# SUMAIYA NAZNEEN

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY AND ASSURANCE

## INCIDENT RESPONSE MANAGEMENT GUIDE TO DEAL WITH ANDROID MALWARE RELATED INCIDENTS

In recent years, with the rapid advancement of technology, a smartphone has significant risks as they contain sensitive information. This can lead to serious security risks in case of unauthorized access or if an important information is being accessed over an unsecured network. The major challenge in countering attacks is the lack of knowledge about the various types of Android malware and their behavior, which makes the existing detection system and incident response management system ineffective. This research aims to provide a better understanding of Android malware and its general behavior by profiling related studies that can be used as a primary guideline to prepare the taxonomy for the android malwares. Hence, it helps in preparing the incident response management guide to deal with malware infected Android devices. Using NIST standards, SANS guidelines and related works to deal with malware related incidents information will be used to develop an incident response management guide that will help an incident responder or a security analyst to deal with an incident related to Android malwares infected devices.

***Research Advisors: Dr. Pavol Zavarsky, Dr. Dale Lindskog***