COSC 647 – Fall 2015 – Group Project – Logan Bair & Mary Snyder
Report 2

1. What has been done from report1?

   We started working with Android x86 version of the OS, but realized there was no easy way to emulate SMS/text sending. We did more research and discovered Android Studio would be able to provide us the SMS/text functionality we needed, still in a VM form. There still may be issue with sending MMS messages, but we should be able to circumvent this using google hangouts or other application that allow videos to be sent/received.

   Research on emulation and Android Studio:

   http://developer.android.com/tools/studio/index.html

   http://developer.android.com/tools/devices/emulator.html

2. What technique that you use/develop/discover? How are you implementing it, and on which platform?

   We are using Android Studio to stand up version of the Android OS and have the ability to emulate sending of SMS/text messages. Since the exploit will be sending a video or other media, an MMS message will be required. We are looking to use the Google hangouts or other similar application to be able to perform this task. We have not yet settled on one version of the OS and are determining which versions this exploit can easily be run and a version that may be more secure, but still able to give the attacker some control.

3. Are you on schedule? What do you expect for your final report?
   By the second report, we expected to have:
   a. Selected an Android OS version and have built the VM for exploitation
   b. Researched and created the code to be sent in the exploit text message to the VM
   c. Work with the code to get the "Stagefright" vulnerability to execute
   d. Begin testing our exploit

   What we actually accomplished since the first report:
   a. Selected an Android OS version and have built the VM for exploitation
   b. Researched and created the code to be sent in the exploit text message to the VM
   c. Determined the medium we had selected, x86 Android project, would not be able to do what we needed
   d. Regrouped and determined an alternate way of running an Android VM.

   By the final report, we expect to have:
   a. Begin testing our exploit and successfully completed the exploit
   b. Test how much control the exploit can give the attacker over the Android OS
   c. Still hopeful there will be time to determine if the exploit can self-propagate as a worm that goes through the phone's contact list and sends itself to each contact
   d. Have complied our research and findings into a completed presentation/paper