

Lab: Abstract Interpretation

(Week 10)

Yulei Sui

School of Computer Science and Engineering

University of New South Wales, Australia

Lab-3 and Assignment-3 Marking

- Assignment-3 marking for the eight methods you need to implement
 - Your implementation (8 methods) will be evaluated against X number of our internal tests. **If you pass Y tests, you will receive $Y/X * 100\%$ marks.**
 - We do not mark each of the eight individual methods separately; instead, **we mark based on the number of test cases you pass.**
- Marks will be released after teaching week (Week 11 for Lab-3 and Week 12 for Assignment-3)
- If you have questions, feel free to post on Ed forums or email our course admins.

Quiz-3 + Lab-Exercise-3 + Assignment-3

- Quiz-3 (5 points) (due date: **23:59, Wednesday, Week 10**)
 - Abstract domain and soundness, widening and narrowing
- Lab-Exercise-3 (5 points) (due date: **23:59, Wednesday, Week 10**)
 - **Goal:** Manually updating abstract states for assertion verification
 - **Specification:** <https://github.com/SVF-tools/Software-Security-Analysis/wiki/Lab-Exercise-3>
- Assignment-3 (25 points) (due date: **23:59, Wednesday, Week 11**)
 - **Goal:** Automated abstract trace update on ICFG for assertion verification and overflow detection
 - **Specification:** <https://github.com/SVF-tools/Software-Security-Analysis/wiki/Assignment-3>
 - **SVF AE APIs:** <https://github.com/SVF-tools/Software-Security-Analysis/wiki/AE-APIs>
 - **Test Cases:**
 - [Assignment-3/Tests/ae](#) (assertion verification)
 - [Assignment-3/Tests/buf](#) (overflow detection)