Journal of The Korea Society of Computer and Information
Vol. 17, No. 11, November 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.11.101

개인정보보호를 위한 안드로이드 로그캣 시스템 연구

장 혜 숙*

Android Log Cat Systems Research for Privacy

Hae-Sook Jang*

요 약

최근 스마트폰의 급격한 보급으로 개인정보 침해사고 및 프라이버시 침해를 통한 여러 가지 사회문제가 급속도로 증가하고 있으며, 이에 따라 개인정보보호를 위한 다양한 연구 및 기술개발이 이루어지고 있다. 개인의 모든 정보가 거의 들어 있다고 해도 과언이 아닌 스마트폰의 정보유출은 우리의 일상에서 쉽고 빈번하게 발생할 수 있는데, 포렌식 분석 툴을 이용하여 증거를 수집하거나 분석하기란 쉽지 않은 일이다. 현재 안드로이드 포렌식 연구는 비휘발성 메모리로부터 데이터를 수집하여 분석하는 기법에 집중되어 왔으며, 휘발성 데이터에 대한 연구는 미미한 실정이다. 안드로이드 로그는 휘발성 저장매체로부터 수집될 수 있는 휘발성 데이터이다. 안드로이드 로그는 안드로이드 시스템에서부터 애플리케이션에 이르기까지 최근의 모든 구동내역과 관련한 기록이 로그로 저장되기 때문에 안드로이드폰 사용을 추적할 수 있는 자료로 활용이 충분하다. 본 논문에서는 포렌식 분석 툴을 이용하지 않고 로그를 필터링하여 개인의 정보 유출 유무를 판단하여 대응할 수 있는 방법을 제시한다.

▸ Keywords : 안드로이드, 컴퓨터 포렌식, 로그캣

Abstract

Various social problems through violating personal information and privacy are growing with the rapid spread of smartphones. For this reason, variety of researches and technology developments to protect personal information being made. The smartphone, contains almost all of the personal information, can cause data spill at any time. Collecting or analyzing evidence is not an easy job with forensic analyzing tool. Android forensics research has been focused on techniques to collect and analyze data from non-volatile memory but research for volatile data is very slight. Android log is the non-volatile data that can be collected by volatile storage. It is enough to use as a material to track the usage of the Android phone because all of the recent driven records from system to application are stored. In this paper, we propose a method to respond to determining the existence of personal information leakage by filtering logs without forensic analysis tools.

▸ Keywords : android, computer forensic, logcat

•제1저자 : 장혜숙
•투 고 일 : 2012. 09. 10, 심사일 : 2012. 10. 06, 게재확정일 : 2012. 10. 12.
* 군산대학교 컴퓨터정보공학과(Dept. of Computer and Information Engineering, Kunsan National University)

I. 서 론

스마트폰의 개인정보 침해사고 및 프라이버시 침해사고는 다른 일반 정보보호 침해사고와는 다르게 당사자에게는 치명적인 경제적, 정신적 피해를 주는 것이 특징이다. 개인정보 침해 사고를 발생시키는 원인으로는 급격한 스마트폰의 보급으로 손쉽게 외부에서의 불법적인 접근이 가능하기 때문일 것이다. 의도에 의한 개인정보 유출, 개인정보 노출 등은 날이 갈수록 우리사회의 범죄의 수단으로 자리 잡고 있다고 해도 과언이 아닐 것이다. 최근 몇 년간 우리는 크고 작은 개인정보 침해사고를 경험했다. 이미 전 국민의 개인정보가 한번 씩은 유출 당했다고 해도 과언이 아닐 것이다. 정유사, 게임사, 금융사, 인터넷쇼핑몰 등 대량으로 개인정보를 취급하는 곳에서 주로 개인정보 유출사고가 일어났으며, 특히 작년에는 SK 컴즈에서 3,500만 개인정보가 유출되는 초대형 사고가 발생해 다시 한번 개인정보 보호의 필요성이 대두되기도 했다. 방송통신위원회에 따르면, 지난 4년간 연이은 대형침해사고 발생으로 인한 개인정보침해건수가 1억 600만여 건에 이른다고 한다. 최근 들어서는 페이스북, 트위터 등 이른바 소셜 네트워크 서비스(SNS)를 통한 개인정보 침해도 눈에 띄게 늘고 있다. 페이스북, 트위터, 카카오 스토리 등은 거의 스마트폰을 이용하기 때문에 스마트폰을 이용한 개인정보 유출로 보아도 무리가 없을 것이다. 스마트폰은 컴퓨터 기능과 휴대폰 기능을 합친 것이다. 스마트폰은 PC와 유사한 수준의 강력한 성능으로 다양한 서비스를 제공하고 있다. 이에 따라 스마트폰의 판매량은 시장조사 업체 SA(Strategy Analytics)의 발표에 의하면 2010년 2분기 현재 3억 3천만대 수준이다. 이동통신 기술이 발전함에 따라 스마트폰 사용자수는 계속 증가하면서, 스마트폰 정보 유출의 문제점도 같이 증가 하고 있는 상황이다. 이에 따라 악의적 사용자에 의해서 저작권 위반, 불법 거래 등 스마트폰을 이용한 범죄가 발생하고 있어 보안대책이 필요하다[1]. 본 논문에서는 페이스북, 트위터, 카카오스토리 뿐만이 아닌 모든 스마트폰의 정보가 보호 받을 수 있고, 스마트폰의 분석 도구 없이 본인 정보가 유출되었는지의 유무를 알 수 있고, 정보 유출시 빠른 대책을 강구 할 수 있도록 하기위한 컴퓨터 포렌식 스마트폰 정보 유출 방지 방안을 제시하고자 한다.

II. 관련 연구

1. 관련연구

1.1 디지털 포렌식

포렌식이란 증거를 수집, 보존, 처리하는 과정들을 법정에서 증거로 사용하기 위해 증거가치가 상실되지 않도록 하는 일련의 과정을 말한다[2]. 현재의 일상생활은 이동 중에도 컴퓨터로 검색하고 메일을 보낼 수 있으며, 영화도 볼 수 있는 모바일 기기들이 동반자가 되었는데, 이러한 기기를 이용한 범죄 또한 증가하고 있다. 이에 따라 컴퓨터에 저장되어있는 정보가 법정에 증거로 제출되는 경우가 많아질 수밖에 없는데, 이와 관련된 분야를 컴퓨터 포렌식 이라고 한다. 초창기 컴퓨터 포렌식은 법집행기관에서 컴퓨터 중심으로 압수, 수색이 이루어지고, 압수된 컴퓨터로부터 잠재적 증거를 발견하는 것에 중점을 두었다. 1998년부터 디지털 증거 자체에 주목하기 시작하여 명칭도 '컴퓨터 포렌식' 용어에서 디지털 포렌식으로 바뀌었다[3].

1.2 로그 정보

컴퓨터 관련 사이버 범죄가 일어났을 경우, 침입자의 흔적을 찾고자 할 때, 우리가 가장 먼저 취하는 행동은 침입자의 흔적(Digital Evidence)을 찾는 행위이다[4]. 이러한 행위에 가장 잘 사용되는 정보가 컴퓨터 내에 남아 있는 로그(Log) 정보라 할 수 있다. 이러한 이유로 로그정보는 불법적인 범죄자를 수사하기 위한 기초적인 정보가 될 수 있고, 재판에서는 범죄자를 구속하기 위한 법적인 증거 자료가 될 수 있다. 특히 초고속 인터넷에서는 웹(Web)을 이용한 중요한 정보와 금융 업무환경의 로그 기록 이 존재하는데, 로그 기록에는 시간이 적용된 로그 히스토리가 반드시 존재한다. 또한 컴퓨터 시스템에 불법적으로 침입한 공격자[5]는 흔적을 남기게 되는데 이러한 흔적이 저장되어 지는 곳을 로그 정보 파일이라 할 수 있다. 이러한 로그 정보 파일에는 시스템에 대한 스캔 행위, exploit 해킹 툴을 이용한 공격, 특정 사용자 계정으로의 접속, root 권한의 획득, 트로이 목마 설치, 자료 유출 및 삭제 등 공격자의 행위[6]들이 기록되어 진다.

1.3 스마트폰 개인정보 유출

스마트폰은 휴대전화와 개인용 휴대정보단말기(PDA)의 장점을 결합시킨 복합형 무선통신기기이다. 휴대전화의 기능에 PDA 기능을 추가한 것이 일반적인데, 음성통신은 물론 PC 연동, 개인정보관리, 무선 인터넷, 팩스 송수신 등이 가능하다. 기존의 일반폰은 전화, 문자, 전화번호부 관리 등, 간단한 기능만을 가지고 있으며 WIPI(Wireless Internet Platform for Interoperability)를 기반으로 응용프로그램들을 다운로드 할 수 있었다. WIPI는 한국 무선인터넷표준화 포럼에서 만든 무선 표준플랫폼으로 PC에서 윈도 운영체제와 비슷한 개념으로,

인터넷을 사용하기 위한 미들웨어이다[7]. 개인 정보 단말기인 PDA(Personal Digital Assistant)는 터치스크린을 이용하여 일정관리, 주소록, 계산기 등을 이용할 수 있으며, PC와 연동이 가능한 운영체제 기반의 작은 컴퓨터인데 여기에 전화기능이 합쳐지면서 스마트폰으로 발달하게 되었다. 스마트폰은 일반 폰보다 진보된 능력, 기능을 가지는 모바일 단말로 범용 운영체제가 탑재된 휴대폰으로 정의 할 수 있다[8]. 결국 스마트폰은 작은 PC라고 볼 수 있다. 폐쇄적인 일반 폰에 비하여 스마트폰에는 여러 가지 환경적인 요소들로 인한 개인정보 유출 위협이 존재한다.

III. 본 론

1.1 Android Logcat System

제안하는 개인정보 보호를 위한 안드로이드 로그캣 시스템은 빈번하게 발생할 수 있는 안드로이드폰의 개인정보 유출 후 유출확인 유무를 확인하여 유출된 정보 이용을 사전에 방지하기위한 시스템이다. 포렌식 분석 툴을 이용하지 않고 개인의 정보 유출 유무를 판단하여 대응할 수 있는 안드로이드 로그캣 시스템은 휴대폰에서 개인의 정보 유출이 의심될 때마다 간단하게 Logcat Tag를 필터링하여 정보유출 확인이 가능하게 된다.

1.2 시스템 설계

개인정보 보호를 위한 안드로이드 로그캣 시스템은 그림 1과 같이 구성하였다. 안드로이드 폰 사용자가 휴대폰을 분실 후 찾았을 때나 다른 누군가가 자신의 휴대폰을 사용한 흔적이 의심 될 때 개인정보가 유출 되었는지를 쉽게 확인 할 수 있도록 설계하였다.

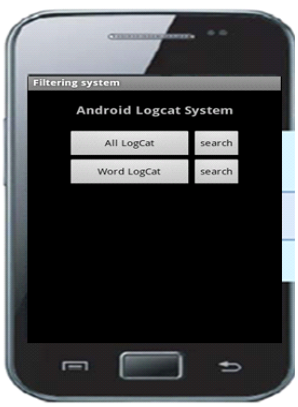

그림 1. 안드로이드 로그캣 시스템
Fig. 1. Android Logcat System

개인정보 유출 확인을 위해서는 안드로이드 로그캣 시스템 을 실행하여 Logcat 정보를 검색하여 불필요한 정보는 필터링하여 자신의 휴대폰 정보 유출 여부를 확인할 수 있도록 하였다.[9] 그림 1은 안드로이드 휴대폰에서 발생한 사소한 일들을 알아볼 수 있도록 로그캣 시스템을 개발하였다, 그림 1의 All Logcat 버튼을 클릭하게 되면 로그에 남아있는 정보를 확인할 수 있다. 그림 2는 전체 Tag를 검색한 경우이다. 전체 Tag를 검색하게 되면 너무 많은 로그정보가 검색되어 일반 사용자들은 어떤 정보가 유출 되었는지를 확인할 수가 없다.

Tag	Text
installd	DexInv: --- BEGIN '/system/app/LatinIME.apk' ---
dalvikvm	DexOpt: load 231ms, verify+opt 1322ms
installd	DexInv: --- END '/system/app/LatinIME.apk' (success) ---
BackupManage...	agentConnected pkg=com.android.inputmethod.latin agent=andro
BackupHelper...	handling new helper 'shared_pref'
LocalTransport	finishBackup()
dalvikvm	GC_EXPLICIT freed 103K, 51% free 2765K/5639K, external 716K/
SntpClient	request time failed: java.net.SocketException: Address famil
SntpClient	request time failed: java.net.SocketException: Address famil

그림 2. 전체 Tag 검색
Fig. 2. Search the entire Tag

그림 3은 Tag 위젯에 Media Scanner를 입력하고 button을 클릭하면 그림 3과 같이 Media Scanner Tag들만 검색되어진다. 휴대폰에 있는 정보 중 중요하거나 유출 의심이 가는 정보만을 Tag로 Logcat을 필터링하여 쉽게 유출확인이 가능하게 된다.

Tag	Text
MediaScanner...	start scanning volume internal
MediaScanner	prescan time: 900ms
MediaScanner	scan time: 262ms
MediaScanner	postscan time: 0ms
MediaScanner	total time: 1162ms
MediaScanner...	done scanning volume internal
MediaScanner...	start scanning volume external
MediaScanner	pruneDeadThumbnailFiles... android.database.sqlite.SQLiteCurs
MediaScanner	/pruneDeadThumbnailFiles... android.database.sqlite.SQLiteCur

그림 3. 필터적용 Tag 검색
Fig. 3. Apply Filter Tag Search

1.3 시스템 구현

안드로이드 로그캣 시스템을 구현하기 위한 프로젝트 구성은 안드로이드 application을 구성하기 위해 필요한 리소스인 자바 소스 코드, 참조할 라이브러리, 화면 레이아웃을 위한 XML과 applecation 컴포넌트들의 상호작용을 정의한 매니페스트 파일등으로 구성하였다. 화면 설계는 LinearLayout 2개와 TextView 위젯과 Button 위젯을 이용하였다. 그림 4는 로그캣 분석을 위한 문자열 검색 java 알고리즘이다. 문자열 검색 알고리즘은 문자열 검색 알고리즘인 kmp알고리즘[10]을 이용하였다. WordLogcat 박스에 검색하고자 하는 문자열을 입력하면 kmp알고리즘에 의해 문자열이 검색되는데 검색된 문자열은 파일로 저장된다. 저장된 문자열은 openFileInput() 메소드로 읽어오게 된다.

```
import java.util.*;
public class logcat {
static String lg,ct;
static int k,e;
static int[] sr = new int[300];
public static void find_sr(){
int i = 0, j = -1;
sr[0] = -1;
while(i < e){
if(j==-1 || p.charAt(i) == p.charAt(j))sr[++i] = ++j;
else j = sr[j]; }
}
public static void logcat(){
int i=0, j=0;
while(i < k){
if(j == -1 || f.charAt(i) == s.charAt(j)){ i++; j++;}
else j = sr[j];
if(j == e){
System.out.println("Hit " + (i-e+1) + " to " + i);
j = sr[j]; }
}
}
public static void main(String[] args){
Scanner sc = new Scanner(System.in);
f = sc.next();
s = sc.next();
k = f.length(); e = s.length();
find_sr();
logcat(); }
}
```

그림 4. 로그캣 문자열 검색 알고리즘
Fig. 4. Logcat string search algorithm

IV. 실험 및 평가

1.1 실험 환경

개인정보 보호를 위한 안드로이드 로그캣 시스템은 최근 사용자가 증가 하고 있는 자바기반의 개방형 모바일 운영체제인 안드로이드를 이용하여 구현하였다. 무료로 배포되는 안드로이드 SDK는 네이티브 application과 써드파티 application에 동일한 API를 지원하며 JDK(Java Development Kit)위에서 구동된다. 본 연구에서는 프로그램 개발의 효율성과 호환성을 높이기 위해 컴퓨터 시스템은 인텔 듀얼코 프로세서와 주기억 메모리 2Gb로 구성하였다. 또한 컴퓨터 운영체제는 윈도우 XP 서비스팩 3와 프로그램 개발 통합도구인 이클립스(Eclipse)를 사용했다. 이클립스의 연계는 ADT(Android Development Tool) 플러그인을 통해 안드로이드 SDK와 이클립스를 연결하였다. 시스템이 구현된 application을 탑재할 안드로이드 폰으로는 갤럭시 에스(Galaxy S)를 사용하였다. JDK(Java Development Kit)는 1.6.0_31을 사용하였으며, 안드로이드 SDK는 2.3.3을 사용하였다. 그리고 구조화된 문서를 지원하여 데이터 처리를 쉽게 처리하기 위해 XML 스크립트 언어를 사용하였다.

1.2 성능 분석

본 연구에서 제안한 개인정보의 노출 및 유출 확인을 위한 안드로이드 로그캣 시스템의 성능을 검증하기 위해, 가상의 AllLogCat 데이터 300개를 작성하여 스마트폰에 저장하였다.

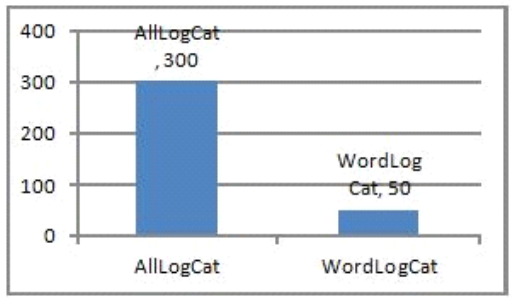

그림 5. 안드로이드 로그캣 시스템 실험결과
Fig. 5. Android Log Cat system test results

가상의 데이터를 필터링 하지 않고 검색한 결과 AllLogCat 가상의 데이터가 모두 검색되었으나, 검색된 데이터들이 사용자가 노출 및 유출된 정보인지를 판별하기에는 많은 어려움이 있었다. 이에 따라 본 논문에서 구현한 시스템을 활용하여 AllLogCat 정보와 WordLogCat 필터를 수행하여 가상의 데이터를 검색하고 결과를 비교 실험을 하였다. 실험 결과 그림 5의 그래프와 같이 WordLogCat은 83% 이상이 필터링되어 일반 사용자들이 쉽게 노출 및 유출되었는지를 판별할 수 있었다. 이러한 시스템이 일반 사용자에게 보급되어 활용된다면, 스마트폰에서 개인정보가 노출 및 유출되었을 때 사고를 미연에 방지하는데 많은 도움이 될 것으로 예상된다.

V. 결 론

2012년 2월 기준으로 국내 스마트폰 가입자는 2,479만명(방송통신위원회 유,무선 가입자 통계)으로 전체 이동전화 가입자의 47.7%에 달한다고 한다. 스마트폰 보급률이 증가하면서 사용자들의 개인정보보호 또한 무시하지 못할 문제로 떠오르고 있다. 스마트폰을 이용하여 언제 어디서든 이동하면서 스마트폰안에 내장되어있는 정보를 이용할 수 있는 편리함 뒤편에는 중요 정보가 노출 및 유출될 수 있는 점을 간과할 수가

없다. 이미 개인정보 유출과 같은 보안문제는 빈번하게 뉴스를 장식하고 있고 개인정보 유출 및 금전적 피해가 더욱 확산될 것이라는 것은 스마트폰의 보급 속도만 보아도 어렵지 않게 예측이 가능하다. 손안의 PC 스마트폰이 급속도로 확산되는 지금, 간단하게 개인의 정보가 노출 및 유출되었는지 여부만이라도 확인할 수 있다면 노출 및 유출된 정보의 불법 이용을 미연에 방지할 수 있을 것이다. 다양하게 활용이 광범위하게 넓어지고 있는 상황에서 스마트폰을 이용한 범죄 때문에 컴퓨터 포렌식 분야에서의 안드로이드 증거수집 및 분석의 필요성이 강하게 제기되고 있다. 하지만 컴퓨터 포렌식 도구들에 의지하여 증거를 수집하고 분석하는 실정이다. 개인의 모든 정보가 거의 들어있다고 해도 과언이 아닌 스마트폰의 정보유출은 우리의 일상에서 쉽고 빈번하게 발생할 수 있는데, 포렌식 분석 툴을 이용하여 증거를 수집하거나 분석하기란 쉽지 않은 일이다. 본 논문에서는 포렌식 분석 툴을 이용하지 않고 개인의 정보 노출 및 유출 유무를 판단하여 대응할 수 있도록 안드로이드 폰 로그캣 필터링을 연구하였다. 안드로이드 로그캣 시스템은 휴대폰에서 개인의 정보 유출이 의심될 때마다 간단하게 LogCat Tag를 필터링하여 정보유출을 확인 가능토록 하였다. 향후 연구는 안드로이드 폰 뿐만 아니라 여러 기종의 정보 유출 확인이 가능한 필터링 시스템을 연구 하고자 한다.

참고문헌

[1] LeeGyuAn, ParkDaeWoo, ShinYongtae, "a forensic investigation to secure the integrity of the data link management methods in the field," Journal of the Korea Society of Computer and Information, 2006

[2] Prosecutor's Office, "maintaining the integrity of digital evidence procedures and facilities for the study," Prosecutor's Office, if Personal Web Media

[3] Takhuiseong two, "Digital Forensic Research Workshop jeonge report, if 46 to 48

[4] Luoma. V., Forensics and electronic discovery: The new management challenge, Computer & Security, 25(2), 91-96, 2006

[5] ParkDaeWoo, SeoJeongMan. "TCP / IP security methods for attacks," Journal of the Korea Society of Computer and Information Science, Volume 10, Issue 5, pp217-226, 2005.11.30

[6] ParkDaewoo, ImSeungRin. "Hacker attacks prevention system for the intelligent study of linkage", the Korea Society of Computer and Information, Volume 11, Issue 2, pp44-50, 2006.5.31.

[7] ParkHyoungBae, Korea Wireless Internet Standardization Forum ", TTA Journal No.121, 2009.

[8] Kim Ki-young, gangdongho, "open mobile environment in the smartphone security technology," Information Security Issue Volume 19, Issue 5, page (s): 10-104, 2009

[9] ParkKiHong, JangHaesook. "Mobile Forensics Android Log Cat filtering for research," Proceedings of the Summer Conference of the Korea Society of Computer and Information.2012 pp217-219

[10] ChoJongKeun, HaSangEun, "Effective Scheme for File Search Engine in Mobile Environments", The Korea Contents Society, Vol.8 No.11, pp41-48, 2008

저 자 소 개

장 혜 숙

1997 : 한국방송통신대학교 전자계산학과 이학사

2000 : 군산대학교 컴퓨터과학과 이학석사

2008 : 군산대학교 컴퓨터과학과 이학박사

현 재 : 군산대학교 컴퓨터정보공학과 강사

관심분야 : 정보검색, 센서네트워크, 보안

Email : hs5486@kunsan.ac.kr