以太坊闪电贷攻击检测

夏清, 黄智榕, 窦文生, 张亚丰, 张凤军, 梁赓, 左春

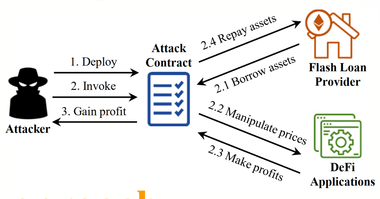
Detecting Flash Loan Based Attacks in Ethereum

The 42nd IEEE International Conference on Distributed Computing Systems (ICDCS 2023)

联系方式：夏清, 18810288615, xiaqing2018@iscas.ac.cn

Background

- **Ethereum**
  - *An open-source Blockchain platform*
  - *Support smart contract*
  - *Two main types of crypto assets: native Ether and various ERC20 tokens*
- **Flash loan based price manipulation attacks (flpAttack)**



Motivation

- **Empirical study of flpAttacks**
  - *Collect 22 real-world attacks in the past two yrs*
  - *17 attacks conform to 3 attack patterns*
  - *4 Keep Raising Price (KRP) attacks*
  - *8 Symmetrical Buying and Selling (SBS) attacks*
  - *6 Multi-Round Buying and Selling (MBS) attacks*

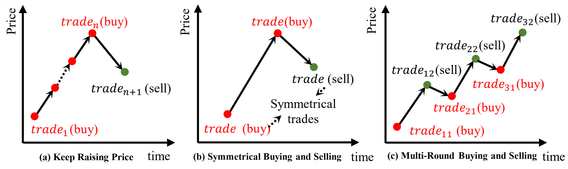
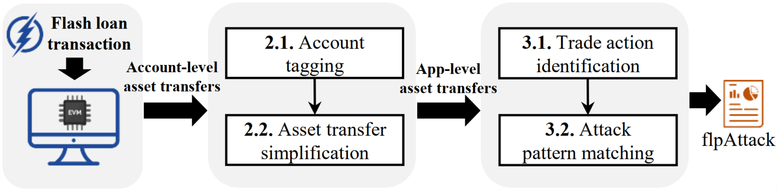


Figure. Three attack patterns summarized from real-world flpAttacks

Approach

LeiShen *is an approach to automatically detect flpAttacks. It takes a flash loan transaction as input and returns a detailed report regarding attack patterns as output.*



- **Extracting transfer history**
  - *Identify flash loan transactions*
  - *Replay a transaction to obtain the history of asset transfers*
- **Constructing application-level asset transfers**
  - *Tag an account with a DeFi application name*
  - *Convert the tagged account-level asset transfers into app-level asset transfers with specified rules*
- **Identifying attack patterns**
  - *Identify key trades*
  - *Check whether these trades conform to an attack pattern*

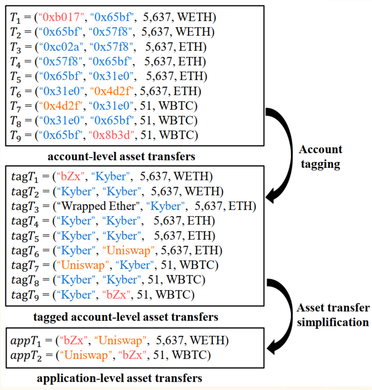


Figure. Construct application-level asset transfers in bZx-1 attack

Evaluation

- **Detecting known flpAttacks**
  - *Detect 14 flpAttacks with correct patterns*
- **Detecting unknown flpAttacks**
  - *Identify 272,984 flash loan transactions in the first 14.5 million blocks*
  - *In the detected 180 attacks, 142 are verified as true attacks (precision: 78.9%)*
  - *109 unknown attacks are firstly detected*
- **Analyze unknown flpAttacks**
  - *TOP3 most attacked applications are well-known decentralized exchanges*
  - *Result in a total profit of over $21.8 million*
  - *The maximum yield rate and net profit are 2.2 ∗ 10^5% and over $6 million*

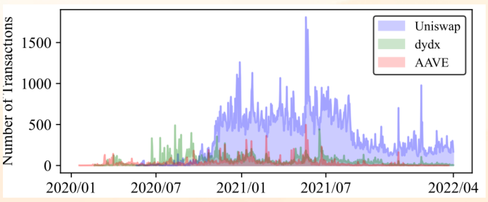


Figure. Weekly flash loan transactions from three popular DeFi applications

Figure. Monthly flpAttacks in Ethereum

Table. The TOP three most attacked apps

Attacked applications	Attacks	Attackers	Attack contracts	Attacked assets
Balancer	31	5	14	13
Uniswap	16	6	8	5
Yearn	11	1	1	1

Table. Attacked profit on detected attacks

	Yield rate (%)	Net profit ($)
Mean	0.3%	3,509
Min.	0.003%	23
Max.	$2.2 * 10^5$%	6,102,198
TOP 10% in AVG	$5.7 * 10^4$%	257,078
TOP 20% in AVG	$3.0 * 10^4$%	135,522