Mobile Privacy & Security

Research Question: Can we tell if an application is malicious based on its network traffic?

**Background**

It is important to protect the data stored on our mobile devices from what are known as malicious applications. Such applications are capable of stealing information from our smartphones that can be dangerous in the hands of the wrong people. As a team, we set out to find ways to secure mobile phones from malicious applications by monitoring the device’s network traffic.

A snapshot from the third annual Mobile Threats Report from Juniper Networks shows some alarming statistics on mobile malware. (Image Source: Juniper Networks)

This gives us a look into the different layers of defense that are built into the Android system. Applications operate in a sandbox, forcing mobile apps to declare if they want access to content such as your contact. (Image Source: LifeHacker.com)

A deeper look into the Android defense layers is shown above. (Image Source: LifeHacker.com)

**Research**

The images above are pictures of the virtual machine we chose to run our applications. This allowed us to use Wireshark to monitor the network traffic.

While Android is not known for their security as we studied apps on our virtual machine Google let us know that they will regularly check installed apps for potentially harmful behavior.

Label Reader is a malicious application that we tested on our VM. When downloading the application you can see that even though it’s a malicious application it still had the visual presence of any normal app. This particular app wants access to texts, contacts, and phone calls.

**Findings**

This is a legitimate application that we ran on the Android Virtual Machine. This application showed us traffic back and forth between the Facebook servers. This traffic seemed to be encrypted after using a packet sniffer to look at the information. All of the servers that Facebook connects to are part of the Facebook domain.

Collage Malicious application goes through pretend to be a program that will allow you to make a collage. One of the first things you notice about this program is that it seems very ad-heavy. It connects to a server and opens the port 443 on the phone. This port is used for the HTTPS protocol and it seems that after analyzing the packet the small amounts of data it sends is encrypted.

Armor for Android acts as a legitimate security system for your Android device. Hidden behind this security system is malware that seems to send small amounts of information to a back-end server. More than likely its main purpose is to charge you for a false sense of security. We noticed that the packets seem to be encrypted and the traffic is pointed to a server in Redmond, Washington.