An investigation of formal verification of authentication protocols with proof score and a new case study

1910186 Shuho FUJII

With the rapid spread and development of the Internet, security protocols that guarantee safe and secure communication on the Internet are becoming more and more popular. Although these security protocols have been carefully designed by security experts, it was not uncommon for security attacks such as interception, tampering and impersonation to happen, leading to lots of serious damages. Ensuring the reliability of security protocols is thus absolutely important. Many approaches have been proposed against the unexpected flaws in these protocols. In formal method, some techniques for formally verifying the correctness of security protocols have been extensively studied.

This research focuses on formal verification of the correctness of authentication protocols and We survey case studies conducted in the past as well as to conduct new case studies. Authentication is the process of verifying the identity of a person, an object, a computer, a program, etc. It is an indispensable technology for preventing unauthorized operations in network systems (also known as access control). Protocols are communication conventions that are necessary to communicate with each other. Thus, an authentication protocol is a communication convention to achieve authentication. Computers, printers, and programs are used and participated in by an unspecified number of entities, and only encoded information is exchanged. Therefore, there is a high possibility of eavesdropping, falsification, and impersonation of communication. There- fore, authentication protocols are intended to realize authentication for secure communication in such insecure communication channels.

This research focuses on two case studies of authentication protocols are presented with the Identify-Friend-or-Foe-System protocol (IFF protocol or just IFF) and the Needham-Schroeder-Lowe Public-Key protocol (NSLPK protocol or just NSLPK). NSLPK can be regarded as an advanced authentication protocol of IFF. We study the specification of two protocols in CafeOBJ, which is a formal specification language, and understand the "proof scores" to prove that they enjoy some desired properties. We present two more ways of verification that IFF enjoys some properties by using CafeInMaude Proof Assistant (CiMPA), and CafeInMaude Proof Generator (CiMPG). By achieving the objectives of this research, we will be able to acquire techniques to mitigate the number of authentication protocol failures, which can contribute to safer and more secure shopping on e-commerce sites and safer and more secure communication on the Internet.

Keywords : CafeOBJ, CiMPG, CiMPA, proof score, algebraic specification language, authentication protocol