다.

Fig. 1.은 최근 구글 플레이 마켓에서 가장 많은 매출을 올리고 있는 게임인 레이븐의 게임 자동화 프로그램을 광고하는 화면이다.

Fig. 1. The mobile game autoplay tool for raven

좌측 상단에 에뮬레이터에서 게임이 구동되고 있으며 우측 상단 자동화 프로그램이 사용자를 대신해 게임을 진행하고 있다.

Windows 환경에서 게임 메모리 조작을 위해 많이 사용하는 오픈소스 도구인 Cheat Engine[4]과 안드로이드 에뮬레이터인 BlueStacks를 활용하여 모바일 게임을 디버깅하고 메모리를 조작하는 방법도 많이 사용되고 있다.

따라서 본 논문에서는 모바일 게임에 위협 요소인 에뮬레이터를 효과적으로 탐지하는 방법에 대해 연구하였다. 최근 많이 사용되는 안드로이드 에뮬레이터인 BlueStacks, GenyMotion, Andy, YouWave와 구글 크롬에서 안드로이드를 동작 시킬 수 있는 ARC Welder 확장 프로그램을 대상으로 클라이언트(앱) 측면에서 최소 권한을 가지고 에뮬레이터를 탐지하는 방법과 게임 서버 및 네트워크 측면에서 탐지하는 방법에 대해 연구하였다.

II. 관련연구

안드로이드 에뮬레이터는 하드웨어 기기 없이 앱 개발 및 디버깅을 편리하게 하거나, 악성 앱 상세분석, 분석 자동화를 위한 목적으로 활용되고 있다. 최근에는 메신저, SNS, 게임 앱을 PC에서 편리하게 즐기기 위한 목적으로 일반 사용자들도 많이 사용하고 있다.

악성 앱 분석을 위해서도 다양한 안드로이드 에뮬레이터가 사용되고 있다. 구글의 경우 마켓에 등록되는 앱을 검수할 때 qemu 기반의 악성앱 분석도구인 Google Bouncer를 사용하며, 백신업체, 정보보호업체 같은 조직에서도 악성앱 분석 및 탐지를 위해 Andrubis, DroidBox, SandDroid와 같은 에뮬레이터를 사용하고 있다.

안드로이드 에뮬레이터 탐지에 관한 연구는 위와 같은 악성앱 분석을 회피하기 위한 관점에서의 연구가 존재하며, 안드로이드 앱 개발자 커뮤니티에서 개발한 앱이 에뮬레이터 환경에서 구동되기 원하지 않는 개발자들에 의해 개발 팁 수준의 탐지 방법이 공유되고 있다.

Timothy Vidas[5] 등은 안드로이드 앱이 에뮬레이터 환경에서 분석되는 것을 회피하기 위한 기술적인 방법을 정리하고 평가하였다. 에뮬레이터 탐지 방법으로 안드로이드 API를 사용하여 기기 빌드 정

보를 조회하는 방법, 네트워크 정보를 활용한 방법, 안드로이드 에뮬레이터의 기반이 되는 qemu와 같은 소프트웨어를 탐지하는 방법, CPU 또는 GPU 성능을 기반으로 탐지하는 방법, 하드웨어 센서와 같은 부품 관련 정보를 사용하는 방법, 설치되어 있는 앱 정보를 바탕으로 탐지하는 방법을 제시하고 악성앱 분석 에뮬레이터인 Andrubis, CopperDroid, ForeSafe를 대상으로 탐지 성능을 평가하였다. 해당 연구는 다양한 방식의 에뮬레이터 탐지 방법을 제시하였으나 모두 클라이언트 측면의 탐지 방법이었으며 모바일 게임 치팅에 활용되는 에뮬레이터는 연구 대상이 아니었다. 또한 센서로 입력되는 정보는 사용하지 않았다는 제한점이 있다.

III. 안드로이드 에뮬레이터

3.1 BlueStacks

BlueStacks는 미국의 Bluestacks社가 개발하여 2012년에 공개한 안드로이드 에뮬레이터로 홈페이지에 공개된 정보에 따르면 9,000만명이 사용하고 있을 정도로 최근 많이 사용되고 있는 에뮬레이터 중에 하나이다[6]. Virtual Box와 같이 별도의 가상화 프로그램 설치가 필요 없으며 구동 속도가 빠르고 앱 설치가 편리하다. Fig. 2.는 BlueStacks의 구동 화면이다.

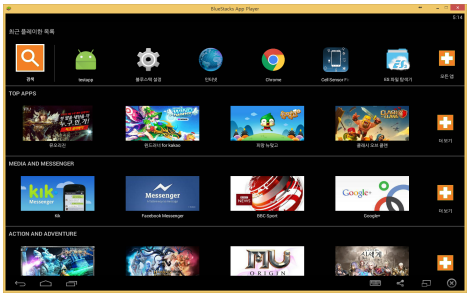

Fig. 2. The BlueStacks android emulator

3.2 GenyMotion

GenyMotion은 Genymobile社에서 2013년에 공개한 안드로이드 에뮬레이터로 VirtualBox를 기반으로 동작한다[7]. 선택에 따라 Google Nexus, 삼성 Galaxy 등의 스마트폰, 태블릿처럼 기기정보

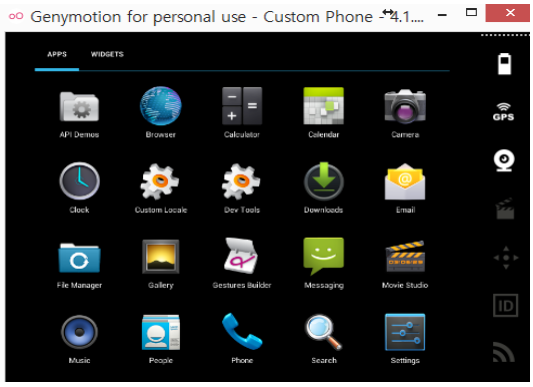

Fig. 3. The GenyMotion android emulator

를 설정할 수 있으며 호스트 PC와의 자료이동이 편리하다. 또한 JAVA API를 제공하여 안드로이드 개발자가 테스트용으로 활용할 수 있다. Fig. 3.은 GenyMotion의 구동 화면이다.

3.3 Andy and YouWave

ANDY와 YouWave는 VirtualBox를 기반으로 동작하며 기능 및 성능은 다른 에뮬레이터와 유사하다.

3.4 ARC Welder

ARC Welder는 웹브라우저인 크롬의 확장 프로그램 형태로 구동되는 안드로이드 에뮬레이터이다. ARC(App Runtime for Chrome)는 구글에서 2014년에 공개한 크롬 기반의 안드로이드 앱 실행 환경이다[8]. ARC Welder는 아직 일반 사용자에 많이 사용되지 않고 있으나, 크롬북과 같은 크롬 OS 기반의 기기 또는 크롬 브라우저가 설치된 환경에서 편리하게 안드로이드 앱을 구동할 수 있어 향후 사용자가 증가될 것으로 예상된다. Fig. 4.는 ARC Welder의 구동 화면이다.

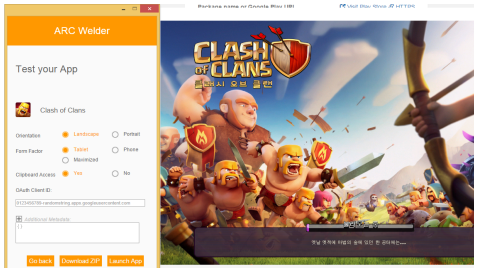

Fig. 4. The ARC Welder android emulator

IV. 안드로이드 에뮬레이터 탐지 방법

4.1 클라이언트 측면에서 탐지 방법

4.1.1 안드로이드 권한(퍼미션)

안드로이드는 보안을 위해 앱이 사용하는 정보나 기능별로 권한을 획득하도록 설계되어 있다. 앱 설치 시 해당 앱이 요청하는 권한을 사용자에게 보여주며, 사용자가 동의해야 정상적으로 설치가 된다. 사용자 입장에서 앱이 너무 많은 권한이나 정보를 요구할 경우에 개인정보 노출 등의 염려로 인해 앱을 설치하지 않거나 사용하지 않을 가능성이 발생한다. 따라서 앱 개발자는 앱의 기능과 무관한 권한의 요청 및 사용을 최소화해야 한다.

클라이언트 측면에서 에뮬레이터를 탐지하기 위한 기능 구현시에도 퍼미션을 고려해야하며 최소한의 권한을 사용하여 에뮬레이터 탐지 기능을 구현하는 것이 적합하다. 에뮬레이터 탐지 기능 구현시 활용 가능한 퍼미션 범위를 확인하기 위해 구글 플레이 마켓에서 매출이 높은 게임 10개를 대상으로 설치시 요구되는 퍼미션을 확인하였다. 대상 게임은 ①레이븐, ②뮤오리진, ③클래시 오브 클랜, ④세븐나이츠, ⑤모두의 마블, ⑥애니팡2, ⑦몬스터 길들이기, ⑧갓오브 하이스쿨, ⑨하스스톤, ⑩캔디크러쉬소다 였으며 결과는 Table 1.과 같다.

Table 1. The requested permission of Top 10 grossing Games on google play market

Permission	Game
In-app purchases	All
Device & app history	①, ②, ④, ⑤, ⑥, ⑦
Identity	All
Photos/Media/Files	①, ②, ③, ④, ⑤, ⑥, ⑦, ⑧, ⑨
Device ID & call information	①, ②, ④, ⑤, ⑥, ⑦, ⑧, ⑨
SMS	②
Contacts	⑩
WIFI connection information	ALL
Receive data from internet	All
Read home settings and shortcuts	①
modify battery statistics	⑥

4.1.2 Build 정보를 이용한 탐지

안드로이드는 기기의 일반적인 정보를 build.prop 파일에 저장하고 있으며 앱에서는 android.os.BUILD 클래스를 호출하여 별도의 퍼미션 없이

Table 2. The build information of the emulators and the real devices

Build Information	Emulator					Real Device		
	Blue Stacks	Geny Motion	Andy	You Wave	ARC Welder	Galaxy Note 3	LG G3	Vaga Racer3
BOARD	universal5410	unknown	clovertrail	piranha	nacl_x84_64	MSM8974	APQ8084	MSM8960
BOOTLOADER	unknown	unknown	unknown	unknown	unknown	N900LKLU0GOD2	unknown	unknown
BRAND	samsung	generic	AndyOS	samsung	chromium	samsung	lge	VEGA
CPU_ABI	x86	x86	x86	x86	armeabi-v7a	armeabi-v7a	armeabi-v7a	armeabi-v7a
HOST	SWDD3913	buildbot.soft.genymobile.com	andy-vm-builder	SEP-96	build28-a75	SWDD5620	LGEARND6B10	bs194
DEVICE	ja3g	vbox86p	AndyWin	espressowifi	nacl_x84_64	hltelgt	tiger6	ef48s
HARDWARE	unknown	vbox86	andy	generic_x86	arc	SWDD5620	tiger6	qcom
MANUFACTURER	samsung	Genymotion	Andy OS Inc	samsung	chromium	samsung	LGE	PANTECH
MODEL	GT-I9500	Google Nexus 5 - 4.4.4 - API 19	AndyWin	GT-P3113	App Runtime for Chrome Dev	SM-N900L	LG-F460S	IM-A850S
PRODUCT	ja3gxx	vbox86p	AndyWin	espressowifiue	arc	hltelgt	tiger6_skt_kr	VEGA_IM-A850S
RadioVersion	N/A	N/A	N/A	N/A	N/A	N900LKLU0GOD1	M9635TAA (이하생략)	M9615A (이하생략)

확인 할 수 있다. 일반적으로 가장 간단하고 많이 알려진 에뮬레이터 탐지 방법이 이 BUILD 정보를 활용하는 방법이다.

Build 정보에서 확인할 수 있는 정보는 CPU 타입, 호스트 이름, 제조사, 모델명, 기기의 보드 종류, Fingerprint 값 등이 있다. 에뮬레이터와 실제 기기에서 수집한 BUILD 정보는 Table 2.와 같다.

BlueStacks와 YouWave는 가상기기를 설정에 따라 삼성 갤럭시, 구글 Nexus 등으로 변경할 수 있어 실제 기기와 동일한 값이 Build 정보에 포함된다. BOARD, BRAND, HARDWARE 정보가 Unknown일 경우 에뮬레이터일 가능성이 있으며 Andy와 Arc Welder는 BRAND, MODEL, PRODUCT에서 특징적인 문자열을 확인할 수 있다. GenyMotion은 HOST, MANUFACTURER에 genymotion이라는 문자가 특징적으로 나타나며 VirtualBox 기반으로 구동 되어 vbox라는 문자열이 나타난다. YouWave는 Device, PRODUCT 정보에서 espressowifi라는 특징적인 문자열을 확인할 수 있다. 대상 에뮬레이터들이 공통적으로 BOOTLOADER 값이 unknown이고 실제 기기도 동일한 값이기 때문에 에뮬레이터 식별 정보로 활용하기 어렵다. 에뮬레이터들의 RadioVersion 값이 공통적으로 비어 있는데 3G나 LTE 통신 기능이 없는 WIFI 전용 태블릿도 해당 정보가 없는 것으로 확인되어 해당 정보를 에뮬레이터의 식별정보로 활용할 수 없다.

Build 정보는 기기가 루팅되어 있을 경우 사용자가 원하는 값으로 변경이 가능하며, 최근 에뮬레이터들은 설정에 따라 실제 기기의 Build 정보와 동일하게 설정할 수 있기 때문에 에뮬레이터를 탐지하기 위한 적합한 정보가 아니다. 또한 모든 에뮬레이터에 공통적으로 적용하기 어렵고 에뮬레이터가 업데이트 되거나 새로운 에뮬레이터가 등장할 경우 탐지 방식을 변경해야하는 단점이 있다.

4.1.3 통화, USIM 및 네트워크 정보를 이용한 탐지

안드로이드는 스마트폰 운영체제 이므로 통화와 관련된 정보와 USIM 정보를 수집할 수 있다. 통화 및 USIM 관련 정보는 TelephonyManager API를 이용하여 수집하며 READ_PHONE_STATE 권한이 필요하다. 개발용 에뮬레이터들은 통화 관련 기능을 실제 기기와 유사한 환경으로 제공하기 위해 특정 전화번호나 USIM 번호 등이 설정되어 있는 경우가 있다.

탐지 대상 에뮬레이터의 경우 실제 WIFI로 연결되는 것이 아니라 호스트 PC의 네트워크를 통해 통신이 이루어지기 때문에 연결된 Network 정보를 확인하여 특징점을 식별하였다. Table 3.은 대상 에뮬레이터의 통화, USIM 및 네트워크 정보를 확인한 결과이다.

GenyMotion의 경우 전화번호, SIM 카드 시리얼번호, MAC 주소값이 고정적이고 네트워크 운영자와 SIM 운영자 정보가 Android로 되어 있어 쉽게 에뮬레이터로 판단이 가능하다. YouWave를 제외한 나머지 에뮬레이터들은 가상 WIFI가 접속하는 SSID 값이 BlueStacks, WiredSSID,

Table 3. The telephony and network information of the emulators

Category	BlueStacks	GenyMotion	Andy	YouWave	ARC Welder
PhoneType	GSM	GSM	GSM	GSM	NONE
Line1Number	N/A	15555215554	N/A	N/A	N/A
NetworkCountryIso	kr	us	N/A	N/A	N/A
NetworkOperatorName	SKTelecom	Android	N/A	N/A	N/A
SIMSerialNumber	Arbitrary value	89014103211118510720	N/A	N/A	N/A
SimState	READY	READY	N/A	StateUnknown	N/A
SimOperatorName	SKTelecom	Android	N/A	N/A	N/A
Mobile DataState	DATA_DISCONNECTED	DATA_DISCONNECTED	DATA_DISCONNECTED	DATA_DISCONNECTED	DATA_DISCONNECTED
Active Network Type	WIFI	WIFI	WIFI	ETH	WIFI
WIFI Activation	YES	YES	YES	NO	YES
WIFI MAC	Arbitrary value	08:00:27:ea:80:56	Arbitrary value	N/A	00:00:00:00:00:00
Connectecd WIFI SSID	BlueStacks	WiredSSID	WiredSSID	N/A	unknown SSID
Connectecd WIFI BSSID	Arbitrary value	01:80:c2:00:00:03	01:80:c2:00:00:03	N/A	N/A

unknownSSID로 실제 환경과 차이가 나며 YouWave는 네트워크를 이더넷으로 연결하는 것으로 확인되어 일반적인 안드로이드 기기와는 다르다.

최근 WIFI 전용 태블릿에서도 게임을 많이 한다는 점에서 통화 정보나 USIM 정보는 에뮬레이터 탐지에 활용하기 어려우나 WIFI SSID와 연결된 네트워크 유형으로 에뮬레이터 여부를 확인 할 수 있다.

4.1.4 하드웨어 정보를 이용한 탐지

스마트폰, 태블릿과 같은 안드로이드 기기는 카메라, 터치 디스플레이, 각종 센서, 배터리 등의 하드웨어가 포함되어 있다. 안드로이드 에뮬레이터들을 카메라, 센서 등의 하드웨어를 가상으로 있는 것처럼 구현하고 있지만 실제 기기와는 차이가 있으므로 이를 이용하여 에뮬레이터를 탐지하는 방법을 제안하고자 한다.

사용 가능한 하드웨어 정보는 PackageManager API를 사용하여 획득하며 별도의 권한은 필요없다. 대상 에뮬레이터의 사용 가능한 하드웨어를 확인한 결과는 Table 4.와 같다.

Table 4. The available hardware of the emulators

Hard ware	Blue Stacks	Geny Motion	Andy	You Wave	ARC Welder
Camera	YES	YES	YES	YES	YES
Bluetooth	YES	YES	YES	YES	NO
Microphone	YES	YES	YES	YES	YES
GPS	YES	YES	YES	YES	YES
Acceleration Sensor	YES	YES	YES	YES	NO
Temperature Sensor	NO	NO	NO	NO	NO
Barometer	YES	NO	NO	NO	NO
Compass	YES	NO	YES	YES	NO
Gyroscope	YES	NO	YES	NO	NO
NFC	NO	NO	NO	NO	NO

최근에는 단가를 줄이기 위해 필수적이지 않은 센서나 하드웨어를 제거한 기기들이 많이 판매되고 있으며 특히 태블릿은 근접 조도센서, 온도센서 같은 부가적인 센서들이 없는 제품이 많이 존재한다. 따라서 사용가능한 하드웨어 존재 여부로는 에뮬레이터를 식별할 수 없다. 따라서 하드웨어의 세부적인 정보 또는 실제 입력되는 정보를 수집하여 에뮬레이터를 탐지해야 한다.

하드웨어의 세부적인 정보 중 센서 이름과 제조사 같은 정보를 활용할 수 있다. 각 에뮬레이터 별로 특징적인 센서 정보는 Table 5.와 같다.

Table 5. The sensor information of the emulators

Emulator	Sensor Information
BlueStacks	- Acceleration Sensor, etc. · Vendor : AOSP
GenyMotion	- Acceleration Sensor · Name : Genymotion Accelerometer · Vendor : Genymobile
Andy	- Acceleration Sensor, etc. · Vendor : GreatFruit or Google Inc.
YouWave	- No Sensor Information
ARC Welder	- No Sensor Information
Other emulator	- Acceleration Sensor, etc. · Vendor : goldfish or The Android Open Source Project

YouWave는 PackageManager API를 통해 얻은 정보에는 가속센서가 있다고 출력되지만 센서의 세부 정보가 표시되지 않았으며, ARC Welder는 센서가 없는 것으로 정보가 수집된다. 현실적으로 실제 기기는 화면 방향 감지를 위해서 최소한 가속도 센서는 탑재하고 있기 때문에 아무런 센서가 없다면 에뮬레이터로 추정할 수 있다.

에뮬레이터는 가상의 하드웨어를 쉽게 생성할 수 있지만 실제 안드로이드 기기에서 발생되는 터치정보, 센서 입력 정보 값은 발생시키기 어렵다. 따라서 안드로이드 기기에 필수적으로 탑재되는 하드웨어인 터치 스크린 정보와 가속도 정보를 사용하여 에뮬레이터를 탐지하는 방법을 제안한다.

터치 정보와 가속도 센서 정보 수집은 별도의 권한이 필요 없다. 터치 정보는 터치 압력과, 터치한 면적(크기) 정보를 수집할 수 있는데 터치 압력은 삼성의 갤럭시 노트 제품과 같이 필압센서가 있을 경우만 동작하므로 수집에서 제외한다. onTouchEvent method를 상속 받아 구현하며 N회 이하의 터치 이벤트에서 터치 면적(크기)정보를 수집하고 평균 및 표준 편차를 구한다.

가속센서 정보는 SensorEventListener 등록하여 구현하며 터치 이벤트와 유사하게 N회 이하의 가

속 센서 이벤트에서 X, Y, Z 좌표별 값을 수집하고 평균 및 표준 편차를 구한다.

각 에뮬레이터와 실제 기기에서의 실험 결과는 Table 6.과 같다. 실험에서 실제 기기는 두 손으로 들고 있는 상태에서 일상적인 사용 수준의 움직임과 터치 및 드래그로 정보를 수집하였다.

에뮬레이터에서 터치 면적은 마우스로 클릭하기 때문에 대부분 0.0 값으로 고정되었으며 Andy 에뮬레이터는 0.00999 정도의 작은 값이 지속적으로 관찰되었는데 변화폭이 크지 않아 표준편차 값이 상당히 작다.

가속도 값은 BlueStacks와 GenyMotion을 제외하고는 0.0 값으로 고정되었다. BlueStack은 중력가속도 값이 Z축에서 관찰되었으며 GenyMotion은 임의의 값이 Y, Z 축에서 관찰되었으나 둘 다 값의 변경이 거의 없어 실제 기기에서 측정한 표준편차와 많은 차이를 보였다. 특히 가속도 센서 X축 값은 모든 에뮬레이터에서 0.0 값으로 고정되었다.

지금까지 클라이언트 측면에서 안드로이드 에뮬레이터를 탐지하는 방법으로 Build 정보를 이용한 방법, 통화 및 네트워크 정보를 이용한 방법 그리고 하드웨어 정보를 이용한 방법에 대해 실험용 앱을 구현하여 결과를 확인하였다. 구현 및 실험 결과 클라이언트 측면에서 에뮬레이터를 탐지할 수 있는 가장 효과적인 방법은 터치 면적 정보를 수집하는 방법과 가속도 센서의 X축 정보를 수집하는 방법이다. 실제 안드로이드 기기에서도 블루투스 마우스나 삼성의 S pen과 같은 입력도구를 사용하면 터치 면적이 0.0 값으로 수집될 수 있으며 가속도 센서가 없는 기기가 있을 수 있으므로 상호 보완적으로 두 가지 방법을 혼용하여 사용하는 것이 효과적일 것으로 판단된다.

4.2 서버/네트워크 측면에서 탐지 방법

안드로이드 앱은 난독화가 되어 있지 않다면 간단한 방법으로 디컴파일하여 소스 수준으로 앱을 분석할 수 있고 원하는 기능을 덧붙이거나 제거하여 새로운 설치 파일을 생성할 수 있다. 이러한 특징은 안드로이드 에뮬레이터를 탐지하고 필요시 앱을 구동시키지 않는 기능을 클라이언트에 구현하였을 경우 우회당할 가능성을 남긴다. 따라서 게임 서버 및 네트워크 측면에서 안드로이드 에뮬레이터를 탐지하는 방법을 적용하는 것이 중요하다.

서버 및 네트워크 측면에서 안드로이드 에뮬레이터를 탐지하는 방법은 크게 두 가지 관점에서 구현할 수 있다.

첫 번째는 모바일 게임 앱에서 에뮬레이터로 판단할 수 있는 정보를 수집하여 서버로 전송하는 방법이다. 클라이언트 측면에서 공격자는 앱을 분석하여도 에뮬레이터 탐지와 관련된 함수를 발견하기 어렵기 때문에 기능을 제거하기 어렵고 게임 업체는 필요한 시점에서 에뮬레이터로 판단되는 접속을 차단하거나 게임을 종료시키는 등 제재를 가할 수 있다. 게임 앱에서 에뮬레이터를 판단할 수 있는 정보는 클라이언트 관점에서 탐지방법에서 사용하는 정보와 동일하다.

게임 앱 내에서 터치크기 정보와 가속도 센서 X축 정보를 기존 게임 로그와 통합하여 서버로 전송하며 이때 잦은 센서 정보 수집은 게임 성능에 악영향을 미칠 수 있으므로 센서 수집 주기 및 시간을 최소화하여 구현한다.

두 번째 방법은 네트워크 패킷만을 활용하여 에뮬레이터 여부를 탐지하는 방법이다. 전통적인

Table 6. The input values from touch screen and acceleration sensor of the emulators and the real devices

Event Type			Emulator					Real Device
			Blue Stacks	Geny Motion	Andy	You Wave	ARC Welder	
Touch Size	Average		0.0	0.0	0,00999999	0.0	0.0	0.02853569
	Standard deviation		0.0	0.0	$6.519*10^{-20}$	0.0	0.0	0.00449454
Acceleration Value	X	Average	0.0	0.0	0.0	0.0	0.0	-0.8260682
		Standard deviation	0.0	0.0	0.0	0.0	0.0	0.69662233
	Y	Average	0.0	9.7762375	0.0	0.0	0.0	4.670394
		Standard deviation	0.0	$1.811*10^{-17}$	0.0	0.0	0.0	0.6049590612
	Z	Average	9.806642	0.8134159	0.0	0.0	0.0	8.473735
		Standard deviation	$6.675*10^{-17}$	$1.132*10^{-19}$	0.0	0.0	0.0	0.6122006611

Passive OS Fingerprinting 방법 중 하나인 TTL(Time To Live)값을 이용하는 방법을 에뮬레이터 탐지에 활용할 수 있다. 대부분의 Windows는 운영체제의 Default TTL 값은 128, Linux 계열은 64 이다[9]. 에뮬레이터와 게임 부정 프로그램은 주로 Windows 환경에서 구동되는 반면 실제 스마트폰의 Android는 Linux 커널을 사용한다는 점에 착안하여 실험을 통해 TTL 값을 수집하고 분석하였다. Table 7.은 에뮬레이터 및 실제 기기에서 전송한 패킷을 서버측 네트워크에서 수집하여 TTL값을 확인한 결과이다.

Table 7. The TCP TTL values of the emulators and the real devices

Emulator	TTL	Real Device	TTL
BlueStacks	109	Galaxy S3	52
GenyMotion	111	Galaxy Note 3	53
Andy	109	Galaxy Note 8.0	64
YouWave	111	Vega Racer 3	53
ARC Welder	111	LG G3	49

실험 결과 에뮬레이터에서 발생한 패킷은 호스트 운영체제인 Windows의 Default TTL 값을 따르는 것을 알 수 있다. 네트워크 라우팅경로에 따라 실제 도착한 패킷의 TTL 값은 상이하겠지만 모바일 게임서버로 도착하는 패킷에서 64보다 크면 에뮬레이터로 판단할 수 있다. 단, Windows 레지스트리를 조작하여 기본 TTL값[1]을 변경한 경우 또는 에뮬레이터가 Linux, MacOS에서 동작되는 경우에는 탐지가 제한적이다.

V. 결 론

모바일 게임은 아직까지 기존 게임에 비해 부정행위가 많이 발생하고 있지 않고 있다. 그러나 모바일 게임의 인기가 점차 증가하고 모바일 게임 내에서 아이템 현금거래가 이루어지기 시작하면서 재화로서 가치가 증가하고 있다. 따라서 향후 부정사례가 많이 발생할 것으로 예상된다.

1) 레지스트리 키 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters의 DefaultTTL 값을 Dword 형식으로 설정하면 기본 TTL값 변경 가능

과거에는 공격자가 게임 부정에 사용되는 다양한 프로그램들을 모바일 기기에서 구현하기 어려웠지만 PC에서 모바일 게임을 구동할 수 있도록 해주는 안드로이드 에뮬레이터의 등장으로 보다 쉽게 게임 치팅 툴, 메모리 조작 프로그램, 게임 자동 플레이 프로그램 등을 제작할 수 있게 되었다. 게임 개발 업체 측면에서는 잠재적인 위험 요소인 에뮬레이터를 탐지하고 필요에 따라 게임 앱을 중지 시키거나 접속을 차단할 수 있는 방법을 강구해야할 필요성이 증가하고 있다.

본 논문에서는 일반 사용자들에게 많이 사용되고 있는 안드로이드 에뮬레이터를 대상을 클라이언트 측면과 서버/네트워크 측면에서 탐지하는 방법에 대해 연구하였다.

클라이언트 측면에서는 기기의 Build 정보, 통화/네트워크 정보, 하드웨어 정보를 활용하여 다양한 방식으로 탐지 방법을 모색하였으며 가장 효과적인 방법으로 터치 면적과 가속도 센서 X축 값을 활용하는 방법을 제안하였다.

서버 및 네트워크 측면에서는 클라이언트에서 수집된 정보를 바탕으로 탐지하는 방식과 네트워크 패킷의 TTL 정보를 바탕으로 간단하게 에뮬레이터를 탐지하는 방법을 제안하였다.

References

[1] KOCCA, “2014 International content market trend,” KOCCA, Jan. 2015.

[2] ″Mobile games′ hit the game item market″, ZDNet Korea, 2012.10.6., http://www.zdnet.co.kr/news/news_view.asp?artice_id=20121006085602

[3] “The hottest trends in the mobile game item trading,” ZDNet Korea, 2014.2.2., http://www.zdnet.co.kr/news/news_view.asp?artice_id=20140202090601

[4] Cheat Engine Homepage, http://www.cheatengine.org/

[5] Timothy Vidas, Nicolas Christin, “Evading Android Runtime Analysis via Sandbox Detection,” In Proceedings of the 9th ACM symposium on Information, computer and communications security, pp. 447-458, June. 2014.

〔6〕 BlueStacks Homepage, http://www.bluestacks.com/local/kor/home-kor.html
〔7〕 GenyMotion Homepage, https://www.genymotion.com/
〔8〕 Run android Apps on Chrome OS, https://developer.chrome.com/apps/getstarted_arc
〔9〕 Default TTL Values in TCP/IP, http://www.switch.ch/docs/ttl_default.html

〈저자소개〉

윤 종 성 (Jongseong Yoon) 학생회원
2005년 3월: 공군사관학교 전산과학과 학사
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석·박사통합과정
〈관심분야〉 디지털 포렌식, 정보보호, 악성코드 분석

이 상 진 (Sangjin Lee) 종신회원
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수