Detection and Localization of Bad Randomness Vulnerabilities in Ethereum Smart Contracts

Hadis Rezaei

Abstract

The Bad Randomness vulnerability is one of the critical security issues in smart contracts, rooted in a fundamental contradiction between the deterministic nature of blockchains and the need for randomness in decentralized applications. This vulnerability, catalogued as SWC-120, has enabled real-world exploits resulting in significant financial losses, including the SmartBillions attack that drained over 400 ETH and the Fomo3D exploit that caused losses exceeding $3 million. Despite being ranked as the fourth most critical smart contract vulnerability by OWASP in 2025, only two specialized detection tools exist for this vulnerability class. General-purpose tools such as Slither and Mythril demonstrate poor detection accuracy with high false positive rates, as they rely on simple syntactic pattern matching without understanding the semantic context of how blockchain values are used. These tools cannot distinguish between safe uses of block attributes for time-locks and dangerous uses for randomness generation.

To address these challenges, this research presents an approach composed of four major components. First, a combined systematic literature review (SLR) and systematization of knowledge (SoK) identifies 24 active smart contract vulnerabilities and analyzes 50 real-world attacks causing financial losses exceeding $1.09 billion, resulting in a new four-tier framework for classifying root causes of vulnerabilities. Second, we construct a risk-stratified benchmark dataset of 17,466 labeled contracts for Bad Randomness (SWC-120) vulnerabilities through a five-phase methodology including function-level validation, which revealed that 49% of apparently protected contracts were actually exploitable. Third, we develop TaintSentinel, a semantic taint analysis system based on graduated taint propagation and context-sensitive rules, trained and evaluated on 4,844 labeled Ethereum contracts. Fourth, we design SmartTaintRL, a deep reinforcement learning system that mitigates path explosion and provides precise vulnerability localization at both function and code-node levels.

The contributions of this study are evaluated at three levels. Theoretically, we introduce a four-tier framework grouping vulnerabilities by fundamental causes: faulty economic design, protocol lifecycle flaws, external dependency weaknesses, and implementation-level defects. We show that 26% of successful attacks exploit chains of multiple vulnerabilities. Technically, we introduce two advanced detection systems: TaintSentinel, using a dual-stream neural architecture that integrates global structural analysis with path-specific patterns; and SmartTaintRL, a Deep Q-Network with an attention mechanism that reduces analysis paths by 44.3% while preserving 96% recall, combined with gradient-based attribution methods for pinpointing vulnerable code locations. Practically, we construct two complementary datasets: a risk-stratified benchmark of 1,758 vulnerable contracts with four-level classification (High_Risk, Medium_Risk, Low_Risk, Safe) that is 51x larger than existing datasets and serves as the first validated benchmark for SWC-120; and a detection-focused dataset of 4,844 real Ethereum contracts with over 1.1 million execution paths, including 252,844 high-quality paths for training machine learning models.

Experimental results on balanced datasets show that TaintSentinel achieves an F1-score of 0.892, representing nearly a fourfold improvement over existing tools. SmartTaintRL further improves performance with an F1-score of 0.930 on balanced and 0.920 on imbalanced datasets. Evaluation

of existing tools on our benchmark showed that both Slither and Mythril failed to detect the majority of vulnerable contracts, confirming the limitations of pattern-based approaches. In terms of localization accuracy, SmartTaintRL identifies 64.3% of vulnerable functions exactly and 92.9% when including caller functions, demonstrating that precise vulnerability localization is achievable through reinforcement learning. The system also introduces a new metric, Path Risk Accuracy, achieving 97% accuracy on balanced data.

Analysis of real-world attacks reveals that access-control vulnerabilities (13 incidents, $417.95 million loss) and price-manipulation attacks (13 incidents, $279.75 million loss) constitute the dominant exploitation patterns, while reentrancy — despite extensive research attention — accounts for only 11% of total losses. Furthermore, 26% of successful attacks involve multi-vulnerability exploitation chains, a phenomenon largely overlooked in prior research.

The scientific impact of this research includes the first path-level analysis method for detecting Bad Randomness, the first localization approach for identifying vulnerable functions and code nodes in Bad Randomness vulnerabilities, the introduction of the graduated taint propagation concept, the first validated risk-stratified benchmark for SWC-120 vulnerabilities, and demonstrating the effectiveness of deep reinforcement learning in addressing path explosion. The main limitation lies in the current model's inability to capture complex inter-contract interactions during online execution. While the system performs effectively for intra-contract analysis and mitigates class imbalance through reinforcement learning and dual-scenario evaluation, runtime multi-contract interactions remain outside the present scope. Future work will focus on runtime detection mechanisms, hybrid static-dynamic analysis, and enhanced modeling of multi-contract execution interactions.

Overall, this research bridges the gap between academic security analysis and real-world needs of smart contract ecosystems, offering deployable technical solutions for addressing emerging blockchain security challenges.

Keywords: Smart Contracts · Bad Randomness · Semantic Taint Analysis · Reinforcement Learning · Path Optimization · Vulnerability Localization · Blockchain Security · Ethereum · Benchmark Dataset

Sommario

La vulnerabilita' di Bad Randomness rappresenta uno dei problemi di sicurezza piu' critici negli smart contract, radicata in una contraddizione fondamentale tra la natura deterministica delle blockchain e la necessita' di casualita' nelle applicazioni decentralizzate. Questa vulnerabilita', catalogata come SWC-120, ha reso possibili attacchi reali con ingenti perdite finanziarie, tra cui l'attacco SmartBillions che ha sottratto oltre 400 ETH e l'exploit Fomo3D che ha causato perdite superiori a 3 milioni di dollari. Nonostante sia classificata al quarto posto tra le vulnerabilita' piu' critiche degli smart contract dall'OWASP nel 2025, esistono soltanto due strumenti di rilevamento specializzati per questa classe di vulnerabilita'. Strumenti generici come Slither e Mythril mostrano scarsa precisione di rilevamento e alti tassi di falsi positivi, poiche' si basano su semplice corrispondenza di pattern sintattici senza comprendere il contesto semantico di come i valori blockchain vengono utilizzati. Questi strumenti non riescono a distinguere tra usi sicuri degli attributi di blocco per i time-lock e usi pericolosi per la generazione di casualita'.

Per affrontare queste sfide, questa ricerca presenta un approccio composto da quattro componenti principali. In primo luogo, una revisione sistematica della letteratura (SLR) combinata con una sistematizzazione della conoscenza (SoK) identifica 24 vulnerabilita' attive negli smart contract e

analizza 50 attacchi reali che hanno causato perdite finanziarie superiori a 1,09 miliardi di dollari, producendo un nuovo framework a quattro livelli per classificare le cause radice delle vulnerabilita'. In secondo luogo, viene costruito un dataset benchmark stratificato per rischio di 17.466 contratti etichettati per le vulnerabilita' Bad Randomness (SWC-120), attraverso una metodologia in cinque fasi che include la validazione a livello di funzione, la quale ha rivelato che il 49% dei contratti apparentemente protetti era in realta' sfruttabile. In terzo luogo, viene sviluppato TaintSentinel, un sistema di analisi semantica della contaminazione basato sulla propagazione graduata della contaminazione e su regole context-sensitive, addestrato e valutato su 4.844 contratti Ethereum etichettati. In quarto luogo, viene progettato SmartTaintRL, un sistema di deep reinforcement learning che mitiga l'esplosione dei percorsi e fornisce una localizzazione precisa delle vulnerabilita' sia a livello di funzione che di nodo del codice.

I contributi di questo studio sono valutati su tre livelli. A livello teorico, viene introdotto un framework a quattro livelli che raggruppa le vulnerabilita' in base alle cause fondamentali: progettazione economica difettosa, difetti del ciclo di vita del protocollo, debolezze delle dipendenze esterne e difetti a livello di implementazione. Si dimostra che il 26% degli attacchi riusciti sfrutta catene di vulnerabilita' multiple. A livello tecnico, vengono introdotti due sistemi avanzati di rilevamento: TaintSentinel, che utilizza un'architettura neurale a doppio flusso che integra l'analisi strutturale globale con pattern specifici per percorso; e SmartTaintRL, una Deep Q-Network con meccanismo di attenzione che riduce i percorsi di analisi del 44,3% preservando il 96% di recall, combinata con metodi di attribuzione basati sul gradiente per individuare le posizioni di codice vulnerabili. A livello pratico, vengono costruiti due dataset complementari: un benchmark stratificato per rischio di 1.758 contratti vulnerabili con classificazione a quattro livelli (High_Risk, Medium_Risk, Low_Risk, Safe), 51 volte piu' grande dei dataset esistenti e primo benchmark validato per SWC-120; e un dataset orientato al rilevamento di 4.844 contratti Ethereum reali con oltre 1,1 milioni di percorsi di esecuzione, inclusi 252.844 percorsi di alta qualita' per l'addestramento di modelli di machine learning.

I risultati sperimentali su dataset bilanciati mostrano che TaintSentinel raggiunge un F1-score di 0,892, rappresentando un miglioramento di quasi quattro volte rispetto agli strumenti esistenti. SmartTaintRL migliora ulteriormente le prestazioni con un F1-score di 0,930 su dataset bilanciati e 0,920 su dataset sbilanciati. La valutazione degli strumenti esistenti sul nostro benchmark ha mostrato che sia Slither che Mythril non sono riusciti a rilevare la maggior parte dei contratti vulnerabili, confermando i limiti degli approcci basati su pattern. In termini di accuratezza della localizzazione, SmartTaintRL identifica esattamente il 64,3% delle funzioni vulnerabili e il 92,9% includendo le funzioni chiamanti, dimostrando che una localizzazione precisa delle vulnerabilita' e' realizzabile attraverso il reinforcement learning. Il sistema introduce anche una nuova metrica, Path Risk Accuracy, raggiungendo il 97% di accuratezza su dati bilanciati.

L'analisi degli attacchi reali rivela che le vulnerabilita' di controllo degli accessi (13 incidenti, perdita di 417,95 milioni di dollari) e gli attacchi di manipolazione dei prezzi (13 incidenti, perdita di 279,75 milioni di dollari) costituiscono i pattern di sfruttamento dominanti, mentre la rientranza — nonostante l'ampia attenzione della ricerca — rappresenta solo l'11% delle perdite totali. Inoltre, il 26% degli attacchi riusciti coinvolge catene di sfruttamento multi-vulnerabilita', un fenomeno ampiamente trascurato nella ricerca precedente.

L'impatto scientifico di questa ricerca comprende il primo metodo di analisi a livello di percorso per rilevare la Bad Randomness, il primo approccio di localizzazione per identificare funzioni vulnerabili e nodi di codice nelle vulnerabilita' di Bad Randomness, l'introduzione del concetto di propagazione graduata della contaminazione, il primo benchmark validato e stratificato per rischio per le vulnerabilita' SWC-120, e la dimostrazione dell'efficacia del deep reinforcement learning

nell'affrontare l'esplosione dei percorsi. Il principale limite risiede nell'incapacita' del modello attuale di catturare le complesse interazioni inter-contratto durante l'esecuzione online. Sebbene il sistema funzioni efficacemente per l'analisi intra-contratto e mitighi lo squilibrio delle classi attraverso il reinforcement learning e la valutazione in doppio scenario, le interazioni multi-contratto in fase di esecuzione rimangono al di fuori dell'ambito attuale. Il lavoro futuro si concentrera' su meccanismi di rilevamento in fase di esecuzione, analisi ibrida statico-dinamica e modellazione avanzata delle interazioni di esecuzione multi-contratto.

Nel complesso, questa ricerca colma il divario tra l'analisi della sicurezza accademica e le esigenze reali degli ecosistemi di smart contract, offrendo soluzioni tecniche implementabili per affrontare le emergenti sfide di sicurezza della blockchain.

Parole chiave: Smart Contract · Bad Randomness · Analisi Semantica della Contaminazione · Reinforcement Learning · Ottimizzazione dei Percorsi · Localizzazione delle Vulnerabilita' · Sicurezza Blockchain · Ethereum · Dataset Benchmark