

# 固态硬盘安全风险分析与攻击实验

刘政林, 陈小强, 刘文超, 郑怡恺, 邹雪城  
(华中科技大学 光学与电子信息学院, 湖北 武汉 430074)

**摘要:** 为了研究固态硬盘由于闪存转换层植入恶意代码引起的安全风险, 分类分析了五种安全风险, 包括: 数据盗取、数据销毁、拒绝服务、攻击主机和性能下降.同时研究了这类恶意代码的作用机理和可能的形式, 根据触发条件和攻击负载进行了分类.通过编写恶意代码并植入到固态硬盘中, 在 Windows 平台上成功实施了攻击实验, 实现了固态硬盘拒绝服务和数据销毁.实验结果表明, 这类固态硬盘安全风险确实存在, 向固态硬盘中植入恶意代码的攻击手段十分隐蔽, 用户难以发觉.最后, 针对这类固态硬盘安全风险, 提出了一种简单有效的防御对策。

**关键词:** 固态硬盘; 闪存转换层; 恶意代码; 安全风险; 攻击实验

## Attack Experiment and Analysis for SSD Security Risks

LIU Zheng-lin, CHEN Xiao-qiang, LIU Wen-chao, ZHENG Yi-kai, ZOU Xue-cheng  
(School of Optical and Electronic Information, Huazhong University of Science and  
Technology, Wuhan 430074, China)

**Abstract:** In order to analyze solid state drive (SSD) security risks caused by malicious code in the flash translation layer (FTL), we classify them into five kinds of risks, including data stealing, data destruction, denial of service, attack host and performance reduction. We also analyze this kind of malicious code about its action mechanism and possible forms, and classify malicious code based on its trigger and attack load. We design malicious code and inject it into SSD, implement attack experiment on Windows platform successfully. Attacks result in SSD denial of service and data destruction. Experiment results show that this kind of SSD security risks is real problem and injecting malicious code into SSD can be very imperceptible, SSD users are unable to aware of it. At last we propose a simple and effective countermeasure for this kind of SSD security risks.

**Key words:** solid state drive (SSD); flash translation layer (FTL); malicious code; security risks; attack experiment

作者简介:

刘政林男, (1968-), 博士, 教授.研究方向为微电子学与固体电子学.

陈小强 (通讯作者) 男, (1993-), 硕士研究生.研究方向为微电子学与固体电子学.

E-mail:chenxiaoqiangmail@qq.com.

刘文超男, (1983-), 博士研究生.研究方向为微电子学与固体电子学.

郑怡恺女, (1994-), 硕士研究生.研究方向为微电子学与固体电子学.

邹雪城男, (1964-), 博士, 教授.研究方向为微电子学与固体电子学.