

安全技术

基于UEFI的可信BIOS研究与实现

周振柳<sup>1,2</sup>, 李 铭<sup>3</sup>, 翟伟斌<sup>1</sup>, 许榕生<sup>1</sup>

(1. 中国科学院高能物理研究所计算中心, 北京 100049; 2. 沈阳航空工业学院计算机学院, 沈阳 110034; 3. 中国电子科技集团信息化工程总体研究中心, 北京 100083)

收稿日期 修回日期 网络版发布日期 2008-4-11 接受日期

摘要 分析固件基本输入输出系统(BIOS)的安全需求, 定义了可信BIOS概念。基于UEFI规范和可信计算机机制设计UTBIOS体系结构。UTBIOS的实现以新一代符合UEFI规范的BIOS产品为基础, 使用可信测量根核对BIOS运行和系统引导过程中各部件进行可信测量, 构建操作系统运行前的可信链, 讨论可信测量对BIOS引导过程的性能影响。

关键词 [可信计算](#) [可信测量](#) [基本输入输出系统](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: 周振柳<sup>1,2</sup>; 李 铭<sup>3</sup>; 翟伟斌<sup>1</sup>; 许榕生<sup>1</sup>

扩展功能
本文信息
▶ <a href="#">Supporting info</a>
▶ <a href="#">PDF(112KB)</a>
▶ <a href="#">[HTML全文](0KB)</a>
▶ <a href="#">参考文献[PDF]</a>
▶ <a href="#">参考文献</a>
服务与反馈
▶ <a href="#">把本文推荐给朋友</a>
▶ <a href="#">加入我的书架</a>
▶ <a href="#">加入引用管理器</a>
▶ <a href="#">引用本文</a>
▶ <a href="#">Email Alert</a>
▶ <a href="#">文章反馈</a>
▶ <a href="#">浏览反馈信息</a>
相关信息
▶ <a href="#">本刊中 包含“可信计算”的 相关文章</a>
▶ 本文作者相关文章
• <a href="#">周振柳<sup>1,2</sup>, 李 铭<sup>3</sup>, 翟伟斌<sup>1</sup>, 许榕生<sup>1</sup></a>