Research Objective
Smartphones become the most essential part of modern life. Five billion people use mobile phones and among the five billion, one billion people use smartphones around the world. There are 91 million smartphone users in the United States. As the smartphone market sharply grows, threats against smartphones also are increasing. For example, mobile botnets/malwares are very critical problems that smartphones encounter. For example, a botmaster uses an application in order to make slave mobile bots. In fact, these bots are infected by downloading applications from application markets. There are more than 200,000 applications in the official Android market in 2011. There have been several attempts to track mobile botnets/malware. Nevertheless, the numbers of mobile botnet/malware infected smartphones are increasing. Moreover, it is threatening the mobile network. Furthermore, mobile botnet/malware tracking techniques will be discussed.

Android Security
Android is based on Linux kernel security. The features of Linux on security are user-based permission models and process isolation. Especially, the process isolation is an important security key in Linux and Android because it prevents a third party from reading files and using resources and memory. Furthermore, the sandbox in the kernel layer isolates application data and code execution from other applications. Since sandbox is in the kernel layer, that effects whole layers in the security. Android 3.0 offers full encryption. The file system encryption makes users to save their data from third parties. The permission is the same as user’s password on Android device. An Android application has the same permission limitation for security in order to protect its data. For example, the application limits call, GPS, SMS/MMS, etc. by permission security. However, the permission can be changed by Android OS. For example, applications ask permissions from users. The application developer codes the permission in manifest. Permission selection can be done when a user installs a new application.

Android Propagation
There are many different methods for the propagation of malware and botnet in Android platform. Today, SMS/MMS (malicious link), malicious application, wireless connections (Bluetooth), and kernel layer hacking are commonly used. We will show the hacking methods and analysis for SMS/MMS, malicious application, and kernel layer hacking on Android smartphones later.

Hacking Method & Analysis
The function doExecuteTask run remote-control on a victim’s smartphone. The function doExecuteTask has five C&C command (execHompage, execInstall, execOpenUrl, execDelete, and execStartApp). The command execHompage opens the website that is prepared by a hacker. The command execInstall install malicious application from the prepared website. The command execStartApp runs the application which is prepared in the URL. The command execOpenUrl is to open the URL. The command execDelete is to delete a file.

The Platform of Android
Understanding Android malware/botnet analysis and tracking techniques requires knowledge on Android operating system (OS). Android is composed of Linux kernel, middleware, libraries, framework, and application software. The structure of Android application is shown in Figure 1. Android OS uses a Linux-based system for smartphones. Developers use Android software development kit written in Java language to make applications. It can be extended in C or C++ in the libraries layer. In the runtime layer, applications are executed in Dalvik virtual machine (DVM). DVM translates javabytecode to Dalvik dex-code. Java virtual machine (JVM) is stack-based. Unlike JVM, DVM is register-based that can assign variables to 216 resistors. So, they can use memory more efficiently. The Linux kernel layer has an important role because it has main system functions such as memory, security, and network.

Android Security
Android is based on Linux kernel security. The features of Linux on security are user-based permission models and process isolation. Especially, the process isolation is an important security key in Linux and Android because it prevents a third party from reading files and using resources and memory. Furthermore, the sandbox in the kernel layer isolates application data and code execution from other applications. Since sandbox is in the kernel layer, that effects whole layers in the security. Android 3.0 offers full encryption. The file system encryption makes users to save their data from third parties. The permission is the same as user’s password on Android device. An Android application has the same permission limitation for security in order to protect its data. For example, the application limits call, GPS, SMS/MMS, etc. by permission security. However, the permission can be changed by Android OS. For example, applications ask permissions from users. The application developer codes the permission in manifest. Permission selection can be done when a user installs a new application.

Hacking Method & Analysis
The function doExecuteTask run remote-control on a victim’s smartphone. The function doExecuteTask has five C&C command (execHompage, execInstall, execOpenUrl, execDelete, and execStartApp). The command execHompage opens the website that is prepared by a hacker. The command execInstall install malicious application from the prepared website. The command execStartApp runs the application which is prepared in the URL. The command execOpenUrl is to open the URL. The command execDelete is to delete a file.

Conclusion
As smartphone users are sharply increasing, a mobile network is targeted to hacker groups. Actually, mobile devices have more private stuffs than PCs. For this reason, hacker groups are focusing on mobile devices than PC. In this project, we have discussed the hacking methods and analysis for android platform. In order to maintain mobile security from the threat of hacker groups, defenders need to make corporation to share their techniques and information for the threat from botnets and malware. Furthermore, mobile carriers and defender groups should work together and keep developing their detection technologies.

Figure 1. Structure of Android Application

Figure 2. Function doSearchReport
You can get imei, ostype, osapi, model, SDKVersion, SDCard information, internal memory size, net operator, phone number, and running service from function updateInfo. Since an attacker got the victim’s all information from function doSearchReport. The attacker needs to get permission on Android platform. Figure 4 shows the function getPermission3 in which attackers are rooting the target smartphone.

Figure 3. Function updateInfo

Figure 4. Function getPermission3
This exploit is /assets/rats, encrypted by AES algorithm. It is executed with description when the application is installed. Figure 5 shows the key for decryption.

Figure 5. Key for Encryption

Figure 6. Function cpLegacyRes
When the rooting process has executed, the application will install a malicious app that is hidden in ‘assets’. This malicious application impersonates the well-known Google search application but this application name is ‘Google Search’. Figure 6 shows function cplegacyRes that installs malicious applications in ‘assets’.

Figure 7. Function doExecuteTask
Android platform is also weak on Wi-Fi packet sniffing. Anyone can catch packets without Android hacking knowledge by using rootkit application. First, you need to jail-break on your Android phone. Then, install Rootkit application. After the installation, you can see all Wi-Fi users’ information through the application. Figure 8 shows Wi-Fi users information. Furthermore, you can get information about personal privacy information by analyzing packets. Figure 9 shows an Android smartphone user who is connected to UART website.

Figure 8. Wi-Fi user information

Figure 9. Android Phone user’s packet information

Daun Lee, Seungwon Keum

Android Hacking and Analysis

The Department of Electrical Engineering

The University of Alabama in Huntsville