DTU Informatics 02239 Data Security
Protocol Security Lab

Hound-out: September 26, 2018
Hand-in: October 12, 2018

Group hand-in is admitted, but **maximum 3 students** per group.
Submit via campusnet

The lab exercises use the protocol analyzer OFMC from Campusnet. The distribution includes executables for Windows and Mac. For compiling the sources yourself, you need the Glasgow Haskell Compiler

`http://hackage.haskell.org/platform/`

For the exercises please use OFMC with the following command line:[1]

`ofmc --numSess 2` *filename*

You can test OFMC on the lecture example `nspk.AnB` in `examples/cj/6.7...`.

Exercise 1: H.530

1. Consider the H.530 example in `examples/classic/h530.AnB`. Try to describe the protocol in your own words—what does it try to achieve, how does it work?

2. Analyze H.530 with OFMC and explain the attack: what does the intruder do, what went wrong? Why does `h530-fix.AnB` fix the problem?

3. Note that the party `s` is a fixed *honest* (*trustworthy*) server. Let us replace `s` by `S`, i.e., a normal role that can be instantiated by the intruder. Why does the protocol have an attack then?

[1] This bounds the state space to two sessions (i.e., each role can be instantiated by at most 2 participants).

Exercise 2: AMP Consider the example `AMP.AnB` on Campusnet.

1. Describe and explain the protocol in the following regards:
   - What security relationship do the parties have initially, according to the initial knowledge?
   - What new security relationship does the protocol (try to) establish?
   - How does the protocol (try to) achieve this?
2. Analyze AMP with OFMC and explain the attack: what does the intruder do, what went wrong?
3. Suggest a fix for the protocol and verify the fixed version for OFMC (again with 2 sessions). Important: the fix must not change the initial knowledge nor modify the goals.
4. Note that the party `s` is a fixed *honest* (*trustworthy*) server. Let us replace `s` by `S`, i.e., a normal role that can be instantiated by the intruder.
   - Why does even the fixed protocol have an attack?
   - Is this new version fixable, i.e., can there be *any* protocol with the same initial knowledge and the same goals that is secure?