AnonDroid

Chris Campbell

May 6, 2012

Abstract

AnonDroid is a project designed to make Android users as anonymous to Google as possible. It will include proxying features, bogus data injections, Google Play download spoofing and much more.

Contents

1 Introduction

It appears that there is a large market of people who are begining to worry about how much information Google is able to obtain about their daily lives. Information such as, contacts, searches, favorite videos, emails, GPS locations, favorite foods, and the list continues. With the recent explosion of Android devices on the market it begs the questions of just how much information is Google now able to collect on a persons? New applications such as FourSquare are just downright creepy. This is where the AnonDroid software is going to come into play.

The primary goal of AnonDroid is to help increase the privacy of the end users by either proxying end users data through alternate sessions with Google, generating false information about the end users, or even going as far as to inject fake searches to throw off potential watchers. By doing so AnonDroid will effectively allow it's users to stay as anonymous as possible.

2 Limitations

Obviously it is impossible to create a fully anonymous Android device simply due to the nature of the data. The android devices will still have hardware identifiers which allow them to connect into the cellular networks. And we will not be able to spoof this ID because it will effectively make the Android device useless on any cellular network. The other issue arises with email. Since uses need to login to their email accounts, there is nothing we can do to break that link from that account to that end user. In the case of email, the only piece of information that we could possibly anonymize is the IP address used to login to Google.

3 Structure

AnonDroid will be a complex system consisting of several pieces of software. There will need to be an Android application that runs on the end device. This software will most likely will need to have root privileges. The second piece of software will be ran on a server which will perform the anonymization of the user data fed to it by the android software.

The Android software will tunnel all non-cellular network traffic to the centralized (for now) server. It will then be the responsibility of the server to anonymize as much of the traffic as possible before sending it onto Google.

4 Android software

4.1 Overview

This software will be ran on the end users devices. It will be responsible for thee main tasks.

- Creating a VPN/SSH tunnel back to the central server
- Intercepting all traffic leaving the phone
- Anonymizing GPS coordinates

As well as implementing these tasks, it will need to incorporate these main features as well

- Easily configurable
- Completely transparent to the user

- One click enable/disable functionality
- Generate reports for the user about what personal information is being leaked

4.1.1 VPN

asdf

4.2 Server Software

4.2.1 Security

4.2.2 Anonymization

4.2.3 Distribution