World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Formal Development of Electronic Identity Card System Using Event-B

Authors : Tomokazu Nagata, Jawid Ahmad Baktash

Abstract : The goal of this paper is to explore the use of formal methods for Electronic Identity Card System. Nowadays, one of the core research directions in a constantly growing distributed environment is the improvement of the communication process. The responsibility for proper verification becomes crucial. Formal methods can play an essential role in the development and testing of systems. The thesis presents two different methodologies for assessing correctness. Our first approach employs abstract interpretation techniques for creating a trace based model for Electronic Identity Card System. The model was used for building a semi decidable procedure for verifying the system model. We also developed the code for the eID System and can cover three parts login to system sending of Acknowledgment from user side, receiving of all information from server side and log out from system. The new concepts of impasse and spawned sessions that we introduced led our research to original statements about the intruder's knowledge and eID system coding with respect to secrecy. Furthermore, we demonstrated that there is a bound on the number of sessions needed for the analysis of System.Electronic identity (eID) cards promise to supply a universal, nation-wide mechanism for user authentication. Most European countries have started to deploy eID for government and private sector applications. Are government-issued electronic ID cards the proper way to authenticate users of online services? We use the eID project as a showcase to discuss eID from an application perspective. The new eID card has interesting design features, it is contact-less, it aims to protect people's privacy to the extent possible, and it supports cryptographically strong mutual authentication between users and services. Privacy features include support for pseudonymous authentication and per service controlled access to individual data items. The article discusses key concepts, the eID infrastructure, observed and expected problems, and open questions. The core technology seems ready for prime time and government projects deploy it to the masses. But application issues may hamper eID adoption for online applications.

Keywords : eID, event-B, Pro-B, formal method, message passing
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020