COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI

MÁSTER EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE MÁSTER

DECENTRALIZED APPLICATIONS' SAFETY AND SECURITY

Autor: Miguel Oleo Blanco

Director: Yue Duan

Co-Director: Sajad Meisami

Madrid

Índice del anexo B

Capítulo 1. INTRODUCCIÓN

En este proyecto se investigar la seguridad que implementan las aplicaciones descentralizadas del blockchain. Es un estudio motivado por todos los precedentes que han ocurrido en esta área de estudio, en la que históricamente ha habido muchos fraudes. En concreto, se estudiarán los permisos que las carteras de criptomonedas dan a las aplicaciones y cómo funcionan los mecanismos de seguridad que implementan las carteras, aplicaciones y los mecanismos propuestos por Ethereum.

En este proyecto, a partir del conocimiento ganado de la investigación, se busca conseguir un mecanismo metódico que indique si una aplicación descentralizada es segura o no. Este mecanismo metódico se implementará con análisis estático del código fuente de las aplicaciones.

Capítulo 2. ESTADO DE LA CUESTIÓN

Como se ha citado anteriormente, han ocurrido ataques a dichas aplicaciones descentralizadas, dejando las carteras de los usuarios expuestas. Un ejemplo de esto es Harevst Keeper [1], la cual fue hackeada y se perdieron alrededor de un millón de dólares de los usuarios. Este tipo de ataques es bastante común ya que, por defecto, cuando conectamos una cartera de criptomonedas a una aplicación, se establece el número máximo de monedas que son accesibles por la aplicación. Esto quiere decir que, al realizar la conexión con la aplicación, se le da permiso a esta para acceder a cierto número de monedas (estén disponibles o no). Por defecto, este número de monedas accesibles es alto, por lo que cuando una de estas aplicaciones tiene problemas de seguridad y es hackeada, pueden retirar de las carteras de los usuarios ese número de monedas sin que los usuarios tengan que aprobar esa transacción (ya que cuando se conecta la cartera, ya se da permiso a manipular dichas monedas)

Otro problema de estas aplicaciones es, que las carteras, por necesidad, se ven obligadas a dar soporte a *APIs* que se certificaron que no son seguras. Esto se debe a que, muchas aplicaciones no migran sus códigos fuentes a las nuevas tecnologías y no implementas las nuevas *APIs* seguras. Un ejemplo de esto son las APIs relacionadas con las firmas. En el mundo del blockchain, se firman (encriptan) las transacciones y mensajes que se transmiten por el blockchain. Estos métodos de firma son sensibles, ya que estos son los sistemas que conforman los mecanismos de seguridad de la aplicación, sus comunicaciones. En estos mensajes cifrados se incorporan datos sensibles como pueden ser: dirección de las carteras del cliente y destinatario, mensajes privados entre usuarios, etc. No usar los nuevos mecanismos propuestos por las carteras y por el EIP [2]. Este es uno de los puntos más críticos de la seguridad de las aplicaciones y del cual los atacantes se aprovechan. Un claro ejemplo de esto es cómo se robaron más de un millón de dólares de la plataforma de NFTs OpenSea [3], que también combino esta vulnerabilidad con un ataque de phishing.

Capítulo 3. MOTIVACIÓN

A partir de lo explicado en la introducción y el estado de la cuestión, queda bastante claro que es necesario un mecanismo para determinar si una aplicación es de fiar. Estas aplicaciones deberían de pasar una serie de pruebas de seguridad antes de ser publicadas para poder detectar este tipo de fallos.

Esto podría impulsar el éxito de las aplicaciones ya que se garantizará una seguridad necesitaría para los usuarios. Esta confianza que se le ofrece al usuario beneficia a la industria de las aplicaciones descentralizadas y al propio blockchain, ya que impulsaría un crecimiento exponencial de usuarios.

Capítulo 4. OBJETIVOS DEL PROYECTO

- Documentación detallada: Al analizar todas estas aplicaciones y las APIs de seguridad que proporcionan las carteras, queda constatada la poca información que hay disponible. Entre otras cosas, con este trabajo se busca poder documentar fielmente estas APIs relacionadas con la seguridad y los permisos que se entregan a las aplicaciones. Es necesario entender cómo funcionan estos mecanismos antes de poder analizar sus posibles fallos de seguridad, por lo que este objetivo es derivado del segundo objetivo.
- Mecanismo para determinan fallos de seguridad: Una vez estudiado cómo funcionan las APIs relacionadas con permisos entre carteras y aplicaciones, y las APIs relacionadas con la firma y encriptación, se buscará cómo encontrar estos fallos en las aplicaciones. Para ello, se analizará el código fuente de dichas aplicaciones en busca de implementaciones erróneas y peticiones de permisos sobredimensionadas.
- *Paper*: como objetivo final está presentar los resultados en formato *Paper*. Los resultados obtenidos pueden tener el impacto suficiente como para que el resto de la comunidad científica deba conocerlo. Por ello, como objetivo final se pretende publicar los resultados siempre que estos estén a la altura de contenidos en un *paper*.

Capítulo 5. ALINEACIÓN CON LOS ODS

Este proyecto se alinea principalmente con los objetivos de desarrollo sostenible números 9, 11 y 12. Estos tres objetivos son correspondientemente: industria, innovación e infraestructura; ciudades y comunidades sostenibles; producción y consumo responsables.

En cuanto al primer objetivo y segundo objetivo, blockchain nos ofrece una nueva infraestructura muy útil de cara al futuro, ya que es una red descentralizada y nos permite trazar todos los elementos que se mueven en esta red. Esta infraestructura ya implementa novedades como puede ser el dólar digital, el cual afecta a comunidades. Para que esto sea sostenible, hay que tener en cuenta el punto número 12 de las ODS. Este es un factor clave, ya que se ha comprobado que esta red de bloques es muy poco eficiente. Esto se debe a la gran cantidad de cálculos que se realizan para que esta red funcione de forma segura y descentralizada. Debido a esto, la red necesita una cantidad de energía superior a la que consumen algunos países. Uno de los puntos clave para que esta tecnología prospere es reducir este consumo. Esto ya se implementa en algunas de sus utilidades como puede ser Ethereum, el cual con la versión dos ha cambiado la forma de comprobar transacciones por una que requiere menos esfuerzo computacional y, por tanto, menos consumo.

Capítulo 6. METODOLOGÍA DE TRABAJO

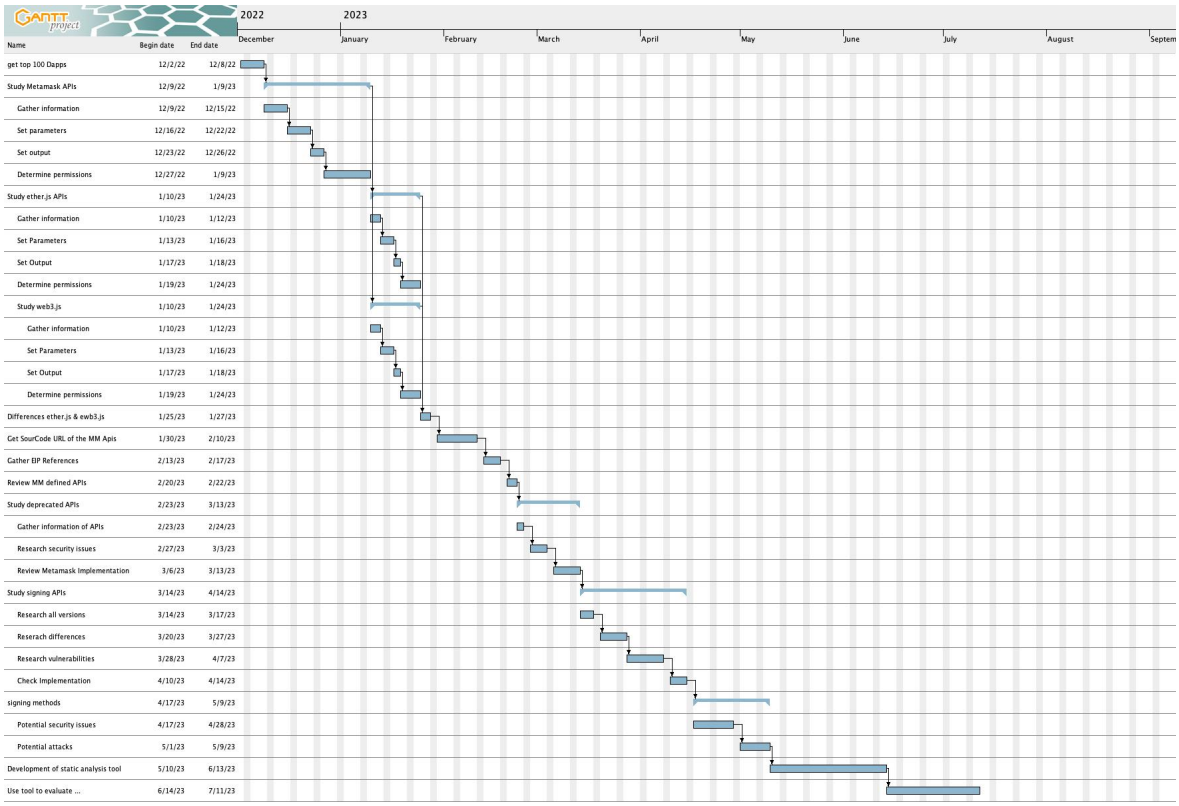

Ilustración 1: Cronograma del proyecto en formato Gantt

Como se puede ver en la ilustración 1, el proyecto se divide en muchas tareas. Alguna de estas está englobada en objetivos más grandes, como puede ser estudiar ether.js. La gran mayoría de fases se dividen en investigación y documentación, y por último la implementación. El cronograma nos aporta información sobre las tareas y las fechas objetivo. El proyecto empieza con una gran carga de investigación sobre las APIs y la documentación de estas. Después, se investiga y documenta en profundidad las APIs con posibles brechas de seguridad, como pueden ser las APIs encargadas de permisos, firmas, etc. Por último, se elaborará una herramienta para poder analizar las aplicaciones de forma sistemática en busca de brechas de seguridad. Una vez la aplicación sea funcional, se realizará un estudio de los resultados obtenidos de analizar las principales aplicaciones. A continuación, se van a comentar de forma breve las distintas fases del proyecto.

Para realizar todas estas tareas, la fase de investigación previa es muy importante. Esta fase es la que nos permite obtener el conocimiento necesario para, al llegar a la fase más técnica, poder afrontar los problemas que se generen.

Otra parte muy importante de la metodología, que se basa en la fase de investigación, es la documentación. Durante el trabajo se han recopilado varios métodos y características sobre APIs de Metamask [4]. En este trabajo nos centramos en Metamask y sus APIs ya que es la cartera de blockchain más usada. Esta cartera, a pesar de estar documentada, es necesario complementar dicha documentación con la información obtenida durante la fase de investigación.

Una vez disponemos de toda la información necesaria, se procederá a crear una herramienta que analice el código fuente de distintas aplicaciones descentralizadas. La creación de esta herramienta es uno de los derivados más importantes de este trabajo.

Estas tres fases *a priori* se implementarán con una metodología de tipo circular, lo que quiere decir que las tres fases se irán repitiendo a lo largo de la duración del proyecto. Esta metodología en la industria es más conocida como *Agile*, ya que se basa en pequeños *sprints* (periodos de corta duración en los que se trabaja para obtener un entregable), y se reiteran a lo largo de la aplicación. Este método nos ofrece la posibilidad de ir teniendo partes del producto final e ir trabajando sobre ellas de forma iterativa para perfeccionar el producto final y poder solucionar problemas y añadir nuevas características.

Una vez se haya creado la herramienta, se realizará un estudio en profundidad sobre las aplicaciones principales y se comentará el resultado obtenido, así como el rendimiento de la herramienta.

Capítulo 7. RECURSOS A EMPLEAR

En cuanto a los recursos que se van a emplear para conseguir el objetivo final, podemos encontrar distintas herramientas y fuentes de información. Una de las páginas que se emplearán varias veces a lo largo del proyecto es DappRadar [5]. Con la información de esta página web, se obtendrá y analizará el código fuente de las aplicaciones usando GitHub [6]. Ya que este trabajo se realiza entre varias personas, se ha establecido que la plataforma colaborativa que se empleará es Google Drive y Google Docs.

En cuanto a la cartera que se estudia en el proyecto, esta es Metamask. Esta cartera nos ofrece documentación [7] y una herramienta interactiva con las distintas APIs llamada Metamask Playground [8]

Capítulo 8. BIBLIOGRAFÍA

[1] Batycka, D. (2023, March 20). *AI dApp Harvester Keeper gets hacked for almost $1M*. CryptoSlate. https://cryptoslate.com/ai-dapp-harvester-keeper-gets-hacked-for-almost-1m/

[2] Proposals, E. I. (n.d.). *Home | Ethereum Improvement Proposals*. Ethereum Improvement Proposals. https://eips.ethereum.org/

[3] Brandom, R. (2022, February 20). *$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users*. The Verge. https://www.theverge.com/2022/2/20/22943228/opensea-phishing-hack-smart-contract-bug-stolen-nft

[4] The crypto wallet for Defi, Web3 Dapps and NFTs | MetaMask. (n.d.). https://metamask.io/

[5] *Website to get top DApps*. (n.d.). Dapp Radar. https://dappradar.com/

[6] *GitHub: Let's build from here*. (n.d.). GitHub. https://github.com/

[7] *Introduction | MetaMask Docs*. (n.d.). https://docs.metamask.io/guide/

[8] *Herramienta interactiva de APIs de Metamask*. (n.d.). Metamask Playground. https://metamask.github.io/api-playground/api-documentation/