You can either do this project on your own or with a partner. If you decide to work with a partner, please send me an e-mail by 21 March to let me know that you are working together. Your submission should include a zip archive with your ProVerif sources and your project report. Please call your zip archive <yournames>.zip and e-mail it to me by Monday, May 12.

This assignment is a mini project, rather than an exercise. Consequently, you have more freedom and choices how to carry out your task than in the previous assignments. Your task is to analyze the TLS handshake protocol with ProVerif.

Start by reading Sections 1 and 2 of Paulson’s article “Inductive Analysis of the Internet Protocol TLS” [Pan99]. Section 2 describes the TLS handshake protocol at a high level, omitting many details of the official TLS specification. You can base your analysis on this description. If you need further information about TLS, use the official protocol specification RFC 4346 [DR06] for reference.

I recommend to first carefully read and understand the protocol and sketch it as an informal narration, using our usual notation. Then think about what its security goals are, and express them informally in terms of correspondence and secrecy assertions. Then formalize the protocol in ProVerif and query for the security goals. You may want to start with a simple version of the protocol (e.g., no optional messages, no session resumption, just two agents, no internal threats, etc.), and then gradually extend your model. It is not strictly required that you model all features that are modeled by Paulson (e.g., you could omit session resumption if that turns out problematic), but the more features you model the better.

In addition to your ProVerif sources, please also submit a short project report. The report should include the following:

- Your protocol model as an informal narration.
- A short discussion of the security goals that you verified and how you modeled them.
- A short discussion of the attacker model that you used. (External threats? Internal threats?).
- A short discussion of the system you model. (Do you model parallel session? Do you model a finite or an arbitrary number of agents? Do you allow agents in multiple roles?)
- A discussion of the limitations of your model and analysis.
- If you find attacks, present them as informal narrations. Discuss the attacks. (Are they benign? If not, how could they be fixed?)
• If some of your queries fail inconclusively (e.g., by ProVerif not terminating or answering inconclusively), detail these queries. In such cases, did you manage to analyze weaker queries conclusively?

• If you faced particular technical modeling problems and got stuck or found nice solutions, describe these.

• If there are other things that you want to bring to my attention or that you want to discuss, include them in your report.

References
