Formalization of security protocol in CafeOBJ

Atsushi Kato (210020)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 13, 2004

Keywords: Security protocol, Otway-Rees Protocol, Observational transition system(OTS),CafeOBJ.

1 Introduction

The purpose of our research is to describe and verify a specification of security protocol formally.

In recent years, with the rapid spread and development of the broadband network technologies, the importance of network security is increasing. A security protocol is a communication protocol that encrypts and decrypts a message for online transmission. It generally provides authentication, and is being used for the electronic commerce, the electronic election and so on.

However, safe communication cannot be performed when a protocol has a defect, even if it uses a powerful cipher. It is important to devise the protocol which guarantees safe communication. But it is difficult to discover a defect of protocol by intuition of man or through experiments.

Formal method may be suited for such problems. With formal method, we can formally specify a target protocol and verify its safety, that is, mathematically there exists no defectin the protocol. Since some problem in a well-known protocol was found with formal method, it is expected to be useful for analyzing security protocols.

2 Otway-Rees authentication protocol

The Otway-Rees protocol is a server-based protocol providing authenticated key transport. The purpose of the Otway-Rees protocol is to mutually authenticate two principals and to distribute a shared-key generated by the server. This protocol is one of the nonce-based protocols. A nonce is a fresh value created for the current run of a protocol and whose value has not been seen in previous runs. The server to provide a shared-key, called a certificate authority, is assumed to be reliable. Since we focus on the reliability of a protocol, we also assume that an encrypted message cannot be decoded without the shared-key.

3 Observational Transition System

We use Observational Transition System(OTS) to formalize the Otway-Rees protocol. OTS consists of the following three sets :

- $\mathcal{O}$: A set of observations
- $\mathcal{I}$: A set of initial conditions
- $\mathcal{T}$: A set of conditional transition rules

In OTS, a state of an object system cannot be treated directly. It can be observed only by observations. It can be changed only by transition rules. The state changes by transition rule are expressed by change of observation values.

An OTS is described in CafeOBJ. CafeOBJ describes behavior of a system using an equation. The execution of CafeOBJ is based on a rewriting machine in which an equation is regarded as a rewriting rule from the left to the right. The simulation and verification of a system become possible by this execution.

4 Modeling

First we give the data types for principals, a certificate authority, shared-keys, cryptograms, messages, and network. An intruder is given as a constant of both principal and certificate authority. An intruder can collect nonces, cryptograms and shared-keys if message including unencrypted ones has been sent on the network.

In our OTS model, the initial state is a network where no message has been sent. Observations return the all of nonces used by the session, messages on the network, and shared-keys distributed by the certificate authority. Four transition rules which follow a protocol are declared. Moreover, twelve transition rules for messages which an intruder forges are also declared.

5 Verification

Verification of a protocol is done according to the following procedures. First, describe a property to be verified by CafeOBJ. Next, describe a proof score to show the property. Then, execute the proof score by CafeOBJ system to verify that each parts of the proof score is correct. For example, we verify the property that "Intruder cannot acquire the shared-key between principal different from intruder and another principal different from intruder."

Verification is done by the induction on the number of applications of the transition rules.

Base step

Prove that the property holds for the initial state.

Inductive step

Prove that when assuming the property holds for a state, it holds for all states that are obtained by applying all transition rules.

In the inductive step, state space is divided into many parts. Terms are reduced at each stage of verification. If all reduction return the expected values, it means that proof was successful. Otherwise, a state should be divided further or a lemma is needed.

In this research, we needed three lemmas to verify the above property.

6 Conclusion

We modeled security protocol using OTS, and verified it has some property. In verification, case analysis and to find lemmas can be almost done based on the effective condition of each transition rule. However, it depends on the experience of a person.

In this research, verification about the secrecy of Otway-Rees authentication protocol was performed. As a result, we checked that intruder could not acquire shared-key unjustly. However, we have not proved safety yet completely. The secrecy which is the necessary condition of safety was verified. Therefore, in order to check that a protocol is safe completely, we have to check that a message is transmitted certainly.