COS 433 — Term Project — Specification Format

Boaz Barak

October 11, 2005

By **Thursday October 20, 2005 1:30pm** you should submit the first draft of the specification. The best way is to submit this by email to me (postscript, pdf or MS-word file) but you can also hand it to me in Thursday's class. This should be a roughly 2-5 pages typed document giving a full description of the application and its security requirement. The idea in this document is to be precise, but not overly verbose or formal. Excitement and informality is fine (even encouraged), as long as you still manage to accurately convey all the information.

The specification draft should contain the following items:

Title Title of the project, names and emails of the participants. Please also write down your status (grad/undergrad and major) and whether you plan to take the course for credit or audit it.

Summary Describe broadly the system and its main usability and security goals.

System description Describe (try to be precise) all the components of the system and how they are supposed to function and be used normally (when the system is not attacked). Write down what is the interface that each component presents to its users (by interface I mean describing in English the functionality a component provides — there's no need to use code or pseudocode). For example, in the EZ-pass system, does a transmitter present any information to the driver (e.g., beeps when it is charged) or not? Note that you are not committed to these choices and you may change such details later.

Entities Describe all the entities (e.g., all the people/groups that use the system). Include also "outside entities" that do not have legitimate access for the system. For example, in an EZ-pass system the entities can be the drivers, the operator, law enforcement, people trying to find out information about the drivers, people trying to ride for free etc. For each entity describe its desires from the system (e.g., drivers want to be charged only for what they used, want their privacy uncompromised etc.., operator want to gets its money). Try to be as precise as possible (for example, you should be more explicit about the drivers' concern for privacy than just saying they want their privacy uncompromised).

Possible attack scenarios. Write down all possible attack scenarios that you envision. An attack scenario describes a setting where a party with illegitimate concerns can get access to some of the resources of the system. For example, in the EZ-pass system an attacker may purchase several copies of the transmitters to study them, and perhaps may also place a listening post near the entrance to the toll road. I call this an attack scenario and not an attack because **(1)** we do not specify what the adversary actually does with this access, only the mode of access and **(2)** the security of the system will ensure that the adversary can not use these scenarios to launch a successful attack.

Security goals. Write down security goals for the system. For each goal give both a short name (e.g., a couple of words) and a longer description. While you need not use mathematical notation (unless it simplifies and clarifies), you should be explicit and accurate. Try to phrase security goals in *positive* rather than *negative* terms, if possible. For example, in a secure communication channel, instead of saying that a goal is that messages are not tampered with (a negative formulation), we can say that if a receiver validates a message m then that message was indeed sent by the sender at some previous time (a positive formulation).

Explain how your security goals are related to the possible attack scenarios. If you already suspect that some of the goals are simply unachievable under some attacks then say so (you may change your mind later) and write down in addition also relaxed/weaker security goals that you believe are achievable.

Plan Write your preference for how to proceed with the project. If it has several parts, what is the part you find most interesting and want to focus on (please say also why). If you already have some ides about the constructions, you may write them here. If there are questions in cryptography that arise out of this project, and you are interested in knowing the answer or perhaps pursuing it as part of the project, please say so.