COSC 647 – Fall 2015 – Group Project – Logan Bair & Mary Snyder
Report 1

1. What your topic is about. And what have you read/done so far.

   "Stagefright" is a component in the core of the Android OS responsible for processing multimedia files (videos, audio, and docs). Whenever you play any video or audio files, the component runs in the background processing the information to present to the user. When an MMS message is received, the Android OS pre-processes the multimedia file in order to display a preview of the message. This pre-processing will cause any malicious code embedded in the multimedia file to be executed even before the multimedia file is viewed.

2. What has been done in the past? You should read at least 3-4 articles/papers about the topic. Cite them.

   Researchers at Zimperium revealed the vulnerability and an initial patch has been released; however, a new version 2.0 has recently been announced.

   Stagefright: Vulnerability Details, Stagefright Detector tool released: https://blog.zimperium.com/stagefright-vulnerability-details-stagefright-detector-tool-released/

   How to Hack Millions of Android Phones Using Stagefright Bug, Without Sending MMS: http://thehackernews.com/2015/07/how-to-hack-android-phone.html

   Hacking any android smartphone using "Stagefright" vulnerability: http://www.hacker9.com/hack-android-smartphone-vulnerability.html

   Websites on the exploit (Exploit Database):

   https://www.exploit-db.com/exploits/38226/

   https://www.exploit-db.com/exploits/38124/

3. What do you expect for Report 2 and the timeline? What do you expect for the final report?

   By the second report, we expect 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

   By the final report, we expect to have:

   e. Successfully completed the exploit
   f. Testing how much control the exploit does/can give over the Android OS
   g. If time, determine if the exploit can self-propagate as a worm that goes through the phone's contact list and sends itself to each contact.
   h. Have complied our research and findings from