The University of Melbourne

SWEN90010: High Integrity Software Engineering

Assignment 3

Due Date: 11:59pm, Sunday 15 May, 2016

1 Introduction

The assignment is worth 20% of your total mark and is done in pairs (the same pairs as assignment 2).

The aim of this assignment is to specify a formal model in Alloy of (part of) the FatBat management system. The assignment evaluates your ability to apply specification and design techniques to engineer a security- and safety-critical system.

2 Your tasks

The file `AMS.als` is an Alloy model which describes part of the requirements outlined in Assignment 1. It contains the relevant signature and predicate definitions to create users, add/read friends & insurers, and update user data.

Your tasks are as follows:

1. **Complete the model [8 marks]** Update the model by adding signatures and predicates/-functions that model the missing requirements from Assignment 1. For requirements that are ambiguous, model the behaviour that was implemented in Assignment 1 by one of the people in your pair.

2. **Check important properties [6 marks]** Select three class I or II hazards identified in the HAZOP performed in Assignment 2.

   For each of these three hazards, write an assertion in Alloy (using the `assert` construct) that models this property, and determines whether or not it holds on the model of the system.

3. **Update the model for implicit constraints [4 marks]** Update your model so that your assertions hold in the way that you intended. You can modify any existing signatures, predicates/functions, or facts.

4. **Report [2 marks]** Write a brief report of no more than a page describing why you chose the assertions you did, what issues you found in the model using the assertions, and what changes were made to the model to make the assertions hold. Any text that is more than a page will not be marked.

3 Criteria

Criterion	Description	Marks
Model	New predicates & functions are correct and complete. New signatures correctly model the data. An appropriate level of abstraction has been used. The solution is clear and succinct.	8 marks
Assertions	At least three valid and sensible implications have been designed and modelled. The assertions are correct and complete.	6 marks
Updated model	The updated behaviour correctly and completely addresses the identified security implications.	4 marks
Report	The report presents a clear and valid reason choice for assertions. The report clearly identifies the changes made to the model	2 marks
Total		20 marks

4 Submission

Submit the assignment using the submission link on the subject LMS. Go to the SWEN90010 LMS page, select *Assignments* from the subject menu, and then select *View/Complete* from the *Assignment 3 submission* item. Following the instructions, upload:

1. An alloy file, named `AMS.als` containing your final model.
2. A PDF file containing your one page report.

Only *one* student from the pair should submit the solution, and the submission should clearly identify both authors.

Late submissions. Late submissions will attract a penalty of 2 marks for every day that they are late. If you have a reason that you require an extension, email Tim *well before the due date* to discuss this. Please note that having assignments due around the same date for other subjects is not sufficient grounds to grant an extension. It is the responsibility of individual students to manage time to avoid bottlenecks. Starting early on this is highly encouraged.

5 Academic Misconduct

The University misconduct policy applies to this assignment. Students are encouraged to discuss the assignment topic, but all submitted work must represent the individual's understanding of the topic.

The subject staff take plagiarism very seriously. In the past, we have successfully prosecuted several students that have breached the university policy. Often this results in receiving 0 marks for the assessment, and in some cases, has resulted in failure of the subject.