Evil Under the Sun:
Understanding and Discovering Attacks on
Ethereum Decentralized Applications

Liya Su\textsuperscript{1,2,3}
Xinyue Shen\textsuperscript{1,4}
Xiangyu Du\textsuperscript{1,2,3}
Xiaojing Liao\textsuperscript{1}
XiaoFeng Wang\textsuperscript{1}
Luyi Xing\textsuperscript{1}
Baoxu Liu\textsuperscript{2}

\textsuperscript{1}Indiana University Bloomington
\textsuperscript{2}Institute of Information Engineering, Chinese Academy of Sciences,
\textsuperscript{3}University of Chinese Academy of Sciences
\textsuperscript{4}Alibaba Group
Background

- Ethereum: computer programs on the blockchain
- Externally Owned Accounts (EOAs)
- Smart Contract: deploy on Ethereum
- Dapp: public smart contract
Background

Dapp Attack

Attacker
Smart contract
Transaction

Call

Dapp

Transaction

Ethereum

Attacker

Dapp

Transaction
Background

Requirement

Facts

3,137 Dapps
63,77k active users
Over 1 million transactions
7.55 million USD

14K Ethers from the victim Fomo3D
No extensive forensic analysis
Research Questions

What like and how the attacks launch on real-world Dapps?

How to automatically reconstruct Dapp attacks?

How to find new attack and 0-day victim Dapps?
Transaction based Forensic Analysis

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TO</strong></td>
<td>0x54*</td>
</tr>
<tr>
<td><strong>FROM</strong></td>
<td>0x73*</td>
</tr>
<tr>
<td><strong>VALUE</strong></td>
<td>0.01 Ether</td>
</tr>
<tr>
<td><strong>DATA</strong></td>
<td>0xc52ab778 (methodID of function execute())</td>
</tr>
<tr>
<td><strong>GAS PRICE</strong></td>
<td>6.3x10^{-9} Ether (6.3 Gwei)</td>
</tr>
</tbody>
</table>

1. (0x73*, 0x54*, execute(0xa6*), 0.1 ETH)
2. (0x54*, 0xa6*, airDropPot_(), 0 ETH)
3. (0x54*, 0xa6*, airDropTracker_(), 0 ETH)
4. (0x54*, 0x07*, execute(0xa6*), 0.1 ETH)
5. (0x07*, 0xf7*, create, 0.1 ETH)
6. (0xf7*, 0xa6*, buyXid(0x0000), 0.1 ETH)
7. (0xf7*, 0xa6*, withdraw(), 0 ETH)
8. (0xa6*, 0xf7*, transfer, 0.1012 ETH)
9. (0xf7*, 0x73*, suicide, 0.1012 ETH)
Example of transaction execution traces.

- `O`: exploit contract, `DXVECTOR`: contract generated in execution, `●`: Dapp, `◇`: EOA.
Analyzing Exploit Transactions

Workflow of the measurement approach.

Data Collection and Derivation
Analyzing Exploit Transactions

Data Collection and Derivation

Table 2: Known Dapp attacks. $D_s$ is the set of data collected from the reports, and $D_e$ includes those derived.

<table>
<thead>
<tr>
<th>Attack type</th>
<th># of Dapps</th>
<th># of exploit contracts</th>
<th># of attacker EOAs</th>
<th># of attack transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$D_s$</td>
<td>$D_e$</td>
<td>$D_s$</td>
<td>$D_e$</td>
</tr>
<tr>
<td>Bad randomness</td>
<td>4</td>
<td>14</td>
<td>9</td>
<td>19</td>
</tr>
<tr>
<td>DoS</td>
<td>4</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Integer overflow/underflow</td>
<td>13</td>
<td>32</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Reentrancy</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Improper authentication</td>
<td>12</td>
<td>18</td>
<td>6</td>
<td>18</td>
</tr>
<tr>
<td>Unique total</td>
<td>25</td>
<td>56</td>
<td>20</td>
<td>45</td>
</tr>
</tbody>
</table>
Analyzing Exploit Transactions

Example of Dapp criminal footprints.
Analyzing Exploit Transactions

Preparation: Testing contracts or transferring fund

Testing transaction in preparation stage.
Analyzing Exploit Transactions

Exploitation: The adversary tends to rapidly evolve his strategies

Exploit contract evolution at the exploitation stage.
DEFIER: Idea and Design

Figure 6: Sequence representation.
DEFIER: Idea and Design

Preprocessing

Transaction clustering

\[ D(g_1, g_2) = \alpha \min_{(o_1, \ldots, o_k) \in O(g_1, g_2)} \sum_{i=1}^{k} c(o_i) + \beta \Delta t \]  \hspace{1cm} (1)

- Structure similarity
- Timing closeness
DEFIER: Idea and Design

Sequence-based Classification

EOA-Dapp-execution attention model: highlight the useful information related to the EOA's intent on the Dapp.

Output types: normal, preparation, exploitation, propagation and completion.
Discussing the Result

Table 6: Dataset and evaluation results.

<table>
<thead>
<tr>
<th>Dataset</th>
<th># transactions</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groundtruth set</td>
<td>badset 57,855</td>
<td>( \text{pre}<em>{\text{micro}} 98.2%, \text{pre}</em>{\text{macro}} 92.4% )</td>
</tr>
<tr>
<td></td>
<td>goodset 39,124</td>
<td>( \text{rec}<em>{\text{micro}} 98.1%, \text{rec}</em>{\text{macro}} 98.4% )</td>
</tr>
<tr>
<td>Unknown set</td>
<td>2,350,779</td>
<td>( \text{pre}_{\text{micro}} 91.7% ) positive 476,334</td>
</tr>
<tr>
<td>Sampled testset</td>
<td>30,888</td>
<td>( \text{pre}_{\text{macro}} 83.6% )</td>
</tr>
</tbody>
</table>

\( \text{pre}_{\text{micro}} \) and \( \text{pre}_{\text{macro}} \): micro of precision, macro of precision

\( \text{rec}_{\text{micro}} \) and \( \text{rec}_{\text{macro}} \): micro of recall, macro of recall

\( \text{positive} \): transactions that labeled as one of attack stages
Discussing the Result

Table 10: Victim Dapps in different categories.

<table>
<thead>
<tr>
<th>Type</th>
<th># Dapps/0-day</th>
<th># attacker EOAs/0-day</th>
<th># exploit transactions/0-day</th>
<th>ex. of victim Dapps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gambling</td>
<td>51/43</td>
<td>65,778 /11,339</td>
<td>360,524 /114,473</td>
<td>Lucky Blocks</td>
</tr>
<tr>
<td>Game</td>
<td>28/27</td>
<td>959/919</td>
<td>52,673 /52,176</td>
<td>SpaceWar</td>
</tr>
<tr>
<td>Finance</td>
<td>5/5</td>
<td>183/183</td>
<td>59,872 /59,872</td>
<td>STOX</td>
</tr>
<tr>
<td>Token</td>
<td>2/1</td>
<td>279/167</td>
<td>4,478/472</td>
<td>Power of Bubble</td>
</tr>
<tr>
<td>Total</td>
<td>85/75</td>
<td>67,199 /12,608</td>
<td>476,342 /226,763</td>
<td></td>
</tr>
</tbody>
</table>

Table 11: Unknown set result.

<table>
<thead>
<tr>
<th>Attack stage</th>
<th># Dapps/0-day</th>
<th># attacker EOAs/0-day</th>
<th># exploit transactions/0-day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack</td>
<td>80/70</td>
<td>42,661/8,237</td>
<td>214,408/106,436</td>
</tr>
<tr>
<td>preparation</td>
<td>85/75</td>
<td>35,955/3,650</td>
<td>143,179/39,908</td>
</tr>
<tr>
<td>Exploitation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack</td>
<td>75/65</td>
<td>18,466/6,545</td>
<td>118,755/80,419</td>
</tr>
<tr>
<td>propagation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The first measurement study and forensic analysis on real-world Dapp attacks.

Our new understanding and CTI discovered can help mitigate the threat to Dapps.

Discover 476,342 exploit transactions on 85 target (with a microprecision of 91.7%).

DEFIER reported 75 0-day victim Dapps.

An attack lifecycle discovery tool can potentially be used to disrupt exploits, sometimes even before damages are inflicted.
Thank you!

Authors: Liya Su, Xinyue Shen, Xiangyu Du, Xiaojing Liao, Xiaofeng Wang, Luyi Xing, Baoxu Liu

Contact: suliya@iie.ac.cn

Availability: The annotated data and the implementation of DEFIER is available at https://drive.google.com/drive/folders/1cdD1gHNbWIS228QXmeUReougSLk1kvf?usp=sharing.