通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

陈波1,于泠1,强小辉1,王岩2.基于隐含格结构ABE算法的移动存储介质情境访问控制[J].通信学报,2014,(4):53~64

基于隐含格结构ABE算法的移动存储介质情境访问控制

Contextual access control based on attribute-based encryption with hidden lattice structure for removable storage media

投稿时间： 2013-10-13

DOI：10.3969/j.issn.1000-436x.2014.4.007

中文关键词：属性加密 移动存储介质 隐藏访问结构 格安全模型 情境访问控制

英文关键词：attribute-based encryption removable storage media hidden access structures lattice security model contextual access control

基金项目：江苏省教育科学“十二五”规划重点基金资助项目(B-a/2013/01/013)；江苏省自然科学重大基金资助项目(产学研联合创新基金)(BY2011108)

作者	单位
陈波1，于泠1，强小辉1，王岩2	1. 南京师范大学 计算机学院，江苏 南京 210023；2. 麦考瑞大学 计算机学院，悉尼 2109

中文摘要：

研究了如何增强可信终端对移动存储介质的访问控制能力，以有效避免通过移动存储介质的敏感信息泄露。首先在隐含密文策略的属性加密方法的基础上，提出了基于格结构的属性策略描述方法。将每个属性构成线性格或子集格，属性集构造成一个乘积格，并利用基于格的多级信息流控制模型制定访问策略。证明了新方法的正确性和安全性。新方法在保持已有隐藏访问策略属性加密算法优点的同时，还能有效简化访问策略的表达，更符合多级安全中敏感信息的共享，能够实现细粒度的访问控制。进一步地，通过将移动存储设备和用户的使用情境作为属性构建访问策略，实现了动态的、细粒度的情境访问控制。最终设计了对移动存储介质进行接入认证、情境访问控制的分层安全管理方案。分析了方案的安全性和灵活性，并通过比较实验说明了应用情境访问控制的方案仍具有较好的处理效率。该方案同样适用于泛在环境下敏感信息的安全管理

英文摘要：

To prevent data breaches via removable storage media, the way to enhance the access control capability of hosts within trusted zone with removable storage media attached was explored. Firstly, based on traditional Cipher-text- Policy hiding Attribute-Based Encryption (CP-ABE) schemes, an expression with lattice for attributes was proposed. Each attribute was described as a linear lattice or a subset lattice, and an attribute set was described as a product lattice. Furthermore, the lattice-based multi-level access control model was applied to construct access policies. The new scheme was proven fully secure under the standard model. It effectively simplifies the expression of access policies and satisfies fine-grained access control of sensitive information shared in the context of multi-level security. Secondly, considering the ubiquitous usage of removable storage media, some security attributes associating with the context of use were adopted to construct a lattice structure. Then a dynamic access control could be achieved. Finally, based on authorization and dynamic access control, a layered security solution providing multi-level protection for removable storage media was presented. Security and flexibility of proposed solution was analyzed, and a comparison experiment shows that it still has pretty good efficiency. It also can be applied to information security management in other ubiquitous environments.

查看全文 查看/发表评论 下载PDF阅读器

关闭