DigApis
安全
让你拥有无限可能

漏洞攻防：自动化与智能化

丁牛科技网安实验室
张云涛博士

DigApis
安全
让你拥有无限可能

目录
CONTENTS

1

漏洞攻防形势

安全事件时有发生，漏洞危害不容忽视

DigApis 安全 让你拥有无限可能

ROARTALK 嘶吼

网络安全攻击

- 2018年2月，上海某公立医院HIS系统被黑，勒索2亿“以太币”。
- 2018年3月，思科高危漏洞被黑客利用发动攻击，国内多家机构中招，配置文件被清空。
- 2018年5月，恶意软件VPNFilter影响范围覆盖全球54个国家，超过50万台路由器和网络设备。

数据泄露事件

- 2018年6月，弹幕视频网AcFun公告，因网站受黑客攻击，已有近千万条用户数据外泄。
- 2018年8月，安全人员通过暗网监测到浙江省1000万条学籍数据正在暗网上售卖。
- 2018年8月，华住旗下多个连锁酒店开房信息数据正在暗网出售，数据总数近5亿。

其它安全事件

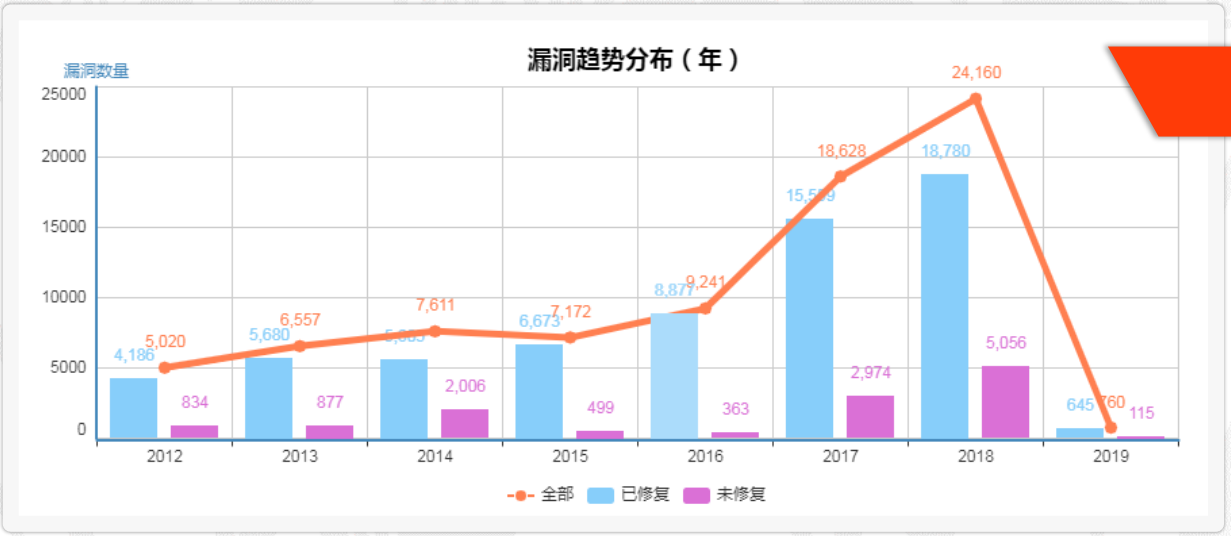
- 2018年1月，英特尔处理器曝“Meltdown”和“Spectre漏洞”。
- 2018年2月，苹果IOS iBoot源码泄露。
- 2018年5月，区块链平台EOS现史诗级系列高危安全漏洞。
- 2018年9月，新型僵尸勒索软件Virobot通过微软Outlook广泛传播。
- 2018年12月，“微信支付”勒索病毒曝光，10万多台电脑被感染。

漏洞数量庞大，且呈逐年上升的趋势

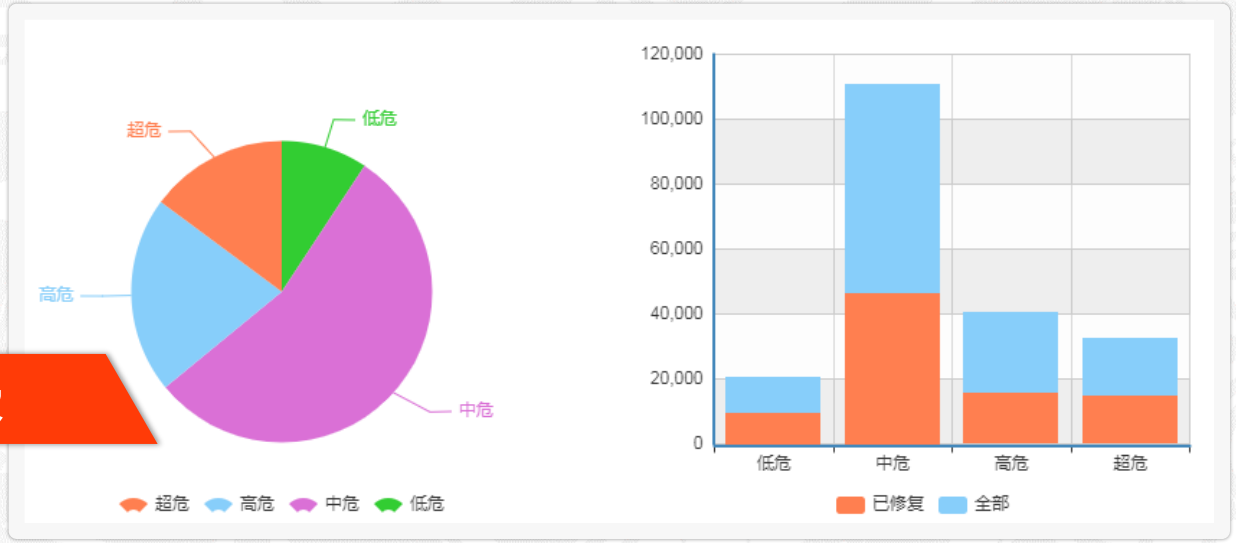
DigApis 安全
让你拥有无限可能

ROARTALK 嘶吼

漏洞分布趋势



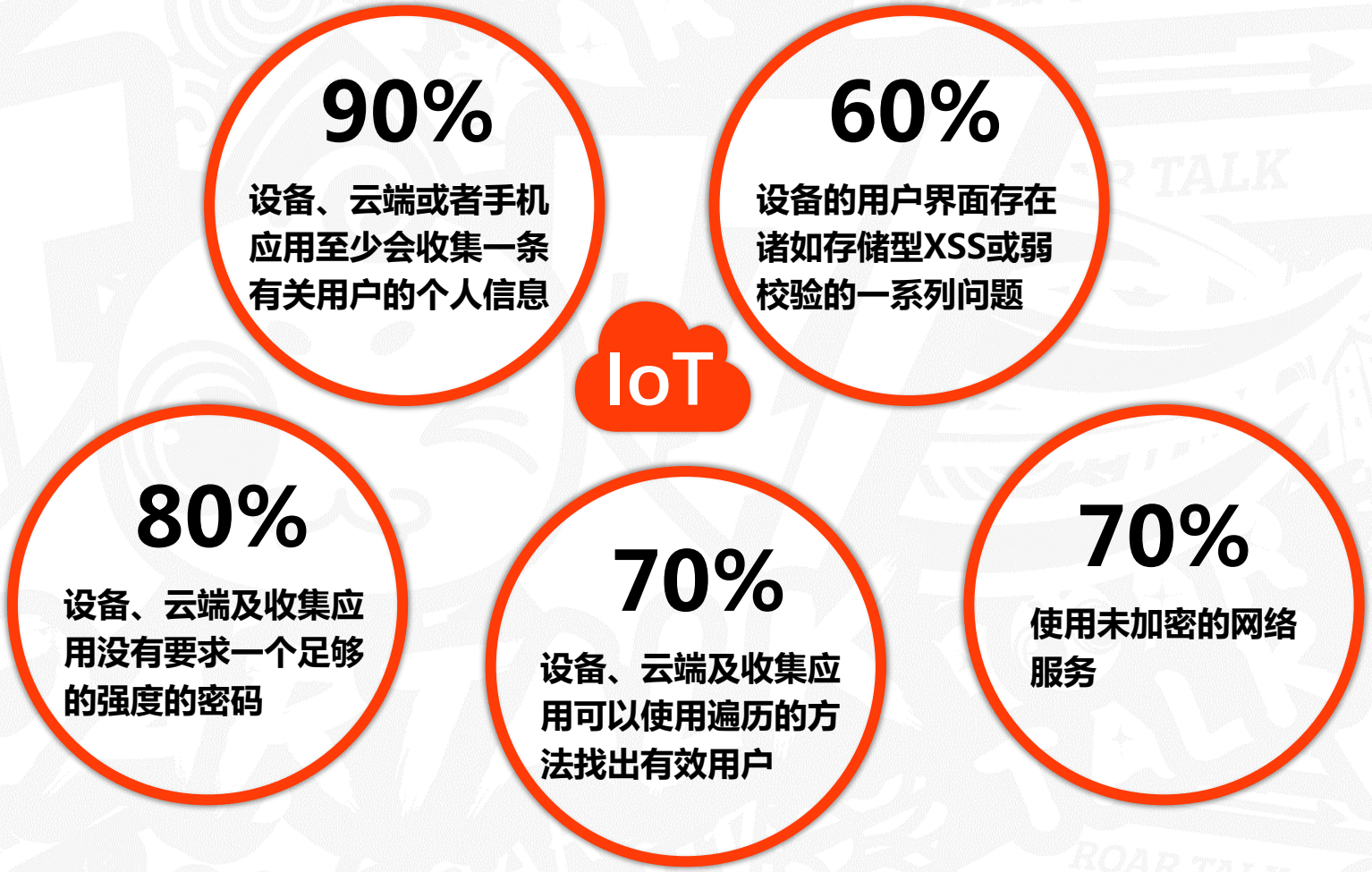
漏洞危害等级



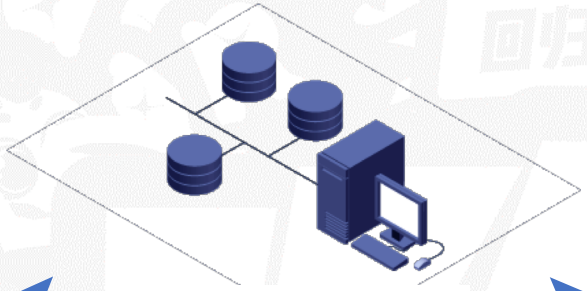
智能硬件野蛮生长，安全隐患迭出

DigApis 安全 让你拥有无限可能

ROARTALK 嘶吼



传统攻防逻辑的局限性



信息系统

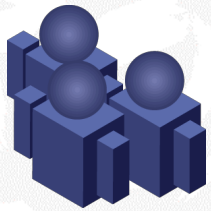
挖掘漏洞、利用漏洞

修复漏洞、部署防御、阻断攻击

漏洞利用

- 漏洞挖掘及利用耗时长
- 安全人员疲于应付
- 繁琐，易出错

- 安全补丁部署时间长
- 攻击时间窗口大



攻击方

漏洞挖掘

漏洞补丁

防守方

如何解决这种问题？

DigApis®
安全
让你拥有无限可能

ROARTALK 嘶吼

自动化攻防

智能化攻防

2

自动化攻防

CGC：Cyber Grand Challenge (2016)

- The need for automated, scalable, machine-speed vulnerability detection and patching is large and growing fast as more and more systems—from household appliances to major military platforms—get connected to and become dependent upon the internet. Today, the process of finding and countering bugs, hacks, and other cyber infection vectors is still effectively artisanal. Professional bug hunters, security coders, and other security pros work tremendous hours, searching millions of lines of code to find and fix vulnerabilities that could be taken advantage of by users with ulterior motives.

- https://www.darpa.mil/program/cyber-grand-challenge

“黄鹤杯”RHG机器人网络安全大赛

- **发展人工智能化的网络安全技术有助于发掘系统未知漏洞，检索安全隐患，推演未知风险，实现安全自动化。**

——中国科学院院士郑建华

漏洞攻防技术

DigApis 安全 让你拥有无限可能

ROARTALK 嘶吼

漏洞挖掘技术

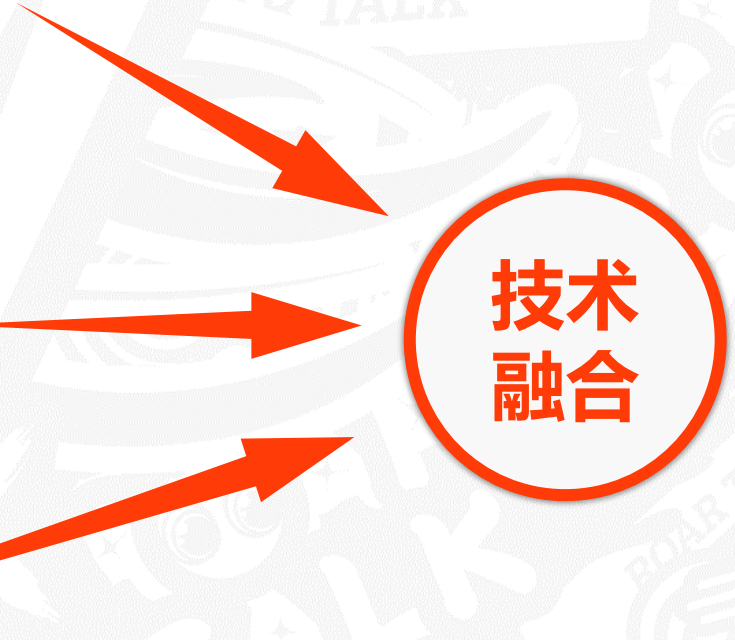
- 基于静态分析（CFG、DFG）
- 基于模糊测试（AFL、JANUS、SAGE）
- 基于动态符号执行（EXE、KLEE）

漏洞利用技术

- Injecting a shellcode
- Return Oriented Programming
- Jmp Esp

漏洞修复技术

- Angelix
- GenProg
- SearchRepair



漏洞挖掘-静态分析

DigApis
安全
让你拥有无限可能

输入信息 → **输出信息**

目标程序

（本系统目标对象是无源码二进制）

数据流信息

控制流信息

优势

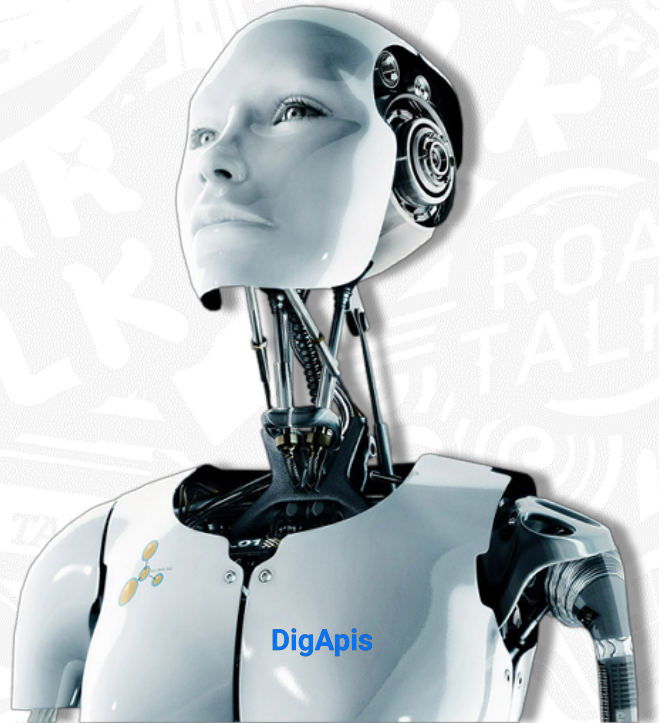
代码覆盖率高

分析成本低

劣势

较高的误报率

（缺少程序运行时信息）



漏洞挖掘-模糊测试

DigApis 安全 让你拥有无限可能

ROARTALK 嘶吼

输入信息 → **输出信息**

具体的输入
目标程序
（本系统目标对象是无源码二进制）

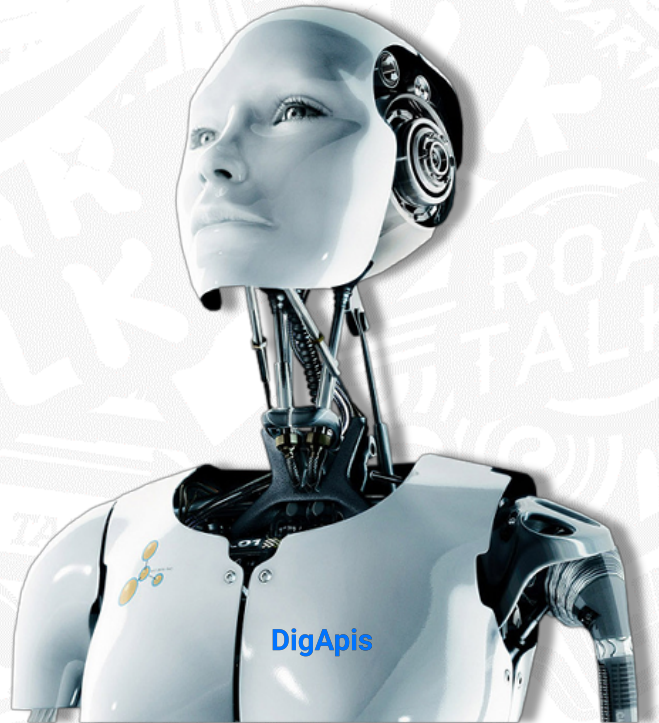
导致程序崩溃的输入

优势

可分析运行时堆栈、寄存器的内容
漏洞定位准确。误报率低
可扩展性高

劣势

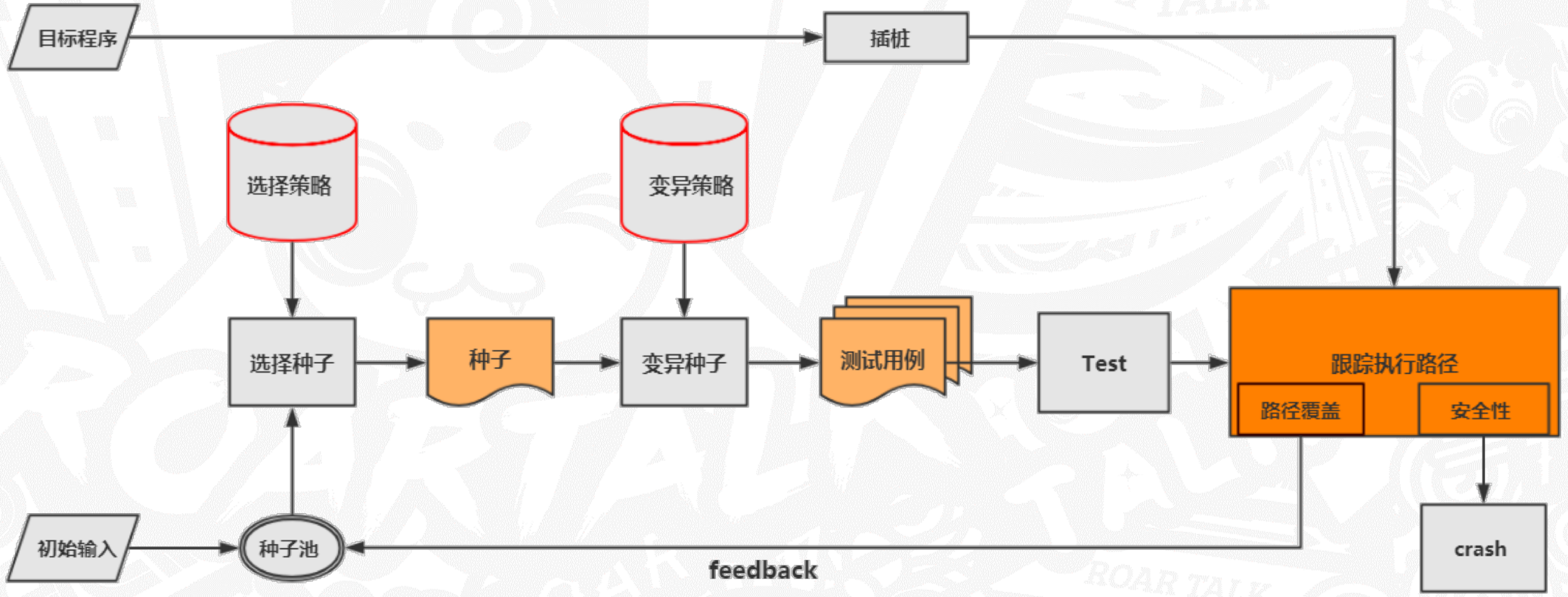
代码覆盖率低



漏洞挖掘-模糊测试

DigApis 安全 让你拥有无限可能

- 把随机数作为程序的输入，监控程序运行过程中的任何异常并分析



漏洞挖掘-动态符号执行

DigApis 安全 让你拥有无限可能

ROARTALK 嘶吼

输入信息 → **输出信息**

目标程序

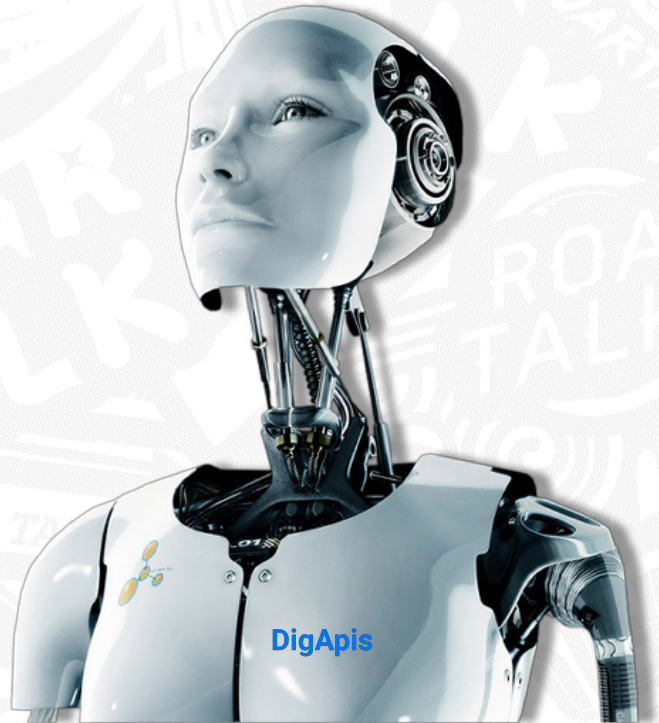
[路径约束]
满足路径约束的测试数据

优势

Sex on paper
理论上，使用符号执行能够
达到100%的代码覆盖率

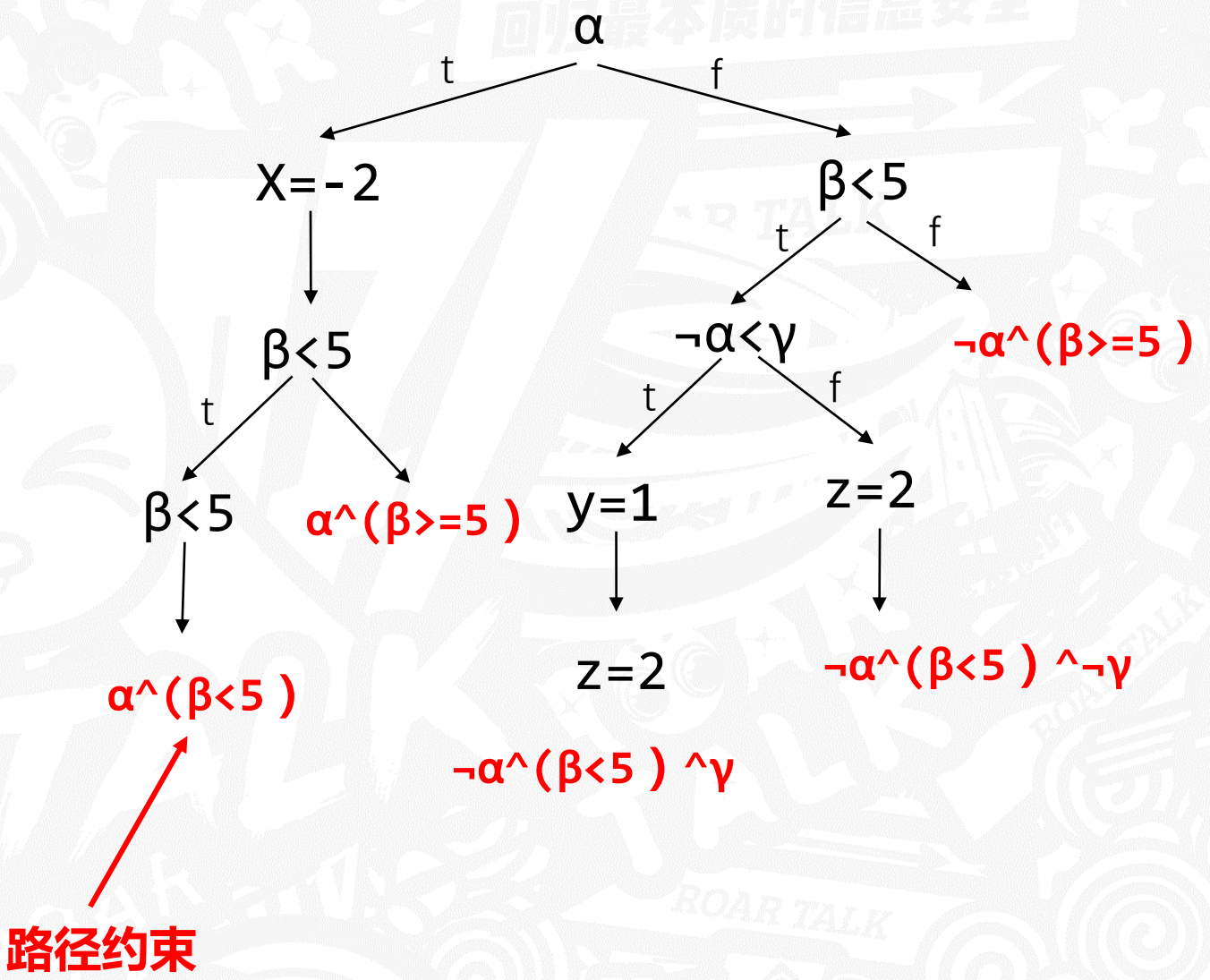
劣势

路径爆炸
约束求解压力
可扩展性低



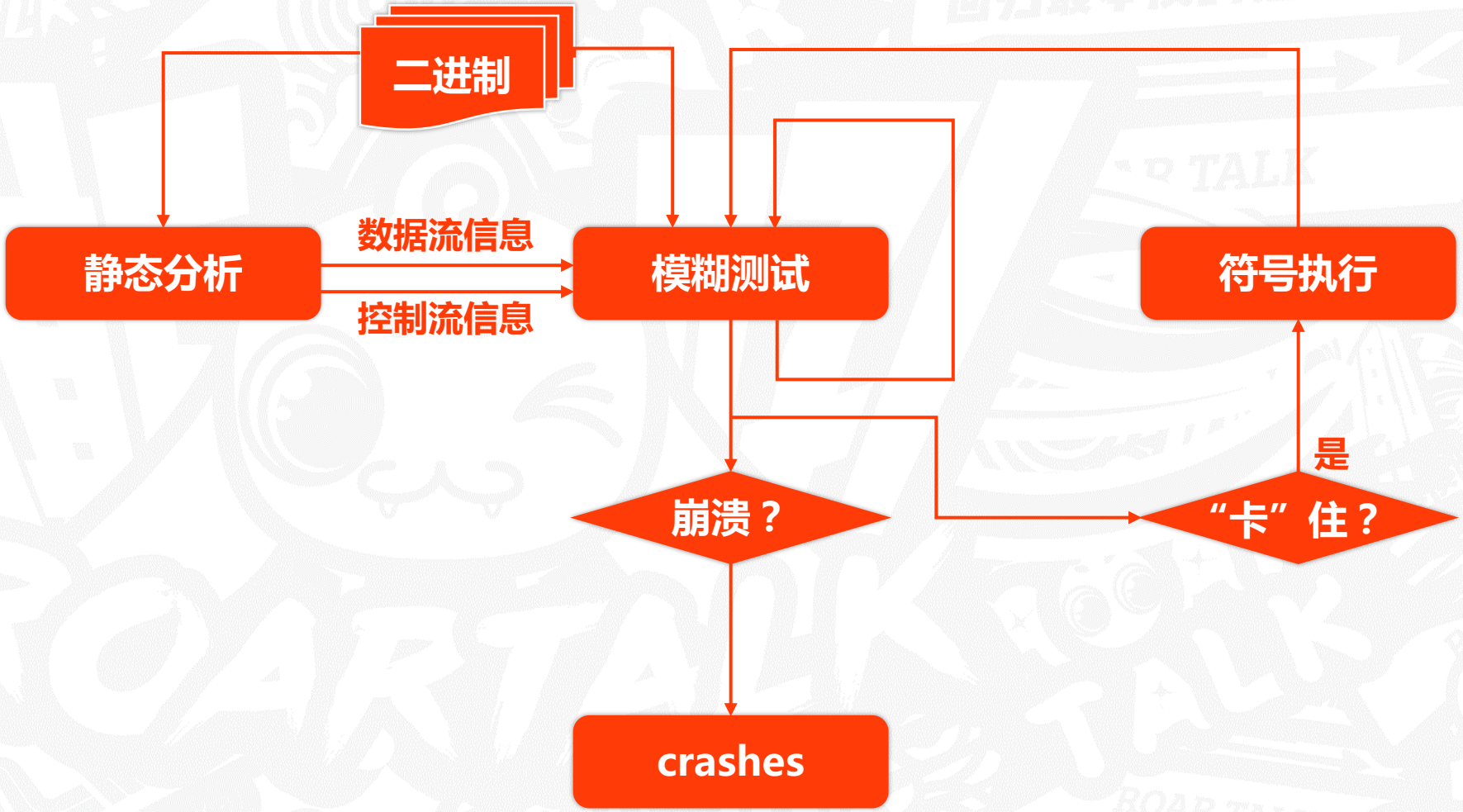
漏洞挖掘-动态符号执行

```
Int a=α , b=β , c=γ
Int x=0,y=0,z=0;
If(a){
      x=-2
}
If(b<5){
      if(!a&&c){
            y=1
      }
      z=2
}
```



缺点：
路径爆炸，约束求解

自动化漏洞挖掘技术融合



自动化漏洞利用

crash

监控程序运行

分析内存信息

获取偏移

构造利用程序

漏洞利用

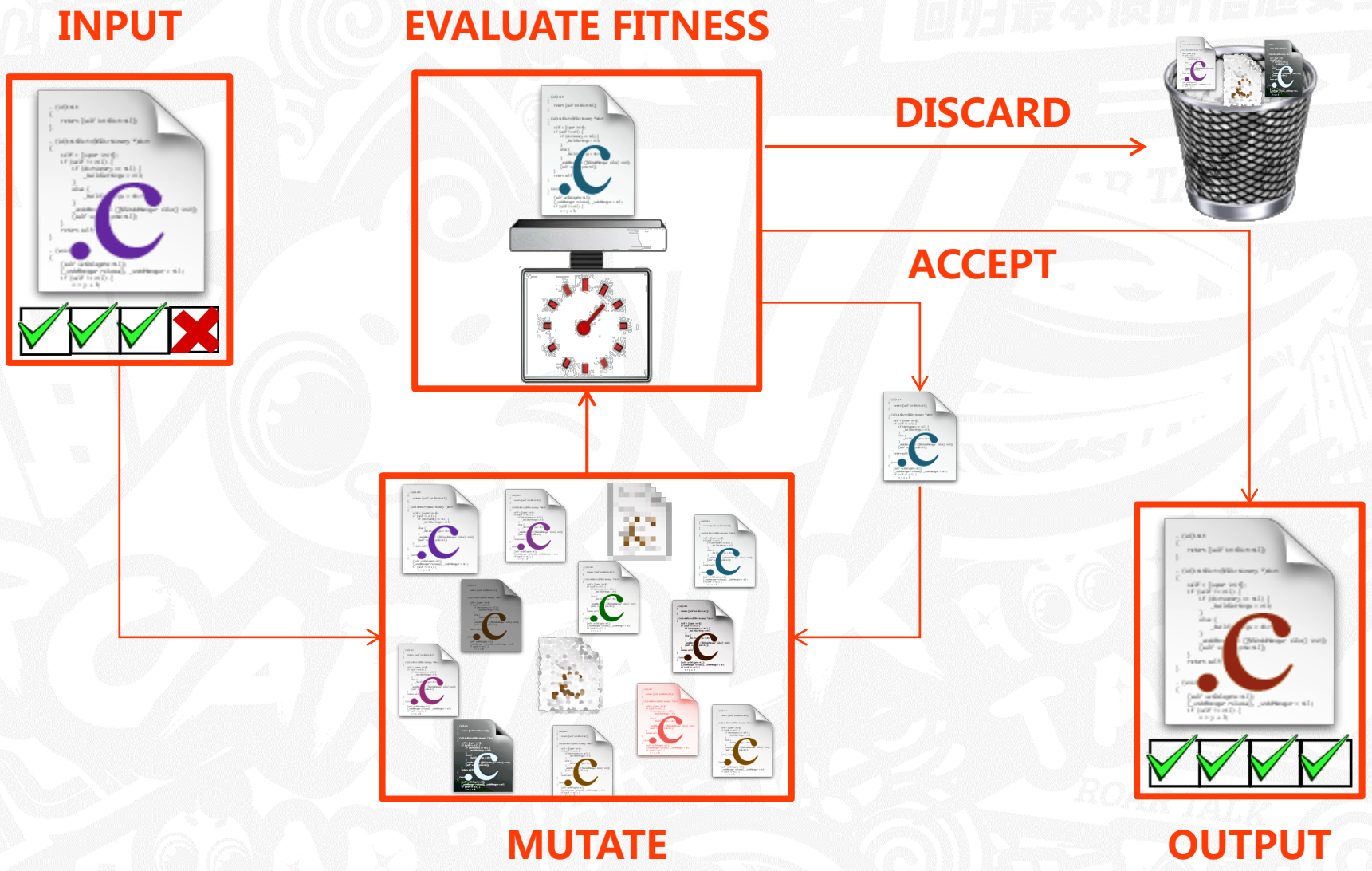
提权？

利用成功

shellcode

利用失败

自动化漏洞修补



自动化攻防的优势与局限

DigApis 安全
让你拥有无限可能

ROARTALK 嘶吼

优势

- 效率性，解决基于人类本身的劳动力查找漏洞已经跟不上漏洞出现的速度和频率的问题；
- 质量性，自动化攻防机器人具备自我进化的能力，碰到越复杂的环境，时间越长，其漏洞挖掘能力也会提高。
- 廉价性，漏洞自动挖掘机器或许有这个能力和机会替代高昂的人工费用，取而代之的是廉价和高效的漏洞挖掘服务。

局限

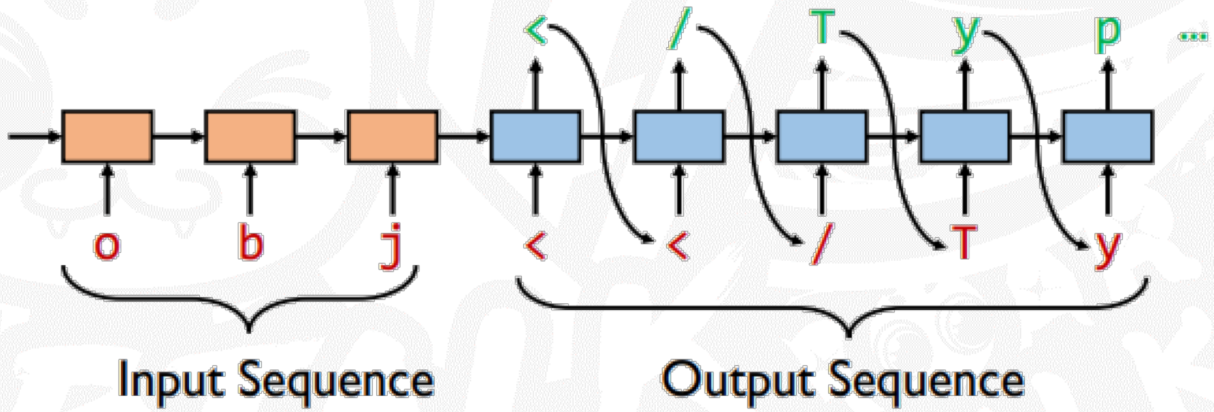
- 自动化修复漏洞不可能是非常完美的防御措施，不是什么东西的漏洞都可以轻易修复的
- 一些常规的漏洞也没有办法完全靠机器去挖掘，比如逻辑漏洞，文件泄露漏洞等
- 在挖掘漏洞的过程中有一定的概率发生一些信息安全事故

智能化攻防

3

通过机器学习方法对模糊测试进行改进

- Godefroid P, Peleg H, Singh R. Learn&fuzz: Machine learning for input fuzzing[C] . ASE, 2017: 50-59.

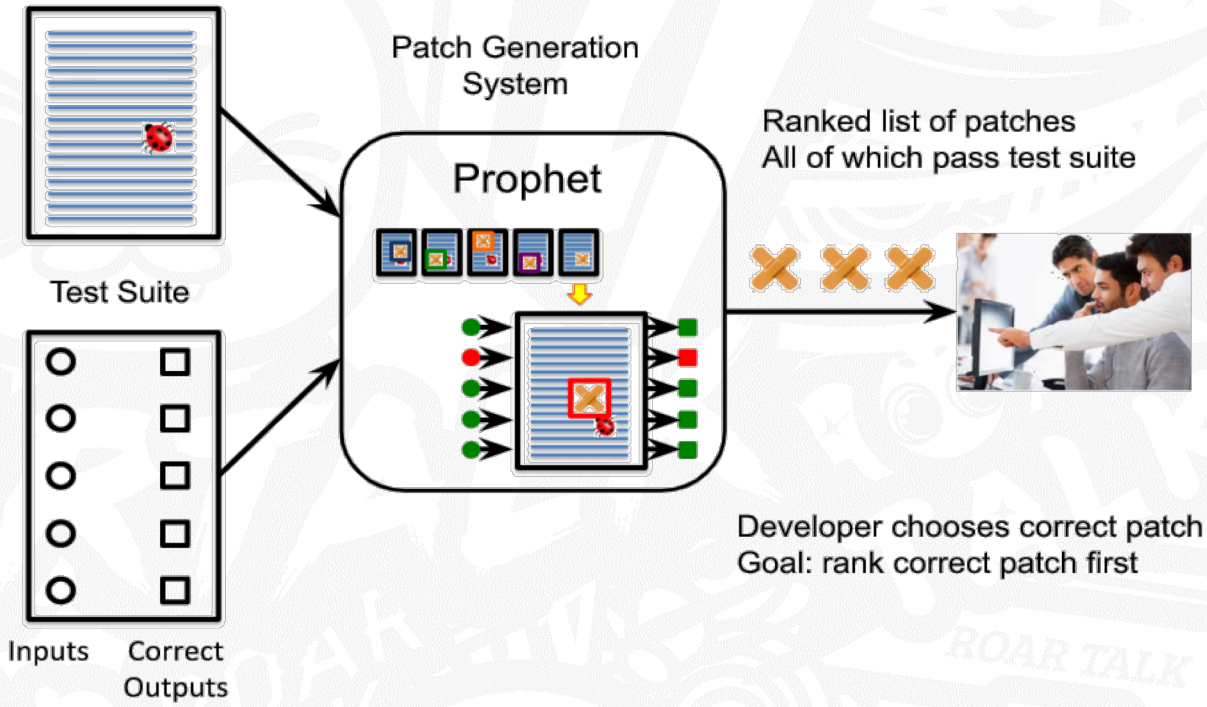


智能化漏洞补丁

DigApis 安全 让你拥有无限可能

通过对正确代码进行学习，产生高质量补丁并进行自动化修复

- Long F, Rinard M. Automatic patch generation by learning correct code[C]. POPL, 2016, 51(1): 298-312.



总结

DigApis®
安全
让你拥有无限可能

ROARTALK 嘶吼

当前是一片蓝海
未来前景广阔

THANKS!