May 25th, 10:30 AM

Forensic Analysis of Smartphone Applications for Privacy Leakage

Diana Hintea
Coventry University, School of Computing, Electronics and Maths, diana.hintea@coventry.ac.uk

Chrysanthi Taramonli
Coventry University, School of Computing, Electronics and Maths, ab7680@coventry.ac.uk

Robert Bird
Coventry University, School of Computing, Electronics and Maths, robert.bird@coventry.ac.uk

Rezhna Yusuf
Department of Information Technology, Kyrgyzstan, contact@dit.gov.krd

FORENSIC ANALYSIS OF SMARTPHONE APPLICATIONS FOR PRIVACY LEAKAGE

Diana Hintea
Coventry University
School of Computing, Electronics and Maths
Coventry, CV1 2JH
diana.hintea@coventry.ac.uk

Chrysanthi Taramonli
Coventry University
School of Computing, Electronics and Maths
Coventry, CV1 2JH
ab7680@coventry.ac.uk

Robert Bird
Coventry University
School of Computing, Electronics and Maths
Coventry, CV1 2JH
robert.bird@coventry.ac.uk

Rezhna Yusuf
Department of Information Technology
Kyrgyzstan
contact@dit.gov.krd

ABSTRACT

Smartphone and tablets are personal devices that have diffused to near universal ubiquity in recent years. As Smartphone users become more privacy-aware and -conscious, research is needed to understand how "leakage" of private information (personally identifiable information – PII) occurs. This study explores how leakage studies in Droid devices should be adapted to Apple iOS devices. The OWASP Zed Attack Proxy (ZAP) is examined for 50 apps in various categories. This study confirms that: (1) most apps transmit unencrypted sensitive PII, (2) SSL is used by some recipient websites, but without corresponding app compliance with SSL, and (3) most apps in iOS environments reveal (leak) smartphone version. The paper concludes that much additional work is needed to assess the privacy dominance between platforms and to raise user awareness of smartphone privacy intrusions.

Keywords: mobile forensics, ZAP, privacy leakage, metadata, security

1. INTRODUCTION

Nowadays, there are a large number of applications, hereafter called "apps," available for smartphone platforms such as iOS and Android. According to the statistics released by Statista (2015), there are 1.5 million

Android apps and 1.4 million iOS apps that have been downloaded 9.19 billion times in 2013 only. Statista (2015) have predicted that this number will rise to 260 billion by 2017. Also, one out of nine apps are free - a strategy aiming to create a financial revenue for the developers, relying on advertisement which is built into the development API, such as iAds for iOS and Ads for Android.

In order to make these advertisements more successful, they need to target the right audience. Therefore, one can expect that app developers and platform providers have a strong incentive of gaining additional information about their users. According to Campbell (2013), there are also other state actors such as the National Security Agency of the United States (NSA) interested in gathering metadata. Although this was suspected previously, the Snowden Revelations have provided proof on how far these actors are willing to go in order to obtain private data. These actors rely on capturing unencrypted network traffic, metadata, and private information broadcasted by third parties, such as smartphone apps.

The research in this paper is concerned with private data leaked by smartphone apps. The user groups benefiting from this research are average smartphone consumers, privacy lobbyist, app developers, policy makers, and regulators. The paper also identifies good and bad practices of app developers. The objectives of this research include i) selecting a number of apps to be investigated; ii) identifying what kind of data is of interest to the actors involved, and iii) identifying what data is leaked.

This paper is structured as follows: Section 2 presents a literature survey identifying and discussing the privacy concerns existent within the smartphone apps environment. Digital forensics areas are also discussed, as well as techniques and tools used for this research. Section 3 discusses the methodology, while Section 4 presents the apps and the experiments carried out. Section 5 illustrates the analysis of the results, while Section 6 concludes the paper.

2. LITERATURE REVIEW

According to the European Convention on Human Rights, "privacy is a basic human right" (Woogara, 2001); however, it has been reported that the Facebook app breached users' privacy (Steel and Fowler, 2010). Therefore, the question "is privacy still possible in the twenty-first century?" was posed (Berman and Bruening, 2001). Such questions arise due to the emergence of new technologies and services that expose users' private information, while users share this data without fully understanding the implications. One of the dominant factors in the development and acceptance of these technologies are smartphones. With the recent proliferation of smartphones, their available capabilities, usage and services, as well as their forecasted growth, researchers are studying their impact on people's lives due to the amount of data that they withheld from their users (Vautin and Walker, 2011).

Nowadays, smartphones withhold information such as SMS, location information, emails, banking details, user habits, time and duration of user activity, and much more. Michalevsky et al. (2015) have shown how easy it is to track the location of an Android user by using an app to send out the battery power consumption information. Furthermore, Stewart et al. (2012) have shown that due the presence of certain peripherals on smartphones, it is possible to automatically identify users' physical activities throughout the day. Although their research was mainly targeting sports activities, it is reasonable to expect that this result is applied to other activities such as sleep and eating patterns.

2.1 Apps Privacy Leakages

As highlighted at the start of this section, privacy is a basic human right to which everyone is entitled. However, ubiquitous computing has brought challenges in a number of fields and privacy is amongst them. On one hand, users prefer free services, but on the other hand, these services are developed with profit in mind (Gandhi et al., 2009). As for apps, users are more likely to download free products rather than paid (Khalid et al., 2014). Some of these apps end up disclosing ample information about the user to the app provider. Companies collect this data and then sell it to other companies for business model purposes; therefore, the private data leaked by these apps has become the indispensable currency that users pay for free apps (Khalid et al., 2014).

The research in this paper is mainly concerned with the security of iOS apps. There is substantial research carried out on Android apps due to their popularity and the fact that they are released for public download after less rigorous testing than iOS apps (Lu et al., 2012). Therefore, this paper explores the dire need for researching the privacy concerns and security implementation for enhancing privacy protection in iOS apps.

2.2 Digital Forensics

Digital forensics is a science field focusing on recovery and investigation to obtain digital evidence (Bommisetty et al., 2014). Moreover, once the evidence is found, it has to be preserved, identified, documented, and then analysed or interpreted. Digital forensics is divided into five main areas which are: Computer Forensics, Memory Forensics, Network Forensics, Multimedia Forensics, and Mobile Device Forensics (Casey, 2011b). The research in this paper is mainly concerned with mobile forensics and network forensics. The main reason for selecting the iOS platform is the noticeable gap in the literature with regards to iOS app testing. Pilli et al. (2010) highlights a number of useful tools, procedures and frameworks for monitoring and capturing data coming from a device on a specific network. Though Wireshark is considered to be the second most popular security tool by administrators (Orebaugh et al., 2006), it is also hailed to be the best network protocol analyser by some researchers (Banerjee et al., 2010). However, according to Pomaska (2009), Wireshark is somewhat complicated to use, and more difficult to demonstrate to others, especially to juries. However, Munoz and Villalba (2013) suggest that web application proxies are very effective in carrying out tasks similar to the ones required for this research, such as the free and open source tool ZAP.

2.3 Tools and Detecting Methods

Numerous methods are used to detect smartphone private information leakage, such as:

1. Framework tools: The developers built these tools according to two methods: static and dynamic security.
    a. Static analysis is an analysis method for mobile application in non-runtime environments. Egele et al. (2011) presented PIOS using this analysis to detect leakage. During the experimentations, the researchers tested more than 1400 iPhone apps and they found that more than half of them had leaked the unique ID of the mobile devices. Therefore, this data leakage allows third parties to create users' profile without their knowledge. It is worth noting that in this experiment, some apps were tested that were on jailbreak

iPhone firmware and did not have any privacy leakage (Egele et al., 2011). Also there are many other frameworks developed based on the static method, shown in Table 1.

b. Dynamic analysis is the real time analysis method consisting in testing and analysing software or mobile apps to detect the vulnerabilities. Chan et al. (2013) identified the privacy leakage of 226 Android apps. The results have been divided into three categories, and the report shows that 46.5% of apps leaked private data. Chan et al. (2013) have used TaintDroid, a real-time monitoring tool. However, they used manual testing to identify what kinds of private data had been leaked as TaintDroid did not provide this information. Table 2 shows the list of dynamic analysis frameworks used to detect privacy leakages.

2. Network sniffing tools: For real-time network sniffing tools, Taylor et al. (2014) used Wireshark and Mallory to test apps for information leakage. Thirty-five applications were tested in three rounds. For the first round, Wireshark was used for a passive analysis. For the second round, Mallory was used to analyse network traffic. An encrypted CA certificate installed on a reliable test device so that Android OS would not refuse Certificates provided by Mallory. The CA certificate was removed in the third round and a typical MITM (Man in the Middle) attack was simulated.

Table 1
List of frameworks based on static analysis conducted on the Android platform

Frameworks	**Platform**	**Year**	**Apps Tested**	**Main findings**
IccTA	Android	2014 (Li et al., 2014)	3000	425 of this apps leaked information related to the phone device ID and location
AppIntent	Android	2013 (Yang et al., 2013)	1000	Sensitive data leakage in 252 apps, out of which 224 contain user unintended and 28 contain user intended data transmission
Leakminer	Android	2012 (Yang and Yang, 2012)	1750	127 apps leaked the device ID, 27 leaked location, 50 leaked phone related information and 12 leaked contacts

Table 2
List of frameworks based on dynamic analysis conducted on the Android platform

Frameworks	Platform	Year	Apps Tested	Main findings
Play Ground	Android	2013 (Rastogi et al., 2013)	3968	Privacy leakage in 946 apps, 844 apps leaked phone related information, while 212 apps location related information
DroidTest	Android	2013 (Rumee and Liu, 2013)	50	36 apps leaked more than one piece of sensitive information, such as ID, mobile number, model number.
TISSA	Android	2011 (Zhou et al., 2011)	24	14 apps leaked location related information, 13 apps leaked IMEI and 6 apps leaked both location and IMEI information.

3. METHODOLODY AND IMPLEMENTATION

The top 5 apps from 10 different categories were downloaded and installed from the iTunes App Store. This will ensure that only the most popular apps, which are likely to be perceived by users as well-designed, are tested and evaluated. This will also ensure that the experiment is unbiased - no faulty or poorly designed apps are selected to influence the outcome of the research. Afterwards, through network monitoring techniques and tools identified in the literature and used in the world of digital forensics, the smartphone traffic was monitored, identifying the consideration given to privacy in the development of these apps.

The experiment was carried out using the OWASP Zed Attack Proxy (ZAP). ZAP can be used to perform scans with the intention either to reveal vulnerabilities and security flaws, or to inform whether the application reveals any kind of information about the user or the device that is being used. As the aim of this project is to investigate privacy, preserving considerations within smartphone applications, only passive scans are of interest. Passive scans are performed each time a HTTP message response is received. In contrast to active scans, which are issued to perform known attacks and therefore modify messages before sending them to the server again in order to search for a specific vulnerability in the response, passive scans do not alter the messages.

ZAP supports the use of SSL connections and gives users the opportunity to generate SSL certificates in order to test SSL enabled communications; however, for the subsequent implementation this feature has not been configured, as properly implemented SSL connections will not leak any private data, and exploiting against SSL is beyond the scope of this project. ZAP is an intercepting proxy that can be used to intercept any traffic that passes through ZAP. In order to intercept the communication between the device and the applications of interest, HTTP Proxy settings, namely the ZAP hosting computer IP address and port, had to be configured accordingly, as shown in Figure 1.

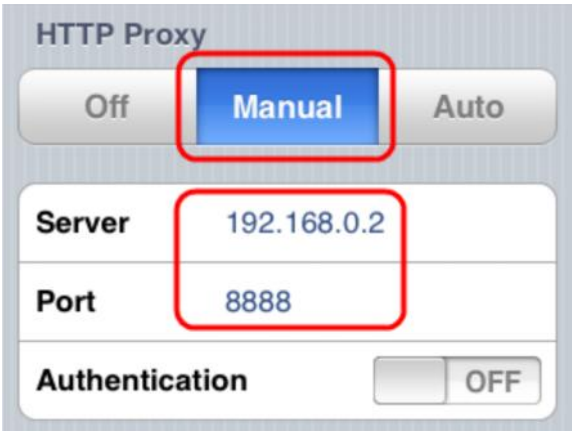

Figure 1. Setting HTTP Proxy setting on iOS 8

For experimental purposes, the five top free applications within their respective categories were downloaded from App Store and accessed from iTunes, with the exception of the games and sports categories, where four and six applications were downloaded respectively as shown in Table 3. For demonstration purposes, interception attempts will be presented for five applications that are described in detail in Section 5. The remaining applications and relative results will be summarized as well.

Table 3
List of categories and number of apps downloaded from each category

Category	Number of Apps downloaded
Education	5
Games	4
Health and Fitness	5
Lifestyle	5
Navigation	5
News	5
Weather	5
Travel	5
Utilities	5
Sport	6

4. RESULTS

This section presents the results derived from the experiment described in Section 4, which aims to investigate whether privacy preservation is taken into consideration in the development of mobile applications. Hereafter it is intended to demonstrate what kind of information is leaked from each application and under what circumstances. Although detailed results are presented for five applications, findings for all 50 applications that have been tested are summarized at the end of the section.

4.1 AA Theory Test

This is an app that helps users prepare for the theory part of the Driving Test in the UK. It comes in two different versions, a paid version and a free version. The paid version currently costs £2.29 and the free version is a restricted version of the app. The app is developed by ABEL learning limited, and is available for other smartphone platforms as well. ABEL

learning limited have developed fifteen more apps, available on the app store for download.

The app was downloaded and tested on the mobile device. Prior to allowing access to app features and content, user registration is required. For testing purposes, the information entered in the registration form was random. Internet connection was successfully established via ZAP, as shown in Figure 2. Information such as the name, gender, email address, and postcode of the user, as well as the phone model and operating system is revealed, as shown in Figure 2. Other optional fields in the app registration form include date of birth, house number, and mobile phone number; however, this information is not shown, as it has not been provided by the user. The main issue with the specific application is that encryption has not been employed and therefore any information exchanged between the two communicating parties would be displayed in plain text, including personal data that the user provides during the registration, as well as information related to the device that is being used. It is interesting to note the fact that, at the time of the investigation, the specific application was the most popular one among similar educational apps.

4.2 Duolingo

Duolingo is a free language learning application offering courses across 23 languages and is available n several platforms. According to the App Store's description, it was chosen as Apple's "App of the year" in 2013. In total, there are four apps available for download on App store. Although there was an error creating the user account, and therefore the app was not functioning, data attempting to leave the network was successfully intercepted by ZAP, as shown in Figure 3. Data such as the phone operating system and its version, Internet Service Provider (ISP) name, type of network, user interface language, phone manufacturer, local network IP address, and local time have been revealed. Sending out information that is not actually required by the app further confirms what was discussed earlier in the literature review; often free apps have a privacy cost. There is no apparent reason for the app to know most of the information sent out such as the ISP name, local IP address, whether the user is connected to a Wi-Fi or 3G network, other than gathering data and selling it off to a third party. Furthermore, data is not encrypted; thus, by monitoring network traffic, one could gain access to private information, which in this case is displayed in plain text as shown in Figure 3.

Figure 2. ZAP screenshot of AA Theory Test Traffic

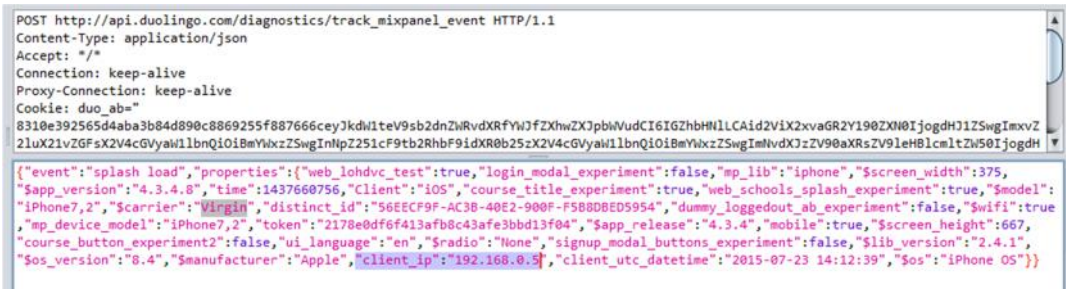

Figure 3. ZAP screenshot of Duolingo

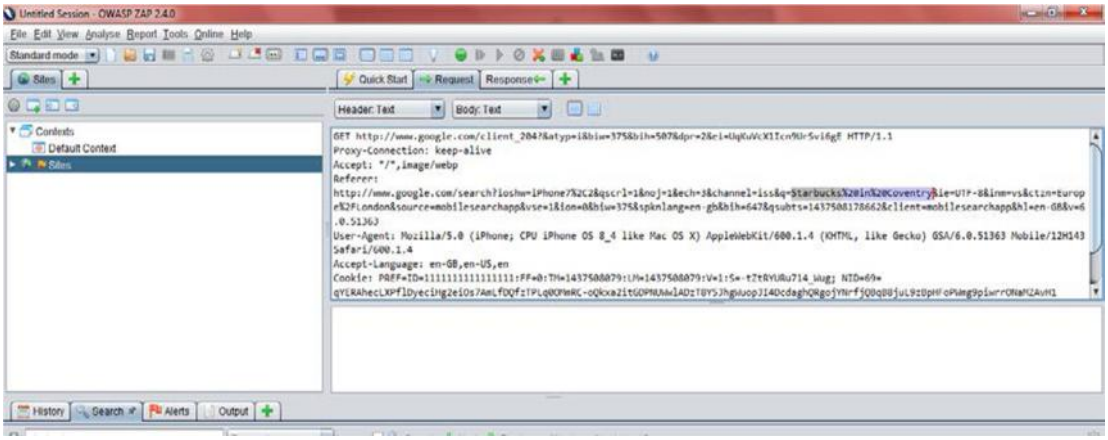

Figure 4. ZAP screenshot of Google

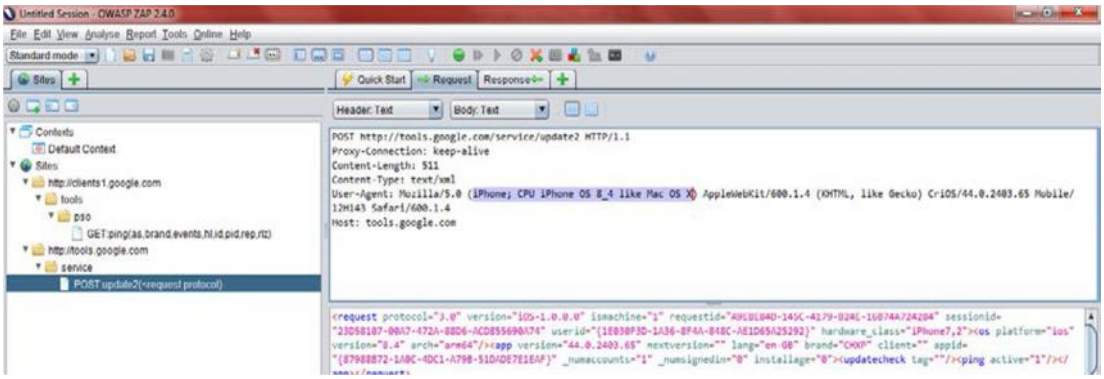

Figure 5. ZAP screenshot of Chrome

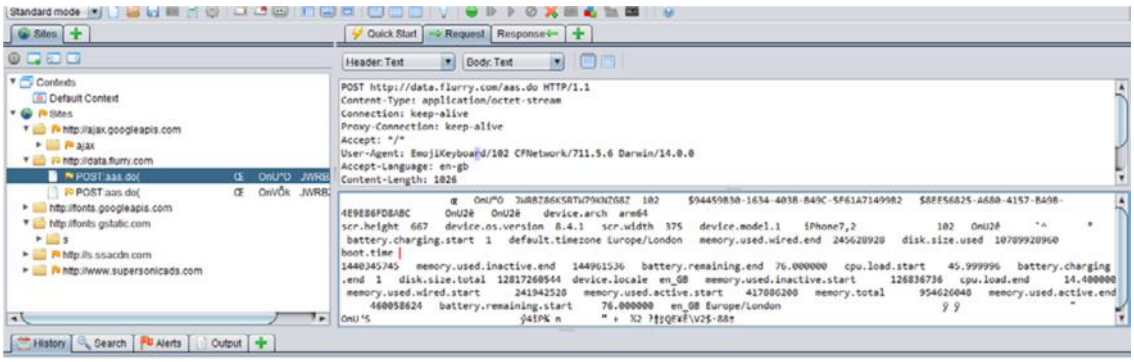

Figure 5. ZAP screenshot of Fancy key for iOS

4.3 Google

Google is a free search engine and is used to search for information on the web. It is developed by Google (Google, 2015b) and is one of the most successful applications on the market. After downloading the app, Siri was used to search for Starbucks coffee shops in Coventry and a connection to the internet via ZAP was successfully established, as shown in in Figure 4. The search term "Starbucks in Coventry" that was used is shown, along with the device information, including the model, version A including the model, version and operating system.

4.4 Chrome

Chrome is a free browser application for retrieving and presenting information from the web, which also supports voice search and is developed by Google. The app was downloaded and tested on the mobile device. Although there was a connection error due to the invalid certificate authority, data attempting to leave the network was successfully intercepted. For testing purposes, the "London" keyword was entered in the search bar and data was intercepted by ZAP attempting to leave the network as shown in Figure 5. Information about the phone model, version, operating system, architecture and user ID has been revealed.

Surprisingly, when using Siri in Google search, HTTP protocol is used to return the results, allowing ZAP to capture the search term. However, when searching with Chrome, the HTTPS protocol is used. This is an indication that Siri does not rely on HTTPS, making the users vulnerable to having their search term monitored and revealed, as it is transmitted in plain text.

4.5 Fancy key for iOS 8

Fancy key is a free keyboard app with several customizable themes and fonts to choose from, allowing users to personalize their keyboards. The app is developed by PinssibleLabs.

The app was downloaded and opened on the testing device. The sent information was captured by ZAP, as depicted in Figure 6. The app 'Fancy key for iOS 8' did not seem to rely on any encryption on first instance opening the file. Although the connection between the device and the app passes through the proxy server, there were no functional problems or error messages, as it would be expected for apps that rely on SSL. This is an indication that the browser is sending information in order to predict the OS of the phone. However, although such information might be needed for

mobile app offloading in order to reduce resource consumption, even in that case, user privacy is not taken into consideration.

Table 4 summarizes the results gathered during the testing of all 50 apps. The abbreviation VER (Version) is used to denote the hardware version number or software version number. LOCATION refers to the location of the mobile device, as well as to locations that have been searched. ID refers to the iPhone ID, email, user name and password, Wi-Fi and IP address. GENINFO (General Information) is used for data that has been used as a search term and it was shown in ZAP. GENINFO* refers to data that differs from the general information searched on the search bar which is shown in ZAP. Also, hyphen symbolizes no leakage, while asterisk (*) symbolizes that it could not be determined whether the data transmitted has been encrypted or not.

Table 4
Privacy leakage of 50 apps conducted on the iOS platform

	Name of Apps	Encrypted	Using SSL	Leakage
Education	AA Theory Test	NO	NO	VER, LOCATION, ID
	Duolingo	NO	NO	VER, LOCATION, ID
	Theory test free for Car Drivers	*	YES	-
	Theory test UK 2015	*	YES	-
	iTunes U	*	YES	-
Games	Candy crash soga	NO	YES	VER
	Jenga	YES	NO	VER, ID
	SongPop	NO	NO	VER, LOCATION, ID
	Arrow	NO	YES	-
Health and Fitness	Pacer	NO	NO	VER, GENINFO, ID
	7 Minute workout	NO	NO	VER, GENINFO, LOCATION, ID
	Sworkit lite	NO	NO	VER
	Nike+ Running	YES	YES	-
	Period Diary	NO	NO	VER, GENINFO, LOCATION, ID

	Name of Apps	Encrypted	Using SSL	Leakage
Lifestyle	eBay	NO	NO	GENINFO
	Boots	NO	NO	GENINFO, VER
	New Look Fashion	NO	NO	VER, GENINFO, LOCATION,
	Amazon	*	YES	-
	Gumtree	*	YES	-
Navigation	GPS Navigation, Maps & Traffic Scout (Sat Nav)	NO	NO	VER, LOCATION
	London Bus Live Countdown	NO	NO	VER, LOCATION
	Just Park	NO	NO	VER, LOCATION
	Waze	YES	YES	-
	Shell Motorist	YES	YES	-
News	MailOnline	NO	NO	GENINFO
	The Guardian	NO	NO	GENINFO, VER
	AOL: Mail, News, Weather & Videos	NO	NO	GENINFO, VER
	BuzzFeed	NO	NO	GENINFO, VER
	Sky News	NO	NO	GENINFO, VER
Weather	The Weather Channel and weather.co.uk	NO	NO	GENINFO, LOCATION
	Weather Live	NO	NO	GENINFO, LOCATION
	10D Weather	NO	NO	GENINFO, LOCATION
	UK Weather forecast	NO	NO	GENINFO, LOCATION
	AccuWeather	NO	NO	GENINFO, LOCATION
Travel	The train line	NO	NO	GENINFO
	Rayinair	NO	NO	GENINFO
	TripAdvisor	YES	YES	VER
	Booking.com	NO	YES	LOCATION
	British Airways Google	NO	NO	GENINFO

	Name of Apps	Encrypted	Using SSL	Leakage
Utilities	Chrome	NO	YES	VER
	Snap Upload for Snapchat	NO	NO	GENINFO*
	Fancy key for iOS 8	NO	NO	VER, GENINFO
	Find IPhone	YES	YES	Encrypted
Sport	Kick 15	NO	YES	GENINFO*
	UFC®	*	YES	-
	Golfshot	*	YES	-
	Dream Team	*	YES	-
	Mirror Fantasy iTeam	NO	YES	VER
	Soccer Saturday super 6			-

4.6 Wider Implications of Privacy Leakage

The implications of privacy leakage in smartphones are becoming an area of study all of its own. First and foremost, the development of the smartphone phenomena from the development of the iPhone has been one of extraordinary growth and adoption by the world wide user community. During 2016 smartphone per capita penetration is estimated at 31.3%, demonstrating the depth of its usage. The particular element that renders the smartphone a privacy fault-line is the extent to which these devices have access to personalized data. The parallel development of social networking and the "Facebook" phenomena means that users "willingly" allow access to their personalized data in a virtual context that in the tangible world would be hard to imagine. However, it is the capability to collect, store, and potentially disseminate disparate personalized data that makes the issue critical in smartphone usage. Not only do these devices enable audio (and increasingly face to face) telephone, messaging, texting, and twitter use, but they have the potential to record 24/7 the location, actions, habits and activities of individuals. When this is linked to the available and emerging "wearable" technologies as exampled by the Apple watch and its Android rivals, the capability of sensor data to collect personal health information adds an additional layer of data that these technologies facilitate - the extent to which this, if breached, enables remote surveillance and observation to an Orwellian level of paranoia.

The mitigations available to prevent such data leakage, for example "new privacy mode," offer some reassurance that users have not been left at the mercy of exploitation by manufacturers and software developers. However, the customization offered is to a large extent dependent upon the sophistication and technical adroitness of the user and this is set against a landscape where making software accessible arguably is at the cost of the levels of security required. The use of encryption, a feature of the latest iterations of iOS and Android, illustrates the extent to which privacy concerns have been heeded. There is, however, and particularly in the context of the

Android user, base that still makes use of legacy versions of the operating system.

All in all, the risks of personalized data being compromised are a "clear and present" danger and one for which, arguably, a proportion of users are inadequately informed and prepared to deal with. In a legal context, End User License Agreement (EULA) is too often ignored by users, allowing the pharming of data for marketing purposes. Users are either blasé, ignorant, or confused by EULAs, finding them overly long and designed to obfuscate rather than illuminate user understanding. As the European vision of clear assent to the "passing onward" of personally identifiable information (PII) comes to the U.S., these apps will require revision and transparent user control over the "leakage" features discussed in this paper. The "clear assent" requirement is likely to force changes which transform EULAs into being positively protective in respect of preventing data leakage, transferring responsibility from the user to the app developer.

5. CONCLUSIONS AND FUTURE WORK

The main goal of this study was to assess the level of private information leaked within smartphone applications. For experimental purposes, 50 applications have been tested for information leakage, using the ZAP proxy to intercept traffic. Over the preceding sections it was found that mobile applications transmit personal user data, including smartphone, resources, ISP, and location related information. The majority of the applications have leaked the version of the mobile device and, in most of the cases that have been examined, there was no encryption employed. Only a few applications that use SSL have not leaked any information, while the rest have either not configured SSL properly, or the applications themselves are not using encryption.

The ideas presented in this paper can be further extended in several ways. One direction of future work is to test and evaluate the smartphone applications on different platforms, such as Windows mobile and Android.

Analyzing smartphone applications for privacy leakage and comparing similar issues across different platforms would allow for a global view of the problem. In addition, although the analysis of data sent out by applications that use SSL certificates is beyond the scope of this paper, it would be interesting to investigate whether such applications are properly configured to handle SSL communications. The results presented in this paper show that privacy can be preserved when SSL is properly configured. However, this might increase the power consumption, and thus reduce the battery life and charge cycle of the device. It is therefore important to investigate the trade-off between privacy preserving and power consumption.

Finally, with a view to increase users' privacy awareness about information leakage and any associated risks, another possibility of future work would be to carry out research into ways of maximizing users' awareness of the possibility of information leakage and its implications.

REFERENCES

AESCHLIMAN, D. P. & OBERKAMPF, W. L. 1998. Experimental methodology for computational fluid dynamics code validation. AIAA journal, 36, 733-741.

AHMED, R. & DHARASKAR, R. V. Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. 6th International Conference on EGovernance, ICEG, Emerging Technologies in E-Government, M-Government, 2008. 312- 23.

BANERJEE, U., VASHISHTHA, A. & SAXENA, M. 2010. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. International Journal of Computer Applications, 6.

BERMAN, J. & BRUENING, P. 2001. Is privacy still possible in the twenty-first century? Social Research, 306-318.

BOMMISETTY, S., TAMMA, R. & MAHALIK, H. 2014. Practical Mobile Forensics, Packt Publishing Ltd.

CAMPBELL, D. 2013. The NSA files [Online]. UK: The Guardian. Available: http://www.theguardian.com/us-news/the-nsa-files [Accessed 20 June 2015].

CARRIER, B. 2002. Open source digital forensics tools: The legal argument. stake.

CARRIER, B. D. & SPAFFORD, E. H. 2006. Categories of digital investigation analysis techniques based on the computer history model. digital investigation, 3, 121-130.

CASEY, E. 2011b. Digital evidence and computer crime: forensic science, computers and the internet, Academic press.

CHAN, J. J. K., TAN, K. W., JIANG, L. & BALAN, R. K. The Case for Mobile Forensics of Private Data Leaks: Towards Large-Scale User-Oriented Privacy Protection. 2013. 4th Asia-Pacific Workshop on Systems (APSYS).

EGELE, M., KRUEGEL, C., KIRDA, E. & VIGNA, G. PiOS: Detecting Privacy Leaks in iOS Applications. NDSS, 2011.

GANDHI, A., HARCHOL-BALTER, M., DAS, R. & LEFURGY, C. Optimal power allocation in server farms. ACM SIGMETRICS Performance Evaluation Review, 2009. ACM, 157-168.

KHALID, H., SHIHAB, E., NAGAPPAN, M. & HASSAN, A. 2014. What do mobile app users complain about? A study on free iOS apps.

LI, L., BARTEL, A., KLEIN, J., TRAON, Y. L., ARZT, S., RASTHOFER, S., BODDEN, E., OCTEAU, D. & MCDANIEL, P. 2014. I know what leaked in your pocket: uncovering privacy leaks on Android Apps with Static Taint Analysis. arXiv preprint arXiv:1404.7431.

LU, L., LI, Z., WU, Z., LEE, W. & JIANG, G. Chex: statically vetting android apps for component hijacking vulnerabilities. Proceedings of the 2012 ACM conference on Computer and communications security, 2012. ACM, 229-240.

MICHALEVSKY, Y., NAKIBLY, G., SCHULMAN, A. & BONEH, D. 2015. PowerSpy: Location Tracking using Mobile Device Power Analysis. arXiv preprint arXiv:1502.03182.

MUNOZ, F. R. & VILLALBA, L. G. Methods to Test Web Applications Scanners. Proceedings of the 6th International Conference on Information Technology, 2013.

OREBAUGH, A., RAMIREZ, G. & BEALE, J. 2006. Wireshark & Ethereal network protocol analyzer toolkit, Syngress.

PALMER, G. 2001. A road map for digital forensics research-report from the first Digital Forensics Research Workshop (DFRWS). Utica, New York.

PILLI, E. S., JOSHI, R. C. & NIYOGI, R. 2010. Network forensic frameworks: Survey and research challenges. Digital Investigation, 7, 14-27.

POMASKA, G. Utilization of photosynth point clouds for 3D object reconstruction. Proceedings of the 22nd CIPA symposium, Kyoto, Japan, 2009.

RASTOGI, V., CHEN, Y. & ENCK, W. AppsPlayground: automatic security analysis of smartphone applications. Proceedings of the third ACM conference on Data and application security and privacy, 2013. ACM, 209-220.

RUMEE, S. T. A. & LIU, D. 2013. DroidTest: Testing Android Applications for Leakage of Private Information.

STATISTA. 2015. Mobile App Usage - Statistics & Facts [Online]. Available: http://www.statista.com/topics/1002/mobile-app-usage/ [Accessed 4 June 2015].

STEEL, E. & FOWLER, G. 2010. Facebook in privacy breach. The Wall Street Journal, 18.

STEWART, V., FERGUSON, S., PENG, J. X. & RAFFERTY, K. Practical automated activity recognition using standard smartphones. PerCom Workshops, 2012. 229-234.

TAPSCOTT, D., LOWY, A. & TICOLL, D. 1998. Blueprint to the digital economy: Creating wealth in the era of e-business, McGraw-Hill Professional.

TAYLOR, V. F., NURSE, J. R. C. & HODGES, D. 2014. Android Apps and Privacy Risks: What Attackers can Learn by Sniffing Mobile Device Traffic. CDT Technical Paper. United Kingdom University of Oxford

VAUTIN, D. A. & WALKER, J. L. Transportation impacts of information provision & data collection via smartphones. Transportation Research Board 90th Annual Meeting, 2011.

WOOGARA, J. 2001. Human rights and patients' privacy in UK hospitals. Nursing Ethics, 8, 234- 246.

YANG, Z. & YANG, M. Leakminer: Detect information leakage on android with static taint analysis. Software Engineering (WCSE), 2012 Third World Congress on, 2012. IEEE, 101- 104.

YANG, Z., YANG, M., ZHANG, Y., GU, G., NING, P. & WANG, X. S. Appintent: Analyzing sensitive data transmission in android for privacy leakage detection. Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013. ACM, 1043- 1054.

ZAP. 2015. The OWASP Zed Attack Proxy (ZAP) [Online]. Available: https://github.com/zaproxy/zaproxy [Accessed May 2015].

ZHOU, Y., ZHANG, X., JIANG, X. & FREEH, V. W. 2011. Taming information-stealing smartphone applications (on android). Trust and Trustworthy Computing. Springer.

