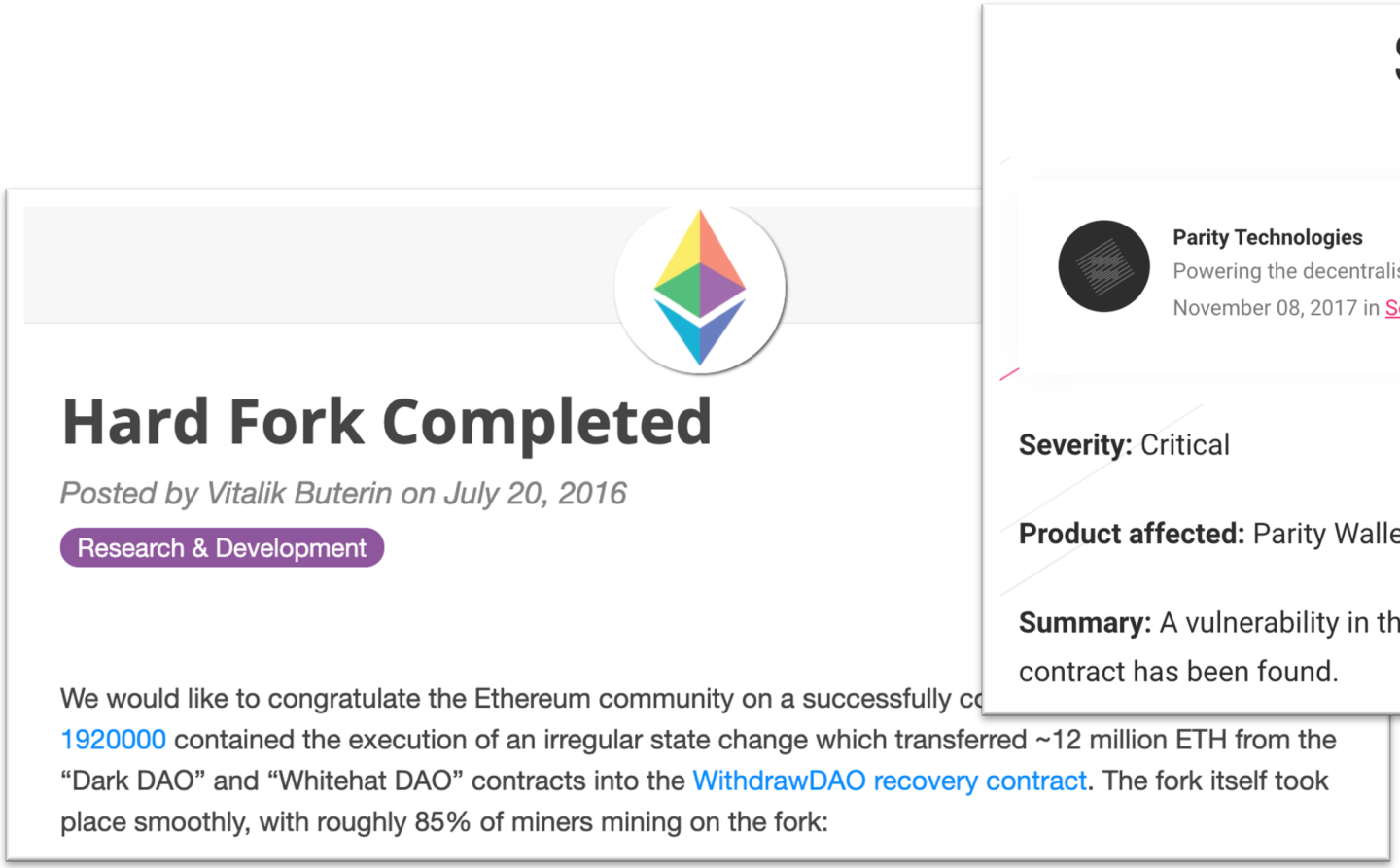
An Ever-evolving Game: Evaluation of Real-world Attacks and Defenses in Ethereum Ecosystem

Shunfan Zhou, Zhemin Yang, Jie Xiang, Yinzhi Cao†,
Min Yang, and Yuan Zhang

Fudan University, † Johns Hopkins University

Smart Contract Incidents

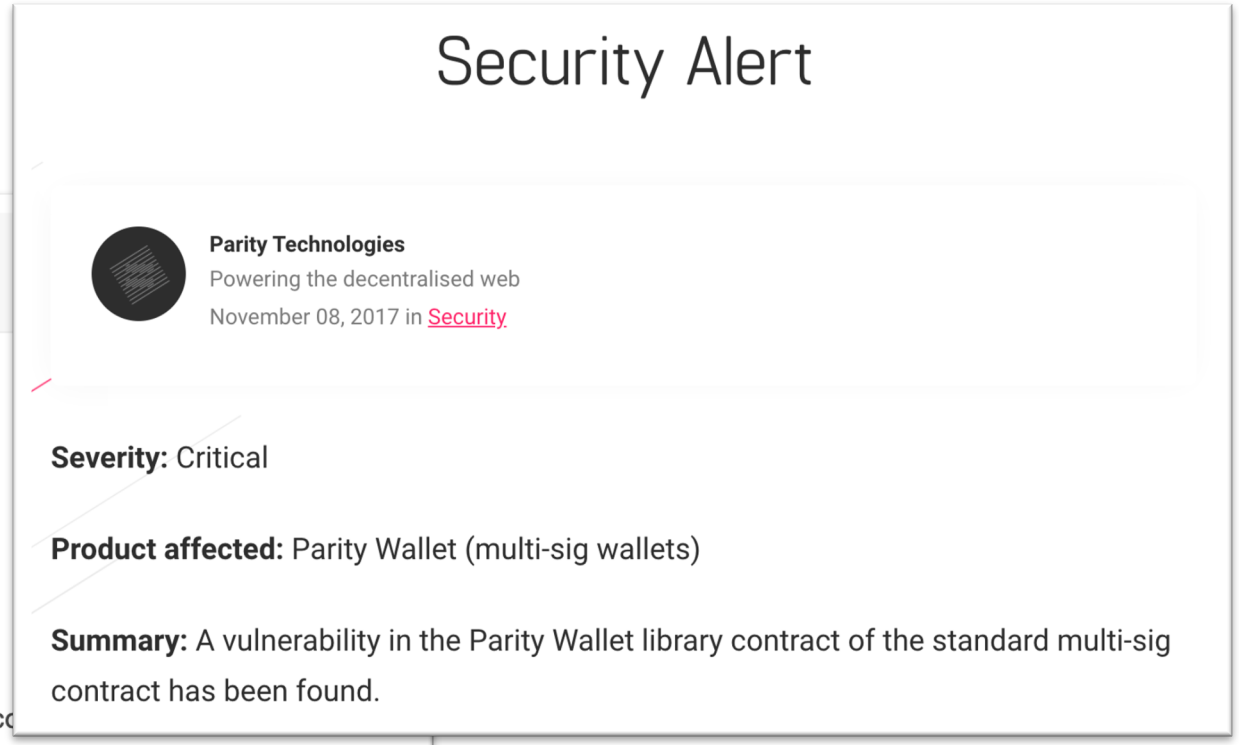


Hard Fork Completed

Posted by Vitalik Buterin on July 20, 2016

Research & Development

We would like to congratulate the Ethereum community on a successfully c
1920000 contained the execution of an irregular state change which transferred ~12 million ETH from the "Dark DAO" and "Whitehat DAO" contracts into the WithdrawDAO recovery contract. The fork itself took place smoothly, with roughly 85% of miners mining on the fork:



Security Alert

Parity Technologies
Powering the decentralised web
November 08, 2017 in Security

Severity: Critical

Product affected: Parity Wallet (multi-sig wallets)

Summary: A vulnerability in the Parity Wallet library contract of the standard multi-sig contract has been found.

https://blog.ethereum.org/2016/07/20/hard-fork-completed/
https://www.parity.io/security-alert-2/

Are they exploited?

- Vulnerable contracts reported
  - 8.8k by Oyente, CCS ’16
  - 5k by Securify, CCS ‘18
  - 21k by ZEUS, NDSS ’18
  - …
- Perez and Livshits, arXiv:1902.06710
  - “at most 504 out of 21,270 contracts have been subjected to exploits”

- Gap exists between vulnerable contracts and real-world attacks!

Questions

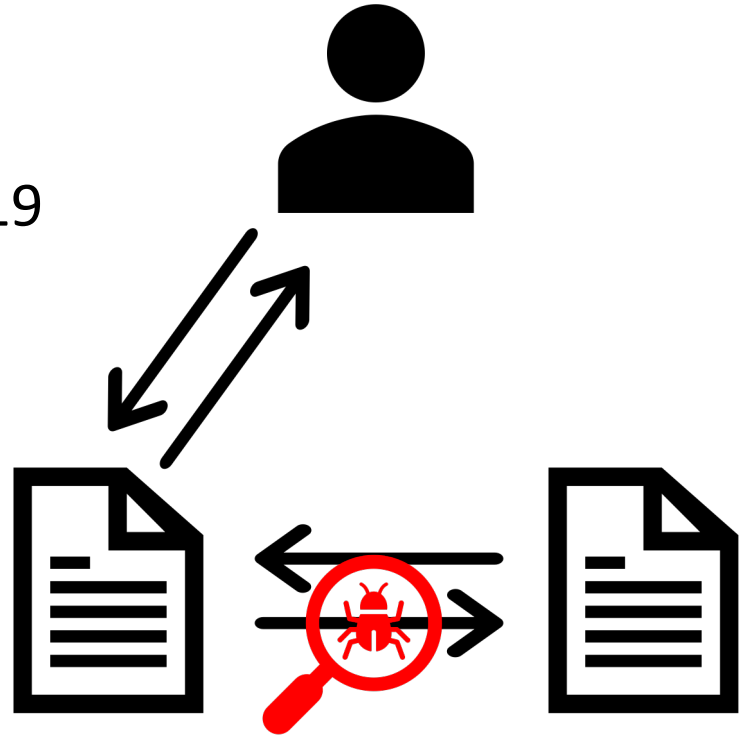
What contracts have been attacked?

and

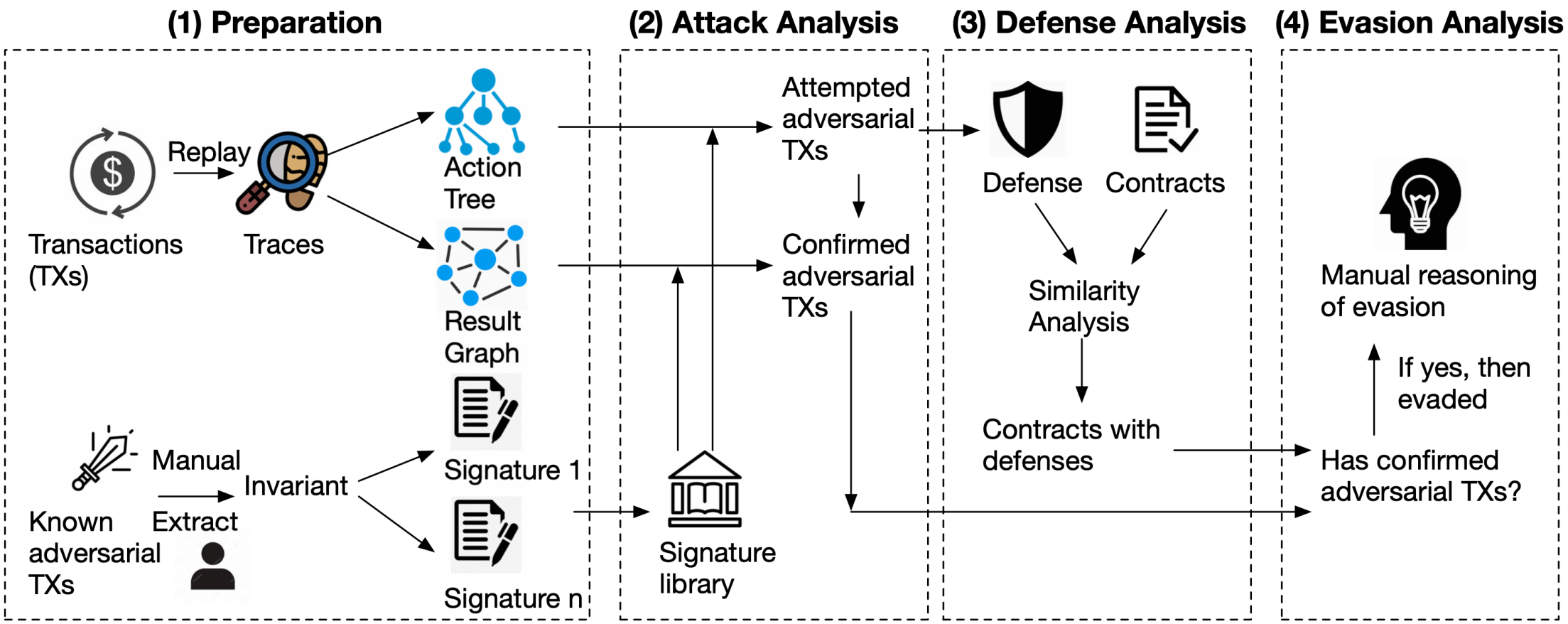
What attacks have been prevented?

From contracts to transactions

- Task: Examine all the transactions in Ethereum
  - 420m transactions from August 2015 to March 2019



Measurement Workflow



Airdrop Hunting Example

```
1   contract Simoleon is ERC20Interface {
2       function transfer(address _to, uint256
            _amount) returns (bool success) {
3           initialize(msg.sender);
4           ...
5       }
6       function initialize(address _address)
            internal returns (bool success) {
7           if (!initialized[_address]) {
8               initialized[_address] = true;
9               balance[_address]=_airdropAmount;
10          }
11      }
12  }
```

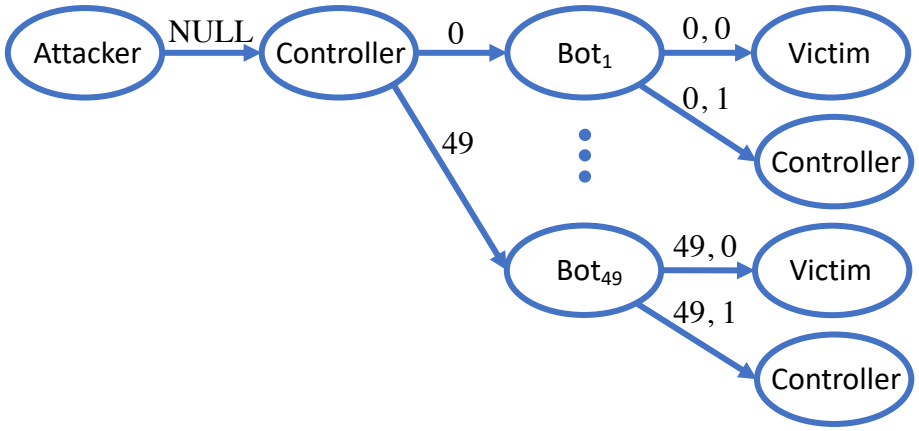
An attack transaction

Address	From	To	Payload		Type	Value	Status
			Entry function	Parameters			
NULL	Attacker	Controller	0x2b6cab44	0x32	call	0	Success
0	Controller	Bot_1	N/A	N/A	create	0	Success
0,0	Bot_1	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
0,1	Bot_1	Controller	N/A	N/A	suicide	0	Success
...	...	...	...	...	...	...	
49	Controller	Bot_{50}	N/A	N/A	create	0	Success
49,0	Bot_{50}	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
49,1	Bot_{50}	Controller	N/A	N/A	suicide	0	Success

An attack transaction

Address	From	To	Payload		Type	Value	Status
			Entry function	Parameters			
NULL	Attacker	Controller	0x2b6cab44	0x32	call	0	Success
0	Controller	Bot_1	N/A	N/A	create	0	Success
0,0	Bot_1	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
0,1	Bot_1	Controller	N/A	N/A	suicide	0	Success
...	...	...	...	...	...	...	
49	Controller	Bot_{50}	N/A	N/A	create	0	Success
49,0	Bot_{50}	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
49,1	Bot_{50}	Controller	N/A	N/A	suicide	0	Success

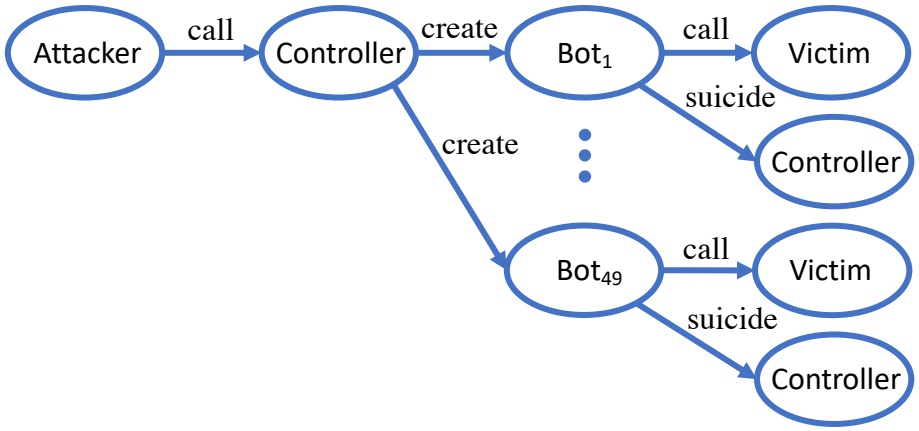
Action Tree



An attack transaction

Address	From	To	Payload		Type	Value	Status
			Entry function	Parameters			
NULL	Attacker	Controller	0x2b6cab44	0x32	call	0	Success
0	Controller	Bot_1	N/A	N/A	create	0	Success
0,0	Bot_1	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
0,1	Bot_1	Controller	N/A	N/A	suicide	0	Success
...	...	...	...	...	...	...	
49	Controller	Bot_{50}	N/A	N/A	create	0	Success
49,0	Bot_{50}	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
49,1	Bot_{50}	Controller	N/A	N/A	suicide	0	Success

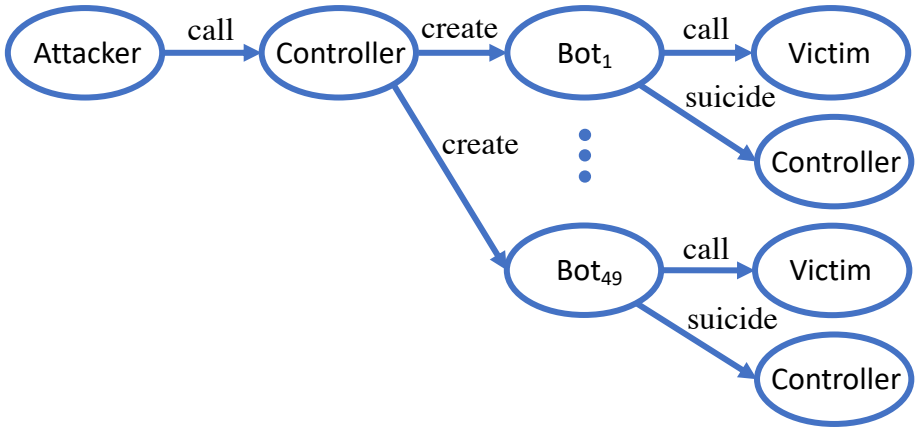
Action Tree



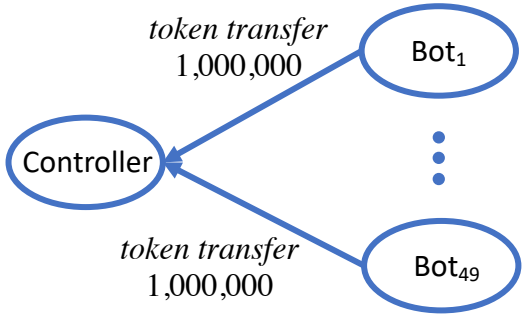
An attack transaction

Address	From	To	Payload		Type	Value	Status
			Entry function	Parameters			
NULL	Attacker	Controller	0x2b6cab44	0x32	call	0	Success
0	Controller	Bot_1	N/A	N/A	create	0	Success
0,0	Bot_1	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
0,1	Bot_1	Controller	N/A	N/A	suicide	0	Success
...	...	...	...	...	...	...	
49	Controller	Bot_{50}	N/A	N/A	create	0	Success
49,0	Bot_{50}	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Success
49,1	Bot_{50}	Controller	N/A	N/A	suicide	0	Success

Action Tree

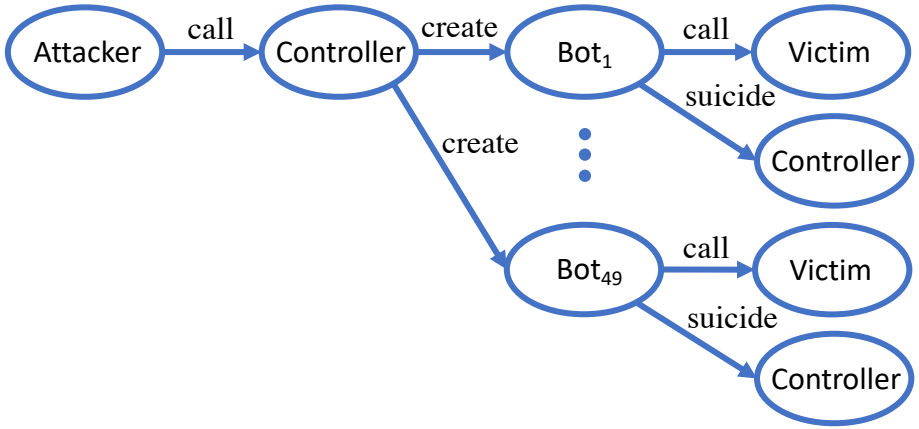


Result Graph

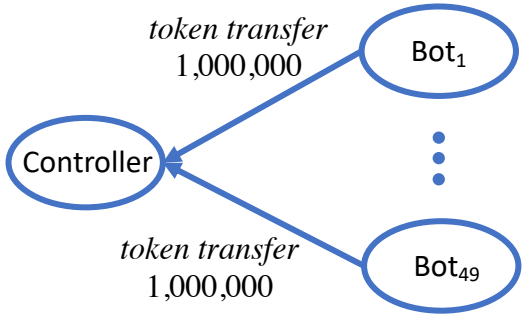


Signature Matching

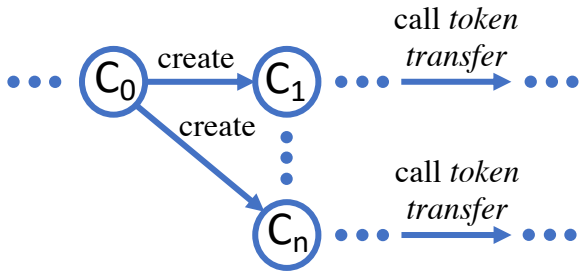
Action Tree



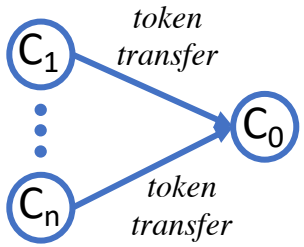
Result Graph



Action Clause

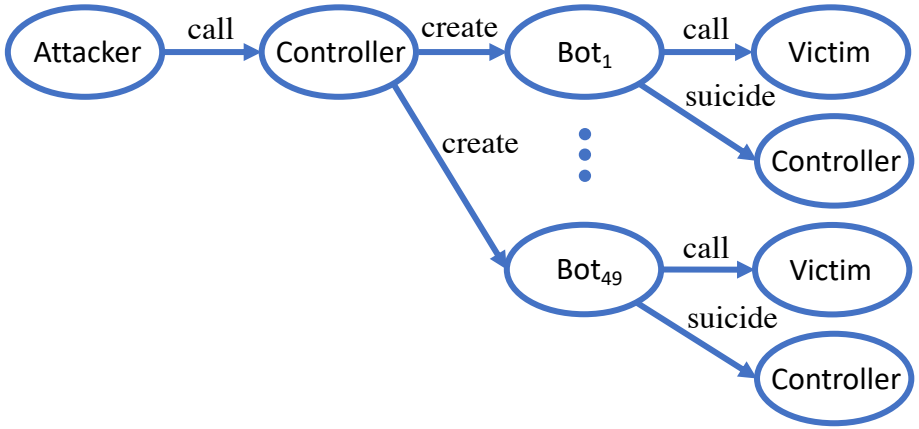


Result Clause

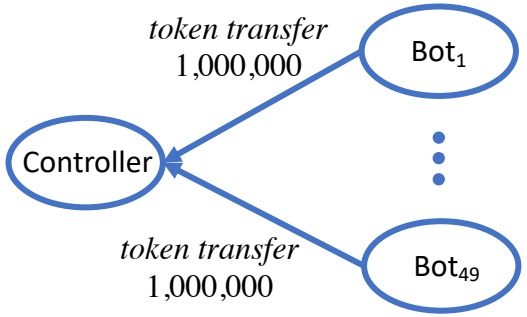


Signature Matching

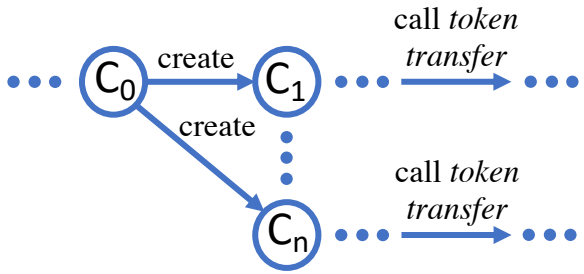
Action Tree



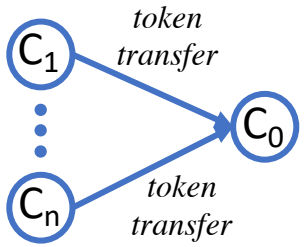
Result Graph



Action Clause



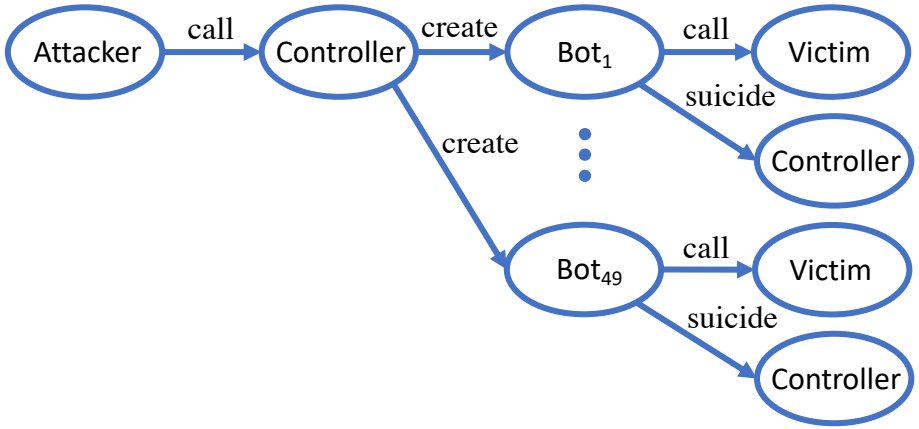
Result Clause



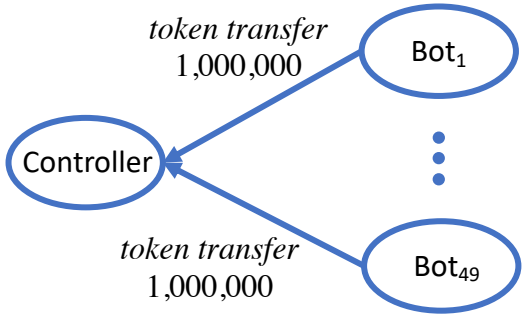
Attempted Adversarial ✓

Signature Matching

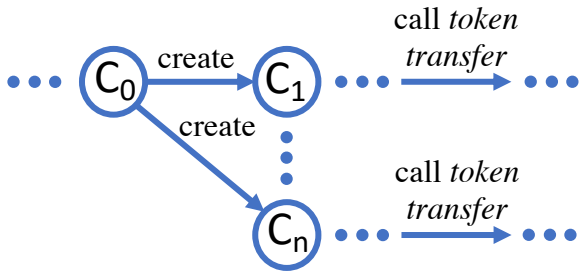
Action Tree



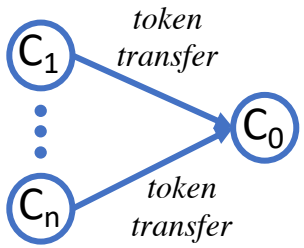
Result Graph



Action Clause



Result Clause



Attempted Adversarial ✓

Confirmed Adversarial ✓

Failed attack transaction

Address	From	To	Payload		Type	Value	Status
			Entry function	Parameters			
NULL	Attacker	Controller	0x2b6cab44	0x32	call	0	Success
0	Controller	Bot_1	N/A	N/A	create	0	Success
0,0	Bot_1	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Reverted
0,1	Bot_1	Controller	N/A	N/A	suicide	0	Success
...	...	...	...	...	...	...	
49	Controller	Bot_{50}	N/A	N/A	create	0	Success
49,0	Bot_{50}	Victim	transfer(address,uint256)	_to: Controller, _amount: 1,000,000	call	0	Reverted
49,1	Bot_{50}	Controller	N/A	N/A	suicide	0	Success

Defense Examples

```
1   modifier isHuman() {
2       address _addr = msg.sender;
3       uint256 _codeLength;
4
5       assembly {_codeLength := extcodesize(_addr
            )}
6       require(_codeLength == 0, "humans␣only");
7       _;
8   }
9   modifier anotherIsHuman() {
10      require(tx.origin == msg.sender, "humans␣
            only");
11      _;
12  }
```

Evaluation: False Positive

Vulnerability	Preliminary Results		False Positives (FPs)				True Positives (TPs) after Manual Filtering		
	# contract	# confirmed atx	# contract	# confirmed atx	% contract	% atx	# contract	# confirmed atx	# attempted atx
call injection	642	2,996	20	286	3.12%	9.55%	622	2,710	1,494
reentrancy	26	1,948	0	0	0	0	26	1,948	32
integer overflow	56	319	6	36	10.71%	11.29%	50	283	1,367
airdrop hunting	198	100,336	0	0	0	0	198	100,336	57
call-after-destruct	228	1,761	0	0	0	0	228	1,761	0
honeypot	156	266	15	29	9.62%	10.90%	141	237	0
Total	1,272	107,610	41	351	3.22%	0.33%	1,231	107,259	2,633

Evaluation: False Negative

Vulnerability	Evaluation Set		False Negatives (FNs)			
	# contract	# atx	# contract	# atx	% contract	% atx
call injection	8	13	0	0	0	0
reentrancy	50	648	0	0	0	0
integer overflow	50	902	0	0	0	0
airdrop hunting	-	-	-	-	-	-
call-after-destruct	50	811	0	0	0	0
honeypot	192	1,100	16	129	8.33%	11.73%
Total	400	4,546	16	129	4.00%	2.84%

Real-world Defenses

Defense	Checked Values	# of deployed ct	Target Attack	# of prevented atx	# of successful atx
onlyOwner	*msg.sender* state variable *owner*	2,148,200	privilege escalation*	0	2,691
isHuman isContract	*extcodesize*()	21,672	airdrop hunting	14	887
anotherIsHuman anotherIsContract	*tx.origin* *msg.sender*	3,416	airdrop hunting	3	0
canDistr	state variable *distributionFinished*	2,505	airdrop hunting	21	65,240
nonReentrant	state variable *_guardCounter*	952	reentrancy	77	0
SafeMath	function parameters	3,110,124	integer overflow	1,161	55

Gap between vulnerable contracts and attacks

Attacks	Known		Zero-day		Total Loss	
	# contract	# atx	# contract	# atx	ether / token	monetary
call injection	-	-	-	-	- / -	-
reentrancy	18	56	6	36	6,080 / 5.01E+23	$142,945
integer overflow	34	167	16	113	- / 7.79E+79	-
airdrop hunting	-	-	197	100,278	- / 3.59E+28	$322,010
call-after-destruct	154	1,547	74	214	472 / -	$100,102
honeypot	90	148	51	-	427 / -	$80,866
Total	285	1,904	344	100,641	6,979 / 7.79E+79	$645,848

- Only 285 of 112,570 (0.25%) reported vulnerable contracts are really attacked

Gap between vulnerable contracts and attacks

Attacks	Known		Zero-day		Total Loss	
	# contract	# atx	# contract	# atx	ether / token	monetary
call injection	-	-	-	-	- / -	-
reentrancy	18	56	6	36	6,080 / 5.01E+23	$142,945
integer overflow	34	167	16	113	- / 7.79E+79	-
airdrop hunting	-	-	197	100,278	- / 3.59E+28	$322,010
call-after-destruct	154	1,547	74	214	472 / -	$100,102
honeypot	90	148	51	-	427 / -	$80,866
Total	285	1,904	344	100,641	6,979 / 7.79E+79	$645,848

- 344 Zero-day contracts, missed by previous works due to
  - Lacking of inter-contract dataflow analysis
  - Code coverage

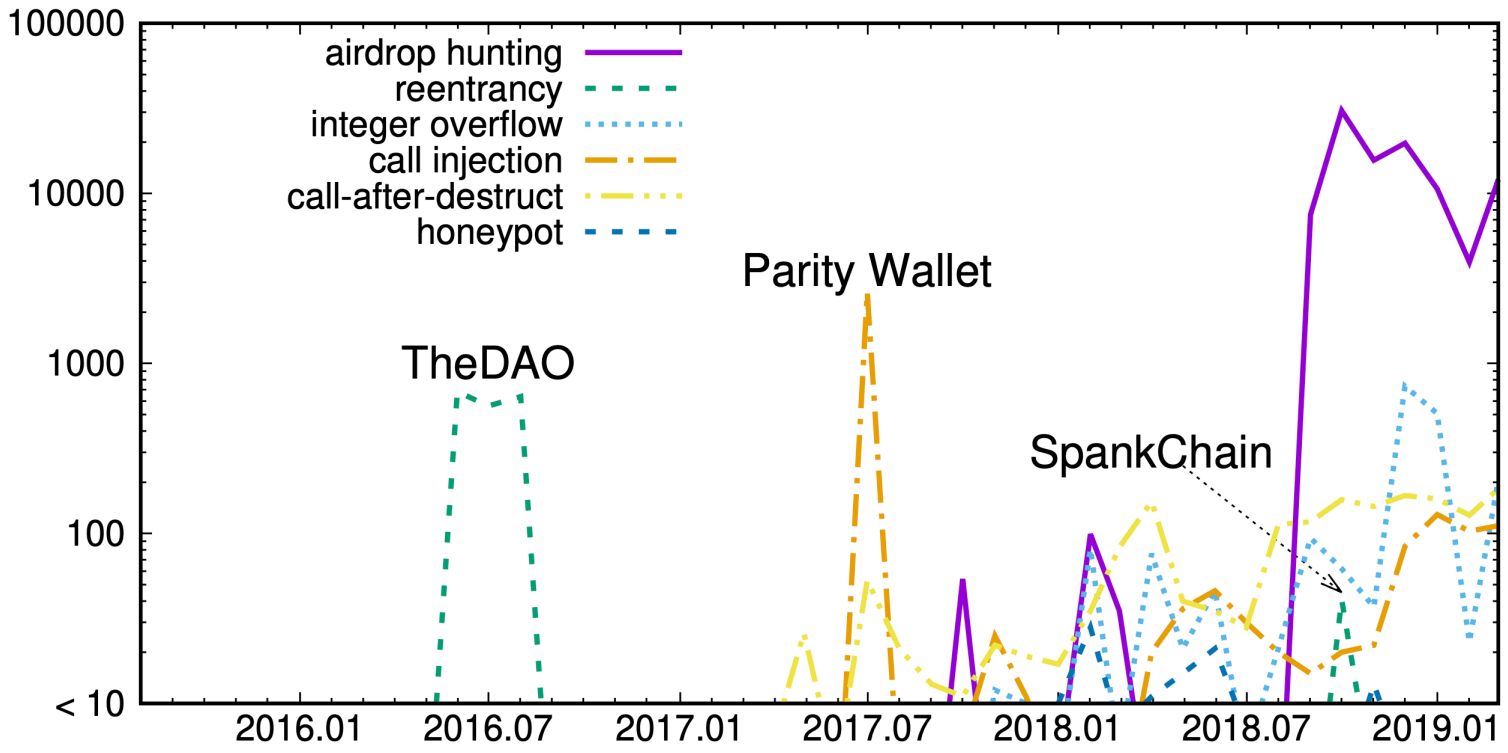
Gap between vulnerable contracts and attacks

Attacks	Known		Zero-day		Total Loss	
	# contract	# atx	# contract	# atx	ether / token	monetary
call injection	-	-	-	-	- / -	-
reentrancy	18	56	6	36	6,080 / 5.01E+23	$142,945
integer overflow	34	167	16	113	- / 7.79E+79	-
airdrop hunting	-	-	197	100,278	- / 3.59E+28	$322,010
call-after-destruct	154	1,547	74	214	472 / -	$100,102
honeypot	90	148	51	-	427 / -	$80,866
Total	285	1,904	344	100,641	6,979 / 7.79E+79	$645,848

- A conservative estimation of losses (excluding well-known incidents)

Advice

- Attack Strategy Shift
  - 2016: Reentrancy
  - 2017: Call injection
  - 2018: Honeypot
  - 2019: Airdrop hunting
  - And 2020?



Thank you!
Q & A

Shunfan Zhou

mail: sfzhou17@fudan.edu.cn