Abstract

A Single Sign–on is a new authentication mechanism for user to use multiple services provided by service provider in distributed computer network. It is a one type of application in that allows users to log in once and access to multiple independent applications without being asked to log in again at every application. It enables a legal user with a single credential to be authenticated by multiple service providers in distributed computer networks. This scheme has security flaws. Service provider is fail to credential privacy and authentication. There is two types of impersonation attacks. First attack is credential recovery attack and impersonation. In this attack the attacker act as harm full service provider, who has successfully communicated with a legal user twice to get the identity of a legal user. In another attack the attacker use the services impersonating any legal user or a nonexistent user without credentials. In this we analyze those security flaws & propose solution for those flaws. We have to recover these two types of attacks.

References

- "Security Analysis of A Single Sign-On Mechanism for Distributed Computer..."

- "Research on the solution of PKI interoperability based on validation authority," Yongli Ma; Beijing GFA E-commerce Security CA CO.; Ltd Beijing, China June 2011.
- "A generic construction of dynamic single sign-on with strong security," J. Han, Y. Mu, W. Susilo, and J. Yan, SECURECOMM – 2010.

- "A generic construction of dynamic single sign-on with strong security," J. Han, Y. Mu, W. Susilo, and J. Yan, secure pro communication spinger 2010.

- "Prof M. T. Savaliya Advance java technology dream tech publication.
- Single sign-on solution for mysea services by Sonia Bu September 2005

**Index Terms**

Computer Science

Distributed Systems
Keywords
  Credential  Impersonating  single sign on.