Securing Log Files through Blockchain Technology

Louis M. Shekhtman
Nokia Bell Labs
louis.shekhtman@nokia.com

Erez Waisbard
Nokia Bell Labs
erez.waisbard@nokia.com

ABSTRACT

Development of secure methods for storing log files is of tremendous importance for cyber security. One of the first actions by a hacker upon penetrating a machine is editing the log files to remove evidence of their presence. We propose to improve the security of these log files through a blockchain based solution. We show how our solution can be used to help organizations to mutually protect their sensitive log data even if some of them are compromised. Our solution allows data confidentiality between the collaborative parties.

INTRODUCTION

Securing log files is a significant problem in the realm of cyber security [1]. Should a hacker manage to penetrate a system, their first move is often to go to the log files and erase traces of their presence. This often leaves system administrators clueless to the fact that they have been hacked and prevents them from taking actions to secure their systems.

BLOCKCHAIN-BASED SOLUTION

In order to solve this problem we suggest utilizing the nascent blockchain technology in order to securely store the logs and maintain multiple copies in a decentralized manner. Our solution involves multiple organizations, for example several large banks, banding together to create a private, permissioned blockchain where each organization uploads partial or entire log files onto the blockchain. Presumably, each orgaization (bank) would encrypt their information prior to uploading onto the blockchain in order to prevent the others from learning proprietary information. In addition, each organization could have multiple peers underneath it which all take part in submitting information to the blockchain and/or mining blocks.

Essentially our blockchain consists of *participants* possessing both a Participant ID and a Participant Name, who submit transactions to the blockchain. Each transaction includes a particular line of text to add to the blockchain, a File ID in which to add this line, and the Participant ID of the participant submitting the line. To get the text of a log file, one queries the blockchain for all transactions that have a particular FileID.

IMPLEMENTATION

We implement a version of our proposed solution using the Hyperledger framework. [2] We create the P2P network using Hyperledger Fabric, an open source tool for building private, permissioned blockchains. We then create logic for our blockchain using the Hyperledger Composer tool and install it on the various nodes of the network.

Using our framework one is able to implement all of the elements described above, including creating a participant, submitting a transaction, and querying the blockchain to obtain the contents of a particular log file.

APPLICATIONS AND CONCLUSIONS

Our main use case is for large organizations willing to securely store log file info in a semi-trusted environment in order to gain additional protection. Aside from that, our system could potentially be used by a single user seeking to create additional barriers against a hacker. In such a case the single user would expend computational power on proof-of-work mining, yet a hacker who penetrated their system would also have to expend the same computational effort on mining in order to edit the log files.

REFERENCES

[1] Rafael Accorsi. 2010. BBox: A distributed secure log architecture. In *European Public Key Infrastructure Workshop*. Springer, 109–124.

[2] Christian Cachin. 2016. Architecture of the Hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

SYSTOR, 2018, Haifa, Israel

ACM ISBN 123-4567-24-567/08/06…$15.00
https://doi.org/10.475/123_4