Research Statement

Enhancing Security in the Age of Decentralization

Tamer Abdelaziz, Ph.D.

tamer@u.nus.edu @Tamer_Abdelaziz https://tamernus.github.io/

Introduction

The rise of blockchain technology and its applications, particularly smart contracts, has revolutionized many industries. However, the security of these systems remains a critical challenge. Attackers are constantly devising new methods to exploit vulnerabilities in smart contracts, leading to significant financial losses. My research focuses on leveraging deep learning techniques to enhance blockchain security and smart contract vulnerability detection [1].

Past Research

My research has focused on leveraging deep learning to bolster software security analysis, with a particular emphasis on smart contracts. I have spearheaded the development of novel deep learning models capable of directly identifying vulnerabilities within smart contract bytecode, eliminating the dependency on source code, which may not always be accessible. This approach relies on program analysis and semantic feature extraction using graph neural networks (GNNs) to understand the relationships and functionalities within the smart contract code. This line of research, entitled "Smart Learning to Find Dumb Contracts", culminated in two first-authored publications at the prestigious USENIX Security conference ([3], [4]). Within this work, I introduced the DLVA tool, which showcases the effectiveness of my models in achieving superior accuracy in vulnerability detection compared to traditional methods. DLVA offers several key contributions. First, it is trained to analyze bytecode directly, even when the supervising oracle (Slither) only operates on source code. My research proposes a novel training algorithm that seamlessly bridges this gap, eliminating the need for manual feature engineering or predefined patterns. Second, the training algorithm exhibits significant robustness, successfully overcoming mislabeled contracts and even identifying vulnerabilities that Slither missed. Finally, DLVA offers a significant speed advantage over conventional smart contract vulnerability detection tools based on formal methods. It can analyze contracts for 29 vulnerabilities within just 0.2 seconds, achieving a speedup of 10x to 1000x.

Furthermore, I have actively pursued research on broader blockchain security. My research resulted in a publication titled "Schooling to Exploit Foolish Contracts" published in IEEE BCCA ([2]). This work delves into a specific type of smart contract attack and proposes mitigation strategies. Recognizing the limitations of supervised learning, which relies on large amounts of labeled training data – expensive and time-consuming to acquire, especially for niche areas like smart contract vulnerabilities – I developed the SCooLS tool. SCooLS utilizes semi-supervised learning to generate more accurate models compared to unsupervised learning, while eliminating the need for the extensive, oracle-labeled training sets required by supervised learning techniques. Similar to DLVA, SCooLS employs GNNs to facilitate direct analysis of smart contract bytecode, again eliminating the need for manual feature engineering or predefined patterns. This work underlines my in-depth understanding of the unique security challenges associated with smart contracts.

Current and Future Research Interests

My current research agenda leverages my expertise in deep learning to tackle critical challenges in blockchain security. Here are the key areas I'm actively pursuing:

- Enhanced Auto-Exploit Generation for Smart Contracts:

  Existing learning-based smart contract vulnerability detection tools often fall short in providing actionable insights. They typically classify contracts as simply "vulnerable" or "non-vulnerable" without pinpointing the exact vulnerability type or its location within the bytecode. Additionally, they fail to demonstrate how an attacker could exploit these vulnerabilities, hindering developers' ability to understand and address potential threats.

  Building upon the foundation established with SCooLS's auto-exploit generator, I aim to further refine this pioneering application of semi-supervised learning in smart contract vulnerability analysis. This approach uniquely enables the precise detection and exploitation of specific vulnerable functions within the bytecode. Significantly, it goes beyond simply identifying vulnerabilities; it generates realistic attack demonstrations for end-users and developers. This shift from labeling entire contracts as vulnerable to providing concrete exploitability testing methods empowers developers to proactively address potential security issues.

- Large Language Models (LLMs) for Smart Contract Security:

  Pre-trained large language models (LLMs) hold promise for enhanced smart contract security analysis. These models can be fine-tuned with task-specific data to optimize their performance for vulnerability detection. However, limitations exist, particularly concerning LLMs' ability to process lengthy texts. I plan to address this challenge while simultaneously exploring LLM techniques for vulnerability detection directly within bytecode. This research has the potential to further expand the scope and effectiveness of smart contract security analysis.

- Deep Learning for Anomaly Detection in Blockchain Transactions:

  Analyzing blockchain transactions can reveal suspicious patterns indicative of malicious activities. I plan to investigate the application of deep learning for anomaly detection in blockchain transactions. This research has the potential to significantly improve the security of blockchain networks by enabling real-time identification of potential attacks. By leveraging deep learning's ability to learn complex patterns from vast datasets, we can develop robust anomaly detection systems capable of flagging suspicious transactions that deviate from established norms.

- Explainable AI (XAI) for Blockchain Security:

  Deep learning models are often criticized for their lack of interpretability, making it difficult to understand their decision-making processes. I am interested in exploring explainable AI (XAI) techniques to provide interpretable insights into how deep learning models identify vulnerabilities in smart contracts and transactions. This line of research is crucial for enhancing trust and transparency in the use of deep learning for blockchain security. By incorporating XAI methods, we can gain valuable insights into the models' reasoning, fostering greater confidence in their effectiveness and enabling further improvements.

Collaboration and Future Goals

I am confident that my research background in deep learning and blockchain security, coupled with my enthusiasm and dedication, will make me a significant asset to your research group. I am eager to collaborate with others, learn from experienced researchers, and contribute meaningfully to the development of secure and reliable systems.
My specific goals include:

- Deepening Expertise: I aim to further my expertise in both blockchain security and software security by actively engaging in challenging research problems. This will involve continuous learning and staying abreast of the latest advancements in these fields.
- Novel Research Directions: I am passionate about exploring innovative research directions that push the boundaries of knowledge and contribute to the progress of both blockchain security and software security.
- High-Impact Publications: I strive to publish high-quality research in top-tier conferences and journals, disseminating my findings to a wider audience and fostering impactful discussions within the research community.
- Collaborative Research: I believe in the power of collaboration. I aim to work alongside leading researchers in the field, fostering knowledge exchange and accelerating the pace of discovery towards impactful results.
- Effective Communication: I plan to actively participate in conferences and workshops, honing my skills in presenting research findings to diverse audiences. This will enable me to effectively communicate complex ideas and contribute to the dissemination of security knowledge.
- Open-Source Advocacy: I am committed to giving back to the open-source security community by releasing tools and datasets developed during my research. This will contribute to a more collaborative and secure environment for everyone.

*References

1. T. Abdelaziz, "Towards secure smart contracts: A deep learning approach for detecting security threats," *Ph.D Thesis, ScholarBank@NUS Repository, National University of Singapore*, 2023. URL: https://scholarbank.nus.edu.sg/handle/10635/247301.
2. T. Abdelaziz and A. Hobor, "Schooling to exploit foolish contracts," in *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*, 2023, pp. 388–395. DOI: 10.1109/BCCA58897.2023.10338924.
3. T. Abdelaziz and A. Hobor, "Smart learning to find dumb contracts," in *32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA: USENIX Association, Aug. 2023, pp. 1775–1792, ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/abdelaziz.
4. T. Abdelaziz and A. Hobor, "Usenix'23 artifact appendix: Smart learning to find dumb contracts," in *32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA: USENIX Association, Aug. 2023, ISBN: 978-1-939133-37-3. URL: https://www.usenix.org/system/files/usenixsecurity23-appendix-abdelaziz.pdf.