|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **아이디어 제안서** | | | | **팀명** |  | | |
| **팀원** | **염재영** | | |
| **제일자** | **2024/06/02** | | |
| 아이디어  설명 |  | 아이디어 종류(분야) | **전장시스템 분야** | | | |
| 아이디어  개요 | 커넥티드 카의 보안 공격을 탐지하고, 이에 따라 사용자에게 알림과 함께 자율주행에서 차량 사용자에게 주행권한을 넘기거나 자율적으로 서버와의 연결 및 원격제어의 권한을 차단하는 보안 시스템 | | | |
| 현재의  문제점 | - 현재 대부분의 차량들은 외부의 서버와 연결되어 차량 탑승자에게 다양한 서비스를 제공해줄수 있는 커넥티드 카이다. 이에 따라 **커넥티드 카에 대한 보안 공격 사례도 늘어나고 있다.**  - 현재 보안 공격 사례로는 차량의 권한을 탈취하여 ECU시스템을 공격자가 제어하는 공격 사례들이 있었으며, 이외에도 탑승자의 정보를 탈취할 수 있는 스니핑 문제들등의 보안 문제들이 발생될 것으로 추정된다. | | | |
| 아이디어  예상 장단점 | 장점 | | | 단점 |
| 1)미래의 자율주행차에 반드시 필요하며 발전될 기술이라고 생각된다.  2)차량 뿐만 아니라 다양한 IOT객체들에도 적용가능하다. | | | 1)개발을 위해서는 보안에 대한 지식이 필요하다  2)공격 방지 범위에 대한 제한적 개발을 해야한다. |
| 기대효과 | 1)현재에도 4단계에 이른 자율주행 차량들에 대한 보안 시스템 강화로 소비자들에게 더 신뢰할 수 있는 자율주행 차량들을 제공할 수 있다.  2)차량 이외에도 IOT객체의 범위가 넓어짐에 따라 해당 객체들에 대한 보안 시스템에도 적용하여 안전하고 믿을 수 있는 보안 시스템을 제공할 수 있다. | | | |
|  |  | 아이디어 예상 구현 방법 | 현재 KIPRIS에 해당 아이디어와 비슷한 AI를 이용한 네트워크 패킷 보안 시스템이 등록이 되어있는 것으로 확인된다. 따라서 구현시에는 단순히 패킷 보안 시스템 자체의 모듈 하나로 완전히 구상하지 말고, 다른 모듈에 삽입할 수 있는 방안을 생각해야한다.  예를 들면, 전기차 무선 충전 모듈과 같은 다른 모듈과 함께 삽입하거나 무선 충전 모듈이 아니더라도 유선 주유할 때 점검을 동시에 할 수 있는 시스템을 구축하는 것도 나쁘지 않을 듯 하다. | | | |