505/E1

Formal verification of PAY HERE SMS protocol using SPIN

M D V C Samasekera
University of Colombo School of Computing, Colombo 07

Present Address/es:
OPRO Lanka (Pvt) Ltd, World Trade Center, Echelon Square, Colombo 01

The PAY HERE is a Short Message Service (SMS) protocol offered by Dialog Telekom PLC. Dialog Telekom subscribers who have Hongkong and Shanghai Banking Corporation Limited (HSBC) credit cards, can use this protocol to top-up their mobile phones. In the PAY HERE system, a subscriber has to first register for this service through HSBC. On successful registration for the PAY HERE service the subscriber will receive a SMS from Dialog Telecom. Now the subscriber can top-up his mobile phone by sending a SMS with his mobile phone number and the top-up amount. Then Dialog Telecom will debit the said amount from subscriber's credit card and send a SMS to the subscriber confirming the amount has been top-up to subscriber's mobile phone account.

The research goal was to find out whether the PAY HERE SMS protocol was reliable and if not, propose modifications to the protocol. For this purpose it was checked whether money atomicity, goods atomicity and validated receipt properties were exhibited by the protocol. The model checking tool, Simple Promela Interpreter (SPIN) was used to model the PAY HERE protocol. The behavior of the subscriber and Dialog Telecom were modeled as Promela processes. The money atomicity, goods atomicity and validated receipt properties were modeled as Linear Temporal Logic (LTL) formulae. When SPIN tool was run in verification mode against LTL formulae, it showed that the PAY HERE protocol exhibits both money atomicity and goods atomicity properties. But it was found out that validated receipt property was violated by the PAY HERE protocol.

The validated receipt property violation was eliminated by introducing a new SMS message for the subscriber, which gets a reference number for the top-up transaction. This reference number is used in the subsequent top-up SMS request send by the subscriber to Dialog Telecom. The said modifications were modeled and the SPIN tool was used to formally check that the modified PAY HERE protocol has validated receipt properties without compromising money atomicity and goods atomicity properties.

*virajsam@sltnet.lk Tel: 011-2346664