논문 18-43-12-17 The Journal of Korean Institute of Communications and Information Sciences '18-12 Vol.43 No.12
https://doi.org/10.7840/kics.2018.43.12.2114

블록체인을 활용한 TEE 기반 인포테인먼트 세션 키 수립 프로토콜

이 성 범◆, 이 종 혁°

TEE Based Infotainment Session Key Establishment Protocol Using Blockchain

Sungbum Lee◆, Jong-Hyouk Lee°

요 약

최근 인포테인먼트 기술들이 활발히 연구되고 있으며, 인포테인먼트 시스템을 탑재한 차량의 수도 점차적으로 증가하고 있다. 그러나 인포테인먼트 시스템 취약점들이 계속해서 발표되고 있으며, 최근에는 공격자가 인포테인먼트 시스템을 장악하여 핸들 조작이 가능함을 시연하기도 하였다. 본 논문에서는 안전한 인포테인먼트 시스템을 위해 블록체인을 활용한 TEE(Trusted Execution Environment)기반의 세션 키 수립 프로토콜을 제안한다. 스마트폰과 같은 사용자 Device와 TCU(Telematics Control Unit)간의 블록체인을 활용한 인증과 공개키 기반의 세션 키 분배를 프로토콜의 동작 관점에서 자세히 설명한다. 본 논문에서 제안한 프로토콜을 활용함으로써 보다 강인한 인포테인먼트 시스템 구축이 가능하다.

Key Words : In-vehicle Infotainment, Trusted Execution Environment, Blockchain, Session Key Establishment

ABSTRACT

Recently, infotainment technologies are actively researched, while the number of vehicles equipped with infotainment systems is gradually increasing. However, security vulnerabilities of an infotainment system are continuously reported. It was also recently showed that an attacker could control the steering wheel through the infotainment system. In this paper, we propose a trusted execution environment based session key establishment protocol using blockchain for secure infotainment systems. From the protocol operation perspective, we present the detailed operations of authentication between a user device like smartphone and a telematics control unit using blockchain and public key based session key distribution. By using the protocol proposed in this paper, it is possible to construct a secure infotainment system.

Ⅰ. 서 론

최근 차량과 IT 기술 간 융합이 가속되어지면서 스마트 카의 기술이 발전하고 있다. 스마트 카 기술 중 하나인 인포테인먼트(Infotainment)를 통해 사용자들은 차량 내 정보를 통합 관리할 수 있고, 운전자가 차 안에서 오락, 정보 등 다양한 컨텐츠를 제공받을 수 있다. Hexa Research사의 보고서에 따르면 인포테인

※ 본 논문은 문화체육관광부 및 한국저작권위원회의 2018년도 저작권기술개발사업의 연구결과로 수행되었음.
◆ First Author : (ORCID:0000-0003-0341-0788)Dept. of Software, Sangmyung University, sungbum@pel.smuc.ac.kr, 학생회원
° Corresponding Author : (ORCID:0000-0002-1753-1284)Dept. of Software, Sangmyung University, jonghyouk@pel.smuc.ac.kr, 종신회원
논문번호 : 201806-B-183-RN, Received May 15, 2018; Revised July 24, 2018; Accepted October 23, 2018

먼트의 세계시장은 2024년까지 40.17억 달러까지 성장할 것으로 예측되어 지고 있다[1].

이러한 인포테인먼트 기술은 추가적인 디바이스를 차량에 연결하여 서비스를 확장하여 사용할 수 있다. 시스템에 연결된 다수의 디바이스들은 각 디바이스별 할당된 서비스들을 제공받게 된다. 2015년 대표적인 국제 보안/해킹 컨퍼런스인 데프콘에서 차량 인포테인먼트 시스템인 유커넥트(Uconnect)를 해킹하는 사례를 보여주었다. 이 사례에서는 차량 인포테인먼트 시스템의 펌웨어에 대한 보안성이 부족하고, 차량 내부 통신과정에서의 안전하지 않은 세션을 통해 차량 핸들을 조작하는 사례도 보여주었다.

본 논문에서는 블록체인을 활용한 인증과, TEE (Trusted Execution Environment)기반의 세션 키 수립 프로토콜을 제안한다. 분산화 된 환경에서 공증기관 없이 개체 인증할 수 있는 방법을 제안하기 위해 블록체인을 활용하고, 안전하게 펌웨어를 관리하고 세션 키를 수립하기 위해 TEE의 Secure Storage, RoT(Root of Trust), Secure Boot를 활용한다. 키 수립 과정에서 공개키 기반의 키 교환 알고리즘을 사용한다.

본 논문의 2장에서 관련연구인 인포테인먼트와 TEE, 블록체인에 대하여 설명한다. 제 3장에서는 제안하는 기법인 블록체인을 활용한 TEE기반 인포테인먼트 세션 키 수립 프로토콜을 설명한다. 제 4장에서 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 관련연구인 인포테인먼트와 TEE, 블록체인에 대하여 설명한다. 제 1절에서는 인포테인먼트에 대하여 설명하고, 2절에서는 TEE(Trusted Execution Environment)에 대해 설명한다. 제 3절에서는 블록체인을 설명한다.

2.1 인포테인먼트

인포테인먼트(Infotainment)는 정보(Information)와 오락(Entertainment)의 합성어로 차량 내에서 차량의 정보(예, 타이어 공기압, 엔진 온도 등)와 오락(예, 영화, 음악)을 한번에 즐길 수 있는 시스템이다[2]. 차량 인포테인먼트 기술은 GENIVI에서 표준화를 진행 하였다[3]. 인포테인먼트 시장의 대표적인 협력관계는 구글과 GM, 애플과 아우디, MS와 도요타, 삼성전자와 현대자동차등이 있다. 이와 같이 인포테인먼트 시스템은 산업에 적용되기 위한 연구는 활발하게 진행되고 있다.

인포테인먼트 시스템에서 주요한 요소는 HMI(Human Machine Interface)와 TCU(Telematics Control Unit)가 있다. TCU는 차량의 내부와 외부의 통신을 중재하는 장비이고, HMI는 사용자들이 차량 인포테인먼트를 활용할 수 있도록 하는 장비이다. 인포테인먼트 시스템에 새로운 디바이스가 연결되기 위해서는 TCU를 통해 연결이 가능하다. 연결된 디바이스들은 인포테인먼트 시스템에서 할당한 서비스만 이용할 수 있게 된다. 디바이스가 할당된 서비스이외의 서비스를 이용하게 되면 차량의 정보를 악용하여 차량의 사고를 유발할 수 있게 된다.

2015년 대표적인 국제 해킹/보안 컨퍼런스인 데프콘에서 인포테인먼트 시스템의 취약점을 이용하여 차량의 핸들 조작을 할 수 있음을 시연하였다[4]. 이 취약점은 인포테인먼트 시스템인 Uconnect의 펌웨어를 타겟으로 공격하였고, 차량의 내부 통신 과정의 안전하지 않은 세션을 통해서 차량의 핸들을 조작하였다. 차량 내에서 인포테인먼트 시스템의 역할이 커지고 있고 이에 따른 보안성도 커져야 한다.

2.2 TEE(Trusted Execution Environment)

TEE는 실행 환경을 분리하여 안전한 실행환경을 제공하는 기술이다. 일반적인 어플리케이션이 실행되는 Non-secure World와 신뢰할 수 있는 어플리케이션이 실행되는 Secure World로 구성된다. GlobalPlatform에서는 두 영역 간 통신을 위한 API에 대해 표준을 정의하고 있다. 민감한 데이터는 Secure World에 저장되게 되고, Non-Secure World에서 민감한 데이터에 접근하기 위해서는 API를 통해 권한이 있는 어플리케이션만이 접근이 가능하다. TEE의 Implementation에 따라 구조도는 달라질 수 있다. 대표적인 Implementation은 ARM TrustZone과 Intel SGX가 있다[6]. 아래 그림 1.은 ARM Cortex-A TrustZone의 구조도 이다.

ARM Cortex-A TrustZone은 ARM Trusted Firmware을 통하여 두 영역간의 통신을 중재한다. 또한 RoT를 제공 하기 위해 CryptoCell을 활용한다. ARM Cortex-A TrustZone에서 두 영역을 분리하고 안전하게 운용하기 위한 주요 기술은 다음과 같다.

- Non-secure World와 Secure World 간의 통신: Non-secure World와 Secure World간의 통신은 Global Platform에서 정의한 API를 활용한다. ARM Cortex-A 시리즈에서 TrustZone은 ARM

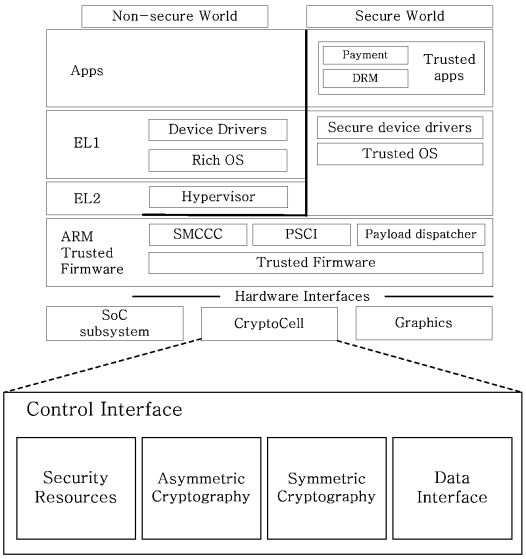

그림 1. ARM Cortex-A TrustZone 구조
Fig. 1. ARM Cortex-A TrustZone Architecture

Trusted Firmware에서 Non-Secure bits를 이용하여 두 영역사이의 통신을 중재한다. Secure World에서 외부 인터넷과 통신하기 위한 방법으로는 Non-secure World에 존재하는 네트워크 인터페이스를 통하여 통신이 가능하다. 이때 생길 수 있는 보안 문제는 Transport Layer Security(TLS)를 통해 보호된다[5].

- Secure Boot: 부팅 전 펌웨어에 대한 공격을 방어하기 위한 기술로, 부팅 시 부트로더는 펌웨어의 무결성 검증을 하고 난 후 펌웨어를 로드하여 Firmware 변조 공격을 방어하는 기술이다.
- RoT(Root of Trust): 하드웨어 적으로 보안 기술을 제공하는 것으로, ARM TrustZone에서는 CryptoCell이 있다. CryptoCell의 대표적인 기능으로는 RNG(Random Number Generator), Crypto Engine(e.g., Cryptography, Hashfunction)을 제공한다. 하드웨어적으로 보안 모듈을 제공함으로써 공격에 강인해진다. TEE는 안전한 실행환경과 저장소를 위해 블록체인[7], 드론[8]과 같은 기술에 적용하기 위한 연구가 진행되고 있다.

2.3 블록체인

2008년 사토시 나카모토가 제안한 비트코인은 블록체인 기술을 이용한 대표적인 암호화폐이다. 비트코인은 기존 서버-클라이언트 구조가 아닌 피어-피어 구조에서 제 3자의 개입이 없고, 사용자간 신뢰 관계가 없이 안전하게 암호화폐 거래가 가능한 플랫폼이다. 비트코인의 주요 기술인 블록체인은 피어-피어 구조에서 암호화폐 거래내역을 안전하게 저장할 수 있도록 하는 기술이다. 사용자들은 자신의 개인키로 서명한 거래(Transaction)를 브로드 캐스팅하고, 마이닝 노드는 거래들을 합의 알고리즘을 통해서 블록으로 생성한다. 생성 된 블록은 아래 그림 2.와 같이 체이닝 형식으로 유지된다. 이때 데이터 무결성 제공을 위해 해시함수와 데이터 체이닝 기법을 활용한다[9]. 또한 데이터에 대한 신뢰성을 제공하기 위해 공개키 기반의 전자 서명을 사용한다.

블록체인의 주요 기술인 합의 알고리즘은 노드들 간에 무결성, 신뢰성을 제공하는 블록을 생성하기 위한 알고리즘이다. 이 알고리즘은 특정 조건을 만족하는 노드가 블록을 생성하고 블록체인에 블록을 연결한다. 대표적인 합의 알고리즘은 PoW(Proof of Work), PoS(Proof of Stake), DPoS(Delegated Proof of Stake)가 있다. 또한 블록을 생성, 검증 하는 주체에 따라 퍼블릭, 프라이빗, 컨소시엄 형태로 유형 분류가 가능하다.

- 퍼블릭 블록체인(Public Blockchain): 블록체인에 참여하는 모든 노드가 운영주체가 될 수 있는 유형이다. 운영주체는 블록체인 네트워크에서 거래를 쓰기, 읽기, 저장할 수 있고, 합의 알고리즘을 통해 블록을 생성할 수 있는 노드를 의미 한다.
- 프라이빗 블록체인(Private Blockchain): 특정 중앙 기관에서 블록체인을 관리하는 형태의 블록체인이다. 중앙 기관에서 지정한 특정 운영주체가 블록체인 네트워크에서 거래를 쓰기, 읽기, 저장할 수 있고, 합의 알고리즘을 통해 블록을 생성한다.
- 컨소시엄 블록체인(Consortium Blockchain): 블

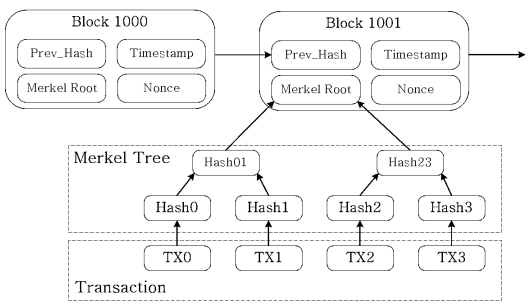

그림 2. 비트코인 블록체인의 블록
Fig. 2. Blocks of the Bitcoin Blockchain

록체인 네트워크에서 컨소시엄 멤버를 선출하여 거래를 쓰기, 읽기, 저장하고, 합의 알고리즘을 통해 블록을 생성하는 유형이다.

이와 같은 블록체인은 유엔 미래 보고서 2050[10]에서 미래를 변화시킬 기술로 선정되었고, 또한 국내/외에서 활발하게 학문적으로 연구되어 지고 있다. 또한 블록체인 기술은 암호화폐 이외의 펌웨어 업데이트 시스템[11], 사용자 인증 시스템[12]와 같은 분야에서도 적용하기 위한 연구가 이루어지고 있다.

Ⅲ. 제안하는 기법

본 장에서는 제안하는 기법인 안전한 인포테인먼트 시스템을 위한 블록체인을 활용한 TEE 기반 세션 키 수립 프로토콜에 대하여 설명한다. 제 1절에서는 세션 키 수립 과정에서의 표기법과 네트워크 모델에 대해서 설명하고, 2절에서는 키 수립 프로토콜을 등록 단계[12]와 세션 키 수립 단계로 나누어 설명한다.

3.1 Overview

B 제조사의 TCU(Telematics Control Unit)가 장착된 인포테인먼트 시스템 환경에 A 제조사의 Device가 안전한 세션을 연결되기 위한 과정을 설명한다. 제조사는 기기(Device, TCU)를 생산할 때 기기의 Secure Storage에 제조사의 공개키와, 기기의 비밀 값을 삽입한 후 판매한다. 제조사는 생산 된 기기의 비밀 값과 제조사의 공개키와 개인키를 제조사 시스템의 데이터베이스에 저장한다. 제조사 A와 제조사 B는 사전에 안전한 세션으로 유지되어 있다. 제안하는 기법의 주요한 노드 및 시스템에 대한 정보는 다음과 같다.

- Blockchain: 장비(TCU, Device)의 가상 아이디와 공개키를 블록으로 저장하는 프라이빗 블록체인
- Database: 생산 된 장비의 정보(비밀 값) 및 제조사 공개키 쌍 저장하는 데이터베이스
- DA(Database Agent): 데이터베이스에 접근 가능한 노드
- BA(Blockchain Agent): 블록체인에 접근 가능한 노드로 블록체인의 블록을 저장하고 있고, 트랜잭션을 발생 가능
- MN(Mining Node): 발생된 트랜잭션을 블록으로 생성하는 노드
- TCU(Telematics Control Unit): 차량 내/외의 통신을 중재하는 장비로, Secure Storage에 비밀 값과 제조사의 공개키를 저장하고 있으며, ARM TrustZone 기술을 지원하는 하드웨어를 사용
- Device: 차량의 TCU에 연결되는 장비로, Secure Storage에 비밀 값과 제조사의 공개키를 저장하고 있으며 ARM TrustZone 기술을 지원하는 하드웨어를 사용

주요 표기법은 아래 표 1.과 같다.

제안하는 기법에서의 네트워크 모델은 아래 그림 3.와 같다.

표 1. 표기법
Table 1. Notations

Notations	Definitions
Dev_A	Manufactured Device by the A
TCU_B	Manufactured TCU by the B
BA_A, BA_B	Blockchain Agent of each manufacturer
DA_A, DA_B	Database Agent of each manufacturer
MN_A, MN_B	Mining Node of each Blockchain
SID_{Dev}	Dev_A Secret ID
SID_{TCU}	TCU_B Secret ID
VID_{Dev}	Dev_A Virtual ID
VID_{TCU}	TCU_B Virtual ID
r_i	ith Random Number
$h(.)$	Hash Function
$E_K(.)$	Encryption with the K
$D_K(.)$	Decryption with the K
$Sig_K(.)$	Signature with the Private Key K
tx	Transaction of blockchain
$K_{Pub}^{Dev}, K_{Pri}^{Dev}$	Dev_A Public Key, Private Key
$K_{Pub}^{TCU}, K_{Pri}^{TCU}$	TCU_B Public Key, Private Key
$K_{Pub}^{man}, K_{Pri}^{mau}$	Manufacturer Public Key, Private Key
$K_{session}^{Dev-TCU}$	Session Key between Dev_A and TCU_B

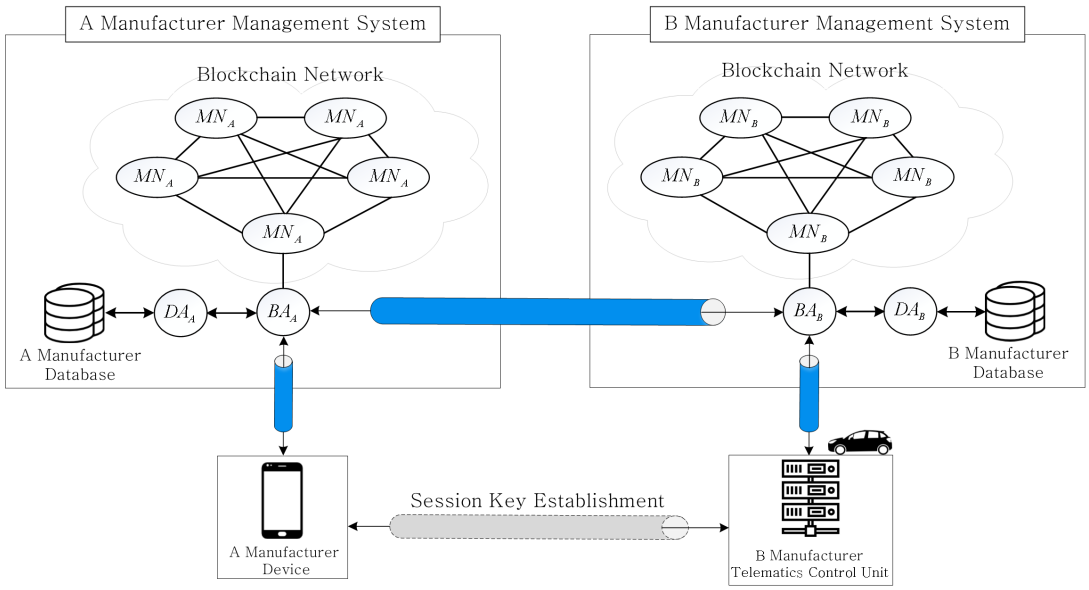

그림 3. 네트워크 모델
Fig. 3. Network Model

3.2 Procedure

본 절에서는 제안하는 기법을 등록 단계와 키 수립 단계로 나누어 설명한다. 등록 단계의 절차는 아래와 같다.

1. $Device_A$의 Secure World에서 CryptoCell의 Random Number Generator(RNG)와 Crypto Engine을 통해 r_1와 K_{Pub}^{Dev},K_{Pri}^{Dev}을 생성하고, VID_{Dev}를 생성하여 CryptoCell의 Secure Storage에 저장. SID_{Dev}와 K_{Pub}^{Dev}와 r_1을 K_{Pub}^{mau}로 암호화하여 CID_{Dev} 생성. VID_{Dev}, K_{Pub}^{Dev}, CID_{Dev}, r_1 를 M_1으로 생성하여 BA_A에게 전달.
2. BA_A는 VID_{Dev}, K_{Pub}^{Dev}, CID_{Dev}를 M_2로 생성하여 DA_A에게 전달.
3. DA_A는 K_{Pri}^{mau}로 CID_{Dev}를 복호화하여 SID_{Dev}, K_{Pub}^{Dev}, r_1 값을 얻어내고, 데이터베이스에 저장되어 있는 SID_{Dev} 값과 복호화 하여 얻어낸 SID_{Dev} 값을 비교, 일치하지 않다면 멈춤. M_2에 포함된 K_{Pub}^{Dev}와 복호화 하여 얻어낸 K_{Pub}^{Dev} 값을 비교, 일치하지 않다면 멈춤. $VID_{Dev}K_{Pub}^{Dev}$,을 K_{Pri}^{mau}로 서명하여 $Signature_{Dev}$생성. $Signature_{Dev}$와 복호화 하여 얻어낸 r_1 값을 M_3로 생성하여 BA_A에게 전달.
4. BA_A는 M_1에 포함된 r_1과 M_3에 포함된 r_1 값을 비교, 일치하지 않다면 멈춤. VID_{Dev}, K_{Pub}^{Dev}, $Signature_{Dev}$를 트랜잭션(tx)으로 작성한 뒤 M_4로 생성하여 MN_A에게 전달.
5. MN_A은 BA_A로부터 수신한 트랜잭션(tx)을 블록으로 생성하고, 블록의 정보를 M_5로 생성하여 BA_A에게 전달.
6. BA_A는 $Signature_{Dev}$와 r_1+1을 M_6로 생성하여 $Device_A$의 Secure World에 전달
7. $Device_A$의 Secure World에서 $Device_A$가 생성한 r_1+1 값과 수신한 r_1+1을 비교, 일치하지 않다면 멈춤. $Signature_{Dev}$를 K_{Pub}^{man}를 이용하여 복호화하여 VID_{Dev},K_{Pub}^{Dev}를 획득, 복호화 시 CryptoCell Crypto Engine을 사용. 자신이 생성한 VID_{Dev}, K_{Pub}^{Dev}와 복호화 하여 얻어낸 VID_{Dev},K_{Pub}^{Dev}를 비교, 일치하지 않다면 멈춤.

등록 단계가 완료되면 $Device_A$는 제조사 A의 블록체인에 자신의 공개키를 등록하였기에, 다른 장비와 사용자 인증이 가능하다. 인증 및 세션 키 수립 단계의 절차는 다음과 같다.

1. $Device_A$의 Secure World에서 CryptoCell의

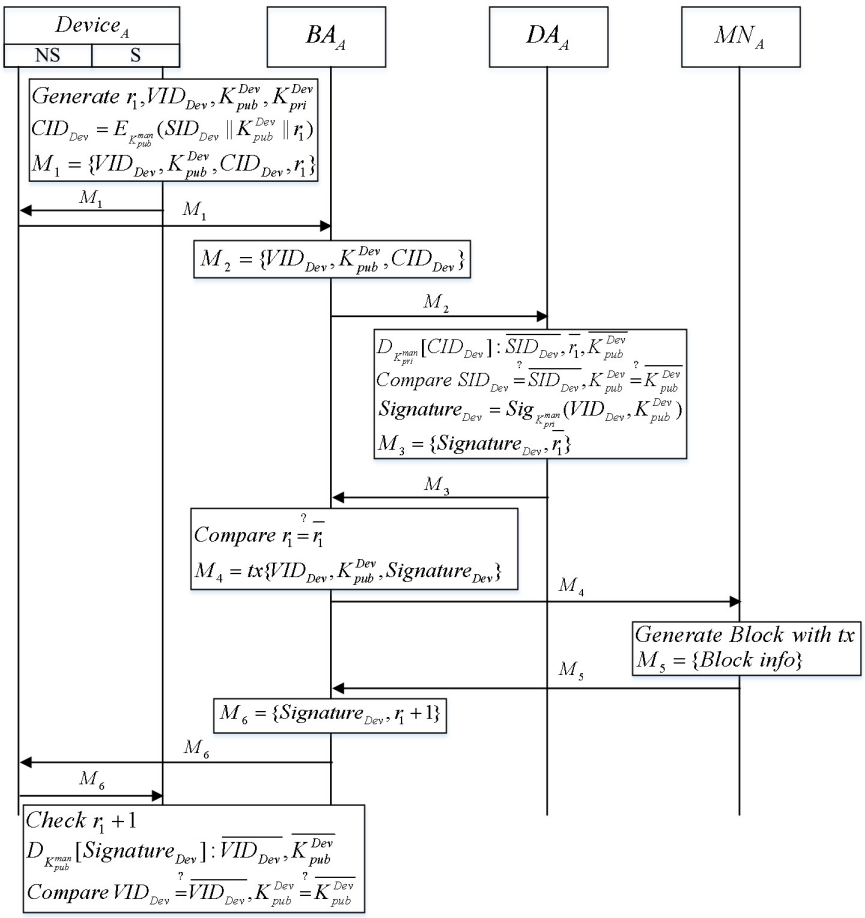

그림 4. 등록 단계
Fig. 4. Registration Phase

Random Number Generator(RNG)을 통해 난수(r_2)를 생성, VID_{Dev}, $Signature_{Dev}$, r_2를 M_7으로 생성하여 TCU_B의 Secure World에 전달.

2. TCU_B의 Secure World에서 VID_{Dev}, $Signature_{Dev}$를 M_8으로 생성하여 BA_B에게 전달.
3. BA_B는 난수 r_3을 생성하고, TCU_B로부터 받은 M_8와 r_3을 BA_A로 전달.
4. BA_A는 M_8로 전달받은 VID_{Dev}, $Signature_{Dev}$과 블록체인에 저장되어 있는 VID_{Dev}, $Signature_{Dev}$을 비교하고, 일치한다면 VID_{Dev}, K_{Pub}^{Dev}을 M_9으로 생성하고, r_3+1 값과 BA_B에게 전달.
5. BA_B는 자신이 생성한 r_3+1와 수신한 r_3+1 값을 비교, 일치하지 않다면 멈춤. M_9을 TCU_B의 Secure World로 전달.
6. TCU_B의 Secure World에서 CryptoCell의 Random Number Generator(RNG) 난수 r_4를 생성. CryptoCell의 Crypto Engine의 해시 함수의 입력 값으로 VID_{Dev}, VID_{TCU}, K_{Pub}^{Dev}, K_{Pub}^{TCU}, r_4를 넣어, $K_{session}^{Dev-TCU}$ 생성. K_{Pub}^{Dev}로 $K_{session}^{Dev-TCU}$를 암호화 하여 M_{10}으로 생성하고, r_2+1값과 $Device_A$의 Secure World로 전달.
7. $Device_A$의 Secure World에서 K_{Pri}^{Dev}를 이용하여 M_{10}를 복호화 하여 $K_{session}^{Dev-TCU}$ 획득. 자신이 생성한 r_2+1과 수신한 r_2+1을 비교, 일치하지 않다면 멈춤.

세션 키 분배 단계가 완료 되면 TCU와 Device간 세션 키가 수립되고, 안전한 세션이 연결된다. Device와 TCU는 생성한 세션키를 자신의 Secure Storage에

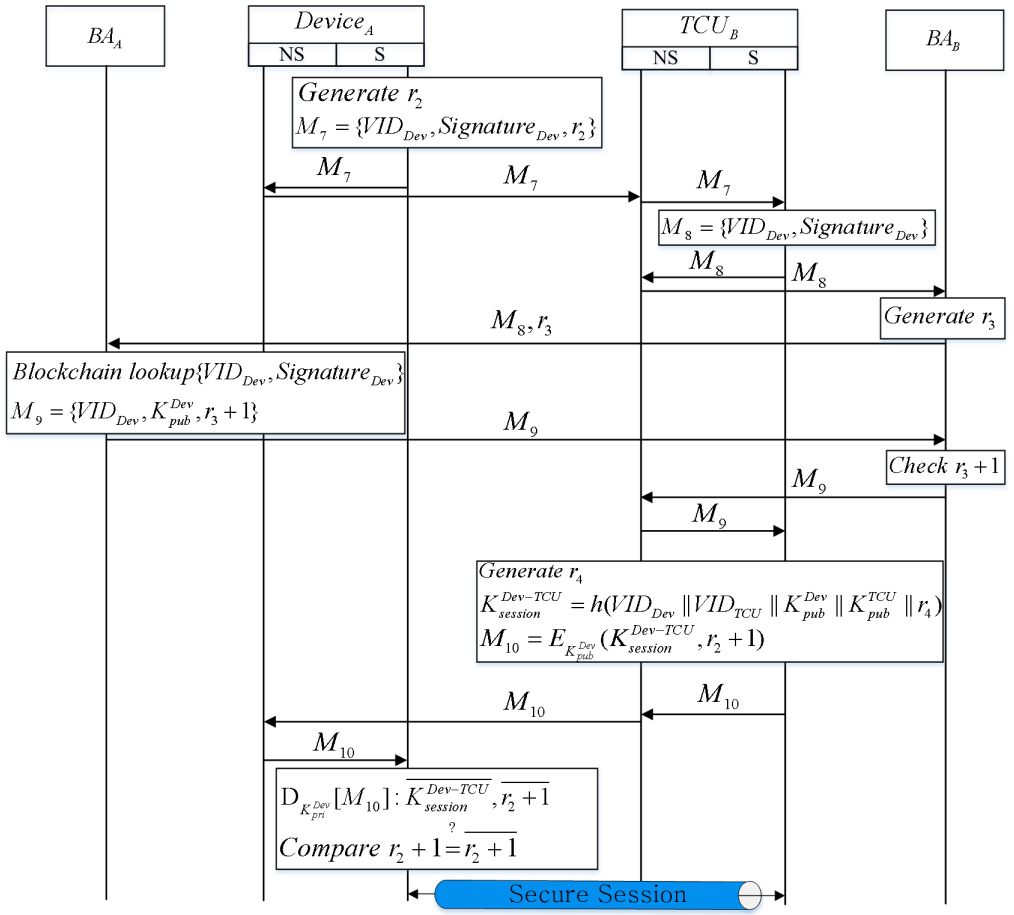

그림 5. 세션 키 분배 단계
Fig. 5. Session Key Distribution Phase

저장한다.

Ⅳ. 결 론

최근 인포테인먼트 시스템 시장이 커지고 있고, 인포테인먼트 시스템을 탑재한 차량의 수가 급격하게 증가하고 있다. 하지만 보안/해킹 컨퍼런스에서 차량 인포테인먼트의 취약점을 통해 인포테인먼트 시스템의 펌웨어와 차량 내부의 통신을 공격하여 핸들을 조작하는 시연을 보여주었다. 이러한 인포테인먼트 시스템을 보호하기 위한 연구는 미비한 편이다.

본 논문에서는 안전한 인포테인먼트 시스템을 위해 블록체인을 활용한 TEE기반의 인증 및 세션 키 수립 프로토콜을 제안하였다. 블록체인을 활용하여 공증기관 없이 피어-피어 환경에서 인증을 제공하고, 개체(e.g., 디바이스, TCU)는 가상 아이디를 사용함으로써 익명성을 제공하였다. 또한 기존의 데이터베이스 시스템이 아닌 블록체인을 활용함으로써 분산화 된 환경에서 안전하고 빠르게 인증할 수 있다. TEE를 통해서 인포테인먼트 시스템의 펌웨어, 개체 간의 세션 키 수립 프로토콜을 통해서 안전한 펌웨어 및 안전한 세션을 제공하였다. 생성된 키 정보들은 TEE의 Secure Storage에 저장함으로써 추후 발생할 수 있는 키 추출 공격에 대해서 방어할 수 있다. 추후 ECC(Elliptic Curve Cryptography)를 활용한 키 수립 과정을 연구하고, 설계된 내용을 오픈플랫폼인 이더리움과 OP-TEE를 활용하여 구현하고자 한다.

References

[1] Hexa Research, "*Automotive Infotainment Market Size and Forecast, By Vehicle*

(Passenger Cars, Commercial Vehicle), By Operating System (Linux, QNX, Microsoft) And Trend Analysis 2014 - 2024," Hexa Research, USA, 2017.

[2] H. W. Chun, "Technology and Service Trends of Smart Car," *Electronics and Telecommun. Trends,* vol. 27, no. 1, 2012.

[3] J. Kim and T. Han, "Trends of the standard open platform for in-vehicle infotainment and GENIVI based human machine interface," *J. KISS : Software and Appl.*, vol. 39, no. 6, pp. 444-452, 2012.

[4] C. Miller and C. Valasek, "*Remote exploitation of an unaltered passenger vehicle*," Black Hat USA 2015, Aug. 2015.

[5] GlobalPlatform, "*Globalplatform Device Technology TEE Sockets API Specication Version 1.0.1*," GPD SPE 100, GlobalPlatform, Jan. 2017.

[6] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," *2015 IEEE Trustcom/ BigDataSE/ISPA,* vol. 1, Aug. 2015.

[7] J. Lind, et al., "Teechain: Scalable blockchain payments using trusted execution environments," *arXiv preprint arXiv:1707. 05454*, 2017.

[8] R. Liu and M. Srivastava, "PROTC: PROTeCting drone's peripherals through ARM trustzone," in *Proc. DroNet '17*, pp. 1-6, Niagara Falls, New York, USA, Jun. 2017.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[10] G. Jerome, et al., "*World Future Report 2050*," Kyobo Book, Korea, 2016.

[11] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *The J. Supercomputing,* vol. 73, no. 3, pp. 1152-1167, 2017.

[12] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274-2278, Feb. 2018.

이 성 범 (Sungbum Lee)

2016년 8월 : 상명대학교 공학사

2018년 8월 : 상명대학교 공학석사

<관심분야> 프로토콜 분석, 시스템 보안, 블록체인 보안

이 종 혁 (Jong-Hyouk Lee)

2010년 2월 : 성균관대학교 공학박사

2009년 6월~2012년 2월 : 프랑스 INRIA 연구원

2012년 3월~2013년 8월 : 프랑스 그랑제꼴 TELECOM Bretagne 조교수

2013년 9월~현재 : 상명대학교 소프트웨어학과 조교수

<관심분야> 정보보안, 프로토콜 분석, 블록체인