Qiling Framework: #HITB2021AMS

May 2021

twitter: @qiling_io @radareorg

About xwings

THE SHEPHERD LAB 京东牧者安全实验室

JD.COM

Beijing, Stays in the lab 24/7 by hoping making the world a better place

- IoT Research
- Blockchain Research
- Fun Security Research

Qiling Framework

Cross platform and multi architecture advanced binary emulation framework

- https://qiling.io
- Lead Developer
- Founder

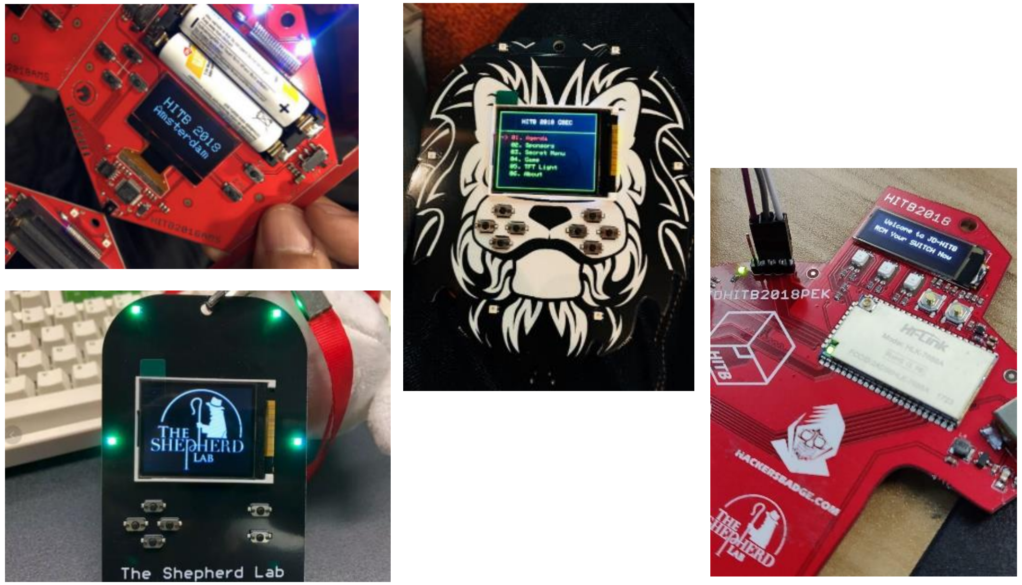
HACKERSBADGE.COM

Badge Maker

Electronic fan boy, making toys from hacker to hacker

- Reversing Binary
- Reversing IoT Devices
- Part Time CtF player

Badge Designer for Hacking Conferences



Some Recent Talk (Partial)

- 2016, Qcon, Beijing, Speaker, nRF24L01 Hijacking
- 2016, Kcon, Beijing, Speaker, Capstone Unicorn Keystone
- 2017, Kcon, Beijing, IoT Hacking Trainer
- 2018, Kcon, Beijing, IoT Hacking Trainer
- 2018, Brucon, Brussel, Speaker, IoT Virtualization
- 2018, H2HC, San Paolo, Speaker, IoT Virtualization
- 2018, HITB, Beijing/Dubai, Speaker, IoT Virtualization
- 2018, beVX, Hong Kong, Speaker, HackCUBE - Hardware Hacking
- 2019, DEFCON USA, Qiling Framework Preview
- 2019, Zeronights, Qiling Framework to Public
- 2020, Nullcon GOA, Building Reversing Tools with Qiling
- 2020, HITB AMS, Building Reversing Tools with Qiling
- 2020, HITB Singapore, Training, How to Hack IoT with Qiling
- 2020, HITB UAE, Training, Lightweight Binary Analyzer
- 2020, Blackhat USA, Building IoT Fuzzer with Qiing
- 2020, Blackhat Singapore, Lightweight Binary Analyzer
- 2020, Blackhat Europe, Deep Dive Into Obfuscated Binary

Qiling Framework

- Cross platform and cross architecture binary instrumentation framework
- Emulate and instrument ARM, ARM64, MIPS, X86 and X8664
- Emulate and instrument Linux, MacOS, Windows and FreeBSD
- High-level Python API access to register, CPU and memory
- 2,200+ Github star, more than 13,000+ pypi download, 70+ contributors worldwide

About lazymio && kabeor

```
~ $ whoami
Lazymio

~ $ file Lazymio
The sheperd lab, JD security, Security Engineer.
CTF player, member of Lancet.
GeekPwn 2019 Hall of Fame.

~ $ ls -l Lazymio
Reverse engineering.
Binary analysis.
Writing code for fun.

~ $ which Lazymio
Github: https://github.com/wtdcode
Blog: https://blog.lazym.io/
Twitter: https://twitter.com/pwnedmio
```

Name: kabeor

Security Engineer at The Shepherd Lab, JD Security.

Core developer of Qiling.

BlackHat Asia & Europe 2020 - Speaker

China kanxue SDC 2020 - Speaker

HITB Training 2020 - Speaker

Github: https://github.com/kabeor

Blog: https://kabeor.cn

Twitter: https://twitter.com/Angrz3_K

Make IoT Reverse Engineering Great

It All Started With IoT

Debugger

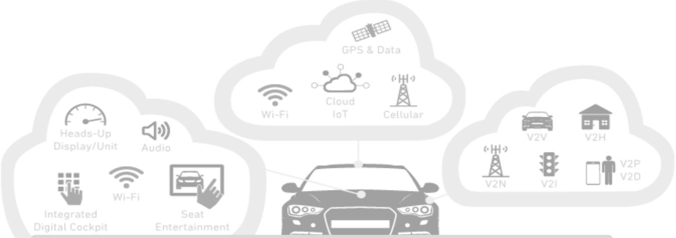
Emulation

Instrumentation

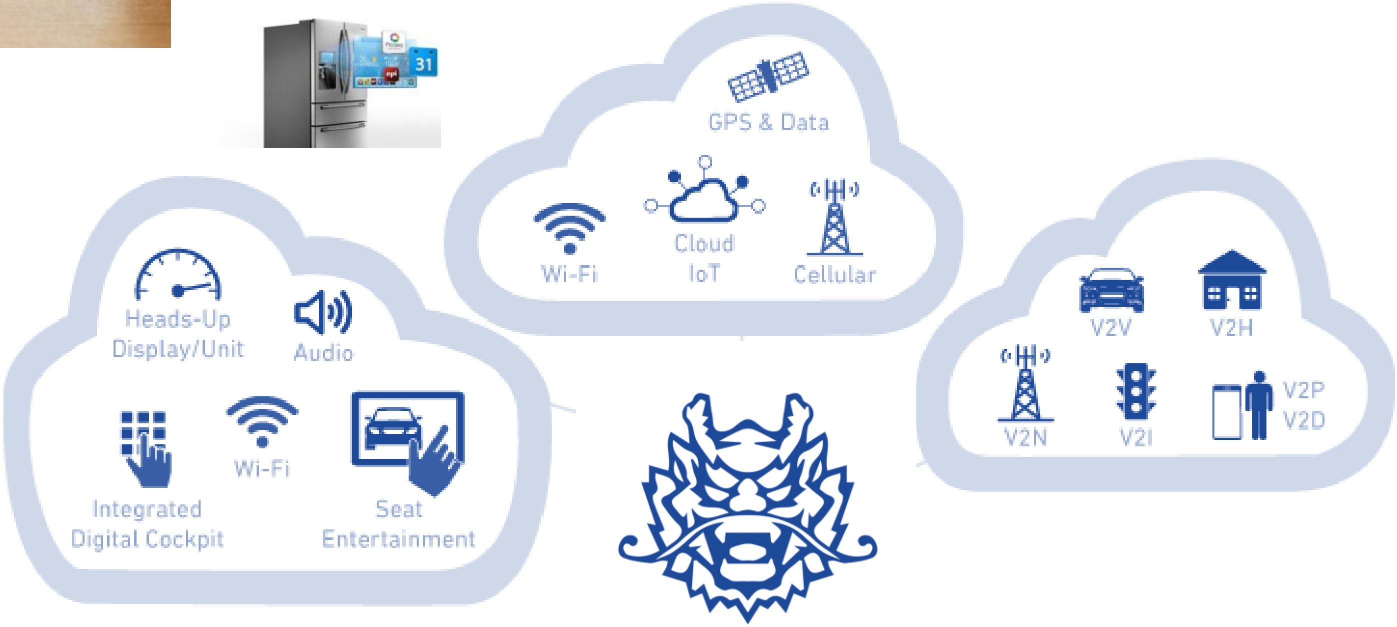
Hot Patch

APIs

And more on our smartphone app: (Now available on Qi teamaker Vita+)
android
iOS



No Actual Hardware Needed

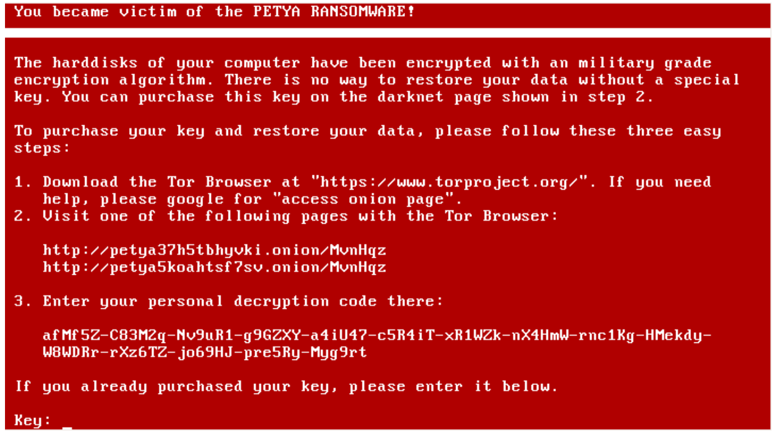


Qiling Framework

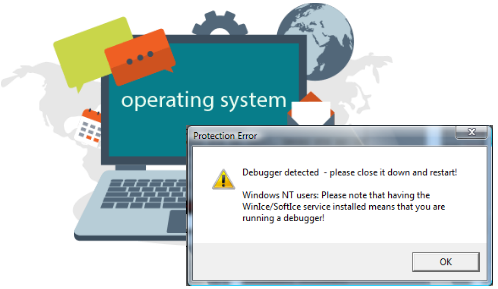
and the list goes on

Wait, There are Virtual Machines

Current Virtual Machine Limitation

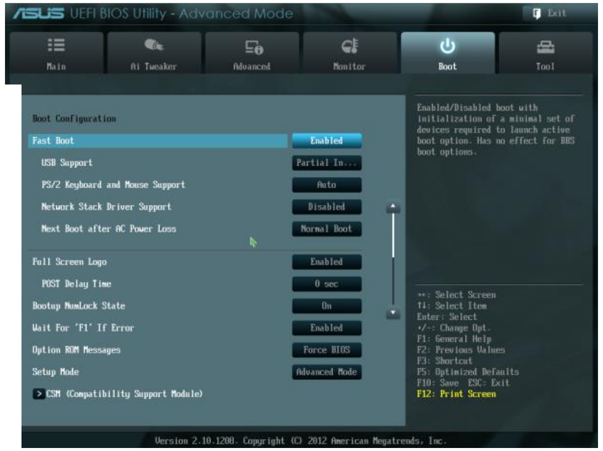


```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/MvnHqz
   http://petya5koahtsf7sv.onion/MvnHqz

3. Enter your personal decryption code there:

   afMf5Z-C83M2q-Nv9uR1-g9GZXY-a4iU47-c5R4iT-xR1WZk-nX4HmW-rnc1Kg-HMekdy-
   W8WDRr-rXz6TZ-jo69HJ-pre5Ry-Myg9rt

If you already purchased your key, please enter it below.

Key: _
```



Debugger detected - please close it down and restart!

Windows NT users: Please note that having the WinIce/SoftIce service installed means that you are running a debugger!



Boot Configuration

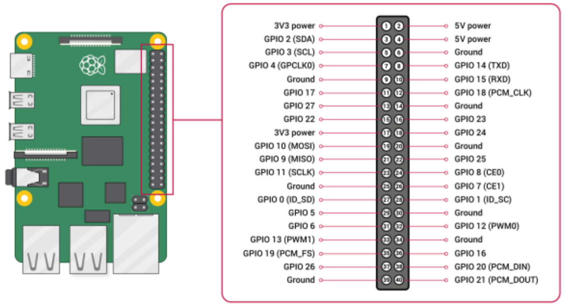
Fast Boot	Enabled
USB Support	Partial In...
PS/2 Keyboard and Mouse Support	Auto
Network Stack Driver Support	Disabled
Next Boot after AC Power Loss	Normal Boot
Full Screen Logo	Enabled
POST Delay Time	0 sec
Bootup NumLock State	On
Wait For 'F1' If Error	Enabled
Option ROM Messages	Force BIOS
Setup Mode	Advanced Mode

> CSM (Compatibility Support Module)

Enabled/Disabled boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.

```
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Shortcut
F5: Optimized Defaults
F10: Save  ESC: Exit
F12: Print Screen
```

Version 2.10.1208. Copyright (C) 2012 American Megatrends, Inc.



3V3 power	1	2	5V power
GPIO 2 (SDA)	3	4	5V power
GPIO 3 (SCL)	5	6	Ground
GPIO 4 (GPCLK0)	7	8	GPIO 14 (TXD)
Ground	9	10	GPIO 15 (RXD)
GPIO 17	11	12	GPIO 18 (PCM_CLK)
GPIO 27	13	14	Ground
GPIO 22	15	16	GPIO 23
3V3 power	17	18	GPIO 24
GPIO 10 (MOSI)	19	20	Ground
GPIO 9 (MISO)	21	22	GPIO 25
GPIO 11 (SCLK)	23	24	GPIO 8 (CE0)
Ground	25	26	GPIO 7 (CE1)
GPIO 0 (ID_SD)	27	28	GPIO 1 (ID_SC)
GPIO 5	29	30	Ground
GPIO 6	31	32	GPIO 12 (PWM0)
GPIO 13 (PWM1)	33	34	Ground
GPIO 19 (PCM_FS)	35	36	GPIO 16
GPIO 26	37	38	GPIO 20 (PCM_DIN)
Ground	39	40	GPIO 21 (PCM_DOUT)

MBR

UEFI

Smart Contract

GPIO

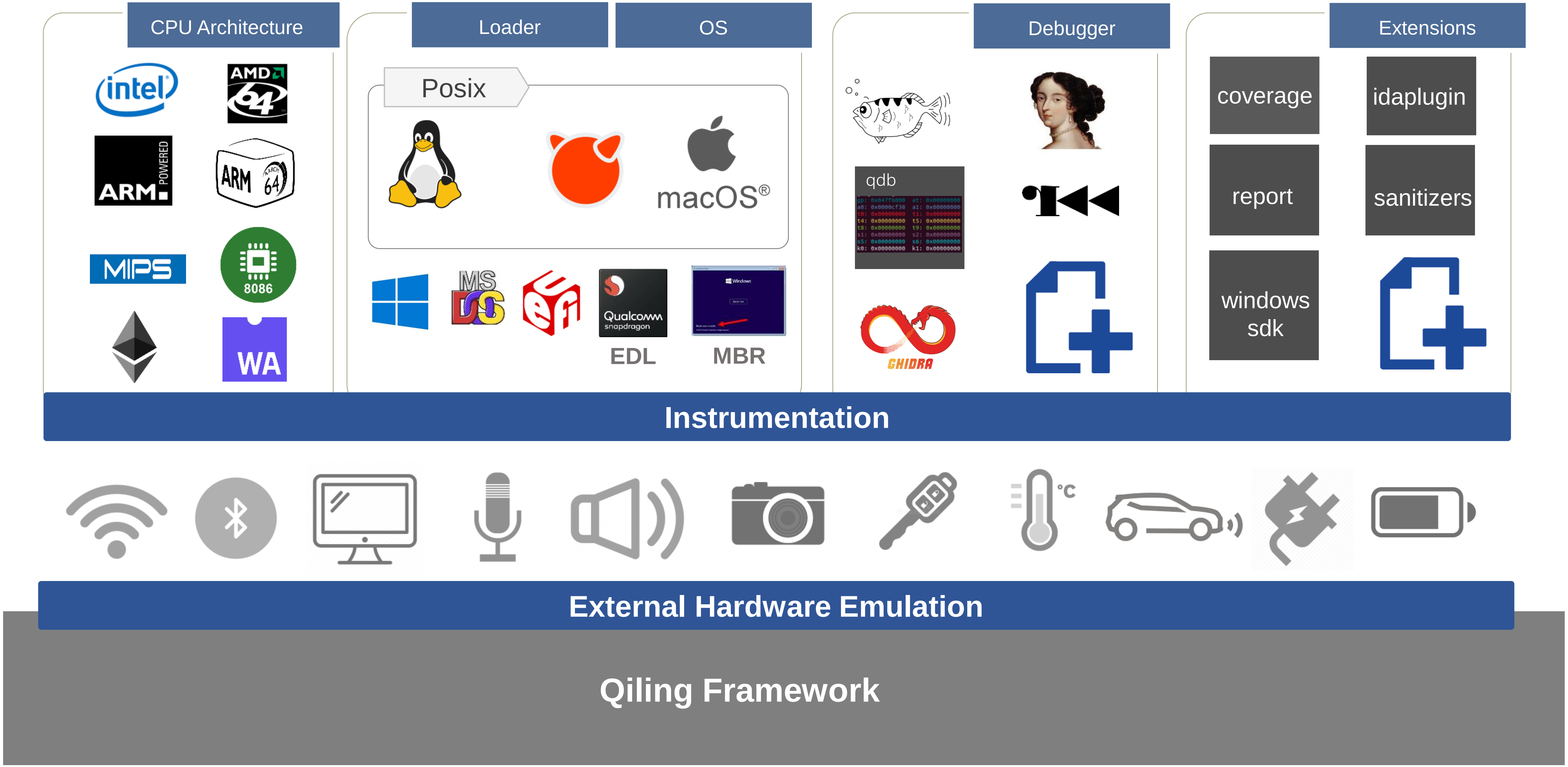
Anti-Anti Debug

Qualcomm EDL

emulator is not for reverse engineers

Qiling Framework

Overview



CPU Architecture

Loader

OS

Posix

Debugger

Extensions

qdb

```
gp: 0x047f6000  at: 0x00000000
a0: 0x0000cf38  a1: 0x00000000
t0: 0x00000000  t1: 0x00000000
t4: 0x00000000  t5: 0x00000000
t8: 0x00000000  t9: 0x00000000
s1: 0x00000000  s2: 0x00000000
s5: 0x00000000  s6: 0x00000000
k0: 0x00000000  k1: 0x00000000
```

coverage

idaplugin

report

sanitizers

windows sdk

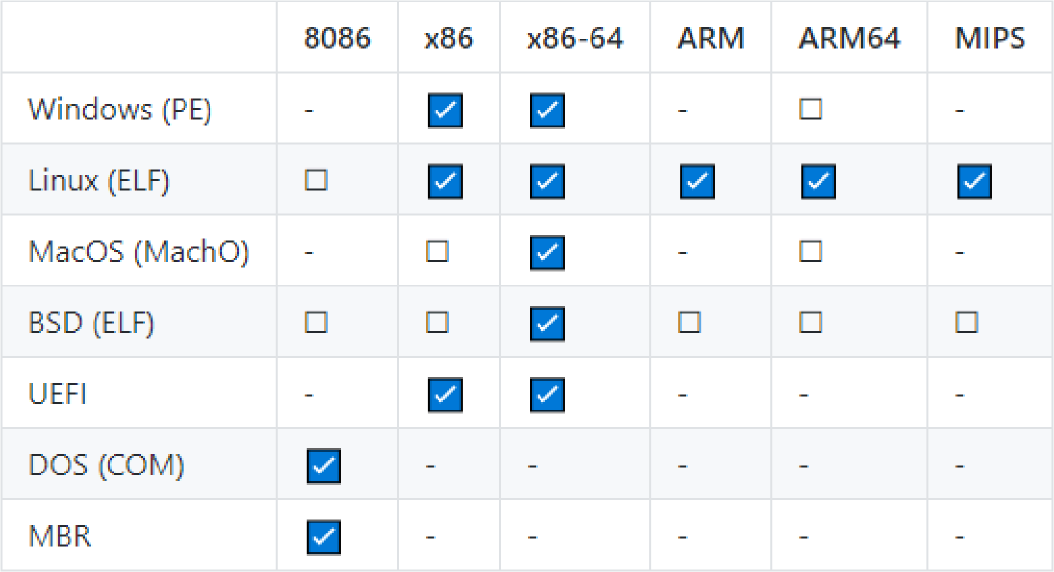
Instrumentation

External Hardware Emulation

Qiling Framework

Features

- Cross platform: Windows, MacOS, Linux, BSD, UEFI, MBR
- Cross architecture: X86, X86_64, Arm, Arm64, MIPS, 8086
- Multiple file formats: PE, UEFI(PE), MachO, ELF, EDL (ELF), COM
- Emulate & sandbox machine code in a isolated environment
- Provide high level API to setup & configure the sandbox
- Fine-grain instrumentation: allow hooks at various levels (instruction/basic-block/memory-access/exception/syscall/IO/etc)
- Allow dynamic hotpatch on-the-fly running code, including the loaded library
- True Python framework, making it easy to build customized analysis tools on top
- GDBServer support - GDB/IDA/r2
- IDA Plugin
- OS profiling support



	8086	x86	x86-64	ARM	ARM64	MIPS
Windows (PE)	-	☑	☑	-	☐	-
Linux (ELF)	☐	☑	☑	☑	☑	☑
MacOS (MachO)	-	☐	☑	-	☐	-
BSD (ELF)	☐	☐	☑	☐	☐	☐
UEFI	-	☑	☑	-	-	-
DOS (COM)	☑	-	-	-	-	-
MBR	☑	-	-	-	-	-

CARDANO

ETH 2.0

Similarity

User Mode Emulation

qemu-usermode

- The TOOL
- Limited OS Support, Very Limited
- No Multi OS Support
- No Instrumentation
- **Syscall Forwarding**

usercorn

- Very good project !
- It's a Framework !
- Mostly *nix based only
- Limited OS Support (No Windows)
- Go and Lua is not hacker's friendly
- **Syscall Forwarding**

Binee

- Very good project too
- Only X86 (32 and 64)
- Limited OS Support
- Only PE Files
- Just a tool, we don't need a tool
- Again, is GO

WINE

- Limited ARCH Support
- Limited OS Support, only Windows
- Not Sandbox Designed
- No Instrumentation

FireEye

Speakeasy

- Very good project too
- X86 32 and 64
- PE files and Driver
- Limited OS Support
- Only Windows

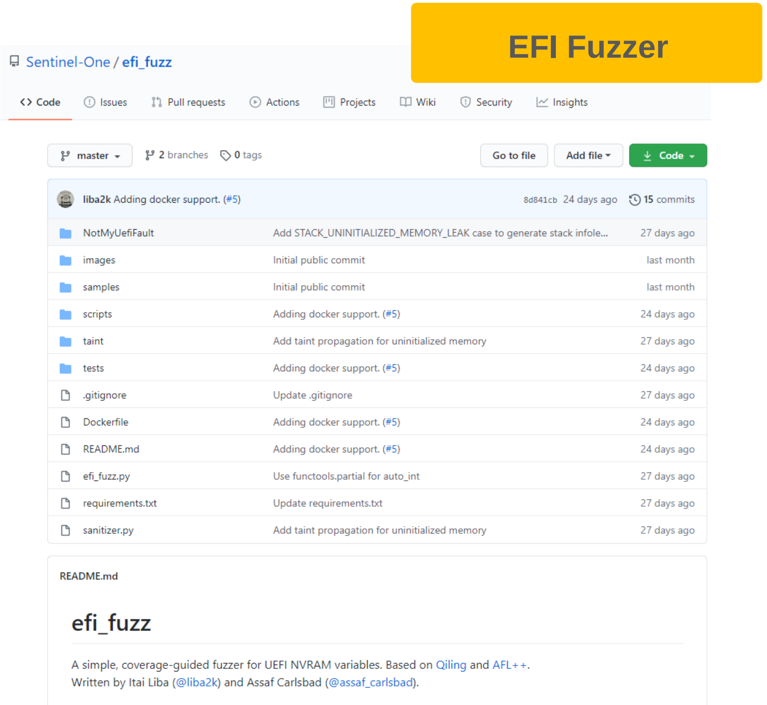
Zelos

- Very good project !
- It's a Framework !
- Linux based only (No Windows)
- Incomplete support for Linux multi arch

Framework

Framework, NOT Tools

EFI Fuzzer



Sentinel-One / efi_fuzz

<> Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

master ▾ | 2 branches | 0 tags | Go to file | Add file ▾ | Code ▾

liba2k Adding docker support. (#5) 8d841cb 24 days ago 15 commits

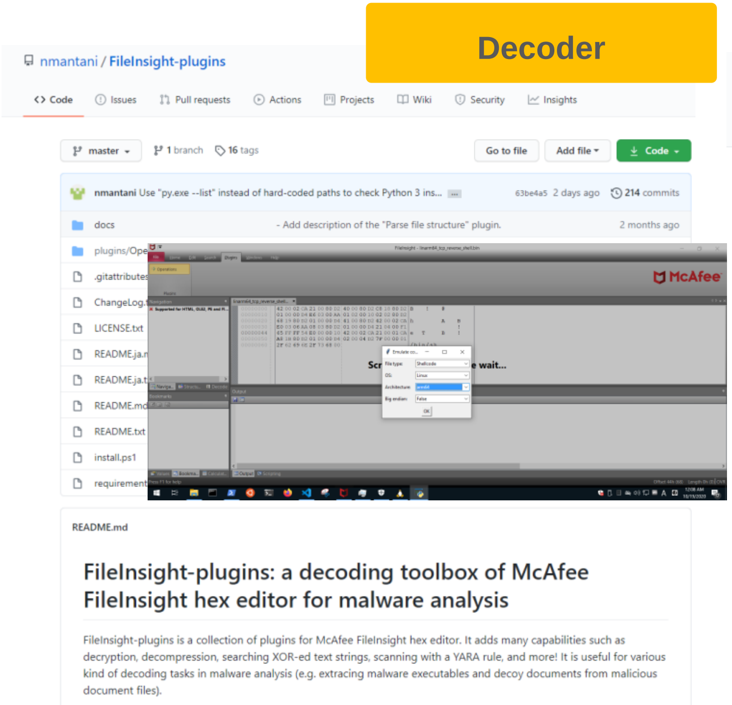
NotMyUefiFault	Add STACK_UNINITIALIZED_MEMORY_LEAK case to generate stack infole...	27 days ago
images	Initial public commit	last month
samples	Initial public commit	last month
scripts	Adding docker support. (#5)	24 days ago
taint	Add taint propagation for uninitialized memory	27 days ago
tests	Adding docker support. (#5)	24 days ago
.gitignore	Update .gitignore	27 days ago
Dockerfile	Adding docker support. (#5)	24 days ago
README.md	Adding docker support. (#5)	24 days ago
efi_fuzz.py	Use functools.partial for auto_int	27 days ago
requirements.txt	Update requirements.txt	27 days ago
sanitizer.py	Add taint propagation for uninitialized memory	27 days ago

README.md

efi_fuzz

A simple, coverage-guided fuzzer for UEFI NVRAM variables. Based on Qiling and AFL++.
Written by Itai Liba (@liba2k) and Assaf Carlsbad (@assaf_carlsbad).

Decoder



nmantani / FileInsight-plugins

<> Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

master ▾ | 1 branch | 16 tags | Go to file | Add file ▾ | Code ▾

nmantani Use "py.exe --list" instead of hard-coded paths to check Python 3 ins... 63be4a5 2 days ago 214 commits

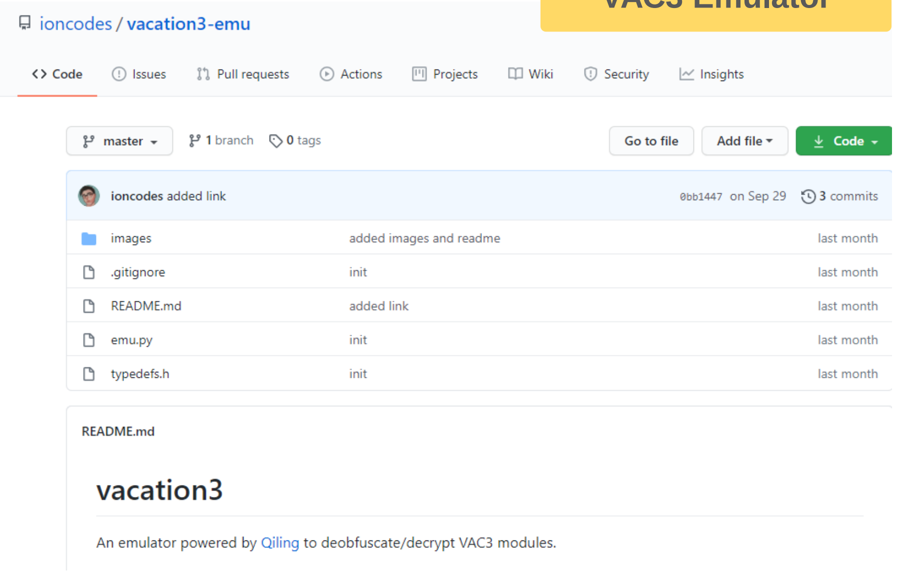
docs	- Add description of the "Parse file structure" plugin.	2 months ago
plugins/Ope		
.gitattributes		
ChangeLog.		
LICENSE.txt		
README.ja.r		
README.ja.t		
README.md		
README.txt		
install.ps1		
requirement		

README.md

FileInsight-plugins: a decoding toolbox of McAfee FileInsight hex editor for malware analysis

FileInsight-plugins is a collection of plugins for McAfee FileInsight hex editor. It adds many capabilities such as decryption, decompression, searching XOR-ed text strings, scanning with a YARA rule, and more! It is useful for various kind of decoding tasks in malware analysis (e.g. extracing malware executables and decoy documents from malicious document files).

VAC3 Emulator



ioncodes / vacation3-emu

<> Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

master ▾ | 1 branch | 0 tags | Go to file | Add file ▾ | Code ▾

ioncodes added link 0bb1447 on Sep 29 3 commits

images	added images and readme	last month
.gitignore	init	last month
README.md	added link	last month
emu.py	init	last month
typedefs.h	init	last month

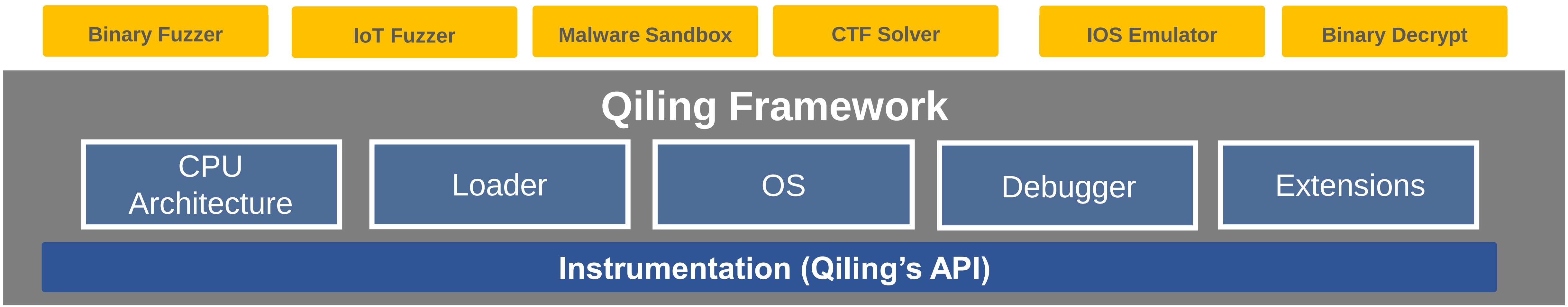
README.md

vacation3

An emulator powered by Qiling to deobfuscate/decrypt VAC3 modules.

IoT Emulator

MacOS Emulator



Binary Fuzzer | IoT Fuzzer | Malware Sandbox | CTF Solver | IOS Emulator | Binary Decrypt

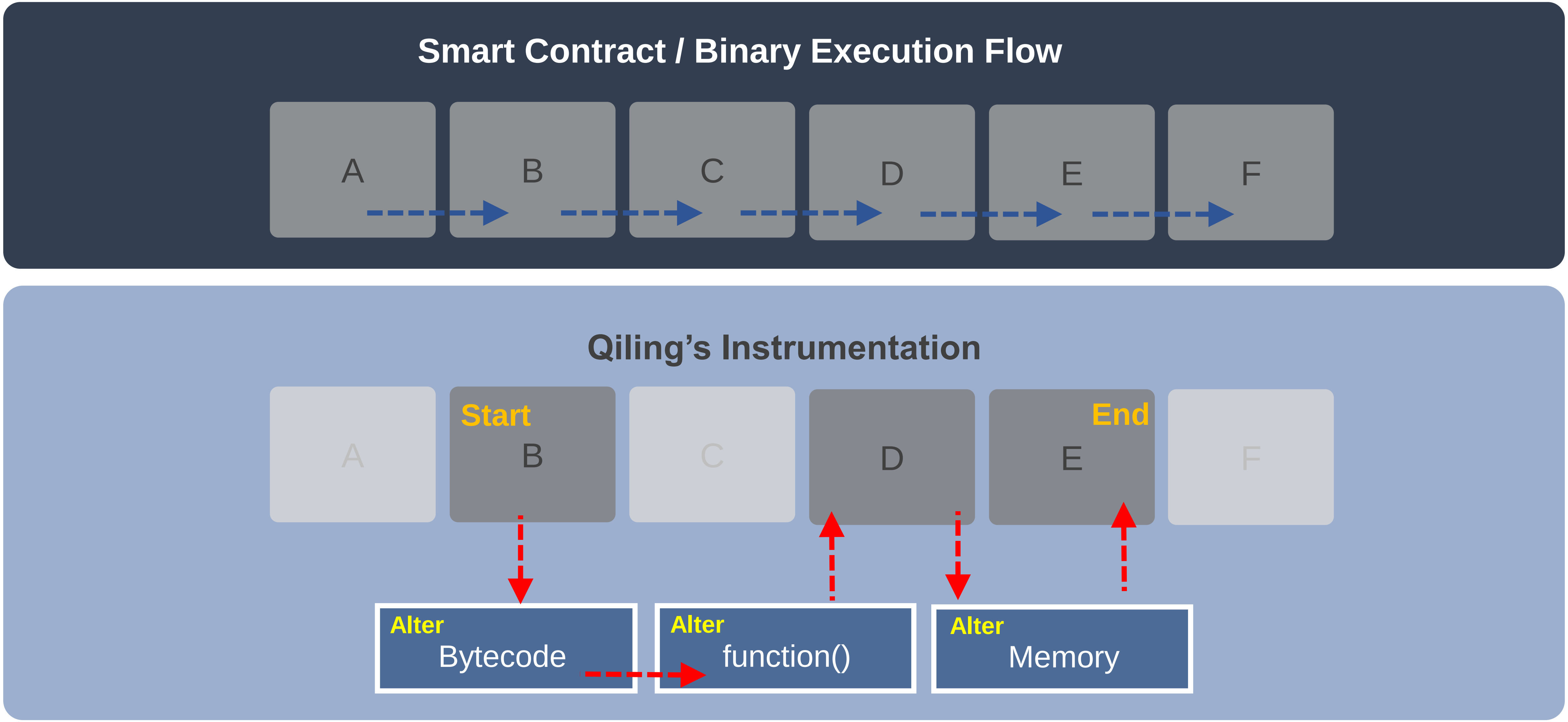
Qiling Framework

CPU Architecture | Loader | OS | Debugger | Extensions

Instrumentation (Qiling's API)

Instrumentation

What Is Instrumentation



When Qiling Meets Radare2

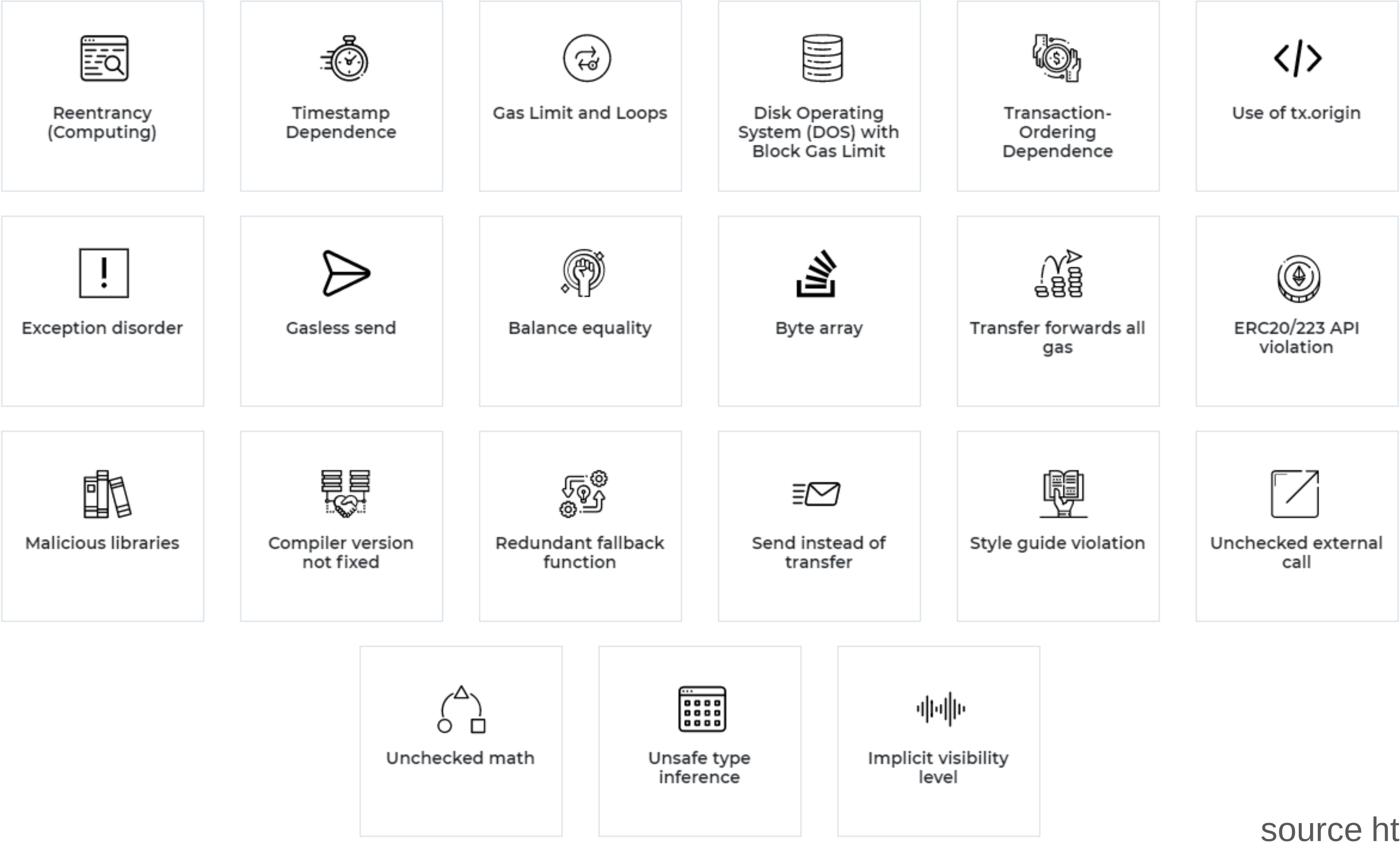
Introduction to Radare2

Next Speaker ZiQiao, Kong

DEMO

Make Smart Contract Analysis Smarter

Greater Functions Comes With Greater Bugs



- Reentrancy (Computing)
- Timestamp Dependence
- Gas Limit and Loops
- Disk Operating System (DOS) with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20/223 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

source https://www.developcoins.com/

> Various types of vulnerabilities

> More complicated after DeFi

> 109B DeFi Market Cap, as of April 2021

> 22B USD thief in 2019/2020

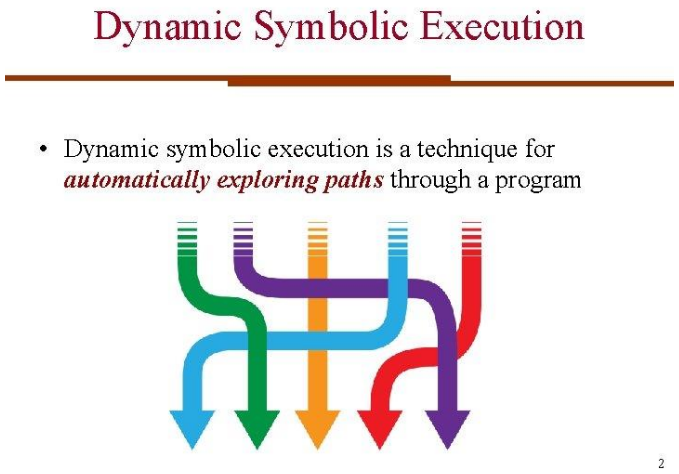
Today’s Smart Contract Analysis Problems

Binary Only Contracts

Complex Symbolic Execution

High False Positive

Require Human Analysis



Dynamic Symbolic Execution

- Dynamic symbolic execution is a technique for *automatically exploring paths* through a program

2

Dynamic cross contract emulation and debug is almost impossible

Not to mention close source smart contract

Wait, There are Official Emulator

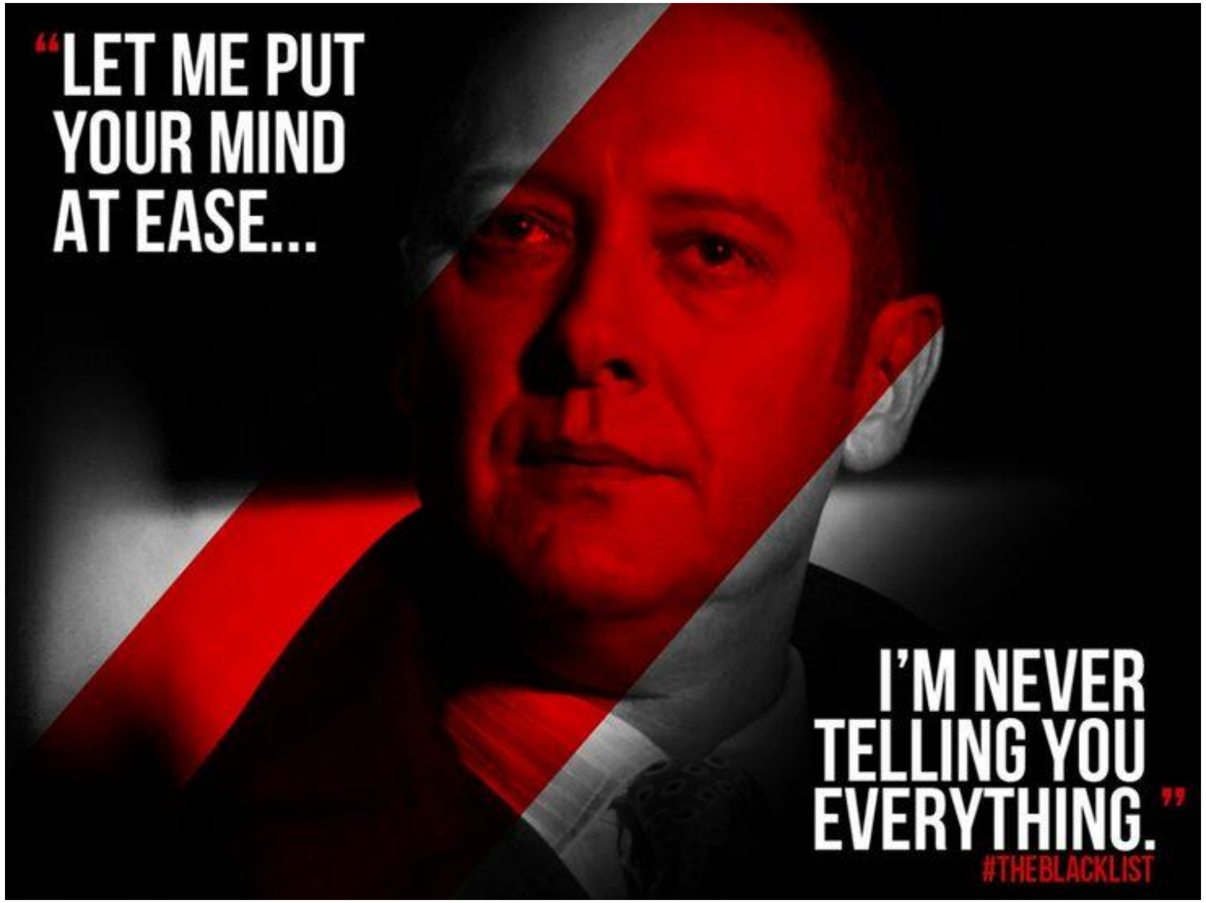
Current Emulator, Symbolic Execution Limitation

What Is Missing

- Dynamic Execution Hook
- Conditional Execution
- Contract Only Fuzzing
- Pattern Execution
- Live Debugging
- Real Instrumentation
- Not a Framework

99% of the smart contract enabled block chain are EVM/WASM

Special Appearance: EVM Demo


"LET ME PUT YOUR MIND AT EASE...
I'M NEVER TELLING YOU EVERYTHING."
#THEBLACKLIST

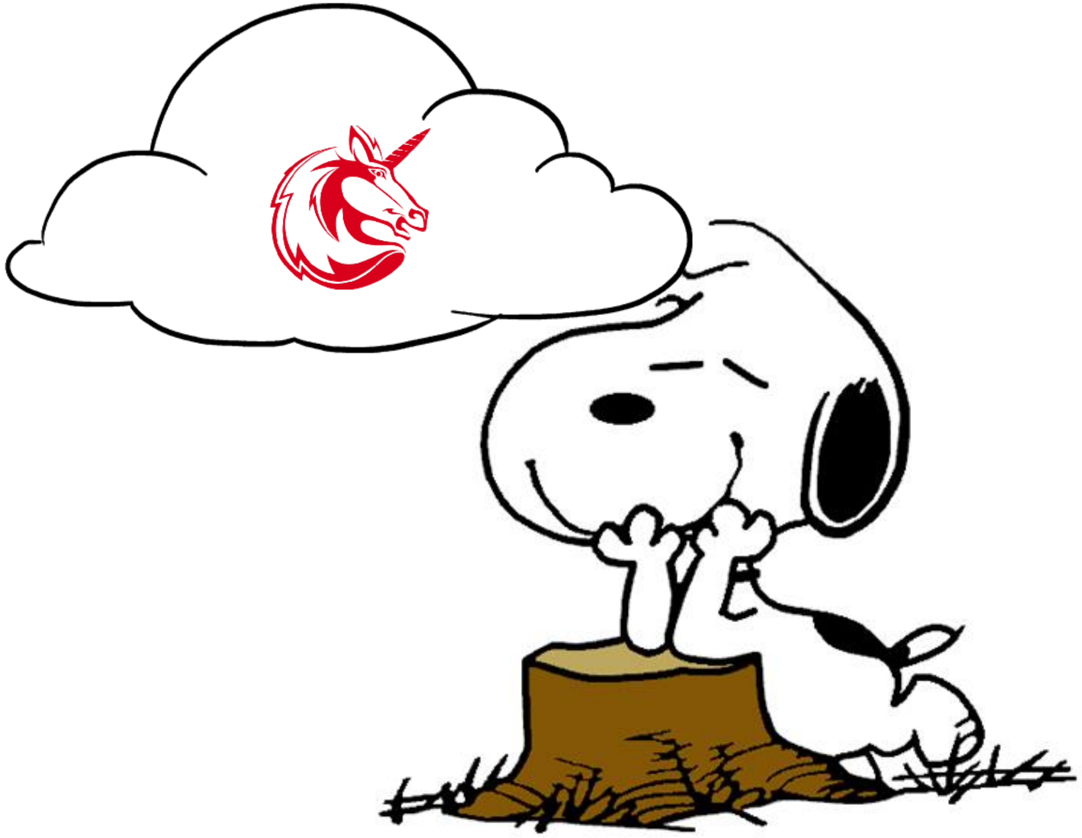
Next Speaker ChenXu, Wu

DEMO

Next Step

Roadmap

- Force Unicorn Engine sync with QEMU 5, Code name **Unicorn 2**
  - More architectures, more CPU instructions set
  - Almost Done
  - **Looking for Release *Sponsor***
- Android Java bytecode layer instrumentation
- **Forward to host implementation**
- iPhoneOS/MacOS/M1 emulation support
- More robust Windows emulation
  - Introduce wine && Cygwin or something
- **ETA: Smart Contract emulation (EVM, soon WASM)**
- MCU emulation



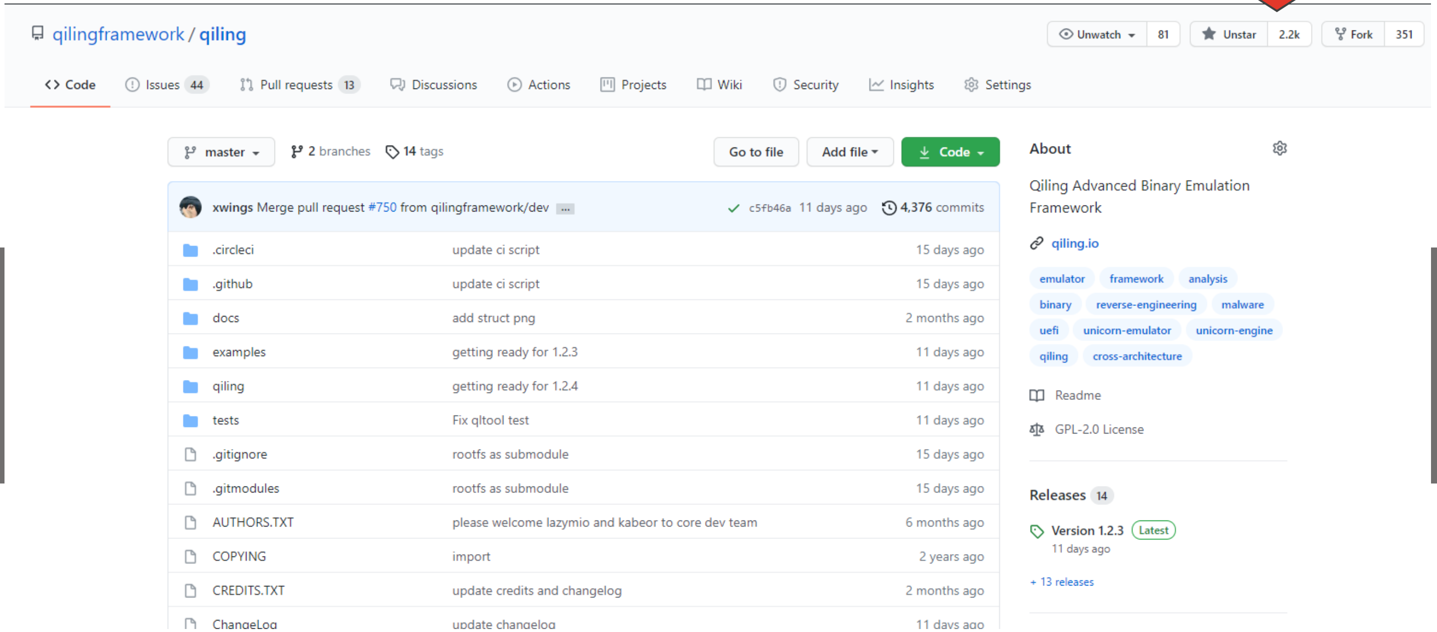
Join Us and Make Pull Request !!!

Everything Else

- About Qiling Framework
  - https://qiling.io
  - https://github.com/qilingframework/qiling
  - https://docs.qiling.io
  - http://t.me/qilingframework
  - @qiling_io

Star us

Questions



xwings Merge pull request #750 from qilingframework/dev … ✓ c5fb46a 11 days ago 4,376 commits

.circleci	update ci script	15 days ago
.github	update ci script	15 days ago
docs	add struct png	2 months ago
examples	getting ready for 1.2.3	11 days ago
qiling	getting ready for 1.2.4	11 days ago
tests	Fix qltool test	11 days ago
.gitignore	rootfs as submodule	15 days ago
.gitmodules	rootfs as submodule	15 days ago
AUTHORS.TXT	please welcome lazymio and kabeor to core dev team	6 months ago
COPYING	import	2 years ago
CREDITS.TXT	update credits and changelog	2 months ago
ChangeLog	update changelog	11 days ago

About

Qiling Advanced Binary Emulation Framework

qiling.io

emulator framework analysis binary reverse-engineering malware uefi unicorn-emulator unicorn-engine qiling cross-architecture

Readme

GPL-2.0 License

Releases 14

Version 1.2.3 Latest
11 days ago

+ 13 releases