软件所在并发漏洞检测方面取得进展

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/7559.html

近期，中国科学院软件研究所蔡彦团队提出了并发程序中并发漏洞检测的新方法，该团队首次基于松弛可交换事件来检测并发漏洞。该团队提出的松弛可交换事件克服了传统检测算法的不足，即使目标事件之前存在复杂的同步约束，也可以通过松弛可交换事件来判断是否可以交换。相关成果以*Detecting Concurrency Memory Corruption Vulnerabilities* 为题，发表于软件工程领域会议27th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE ’19)。

并发漏洞常常被攻击者利用和攻击，给软件的安全带来严重威胁，但是并发漏洞的检测十分困难。一种直观的检测方法是遍历所有的线程交错来检测并发漏洞，但是会带来交错状态空间爆炸的问题。目前一些研究者用数据竞争的检测方法来检测并发漏洞，但是由于数据竞争和并发漏洞并不等价，这种方法实际应用中并不是很有效。一些最新的基于约束求解的工作也存在较多误报问题。 该团队提出的方法目前主要针对与事件发生序相关的三类并发漏洞（释放后重用UAF、空指针解引用NPD和双重释放DF）进行检测。例如，在图1中有两个线程，线程t1对指针p解引用，线程t2释放指针p。如果对指针p的释放发生在对其解引用之前，就会产生并发漏洞UAF。在对这三类漏洞的研究中，该团队发现：检测并发漏洞的关键就是判断目标事件之间的顺序是否可以交换。该团队通过引入第三个事件（图2中的eany）来重新定义了给定的两个事件（e1和e2）的可交换性。该定义直观理解如下：给定两个距离较近的事件，如果它们和第三个事件满足一定的关系，那么这两个事件将有较高的概率可被交换。基于此，该团队提出了松弛可交换事件的概念。基于松弛可交换事件，团队进一步提出了针对上述三类并发漏洞的检测算法并实现了相应的原型工具。在一些CVE数据集和一个真实大规模的程序上的实验结果表明，提出的方法可以检测到更多的并发漏洞。

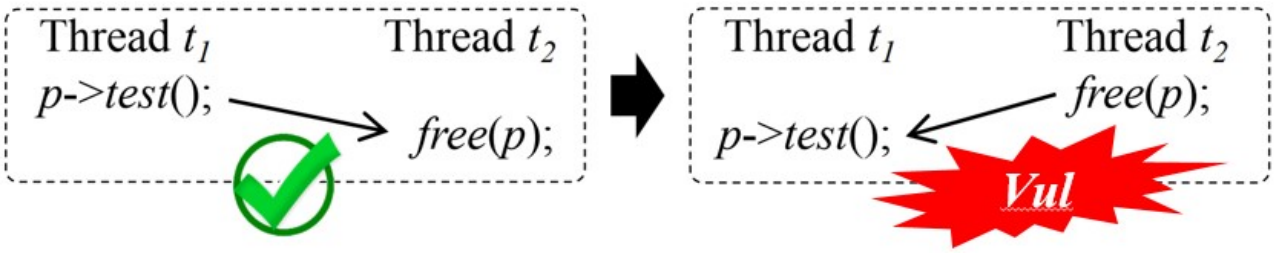

图1. 由事件发生序引发的并发漏洞

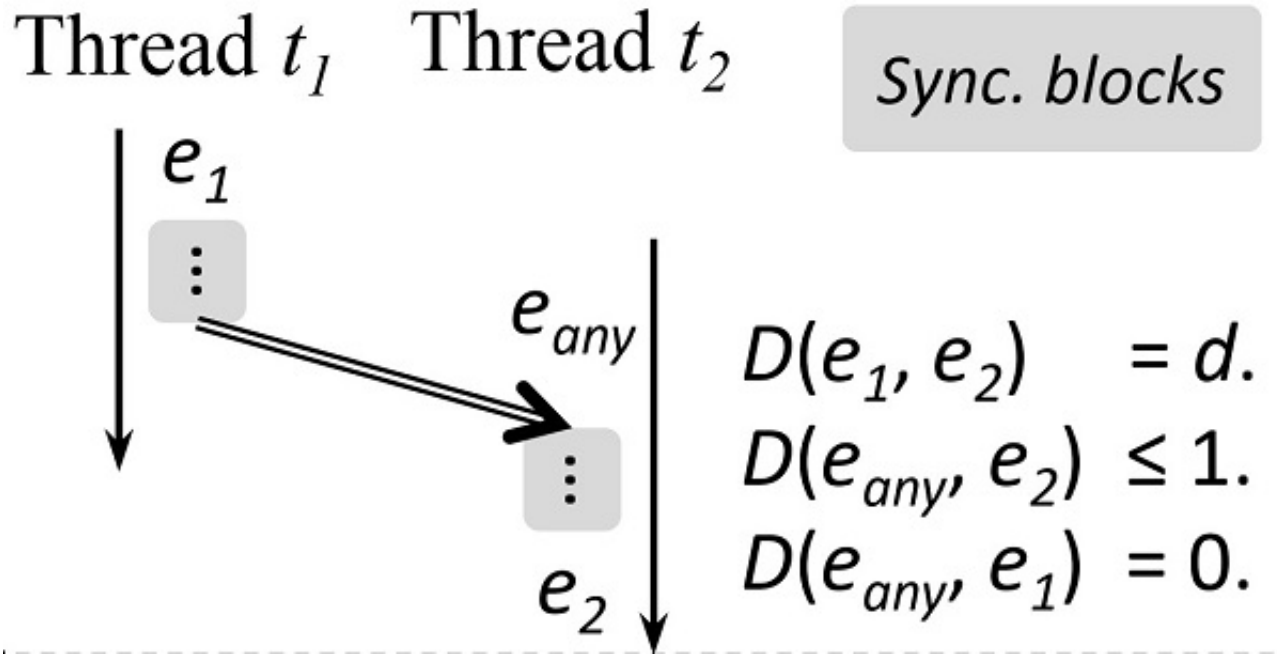

图2. 松弛可交换事件的解释

研究团队单位：软件研究所