Improving Privacy of OpenID Cloud Identity Management Framework: Formal Analysis, Verification of Protocol

Abstract

Cloud computing is a new trend of computing paradigm that provides a set of scalable resources on demand. However, it also being a target of cyber attacks and creates risk for data privacy and protection. An Identity Management System (IDM) supports the management of multiple digital identities for authentication and authorization. The various identity management frameworks that help making Cloud environment more secure. OpenID 2.0 is a user-centric Web single sign-on protocol with over one billion OpenID-enabled user accounts, and thousands of supporting websites. The security of the protocol is critical.

In OpenID Identity Management Framework, User Privacy is the issue. In this paper we had introduced the results of a systematic analysis of the OpenID authentication protocol using scyther tool. Our formal analysis reveals that the protocol does not guarantee the authenticity and integrity of the authentication request, and it lacks bindings among the protocol messages and the browser. We provide a simple and scalable defense mechanism for service providers to ensure the authenticity and integrity of the protocol messages.
Improving Privacy of OpenID Cloud Identity Management Framework: Formal Analysis, Verification of Protocol

References


Index Terms

Computer Science  Information Sciences

Keywords

Single Sign-on, OpenID, Authentication, Protocol Analysis