

# 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

**中图分类号:** TP333      **文献标识码:** A      **文章编号:** 1000—7180(2018)12—0016—05

## 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

### 1 引言

固态硬盘(Solid State Drive, SSD)是由存储芯片阵列作为存储介质的固态存储设备,存储芯片可以是 Flash 或者 DRAM 等。随着闪存颗粒成本的降低,SSD 凭借优越的性能已经获得了极为广泛的应用,SSD 的存储安全问题也变得越来越重要。

目前,国内外对 SSD 的研究主要集中在 SSD 性能和稳定性的提高<sup>[1-3]</sup>,对 SSD 的数据安全问题研究仍然较少。文献[4]分析了由于 SSD 固件专利保护带来的存储系统安全漏洞,并提出以 RAID 技术结合保存所有

数据页摘要的方法抵御安全威胁。文献[5]介绍了一种针对 SATA -I 型接口固态硬盘的数据加密方案和密钥管理方法,并进行了 FPGA 实现。文献[6]提出了一种可信 SSD,通过增加一层访问控制层,把对数据的访问控制从主机下放到 SSD 中,实现存储内安全。本文将分析由 SSD 闪存转换层中植入恶意代码引起的安全风险,并对这类恶意代码进行分类分析。之后,我们通过向 SSD 闪存转换层中植入恶意代码,在 Windows 平台上实施攻击实验,说明这种攻击手段的可行性和对用户数据的危害。最后,针对这类 SSD 安全风险,提出一种简单有效的防御对策。

2 SSD 安全风险

固态硬盘的层级结构如图 1 所示,可以分为 SSD 固件、SSD 控制器和 NAND Flash 三层. 其中 SSD 固件又可以分为主机接口、闪存转换层和底层驱动三层,主机接口负责与主机通信;闪存转换层把主机针对磁盘的独立扇区操作转换为对 NAND Flash 的操作;底层驱动负责配置 SSD 控制器.

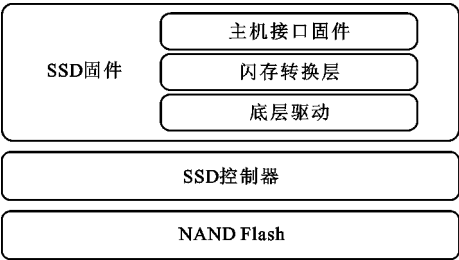


图 1 固态硬盘层级结构

闪存转换层(Flash Translation Layer, FTL)是 SSD 固件设计的关键,因此 SSD 固件也可以简单称之为 FTL. FTL 将逻辑地址和物理地址进行灵活地重新映射,实现异地更新,可以减少擦除 NAND Flash 的次数. 同时,FTL 还进行垃圾回收、坏块管理、磨损均衡等工作,FTL 的效率直接影响 SSD 的性能和寿命. 为了高效运行 FTL,提高 SSD 性能,SSD 控制器中集成了高性能的嵌入式处理器,并配备大容量缓存.

SSD 控制器的基本结构如图 2 所示. 可以看出 SSD 已经具有了 CPU、内存和 ROM,可以看作是一个小型计算机系统,在固件的控制下可以有自己的行为. SSD 可以自主地读写、擦除 NAND Flash,也可以将某些数据块标记为坏块,或者对数据进行加密,不一定需要主机授权. 而且,由于闪存转换层的存在,主机无法有效地监督 SSD 内部的活动,可能导致用户无法确切知道 SSD 的容量大小、坏块多少、有无隐藏空间、有无预存数据,以及 FTL 中是否有恶意代码. 如果 FTL 中包含一些恶意代码,用户的数据安全将面临威胁,主机对 SSD 执行格式化和重装系统也无法消除这些安全风险.

固态硬盘 FTL 植入恶意代码之后,用户使用这种固态硬盘,将面临存储安全风险. 这些安全风险包括但不限于以下 5 种:(1)数据盗取. 恶意的 FTL 可以自行在 SSD 中开辟出一些隐藏存储空间,盗取用户数据并存储下来,等待机会外传. 精巧的恶意代码能够发起自下而上的攻击,感染主机并外传数据<sup>[7]</sup>.

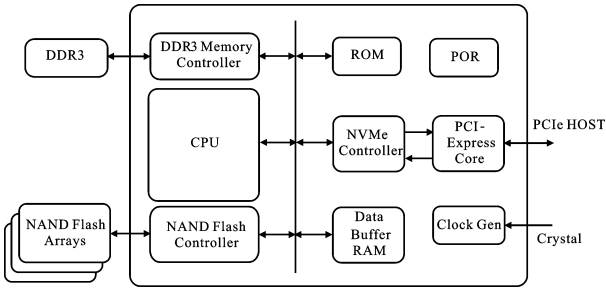


图 2 SSD 控制器基本结构

另外,由于 SSD 擦写次数有限,更换较为频繁,攻击者也可以从报废 SSD 中的隐藏空间取出数据.(2)数据销毁. 恶意的 FTL 可能会擦除 SSD 中的数据,如果采用 AFSSI-5020 等数据清除方法进行安全擦除,用户数据将永久丢失.(3)拒绝服务. 恶意的 FTL 可能会使 SSD 拒绝服务. 如果 SSD 作为系统盘,SSD 拒绝服务会造成系统崩溃;如果 SSD 不是作为系统盘,SSD 拒绝服务会造成系统持续卡顿.(4)攻击主机. 恶意的 FTL 也可能自下而上攻击主机,比如让主机不断重启,或者利用操作系统漏洞感染主机,取得系统的控制权<sup>[8]</sup>. (5)SSD 性能下降、坏块增加、频繁出错. 这一类安全风险比较温和,没有很强的破坏性,但是会持续地影响整个系统的正常运行,造成的损失可能更大.

3 恶意代码

用户在使用 SSD 之前,一般会对 SSD 进行全面的检测. 为了避免在初期被发现和排除,这些植入 FTL 的恶意代码需要一种隐藏措施,一种可能的形式为:恶意代码长期保持“沉默”,只有在满足一定条件时才开始执行. 这种攻击手段采用“触发”加“负载”的方式,只有当触发条件满足时,攻击负载才会开始执行,以达到最佳的攻击效果. 根据触发和负载不同,我们可以对植入固态硬盘 FTL 中的恶意代码进行分类分析. 如图 3 所示.

触发条件包括但不限于以下 5 种:(1)特殊数据序列触发. 恶意代码会扫描存入固态硬盘的文件内容,检测特殊数据序列,作为触发条件.(2)时间节点触发. 恶意代码检测系统时间,到达预定的时间就触发攻击.(3)硬盘工作模式触发. 一般情况下用户对硬盘的读写是随机和低频的,因此触发条件可以选择高强度的硬盘读写、对同一逻辑地址的高频更新等情况.(4)病毒程序触发. 病毒程序可以修改 SSD 固件,植入恶意代码,之后可以主动触发攻击<sup>[7]</sup>. (5)近场通讯触发. 攻击者携带近场通讯设备靠近目标

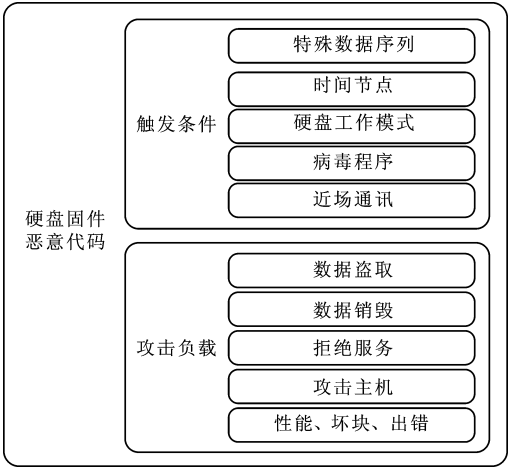


图 3 恶意代码分类

SSD,激活恶意代码,同时可以篡改或窃取数据,这一触发方式需要攻击者预先向 SSD 硬件中植入近场通讯模块。

攻击负载也归纳为五种:(1)数据盗取.(2)数据销毁.(3)拒绝服务.(4)攻击主机.(5)SSD 性能下降、坏块增加、频繁出错.与固态硬盘 FTL 植入恶意代码引起的安全风险一一对应。

恶意代码的形式非常灵活,可以是以上触发方式和攻击负载的任意组合.为了将恶意代码植入固态硬盘 FTL,攻击者可能采取以下三种方法:

(1)在 SSD 生产过程中植入. SSD 的技术壁垒没有机械硬盘那么高,一般厂商通过购买 SSD 控制器芯片和闪存颗粒,自行设计电路板和 FTL(或者采用解决方案),也可以量产 SSD,类似于电脑整机的生产.因此,SSD 厂商鱼龙混杂,很难保证其中没有恶意厂商,向 SSD 的 FTL 中植入恶意代码,威胁目标用户的数据安全。

(2)在 SSD 固件升级过程中植入.为了解决 SSD 的故障和提高性能,厂商往往会提供固件更新的接口,用户可以刷新固件来解决问题,这也给了攻击者注入恶意代码的机会.如果攻击者掌握了一种 SSD 主控芯片的 FTL,就有可能利用固件升级的机会攻击采用这一主控的同类 SSD 产品.高效可靠的 FTL 设计虽难,但也不是没有借鉴,攻击者如果能够得到 SSD 控制器厂商的 FTL 解决方案或技术文档,攻击的难度就会大大降低。

(3)病毒程序修改 SSD 固件.这种植入恶意代码的手段比较复杂,攻击者先用病毒程序感染用户的主机,再修改硬盘固件,使病毒程序可以常驻硬盘.这种攻击手段威胁范围最广,技术难度最高,2015 年卡巴

斯基实验室披露的“方程式”组织采用了这种攻击手段,该组织所创造的恶意软件 Equation Drug 和 Gray Fish 拥有重新编程硬盘固件的能力<sup>[8]</sup>。

固态硬盘在生产、物流、安装、使用过程中都有可能被植入恶意的 FTL,这些 FTL 中包含的恶意代码触发方式和攻击负载可以非常灵活、非常隐蔽.固态硬盘 FTL 中被植入了恶意代码之后,用户对 SSD 的检测很难发现这些隐患,使用这种 SSD 将面临巨大的数据安全风险。

4 SSD 植入恶意代码实验

4.1 实验环境

目前,固态硬盘 FTL 中植入恶意代码的攻击事件还没有被公开报道过.为了证明这类安全风险的存在和危害,我们在 SSD 硬件平台和 Windows 应用场景下进行了一种攻击实验。

实验主机和 SSD 硬件平台通过 PCIe 线缆相连,实验主机是装有 Windows 10 操作系统的个人电脑,模拟一般用户的使用场景,实验 SSD 基于 OpenSSD Cosmos 平台<sup>[9]</sup>开发,该平台提供开源的硬件和固件,FTL 采用页映射方式.在 Xilinx SDK 开发环境下,对该 SSD 平台的 FTL 进行重新编程和写入,模拟恶意厂商用篡改过的 FTL 给 SSD 开卡的情况。

实验主机的配置信息如表 1 所示。

表 1 实验主机配置信息

| 主板       | 联想 N1996       |
|----------|----------------|
| BIOS 版本  | 联想 BIOS ver2.0 |
| 操作系统     | Windows10 64 位 |
| 与 SSD 接口 | PCIe gen2      |
| SSD 驱动程序 | 微软 NVMe 驱动     |

4.2 实验过程

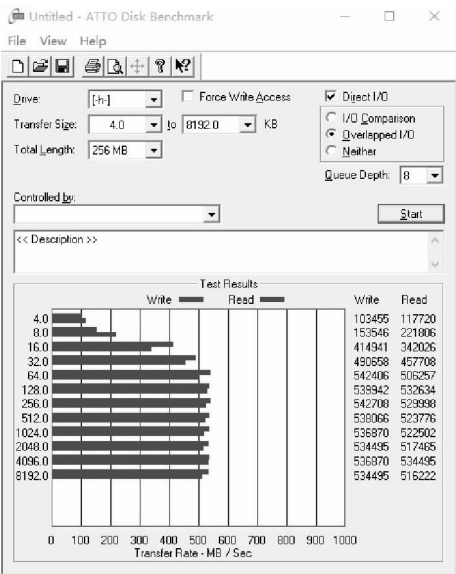
我们设计了一种恶意代码,植入到正常的固态硬盘 FTL 中,然后模拟用户在 Windows 操作系统下使用 SSD 的场景,采用检测特殊数据序列的方式触发攻击,评估攻击负载达到的效果,说明这类安全风险的危害。

首先,设计恶意代码,并整合到正常的 FTL 中.根据之前的分析,设计触发方式为检测特殊的数据序列,同时设计了两种攻击负载,根据检测到的特殊数据序列的不同,执行拒绝服务,或者数据销毁.伪代码如下所示:

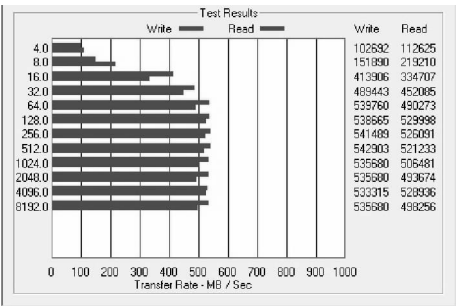
恶意代码示意  
for (DMA 写入)

```
{
  执行 DMA;
  获取 DMA 命令中的设备地址;
  根据 NTFS 文件系统的属性追踪文件位置;
  读取文件中特定位置的数据 data;
  if (data == 特殊序列 1)
    拒绝服务;
  else if (data == 特殊序列 2)
    数据销毁;
  else
    不执行任何操作;
}
```

然后,用恶意篡改过的 FTL 给 SSD 开卡,并将该 SSD 提供给用户使用. 初次安装 SSD 需要进行初始化,选择最常用的 NTFS 文件系统并格式化该盘,实验中 SSD 盘符为 H. 用户采用 ATTO Disk Benchmark 软件测试该 SSD 的性能,如图 4(b)所示. 植入恶意代码之前,对该 SSD 的读写性能测试如图 4(a)所示. 比较发现,植入恶意代码前后,SSD 性能无明显区别,用户不会觉察到异常.



(a)植入恶意代码前



(b)植入恶意代码后

图 4 对 SSD 的性能测试

最后,用包含特殊序列的文件触发恶意代码,评估攻击负载达到的效果. 攻击者发动攻击时,将包含特殊序列的文件拷贝或发送给用户,该文件只要从主机缓存写入到目标 SSD 缓存,文件中的特殊序列就会被检测到,攻击负载就会被执行.

4.3 实验结果分析

实验结果显示,特殊数据序列可以成功检测,攻击负载顺利执行. 当检测到特殊序列 1 时,目标 SSD 拒绝服务,用户对 SSD 进行读写操作将异常终止.

当检测到特殊序列 2 时,目标 SSD 执行数据销毁. 使用 WinHex 软件来查看执行数据销毁后 SSD 的底层数据,如图 5 所示. 可以看到,数据销毁后 SSD 从起始位到终止位的十六进制值全为“FF”,说明数据销毁成功执行.

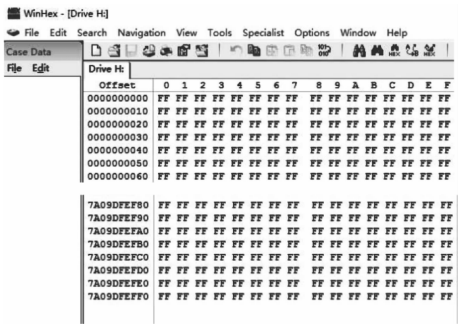


图 5 固态硬盘数据销毁

在 SSD 拒绝服务模式下,用户可以读取已经缓存在主机内存中的小文件,但是无法对 SSD 进行其他的操作. 在 SSD 数据销毁模式下,恶意 FTL 自发执行全盘擦除,用户数据丢失.

实验说明了向固态硬盘 FTL 中植入恶意代码的攻击手段是可行的. 如果恶意厂商想要实施这一攻击,付出的代价可以忽略,但是对用户数据的危害却非常大.

5 防御对策

上文研究了五种由于 SSD 植入恶意代码带来的安全风险:(1)数据盗取.(2)数据销毁.(3)拒绝服务.(4)攻击主机.(5)SSD 性能下降、坏块增加、频繁出错. 要检测并排除出这些安全风险,除了检查 SSD 厂商的 FTL 源代码之外,暂时还没有更有效的办法. 同时,FTL 作为 SSD 厂商的商业机密,厂商一般也不会提供源代码给用户检查. 因此,在目前缺乏有效检测措施的情况下,我们提出了一种防御对策,能够在 SSD 不可信的情况下,在一定程度上保证用户的数据安全. 这种防御对策由两部分构成:

一是采用镜像存储技术,并保证构成镜像存储的两块 SSD 来自不同的厂商.这种方法可以在一定程度上抵御数据销毁、拒绝服务,以及 SSD 性能下降、坏块增加、频繁出错等安全风险<sup>[4]</sup>.

二是在 SSD 和主机之间插入一个加密模块.不同于 SSD 全盘加密,这里用到的加密模块与 SSD 独立,即 SSD 不知道存储的数据已被加密.这种方法可以抵御数据盗取和恶意代码从 SSD 加载病毒程序攻击主机,同时防止特殊数据序列或病毒程序触发 FTL 中的恶意代码.

采用 RAID 控制器搭建一个镜像存储系统,如图 6 所示.镜像存储系统中的 SSD0 和 SSD1 来自不同的厂商,除非这两块 SSD 同时发生故障,否则用户就可以抵御 SSD 数据销毁、拒绝服务,以及 SSD 性能下降、坏块增加、频繁出错等安全威胁,提高存储安全性.

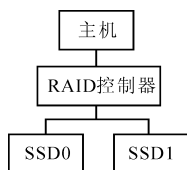


图 6 SSD 镜像存储系统

加密模块可以集成在上述 RAID 控制器中,数据写入 SSD 时都经过加密,从 SSD 读出的数据解密后再发送到主机.数据读写流程如图 7 所示.

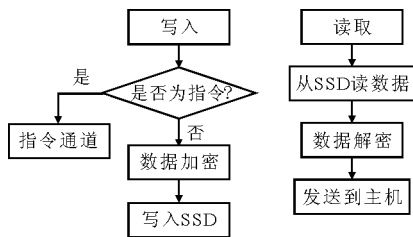


图 7 加入防御对策的数据读写流程

首先,加密模块混淆了存入 SSD 的数据,可以防止不可信 SSD 盗取数据,保存在不可见区域,因为 SSD 中存储的数据都是密文,且 SSD 无法自行解密.其次,加密模块也混淆了从 SSD 读取的数据,可以防止不可信 SSD 攻击主机,因为攻击者预存在 SSD 不可见区域或固件中的病毒程序,在读取过程中经过解密变成了乱码.也就是说,在加密模块存在的情况下,只有用户自行写入到 SSD 中的数据能被正确读出.这种防御对策的性能开销很低,因为硬件 RAID 控制器和硬件加解密已经可以达到很高的吞吐量.这种防御对策的硬件成本是一个显著问题,为

了实现该防御策略,需要一个额外的 SSD 和集成了加密模块的 RAID 控制器.为了降低成本,在一些对数据安全要求不是很高的场合,可以根据需要只采用加密模块作为防御对策,这种折衷方案也可以抵御大多数由固态硬盘 FTL 植入恶意代码引起的安全风险.

另外,我们建议在一些数据安全至关重要的应用场合中,一定要选择可信厂商生产的 SSD,封闭固件升级接口,并且在生产、物流、安装、使用的各个环节严防 FTL 被恶意篡改,才能最大程度保证 SSD 安全可靠.

## 6 结束语

通过设计恶意代码并植入到固态硬盘 FTL 中,我们在 Windows 平台上成功实施了攻击实验,实现了 SSD 拒绝服务和数据销毁,证明了向固态硬盘 FTL 中植入恶意代码实施攻击的可行性和对用户数据的危害.研究这类安全风险,可以帮助 SSD 用户发现问题,排除隐患,建立基于 SSD 的安全存储系统.为了进一步给出切实可行的安全措施,针对这种 SSD 安全风险,我们提出了一种镜像存储和数据加密的防御对策,并将在今后继续深入研究.

## 参考文献:

- [1] Hsieh J W, Lin H Y, Yang D L. Multi-channel architecture-based FTL for reliable and high-performance SSD[J]. IEEE Transactions on Computers, 2014, 63 (12): 3079-3091.
- [2] Seo B K, Maeng S, Lee J, et al. DRACO: a deduplicating FTL for tangible extra capacity[J]. IEEE Computer Architecture Letters, 2015, 14(2): 123-126.
- [3] Zhou J, Chen X C, Wang J, et al. Leveraging semantic links for high efficiency page-level FTL design[C]// 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops. Nara, Japan, 2016: 84-89.
- [4] Cui X T, Zou M H, Shi L, et al. Towards trustable storage using SSDs with proprietary FTL[C]// 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE). Grenoble, France, 2015: 1213-1216.
- [5] 韩煜, 刘政林. 一种高吞吐量、低成本的固态硬盘数据安全方案[J]. 信息与电子工程, 2011, 9(5): 638-641.
- [6] 田洪亮, 张勇, 许信辉, 等. 可信固态硬盘: 大数据安全的新基础[J]. 计算机学报, 2016, 39(1): 154-168.

参考文献:

[1] Yang X S, Deb S. Cuckoo search via levy flights[C]// Proceedings of the World Congress on Nature & Biologically Inspired Computing (NaBIC'09). India, Coimbatore, 2009: 210-214.

[2] Mohammad Shehab, Ahamad Tajudin Khader, Mohammed Azmi Al-Betar. A survey on applications and variants of the cuckoo search algorithm[J]. Applied Soft Computing, 2017(61): 1041-1059.

[3] Luus R, Jaakola T H I. Optimization by direct search and systematic reduction in the size of search region [J]. Aiche Journal, 1973, 19(4):760-766.

[4] Ghodrati A, Lotfi S. A hybrid CS/PSO algorithm for global optimization[C]// Proceedings of the 4th Asian conference on Intelligent Information and Database Systems -Volume Part III. Berlin, Springer-Verlag, 2012:89-98.

[5] 江浩, 阮奇, 念美玲, 等. 改进的布谷鸟搜索算法及其在多效蒸发优化中的应用[J]. 计算机与应用化学, 2014, 31(11):1363-1368.

[6] 聂慧, 刘波, 韦向远, 等. 求解资源受限项目调度问题的改进布谷鸟搜索算法[J]. 桂林理工大学学报, 2013, 33(33):529-536.

[7] 李娜, 贺兴时. 基于粒子群算法的布谷鸟搜索算法[J]. 纺织高校基础科学学报, 2014, 27(3):374-379.

[8] He Y, Chen D, Zhao W. Ensemble classifier system

based on ant colony algorithm and its application in chemical pattern classification [J]. Chemometrics & Intelligent Laboratory Systems, 2006, 80(1):39-49.

[9] Söbester A, Forrester A I J. Ant colony optimization [J]. Alphascript Publishing, 2010, 28(3):1155-1173.

[10] Yang X S, Deb S. Cuckoo Search: recent advances and applications[J]. Neural Computing and Applications, 2014, 24(1):169-174.

[11] Naik M, Nath M R, Wunnava A, et al. A new adaptive cuckoo search algorithm[C]//2015 IEEE 2nd International Conference on Recent Trends in Information Systems. Kolkata, India, 2015:1-5.

[12] Vazquez R A. Training spiking neural models using cuckoo search algorithm[J]. Evolutionary Computation, 2011, 30(1):679-686.

作者简介:

张烈平 男, (1971-), 博士, 教授. 研究方向为无线传感器网络、系统优化与调度. E-mail: 25761108@qq. com.

何佳洁 女, (1992-), 硕士研究生. 研究方向为检测技术与自动化装置.

于滢琳 女, (1993-), 硕士研究生. 研究方向为检测技术及自动化装置.

杨振宇 男, (1993-), 硕士研究生. 研究方向为控制工程.

骆颖雄 男, (1990-), 硕士. 研究方向为计算机应用.

(上接第 20 页)

[7] 安天实验室. 修改硬盘固件的木马: 探索方程式组织的攻击组件 [EB/OL]. (2015-03-13). [2017-12-01]. <https://www.secpulse.com/archives/5326.html>.

[8] Kaspersky Lab. Equation: the death star of malware galaxy [EB/OL]. (2015-02-16). [2017-12-01]. <https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/>.

[9] ENC Lab. The open SSD project [EB/OL]. (2017-06-05). [2017-12-01]. [http://www.openssd-project.org/wiki/The\\_OpenSSD\\_Project](http://www.openssd-project.org/wiki/The_OpenSSD_Project)

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.