CS 444/544 Spring 2011 Lab 3a: Policy

Due: Friday, 10 March 2011, at 11:59pm

50 points (Lab 3b will be worth another 50).

I've already assigned groups. This is a group assignment, everyone in the group will receive the same grade unless there is some otherwise unresolvable problem among the group members, in which case I reserve the right to assign separate grades. All group members should participate in all aspects of this lab, including the writeup. Your writeup should be sent to me in PDF format at my gmail account, jedcrandall@gmail.com. The writeup should be no more than four pages in length, including figures, with 1 inch margins and size 10 font. The writeup should be your own work, cutting and pasting even a single sentence from an existing information source will be considered cheating and the entire group may receive a zero in that case.

The purpose of this lab is to learn about policy and how formal policies can help us to instantiate systems that behave the way we expect them to with respect to access control. You are to design a policy for a mock scenario in which nonprofit organizations can submit network security forensics problems for students to work on. Keep in mind that you will probably be asked to implement your policy in SELinux for lab 3b, so don't make the policy so complicated that you can't implement it.

Mock scenario:

Suppose we're applying for funding from the federal government to set up a center where students can work on “hacking” problems that are related to a free and open Internet. For example, students might analyze network traces to look for evidence of Internet censorship or analyze web server log files to give a human rights organization some advice on how to prevent repeated distributed denial of service attacks. Any nonprofit organization can submit problems that they need someone with technical skills to work on, along with the necessary data, and specify access restrictions on the data.

Assume four general levels of trust that can be assigned to any person involved:

1. **PIs**, or Principal Investigators, are the most trusted. These are the faculty members who manage the grant. Faculty are all as pure as the driven snow, but some auditing functions would be nice so that if a PI goes to the dark side we can find out who did what.

2. **FTEs**, or Full Time Equivalents, are students who work full-time on the grant and are trusted with data necessary for them to work on whatever problem they're working on at the time. Again, auditing is important, and also note that “data necessary for them to work on whatever problem they're working on at the time” might imply discretionary access controls or a lattice structure or something to account for that, so think hard about how you're going to handle that.

3. **LTs**, or Lab Trash, are typically summer interns or work study students, or web admins, or
anybody who is given some small amount of trust but is not as trusted as an FTE. Note that the webadmin will need to somehow administer the website without having access to data that they're otherwise not allowed to access.

4. **UPs**, or unprivileged folks, are anyone else who has an account on the system but is not officially part of the project. This could be students in a class that one of the PIs is teaching or just anybody who's interested in helping out. Note that some nonprofit organizations might specify no access restrictions for their data, in which case UPs can work on that particular problem as a way to gain some experience and move up to becoming an LT or FTE.

Assume that all operations related to this project will happen on a single Linux system that supports SELinux (using virtual machines). When a nonprofit submits data through the web server that is hosted on this machine, it should automatically be marked so that only PIs can look at it. PIs need some way to declassify things, so that a PI can look at the submission and see that the nonprofit has said that it's okay to share the data openly, and then downgrade the data to UP. Whether or not they should do this in a separate role is something your group should discuss. In general, one of the first things you should discuss is what the different roles of each person at any of the four levels might be.

Are there any integrity concerns? Is it possible to combine a confidentiality policy with an integrity policy? You should consider hybrid models such as the Chinese wall model, too, but keep in mind that you will probably be asked to implement your policy for lab 3b. Or, alternatively, some other group may be asked to implement your policy, with the two groups sharing part of the final grade. So you will want to make sure that your policy is clear. I expect to see some mathematical rigor in the writeups to show exactly what you mean in the specification of your policy. I hope that you'll consider all aspects of policy that we discuss in class, but keep the policy you ultimately come up with as simple as possible. I'm the customer, so ask me lots of questions to make sure that your policy includes all the features and such that I need.

Some additional considerations:

- For some sensitive countries, it may be necessary to ensure that no students who are a citizen of that country can view certain data items about that country, or else they may violate laws back home. For example, a PI may want to mark a certain piece of Canadian Internet censorship data so that no Canadian students can view it.
- If it doesn't complicate the implementation too much, it would be nice if we could require multiple PIs to approve declassifying a data item.

Some resources that will help you:

- Chapters 1-7 of Bishop's book.
- Chapters 14 and 15 of Bishop's book.
- Chapter 16 in the Gray Hat Hacking book.
• http://www.ukfastblog.co.uk/2010/08/16/role-based-access-controls-in-enterprise-linux-6/