***Vulnerability Detection in Mobile Applications Using State Machine Modeling***

*Mobile applications play an ever-more important role in modern society lives. Although the applications are widely adopted, their security is often not guaranteed. State machine learning has proven to be an effective method for vulnerability detection in software implementations and can thus be extended to improve the security of mobile applications. The extension requires a method to learn state machines for mobile applications and the establishment of an approach that detects vulnerabilities from the inferred models. To the best of our knowledge, there exists no framework that automatically infers behavioral state machine models on general mobile applications and neither does there exist a methodology for automatic vulnerability detection on the inferred models. This thesis proposes two solutions to the above-mentioned challenges. First, a framework for inferring a model on general mobile Android applications is presented, that uses active state machine learning algorithms to ensure model correctness and time minimization on the learning process. Secondly, algorithms are designed that utilize the inferred model and determine the presence of vulnerabilities. Both solutions can be combined to provide a new insight into an application's behavior and achieve the goal of vulnerability detection. Moreover, the solution is able to detect rogue applications such as a malicious WhatsApp version in the Android’s Play Store, which infected more than 1 million devices in three days.*