Formal Analysis of Cryptographic Procotols

Karel Koranda
ikoranda@fit.vutbr.cz

Department of Intelligent Systems
Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic

Abstract

One of the fields of my research is cryptography, since it is one of the headstones of computer security. Cryptography which consists of either cryptology or cryptoanalysis is also connected to formal languages theory even if this connection is not always noted. Even more then in formal languages it has roots in complexity theory - almost all cryptographic algorithms are based on different computation complexity under different circumstances, e.g. owner of encryption key can derivate plaintext for received ciphertext with the use of encryption algorithm in polynomial time, but it has to be intractable for the potential codebreaker to derivate this plaintext without knowing the key.

It is known that computer security is becoming more and more essential with the unstoppable growth of non-professional usage of computer systems and enormous expansion of the internet network. Since most of the traffic is transferred over unsecured channels and this traffic can contain sensitive data, it is the aim of study and research how to secure transferred data from being either stolen or corrupted. There are also other aspects, one of which is the fact that computer security is also underestimated by professionals who are creating information systems. Let us assume that security flaws are completely unintentional, but the impact of exploitation of these flaws could have severe aftermath for the exploited system, the company using it and in some cases even to the society. In these cases also intrusion detection and prevention systems are useful for dealing with unknown or untreated security flaws of operating and information systems.

As we can see, the goal of computer security is mainly to secure our private data and to prevent attackers to get either data or unauthorized access to an insecure system. However, security systems such as firewalls are also created by humans and can contain the same security flaws, which is, of course, in this case the most undesirable fact. And here among others comes the need of using formal analysis and verification methods for proving the correctness of proposed and designed security systems, mechanisms, protocols and algorithms and their ability to provide the goals we seek.

In the first part of my lecture we will focus on cryptografic protocols used for solving problems of communication over unsecured channel between two users without participation of any third party. We shall present some existing languages for the description of such protocols. Note that it is possible that those users can communicate for the first time and it is essential to establish a private conversation between them even if they do not know each other - we must count with potential pretender being on the other side. We will see that it is possible to solve such a problem with the use of public-key cryptography. The second part of lecture will aim on formal analysis and verification of the above mentioned cryptographic protocols. The tools for automated approach to do these analyses are mainly based on model checking, SAT solving and tree automata. Some of these and their possible application will be also explained as a part of the lecture.