18 types of bugs injection methods

Pnegcheng Zhang, Feng Xiao, Xiapu Luo, Hai Dong

Jan 2021

1 introduction

In our paper, we introduce the methods of injecting *re-entrancy* bugs and *integer overflow and underflow* bugs into *HuangGai* in detail. And we write this doc to help users understand how *HuangGai* injects 18 other types of bugs.

2 Predefined extraction criteria and injection methods of 18 types of bugs

1. Transaction order dependence.
    - Predefined extraction criteria: The contract needs to be developed based on *ERC-20 token standard* and includes the *approve* function.
    - injection methods: *HuangGai* invalidates security measures to allow the quota of the approved address is set from one nonzero value to another nonzero value, and label the assignment statement as a bug.
2. Results of contract execution affected by miners.
    - Predefined extraction criteria: *HuangGai* searches for the *if-statements* in a contract that meet the following conditions: When the type of the condition part of the *if-statement* is one of *bytes32*, *address payable*, *uint256*, or *address*, *HuangGai* will record the location and type of the *if-statement*. When such statements exist in a contract, *HuangGai* will be able to inject *results of contract execution affected by miners* bugs into the contract.
    - injection methods: *HuangGai* replaces an operand in the conditional part of the *if-statement* with the following global variables: *block.coinbase* (for address type), *block.coinbase* (for address payable type), *block.gaslimit* (for uint256 type), *block.number* (for uint256 type), *block.timestamp* (for uint256 type), *blockhash(block.number)* (for bytes32 type), and label the *if-statement* as a bug.
3. Unhandled exception.

- Predefined extraction criteria: The contract shall contain at least one of the following three types of statements: *call-statement*, *send-statement*, *delegatecall-statement*.
- injection methods: *HuangGai* uses the following two ways to invalidate the security measures of low-level call statement (*call-statement*, *send-statement*, *delegatecall-statement*): receiving the return value but not checking the return value, or not receiving the return value. And *HuangGai* labels the *if-statement* as a bug.

4. Use *tx.origin* for authentication.
   - Predefined extraction criteria: *HuangGai* first captures the address type variables assigned in the *constructor* (we call these variables *ownerCandidate*) and then searches for bool expressions such as *ownerCandidate = = address type variable* or *ownercandidate != address type variable* in the contract. A contract needs to contain the bool expressions that meet the above conditions.
   - injection methods: *HuanggGai* replaces address type variable (no *ownerCandidate*) in the bool expression that meets the condition with *tx.origin* and labels the bool expression as a bug.
5. Wasteful contracts.
   - Predefined extraction criteria:
   - injection methods:
6. Short address attack.
   - Predefined extraction criteria:
   - injection methods:
7. Suicide contracts.
   - Predefined extraction criteria:
   - injection methods:
8. Locked ether.
   - Predefined extraction criteria:
   - injection methods:
9. Forced to receive ether.
   - Predefined extraction criteria:
   - injection methods:
10. Pre-sent ether.
    - Predefined extraction criteria:

- injection methods:

11. Uninitialized local/state variables.
    - Predefined extraction criteria:
    - injection methods:
12. Hash collisions with multiple variable length arguments.
    - Predefined extraction criteria:
    - injection methods:
13. Specify *function* variable as any type.
    - Predefined extraction criteria:
    - injection methods:
14. Dos by complex *fallback* function.
    - Predefined extraction criteria:
    - injection methods:
15. *Public* function that could be declared *external*.
    - Predefined extraction criteria:
    - injection methods:
16. Non-public variables are accessed by *public*.
    - Predefined extraction criteria:
    - injection methods:
17. Nonstandard naming.
    - Predefined extraction criteria:
    - injection methods:
18. Unlimited compiler versions.
    - Predefined extraction criteria:
    - injection methods: