International Journal of Distributed Sensor Networks, 5: 14, 2009

ISSN: 1550-1329 print / 1550-1477 online
DOI: 10.1080/15501320802505986

Taylor & Francis
Taylor & Francis Group

Automatic Verification for Secrecy of Cryptographic Protocols in First-Order Logic

JIHONG HAN, ZHIYONG ZHOU, and YADI WANG

Zhengzhou Information Science and Technology Institute, Henan, China

In this article, we present a new formal approach for specification and automatic verification of cryptographic protocols. First, we use the first-order theory to formalize cryptographic protocols and intruders. Assuming that messages transmitted by each principal can be received by the intruder, and messages received by each principal can be known by the intruder, we test the security of cryptographic protocols at the standpoint of the intruder. The protocol representation includes three parts: initial knowledge of the intruder, message exchange of the protocol itself, and computation abilities of the intruder. After defining the term and its typeset, we give a first-order frame to formalizing the protocol based on roles, using axioms to depict the communicating actions of each role. The predicate corresponding to the role's message receiving can be affiliated to the axiom by logical connective $\wedge$*, and the predicate corresponding to the role's message transmitting can be the conclusion of the implication relation. The universal quantification* $\forall$ *is used to eliminate the limitation for protocol runs, and existential quantification* $\exists$ *is used to denote generating of the key or the nonce, and through renaming and consistency check, ensure the refreshness and boundlessness of the new value. In order to implement the automatic verification, we propose a normal approach to transform the axioms into Horn clauses. Following the Dolev-Yao Model, the computation abilities of the intruder are modeled in Horn clauses too. We adopt the deductive reasoning method to verify the secrecy property of cryptographic protocols. The secrecy property is considered as a goal, and based on a deductive algorithm we can check whether the goal can be inferred from the known rules. The known rules form a rule base B containing the Horn clauses of protocol description and the intruder's abilities and initial knowledge. If the goal can be inferred from the base, the sequence of rules applied will lead to the description of an attack scenario. This approach is fully automatic and terminable. The main contributions of the paper are: a general framework of formalizing cryptographic protocol and abilities of the intruder, a practical solving algorithm based on automatic reasoning, and a simple method to find the attack scenarios.*

Keywords Cryptographic protocol; First-order logic; Automatic verification; Secrecy; Attack scenario

Address correspondence to Jihong Han, Zhengzhou Information Science and Technology Institute, Henan, 450004, China. E-mail: hnhanjh@yahoo.com