CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Over-the-Air Penetration Testing

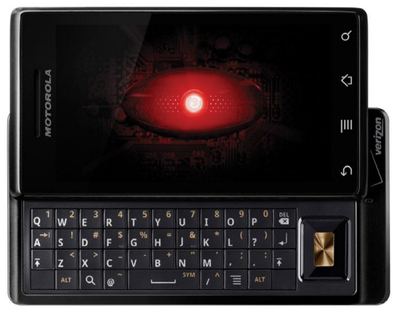
Eric Katz, Bryan Lee, Richard Mislan

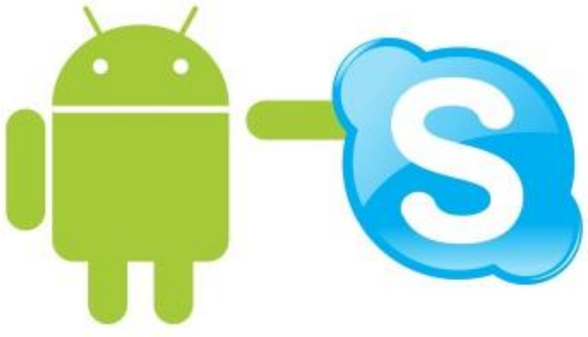
Abstract

The purpose of this study is to determine whether it is possible to penetrate a mobile device from another device that is on the same cellular network. The study will concentrate on the Android platform and focus on attempts to penetrate the most popular applications for the platform. For this study, we will be testing some of the top free Android Play Store applications, such as Facebook for Android and Skype for Android. The purpose will be to see if it is possible to gather pertinent information ranging from contacts and messages to a full forensic image of the device from the target. Previous research in this area has involved man-in-the-middle techniques that require the target device to connect to hardware controlled by the attacker, which then forwards the information to the cellular network. This means that special equipment and the target phone are required in order to carry out the attack. If a mobile-to-mobile attack is possible, all that is needed is a phone that is able to connect to the network the target is on and any scripts and software created for the exploit. This could be a very useful technique in areas where pertinent information is passed over cellular networks, such as a drug trafficking ring or terrorist cell.

Problem Statement

Vital information for intelligence gathering operations and criminal investigations is passed over the air in modern mobile phone networks. The problem with this is that it is hard to acquire this information without seizing the phone and letting the suspect(s) know what is happening. It would be very beneficial to the intelligence community to be able to acquire pertinent information ranging from contacts, pictures, and messages from one phone to another using over the air techniques.





Methodology

All of these tasks will be performed using a 3G mobile testing bed and a Motorola Droid running Android version 2.2.3. Using the test bed, we will create our own private cellular network. This will allow us to attach phones to the network and send system and control commands to them. We can monitor the traffic going back and forth as the phones and tower talk to each other. We will examine this information for the applications we wish to test in order to understand both the formatting of the messages and how they are sent across the network. As we inject commands from one phone to another, we can see how far the message is getting through the network and what is happening at both end points. Once we are able to have two devices communicating with each other properly, we will search for techniques to mask this communication on the target phone. Where possible, we will look through available code for the various applications to locate potential exploits. Some of this information has been proven to be exploitable using the Android software development kit and virtual devices. Once we understand the communication between devices over the network through the applications we are examining, we will attempt to gather pertinent information from the target using the information obtained in the previous steps. We will also explore if it is possible to obtain a full forensic image of the phone, either through commands to the Android operating system or through the use of software pushed to the target phone over the air.