Modelling and Analysis of Security Protocols:
   Homework 2

Handed out on: 12/10/2007       Return in class & by email: 26/10/07

This assignment is more open ended than the last one. It will be more work but it is also much more similar to the kind of work you may be asked to do in a real job. Good Luck.

1 BAN logic

Analyse a protocol of your choice using BAN logic.

15 marks

Pick any protocol you like and analyse it using BAN logic. Carefully consider which protocol you choose to analyse, you will receive low marks for choosing to analyse a protocol that has already been analysed in BAN logic or that is very simple, but if you choose a protocol that is too complicated the analysis may be very hard or even impossible.

You may use the Jape tool or pencil and paper to do the analysis. If you use Jape, please e-mail me your files and give me a print out of your proofs. To get full marks you must convince me that you understand BAN logic and that you can effectively use it to analyse protocols you might come across in the future.

2 ProVerif

Analyse the protocol you designed for Assignment 1 using ProVerif.

20 marks

You have not yet received your marks for Question 3 of Assignment 1. Use ProVerif to analyse the protocol you designed and look for faults. If there are faults, you will have already lost marks in Assignment 1, but if you find the faults using ProVerif, you can win back half the marks you lost, i.e., finding an error in your own protocol is a good thing. Consider the case where the player and the server are honest and the host is the attacker. Explain your analysis and e-mail me the ProVerif files.