计算机应用 2006 26 (05): 1061-1063 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

XML文档的加密访问控制与传输

孟健, 曹立明, 王小平, 姚亮

同济大学电子与信息工程学院计算机系

收稿日期 2005-11-4 修回日期 网络版发布日期 接受日期

摘要 以XML文档的特殊结构为基础，将加密与访问控制结合起来，提出了一个访问控制模型（Access Control Model, ACM）。根据访问控制模型，按照主机角色及其特点、主机角色间的关系和访问控制策略库（Access Control Base, ACB），设计了XML文档分组加密算法，产生密钥对照表，进行密钥分配与管理，将依据一个或多个密钥对XML文档解密的任务交给主机，减轻服务器的负担；根据访问控制策略对主机的访问权限进行时间限制，在访问控制模型的基础上提出依据访问控制权限，将加密后的XML文档安全传送给不同级别主机，并进行安全检查的方法。

Abstract Extensible Markup Language (XML) has become the standard for data interchange on the Internet. In this paper, based on the special structure of XML documents, an access control model (ACM) was brought forth. According to this access control model and different roles of hosts, their characteristics, their relationships and access control base (ACB), an algorithm of grouping and encrypting XML documents was designed. Key-collation table was created and keys were distributed and managed. Hosts use one or more keys to decrypt XML documents and the server is set free. The access of hosts is temporally controlled by ACB. On the basis of access control model, the method of transmitting securely XML documents encrypted according to access control privileges, to hosts of different grades, and the method of security check-up were put forward.

关键词 XML,访问控制,粒度,加密

Key words XML,access control,granularity,encryption

分类号

DOI:

通讯作者:
孟健 meng_jian@citiz.net

作者个人主页: 孟健; 曹立明; 王小平; 姚亮

扩展功能

本文信息

- Supporting info
- PDF(570KB)
- [HTML全文](0KB)
- 参考文献[PDF]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“XML,访问控制,粒度,加密”的 相关文章

本文作者相关文章

· 孟健
· 曹立明
· 王小平
· 姚亮