DeFi 보안 취약점 기반 디지털 헬스케어 공격 시나리오

박상현[1], 송유래[2], 곽진[3]
[1]아주대학교 사이버보안학과, 정보보호응용및보증연구실 학부생
[2]아주대학교 사이버보안학과, 정보보호응용및보증연구실 석사과정
[3]아주대학교 사이버보안학과 교수
chipkkang9@ajou.ac.kr, clara701@ajou.ac.kr, security@ajou.ac.kr

Digital Healthcare Attack Scenario based on DeFi Security Vulnerability

Sang-Hyeon Park[1], Yu-Rae Song[2], Jin Kwak[3]
[1,2]ISAA Lab., Dept. of Cyber Security, Ajou University
[3]Dept. of Cyber Security, Ajou University

요 약

IT(Information Technology) 기술이 고도화됨에 따라 금융 분야에서는 스마트 컨트랙트에 기반하여 자산을 거래할 수 있는 DeFi(Decentralized Finance)가 발전하고 있다. 또한, 다양한 IoT(Internet of Things) 기기들로 구성된 융합환경이 상호 연결되며 IoBE(Internet of Blended Environment)가 조성되고 있다. IoBE의 구성요소 중 의료융합환경인 디지털 헬스케어는 스마트 의료 기기를 통해 진료 서비스를 제공한다. 최근에는 디지털 헬스케어 내 자산 거래 수단으로 DeFi를 활용하기 위한 연구가 진행되고 있다. 그러나, 디지털 헬스케어 서비스에 DeFi가 활용될 수 있음에 따라 DeFi 내 보안 위협이 전파될 수 있다. 전파된 보안 위협은 DeFi에서의 디지털 화폐 탈취뿐만 아니라, 디지털 헬스케어 내 민감 정보 탈취, 서비스 거부 공격 등 복합 위협으로 이어질 수 있다. 따라서, 본 논문에서는 DeFi의 취약점을 분석하고 이를 기반으로 디지털 헬스케어에서 발생 가능한 공격 시나리오를 도출한다.

1. 서론

IT(Information Technology) 기술이 고도화됨에 따라 금융 분야에서는 스마트 컨트랙트에 기반하여 자산을 거래할 수 있는 DeFi(Decentralized Finance)가 발전하고 있다[1]. 또한, 다양한 IoT(Internet of Things) 기기들로 구성된 융합환경이 상호 연결되며 IoBE(Internet of Blended Environment)가 조성되고 있다. IoBE의 구성요소 중 의료융합환경인 디지털 헬스케어는 스마트 의료기기를 통해 대면 및 비대면 진료 서비스를 제공한다. 디지털 헬스케어 서비스를 운영하는 병원의 수가 증가하고 DeFi가 발전함에 따라, 디지털 헬스케어 서비스의 자산 거래 수단으로써 DeFi를 활용하기 위한 연구가 진행되고 있다[2]. 그러나, 디지털 헬스케어에 DeFi가 활용되며 이를 대상으로 한 새로운 복합 위협이 발생할 수 있다. 따라서, DeFi가 디지털 헬스케어와 연결되었을 때 발생 가능한 공격 시나리오 도출이 필요하다.

본 논문은 2장에서 디지털 헬스케어와 IoBE, DeFi에 대해 설명하고, 3장에서 DeFi의 취약점을 분석한다. 4장에서는 분석한 취약점에 기반하여 디지털 헬스케어를 대상으로 발생 가능한 공격 시나리오를 도출하고, 5장에서 결론을 맺는다.

2. 관련 연구

2.1 디지털 헬스케어

디지털 헬스케어는 의료 영역에 ICT(Information and Communication Technology) 기술을 활용하여 개인 건강 및 질환을 관리하는 산업 영역이다. 디지털 헬스케어는 개인 건강관리, 건강 검진 등의 서비스를 제공하기 위해 환자의 개인정보 및 민감정보를 수집한다. 이때 수집된 환자의 데이터는 의료 빅데이터 분석을 통한 사용자 맞춤 디지털 치료 서비스 제공에 사용된다[3]. 최근에는 디지털 헬스케어 서비스 제공 이후의 자산 거래 수단으로 DeFi를 도입하는 연구가 진행 중이다[2].

2.2 IoBE

IoBE는 센싱, 네트워킹, 빅데이터, 인공지능, 클라우드 등 다양한 IT 기술 기반 융합환경이 상호 연결된 환경으로, 디지털 헬스케어, 스마트 팩토리, 스마트 그리드 등을 포함한다. 그러나, 융합환경에서 통신하는 데이터의 종류가 다양해지고, 네트워크 복잡도가 증가함에 따라 공격 표면이 증가할 수 있다. 이에 따라, IoBE 내 취약점이 융합되어 예측하기 어려운 복합 위협(Blended Threat, BT)이 발생할 수 있다[4].

2.3 DeFi

DeFi는 블록체인 네트워크에서 스마트 컨트랙트의 소스코드를 기반으로 동작하는 탈중앙화 금융 환경이다. 중앙기관의 개입 없이 분산 환경에서 탈중앙화 거래소를 통한 디지털 화폐 생성, 개인 간 거래 및 폐기가 가능하다[1].

3. DeFi에서 발견된 취약점

3.1 DoS(Denial of Service) 취약점

DoS 취약점은 공격자가 악성 토큰을 발행한 후 공격 대상자의 가상 지갑에 추가되었을 때 실행되며 지갑의 거래를 정지시킨다. 예로, setCreatorRoyaltiesReceiver 함수는 DoS 공격을 실행할 수 있다. 해당 취약점은 DeFi의 자산 흐름을 정지시킬 수 있다[5].

3.2 자격 증명 위장 취약점

자격 증명 위장 취약점은 특정 사용자의 토큰을 탈취하기 위해 토큰 출금 자격을 위장함으로써 출금 과정에서의 인증 단계를 통과한다. 예로, EthStakeStrategy 함수에 자격 증명 위장 공격을 실행할 수 있는 취약점이 있다. 해당 취약점은 블록체인의 투명성으로 인해 토큰뿐만 아니라, 사용자 정보까지 탈취할 수 있다[6].

4. DeFi 취약점 기반 디지털 헬스케어 공격 시나리오

Step 1. 공격자의 악성 토큰 생성

공격자는 스마트 컨트랙트 내에 출금 자격 증명 위장 및 DoS 취약점이 포함된 악성 토큰을 생성한다.

Step 2. 탈중앙화 거래소에 악성 토큰 등록

공격자는 탈중앙화 거래소에 악성 토큰을 등록하여 유입시킨다.

Step 3. 공격자의 지속적인 악성 토큰 흐름 추적

공격자는 토큰 거래 내역을 확인할 수 있는 Etherscan, Btc 등의 블록체인 익스플로러를 사용하여 지속적으로 악성 토큰의 흐름을 추적한다.

Step 4. 공격 대상의 가상 지갑으로 악성 토큰 유입

탈중앙화 거래소에 유입된 악성 토큰이 거래소와 사용자 간 거래를 통해 공격 대상의 가상 지갑으로 유입된다. 공격 대상은 해당 토큰이 악성임을 인지하지 못한 상태이다.

Step 5. 공격 대상과 병원 간 토큰 거래

사용자는 디지털 헬스케어 서비스 사용 후 악성 토큰을 병원에 지불한다. 사용자가 지불한 악성 토큰은 병원의 가상 지갑에 등록된다.

Step 6. DoS 공격 실행 및 금전 요구

공격자는 병원의 가상 지갑에 악성 토큰이 추가된 것을 확인하고 DoS 취약점을 실행시켜 DeFi를 활용하는 병원의 모든 자산 거래를 정지시킨다. 공격자는 DoS 공격을 중단하는 조건으로 병원에 금전을 요구한다.

Step 7. 자격 증명 위장 공격 실행 및 정상 토큰 탈취

공격자는 병원으로부터 금전을 갈취한 이후, 자격 증명 위장 취약점을 실행시켜 병원 가상 지갑에 등록된 정상 토큰을 탈취한다. 이때 탈취한 정상 토큰으로부터 사용자의 개인정보 및 민감정보까지 탈취할 수 있다.

5. 결론

본 논문에서는 DeFi에서의 취약점을 분석하고, DeFi와 디지털 헬스케어가 연결되었을 때 발생 가능한 DeFi 취약점 기반 공격 시나리오를 도출하였다. 이와 같이 DeFi가 다양한 IT 기술 및 융합환경과 연결됨에 따라 DeFi 취약점 기반 공격이 전파될 수 있다. 따라서, IoBE와 DeFi가 연결되었을 때 발생할 수 있는 새로운 복합 위협에 대한 연구가 필요하다. 추후, IoBE 내 다른 융합환경과 DeFi가 연결됐을 때의 복합 위협에 대응하기 위한 연구를 진행할 예정이다.

사사문구

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2021R1A2C2011391)

참고문헌

[1] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt, “SoK: Decentralized Finance(DeFi)”, AFT’2022, pp.30-46, Jul. 2022.

[2] the Cryptonomist, “Binance Pay with Solve.Care enable crypto payments for healthcare services”, 2023. [Online]. Available: https://en.cryptonomist.ch/2023/09/13/binance-pay-solve-care-enable-crypto-payments/

[3] KISA, “디지털 헬스케어 보안모델”, Dec. 2021.

[4] Minkyung Lee, Julian Jang-Jaccard, and Jin Kwak, “Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment”, CMC-COMPUTERS MATERIALS&CONTINUA, Vol. 73, No. 1, pp.199-223, Mar. 2022.

[5] Immunefi, “Charged Particles Griefing Bugfix Review”, 2023. [Online]. Available: https://medium.com/immunefi/charged-particles-griefing-bug-fix-postmortem-d2791e49a66b

[6] Tranchess, “Tranchess Liquid Staking Deposit Firstrun Vulnerability Analysis”, 2023. [Online]. Available: https://www.kalos.xyz/blog/tranchess-liquid-staking-deposit-firstrun-vulnerability-analysis