usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

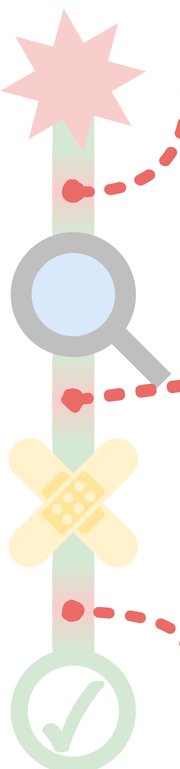
Attacker Control and Bug Prioritization

Guilhem LACOMBE
guilhem.lacombe@univ-grenoble-alpes.fr
UGA Université Grenoble Alpes Verimag — université PARIS-SACLAY — cea list

Sébastien BARDIN
sebastien.bardin@cea.fr
université PARIS-SACLAY — cea list

PROBLEM

A bug's life



Discovering bugs

Automated bug-finding: fuzzing, symbolic execution...
Effective, practical, lots of research

Large-scale public efforts: Syzbot, OSS-Fuzz

!!! too many reports, exact threat unclear !!!

Fixing bugs

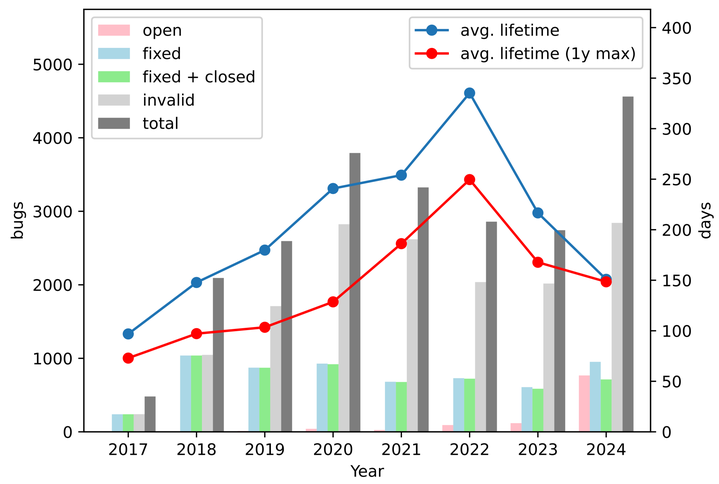
Automated bug-fixing? patterns? machine learning?
Still a long way away...

!!! scalability, limited manpower, motivation !!!

Propagating patches

!!! unclear threat ⇒ delays !!!

Syzbot: bugs per year of discovery



2018 ➜ 2023: +47% post-discovery lifetime!

Quick discovery is pointless (dangerous?) without quick resolution.

We need automated, precise, scalable and explainable prioritization!

METHOD

Out-of-the-box approaches are lackluster

	Automated	Correct	Explainable
Human	✗	✓?	✓
Vuln. types	✓	✗	✓
AEG	✓	✓/✗	✓
ML	✓	✗	✗
Us	✓	✓	✓

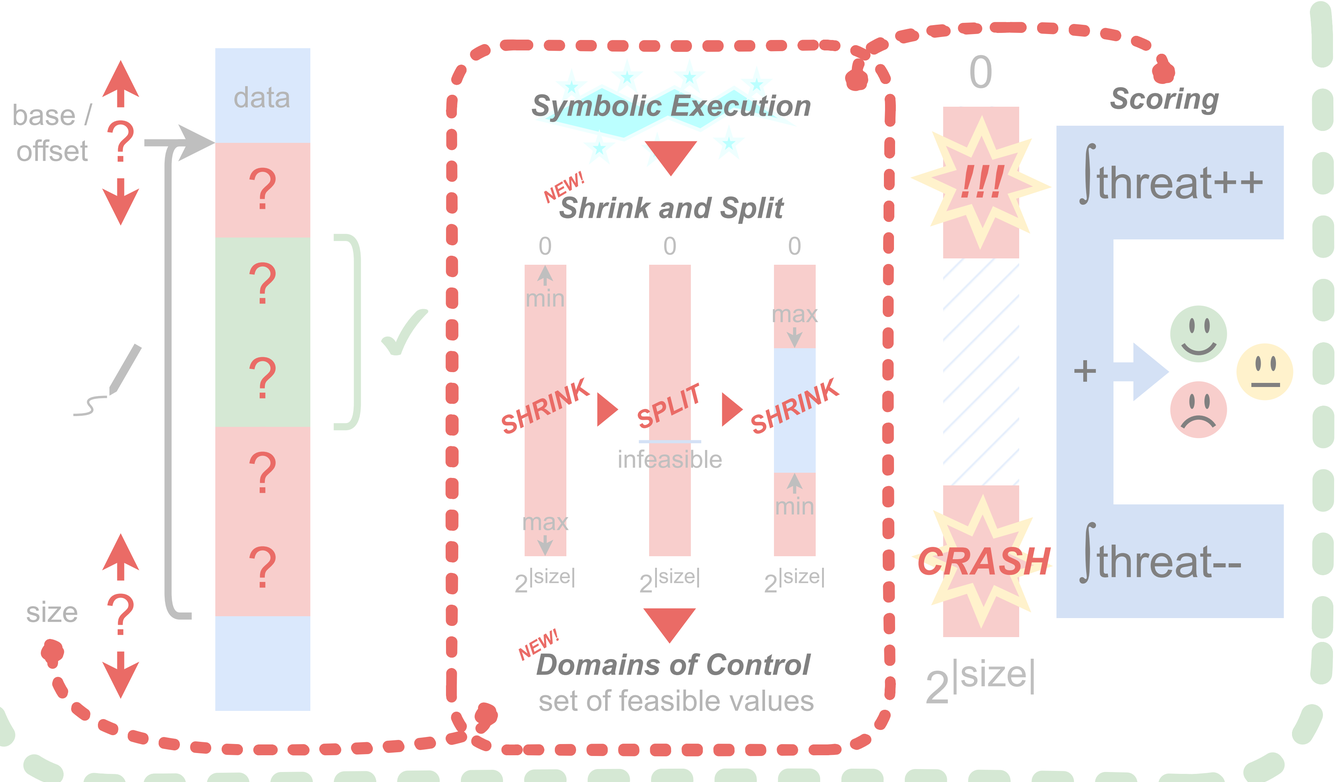
Our approach

Use **formal methods** to evaluate **well-defined aspects of exploitability**

Key Notion: *Attacker Control*

An attacker's ability to tailor vulnerabilities to their needs by choosing their parameters

Illustration on an Out-Of-Bounds Write



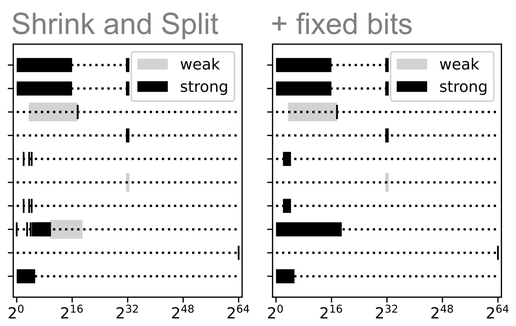
RESULTS

Research questions

How ***precise*** is our approach?

How ***practical*** is out approach?

Visualization of domains of control for some CVEs



Ranking CVEs

issue with prior analysis!!!

Vulnerability	CVSS	Expect	Us
OOB writes			
cve-2021-3246	😟	😟	😟
cve-2019-14192	😟	😟	😟
cve-2019-14202	😟	😟	😟
cve-2022-30790	😟	🙂	🙂
cve-2022-30552	😐	🙂	🙂
cve-2022-30790-2	-	😐	😐
OOB reads			
cve-2023-37837	😐	😟	😟
heartbleed	😟	😟	😟
Code ptr corr.			
cve-2021-26567	😟	🙂	🙂
cve-2020-14393	😟	😟	😟
cve-2024-41881	😟	🙂	🙂
cve-2024-43700	😟	🙂	🙂
cve-2023-43338	😟	😟	😟

Ensuring practicality through automation

OOB CVEs from the MAGMA fuzzing benchmark

No manual analysis / instrumentation