mHealth Cross-Contamination of User Health Data: Android Platform Analysis

Emergent Research Forum (ERF)

Aleise H. McGowan
University of South Alabama
Am1828@jagmail.southalabama.edu

Scott Sittig
University of South Alabama
sittig@southalabama.edu

Philip Menard
University of South Alabama
pmenard@southalabama.edu

Abstract

Although a plethora of mobile health (mHealth) applications containing user data and patient generated health data (PGHD) exist, there appears to be a research gap addressing the user's susceptibility of cross-contamination of data. The objective of this study is to seek a deeper understanding of the risk of cross-contamination of health data from the use of multiple mHealth applications, wearables, and other Internet of Things (IoT) devices. Through the review of recent publications addressing the prevalent information leaks in Android devices, the cross-talk between mobile applications, the vulnerability of mHealth applications, and user habits in regard to account creation this research study aims to explore the possibility that the user data, although held in silos, can be penetrated to create a compilation of the users' comprehensive health information.

Keywords

mHealth, IoT, wearables, cross-contamination PGHD.

Introduction

In today's high-tech healthcare market, an application (app) is so much more than an app. The use of mHealth apps has expanded into nearly every aspect of modern life (Bagheri et al. 2017). As the sophistication of mHealth devices has matured, these devices have intrinsically embedded themselves into the lives of their users. Mobile device usage has expanded from communication facilitation to sensitive tasks such as storing, managing and visualizing patient generated health data (PGHD). Mobile Health (mhealth) apps present new opportunities for monitoring health data outside of the doctor's office. This expansion creates an increased risk of user health data exposure.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires privacy and protection for sensitive medical data used by an applicable entity, such as a physician, hospital, or health plan (Hughes 1996). Most mHealth applications fall outside of the regulatory guidelines of HIPAA, which results in the widespread use of unsecured internet communications and third-party servers (He et al. 2014). Data collected by mHealth applications can provide unique visibility into a user's health status especially when PGHD is collected. Due to the mobile nature of mHealth platforms, additional information such as GPS coordinates and audio data can be leveraged to obtain and store sensitive user health data.

With 54.5% of the U.S. smartphone market and 81.7% worldwide, the Android operating system is one of the most popular operating systems used in smartphones today (Statista 2018). A recent app store analysis showed that Google Play Store has overtaken the Apple App Store as the number one mHealth app provider (Research2Guidance 2017). The open source nature of the Android operating system allows its source code to be inspected, modified and enhanced by computer programmers. Due to being open source, the Android operating system is modifiable by anyone, including both developers and hackers (Singh and Sharma 2016). Coupled with the lack of a controlled marketplace, Android is a prime target for those desiring to exploit smartphone users. As of September 2018, there are a total of 1,986 known vulnerabilities in Android devices

(Ozkan 2018). The proliferation of vulnerabilities increases the potential for user data exploitation. While these vulnerabilities vary in type, a recent survey of Android device vulnerabilities shows "gain privilege" and "gain information" as the third and fourth largest exploitation categories respectively (Ozkan 2018). These vulnerabilities provide attackers with a mechanism by which they can obtain credentials and personal information from users (Joshi and Parekh 2016). Users' tendencies toward reusing passwords and not utilizing two-factor authentication only exacerbates the threats to privacy exposure created by these vulnerabilities.

Health data cross-contamination is the process by which patient data are unintentionally transferred from one app to another. In order to better understand the risk of health data cross-contamination from the use of multiple mHealth apps, wearables, and other Internet of Things (IoT) devices, we present a study on the use of mHealth apps utilizing the Android platform. We will use a multi-stage study to answer: How does mHealth app usage on the Android platform affect the risk of health data vulnerability (cross-contamination) and how does cross-contamination contribute to the compilation of users' health data (particularly PGHD).

Literary Review

Information Leak

The Android operating system relies on a permission-based model to determine access rights (Joshi and Parekh 2016; Karthick and Binu 2017) in order to prevent unauthorized access to resources and information. These permissions which are declarative in nature, are typically granted during installation. Where previous Android versions declared static permissions in the AndroidManifest.xml file, with Android version 7 came the shift toward categorizing permissions as dangerous or normal (Iqbal et al. 2018; Karthick and Binu 2017). Normal permissions are those which are not stored in AndroidManifest.xml because they are granted automatically. These permissions do not contain any information related to the user's privacy. On the other hand, "dangerous permissions" must be granted to applications by the user. These permissions can access the user's private information that they may wish to keep confidential.

Android also utilizes a feature called sandboxing in order to ensure that one application does not have permission to access another application (Hur and Shamsi 2017). Sandboxing provides each application with an unique identifier which is used to access files (Hur and Shamsi 2017) and isolates the application's code and data from other applications. In order to access files outside of its sandbox, an application is required to request permission. The requesting of application permissions that are not required for a particular app to function is called over claiming of permissions. Karthick posits that the overclaiming of permissions is the main reason for data theft on Android applications (Karthick and Binu 2017) such as the FlashLight Android app which is given full internet access (Taenam et al. 2013).

With the increasing reliance on smartphones for activities ranging from data driven communication to healthcare management the value of user data that traverses mobile platforms has grown. During the installation process of Android apps, users are presented with a Table d'hôte styled permissions listing which users must either accept or abort the installation process (Talreja and Motwani 2017). When presented this chef's choice nomenclature most users tend to install the app instead of cancelling the installation (Felt et al. 2012; Gerber et al. 2015). Hornyack et al. (Hornyack et al. 2011) credits the creation of an application ecosystem where applications lack regard for an individual's privacy with the influence of permission ultimatums along with the inevitability that data will be misappropriated for exfiltration. The common overclaiming of permissions by permission-hungry applications provides a mechanism for the theft of user data which is often sent to third party servers for analysis. A research study conducted by the Massachusetts Institute of Technology (MIT), Harvard and Carnegie-Mellon revealed that Android apps are leaking large amounts of data and seventy-three percent of the Android apps that were tested were found to leak private information (Gupta 2015).

Cross-talk Between Mobile Applications

While many 3rd party apps request access to "dangerous permissions" for which they do not have a legitimate need, there are many apps that have a legitimate need for the access to "dangerous permissions" that they request. Many apps, although benign in nature, pose a threat to user privacy due to poor design

or bugs (Herbster et al. 2016). According to Herbster et al., 92% of the top 500 Android applications available in Google Play pose a threat to user privacy due to the use of insecure protocols and/or by leaking sensitive data by other methods (Herbster et al. 2016).

While the Android architecture relies on sandboxing to manage code and data, it also relies on ContentProviders to manage data sharing. Through the use of ContentProviders, apps are able to share information with other applications. "Content Provider Leakage" vulnerabilities that lead to leakage of data from the provider have not been widely addressed (Shahriar and Haddad 2014). Shahriar et al. (Shahriar and Haddad 2014) define this vulnerability as the leakage of confidential data, managed by a vulnerable application, to other applications running on the same device. ContentProvider protection level settings are optional and include normal, dangerous, signature, and SignatureOrSystem.

TaintDroid (Enck et al. 2014) taints (labels) sensitive data in order to perform system-wide dynamic tracking during application execution. Adding taint sources to content providers allowed TaintDroid to track shared information stored in information databases. As pointed out by Taenam et al. (Taenam et al. 2013) when queries are sent to ContentProviders the Android system checks to see if apps own the permission. The results of their study (Taenam et al. 2013) indicates that unauthorized database access and modifications can occur. Shahriar et al. (Shahriar and Haddad 2014) indicated the vulnerability also avails itself through the deviation of operations (e.g. querying messages as opposed to the calendar).

mHealth App Vulnerability

Over the last few years, mHealth app vulnerabilities have been examined. While Knorr et al. (Knorr and Aspinall 2015) warned that current HIPAA and FDA regulations only succinctly address the security requirements of mHealth apps, He et al. (He et al. 2014) expound upon the user data and PGHD that can be revealed due to the freedom availed to mHealth apps as a result of the absence of HIPAA and FDA regulations. One component of the study revealed that 63.6% of the apps studied were sending unencrypted data over the internet. This data included sensitive information such as app login credentials, personal profiles (e.g. name, email, password) and PGHD (e.g. blood glucose).

Hussain et al. presents a security framework for mHealth apps on the Android platform (Hussain et al. 2018a) which fulfills phase one of their three phase conceptual framework for the security of mHealth apps on the Android platform (Hussain et al. 2018b). The security framework uses security checks and policies to protect mHealth app users against both traditional as well as recently published security threats. Lewis et al. (Lewis and Wyatt 2014) presents a framework to access the risk of mHealth apps and to promote safer use. This framework identifies various risks that mHealth apps can contribute to and lists contextual variables which can modify these risks.

User Habits Regarding Password Creation

Morris et al. (Morris and Thompson 1979) identified password security as being an essential component to system security. Through the use of an empirical analysis of a large collection of leaked password datasets, Wang et al. (Wang et al. 2018) found that a majority of users (52%) reuse or modify passwords. Haque et al. (Taiabul Haque et al. 2014) credits the cognitive capacity of users with password reuse behavior, citing that the typical user should only be expected to adequately cope with four or five passwords. Ciampa (Ciampa 2011) also attributes password complexity requirements, multiple accounts and passwords, and security policies which require time-limited passwords to users taking shortcuts which result in weak or reused passwords.

Ives et al. (Ives et al. 2004) posits password reuse across more than one account could result in a domino effect if one site is compromised by a hacker. They speculated hackers would anticipate the reuse of passwords and reuse the login credentials to compromise another system. In what Das et al. (Das et al. 2014) classifies as the first analytical study of cross-site password security their examination of several leaked password data sets finds that exact password reuse is often mitigated by varying password complexities across sites (43% of users directly reuse passwords between sites).

Methods

Our research is designed to analyze the security design and cross-contamination (residual data) of patient information that is gathered and stored by multiple mobile apps. We posit the analysis of mobile app security designs, data required for account creation and data collected/stored by mobile applications will reveal user susceptibility to health information exposure through the leveraging of the insecure mobile environment.

The evaluation process will involve reviewing and testing the top apps in the Google Play rated by popularity. We will then primarily analyze the mobile app security design and the user data required for app functionality. A set of selected n=180 free applications will be installed from the following categories: health and fitness (30), medical (30), social (30), finance (30), essentials to WearOS (30) and general (30) to represent the broad range of apps available for Android mobile devices. We will create fictious user accounts to install the apps from the Google Play store and to populate the apps with the required information necessary to utilize each app.

Examination and forensic analysis of the data required for app functionality will be conducted utilizing an XRY forensic device to extract residual health data, files and artifacts. This forensic examination will be conducted to determine if cross-contamination and granted permissions can lead to the identification of individuals and their protected health information (including PGHD). In addition, a full technical security analysis of each mobile application will be evaluated, and a table will be created to log all security violations.

Conclusion

Examining user's susceptibility to health information exposure is an important research topic due to the pervasive nature of mHealth apps on unsecure mobile devices. Our research seeks to expand knowledge in this area by analyzing data collected by mobile apps via user input (e.g. name, gender, health data and PGHD) and granted permission (e.g. location, access to contact). These findings will potentially allow us to showcase user health data susceptibility across the Android mobile application platform and provide a guiding framework for securing health information across mobile applications.

REFERENCES

"Android Api Guide-Permission." Retrieved November, 2018, from https://developer.android.com/guide/topics/manifest/permission-element

Bagheri, H., Kang, E., Malek, S., and Jackson, D. 2017. "A Formal Approach for Detection of Security Flaws in the Android Permission System," *Formal Aspects of Computing* (30:5), pp. 525-544.

Ciampa, M. 2011. "Are Password Management Applications Viable? An Analysis of User Training and Reactions," *Information Systems Education Journal (ISEDJ)*).

Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X. 2014. "The Tangled Web of Password Reuse," in: *Proceedings 2014 Network and Distributed System Security Symposium*. pp. 23-26.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. 2014. "Taintdroid," *ACM Transactions on Computer Systems* (32:2), pp. 1-29.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. 2012. "Android Permissions: User Attention, Comprehension, and Behavior," in: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. Washington, D.C.: ACM, pp. 1-14.

Gerber, P., Volkamer, M., and Renaud, K. 2015. "Usability Versus Privacy Instead of Usable Privacy: Google's Balancing Act between Usability and Privacy %J Sigcas Comput. Soc," (45:1), pp. 16-21.

Gupta, A. 2015. "Ios and Android Apps Found to Be Leaking Sensitive User Information.Pdf." Retrieved 01 Nov, 2018, from https://news.thewindowsclub.com/ios-android-apps-found-leaking-sensitive-user-information-80843/

He, D., Naveed, M., Gunter, C. A., and Nahrstedt, K. 2014. "Security Concerns in Android Mhealth Apps," *AMIA ... Annual Symposium proceedings. AMIA Symposium* (2014), pp. 645-654.

Herbster, R., DellaTorre, S., Druschel, P., and Bhattacharjee, B. 2016. "Privacy Capsules," in: *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '16*. pp. 399-411.

Hornyack, P., Han, S., Jung, J., Schechter, S., and Wetherall, D. 2011. "These Aren't the Droids You're Looking For," in: *Proceedings of the 18th ACM conference on Computer and communications security - CCS '11*.

Hughes, S. J. D. I. a. A. C. W. a. K. K. 1996. "Health Insurance Portability and Accountability Act,").

Hur, J. B., and Shamsi, J. A. 2017. "A Survey on Security Issues, Vulnerabilities and Attacks in Android Based Smartphone," in: *2017 International Conference on Information and Communication Technologies (ICICT)*. pp. 40-46.

Hussain, M., Al-Haiqi, A., Zaidan, A. A., Zaidan, B. B., Kiah, M., Iqbal, S., Iqbal, S., and Abdulnabi, M. 2018a. "A Security Framework for Mhealth Apps on Android Platform," *Computers & Security* (75), pp. 191-217.

Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., and Albahri, A. S. 2018b. "Conceptual Framework for the Security of Mobile Health Applications on Android Platform," *Telematics and Informatics* (35:5), pp. 1335-1354.

Iqbal, S., Yasin, A., and Naqash, T. 2018. "Android (Nougats) Security Issues and Solutions," in: *2018 IEEE International Conference on Applied System Invention (ICASI)*. pp. 1152-1155.

Ives, B., Walsh, K. R., and Schneider, H. 2004. "The Domino Effect of Password Reuse," *Communications of the ACM* (47:4), pp. 75-78.

Joshi, J., and Parekh, C. 2016. "Android Smartphone Vulnerabilities: A Survey," in: *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*. Dehradun, India: pp. 1-5.

Karthick, S., and Binu, S. 2017. "Android Security Issues and Solutions," in: *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. pp. 686-689.

Knorr, K., and Aspinall, D. 2015. "Security Testing for Android Mhealth Apps," in: *2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*. Graz, Austria: pp. 1-8.

Lewis, T. L., and Wyatt, J. C. 2014. "Mhealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use," *J Med Internet Res* (16:9), p. e210.

Morris, R., and Thompson, K. 1979. "Password Security: A Case History," *Communications of the ACM* (22:11), pp. 594-597.

Ozkan, S. 2018. "Https://Www.Cvedetails.Com/Product/19997/Google-Android.Html?Vendor_Id=1224." Retrieved 20 October, 2018

Research2Guidance. 2017. "Mhealth App Developer Economics, 2017." Retrieved April 23, 2019, from https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health

Shahriar, H., and Haddad, H. M. 2014. "Content Provider Leakage Vulnerability Detection in Android Applications," in: *Proceedings of the 7th International Conference on Security of Information and Networks*. Glasgow, Scotland, UK: ACM, pp. 359-366.

Singh, V., and Sharma, K. 2016. "Smartphone Security: Review of Challenges and Solution," in: *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*. Udaipur, India: ACM, pp. 1-3.

Statista. 2018. "Subscriber Share Held by Smartphone Operating Systems in the United States from 2012 to 2018." Retrieved December 6, 2018, from https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/

Taenam, C., Jae-Hyeong, K., Hyeok-Ju, C., Seung-Hyun, S., and Seungjoo, K. 2013. "Vulnerabilities of Android Data Sharing and Malicious Application to Leaking Private Information," in: *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*. pp. 37-42.

Taiabul Haque, S. M., Wright, M., and Scielzo, S. 2014. "Hierarchy of Users′ Web Passwords: Perceptions, Practices and Susceptibilities," *International Journal of Human-Computer Studies* (72:12), pp. 860-874.

Talreja, R., and Motwani, D. 2017. "Sectrans: Enhacing User Privacy on Android Platform," in: *2017 International Conference on Nascent Technologies in Engineering (ICNTE)*. pp. 1-4.

Wang, C., Jan, S. T. K., Hu, H., Bossart, D., and Wang, G. 2018. "The Next Domino to Fall," in: *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy - CODASPY '18*. pp. 196-203.