17-614 Formal Methods
Project: Structural Modeling

Team 16

yashanan
salonisi
halkhala
ktakayam

October 10, 2022

Task1

1. Include an object model diagram for your system.

2. Describe any decisions that your team made in resolving ambiguities in the English document. Also describe alternatives you considered and rejected.

3. Describe any invariants that are not explicitly mentioned in the given document but were discovered during the modeling process.

4. Describe an invariant that was violated by an operation in your model and how it was fixed.

5. List the scope used for the analysis of invariant preservation. Why did you choose this scope, and why do you think it is sufficient?

Task2

1. Define an Alloy function called canView, which takes at least one parameter that represents some user in the social network, and returns the set of all content that can be viewed by that user. You may use any number of helper predicates or functions to define canView.

2. You will use canView to check whether it is possible for a user to access a piece of content against the intent of the owner. In particular, we say that a privacy violation has occurred if a user is able to view a piece of content without adhering to the privacy level that is assigned to the content by its owner. For example, suppose that Alice and Bob are not friends, and Alice has a photo that is assigned privacy setting Friends; if Bob is able to view the photo, this would be considered a privacy violation. Define an Alloy assertion called NoPrivacyViolation to check that no such violation is possible.

3. Does your model satisfy NoPrivacyViolation? If so, explain why. If not, include a counterexample that demonstrates a violation, and suggest a modification to the design of privacy settings in Nicebook. Describe any alternatives you considered and rejected, along with justifications for your decision.

Task3

1. What are the strengths and weaknesses of Alloy and its tool, the Alloy Analyzer?

2. Under what situations would you recommend its use (or not)? Why?

3. With respect to this notation, what is the single most-important future development that would be needed to make it more generally useful to practitioners?