Alloy Gateway

To: CSci 8801, All students
From: Dr. Mats Heimdahl
Date: 10/6/2006
Re: Homework Assignment 2

The Problem
A simple gateway routing email traffic from a high security system to either a high or a low security external system.

We will have a simplistic view of the world and see if Alloy will serve us better in this example.

There are email messages being sent on the channels. An email message has a sender, recipients (To field), and possibly persons on the cc and bcc lines. Each email is classified to be secret or not secret. Secret messages can only be forwarded to the secure output stream.

Persons using the system are classified to be secret, trusted, not-trusted, and neutral (trusted, neutral, and not-trusted are mutually exclusive classifications; a trusted user can also be classified as secret). Not-trusted users cannot send secret messages. Not-trusted and neutral recipients cannot receive messages sent from a sender classified as secret. Not-trusted users cannot be in the To field in any secret message. Secret users cannot send messages of any kind on the not secure channel. There might be additional constraints we need to add (or remove in chase the ones above are inconsistent).

A few properties we want to hold.

1. A not-trusted user cannot receive any mail from a secret user.
2. No secure messages will ever appear on the OutNotSecure channel.
3. Not trusted users should never receive a secret message.
4. All non-secure messages will never be rejected.

You might be able to think of a few more.
Your Task
Define this system in Alloy and explore the properties to some reasonable level. If there are problems with the description or the properties (or both), please discuss it on the forum and we’ll try to come up with a consistent description.

Deliverables
I expect you to make sure the specification is (1) syntactically correct and (2) type checked. Also, check the properties of your model. Hand in the following

1. A printout of the specification.
2. Soft copy via email

Due Date
Thursday, October 12 in class.