COS 433 — Term Project

Boaz Barak

September 20, 2005

1 Short Description

The project will be to take an existing or invented security application, suggested by you, and to write up a detailed security specification, a construction (algorithms only, no implementation), and prove that the construction meets the specification.

As an example for a security application, consider a toll-road billing mechanism such as the EZ-Pass system here in New Jersey. The system involves several parties and security concerns: the operators want to make sure they receive the money and that the transaction is as smooth as possible, the drivers want to make sure they are not overcharged, and that no one can impersonate them and charge tolls to their account. The drivers might also be concerned about their *privacy*, and want to ensure that no one but the operators can track their movements, and even the operator should get only the minimal amount of information necessary.

2 Phases and Timetable

Below is an outline of the project's phases and its outline. I will hand out a fuller description of the requirements for each phase as its due date approaches. As you can see, we'll have several drafts and iterations spread across the term, so hopefully your workload will be reasonable. The phases of the project will be as follows:

Form group Find a group of 1-3 students.

Initial proposal. Come up with an idea for such an application, and some rough ideas for the security requirements. Security comes up everywhere - try to think of ideas for useful applications that exist or should exist. You don't have to think about implementation details - imagine that you have at your disposal an unlimited supply of computing devices that cost a dime and are the size of a dime, and are as powerful as a general purpose computer, (i.e., are capable of running any polynomial time algorithm). Some examples for the types of secure applications you should consider are the toll-road system I mentioned above, a system that enables customers to print train or bus tickets at home, a smart national ID card that improves national security but does not infringe on the citizens' privacy, it can be a secure system to manage the contents of the department's tea-room refrigerator, using visual cryptography to print secret documents on a shared printer, or anything else you can think of.

You should send me an email by **Thursday September 29th, 2005 1:30pm** with your names, the project title, and a short description (2-6 paragraphs) of the project, and then schedule a meeting with me to discuss this further.

Specification draft. After some input from me, come up with security requirements for the application. I want you to think of the "dream version" of security: the maximum security for all parties you can think of, without taking into account implementation considerations. I do not want you to do any research to existing systems or implementations — feel free to "reinvent the wheel" (and maybe in a better way). Although I don't want you to think of implementations when defining security, you may mention some desired implementation characteristics.[1] It is possible that some of the security requirements conflict with one another, or with the desired implementation characteristics. This is fine.

After meeting with me and obtaining feedback, by **Thursday October 20, 2005 1:30pm** you should submit the first draft of the specification. This will be a typed document giving a full description of the application and its security requirement.

Specification document and construction suggestion. Polish and fix the specification document and come up with a construction for the application that meets at least some of your security requirements. By a construction I mean specifying polynomial-time algorithms (no need to actually implement).

After receiving feedback from me, by **Monday November 28, 2005 1:30pm** you should submit the final specification document, and a description of your suggested construction. (The specification document should be full and precise, the construction can still be rough and subject to change.). You may also add a list of questions/tasks you'd like to tackle in the final phase.

Final phase. The final phase will be for you to answer several questions about your project. This may include proving some properties of your construction, and also proving that compromises and tradeoffs you made were necessary (for example, proving that some desirable security properties are in fact impossible to obtain). In case you'd like to implement part of the project, and this is appropriate/possible for the particular application and construction, this may be part of this final phase.

I will provide you with feedback and a list of questions/tasks by December 15th. You will need to submit the final description of the construction, and your answers to the questions by **Friday, January 13th 2006 1:30pm**.

The project will be graded based on the entire process and the end result. There will be no grades for the individual phases.

[1] For example, in an EZ-Pass style system, a desirable implementation characteristic is that the car transmitter only uses read-only memory. Another desired characteristic can be that the interaction between the transmitter and the toll-booth is *non-interactive.* That is, the transmitter sends a single message to the booth.