ISCAS 中国科学院软件研究所学术年会'2021
暨计算机科学国家重点实验室开放周

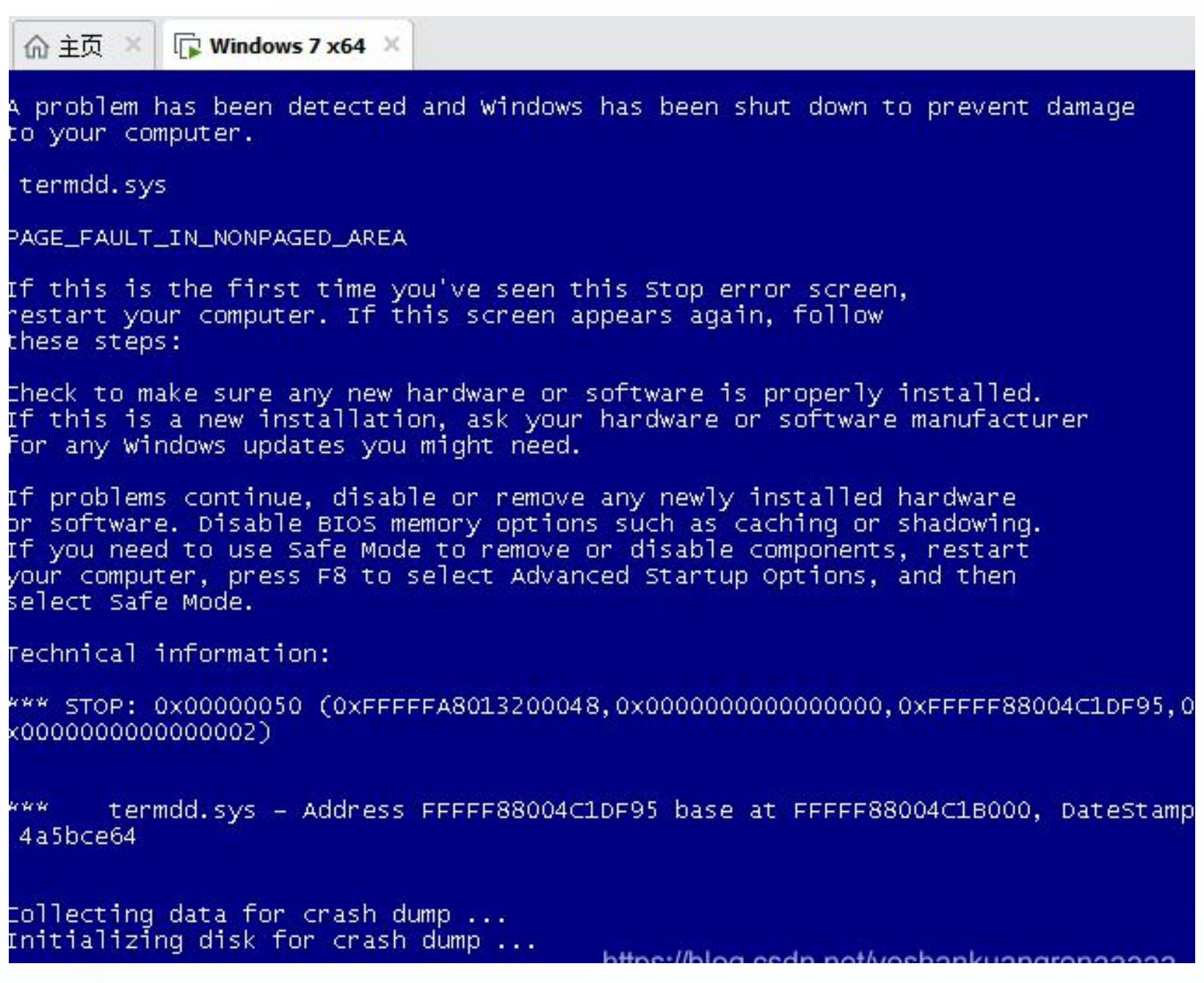
关键技术

释放后重用漏洞的自动化分析

和亮 苏璞睿

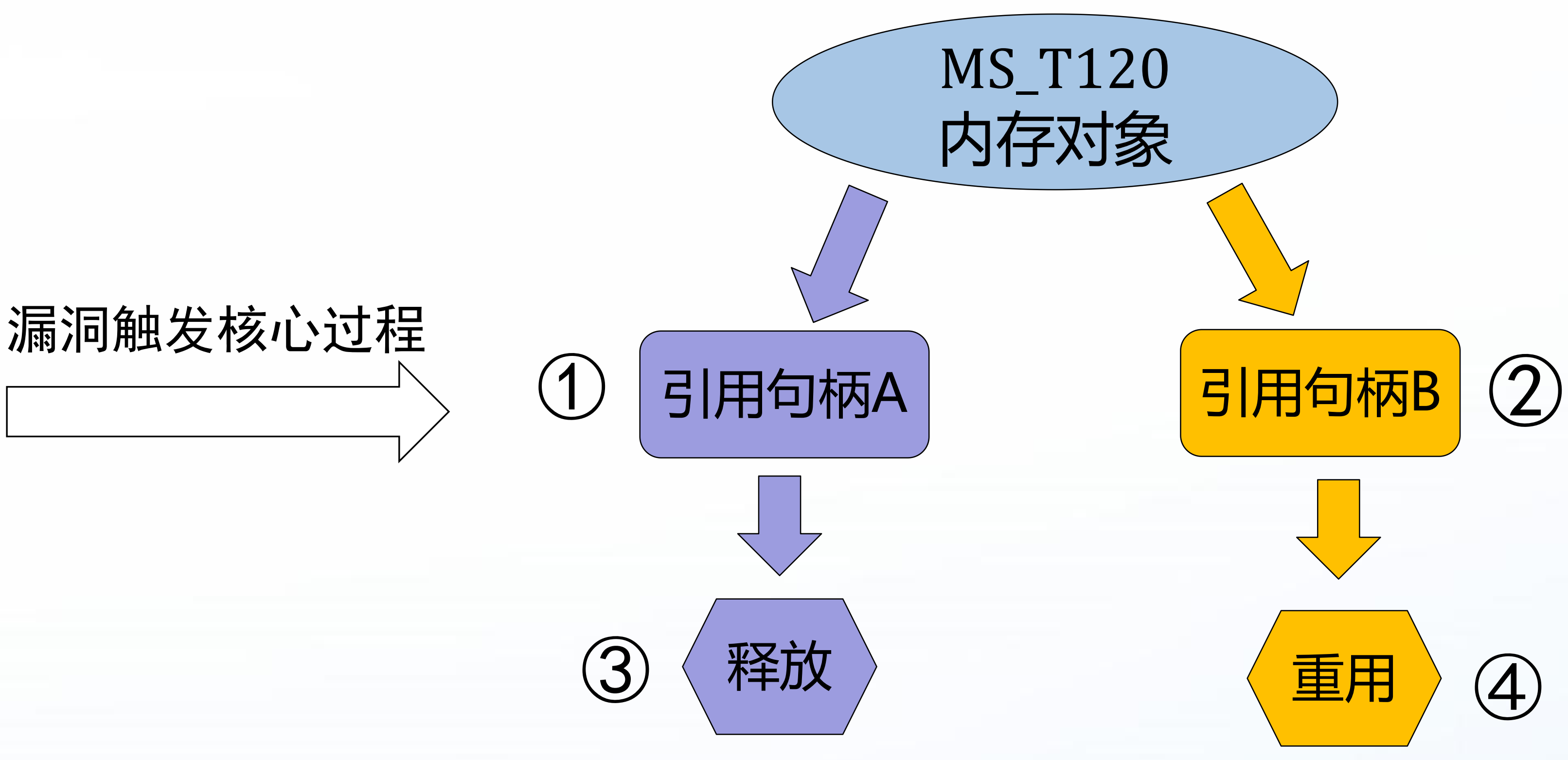
heliang@iscas.ac.cn

释放后重用漏洞仍然是目前各类网络攻击软件（例如，勒索软件、挖矿病毒）中频繁使用的一类内存破坏漏洞。在大规模软件中，释放后重用漏洞的触发往往涉及到多个不同模块之间的连续操作。因此，相比较其他漏洞而言，软件开发者或者生产厂商需要花费更长的周期来分析该类漏洞的机理并产生有效补丁，结果是延长了漏洞存活时间和潜在的攻击持续时间。



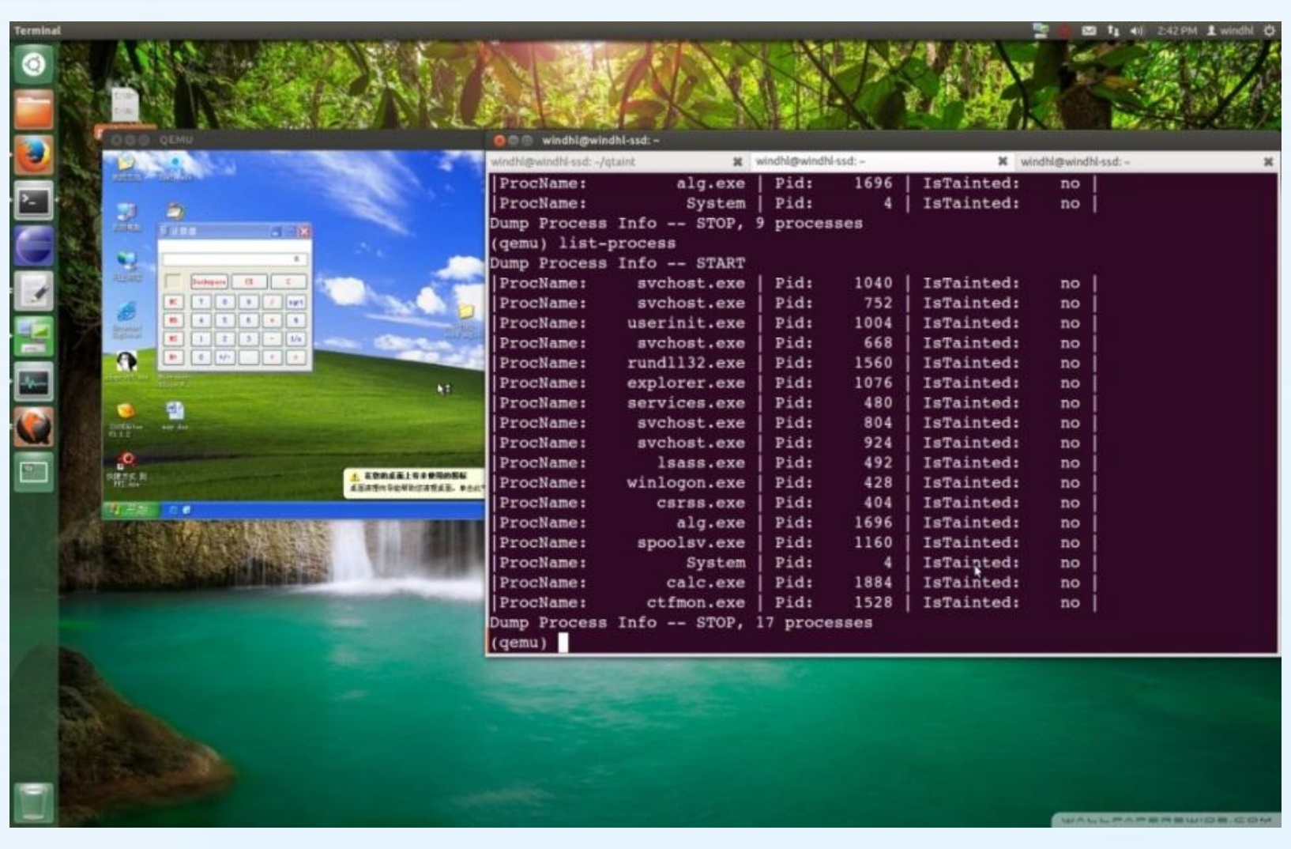
```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

termdd.sys

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFFA8013200048,0x0000000000000000,0xFFFFF88004C1DF95,0
x0000000000000002)


***    termdd.sys - Address FFFFF88004C1DF95 base at FFFFF88004C1B000, DateStamp
 4a5bce64


Collecting data for crash dump ...
Initializing disk for crash dump ...
```

“臭名昭著”的BlueKeep攻击

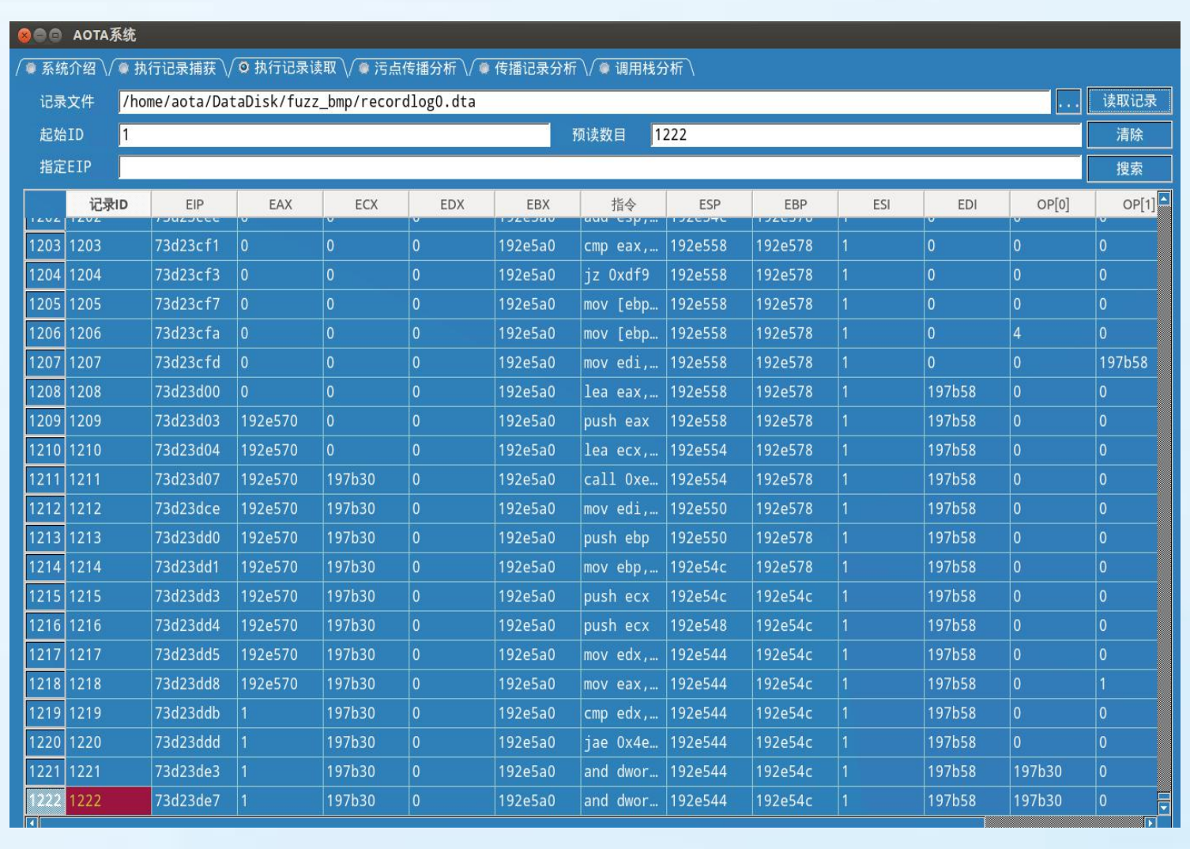


漏洞触发机理

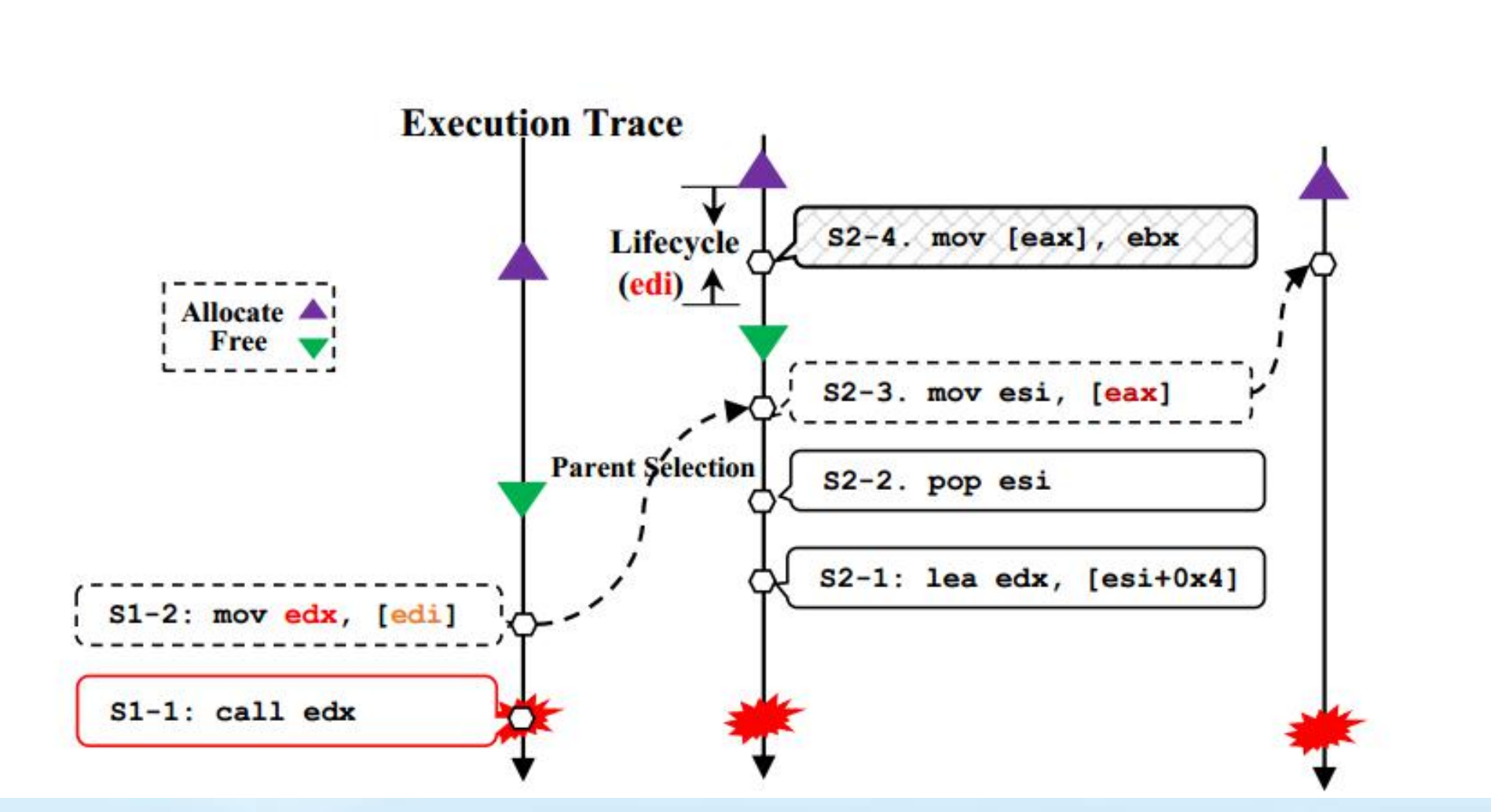
为此，我们通过监控释放后重用漏洞的主要触发阶段，归纳、总结各类导致该漏洞发生的原因，综合运用动态虚拟化监控、污点回溯分析、多级指针解引用以及内存对象引用计数关联等技术，实现了释放后重用漏洞的自动化分析能力。我们通过该技术自动化分析了操作系统内核（Linux和MacOS）、浏览器（IE和Chrome）等大规模软件中的百余个释放后重用漏洞，相关结果证明了该技术的有效性和可靠性。



① 程序动态监控

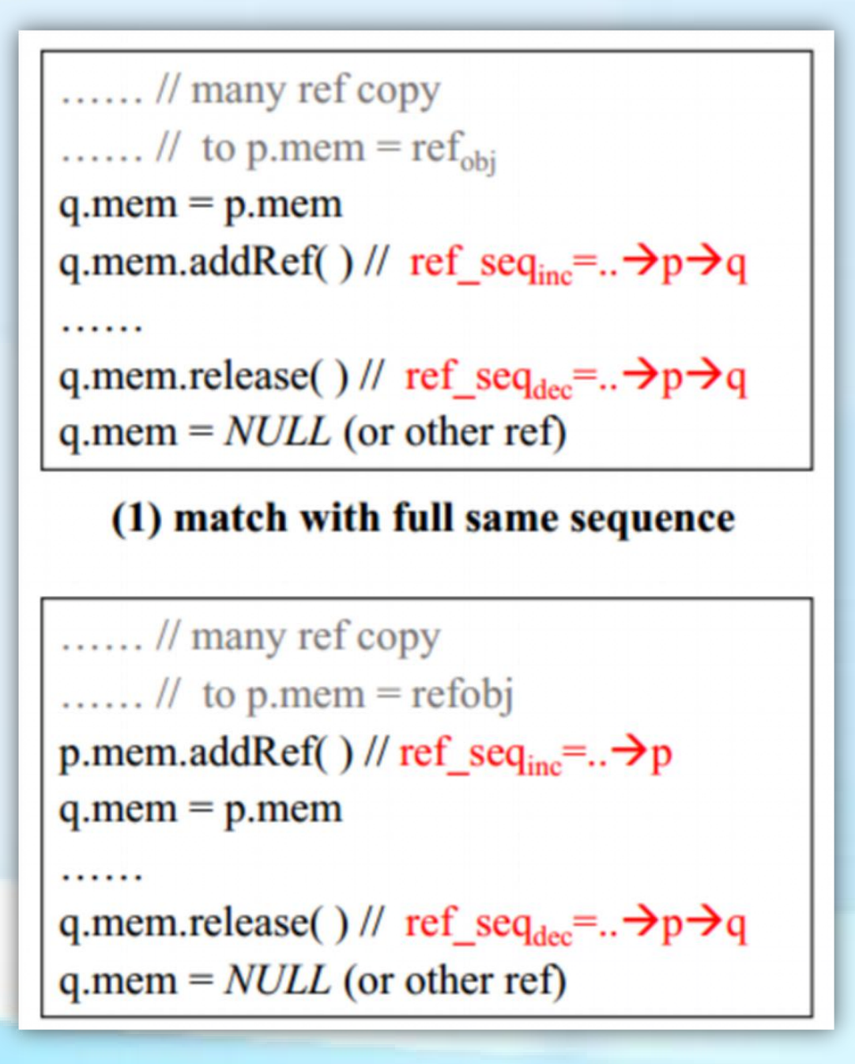


② 污点传播分析



③ 多级指针解引用

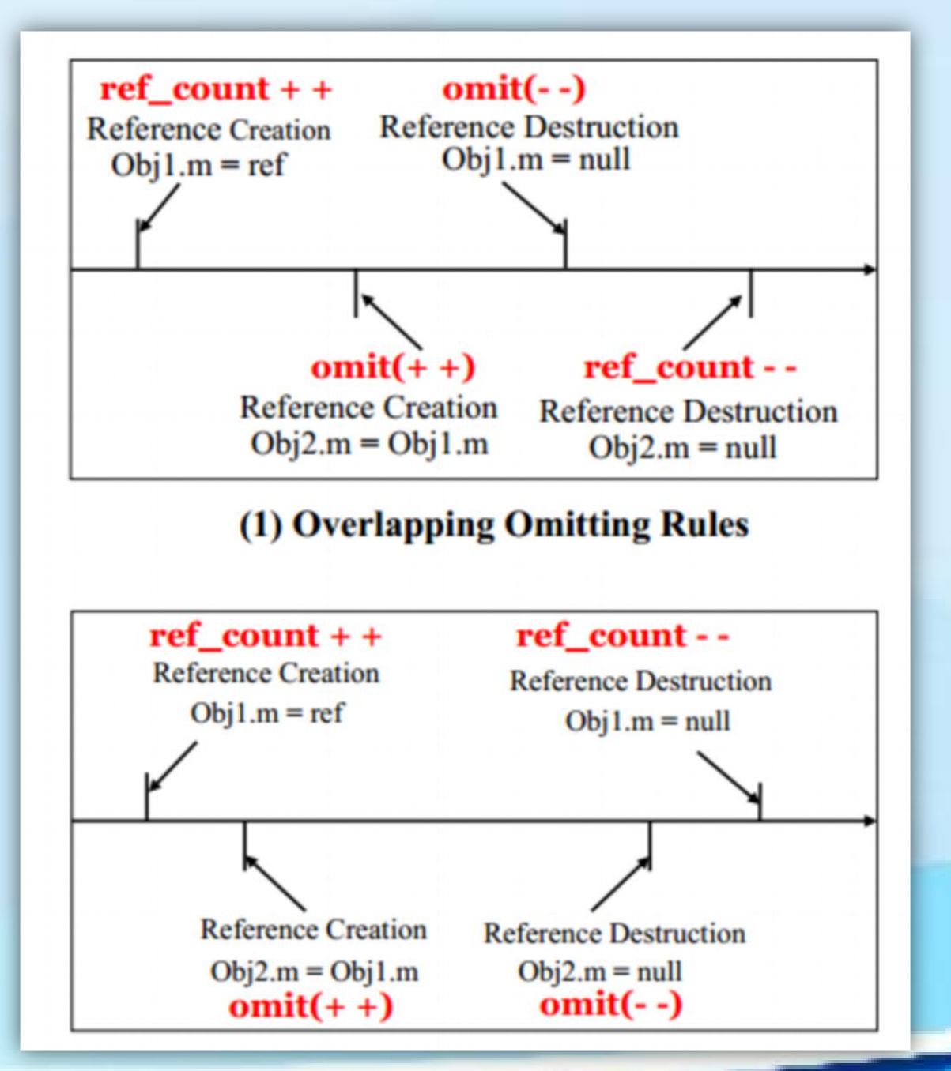
④ 内存对象引用计数关联



```
...... // many ref copy
...... //  to p.mem = ref_obj
q.mem = p.mem
q.mem.addRef( ) //  ref_seq_inc=..→p→q
......
q.mem.release( ) //  ref_seq_dec=..→p→q
q.mem = NULL (or other ref)
```

(1) match with full same sequence

```
...... // many ref copy
...... //  to p.mem = refobj
p.mem.addRef( ) // ref_seq_inc=..→p
q.mem = p.mem
......
q.mem.release( ) //  ref_seq_dec=..→p→q
q.mem = NULL (or other ref)
```



(1) Overlapping Omitting Rules

⑤ 成因自动化分析