CIADROID: Causality-Based Information Flow Activity Path Identification on Android

Technology #015-048-lan

George Washington University researchers have developed a unique malware protection tool named CIAdroid which can notify users about the undesirable information leakage and applications' other undesirable runtime behaviors. The user can then take actions to protect their privacy and security.

Whenever an app is installed in any Android phone, at the time of installation it explicitly asks for a permission to access the information stored in the phone. However, once the app is installed, users have no way to know what tasks that app is performing in the background. Either malware or the official app can collect and leak users' private data such as account numbers, SMS, etc.

The “CIAdroid” (short for Causality-based Information flow and Activity path identification on Android) system consists of two parts: 1) An activity monitoring system implemented on each user's device, 2) An analysis center implemented on server. This overall framework is shown in the image. The analysis center is the one which determines whether the actions performed by apps are undesirable or not. Since, this part is implemented in the cloud it doesn’t affect the device performance. At present, there are many malware protection applications available in the Android environment. However, these apps require a significant amount of resources (RAM) and hence, slow down the device.

In addition, the CIAdroid is user-friendly and doesn’t show pop-ups with alerts and warnings unnecessarily. If the user wants to know about the runtime functions of an app, he just needs to offload the log files to the analysis center and the corresponding results will be available in the device. Problems are immediately visible. In sum, CIAdroid avoids problems created by today's malware protection tools and does it in a very user-friendly manner.

Applications:

- Can be used in any kind of android OS device to notify user about undesirable operations

Advantages:

- Provides high accuracy
- Requires minimal performance overhead
- Presents information flows, activities and vulnerabilities of applications
Inventors

Tian Lan
Asst. Professor at the Department of Electrical Engineering and Computer Engineering

Guru Venkataramani
Asst. Professor at the Department of Electrical Engineering and Computer Engineering

Fan Yao
Research Assistant, Ph.D. Candidate

Yongbo Li
Research Assistant, Ph.D. Candidate