ETRI

2012
Electronics and
Telecommunications
Trends

차량용 블랙박스 보안 이슈 동향

Security Issues and Trends in Automotive Black-box

김무섭 (M.S. Kim) 영상감시연구팀 선임연구원
최수길 (S.G. Choi) 영상감시연구팀 선임연구원
정치윤 (C.Y. Jeong) 영상감시연구팀 선임연구원
한종욱 (J.W. Han) 영상감시연구팀 팀장

최근 교통사고가 발생하는 경우, 사고 발생의 책임 소재에 대한 판단을 용이하게 하고, 사고예방의 효과가 높은 이유로 택시, 버스와 같은 대중교통 시설과 개인 차량에 교통사고 상황을 영상으로 기록할 수 있는 차량용 영상기록 블랙박스(VEDR: Video Event Data Recorder)의 장착이 증가하고 있다. 그러나 이러한 블랙박스의 설치 및 활용에 대한 법적 규정이 미비하여 개인의 사생활 침해 가능성과 범죄에의 악용 우려가 높다. 본고에서는 차량용 블랙박스의 사용과 함께 발생할 수 있는 보안적인 문제점들을 살펴보았다. 특히 차량용 블랙박스에서 발생할 수 있는 보안적인 문제들 중에서 현재 사회적으로 가장 이슈가 되고 있는 블랙박스에 저장된 데이터의 위 · 변조 문제와 개인의 프라이버시 보호 문제를 중심으로 살펴보았다. 또한 이러한 보안 문제와 관련한 국내 · 외의 법률 동향을 살펴보았으며, 향후 제정될 이러한 법률들을 지원하기 위하여 보완하여야 할 문제와 추가로 고려되어야 하는 문제 등을 함께 살펴보았다.

Ⅰ. 서론

일반적으로 Event Data Recorder(EDR)로 알려져 있는 블랙박스 장치는 비행기에 장착되어 항공기의 추락이나 대형 참사 등으로 동체가 거의 소멸되었을 때, 사고의 원인 규명에 결정적인 역할을 하는 장치로 사용되어 왔다. 이러한 블랙박스의 개념을 차량에 의한 교통사고 해결에 적용한 것이 차량용 블랙박스 장치이다.

최근까지 교통사고의 원인 분석은 (그림 1)과 같이 사고 현장에 남겨진 타이어의 skid mark와 사고 차량의 최종 정지 위치와 방향 또는 사고 차량의 충돌 부위 및 파손 정도, 목격자의 진술을 토대로 사고 재구성 프로그램들을 활용하여 왔다.

그러나 이러한 방법은 사고 당시의 도로 상황과 차량의 상태에 따라 정확한 원인의 규명이 어려우며, 목격자가 바라보는 시각이나 이해관계에 따라 가해자와 피해자가 바뀌는 등 신뢰성 있는 분석에는 한계가 있었다.

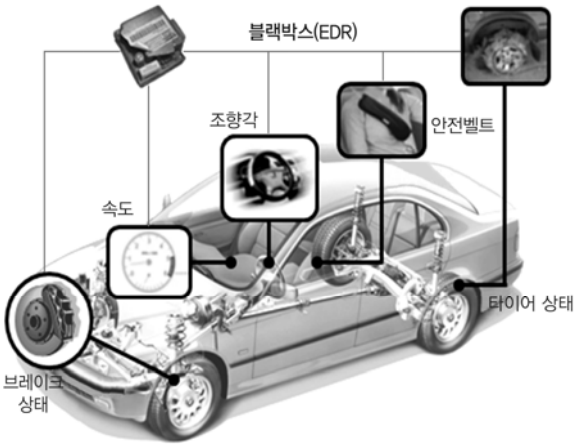
차량용 블랙박스는 차량 충돌 사고 시점의 전 · 후 일정 시간 동안의 상황을 기록하여 피해자와 가해자의 주장이 서로 상반되어 문제를 일으키거나, 쌍방 간의 과실 및 사고의 원인 규명이 어려웠던 교통사고를 정확히 파악할 수 있게 해준다는 장점으로 최근 각광을 받고 있다.

무엇보다 사고 순간이 왜곡될 수 있는 운전자의 증언이 아닌 사고 시점의 차량 운행 정보와 사고 지점의 운행 정보(교통 신호 정보 및 차선 이탈)를 포함하는 데이터가 영상 기록으로 저장되기 때문에 사고의 과실 여부를 판단하는 증거로 활용될 수 있다. 또한, 운전자가 원하는 시점에 수동으로 녹화할 수도 있으므로 위급 상황이나 범죄 수사 등과 같은 용도에도 적용할 수 있다.

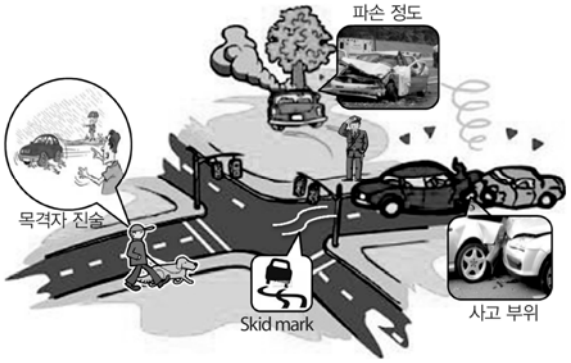
차량용 블랙박스에 대해서는 제작사와 서비스 사용자에 따라 다양한 형태의 정의가 존재한다. 현재 보편적으로 사용되는 차량용 블랙박스는 다음과 같이 크게 2가지로 분류할 수 있다.

첫번째는 (그림 2)에 나타낸 것과 같이, 기존의 운행기록계(tachograph) 기능에 차량의 주행 상태 등을 추가적으로 기록하여 차량의 정보를 보관하는 장치로써, 일반적으로 블랙박스 장치(EDR)로 알려져 있다.

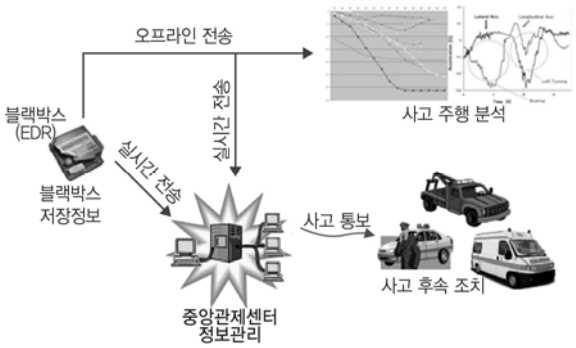
차량용 블랙박스 장치에 저장된 데이터는 (그림 3)에



(그림 2) 차량용 블랙박스 장치(EDR)



(그림 1) 기존의 교통사고 분석



(그림 3) 차량용 블랙박스의 정보 활용[1]

서와 같이 실시간 전송을 통한 신속한 사고 처리에 활용될 수 있으며, 실시간 전송 또는 블랙박스의 회수를 통한 사고의 원인 규명과 사고 상황의 분석에 활용될 수 있다.

또 다른 형태의 블랙박스는 차량 내부 또는 외부 상황의 영상 및 음성 데이터를 저장하는 기능을 수행하며, 현재 국내에 판매되고 있는 대다수의 차량용 블랙박스가 이러한 형태를 가지고 있다.

현재 판매되고 있는 차량용 블랙박스는 제품에 따라 제공하는 기능에 약간의 차이는 있지만, 기본적으로 차량에 미리 설정해 둔 기준치에 해당하는 충격을 받으면 블랙박스에 부착된 카메라와 마이크를 통해 사고 당시의 상황을 기록 및 저장하는 기능을 수행한다[2].

블랙박스 장치의 의미는 신뢰할 수 있는 제3자에 의해 내부의 데이터가 접근되고 분석된다는 점으로 볼 때, 현재 시중에서 판매되는 대다수의 장치는 블랙박스로 포괄적으로 정의하기에는 적합하지 않다. 보다 엄밀하게 정의한다면, 기존의 차량용 블랙박스와 달리 차량의 주행 정보와 관련한 영상 데이터의 기록에 우선적인 기능을 수행하므로, 차량용 영상기록 블랙박스(Video Event Data Recorder: VEDR)로 정의하는 것이 타당하다.

차량용 영상기록 블랙박스는 (그림 4)에 나타낸 것과 같이, 블랙박스를 룸미러에 장착하여 자체 카메라(보통 100만 화소 이상으로써 제품마다 차이가 있음)를 통해 전송되는 영상을 저장한다. 보통 차량이 진행하는 전면의 데이터를 저장하는 경우가 대부분이나, 최근에는 차량의 내부를 포함하여 후면 또는 측면 데이터까지 저장할 수 있는 제품도 있다. 일부 제품의 경우 위성 위치정보 시스템(GPS)을 내장해 차량의 이동 경로를 기록하기 때문에 보다 자세한 사고 상황을 분석할 수 있다.

영상 데이터는 블랙박스 자체에 내장된 메모리 또는 외장 메모리를 사용하여 저장하는데, 차량의 운행 시작 시점부터 자동으로 저장하기 때문에 사고 내용이 누락되는 경우는 없다. 또한 일부 블랙박스의 경우, 물체의

(그림 4) 차량용 영상기록 블랙박스 장치(Video EDR)

움직임을 감지하는 위치 센서(G 센서)를 내장하여 일정 수준 이상의 움직임이 감지되는 경우 교통사고로 판단하여 별도의 메모리 영역에 데이터를 저장한다.

저장하는 데이터는 보통 충격 시점의 15초 전부터 충격 후 15초 정도의 데이터를 저장하며, 평상시에 측정되는 데이터는 normal folder에, 충격이 감지되면 event folder에 저장한다. 차량 운행 정보의 저장에는 SD 메모리가 주로 사용되나, 최근에는 내장 메모리 또는 USB를 이용해서 외장 메모리에도 저장할 수 있는 제품이 판매되고 있다. 메모리에 저장되는 영상 데이터는 SD급 화질의 제품이 주종을 이루었으나 2009년부터는 고화질 HD급 영상을 제공하는 제품들로 변화하고 있다.

II. 차량용 블랙박스의 보안 이슈

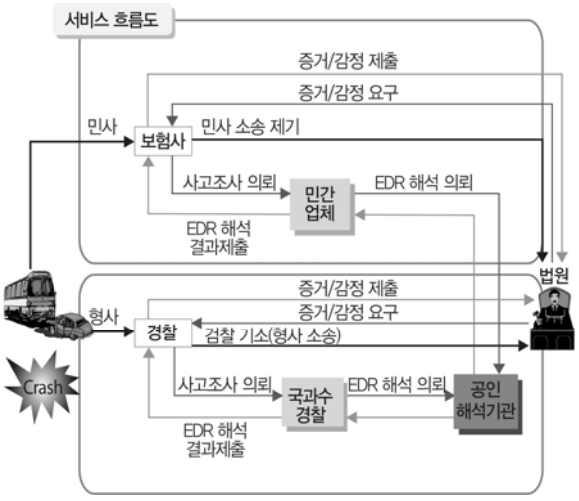
최근 교통사고 책임 소재에 대한 판단을 용이하게 하고, 사고예방의 효과가 높은 이유로 택시, 버스와 같은 대중교통 시설과 개인 차량에 교통사고 상황을 영상으로 기록할 수 있는 차량용 블랙박스의 장착이 증가하고 있다.

그러나 이러한 블랙박스의 설치 및 활용에 대한 법적 규정이 미비하여 개인의 사생활 침해 가능성과 범죄에의 악용 우려가 높은 실정이다. 이러한 문제들과 관련하여 가장 두드러진 보안 문제는 프라이버시 침해 문제와 블랙박스에 저장된 데이터의 위 · 변조 문제이다.

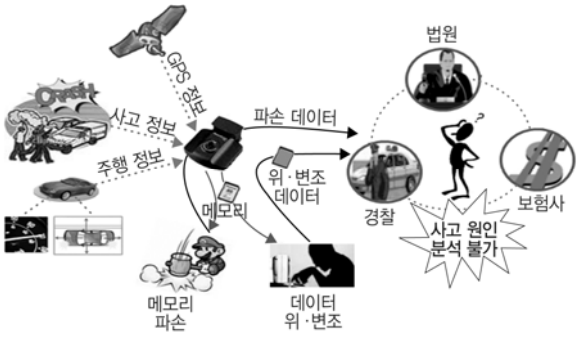
1. 블랙박스 데이터의 위 · 변조 가능성

차량용 블랙박스에서 발생할 수 있는 가장 직접적인 문제는 블랙박스에 저장된 데이터의 위 · 변조 문제이다. 차량용 블랙박스 데이터의 경우, 사고 원인의 규명 및 사고 상황을 판단하는 데 참고 자료로 사용될 뿐 아직까지 법적인 구속력은 없다. 그러나 앞으로는 (그림 5)에서와 같이 사고 데이터를 법적인 증거로서 활용하기 위한 움직임이 최근 벌어지고 있다.

차량용 블랙박스는 특성상 블랙박스에 접근할 수 있는 대상이 차량 소유자나 운전자와 같이 제한적이므로 블랙박스에 저장된 데이터에 대한 공격자는 차량의 주인이나 운전자일 가능성이 크다. 따라서 블랙박스 데이터에 대한 공격자는 차량에 부착된 블랙박스 데이터에 대해 완벽한 접근 권한을 갖고 있을 확률이 높으며, 공격을 수행하는데 필요한 시간적인 제약도 없는 상황이다[3]. 따라서 일반적인 차량용 블랙박스 데이터는 (그림 6)에서와 같이 공격자의 이해관계 또는 필요에 따라 위 · 변조 가능성에 항상 노출되어 있다.



(그림 5) 차량용 블랙박스의 법적 증거로의 활용[1]



(그림 6) 차량용 블랙박스 데이터의 위 · 변조 문제

일반적으로 차량용 블랙박스 데이터는 자체 메모리를 장착한 경우와 별도의 SSD(Solid-State Drive) 메모리를 사용하는 경우가 있다. 차량용 블랙박스에 저장된 데이터는 필요에 따라 사용자가 불리한 경우 메모리 자체를 파손해서 데이터의 사용 자체를 방해할 수도 있다. 또한 메모리에 저장된 일부 데이터에 대하여 사용자의 이익에 따라 부분적인 삭제, 위조 또는 변경에 대한 위험이 존재한다. 따라서 블랙박스 데이터에 대하여 원본 데이터의 진위 여부를 판단할 수 있는 무결성과 데이터의 위 · 변조 방지 방법 또는 위 · 변조의 판별을 확인할 수 있는 기술적 방안이 필요하다.

이러한 보안 요구 사항들을 반영하여 2011년 6월에 제정된 "KS-R-5078: 차량용 영상 사고기록 장치" 표준에는 블랙박스에 저장되는 사고기록 데이터의 무결성 및 기밀성이 제공되어야 함을 명시하였다[4].

"KS-R-5078: 차량용 영상 사고기록 장치" 표준에 따르면 차량용 블랙박스가 제공하는 보안 기능에 따라 일반형과 보안형 블랙박스로 구분하고 있다. 일반형 블랙박스는 저장된 교통사고 관련 정보에 대한 사고기록 정보에 대하여 무결성을 갖추고 기밀성은 제공하지 않는 제품으로 규정되어 있으며, 보안형 블랙박스는 저장된 사고기록 정보에 대하여 무결성과 기밀성을 모두 갖춘 제품으로 규정되어 있다. KS-R-5078 표준에서는

무결성과 기밀성에 대하여 다음과 같이 정의하고 있다.

- 사고기록 정보 무결성: 영상 사고기록 장치에 저장된 사고기록 정보가 오손 또는 훼손 없이 그대로 유지되는 특성
- 사고기록 정보 기밀성: 영상 사고기록 장치에 저장된 사고기록 정보를 출력하여 분석 또는 표출하고자 할 때, 정보의 접근이 인가된 특정인 또는 특정기관에서만 유의미한 정보로 취득할 수 있는 특성

따라서 2011년 6월에 제정된 "KS-R-5078: 차량용 영상 사고기록 장치" 표준에 따르면 모든 블랙박스는 기본적으로 저장된 영상 데이터에 대하여 영상이 위·변조 되었는지를 판단할 수 있는 기능이 제공되어야 함을 알 수 있다. 그러나, KS-R-5078 표준에는 블랙박스 데이터의 무결성 및 기밀성 확보를 위해 사용하는 암호화 및 복호화 규격은 제조사의 재량에 따르도록 하고 있다.

일반적인 보안 시스템에서 법적 효력을 제공하기 위한 신뢰성을 확보하기 위해서는 암·복호에 사용하는 보안 알고리즘의 종류와 사용하는 키의 길이 및 키의 관리에 대한 규정이 필요하다. 따라서 앞으로 블랙박스에 대한 KS-R-5078 표준에도 일반적인 보안 시스템에 준하는 보안 규약을 반영하여 보완하는 추가적인 작업이 필요할 것으로 판단된다.

2. 프라이버시 문제

블랙박스 데이터의 위·변조 문제와 더불어 추가로 고려하여야 하는 문제가 개인의 프라이버시 침해 문제이다. 차량용 블랙박스와 관련한 프라이버시 문제는 다양한 형태로 나타날 수 있다[5].

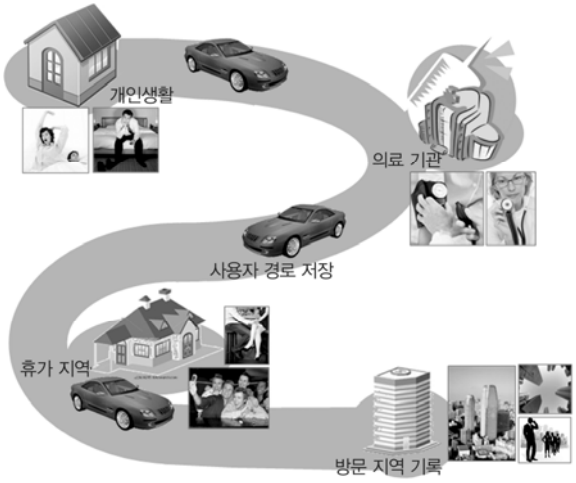
먼저, 사고의 위험을 낮추고 불필요한 시비를 줄일 수 있다는 장점으로 최근 택시 등의 상용차량에 장착된 블랙박스의 경우, 사생활 침해 소지에 대한 논란의 중심

(그림 7) 상용 차량 블랙박스의 프라이버시 문제

에 있다. 택시에 장착하는 블랙박스의 경우, 사고 발생 시 정확한 사고 규명을 위해 차량의 전방 영상에 차량 내부의 영상과 음성까지 기록하는 2채널 블랙박스를 장착하고 있다. 그러나 택시 내부의 영상 및 음성 촬영은 (그림 7)에서 볼 수 있듯이 밀폐된 공간에서 이용자들의 전화 통화부터 사적인 대화 및 무의식 중에 행동하는 개인 습관까지 기록할 수 있다. 따라서 블랙박스에 저장된 데이터가 인터넷에 유출되거나 협박 도구로 사용될 수 있는 부작용이 발생할 수 있다.

상용 차량을 이용하는 승객 입장에서는 사용자의 의사와 상관없이 일방적으로 녹화되는 블랙박스에 대한 거부감과 개인 사생활 침해에 대한 문제점을 일부 사회단체가 제기하면서 업체와 이용자 간에 대립적인 입장이 발생하고 있다. 이러한 문제에 대하여 국토해양부에서는 승객의 사생활 침해소지가 있어 실내 영상 촬영을 하지 못하도록 권고하고 있으나, 버스 및 택시 등 상용차량 업체에서는 운행 중 발생하는 분쟁의 시시비비를 가리기 위해 실내 촬영을 강력히 요구하고 있는 상황이다.

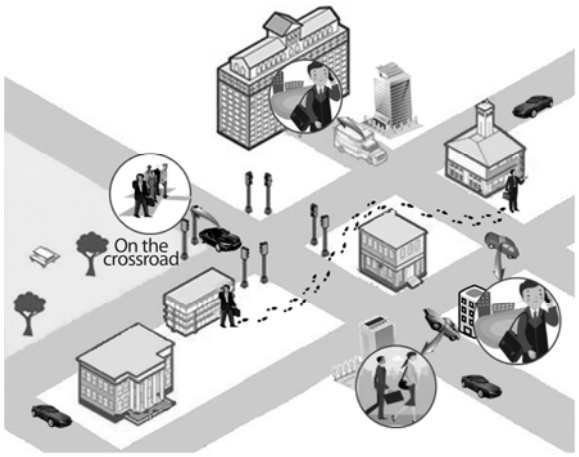
상용 차량에 사용되는 블랙박스와 관련한 프라이버시 문제와 별도로 개인 차량에 사용되는 블랙박스도 프라이버시 문제가 발생할 수 있다. 개인 차량 운전자의 경우, (그림 8)에서 볼 수 있듯이 차량의 운행 시작과 함께 저장되는 정보가 운전자의 운행 정보와 관련되는 부가적인 정보들을 고스란히 저장하게 된다. 이렇게 저장된 부가적인 정보들은 운전자의 이동 경로와 관련한 개인



(그림 8) 개인 차량용 블랙박스의 프라이버시 문제

적인 정보들을 유추할 수 있는 도구로 사용될 수 있다. 개인 차량에 저장된 데이터는 차량에 접근할 수 있는 사람이 차량 소유주 또는 차량 소유주의 가족과 같이 제한적이므로 개인 정보에 대한 문제는 상대적으로 적을 수 있다. 그러나 블랙박스에 저장된 정보가 의도하지 않은 경로로 외부로 유출되는 경우에는 운전자의 사생활에 대한 침해를 가져올 수 있다.

프라이버시와 관련한 또 다른 문제는, 차량용 블랙박스의 사용이 증가하면서 (그림 9)에서와 같이 사용자가 원하지 않는 상황에서 아무런 동의 없이 타인의 영상 데이터가 무분별하게 촬영되어 저장된다는 점이다. 이렇게 무분별하게 수집된 데이터가 온라인상에 유포되는 경우, 개인정보 유출에 따른 사생활 침해 문제가 발생할 수 있으므로 적절한 대응 방안이 필요하다.



(그림 9) 차량용 블랙박스와 타인의 프라이버시 문제

블랙박스 관련 프라이버시 보호에 관하여 가장 선도적인 움직임을 보이고 있는 미국에서 2003년에 캘리포니아에서 California Assembly Bill 2133 (AB213)으로 먼저 제안되었으며, 아칸소(Arkansas Senate Bill 51), 네바다(Nevada Assembly Bill 315), 텍사스(Texas House Bill 160), 노스다코타(North Dakota Senate Bill 2200) 등 10개 주가 잇따라 차량용 블랙박스와 관련한 사생활 보호법률을 제정하였으며, 일리노이 등 20개 주는 이와 유사한 법률 제정을 추진 중에 있다.

이들 법안들의 주요 내용은 블랙박스에 담긴 정보는 법원이 명령할 때만 공개할 수 있으며, 운전자와 차량 번호 등 신상정보는 공개 대상에서 제외하는 등 미국 전역에서 프라이버시를 보호하면서도 차량용 블랙박스를 보급할 수 있는 법률적 조치들을 제안하고 있다.

국내에서도 '개인정보보호법'과 '택시 내 CCTV(Closed Circuit Television) 설치 관련 개인정보보호 가이드라인' 등의 제도적 조치들이 진행되고 있으나, 개인 프라이버시 보호를 위해 필요한 기술적인 내용에 대해서는 아직 명시되지 않고 있다.

따라서 이러한 국내 · 외적인 동향을 살펴볼 때, 향후 블랙박스는 이러한 시장의 상충된 요구사항들을 효율적으로 해결하기 위한 정책과 이러한 정책들을 지원할 수 있는 기술적 방안이 추가적으로 마련 및 보완되어야 할 것으로 예측된다.

지금까지 살펴본 차량용 블랙박스의 정책 동향을 기반으로 향후 블랙박스에 대한 기술 발전 방향을 살펴보면 (그림 10)과 같이 예측할 수 있다.

초기 블랙박스 제품부터 현재 상용으로 판매되는 대부분의 블랙박스 제품들은 영상기록 블랙박스로 볼 수 있으며, 2011년에 제정된 "KS-R-5078: 차량용 영상사고기록 장치" 표준과 "개인정보보호법"의 요구사항

(그림 10) 차량용 블랙박스의 기술 로드맵

과 규격을 만족하기 위해 보안 기능을 탑재한 보안 블랙박스는 빠르면 2012년부터 상용 제품이 출시될 것으로 예상된다.

향후에는 현재 국제적으로 진행되는 법률 문제와 시장에서 발생하는 프라이버시 보호 문제를 해결하기 위해서는 법률과 제도의 보완과 함께, 블랙박스에 저장되는 영상 데이터에 보안 기술과 지능형 영상인식 기술을 접목하여 실시간으로 사용자의 얼굴이나 신체의 일정 영역에 대하여 마스킹 기능을 적용하는 등의 프라이버시 보호 기술을 제공하는 지능형 블랙박스 제품들이 시장을 주도할 것으로 예측된다.

Ⅲ. 결론

본고에서는 차량용 블랙박스 장치에서 발생할 수 있는 보안 문제들을 분석하였다. 차량용 블랙박스 장치에서 가장 시급하게 다루어야 할 보안 문제는 크게 개인의 프라이버시 침해 문제와 블랙박스에 저장된 데이터의 위·변조 문제로 구분할 수 있다. 블랙박스 데이터의 위·변조 문제는 국내에서도 최근 관련 표준이 제정되었으나 추가적인 보완이 필요하며, 프라이버시 문제에 대해서는 미국 등의 선진국에서만 관련 법안이 제안되고 있는 상황이다. 따라서 각 문제들에 대하여 제도적인 보완과 제정이 필요하며, 이러한 제도들을 효율적으로 지원할 수 있는 기술의 개발이 시급하다.

용어해설

차량용 블랙박스(Automotive EDR) 비행기에 장착된 블랙박스와 유사한 기능을 수행하는 장치로서, 교통사고가 발생하는 순간 차량의 운행 속도, 가속기와 브레이크의 작동 상태 및 운전자의 목소리 등과 같은 주행 정보와 사고 상황에 관련된 영상 정보 등을 차량에 설치된 카메라와 메모리에 기록하는 장치

운행기록계(tachograph) 차량의 시계, 속도계 및 주행거리계의 정보를 자동적으로 기록하여, 각 순간에 있어서 차량의 속도, 시각 사이의 주행거리 등을 이용하여 속도위반이나 운전자의 노동 상태 등을 점검할 수 있는 장치

약어 정리

CCTV	Closed Circuit Television
EDR	Event Data Recorder
GPS	Global Positioning System
SSD	Solid-State Drive
USB	Universal Serial Bus
VEDR	Video Event Data Recorder

참고문헌

[1] 한인환, “차량용 블랙박스 표준화 동향과 전략,” 표준화 우수논문수상논문집, 한국표준협회, 2005.

[2] 데이코산업연구소, 차량용 블랙박스 시장/기술 동향 및 전망, 2010.

[3] M. Wolf, A. Weimerskirch, and T.Wollinger, “State of the Art: Embedding Security in Vehicles,” *EURASIP J. Embedded Syst.*, vol. 2007, Article ID 74706, June 2007.

[4] KS-R-5078, 차량용 영상 사고기록 장치, 기술표준원, 2011. 6. 30. http://www.standard.go.kr/ (2012. 8. 7. 확인)

[5] T.M. Kowalick, *Fatal Exit: The Automotive Black Box Debate*, IEEE Press, 2005.