Security Implications of IMSI Catchers

Jared Stroud, Bryan Harmat, Bill Stackpole, Daryl Johnson, Tom Oh, Rick

February 15, 2015

Abstract

According to various news sources, rogue towers referred to as "IMSI catchers" have been deployed across the nation. We have taken an academic interest in determining what information can be acquired when a mobile device associates with one of these towers. These towers focus on manipulating authentication methods to pose as a legitimate GSM tower. We were able to construct a low-cost cell phone tower with the intention of determining what security vulnerabilities exist in the current mobile network infrastructure, if any.

Introduction

The Global System for Mobile communication (GSM) is a standard protocol that the majority of cell phones operate on today. The original specifications were developed by the European Telecommunication Standards Institute (ETSI) in 1987. GSM communication accounts for the majority of cellular traffic today. Historically, some of the GSM protocol has been kept proprietary. These "secret items" include encryption and authentication methods. In an effort to make GSM obtainable for academia, open source movements such as OpenBTS have been developing freely available tools to deploy a personal GSM tower. OpenBTS allowed for the Computing Security Department at the Rochester Institute of Technology (RIT) to build a low cost GSM tower for their mobile forensic curriculum during the Fall of 2014. By utilizing hobbyist Software Defined Radios (SDRs) and OpenBTS, students were able to associate their phones to RIT's tower "Tiger Net" and examine traffic generated by GSM association as well as SMS messages.

GSM Architecture

SIM Cards

GSM Authentication

Surveyed Attack Vectors

Defense Architecture

Defense Architecture

Future Work