Protocolo de autenticación de transacciones con identificación de usuarios

Daniel Adalaid Carranza Alvarez

Tecnológico de Monterrey Campus Querétaro, Epigmenio González #500, Querétaro Qro, Mexico

**Abstract.** Autenticarse en una aplicación tanto móvil como de escritorio, web o de otra índole es muy común en las tecnologías de hoy en día, ya que esto garantiza que la persona correcta está ingresando a dichas aplicaciones. Por esta razón, es muy importante tanto para el usuario como para la aplicación saber la identidad de cada uno. Por lo tanto, en esta propuesta se busca generar un protocolo de autenticación que, utilizando características tanto de protocolos distribuidos como centralizados, permita la autenticación de usuarios de manera segura y que a la vez permita identificar al usuario sin solicitar más información de la necesaria.

**Keywords: A**utenticación distribuida, autenticación, protocolos, seguridad.

1 Antecedentes

La autenticación e identificación son mecanismos en los sistemas informáticos usados para acceder a los recursos que estos tienen. Redes sociales, correos electrónicos o inclusive cuentas bancarias necesitan una autenticación por parte del usuario y como tal una parte autenticadora que verifique dicha identidad. Es decir, la autenticación es el proceso de comprobar la identidad del usuario o equipo que desea ingresar al sistema [1], hablando de identidad como algo que permite diferenciarse de otros [4]. Mientras que la identificación es un proceso que sirve para corroborar que una entidad es quien dice ser [1].

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 de confianza que se encarga de la mayoría de las tareas [5]. C.A.S. servicio de autenticación centralizada por sus siglas en inglés, es un claro ejemplo. Creado por la Universidad de Yale, este protocolo utiliza un servidor que pide al usuario sus credenciales para acceder y, si estas son correctas, el usuario puede consumir los servicios [11].

Además de esto, también encontramos los sistemas distribuidos que son cada vez más usados, caracterizados por ser un conjunto de computadoras separadas físicamente, pero conectadas entre sí, percibiendo a este conjunto como un solo sistema [2]. Blockchain es un ejemplo de esto, siendo este una base de datos distribuida que funciona como libro para el registro de operaciones compra-venta o de cualquier otra transacción. Esto ha permitido generar una arquitectura en donde Blockchain se usa como notario público distribuido no modificable de todo el sistema de transacciones, a fin de evitar el problema de que, por ejemplo, una moneda se pueda gastar dos veces [3].

Se puede observar que Blockchain utiliza los mismos principios criptográficos que podrían aplicarse a una autenticación de manera distribuida. Al distribuir un archivo de registro entre todos los miembros de la red, la autenticación distribuida erradica el poder modificar maliciosamente el archivo. Ya que, al añadir un nuevo bloque de datos a la cadena, la mayoría de los nodos de la red debe verificar su validez, lo que garantizaría también la integridad de la información [1].

2 Planteamiento del 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. Un ejemplo de ello es el ataque de negación de servicios, DoS por sus siglas en inglés, que se realizó hace poco más de un año a Dyn, un importante proveedor de nombres de dominio, que daba servicio a clientes importantes como Spotify, Netflix y Twitter [7]. Ya que el servicio de DNS es un servicio centralizado, similar a la Autoridad Certificadora, es posible que un ataque similar sea realizado a un servicio de autenticación centralizada generando un impacto similar.

Por otro lado, la autenticación distribuida también tiene ciertos inconvenientes. Principalmente, por ser un sistema basado en confianza en donde el usuario no es identificado, no existe una forma criptográfica de verificación de la identidad de las personas que están realizando algún tipo de transacción u otro tipo de movimiento. Es decir, que en un protocolo de autenticación distribuido sólo se puede autenticar a la entidad involucrada mas no identificarlo provocando el anonimato del usuario y de esta manera, que, si una transacción ilícita es realizada, no sea posible identificar al usuario de esa transacción.

3 Justificación

Dado que los protocolos de autenticación son la base de acceso de muchos de los sistemas usados hoy en día, es muy importante que esta se realice de manera segura. La solución óptima sería un protocolo que solo otorga acceso a cierta información quitando la necesidad de que cada sistema almacene credenciales por usuario. Es decir, que el protocolo le ayude al sistema o servicio a conocer 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.

Blockchain 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 libro compartido que es distribuido a cada entidad, reflejando un registro de cada transacción realizada. Mientras que C.A.S. o cualquier otro protocolo de autenticación centralizada permitirá que el usuario sea identificado mediante la autoridad certificadora y así poder conocer la identidad del usuario.

4 Contribuciones Esperadas

Se espera contribuir con un prototipo de protocolo de autenticación para mejorar la autenticación del usuario tanto para la aplicación como para el usuario que desea autenticarse, utilizando ciertas características tanto de protocolos centralizados como distribuidos. Es decir, el protocolo se comportaría de la manera en que el centro de la autenticación de bloque de bloques sería un ID de bloque de bloques y sea otorgado por la autoridad certificadora. Este ID es un bloque de datos en la cadena que podrá ser verificada por algún tercero y que solo muestre la información necesaria.

Para la verificación se usará un algoritmo de firma digital de manera que, cuando se añada un ID a Blockchain, un servicio de emisión de identificación enlace una clave pública de forma predeterminada y luego transfiera la propiedad de la clave privada al usuario. Esto permite que solo el usuario firme una firma que se puede verificar contra la clave pública almacenada en la cadena de bloques. Esta identificación de un usuario sería una fuente distribuida de autenticación. Sería esencialmente un portal de inicio de sesión único al que cualquier aplicación puede acceder pero que no pertenece a ninguna entidad individual.

Se espera generar el prototipo del protocolo con estas características y que de esta manera se pueda asegurar la autenticación como una propiedad de seguridad, permitiendo así una autenticación de manera segura y eficaz.

5 Metodología

Para lograr complementar esta investigación, se desarrollará el prototipo de un protocolo de autenticación que permita autenticar a los usuarios de una manera segura, simple y lo más distribuida posible. Así mismo para el desarrollo de este protocolo se utilizará un marco de referencia para desarrollar el proyecto, en este caso se utilizarán algunas prácticas que sugiera Disciplined Agile [9] para el desarrollo del proyecto. Además de esto, se utilizarán procesos previamente definidos para el desarrollo del protocolo que faciliten su implementación, utilizando el marco de referencia de CMMI [10]. Esto con la finalidad de que se logren hacer pruebas al protocolo y pueda ser comparable con algunos de los protocolos de autenticación ya existentes.

6 Bibliografía

|  |  |
| --- | --- |
| [1] | Internet Security Glosary in RFC 2828. In http://www.ietf.org/rfc/rfc2828.txt. |
| [2] | Pradep, S. Distributed Operating Systems: Concepts and Design. PHI Lerning Private Limited: 2012. |
| [3] | Hari, A. The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet. Proceeding. HotNets '16 Proceedings of the 15th ACM Workshop on Hot, 2016. |
| [4] | Cambridge Dictionary. Definition of Identity. Retrieved From http://dictionary.cambridge.org/es/diccionario/ingles/identity |
| [5] | Somerville, I. Ingeniería del Software. Pearson: 2006. |
| [6] | González, M. La gran inseguridad del internet de las cosas, la culpable del ataque DDoS qué noqueó la web. Recuperado de: https://www.xataka.com/servicios/los-responsables-del-ddos-a-dyn-usaron-camaras-ip-y-dvrs-para-tumbar-medio-internet |
| [7] | Ramiro, R. Gestion de identidades y accesos, Blockchain. Recuperado de: https://ciberseguridad.blog/blockchain-para-la-autenticacion-y-verificacion-de-nuestra-identidad/ |
| [8] | Ambler, S. Disciplined Agile Delivery: A Practitioner’s Guide to Agile Software Delivery in the Enterprise. IBM Press: 2012. |
| [9] | Chrissis, M. CMMI Guidelines for Process Integration and Product Improvement. Addison-Wesley: 2007 |
| [10] | Unicon. Central Authentication Service (C.A.S.). Recuperado de https://www.unicon.net/opensource/cas |