Location Detection of Rogue Base Stations/ IMSI Catchers

Situational Awareness

Rogue base stations are devices that masquerade as legitimate cell phone towers, tricking cell phones within a certain radius into connecting to the device rather than a tower. In recent pilot test conducted over the public airwaves, DHS detected anomalous activity that appeared to be consistent with rogue technology being used in proximity to sensitive facilities such as the White House. Some rogue base stations may have advanced features allowing interception and alteration of communication content. There is a need to detect rogue base stations to protect the mobile communications critical infrastructure.

Project Overview

Researchers from the University of Washington and Subject Matter Experts (SMEs) from T-Mobile will conduct a detailed analysis to identify any anomalous activity. Using the unique access and subject matter expertise of internal network operations, the T-Mobile SMEs and UW researchers will be able to differentiate between normal network traffic and potentially malicious traffic associated with rogue base stations. These indicators will form the basis for the development of potential detection signatures.

This technology enables counter-intelligence, government agencies and corporations to identify rogue base stations and protect sensitive data from being misdirected to them. This research will lead to future development of tools so industry can confirm, identify, and classify when a cell site is legitimate versus a rogue base station. End users that will be positively impacted by this research include both wireless consumers (protecting sensitive data) and the federal government (resiliency in critical infrastructure).

This task is a continuation of a research project jointly conducted by T-Mobile and UW. As part of the current endeavor, the researchers have developed updates to existing sensors and prepared network logging capabilities to collect network event logs at specific field test areas within the network where rogue base station activity has been recorded in the past. This data set will be used as the initial starting point for the research project. Using the detection signatures and gathered data as an input, the researchers will then be able to differentiate between normal network travel and potentially malicious traffic associated with rogue base stations. From the detection signatures and gathered data, the researchers will develop an approach to developing an algorithm for identifying the rogue base (s).

Next Steps

The project will result in a white paper providing research findings, a proposal for the development of a tested algorithm that will mitigate and remediate man-in-the-middle attacks, and a set of recommendations for best practices for the communications industry.

To learn more about this project, contact
Jay Robinson, DHS Program Manager, at jay.robinson@hq.dhs.gov or
John Taylor, CEO, NIHS at jdtaylor@thenihs.org

2018-12.1pager