A System for Oblivious Decentralized Identity Resolving

DINH DUY KHA - 2019712308

April 19, 2021

1 Background

Decentralized ID. *Decentralized ID* (DID) is an emerging direction towards decentralized identity management systems. It allows user to store there identity on the internet without involement from any central authorities. The Decentralized ID Foundation [2] (DIF) proposes a three-step sheme for Decentralized Identity: verifiable credential issurance, DID generation, and identity authentication. In the said sheme, the requesting party "resolve" DID and get a public proof material called a *DID document*. It contains information for establishing secure interaction with the subject (i.e. the public key). The *resolve* process is typically done by a *DID resolver* through a HTTP connection. A decentralized identifier is then resolved to a DID document in JSON format, which is stored in a distributed ledger. This document contains a public key, authorization information, a list of interactive services with the ID. With the DID document, a requester could validate the credential of the ID's owner.

2 Motivation

DID resolver designs lack considerations for obliviousness. Current DID resolver designs do not take into account the fact that the cloud provider could *learn and remember* the spatial and temporal pattern of requests. As an example, when DID is used for authenticating physical entrance [3], with the time of request and the location of request gotten during authentication, the identity of the ID owner could be leaked. Moreover, due to the performance limitations of blockchain networks [1], the DID documents are often cached in the DID resolvers infrastructure. This lead to the *cache timing side-channel*, where an adversarial measure the response time before getting the document to infer if it has been accessed or not.

3 Challenges

Preserving confidentiality of DID and the document. Because of DID and document correlation, the universal resolver must perform the resolving process without knowing the requested DID and retrieved DID document.

Mitigate response time side-channel. DID document caching scheme must have a uniform response time to mitigate response time side-channel.

4 Plan and schedule

I plan to first perform a security analysis on the common DID Resolver infrastructure to come up with a set of security requirements. I will measure the response time of common DID infrastructures

for a concrete envidence of the response time side-channel. THe estimated time is 1 week. Then, I will propose a DID resolver design that satisfy the security requirements. A prototype will be implemented based on the design. The estimated time for this task is 2-3 weeks. Finally, I will measure the performance of the prototype with the *request-per-minute* metric, which shows how much request the resolver design could serve in a minute. Moreover, I will also measure the average response time as another performance metric. It will take approximately 1 week to finish. The final report will be written durring the whole process.

References

[1] T.-H. Kim, G. Kumar, R. Saha, M. K. Rai, W. J. Buchanan, R. Thomas, and M. Alazab, A privacy preserving distributed ledger framework for global human resource record management: The blockchain aspect, IEEE Access, vol. 8, pp. 96 45596 467, 2020.

[2] DIF, "Dif", `https://identity.foundation`, 2021

[3] W. P. Rachel Lerman, "Vaccine passport apps are here. but the technical challenges are still coming." `https://www.washingtonpost.com/technology/2021/04/02/vaccine-passports-apps-faq/`, 2021, last accessed Apr 2 , 2021,.