[별첨 5]

안전한 V2N 통신을 위한 헤드유닛 보안 접근제어 기술

권혁찬 (hckwon@etri.re.kr)
정보보호연구본부

ETRI 한국전자통신연구원
www.etri.re.kr
초연결통신연구소/정보보호연구본부

목 차

▣ 배경 및 필요성

◈ 차량 IVN(head-unit)에 대한 해킹 사례 급증

Jeep Cherokee hack (2015)
C.Miller, C.Valasek

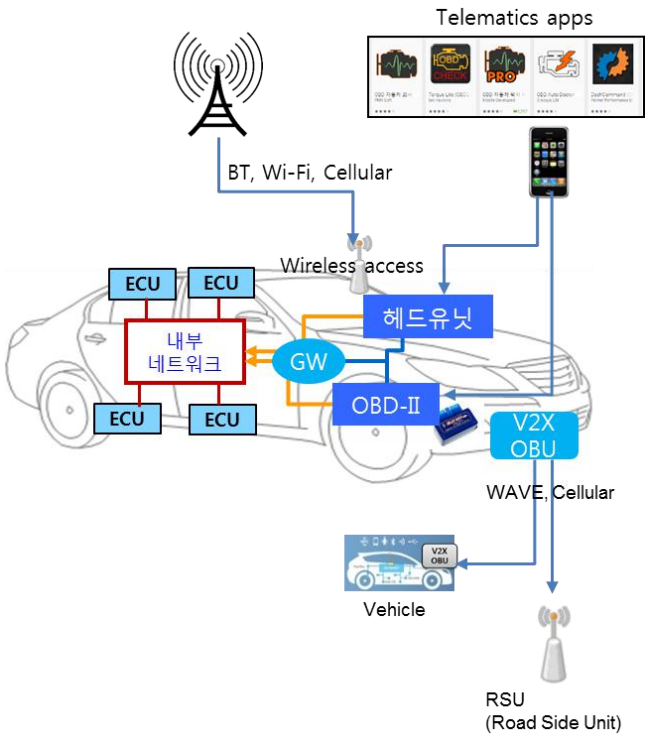
Mitsubishi outlander PHEV hack (2016)
Pen test partners

Tesla Model S hack (2016, 2017)
Keen Security Lab. (Tencent)

▣ 배경 및 필요성

◈ 위협

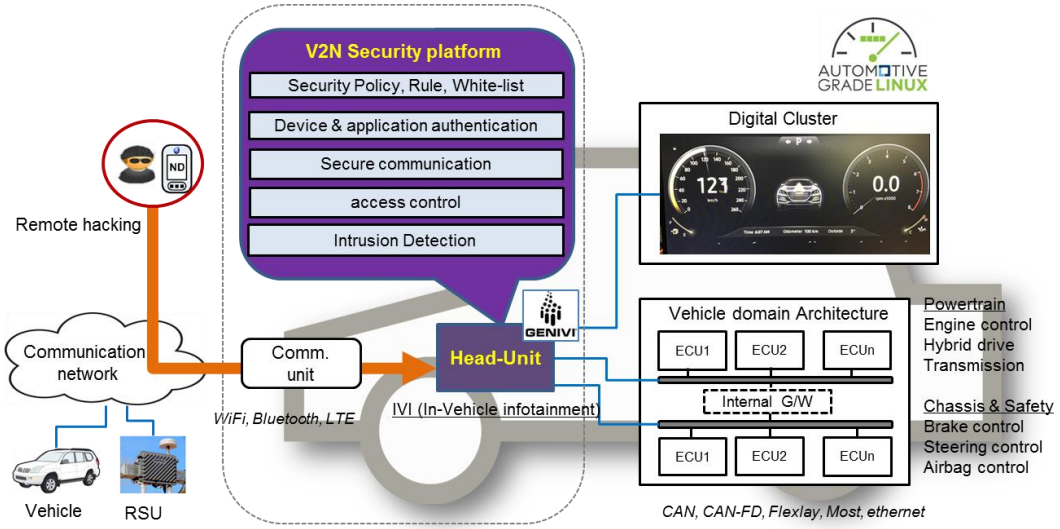
- **Types of Attack**
  - **Injection of malicious control commands**
  - **Prevention of correct system function (insertion, deletion, manipulation, replay and delay of messages)**
- **Points of attack**
  - **Additional nodes (e.g. via OBD connector or wireless access)**
  - **Corrupted and misused existing nodes (e.g. root access to infotainment system via cellular network)**
  - **Nodes replaces by manipulated ones**



출처 : Secure Ethernet communication for Autonomous Driving, Elektrobit, 2015

▣ 안전한 V2N 통신을 위한 헤드유닛 보안 접근제어 기술

- ❖ 스마트폰 등 외부접속기기를 통한 자율주행차량 사이버공격 및 원격해킹방지를 위한 헤드유닛용 접근제어 플랫폼 제공
- ❖ 주요 특징
  - ❖ V2N(vehicle to Nomadic Device) 원격 해킹 대응
  - ❖ 화이트리스트 기반 V2N 접근제어
  - ❖ GENIVI 표준 플랫폼 적용



2. 기술이전 내용 및 범위

▣ 기술이전 내용

❖ 안전한 V2N 통신을 위한 헤드유닛 보안 접근제어 기술

▣ 기술이전 범위

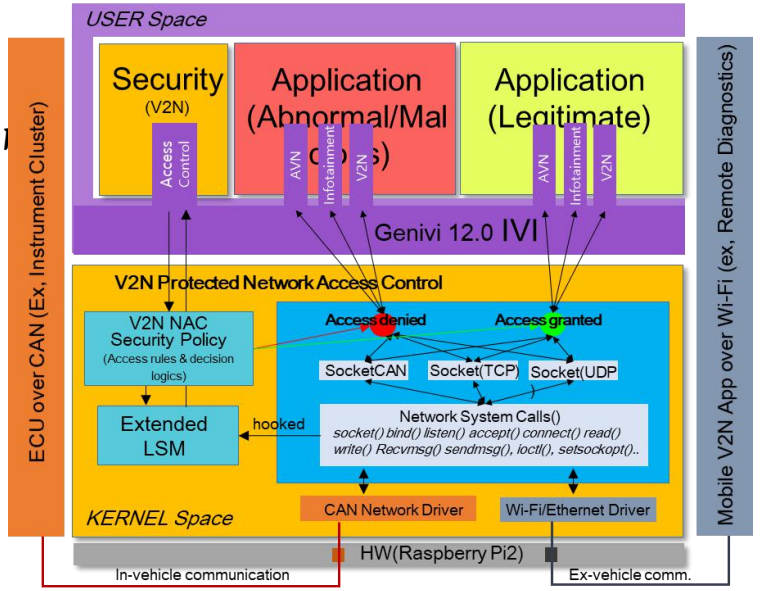
❖ 안전한 V2N 통신을 위한 헤드유닛 보안 접근제어 엔진

- SW 플랫폼
  - ✓ GENIVI (GDP 버전 12) over Yocto Linux
- LSM 확장 보안 모듈 (Extended Linux Security Module)
  - ✓ White-list 기반 접근제어 룰 관리/적용
  - ✓ Socket API 커널 레벨 후킹 기반 CAN, TCP 권한적용
    (각 API 단계별 후킹 후 권한체크, socket(), bind(), connect(), send(), recv() 등)
  - ✓ TCP/IP, SocketCAN 적용
- White-list 기반 V2N 접근제어 모듈
  - ✓ 차량 IVN 접근제어 모듈 (커널 탑재 형)
  - ✓ 접근제어 정책 관리 모듈 (접근주체, 리소스, 권한 등)
  - ✓ GENIVI AppFW(응용 프레임워크) 위한 룰 설정 API
  - ✓ 네트워크 레벨 패킷 필터링 엔진
  - ✓ GENIVI Platform 커널 수준 제어 (응용 악성감염 등 다양한 해킹 시나리오 고려)

▣ 기술 개발 현황

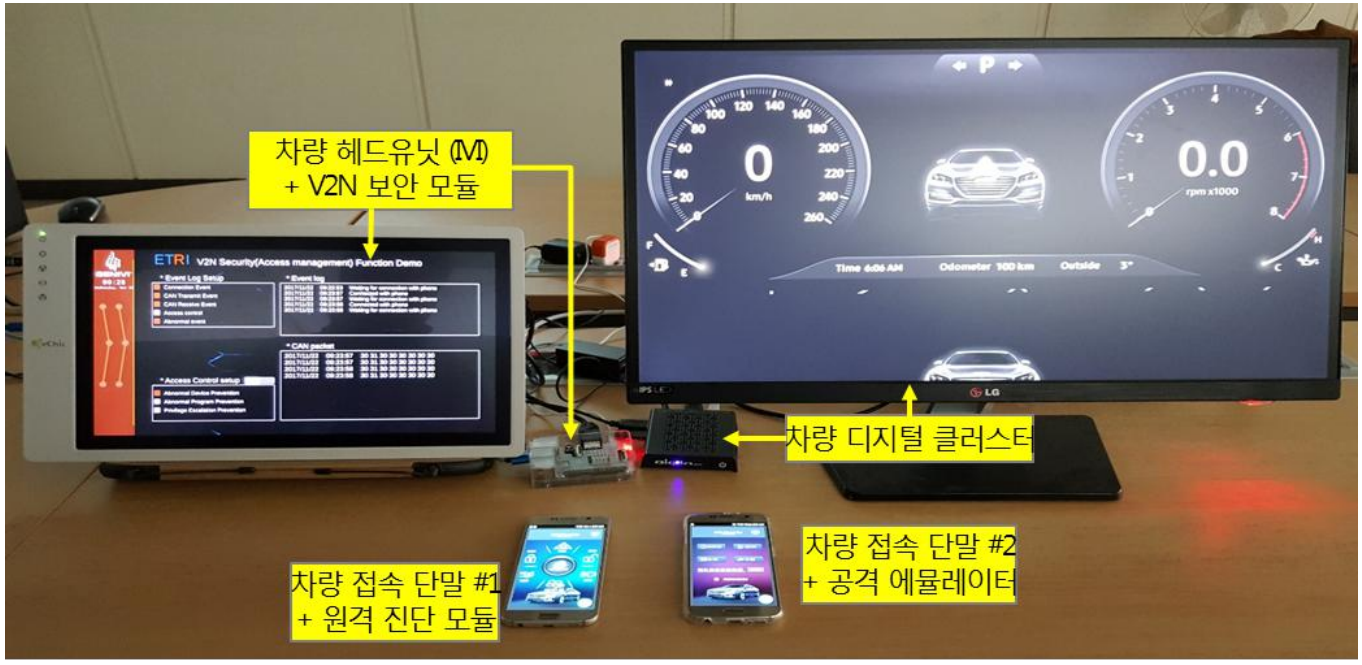
❖ 기술 개발 환경

- HW 플랫폼
  - ✓ Raspberry Pi 2 Model B
  - ✓ ARM Cortex-A7 Quad Core CPU, 1G RA
- SW 플랫폼
  - ✓ GENIVI (GDP 버전 12) over Yocto Linux
- 보안 메커니즘 속성
  - ✓ LSM 확장 보안 모듈
    - ➢ Extended Linux Security Module
  - ✓ WhiteList 기반 접근제어 툴
  - ✓ Socket API 커널 레벨 후킹
    - ➢ TCP/IP, SocketCAN 적용

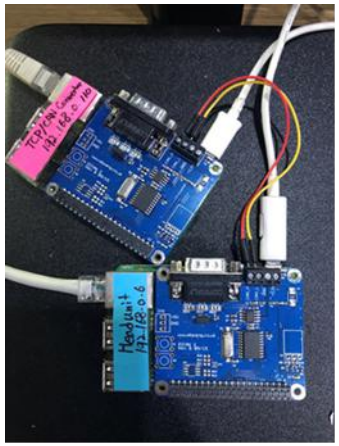


▣ 기술 개발 현황

❖ 테스트베드



V2N 보안 테스트베드



PiCAN2 - CAN 송수신모듈

▣ 기술 개발 현황

❖ 기술성숙도(TRL : Technology Readiness Level) 단계 :

구 분	단계	정 의	세 부 설 명
기초 연구 단계	1	기초 이론/실험	▫기초이론 정립 단계
	2	실용 목적의 아이디어 특허 등 개념정립	▫기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	▫실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 ▫개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	▫시험샘플을 제작하여 핵심성능에 대한 평가가 완료된 단계 ▫3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 ▫컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/시스템 시작품 제작 및 성능 평가	▫확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 ▫개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 ▫경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일롯 규모 시작품 제작 및 성능 평가	▫파일롯 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 ▫파일롯 규모 생산품에 대해 생산량, 생산용량, 불량률 등 제시 ▫파일롯 생산을 위한 대규모 투자가 동반되는 단계 ▫생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 ▫성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	▫실제 환경에서 성능 검증이 이루어지는 단계 ▫부품 및 소재개발의 경우 수요업체에서 직접 파일롯 시작품을 현장 평가(성능 및 신뢰성 평가) ▫가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	▫표준화 및 인허가 취득 단계
사업화	9	사업화	▫본격적인 양산 및 사업화 단계 ▫6-시그마 등 품질관리가 중요한 단계

▣ 기술의 특징

❖ 기술의 특징

- V2N 해킹 공격 대응
  - Malicious App. 실행
  - 차량 정보 불법 외부 네트워크 전송
  - TCP/IP 및 내부네트워크(CAN) 패킷 임의 주입
- WhiteList 기반 V2N 접근제어
  - 세밀한 접근제어 정책 관리 (접근주체/리소스/권한)
- GENIVI AppFW(응용 프레임워크) 위한 툴 설정 API 제공

▣ 경쟁기술과 비교

- 기존 기술은 원격접속기기 인증, CAN ID 및 DPI(Deep packet inspection) 기반의 IVN(In vehicle network) 침투 대응 기술 중심
- 테슬라 해킹(2016, 2017), 미쓰비시 해킹(2016) 사례에서도 볼 수 있듯이 차량 헤드유닛이 해킹되거나 악성 감염되는 경우 IVN 불법 침투 대응에 한계
- 본 보안 모듈은 헤드유닛 표준 플랫폼(GENIVI) 커널에 탑재되어 Socket API 커널 레벨 후킹 기반으로 권한을 체크하는 방식으로 헤드유닛이 해킹 및 악성감염된 경우에도 차량 내부로 불법적인 패킷 침투 공격을 효과적으로 차단

▣ 예상 제품 및 사업성

❖ 예상 응용 제품 및 서비스

예상 제품/서비스	예상 수요자(층)
자율주행차량용 헤드유닛/인포테인먼트 기기용 보안 SW	• 차량용 인포테인먼트/헤드유닛 제품 수요자 • 차량용 헤드유닛 및 보안 솔루션 개발 업체 • 자율주행자동차, 커넥티드카, 전기차 OEM 및 Tier-1

❖ 사업성

- 가격경쟁력면: 기존의 헤드유닛 플랫폼에 이식 가능한 SW 형태의 보안 기술로 전용 보드설계/제작 등 추가적인 비용 없이 구현할 수 있어 가격경쟁력이 높음
- 시장환경면: 자동차가 C-ITS, 자율주행 환경으로 진화하면서 차량의 연결성이 증가하고 있고 이에 따른 공격벡터의 증가 및 실제 해킹 사례의 증가등으로 관련 보안 솔루션에 대한 수요가 증가하고 있어 제품 출시 시 시장 및 제품 경쟁력우위를 점할 수 있음

▣기술이전 제약 조건

❖ 기술이전 업체 조건

- 자동차 헤드유닛/인포테인먼트/텔레매틱스 기기 생산업체 혹은 암호 플랫폼, 암호기기 및 서비스 솔루션 관련 업체

❖ 사업화시 제약 조건

- **구현 플랫폼 조건:** 본 기술은 오픈 소스 인포테인먼트 플랫폼인 GENIVI Development Platform 12를 요구하며, 해당 플랫폼 기술은 Yocto Linux에 기반하여 구성된 기술임. 본 기술이전에서 GENIVI 대신 다른 인포테인먼트 플랫폼(예, AGL)을 이용하거나 버전이 상이한 경우, 별도의 포팅 및 최적화 작업이 필요할 수 있음
- **극복 방안:** ETRI 담 부서에서는 기술전수를 받은 업체와 협의하여 기술 자문 및 지원을 고려할 수 있음

▣제품/서비스 시장 규모

❖ 암호고속처리를 요구하는 V2X 자동차보안 (1차적)시장 근거 추정

- Automotive cyber security Market – Global forecast to 20 21, MarketsandMarkets, CAGR 17.2%, 2016-2(

시장	2018년	2019년	2020년	2021년	2022년	합계
해외(M$)	25.35	28.70	32.48	36.77	41.63	164.93
국내(억원)	229.07	257.34	289.12	324.83	364.95	1465.30

- 국내시장은 2017년 국내 정보보호산업 실태조사보고서(KISA, 2018.04)의 시장 중에서, 암호/인증시장 (1,205억원, CAGR 14.6%)의 1%를 관련제품 시장으로 그리고 네트워크 보안시장 (6,395억원, CAGR 12.2%)의 3%를 관련 기기/시스템 시장으로 추정
- 해외시장은 Embedded Security 및 Cyber security (2차적)시장은 포함하지 않았으며 이를 포함시 시장 규모는 더 커질 수 있음 (출처: Automotive cyber security Market – Global forecast to 2021, MarketsandMarkets)

감사합니다.

www.etri.re.kr

※ 하단의 문의처 소개후, 발표후 개별기술 상담이 가능함을 다시 한 번 안내함

♣ 연락처 : 정보보호연구본부, 권혁찬 책·연/PL (042-860-5941, hckwon@etri.re.kr)