DID 인증 기반 Matter Commissioning 에서의 PASE 단계 보안성 강화 방안

최재호, 송해준, 오한수, 김기형*
*아주대학교

cjh7748@ajou.ac.kr, young7135@ajou.ac.kr, ogemini@ajou.ac.kr, kkim86@ajou.ac.kr

A Method of Enhancing Security in PASE Session of Matter Commissioning Based on DID Authentication

Choi Jae Ho, Song Hae Jun, Oh Han Su, Kim Ki Hyung*
*Ajou Univ.

요 약

최근 몇 년 동안 사물인터넷(IoT) 기술과 스마트 홈 시장이 급성장하면서, IoT 기기 간의 연결성과 호환성을 강조하는 새로운 표준으로 'Matter'가 등장하였다. 본 논문에서는 Matter 기기의 Commissioning 중 비밀번호 인증방식인 PASE 단계에 분산 식별자(DID) 기반의 인증 메커니즘을 통합하여 IoT 환경의 보안 취약점을 해결하는 방안을 제안한다. 해당 연구는 Matter 환경에서의 탈중앙화 인증 및 제어 방안을 제안하며 Matter 환경에서 DID 인증이 적용될 경우 도출될 수 있는 보안 이점을 제시한다.

.

Ⅰ. 서 론

지난 몇 년간, 사물인터넷(IoT) 기기의 판매량과 가정 내 도입이 꾸준히 증가하고 있다. IoT 기술의 진보와 함께 가전기기의 효율성과 편의성을 중시하는 추세가 점점 증가하고 있기 때문에 이러한 증가 현상은 지속될 것으로 전망된다. 조사에 따르면 2030 년 스마트 홈 시장은 최대 8,300 억 달러의 가치가 있을 것이라고 예상된다[1].

스마트 홈 시장의 변화와 함께 제조사별이나 통신 방식별로 다양한 IoT 기기들이 출시되고 있는데 서로 다른 IoT 기기의 통합을 위해 Matter 표준이 등장하였다[2]. 구글, 애플 등 주요 제조사들은 Matter 표준을 도입하고 연구하여 다양한 제조사의 IoT 기기들이 서로 원활하게 상호작용하는 환경을 조성하려 하고 있다.

하지만, 아직 IoT 의 보안은 절대 완벽하지 않으며, 패스워드 탈취 등 다양한 취약점이 존재한다. 조사 결과에 따르면, IoT 장치의 83%가 안전하지 않은 채널을 통해 통신하고 있으며, 이 중 대다수는 홈 어시스턴트, 스마트 홈 등과 관련된 일상생활 기기이다[3]. 더 나아가, IoT 기기의 57%가 해커에 의한 다양한 공격에 취약한 것으로 나타났다[4].

본 논문은 분산 식별자(Decentralized Identity, 이하 'DID') 기반의 인증 메커니즘을 Matter 표준의 Commissioning 과정에 적용하여 Matter 지원 기기의 보안성을 강화하는 방법을 제안한다. 해당 연구는 Matter 환경에서의 탈중앙화 기반 인증 및 제어 방안을 연구하고 더 안전하고 효율적인 디지털 상호인증을 가능하게 하는 것을 목표로 한다.

Ⅱ. 관련 연구

1. Matter 의 PASE 단계

Matter 기기를 홈 네트워크에 연결하여 활성화하려면 Fabric 에 신규 등록을 하는 과정이 필요하다. 이러한 과정을 Commissioning 이라고 하며 해당 과정은 다음과 같다[5].

① QR 코드 스캔하여 장치 설정에 필요한 정보를 얻음
② PASE: PAKE 기반 비밀번호 생성 및 보안 채널 생성
③ Commissionee(새로 등록하려는 Matter 기기)는 DAC(제품을 고유하게 식별하는 인증서, Device Attestation Certificate)를 Commissioner(등록을 수행하는 주체)에게 제출
④ DAC 검증 완료 시 NOC(Node Operational Credential, Fabric 내에서 다른 기기를 식별하 는데 사용하는 자격증명)를 Commissionee 에게 제공
⑤ Commissionee 의 Fabric 진입

해당 논문은 비밀번호 인증의 취약성을 개선하기 위해 PASE 단계까지의 과정에 DID 기반 인증 과정을 추가할 것을 제안한다.

2. Matter 의 보안성 분석

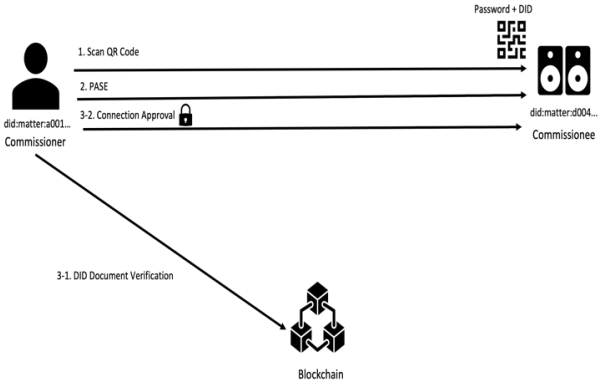
2023 년에 발표된 'Security Analysis of the Matter Protocol'[6] 논문은 Matter 환경에서 발생할 수 있는 다양한 보안 위협을 정의하고 있다. 해당 연구에서는 특히 비밀번호의 관리 문제와 유출 위험성을 강조하며, 비밀번호 유출로 인한 중간자 공격 가능성을 지적하여 비밀번호 보안의 개선이 필요하다는 것을 제시한다.

동일한 해에 발표된 'Security Analysis of Trust on the Controller in the Matter Protocol Specification'[5]에서는 Matter 컨트롤러의 IoT 장치 접근에 대한 보안 취약점을 분석한다. 해당 논문은 악의적 사용자와 애플리케이션을 포함한 Matter 컨트롤러의 무단 접근이 기기의 기능을 악용하고 제어할 수 있는 가능성을 제시하며, 플랫폼 및 애플리케이션에서 Commissioner 의 인증 강화가 필요하다고 강조하고 있다.

두 연구를 통해 Matter 환경에서는 IoT 기기와 컨트롤러 모두에 대한 확실한 인증이 중요하다는 것을 인지할 수 있다.

Ⅲ. DID 인증 기반 Matter 의 PASE 단계 개선 방안

해당 장은 논문에서 제안하는 DID 기반 Matter 의 PASE 과정을 설명한다. 해당 단계는 [그림 1]과 같이 이루어진다.



[그림 1] DID 인증 기반 Matter PASE 과정

먼저, Commissioner 는 Commissionee 의 본체에 부착되거나 별도의 위치에 프린팅된 QR 코드를 스캔하여 해당 기기의 인증 정보를 획득한다. 이 논문에서 제안하는 방식에서는 기존의 QR 코드에 포함된 패스워드뿐만 아니라 해당 기기의 DID(그림 상 did:matter:d004...) 정보도 함께 포함된다. 그 후, 기존의 Commissioning 단계와 유사하게 PASE 단계를 진행한다. 이로써 암호화된 통신이 가능해져 보안성 있는 채널이 형성된다. 이후, Commissioner 는 Commissionee 의 DID Document 를 블록체인 원장에서 조회한다. 해당 기기의 DID Document 구조는 [그림 2]와 같다.

[그림 2] Commissionee 의 DID Document 예시

DID Document 조회를 통해 기기의 정보확인이 이루어지면, 나머지 Commissioning 과정 수행 및 기기의 Matter Fabric 참여가 가능하다.

Ⅳ. 결 론

해당 논문은 Matter 의 Commissioning 과정에 DID 인증 개념을 통합하는 방법을 제안하였으며 이에 따라 기존 비밀번호 인증의 보안성을 강화하고 IoT 기기 연결의 신뢰성을 보장하는 방안을 제시하였다 이 연구가 실제로 Matter 환경에 적용될 경우, 인증 과정의 강화를 통해 악의적인 IoT 기기와 해커로부터 스마트 홈을 보호할 수 있으며, 이는 Matter 기반 스마트 홈 시스템이 구축된 가정의 보안을 크게 향상할 것으로 기대된다. 또한, 이 방법은 기존의 패스워드 기반 통신 시스템에서 발생할 수 있는 신뢰성 문제와 정보 유출 문제를 해결하는 데에도 기여할 수 있다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음(IITP-2024-2021-0-01835). 이 논문은 2023 년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2023 년 산업혁신인재성장지원사업). 이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(2021-0-00590, 대규모 노드에서 블록단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발). 이 논문은 2024 년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (KRIT-CT-23-041, LiDAR/RADAR 지원 엣지 AI 기반의 고신뢰 IR/UV FSO/OCC 특화연구실).

참 고 문 헌

[1] Lionel Sujay Vailshery, Internet of Things (IoT) - statistics & facts, Statista, October 2023.

[2] W. Zegeye, A. Jemal and K. Kornegay, "Connected Smart Home over Matter Protocol," 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2023, pp. 1-70.

[3] Badis Hammi, Sherali Zeadally, Rida Khatoun, Jamel Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures," Computers & Security, Volume 117, 2022.

[4] Wells, Jonathan. Better Practices for IoT Smart Home Security. Diss. Utica College, 2020.

[5] K. Shashwat, F. Hahn, X. Ou and A. Singhal, "Security Analysis of Trust on the Controller in the Matter Protocol Specification," 2023 IEEE Conference on Communications and NetworkSecurity(CNS), 2023.

[6] Loos Melissa, "Security Analysis of the Matter Protocol," Open Access Repositorium der Universität Ulm und TechnischenHochschule Ulm, 2023.