Inception Deliverables

Project Idea:

To make improvements to Existing tools for Analyzing Smart Contracts named Echidna which takes solidity code to make it more efficient.

GITHUB Repository Link:

https://github.com/AtulUpadhye17/CSE-6324-Team4

Competitors :

We are going to take Echidna tool which takes solidity code and add more features to make it more efficient. The competitors to this tool will be Manticore which takes python code.

Echidna Features:

The existing features of Echidna are

- Generates inputs tailored to your actual code.
- Optional corpus collection, mutation and coverage guidance to find deeper bugs.
- Source code integration to identify which lines are covered after the fuzzing campaign.
- Automatic test case minimization for quick triage.

- Seamless integration into the development workflow.

How Echidna Support for smart contract build systems:

- Echidna can test contracts compiled with different smart contract build systems, including Truffle or hardhat using crytic-compile .
- On top of that, Echidna supports two modes of testing complex contracts. Firstly one can describe an initialization procedure with Truffle and Etheno and use that as the base state for Echidna. Secondly, echidna can call into any contract with a known ABI by passing in the corresponding solidity source in the CLI.

Improvisations we want to make on this tool:

- Introduce more automation in this tool to make the test instances more easier.
- Improve upon code coverage.
- Improving the inputs based on our program.

Risks Associated with this tool:

- Online resources i.e documents and community support which gives more knowledge on the tool are very limitedly available.
- Some not considered security vulnerabilities might turn into existential threats.
- Limitations of the existing tool.

Limitations and some known issues of this tool:

- EVM emulation and testing is hard.
- Echidna has a number of number of limitations in the latest release where some of those are inherited from hevm while some are from design/performance decisions or simply bugs in our code.
- Some issues can be fixed by next release and some may take time and some cannot be fixed.
- Some issues identified were

  1. There is limited library support for testing which cannot be fixed at all.
  2. Also lack of support for function pointers in solidity which is on hold and might be fixed in future.

Customers and Users:

- Smart contract auditors from the following domains can perform audits whenever requested.

  * Finance , Gaming, Healthcare, Real estate etc;

REFERENCES:

- C, C. (n.d.). *GitHub - crytic/echidna: Ethereum smart contract fuzzer*. GitHub. Retrieved September 12, 2022, from https://github.com/crytic/echidna
- T, T. (n.d.). *GitHub - trailofbits/manticore: Symbolic execution tool*. GitHub. Retrieved September 12, 2022, from https://github.com/trailofbits/manticore