Learning to Fuzz from Symbolic Execution with Application to Smart Contracts

Jingxuan He, Mislav Balunovic, Nodar Ambroladze, Petar Tsankov, Martin Vechev
## Random Fuzzing vs. Symbolic Execution

<table>
<thead>
<tr>
<th></th>
<th>Random Fuzzing</th>
<th>Symbolic Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed</strong></td>
<td>Fast</td>
<td>Slow</td>
</tr>
<tr>
<td><strong>Inputs</strong></td>
<td>Ineffective</td>
<td>Effective</td>
</tr>
<tr>
<td><strong>Coverage</strong></td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Smart Contract Testing: Challenge

```solidity
contract Wallet {
    address owner;

    constructor() {
        owner = msg.sender;
    }

    function setOwner(address newOwner) {
        // fix: require(msg.sender == owner);
        owner = newOwner;
    }

    function deposit() payable {}

    function withdraw(uint amount) {
        require(msg.sender == owner);
        owner.transfer(amount);
    }
}
```
Smart Contract Testing: Challenge

**Wanted:** Transaction sequences that thoroughly explore the state space
Wallet bug freezes more than $150 million worth of Ethereum

By Stan Schroeder

A bug in Parity, a popular wallet for the cryptocurrency and decentralized application platform Ethereum, may have resulted in more than $150 million worth of ether being permanently frozen.

BatchOverflow Exploit Creates Trillions of Ethereum Tokens, Major Exchanges Halt ERC20 Deposits

April 25, 2018 at 10:18 pm UTC - 3 min read

A newly discovered Ethereum smart contract exploit has resulted in the generation of billions of ERC20 tokens, causing major exchanges to temporarily halt ERC20 deposits and withdrawals until all tokens can be assessed for vulnerability.

The DAO Attacked: Code Issue Leaked $60 Million Ether Theft

By Michael del Castillo

The DAO, the distributed autonomous organization that had collected over $150m worth of the currency ether, has reportedly been hacked, sparking a broad market sell-off.

DAO is an experimental,Surname the “child DAO”.

ديرلس organization comprised of a series of smart contracts written on the ethereum co

DAO has lost 36m ether, which is currently sitting in a separate wallet after being split off.
# Random Fuzzing vs. Symbolic Execution

<table>
<thead>
<tr>
<th></th>
<th>Random Fuzzing</th>
<th>Symbolic Execution</th>
<th>ILF (this work)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed</strong></td>
<td>✔️ Fast</td>
<td>✗ Slow</td>
<td>✔️ Fast</td>
</tr>
<tr>
<td><strong>Inputs</strong></td>
<td>✗ Ineffective</td>
<td>✔️ Effective</td>
<td>✔️ Effective</td>
</tr>
<tr>
<td><strong>Coverage</strong></td>
<td>✗ Low</td>
<td>✗ Low</td>
<td>✔️ High</td>
</tr>
</tbody>
</table>

- Analyzing Ethereum’s Contract Topology. Kiffer et al.. IMC ’18

**Imitation Learning based Fuzzer**

| ~120K contracts | ~16K clusters |

- Analyzing Ethereum’s Contract Topology. Kiffer et al.. IMC ’18
Imitation Learning

- Human expert
- Robot

Demonstration

- Symbolic execution
- Fuzzer

Demonstration
Learning to Fuzz from Symbolic Execution

Training

- Smart contracts
- Transaction sequences

Symbolic execution expert

Fuzzing

- New contract
- Fuzzing policy (neural networks)

Coverage

Vulnerability Report

≈ 15K contracts
Learning to Fuzz from Symbolic Execution

Training

Symbolic execution expert

Smart contracts

Transaction sequences

Fuzzing

New contract

Fuzzing policy (neural networks)

Coverage

Vulnerability Report
Smart Contract Fuzzing Policy

Example: a Uniformly Random Policy

- : Uniform($F$)
- : Uniform(Signature($f$))
- : Uniform(SENDERS)
- : $\begin{cases} Uniform([0, MA]) & \text{f is payable} \\ P(0) = 1 & \text{otherwise} \end{cases}$

Transaction

Fuzzing Policy

Tested Contract

Feedback

may modify blockchain state
Neural Network Fuzzing Policy

Feature of $f_{i-1}$ → GRU_{fuzz} at step $i$ → hidden state $h_i$ → GRU_{fuzz} at step $i + 1$

Features of $F$

- FCN_{func} → $f_i$
- GRU_{int} + FCN_{int} → $\bar{x}_i$
- FCN_{sender} → $sender_i$
- FCN_{amount} → $amount_i$
Neural Network Fuzzing Policy – Fuzzing State

Feature of $f_{i-1}$

[1, 6.2, 5, ...]

e.g., Coverage, opcodes, function name. (can be dynamic)

GRU$_{\text{fuzz}}$ at step $i - 1$

[3.5, 0.3, 4.0, ...]

Last hidden state

GRU$_{\text{fuzz}}$ at step $i$

[1.2, 8.7, 2.5, ...]

Current hidden state
Neural Network Fuzzing Policy

Features of $F$

- $GRU_{fuzz}$ at step $i - 1$
  - hidden state $h_{i-1}$
- $GRU_{fuzz}$ at step $i$
  - hidden state $h_i$
- $GRU_{fuzz}$ at step $i + 1$

- $FCN_{func}$
- $GRU_{int} + FCN_{int}$
- $FCN_{sender}$
- $FCN_{amount}$

Features of $F$:

- $f_i$
- $\tilde{x}_i$
- $sender_i$
- $amount_i$
Neural Network Fuzzing Policy – Function

Current hidden state: [1.2, 8.7, 2.5, ...]

Feature of $F$: 
- [[1, 6.2, 5, ...],
  [4, 3.7, 6, ...],
  ...,
  [2, 9.2, 7, ...]]

$\text{FCN}_{\text{func}} + \text{Softmax}$

- SetOwner
- Deposit
- Withdraw

Withdraw
Neural Network Fuzzing Policy

$\text{GRU}_{\text{fuzz}}$ at step $i - 1$

$\text{GRU}_{\text{fuzz}}$ at step $i$

$\text{GRU}_{\text{fuzz}}$ at step $i + 1$

Hidden state $h_{i-1}$

Hidden state $h_i$

Feature of $f_{i-1}$

Features of $F$

$\text{FCN}_{\text{func}}$

$\text{GRU}_{\text{int}} + \text{FCN}_{\text{int}}$

$\text{FCN}_{\text{sender}}$

$\text{FCN}_{\text{amount}}$

Feature of $f_i$

$\bar{x}_i$

$\tilde{x}_i$

$\text{sender}_i$

$\text{amount}_i$
Neural Network Fuzzing Policy – Arguments

Current hidden state
[1.2, 8.7, 2.5, ...]

Distribution over 50 seed integer values from expert

One-hot
[0, 0, 1, 0, ...]
Neural Network Fuzzing Policy

{\text{GRU}_\text{fuzz} \text{ at step } i - 1 \rightarrow \text{hidden state } h_{i-1} \rightarrow \text{Feature of } f_{i-1} \rightarrow \text{GRU}_\text{fuzz} \text{ at step } i \rightarrow \text{hidden state } h_i \rightarrow \text{GRU}_\text{fuzz} \text{ at step } i + 1

Features of \( F \)

\rightarrow \text{FCN}_\text{func} \rightarrow f_i

\rightarrow \text{GRU}_\text{int} + \text{FCN}_\text{int} \rightarrow \bar{x}_i

\rightarrow \text{FCN}_\text{sender} \rightarrow \text{sender}_i

\rightarrow \text{FCN}_\text{amount} \rightarrow \text{amount}_i
Learning to Fuzz from Symbolic Execution

Symbolic execution expert

Training
Smart contracts
Transaction sequences

Fuzzing
New contract
Fuzzing policy (neural networks)
Coverage
Vulnerability Report

(neural networks)
Symbolic Execution Expert

Revisit

$\text{Execute}$

$\text{Revisit}$

Symbolic: VerX
S&P 2020
Learning to Fuzz from Symbolic Execution

Symbolic execution expert

Transaction sequences

Fuzzing policy (neural networks)

Coverage

Vulnerability Report

Training Smart contracts

Fuzzing New contract
Training Neural Network Fuzzing Policy

NN Policy at step $i - 1$

Hidden State

Features

NN Policy at step $i$

Inference

Cross-Entropy loss

$t_i$ by expert

$f_i$

$\bar{x}_i$

$sender_i$

$amount_i$
Learning to Fuzz from Symbolic Execution

Training

Symbolic execution expert

Smart contracts → Transaction sequences

Fuzzing

New contract → Fuzzing policy (neural networks)

Coverage

Vulnerability Report
ILF System: Coverage & Vulnerability Detection

- **Instruction** coverage.
- **Basic block** coverage.

- **Locking**: The contract cannot send out but can receive ether.
- **Leaking**: An attacker can steal ether from the contract.
- **Suicidal**: An attacker can deconstruct the contract.
- **Block Dependency**: Ether transfer depends on block state variables.
- **Unhandled Exception**: Root call does not catch exceptions from child calls.
- **Controlled Delegatecall**: Transaction parameters explicitly flow into arguments of a `delegatecall` instruction.
Evaluation

- 18,496 Contracts (5,013 Large & 13,483 Small)
- 5-fold Cross Validation

- UNIF
- Echidna
- EXPERT
- MAIAN
- ContractFuzzer

- Coverage & Speed
- Fuzzing Components
- Vulnerability Detection
- Case Study
Coverage: ILF vs. Fuzzers

Small contracts

Large contracts
Coverage: ILF vs. Symbolic Expert

![Graph showing coverage for small and large contracts for ILF and Symbolic Expert]

- **Small Contracts**
  - ILF (#tx same as EXPERT): 30 txs, 547s
  - ILF (2k txs): 148 txs/s

- **Large Contracts**
  - ILF (#tx same as EXPERT): 49 txs, 2,580s
  - ILF (2k txs): 17s

Small: 30 txs, 547s  
Large: 49 txs, 2,580s  
Small: 13s  
Large: 17s  
148 txs/s
Vulnerability Detection

% of True Vulnerabilities

Leaking  Suicidal  Locking

ILF  UNIF  MAIAN

13 FPs

% of True Vulnerabilities

Block Dependency  Unhandled Exception  Controlled Delegatecall

ILF  UNIF  ContractFuzzer

6 FPs

ILF: 0 FPs
Importance of Policy Components

All components are necessary

Most important
Summary

Q & A