1. 基于硬件分支事件的控制流劫持攻击防御方法

本文提出了一种基于硬件分支处理的控制流劫持攻击防御方法（简称BranchChecker）。该方法以硬件性能监控单元（Performance Monitoring Unit）产生的间接分支预测失败事件为检测触发点，基于最近分支记录（Last Branch Record）获取精确的分支信息，结合内存指令信息和系统调用参数信息，根据相应的检测规则进行配件（gadget）检测，并识别出ROP攻击可能利用的配件链（gadgets chain）。

本节将先对本文针对的威胁模型进行描述，然后对BranchChecker设计过程中涉及到的采样事件的选择以及攻击检测算法进行详细描述。

2.1威胁模型

本文采用与内存破坏及代码重用攻击文献一致的威胁模型：攻击者可以通过远程或本地正常终端访问应用，可以利用应用程序中的内存漏洞任意读取或修改应用数据内存页内容，也可以通过这些漏洞获取所有内存空间排布信息。但假定硬件，操作系统，动态链接器是可信的，目标操作系统支持NX或DEP技术，攻击者不能插入或修改应用代码，即攻击者被限定为仅能采用代码重用攻击。

2.2 采样事件选择

本文基于采样事件触发的PMI事件作为检查点，需要针对所有可能用于ROP攻击的指令片段进行检查。现代CPU提供了多种多样的PMU事件采样用于调试。ROP攻击的指令片段的一个重要特征是需要通过分支操作来实现指令片段间的衔接，因此，本文需要在分支相关事件中进行筛选。筛选的主要原则是：尽量降低采样事件频率，且不会遗漏ROP攻击相关分支。

本文结合ROP攻击特征及硬件相关特性进行了分支事件的选择：

1. PerfCFI针对应用程序进行保护，因此可将事件限定为用户态事件；
2. 基于我们的威胁模型，攻击者不能修改程序代码，因此直接分支的语义不会被修改，ROP攻击只能借助间接分支来进行攻击，因此触发事件可限定为间接分支事件；
3. 现代CPU为了提高效率基本都支持乱序执行技术，部分分支会被投机执行，但最终可能会被抛弃，最终不会提交，所以采样事件分为执行时的分支事件和提交时的分支事件。ROP攻击过程中的分支是程序真正运行时用到的分支，都属于提交的分支（只是攻击者破坏了控制流完整性，使其偏离了程序开发人员的本意），因此可将触发事件限定为分支提交事件；
4. ROP攻击链所需要的分支应该均为跳转的分支，如果不跳转，那么直接执行下一条指令，攻击者不能利用该分支跳转到他预期的目标，因此可将触发事件限定为跳转分支事件
5. 现代CPU的分支预测机制主要基于历史信息来对分支进行预测，由于ROP攻击会让分支偏离原有的跳转目标，将会与历史跳转目标或方向不一致，因此该分支会导致分支预测失败，因此可将事件限定为预测失败的分支事件；

综上所述，最为理想的分支事件为：用户态预测失败的跳转间接分支提交事件。但实际中各类CPU支持的事件粒度略有不同，因此可供选择的事件并不能保证能够包含最理想的情形，在原型系统实现中会详细描述具体采样事件的选择。

2.3 ROP攻击检测策略

BranchChecker通过捕获系统运行时的硬件分支处理相关的特征，基于特征设计相应的ROP攻击检测策略。

* **疑似配件的识别**

当满足下列条件之一时，认为当前指令片段为疑似配件（gadget）：

1. 非调用型返回指令Call-preceded ret：对于所有的返回指令，如果目标地址的上一条指令不是调用指令，将其标为疑似配件；
2. 分支短指令序列：如果上一个可疑分支到下一个可疑分支的指令长度低于一定阈值（maxGadgetLength），将其标为疑似配件。

* **长无效片段的识别**

为了提高检测的准确性，并且避免对历史信息的覆盖，PerfCFI对长无效片段进行识别和过滤。长无效片段是指副作用较小的长指令片段，通常用于绕过基于连续配件特征检测的CFI检测方式。如果在上一个疑似配件末尾到下一个疑似配件开始，系统状态（本文用系统架构寄存器的值来表征系统状态）的修改粒度低于一定阈值，将该段代码标为疑似长无效片段。

* **配件长度统计策略**

BranchChecker基于以下策略对配件长度进行统计：

1. 初始配件长度为0；
2. 如果是当前分支片段为疑似配件结尾，那么将配件长度加1；
3. 如果当前分支片段为疑似长无效片段，那么配件长度不变；
4. 非2）和3）的情形则将配件长度清0。

* **攻击检测策略**

BranchChecker基于以下两个条件进行攻击检测，当满足其中一个条件，认为程序遭受了ROP攻击：

1. 连续的配件数超过一定阈值（minChainLength）；

该检测条件适用于由一连串的配件链构成的攻击类型，也是最常见的ROP攻击情形；

1. 敏感系统调用中的参数和上一个疑似配件的系统状态（本文用系统架构寄存器的值来表征系统状态）基本一致；

该检测条件适用于通过较短的配件链直接进行敏感系统调用的情形。