Mobile Devices have made us the most monitored individuals in history

SEM2220 - Assignment 4

090932464

Contents

1 Introduction

There has been a lot of news in the press in the last year about surveillance programs run by many countries security agencies, particularly focused on the collection of phone records by the National Security Agency (NSA)[1].

It comes as no surprise that this has brought about the question:

"Have mobile devices made us the most monitored individuals in history?"

To fully understand the depth of this question, one must consider the technical methods which are employed to monitor mobile devices and how these methods differ across different mobile platforms. In hand with this, one must investigate the methods for preventing unwanted monitoring on mobile devices and how effective these methods really are.

Finally there are many legal and professional issues which govern the collection of data from mobile devices; but there are also a host of ethical and social issues which legal and professional element cannot, necessarily, cover.

Of course monitoring of data, especially from mobile devices, doesn't have to be used for nefarious purposes. Applications commonly use data mining techniques to provide a better experience for their users and cloud services are so popular that imagining a world where all a users data is stored solely on a single device is almost impossible.

2 Technical Methods for Monitoring Mobile Devices

Because of the structure of the Global System for Mobile Communications (GSM), any mobile device which accesses the mobile network can be tracked to, at worst, the nearest cell tower. In fact the NSA is known to use this data to track targets and identify possible accomplices[2]. There are also other stories of UK public organisations performing similar actions[3][4].

Though this is a worrying concept, there is some important information that the U.S. has given in [5] which denies that any information collected cannot be used to target any individual without a prior specific and documented reason to do so. In the case of monitoring of non-U.S. citizens there must also be a agreement with the country of their citizenship.

It is the monitoring which the users agrees to have performed upon them that is perhaps more worrying.

Mobile devices, especially tablets and smart phones, have a range of sensors which third-party applications may be able to access. These sensors typically include a camera, microphone, WiFi antenna and GPS system. As technology progresses the accuracy of these sensors is increasing and other sensors such as accelerometers are becoming more prevalent.

It could, therefore, be easy for an attacker to write a malicious application which simply monitored the GPS location of a person or recorded their conversations through the microphone. Or even use any of these systems combined to gather a lot of sensitive data.

There have been cases which have been formally investigated[6] in which legitimate applications collect data from users on the side, which are then sold to other companies for advertisement revenue.

However, a lot of applications have legitimate uses for these sensors. Most applications require network access to load data from external servers. More specific applications, which perform tasks like route tracking, will require the use of more than one of these sensors.

3 Protection Against Unwanted Monitoring

Unfortunately, due to the structure of the GSM network, as long as a mobile device is on and allowed to connect to the network it can be tracked. With the addition of a Subscriber Identity Module (SIM) card it can even be tied to a specific individual. Under [7]

Modern mobile platforms typically have some sort of security system and ways in which applications can be given access to secure elements of the mobile device. Most of these platforms sandbox third-party application allowing the kernel to control the access to the various facilities of the device.

3.1 Android Security Facilities

[8] describes the methods that the Android system uses to secure the environment. The main advantage Android gains in this area is that uses Security-Enhanced Linux (SELinux), which confines the access of programs based on different policies.

Android adds many features on top of this, the most applicable of these to the question of monitoring is the permission model. For a third party application to access protected APIs such at GPS positioning or network connections they must implicitly define which of these elements they require in the manifest file of the application.

This information is displayed to the user when they first install the application and when the application updates to add new access to secure APIs.

There are also certain APIs which are not available to third-party applications, but which may be used by pre-installed applications if they are signed as part of the OS.

Because applications are sandboxed from one another it should be an impossible task to gain confidential information from another application, unless it provides it somehow.

3.1.1 Additional Security Features Provided by the Google Play Store

Obviously, telling legitimate use of secure API elements from illegitimate use is not an easy task, especially for automated systems.

In the mobile ecosystem, the typical method of performing this is to have a trusted place, where developers can distribute their applications. In the case of Android this is usually the Google Play store, however other stores such as the Amazon Appstore do also exist.

The maintainers of such places can then regulate the applications accepted, monitor them for any malicious activities and remove them where needed. Google even added a service in 2012 which scanned the Play store for applications with a malicious intent by running them on a range of emulated services[9].

3.2 iOS Security Facilities

[10] defines the methods that the iOS system uses to secure the environment. Similar to Android iOS third-party applications are sandboxed from each other, although a lot

of this is done by the iOS runtime. All applications have their own file spaces which can only be accessed through the iOS defined API.

Access to secure API elements is defined through entitlements; signed key-value pairs specific to applications. However, it should be noted that these entitlements are not required to access elements such as the GPS or microphone and are more typically used by system applications and daemons to perform tasks that would typically require root access.

The iOS ecosystem is heavily reliant on the Apple App Store[11] to provide security against the malicious collection of data from iOS applications.

4 Implications of Mobile-based Monitoring

References

[1] G. Greenwald, E. MacAskill, and S. Ackerman, “NSA collecting phone records of millions of Verizon customers daily,” *The Guardian*, 6 Jun. 2013, [Accessed Jan. 15, 2014]. [Online]. Available: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[2] *Summary of DNR and DNI Co-Travel Analytics*, white paper, NSA, 1 Oct. 2012.

[3] R. Gallagher and R. Syal, “Met police using surveillance system to monitor mobile phones,” *The Guardian*, 30 Oct. 2011, [Accessed Jan. 15, 2014]. [Online]. Available: http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance

[4] N. Hopkins, “UK gathering secret intelligence via covert NSA operation,” *The Guardian*, 7 Jun. 2013, [Accessed Jan. 15, 2014]. [Online]. Available: http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

[5] J. R. Clapper, U.S. Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillence Act*, fact sheet, U.S. Govt., 8 Jun. 2013.

[6] “Android Flashlight App Developer Settles FTC Charges It Deceived Consumers,” press release, Fedral Trade Commission, 5 Dec. 2013. [Online]. Available: http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived

[7] “Directive 2006/24/EC of the european parliament and of the council,” *Official Journal of the European*, 15 Mar. 2006.

[8] *Android Security Overview*, The Android Open Source Project, [Accessed Jan. 15, 2014]. [Online]. Available: http://source.android.com/devices/tech/security/

[9] H. Lockheimer, “Android and Security,” blog, 2 Feb. 2012, [Accessed Jan. 17, 2014]. [Online]. Available: http://officialandroid.blogspot.co.uk/2012/02/android-and-security.html

[10] *iOS Security*, Apple Inc., Oct. 2012. [Online]. Available: https://www.apple.com/ipad/business/docs/iOS_Security_Oct12.pdf

[11] “App Store,” Apple Inc., [Accessed Jan. 16, 2014]. [Online]. Available: https://itunes.apple.com/us/genre/ios/id36?mt=8