Apr 1st, 1:00 PM - 1:20 PM

Automated Program Repair for API Misuse Vulnerabilities

Dip Kiran Pradhan Newar
dpradhannewar@unomaha.edu

Automated Program Repair for API Misuse Vulnerabilities

Dip Kiran Pradhan Newar, Graduate Student, Computer Science
Faculty Mentors: Myoungkyu Song, Harvey Siy, Rui Zhao

Application Programming Interfaces (APIs) in cryptography typically impose concealed usage constraints. The violations of these usage constraints can lead to software crashes or security vulnerabilities. There are several professional tools that can detect these constraints(API misuses) in cryptography. However, in the educational programs, the focus has been on helping students implement an application without cryptographic API misuses that are caused either by a lack of cryptographic knowledge or by programming mistakes.

To address the problem, we present an intelligent tutoring approach **SSDTutor** for educating Secure Software Development. Our tutoring approach helps students repair cryptographic API misuse defects by leveraging an automated program repair technique based on the usage patterns of cryptographic APIs. We studied the best practices of cryptographic implementations and encoded eight cryptographic API usage patterns. For quality feedback, we leverage a clone detection technique to recommend related feedback for helping students understand why their programs are incorrect, rather than blindly accepting repairs.

We evaluate **SSDTutor** on 456 open source subject projects that have been implemented with cryptographic APIs. We assess **SSDTutor**'s capability of whether to successfully detecting vulnerabilities (1567 out of 1606 detections with 97.9% accuracy) and repair misuse defects (1561 out of 1567 repairs with 99.8% accuracy). In a user study involving 20 students, we will report whether **SSDTutor**'s feedback recommendation can be valuable for the participants to interactively learn about correct usages of cryptography APIs.