论文笔记

题目：Reactive redundancy for data destruction protection (R2D2)
出处：Computers & Security 2018
作者：Christopher N.Gutierrez, Eugene H.Spafford, SaurabhBagchi, ThomasYurek
单位：Purdue University, CERIAS, 656 Oval Dr., West Lafayette, IN 47907, USA
原文： https://www.sciencedirect.com/science/article/pii/S016740481730281X
相关材料： HomePage

一、背景

恶意软件种类繁多，但是在这篇文章中，作者主要关注两种类型的恶意软件，分别是Cropto Ransomware和Wiper Malware。像 Wiper Malware这样的恶意软件，目的是摧毁我们的文件，如果在此之前，我们没有对文件进行备份，那就很难恢复被摧毁的文件；然而，像Cropto Ransomware这样的勒索软件，目的是加密某些特定类型的文件，使得受害者必须支付一定的费用之后才能恢复文件。另一方面，Cropto Ransomware在覆盖原文件的时候，会产生很高的熵值，因为它采用了加密技术，同时，它也不会摧毁整个系统，因为它要向受害者展示一个勒索界面，提示受害者要支付一定的费用，以解密电脑上的文件。与Cropto Ransomware不同的是，Wiper Malware可能会使用任意的数据来覆盖原始的文件，并且也不关心文件被覆盖之后，系统是否还能正常运行。

二、提出的方法以及解决的问题

对于Cropto Ransomware和Wiper Malware这两种恶意软件，它们都有一个共同的特征，就是使得系统中的文件遭受破坏，为了对抗这种现象，作者在这篇文章中提出了一种应对的策略R2D2（Reactive redundancy for data destruction protection），即，能够使得被恶意软件破坏之后的文件完整的恢复回来，该系统不仅对以上这两种恶意软件有效，而已对于一些专业的数据擦除软件也很有效。

R2D2与之前的工具不太一样，之前的工具使用的方法是让工具本身与恶意软件（或者说是攻击者）同处于同一个环境当中（例如，同处于一个OS当中），但是这样做的缺点也是很明显，即，攻击者可以disable我们的防御系统。因此，R2D2采用了一种新的方法，即，让我们的检测工具与攻击者隔离，处于不同的环境中（不同的系统中），这样使得R2D2以99.8%的精确度来保证用户数据免遭恶意软件的破坏。

三、技术方法

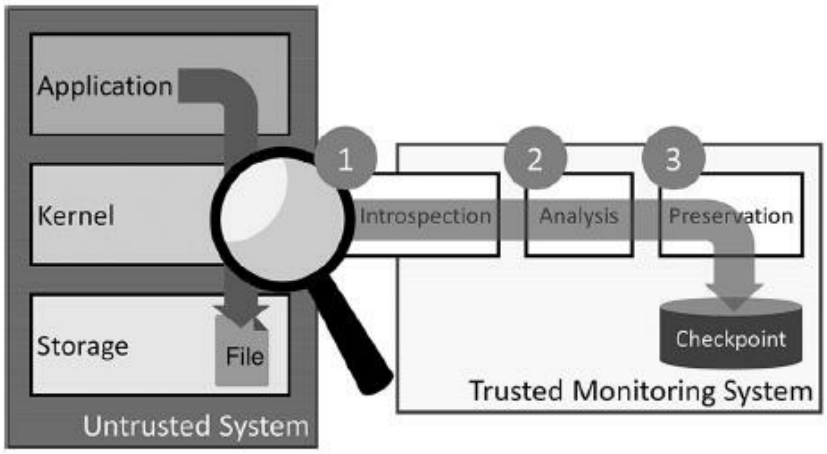

Fig. 1 – R2D2 interposes storage medium I/O in isolation. If the I/O appears to be destructive, R2D2 preserves the data.

如图1所示，是R2D2的总体结构图，前面也已经提到，R2D2是与攻击者隔离的，处于不同的环境中，这就使得攻击者无法发现以及disable R2D2。从图1中我们可以知道，左边是Untrusted System，是攻击者所在的环境；而右边是Trusted Monitoring System，是R2D2所在的环境。R2D2运行在Virtual Machine Monitor（VMM）里面，通过Virtual Machine Introspection（VMI）技术监视左边的Untrusted System。R2D2主要由三个Policy构成，分别是：Introspection Policy、Analysis Policy和Preservation Policy。

图2以更细致的方式描述R2D2的运行原理，首先，①在Untrusted System中（图2的上半部分），一旦发现有文件以写的方式打开，R2D2就开始通过VMI来检测它的行为，并创建一个临时的检查点（Checkpoint），因为R2D2的Introspection Policy会在R2D2启动的时候定义一系列被监控的系统调用和一系列被保护的文件；②当文件被写入的时候，R2D2就会拦截这个系统调用，调用Analysis Policy分析调用参数，根据分析结果来确定该写操作是恶意的还是良性的，如果被确定为恶意的写操作，则R2D2会把刚才创建的临时检查点转化为持久性的系统快照（Snapshot），并保存到磁盘当中，以便管理员可以通过该快照恢复被破坏的文件。最后，根据Preservation Policy，临时创建的检查点会被垃圾回收机制定时回收，以释放磁盘空间。

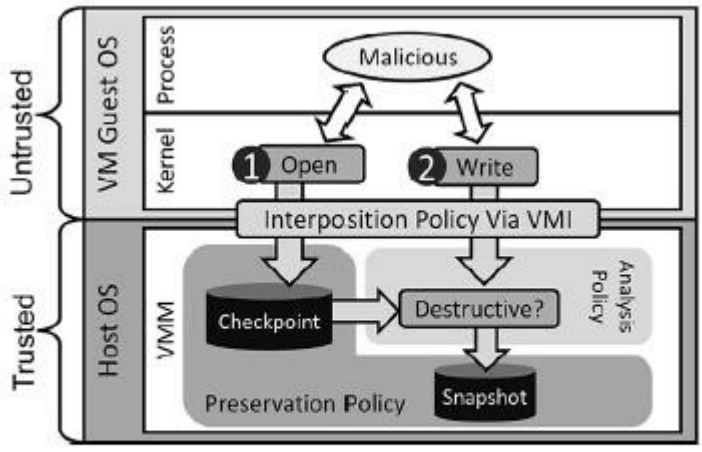

Fig. 2 – R2D2 examines file modifications and preserves the file if data destruction is suspected.

四、实验评估

在作者的实验中，展示出极高的准确性。如图4所示，左图是实验测试得出的结果，右图是稍微改正Analysis Policy之后得出的结果（其实是添加了签名库）。在989个测试样例中（所有操作都是恶意的destructive的写操作），只有两个被错误的划分为良性操作，True Positive Rate为99.8%，False Negative Rate为0.2%。而在989个测试样例中（所有操作都是良性的写操作），只有5个被错误的识别为destructive，True Positive Rate为99.49%，False Negative Rate为0.51%。可以看出，R2D2的识别率还是很高的。

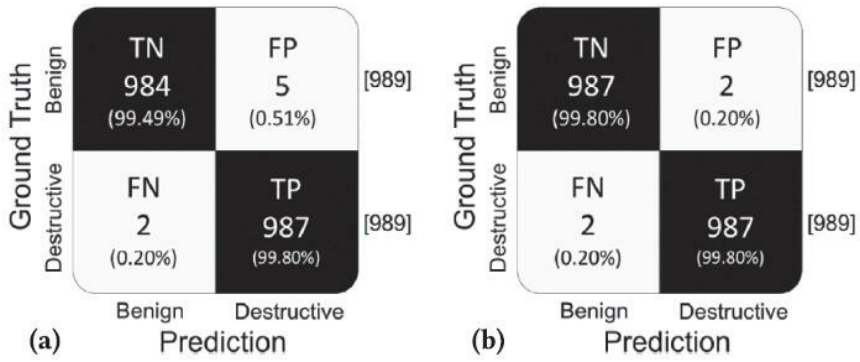

Fig. 4 – Confusion matrix for PRNG data destruction, the worst performing test. (a) Initial Results. (b) Corrected Results.

图5所示是演示Office办公的时候产生的性能开销，左边显示的是Work Benchmark Test性能开销，右边显示的是Storage Benchmark Test性能开销。深灰色是由于VMI产生的性能开销，浅灰色是由于R2D2生产的性能开销，从图中可以看出，主要的性能开销都是由于VMI产生的。

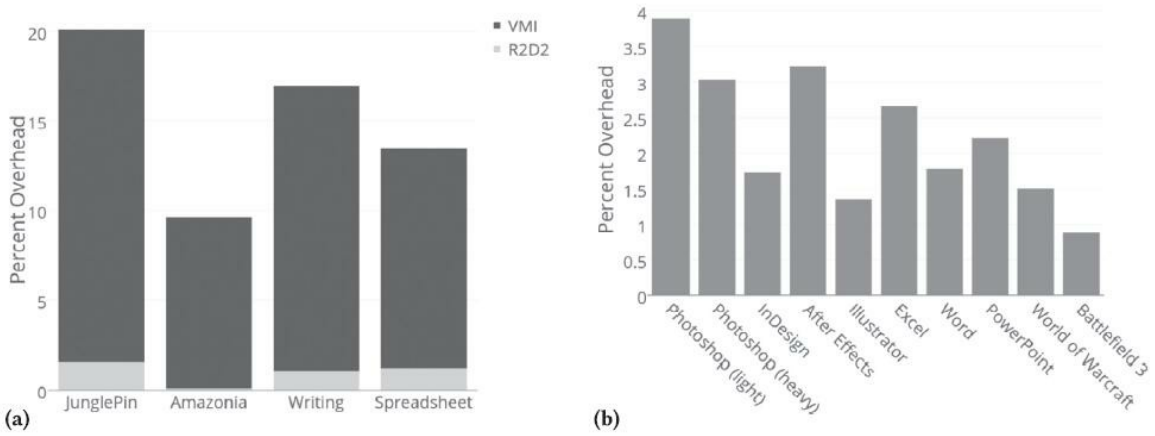

Fig. 5 – PCMark 8 office benchmark results showing the overhead incurred by R2D2 for a variety of common office tasks. The results are with respect to our baseline where no VMI but with NILFS in use. We observe that the bulk of the overhead arises from VMI provided by the Drakvuf analysis system (Lengyel, 2016). (a)Work Tests. (b) Storage Tests.

图6显示的是：由于写入固定的数据到文件中导致的延迟，由图可知，当写入的数据越小，由R2D2产生的性能开销所占的比重越大，当写入的数据越大，由R2D2产生的性能开销所占的比重越小。

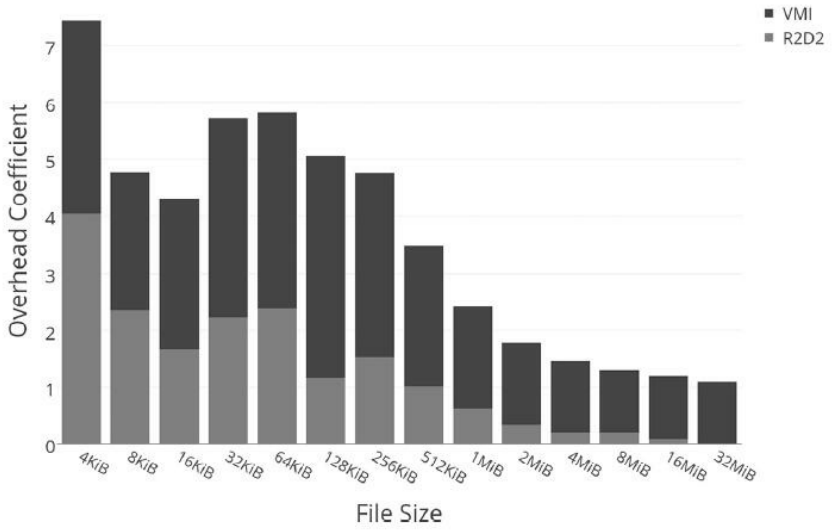

Fig. 6 – Median Latency introduced by R2D2 and VMI when data destruction is suspect.

五、R2D2的优缺点

R2D2有以下优点：

- R2D2的Introspection Policy通过添加白名单和黑名单来提高检测机制的运行效率、减少系统延迟。
- R2D2的分析策略（Analysis Policy）不是基于单一的签名策略，而是结合三种不同的策略来判断一个写操作是否是可疑的，这样可以提高识别恶意操作的准确性。
- R2D2最大的优势在于它与攻击者工作在隔离的环境当中。使得自己运行在一个可信的环境中，不会被攻击者disable。
- R2D2以极高的准确性发现恶意操作，使得在这些恶意的操作之后，用户的文件依然可以被完好的恢复。

R2D2有以下缺点：

- R2D2是运行在VMM中的，而VMM本身就会给系统带来一定的延迟，因此，R2D2需要考虑的延迟是自己本身带来的延迟加上VMM带来的延迟。
- 攻击者任然可以通过Kernel Object Hooking (KOH) 和 Dynamic Kernel Object Manipulation(DKOM)等技术来逃避VMM的监视，因此，也就可以逃避R2D2的监视。
- 攻击者如果在Untrusted System之外修改Untrusted System内部的文件，则也有可能绕过R2D2的检测。
- 如果一个合法的用户要执行删除文件，或者是加密/解密、压缩/解压等操作，则也会触发R2D2系统，会被认为是恶意操作。
- 如果一个合法的用户要执行删除文件，或者是加密/解密、压缩/解压等操作，则必须要先通知管理员，让管理员暂时关闭R2D2系统，等执行完相应的操作之后再让管理员恢复R2D2系统，这样做不但很麻烦，而且还给攻击者带来了一个潜在的攻击窗口。
- 一个最致命的缺点是：当系统中进行随机的写入操作的时候，会产生极高的性能开销。例如，作者在测试CrystalDiskMark的时候，随机写带来的性能开销分别是：VMI：95.4%，R2D2：57.5%。

六、个人观点

个人觉得，这篇文章没有用的什么新的技术，主要的贡献在于它把几项现存的技术（例如VMI、

Snapshot、R2D2与攻击者隔离等）融合于一体，形成了一个新的系统（R2D2）。另外，作者通过R2D2与攻击者隔离，使得R2D2处于一个可信的环境当中，攻击者无法直接disable R2D2，这就给R2D2带来很大的好处，可以在Untrusted System之外监视Untrusted System，以一种上帝视角的形式监控攻击者的行为，可以避免不必要的干扰，这种思想在分析恶意软件的时候很常用，也很奏效。R2D2也存在不足：合法用户进行删除文件、加密/解密的操作的时候也会触发R2D2系统，并且，当OS中国存在大量的随机写操作的时候，OS的性能开销会很大，OS的延迟也会大大增加。