Automated Tool Support for Security Bug Repair in Mobile Applications

Larry Singleton, Graduate Student, Computer Science
Faculty Mentor: Myoungkyu Song and Harvey Siy, Computer Science, Rui Zhao, Cybersecurity

Cryptographic misuse is becoming one of the most common issues in development. Attackers usually make use of those flaws in the implementation of mobile apps. The manual implementation of mathematical equations into applications is a difficult task that often causes failures in the correct usage of cryptographic Application Program Interfaces (APIs) or algorithms (i.e., cryptographic misuse). For example, in mobile banking and payment apps for CitiBank and Starbucks, developers used plaintext to store the customer's privacy information such as payment passcodes and bank account numbers, which can easily expose these vulnerabilities to malicious attackers. It is crucial to evaluate the correctness of cryptographic misuses in mobile apps. The right way to use these algorithms and APIs provides strong security guarantees and the wrong way invariably leads to security vulnerabilities. An automated approach is needed to address the security issues to detect security vulnerabilities and to dynamically repair those problems.

To address the problem, we propose an automated approach to Finding and Repairing Bugs based on security patterns (FIREBUGS), which aims to detect vulnerabilities, automate the generation of repair patches, and dynamically apply bug fixes at runtime. Our project focuses on the implementation of this approach by developing a proof-of-concept prototype "FIREBUGS", as a plug-in for Integrated Development Environments (IDE). Given a buggy program that misuses cryptographic APIs, FIREBUGS automatically detects vulnerabilities and generates a repair patch that passes a test suite encoding the required behavior. Our goal is to design FIREBUGS to repair common types of cryptographic API misuses in mobile applications. Since most common vulnerabilities have recurring patterns, FIREBUGS generates repair patches by utilizing a template-based approach and dynamically applies patches to vulnerable locations at runtime. Thus, FIREBUGS helps developers protect mobile applications from attackers who may take advantage of cryptographic misuse vulnerabilities. FIREBUGS focuses on a special family of software bugs in the area of cryptographic misuses and leverages specialized domain knowledge to achieve a much higher success rate of repair.