Vulnerability Detection in Mobile Applications Using State Machine Modeling

Mobile Android applications play an ever-more important role in enabling services on smart devices such as phones, televisions and cars. Although the applications are widely adopted, their security is often not guaranteed, because economic incentives drive application providers to retrench on testing and secure software development. Initiatives like the *Open Web Application Security Project* (OWASP) provide documents to structure the testing process. One of the documents is a list of vulnerability classifications that are prominently present in today's mobile application market and impose security risks.

Recent research on protocol implementation has shown that inference of the software's behavioral model provides additional insight into the software system. As a results, the inferred model can be manually assessed for the presence of a security risk. The aim of this thesis is to identify vulnerabilities in mobile applications by inferring such a behavioral model and use the model as input for automatic vulnerability detection. To identify the presence of a vulnerability, one must overcome two main challenges. Foremost, a technique for behavioral model inference on mobile applications should be established in order to create such a model. Secondly, an approach is required that utilizes the inferred model and identifies the presence of the vulnerabilities based on the model.

This research 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 learning process. Next, algorithms are designed that utilize the inferred model and determine the presence of vulnerabilities for classes defined by OWASP. This thesis shows that both solutions can be combined to provide a new insight into an application's behavior and achieve the goal of vulnerability detection. To the best of our knowledge, there exists no framework for automatically inferring behavioral state machine models on general mobile applications and neither does there exist a methodology for automatic vulnerability detection on the inferred models.