UNIVERSITI TEKNOLOGI MARA

INTERCEPTING AND ANALYSING DATA PACKET FROM ANDROID APPLICATIONS TO GAIN PERSPECTIVE OF UNAUTHORISED DISEMMINATION OF LOCATION INFORMATION

MUHAMAD IQBAL BIN BASIR

Dissertation submitted in partial fulfilment of the requirements for the degree of
Master Of Science

FACULTY OF ELECTRICAL ENGINEERING

June 2017

ACKNOWLEDGEMENT

I would like to thank my supervisor, Prof. Dr. Habibah Hashim for her guidance continuous support throughout the completion of the Thesis. I also would like to extend my gratitude to my wife, family and friend for their continuous support for completing this project.

ABSTRACT

The mobile phone is a modern marvel to humankind since its main role has expanded far from just making a simple call. Other than making calls or sending messages, the mobile phone now offers high speed processing power, high RAM capacity and built-in Global Positioning System (GPS) navigation device just to name a few. The Android operating system is a major player in the mobile phone industry. Its operating system provide programming interfaces and platforms to fully utilize the mobile phone resource capability. No overhead cost and third party application support from Google Play, has made the operating system (OS) the discernible choice for mobile phones. As the mobile phone becomes more advanced, it is disturbing to know that it is also capable of silently spying on our privacy to the point of disseminating user location information stored in the android device to unauthorized parties. This study aims to identify how users' location information are being transmitted to public domain through analyzing data packet transmitted through our mobile phone. This work also proposes a feasible method for users to closely monitor their location privacy when using an android device. The result of data collection and intensive observation of more than 8000 (0.3% of total application available in Google Play Store) sample applications, it was found that more than 3000 of them had requested android location information.

Table Of Contents

CHAPTER 1

INTRODUCTION

1.1 Background

Most of the research paper related to mobile phone privacy are more toward on the user behaviour and their action when privacy being compromised subject to nudging and permission control flexibility at user level. Regardless mobile phone OS platform (iOS and Android recently dominate the market share) their intention is to create an awareness and develop an approach in order to inform user that some of installed application are compromising their privacy.

Another research trend related to this area is a few papers suggesting that mobile phone privacy particular to user location information are disseminate. But all that paper presenting the evidence of location information that were requested by mobile phone application. Thus, method should be seen as incomplete method as to conclude user location information really were disseminated to 3rd party and were used without user consent. There is no study or proving that any information that acquire mobile phone location information were actually disseminate that information.

In this research paper, the platform used mostly is an Android platform due to its dominance in mobile phone market (80% market share Q2 2015). Most of the research also use android as their research platform because iOS (2nd highest market share, 15% Q2 2015) has better privacy and permission policy imposed by Apple Inc (eg. Apple versus FBI case) that were translated into their product. It is also well known as Android is a open platform and govern by advertised based company, so user information is a commodity for their trade.