Formal verification and its application in the security of information systems

František Mazura

xmazur06@stud.fit.vutbr.cz

Abstract

This presentation discusses the possibilities of using formal verification of security and its limitations that occur in real use.

Formal verification can be used to answer the most important question in security - whether this particular system is safe. The advantage of solving this problem with formal verification is that ideally, formal verification gives us a yes or no answer. The disadvantage of this answer is that if the answer is in the affirmative, this is a bad answer for deploying the system. Using this approach to prove that the system is safe, we must always consider the environment and the implementation problem itself. So we have to take into account that in the formal verification we can not include the environment and also we are limited in verifying the source code itself, which usually can not be verified directly, but must be transformed into a form in which this verification can already be made. It is always necessary to realize how formal verification has its limits and correctly interpret the answer given to us by formal verification.