Attack Goal Generation Using Description Logic-based Knowledge Representation

Taufiq Rochaeli and Claudia Eckert
Research Group IT-Security
Technical University of Darmstadt
Darmstadt, Germany
{rochaeli,eckert}@sec.informatik.tu-darmstadt.de

An attacker threats the computer network security by exploiting known vulnerabilities of communication mechanisms. Thus, a security threat assessment on the computer network using attack goal generation tool is required to assess the vulnerabilities and to search the possible attack goals. Therefore, the appropriate countermeasures against the attacks could be determined.

We use a description-logic based knowledge representation system to store the computer network model and its vulnerabilities. The T-Box defines concepts and roles of the reference model of the computer network system. Firstly, we define CommunicationSession, which represents a concept of communication session between the two subjects. These subjects require a communication medium / service to perform data transfer. Therefore, we introduce CommunicationService, which represents a concept of communication medium / service. We also describe other concepts and roles to represent dependencies between the reference model and the communication mechanisms (communication protocol and/or cryptographic function), which have known vulnerabilities. Lastly, the A-Box contains instances of the model, which reflect the actual network and its vulnerabilities.

We choose the latest RACER system to store our knowledge representation and perform the attack goal generation using the Racer Query Language (RQL).

An exploited vulnerability can cause violation of one or more security goals in a communication session. This vulnerability could be a flawed mechanism design or a flawed mechanism implementation. These security goals are common in a communication session: *confidentiality, integrity* and *authenticity*. As an example, we consider the confidentiality goal: a communication session satisfies the confidentiality goal if and only if, an attacker can not read/gain the sensitive information, which is transferred between the sender and the receiver.

To generate the attack goal which violates the confidentiality goal, a RQL query is constructed to search for all communication session carrying the sensitive information and also having any vulnerability, which can cause the violation of confidentiality goal.