CS 591 Cybersecurity, HW2

Prof. Jared Saia, University of New Mexico

Due April 18th

1 Project Proposal

The deliverable for this homework will be a 3-5 page proposal for the class project. This project can be done in groups of 1-3 people. Working with at least one other person will likely increase the amount you are able to learn in the course of the project and your chances of success. I would like each project team to meet with me briefly during office hours or after class *before* turning in your project proposal. This will allow us to work together to make sure that you have a project proposal which is reasonably challenging but which you can complete in a timely manner. I will be much more excited about partial progress on a challenging problem than significant progress on an easy problem.

Following are some general project ideas.

1. Use a problem related to your own research. Security pops up in many areas of computer science. Come talk to me if you'd like possible pointers in this direction.

2. Find a problem that has been mentioned in the research literature. Do a citeseer(www.citeseer.org) or google scholar search on topics that interest you. "Future Work sections of papers you find can be good starting points for problems. Note however to turn these problems into good project proposals, you will almost certainly want to simplify the problems in some way (e.g. making the random oracle assumption, focusing on a special case)

3. Come talk to me. I have several problems that can be starting points for research projects.

2 Deliverables

Your project proposal should contain the following information.

1. An introduction stating the problem you want to solve in as much detail as possible. Your problem should ideally contain both a theoretical or analytical component and an empirical component. You can phrase the problem in terms of a question or hypothesis. Note: for the empirical component, I'm looking for something more detailed here than e.g. "I'm going to implement algorithm X". You should rather say *what* questions you hope to answer by doing experiments on algorithm X.

2. A related work section presenting the problem you want to solve in the context of past work. You should review past literature and find around 7 to 20 papers related to your problem. This section of your proposal should summarize these past results in the context of the new problem you are trying to solve. In particular, you should give details on how your project will build on past literature and, in addition, how you plan to solve a problem which has not previously been addressed. Note that you don't need to have a separate summary of every paper in your collection - it's ok to group papers together with respect to how they relate to your project.

3. Project design. This should give the details of how you plan to accomplish your project. This can contain both an empirical design and a theoretical design. The empirical design will give information on: what you will measure, what are the experimental conditions, what are your goals, what are your expectations, what software will be used, etc. The analytical or theoretical design will give information on: what you plan to prove, what mathematical tools you will use, what you expect your proof framework will look like, etc.