西安电子科技大学学报 2006 33 (5): 792-796 ISSN: 1001-2400 CN: 61-1076/TN

基于令牌的单点登录协议及其形式化分析

申婷,李晖,于明zhe

西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071

收稿日期 修回日期 网络版发布日期 2006-11-28 接受日期

摘要 提出一种新的适用于分布式网络的单点登录协议，利用令牌将身份认证和服务授权结合起来由一个验证服务器实现，授权校验的同时进行密钥分配，实现了用户和应用服务器的双向认证．令牌使用户只需在登录网络时进行一次身份认证即可接入各应用服务器，从而提高了网络认证效率，同时使验证服务器不需要保存用户的状态，有效提高验证服务器的性能．采用BAN逻辑对该协议进行形式化分析表明，协议达到了认证和密钥分配的目标，具有较强的安全性．

关键词 单点登录 令牌 BAN逻辑

分类号 TP393.08

Token-based single sign-on protocol and its formal analysis

SHEN Ting,LI Hui,YU Ming-zhe

Ministry of Edu. Key Lab. of Computer Network and Information Security, Xidian Univ., Xi′an 710071， China

Abstract

A new single sign-on protocol used for the distributed network is proposed to achieve double-way authentication between user application servers. With a service token, identity authentication and service authorization are implemented by an authentication server, and the key is saved in the token which can be used in the verification process. The token not only makes the user that has been authenticated when it enters the network communicate with any application server, and improves the authentication efficiency of the whole network, but also makes the authentication server unnecessarily save the sate of users, and promotes authentication server's performance. Using the BNA logic, the objective and the security of this protocol are proved by the formal analytical process.

Key words single sign-on token BAN logic

DOI:

通讯作者