Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.829

안드로이드 소비 전력 및 네트워크 트래픽을 기반으로 한 도청 관련 스파이웨어 탐지 시스템

박 범 준,† 이 욱, 조 성 필,‡ 최 정 운
한양대학교

Spyware detection system related to wiretapping based on android power consumption and network traffics

Bum-joon Park,† Ook Lee, Sung-phil Cho,‡ Jung-woon Choi
Hanyang University

요 약

스마트 폰의 보급이 확대됨에 따라 많은 종류의 악성코드가 등장하였다. 이 중 스파이웨어는 기존과 다르게 운영체제가 제공하는 기능을 보안 정책에 따라 사용자의 동의를 정상적으로 획득하여 설치된다. 하지만 사용자가 의도하지 않은 기능을 내포하고 있는 스파이웨어는 기존의 악성코드 감지방법으로 쉽게 잡아내지 못하고 있다. 이러한 상황에서 본 논문은 스파이웨어 중 도청을 감지하는 연구를 진행하였으며, 스파이웨어가 가진 문제를 해결하기 위한 새로운 접근을 통해 도청 감지 모델과 이를 실행하는 어플리케이션을 개발했다. 음성 도청을 판별하기 위해서 각 어플리케이션별 전력 사용량 도출 기능, 모듈별 전력 사용량 도출 기능, 네트워크 사용량 감지를 수행하였다. 전력 사용량 도출을 위한 Open Source Project인 Power Tutor에 네트워크 사용량 감지 기능을 추가하였으며, 여기서 측정 및 수집된 데이터를 알고리즘을 거쳐 도청 위험도를 판별했다. 또한 이 논문에서 구축된 어플리케이션은 데이터 수집, 데이터 분석, 그리고 위험군 산출을 통해 도청 위험군을 감지한다. 어플리케이션을 스마트 폰에 설치하여 데이터의 측정 및 수집을 진행하였으며, 도청 시뮬레이션을 위해 Vice Application을 Background로 하여 사용하였다.

ABSTRACT

As the number of smartphone users have increased, many kinds of malwares have emerged. Unlike existing malwares, spyware can be installed normally after user authentication and agreement according to security policy. For this reason, it is not easy to catch spywares involving harmful functionalities to users by using existing malware detection system. Therefore, our paper focuses on study about detecting mainly wiretapping spywares among them by developing a new wiretapping detection model and application. Specifically, this study conducts to find out power consumption on each application and modular and network consumption to detect voice wiretapping so Open Source Project Power Tutor is used to do this. The risk assessment of wiretapping is measured by gathered all power consumption data from Open Source Project Power Tutor. In addition, developed application in our study can detect at-risk wiretapping spyware through collecting and analyzing data. After we install the application to the smartphone, we collect needed data and measure it.

Keywords: smartphone, spyware, wiretapping, detection

접수일(2015년 4월 14일), 수정일(1차: 2014년 6월 8일, 2차: 2014년 7월 20일), 게재확정일(2014년 7월 21일)

† 주저자, blackss2@nate.com
‡ 교신저자,dalycity@hanyang.ac.kr(Corresponding author)

I. 서 론

1.1 배경

안드로이드는 2008년 Virtual Machine 부분 소스코드를 제외한 나머지 부분에 한한 오픈 소스 기반의 운영체제로 출범하였다[1]. 이러한 안드로이드 운영체제는 출범 이후 스마트폰 시장이 급격하게 성장함에 따라 같이 성장하였으며, 오픈 소스와 Java기반의 운영체제라는 강점을 통하여 현재 가장 높은 점유율을 보이고 있다. 하지만 이러한 높은 성장률과 더불어 안드로이드의 취약점을 이용한 악성코드나 스파이웨어 등 보안에 대한 문제도 함께 빠르게 증가하였다[2].

Fig. 1.은 스마트폰 악성코드의 종류와 수를 나타내며, Fig 2.는 스마트폰 악성코드 유형의 종류와 수를 나타낸다. 그래프를 보면 스마트 폰 악성코드는 2004년에 처음 발견되었으며, 초기에는 그 수와 종류가 상대적으로 적었음을 알 수 있다 [3]. 그 후 스마트 폰 악성코드는 그 종류가 지속적으로 증가해왔으며, 최근에 이르러서는 증가 추세는 감소하고 있으나, 새로운 유형의 악성코드는 지속적으로 나타나고 있다. 이는 악성코드가 시스템을 공격하는 방식이 다양화 되고 있다는 점을 시사하고 있으며, 이에 따라 악성코드에 대한 방어 방법이 새로 개발되어야 하고 지속적인 대응 소프트웨어의 업데이트 또한 요구된고 할 수 있다.

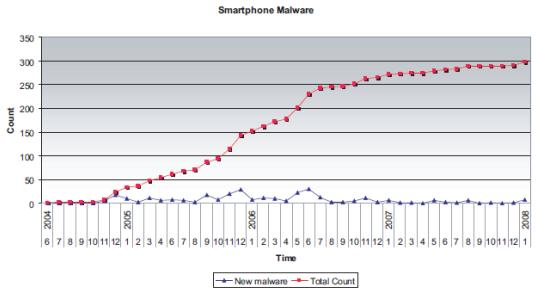

Fig. 1. Changes of smartphone malware count[3]

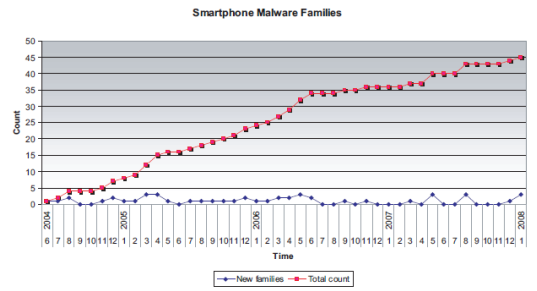

Fig. 2. Changes of smartphone malware families[3]

Table 1.을 보면 악성코드들의 공격 경로가 다양해지고 있는데, 대표적으로 스마트 폰을 감염시켜서 파일을 임의로 조정하거나 개인정보에 접근해서 데이터를 외부로 유출시킨다. 또한 스마트 폰의 어플리케이션을 사용할 수 없게 만들거나 메모리 카드에 접근할 수 없도록 한다.

Table 2.와 같이 악성코드의 감염이 전파되는 매개체들 또한 다양해지고 있다. 이 중 블루투스를 통한 근거리 감염과 MMS로 인한 감염이 가장 큰 비중을 차지한다.

이 때 감염된 스마트 폰은 작은 지역 네트워크를 형성할 수 있는데, 이러한 네트워크가 확산되면서 조직화된 정보 수집 및 감염 확산을 야기할 수 있다 한다[3].

이러한 여러 악성코드 중에서 스파이웨어는 사용자의 스마트폰에 설치되어 피해를 주고 있으나 대다수의 사용자들은 자신의 스마트폰에 스파이웨어가 설치되어 있는지 조차 인지하지 못하고 있다. 또한 설치가 된 것을 인지했다 하더라도, 언제 어떻게 설치되었는지 확인할 길이 없다고 한다. 이러한 이유로 근본적으로 배포가 되지 않도록 차단하기도 어려운 상황이며, 한 번 배포가 되면 지속적으로 피해를 야기하게 된다[4].

구체적인 사례를 통해 살펴보면, 스마트 폰 도입 초기 백신 프로그램에 감지되지 않았던 악성코드인

Table 1. Smartphone Malware Payload[3]

Payload	Quantity
Manipulate Files	155
Disable Applications	125
Drop	84
None	47
Disable Device	45
Infect Memory Card	32
Access Private Information	12
Send Private Information	8
Abuse Messaging	7
Boot Loop	2
Lock Memory Card	1
Backdoor	1

Table 2. Smarpthone Malware Infection Vector[3]

Medium	Quantity
Bluetooth	55
MMS	20
Memory Card	3
File Injection	2
Send Download Link	2

Caribe Security Manager가 있다. 심비안 운영체제에 존재한 이 어플리케이션은 자신을 보안 관리자라고 속인 후 주변의 블루투스를 통해 악성코드인 Caribe Worm을 전파하며, 지속적인 전파 시도로 인해 빠른 배터리 방전 및 수명 감소 등의 피해를 발생시켰다[3].

이제 안드로이드에 대해 살펴보면, 안드로이드의 보안 체계는 운영체제와 어플리케이션으로 나누어 구성되어 있으며, 어플리케이션은 운영체제가 제공하는 각 권한들을 보안 정책에 따라 획득하여 사용한다. 여기서 권한은 사용자 집단과 각 집단별 기능들에 대한 권한이 따로 존재하며, 각각의 어플리케이션은 이러한 기능들 중 필요한 기능을 명시하여 권한 내에서 사용 가능한 기능을 얻는 방식으로 구동된다[3]. 이러한 구동 방식에 문제점은 사용자 동의를 획득하여 설치되었지만, 위에서 언급한 것처럼 사용자가 의도하지 않은 기능을 내포하고 있는 스파이웨어가 나타날 수 있다는 점이다. 불법적으로 설치되지 않았으며, 사용자의 동의를 얻어서 설치되었기 때문에 쉽게 잡아내기 어렵다. 따라서 이러한 문제를 해결하기 위한 새로운 접근이 요구된다.

1.2 연구의 필요성

개인 정보가 침해되는 것은 사회문제로 대두되고 있다. 2010년 6월 9일 AT&T를 통해 일반인은 물론 미 정부 관계자, 기업 최고 경영자 등 아이패드 사용자들의 개인 정보가 누출되었다. 그리고 2010년 9월 국내 주식 정보 제공 업체 e토마토가 사용자 정보를 허가 없이 수집한 혐의로 기소되었다. 해당 회사는 '증권통'이라는 주식 정보 제공 어플리케이션을 통해 사용자들에게 동의를 받지 않고 휴대전화 번호, 국제단말기인증번호(IMEI), 범용가입자식별모듈(USIM) 카드 일련번호 등을 수집하였다. 이는 사용자들에게 표시되지 않은 형태로 데이터를 유출시키는 소프트웨어인 일종의 스파이웨어로 분류되어 기소

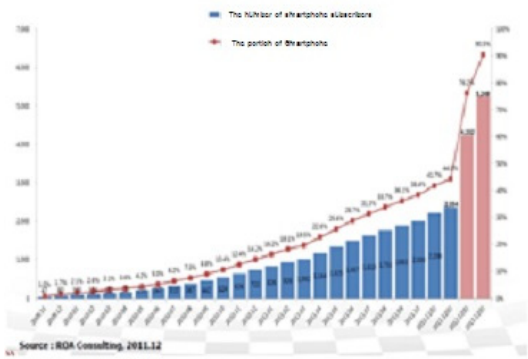

Fig. 3. Smartphone importance contrasting with number of domestic subscribers to the smartphone and number of total subscribers[6]

되었다.

Fig.3.을 보면 국내에서 스마트폰 가입자 수가 2009년 이후 꾸준히 증가했고 2011년 이르러서는 기하급수적으로 증가 했다는 것을 알 수 있다. 또한 스마트폰 비중은 2013년 90.5% 차지하게 되어 국민 대부분이 스마트폰을 이용하고 있다는 사실을 반증하고 있다.

Fig.4.은 개인정보 침해신고 상담건수를 나타내는데 개인 정보 침해 건수도 증가하게 되었다는 점을 우리는 알 수 있다. 상담건수가 2003년 ~ 2005년까지 2만 건 미만의 신고가 접수되었다, 하지만 2008년에 들어서 4만 건으로 증가하였고, 2012년에 들어서는 16만 건으로 2010년도 대비 3배 증가하였다. 이를 통해 우리는 스마트 폰 보급의 증가에 따라 개인 정보 침해신고 상담건수도 이에 비례하여 증가하였다는 점을 알 수 있다. 2010년도부터 개인정보

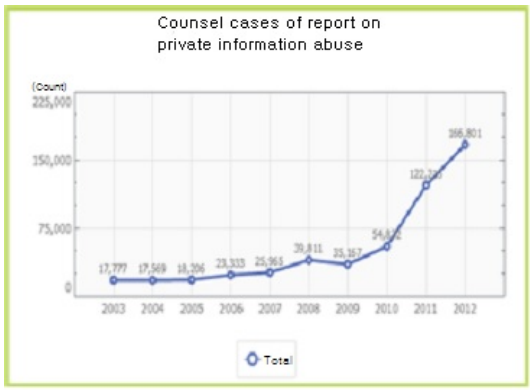

Fig. 4. Counsel cases of report on private information abuse[5]

침해 건수가 급증 하였으며 2012년에 들어서는 16만 건이 된다. 이는 스마트 폰 보급이 증가하기 시작하는 시기와 맞물린다. 이런 점에서 스마트 폰의 사용이 확산됨에 따라 스마트 폰 내부에 저장되는 이메일과 같은 개인정보 또한 증가하고 있다고 볼 수 있다. 이러한 현상은 해킹, 스파이웨어, 바이러스 등으로 인한 보안상의 사고를 야기할 수 있다.

스마트 폰의 개방형 플랫폼은 자유로운 소프트웨어 시장을 형성하였다. 하지만 동시에 많은 보안 취약점을 가지고 있어 개인에게 많은 피해를 줄 수 있다. 이러한 개방형 플랫폼은 어플리케이션에 대한 제작, 유포 등이 통제되지 않고, 앱 스토어를 통해서 악의적인 목적으로 제작된 소프트웨어가 대규모로 사용자에게 노출될 수 있기 때문이다.

'스마트 혁명이 가져온 변화 : 주요 성과와 과제'[7]에 따르면 국내 주요 기업의 스마트워크 도입 비율은 7.7%(136개)이고, 스마트 오피스 도입 비율은 2010년 이전에 16%에서 2010년 32%, 2011년 52%이다. 이러한 수치는 스마트 폰의 확산에 따라 모바일 오피스가 확산되고, 이에 따라 개인 및 기업 정보의 유출 위험이 증가하고 있음을 시사한다. 따라서 스마트 폰에서 개인 정보 유출을 야기하는 스파이웨어의 감지 및 대처가 중요해지고 있다.

Table 3.를 참고하면 스마트 폰에는 현재 여러 종류의 취약점이 존재하는데 세계보안엑스포 2013에서 발표한 보안 방안 에스원의 자료에 따르면 5가지 종류의 보안 취약점이 존재함을 명시하고 있다.

상기 보안 취약점 중 악성코드와 스파이 어플리케이션은 실제 사용자 스마트 폰의 소프트웨어 상에서 작용을 한다. 감염된 악성코드는 사용자의 스마트 폰에 악영향을 끼치지만 스파이 어플리케이션은 사용자의 스마트 폰에 영향을 주지는 않으나, 정보를 지속적으로 유출시킨다. 예로 2013년 4월 스마트 폰을 이용해 도청, 위치추적 등에 이용되는 소프트웨어를 판매 및 운영한 혐의로 30대 남성이 구속된 사건이 있다[9]. 이러한 도청 어플리케이션은 피해자의 통화, 영상, SMS, 위치(GPS), 인터넷 사용 정보 등 거의 모든 사생활 정보를 유출시킬 수 있다.

그 동안은 문제를 발생시키는 코드 탐지를 기반으로 하는 악성코드에 대한 위주로 다양한 방법론적인 연구가 이루어져 왔었다[10]. 하지만 위의 예시와 같이 악성코드 외에도 정상적인 코드와 기능을 조합하여 사생활 정보 유출과 같은 피해를 주는 스파이웨어 어플리케이션이 증가하고 있으며, 이에 따라 정보

Table 3. Types of Smartphone Hacking[8]

Type	Content
Theft/Loss	the leakage of private information or storage data. addition probability of a crime associated with finance.
Malware	billing induced : SMS transmission to unspecified individuals. information leak : user private information leakage outside. computer Errors : unavailable with terminal function except calling. battery consumption : power consumption of smartphone.
WLAN	automatic connection of fake wireless AP or wifi : Hackers feigned as known wifi leak private information though automatic connection.
Spy App	stealth mode, telecomputing. children • employee • spouse monitering. telephone records, SMS, location information, e-mail, accessing URL, picture leakage.
Smishing	Combined word of SMS and Phishing. Message involved in shortening URL with message to invite app installation and to arrive free coupon. New method getting pin number of micropayment by infecting malware that can steal SMS when accessing website.

유출에 관한 피해가 증가하고 있다. 따라서 악성 코드는 아니지만 사용자의 데이터를 지속적으로 누출시켜 피해를 입히는 스파이웨어에 대한 다른 접근이 필요하고, 스파이웨어 탐지에 대한 연구 또한 이루어져야 한다.

1.3 목적

스마트 폰의 스파이웨어는 일반적인 바이러스와는 달리 정상적인 동작들을 기반으로 존재하기 때문에 개인이 자신의 정보가 유출되고 있다는 사실을 인지하기 어려운 면이 있다. 스파이웨어는 목적에 따라 다양한 형태로 존재하는데, 이 중 유출 시 개인적인 피해는 크나, 상대적으로 감지 가능성은 다소 높은 도청 관련 스파이웨어를 탐지하려는 연구를 진행시켜 보고자 한다.

II. 이론적 배경

바이러스가 아닌 형태의 악성코드를 연구하기 위한 다양한 접근방법들이 제시되었다. 한 접근방법으로 스마트 폰을 위한 'Intrusion Detection System'이 있다[11]. 이 접근방법은 모바일 폰 네트워크의 요청 전에 서로의 송수신 내역을 검토하여 네트워크 주소 변환이나 데이터 도청과 같은 비정상적인 행동들을 차단하는 방법이다. 해당 알고리즘은 학습을 기반으로 하고, 비정상적인 내역들에 대하여 사용자 정보를 토대로 이를 재감지 하기 위한 신호를 생성한다.

상기 'Intrusion Detection System'을 체제화하자는 제안이 있었다[12]. 이는 우선 학습된 내역들이 백 엔드 서버에 전송된다. 이후 발견된 비정상적인 행동들은 이 서버를 통해 새로운 감지 방법을 받는 방식으로 구성되어있다. 또한 상관관계를 가진 엔진을 이용하여 기기에 맞는 네트워크 침해 감시 방법을 제안하였다.

다른 접근 방법으로 동력 고갈 공격을 감지하기 위한 연구가 있다[13]. 이 방법은 전력의 사용을 예측하고, 전력이 누수되고 있을 가능성이 존재하는지 예측한다.

또 다른 접근 방법으로는 위의 방식과 다른 배터리 기반 감지 연구방법이 있다[14]. 해당 연구는 기기의 전력 소모를 어플리케이션의 행동과 'Rule-based Host Intrusion Detection Engine'를 이용하여 측정하여 감지한다.

마지막으로 스마트 폰이 가진 자료 사용에 대한 부담을 모으고, 해당 데이터를 분석하여 감지하는 연구방법이 있다. 해당 연구는 미처리 데이터를 분석한 후 결과를 수집하는 것이 아니라 수집 후 분석하여 좀 더 다양한 분석이 가능하였다.

III. 연구 방법

3.1 감지 모델 도출

불법적인 목적을 가지고 개발된 어플리케이션은 감지가 어렵다. 스파이웨어 감지 알고리즘은 연구가 미비하고, 기존에 존재하는 알고리즘은 재 배포되는 어플리케이션만을 감지할 수 있거나, 악성코드를 탐지하는 방법을 이용하기 때문이다. 코드 감지를 이용한 방법 또한 모니터링과 결합한다 해도 합법적인 어플리케이션과 불법적인 어플리케이션을 구분하기가 어렵다.

이러한 어려움은 불법적인 어플리케이션 전체를 감시하려는 접근에서 발생하며, 각 불법적인 어플리케이션을 유형별로 나누어 접근한다면 현실 가능성 있는 감지 모델이 도출될 수 있다. 본 논문에서는 이와 같은 문제를 해결하고자 도청 감지 모델 수립을 목표로 잡았으며, 어플리케이션의 행동 패턴을 이용하여 감지하는 방법을 사용하였다. 행동 패턴을 이용하기 위하여 전력량 및 네트워크 통신량에 대한 데이터 수집이 필요했으며, 2장에서 제시된 논문들의 기법을 참고하여 전력 소모량 수집 데이터와 기기 자료 소모 데이터를 이용한 감지 모델을 도출하였다. 상기 모델에서 제시된 것들이 주로 전력 소모 공격을 감지하는 모델들이었다면, 도출한 감지 모델은 음성 도청을 감지한다. 기존 모델에서는 기기에서 제공하는 배터리 상태를 이용하는 전력 소모 감지 방법을 사용하였다. 하지만 스마트 폰에서는 어플리케이션별로 배터리 소비를 판별하여야 한다. 이에 따라 운영 중인 어플리케이션별, 모듈별 전력 소모를 산출하고 이를 통해 각 어플리케이션별 전력 소모와 총 전력 소모를 산출한다. 여기에 전력 소모 모니터링을 중심으로 CPU 사용량과 네트워크 사용량, 그리고 어플리케이션이 활성화된 시간 데이터를 추가적으로 수집한다.

일반적으로 사용자 설치한 어플리케이션은 사용자가 이용하기 위하여 선택하여 설치하게 되며, 이는 대다수의 어플리케이션이 활성화되는 동안 주로 활동함을 알 수 있다. 이러한 점에 착안하여 대다수의 어플리케이션이 활성화 시간 동안 전력 및 기기 자원을 소모한다는 점을 이용해 기기가 비활성화 되어있는 동안의 전력 및 기기 자원을 수집하였으며, 네트워크 데이터 사용량에 대한 정보 또한 함께 수집하여 외부로 데이터를 보내는 어플리케이션을 선별하였다.

상기 수집된 데이터로 도청 감지 모델을 수립하기 위하여 도청 어플리케이션의 행동 유형을 크게 두 분류로 나누어 예측해 보았다.

1) 음성 도청을 수행하면서 동시에 도청 데이터를 외부에 송신
2) 음성 도청을 수행한 데이터를 저장해두고 후에 도청 데이터를 외부에 송신

1)의 경우 외부 사용자가 도청을 시작하고 종료할 수 있어야하며, streaming 방식의 전송이 필요함을

알 수 있다. 2)의 경우 외부 사용자가 도청을 시작하고 종료하는 것을 정하기 어려우므로, 지속적으로 도청을 하고 이를 압축한 후 외부에 데이터를 전송해야 함을 알 수 있다. 2)의 방법의 경우 전력사용량 등이 과다하여 배터리가 빠르게 방전되거나 조기에 발견될 여지가 있어서 1)의 방법을 중점적으로 탐구하였다.

도청을 위해서 어플리케이션은 Background에서 지속적으로 동작하고 있어야하며, 외부의 도청 시작/종료 신호를 받기위한 신호 감지하는 행동과 음성 정보를 획득하고 이를 변환하여 외부에 전송하는 행동을 해야 하며, 정리하면 다음과 같은 특징을 가지게 된다.

1) Background에서 실행되며, 지속적으로 실행되고 있음
2) 네트워크 트래픽을 발생시키며, 최소 음성 bps 이상을 발생시킴
3) 네트워크 수신량은 적고 송신량은 많음

이러한 점을 이용하여, Network Tx(Transfer)가 존재하는 어플리케이션을 산출하고, 총 전력 사용량 및 데이터 전송량이 어플리케이션 활성화 시간을 나타내는 지표인 LCD(화면) 전력 소모에 비해 많은 어플리케이션을 산출하여 음성 도청 위험군을 산출하였다.

좀 더 정확한 전력량을 산출하기 위해 Open Source Project인 Power Tutor를 이용하였다. Open Source Project인 Power Tutor는 전력 소모량에 대한 데이터를 수집하고 수집된 데이터를 일부 저장해두었다가 그래프로 보여주는 어플리케이션이다.

Power Tutor는 전력 소모를 측정하기 위해서 스마트 폰에 존재하는 여러 모듈들(GPS, Network, Wifi, LCD 등)의 작동 시간을 측정하고, 안드로이드 운영체제 버전 및 스마트 폰 기종에 따른 가중치를 이용해서 측정된 소모 값에 대한 데이터 품질을 높인다. 이렇게 Power Tutor에서 제공하는 기능에 네트워크 데이터 소모량에 대한 데이터를 측정하는 모듈을 추가하여 데이터를 수집하고, 내부에 측정된 데이터를 어플리케이션 별로 모아서 해당 데이터를 서버 상의 DB에 계속 축적하였으며, 분석 시점에 해당 DB에서 데이터를 내려서 모듈별 측정값을 어플리케이션 별 측정값으로 변환하고 연속 이용 시간 등을 재산출 하였다.

3.2 알고리즘을 적용한 어플리케이션 제작

음성 도청을 판별하기 위한 시스템에는 다음과 같은 3가지 기능이 필요했다. 해당 기능들은 각 어플리케이션 별 전력 사용량 도출 기능, 모듈 별 전력 사용량 도출 기능, 그리고 네트워크 사용량 감지 기능이다. 전력 사용량 도출을 위한 Power Tutor에 네트워크 사용량 감지 기능을 추가하였으며, 여기서 측정 및 수집 된 데이터를 알고리즘을 거쳐 도청 위험도를 판별한다.

Network Tx를 구하기 위해서는 안드로이드 API에 존재하는 트래픽 상태를 이용하였다. 우선 안드로이드에서 실행중인 어플리케이션 목록을 수집하고, 해당 어플리케이션의 처리정보 및 uid를 기반으로 한 전력데이터에 Network Tx 데이터를 추가하였다.

UID 별로 수집된 정보 어플리케이션 정보와 조합시키고, 어플리케이션별/모듈별 전류, 네트워크 수신량(Bytes), 네트워크 송신량(Bytes)으로 구성된 데이터를 6초 간격으로 수집하였다. 분석 시 대기하고 있는 부분으로 인해 불필요하게 네트워크 사용량이 제대로 잡히지 않을 것을 고려하여 네트워크 송수신이 없는 데이터는 제외시키고 분석하였다. 수집된 데이터에서 LCD 모듈의 사용량을 통하여 직접 사용중 여부를 산출하였고, 이를 통하여 사용시간과 송신량(Rx)와 수신량(Tx)에 대해서 bps를 산출하였다.

또한 네트워크 대역폭이 존재하는 어플리케이션 58개에 대해서 12개의 유형으로 분류하였다. 12개의 유형으로는 시스템, 위치기반, 구글(동기화 등 도청 패턴과 유사), 메신저, 주식, 웹하드, SNS, 쇼핑, 미디어, 스토어, 인터넷, 게임가 존재한다.

음성 도청 어플리케이션의 시뮬레이션은 음성 어플리케이션을 배경으로 구동해둔 채 실제 스마트 폰을 사용하여 이루어졌다. 사용된 어플리케이션은 되도록 낮은 bps를 가지도록 설계되었으며, 외부에서 원하는 시점에 한하여 음성 데이터를 송신하도록 설정되었다. 그 외의 시간 동안은 외부에서 신호를 받기 전까지는 도청이 동작하지 않도록 설정하였다.

이렇게 측정한 결과는 Table 4.와 같다.

IV. 연구 결과 및 논의

Table 4.를 보면 스마트폰 어플리케이션 사용량 분석 데이터가 존재한다. 해당 표는 12개의 분류와 1개의 도청 분류로 총 13개의 분류를 가진다. LCD 사용량은 적으면서 송신량(Tx)가 많은 순으로 정렬하였다. 그리고 모든 데이터는 사용 편차를 줄이고자 10분 단위로 샘플링하여 합산하였다.

각 유형 중 도청 어플리케이션이 화면 전면에 나타나지 않는 특성을 이용하여 LCD의 Median값이 0인 분류를 선별하였으며, 이에 해당하는 3개의 분류로는 시스템, 위치기반, 구글이 존재하였다.

음성 도청이 가능한 네트워크 대역폭을 조사하였으며, streaming이 불가능한 낮은 bps 대역을 제외한 telephone quality를 위한 최소 kbps인 8kbps에서 Android 기본 음성 포맷 중 하나인 mp3 음성 포맷의 최고품질 포맷인 320kbps 사이의 네트워크 대역을 가진 네트워크 송신 대역을 확인하였다[15].

양쪽 데이터를 겹쳐서 비교해보면, 도청 어플리케이션이 이에 적합함을 확인할 수 있다. 도청 어플리케이션과 유사한 행동 패턴을 보일 수 있는 유형들로는 구글(동기화 어플리케이션), 웹하드(백그라운드 송수신 어플리케이션), 위치기반이 존재한다. 여기서 각 패턴별로 구글과 같은 동기화 어플리케이션들은 평균 송수신량이 낮았으며, 실행시간이 30일간 1시간 내외로 낮은 양상을 보였다. 웹하드의 경우는 평균 수신량이 10mbps 이상이며, 실행 시간이 30일 간 1시간 미만으로 낮은 양상을 보였다. 위치기반은 송신량보다는 수신량이 큰 양상을 보였다.

위와 같은 유형별 분석을 통하여 음성 도청이 가능한 네트워크 대역폭을 가지며, 이와 비슷한 패턴을 가지는 어플리케이션은 실제 사용자가 사용하는 어플리케이션들 중에서 거의 존재하지 않음을 확인할 수 있었다. 우선 거의 대부분 시간 동안 백그라운드에서만 동작한다는 점에서 일반 어플리케이션은 제외되며, 시스템/동기화 어플리케이션과 정보/서비스제공 어플리케이션 그리고 송수신용 어플리케이션이 남은 경우에 해당함을 알 수 있다. 여기서 시스템/동기화 어플리케이션은 단위 시간당 평균 사용 시간이 낮고 총 사용 시간 또한 낮아서 다른 어플리케이션과 확연하게 구분되는 특징을 가지고 있었다. 그리고 정보/서비스 제공 어플리케이션은 외부의 정보와 서비스를 제공 받는 입장이므로 주로 수신에 치중되어 있으며 송신량은 평균 1kbps 미만으로 많지 않음을 알 수 있었다. 마지막으로 송수신용 어플리케이션은 송수신 속도에 초점을 맞춘 만큼 수신량이 훨씬 많고 그 대역폭이 몇 백배 차이가 나며, 필요할 때만 켜는 만큼 총 사용 시간은 전체에서 낮은 편에 속하였다. 이러한 특성을 통하여 도청 어플리케이션은 동작 패턴과 네트워크 송수신량 패턴에서 다른 어플리케이션과 확연히 구분되는 특징을 가짐을 보였다.

실험 결과를 토대로 도청 가능성을 탐색하는

Table 4. Smartphone Application Usage Analysis

Type	Number	Mid LCD (mA)	Avg LCD (mA)	Seconds (30 days)	Mid Rx kbps	Avg Rx kbps	Mid Tx kbps	Avg Tx kbps	Alice Index
Wiretapping	1	0	0	237180	0	6	20	27	20.50
System	1	0	0	10392	2	29	0	25	-3.00
LBS	1	0	0	9822	10	11	0	1	-10.00
Google	3	0	0	4026	6	8	0	0	-7.00
Messenger	4	1	193	62016	20	15	4	5	-401.00
Stock	2	108	166	176034	6	6	1	1	-553.00
Webhard	2	255	222	3216	13190	11970	4.5	14	-13524.75
SNS	3	396	338	16500	164	309	16	137	-1628.00
Shopping	4	410	302	3972	430	415	31	25	-1818.50
Media	12	436	327	156786	2240	2063	23	368	-3482.00
Store	1	453	456	1668	626	567	31	28	-2385.00
Internet	7	467	450	62718	422	651	17	21	-2351.50
Game	18	484	427	182820	2	70	1	2	-1856.50

Alice Index를 정의하였으며, 그 공식은 (Mid Tx + Avg Tx)/2 - Mid(Rx + Avg Rx)/2 - (Mid LCD + Avg LCD)/2/512*1024 이다. 네트워크 송신량이 높고, 수신량이 낮을 수록 지수가 높아지고 사용자가 지속적으로 직접 사용하는 앱은 도청앱일 가능성이 낮음을 나타내었다. 주 음성통신 네트워크 대역폭 단위인 kbps로 나누어 네트워크 송수신량 수치를 쉽게 비교할 수 있도록 하였다. 또한 LCD 사용량의 경우 초당 최대 사용 측정량인 512mA로 나누어 연속된 LCD 사용이 초당 1Mbps의 수신과 같은 의미를 가지도록 1024를 곱하여 사용자가 직접 사용하는 앱은 도청앱이 아닐 가능성이 높도록 가중치를 부여하였다. 그 결과 유일하게 도청앱이 양수의 Alice Index를 가졌으며, 이와 유사한 동기화(System, Google) 앱이 다른 앱에 비해 상대적으로 높은 가중치를 가지었다. 사용자가 매일 사용하는 Daily 앱이나 송신 위주의 앱은 굉장히 낮은 Alice Index를 보였으며, 이를 통하여 Alice Index가 도청앱을 식별하고 유사한 패턴을 가지는 앱을 확인 할 수 있음을 알 수 있다.

완성된 어플리케이션은 Power Tutor를 기반으로 하며 이를 통해 추출된 데이터 수집 및 가공을 통하여 감지한다. Power Tutor에서 데이터 수집을 표현하는 화면은 Fig.5.와 같다.

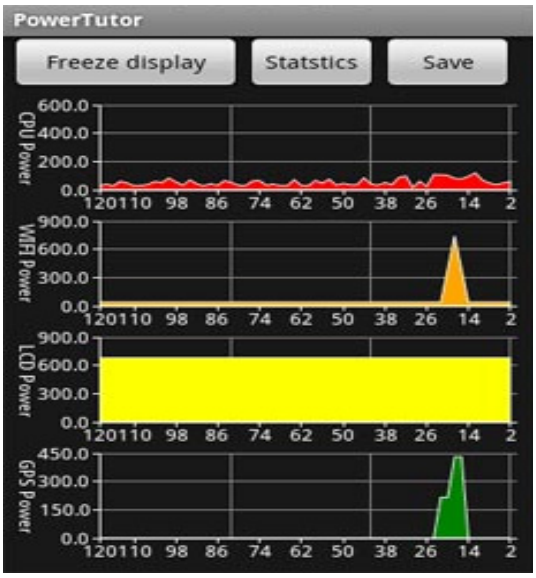

Fig. 5. PowerTutor operating with added Network Module

V. 결 론

도청 감지 모델을 통하여 배경에서 음성을 수집하여 전송하는 어플리케이션의 전력 및 네트워크 사용량 데이터 패턴을 파악할 수 있었다. 그리고 사용 패턴을 통해 음성을 수집하여 전송하는 어플리케이션이 도청 감지 모델에서 높은 위험성을 가짐을 보았다. 현재 모델은 기존의 바이러스와 탐지와 같은 코드 변조 기반의 탐지 방법이 아닌 정상적인 기능들을 조합하여 사용자의 정보를 유출하는 스파이웨어 중 음성 도청을 탐지 하는 한 가지 방법이며, 이러한 모델을 통하여 스파이웨어의 탐지는 기존 코드 변조 기반의 탐지 방법을 통하여 찾아내기 어려우며, 각 스파이웨이 목적별로 감지 모델이 서로 달라야함을 나타낸다.

현재 알고리즘의 한계점은 어플리케이션의 탐지 데이터를 샘플링하여 사용하므로, 탐지 데이터를 수집하는데 걸리는 시간이 길다는 점과 감지 가능한 어플리케이션이 위의 감지 모델을 고의적으로 회피하는 경우 파악하기 어렵다는 점이 있다. 이러한 한계점의 주요 원인은 도청이라는 특정 행위를 감지하고자 하는 목표와 제시된 모델을 알지 못 한 채로 개발된 도청감지 어플리케이션을 감지한다는 가정에 있다. 이를 해소하기 위해서는 어플리케이션들이 가지고 있는 퍼미션을 조사하여 실제 도청이 가능한 어플리케이션을 선별하고, 이 후 사용 패턴을 조사하여 모니터링을 수행하는 시스템을 개발하여야 한다.

References

〔1〕 Android (operating system),Wikipedia, 2013.07,http://ko.wikipedia.org/wiki/%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C_(%EC%9A%B4%EC%98%81_%EC%B2%B4%EC%A0%9C).

〔2〕 Symantec internet security threat report, Symantec Corporation, vol.18, pp.10,Apr.2013.

〔3〕 Aubrey-Derrick Schmidt and Sahin Albayrak ,"Malicious Software for Smartphones," Technical Report, pp.19-20,Feb. 2008.

〔4〕 Sang Wook Nam, "A study on counterplan of Spyware being abused on the Web,"

Korea University, pp.1-47, Dec.2014.
〔5〕 e-Nara Jipyo ,The number of counseling for private information abuse, 2012.,http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366
〔6〕 Jin-young Kim, “2012 Mobile Market Forecasts,” ROA CONSULTING, pp.6, Feb.2011.
〔7〕 Junbong Baik, MyoungHo Choi, Bumseok Hong and Eugene Park, "Variation from Smart Revolution : The Achievements and Tasks," kt economy & business research institution, pp.12, 2012.
〔8〕 SungIl Kim and Hyunna Cha, "The threats and responses of smartphone hacking," kt economy & business research institution pp.2, 2013.
〔9〕 Heongdu Park, "The first detetion of tapping-app in korea", The KyungHyang
〔10〕 Hwashin Moon, Bohong Jung, Yongsup Jeon and Jungnyou Kim, "A Survey of Mobile Malware Detection Techniques," ETRI, pp.5-7, 2013.
〔11〕 D. Samfat and R. Molva , "IDAMN: An Intrusion Detection Architecture for Mobile Networks," IEEE Journal on Selected Areas in Communications,Vol 15. ,no. 7, pp.1373 - 1380, Sep. 1997.
〔12〕 M. Miettinen , P. Halonen and K. Hätönen, "Host-Based Intrusion Detection for Advanced Mobile Devices," In: AINA '06: Proceedings of the 20th International Conference on Advanced Information Networking and Applications - Vol. 2 (AINA'06), Washington, DC, USA, IEEE Computer Society, pp. 72 - 76, 2006.
〔13〕 D.C. Nash, T.L. Martin, D.S. Ha and M.S. Hsiao , "Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices," In: PERCOMW'05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, Washington, DC, USA, IEEE Computer Society, pp. 141 - 145, 2005.
〔14〕 G.A. Jacoby , R. Marchany and N.J.Davis IV. , "How mobile host batteries can improve network security," IEEE Security and Privacy, Vol 4., no 5.,pp. 40 - 49, 2006.
〔15〕 J. Cheng, S.H. Wong, H. Yang and S. Lu, "Smartsiren: virus detection and alert for smartphones," In: MobiSys '07: Proceedings of the 5th iternational conference on Mobile systems, applications and services, New York, NY, USA, ACM, pp. 258 - 271, 2007
〔16〕 Audio, Multimedia, Bit_rate : http://en.wikipedia.org/wiki/Bit_rate

〈저 자 소 개〉

박 범 준 (Bum-joon Park) 정회원
2012년 2월: 한양대학교 제2공과대학 컴퓨터전공과 졸업
2014년 2월: 한양대학교 정보시스템학과 석사
2014년 3월~현재: 한양대학교 정보시스템학과 박사과정
〈관심분야〉 정보보호, 의료시스템, 기기보안

이 욱 (Ook Lee) 정회원
1987년 2월: 서울대학교 계산통계학과 졸업
1989년 6월: Northwestern대학교 전산학과 석사
1997년 1월: Claremont대학교 경영정보학과 박사
2002년 3월~현재: 한양대학교 정보시스템학과 교수
〈관심분야〉 정보보호, IT 형태/철학/응용

조 성 필 (Sung-phil Cho) 정회원
2008년 2월: 한양대학교 정보기술경영학과 졸업
2011년 1월: Claremont대학교 경영정보학과 석사
2014년 2월: 한양대학교 정보시스템학과 박사
〈관심분야〉 IT 거버넌스, 정보보호, 전자정부

최 정 운 (Jung-woon Choi) 정회원
2012년 8월: 홍익대학교 경영학과 졸업
2014년 9월~현재: 한양대학교 정보시스템학과 석사과정
〈관심분야〉 정보처리, 정보보호