Unsolvable Solutions

Client: Francois Mouton at the CSIR DSSR

User Manual

Eavesdrop

Github link: `https://github.com/Unsolvable-Solutions/Project-EPIC`

Members:	*Student Number:*
Edwin Fullard	12048675
Jaco Bezuidenhoudt	11013878
Jandre Coetzee	10693077
Maret Stoffberg	11071762
Ryno Pierce	12003922

Contents

1 System Overview

The Malware is developed as a proof of concept for the Eavesdropping Protection in Conclave (EPIC) product. The Malware has the ability to eavesdrop on unsuspecting victims via their own Android device.

2 System Configuration

The Malware consistes of two parts: the application and the server.

The application is installed on your Android device and the server. A request to start recording is send from the server to the application to start recording by the user. The user then stops the recording and it is stored on the server.

3 Installation

3.1 Android Malware Application

1. Copy the file named *EPICMalware.apk* over to your device. You can download the file from `https://github.com/Unsolvable-Solutions/Project-EPIC/tree/master/EPICMalware/MalwareApp/Eavesdrop`.
2. Locate the file on your device and tap on the file.
3. A list of permissions will pop-up that the application needs in order to function. Click on the *install* option.
4. The application is now ready to use.

3.2 Java Malware Server

1. Make sure a minimum version of Java 7 is running on your system.
2. Download(or clone) the source files from `https://github.com/Unsolvable-Solutions/Project-EPIC/tree/master/EPICMalware/MalwareServer`
3. In your command line
   - Redirect to the folder that you have just downloaded.
   - Run

     ```
     java -jar EPICMalwareServer.jar
     ```
4. Follow the on-screen instructions.

4 Getting Started

4.1 Java Malware Server

1. To use the EPICMalware application you first need to start the malware server. Please refer to the installation of the EPICMalwareServer to start the server.

2. There are two options for using the malware server, the server can control the recording or the Android application can be used to control the recording.

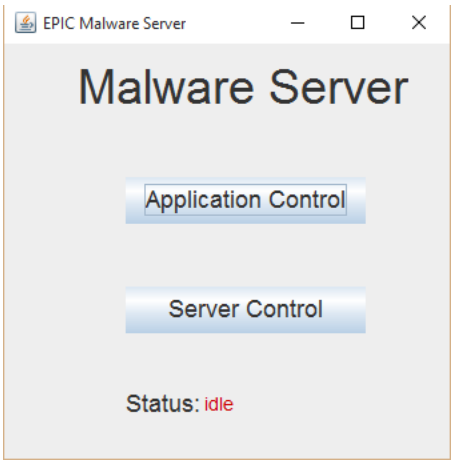

Figure 1: Malware Server main screen

4.2 Android Malware Application

1. Navigate to to application shortcut named *Eavesdrop* on your phone and open it.

2. If application control was selected on the server the *Start Recording* and *Stop Recording* buttons can be used to interact with the server.

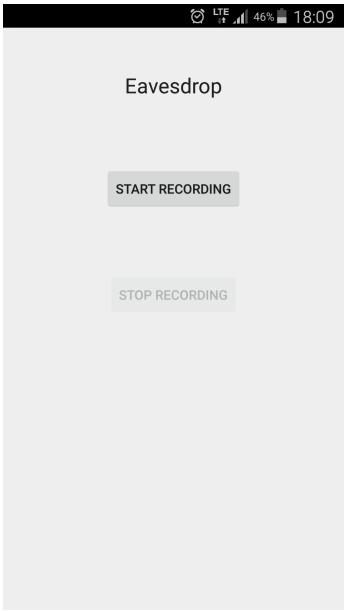

Figure 2: Android Malware Application main screen

5 Using The System

5.1 Java Malware Server

1. If application control is selected the server waits for an incoming connection and starts recording. Using this option the android application is manually controlled. When local recording and streaming needs to be stopped select yes from the stop recording, dialog this will terminate and save the recording.

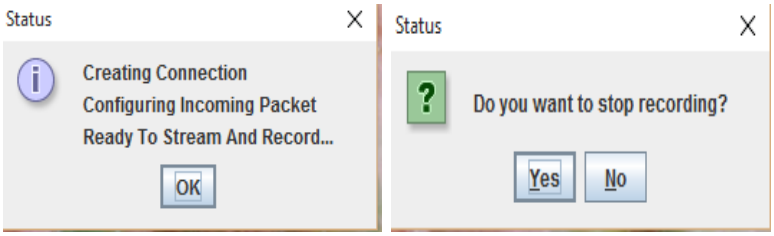

Figure 3: Malware Server options

2. If server control is selected the server will wait for incoming requests to connect to the server and add them to a list.

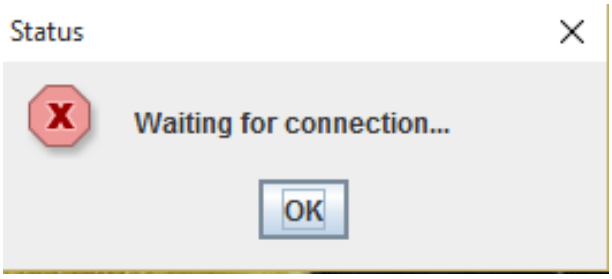

Figure 4: Malware Server server control option selected

3. The user will be able to select a device from the list to eavesdrop on.

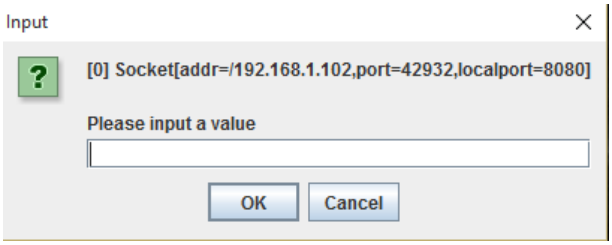

Figure 5: Malware Server device list

4. When a device is selected from the list the server will start to record the incoming stream.

5. When the you want to stop the recording select *Yes* on the stop recording dialog and the server will terminate and save a local recoding of the stream.

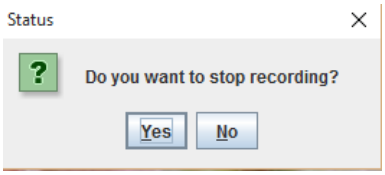

Figure 6: Malware Server recording from device

5.2 Android Malware Application

1. The android application can only be manually controlled when application control is selected on the Malware server.

2. After the *Start Recording* button is pressed, the audio stream will be sent to the server. The *Start Recording* button is now greyed out.

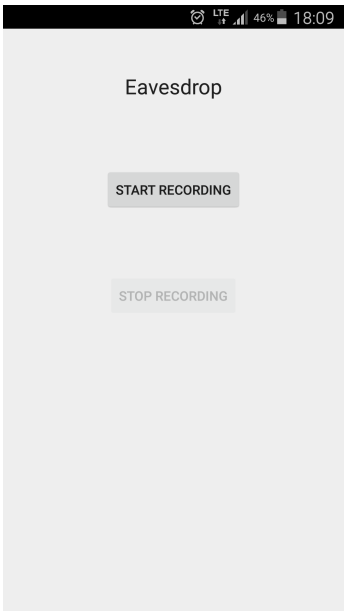

Figure 7: Android malware application start recording

3. After the *Stop Recording* button is pressed, the application stops to send a audio stream to the server. The user must also stop the server to save a copy of the stream on the device running the server.

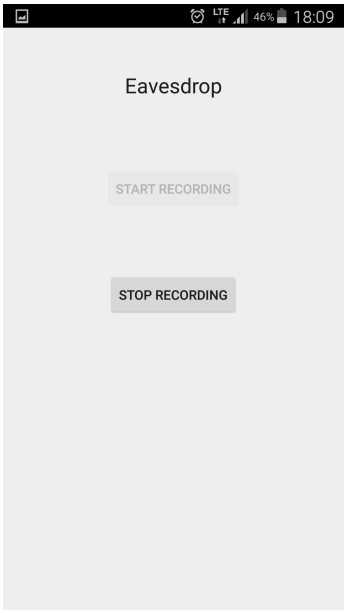

Figure 8: Android malware application stop recording

6 Troubleshooting

6.1 Java Malware Server

- If the server cannot stream the audio or no devices are detected open ports 4545 and 8080 on your firewall. These ports are used for communication between the application and the server.

6.2 Android Malware Application

- If any problems occur within the application just restart the application.