Security Protocols in Perfect Developer

A dissertation submitted to University of Manchester for the degree of MSc in the Faculty of School of Computer Science

2013

Nan Zheng

School of Computer Science
Abstract

This project is a sequential process to solve an open problem verifying security protocols in *perfect developer* [2]. The aim of the project is to create a model of security protocols in a new tool-*perfect developer (PD)*. Some experience of using PD with its automated reasoning system to verify Security Protocol can be gained through the project. The project result is a critical evaluation of the verification results.

First of all, some clues can be found through searching key words like *Perfect Developer*, security protocol, and protocol verification. The literature review clarifies these key words as well as some of the relevant achievements of the protocol modelling and verification. The object of the project is security protocols so that in one instance the Needham-Schroeder symmetric-key protocol (NSP) is used to provide a brief picture for us. In addition, the NSP performs as a chain throughout the project as it is used as an example in sections of protocol analysis, modelling, implementation and verification too.

The creative part of the project is to create a protocol model for verification in PD. Previous achievements of protocol modelling can provide some clues. One instance of the protocol verification model CSP approach [6] is used to explain what a protocol verification model is.

A lot of effort is assigned to clarifying PD as a new tool for protocol verification with its automated verifying system. PD is a tool for specifying and modelling the protocol verification system (e.g. protocol model in PD), providing formal proofs as to whether protocol properties can be achieved. Optionally, code can be generated from the model, in a choice of languages like Java.

To achieve the final goal of the project, it goes through a sequential process including protocol analysis, modelling, verifying in PD, and critical evaluation of the verification results.

The literature review provides a guide for the project. It is followed by designing, implementation, and verifying protocols in PD. The creative part of the project is to
design a protocol model in PD. In other words, the model performs like a framework specifying and implementing protocols in PD.

The conclusion of the protocol includes critical evaluation of the verification results is logically correct even though some errors. Some experience of using the new tool PD can be gained through the project. It is a chance to learn the perfect language systemically and use it proficiently. Lastly, some improvement of the protocol model, implementation in PD and etc. can be done using PD for protocol verification as this is just the start.