SIG ONE

2026년 8월 · v1.0

기 술 백 서

비밀번호 없이 신뢰가 성립하는 원리

SIG ONE의 BSA(Blockchain Secure Authentication)가 비밀번호·OTP·토큰 같은 '저장되는 비밀' 없이 어떻게 신뢰를 성립시키는지, 4계층 신뢰사슬의 작동 원리를 설명합니다.

발행 **주식회사 시그원 (SigOne Co., Ltd.)**

대상 **www.sigone.net**

요약

BSA는 저장되는 비밀에 의존하지 않습니다. 매 인증마다 새로 만들어지고 즉시 사라지는 일회성 재료와 키, 그리고 무작위로 선정된 다수 노드의 분산 검증으로 신뢰를 성립시킵니다. 재료(MIRC) → 키(OTAK) → 검증(MDV) → 원장(Hybrid DLT)으로 이어지는 단방향 신뢰사슬은, 각 단계가 앞 단계의 산물을 소비하고 아무것도 남기지 않는 파이프라인입니다. 탈취할 자산도, 장악할 단일 지점도 존재하지 않습니다.

MIRC 재료 › **OTAK** 키 › **MDV** 검증 › **Hybrid DLT** 원장

설계 배경 · 문제

모든 인증 공격은 두 가지 구조적 전제에서 출발합니다

개별 공격 기법을 하나씩 막는 대신, 그 기법들이 성립하는 공통 전제 자체를 구조에서 제거하는 것이 BSA의 설계 목표입니다.

취약점 01

고정 크리덴셜의 존재

저장·재사용·탈취가 가능한 고정 자산(비밀번호·키)이 존재하는 한, 아래 공격은 계속 성립합니다.

성립하는 공격

피싱 · 크리덴셜 스터핑 · 패스워드 DB 탈취 · 중간자 재사용

취약점 02

단일 검증점의 존재

검증이 한 지점에 집중되면, 그 지점 하나를 장악하는 것만으로 인증 결과 전체를 조작할 수 있습니다.

성립하는 공격

검증서버 침해 · 내부자 조작 · 단일장애점(SPOF)

설계 원칙

훔칠 자산을 만들지 않는다 · 믿을 지점을 하나로 두지 않는다

원칙 01

훔칠 자산을 만들지 않는다

저장·재사용·탈취의 대상이 되는 고정 자산 자체를 남기지 않습니다. 매 요청 재료를 무작위로 조합하고(MIRC), 키를 요청마다 생성·즉시 폐기합니다(OTAK).

원칙 02

믿을 지점을 하나로 두지 않는다

검증과 기록을 분산해, 한 지점의 장악이 전체 결과를 좌우하지 못하게 합니다. 무작위 복수 노드의 합의로 판정하고(MDV), Public·Private로 분산 기록합니다(Hybrid DLT).

메커니즘

4계층 신뢰사슬

재료 → 키 → 검증 → 원장. 각 단계의 출력이 다음 단계의 입력이 되며, 어느 단계도 재사용 가능한 자산을 다음으로 넘기지 않습니다.

LAYER 01 · 재료 **MIRC**

다중 식별자를 무작위로 조합해 예측 불가능한 재료를 만든다

단일 비밀값이 아니라 소유(등록 단말)·장치·위치·지식/생체 등 서로 다른 식별자 집합에서, 매 요청마다 부분집합을 무작위로 선별·결합합니다. 동일 사용자라도 요청마다 재료가 달라져 관측·재현이 성립하지 않습니다.

남지 않는 것: **저장되는 고정 식별자 조합**

LAYER 02 · 키 **OTAK**

일회성 인증키를 요청마다 생성하고 인증 직후 폐기한다

키가 존재하는 시간을 단일 요청 구간으로 제한합니다. 300자 이상으로 생성된 키는 다단계 암호화(생성→축약→병합, 각 단계마다 암호화)를 거치고, 인증 결과 반환 후 즉시 소멸합니다. 탈취해도 사용할 시점이 남지 않습니다.

남지 않는 것: **재사용 가능한 키**

LAYER 03 · 검증 **MDV**

무작위로 선정된 복수 노드의 합의로 검증한다

검증 권한을 한 곳에 두지 않고, 무작위로 선정된 여러 노드가 동시에 병렬 검증해 사전 정의된 합의 규칙으로 판정합니다. 공격자가 검증 노드를 미리 지목할 수 없고, 노드 하나를 장악해도 결과를 좌우하지 못합니다.

남지 않는 것: **조작 가능한 단일 검증점**

LAYER 04 · 원장 **Hybrid DLT**

Public·Private 체인이 역할을 나눠 불변 기록으로 보존한다

개방 검증·익명성을 담당하는 Public 체인과, 인증 처리·불변 기록을 담당하는 Private 체인을 분리해 서로를 보완합니다. 한쪽의 노출·손상이 다른 쪽의 신뢰를 대체하지 못하며, 인증 사실은 사후 대조가 가능한 불변 기록으로 남습니다.

남지 않는 것: **위·변조 가능한 단일 원장**

보안 성립 증명

네 가지 위협에 대한 구조적 방어

BSA의 방어는 확률이 아니라 구조에서 성립합니다. 공격이 성립하려면 존재하지 않는 자산이나 지점이 필요합니다.

✔ 위조 방어

재료를 위조하려면 소유·장치·위치·지식/생체 조건과 그 요청 시점의 무작위 조합까지 동시에 맞아야 합니다. 하나를 확보해도 나머지와 그 시점의 조합이 맞지 않으면 재료는 성립하지 않습니다.

✔ 재사용 방어

키의 수명은 단일 요청 처리 구간뿐입니다. 공격자가 키를 확보하는 시점에는 이미 폐기되어 있고 다음 요청은 다른 키입니다. 재사용할 대상 자체가 존재하지 않습니다.

✔ 검증 조작 방어

검증은 무작위 선정된 복수 노드에 분산됩니다. 특정 노드를 미리 지목할 수도, 단독으로 결과를 결정할 수도 없으며, 부분 장악은 합의에서 무효화됩니다.

✔ 부인 방지

인증 결과는 Hybrid DLT의 불변·투명 기록으로 보존되어 사후에 인증 사실을 대조·입증할 수 있습니다. 생체 원본과 고정 패스워드는 애초에 저장되지 않습니다.

국제표준 · 인증

세계 최고 권위가 이미 검증한 기술

BSA는 UN 산하 국제표준으로 채택되고, 국제 보안 인증과 글로벌 어워드로 검증되었습니다. 별도 검증이 필요 없는 이유입니다.

- ✔ **ITU-T X.1284 · X.1286**
  UN 전문기구 ITU-T 국제표준 채택
- ✔ **TTAK.KO-12.0411**
  국내 표준 제정
- ✔ **Common Criteria EAL2**
  국제 공통평가기준 인증
- ✔ **Patents · 8개국**
  핵심 기술 특허 등록

기술 검토를 시작하시겠습니까?

합의 임계값·키 길이·암호 알고리즘·난수원 등 상세 기술 명세는 보안 검토 요청 시 기술명세서로 별도 제공합니다.