

Extended CTF

- Some Modern IS Tools
 - By M4x@10.0.0.55

Why Play CTF?

- Learn vulnerabilities quickly(MSRC)
- Inspire new ideas(SROP, BROP, house of *, ...)
- Make friends
- A bridge between theory and reality
- It's so INTERESTING(打怪, 升级, 吊打全场)

Modern CTF

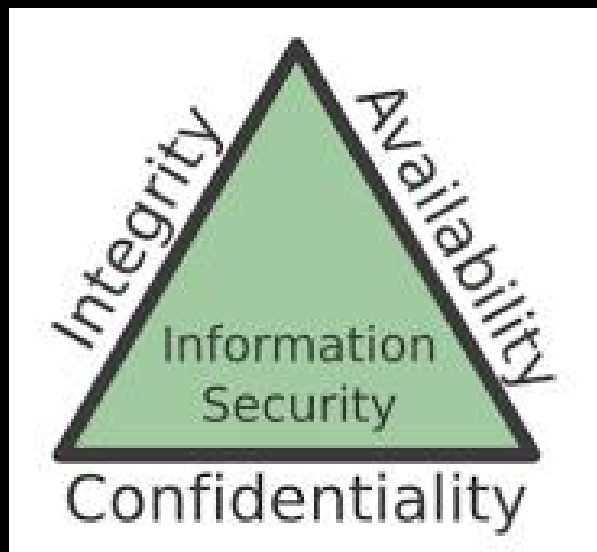
- QWB2018 - xx_game
- CGC超级挑战赛
- Defcon final
- pwn2own
- ...

结构原来越复杂
环境越来越真实
代码量越来越大
漏洞越来越隐蔽



What Are Vulnerabilities?

Errors introduced in the **design or implementations** of **software/system/hardware/protocol/algorithms**, that **could be exploited** to break victims' **CIA** attributes.



机密性C: Heartbleed, meltdown, spectre

完整性I: Man-in-the-middle attack

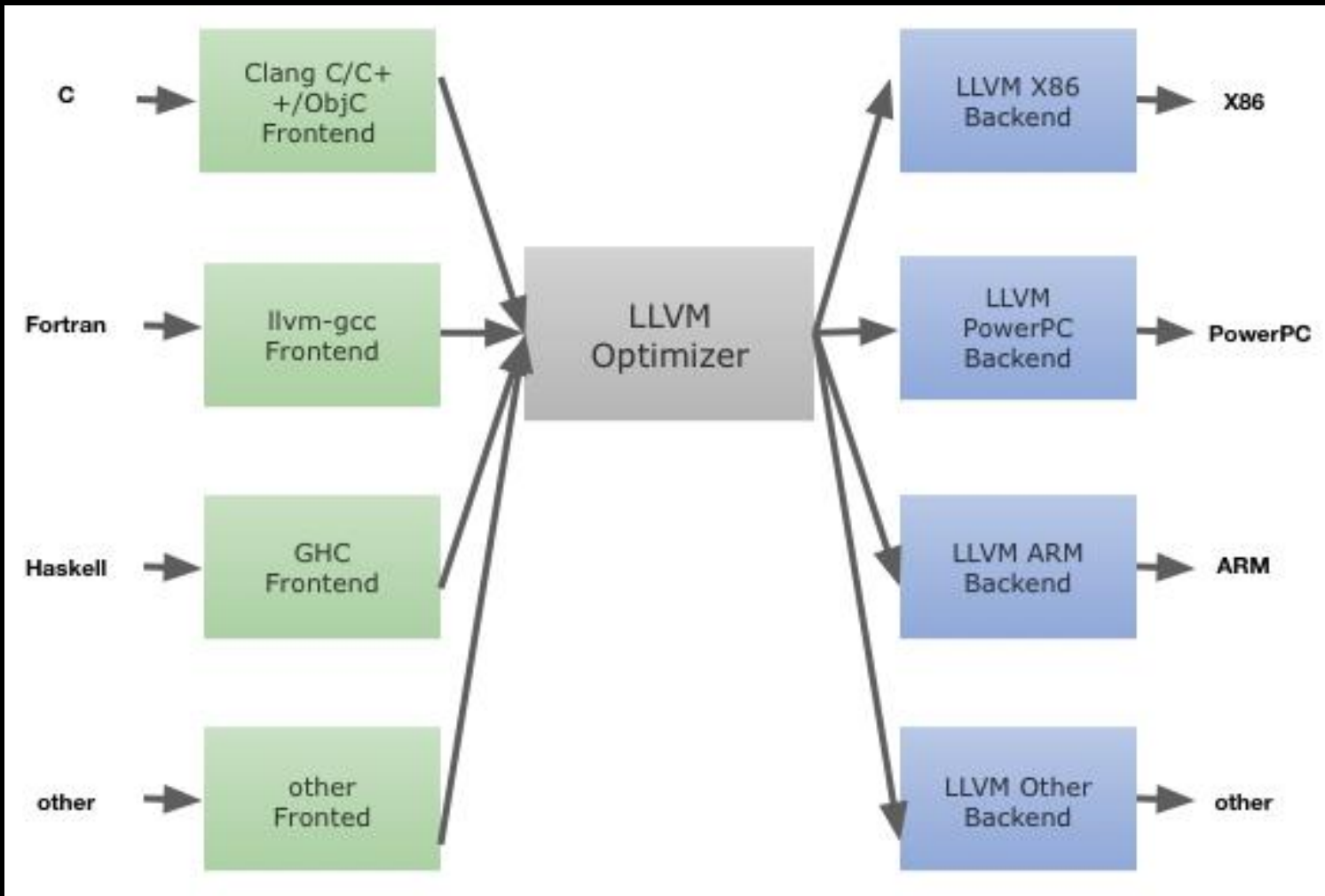
可用性A: DDOS, CC, crash

Modern Tools

- LLVM(`clang`)
- `qemu`
- `unicorn`
- ...



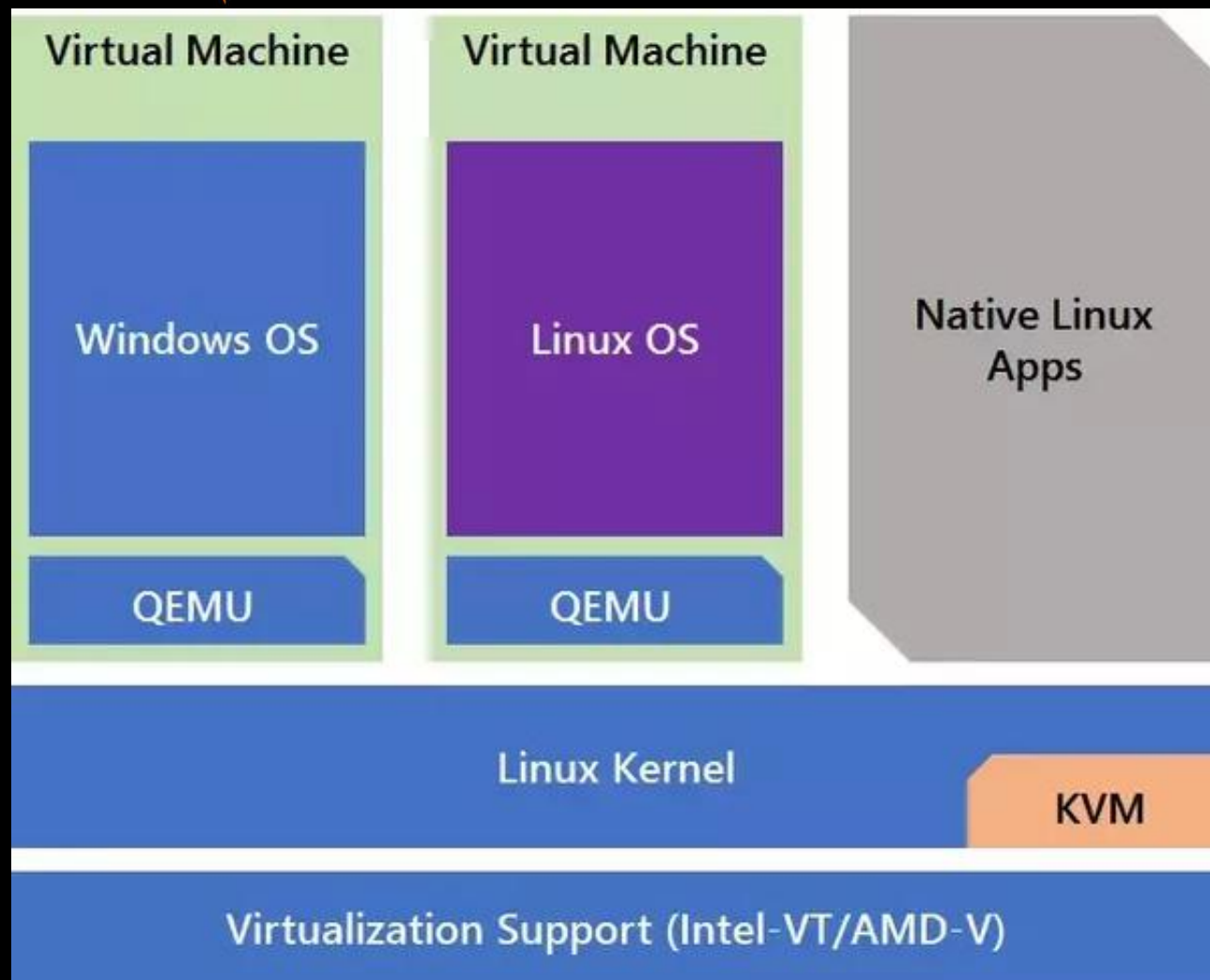
Low-Level-Virtual-Machine



- 编译器基础设施
- 为了任意一种编程语言
- IR



qemu



- 模拟处理器
- the FAST! processor emulator



Unicorn

- 无法模拟整个程序
- 不支持系统调用
- 需要手动映射内存

Unicorn

nccgroup



*"...a lightweight multi-platform,
multi-architecture CPU emulator framework"*

<http://www.unicorn-engine.org>
<https://github.com/unicorn-engine/unicorn-engine>

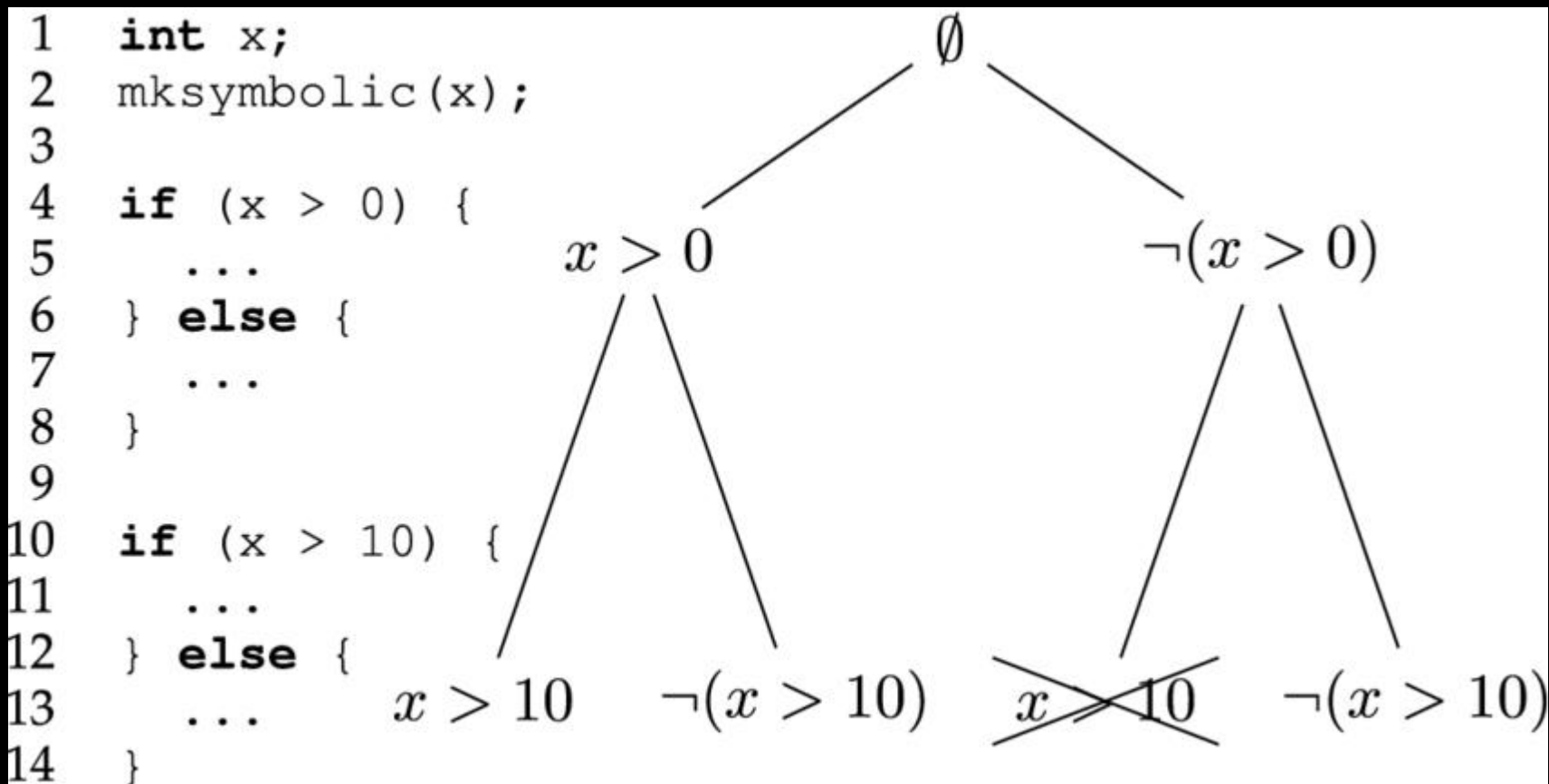


Modern Teches

- 符号执行 (z3, angr)
- 污点分析
- 插桩 (pintool)
- 模糊测试 (af1, peach, libFuzzer)
- ...

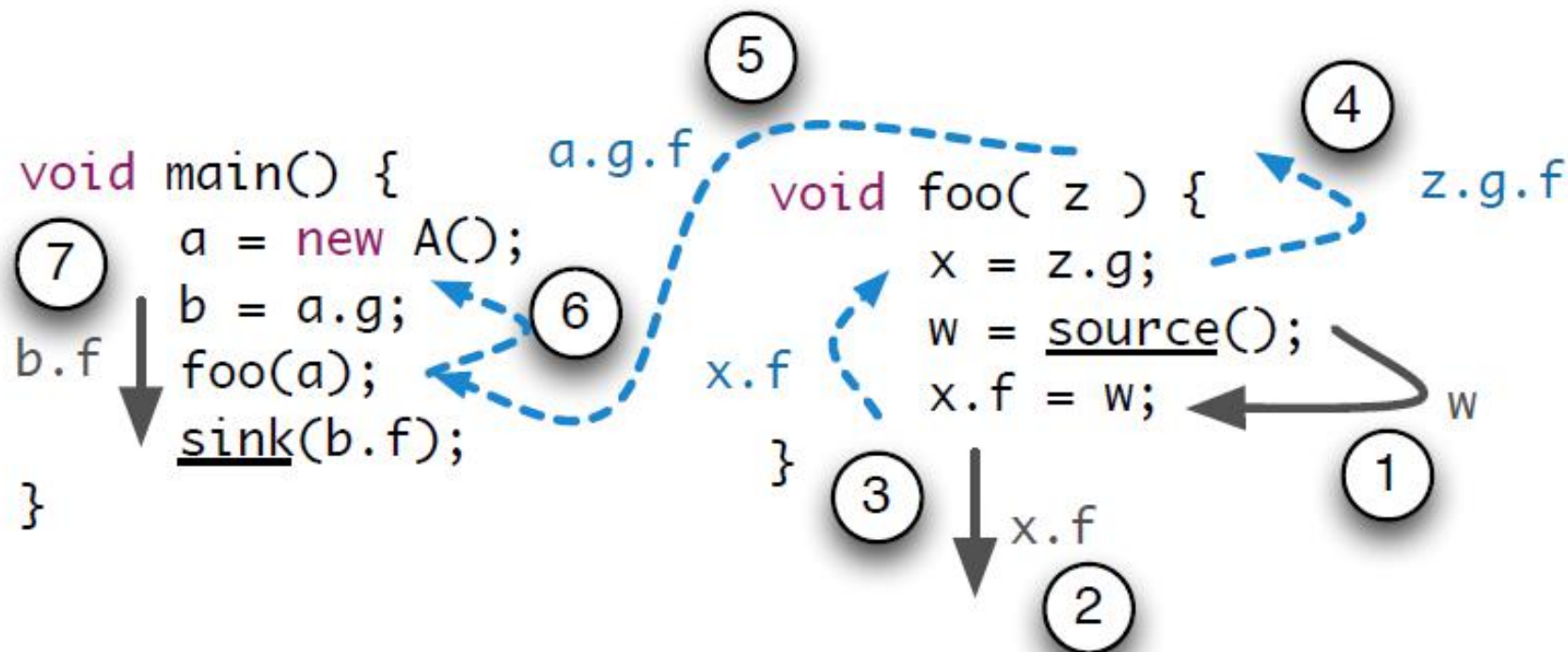


Symbolic Execution



- 符号
- 约束(Constraints)
- 解方程?

Taint Analysis



- 污点
- 信息流



Instrument

```
mov  eax, [eax+0x40]
call 0deadbeefh
cmp  ecx, edx
jz    0caffbabeh
```



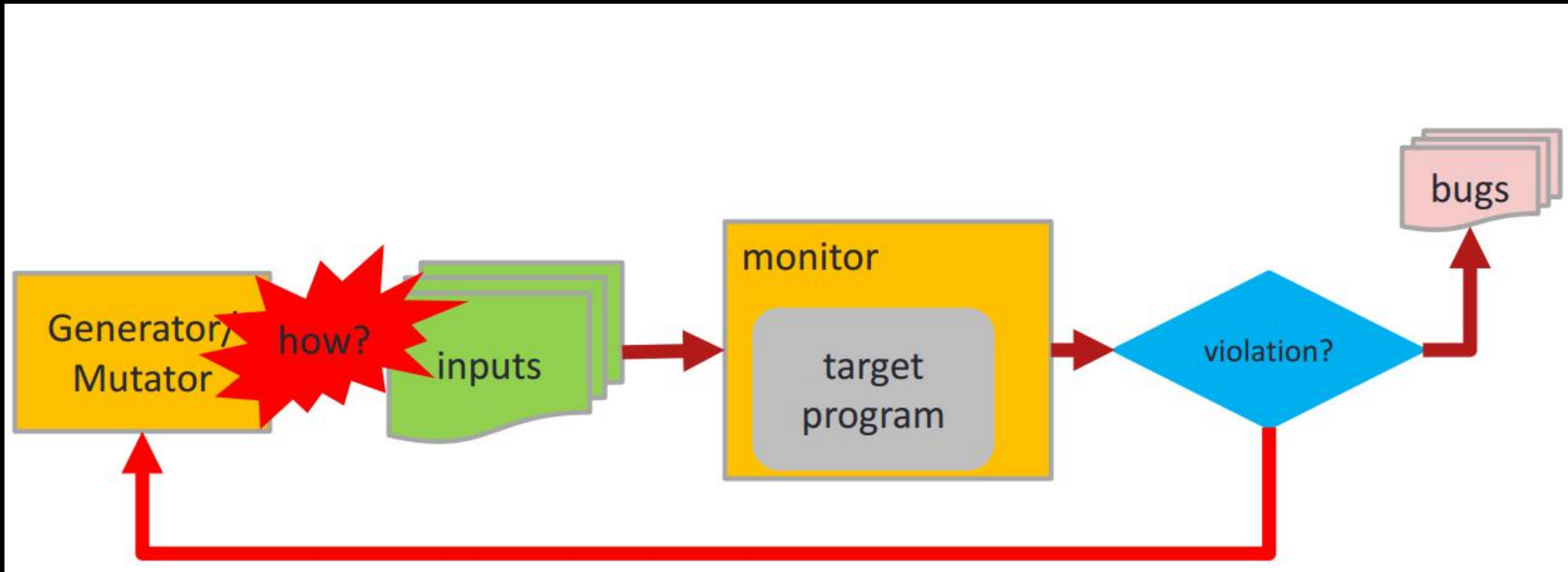
```
some code (memory access range)
some code (cache hit rate)
    mov  eax, [eax+0x40]
some code (callee name)
some code (invocation count)
    call 0deadbeefh
some code .. .. .
some code .. .. .
    cmp  ecx, edx
some code (prediction hit rate)
Some code (list of branch targets)
    jz    0caffbabeh
```

[Definition Source: Intel PIN manual](#)

- 探针/桩
- 粒度



Fuzz



- Seeds
- Binary
- mutate
- crash

And more and more teches and tools are coming up

