EBSI digital identity DDoS hardening using IP reputation

Adrian-Tudor Dumitrescu, 5810825

I. Problem description

Digital identity systems are integral components of modern online interactions, facilitating secure and reliable authentication of users across various digital platforms. However, these systems are susceptible to Distributed Denial of Service (DDoS) attacks, which can disrupt the availability and functionality of digital identity services, leading to potential security breaches and user inconvenience. This problem started to affect the Internet from the 90s [2] and continues to be unsolved even with new prevention/mitigation tools and architectures [3]. To address this issue, there is a need for robust DDoS mitigation solutions tailored specifically to protect digital identity systems.

The European Blockchain Services Infrastructure (EBSI) presents a promising platform for implementing secure and decentralized digital identity solutions. Leveraging blockchain technology, EBSI offers the potential to enhance the resilience and integrity of digital identity systems against DDoS attacks. However, simply deploying EBSI-based digital identity services does not guarantee immunity from DDoS threats. Additional measures are required to harden these systems and mitigate the risk of DDoS-induced disruptions.

Concepts of leveraging an IP reputation system for enhancing DDoS mitigation strategies were already explored(presented in related works) but with no system deployed, most ideas stopping at the design stage. By categorizing IP addresses based on their reputation scores, this approach enables more effective identification and filtering of malicious traffic, thereby reducing the impact of DDoS attacks on network resources.

Applying the principles to the context of EBSI-based digital identity systems presents an opportunity to develop a comprehensive DDoS hardening solution. By integrating an IP reputation system into the infrastructure of EBSI digital identity services, it becomes possible to proactively identify and mitigate DDoS attacks targeting these critical systems.

A. Scientific challenges?

- **Integration Complexity**: Integrating an IP reputation system into the architecture of EBSI digital identity services may introduce complexity and compatibility issues that need to be carefully managed to ensure seamless operation.
- **Accuracy and Reliability**: The effectiveness of the IP reputation system relies on the accuracy and reliability of the reputation scores assigned to IP addresses. Ensuring the trustworthiness of these scores is essential to avoid false positives or negatives in DDoS detection and mitigation.
- **Scalability and Performance**: As digital identity systems often handle large volumes of user authentication requests, the DDoS hardening solution must be scalable and capable of maintaining optimal performance under heavy load conditions.
- **Regulatory Compliance??**: Compliance with regulatory requirements and data protection laws, such as GDPR in the European Union, is paramount when implementing DDoS mitigation solutions for digital identity services. Any solution must adhere to relevant legal and ethical standards governing data privacy and security.

By developing a robust DDoS hardening solution based on the principles of collaborative blockchain-based mitigation and IP reputation systems, it becomes possible to enhance the resilience and security of EBSI digital identity services, ensuring their continued availability and integrity in the face of evolving cyber threats.

II. Related work

1) Very close and short related work [6](just a concept, no system yet created): Introduces a collaborative blockchain-based approach to mitigate Distributed Denial of Service (DDoS) attacks, which are significant threats affecting system availability and categorizes DDoS attacks into volume-based, protocol-based, and application-layer attacks.
   Various protocols mentioned including:
   - DOTS Protocol, which facilitates intra-organization and inter-organization communications for DDoS attack mitigation. [8]
   - Cochain-SC, which proposes solutions for both intra-domain and inter-domain DDoS mitigation using Blockchain and SDN. [1]
   - BloSS, which focuses on cooperative defense against DDoS attacks through Blockchain and SDN, incentivizing service providers for collaboration.
   - Other research that explores the use of blockchain in IP reputation and attack information sharing. [9]

   Several research gaps and challenges in existing DDoS mitigation schemes including:
   - Minimizing the false-positive rate of DDoS attack detection.
   - Decreasing the management cost of the IP reputation system.

- Reducing the severity of DDoS attacks.
- Providing transparency, security, and authenticity in sharing attack information.
- Assigning IP Reputation scores to detected IP addresses from Firewall and Intrusion Prevention and Detection Systems.

They propose a system that aims to address these challenges by integrating blockchain technology with an IP reputation system. Blockchain facilitates transparent and secure sharing of whitelisted and blacklisted IP addresses, along with their reputation scores, among collaborators resulting in improved accuracy and validation, decentralization, transparency, early detection, and compatibility with existing infrastructure. The paper concludes by emphasizing blockchain's potential in DDoS mitigation and the need for further research to address scalability and storage challenges in blockchain-based solutions.

2) **TrustGuard** [4] introduces a flow-level reputation-based defense mechanism. It focuses on analyzing the reputation of individual network flows rather than solely relying on IP addresses or packet-level attributes. By considering the reputation of each flow, TrustGuard aims to accurately identify and mitigate DDoS attack traffic while minimizing false positives.

   TrustGuard Architecture consists of several components:

   - Flow Collector: Gathers flow-level data, including traffic characteristics and behavior.
   - Reputation Manager: Calculates reputation scores for each flow based on historical behavior and real-time observations.
   - Decision Engine: Utilizes reputation scores to make traffic filtering decisions, distinguishing between legitimate and malicious flows.
   - Feedback Loop: Provides feedback to the Reputation Manager to continuously update reputation scores based on observed behavior.

   Reputation scores are calculated using a combination of historical data and real-time observations. It employs machine learning techniques to adaptively adjust reputation scores based on evolving traffic patterns and attack characteristics.

3) DiDoS [5] solution architecture is designed to mitigate DDoS attacks at the network layer using reputation-based techniques. Similar to TrustGuard components:

   - Reputation Manager: Collects and analyzes network traffic data to calculate reputation scores for IP addresses and network flows.
   - Decision Engine: Utilizes reputation scores to make real-time decisions about traffic routing and filtering, distinguishing between legitimate and malicious traffic.
   - Feedback Loop: Provides feedback to the Reputation Manager to continuously update reputation scores based on observed behavior and evolving attack patterns.

   DiDoS calculates reputation scores based on various factors, including historical behavior, traffic patterns, and real-time observations. It employs reputation-based algorithms to adaptively adjust scores and prioritize traffic based on their reputation levels. Also uses a Collaborative Defense Mechanism promoting collaborative defense by allowing participating network domains to share reputation data and coordinate responses to DDoS attacks. By leveraging collective intelligence and sharing information across domains, DiDoS aims to enhance the effectiveness of DDoS mitigation efforts.

4) Orchestrating DDoS mitigation via blockchain-based network provider collaborations [7] outlines a concept framework, which involves the following components and processes:

   - Blockchain Infrastructure: Establish a blockchain network among participating network providers to serve as a decentralized and immutable ledger for recording DDoS attack information, mitigation strategies, and collaboration agreements.
   - Smart Contracts: Implement smart contracts on the blockchain to automate and enforce agreements between network providers, including terms for sharing attack data, coordinating mitigation efforts, and distributing rewards or incentives for participating in the collaboration.
   - Attack Detection and Mitigation: Integrate detection and mitigation mechanisms into the blockchain network, allowing participating providers to share real-time attack information, analyze attack patterns, and coordinate mitigation responses in a synchronized manner.
   - Incentive Mechanisms: Design incentive mechanisms to encourage active participation and contribution to the collaborative DDoS mitigation efforts, such as rewarding providers for sharing attack data, deploying mitigation measures, or providing network resources during attacks.

REFERENCES

[1] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and Lyes Khoukhi. Cochain-sc: An intra- and inter-domain ddos mitigation scheme based on blockchain using sdn and smart contract. *IEEE Access*, 7:98893–98907, 2019.

[2] Richard R Brooks, Lu Yu, Ilker Ozcelik, Jon Oakley, and Nathan Tusing. Distributed denial of service (ddos): a history. *IEEE Annals of the History of Computing*, 44(2):44–54, 2021.

[3] G Dayanandam, TV Rao, D Bujji Babu, and S Nalini Durga. Ddos attacks—analysis and prevention. In *Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017*, pages 1–10. Springer, 2019.

[4] Haiqin Liu, Yan Sun, Victor C Valgenti, and Min Sik Kim. Trustguard: A flow-level reputation-based ddos defense system. In *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, pages 287–291. IEEE, 2011.

[5] Andikan Otung and Andrew P Martin. Distributed defence of service (didos): A network-layer reputation-based ddos mitigation architecture. In *ICISSp*, pages 619–630, 2020.

[6] Darshi Patel and Dhiren Patel. Collaborative blockchain based distributed denial of service attack mitigation approach with ip reputation system. In *International Conference on Database Systems for Advanced Applications*, pages 91–103. Springer, 2022.

[7] Adam Pavlidis, Marinos Dimolianis, Kostas Giotis, Loukas Anagnostou, Nikolaos Kostopoulos, Theocharis Tsigkritis, Ilias Kotinas, Dimitrios Kalogeras, and Vasilis Maglaris. Orchestrating ddos mitigation via blockchain-based network provider collaborations. *The Knowledge Engineering Review*, 35:e16, 2020.

[8] Bruno Rodrigues, Eder Scheid, Christian Killer, Muriel Franco, and Burkhard Stiller. Blockchain signaling system (bloss): cooperative signaling of distributed denial-of-service attacks. *Journal of Network and Systems Management*, 28(4):953–989, 2020.

[9] Jessica Steinberger. *Distributed DDoS Defense - A collaborative Approach at Internet Scale*. Phd thesis - research ut, graduation ut, University of Twente, Netherlands, September 2018.