Reading List

智能合约安全相关

Ethereum 安全相关

标黑为重点阅读

- 智能合约漏洞：
  - **以太坊基础漏洞与分析**：http://rickgray.me/2018/05/17/ethereum-smart-contracts-vulnerabilities-review/#
  - **基础的漏洞 survey**：http://courses.cse.tamu.edu/chiache/csce678/s19/download/atzei16.pdf
  - 目前最全的漏洞 survey（**有能力看这个，推荐**）：https://arxiv.org/pdf/1908.04507.pdf
- **智能合约字节码相关**：
  - 字节码结构：https://arxiv.org/pdf/1905.00272.pdf（Sec II）
  - **字节码逆向工程**：https://arvanaghi.com/blog/reversing-ethereum-smart-contracts/

Ethereum 安全相关

标黑为重点阅读

- 扫描工具：
  - **对目前大多数的扫描工具的一个 review**：https://arxiv.org/pdf/1910.10601.pdf（可以通过参考文献找到大多数的知名的扫描器的 paper，可以详细阅读）
- 分析工具：
  - 有许多针对 EVM、智能合约的 fuzzer，可以在 Google scholar 上了解一下
- Misc:
  - **智能合约字节码反编译工具**：https://ethervm.io/decompile
  - Remix 可以选择编译版本并单步调试：https://remix.ethereum.org/

EOSIO 安全相关

标黑为重点阅读

- 智能合约漏洞：
  - **PeckShield 的一些案例分析**：https://blog.peckshield.com/blog.html
  - Slowmist 整理了一些 EOSIO 上的攻击事件，**可以根据攻击方法寻找相应解析文章**：https://hacked.slowmist.io/?c=EOS%20DApp
- 智能合约字节码（WebAssembly）：
  - EOSIO 智能合约底层 Wasm 的文档：https://webassembly.github.io/spec/core/
  - Wasm 较 Solidity 字节码来说更为复杂，最好自己在本地编译一个合约的 Wasm 文件，然后转换为 wast 格式，然后对照源码手动逆向
  - **对 Wasm 的安全分析的 paper**：
    - https://arxiv.org/pdf/1808.10652.pdf
    - **对 EOSIO 智能合约的漏洞检测器**：https://arxiv.org/pdf/2003.06568.pdf

EOSIO 安全相关

目前已知的关于 EOSIO 智能合约的所有漏洞