Wardrive for GSM Networks - Are You Being Intercepted?

Sanil Sinai Borkar, Suresh Koppisetty
{*sanilborkar@ufl.edu, sureshk@ufl.edu*}

October 24, 2014

1 Abstract

GSM standards mandate every cellphone to be 2G backward compatible, thereby making it the "weakest" target in the GSM security model. Many rogue base stations exploit this vulnerability by downgrading the user's cell network to 2G without their knowledge. In this paper, we seek to wardrive the GSM networks by using commodity phones and identifying the illicit cellular base stations. The approach proposed is to develop an Android application that can measure relevant information about the current cellular connection and relay it back to a data collection server for detailed analysis. In particular, we developed new optimal techniques for locating the rogue base stations. Using this application, we were able to identify and construct a map of the rouge base stations in the nearby area with a high degree of accuracy. Since cellular security is a major concern, this application provides an interface for the general public to easily identify a compromise in their cellular network by rogue base stations.

Index terms: IMSI-Catchers, rogue base stations, security in GSM