Secure Coding in Java

Building secure software can be challenging and hard. This course provides a detailed explanation of common programming errors in Java and describes how these errors can lead to code that is vulnerable to exploitation. The course concentrates on security issues that are relevant to the Java programming languages and associated libraries.

The course requires basic Java programming skills but does not assume an in-depth knowledge of software security.

Learning Objectives

The participants would get a working knowledge of common programming errors that lead to software vulnerabilities, how these errors can be exploited and how we can prevent the introduction of these errors. In particular, they will learn how to:

- Improve the overall security of any Java application
- Avoid injection attacks, such as SQL injection and XSS
- Understand Java's memory model and the JVM byte-code verifier
- Learn when to throw and catch exceptions
- Avoid I/O vulnerabilities
- Implement safe serialization and deserialization
- Use static analysis tools like FindBugs to detect errors

Course Contents

The course will be delivered in 6 sessions over 3 days. Each session has a presentation followed by a lab or demo. For the lab and demos, participants are encouraged to bring in their laptops to practice.

Session 1 – Introduction and OWASP Top 10 vulnerabilities

Session 2 – Java security model and language based security

Session 3 – Input validation and Injection vulnerabilities

Session 4 – Object construction, mutation and deserialization

Session 5 – Exceptions, concurrency and I/O

Session 6 – Using static analysis to find bugs

Contact asankhaya@u.nus.edu for more details and pricing.