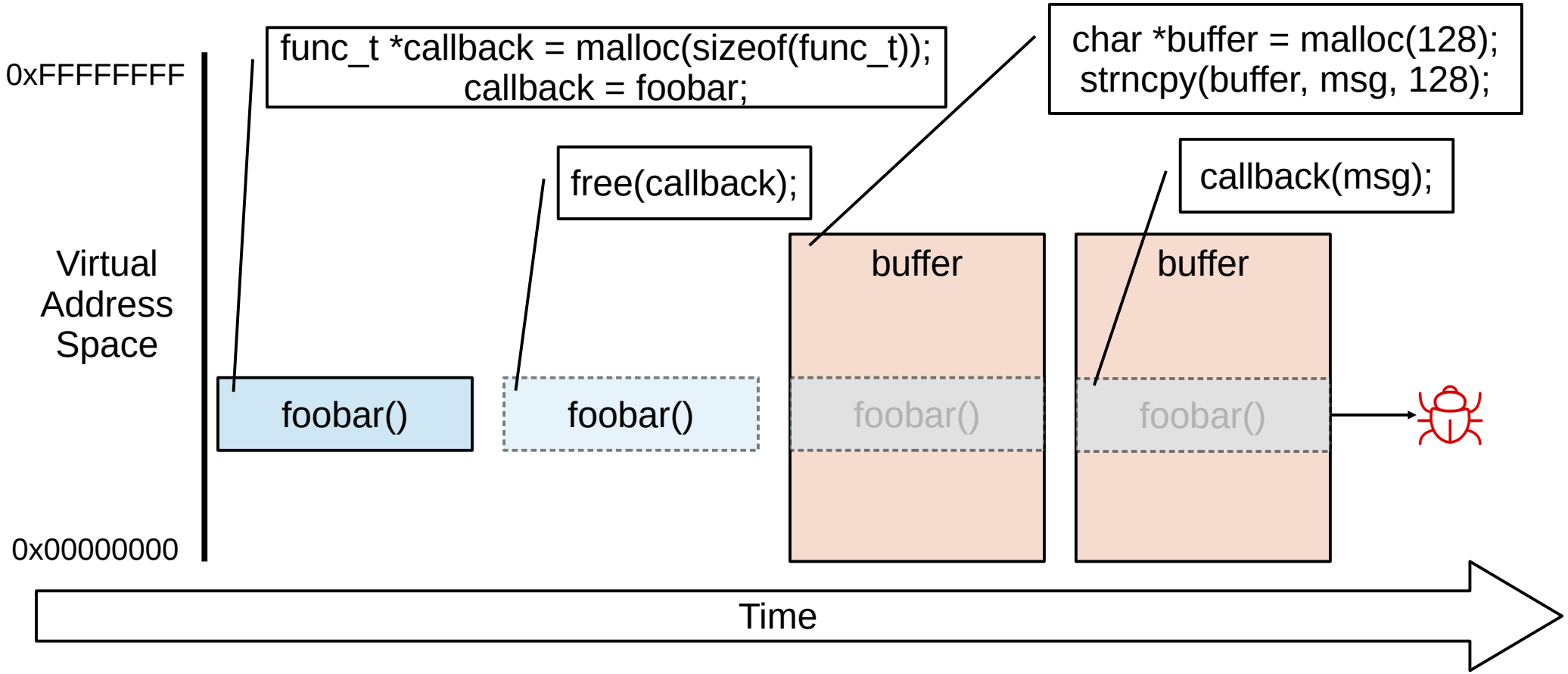
PUMM: Preventing Use-After-Free Using Execution Unit Partitioning

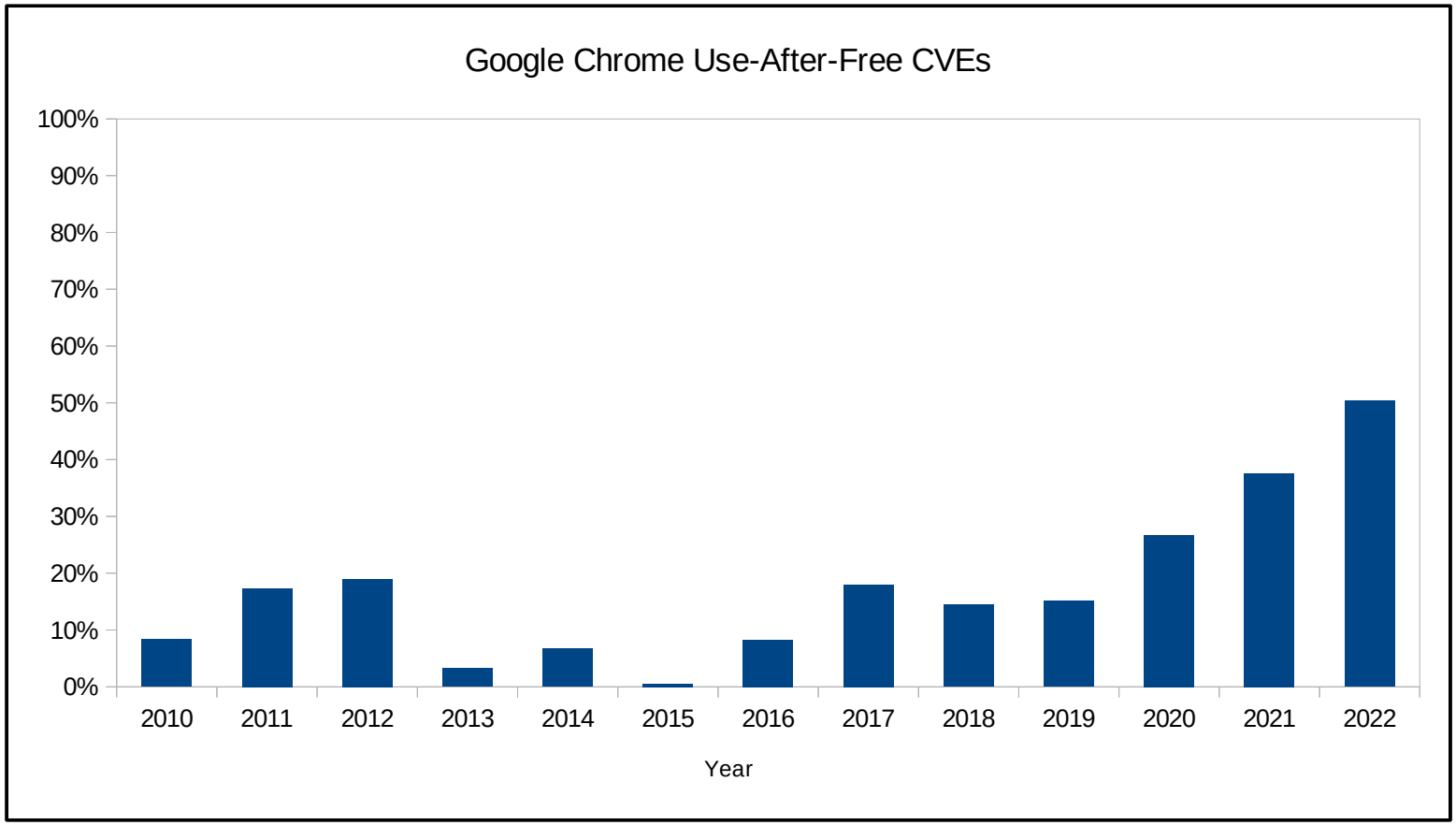
Carter Yagemann[†], Simon P. Chung,
Brendan Saltaformaggio, Wenke Lee

[†]Work done while at Georgia Tech

What is a Use-After-Free Vulnerability?

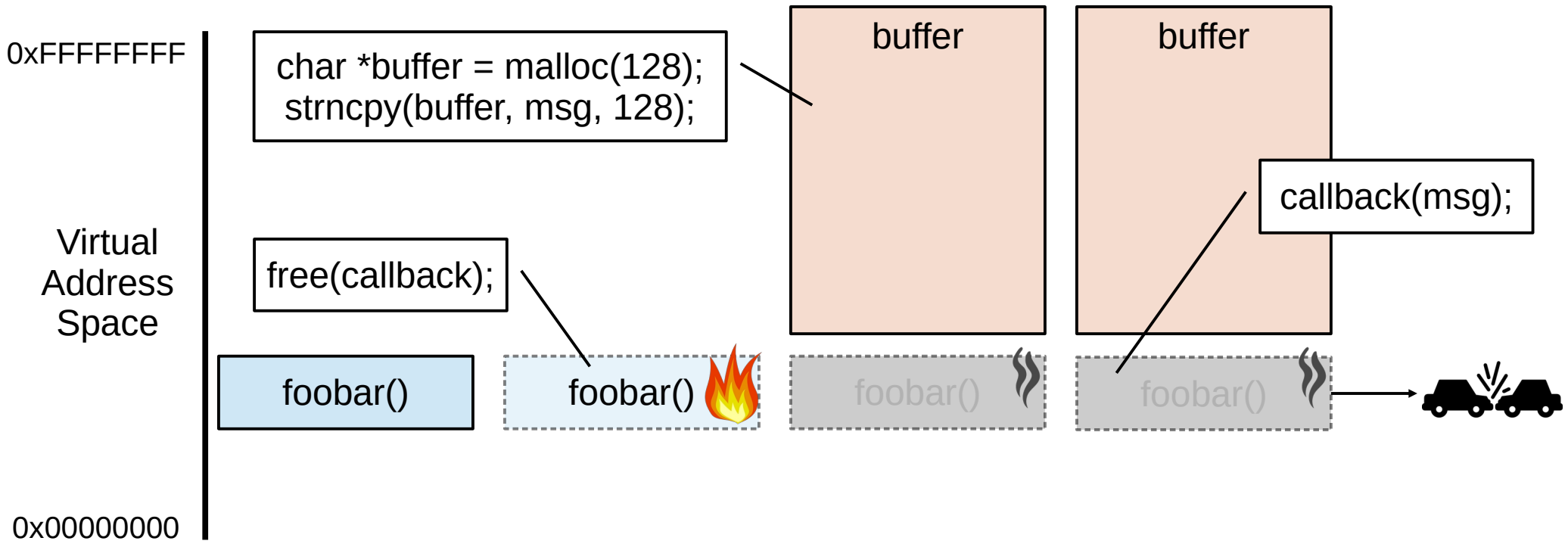


Prevalence of Use-After-Free

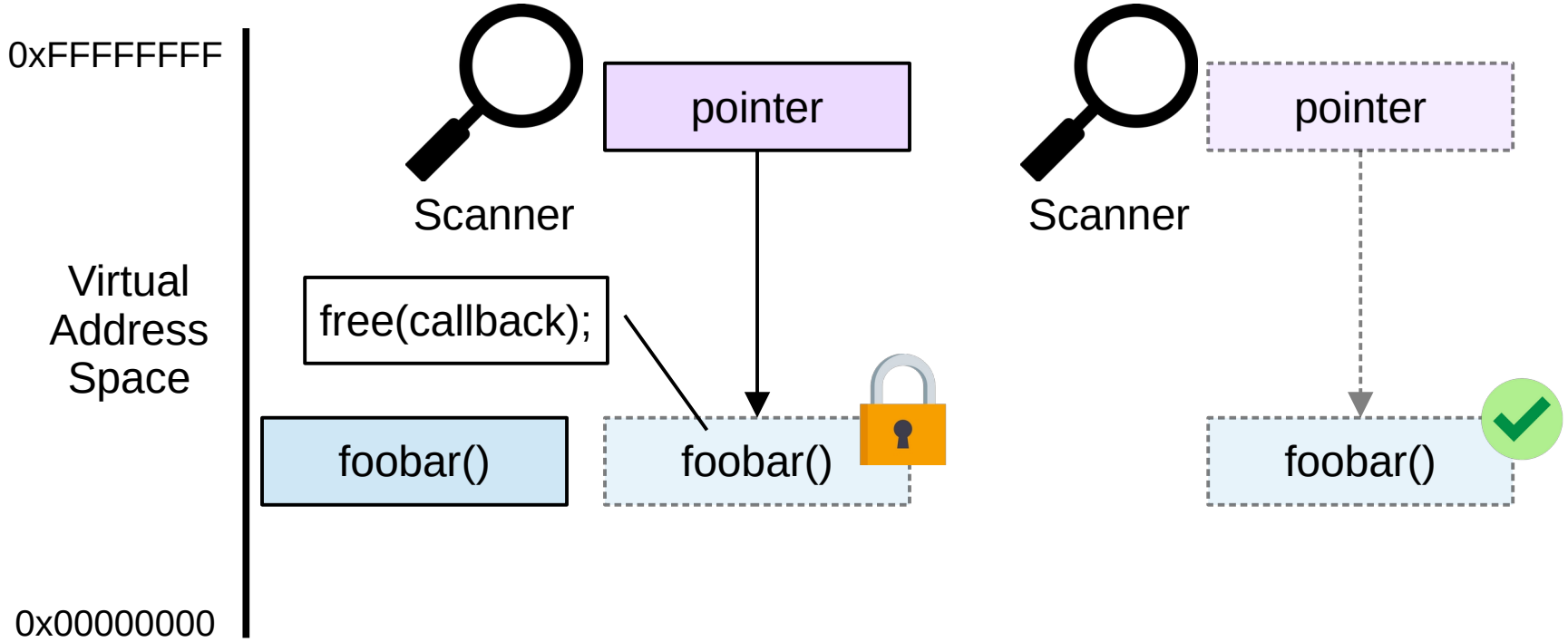


How do we solve this?

Prior Work: One-Time Allocation



Prior Work: Retrofit Garbage Collection



Goal

One-Time Allocation

[+] Secure
[-] Exhausts AS

Retrofit GC

[+] Releases AS
[-] False Positives

(*AS: address space)

Is there a way to quarantine addresses *just* long enough?

Key Insight: “Units of Work”

Alice’s Request

Bob’s Request

Charlie’s Request

Alice’s Request

Charlie’s Request

Bob’s Request

. . .

Developers minimize dependencies between tasks!

Hypothesis

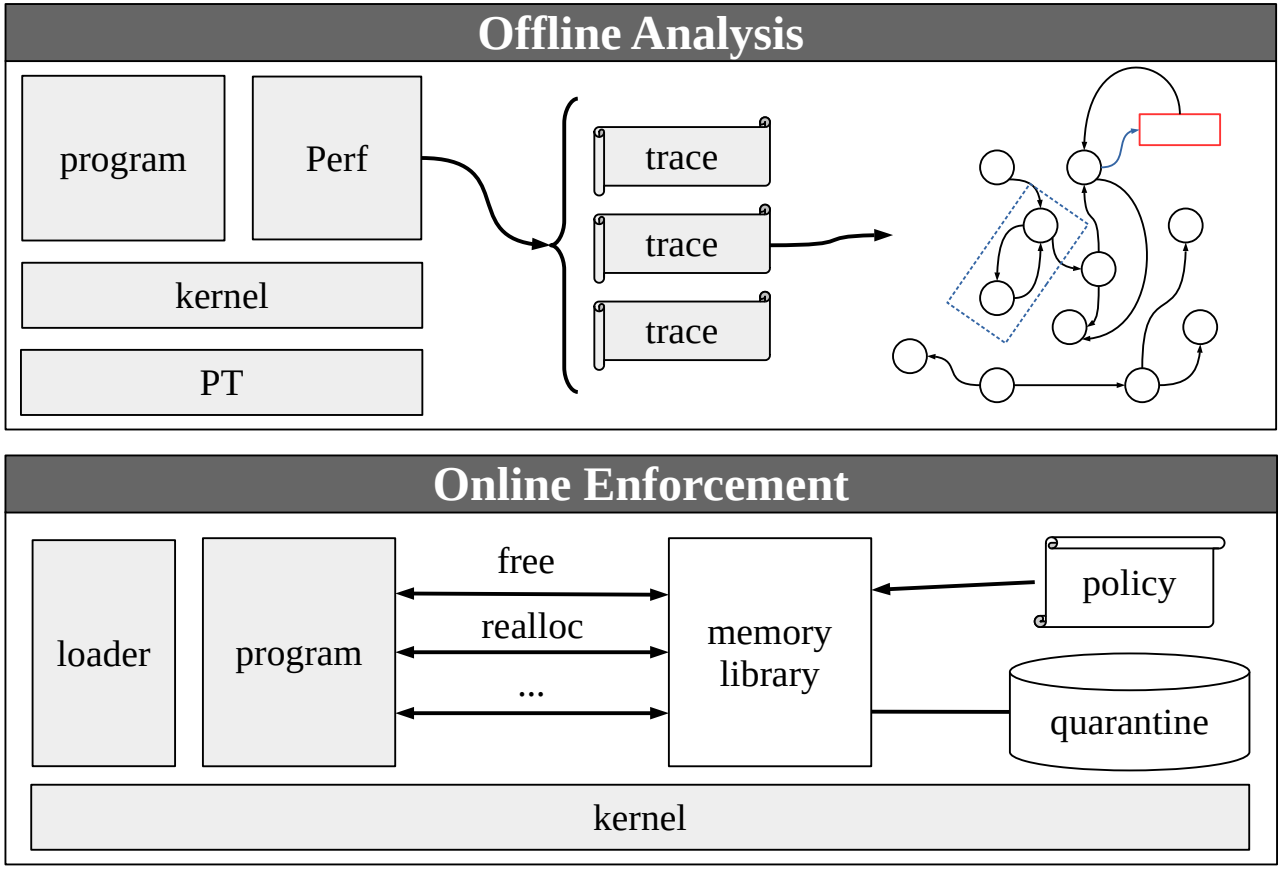
Use-after-frees occur across **dependencies**.

If two codes share **no dependencies**, they share **no use-after-frees**.

Developers **minimize dependencies between tasks**.

∴ Developers minimize the likelihood of use-after-frees across tasks. ∎

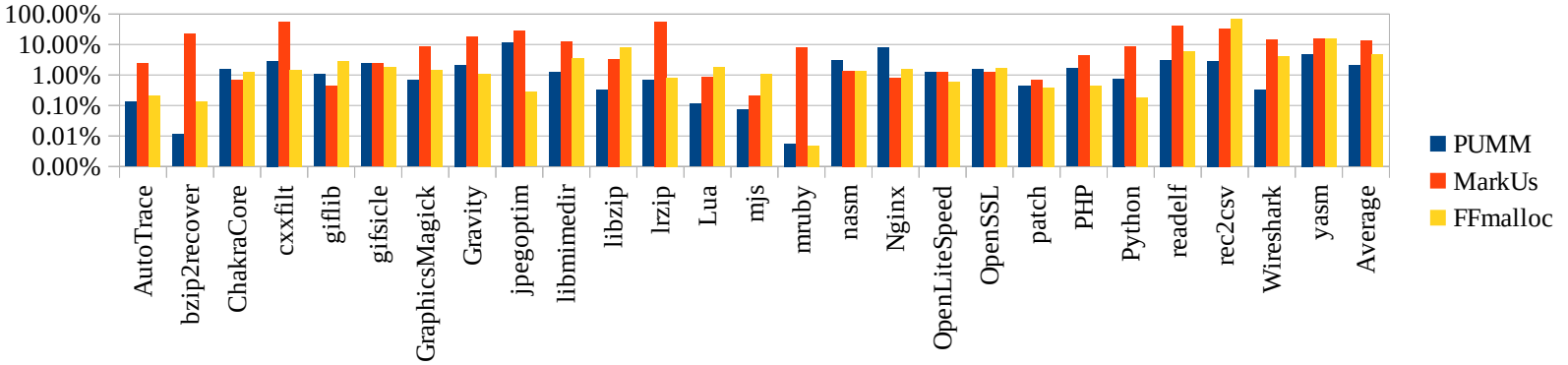
Architecture



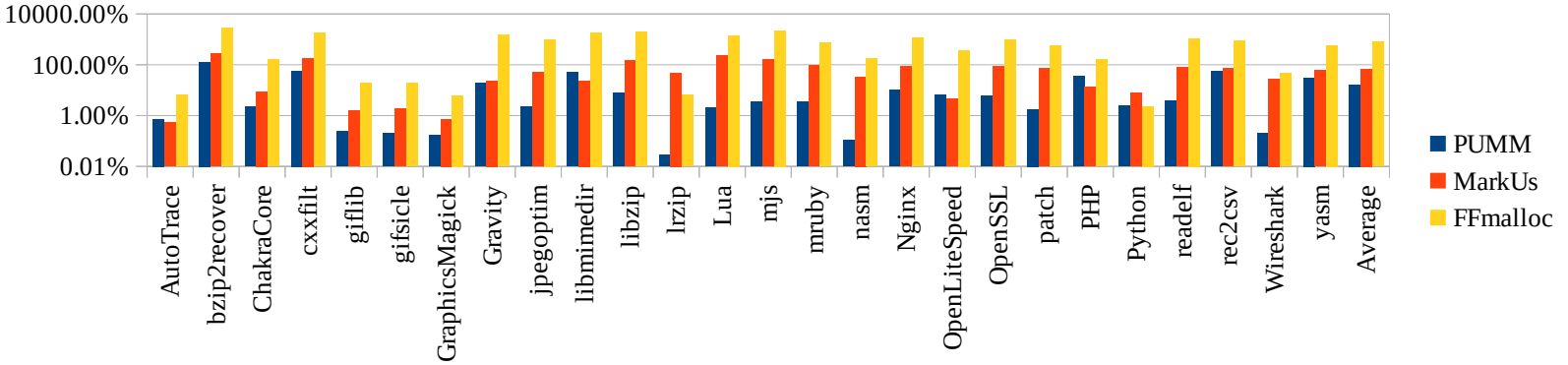
Prevented UAF Vulnerabilities (40 vulnerabilities, 26 programs)

CVE-2016-3189	bzip2recover	6.5 Medium
CVE-2016-4487	cxxfilt	5.5 Medium
CVE-2017-10686	nasm	7.8 High
CVE-2018-10685	lrzip	9.8 Critical
CVE-2018-11496	lrzip	6.5 Medium
CVE-2018-11416	jpegoptim	8.8 High
CVE-2018-20623	readelf	5.5 Medium
CVE-2019-20633	patch	5.5 Medium
CVE-2019-6455	rec2csv	6.5 Medium
Issue 74	giflib	
Issue 122	gifsicle	
Issue 73	mjs	
Issue 78	mjs	
Issue 91	yasm	
CVE-2015-2787	PHP	7.5 High
CVE-2015-6835	PHP	9.8 Critical
CVE-2016-5773	PHP	9.8 Critical
Issue 3515	mruby	
CVE-2015-3205	libmimedir	7.5 High
Issue 144	Gravity	
Issue 24613	Python	
CVE-2019-0568	ChakraCore	7.5 High
CVE-2020-24346	Nginx	7.8 High
CVE-2017-9182	AutoTrace	7.5 High
CVE-2017-9190	AutoTrace	7.5 High
CVE-2019-19005	AutoTrace	7.8 High
CVE-2017-11139	GM	9.8 Critical
CVE-2017-11403	GM	8.8 High
CVE-2017-12936	GM	8.8 High
CVE-2017-14103	GM	8.8 High
CVE-2017-15238	GM	8.8 High
CVE-2017-18220	GM	8.8 High
CVE-2017-12858	libzip	9.8 Critical
CVE-2019-17582	libzip	9.8 Critical
CVE-2019-6706	Lua	7.5 High
CVE-2015-3890	OLS	7.5 High
CVE-2010-2939	OpenSSL	4.3 Medium
CVE-2015-8727	Wireshark	5.5 Medium
EDB-39503	Wireshark	
EDB-39529	Wireshark	

Performance



2.04% Performance Overhead



16.48% Memory Overhead

Thank You!

Carter Yagemann

yagemann.1@osu.edu
carteryagemann.com