中国科学院研究生院学报 2011, 28(5) 648-658 DOI: ISSN: CN:

本期目录 | 下期目录 | 过刊浏览 | 高级检索 [打印本页] [关闭]

论文

TPM虚拟域安全模型

秦宇, 兰海波

中国科学院软件研究所信息安全国家重点实验室, 北京 100080

摘要:

针对TPM访问控制机制无法直接应用于虚拟计算、云计算等环境的问题,重点分析TPM内部对象间依赖关系,并结合虚拟域的安全需求,建立TPM虚拟域安全模型.该模型对TPM对象的访问请求增加了虚拟域的完整性、机密性等安全约束,解决了多虚拟域环境下的TPM对象的创建、使用、销毁等问题.还进一步对该模型的安全规则进行了相关逻辑分析,并通过实际原型系统的测试,证明了TPM虚拟域安全模型的实施对可信虚拟平台的性能影响非常小.

关键词: TCG TPM安全模型 虚拟化 虚拟域 安全级

TPM security model for virtual domains

QIN Yu, LAN Hai-Bo

State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China

Abstract:

Considering that TPM access control mechanism can not be directly applied in virtualization computing, we build the security model for virtual domains based on the dependent relationships of TPM objects and the security requirements of the virtual domains. We add the security constraints of virtual domain, integrity and confidentiality, for the TPM objects' access requests in the model and solve the problems about TPM objects creation, usage, and destroy in multiple virtual domains. The logic analysis for the security rules in the model are further given in this paper. Through the tests on the prototype system, we show that the model has very small performance impact on trust virtualization platform.

Keywords: TCG TPM security model virtualization virtual domain security level

收稿日期 2010-09-01 **修回日期** 2010-10-17 **网络版发布日期**

DOI:

基金项目:

国家科技支撑计划项目(2008BAH22B06)和中国科学院知识创新工程前沿项目(ISCAS2009-DR14,ISCAS2009-GR03)资助

通讯作者:

作者简介:

作者Email: qin_yu@is.iscas.ac.cn

扩展功能

本文信息

- Supporting info
- PDF(1009KB)
- [HTML全文]
- 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

本文关键词相关文章

- TCG
- TPM安全模型
- 虚拟化
- 虚拟域
- 安全级

本文作者相关文章

PubMed

参考文献:

[1] Trusted Computing Group. TPM main part 1, design principles specification, version 1.2 revision 62 (2003-10) https://www.trustedcomputinggroup.org/home.

[2] Trusted Computing Group. TCG software stack (TSS) specification, version 1.10 . (2003) https://www.trustedcomputinggroup.org.

[3] Trusted Computing Group. TCG trusted network connect, TNC architecture for interoperability specification version 1.0 revision 4,3 . (2005-05) https://www.trustedcomputinggroup.org/home.

[4] Danilo B, Lorenzo C, Andrea L, et al. Replay attack in TCG specification and solution //21st Annual

Computer Security Applications Conference. 2005.

[5] Evan R S. A security assessment of trusted platform modules, TR2007-597 . Department of Computer Science, Dartmouth College, 2007.

[6] Safford D, Zohar M. A trusted linux client(TLC) . http://www.research.ibm.com/gsal/tcpa/tlc.pdf.

[7] Biba K J. Integrity considerations for secure computer systems, ESD-TR-76-372 . USAF Electronic Systems Division, Hanscom Air Force Base, Bedford, Massachusetts, 1977.

[8] Bell D E, LaPadula L J. Secure computer systems: A refinement of the mathematical model . Electronic Systems Division,Air Force Systems Command, Hanscom Aidr Force Base, Bedford, MA, 1974.

[9] Fraser T. LOMAC: low water-mark integrity protection for COTS environments // the 2000 IEEE Symposium on Security and Privacy. USA: Oakland, California, 2000.

[10] Jaeger T, Sailer R, Shankar U. PRIMA: policy-reduced integrity measurement architecture // ACM Symposium on Access Control Models and Technologies (SACMAT). California, 2006.

[11] Shankar U, Jaeger T, Sailer R. Toward automated information-flow integrity for security-critical applications // the 13th Annual Network and Distributed Systems Security Symposium. 2006.

[12] Huang Q, Shen C X, Chen Y L, et al. Secrecy/integrity union MLS policy based on trusting computing
[J]. Computer Engineering and Applications, 2006, 42(10):15-18 (in Chinese). 黄强,沈昌祥,陈幼雷,等.基于可信计算的保密和完整性统一安全策略
[J].计算机工程与应用,2006,42(10):15-18.

[13] Sandhu R, Zhang X W. Access management for distributed systems: Peer-to-peer access control architecture using trusted computing technology //the 10th ACM Symposium on Access Control Models and Technologies. 2005.

[14] Berger S, Cáceres R, Goldman K A, et al. vTPM: virtualizing the trusted platform module, RC23879 . IBM Research Division Thomas J. Tech Rep: Watson Research Center, 2006.

[15] Sadeghi A, Stüble C, Winandy M. Property-based TPM virtualization // the 11th International Conference on information Security. Lecture Notes in Computer Science, 5222. Berlin, Heidelberg: Springer-Verlag, 1-16.

[16] England P, Loeser J. Para-virtualized TPM sharing //the 1st International Conference on Trusted Computing and Trust in Information Technologies: Trusted Computing-Challenges and Applications (Villach, Austria, March 11 - 12, 2008). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer-Verlag, 2009,4968:119-132.

[17] Trusted Computing Group. TCG PC client specific implementation specification for conventional BIOS, version 1.2 final, revision 1.00 . July 2005, https://www.trustedcomputinggroup.org/home.

[18] Denning D E, A lattice model of secure information flow
[J]. Communications of the ACM, 1976, 19(5): 236-243.

[19] Microsoft, Microsoft NGSCB home page . (2003) http://www.microsoft.com/resources/ngscb.

[20] Garfinkel T, Pfaff B, Chow J, et al. Terra: A virtual machine-based platform for trusted computing // the Symposium on Operating System Principles (SOSP). 2003.

[21] Barham P, Dragovic B, Fraser K, et al. Xen and the art of virtualization // the 19th ACM Symposium on Operating Systems Principles. Bolton Landing, NY, 2003.

本刊中的类似文章

1．崔奇 石文昌，.一种通过应用程序验证TPM标准符合性的方法[J]. 中国科学院研究生院学报, 2008,25(5): 657-664