무결성을 보장하는 차량용 블랙박스 동영상 전송 및 관리 시스템

현종환 [1,O], 정재윤 [1], 리건 [2], 홍원기 [2]

[1] 포항공과대학교 컴퓨터공학과

[2] 포항공과대학교 정보전자융합공학부

{noraki, dejavu94, gunine, jwkhong}@postech.ac.kr

요 약

차량용 블랙박스는 차량 전·후방의 영상을 촬영하여 저장하는 장치이다. 차량 사고가 발생한 경우 사고 발생 시점 전후의 영상을 제공함으로써 사고 원인 규명 및 책임 소재를 가리는 데 중요한 역할을 담당하고 있다. 하지만 영상이 저장된 이후 위, 변조 혹은 고의 누락될 수 있는 가능성 때문에, 블랙박스를 통해 촬영된 영상은 법적 효력을 갖지 못한 채 참고자료로만 사용될 수 있는 문제가 있다. 본 논문에서는 통신 모듈이 탑재된 차량용 블랙박스에서 촬영된 영상을 직접 서버로 전송하여 보관하는 서비스를 소개한다. 또한 영상 전송 과정에서 발생할 수 있는 보안 위협을 확인하고 이를 해결하기 위한 단말 등록 및 인증 과정을 제안한다. 이를 통해 블랙박스와 서버 사이에 사용자 혹은 공격자의 개입을 미연에 방지하여 사고 영상에 대한 보안을 강화할 수 있다.

1. 서론

차량용 블랙박스는 차량 사고 발생 시 블랙박스에 촬영된 영상을 통해 사고의 원인을 쉽고 간편하게 규명할 수 있다는 장점으로 인해 최근 수 년간 급속도로 보급되었다. 또한 보험료 할인, 차량 법규 위반 신고의 근거 자료로 활용되는 등 블랙박스의 효용성은 날로 증대되고 있다. 하지만 아직 해결해야 할 문제점들도 존재한다. 영상의 무결성이 보장되지 못하기 때문에 블랙박스 영상이 법적 효력을 가질 수 없고[1], 전원 공급 차단 및 메모리 탈거 후 파일 조작이나 삭제 등의 방법으로 영상을 고의 누락할 수 있다. 본 논문에서는 네트워크를 사용한 차량용 블랙박스 동영상 관리 시스템 및 영상의 위, 변조 가능성을 차단하여 무결성이 보장되는 전송 기법을 제안하고자 한다.

2. 관련 연구

일반적으로 차량용 블랙박스는 Event Data Recorder (EDR)를 의미하며, 차량에 장착되어 차량 속도와 엔진 RPM, 브레이크 사용 기록 등 각종 차량 운행 데이터를 주기적으로 기록하여 차량의 운행 정보를 보관하는 장치이다. 차량용 영상 사고기록장치(VEDR: Video Event Data Recorder)[2]는 기기에 부착된 카메라를 통해 차량의 전후 좌우 영상을 촬영하는 장치이며, [3]과 같이 GPS 가 내장된 스마트폰을 활용하여 차량용 블랙박스의 기능을 구현한 것을 소프트웨어 블랙박스라 한다. 본 논문에서는 차량용 영상 사고기록장치 및 소프트웨어 블랙박스를 차량용 블랙박스로 칭한다.

차량용 블랙박스 데이터의 무결성을 보장하기 위해 스마트카드를 사용한 실시간 무결성 데이터 생성 방법[1], 기기마다 고유한 IPv6 주소를 할당하여 데이터의 무결성을 보장하는 방법[4], 인증서를 사용하여 블랙박스에서 생성된 데이터에 전자서명을 함으로써 데이터의 무결성을 보장하는 방법[5] 등이 제안되었다.

3. 블랙박스 동영상 전송 및 관리 시스템

3.1. 서비스 개요

그림 1은 제안하는 시스템을 활용하는 서비스 개요를 나타낸 것이다. 서비스 가입자의 차량 내부에 장착된 블랙박스는 주행 중 차량 주변의 영상을 촬영한다. 촬영된 영상은 기기 인증 후 Wi-Fi 나 3G, LTE 등의 네트워크 인프라를 통해 서버로 전송된다. 서버에 저장된 영상은 사용자가 접속하여 언제 어디서나 확인할 수 있으며, 사고 영상의 경우에는 경찰서나 보험사 등에 법적 효력을 가진 증거물로써 제공될 수 있는 것을 목표로 한다.

그림 1 서비스 개요

본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업 (NIPA-2013-H0301-13-3002)과 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU)으로부터 지원받아 수행되었습니다 (R31- 10100).

3.2. 보안 요구사항

블랙박스 동영상 관리 플랫폼이 가지는 특성 중 하나는 블랙박스 소유자가 공격자가 될 수 있다는 점이다. 블랙박스 소유자에 불리한 내용이 영상에 담기는 경우가 발생할 수 있으며, 이 경우 소유자가 영상의 위, 변조를 시도할 수 있다. 이러한 특성을 감안하여, 제안하는 플랫폼에서 필요로 하는 요구사항은 무결성, 부인 방지, 접근 제어로 정리할 수 있다.

3.3. 단말 등록 및 서명키 관리

서명키는 블랙박스 영상의 무결성을 보장하는 데 있어 가장 중요한 요소이다. 블랙박스 소유자도 공격자가 될 수 있기 때문에 인증 과정에 참여해서는 안되며, 서명키에 접근할 수 없어야 한다. 또한 서명키를 재발급해야 할 상황이 발생할 수 있다.

서명키를 발급받는 절차는 다음과 같다. 우선, 블랙박스 기기에서 서명키 발급 요청과 함께 기기 고유번호 및 사용자 ID 를 전송한다. 서버에서는 서명키와 서명 검증용 키 쌍을 인증기관에서 발급받아 기기 고유번호와 함께 서버에 저장하며, 서명키는 SSL 통신을 사용하여 블랙박스 기기로 전송된다. 전송된 서명키는 블랙박스 소유자가 접근할 수 없도록 암호화된 후 키 관리 모듈에 저장된다.

3.4. 기기 인증 및 영상 전송

영상 전송을 위해 기기에서 서버에 연결할 때 항상 기기 인증 과정을 수행하여야 하며, 인증 후 수립된 세션에서 전송된 영상에 한해서 무결성을 보장할 수 있다.

기기 인증 과정에서는 기기에 저장된 개인 키를 검증하는 절차를 통해 기기 인증을 수행한다. 자세한 기기 인증 과정은 그림 2와 같다. 먼저, 기기에서 서버에 접속 후 기기의 고유번호와 함께 영상 전송 허가 요청 메시지를 보낸다. 서버에서는 난수(N_1)를 생성하여 기기로 전송한다. 기기에서는 전송받은 난수와 기기 고유번호 및 연결된 서버 IP 를 개인 키($Priv_k$)로 RSA 알고리즘을 사용하여 암호화한 후 다시 서버로 전송한다. 서버에서는 해당 개인키와 짝을 이루는 공개 키(Pub_k)를 갖고 있기 때문에 기기에서 보내온 암호화된 메시지를 해독할 수 있다. 해독된 결과가 처음 전송한 난수 및 기기 고유번호와 일치할 경우 등록된 기기임을 인증할 수 있다. 또한 기기에서 연결된 서버의 IP 를 함께 암호화하여 전송하기 때문에 MITM (Man In The Middle) 공격을 방지할 수 있다. 그리고 세션을 맺을 때마다 난수를 암호화하여 전송하기 때문에 Replay Attack 과 같은 네트워크로부터의 공격과 이를 통한 영상의 조작 가능성을 차단할 수 있다.

영상에 대한 전자 서명을 생성한 후 해당 세션을 통해 영상과 함께 전송한다. 이러한 과정을 거침으로써 전송된 영상에 대해 무결성을 보장할 수 있고 부인 방지도 가능하다.

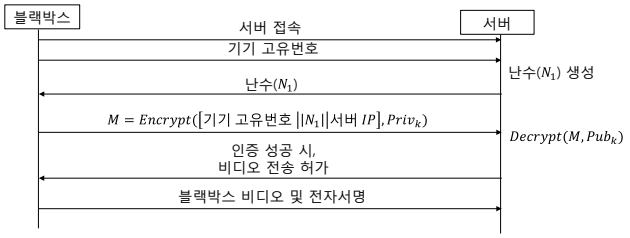

그림 2 블랙박스 영상 전송을 위한 단말 인증 절차

4. Prototype 구현

제안한 구조와 같이 블랙박스 기기 인증 및 영상 전송이 가능한지 확인하기 위해 안드로이드 OS 가 탑재된 스마트폰과 리눅스 서버에 Prototype 을 구현하였다. 블랙박스는 안드로이드 플랫폼을 활용해 구현하였으며, 추후 이와 같은 3G/4G 통신 모듈을 탑재한 블랙박스 기기를 통해 구현할 수 있다.

KS 표준[6]에 따라 프레임율(frame rate)이 30fps 이며 사고발생 전후 각 10 초 분량의 영상을 가정하여 사용하였다. 영상의 해상도는 1280x720, H.264/AVC 코덱을 사용하여 인코딩되었으며, 용량은 20.4MB 이다. Wi-Fi 환경에서 영상을 전송하는 경우 약 10.36 초가 소요되었다.

5. 결론

본 논문에서는 네트워크 연결 기능이 탑재된 블랙박스 기기를 사용하여 블랙박스 기기에 저장된 동영상을 서버로 전송할 수 있는 구조를 소개하고, 네트워크를 통한 영상 전송 과정에서 영상의 무결성을 보장할 수 있는 기법을 제시하였다. 또한 인증에 사용되는 서명 키를 안전하게 발급 및 관리할 수 있는 방법을 제시하였다.

6. 참고 문헌

[1] 김윤규, 김범한, 이동훈, “차량용 블랙박스 시스템을 위한 실시간 무결성 보장 기법”, 정보보호학회논문지, 제 19 권 6 호, pp. 49-61, 2009 년 12 월

[2] 김무섭, 최수길, 정치윤, 한종욱. “차량용 블랙박스 보안 이슈 동향”, Electronics and Telecommunications Trends, 제 27 권 4 호, pp. 123-129, 2012 년 8 월

[3] 윤장혁, 김진일, “스마트폰을 시용한 자동차 영상블랙박스 시스템 구현”, 한국정보기술학회논문지, 제 8 권 10 호, pp. 135-142, 2010 년 10 월

[4] 박대우, 서정만, “자동차의 블랙박스를 이용한 실시간 포렌식 자료 생성 연구”, 한국컴퓨터정보학회 논문지, 제 13 권 1 호, pp. 253-260, 2008 년 1 월

[5] 이정환, “모바일 환경에서 차량 주행기록 시스템에 관한 연구”, 단국대학교 대학원 석사학위논문, 2012

[6] KS R 5078:2013, “자동차용 영상 사고기록장치”, 기술표준원, 2013. 2. 15, http://www.kats.go.kr