Security of decentralized applications

Agenda

- How does it work?
- Examples of vulnerable contracts
- Client-side vulnerabilities
- Common attack vectors
- Common attack vectors at ICO address substitution
- Last security incidents overview

DAPP

Browser

address = “0xdeadbeef…”
ABI = [{“name”: “crowdsale”…}]

web3 object

HTTP Requests

Transaction

Gateway

- Geth
- Parity
- cpp-Ethereum

Transaction

Ethereum

Smart Contact

Call results, **events**…

Smart contracts vulnerabilities

Blockchain specifics:

- Front-running attack
- Timestamp dependency
- Generating randomness
- Unpredictable state
- Keeping secrets

EVM specifics:

- Integer overflow (no exceptions)
- ABI encoding/decoding
  - Short Address Attack
- Type confusion
- Uninitialized storage pointer

Solidity specifics:

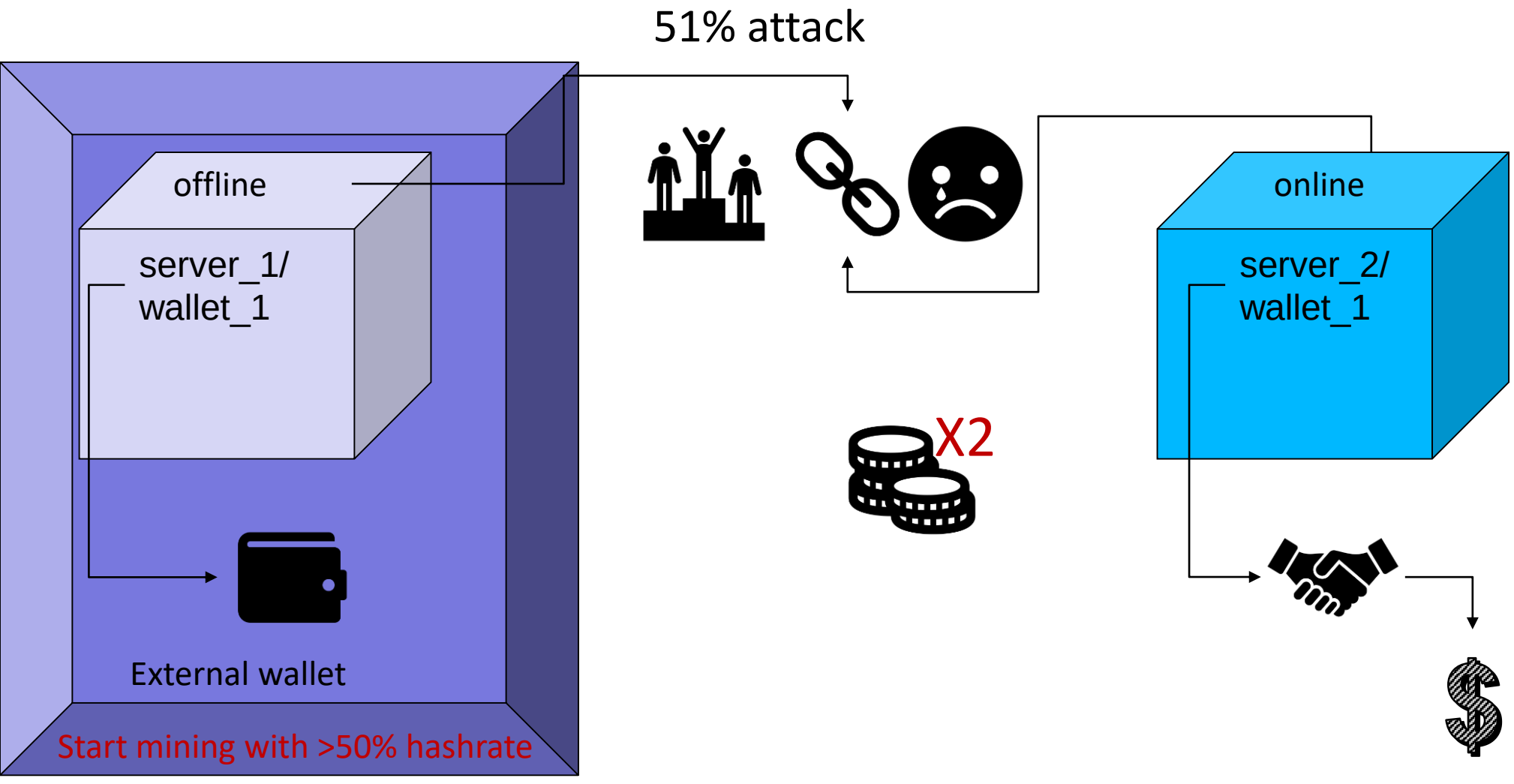
- Evolution of money sending:
  - Reentrancy
  - Gasless send
  - DOS (due to exception disorders)
  - Self-destruction
- Inheritance

Logical (project specifics):

- Whatever

51% attack

Victims 2018


51% attack
offline
server_1/
wallet_1
External wallet
Start mining with >50% hashrate
X2
online
server_2/
wallet_1

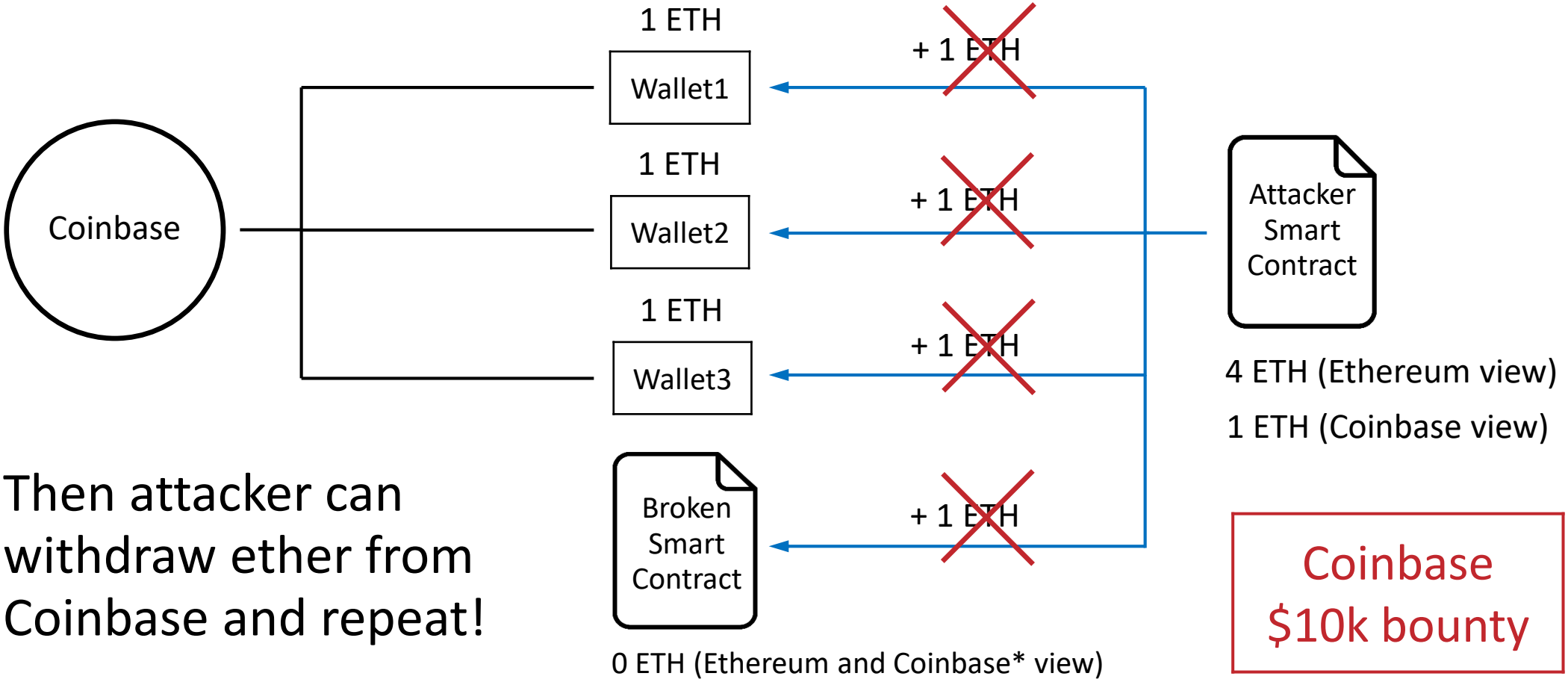
51% attack

Reccomendations:

choose wisely

Hybrid Proof of stake

Account balance manipulation



Then attacker can withdraw ether from Coinbase and repeat!

Coinbase $10k bounty

Client side Vectors

Leaving blockchain aside, can I hack ICO without blockchain knowledge?

- XSS
- Phishing
- Site defacement + clipboard manipulation
- Social Engineering
- etc

And other vectors:

- Weak passwords for Social Network accounts (twitter, slack, FB, etc.)
- Hacking related infrastructure and pivoting

Phishing

Tree steps to phishing:

Register a domain name similar to a victim's one: kickico.com -> kickico.co

Copy a victim's website and replace ICO smart contact address

Spam spam spam!

kickico
$50k Hack

Mitigations:

- Be offensive! Monitor similar domains and inform users (URLCrazy)
- Metamask EtherAddressLookup blacklist
- Register phishing site at local DNS and resolve them to alert page (for team only)

injections

Easy to understand:

- Hack website -> full control information on it
- Change ICO address to your own

CoinDash.io
$7 Million
Hack

Clipboard manipulation:

```
document.addEventListener('copy', function(e){
  e.preventDefault();
  let real_eth_address = window.getSelection().toString();
  let fake_eth_address = '0xc24c2841b87694e546a093ac0da6565c8fdd1800';
  e.clipboardData.setData('text/plain', fake_eth_address);
});
```

Weak passwords

There is nothing new here, same old story.

Enigma Hacked Before ICO Date -- CEO Had Not Changed A Compromised Password

$500k HACK

Protection? You already know:

- 2FA
- Password managers
- OAuth
- etc.

Social engineering

Transactions | Token Transfers | Comments

Latest 25 txns from a total Of 47 transactions

View All

TxHash	Block	Age	From		To	Value	[TxFee]
0x28efb733e35a57d...							41
0x468a72f262ed63d...							2
0x0e2fa661f7aefae0...	5012934	6 days 2 hrs ago	0xe080192f9968ca9...	IN	0x24abaca692f429e...	0 Ether	0.00042
0x0cbb816dd9f9beb...	5012910	6 days 2 hrs ago	0x4dfe2dc7ac3e5af...	IN	0x24abaca692f429e...	0.25 Ether	0.000861
0x3a889522a54757...	5012836	6 days 3 hrs ago	0x24abaca692f429e...	OUT	0xd693998f894a265...	6 Ether	0.000441
0x1f67dff4c6d246e7...	5012828	6 days 3 hrs ago	0xf3c2afcd5429927...	IN	0x24abaca692f429e...	0.2 Ether	0.00105
0x9eedc0ac157780f...	5012797	6 days 3 hrs ago	Bittrex	IN	0x24abaca692f429e...	0.2 Ether	0.00189
0x1b58d8e558af1de...	5012790	6 days 3 hrs ago	0x86bcf7009c80ad4...	IN	0x24abaca692f429e...	0.2 Ether	0.00084
0xdfdb74010b31692...	5012747	6 days 3 hrs ago	0x2e85d3b14ef4570...	IN	0x24abaca692f429e...	0.2 Ether	0.000441
0xa900e2c2ff531c9...	5012741	6 days 3 hrs ago	0x24abaca692f429e...	OUT	0x81d941cee190b7...	0.1 Ether	0.000441
0xcabed1bd28abc9...	5012739	6 days 3 hrs ago	0x24abaca692f429e...	OUT	0x81d941cee190b7...	2 Ether	0.000441
0xa73ace3eb40cf48...	5012702	6 days 3 hrs ago	0x0975ca9f986eee3...	IN	0x24abaca692f429e...	0.22 Ether	0.000966
0xb414f0a852ff58e5...	5012668	6 days 3 hrs ago	0x506e239b78608b...	IN	0x24abaca692f429e...	0.2 Ether	0.002079

pivoting

Attack surface:

- Interfaces (web)
- Social network and email accounts
- Third-party Lib/Apps/Chats/API
- Oracles (shapeshift and similar)
- Mail/VPN/WEB/Mobile/… server
- Totally ALL host you control (laptops too)

→ Numerous attack vectors!

recommendations

Smart Contract security:

Best practices

Code auditing

Bug Bounty (almost free for you!)

Infrastructure:

- Best practices
- Auditing / Security assessment / Penetration testing
- Close/hide all optional services

Thanks' for attention

Lyrchikov Igor

@hd_421

i.lyrchikov@dsec.ru