http://dx.doi.org/10.14400/JDC.2014.12.8.229

자동차 보안시스템에서 통신 인증프로토콜의 보안성 검증

한명석*제1저자, 배우식**
아주자동차대학 자동차디지털튜닝전공*, 아주자동차대학**

Security Verification of a Communication Authentication Protocol in Vehicular Security System

Myoungseok Han*1st Author, WooSik Bae**
Dept. of Automobile Digital Tuning, Ajou Motor College*
Dept. of AIS Center, Ajou Motor College**

요 약 자동차산업의 발전과 함께 차량전자통신시스템이 고성능화 되어가고 있으며 사용자 편의 면에서도 상당히 많은 발전을 거듭해가고 있다. 그러나 통신시스템의 특성상 전송구간에서 공격자의 공격에 대한 문제가 제기되고 있으며 안전한 통신에 대한 필요성이 중요시 되고 있다. 자동차의 운행, 제어계통 및 영상장비 등에 공격자의 공격이 성공하게 되면 안전 및 프라이버시에 심각한 문제가 발생하게 된다. 따라서 하드웨어적인 보안 및 보안통신프로토콜에 대한 연구가 중요한 부분으로 이루어지고 있다. 본 논문에서는 안전한 차량 통신프로토콜을 제안하며 공격자의 각종 공격에 안전한 프로토콜을 정형검증도구인 Casper/FDR 도구를 이용하여 실험하였으며 제안 프로토콜이 안전하며 문제없이 종료됨을 확인하였다.

주제어 : 차량보안시스템, 인증프로토콜, Casper, 보안인증, 모델검증

Abstract Vehicular electronic communication system has continued to develop in favor of high performance and user convenience with the evolution of auto industry. Yet, due to the nature of communication system, concerns over intruder attacks in transmission sections have been raised with a need for safe and secure communication being valued. Any successful intruder attacks on vehicular operation and control systems as well as on visual equipment could result in serious safety and privacy problems. Thus, research has focused on hardware-based security and secure communication protocols. This paper proposed a safe and secure vehicular communication protocol, used the formal verification tool, Casper/FDR to test the security of the proposed protocol against different types of intruder attacks, and verified that the proposed protocol was secure and ended without problems.

Key Words : Vehicular Security System, Authentication protocol, Casper, Security authentication, Model Checking

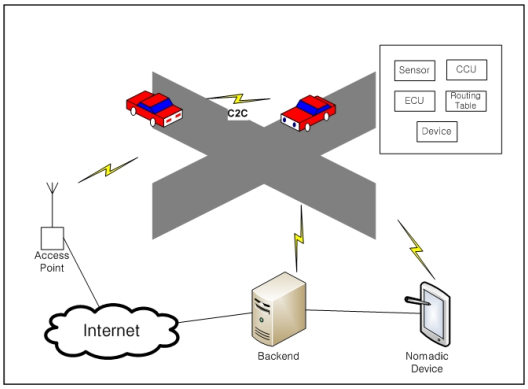
Received 29 May 2014, Revised 29 June 2014
Accepted 20 August 2014
Corresponding Author: WooSik Bae(Ajou Motor College)
Email: drbws@daum.net

ISSN: 1738-1916

1. 서론

최근 자동차 산업의 기술발전으로 차량의 안전성능과 함께 기계부품을 전기전자 부품으로 대체하여 적용 되고 있다. 그러나 차량의 전기전자부품으로 편리한 기술과 기능을 사용할 수 있지만 제어 소프트웨어가 복잡해지고 오류 문제도 발생하게 되었다. 또한 [Fig. 1]과 같이 차량 내부의 각종 디바이스간 제어와 통신이 증가하고 향후 더욱더 많은 도입이 예상된다. 이는 중요한 차량제어시스템에 보안 위협으로 다가오게 되며 탑승자의 안전과 프라이버시 침해의 위험이 발생하게 되었다[1][2].

차량의 기능 안전성의 국제규격인 ISO 26262가 제정되었으나 보안위협에 대해서는 미진한 상태이다[3]. 이는 악의적인 공격에 대한 대응이 없어 심각한 문제로 여겨지고 있다. 실제로 미국에서 자동차 통신을 통하여 취약점을 공격함으로써 각종 제어 등에 영향을 주는 것을 실험하였으며 인증 등에 대해서 취약한 부분이 있다는 사실이 밝혀졌다. 따라서 통신공격에 의한 사고가 발생하는 것을 자동차 개발시 고려하여야 하며 보안의 중요성을 파악하고 대응해야 한다[4].



[Fig. 1] Communication System Overview

최근 이러한 보안 문제를 해결하기 위해서 많은 연구자들이 자동차 보안통신을 위해서 활발한 연구를 하고 있다. 본 논문에서는 정형검증 분야에서 많이 사용하는 Casper/FDR[5][6] 도구를 사용하여 제안한 프로토콜을 검증실험 하였으며 보안적으로 안전한 통신 프로토콜임이 증명되었다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 자동차 보한 위협과 CASPER/FDR에 대하여 알아본다. 3장에서는 인증프로토콜을 제안하고, Casper/FDR을 이용하여 실험 검증하며 4장에서 실험 결과의 안전성을 확인하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 자동차 보안위협

차량 통신 보안요구사항은 다음과 같다[1][7].

1) 인증 및 데이터 무결성 : 차량 통신에서 개체가 자신이 정당한 소유자임을 확인해야 하는데 이를 충족하기 위해 모든 개체는 서로 다른 유일한 ID를 가져야 한다.
2) 비밀성 : 차량통신에서 인증된 통신 개체 간 송·수신되는 데이터는 인증되지 않은 개체에 대해 비밀성이 유지되어야 한다.
3) 익명 및 프라이버시 : 차량 통신에서 익명성이 결여되면 프라이버시 침해의 위험이 존재한다. 따라서 프라이버시 보호방안이 제공되지 않는다면, 공격자가 차량의 주행, 위치, 영상 등 정보를 확인할 경우 심각한 문제가 발생할 수 있다.
4) 부인방지 : 데이터를 송신한 개체는 데이터 송신 사실을 부인할 수 없어야 한다. 일반적으로 차량 통신 시스템에서는 디지털서명을 사용함으로써 부인방지를 제공할 수 있다.

2.2 CASPER/FDR

Casper는 CSP(Communication Sequential Process)방식으로 프로토콜을 명세하기 쉽게 개발 되어진 컴파일러이다. Casper(a Compile for the Analysis of Security Protocols)[5]는 기존의 CSP[8] 언어를 이용한 정형명세 과정에서 오류가 생겨 설계 및 분석을 어렵게 진행하는 단점이 있었다. 이를 개선하기 위해 보안프로토콜의 동작을 간략히 설계할 수 있도록 개발된 프로그램이 Casper이다.

Casper 에서 컴파일된 파일을 FDR(Failure Divergence Refinements)[6] 프로그램을 이용하여 보안성과 인증속성 같은 보안속성을 만족하는지 검증한다. 아울러 추적

모델(trace model), 실패모델(failure model), 실패/분기모델(failure/divergence model)을 지원한다[6].

1) 추적모델(trace model)

프로세스는 그 프로세스가 갖는 행위에 의해 유한 순서 집합으로 표현되며, P 프로세스가 Q 프로세스의 모든 행위를 포함할 때 $P \sqsubseteq TQ$ 라고 표기한다.

$$P \sqsubseteq TQ \triangleq traces(Q) \subseteq traces(P)$$

2) 실패모델(failure model)

교착상태를 의미하며, 다음과 같이 표기한다.

$$P \sqsubseteq FQ \triangleq failures(Q) \subseteq failures(P)$$

3) 실패/분기 모델(failure/divergence model)

실패/분기 모델은 교착(deadlock)상태이면서 라이브락 상태를 의미하며, 다음과 같이 표기한다.

$$P \sqsubseteq FDQ \triangleq$$
$$failures(Q) \subseteq failures(P) \wedge divergences(Q) \subseteq divergences(P)$$

3. 제안 프로토콜

자동차 통신장치는 유무선 통신방식을 이용하여 정보를 송수신 한다[9][10]. 따라서 통신 구간에 다양한 보안 위협이 있으며 공격자의 공격 등 보안위협으로부터 안전한 통신환경을 제공하고자 본 논문에서는 매 세션 바뀌는 변수 값을 이용하고 실시간 에이전트값 및 해시함수를 기반으로 설계하였다.

기호의 정의는 <Table 1>과 같다.

〈Table 1〉 Symbols and definition

Symbols	Definition
ALICE	Agent
BOB	Agent
S	Server
H	Hash Function
x,k	Nonce
a1, a2	Session Key
PK	PublicKey
SK	SecretKey
realAgent	Agent -> Bool

3.1 동작설명

본 논문에서 제안하는 프로토콜의 단계별 처리내용을 pseudo code 형식으로 기술하면 다음과 같다.

◎ Step 1 : ALICE → BOB

Step 1 ALICE → BOB
Input Query
Output $xa\%enc1$
1: **Begin**
2: Create a Nonce x;
3: Initialize (x);
4: Update a ALICE Key (x);
5: Create a Session Key (a1);
6: Compute the $xa\%enc1$;
7: Send $xa\%enc1$ To BOB;
8: **End;**

[Fig. 2] Generation of data to be transmitted from ALICE to BOB

ALICE는 BOB로부터 Query를 수신한 후 [Fig. 2]와 같은 순서로 ALICE에서 x 값과 $xa\%enc1$ 값을 생성하고 각 값을 연접하여 BOB에게 전송한다. 이때 x 값은 고유한 값으로 다른 ALICE에서 생성할 수 없는 값이다.

◎ Step 2 : BOB → S

Step 2 BOB → Server
Input $xa\%enc1$
Output $H(BOB) \oplus (enc1\%xa1, a2, ka2, PK(a))$
1: **Begin**
2: Create a HashFunction BOB;
3: Initialize PK(a);
4: Create a Session Key a1,a2;
5: Create a Nonce x,k;
6: Compute the ;
$H(BOB) \oplus (enc1\%xa1, a2, ka2, PK(a))$;
7: Concatenation operation
$H(BOB) \oplus (enc1\%xa1, a2, ka2, PK(a))$;
8: Send $H(BOB) \oplus (enc1\%xa1, a2, ka2, PK(a))$
To Database;
9: **End;**

[Fig. 3] Generation of data to be transmitted from BOB to Server

ALICE에서 전송한 $xa\%enc1$ 값과 BOB이 계산한 $H(BOB) \oplus (enc1\%xa1, a2, ka2, PK(a))$ 값을 [Fig. 3]과 같이 서버로 전송한다. 이때 해시계산은 다음의 식과 같이 계산한다.

$$h_a(\overline{x}) = h \int ((\sum_{i=0}^{k} x_i \cdot a^i) \bmod p)$$

◎ Step 3 : S → BOB

Step 3 S → BOB
Input $H(BOB)\oplus(enc1\%xa1,a2,ka2,PK(a))$
Output $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$
1: Begin
2: Compute the $H(BOB)\oplus(enc1\%xa1,a2,ka2,PK(a))$;
3: Compute the $ALICE,x,ka1\%enc2a2\oplus H(BOB),PK(b)$;
4: Send $ALICE,x,ka1\%enc2a2\oplus H(BOB),PK(b)$ To BOB;
5: End;

[Fig. 4] Data first authenticated by the server and then transmitted to BOB

BOB에게서 전송된 $H(BOB)\oplus(enc1\%xa1,a2,ka2,PK(a))$ 값과 서버에서 생성한 값 $ALICE,x,ka1\%enc2a2\oplus H(BOB),PK(b)$을 인증 값으로 생성하고 [Fig. 4]와 같이 BOB에게 전송한다.

◎ Step 4 : BOB → ALICE

Step 4 BOB → ALICE
Input $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$
Output $m2\%(k)(sk1),H((x)(k))$
1: Begin
2: Create a $enc2\%ka1,xk$;
3: Compute the $enc2\%ka1,xk\oplus H(BOB)$
4: Send $enc2\%ka1,xk\oplus H(BOB)$ To ALICE;
5: End;

[Fig. 5] Data transmitted to the tag to authenticate BOB

BOB는 서버에서 수신한 $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$ 값을 [Fig. 5]와 같이 인증을 위해 $enc2\%ka1,xk\oplus H(BOB)$ 값을 생성한 후 태그에게 전송한다. 이 부분은 태그에서의 연산을 줄여 전송한다.

◎ Step 5 :ALICE → BOB

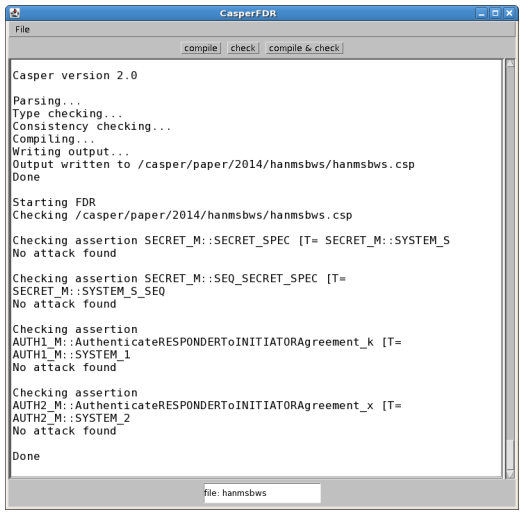
Step 5 ALICE → BOB
Input $enc2\%ka1,xk\oplus H(BOB)$
Output $H(ALICE)\oplus xk\%PK(b)$
1: Begin
2: ALICE receive $enc2\%ka1,xk\oplus H(BOB)$;
3: Compare a $enc2\%ka1,xk\oplus H(BOB)$ with; $enc2\%ka1,x$;
4: Compute the $H(ALICE)\oplus xk\%PK(b)$;
5: Send $H(ALICE)\oplus xk\%PK(b)$ to BOB;
6: End;

[Fig. 6] Generation of hashed tag information

마지막으로 ALICE는 BOB에게 $enc2\%ka1$, $xk\oplus H(BOB)$ 값을 전송한 이후 ALICE에서 생성한 값과 비교하여 확인되면 [Fig. 6]과 같이 자신의 ID를 해시연산 암호화하여 xk%PK(b)와 함께 BOB에게 전송함으로 ALICE에서의 인증 세션을 완료한다. 이후 BOB는 ALICE 값을 서버에 전송하게 되면 서버는 ALICE의 해시된 값을 검색하게 된다. 정상적인 검색이 완료되면 해시된 코드와 ALICE코드를 확인 할 수 있음으로 세션을 종료한다.

4. 실험결과

제안한 차량 통신프로토콜을 FDR의 모델검증 도구를 이용하여 안전성(safety), 교착상태(deadlock), 라이브락(livelock) 등의 동작을 검증하였다. [Fig. 7]은 설계한 소스파일을 로딩 하여 기본적인 오류 없이 실행 완료된 상태이다. 아울러 프롬프트 상태에서 공격에 대한 안전성을 검증하여 완료된 상태이다. 제안한 프로토콜을 FDR 엔진을 이용하여 보안프로토콜을 검증한 결과 그림과 같이 모든 보안속성에 대하여 만족함이 확인되었다.



[Fig. 7] Security verification results of the protocol

[Fig. 7]에는 4가지 검증결과가 제시되며 각 결과의 표현은 다음과 같이 분석된다.

1)SECRET_M::SECRET_SPEC[T=SECRET_M::SYSTEM_S

프로토콜의 보안성 확보로 메시지 앞의 체크표시는 프로토콜이 공격자에게 노출되지 않았고 보안상 안전한지를 표현한다. 검증한 Agent간 통신과 해시와 세션키의 보안성이 안전한지 확인하였으며 각종 공격에 문제가 있는지 확인하였다.

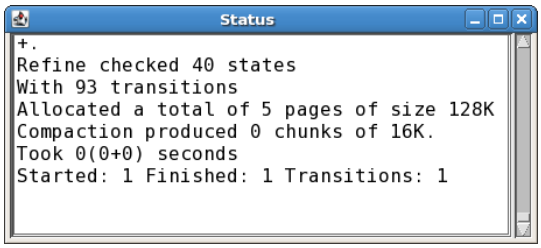
2)SECRET_M::SEQ_SECRET_SPEC[T=SECRET_M:: SYSTEM - S_SEQ

이 항목은 프로토콜이 시스템에서 정상적인 프로세스로 동작하는지를 확인한 결과이며 제안한 프로토콜은 안전한 프로세스로 동작함을 확인하였다.

3)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_k[T=AUTH1_M::SYSTEM_1

4)AUTH1_M::AuthenticateRESPONDERToINITIATORAgreement_k[T=AUTH1_M::SYSTEM_2

3), 4)는 k를 통해서 Responder와 Initiator가 서로 보안상 문제없이 인증할 수 있는지 검증하는 부분으로 제안한 프로토콜은 서로 안전하게 인증함이 확인되었다.



[Fig. 8] Post-verification status

[Fig. 8]은 프로토콜검증을 완료한 후 상태창으로 검증완료결과 세션간 안전성이 충족되었으며 스텝별로 마무리가 되어 교착상태에 빠지지 않았다. 아울러 무한반복으로 시스템에 문제를 일으키지 않고 검증을 종료하였다.

5. 결론

본 논문에서는 먼저 차량 통신시스템의 개념 및 보안요구 사항에 대하여 확인하였다. 이는 전자 및 자동차산업의 발전과 전자화 되어가는 비율이 증가하는 최근 자동차는 외부공격자의 공격, 전자부품의 내부결함 등에 의한 심각한 피해로 이어지며 나아가 개인의 프라이버시 침해문제도 발생한다. 따라서 통신위협을 보완하기 위해 보안시스템의 적극적 도입이 필요하다.

최근 자동차 통신 분야에서 보안시스템에 많은 연구가 이루어지고 있다. 적용범위도 차대 차, 차대 교통시설, 차 내부 디바이스간 통신 등 그 범위가 다양하게 사용되고 있다. 따라서 공격자의 공격에 안전하도록 보안문제를 해결하기 위해서 하드웨어적 개발, 각종 암호화, 암호프로토콜 등으로 보안적 안전성을 확보하는 다양한 방법의 연구가 활발히 진행 중이다. 본 논문에서는 해시함수에 실시간 에이전트 및 암호화키 값을 이용하고 세션키와 난수를 삽입함으로 매 세션에서 다른 값이 전송되도록 설계하였다.

본 논문에서는 프로토콜을 설계하여 Casper 언어로 명세한 후 제안 프로토콜이 FDR 도구의 보안속성을 만족하는지 검증을 실시하였다. 검증결과 보안적인 측면에서 만족함을 보였다. 본 실험의 결과로 향후 자동차통신에서 보다 안전한 보안환경이 확보될 것이며 개인의 프라이버시 보호에도 안전한 드라이빙 환경이 될 것이다. 향후 무선 통신 및 고속 이동통신 분야에서 효율적이고 안전하게 사용할 수 있는 추가연구를 진행할 예정이다.

REFERENCES

[1] Stephen C., Damon M., Brain K., Danny A., Hovav S., Stefan S., Karl K., Alexei C., Franziska R. and Tadayoshi K., Comprehensive experimental analyses of automotive attack surfaces. SEC, Vol. 11, pp. 1-16, 2011.

[2] P. Papadimitratos, A. de La Fortelle, K. Evensen, R. Brignolo, and S. Cosenza, Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Communications Magazine, Vol. 11, No. 1, pp. 84-95, 2009.

[3] ISO 26262, Road vehicles - Functional safety,

Management of functional safety & Concept phase
[4] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, Securing Vehicular Communications Assumptions, Requirements, and Principles. Workshop on Embedded Security in Cars(ESCAR), Berlin, Germany, 2006.
[5] G. Lowe. Casper: A compiler for the analysis of security protocols. User Manual and Tutorial. Version 1.12, 2009.
[6] Formal Systems(Europe) Ltd, Oxford University Computing Laboratory, Failures-Divergence Renement. FDR2 User Manual, 19th, October 2010.
[7] PRESERVE(PREparing SEcuRe VEhicle-to-X Communication Systems)Deliverable 1.1, Security Requirements of Vehicle Security Architecture. June 2011.
[8] C.A.R Hoare. Communicating Sequential Processes. Prentice-Hall. 1985.
[9] A. Festag, P. Papadimitratos, and T. Tielert, Design and Performance of Secure Geo-cast for Vehicular Communication. IEEE Transactions on Vehicular Technology (IEEE TVT), Vol. 59, No. 5, pp. 1-16, 2010.
[10] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux and J.-Y. Le Boudec, Adaptive Message Authentication for Multi-Hop Networks. IEEE/IFIP International Conference on Wireless On-demand Network Systems and Services (IEEE/IFIP WONS), Bardonecchia, Italy, 2011.

한 명 석(Han, Myoung seok)

- 1995년 3월 ~ 현재 : 아주자동차대학 자동차계열 교수
- 1991년 8월 : 한국항공대학교 항공전자공학과(공학석사)
- 2002년 8월 : 한국항공대학교 항공전자공학과(공학박사)
- 관심분야 : 자동차통신, 자동차전자제어, 자동차센서제어

- E-Mail : mshan@motor.ac.kr

배 우 식(Bae, Woo Sik)

- 1997년 3월 ~ 현재 : 아주자동차대학 전산소
- 2006년 8월 : 백석대학교 정보기술대학원(공학석사)
- 2012년 2월 : 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 관심분야 : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템

- E-Mail : bws@motor.ac.kr