Technical Disclosure Commons

Defensive Publications Series

April 07, 2017

Imsi-Catcher Detection For Mobile Operating Systems

Tanmay Wadhwa

Neil Dhillon

IMSI-CATCHER DETECTION FOR MOBILE OPERATING SYSTEMS

ABSTRACT

Systems and methods for detecting and notifying a mobile device user of an IMSI-catcher are disclosed. The system includes a mobile device installed with an application that collects signal data and wirelessly transmits the data to a server. The application may be part of a remote attestation service and communicates directly with radio interface layer (RIL) to collect telephony network and diagnostic information data from the device's baseband. The collected data is sent to the server for remote attestation. The method includes detecting anomalies in the signal data from crowd-sourced heuristics and notifying the device user discreetly of the presence of an IMSI-catcher. The system and method provide identification of IMSI catchers with high reliability since the detection is done using crowd-sourced data from many devices and on the server-side, it's more difficult for an attacker to conceal being identified and to counter the detection.

BACKGROUND

Government agencies and other malicious actors currently use a device known as an IMSI-catcher to infringe on a mobile phone user's privacy by eavesdropping on telecommunications and tracking their locations. Furthermore, law-enforcement agencies in the United States are permitted to use IMSI-catchers without a search warrant. These devices are used to perform a man-in-the-middle attack by acting as a "fake" mobile tower between the user and the cellular carrier's actual mobile phone tower. These devices exploit vulnerability in the GSM standard whereby subscribers are required to authenticate to base stations, however base stations are not required to reciprocally authenticate to subscribers. IMSI-catchers force nearby subscribers to fall back to using the unencrypted A5/0 mode or the weakly encrypted A5/1 and

A5/2 modes for voice calls and SMS. Since SMS is often used for second-factor authentication, this vulnerability can also be used to assist in hijacking user accounts.

IMSI-catchers can only operate under specific conditions, such as physical proximity to the targeted subscriber, higher signal strength than neighboring base stations and a call or SMS to be placed or received by the targeted subscriber. There are several IMSI-catcher detection applications available for use in various mobile operating systems. These applications are severely limited by the capabilities available on the operating system's application layer APIs, especially to radio and telephony interfaces. As a result, many of these applications require superuser privileges on a device in order to function.

DESCRIPTION

Systems and methods for detecting and notifying a mobile device user of an IMSI-catcher are disclosed. The system is depicted in FIG. 1 and includes a mobile device installed with an application in wireless communication with a server. The server includes a framework which detects anomalies in the cellular connectivity data and notifies the user discreetly. The mobile device may be running on any mobile operating system. The application may be part of a remote attestation service and communicates directly with radio interface layer (RIL) to collect telephony network and diagnostic information data from the device's baseband. The collected data is compressed and sent to the server for remote attestation. The server includes a framework for crowd-sourced heuristics or machine learning classifier to detect anomalies. The crowd-sourced heuristics can include factors such as signal strength of other devices connected to the geolocated cell tower, mode of telephony, and if the account associated with device is being targeted by malicious actors, etc.

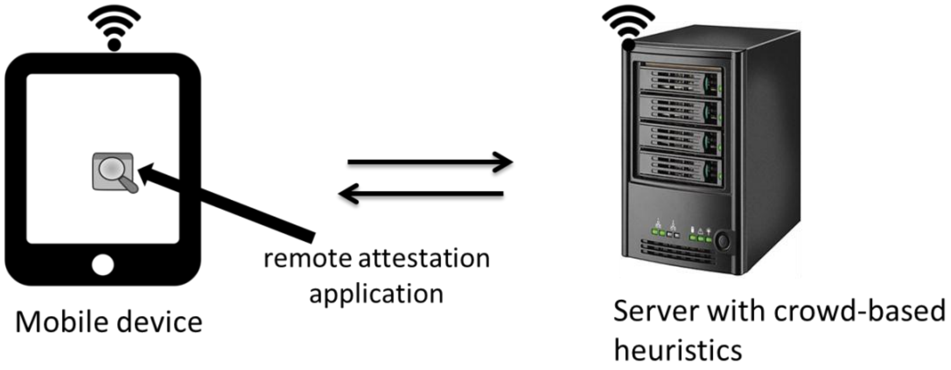
Mobile device
remote attestation application
Server with crowd-based heuristics

FIG. 1: System for detecting and notifying a mobile device user of an IMSI-catcher

The method as depicted in FIG. 2 includes collecting telephony network and diagnostic information from the device’s baseband by communicating directly with the radio interface layer (RIL) and sending compressed data packets to the server for remote attestation. The server decompresses the data and applies crowd-based heuristics or machine learning classifiers to detect anomalies and generates a score. If the score is above a certain threshold, the server notifies the user of the mobile device through discreet means, such as a predetermined notification, symbol or behavior to be displayed across devices. For instance, the notification or symbol may be an exclamation mark over the cellular status symbol on the top bar, or a text message informing the user that the calls and SMS may be eavesdropped on the cellular connectivity status indicator.

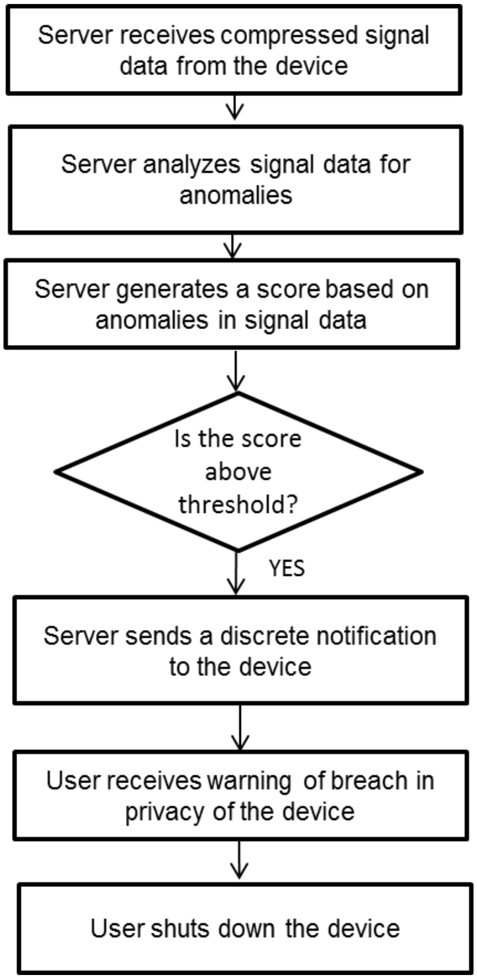
Server receives compressed signal data from the device
Server analyzes signal data for anomalies
Server generates a score based on anomalies in signal data
Is the score above threshold?
YES
Server sends a discrete notification to the device
User receives warning of breach in privacy of the device
User shuts down the device

FIG. 2: A method for detecting and notifying a mobile device user of an IMSI-catcher

In one instance, when the user receives an incoming or places an outgoing call, the dialer displays bright red text explicitly notifying the user that traffic may currently be eavesdropped. Additionally, during the call a persistent notification may be presented informing the user that the presence of an IMSI-catcher has been discovered. If the user taps on the notification or cellular connectivity quick-tile, he/she will be presented with the option to disable cellular connectivity until the connection is safe.

The disclosed system and method allows for crowd-sourced information to be used in detection as opposed to user data. Solving this problem at the platform level automatically bootstraps the data collection efforts from thousands of individual devices, as it is currently done using application based IMSI-detectors, to hundreds of millions of devices distributed globally and all contributing crowd-based information. Since the identification is done using a server-side component, more CPU resources along with the additional data allows for more sophisticated and up-to-date detection of IMSI-catchers.

The systems and methods have several advantages over application-level solutions. First, superuser privileges are not needed since the system is capable of collecting diagnostic telephony information from the baseband using without compromising the security model of the device. Second, the sources of data collected can more easily be updated at the system-level as opposed to the application-level especially since the user does need to grant additional permissions. This will provide additional privacy for users who are not aware of the vulnerability. Third, since detection is done server-side, heuristics can more easily be updated without requiring an update to the device. This not only improves the speed of updates, but also makes it more difficult for attackers to counter improvements made in the crowd-sourced detection and for an attacker to conceal being identified. Bulk data collection and server-side analysis of diagnostic information will make it harder for attackers to determine which signals are used in detecting IMSI-catchers. Lastly, solving this problem at the system-level will allow users to be notified using familiar and consistent methods just like all other security and privacy protections built into the operating system.