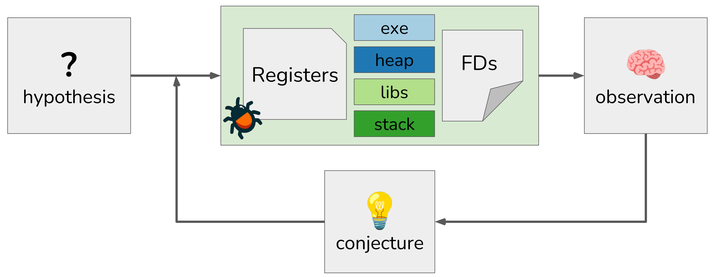
libdebug, Build Your Own Debugger for a Better (Hello) World!

Gabriele Digregorio — gabriele.digregorio@polimi.it
Roberto Alessandro Bertolini — robertoalessandro.bertolini@mail.polimi.it
Francesco Panebianco — francesco.panebianco@polimi.it
Mario Polino — jinblack@libdebug,org

POLITECNICO MILANO 1863

Context and Motivation

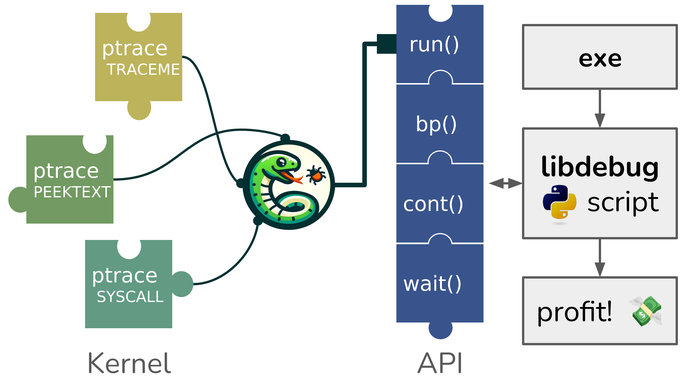
Debugging is a **hypothesis verification process**[1,2], commonly applied to reverse engineering, exploitation, and other fields.



Debugging requires **programmability**, **performance**, **flexibility**, and **reproducibility**, but current user space solutions do not provide those[3].

Your Own Debugger

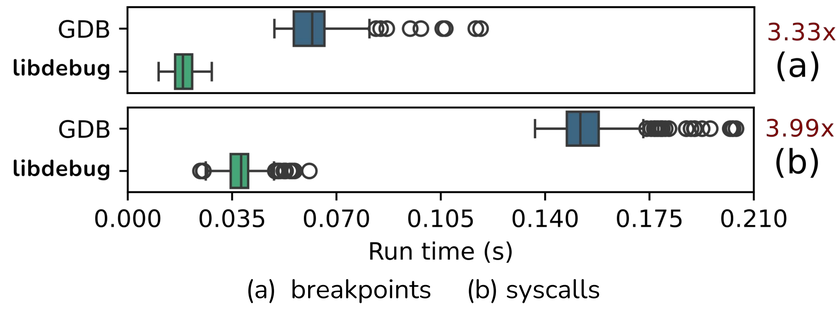
libdebug provides the building blocks for your **custom debugging workflows**.



libdebug *abstracts* all arch-specific differences[4,5].

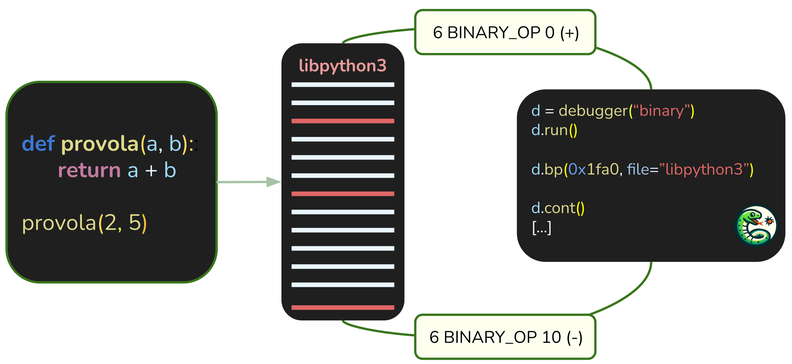
Evaluation

Performance can be **crucial** during debugging, especially **when tracing** repeated **operations**.

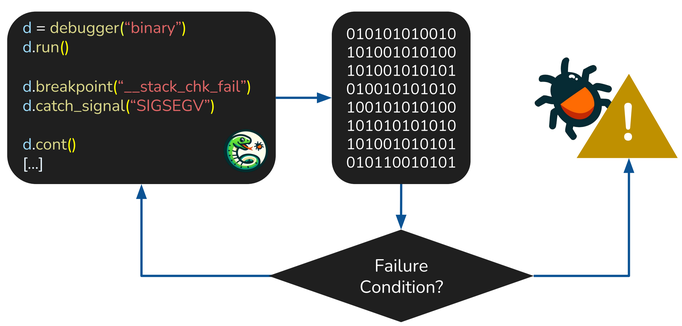


libdebug is more than **3 times faster** than GDB [6], with a **shorter script length**.

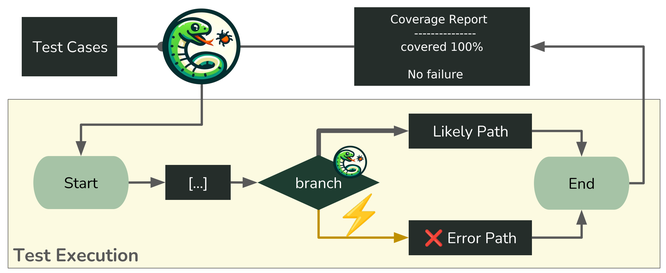
Reverse Engineering



Software Security



Testing and Coverage



[1] Andreas Zeller. 2009. Why programs fail: a guide to systematic debugging. Morgan Kaufmann.
[2] Andreas Zeller. 2024. The Debugging Book. CISPA Helmholtz Center for Information Security. https://www.debuggingbook.org/
[3] Omar Sandoval. 2023. Live userspace process debugging #320. https://github.com/osandov/drgn/issues/320
[4] 1999. ptrace source code. https://github.com/torvalds/linux/blob/master/kernel/ptrace.c
[5] Microsoft Corporation. 2023. Debugging Functions. https://learn.microsoft.com/en-us/windows/win32/debug/debugging-functions
[6] Richard Stallman, Roland Pesch, Stan Shebs, and others. 1988. Debugging with GDB. Free Software Foundation, Inc. 675 (1988).

Future Work

OS · CPU

POLITECNICO MILANO 1863
NECST laboratory