제로트러스트 관점에서 본 국방 DID 출입통제체계의 구조적 보안 분석

전채민 · 전병진
육군사관학교
c20759@kma.ac.kr

Structural Security Analysis of Military DID-based Access Control Systems using Zero Trust Principles

Chaemin Jeon · Byungjin Jun
Korea Military Academy

요 약

육군사관학교는 인터넷 기반 환경에서도 안전한 출입 관리를 위해 분산신원증명(DID) 기반 출입통제 시스템을 도입하였다. 국방 정보체계에서 인터넷 기반 출입통제 체계의 적용은 상대적으로 새로운 시도로, 기존 망 분리 중심 보안 모델과는 다른 위험 요소를 내포한다. 본 논문은 해당 시스템을 NIST SP 800-207에서 정의한 제로 트러스트 7대 원칙을 기준으로 분석하여, 인증 방식과 서버 간 신뢰 구조 측면에서의 구조적 보안 취약점을 분석하였다. 분석 결과, 정적 QR 기반 인증 방식과 DMZ 중계 서버에 대한 과도한 신뢰로 인해 보안 공백이 발생할 수 있음을 확인하였다. 또한 이러한 취약점을 바탕으로 위협 시나리오를 구성하고, 제로 트러스트 원칙에 부합하는 보완 방향을 정리하였다. 본 연구는 실제 DID 출입통제 시스템을 대상으로 한 사례 분석을 통해, 향후 인터넷 기반 출입통제 체계 설계에 참고 자료를 제공한다.

Ⅰ. 서 론

육군사관학교는 블록체인 기반 분산신원증명(Decentralized Identifiers, DID) 출입통제체계를 도입하였다. 해당 시스템은 모바일 단말을 활용한 인터넷 기반 구조를 채택하여, 폐쇄적 국방망을 전제로 설계된 기존 출입통제 환경과는 다른 보안 요구사항을 수반한다[1]. 이러한 구조적 변화로 인해 경계 기반 보안 모델만으로는 접근 요청의 신뢰성을 충분히 보장하기 어렵고, 인증 및 서버 간 신뢰 관계에서 보안 공백이 발생할 수 있다. 본 논문은 육군사관학교 DID 출입통제 시스템을 대상으로 NIST SP 800-207에서 정의한 제로 트러스트 원칙을 적용하여, 인증 방식과 서버 간 신뢰 구조 측면에서의 구조적 보안 취약점을 식별한다. 이를 바탕으로 위협 시나리오를 구성하고, 제로 트러스트 원칙에 부합하는 보완 방향을 정리함으로써 향후 인터넷 기반 출입통제 체계 설계에 참고 자료를 제공하고자 한다.

Ⅱ. 본 론

1. 육군사관학교 DID 출입통제체계 구조

DID 기반 출입통제 시스템은 외부망, DMZ(DeMilitarized Zone), 내부망으로 구분된 3계층 구조로 운영된다. 사용자가 모바일 단말에서 생성한 출입 인증 요청은 외부망에서 DMZ 구간의 애플리케이션 서버로 전달되며, 해당 서버는 요청을 중계하여 블록체인 서버에서 유효성 검사를 수행한다. 검증된 인증 결과는 내부망의 시스템 서버로 전달되며, 해당 서버는 출입통제 처리와 관련 데이터를 통합 관리한다. 출입 여부에 대한 최종 결정 권한은 내부망의 시스템 서버가 보유하며, DMZ 구간에서 전달된 인증 결과를 기반으로 접근 허용 여부를 판단한다. 블록체인 네트워크는 프라이빗 체인 형태로 구성되어 외부와의 통신은 단일 프록시를 통해 제한적으로 이루어진다.

QR 코드는 사용자의 모바일 단말에서 생성된 인증 세션을 식별하는 수단이며, 블록체인 네트워크는 프라이빗 체인 형태로 구성되어 외부와의 통신은 단일 프록시를 통해 제한적으로 이루어진다. 사용자의 모바일 단말에서 생성된 인증 세션을 식별하는 수단이며, 서버 측에서는 해당 세션의 유효성 여부만을 확인한다. 내부망 시스템 서버가 DMZ 구간으로부터 수신한 인증 결과에 대해 별도의 재검증 절차를 수행하지 않는다. 이로 인해 DMZ 구간의 중계 서버는 외부망과 내부망을 연결하는 핵심 신뢰 지점으로 기능한다.

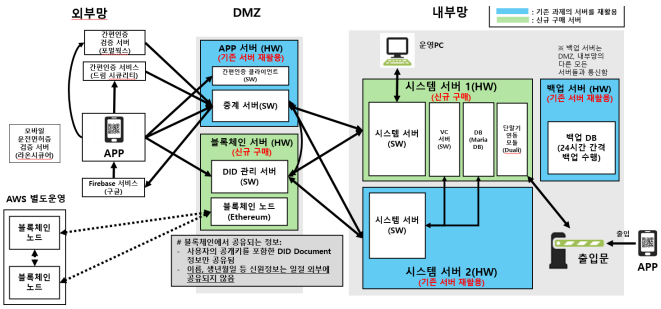

그림 1. 육군사관학교 DID 구조[1]

2. 제로 트러스트 아키텍처기반 취약점 분석 및 보완 방안

본 연구는 NIST SP 800-207에서 정의한 제로 트러스트 아키텍처(Zero Trust Architecture, ZTA)원칙을 분석 프레임워크[3]로 활용한다. 제로 트러스트는 네트워크 경계 내부의 구성 요소라 할지라도 신뢰하지 않고, 모든 통신 행위에 지속적인 검증을 요구한다. 이를 육군사관학교 DID 출입통제 시스템에 적용하여, 기존 경계 기반 보안 모델에서 간과될 수 있는 구조적 취약점과 신뢰 구간의 허점을 분석한다.

분석 대상은 외부망-DMZ-내부망으로 구성된 DID 출입통제체계 전반이며, '권한 관리', '출입증 위임 ','인가-검증 연계'의 세 가지 체계 구조로 구분하여 검토하였다. 이를 바탕으로 보안 위협 시나리오를 구성하고, 군 환경에서 DID 출입통제 시스템 운용 시 고려해야 할 현실적인 위험 요소와 이에

대응하기 위한 보완 방향을 도출한다.

2-1 권한 상태의 정적 신뢰 및 폐기 구조 문제

현 DID 출입통제 체계에서는 출입 허용 여부 판단을 위해 블록체인에 기록된 권한 상태 정보를 일정 기간 정적으로 신뢰하는 구조를 채택하고 있다. 이는 성능 및 운용 효율성을 고려한 합리적인 설계 선택이지만, Zero Trust 관점에서는 구조적 한계로 작용할 수 있다.

Zero Trust 아키텍처는 접근 요청마다 신뢰를 재설정하고 지속적으로 검증할 것을 요구하지만 현재의 일정 기간 정적 신뢰 구조에는 해당 권한이 요청 시점의 실제 환경이나 맥락에 여전히 적합한지에 대한 재평가 과정이 명확히 포함되지 않는다. 따라서 권한이 부여된 이후 사용자 환경이나 행위 조건이 변화하더라도, 동일한 권한 상태가 반복적으로 수용될 가능성이 존재한다. 현 체계의 권한 관리 방식은 성능과 보안 간의 트레이드오프에 기반한 설계 선택일 수 있으나, 출입 권한을 동적인 검증 대상이 아닌 정적인 상태 정보로 취급하는 구조는 접근 요청 단위로 신뢰를 최소화해야 한다는 Zero Trust 원칙에서 볼 때는 구조적 취약점이다.

이러한 정적 신뢰의 한계는 권한 폐기(revocation) 이벤트 처리 과정에서 더욱 명확히 나타난다. 현 체계는 블록체인 트랜잭션을 통해 권한 상태를 변경하지만, 폐기 정보가 실제 출입 판단에 반영되는 시점, 검증 주체 및 요소가 불명확하다. 즉, 권한 폐기 자체의 가능성과 폐기된 권한이 실제 출입 요청 처리 과정에 어떻게 반영되는지는 구분하여 분석할 필요가 있다. Zero Trust 환경에서는 권한 부여뿐만 아니라 폐기 상태 역시 일관되게 검증되어야 하지만, 특히 DMZ 구간과 내부망 시스템 서버 간 역할이 분리된 환경에서 권한 폐기 정보가 어느 신뢰 경계에서 최종 검증되는지가 불분명할 경우 암묵적 신뢰 구간이 형성될 수 있다.

이에 대한 보완 방식은 인가 결과를 시간, 출입 대상, 출입 구간 등 사전에 정의된 조건이 결합된 제한적 권한 상태로 관리하며 권한이 장기간 정적으로 신뢰하는 구조에서 발생할 수 있는 오용 가능성을 최소화하는 방안이 있다. 또한, 폐기 이벤트 발생 시 해당 정보가 출입증 생성 및 검증 과정에 반드시 반영되도록 Zero Trust의 '명시적 검증 지점'을 확립하는 방향으로 보완해야 한다. 이는 추가적인 실시간 검증 없이도 인가 결과의 신뢰 범위를 구조적으로 축소하는 효과를 가지며, Zero Trust 관점에서 요구되는 지속적 검증을 현실적인 제약 아래 간접적으로 반영한 보완 방안이며 권한 관리 전반의 신뢰성을 강화하는 효과를 가진다.

2-2. bearer credential 구조의 한계

본 체계에서 QR 코드는 외부 신원 인증과 다단계 인가 절차(업무 담당자 및 최종 승인자 승인)가 완료된 이후에만 생성되며, 출입증(pass)의 역할, 즉, bearer credential로 기능한다. 출입구 단계에서는 해당 QR 코드의 유효성만을 검증하며, 추가 인가 판단이나 정책 평가가 이루어지지 않아 정당하게 승인된 출입 권한을 제3자가 대리 행사하는 QR 탈취 및 리플레이 공격이 발생할 수 있는 본질적인 한계가 있다.

Zero Trust 관점에서 이는 신뢰가 사용자나 단말이 아닌 토큰에 귀속된 구조적 위험 요소로 볼 수 있다. 즉, QR 코드는 인가 단계에서 이미 완료된 출입통제의 신뢰 판단을 재사용 가능하게 전달하는 수단으로 작동하므로, QR 코드가 탈취될 경우, 제시자와 인가 대상자의 일치 여부를 기술적으로 보장하기 어렵다. 현 체계에서는 이러한 위험을 완화하기 위해 QR 코드의 짧은 유효시간 제한과 화면 캡처 차단과 같은 보호 기법을 적용하였으나, 이는 토큰 탈취 가능성을 감소시키는 보조적 대응에 해당하며 bearer credential 구조적 해결책은 아니다. 초병의 출입구 확인도 인간 기반 보조 통제(compensating control)로서 토큰 기반 위임 구조의 한계를 보완하는 현실적인 수단이나 근본적인 해결은 되지 않는다.

QR 리플레이 위험을 구조적으로 완화하기 위한 가장 확실한 보완 방안은 출입증을 사용자 단말과 암호학적으로 연동(binding)하는 방식이다. 예를 들어 QR 코드 생성 시 단말 내 개인키로 서명된 응답이나 단말 고유 식별 정보와의 결합을 요구할 경우, 토큰이 탈취되더라도 다른 단말에서의 재사용은 원천적으로 차단할 수 있다. 이러한 단말 연동 방식은 출입구 단계에서 추가 인가를 요구하지 않으면서도, bearer credential 구조가 갖는 대리 행사 위험을 실질적으로 감소시키는 Zero Trust 친화적 보완 방안으로 평가할 수 있다.

2-3. 사람 기반 인가 판단과 기술적 검증 간의 구조적 단절

현 체계에서 출입 인가는 업무 담당자와 최종 승인자에 의한 사람 기반 승인 절차를 통해 수행되며, 인가 후에만 QR 기반 출입증이 생성된다. 출입 단계에서는 출입증의 유효성 검증을 통해 출입 여부를 판단하며, 이 과정에서 새로운 인가 판단은 이루어지지 않는다. 즉, 출입 시점의 판단은 사전에 확정된 인가 결과를 소비하는 구조로 설계되어 있다.

Zero Trust 관점에서 접근 제어는 신뢰 판단의 근거가 명시적으로 전달되고 검증되는 구조를 요구한다. 그러나 본 체계에서는 인가 단계의 판단 맥락이 출입 시점의 기술적 검증으로 전달되지 않으며, 출입구의 인가 결과의 유효성만이 판단 근거로 사용된다. 이로 인해 인가 판단과 출입 판단 사이에 신뢰 해석의 단절이 발생하며, 신뢰가 특정 시점의 인가 결과에 고정되는 구조적 특성이 형성된다.

이러한 단절을 완화하기 위해 인가 시점에 정의된 판단 조건이 출입 시점의 검증에 반영되도록 신뢰 범위를 명시화할 필요가 있다. 예를 들어 인가 결과를 단순한 허용 여부가 아니라, 역할, 허용 시간, 출입 대상과 같은 조건이 결합된 제한적 권한으로 표시하여 출입 시점의 검증 기준을 구체화할 수 있다. 이는 기존 인가 구조를 유지하면서도 인가의 의미가 출입 판단 과정에서 소실되지 않도록 하는 Zero Trust 관점의 보완 방향이다.

Ⅲ. 결 론

본 논문에서는 육군사관학교 DID 시스템을 NIST SP 800-207 원칙으로 분석하여 권한 상태의 정적 신뢰와 불명확한 폐기 검증 지점, 토큰 귀속적 성격의 QR 구조, 사람 기반 인가와 기술적 검증 간 연결 구조의 세 가지 측면에서 현 출입통제체계의 한계 및 보완 방안을 제시하였다. 본 연구는 공개 가능한 정보를 기반으로 국방 DID 출입통제체계의 보안 구조를 제로트러스트 관점에서 분석했다는 점에서 의의가 있으나, 실제 운용 환경의 세부 설계와 내부 정책까지는 반영하지 못하였다. 따라서 향후 연구에서는 비공개 내부 구조와 운용 절차를 포함한 보다 심층적인 구조 분석을 통해, 실제 취약점과 한계를 구체적으로 식별하는 방향으로 연구를 확장할 예정이다.

ACKNOWLEDGMENT

이 논문은 서울시 산학연 협력사업 2024년도 서울 테스트베드 실증사업 (TE240062)의 지원을 받아 수행된 연구임.

참 고 문 헌

[1] 전병진, 신규용, 최현돈,"인터넷 기반 군 DID 출입통제시스템을 위한 망분리 보안 및 트래픽 거버넌스 아키텍쳐," 한국통신학회논문지, 제51권, 제1호 2026년 1월.

[2] 신규용, 길총경, 최현돈, 이종관,"분산 신원 증명 기반의 군 출입 통제 체계 구축에 관한 연구,"pp.167-176, 2021년

[3] S. Rose, O.Borchert, S.Mitchell, and S. Connelly,"Zero Trust Architecture,"NIST Special Publication 800-207, Aug. 2020.