

Data Protection with SMSD Labware

Hossain Shahriar, *Kennesaw State University*

Kai Qian, *Kennesaw State University*

Md Arabin Islam Talukder, *Kennesaw State University*

Reza Parizi, *Kennesaw State University*

Contact: hshahria@kennesaw.edu

The majority of malicious mobile attacks take advantage of vulnerabilities in mobile applications, such as sensitive data leakage via inadvertent or side channel, unsecured sensitive data storage, data transmission, and many others. Most of these mobile vulnerabilities can be detected in the mobile software testing phase. However, most development teams often have virtually no time to address them due to critical project deadlines. To combat this, the more defect removal filters there are in the software development life cycle, the fewer defects that can lead to vulnerabilities will remain in the software product when it is released. As part of Secure Mobile Software Development (SMSD) project, we are currently developing capacity to address the lack of pedagogical materials and real world learning environment in secure mobile software development through effective, engaging, and investigative approaches. In this session, we provide details of a new implemented module named *data protection*. We also share our initial experience and feedback on the developed module.

Keywords: Mobile Software; Data sanitization; input validation; SQL injection;

DOI: <http://dx.doi.org/10.1145/3287324.3293785>.

CCS Concepts: Computing Education → Mobile Software