中国科学院软件研究所学术年会’2020
暨计算机科学国家重点实验室开放周
ESEC/F'SE 2019：The 27th ACM Joint European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering

学术论文

内存损坏型并发漏洞的检测

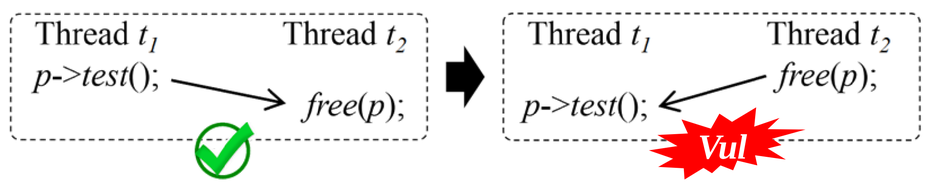
Detecting Concurrency Memory Corruption Vulnerabilities

蔡彦，朱碧云，孟瑞杰，云昊，和亮，苏璞睿，梁彬
中国科学院软件研究所(计算机科学国家重点实验室)，中国人民大学

软件漏洞常常被攻击者利用，带来严重威胁。由于多线程程序执行的不确定和复杂性，并发漏洞也非常普遍。一种直观的并发漏洞检测方法是遍历所有的线程交错顺序来检测并发漏洞，但是会带来交错状态空间爆炸的问题。由于并发漏洞中竞争条件与数据竞争的相似性，目前一些研究者用检测数据竞争的方法来检测并发漏洞；然而数据竞争和并发漏洞并不等价，这种方法在实际应用中并不是很有效。最近的一些基于约束求解的并发漏洞检测工作也存在较多误报问题。

该工作主要检测与事件发生序相关的三类并发漏洞即 UAF、NPD 和 DF。例如在图中，如果过对指针*p*的释放操作发生在对其解引用之前，就会产生并发漏洞 UAF。在对这三类并发漏洞的研究中我们发现，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互。我们由此提出松弛可交换事件的概念，并基于此进一步设计针对这三类并发漏洞的检测算法。在一些 CVE 数据集和真实的大规模程序上的实验结果表明，我们提出的方法可以更有效检测并发漏洞。

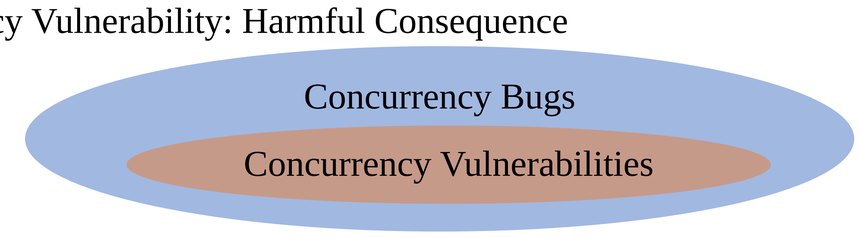
DirtyCow (CVE-2016-5195)：Linux内核中的并发漏洞，该漏洞可以使普通用户获取root权限，在Linux内核中潜藏十年之久。



Differences

◆ **Concurrency bugs vs Concurrency Vulnerabilities**

- ➢ Concurrency Bugs: Execution Correctness
  - The result may be not harmful
- ➢ Concurrency Vulnerability: Harmful Consequence



Exchangeable Events

◆ **Root Cause of Concurrency Vulnerabilities**

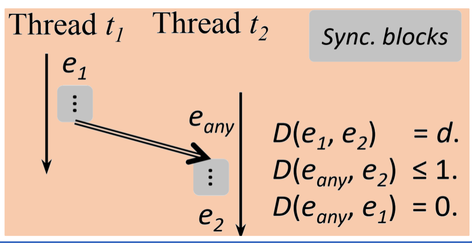
Non-determinism of multithread execution

- ➢ Some events can be executed in different orders across executions;
- ➢ Unexpected orders can cause vulnerabilities.

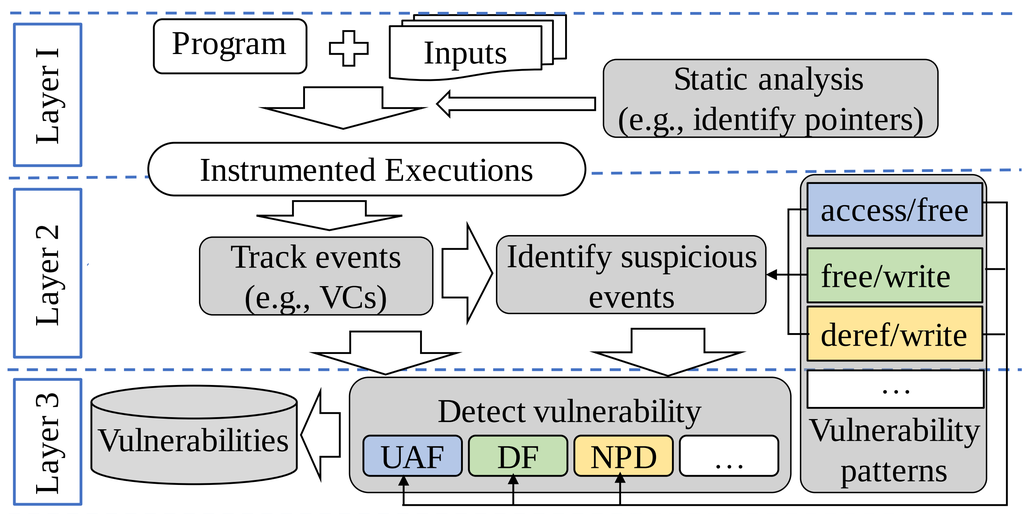
◆ **Definition of exchangeable events**

<e_1, e_2> is a pair of Exchangeable events if

- ➢ With a short distance $d = D(e_1, e_2)$
- ➢ A third event e_{any} as an evidence to exchange them:
  (1) $D(e_{any}, e_2) <= 1$
  (2) $D(e_{any}, e_1) = 0$



Tool Framework



◆ **Layer 1: Instrumented Execution**

- ➢ Instrument both Memory Events and Synchronization Events.
- ➢ Add static analysis to reduce the number of events tracked.

◆ **Layer 2: Events Tracking:**

Track and update the states of Memory and Thread.

◆ **Layer 3: Vulnerability Detection**

Convul detects concurrency vulnerabilities in two parts:

- ➢ Part 1: Determine the suspicious events involved into vulnerabilities
- ➢ Part 2: Judge whether they are exchangeable events.

Experiment

◆ **Comparisons**

- ➢ Data Race Detectors:
  FastTrack (FT, PLDI’09), Helgrind (Hel), ThreadSanitizer (Tsan)
- ➢ Concurrent UAF/NPD: UFO (ICSE’18)

◆ **On 10 known CVEs**

CVE ID	Category	Program	Detection Results: ConVul	FT	Hel	TSan	UFO	UFO$_{NPD}$
cve-2009-3547	NPD	Linux-2.6.32-rc6	✓	✓	✓	✓	-	✓
cve-2011-2183	NPD	Linux-2.6.39-3	✗	✗	✗	✗	-	✗
cve-2013-1792	NPD	Linux-3.8.3	✓	✗	✗	✗	-	✗
cve-2015-7550	NPD	Linux-4.3.4	✓	✗	✗	✗	-	✓
cve-2016-1972	UAF	Firefox-45.0	✓	✗	✗ (⋆)	✗ (⋆)	✗	-
cve-2016-1973	UAF	Firefox-45.0	✓	✗	✗	✗	✗	-
cve-2016-7911	NPD	Linux-4.6.6	✓	✗ (⋆)	✗ (⋆)	✗ (⋆)	-	✗
cve-2016-9806	DF	Linux-4.6.3	✓	✗ (⋆)	✗	✗ (⋆)	-	-
cve-2017-6346	UAF (DF)	Linux-4.9.13	✓	✗ (⋆)	✗ (⋆)	✗ (⋆)	✗	-
cve-2017-15265	UAF	Linux-4.13.8	✓	✗	✗	✓	✓	-
		Total	**9**	**1**	**1**	**2**	**1**	**2**
			Our	Three Race Detectors			A latest work	

◆ **Benchmarks**

- ➢ On existing **10 CVEs** (i.e., known vulnerabilities)
  - From Linux kernel, Firefox
- ➢ On the latest MySQL database servers (detect **zero-day** vulnerabilities)
  - SLOC: **2,244,927** ;
  - **933** test cases (built-in)

Detected: 6
Confirmed: 4

◆ **On MySQL**

Bug ID	Category	Status	Detected by Others? FT	Hel	TSan	UFO
MySQL-88311	UAF	Confirmed	✗	✗	✗	✗
MySQL-88911	NPD	Submitted	✗	✗	✗	-
MySQL-88914	NPD	Submitted	✗	✗	✗	-
MySQL-91448	NPD	Confirmed	✓	✗	✓	-
MySQL-91449	NPD	Confirmed	✗	✗	✗	-
MySQL-91896	NPD	Confirmed	✗	✗	✗	-
		Total	0	1	1	0
			Others: Only detected 1.			

联系方式: 蔡彦，*yancai@ios.ac.cn*， *http://yancai.site*，010-62661614
文章引用: Yan Cai, Biyun Zhu, Ruijie Meng, Hao Yun, Liang He, Purui Su, and Bin Liang. Detecting concurrency memory corruption vulnerabilities. In Proc. ESEC/FSE, 706–717, 2019.