

독일 AZT의 가상 자동차키 설계요건 연구

[Virtual vehicle key & AZT activities]

『AZT, 독일』

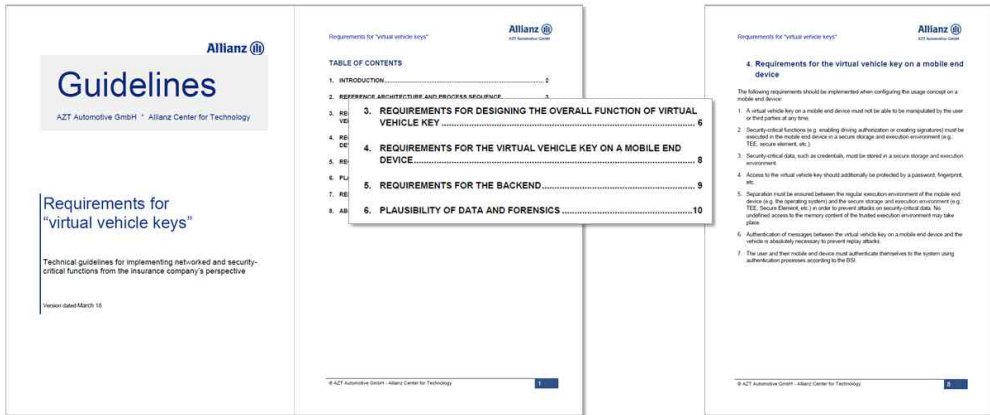
I. 개요

스마트폰을 자동차키로 사용하는 것은 차세대 혁신 기술 중 하나이다. 새로운 기능이 탄생하는 것은 새로운 취약점도 동시에 나타남을 의미한다. 현재 새롭게 개발되어 차량에 적용된 전자장치들은 소프트웨어를 통해 작동되고 있다. 이는 무선장치에 의한 업데이트를 필요로 하며, 테슬라는 세계 최초로 자동차 무선업데이트를 실시 중이다. 향후 자동차 도난방지 장치는 가상의 키나 스마트기기에 탑재되어 이동성이 더욱 강화 될 것이다. 그러나 접근 및 사용 권한 미부여자의 사용 문제와 해커들의 새로운 공격 대상이 될 수 있다는 문제의 소지가 있다.

II. 가상의 자동차키(Key) 요구사항

AZT는 최근 SIT(Fraunhofer Institute for Information Technology Security)에 ‘가상 자동차키’ 환경에 대한 일반적 특성에 관해 분석을 의뢰하였다. 해당 분석은 차량, 모바일 장비, 기반시설과 데이터 전송 경로(NFC, Bluetooth, LTE/GSM) 등에 대해 이루어졌다. AZT는 본 연구결과를 토대로 도난 위험에 대응하기 위한 ‘가상 자동차키’ 요구사항을 도출하였다. 또한 기능적으로 서로 다른 형태로 구현된 개체를 구분하였다. 첫째로 메르세데스-벤츠와 같이 차량과 가상 자동차키가 직접적으로 연결되

는 경우, 두 번째로 가상 자동차키가 주변 다른 장치(ex: 스마트폰, 스마트워치 등)로 그 기능을 확대 가능한 경우, 마지막으로 카 셰어링 시스템에서 사용하는 방식과 같이 다른 장치에 그 기능을 일부로 제한하여 확대하거나 서버에서 개개인에게 인증을 매번 해주는 방식을 포함한다.



<그림 1> AZT가 정의한 가상 자동차키에 대한 요구사항

Ⅲ. 디지털 증거 수집 및 분석 요구사항

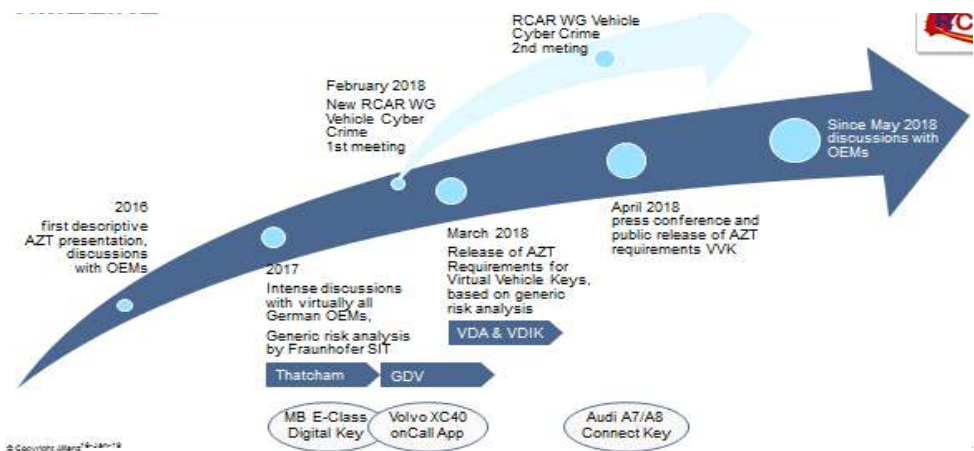
가상 자동차키의 사용 증가에 따라 이를 이용한 자동차 범죄에 대한 디지털 증거 수집 및 분석에 대한 요구사항도 함께 등장하게 되었다. 사용자 입장에서는 차량 소유주 또는 사용자가 사용하는 모든 장비에 대해 권한을 부여 받아야 한다. 또한 관련 범죄가 발생하는 즉시 모든 권한을 무효화 시킬 수 있어야 한다. 마지막으로 사용자 자신에 대한 증명(신체, 행동 패턴 등)을 할 수 있어야 한다. 차량 도난이 발생했을 때, 유효한 가상 자동차키에 대한 정보를 제공할 수 있도록 모든 사용기록이 서버에 저장되어야 하는 이유이다. 수집된 디지털 증거 데이터는 타당성 검증 및 문제해결에 결정적인 역할을 할 것이므로 다음과 같은 정보를 포함해야 한다.

<표 1> 디지털 증거 수집 및 분석 요구사항 리스트

순번	요구사항
1	사용자 등록정보
2	모든 가상 자동차키 다운로드 기록 저장
3	사용 인증된 모든 차량 기록
4	다중 사용 가상 키, 카드 키, 임시 키 등 모든 가상 자동차키 수량
5	가상 자동차 키 삭제 정보
7	가장 최근 사용된 가상 자동차키 리스트와 위치정보

IV. AZT의 가상 자동차키 관련 활동

AZT의 가상 자동차키에 대한 요구사항은 Thatcham에서 우선 공표하였으며, 독일보험자협회에서 최종적으로 공표되었다. 또한 RCAR 사이버 보안 워킹그룹에 전달하여 논의 중이다. 이후 독일자동차협회 및 독일자동차수입자협회에도 전달되었다. AZT는 본 내용을 Allianz 국제세미나에서 수석엔지니어와 기술관리자 등을 대상으로 발표하였으며, 독일 알리안츠 홍보임원인 Jochen Haugd와 보도관련 컨퍼런스를 진행하였다. 현재는 독일 내 차량 제작사와 협의 중이다.



<그림 2> AZT의 가상 자동차키 관련 활동 Timeline

V. 공표 후 추가 논의내용

독일 자동차제작사의 경우 실제 자동차키와 같이 가상 자동차키도 사용자에게 관리의 책임이 있다고 생각한다. 제작사들은 그 어떤 개인 정보를 관리하려고 하지 않고 있으며, US-Cert와 유사한 보고 프로세스를 구축하는 것도 원하지 않고 있다. 특히 모든 주체에 대해 각각의 요구 사항을 모두 구현하는 것은 사실상 불가능하다는 의견을 제시하고 있으며 차량의 ‘life cycle’ 을 새롭게 정의하는 것이 필요하다고 주장한다. Allianz 내부에서는 개인 공유 및 차량 관리를 위한 제3자의 이행조건을 명확히 해야 하며, 투명한 로그기록이 요구된다는 의견이 있었다. 또한 고객의 개인정보 취급은 아직 명확하지도 않다는 의견도 있었다.

독일 AZT는 앞으로 메르세데스 벤츠 A-클래스의 디지털 자동차키 및 카쉐어링 시스템에 대해 조사할 예정이다. A-클래스의 경우 E-클래스와 NFC 기술을 이용한다는 점에서는 동일하지만, 다른 형태를 가지고 있다. 또한 자동차 사이버 보안 RCAR 워킹그룹의 표준과 공통된 의견을 도출할 예정이다.