**Guía para la presentación de la propuesta**

**Introducción**

Muy buenas tardes a todos los presentes. Mi nombre es Daniel y la investigación que realice fue sobre protocolo de autenticación para el mejoramiento de la privacidad del usuario.

**Agenda**

Podemos ver en la agenda que iniciaré con un contexto y de ahí pasaremos al problema como tal, la justificación de porque es importante, la solución que yo ofrezco y, por último, un breve demo de lo que realice, así como los resultados de las pruebas.

**Contexto**

Normalmente tu como persona tienes una identidad, algo que te permite diferenciarte de otras personas. Esta identidad se utiliza para identificarte, es decir, para corroborar que que tú eres en realidad quien dice ser y comprobarlo mediante una autenticación. La autenticación e identificación son utilizados en diversos tipos de sistemas, no solo informáticos, sino también para sistemas como bancos, votación, entre otros. Por lo tanto, en un sistema, una autenticación es muy importante para darte accesos a diferentes recursos del sistema.

La autenticación de usuarios se ha basado mayormente en arquitecturas centralizadas, es decir, aquellos sistemas que están organizados de tal forma que exista una sola entidad que se encarga de la mayoría de las tareas. Tomando C.A.S., Centralized Authentication Service como un ejemplo de ello.

Además de esto, también encontramos los sistemas distribuidos que son cada vez más importantes hoy en día. Caracterizados por ser un conjunto de computadoras separadas físicamente, pero conectadas entre sí, se percibe a este conjunto como un solo sistema. Blockchain por ejemplo.

**El Problema**

Actualmente, uno de los problemas que se generan al momento de la autenticación, presentados en los protocolos centralizados, es que quien identifica a los usuarios es una sola entidad, la autoridad certificadora. De esta manera, un ataque realizado por un tercero malicioso se centrará en corromper dicha entidad. Este tipo de ataques pueden negar el acceso a servicios de la aplicación a diferentes usuarios, entre otras cosas.

Por otro lado, la autenticación distribuida también tiene ciertos inconvenientes. Principalmente, al ser un sistema basado en confianza en donde el usuario no se identifica, es muy difícil saber la identidad de las personas que están realizando algún tipo de transacción u otro tipo de movimiento. Por lo cual, si una transacción es ilícita, no se sepa quiénes son los usuarios de esa transacción.

**Justificación**

Lo que digo con esto es que los sistemas tipo, bancos o de voto que son centralizados, si yo ataco directamente un banco podría robarme el dinero de varias cuentas. Y en el caso de los distribuidos es que aún no se encuentra tan regulado como algo centralizado.

De esta manera, dado que uno de los protocolos más utilizados en los sistemas son los de autenticación, es muy importante que se realice de manera segura. La solución óptima sería un protocolo que solo otorga acceso a cierta información. Es decir, que el protocolo le ayude al sistema a saber la identidad de sus usuarios y que a su vez permita cierto anonimato del usuario en transacciones en las que no se requiera ser identificado.

Corda, utilizando tecnología tipo blockchain, nos ofrece este enfoque mediante la distribución de la propiedad de las credenciales y la disponibilidad de almacenar en una cadena inmutable de datos. Estos son almacenados en un ledger que es distribuido a cada nodo de la transacción, reflejando un registro de cada transacción realizada. Mientras que C.A.S. ayudará a regular a las entidades que intenten ingresar al sistema otorgando certificados a cada entidad. Que estos posteriormente se utilizarán para la autenticación distribuida.

**Solución**

Lo que yo ofrezco como solución es un prototipo de protocolo de autenticación el cual utiliza estás dos tecnologías Corda como una plataforma de ledger distribuida y C.A.S. como servicio de autenticación centralizado. De esta forma, C.A.S. realiza una autenticación de la identidad de las personas, las procesa y si la autenticación es exitosa le otorgaba un token para poder realizar contratos en Corda. Mientras que Corda, al ser una red de autorización, existe un Doorman que firma si el token es válido o no, una vez que le token fue firmado por el Doorman el usuario ya puede realizar sus contractos en una red de nodos los cuales a su vez autentican al nodo con el que están realizando la transacción.

**Demo**

A continuación, les enseñaré un demo de la aplicación que realiza está autenticación.

“Proyecta demo 1:30”

**Resultados**

Los resultados que nos mostraron las pruebas para este protocolo es que los usuarios pueden acceder sin ningún problema, mientras que los maliciosos se quedan estancados en un proceso de la autenticación entre la autenticación centralizada y el Doorman de Corda. Esto en gran manera por lo implementado hasta el momento por corda que normalmente lo realiza internamente. En las pruebas se demostró que una entidad llamada partyA y una entidad llamada partyB realizaron una transacción exitosa siendo autenticados satisfactoriamente, mientras que otras entidades no lograron acceder a la plataforma del ledger al tener un certificado falso que el Doorman no pudo firmar o una autenticación fallida durante el proceso de autenticación centralizado.

**Finalización**

Para terminar, mi propuesta de mejora es realizar pruebas en un ambiente mayor donde haya más usuarios y más entidades maliciosas. Además de que, como había mencionado antes, pienso en que se podría utilizar para autenticación en los protocolos de votación o de esta índole por ejemplo SAT. Finalizando con mi presentación, doy las gracias por su atención y quedo atento a cualquier pregunta.