정 보 보 호 학 회 지
제24권 제2호, 2014. 4

자동차 융합 정보통신 장치들의 보안 기술 현황 및 발전 방향

윤 겸 주*, 박 대 혁**

요 약

사용자의 편리함과 유익함 뒤에는 높은 위험성이 공존한다. 특히 자동차의 경우에는 빠른 속도로 장소를 이동할 수 있다는 장점이 있지만, 사고 발생 시에 생명을 위협할 만큼의 위험을 가지고 있다. 자동차 사고 발생 후에는 시시비비를 가리기 위해서 많은 분쟁이 발생하는 것이 일반적인 판례였다. 자동차용 블랙박스는 자동차 사고 발생 시에 정확한 현장의 영상, 음성 및 기타 센서 정보를 기록한다. 이를 이용해서 전후좌우, 차량의 상태를 분석하여 사건 발생의 실마리를 찾을 수 있는 중요한 단서로 사용 된다. 하지만, 아직은 블랙박스 영상만으로는 법적인 자료로 사용될 수는 없다. 즉, 법적인 자료로 채택되기 위한 기밀성과 무결성 측면에서 약점을 가지고 있다. 이에 따라서 기록된 정보를 암호화하고, 접근 자에 대한 기록을 남기는 기능이 연구 및 표준화 제정되고 있다. 차량 내외에서 수집된 정보에 암호화를 적용하여 이종 기기간 데이터 공유를 차단하고, 자동차 정보기기 보안 인증서를 가지고 있는 단체를 통하여 보안키를 이용하여 정보를 활용하기 위한 시스템이 구성되고 있다. 이를 통하여 자동차 융합 정보통신 장치들로부터 기록된 정보를 법적인 객관적 근거로 활용할 수 있도록 자동차용 정보통신 기기들이 기밀성과 무결성을 준수할 수 있도록 발전할 것이다.

Ⅰ. 서 론

최근 자동차 IT 융합의 정보통신 단말기의 보급이급속도로 증가하고 있다. 특히 임베디드 기술의 발전에 의해서 복잡한 기능은 간단하고, 저렴한 가격으로 제품화 되고 있다.

자동차 융합기술로써 디지털운행기록계(DTG, Digital Tachograph)는 2013년부터 의무적으로 장착하도록 되어있다. 이미 택시, 버스와 같은 대중교통 차량은 100% 장착이 완료되어 운행 중에 있다. 또한 지능형 자동차에 대한 다양한 연구가 진행 중에 있으며, 자동차에 장착된 애프터마켓의 대표 제품이 자동차용 블랙박스이다. 2011년부터 본격적으로 시장이 급성장하여 국내 자동차를 소유자의 80%가 블랙박스를 장착하고 있으며 후방카메라, TPMS 센서 등이 인기 제품으로 부상중에 있다.

하지만 자동차의 정보통신기기 장착의 유익한 부분 이외에 개인 정보를 비롯해서 주변의 상황 및 프라이버시를 침해하는 자료가 공유되어서 많은 문제점이 발생되고 있다. 이러한 문제점을 극복하기 위해서 단말기에 보안 솔루션을 적용하고, 데이터에 접근하는 사용자를 제한하는 것에 대한 연구를 진행해본다.[1]

Ⅱ. 자동차 융합 기술 현황

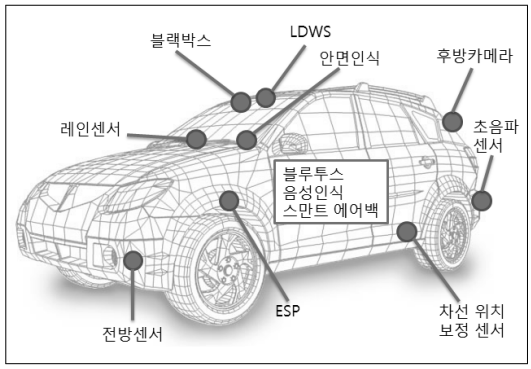
차세대 산업혁명은 단일 기술보다는 다수의 기술이 복합적으로 융합되어 시너지를 발생하는 산업에서 나타날 것으로 전망하고 있다.[2] 국가경제를 견인할 수 있는 핵심 산업을 육성하기 위한 융합 기술의 한축인 자동차IT 융합 기술은 기존 기계 중심의 자동차에서 전자기술과 IT 기술이 적용되고 있다.

자동차 분야는 3대 트렌드로 표현할 수 있다. 지능형

This work was supported by the Technology Innovation Program (or Technology Innovation Program, 10043358, Information Composition and Recognition System for surrounding images possible for top view and panorama view of resolving power less than 10cm) funded By the Ministry of Trade, industry & Energy(MI, Korea)"

* 주식회사 대덕위즈 대표(ddwiz@naver.com)
** 주식회사 세인, 전장연구소(dh.park@sane-auto.com)

자동차(SmartCar), 그린카(GreenCar), 소형경량화이며, 이러한 중요 트렌드는 자동차와 IT 기술의 융합에 의해 문제 해결이 가능하고, 새로운 융합 산업으로 발전하여 고부가가치를 창출할 수 있다. 지능형 자동차는 안정성과 편의성을 도모한다. 내비게이션을 비롯해서 블랙박스, DTG, TPMS, FCWS, LDWS와 같은 시스템들이 지능형 자동차를 대표하는 제품이다. 그린카는 급등하는 유가와 환경문제에 대한 해결책을 제시하기 위해서 대체 친환경에너지를 이용하거나, 연비를 향상시키고, 전지와 결합하여 RE-EV 운행 및 하이브리드, 전지만으로 운행하는 등의 새로운 모습의 자동차를 제안한다. 또한 소형경량화를 위해서 기계적으로 구성되어 있던 장치들이 전자부품을 이용한 ECU 제품으로 변화되고 있다.[3]



〔그림 1〕 스마트 자동차 ECU 배치

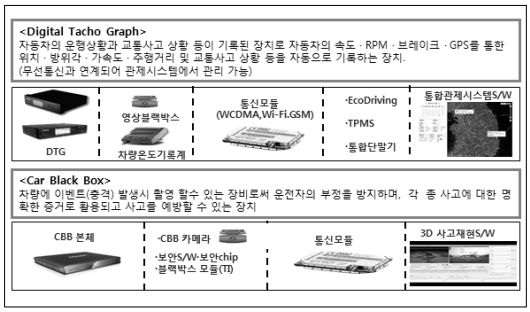
[그림1]은 지능형, 그린차 관련 ECU의 위치를 이미지로 표현한 것으로 앞으로는 더욱더 복잡한 기능 할 수 있는 임베디드 시스템이 적용될 것으로 예상된다.

Ⅲ. 자동차 융합 장치들의 보안 기술 현황

자동차 IT 융합 장치들의 현황에 대해서 살펴보고, 각 제품별 보안의 필요성과 현재 적용된 제품의 보안 기술 현황 및 문제점을 국내외 분석을 통해서 살펴보고자 한다.

3.1. 자동차 IT 융합 장치 현황

[그림2]는 차량내부에 장착되어 있는 운행기록장치(DTG, Digital Taco Graph), 블랙박스(Black Box), 사고기록장치(EDR, Event Data Recorder), 위치추적기(GPS Tracker System), 내비게이션의 예이다.



〔그림 2〕 DTG, Car Black Box 소개

2002년 유럽은 Commission Regulation (EC) 1360/2002에 DTG의 기본 기능 및 기술적인 요구사항을 규정하고, 지멘스의 제품으로 세계최초로 DTG 의무화 법안과 규정이 시작 되었다.

중국은 지역마다 예산 지원· 패널티· 의무사항 등 일부 차이가 있지만, 영업용 차량에 대한 장착 의무화를 규정하고 있다. 중국 품질시험 검사기구인 “국가질량감독검험검역총국”에서는 장치의 성능 및 표준을 관리하고 있고 법규 관리는 공안부에서 관리되고 있다. 관리하는 항목으로는 장치의 안전성과 신뢰성, 성능, 시험방법, 데이터의 안정성, 자료의 입출력, 운전자관리, 설치 등에 이르기까지 구체적으로 규범하고 있다.

일본은 『JIS 5607 자동차용 운행기록계』를 규정하고 대형 화물차의 속도 표시 및 택시의 시가표시 기능을 가진 소형DTG를 시작으로 자동차 검사 시와 사고 발생시 장치 및 자료제출이 의무화 되어 있다. 2013년부터 전국화물차를 대상으로 블랙박스와 운행기록장치의 의무화 장착을 강화하고 있으며, 50%의 국가예산이 지원되고 있다.

자동차 선진국의 DTG 규정과 법안을 참고하여 KS-R-5029, KS-R-5072를 통해서 DTG 제조 업계의 발전된 기술과 기기간의 호환성 증대를 위해 이 규격을 개정하고, “교통안전법 제 55조 운행기록관리지침” 법안을 개정하여 2013년부터 운행기록자료 미제출시 과태료를 징수하고 있다.[4]

블랙박스 제품은 항공사고 발생 시 비행 기록 정보를 기록하고, 원인 규명을 분석하는 시스템에서 자동차용

블랙박스는 사고당시의 영상, 차량의 속도, 충돌각도, 충격의 크기, 사고 발생원인 분석을 위해서 실시간 주행 자료가 그대로 저장된다. 교통사고 발생 시에 목소리 큰 사람이 이긴다는 이야기처럼 분쟁이 많은데, 블랙박스 자료에 의해서 분쟁이 최소화되고, 정확한 판단의 도움이 되는 자동차 IT 융합 제품으로 큰 파급 효과를 얻은 제품이다. 2010년 본격적으로 시판되어서 최근 승용차의 80% 이상이 블랙박스를 장착하고 있으며, 불안정적인 블랙박스 난립에 의한 소비자 피해를 예방하기 위해서 2013년 2월부터 KS 인증제도가 시행되고 있다.

블랙박스의 카메라 기본 성능을 확인하기 위한 테스트(화소, 컬러, 저장주기, 생성시간 화면표시, 카메라 렌즈, 번호판 인식 기능 등)와 데이터 유지, 전원부 성능, 전자파 성능, 가속도, 사고기록 정보 생성 시간 등에 우수한 품질을 검증하기 위한 테스트를 진행하고 있다. KS규격 차량용 블랙박스의 사고기록정보는 자동차 충돌사고 일시, 차량고유 식별번호, 가속도, 충돌 물리량(속도변화), 엔진회전수, 브레이크 상태, 안전벨트 착용, GPS정보, 카메라 영상정보 등이 기록된다.

EDR에 기록되는 정보는 자동차 사고 전에 RPM/ 엑셀 on,off 상태/ 브레이크 on,off상태/ 시속 등등이 이벤트 데이터로 기록된다.[3]

버스, 택시를 비롯하여 대형 트럭을 시작으로 의무장착되고 있으며, DTG, EDR, 후방카메라, 블랙박스, 내비게이션, 에코드라이빙장치 및 통신을 이용한 텔레매틱스 기능 등의 차량 IT 융합 제품이 결합되고, 다양한 응용 분야로 발전하고 있다.

3.2. 자동차 IT 융합 제품의 보안 기술 문제점

자동차 블랙박스의 차량 설치에 따라서 최근 교통사고 책임 소재에 대한 판단이 객관화되고, 사고 예방 효과가 매우 높다는 평가를 갖고 있다. 대중교통을 비롯해서 개인 자동차도 블랙박스 장착이 보급화 되고 있다. DTG, 블랙박스, EDR 등 고성능의 영상, 음성 내용을 기록하고 차량의 위치, 차량 내부의 정보가 통제 없이 인터넷을 통해서 배포되면서 개인의 사생활을 침해하는 문제점이 발생하고 있다. 특히, 대중교통의 경우에는 운행 중에 발생하는 문제를 기록하기 위해서 실내의 영상, 음성을 기록하는 장착하는 경우가 많이 있다. 자가용에 장착한 블랙박스는 개인의 이동 경로 및 주변의 영상이 기록되어서 의도하지 않아도 온라인상에 유포되면서 사생활 침해 문제가 발생하고 있다.

아직은 자동차 IT 융합 제품에 의해서 기록된 데이터를 법적인 증거로 활용할 수는 없지만, 자신에게 불리한 증거를 갖는 경우에 데이터를 파손하거나, 데이터를 변형하여 기록하는 경우가 발생하고 있다. 이러한 데이터의 위/변조는 기록된 데이터에 대한 접근이 매우 손쉬우며, SD 카드에 파일 형태로 기록되고, 임의의 사용자가 데이터에 접근하여 내용을 확인 및 일부 혹은 전부를 삭제, 변경할 수 있다. 2011년 6월에 제정된 “KS-R-5078(자동차용 영상 사고기록 장치)” 표준에는 블랙박스에 기록되는 데이터가 기밀성 및 무결성을 준수하도록 되어 있지만 의무 규정이 아니다.[5]

기밀성 측면에서 보면 블랙박스의 정보를 임의의 사용자가 접근 할 수 없도록 막을 수 있어야 개인의 프라이버시를 지킬 수 있지만. 블랙박스의 최고 책임자가 운전자이고, SD 카드 형태로 존재하기 때문에 기밀성을 지키기가 어렵다. 또한 정보를 기록하는 방법에 대해서도 제조 회사 별로 다르고, 블랙박스를 선택하는 운전자의 선호도에 의해서 선택 되므로 특정인 혹은 특정기관(경찰, 소방서 등)에서만 정보를 이용할 수 있게 하는 것은 해결할 수 없는 문제이다.

무결성 측면에서 보면 블랙박스의 사용 목적이 사고 발생 시에 기록된 정보를 이용함에 있지만 정보가 파손되거나 일부 데이터가 유실되는 경우가 발생한다. 이는 최고 책임자가 자신에게 분리한 영상을 삭제, 변형하는 경우가 발생하며, 이를 예방하기 위해서 SD 카드 이외에 별도의 메모리 영역에 기록되는 블랙박스 형태도 나타나고 있다.

3.3. 자동차 IT 융합 제품의 보안 기술 현황

블랙박스에 기록되는 정보에 개인의 얼굴과 신체의 일부분에 대해서 지능형 블랙박스는 영상 인식 기능을 통해서 모자이크로 처리하는 제품들이 있지만, 영상 인식 기술의 한계와 처리 시간의 한계로 인하여 기밀성을 모두 보장하기 힘들다. 또한 무결성에 대해서는 대안의 제품이 극히 일부 있다.

따라서 DTG, 블랙박스를 비롯한 자동차 IT 기록 매체들에 대해서 유럽에서는 데이터를 접근하는 것을 자체적으로 제한하고 있다. 즉 ‘잠금’ 관리를 시행하고 있

다. 잠금 기능을 해제하기 위해서는 장치와 데이터 관리에 대한 자격인증서를 부여받은 관리자만 제어를 할 수 있으며, 자격인증서 부여와 주기적인 교육 관리를 진행하고 있다. 하지만, 한국과 일본, 중국에서는 보안에 대한 내용을 시행하고 있지는 않다.[6]

베트남 등 동남아시아 국가와 이스라엘, 페루 등 최근에 도입되는 나라들에서는 '통신과 호환성(특히 자동차 블랙박스 등)'의 기능을 추가하여 도입하고 있으며, 사고기록정보의 수집 기능을 추가하고 있는 추세이다. 보안은 주로 소프트웨어를 통해 자료를 보안하는 방법으로 적용되고 있어 아직은 보안모듈 등을 별도로 적용하고 있지 않고 한국에서 자동차 블랙박스에 데이터 위변조 방지를 위한 보안 인증을 도입하고 있는 중이다.

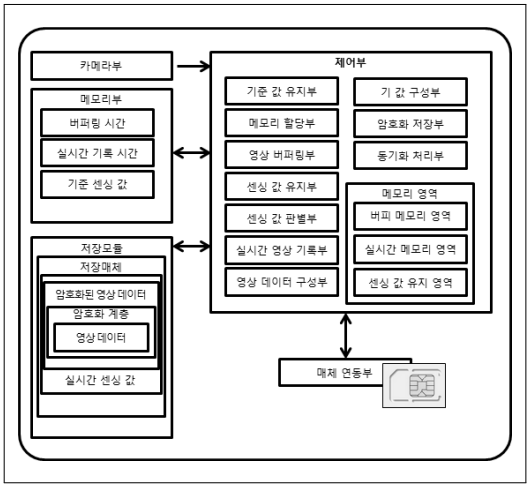
Ⅳ. 기기의 암호화 방법과 검증 인증

자동차 IT 융합 단말기의 암호화 방법에 의해서 차량 내부, 외부 기록 데이터에 대한 기밀성 및 무결성을 보장하기 위한 방법을 제안하고 이를 검증을 통해서 시스템의 적용 가능성을 확인해보자 한다.

4.1. 차량 내부/외부 기밀성, 무결성 유지를 위한 방법

블랙박스, DTG에 기록되어 있는 차량의 내부/외부의 센서 및 영상 데이터, 그리고 기타 데이터에 대해서 기밀성을 유지하기 위한 방법으로 보안 매체를 이용하여 키 값을 이용하고 암호화키를 이용해서 데이터를 암호화되고, 기록하는 방법이 있다.[7]

[그림3]은 카메라부로 획득한 영상, 실시간으로 기록되는 차량 내부/외부 데이터, 보안 매체의 데이터가 제어부로 전달되고, 전달된 정보인 실시간 기록되는 영상과 충격량 등의 센싱 값이 암호화되어 비휘발성 메모리 저장모듈로 전달되어 기록된다. 영상과 데이터의 실시간성을 유지하기 위해서 버퍼링 처리부와 동기화 처리부가 필요하며, FIFO(First Input First Output) 방법을 이용하여 데이터가 유지된다. 실시간 메모리 영역에 기록되는 영상 데이터와 결합하여 암호화 대상 데이터들이 암호화 키 생성부에서 보안매체로부터 생성되는 키를 이용하여 데이터가 암호화된다. 그리고 저장부에 기록된다.



〔그림 3〕 차량 내부/외부 기밀성 유지를 위한 방법

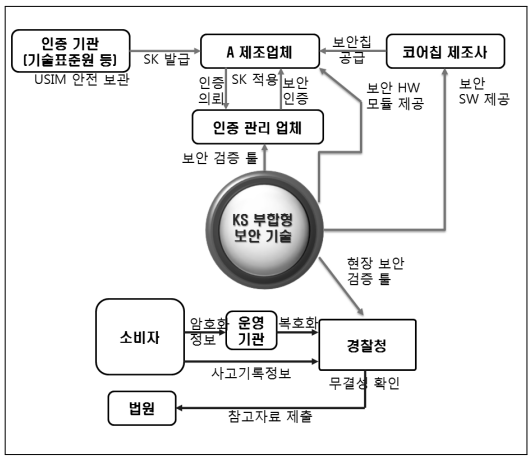
암호화키를 보유하고 있는 사용자는 보안 매체로 부터 추출 생성되는 암호화키를 이용하여 데이터를 복호화 하기 위한키를 받아 실시간 기록된 데이터를 복원 재생하기 때문에 차량 내부/외부의 데이터의 기밀성을 유지할 수 있다.

4.2. 보안 검증 툴을 이용한 인증 활용 방법

최근 자동차의 실내외 정보를 기록하는 장비에 대해서 기술기준을 제정하고 표준이 등록되고 있다. 보안기술 필요성은 인지하지만, 제조업체들이 참고하여 제작하기 위한 실질적인 참고가 필요한 보안 기술은 수록되지 않고 있다. 따라서 데이터의 기밀성과 무결성을 유지하기 위한 보안기술이 표준화되는 것이 시급하며, 기업들이 중복투자를 줄이고, 표준에 적합한 보안이 적용된 기술의 제품을 소비자가 사용하기 위해서는 보안 검증 툴이 제공되어야 한다.

[그림4]는 경찰청과 같이 자동차의 사고 발생 시에 실내외 정보를 확인하여 정확한 사건을 예측하기 위한 증거의 수거, 분석, 제출을 담당하는 경찰들이 모든 제품의 데이터를 확인 할 수 있는 보안 검증 툴의 예이다. 이렇게 무결성을 보존함으로써 기록 데이터의 법적인 증거 능력이 향상 및 보급 확대 될 수 있다. 국내의 블랙박스 솔루션은 코어칩 2개의 회사가 시장의 90%을 차지하고 있으므로 보안 기능 인증에 활용하여 코어칩 단계에서부터 데이터의 기밀성과 무결성을 보존하기 위

한 보안기능 인증을 활용 할 수 있다.



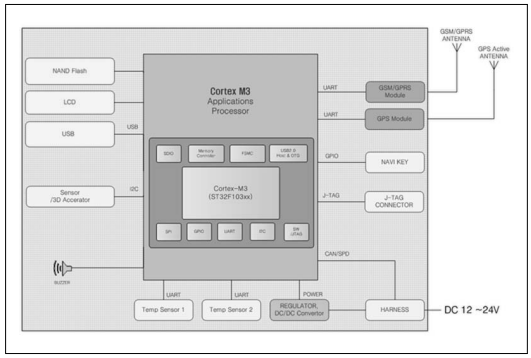
〔그림 4〕 보안 검증 툴을 이용한 인증 활용 방법

국내는 차세대 표준 암호기술을 민간으로부터 공모 중이며 정부는 자체 안전성 분석 기술을 바탕으로 선정에 관여하여 블록암호, 스트림암호, 공개키 암호, 메시지인증, 해쉬 암호, 전자서명, 사용자인증 7개 분야에 대한 표준 암호기술 공모사업 추진하였다. 미국은 표준 알고리즘인 DES를 이용하고, 유럽은 차세대 표준 암호기술 개발 사업(NESSIE)을 통해 다양한 알고리즘을 발굴하고 있으며, 일본의 경우 CRYPTREC 이라는 이름의 프로젝트로 알고리즘을 발굴하고 있다.

국내는 2000년 초부터 128비트 키 길이를 지원하는 128비트 SEED 암호 알고리즘과 128/192/256 비트의 키 지원하는 128비트 ARIA 암호 알고리즘을 개발하여 민간·정부의 전자성거래, 금융, 무선통신 등 활용 중에 있으며, 최근에는 초경량 구현 환경에 적합한 블록암호 HIGHT(High security and light weigHT) 64비트 블록 암호 알고리즘이 있으며(2005년), 2006년 TTA 표준으로 제정되었으며, 2009년 ISO/IEC 국제 블록 암호 알고리즘으로 표준화를 추진 중에 있다.

4.3. 자동차 IT 기기의 보안 적용 시스템

자동차 IT 기기가 기록하는 데이터에 보안을 적용하기 위해서는 다음의 [그림5]와 같은 블록 도를 갖는다.



〔그림 5〕 자동차 IT 기기의 보안 적용 시스템

[그림5]에서 볼수 있듯이 시스템은 자동차 내부 센서를 수집하고, 영상을 기록 할 수 있는 부분으로 구성된다. 또한 데이터를 암호화하기 위해서 키를 이용하여 암호화 할 수 있도록 ASIC이 적용되고 MCU의 암호화를 처리하는데 부하를 최소화하여 동작 할 수 있도록 시스템이 구성되어 있다.

자동차의 ECU는 동작 테스트, 온도 특성과 같은 신뢰성 테스트가 강하게 진행되어서 PPAP 테스트를 완료한 제품에 대해서 안정성을 인정하고 양산을 하는 시스템을 적용하고 있다. ACE-Q100 적용 반도체만을 이용하기를 요청하는 곳도 있다.

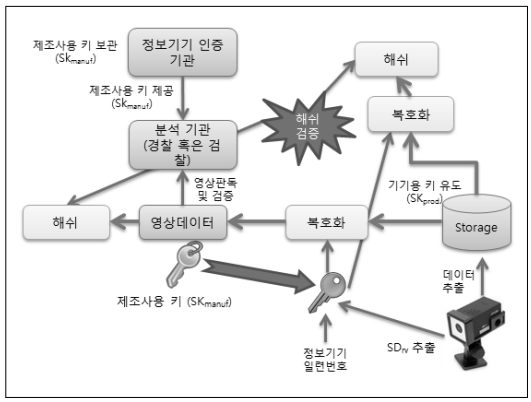
러시아의 경우 2011년부터 블랙박스 제품이 상용화되어서 매년 400%이상으로 성장하고 있다. 수요에 민감하고 빠르게 반응하며 중국산의 품질이 낮은 제품보다는 안정성이 확보되고, 자신의 선호도에 맞는 제품을 구매하는 경향이 있다. 반면에 유럽과 미국의 경우는 차량용 블랙박스의 단점인 개인정보 유출과 보호로 인하여 적극적으로 차량에 블랙박스를 장착하지는 않는다.[8] 택시와 특수 차량 및 완성차를 시작으로 블랙박스가 장착되고 있다.

4.4. 자동차 IT 기기의 보안 적용 방법

보안을 적용하기 위해서는 데이터를 생성하는 단말기에서 암호화 알고리즘이 적용되어 데이터가 생성되고, 생성된 데이터는 권한이 부여되지 않는 한 일반 바이너리 데이터를 열어보는 것에 불가하다.

[그림6]처럼 기밀성 검증을 위한 키 관리 방법이 적용되어야 권한이 부여된 단말 혹은 사용자에 의해서만 데이터가 사용될 수 있다. 이렇게 저장된 데이터를 복호

화하기 위한 안전한 키 관리 방안 구현을 위해서 분석 기간이 제조사용 키(SKmanuf)와 블랙박스 일련번호 및 블랙박스의 SDrv 값을 이용하여 기기용 복호화 키를 유도하여 복호화 할 때 사용될 수 있도록 한다.

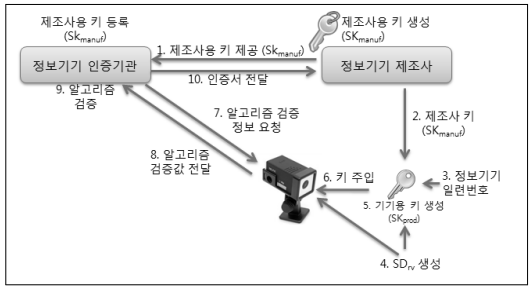


〔그림 6〕 기밀성과 무결성 현장검증 처리 방법

보안 모듈을 처리하기 위해서는 단일 마이크로프로세서를 이용해서 기본 동작에 해당하는 작업과 암호화에 해당하는 작업을 모두 처리하는 것은 시스템 안정화 측면에서 역효과를 발생하고, 시스템의 기밀성을 더욱 강화하기 위해서 ASIC 칩을 내장하는 방법을 적용한다.

데이터의 기밀성과 무결성을 보장하기 위해서는 표준화된 ASIC 칩 개발 및 채택이 필요하며, 업체 간의 표준화를 위해서 소프트웨어 개발과 키 배포 및 관리를 위한 방안, 그리고 업계 국제, 국내 표준화 진행과 디바이스들의 암호화를 적용하기 위한 방안이 채택되어야 한다. 디바이스는 무결성 데이터를 생성하고 사고기록 정보 삭제에 대비한 무결성 데이터를 생성, 기밀성을 실시간 암호화 저장하고, 데이터의 접근자 및 접근 보호기술을 적용하고, 삭제하는 행위에 대해서 탐지 및 로그 기록으로 저장 데이터의 무결성을 안정하게 지킬 수 있도록 해야 한다.

[그림7]에서 볼 수 있듯이 정보기기의 제조사는 인증기관으로부터 키를 제공하고 해당키와 제조 제품의 일련번호를 결합하여 SDrv를 생성한다. 기기에 해당하는 키(SKprod)가 생성되면 키를 제품에 주입하여 동작 할 수 있도록 한다. 정보기기는 주입된 키를 이용하여 암호화하여 데이터를 기록하게 된다.



〔그림 7〕 키 배포 및 주입 및 인증 방안

정보기기의 알고리즘 검증 단계를 통해서 제품의 기밀성과 무결성에 대한 적용 알고리즘에 대한 검증을 할 수 있다. 인증기관으로부터 알고리즘 검증 정보 요청을 받고 알고리즘 검증 값을 전달하면, 알고리즘 검증을 완료하고 인증서를 제조사에 제공하는 방법으로 정보기기의 보안 적용 유무 및 품질을 확인 할 수 있다. 정부는 제조사들에게 의무적으로 “자동차 정보기기 보안 인증서” 보유하도록 의무화함으로써 보안 기술 적용을 현실화 할 수 있다.

Ⅴ. 결 론

자동차의 편의성과 안정성을 확보하기 위해서 다양한 정보통신기기들이 자동차에 설치되고 있으며, 특히 사고 발생 시에 매우 유익한 DTG, 블랙박스, EDR등 자동차의 실시간 실내외 정보를 기록하는 장치의 수요는 계속해서 급성장 할 것이다. 많은 장점에도 불구하고 운전자 혹은 주변의 개인정보가 인터넷으로 마구 유포되는 경우가 많이 발생하고 있다.

무차별적인 유출을 예방하기 위해서 보안 솔루션을 적용하는 방법에 대해서 제안, 적용 해보았으며, 앞으로 ASIC 칩을 이용하여 실시간 기록, 복원을 할 수 있는 측면과 “자동차 정보기기 보안 인증서” 보유 시스템을 적용하여 정보의 기밀성과 무결성을 지킬 수 있는 방법에 대해서 살펴보았다.

현재 제안하는 해시 알고리즘을 적용한 단일키를 이용하여 적용된 방법의 해킹 가능성을 대비하여 셋트에 정적인 키가 아닌, 상황에 따라서 변경되는 동적키 방법을 적용을 검토 및 연구를 진행하고 있다. 또한 관제 시스템 전달된 정보의 보안에 대해서도 사용자 레벨과 권한에 한정적으로 정보가 접근 가능하도록 하는 연구를 진행하고 있다.

참 고 문 헌

[1] 김길동, 김낭자, “정보보호의 발전에 관한 연구”, 한국태평양학회논문지 (C), 3(2), pp. 115-126, 1997

[2] “The next big thing! 대한민국 산업, 기술 비전 2020”, 융합신산업,

[3] 구제길, 국중진, 박대혁, 박지훈, 최수한, 한철민, 김원희, “임베디드의 모든 것 대한민국 임베디드 산업 백서”, 위키북스, 2014.3

[4] “자동차관리법” 일부개정법률안, 2012.

[5] KS R 5078:2013, “자동차용 영상 사고기록장치”, 기술표준원, 2013. 2. 15

[6] 한종욱, 이병길, 손명희, 최병철, 김무섭, 나중찬, 조현숙, “지능형 차량·교통 보안 기술 동향”, 한국전자통신연구원, 2013

[7] 이상우, 이병길, “차량 통신 보안 기술 동향”, 주간기술동향, vol. 1556, 2012. 7

[8] “글로벌 정보보호 산업 동향 조사”, 인터넷진흥원, 2013년 제4호 유럽 중동

〈저 자 소 개〉

윤 겸 주 (Yun, KeumJu)
정회원

1992년 2월 : 대덕대학교 정보통신과 졸업
1994년 2월 : 한밭대학교 전자공학과 수료
1994년 2월 : 엣필닷컴(주) 설립 대표이사 역임
1996년 3월~현재 : 대덕위즈(주) 대표이사
관심분야 : 자동차 융합, 디지털운행기록계, 전자공학, 통신공학, 정보보호, 네트워크

박 대 혁 (Park, DaeHyuck)
비회원

2007년 2월 : 숭실대학교 미디어공학 박사 졸업
2009년 10월 : SK이노에이스, IMS 서비스 상용화
2010년 05월 : KIST, 가상머신 상용화 연구
현재 : (주)세인, 자동차 IT 분야 연구
관심분야 : 임베디드, 멀티미디어, 자동차 IT 융합, 하드웨어, 소프트웨어, 정보보호, 네트워크, 유비쿼터스