

자동차 해킹

실제차량에서 찾아내고 평가

차량보안 침입탐지·시험으로 모빌리티 생태계 보호



자체개발 모빌리티 사이버보안 검증 플랫폼 상용화

대표연구자

심상규

/

소속

아우토크립트(주)

연구배경

왜 통합 보안평가가 필요할까?

01

해킹 경로의 확대

차량·스마트폰·도로 인프라·클라우드가 연결되며
조향·제동과 개인정보까지 위협

02

부분적 검증의 한계

특정 통신망이나 개별 부품 점검만으로는
실제 해킹 경로와 방어 성능을 종합 검증 불가

03

일회성 인증의 한계

진화하는 해킹에 대응하려면 실시간 탐지와
상시·반복 취약점 점검이 필요

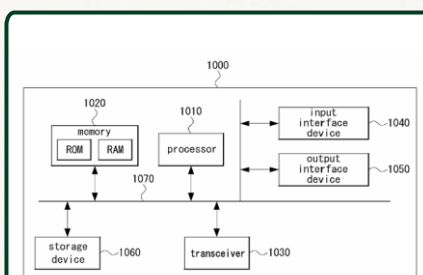
그래서 필요한것 → 객관적·정량적·반복 검증

핵심성과

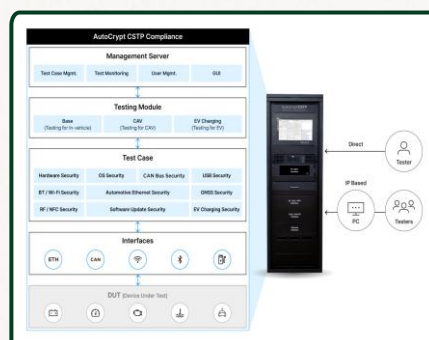
침입탐지부터 실제차량 보안평가까지 연결한 차량 통합 보안평가



안전 상태 학습



해킹 위험 즉시 탐지



차량 공격·방어 재현

IP

국제 지식재산 성과

출원·등록 상태를 구분해 제시

미국·유럽·일본 대상

4 건 추진 중

유럽특허청(EPO)

1 건 등록

모빌리티 생태계 해킹 탐지 방법·장치 EPO 등록으로 해외 사업화 기반 확대

차별점

규칙 점검을 넘어 실제 보안 성능을 평가

기존 단편적 검증



알려진 공격
규칙 중심



특정 통신망·
개별 부품



객관적 지표
초기 단계



실차 통합 보안평가



정상 상태 학습
+ 차량별 특성



실차·부품·
외부망 통합



차단 효과
정량평가

‘점검’에서 → ‘보안 성능 평가’로

파급효과

자동차 보안에서 모빌리티 생태계 보호로



글로벌 사업화

자체개발 플랫폼 상용화 및
국제 기준 기반
시험·인증 시장 진출



공급망 경쟁력

자동차·보안·사물 인터넷·
클라우드 시험인증 융합으로
수출 기반 강화

핵심기술 모빌리티 생태계 통합 보안망



국민 안전·신뢰

차량 해킹 사고 예방과
미래차 안전의
사회적 수용성 제고

사후 수습에서 실시간 감시·예방 중심 보안 전환