Abstract

In this paper we give a brief description of the NRL Protocol Analysis Tool, and contrast its approach with other approaches discussed in this panel.

Key distribution and key management protocols often contain security flaws that are vulnerable to exploitation by a hostile intruder or a dishonest user of a network. An intruder with the ability to read all message traffic, insert, destroy and alter messages, and perform cryptographic operations may take advantage of protocol flaws to find out secret information or impersonate honest users of the network. Moreover, since intruder attacks are usually counterintuitive, it is not easy to identify such flaws simply by careful examination of the protocol. Thus some use of formal methods is desirable.

A number of approaches have been followed. One, which is described by Yacov Yacobi in this panel, is to develop a very strong model of security and construct protocols that satisfy it. This has the possible disadvantage of ruling out many secure protocols, but one has the assurance that the protocols satisfying the model are secure given certain assumptions. Another is to develop automated means for proving the security of protocols that are specified in terms of rules that govern the communication between protocols participants; as is shown by Jon Millen in his position paper, this approach has certain complexity-theoretic limitations. Another approach is that taken by Burrows, Abadi, and Needham; that is, to abstract certain properties away from the protocol and to reason about them formally. This approach has been shown to be very useful in pointing out flaws in protocols, but one has somewhat less confidence in security proofs that use these techniques, since the abstraction does not provide a complete description of security-relevant features the protocol, nor is any pretence made that it does.

In the development of the NRL Protocol Analysis Tool, we have taken another approach. We attempt to provide mechanical assistance in the analysis of protocols that are specified in terms of rules that govern the communication between protocol participants; however, we do not attempt to automate the process completely. Instead, the NRL Protocol Analysis Tool is an interactive system that, given a description of a state by a protocol analyst, gives a complete description of all states that can immediately precede it. It also includes several features that assist an analyst in proving a state is unreachable. The analyzer can use the tool to show that certain sequences of preceding states form an infinite loop that never involves an initial state, and thus that each member of the state is unreachable. He can also request the tool not to display descriptions of states that have been shown to be unreachable. Finally, in attempting to find all states that immediately precede a given state, he can give the analysis tool only a partial description of that state. This has the effect of limiting the search space.

The NRL Protocol Analysis Tool was developed in order to assist in security proofs for protocols. However, it has also proved to be useful in pointing out previously undiscovered flaws in already published protocols. In one of these, the tool led the analyzer directly to the flaw in the course of an attempted proof; in the other, the flaw was found in an effort to formalize the protocol so that it could be analyzed using the tool. We have also successfully completed proofs of security properties of several protocols using the Protocol Analysis Tool.

The success that we have had using the Protocol Analysis Tool suggests, that in many cases a hybrid approach, relying upon human intuition when possible, and providing mechanical assistance when necessary, will provide the most practical advantage.