学术论文

Towards Efficient Heap Overflow Discovery
堆溢出漏洞的有效挖掘

贾相堃、张超、苏璞睿✉、杨轶、黄桦烽、冯登国

USENIX Security 2017, 2017.8.16-8.18, pp. 989-1006.

{purui@iscas.ac.cn}

堆溢出漏洞是内存破坏漏洞的一种，目前已成为最具威胁的漏洞类型之一，如图1所示。

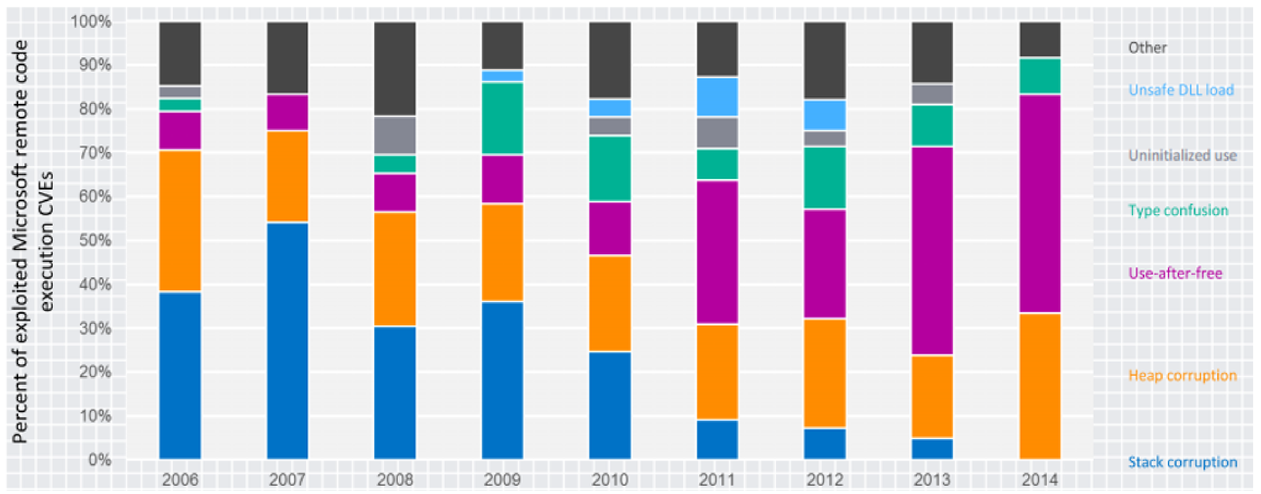

图1 2006-2014年漏洞利用趋势报告（微软）

堆溢出漏洞涉及到堆分配和访问两个方面。漏洞的发生条件是堆访问的范围超过了堆分配的范围，而堆溢出漏洞存在的根本原因是攻击者对堆分配或堆访问具有控制能力，此时正常访问的堆操作可能因为外部的恶意输入变为溢出访问的异常操作，如图2 所示。

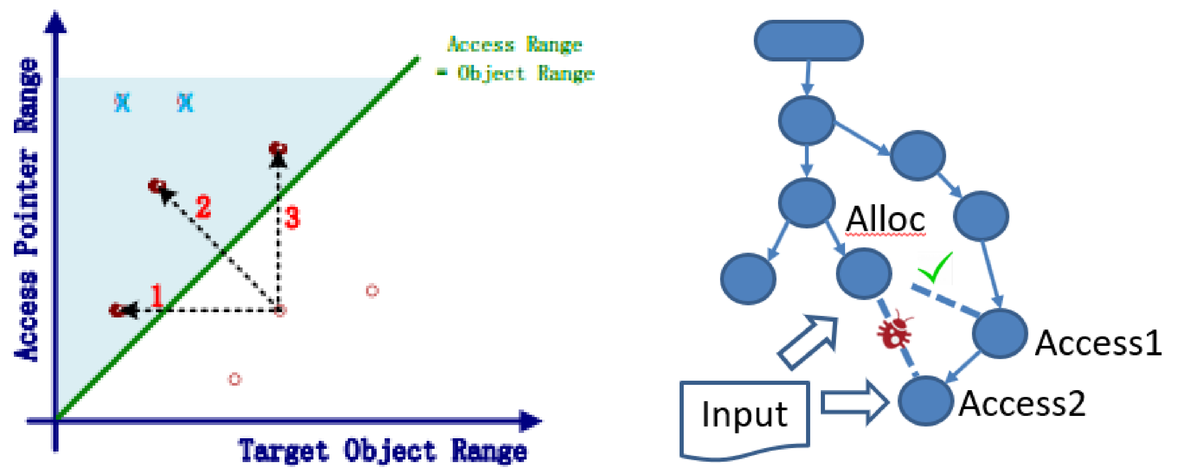

图2 堆溢出漏洞的关系模型

基于动态执行记录，可以分析与堆溢出漏洞相关的堆分配和访问操作，建立“分配-访问”之间的关系模型，同时跟踪堆操作的空间属性和可控属性，最终判断堆溢出漏洞的发生和潜在堆溢出的可能，如图4所示。

该方法形成了原型系统HOTracer，在实际程序中共发现了47个未知漏洞，涉及到Apple、Microsoft、腾讯等厂商，其中2个漏洞已获得了CVE编号（CVE-2016-6164 for ffmpeg, CVE-2016-9931 for RealPlayer），如图3所示。

ID (count)	Application	version	input	bug status
new (1)	Feiq	3.0.0.2	tcp	reported
new (1)	WMPlayer	12.0.7601	mp4	reported
new (3)	VLC	2.2.1	mp4	fixed
new (1)	VLC	2.2.4	mp4	reported
new (2)	iTunes	12.4.3.1	mp4	reviewing
new (1)	ffmpeg	c0cb53c	mp4	CVE
new (6)	QQPlayer	3.9(936)	mp4	rewarded
new (1)	QQMusic	11.5	m4a	rewarded
new (1)	BaiduPlayer	5.2.1.3	mp4	reviewing
new (2)	RealPlayer	16.0.6.2	mp4	CVE
new (1)	MPlayer	r37802	mp4	reported
new (3)	KMPlayer	3.9.1.138	mp4	fixed
new (4)	KMPlayer	4.1.1.5	mp4	reported
new (7)	Potplayer	1.6.60136	mp4	fixed
new (2)	Potplayer	1.6.62949	mp4	reported
new (5)	Splayer	3.7	mp4	reported
new (2)	MS Word	2007,10,16	rtf	reviewing
new (1)	WPS Word	10.1.0.5803	doc	reported
new (2)	OpenOffice	4.1.2	doc	reviewing
new (1)	IrfanView	4.41	m3u	fixed

图3 HOTracer发现的0day漏洞

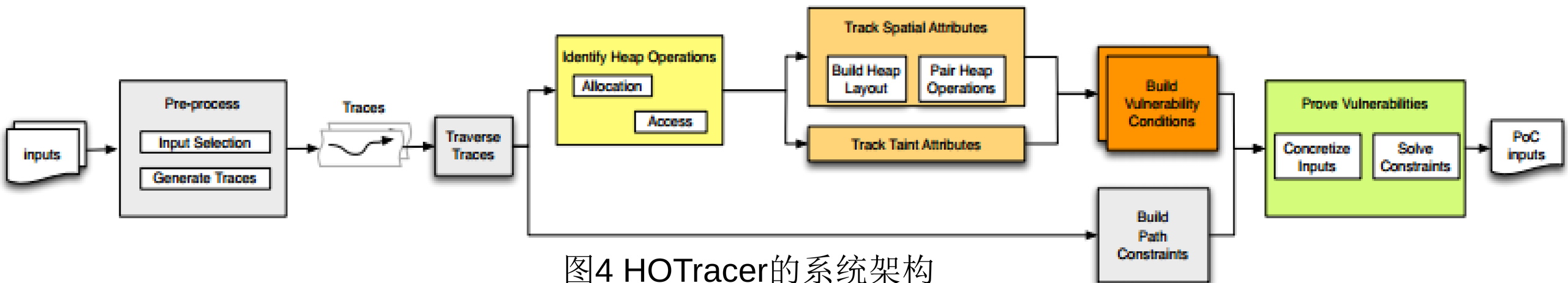

图4 HOTracer的系统架构