지능형 자동차의 사용자 인증에 대한 위협 및 대응 기법

김승환, 이근호*
백석대학교 정보통신학부

User Authentication Risk and Countermeasure in Intelligent Vehicles

Seung-Hwan Kim, Keun-Ho Lee*
Division of Information Communication, BaekSeok University

요 약 지능형 자동차의 최종 목표는 사고 위험이 전혀 없는 무인 자동차이다. 지능형 자동차의 구현을 위해서는 무선 네트워크 데이터 통신 기술이 중요하다. 본 논문에서는 데이터 통신 기술이 구현이 되었을 때를 가정하여 네트워크 침입 기술에 대해 알아보고, 사용자 인증 및 데이터 위·변조시 그에 따른 보안 취약점과 그에 따른 대응기법을 생체인식 알고리즘 통해 적용하고자 한다. 확실한 사용자 인증 기법과 데이터 전송 기술에 대한 암호화를 통해 더욱 더 안전한 대응 기법을 제안하고자 한다.

• **주제어** : 지능형자동차, 네트워크해킹, 사용자 인증, 보안위협, 대응기법

Abstract Intellgent Vehles network capabilities can cause a lots of security issues such as data hacking, privacy violation, location tracking and so on. Some possibilities which raise a breakdown or accident by hacking vehicle operation data are on the increase. In this paper, we propose a security module which has user authentication and encryption functionalities and can be used for vehicle network system.

• **Key Words** : Intelligent Vehicles, Network hacking, User authentication, Security risk, Countermeasure

1. 서론

국내 교통사고 사망자수는 지속적인 감소추세이긴 하지만 2011년 교통사고 사망자가 무려 5200여명 가량 된다. 이러한 교통사고 사망자 수를 줄이기 위해 현재 자동차 기술과 IT기술을 융합한 지능형 자동차를 개발 중에 있다[1].

지능형 자동차의 최종 목표는 사고 위험이 전혀 없는 무인 자동차인데, 이러한 지능형 자동차는 자동차에 기계, 전자, 통신, 제어, 인공지능, 감성공학, IT 기술을 비롯한 각종 첨단기술을 접목시킨 미래형 자동차를 일컫는다. 예를 들어 차량 사고를 미연에 방지하기 위한 능동안전시스템, 차선이탈경보시스템, 위치측정시스템(GPS)과 인터넷 휴대전화망을 이용한 정보의 실시간 송수신 등 자동차의 안전성과 편의성 그리고 정보화를 획기적으로 향상시킨 미래형 자동차가 바로 지능형 자동차다[2].

현재 국내에선 2010년 11월 5일 현대자동차그룹 자율주행자동차 경진대회를 통해 현재 국내의 지능형 자동차 개발 진행정도를 알 수 있었으며, 2013년에도 국내 대회 일정이 현재 진행 중에 있다. 이러한 대회들을 통해 차에 설치되어 있는 센서들을 통해 장애물을 피하고, 저속주행 차량을 피하고, 자동으로 주차를 하고 횡단보도 및 신호등을 인지하고 정차를 하는 무인 자동차를 만나볼 수 있다.

위의 대회들을 통해서 지능형 자동차는 매우 빠른 속

*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2011년 11월 5일 수정일 2012년 1월 25일 게재확정일 2012년 2월 10일

도로 발전하고 있음을 확인할 수 있다. 물론 여러 가지 제약 조건으로 인해 무인 자동차가 당장 현실화될 수는 없지만 그 근간을 이루는 기술들은 이미 하나씩 연구 개발되고 있다. 지능형 자동차가 발전되고, 상용화되어짐에 따라 그에 따른 사용자 인증 취약점들이 발생하게 된다.

현재 지능형 자동차의 사용자 인증 방식은 자동차 키 하나로만 해결이 되고 있다. 이러한 인증 방식은 자동차 키의 도난·분실 시 차량 도난, 사용자의 개인 정보 등 많은 분실의 경우가 있고 차량의 정보가 이렇게 노출되어 차량으로부터 서버로 내보내는 데이터의 위조·변조가 될 경우, 공격자의 의도에 따라 사용자의 개인정보는 물론 차량의 목적지를 바꾼다거나, 차량 네트워크 내부에 침입해서 의도적으로 사고회피 기술을 마비시켜서 큰 인명 사고를 발생하게 할 가능성도 있다. 차량(호스트)으로부터 내보내는 데이터의 위·변조에 대한 보안 대책과 사용자 인증에 대해 더 많은 연구가 필요 할 것이다.

2. 관련 연구

지능형 자동차란 여러 기술 융합을 통하여 편의성을 획기적으로 향상시킨 자동차라 정의할 수 있다. '지능형'이라는 표현이 매우 넓은 의미를 갖기 때문에 구체적인 기술 또는 기능보다는 추상적인 개념으로 표현한 것이다. 이 안전성과 편의성을 좀 더 구체화하자면 다음과 같은 기술들을 지능형 자동차의 범주에 포함할 수 있을 것이다.

[Table 1] Technology of Intelligent Vehicles

기술 명	내용
예방안전기술	사고가 나지 않도록 사전에 예방하는 기술
사고회피기술	사고가 나더라도 피해를 최소화하기 위해 예방하는 기술
자율주행기술	운전자의 지시만으로 원하는 목적지까지 주행하는 기술
충돌안전기술	충돌 시 피해를 최소화시키기 위한 능동, 수동 안전 기술
편의성 향상 기술	자동 주차, 네비게이션 시스템 등 운전자의 편의성을 지원하는 기술
차량 정보화 기술	차량 자체의 네트워크와 외부 통신을 기반으로 운전자에게 필요한 정보를 실시간으로 전달하는 기술

Table. 1에서 보이는 것은 지능형 자동차에 포함되는 기술들이다. 위의 기술들을 하나하나 언급할 수는 없고, 이 글에서는 차량 정보화 기술에 대해 다루기로 하겠다. 차량 정보화 기술은 차량 자체의 네트워크와 외부 통신을 기반으로 운전자에게 필요한 정보를 실시간으로 전달하는 기본 기능과 IT 산업과 연계한 확장 기능이다[3].

이 글 아래에서는 지능형 자동차의 데이터 통신 기술이 구현 되었을 때를 가정하고 네트워크 환경에서의 침입 기술과 사용자 인증에 대한 취약점 및 대응 기법에 대해서 설명하도록 하겠다.

2.1 네트워크 환경에서의 침입 기술

현재 혼잡 에러 등에 관한 데이터 송·수신문제는 많은 연구를 통해 진행되어지고 있기 때문에 데이터 통신 기술이 구현 되었다고 가정하고, 네트워크의 침입 기술에 대해서 설명하겠다.

네트워크 침입 기술은 여러 가지 기술들이 있지만, 지능형 자동차의 네트워크 통신에 맞춰서 스니핑, 스푸핑, DoS 정도만 나열하도록 하겠다. 스니핑(sniffing)이란 사전적으로 '코를 킁킁거리다', '냄새를 맡다.' 등의 뜻으로 스니퍼는 네트워크상에 흘러다니는 트래픽을 엿듣는 도청장치를 말한다. 스니핑은 수동적(passive)공격이라고도 말하는데 공격할 때 아무 것도 하지 않고 조용히 있기만 해도 충분하기 때문이다. 이러한 스니핑에 대한 대책은 그리 많지 않다. 스니핑 공격은 스니퍼를 설치한 이후에는 매우 쉬우며 네트워크에 별다른 이상 현상을 만들지 않기 때문에 사용자가 이를 인지하기 어렵다. 따라서 네트워크 관리자나 보안 관리자라면 주기적으로 네트워크에 스니퍼가 있는지 탐색해야 한다. 그 다음 스푸핑 공격에 대해서 알아보겠다. 스푸핑(spoofing)이란 '속이다'라는 사전적인 의미를 갖고 있다. 인터넷이나 로컬에서 존재하는 모든 연결에 스푸핑이 가능하다. 스푸핑은 정보를 얻어내는 것 외에 시스템을 마비시킬 수도 있다. 스푸핑 공격에는 ARP 스푸핑, IP 스푸핑, DNS 스푸핑 공격이 있다. APR 스푸핑이란 로컬에서 통신하고 있는 서버와 클라이언트의 IP 주소에 대한 2계층 MAC 주소를 공격자의 MAC주소로 속인다. 그래서 클라이언트에서 서버로 가거나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여, 공격자가 이 패킷을 읽은 후 정상 목적지로 돌려보내 연결이 끊어지지 않도록 유지하는 공격이다.

IP 스푸핑이란 트러스트 관계가 맺어진 서버와 클라이언트를 확인한 후 클라이언트에 DoS 공격을 하여 연결을 끊는다. 그런 후 공격자가 클라이언트의 IP 주소를 확보하여 서버에 실제 클라이언트처럼 패스워드 없이 접근하는 공격이다. 여기서 트러스트 관계란 시스템을 용이하게 관리할 목적으로 개발되었는데, 트러스트 관계에 있으면 시스템에 접속할 때 자신의 IP주소로 인증을 하고 로그인 없이 접속을 가능하게 만든 것이다.

DNS 스푸핑이란 공격 대상이 특정 웹에 로그인할 경우, 같은 형태의 도메인 이름으로 접근한다. 도메인 이름은 IP주소로 변환되어야 실제 접속이 가능하기 때문에 DNS 서버에 도메인 이름에 대한 IP 주소를 물어본다. 이때 공격자는 도메인 이름에 대한 이름 해석 패킷, 즉 DNS Query 패킷을 탐지하고 실제 DNS 서버보다 빨리 공격 대상에서 DNS Response 패킷을 보내 공격 대상이 잘못된 IP 주소로 이름 해석을 하도록 하여, 잘못된 웹 접속을 유도하는 공격이다.

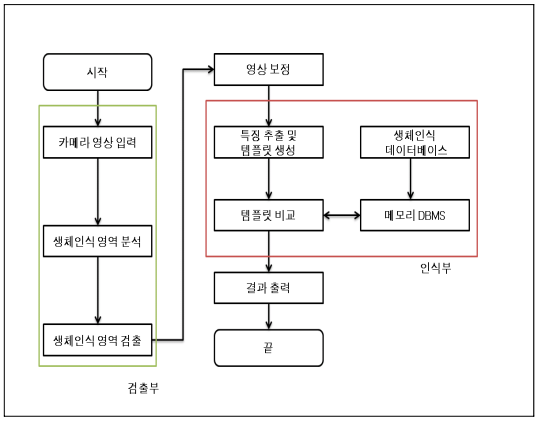
마지막으로 DoS(Denial Of Service) 공격은 다른 해킹에 비해 비교적 간단하다. 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나, 사용자 또는 네트워크의 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격인데 DoS공격은 Ping of Death, SYN Flooding, Land 공격 등이 있다.

Ping of Death공격은 ping을 이용하여 ICMP 패킷을 정상 크기보다 아주 크게 만드는 공격으로, 크게 만들어진 패킷은 네트워크를 통해 라우팅 되어 공격 네트워크에 도달하는 동안 아주 작은 조각으로 쪼개지고 공격 대상은 조각화된 패킷을 모두 처리해야 하므로 정상적인 ping보다 부하가 훨씬 많이 걸리게 되는 공격이다. SYN Flooding공격은 네트워크에서 서비스를 제공하는 시스템은 동시 사용자 수가 제한되어 있는데, SYN Flooding은 존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 하는 것이다. Land공격은 Land의 사전적인 뜻은 '(나쁜상태에)빠지게 하다' 라는 의미 그대로 시스템을 나쁜 상태에 빠지게 하는 것이며, 방법도 아주 간단하다. 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소 값을 똑같이 만들어서 공격 대상에 보내는 것인데, 이때 조작된 IP 주소 값은 당연히 공격대상의 IP 주소여야 한다. SYN Flooding처럼 동시 사용자 수를 점유해버리며, CPU 부하까지 올리는 공격이다. 이러한 공격들을 전부 막을 수는 없겠지만, 최대한 대응할 수 있는 대응 기법들에 대해서 설명하겠다.

3. 보안취약점 및 대응 기법

지능형 자동차의 보안 취약점으로는 사용자 인증을 하는 방법이 너무 단순화되어있고, 지능형 자동차로부터 보내는 데이터를 공격자가 의도대로 위조, 변조 하게 될 경우에 사용자가 원하는 목적지에 도달할 수 없을 것이고, 고속도로에서 차가 멈춘다거나 할 경우에 대형 사고가 발생 할 가능성이 매우 크다. 그리고 현재 자동차들은 자동차 키 또는 리모콘 키 하나만으로 사용자 인증을 하기 때문에 키의 도난, 분실 등의 경우 차량 분실, 사용자의 개인정보 등 많은 분실의 우려가 있고, 지능형 자동차의 경우에는 차량의 정보가 노출 될 경우, 공격자가 임의로 차량을 제어할 수 있기 때문에 인명사고의 위험도 있다.

따라서 이에 대한 대응방안으로는 자동차 키를 통해 차의 문을 열 수 있는 현재의 방식에 시동을 걸기 전 생체인식(얼굴, 홍채, 지문 등)을 한번 더 함으로써, 사용자 인증을 보다 확실하게 할 수 있다.

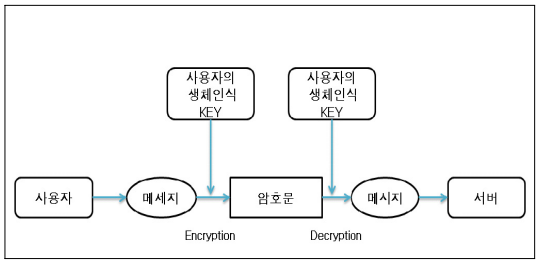


[Fig. 1] Biometrics Algorithm

위의 Fig. 1은 간단한 생체인식 알고리즘인데, 먼저 사용자의 생체인식 정보를 카메라에 입력하면 카메라는 생체인식을 영역별로 분석 및 검출 한 후, 특징을 추출한다. 이렇게 추출한 특징으로 탬플릿을 생성하고 기존 데이터베이스에 저장된 템플릿과 비교해서 사용자 인증을 하게 된다.

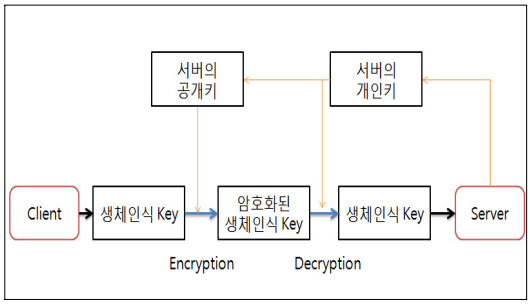
이렇게 해서 얻은 생체인식의 Key값은 대칭키 방식을 사용해서 Fig. 2처럼 사용자가 서버로 보내는 패킷에 암

호화를 하고, 서버는 생체인식 Key값으로 암호화된 패킷을 복호화함으로서, 데이터의 무결성을 유지한다.



[Fig. 2] Symmetric Cryptography

그리고 암호화 방식에서 대칭키 방식을 선택한 이유는 대칭키 방식은 공개키 방식에 비해서 패킷의 전송속도가 빠르기 때문에 전송속도가 중요한 지능형 자동차의 무선네트워크에서 실용적으로 사용될 것이다. 이러한 암호화 방식을 통해 공격자가 스푸핑 공격을 하더라도 패킷 자체에 암호화를 함으로써 노출 된 데이터를 원본으로 되돌릴 수 없게 한다. 그리고 이렇게 생성된 Key값은 서버와 사용자가 공유를 해야 하는데, 공유를 하는 방식으로 Fig. 3와 같은 공개키 방식을 사용해서 공유를 한다.



[Fig. 3] Public-key Algorithm

대칭키를 공유하는 과정에서 공개키 방식을 사용하는 이유는, 대칭키보다 공개키 방식이 조금 더 신뢰성, 안전성이 높기 때문이다. 그 이유로는 자물쇠를 예로 들 수 있는데, 자물쇠는 누구나 잠금이 가능하지만 키를 갖고 있는 사람만 자물쇠를 열 수 있다. 따라서 키를 공유할 때, 생체인식 Key값을 서버의 공개키로 암호화를 시키면 암호화된 생체인식 Key값은 서버의 개인키만으로 복호화가 가능하기 때문에 서버만 생체인식 Key값을 열람할 수 있다.

그러나 사용자의 생체인식 Key(공유키)가 공격자의 스니핑 공격을 통해 노출이 될 경우 데이터의 암·복호화가 가능하기 때문에 네트워크 관리자나 보안 관리자라면 주기적으로 네트워크에 스니퍼가 있는지 탐색해야 한다. 그리고 마지막 DoS공격에 대한 대응방책으로는 안정적인 네트워크 설계를 해야한다. 안정적인 네트워크 설계 방법은 여러 가지이다. 라우터로 일정량 이상의 패킷이 들어올 경우, 그 이상의 패킷을 통과시키지 않거나 백업 서버를 운영하는 것도 좋은 방법이고, 침입 탐지 시스템(IDS) 또는 침입 차단 시스템(IPS)를 설치하며 시스템에 패치를 하는 것만으로도 DoS공격의 대부분은 차단이 된다.

4. 보안 검증

이 장에서는 지금까지 제안한 지능형 자동차의 사용자 인증에 대한 위협 및 대응 기법을 정보보안의 3요소에 맞춰서 안전성과 그에 따른 이유를 살펴보도록 하겠다.

[Table 2] Security Verification for Countermeasure

정보보안 3대 요소(CIA)	안전성 여부
기밀성(Confidentiality)	안전함
무결성(Integrity)	제공함
가용성(Availability)	제공함

(1) 기밀성(Confidentiality) : 기밀성이란 허가받지 않은 자가 정보를 읽지 못하도록 하는 것이다. 본 논문에서 사용자의 Fig. 1을 통해 사용자 인증을 하기 때문에 생체 인식 정보를 데이터베이스에 저장하지 않은 사용자에 대한 접근은 허가되지 않기 때문에 데이터의 기밀성을 유지할 수 있다.

(2) 무결성(Integrity) : 무결성이란 허가되지 않은 자가 정보에 다른 내용을 기록할 수 없게 하여 그 정보의 원본을 보호하는 것이다. 3장 보안 취약점 및 대응기법에서 Fig 2, Fig. 3을 통해 사용자 인증을 할 때 사용했던 생체인식 정보의 Key값으로 데이터 전송 시 원본의 데이터를 암호화함으로써 무결성을 제공한다.

(3) 가용성(Availability) : 가용성이란 허가된 사용자가 데이터에 접근하려 할 때 이것이 방해받지 않도록 하는 것이다. 3장에서 언급한 것처럼 대칭키 방식은 공개키 방식보다 패킷의 전송속도가 빠르

고, 데이터의 혼잡제어에 도움을 주고 있기 때문에 직접적인 영향은 주지 않지만, 간접적으로 가용성을 제공하고 있다.

5. 결론

지능형 자동차의 기술 발전은 자동차 안전 분야에 대한 운전자의 관심과 요구가 증가함에 따라 세계 각국이 이러한 기술들에 대한 연구를 진행해 왔다. 그리고 운전자의 안전과 편의를 위한 차량의 전자화는 차량 정보시스템, 안전 시스템, 차량 네트워크 시스템 등에서 급속도로 발전하고 있다. 현재 이 글에서 언급한 네트워크 관련 기술 외에도 차량 기술 등이 융합되어 구현되고 있다. 이러한 기술들이 발전을 해서 최종 목표인 사고 위험이 전혀 없는 무인자동차가 개발되어 상용화가 될 경우. 미래에 안전한 교통수단으로써 우리의 삶에 많은 변화를 가져 올 것이다. 안전하고 신뢰성 높은 기술의 구현하기 위해 무선 네트워크상의 데이터 통신 기술 및 그에 따른 네트워크 보안 취약점에 관한 기술의 연구·개발이 필요하며 이로 인해 현재보다 더 안전하고 편리한 사회가 실현되기를 바란다.

감사의 글

“이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2012-0003141)”

REFERENCES

[1] Traffic Accident Analysis System URL : http://taas.koroad.or.kr/index.jsp

[2] Myoungho Sunwoo, Dohyun Jung “The Concept and Technologies of Intelligent Vehicle”, 2005

[3] In-Beom Yang “Technologies of intelligent Vehicles”, KATECH

[4] Dae-Il Yang “Information security outline and practice(Network hacking and security)”, Hanbit Media, 2012.

[5] Korea Information Security Agency “Guideline for Test and Evaluation of Facial Recognition Algorithm”, 2008.

저자소개

김 승 환(Seung-Hwan Kim) **[학생회원]**

· 2008년 3월 ~ 현재 : 백석대학교 정보통신학부 재학

<관심분야>
정보보안, 사용자 인증, 네트워크

이 근 호(Keun-Ho Lee) **[종신회원]**

· 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
· 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
· 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야>
M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호