计算机工程 2012, 38(04) 23-27 DOI: 10.3969/j.issn.1000-3428.2012.04.008 ISSN: 1000-3428 CN: 31-1289/TP

博士论文

基于TPM的强身份认证协议研究

徐 贤 [1]，龙 宇 [2]，毛贤平 [2]

(1. 华东理工大学计算机科学与工程系，上海 200237；2. 上海交通大学计算机科学与工程系，上海 200240)

摘要： 根据可信计算领域中对身份认证的要求，提出一种基于TPM的强身份认证协议。介绍可信平台模块架构，给出其支持的密钥类型，按照进程理论建立协议模型，阐述协议扩展方案，包括引入PCR挑战、实现跨平台认证，并采用网络开发技术加以实现。实验结果表明，该协议可有效对用户身份进行验证。

关键词： 可信平台模块 数字签名 公钥加密 Java平台

Research on TPM-based Strong ID Authentication Protocol

XU Xian [1], LONG Yu [2], MAO Xian-ping [2]

(1. Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China; 2. Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: In terms of the requirement of ID authentication in trusted computing filed, this paper proposes a Trusted Platform Module(TPM)- based strong ID authentication protocol. TPM is reviewed as well as the types of keys supported and their relationship. A mathematical model of the protocol using the formal method of process theory is designed. The extension of the protocol is discussed, including Platform Configuration Register(PCR) challenging and implementing platform independence. An application scenario of the protocol by network development technology is implemented. Experimental results show the protocol can authenticate users' ID effectively.

Keywords: Trusted Platform Module(TPM) digital signature public key encryption Java platform

收稿日期 2011-07-20 **修回日期** **网络版发布日期** 2012-02-20

DOI: 10.3969/j.issn.1000-3428.2012.04.008

基金项目:

国家自然科学基金资助项目(60903020, 60903189, 607 73094)；国家“863”计划基金资助项目(2008AA01Z403)；上海市曙光计划基金资助项目(07SG32)

通讯作者:

作者简介: 徐 贤(1979－)，男，副教授、博士，主研方向：分布式计算，并发控制理论，信息安全；龙 宇，讲师、博士；毛贤平，博士研究生

通讯作者E-mail: xuxian@ecust.edu.cn

参考文献：

[1] Trusted Computing Group. TCG Specification Architecture Over- view[EB/OL]. (2007-11-21). http://www.mendeley.com/research/ tcg-specification-architecture-overview/.

[2] Edward L. Cyber Physical Systems: Design Challenges[EB/OL]. (2010-11-21).

http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/ EECS-2008-8.html.

[6] Kinney S. Trusted Platform Module Basics: Using TPM in Embedded Systems[M]. [S. l.]: Elsevier.[J]..2006,:-

[7] Trusted Computing Group. Cloud Computing and Security——A Natural Match[EB/OL]. (2010-09-21). http://www.trusted-computing- group.org.

[8] Hanna S. A Security Analysis of Cloud Computing[EB/OL]. (2010-12-21). http://cloudcomputing.sys-con.com/node/1203943.

[9] Challener D.[J].Yoder K, Catherman R, et al. A Practical Guide to Trusted Computing[M]. [S. l.]: IBM Press.2008,:-

[10] Stinson D R. Cryptography: Theory and Practice[M]. 3rd ed. [S. l.]: Chapman & Hall. [J]..2005,:-

[12] National Technical Information Service. 180-2-2002 Specifications for the Secure Hash Standard[S]. 2002.

[13] Milner R. Communication and Concurrency[M]. [S. l.]: Prentice Hall.[J]..1989,:-

[15] Oracle Corporation. Jsr-000316-2009 Java Platform, Enterprise Edition 6, Specification 6.0[S]. 2009.

[16] MIT CSAIL. TPM/J Developer's Guide[EB/OL]. (2009-11-21). http://projects.csail.mit.edu/tc/tpmj/DevelopersGuide.html.

[17] Apache Software Foundation. Apache Tomcat 6.0[EB/OL]. (2010- 11-21). http://tomcat.apache.org/tomcat-6.0-doc/setup.html.

[18] Oracle and/or Its Affiliates. MySQL 5.1 Reference Manual[EB/OL]. (2007-11-21). http://dev.mysql.com/doc/refman/5.1/en/.

[19] Apache Software Foundation. Apache Struts 1.3, Spring Frame- work 2.5 and Hibernate 3.2 Reference Documentation[EB/OL]. (2008-01-21). http://www.apache.org/.

[20] Milner R, Parrow J, Walker D. A Calculus of Mobile Processes, Part I and Part II [J].Information and Computation.1992, 100(1):1-77

[21] 曹爱霞, 赵一鸣. Ad Hoc网络中基于身份的认证密钥交换协 议[J].计算机工程.2007, 33(10):150-152 浏览

本刊中的类似文章

1. 王明辉, 王建东.基于口令的三方认证密钥交换协议[J]. 计算机工程, 2012,38(2): 146-147
2. 邓宇乔.一种前向安全的代理重签名方案[J]. 计算机工程, 2012,38(2): 144-145
3. 王秀利, 王萌.一种应用于双重数字签名的电子拍卖方案[J]. 计算机工程, 2012,38(04): 4-6
4. 杨帆, 高振华, 柴志雷.WCET可预测的Java指令集硬件实现[J]. 计算机工程, 2012,38(01): 14-18
5. 杨宏宇, 李东博.EFBS数据交换模型与完整性检查机制[J]. 计算机工程, 2012,38(01): 29-32
6. 马昌社.PPK模型下的有序多重数字签名方案[J]. 计算机工程, 2011,37(9): 19-21
7. 王勇兵, 张学亮, 仇宾.一种新的基于身份的代理签名方案[J]. 计算机工程, 2011,37(7): 157-159
8. 归奕红.无线传感器网络HEDSA数据聚合研究[J]. 计算机工程, 2011,37(7): 160-162
9. 钟翔.具有失败-中止性质的代理签名[J]. 计算机工程, 2011,37(5): 179-180,183
10. 黄玉颖, 马华, 张应辉, 史来婧.基于身份的链式验证签名方案[J]. 计算机工程, 2011,37(4): 142-144

文章评论

反馈人		邮箱地址	
反馈标题		验证码	3444

5