Assignment 3: Protocol Design and Analysis

1 Problem

You are to write a design document for a "secure" version of the DUP protocol. DUP is a system for distributed stream computations. You can find details of the existing DUP protocol as well as a paper describing the system at `http://dupsystem.org/`. Your design document should specify which security properties your protocol achieves. The document should also provide an analysis detailing how these security properties are achieved. Include a discussion of the mayhem different kinds of adversaries (Eve, Mallory) could cause in your system.

Detail the protocol for the three types of message exchanges between `dup` and `dupd` as well as the exchanges between different `dupd`s. Your security protocol must be an extension of the existing DUP protocol (communicate the same information between the same parties). You are free to add the use of additional cryptographic elements (hash, encrypt, sign, random nounce) as you see fit.

Detail messages for determining members currently participating in the chat and sending messages to individual members or the entire group in the same style as used in the textbook and/or the existing DUP protocol specification. In addition to specifying the protocol, your report should also specify how the various components of the system should act on the various security features that you introduce (including handling of malformed requests).

It is up to you to decide which security properties your protocol is supposed to provide. You will be graded on correctness (of the design), quality of the security analysis, simplicity of the design, scope of the chosen security properties and protocol efficiency.

Suggested security properties include (in no particular order):

- Access control
- Availability / DoS protections
- Authenticity
- Consistency

- Confidentiality
- Integrity

Note that you should define precisely what the meaning of these security properties is in the context of your protocol.

2 Submission

You must submit the design and analysis in LaTeX format to your subversion repository to the directory `courses/comp3704/s2009/$USER/p3/`. Do not include generated files.

- `protocol.tex`
- `Makefile`

You must check that the submitted LaTeX file compiles by invoking `make`, producing a file `protocol.pdf` (use `pdflatex` in your makefile).