Homework 2: Common Criteria and UMLSec

See Webcourses and the syllabus for due dates.
This homework is about the common criteria for information technology security evaluation [Cri12] as well as UMLSec [JÖ5].

General Directions

This homework can be done in groups. You should form a "group" under the webcourses group set named "HW2 Groups" for it, even if it consists of yourself only. Note: do *not* use the group you may formerly have had in "Student Groups" as that does not work to communicate properly with webcourses, but only use one you will now set up in "HW2 Groups". If you do work in a group with others, be sure to certify that you all understand and participated in the solutions as required by the course grading policy, see the cooperation section of the course grading policy.
Answers to English questions should be in your own words; don't just quote from articles or books.

What to turn in

For problems that require an English answer, please paste the text of your answer into the text box on webcourses. If the problem may benefit from formatting support, we will instead have you upload a word document or a PDF file.

Problems

Consider the "Low Assurance Protection Profile for a VPN gateway" [FA05], which is available from the Common Criteria site [Cri12] or directly from `https://www.commoncriteriaportal.org/files/ppfiles/pp0013b.pdf`.[1] Your task in this problem is to understand the requirements from that protection profile, and to translate them into a design in UMLSec [JÖ5].
In your design, the Client must support the following operations: `connect()`, `send(d:Data)`, `receive():Data`, and `disconnect()`. The `send` and `receive` operations can only be used when the Client is connected (i.e., after a successful call to `connect()` and before a call to `disconnect()`. You can assume that the Client knows the account information for its user, so there is no need to complicate the diagrams by discussing how the client gets authentication information from its user (i.e., assume this has already been done).

1. (15 points) [SecurelyConstruct] Draw a UMLSec statechart diagram [JÖ5, Section 3.2.3] for the Client. You should be sure to include the operations described above, as well as all messages that are sent to and received from the Gateway, and any conditions that need to be checked. In your diagram, you can concentrate on the happy path by assuming that errors stop execution of the client code. Be sure that the messages sent by the Client are received by the Gateway and vice versa.

   Hint: for writing statechart diagrams for establishing a VPN connection you may find it helpful to adapt the (fixed) TLS protocol shown in Figure 5.4 of the UMLSec book [JÖ5]. However, if you do that, be sure to change all the names in a consistent way and also the UMLSec book if you do use it.

2. (15 points) [SecurelyConstruct] Draw a UMLSec statechart diagram [JÖ5, Section 3.2.3] for the Gateway. You should be sure to include the operations described above, as well as all messages that are sent to and received from the Client, and any conditions that need to be checked. In your diagram, you

[1] On page 4, under OE.ADMIN, you can correct the phrase "S.ADMIN shall keep the computing platform of the TOE integer." to "S.ADMIN shall maintain the integrity of the computing platform."

can concentrate on the happy path by assuming that errors stop execution of the gateway code. Be sure that the messages sent by the Gateway are received by the Client and vice versa.

3. (10 points) [SecurelyConstruct] Draw a UMLSec class diagram [JÖ5, Section 3.2.2] which has (at least) 2 classes: the Client and the Gateway. It should include all the attributes needed to carry out the authentication and for tracking the state of the protocol between the client and the gateway. Include any appropriate security stereotypes, labels, and tags that correspond to the requirements in the protection profile for the VPN gateway. This can be done either by hand (and then scanned or photographed) or with powerpoint or some other drawing tool, but however this is done it should be part of the document you turn in.

   Hint: for drawing class diagrams, you can also refer to Figure 5.4 of the UMLSec book [JÖ5] as an example. Be sure to collect all the attributes and operations used in the diagram. The operations of the Client class are the messages sent to it; similarly, the operations of the Gateway class are the messages sent to it. If you name the messages originating from each class uniquely (which helps readability), then those messages will all appear as operations in the other class.

4. (30 points) [SecurelyConstruct] Draw a UMLSec sequence diagram for the interactions between the client and the gateway for the normal case of the client connecting to the gateway, sending a message to the LAN, receiving a message from the LAN, and then disconnecting.

   Hint: This diagram should be consistent with both of the statechart diagrams. See Figures 5.4, 5.2, and 4.14 in the UMLSec book [JÖ5] for examples.

Points

This homework's total points: 70.

References

[Cri12] Common Criteria. Common criteria for information technology security evaluation. Version 3.1, revision 4, September 2012.

[FA05] Dirk Feldhusen and Sandro Amendola. Low assurance protection profile for a VPN gateway. Protection Profile on the Common Criteria site, April 2005.

[JÖ5] Jan Jürjens. *Secure Systems Development with UML.* Springer-Verlag, Berlin, 2005.