runtime verification

Debug First, or Regret Later

An Arsenal of Tools can Build Solid Ethereum Foundations

Aellison Cassimiro

Runtime Verification Inc.

Untested code is the root of all evil!

Lurking Where We Least Expect

APR 25, 2022

Becoming a Millionaire, 0.000150 BTC at a Time

How we discovered a critical issue in Solana's stable swap implementation. A story about arbitrage and rounding.

https://osec.io/blog/2022-04-26-spl-swap-rounding

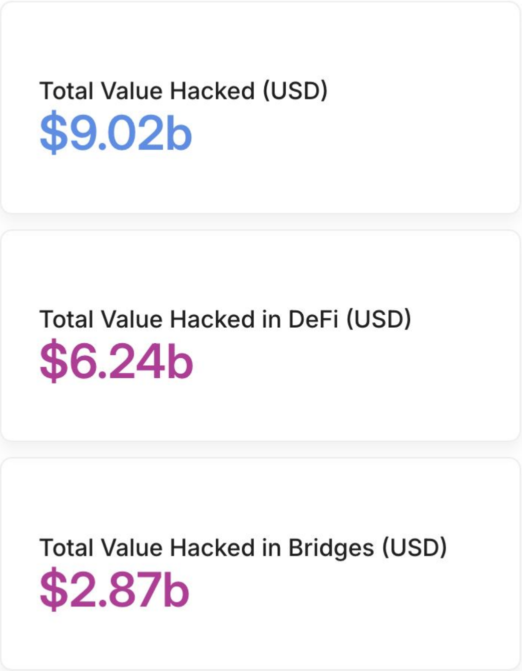
[redacted] loses $199 million in flash loan attack

https://www.chainalysis.com/blog/euler-finance-flash-loan-attack/

DeFi protocol removed an important line of code that led to a $212K hack

https://cointelegraph.com/news/defi-protocol-convergence-removed-code-leading-to-212k-hack

Lurking Where We Least Expect



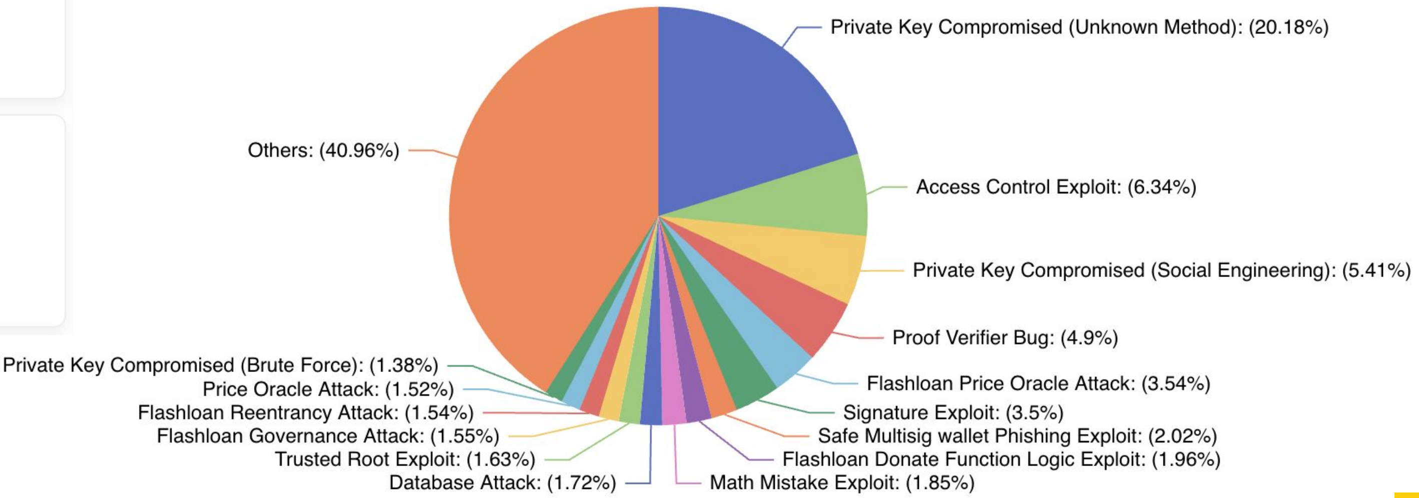
Total Value Hacked (USD)
$9.02b

Total Value Hacked in DeFi (USD)
$6.24b

Total Value Hacked in Bridges (USD)
$2.87b

DefiLlama

https://defillama.com/hacks



What to test?

How to test?

When to test?

...

Testing Methodologies

Unit Testing

Does this feature work?

Integration Testing

Do these features work together?

Mutation Testing

If something goes wrong, would this still work?

Fuzzing

Will this scenario work for a set of random inputs?

Formal Verification

Will this scenario work for any input?

Situational Approaches

Regression, acceptance, coverage, etc.

Testing Methodologies

Unit Testing
Does this feature work?

Integration Testing
Do these features work together?

Mutation Testing
If something goes wrong, would this still work?

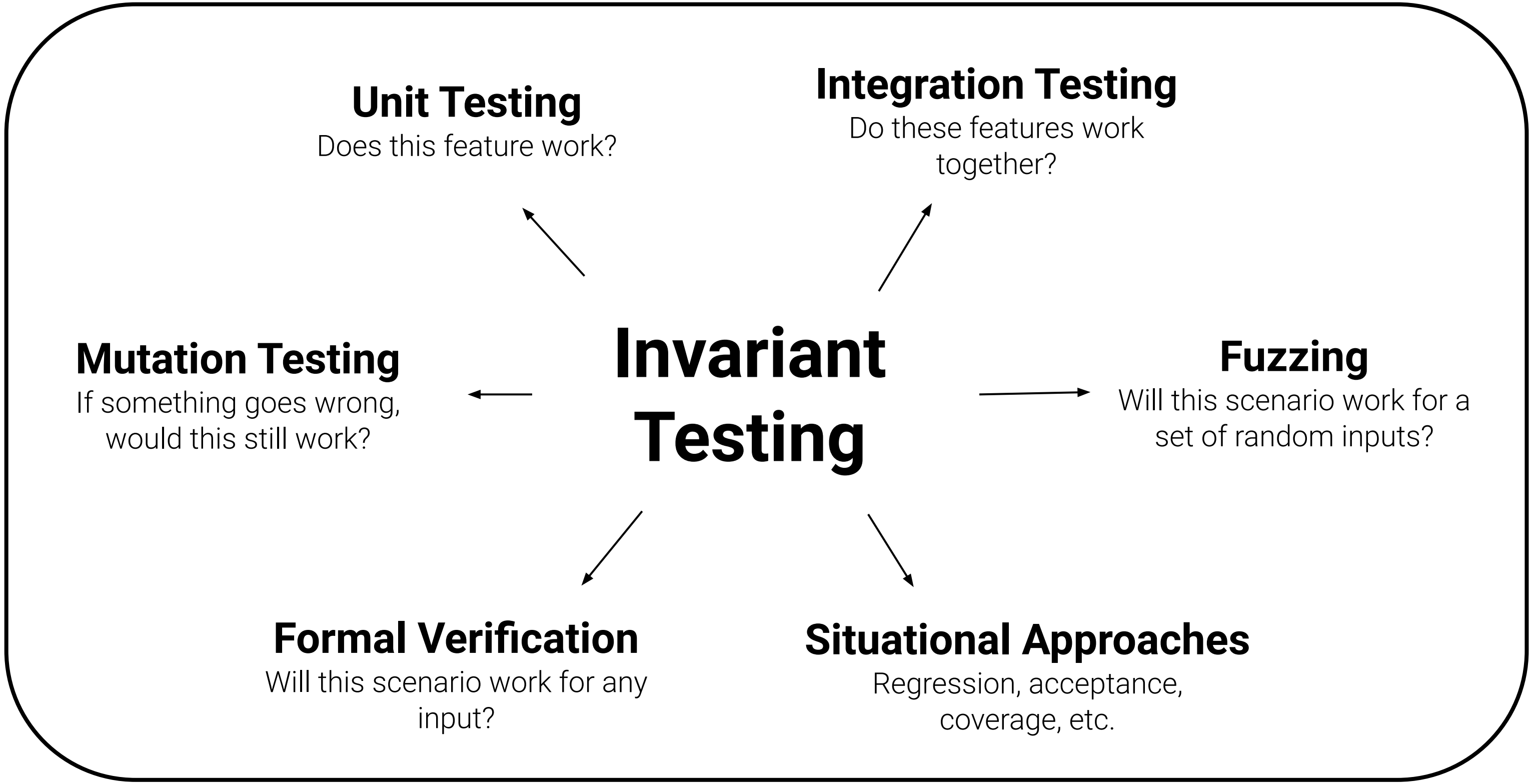
Fuzzing
Will this scenario work for a set of random inputs?

Formal Verification
Will this scenario work for any input?

Situational Approaches
Regression, acceptance, coverage, etc.

Testing Methodologies

runtime verification



Invariant Testing

Unit Testing
Does this feature work?

Integration Testing
Do these features work together?

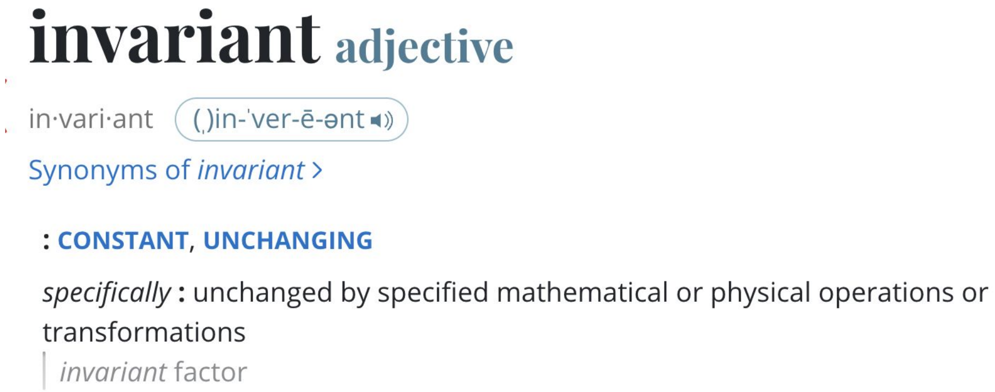
Mutation Testing
If something goes wrong, would this still work?

Fuzzing
Will this scenario work for a set of random inputs?

Formal Verification
Will this scenario work for any input?

Situational Approaches
Regression, acceptance, coverage, etc.

Testing Methodologies



invariant adjective

in·vari·ant (ˌ)in-ˈver-ē-ənt

Synonyms of *invariant* >

: **CONSTANT**, **UNCHANGING**

specifically **:** unchanged by specified mathematical or physical operations or transformations

> *invariant* factor

Sample invariants of an elevator:

1. Does not move with its doors open;
2. If moving, does not open its doors;
3. It always is between a range of floors;

…

Tools For Building Your Solid Ethereum Foundations 🔨

Your Testing Arsenal

General testing frameworks, test Generators, environment testing, and fuzzers

- Foundry
- Echidna
- Hardhat
- Gambit
- Medusa
- fuzz-utils
- Bulloak
- Buildbear
- ItyFuzz
- Waffle
- Vertigo
- Ape

Formal Verification

- Kontrol
- Certora Prover
- Halmos
- Clear
- coq-of-solidity
- hevm

Smart Contract Debugging

With visual aids

- Simbolik
- Tenderly
- Remix

Static Analysis

- Slither
- Remix Analysis
- Solhint

Resources

Foundry - https://book.getfoundry.sh/

Echidna - https://github.com/crytic/echidna/

Hardhat - https://github.com/NomicFoundation/hardhat

ItyFuzz - https://github.com/fuzzland/ityfuzz

Gambit - https://www.certora.com/gambit

Medusa - https://github.com/crytic/medusa

Fuzz-utils - https://github.com/crytic/fuzz-utils

BuildBear - https://www.buildbear.io/

Bulloak - https://github.com/alexfertel/bulloak

Vertigo - https://github.com/JoranHonig/vertigo

Kontrol - https://kontrol.runtimeverification.com/

Certora Prover - https://www.certora.com/prover

Clear - https://github.com/NethermindEth/Clear

Halmos - https://github.com/a16z/halmos

coq-of-solidity - https://github.com/formal-land/coq-of-solidity

hevm - https://github.com/dapphub/dapptools/tree/master/src/hevm

Slither - https://github.com/crytic/slither

Remix Analysis - https://remix-ide.readthedocs.io/en/latest/static_analysis.html#remix-analysis

Solhint - https://github.com/protofire/solhint

Simbolik - https://simbolik.runtimeverification.com/

Tenderly - https://docs.tenderly.co/debugger

Remix - https://remix.ethereum.org/

Waffle - https://github.com/TrueFiEng/Waffle

Ape - https://github.com/ApeWorX/ape

Questions?

aellison.cassimiro@runtimeverification.com

@actsant

Runtime Verification