LTE-V2X 네트워크 환경에서의 제로 트러스트 아키텍처 제안

정다윗 [1], 이선영*[2]
순천향대학교

djung0605@sch.ac.kr[1], *sunlee@sch.ac.kr[2]

A Zero-Trust Architecture for LTE-V2X Network

Da Wit Jeong[1], Sun-Young Lee*[2]
Department of Mobility Convergence Security, Soonchunhyang Univ.[1]
Department of Information Security Engineering, Soonchunhyang Univ.[2]

요 약

자동차 산업은 연결 기반 자율주행 차를 목표로 연구를 진행하고 있다. 연결 기반 자율주행 차량의 완전한 자율주행 차량을 위해선 V2X 에 대한 연구가 필수적이며 국내에서도 LTE-V2X 를 기반한 자율주행을 목표로 연구를 진행하고 있다. 그러나 LTE-V2X 에는 외부와 통신하기 때문에 보안 위협이 존재하고 공격이 발생했을 때 주행 사고를 발생시킬 수 있다. 본 논문에서는 LTE-V2X 에서 보안성을 높이고 안전한 자율주행을 제공할 수 있는 제로 트러스트 아키텍처를 제안하였다.

Ⅰ. 서 론

최근 자동차 산업은 자율주행 차량(Autonomous Vhicle, AV)과 커넥티드 카(Connected Vehicle, CV)를 결합한 연결 기반 자율주행 차(Connected and Autonomous Vehicle, CAV)에 대한 연구가 진행되고 있다. 이러한 CAV 의 자율 주행 기술의 단계는 레벨 0 부터 레벨 5 까지 분류된다. 현재 상용화된 자율 주행 기술은 레벨 2~3 단계에 머무르고 있고 완전한 자율주행을 위해선 4~5 단계에 대한 연구가 필요하다. 이를 위해서는 차량 통신 기술인 V2X 에 대한 연구가 진행되어야 한다.

V2X 는 차량과 차량, 차량과 인프라, 차량과 네트워크 등 차량과 주변요소들과 통신하는 기술이다[1][2]. 국내에서도 V2X 에 대한 연구를 진행하고 있으며 C-ITS 의 단일 통신 방식을 LTE-V2X 로 지정하였다. 그러나 LTE-V2X 를 상용화하기 위한 인프라와 실증 연구 및 테스트가 충분히 진행되지 않았다. 또한, V2X 통신은 외부와 통신하기 때문에 보안 위협에 취약할 뿐만 아니라 통신 데이터에 따라 차량 주행에 영향을 끼치기 때문에 주행 사고가 발생할 수 있다[3][4].

본 논문에서는 V2X 의 네트워크 환경을 분리하고 지속적으로 무결성을 검증함으로써 CAV 의 안전한 자율주행을 보장하기 위한 LTE-V2X 네트워크 환경에서의 제로 트러스트 아키텍처를 제안한다.

Ⅱ. 관련 연구

2.1 V2X

V2X(Vehicle-to-Everything)는 차량과 외부 요소들과 통신을 수행하는 기술이며 차량과 차량(Vehicle-to-Vehicle), 차량과 인프라(Vehicle-to-Infrastructure), 차량과 네트워크(Vehicle-to-Network), 차량과 보행자(Vehicle-to-Pedestrian) 등을 총칭한다[1][2]. 있다. V2X 의 통신 구성 요소로는 크게 네 가지로 구성되어 있다. 먼저 OBU(On Board Unit)는 각 차량에 장착되어 있는 단말장치로 차량의 정보와 차량 주변 정보를 송수신한다. 또한, RSU(Road Side Unit)는 차량의 정보를 주변 차량에게 송수신하며 노면에 설치되어 있는 기지국이거나 C-V2X 의 경우 모바일 기지국이 RSU 역할을 수행한다. Roadside users 는 보행자, 오토바이, 등 차량 외 주행에 영향을 끼칠 수 있는 요소를 말한다. Central/Cloud Server 는 V2X 를 통한 통신 데이터를 기반하여 교통에 필요한 데이터를 제어한다.

2.2 제로 트러스트

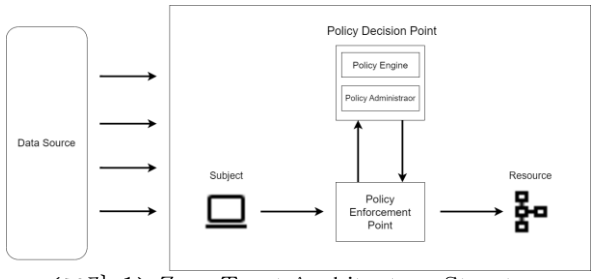
제로 트러스트(Zero-Trust)는 미국 표준 NIST SP 800-207 에 의해 정의된 보안 메커니즘으로 주체의 위치에 관계없이 네트워크와 리소스에 접근할 때마다 인증을 수행하고 최소한의 접근 권한을 제공하는 보안 모델이다[6][7]. 기존 경계 보안 모델은 방화벽을 기준으로 내부와 외부를 경계로 접근을 제어하는 방식이다. 그러나 VPN, 클라우드 서비스 등의 도입으로 네트워크 경계에 대한 불확실성으로 인한 접근 주체 및 리소스에 대한 낮은 신뢰성을 보인다. 제로 트러스트는 이러한 문제를 해결하기 위해 모든 네트워크를 분리하고 새로운 리소스에 접근할 때마다 인증을 수행하도록 하여 신뢰성을 보장하는 것을 목표로 한다.

제로 트러스트는 PE(Policy Engine), PA(Policy Administrator), PEP(Policy Enforcement Point), PDP(Policy Decision Point), Data Source 와 같은 논리적 구성요소가 요구된다.

[그림 1]은 제로 트러스트의 동작 방식을 보인다. 주체가 리소스에 대한 권한을 얻기 위해선 주체가 PEP 에 접근 요청을 한다. PEP 는 PDP 에 요청을 리다이렉션하고 PDP 는 정책과 데이터 소스의 입력을 토대로 주체에 대해 평가한다. 평가 결과를 토대로 PE 는 리소스에 대한 접근 권한을 부여하고 PA 는 접근에 필요한 자격 증명을 생성하여 PEP 에 전달한다. PEP 는 리소스에 대한 주체의 통신을 연결하고 지속적으로 통신을 모니터링하여 주체의 행위를 평가한다.

<표 1> Logical Components of Zero Trust

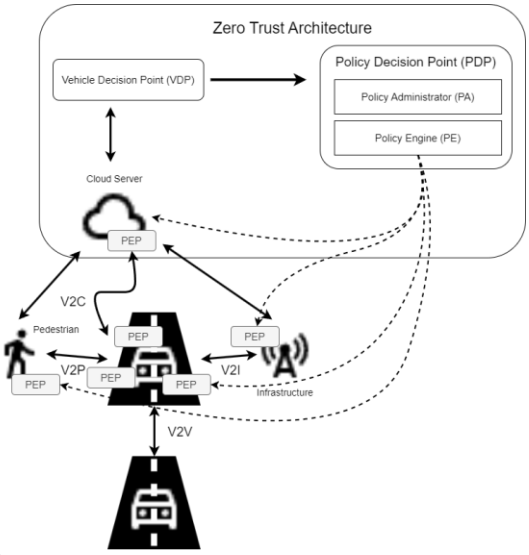
Logical Component	Role
PE	주체의 리소스 접근 권한 부여에 대한 최종 결정
PA	주체와 리소스의 통신 경로 설정, 자격 증명 생성
PDP	주체와 리소스 간 통신 연결 및 차단
PEP	PDP 에 요청 전달, 주체와 리소스 연결, 네트워크 모니터링
데이터 소스	정책으로 사용되거나 액세스를 결정하는데 필요한 요소



<그림 1> Zero Trust Architecture Structure

Ⅲ. LTE-V2X 환경에서 제로 트러스트 아키텍처 제안

LTE-V2X 는 무선 통신을 수행하기 때문에 내부와 외부 네트워크에 관계없이 공격이 발생할 수 있다. 또한, V2X 시스템은 자율주행차량의 자율주행 능력에 영향을 끼치기 때문에 사이버 공격을 통해 물리적 공격이 가능해질 수 있다. 따라서 본 논문에서는 안전한 자율주행 환경을 제공할 수 있는 LTE-V2X 네트워크 환경에서의 제로 트러스트 아키텍처를 제안한다. 제안하는 제로 트러스트 아키텍처에서는 논리적 구성요소인 PA, PE, PDP, PEP 외에 VDP(Vehicle Decision Point)를 도입했다. VDP 는 차량과 통신하는 모든 요소들에 대해 통신 데이터에 대한 필터링을 수행한다.



<그림 2> LTE-V2X Zero-Trust Architecture for LTE-V2X

<그림 2>는 제안하는 LTE-V2X 에서 제로 트러스트 아키텍처의 구조이다. 각 요소들이 통신을 수행하기 위해선 각각의 PEP 에 접근 요청을 수행한다. PEP 는 접근 요청을 클라우드 서버에 전송하고 클라우드 서버는 VDP 에 요청을 전달한다. VDP 는 요청에 대해서 사전에 정의된 정책에 따라 필터링을 수행한다. 접근 요청은 VDP 에서 필터링을 거쳐 PDP 에 전달되고 PE 와 PA 는 접근 권한과 자격 증명을 생성하여 다시 PEP 로 전달한다. PEP 는 접근 권한과 자격 증명을 토대로 특정 요소들과 접근하고자 하는 대상 간의 통신을 연결한다.

Ⅳ. 결론

LTE-V2X 가 적용된 자율주행 환경에서는 많은 보안 위협이 존재하고 공격이 가해질 경우 물리적인 피해가 발생할 수 있다. 따라서 본 논문에서는 모든 네트워크를 분리하고 모든 측면에서 보안성을 높일 수 있는 LTE-V2X 네트워크 환경에서 제로 트러스트 아키텍처를 제안하였다. V2X 는 세분화되는 네트워크가 많지만 제로 트러스트를 적용함으로써 발생할 수 있는 보안 위협을 사전에 방지할 수 보인다. 그러나 제안하는 제로 트러스트 아키텍처에 대한 실효성에 대한 연구는 부족하다. 이에 대해 자율주행 시뮬레이션을 통한 공격 시나리오 실증 연구 및 제로 트러스트 아키텍처 실효성에 대한 추가 연구가 필요하다.

ACKNOWLEDGMENT

※ 본 연구는 2021 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임.(NRF-2021R1A4A2001810)

참 고 문 헌

[1] 정소이, 이동훈, "자율주행을 위한 C-V2X 표준화 동향," 한국통신학회지(정보와통신), vol. 40, no. 6, pp. 67-72, 2023.

[2] 강영흥, "자율주행 V2X 도입을 위한 표준화 및 주파수 정책," 한국전자파학회논문지, vol. 32, no. 2, pp. 110-118, 2021.

[3] Takahito Yoshizawa, Dave Singelée, Jan Tobias Muehlberg, Stephane Delbruel, Amir Taherkordi, Danny Hughes, and Bart Preneel. “A Survey of Security and Privacy Issues in V2X Communication Systems,” ACM Comput. Surv. vol. 55, no. 9, Article 185, pp. 1-36. 2023.

[4] 오인수, 뭉흐델게레흐, 임강빈, "안전한 자율협력주행을 위한 C-V2X 에서의 보안 위협 분석," 대한전자공학회 학술대회, pp. 98-98, 2023.

[5] cott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, Zero Trust Architecture, NIST Special Publication 800-207, Aug. 2020.

[6] 제로트러스트 가이드라인 1.0, 한국인터넷진흥원, 2023.