SMART CONTRACT AUDIT REPORT

for

AirSwap Protocol

Prepared By: Yiqun Chen

PeckShield

February 15, 2022

Document Properties

Client	AirSwap Protocol
Title	Smart Contract Audit Report
Target	AirSwap
Version	1.0
Author	Xuxian Jiang
Auditors	Xiaotao Wu, Patrick Liu, Xuxian Jiang
Reviewed by	Yiqun Chen
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	February 15, 2022	Xuxian Jiang	Final Release
1.0-rc	January 30, 2022	Xuxian Jiang	Release Candidate #1

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Yiqun Chen
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related source code of the `AirSwap` protocol, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About AirSwap

`AirSwap` curates a peer-to-peer network for trading digital assets. The protocol is designed to protect traders from counterparty risk, price slippage, and front running. Any market participant can discover others and trade directly peer-to-peer. At the protocol level, each swap is between two parties, a signer and a sender. The signer is the party that creates and cryptographically signs an order, and the sender is the party that sends the order to the Ethereum blockchain for settlement. As a decentralized and open project, governance and community activities are also supported by rewards protocols built with on-chain components. The basic information of audited contracts is as follows:

Table 1.1: Basic Information of AirSwap

Item	Description
Name	AirSwap Protocol
Website	https://www.airswap.io/
Type	Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	February 15, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit:

- https://github.com/airswap/airswap-protocols.git (ac62b71)

And this is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/airswap/airswap-protocols.git (84935eb)

1.2 About PeckShield

PeckShield Inc. [10] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [9]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact, and can be accordingly classified into four categories, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.
- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [8], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings. Moreover, in case there is an issue that may affect an active protocol that has been deployed, the public version of this report may omit such issue, but will be amended with full details right after the affected protocol is upgraded with respective fixes.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 | Findings

2.1 Summary

Here is a summary of our findings after analyzing the design and implementation of the `AirSwap` protocol smart contracts. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	■
Low	3	■ ■ ■
Informational	0	
Total	4	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerability and 3 low-severity vulnerabilities.

Table 2.1: Key Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Proper Allowance Reset For Old Staking Contracts	Coding Practices	Fixed
PVE-002	Low	Removal of Unused State/Code	Coding Practices	Fixed
PVE-003	Low	Accommodation of Non-ERC20-Compliant Tokens	Business Logics	Fixed
PVE-004	Medium	Trust Issue of Admin Keys	Security Features	Mitigated

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Proper Allowance Reset For Old Staking Contracts

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `Pool`
- Category: Coding Practices [6]
- CWE subcategory: CWE-1041 [1]

Description

The `AirSwap` protocol has a `Pool` contract that supports the main functionality of staking and claims. It also allows the privileged owner to update the active staking contract `stakingContract`. In the following, we examine this specific `setStakingContract()` function.

It comes to our attention that this function properly sets up the spending allowance to the new `stakingContract`. However, it forgets to cancel the previous spending allowance from the old `stakingContract`.

```
/**
 * @notice Set staking contract address
 * @dev Only owner
 * @param _stakingContract address
 */
function setStakingContract(address _stakingContract)
  external
  override
  onlyOwner
{
  require(_stakingContract != address(0), "INVALID_ADDRESS");
  stakingContract = _stakingContract;
  IERC20(stakingToken).approve(stakingContract, 2**256 - 1);
}
```

Listing 3.1: `Pool::setStakingContract()`

Recommendation Remove the spending allowance from the old `stakingContract` when it is updated.

Status This issue has been fixed in the following PR: `776`.

3.2 Removal of Unused State/Code

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `Multiple Contracts`
- Category: Coding Practices [6]
- CWE subcategory: CWE-563 [3]

Description

AirSwap makes good use of a number of reference contracts, such as `ERC20`, `SafeERC20`, and `SafeMath`, to facilitate its code implementation and organization. For example, the `Pool` smart contract has so far imported at least four reference contracts. However, we observe the inclusion of certain unused code or the presence of unnecessary redundancies that can be safely removed.

For example, if we examine closely the `Staking` contract, there are a number of states that have been defined. However, some of them are never used. Examples include `usedIds` and `unlockTimestamps`. These unused states can be safely removed.

```
// Mapping of account to delegate
mapping(address => address) public accountDelegates;

// Mapping of delegate to account
mapping(address => address) public delegateAccounts;

// Mapping of timelock ids to used state
mapping(bytes32 => bool) private usedIds;

// Mapping of ids to timestamps
mapping(bytes32 => uint256) private unlockTimestamps;

// ERC-20 token properties
string public name;
string public symbol;
```

Listing 3.2: The `Staking` Contract

Moreover, the `Wrapper` contract has a function `sellNFT()`, which is marked as `payable`, but its internal logic has explicitly restricted the following `require(msg.value == 0)`. As a result, both `payable` and the restriction can be removed together.

```
function sellNFT(
  uint256 nonce,
  uint256 expiry,
  address signerWallet,
  address signerToken,
  uint256 signerAmount,
  address senderToken,
  uint256 senderID,
  uint8 v,
  bytes32 r,
  bytes32 s
) public payable {
  require(msg.value == 0, "VALUE_MUST_BE_ZERO");
  IERC721(senderToken).setApprovalForAll(address(swapContract), true);
  IERC721(senderToken).transferFrom(msg.sender, address(this), senderID);
  swapContract.sellNFT(
    nonce,
    expiry,
    signerWallet,
    signerToken,
    signerAmount,
    senderToken,
    senderID,
    v,
    r,
    s
  );
  _unwrapEther(signerToken, signerAmount);
  emit WrappedSwapFor(msg.sender);
}
```

Listing 3.3: `Wrapper::sellNFT()`

Recommendation Consider the removal of the redundant code with a simplified, consistent implementation.

Status The issue has been fixed with the following PRs: `777`, `778`, and `779`.

3.3 Accommodation of Non-ERC20-Compliant Tokens

- ID: PVE-003
- Severity: Low
- Likelihood: Low
- Impact: High
- Target: Multiple Contracts
- Category: Business Logic [7]
- CWE subcategory: CWE-841 [4]

Description

Though there is a standardized ERC-20 specification, many token contracts may not strictly follow the specification or have additional functionalities beyond the specification. In the following, we examine the `transfer()` routine and related idiosyncrasies from current widely-used token contracts.

In particular, we use the popular stablecoin, i.e., `USDT`, as our example. We show the related code snippet below. On its entry of `approve()`, there is a requirement, i.e., `require(!((_value != 0) && (allowed[msg.sender][_spender] != 0)))`. This specific requirement essentially indicates the need of reducing the allowance to 0 first (by calling `approve(_spender, 0)`) if it is not, and then calling a second one to set the proper allowance. This requirement is in place to mitigate the known `approve()/transferFrom()` race condition (https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729).

```
/**
* @dev Approve the passed address to spend the specified amount of tokens on behalf
    of msg.sender.
* @param _spender The address which will spend the funds.
* @param _value The amount of tokens to be spent.
*/
function approve(address _spender, uint _value) public onlyPayloadSize(2 * 32) {

    // To change the approve amount you first have to reduce the addresses`
    //  allowance to zero by calling `approve(_spender, 0)` if it is not
    //  already 0 to mitigate the race condition described here:
    //  https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
    require(!((_value != 0) && (allowed[msg.sender][_spender] != 0)));

    allowed[msg.sender][_spender] = _value;
    Approval(msg.sender, _spender, _value);
}
```

Listing 3.4: USDT Token **Contract**

Because of that, a normal call to `approve()` is suggested to use the safe version, i.e., `safeApprove()`, In essence, it is a wrapper around ERC20 operations that may either throw on failure or return false without reverts. Moreover, the safe version also supports tokens that return no value (and instead revert or throw on failure). Note that non-reverting calls are assumed to be successful. Similarly, there is a safe version of `transfer()` as well, i.e., `safeTransfer()`.

```
    /**
     * @dev Deprecated. This function has issues similar to the ones found in
     * {IERC20-approve}, and its usage is discouraged.
     *
     * Whenever possible, use {safeIncreaseAllowance} and
     * {safeDecreaseAllowance} instead.
     */
    function safeApprove(
        IERC20 token,
        address spender,
        uint256 value
    ) internal {
        // safeApprove should only be called when setting an initial allowance,
        // or when resetting it to zero. To increase and decrease it, use
        // 'safeIncreaseAllowance' and 'safeDecreaseAllowance'
        require(
            (value == 0)  (token.allowance(address(this), spender) == 0),
            "SafeERC20: approve from non-zero to non-zero allowance"
        );
        _callOptionalReturn(token, abi.encodeWithSelector(token.approve.selector,
            spender, value));
    }
```

Listing 3.5: `SafeERC20::safeApprove()`

In the following, we show the `unstake()` routine from the `Staking` contract. If the `USDT` token is supported as `token`, the unsafe version of `token.transfer(account, amount)` (line 178) may revert as there is no return value in the `USDT` token contract's `transfer()/transferFrom()` implementation (but the `IERC20` interface expects a return value)!

```
168  /**
169   * @notice Unstake tokens
170   * @param amount uint256
171   */
172  function unstake(uint256 amount) external override {
173    address account;
174    delegateAccounts[msg.sender] != address(0)
175      ? account = delegateAccounts[msg.sender]
176      : account = msg.sender;
177    _unstake(account, amount);
178    token.transfer(account, amount);
179    emit Transfer(account, address(0), amount);
180  }
```

Listing 3.6: `Staking::unstake()`

Note this issue is also applicable to other routines in `Swap` and `Pool` contracts. For the `safeApprove()` support, there is a need to approve twice: the first time resets the allowance to zero and the second time approves the intended amount.

Recommendation Accommodate the above-mentioned idiosyncrasy about ERC20-related approve()/transfer()/transferFrom().

Status This issue has been fixed in the following PRs: 781 and 782.

3.4 Trust Issue of Admin Keys

- ID: PVE-004
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: Multiple Contracts
- Category: Security Features [5]
- CWE subcategory: CWE-287 [2]

Description

In the AirSwap protocol, there is a privileged owner account that plays a critical role in governing and regulating the system-wide operations (e.g., parameter setting and payee adjustment). It also has the privilege to regulate or govern the flow of assets within the protocol.

With great privilege comes great responsibility. Our analysis shows that the owner account is indeed privileged. In the following, we show representative privileged operations in the Pool protocol.

```
/**
 * @notice Set staking token address
 * @dev Only owner
 * @param _stakingToken address
 */
function setStakingToken(address _stakingToken) external override onlyOwner {
  require(_stakingToken != address(0), "INVALID_ADDRESS");
  stakingToken = _stakingToken;
  IERC20(stakingToken).approve(stakingContract, 2**256 - 1);
}

/**
 * @notice Admin function to migrate funds
 * @dev Only owner
 * @param tokens address[]
 * @param dest address
 */
function drainTo(address[] calldata tokens, address dest)
  external
  override
  onlyOwner
{
  for (uint256 i = 0; i < tokens.length; i++) {
    uint256 bal = IERC20(tokens[i]).balanceOf(address(this));
    IERC20(tokens[i]).safeTransfer(dest, bal);
  }
  emit DrainTo(tokens, dest);
```

```
    }
```

Listing 3.7: Various Privileged Operations in `Pool`

We emphasize that the privilege assignment with various protocol contracts is necessary and required for proper protocol operations. However, it is worrisome if the `owner` is not governed by a `DAO`-like structure.

We point out that a compromised `owner` account would allow the attacker to invoke the above `drainTo` to steal funds in current protocol, which directly undermines the assumption of the `AirSwap` protocol.

Recommendation Promptly transfer the privileged account to the intended `DAO`-like governance contract. All changed to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status This issue has been confirmed and partially mitigated with a multi-sig account to regulate the governance privileges. The multi-sig account is a standard Gnosis Safe wallet, which is controlled by multiple participants, who agree to propose and submit transactions as they relate to the DAO's proposal submission and voting mechanism. This avoids risk of any single compromised EOA as it would require collusion of multiple participants.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `AirSwap` protocol, which curates a peer-to-peer network for trading digital assets. The protocol is designed to protect traders from counterparty risk, price slippage, and front running. Any market participant can discover others and trade directly peer-to-peer. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that `Solidity`-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1041: Use of Redundant Code. https://cwe.mitre.org/data/definitions/1041.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

[4] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

[5] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[6] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[7] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[8] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[9] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[10] PeckShield. PeckShield Inc. https://www.peckshield.com.