Volume XXVII 2024
ISSUE no.1
MBNA Publishing House Constanta 2024

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Threats and Countermeasures in Software Security with a Deep Dive into Click Baiting

To cite this article: Marius Iulian Mihailescu, Stefania Loredana Nita, Valentina Marascu, Marius Rogobete and Ciprian Racuciu, Scientific Bulletin of Naval Academy, Vol. XXVII 2024, pg. 61-68.

Submitted: 28.04.2024
Revised: 22.06.2024
Accepted: 01.08.2024

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-24-I1-008

Threats and Countermeasures in Software Security with a Deep Dive into Click Baiting

Marius Iulian MIHAILESCU[1,2], Stefania Loredana NITA[2,3], Valentina MARASCU[1,4], Marius ROGOBETE[5], Ciprian RACUCIU[3]

1) Faculty of Engineering and Computer Science, Scientific Research Center in Mathematics and Computer Science, SPIRU HARET University, Bucharest, Romania
2) Institute for Computers, Bucharest, Romania
3) Military Technical Academy, "Ferdinand I", Bucharest, Romania
4) National Institute for Laser, Plasma and Radiation Physics, Magurele, Romania
5) HARMAN International

Corresponding author name and e-mail address: Marius Iulian Mihailescu (m.mihailescu.mi@spiruharet.ro)

Abstract. The widespread issue of click baiting poses a serious challenge in the ever-changing field of cybersecurity, since it has the potential to jeopardize program integrity and data security. This study introduces a new strategy aimed at enhancing the security of data shared in blockchain networks by efficiently combating click baiting strategies. Our solution utilizes the fundamental characteristics of blockchain technology, such as decentralization, transparency, and immutability, to create a strong framework that guarantees the integrity and privacy of data, protecting it against click baiting assaults.

Keywords: blockchain security; decentralized verification; click baiting countermeasures, cryptographic techniques; real-time threat detection; scalable blockchain framework

1. Introduction

Cybersecurity threats in the digital era have grown more complex, requiring new defense mechanisms. Click baiting is a common vulnerability that exploits user interest by using false links and information to undermine system security. The outcomes of these attacks vary from minor inconveniences to serious breaches resulting in significant loss of sensitive information and financial assets. With the increasing interconnectedness of the world, it is crucial to have strong security mechanisms that can adjust to new threats and safeguard user data.

Incorporating blockchain technology into cybersecurity provides a possible solution to these difficulties. Blockchain's decentralized structure, transparency, and immutability make it an ideal foundation for creating security solutions that can withstand classic attacks and combat advanced threats such as click baiting. This technology allows for the establishment of a secure environment emphasizing data integrity, secrecy, trust, and reliability throughout transactions and interactions.

Utilizing a blockchain-based system to protect data transactions is quite significant. This technique guarantees that any data or digital asset shared across a network is authenticated and unaltered, hence decreasing the risk of dangerous behaviors enabled by misleading material. Utilizing a decentralized verification mechanism with blockchain can remove vulnerable single points of failure commonly targeted in click baiting attacks, hence improving the network's security.

The paper suggests a detailed security plan to prevent click baiting by utilizing sophisticated cryptographic methods and real-time threat detection systems within a blockchain framework. This plan not only deals with vulnerabilities caused by click baiting but also enhances the security of data exchange within blockchain networks. Our proposed solution aligns with digital security by safeguarding data to maintain confidence and reliability in applications such as financial services and personal data management.

Developing a blockchain-based security mechanism to combat clickbait is crucial in today's digital environment. The action not only deals with a crucial weakness but also establishes a standard for future cybersecurity measures in a more decentralized digital environment. This article will examine the complexities of the scheme, how it is put into practice, and its possible effects on the wider realm of software security and data protection.

2. Background and related work

This section of the study discusses click baiting as a cybersecurity concern, current solutions, and the impact of blockchain technology on software security. We want to justify the development of our innovative blockchain-based strategy to counter click baiting by providing this background.

Click baiting threats

Click baiting is a deceptive strategy employed to entice people to click on a link that directs them to a webpage that is different from what was anticipated, typically done to generate advertising income or distribute malware. This manipulation takes advantage of user interest and can lead to compromised personal information, malware installation, or other security breaches. The complexity of these attacks has advanced, rendering conventional detection systems less efficient.

Current countermeasures

Current methods to combat click baiting are browser extensions that alert users about questionable links, machine learning algorithms that identify unusual patterns in link architecture and content, and educational initiatives to enhance user understanding of these risks. Although somewhat effective, these methods frequently do not effectively counter the advanced and constantly evolving strategies used by attackers, highlighting the necessity for stronger and more flexible solutions.

Blockchain in cybersecurity

Blockchain technology is gaining recognition for its ability to improve cybersecurity. The core qualities of blockchain technology, which include decentralization, transparency, and immutability, make it well-suited for safeguarding data and transactions across various applications. Blockchain technology has been utilized to generate unalterable records of security incidents, decentralized systems for managing identities, and secure messaging platforms. The applications showcase how blockchain may reduce typical security risks, such as those associated with centralized control and single points of failure, sometimes found in clickbait situations.

Studying how blockchain contributes to cybersecurity has resulted in new methods that may surpass conventional security measures. Utilizing blockchain technology allows for the establishment of a decentralized system for content verification, which lessens dependence on a single entity, hence diminishing the vulnerability to manipulation and enhancing the system's resistance to attacks. This feature is well-suited for countering advanced click baiting strategies, making blockchain an excellent technology to build our suggested security system on.

This backdrop establishes a strong basis for recognizing the urgent necessity for a new strategy to address click baiting and demonstrates why blockchain technology is well-suited for this task. The next parts will elaborate on the suggested plan and its execution, expanding upon this fundamental understanding.

3. The proposed scheme

The suggested blockchain-based method is aimed to strengthen software security by eliminating click baiting attacks through a combination of decentralized verification, advanced cryptographic techniques, and real-time threat detection tools. This complete method not only solves the vulnerabilities exploited by click baiting but also assures the integrity and confidentiality of data exchanges on the blockchain.

System architecture. The architecture of our proposed system consists of several key components:

- *Blockchain network*. A decentralized network that maintains a secure and immutable ledger of all content verification records and user interactions.
- *Smart contracts*. Deployed on the blockchain to automate the verification processes and ensure compliance with security protocols.
- *Cryptographic modules*. Integrated within the blockchain to handle encryption, decryption, and secure data storage.
- *User Interface (UI)*. A front-end platform that allows users to interact with the system, submit content for verification, and access verified content.
- *Threat detection engine*. A machine learning-based system that analyzes content and user behavior patterns to identify potential click baiting threats.

Decentralized verification process. The decentralized verification process works as follows:

- *Content submission*. Users submit content (links, advertisements, media) to the blockchain network via the UI.
- *Smart contract activation*. A smart contract is triggered upon content submission, which initiates the verification process.

- *Consensus mechanism*. The content is distributed to various nodes in the blockchain network. These nodes independently verify the content's authenticity and integrity based on predefined criteria. This might include checking the content against known databases of phishing and malware URLs, analyzing the metadata for inconsistencies, and other relevant security checks.
- *Verification result*. Once a consensus is reached among the nodes, the result (verified or rejected) is recorded on the blockchain. Verified content is flagged as safe for user interaction, while rejected content is flagged and reported.

Integration of cryptographic techniques. To ensure data security and privacy, the following cryptographic techniques are integrated:

- *Homomorphic Encryption*. Allows computations to be performed on encrypted data, enabling the verification process without exposing the actual content. This is critical for maintaining confidentiality while still allowing data to be processed and verified.
- *Zero-Knowledge Proofs (ZKP)*. Employed to enable the verification of data authenticity without revealing the data itself. ZKP allows a prover to convince a verifier that a certain assertion is true, without conveying any additional information apart from the fact that the assertion is indeed true.

Real-time threat detection mechanism. The threat detection engine incorporates machine learning algorithms to identify and respond to click baiting threats in real-time:

- *Pattern recognition*. The engine continuously learns from incoming data, adjusting its models to recognize new and evolving click baiting patterns.
- *Anomaly detection*. Any deviation from normal behavior is flagged as a potential threat. This includes unexpected surges in traffic, abnormal click-through rates, and suspicious redirection patterns.
- *Automated response*. Upon detecting a potential threat, the system automatically triggers a response. This may involve isolating suspicious content, alerting users, and initiating additional verification processes.

The suggested approach offers a strong framework for protecting data from click baiting by combining blockchain technology, powerful cryptography, and dynamic threat detection. This guarantees a strong level of security, privacy, and efficiency, making it a powerful instrument for addressing advanced cyber threats in the digital realm.

4. The implementation

The proposed blockchain-based security scheme to combat click baiting requires a thorough setup and deployment in many phases, leveraging various tools and technologies to guarantee strength and usefulness.

The development environment is set up using Ethereum as the blockchain platform because of its extensive support for smart contracts and decentralized applications (DApps). Solidity is utilized for smart contract creation, while JavaScript, supported by the web3.js framework, is employed to design the user interface. Tools like the Truffle Suite are crucial for developing, deploying, and administering smart contracts. Ganache offers a simulated blockchain for testing purposes, and MetaMask allows secure user interactions with the DApp.

Smart contracts play a key role in the system by overseeing the verification process, documenting consensus outcomes, and regulating access to verified information. Once tested locally using Ganache, these contracts are deployed to an Ethereum testnet such as Rinkeby or Ropsten for real-world trials to confirm proper functionality before deployment on the mainnet.

The method incorporates homomorphic encryption and zero-knowledge proofs (ZKPs) to maintain data secrecy and authenticity while safeguarding sensitive information. Microsoft's SEAL and IBM's HELib libraries support homomorphic encryption, whereas frameworks like ZoKrates are utilized for implementing zero-knowledge proofs in the Ethereum environment.

The system includes a real-time threat detection mechanism that uses machine learning algorithms to detect and respond to clickbait activity. The models are created using Python and frameworks like TensorFlow or PyTorch, then connected to the blockchain through an Oracle service such as Chainlink. This configuration enables secure interaction between smart contracts and external machine learning computations.

The last step includes creating a user-friendly interface and launching the entire system on the Ethereum mainnet, then continuing to monitor and maintain it. Regular upgrades are made to the smart contracts and machine learning models to address new threats and maintain the system's effectiveness against changing click baiting strategies. The careful combination of blockchain technology, powerful cryptographic methods, and machine learning guarantees that the proposed system is secure and can adjust to emerging cybersecurity threats.

5. The evaluation

We evaluated the efficiency and effectiveness of our suggested blockchain-based solution for combating clickbait by using a thorough evaluation process that included simulated testing and real-world attack scenarios. This thorough approach assures that the system is strong, adaptable, and easy to use in various situations.

Testing of the system commenced in a simulated blockchain environment using technologies like Ganache, which replicate the functions of Ethereum's live network without incurring any expenses. We were able to perform thorough and replicable testing in this controlled environment. We created different attack scenarios such as phishing attempts, advertising, and social engineering methods to test the system's ability to detect and respond. Stress testing assessed system scalability and stability under high request volumes, while penetration testing identified potential vulnerabilities in smart contracts and system design.

Various performance criteria were used to evaluate the system's capacities. The system's accuracy was measured by its ability to correctly distinguish instances of clickbait from false positives and false negatives, offering valuable information about the reliability of the threat detection techniques. Response time was a crucial statistic that assessed the system's ability to promptly detect and address threats, which is essential for real-time performance. Throughput, which measures the system's capacity to process transactions within a specific timeframe, was assessed to determine scalability. We measured resource utilization to evaluate the system's efficiency in utilizing computer and memory resources. User satisfaction was assessed by gathering input from people who interacted with the system, offering significant insights into its usability and practicality.

The test results were meticulously examined. The system's usefulness in dynamically identifying and mitigating threats was proved by its high accuracy rates and low response times in diverse attack scenarios. The throughput data showed strong scalability for high-traffic situations, while resource utilization indicators indicated that the system was optimized for efficiency, sustaining performance without excessive resource consumption. The user reaction was predominantly good, emphasizing the system's practicality and user-friendliness.

Our assessment of the blockchain-based security system against click baiting demonstrated that it meets the required standards for security and effectiveness while also identifying potential areas for enhancement. This investigation validates the system's preparedness for wider use and its capacity to enhance cybersecurity in blockchain settings.

6. Discussion

The *primary advantages and downsides of the available techniques are compared*. The blockchain-based technique for combating click baiting represents a notable improvement compared to conventional security measures. Traditional methods typically involve centralized databases, browser extensions, and user training to address issues such as click baiting. Although conventional approaches offer fundamental safeguards, they lack effectiveness in crucial aspects where our blockchain system outperforms.

1. **Effectiveness**. Traditional methods often struggle with the rapid evolution of click baiting techniques, as attackers continuously refine their strategies to bypass security measures. Our blockchain solution, however, leverages decentralized verification and real-time threat detection using machine learning, which enhances its ability to quickly adapt to new threats. Zero-knowledge proofs and homomorphic encryption are integrated to guarantee data authenticity and privacy while ensuring security, an aspect sometimes overlooked in traditional systems.
2. **Scalability**. Existing techniques can be hampered by their reliance on centralized structures, which may struggle under high load situations and are subject to single points of failure. In contrast, the suggested blockchain technology is intrinsically more scalable due to its decentralized structure. Each node in the network may handle verifications separately, dispersing the burden and eliminating bottlenecks, which is critical for situations with huge volumes of data and transactions.
3. **Efficiency**. Efficiency in conventional systems is typically reliant on the resources accessible at the central control point, potentially resulting in elevated expenses and delayed reaction times during peak hours. Our approach enhances resource utilization by employing distributed processing and smart contracts to automate tasks that are usually done manually or through more resource-intensive methods in traditional setups. This accelerates the entire process and lowers operational expenses.

Implications for software security

The deployment of a blockchain-based scheme for combating clicks baiting carries broader implications for global software security practices:

1. **Shift to decentralization**. The proposed solution could promote a transition from centralized security models to decentralized security measures by showcasing their effectiveness in mitigating targeted assaults and failures. This change could result in stronger security frameworks in different areas, not only in addressing clickbait but also in overall cybersecurity defense systems.
2. **Enhanced data privacy**. The suggested system establishes a new standard for privacy-preserving security procedures by incorporating cryptographic techniques such as zero-knowledge proofs and homomorphic encryption. This is especially important due to the rising data privacy issues worldwide, prompting more corporations and organizations to implement comparable approaches.
3. **Increased adoption of blockchain in security**. Effective execution of this plan could hasten the integration of blockchain technology in several cybersecurity domains. The unchangeable and easily visible characteristics of blockchain make it well-suited for recording and overseeing security occurrences, potentially transforming incident response and forensic investigation.

4. **Regulatory and compliance changes**. With the increasing prevalence of blockchain and cryptography solutions, regulatory authorities may need to revise compliance requirements and frameworks to appropriately integrate and control these emerging technologies. This may result in the development of more thorough and visionary cybersecurity strategies.

The proposed blockchain-based solution not only tackles click baiting difficulties but also paves the way for substantial changes in global security approaches. Blockchain has the potential to revolutionize software security methods by providing a more secure, private, and resilient framework to battle various digital threats due to its effectiveness, scalability, and efficiency.

7. Conclusion

The article has presented a new blockchain-based strategy designed to combat the widespread and complex cybersecurity problem of click baiting. This plan utilizes the distinctive benefits of blockchain technology, such as decentralization, transparency, and immutability, along with advanced cryptography methods and real-time threat detection systems. The proposed solution showed significant enhancements compared to standard security techniques in terms of efficacy, scalability, and efficiency through a thorough evaluation methodology.

Existing methods were shown to have shortcomings in dealing with changing threats and maintaining scalability under heavy loads, as revealed by the comparison. Our blockchain technology tackles these difficulties by dispersing the verification process among numerous nodes, improving the system's capacity to scale and adjust dynamically to emerging threats. The use of cryptographic advancements like zero-knowledge proofs and homomorphic encryption guarantees the preservation of data privacy while upholding security.

This technique has further consequences beyond just addressing click baiting. They propose that blockchain technology can alter worldwide software security standards. This involves promoting a transition to decentralized security systems, improving data privacy, and advocating for regulatory adjustments to support and utilize these sophisticated technologies. The successful establishment of a blockchain-based security system has the potential to create a new benchmark in cybersecurity, leading to a reassessment and potential overhaul of security procedures and measures in several sectors.

References

[1]. A. Kalhoro, N. I. Ali, I. A. Brohi, S. Kalhoro, M. Kalhoro and N. A. B. Salleh, "Security Threats and Countermeasure for IoT Based Library Management System," *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, Tandojam, Pakistan, 2024, pp. 1-5, doi: 10.1109/KHI-HTC60760.2024.10481857.

[2]. U. Kuzmina, O. Kazakov and B. Erushev, "Building an Attack Tree for Analysis of Information Security Risks," *2023 International Russian Smart Industry Conference (SmartIndustryCon)*, Sochi, Russian Federation, 2023, pp. 164-168, doi: 10.1109/SmartIndustryCon57312.2023.10110738.

[3]. B. Hammi and S. Zeadally, "Software Supply-Chain Security: Issues and Countermeasures," in *Computer*, vol. 56, no. 7, pp. 54-66, July 2023, doi: 10.1109/MC.2023.3273491.

[4]. T. Hemalatha, S. Venkatakiran, M. Kaur, M. S. B, V. V. Prasad and A. B, "Real-Time Threat Detection and Countermeasures in IoT Environments," *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2023, pp. 1349-1357, doi: 10.1109/ICECA58529.2023.10395098.

[5]. Y. Hayashi, F. Leferink and M. Nagata, "Introduction to Physical Layer Security and Hardware Supply Chain Security: EM Tricks to Keep Your Information and Devices Safe," 2023

International Symposium on Electromagnetic Compatibility – EMC Europe, Krakow, Poland, 2023, pp. 1-6, doi: 10.1109/EMCEurope57790.2023.10274206.

[6]. A. S. Abdalla and V. Marojevic, "End-to-End O-RAN Security Architecture, Threat Surface, Coverage, and the Case of the Open Fronthaul," in IEEE Communications Standards Magazine, vol. 8, no. 1, pp. 36-43, March 2024, doi: 10.1109/MCOMSTD.0001.2200047.

[7]. S. Pandey, P. C. Pathak, S. Tripathi, S. Halwai, S. Aggarwal and N. Nishant, "Security Risks and Their Mitigation Strategies: Cloud Computing Perspective," *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, Gautam Buddha Nagar, India, 2023, pp. 1015-1019, doi: 10.1109/UPCON59197.2023.10434361.