Homework 5

Due Date: Thursday, December 8, 2005 **Points**: 100

1. (*30 points*) A file system integrity checking program does not encrypt the signatures of the files it checks. What precautions must be taken to ensure the integrity of the database containing the signatures?
2. (*30 points*) A company called UserSnoop wants to determine where you browse on the World Wide Web. It contracts with a large number of web sites to place an image, one pixel big, on each page of those companies' sites. Please describe, in detail, how UserSnoop can generate a report of pages on those companies' web sites that you have visited by using cookies. In your answer, you *must* assume that the companies merely place the image on their web pages, and do not monitor your activities. Also, assume that your browser neither sends nor accepts third party cookies (that is, it only accepts and sends cookies that belong to the site to which you are connected).
3. (*40 points*) A company has a list of email addresses to which it wants to send sexually explicit spam. The state has a "do not email" list that consists of email addresses to which spammers may not send email. This includes children's email addresses. The company wants to respect the state's list, and so has decided it will not send email to addresses on that list. But the addresses on the state's list are to be confidential. There are two ways the state and the company can handle this situation.

   The company can send its list to the state, and the state can send back a set of "collisions," or names on both lists. But the company does not want to make its list available to any other organization (including the state) because the contents of the list may be leaked to its competitor. So it asks the state to provide a cryptographic hash for each name on the state's list. The company will then hash the names on its list, and strike any whose hash matches a hash on the state's list.

   a. Will this work? That is, will it allow the company to delete the names of people on the state's list without knowing the names are on the state's list?

   The second approach is for the company to send letters to each of the addresses on its mailing list, but route them all through a server that has access to the state's list. That server then simply declines to forward the latters addressed to email addresses on the state's list.

   b. Will this work? That is, will it prevent email from going to people on the state's list without any other organization knowing the email addresses on the company's list?

Extra Credit

4. (*25 points*) Referring to the situation in problem 3, either devise a method that allows the company to send emails to everyone on its list who is not on the state's "do not email" list, or show that it is impossible to devise such a method.