



看好你的钱包！从攻击和防御 角度分析以太坊RPC攻击

演讲人：王凯 @ 腾讯安全湛泸实验室

自我介绍

- 王凯，Kame Wang
- 腾讯安全湛庐实验室，信息安全研究员；
- 中国科学院大学，信息安全专业博士；
- 研究方向：
 - 区块链安全；
 - 移动安全；
 - 代码自动化分析。

演讲内容

- ✓ 以太坊RPC攻击介绍
- 分析工具的设计与实现
- 研究结果统计与分析
- 总结与安全建议

以太坊简介

- 著名区块链公链项目；
- 以太币：第二大数字加密货币，总市值约五百七十亿；
- 智能合约：部署于区块链网络中的一段代码及相应数据；
- 代币（Token）：一类特殊的智能合约，用于发币（ICO）。
- 已知直接经济损失千万美元以上的安全事件举例：
 - The DAO攻击：2016年6月，窃取三百六十万以太币；
 - Parity钱包攻击：2017年7月，窃取十五万以太币；
 - Parity钱包拒绝服务：2017年11月，冻结九千万以太币。

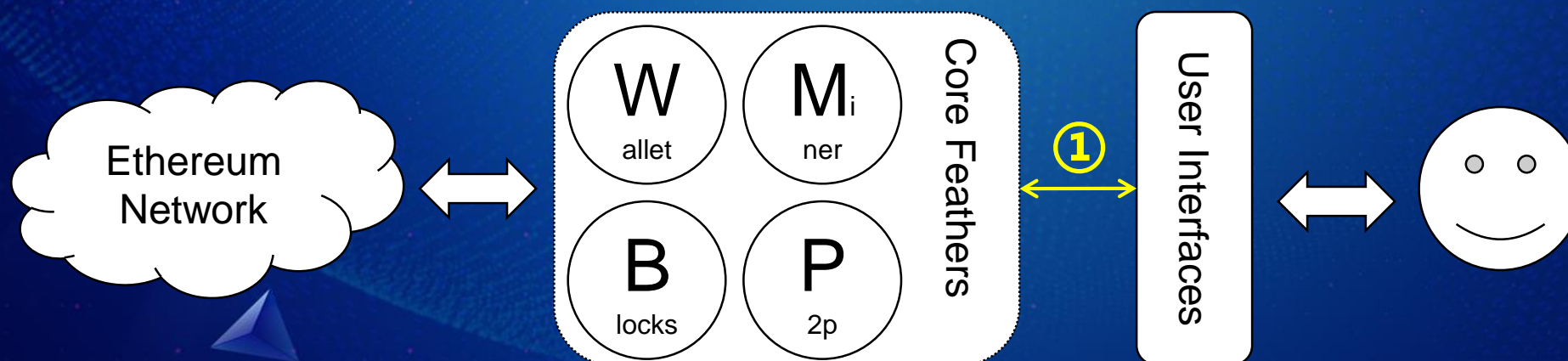


以太坊基本概念

- **本质：在点对点（P2P）网络上的分布式账本：**
 - 账户：公私钥对；
 - 账户地址：针对账户公钥的一系列Hash计算的结果；
 - 钱包：包含多个账户信息；
 - 交易发布：使用私钥签署交易信息 & 广播至区块链网络；
 - 区块：账单“页”，记录多条最新发布的交易信息；
 - 区块链：账单“本”，区块包含前一区块的Hash，形成链式关系，防止数据篡改；
 - 挖矿：节点代码记录新的交易到新的区块；
 - 新币的签发：作为挖矿的奖励，奖励给挖矿成功的矿机持有账户。

以太坊RPC机制

- 核心功能四大模块：钱包管理、挖矿代码、区块维护、P2P网络通信；
- 用户界面：提供配置各模块功能的接口，最基本的是命令行等形式；
- RPC机制：用户界面与核心功能的主流交互方式，使用HTTP协议POST方法。



常见客户端的默认RPC配置

- 默认配置是安全的，却可以被修改。

Client	Language	URL
cpp-ethereum	C++	http://localhost:8545
go-ethereum	Go	http://localhost:8545
pyethapp	Python	http://localhost:4000
Parity	Rust	http://localhost:8545



```
ubuntu@VM-0-3-ubuntu:~$ geth --help | grep rpcaddr  
--rpcaddr value      HTTP-RPC server listening interface (default: "localhost")
```

RPC模块及接口举例

- eth: 账户、交易操作，如accounts, getBalance, sendTransaction...
- personal: 拥有者相关操作，如unlockAccount, sendTransaction...
- net: 网络相关操作，如version...
- miner: 挖矿相关操作，如hashrate, setEtherbase
- **parity**: parity_listAccounts, parity_signMessage...
- **parity**_accounts: parity_killAccount, parity_testPassword, parity_exportAccount...
- **parity**_set: parity_addReservedPeer, shh_getPrivateKey, shh_deleteKey...

默认启动的RPC模块及修改方式



```
ubuntu@VM-0-3-ubuntu:~$ geth --rpc
```

```
... ..
```

```
INFO [05-27|01:32:53] IPC endpoint opened   url=/home/ubuntu/.ethereum/geth.ipc
```

```
INFO [05-27|01:32:53] HTTP endpoint opened url=http://127.0.0.1:8545
```

```
ubuntu@VM-0-3-ubuntu:~$ curl -H "Content-Type: application/json" --data
```

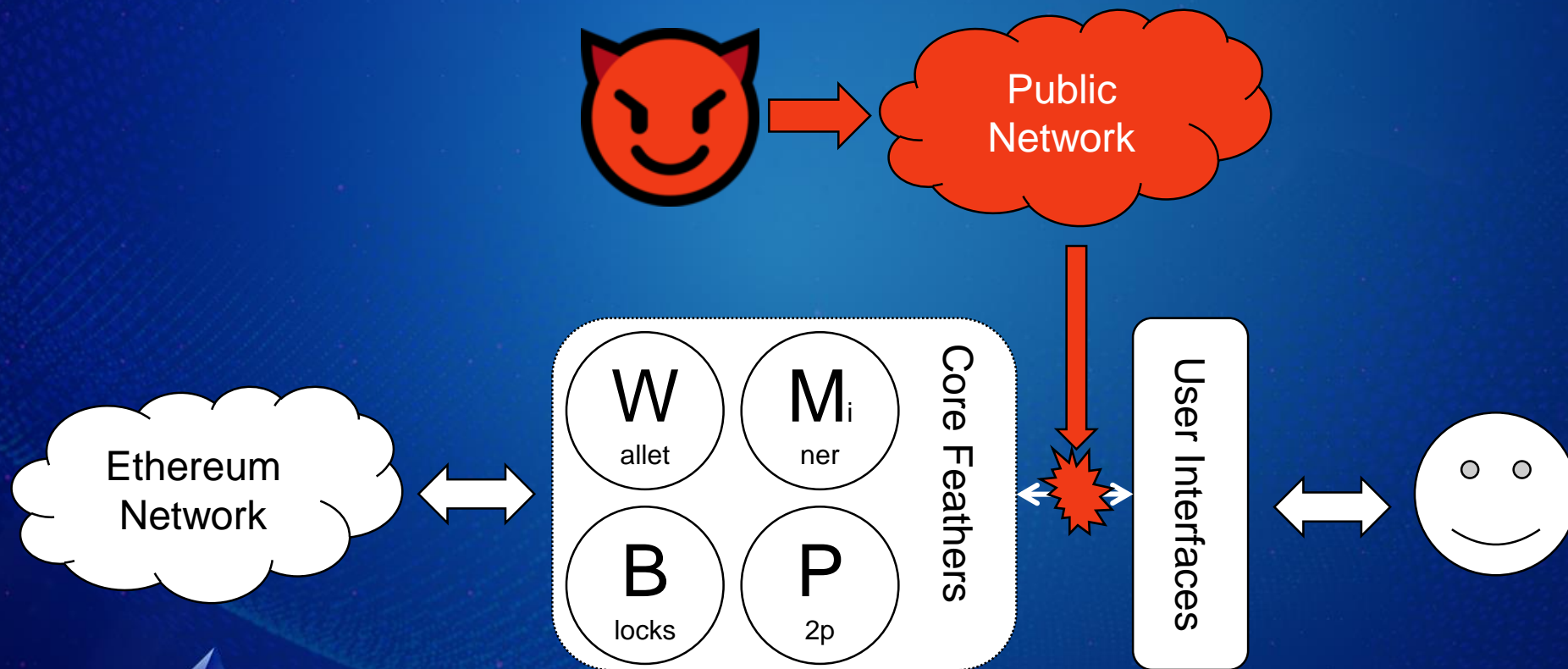
```
'{"jsonrpc":"2.0","method":"rpc_modules","id":233}' 127.0.0.1:8545
```

```
{"jsonrpc":"2.0","id":233,"result":{"eth":"1.0","net":"1.0","rpc":"1.0","web3":"1.0"}}
```

```
ubuntu@VM-0-3-ubuntu:~$ geth --help | grep rpcapi
```

```
--rpcapi value      API's offered over the HTTP-RPC interface
```

以太坊RPC攻击示意图



窃取以太坊攻击示例



- S1. 检查目标节点是否存活：`eth_getBlockByNumber`；
- S2. 获取目标节点账户信息：`eth_account`；
- S3. 命令目标节点发送余额：`eth_sendTransaction`。

以太坊RPC攻击成功条件

- 账户解锁：
 - 目标账户必须处于解锁状态，发送余额的命令才能成功执行；
 - 密码正确的前提下，账户可以通过personal_unlockAccount RPC调用解锁；
 - 在被解锁且未手动上锁的情况下，默认有300秒的时间窗口账户处于解锁状态；
 - 攻击者可以利用这个时间窗口展开攻击。
- 受害者暴露：
 - 受害者对公网暴露其RPC端口；
 - 攻击所使用接口模块需该对外暴露（上例为eth模块，默认配置下对外暴露）。

一个“超级”攻击者的账户信息（8月16日）


- 以太币余额: >\$11,000,000
- 各种代币余额: >\$83,000

 Address `0x957cD4Ff9b3894FC78b5134A8DC72b032fFbC464` 

Home / Accounts / Address

Sponsored: **Kirik Meta Protocol** - New Generation of Blockchain - [Join Pre-Sale Aug 15-17](#)

Overview




Misc More Options

Balance: 39,327.471107392491714997 Ether

Ether Value: \$11,145,798.59 (@ \$283.41/ETH)

Transactions: 5192 txns

Address Watch: Add To Watch List

Token Balances: View (\$83,467.06) >200 

Transactions

Erc20 Token Txns

Comments (78)

Latest 25 txns from a total Of 5192 transactions

TxHash	Block	Age	From		To	Value	[TxFee]
0x5bbc377fcfc9912...	6154425	7 hrs 54 mins ago	0x627306090abab3...	IN	0x957cd4ff9b3894fc...	0.0000000000000011 Ether	0
0xb4b321e75b6427...	6153294	12 hrs 31 mins ago	0x19e7e376e7c213...	IN	0x957cd4ff9b3894fc...	1 wei	0

已有研究和报告

Ethereum nodes with insecure RPC settings are actively exploited self.ethereum

Etherchain 於 1 年前 發表

Today I setup a small honeypot which simulates an Ethereum node with its HTTP RPC API exposed to the internet.

The honeypot forwards save RPC calls to a backend node and responds to certain calls like "eth_accounts" and "eth_sendTransaction" with data that make the node seem vulnerable. You can find the honeypot code [here](#).

Within a few minutes after bringing the honeypot online an attacker tried to steal funds. The attack has the following pattern:

- First the attacker calls `eth_getBlockByNumber("0x00", false)`
- After that the attacker retrieves a list of accounts with the `eth_accounts` calls
- The the attacker issues several `eth_sendTransaction` calls for each of the retrieved account where all account funds are swept to a target address (`0x96a5296eb1d8f8098d35f300659c95f7d6362d15` in this case).

This pattern is repeated over and over again and `eth_sendTransaction` calls are issued approximately every second, most likely to catch a moment when the account is unlocked.

As the [balance](#) of this account is already at ~50 Ether the attacker seems to be successfully with this tactic. A few minutes later another attacker joined the honeypot trying to sweep the funds to `0x08fe986e830cf4d30500fc0ceb8fe65eb7ee58b7`.

Thus I would emphasize again the advice to never, ever allow access to the HTTP RPC API via the internet. Currently all Ethereum clients limit access to the HTTP RPC API by default.

Electrum Bitcoin Wallets Were Vulnerable to Hackers for Two Years

Developers left the vulnerability unpatched for months after being alerted.

Billions of Tokens Theft Case cause by ETH Ecological Defects

原创：SlowMist Team 慢雾区 3月21日



金钱难寐，大盗独行——以太坊JSON-RPC 接口多种盗币手法大揭秘

2018年08月01日

区块链 · 404专栏

作者：知道创宇404区块链安全研究团队

发布时间：2018/08/01

0x00 前言

2010年，[Laszlo](#) 使用 [10000](#) 个比特币购买了两张价值25美元的披萨被认为是比特币在现实世界中的第一笔交易。

要解答的三个问题

1. 以太坊网络中的RPC攻击有多严重？
2. 除了窃取以太币外，攻击手法还有哪些？
3. 目前有多少节点依然暴露了其RPC端口，它们面临者怎样的安全威胁？

演讲内容

- 以太坊RPC攻击介绍
- ✓ 分析工具的设计与实现
- 研究结果统计与分析
- 总结与安全建议



RPC蜜罐模块——从防御的角度开展分析

- 暴露端口：对外暴露TCP端口8545（Geth、Parity等默认RPC端口）；
- 暴露功能：所有RPC模块：

```
ubuntu@VM-0-3-ubuntu:~$ curl -H "Content-Type: application/json" --data  
'{"jsonrpc":"2.0","method":"rpc_modules","id":233}' 127.0.0.1:8545  
{  
  "id": 233,  
  "jsonrpc": "2.0",  
  "result": {  
    "admin": "1.0",  
    "db": "1.0",  
    "debug": "1.0",  
    "eth": "1.0",  
    "miner": "1.0",  
    "net": "1.0",  
    "personal": "1.0",  
    "shh": "1.0",  
    "txpool": "1.0",  
    "web3": "1.0",  
    "parity": "1.0",  
    "parity_accounts": "1.0",  
    "parity_set": "1.0",  
    "rpc": "1.0",  
    "signer": "1.0",  
    "traces": "1.0"  
  }  
}
```

- 基本思路：模仿安全脆弱节点对RPC请求进行反馈，并记录请求数据。



RPC蜜罐模块工作流程

- 蜜罐监听TCP:8545端口；
- 新接收RPC请求的处理过程如右图；
- 被请求的RPC接口可以分为两类：
 - 普通接口：如获取区块高度；
 - 特殊接口：如发送以太坊。
- 如何获取正常数据：
 - 自己维护一个节点；
 - 找一个公网上的“受害者”。🙄



RPC特殊接口列表

接口名	描述	伪造回复
eth_accounts、 personal_listaccounts、 personal_listwallets、 parity_allaccountsinfo	获取节点账户信息。	有以太币和代币余额的真实账户。
eth_sendTransaction、 personal_sendtransaction、 eth_signTransaction	发送/签署交易信息	随机生成Hash串，作为交易记录的Hash值进行返回。
eth_coinbase	获取挖矿奖励接收账户的信息。	有以太币和代币余额的真实账户。
personal_unlockaccount	参数：账户 + 密码 作用：如果密码正确，则解锁目标账户。	解锁失败。
parity_exportaccount	参数：账户 + 密码 作用：如果密码正确，则导出目标账户	导出失败。
miner_setetherbase	参数：账户 作用：设定挖矿奖励接收账户为给定账户。	新的挖矿奖励接收账户。
rpc_modules	查询目标节点暴露的RPC模块列表	所有模块。

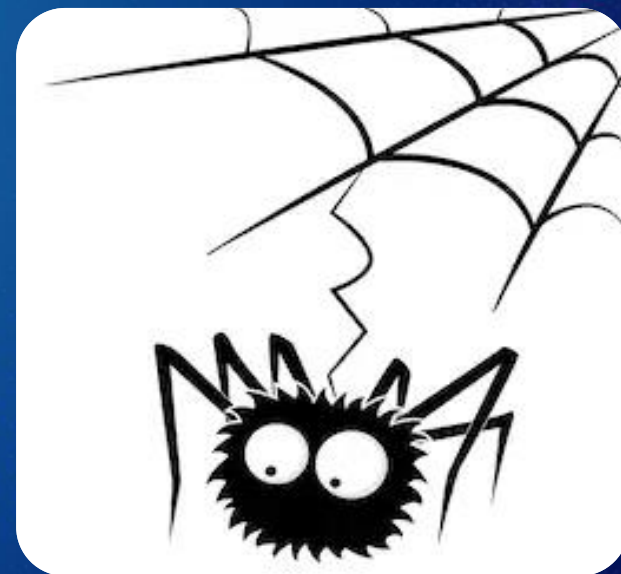
脆弱节点嗅探——从攻击的角度开展分析

- 嗅探暴露了RPC端口（TCP:8545）的节点；
- 尝试利用其RPC接口收集节点信息：
 - IP地址：外来信息，从全网节点探测模块获知；
 - 开放RPC模块：rpc_modules；
 - 节点：web3_clientVersion；
 - 账户列表：parity_allAccountsInfo / personal_listAccounts / eth_accounts；
 - 网络类型：net_version；
 - 挖矿状态：eth_mining；
 - 挖矿算力：eth_hashrate；
 -



全网节点探测

- 实现方法：
 - 修改Geth客户端的P2P网络连接代码；
 - 一旦发现一个新节点，立即向其查询其邻居节点；
 - 尝试与返回的邻居节点建立连接。
- 模块功能：
 - 如果和蜜罐配置于同一主机，可使蜜罐更易被攻击者发现；
 - 为脆弱节点嗅探模块提供待测节点的IP地址等信息。



演讲内容

- 以太坊RPC攻击介绍
- 分析工具的设计与实现
- ✓ 研究结果统计与分析
- 总结与安全建议

测试平台

- 对测试设备的性能要求较低：
- 利用腾讯云节点，在亚、欧、美洲部署了三个测试设备，性能如表格所示。

节点位置	CPU	内存	带宽	存储
香港	单核	1GB	2Mbps	50GB HDD硬盘
硅谷	单核	1GB	1Mbps	50GB HDD硬盘
法兰克福	单核	1GB	1Mbps	50GB HDD硬盘

测试结果统计

- 测试在2018年6月开展，为期一个月。
- 各节点捕获数据如下表：

节点位置	捕获RPC请求数	探知全网节点数	发现脆弱节点数
香港	11,614,335	69,332	1,757
硅谷	41,984,376	74,636	1,779
法兰克福	36,508,897	86,599	1,804

发现1：网络类型的分布

- 基于区块链网络类型的统计，不只主网节点暴露了RPC接口。
- 脆弱的主网节点才是我们真正感兴趣的测试目标。

节点位置	主网脆弱节点数	Akroma网络	各类测试网络
香港	615	560	582
硅谷	629	565	585
法兰克福	631	572	601

发现2：窃取数字货币

- 敏感RPC模块：eth、personal；
- 敏感RPC接口：eth(personal)_sendTransaction、eth_signTransaction；
- 窃取数字货币是主要攻击手段，但窃取目标不仅是以太币。

节点位置	捕获攻击者账户	代币种类	探知脆弱节点	受威胁帐号数量
香港	35	0	158	53,082
硅谷	36	22	163	54,095
法兰克福	17	21	165	54,220

发现3：账户暴力破解

- 敏感RPC模块：personal、parity_accounts；
- 敏感RPC接口：personal_unlockAccount、parity_exportAccount；
- 接受账户地址及密码参数，并能反馈给攻击者密码是否正确信息。

节点位置	捕获字典大小	探知脆弱节点	受威胁帐号数量	节点位置
香港	731	123	53,043	香港
硅谷	721	124	54,050	硅谷
法兰克福	629	126	54,176	法兰克福

发现4：丢失挖矿奖励

- 敏感RPC模块：miner；
- 敏感RPC接口：miner_setEtherbase；
- 将挖矿奖励的接收账户设置为指定账户。

节点位置	捕获攻击账户	探知总脆弱节点 / 正在挖矿脆弱节点
香港	0	54 / 8
硅谷	2	54 / 7
法兰克福	1	53 / 8

演讲内容

- 以太坊RPC攻击介绍
- 分析工具的设计与实现
- 研究结果统计与分析
- ✓ 总结与安全建议

总结

- 以太坊的RPC攻击仍在全球范围内进行；
- 黑客采取的攻击手段多种多样；
- 以太坊主网络中，面临安全威胁的节点仍为数众多。

面对这种安全形势，我们从各方面给出一些安全建议：

安全建议

- 区块链开发社区：加强对节点RPC接口的保护；
- 以太坊节点部署者：避免远程RPC控制节点的需求，如不能避免，利用修改RPC端口号、设置防火墙策略等方式，保护节点安全；
- 跃跃欲试的攻击者：“蜜罐”恢恢，疏而不漏；
- 虚拟货币投资者：“这不是投资，这是赌博”。



THANKS

欢迎交流：kamewang@tencent.com