Abstract

Name of the student: **Gaurav Kumar** Roll No: **16111036**
Degree for which submitted: **M.Tech.** Department: **Computer Science and Engineering**
Thesis title: **Automatic malware detection using memory forensics**
Thesis supervisor: **Dr. Sandeep Shukla**
Month and year of thesis submission: **May 2018**

Detection of a malware when a new binary is downloaded, to distinguish it from 'benign-ware' is an important part of computer security. There exist various techniques proposed by researchers using both static and dynamic analyses to detect malware. But day by day, malware authors have improved its evasion capability using non-persistence, obfuscation techniques, and use of volatile payloads that operate only in memory. With obfuscation techniques, malware authors make the reverse engineering of binary tougher. So now malware analysis is not limited to static and dynamic analysis. By memory forensics techniques we can get a comprehensive view of the actions of an executable. We have used an interval-based approach to take the memory dumps and then selected one memory dump for further analysis. In this work we have extracted various features from memory dump such registry bindings, suspicious DLLs, hidden processes, orphan threads, code injection, injected DLLs, file system etc., and automated the classification of malware vs. benign-ware. For evaluation purposes we used 1730 malware and 1571 benign files. We achieved 99.09% accuracy with 0.43% false positive rate using XG-Boost classification method.