Project: Efficient compromise analysis of the Clark-Jacob library of protocols

Motivation

Humans are notoriously bad at developing and analyzing security protocols. Recent developments at ETH in automatic analysis of security protocols have enabled new types of analysis. For example, we now have tool support to automatically analyze new properties of protocols such as Perfect Forward Secrecy, or resilience against Key Compromise Impersonation.

The Clark-Jacob library of protocols, well-known set of security protocols, has never been analyzed with respect to these more advanced properties. To advance the state-of-the-art, it would be beneficial to analyze these protocols using the new tool.

However, the new analysis types are computationally expensive and are currently executed sequentially on a single workstation, making it very hard to analyze the set of protocols. The project aims to perform this analysis, by exploiting the parallel BRUTUS cluster at ETH.

Project details

The project consists of two phases. In the first phase, the student is required to adapt the Scyther tool chain setup to be parallelized on the BRUTUS cluster of ETH. This will enable the second step, in which the student performs a compromise analysis of the library of protocols.

Prerequisites

The student should have succesfully completed the course "Information Security".

It is helpful, but not required, to have some experience with the Python language; the current tool is written in C but Python wrappers exist.

Supervision

Cas Cremers