Vultron: Towards Secure Smart Contracts – A Runtime Monitoring Approach

Student: Yang Xuan             Supervisor: Asst Professor Li Yi

Overview

Vultron is a solution designed to detect and mitigate vulnerabilities during the execution of Ethereum smart contracts. It does so by replicating and inserting debugging instructions into contracts which is executed at no cost.

Advantages

• **Generic:** Vultron is not limited in its detection capabilities to a specific set of vulnerabilities.
• **Accuracy:** Vultron ensures that each detected vulnerability can be exploited and does not generate false positives and false negatives.
• **Informative:** The state of contract and its execution can be traced.

Implementation

```solidity
function add(uint8 x, uint8 y) public
returns (uint8 res) {
    res = x + y;
    assembly {
        gasstop();
    }
    if (res < x) {
        revert();
    }
    assembly {
        gasstart();
    }
}
```

Case Study

Gas manipulating and debugging instructions inserted into smart contract to detect and mitigate vulnerabilities.

Contract is compiled by the modified compiler, which generates the contract’s bytecode and application binary interface.

Ethereum virtual machine executes the specifications generated by the modified compiler as described in the smart contract.