1. 相关研究

控制流完整性（Control Flow Integrity，简称CFI）作为一种有效的ROP攻击防御技术，最早由Abadi等人提出[5]，该方法假设程序在其执行过程中，应当遵循预先定义好的控制流图（Control Flow Graph，简称CFG），以确保程序控制流不被劫持或非法篡改。具体作法是在控制流转移指令前插入检验代码，来判断目标地址的合法性。CFI技术分为细粒度和粗粒度两种类型。

Abadi等[5]提出的细粒度的CFI技术，预先计算出所有间接转移指令的可能的目标地址，并为之赋予唯一的ID；在检查时，在每条间接跳转指令执行前增加检查，一旦违反控制流图的间接跳转就会报错。Abadi等[6]利用CFI思想保证控制流的正确性，并结合内存访问控制、影子栈等，将传统的应用程序包装成XFI模块，在运行时提供保护与监控，并通过设置外部接口与操作系统交互。虽然这些细粒度的CFI技术能够提升系统的安全性，但其开销过大，难以得到实际部署。

粗粒度的CFI技术将一组或相近类型的目标归到一起进行检查，可在一定程度上降低开销。Zhang等[7]提出了CCFIR，该方法对间接调用指令和函数返回指令的目标进行区分，阻止未经验证的返回指令跳转到敏感函数的行为。Zhangn等[8]提出了binCFI，该方法将间接转移指令的操作数分为代码指针、异常处理程序入口、导出符号地址和返回地址等类型，通过精细的静态分析，得到不同类型的间接控制转移的合法目标集合，并基于此进行攻击检测。Mashtizadeh等[12]提出了CCFI方法对代码指针进行更细致的划分。该方法将代码指针细分为函数指针类、return指针类、方法指针类、虚表指针类，通过对代码指针进行加密来增强CFI方法。以上方法都是只实施了控制流不敏感策略，然而上下文信息的缺少会降低方法的有效性。因此Veen等[13]提出了上下文敏感的CFI技术，该方法能够监控通往敏感函数（可用于实施控制流转移攻击）的执行路径，通过使用二进制插桩涉及，在被监控路径上强制执行上下文敏感CIF的不变量。

以上的CFI技术均是基于二进制插桩的，需要修改源码或者通过反汇编重写二进制代码，这给这些技术的使用带来额外的工作量；并且会引入较大的性能开销或者检测效果不够精确。本文方法并不属于该类别，本文方法不依赖于源代码，同时可以直接作用于传统程序。进一步的，本文提供的检测框架可以和基于二进制程序的方式结合实现基于CFG的CFI检查，该方法将作为我们未来的研究方向之一。

此外，一些研究引入硬件机制来降低CFI技术的开销，提高检测精度。Pappas等提出了kBouncer方法[10]，该方法利用最近分支记录（Last Branch Record，简称LBR）捕获最近的16次跳转信息，在敏感系统调用处对捕获的16次跳转进行安全性判断。Cheng等提出ROPecker方法[2]，该方法也是利用最近分支记录捕获程序程序流的方式进行ROP攻击检测。该方法在运行时检测过去和未来的执行流中是否存在长配件链来进行攻击检测，还通过滑动窗口的机制来进一步提高准确性和高效性。但是，这两种方法都是一次性针对16个间接分支进行检查，会面临历史覆盖不足的问题，容易遭受历史覆盖攻击，导致检测精度下降。Xia等提出了CFIMon[11]，该方法采用分支跟踪缓冲区（Branch Trace Store，简称BTS）来捕获程序运行过程中跳转指令的信息。虽然分支跟踪缓冲区能够程序整个执行过程中的所有跳转指令的历史信息都记录下来，但相比使用最近分支记录，使用分支跟踪缓冲区会引入更大的性能开销。此外，以上三种方法均是针对长配件链的攻击进行检测，对于短配件链的攻击情况检测效果不佳。

本文提供的方法属于该类别，但本方法只对预测失败的间接分支进行检测，避免了对所有间接分支检测[2,10,11]导致的开销过大的问题，同时也避免了历史记录被覆盖导致的检测精度下降的问题[2,10]。进一步的，本方法专门设计了系统调用相关的检测，能够有效检测已有方法[2,10,11]难以检测到的短配件链的攻击。

除了CFI方法，另一个ROP攻击防御方面的研究热点是随机化技术[14-18]，该类技术通过将函数、内存页、基础块或指令排布等随机化，让攻击者不能准确预测所需配件的位置，无法进行ROP攻击。我们的方法可以和这些一起作用，用于阻止攻击者对应用程序进行ROP攻击。

1. 总结及展望

本文针对当今软件安全领域面临的主要安全威胁之一ROP攻击展开研究，提出了一种基于硬件分支处理的ROP攻击防御方法。该方法以硬件性能监控单元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一起根据相应的检测规则进行配件检测，并识别出ROP攻击可能利用的配件链。

由于本方法是基于最近分支记录和内存指令信息检测疑似配件，所以不需要修改源码或者重写二进制码，能直接针对二进制代码进行保护，增加了方法的实用性。进一步的，本方法通过性能监控单元采样预测失败的间接分支事件，针对每个预测失败的间接分支处触发性能监控中断进行CFI检测，避免了对预测正确的间接分支进行检查，一方面能够有效减少检测点，控制性能开销；另一方面能够避免历史覆盖的问题，提高检测精度。并且，本方法还引入了“长空配件”和“系统调用配件”的识别，能够避免长空配件引起的配件链检测中断的情况和短配件链攻击的情况，进一步提高检测精度。未来工作会将本文方法和细粒度的CFI技术[5,6]相结合，细粒度的CFI技术优点是检测精度高、缺点是性能开销较大。将本文思想应用到细粒度CFI技术中，能够降低已有方法中对程序控制流图检测频率，从而降低基于细粒度CFI技术的性能开销，提高方法的可用性。

**References**:

1. Davi L, Sadeghi A R, Winandy M. ROPdefender: A detection tool to defend against return-oriented programming attacks,Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 40-51, 2011.
2. Yueqiang Cheng, Zongwei Zhou, Miao Yu, Xuhua Ding, and Robert H Deng. ROPecker: A generic and practical approach for defending against rop attacks. NDSS14, 2014.
3. Ping Chen, Hai Xiao, Xiaobin Shen, Xinchun Yin, Bing Mao,and Li Xie. DROP: Detecting return-oriented programming malicious code. In Proceedings of the 5th International Conference on Information Systems Security (ICISS), 2009.
4. T. Bletsch, X. Jiang, V. W. Freely and Z. Liang, Jump-oriented programming:a new class of code-reuse attack, in Proceedings of the 6th ,4CM Symposium on Information, Computer and Communications Security,New York, NY, USA, pp. 30-40, 2011.
5. M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti. Control-flow integrity: Principles, implementations, and applications. In ACM Conference on Computer and Communications Security (CCS), 2005.
6. M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti.Control-flow integrity principles, implementations, and applications. ACM Transactions on Information and System Security (TISSEC), (1), Nov. 2009
7. Zhang, T. Wei, Z. Chen, L. Duan, L. Szekeres,S. McCamant, D. Song, and W. Zou. Practical Control Flow Integrity & Randomization for Binary Executables. In IEEE Symposium on Security and Privacy, 2013.
8. M. Zhang and R. Sekar. Control flow integrity for COTS binaries. In USENIX Security Symposium, 2013.
9. B. Niu and G. Tan. Modular control-flow integrity. In PLDI’14, 2014.
10. Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis. 2013. Transparent ROP exploit mitigation using indirect branch tracing. In Proceedings of the 22nd USENIX conference on Security (SEC'13). USENIX Association, Berkeley, CA, USA, 447462.
11. Yubin Xia, Yutao Liu, Haibo Chen, and Binyu Zang. 2012. CFIMon: Detecting violation of control flow integrity using performance counters. In Proceedings of the 2012 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (DSN '12). IEEE Computer Society, Washington, DC, USA, 112.
12. Ali Jose Mashtizadeh, Andrea Bittau, Dan Boneh, and David Mazières. 2015. CCFI: Cryptographically Enforced Control Flow Integrity. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). ACM, New York, NY, USA, 941951.
13. Victor van der Veen, Dennis Andriesse, Enes Göktaş, Ben Gras, Lionel Sambuc, Asia Slowinska, Herbert Bos, and Cristiano Giuffrida. 2015. Practical ContextSensitive CFI. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). ACM, New York, NY, USA, 927940.
14. L. Davi,A. Dmitrienko, S. Nűrnberger,A-R. Sadeghi. Gadge me if you can: Secure and efficient ad-hoc instruction-level randomization for x86 and arm. In 8th ACM SIGSAC symposium on Information, computer and communications security ,2013.
15. Wartell, R., Mohan, V., Hamlen, K.W., Lin, Z. Binary stirring: self-randomizing instruction addresses of legacy x86 binary code. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 157–168, 2012.
16. M. Backes, S. Nurnberger, Oxymoron: Making Fine-Grained Memory Randomization Practical by Allowing Code Sharing, in the Proceedings of the 23rd USENIX Security Symposium,2014
17. V. Pappas, M. Polychronakis, and A. D. Keromytis. Smashing the gadgets: Hindering return-oriented programming using in-place code randomization. In IEEE Symposium on Security and Privacy, 2012.
18. 詹珣. 针对ROP攻击的块粒度地址空间随机化防御技术的研究[硕士学位论文]. 南京. 南京大学软件学院 2014
19. Pinghai Yuan, Qingkai Zeng, Xuhua Ding. Hardware-Assisted Fine-Grained Code-Reuse Attack Detection. International Workshop on Recent Advances in Intrusion Detection. Pp.66-85
20. “HT Editor 2.0.20 Buffer Overflow（ROP PoC）,” http://www.exploit-db.com/exploits/22683/.
21. “JAD Buffer Overflow（ROP PoC）,” <http://www.exploit-db.com/exploits/42357/>.