The University of Melbourne

SWEN90010: High Integrity Software Engineering

Assignment 3

Due Date: 11:59pm, Sunday 13 May, 2018

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 ICD system, and to carry out some formal security analysis. The assignment evaluates your ability to apply formal specification techniques to help engineer a security- and safety-critical system.

2 Your tasks

The file `icd.als` (available on the LMS) is an Alloy model of (part of) the ICD system from Assignments 1 and 2, focussing on the system's *external* interface from the point of view of the Network, and describing aspects of its behaviour in response to the receipt of Network messages.

Recall that the Network interface for the ICD system is a wireless network. This interface has become a common vector by which various "pacemaker hacking" and similar attacks and demonstrations have been carried out in recent years [1].

The provided Alloy model focuses on the interactions between the cardiologist and the ICD device, via the Network. To keep the assignment tractable, it does *not* model the clinical assistant nor any of the interactions between the ICD device and the heart, and it models only a small part of the system's external interface via the Network.

It has declarations for predicates (some of whose bodies you will have to fill in as part of the assignment) to model a subset of the system's behaviour, such as sending and receiving the *ModeOn* message, and sending and receiving *ChangeSettingsRequest* messages. It also includes a predicate to model the actions of a potential *attacker*, which we assume has access to the wireless Network. Part of the assignment involves using Alloy to help reason about the ICD system in the presence of such an intruder which, if recent history is any guide, is not an unreasonable assumption.

Traces of system actions are captured using the `util/ordering` module described in lectures. *Hint: you may find it helpful to make use of the functions defined in that module when writing assertions and predicates for this assignment. A copy of the Alloy source for the module is available on the LMS with the assignment.*

Your tasks are:

1. **Modelling Actions in Alloy (6 marks).** Read the comments in the provided Alloy file and, in the *Actions* section of the file, fill in both the missing comments describing the pre- and postconditions of each action as well as the missing action predicate bodies.

2. **Specifying and Checking Simple Properties (3 marks).** Besides an initial example assertion, there are two simple assertions in the *Properties* section of the provided file (and a third one that we come to later). The first assertion states that the predicate `inv`, described in the comment above its declaration, always holds in all states. `inv`'s body is missing. Fill in its body by referring to the comment and to the requirements listed in the Assignment 1 sheet.

   For the second assertion, `unexplained_assertion`, your job is to read and understand what the assertion is saying. Then fill in the comment above to show your understanding of the assertion.

   Use Alloy to check whether these two assertions hold, increasing the scope of the checks as necessary to increase your confidence in the results. Add comments below each of the checks describing whether each is true or not and why.

3. **Updating the Attacker Model (5 marks).** The model of the attacker, captured by the `attacker_action` predicate, is very powerful. It models an attacker that has the ability not only to alter the contents of messages on the network, but also to inject new messages onto the network, amongst other things. By doing so, the attacker can for example *impersonate* the authorised cardiologist, by sending a new message whose `source` field names the authorised cardiologist.

   Suppose we were to try to guard against this kind of attack by using *unguessable* names for Principals on the network. For instance, rather than being identified by their name, suppose the authorised cardiologist was identified by a random 256-bit string. Under this design, the attacker cannot for example create a message whose `source` field purports to be from a particular Principal unless they have somehow learned the random bitstring that identifies that Principal.[1]

   Update the `attacker_action` predicate to faithfully model the attacker's reduced abilities under this new design, remembering to update the comments accordingly. For any checks that might have failed before, if they now hold you should add a comment to explain why. If they still fail to hold, make sure your explanation includes why they still fail even under the updated attacker model.

4. **Specifying and Checking a More Advances Property (4 marks).** For this part of the assignment, you now need to examine the `turns_on_safe` assertion. Read its description in the comment and then fill in the body of the assertion.

   If your updated attacker model correctly captures the attacker's new (reduced) abilities, and you have correctly specified the `turns_on_safe` assertion, then you should find that this assertion does *not* hold. However, the new attack given in the counter-example by Alloy is more involved than the simplest attacks on this property under the original attacker model.

   Add comments explaining this attack, and why in a real implementation of this system one would need to restrict the attacker's abilities even further. Explain what extra restriction is required. You are not required to explain how one might *implement* that extra restriction, however.

   Add comments to the file to describe the kinds of attacks that are still possible under the updated attacker model.

[1] Technically it might be possible for the attacker to still guess the bitstring, but the probability of them doing so would be so small that for the purposes of this assignment we will treat it as impossible.

Note: to get full marks here, your description of what kinds of attacks are possible in the updated attacker model will need to include kinds of attacks that may not be captured by the counter-examples you get to the assertions in the Alloy file. You might therefore like to try to write some additional assertions to see if there are other kinds of attacks that Alloy can identify.

5. **Relationship to HAZOP Study (2 marks).** Consider *your* HAZOP study in Assignment 2. Add comments describing:

   (a) Which of these attacks are covered by hazards that you identified.

   (b) Any new hazards suggested by these attacks, including the design item that each applies to and an appropriate HAZOP guideword for each.

3 Criteria

Criterion	**Description**	**Marks**
Model	Action predicates bodies and comments are correct and complete. Updated attacker model and comments are correct and complete. The solution is clear and succinct.	11 marks
Assertions	Appropriate choice for `inv`. Correct definition of `turns_on_safe`. Formal properties accurately capture their descriptions. The attacks under the updated attacker model are identified. The solution is clear and succinct.	7 marks
Relationship to HAZOP	Correct identification of hazards and guidewords.	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. Upload your commented `icd.als` file, ensuring that it has this file name and that the comments in the file clearly identify *both* authors in your pair.

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 Toby *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 ensure that, if they have a cluster of assignments due at the same time, they start some of them early to avoid a bottleneck around the due date. The content required for this assignment was presented before the assignment was released, so an early start is possible (and 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.

References

[1] Johannes Sametinger, Jerzy Rozenblit, Roman Lysecky, and Peter Ott. Security challenges for medical devices. *Communications of the ACM*, 58(4):74–82, April 2015.