|  |
| --- |
| https://lh5.googleusercontent.com/B47gv9nQ5_TX1uXPhlnxR_mw4_i6hRtYoWRBceJrd0IGeGh6qrYBK7l5Yx46Vx6Nr8e-kndYAveAB3GFyJelSW6hY3CFObQzv8LyB6WuRrf8V1VqWgvARHSFG_1H9PWU25ECbsdR제목 |
|  |

**보고서명:** 기말과제보고서

**제출일**: 20. 12. 06

**과목명**: 정보보호이론 2분반

**담당 교수님**: 우사무엘 교수님

**전공**: 소프트웨어학과

**학번**: 32154579

**이름**: 차성민

목차

1. 사이버보안 사고 사례 분석

1-1 사고 사례 소개

1-2 사고 사례 분석

1-3 해결 방안 제시

1. 자동차 내부 네트워크 보안 기술 설계

2-1 자동차 내부 네트워크(CAN)의 취약점

2-2 자동차 내부 네트워크(CAN)의 취약점 제거를 위한 방법

2-3 자동차 내부 네트워크(CAN)를 위한 정보보호 기능 설계

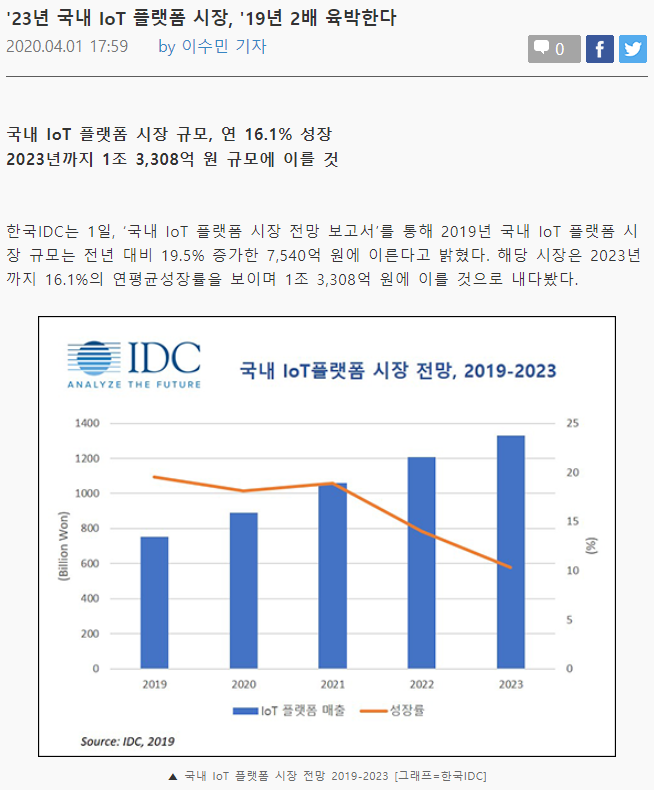
1. 자동차 외부 네트워크 보안 기술 설계

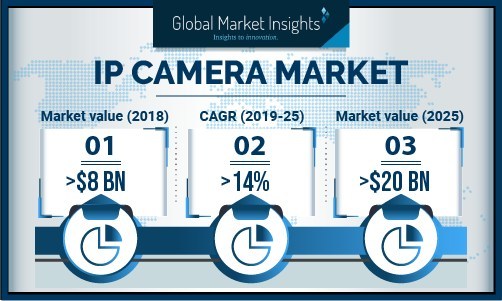
3-1 Keyless entry system의 취약점

3-2 Keyless entry system의 취약점 제거를 위한 방법

3-3 Keyless entry system를 위한 정보보호 기능 설계

1. 윤리적 딜레마
2. 참고 문헌 및 사이트 목록
3. 사이버보안 사고 사례 분석
   1. 사고 사례 소개

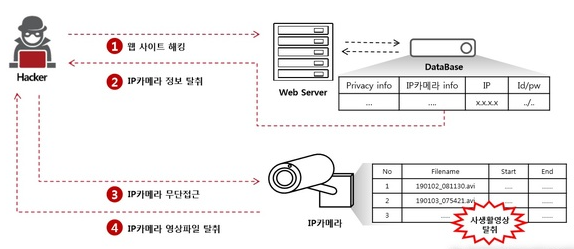
테이블이(가) 표시된 사진

자동 생성된 설명사례 명: **IP 카메라 해킹 사고들(IoT 해킹)**

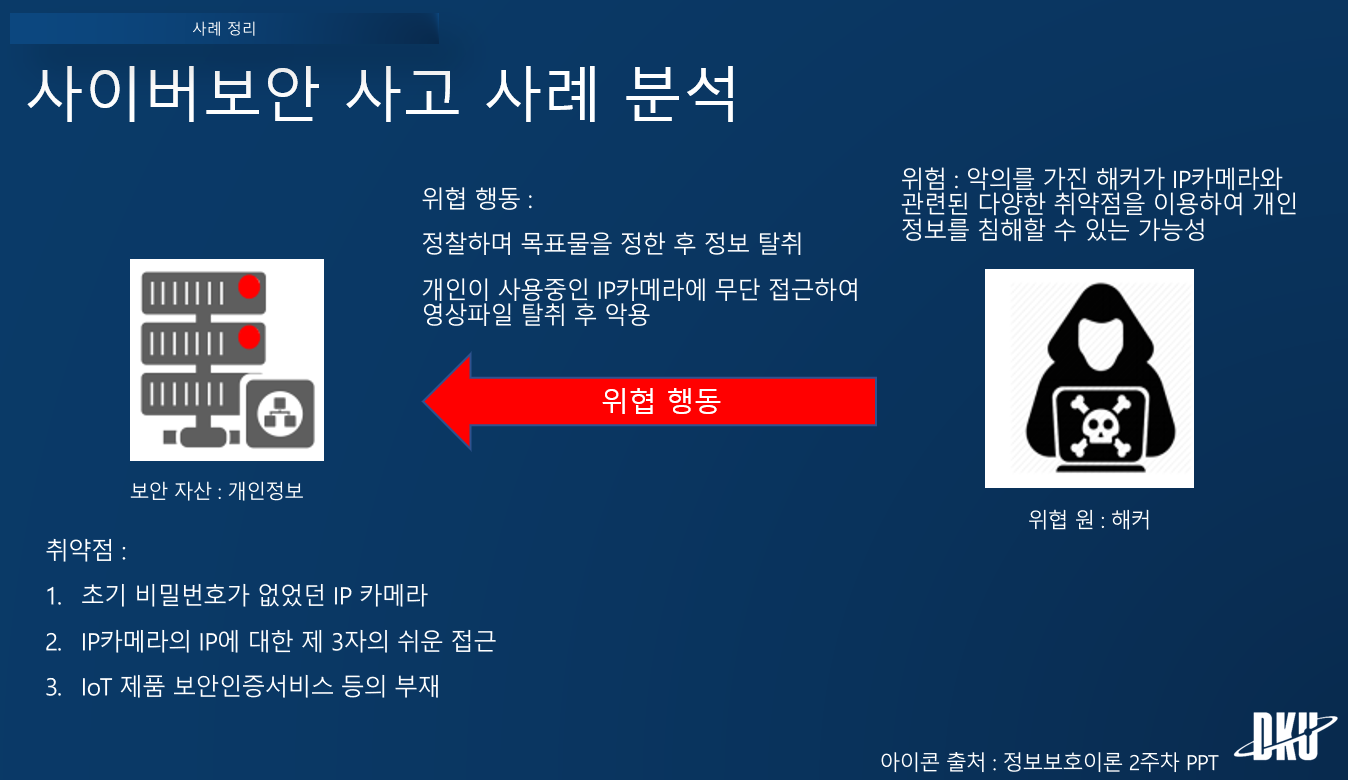
* 배경 설명: 네트워크의 발전으로 인하여, IoT 장비들의 사용이 보편화 됨에 따라 집에 다양한 IoT 장비들이 설치가 되고 있지만, IoT 장비들의 보안은 크게 주목받지 못하였고, 그에 따라 여러 IoT 해킹 사례가 발생하고 있다. 그 중 가장 사람들의 사생활을 침해하는 부분인 IP 카메라 해킹 사고 사례들에 대하여 분석을 하게 되었다.

텍스트이(가) 표시된 사진

자동 생성된 설명

* 대표적인 공격 방법: 먼저, 공격자는 IP카메라 관련 웹 사이트를 둘러보며 충분한 정찰을 하며 목표물(IP카메라)를 정한 후 웹 사이트를 해킹하여 특정 IP카메라에 대한 정보들(카메라 정보, IP, ID/PW 등)을 탈취한다. 그 후 개인이 사용중인 IP카메라에 수집한 정보들을 활용하여 무단 접근하여 IP카메라의 영상파일을 탈취하여 목적을 달성하고 영상을 악용한다.

1-2 사고 사례 분석



* 보안 자산: 보안 자산이란 개인정보 및 기업의 기밀 정보이고, 유형 및 무형의 상태를 가지는데, 이번 사례에서의 보안 자산은 무형 자산인 개인의 사생활 영상, 즉 개인정보이다.
* 취약점: 취약점이란, 시스템을 위협의 영향에 노출시키는 시스템의 약점인데, 이번 사례에서의 취약점들은 다음과 같다. 초기 비밀번호가 설정되어 있지 않았던 IP카메라, IP카메라의 IP에 대한 제 3자의 쉬운 접근, IoT 제품 보안인증서비스 등의 부재(현재는 존재함.).
* 위협원과 위협행동: 위협원은 어떠한 목적을 가지고 위협을 수행하거나 그 원인이 될 수 있는 활동을 수행, 지원하는 사람이나 조직으로 정의되는데, 이번 사례에서의 위협원은 남의 사생활에 관심이 있는 해커이다. 위협행동은 피해를 입힐 의도로 목표 대상에 취한 모든 조치인데, 이번 사례에서의 위협행동은 위의 1-1 부분에 적은 대표적인 공격 방법의 내용들이다.
* 위험: 위험이란 외부의 위협이 내부의 취약성을 이용하여 보유한 각종 자산에 피해를 입힐 수 있는 잠재적인 가능성을 말하는데, 이번 사례에서는 악의를 가진 해커가 IP카메라와 관련된 다양한 취약점을 이용하여 개인정보를 침해할 수 있는 가능성을 뜻한다.

위 상황에서 적절한 보안조치를 통해 취약점을 제거하고, 보안 위험을 줄일수가 있는데 그 방안은 1-2에서 제시한다.

* 1. 해결 방안 제시

1. 보안 자산은 무엇인가?

* 보안 자산: 무형 자산인 개인의 사생활 영상, 즉 개인정보.

1. 보안 목적은 무엇인가?

* 보안 자산인 IP카메라 사용자들의 개인정보를 위협원의 위협행동으로 안전하게 보호하기 위함.

1. 보안 요구사항은 무엇인가?

* 사용자 데이터의 암호화(기밀성)
* 사용자 인증을 통한 접근 제어(인증)
* 변조되지 않은 메시지 전송(무결성)
* 사용자가 보낸 메시지에 대한 부인방지(부인방지)

1. 보안 조치는 어떻게 할 것인가?

* 기밀성: 대칭 키 기반의 데이터 암호화를 사용하고, 운용모드는 ECB가 아닌 다른 모드를 사용하고, 키 관리는 공개키 방식을 사용하여 관리하여 해결할 것.

암호화에는 크게 대칭키와 공개키 두가지 방식이 존재하는데, 공개키는 각각이 자신의 개인키만 관리를 하기 때문에 키 관리에 유리하고, 대칭키는 시프트 연산 같은 간단한 연산을 사용하기 때문에 속도측면에서 장점이 있다. 그렇기에 대칭 키 기반의 데이터 암호화를 사용하여 암호화를 진행하며 키 관리만 공개키 방식을 사용하여 관리할 것이다.

추가로, 대칭 키 기반의 암호화의 운용모드 중 ECB 운영 모드는 각 블록이 독립적으로 암복화가 이루어지기 때문에 병렬처리가 가능하 지만 이로 인해 블록 간의 독립성으로 블록 단위의 패턴이 유지가 되기 때문에 ECB 모드는 패턴 분석을 하면 취약하다는 단점이 존재한다. 그렇기에 운용모드는 ECB가 아닌 CBC 등의 모드를 사용할 것이다.



대칭 키 암호 기법과 공개키 암호기법 비교 출처: 정보보호이론 9주차ppt

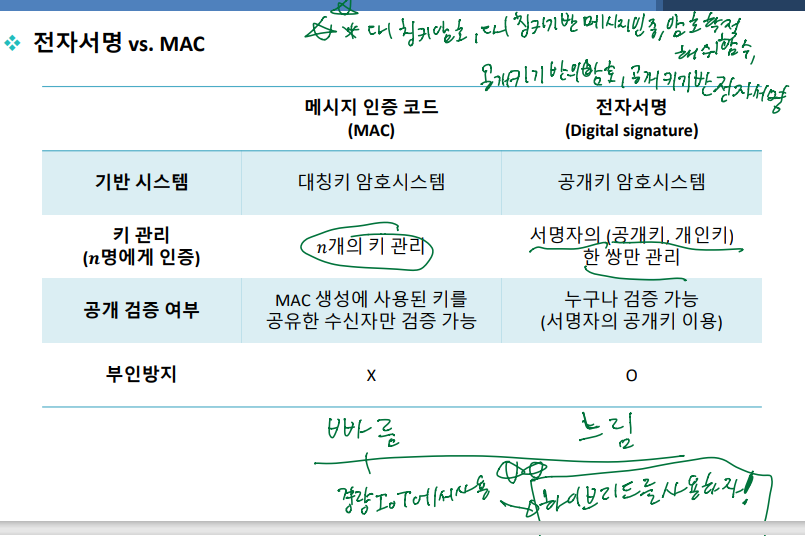
* 인증: 인식, 소유, 신체특징기반 중 하나를 선택한 후, 이 개체 인증을 통한 접근 제어를 통해 해결할 것.

개체의 신원을 증명하기 위한 개체 인증에는 크게 인식기반, 소유기반, 생체기반 이렇게 3가지 인증 방식이 존재한다. IP카메라는 주로 어플리케이션을 통해 제어가 되기 때문에 패스워드 같은 인식 기반 방식이나 지문 같은 신체특징기반 개체 인증을 사용할 것이다.

* 무결성, 부인방지: 변조되지 않은 메시지 전송과 부인방지는 해시 함수를 사용하여 메시지의 길이를 줄인 전자서명을 통해서 해결할 것.

전자서명은 메시지 출처 인증과, 부인방지, 그리고 메시지 무결성을 제공한다. 하지만, MAC과의 비교가 필요한데, 대칭 키 암호 방식을 사용하는 MAC은 빨라서 경량IoT에서 사용하지만 부인 방지 기능이 없다. 반면, 전자서명은 공개키 암호 방식을 사용하고, 키 관리에 유리하지만, 메시지의 길이가 긴 경우가 많기도 하고, 처리 속도도 느린 편이다.

나는 위사실들을 토대로 부인방지가 되는 전자서명을 사용하면서, 메시지의 길이를 줄일 수 있는 해시 함수를 사용하여 처리 속도를 향상시키는 하이브리드 방식을 이용할 것이다.



전자서명과 MAC비교 표 출처: 정보보호이론 9주차ppt

1. 보안 조치를 위한 또 다른 보안 목적은 안 생기는가?

* 개체 인증을 거친 후 메시지를 주고받게 되는 시점에 IP카메라 사용자 간 권한을 다르게 부여해야 할 일이 있을 경우(아이들과 어른들의 열람 권한을 다르게 부여해야 한다는 등)에는 어떻게 할 것인가? (인가 목적)

: 인가란 주체가 하고자 하는 작업이 허가된 작업인지 확인하고 권한을 부여하거나 제어하는 것이다. 인가의 접근 제어의 요소에는 주체, 접근제어, 객체, 접근 이렇게 4가지가 존재한다.

인가를 위한 접근 제어 기술도 ACL, ACM, MAC, RBAC 이렇게 4가지가 존재하는데, IP카메라 사용자 간의 권한을 다르게 부여해야 할 경우에는 역할별로 권한을 부여하는 RBAC를 사용하여 해결할 수 있다.

1. 자동차 내부 네트워크 보안 기술 설계

2-1 자동차 내부 네트워크(CAN)의 취약점

CAN의 취약점은 CAN네트워크가 브로드캐스트 환경이라 누군가 통신하면 모두가 볼 수 있기 때문에 아래와 같은 문제가 발생할 수 있다는 것이다.

1. 인증 또는 접근 제어 메커니즘이 없다.

* CAN 버스에 연결된 모든 장치가 규칙없이 읽기/쓰기를 수행하는 것이 이 때문.

1. 공격자가 절대로 CAN 버스에 대한 무단 액세스를 얻지 못한다는 가정이 되어 있다.

* 이로 인해 시스템 내에서 CAN 버스의 모든 데이터는 신뢰되기 때문에 진짜 오류 메시지와 위협원들로 인해 만들어진 가짜 오류 메시지를 구별할 수 없다. (데이터의 기밀성 X)

CAN통신의 취약점 출처: 12주차 pdf



2-2 자동차 내부 네트워크(CAN)의 취약점 제거를 위한 방법

근본적인 해결을 위해서는 보안을 고려하여 새로운 CAN 버스를 만드는 것이 가장 좋지만, 규격을 바꾸는 것은 어려운 일이기 때문에 물리적으로는 아래와 같은 노력을 할 수 있다.

1. 버스 전류에 추가된 새로운 전원 드레인을 감지하여 악의적인 장치를 알리는 시스템 또는 프로그램을 구축하고 만든다.
2. OBD-2 포트가 물리적으로 존재하기 때문에, 이 부분에 추가적인 하드웨어 키나 암호화를 해주어 포트를 통한 CAN 유입을 방지한다.
3. 새로운 네트워크 토폴로지를 만들어 중요 기능은 따로 분리를 하던가 다양한 CAN 서브 버스를 만들어 오류가 특정 시스템들에 영향을 끼칠 수 없도록 한다.

보안 목적에 맞는 보안 조치는 아래에서 다룰 것이다.

* 1. 자동차 내부 네트워크(CAN)를 위한 정보보호 기능 설계

1. 보안 자산은 무엇인가?

보안 자산: 자동차 내부 네트워크 중 가장 많이 쓰이는 CAN이다. CAN의 보안이 취약하여 위협원들의 위협행동에 뚫린다면 운전자에게 치명적인 영향을 끼칠 수 있다.

CAN의 특징은 아래와 같다.

* 동기 시간에서의 Multicast Reception (CDMA/CA)이라 네트워크 설계가 쉽다.
* 다양한 CAN Controller/Transceiver 선택이 가능해 저렴한 가격이다.
* 메시지 식별자 (Identifier)에 의한 우선 순위(Priority) 설정이 가능하다.
* 송신자는 고유한 ID(식별자)를 가진다
* 메시지 충돌 시 고유한 ID를 기반으로 우선순위 결정한다
* 송신자 ID 기반의 브로드캐스트 통신 프로토콜이라 통신 회선에 접속한 누구나 통신 내용 확인 가능하다.

1. 보안 목적은 무엇인가?

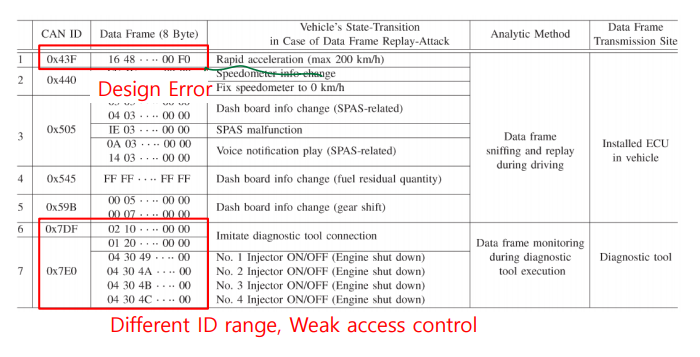
운전자의 생명과도 관계 있는 자동차 내부 네트워크(CAN)를 안전하게 지키면서, 동시에 차량 내부라는 특수 환경에 걸맞게 빠르게 처리가 가능한 보안체계를 확립하여야 한다.

1. 보안 요구사항은 무엇인가?

* 사용자 데이터의 암호화(기밀성)
* 메시지 인증을 통한 접근 제어(무결성)
* 메시지 인증에 사용되는 키 관리 (키 관리)

1. 보안 조치는 어떻게 할 것인가?

* 기밀성: CAN 프레임 ID 필드를 대칭 키 기반의 데이터 암호화를 사용하고, 운용모드는 ECB가 아닌 다른 모드를 사용하여 해결할 것.

CAN의 특징에서 알 수 있듯, 송신자는 고유한 ID를 가지고 공격자는 이를 분석하여 공격을 할 수 있기 때문에 CAN 프레임 ID 필드를 암호화하는 것이 필요하다. 그리고, 자동차의 특성상 빠른 처리가 필요하기 때문에 공개키 기반보다는 DES나 AES같은 대칭 키 기반의 데이터 암호화를 사용하고, 대칭 키 기반의 암호화의 운용모드 중 ECB 운영 모드는 각 블록이 독립적으로 암복화가 이루어지기 때문에 병렬처리가 가능하지만 이로 인해 블록 간의 독립성으로 블록 단위의 패턴이 유지가 되기 때문에 ECB 모드는 패턴 분석을 하면 취약하다는 단점이 존재한다. 그렇기에 운용모드는 ECB가 아닌 CBC 등의 모드를 사용할 것이다.

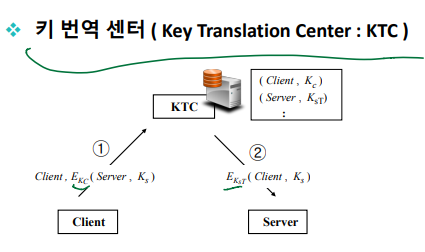
CAN ID를 통해 특정 기능을 조작하기 위한 공격을 준비할 수 있다.

**그렇기에 CAN 프레임 ID 필드를 암호화해줘야 한다. 참고: 13주차 PDF**

* 무결성: 기존의 메시지 인증 방식에 재전송공격에 대비하여 Timestamp값이나 challenge response값 등을 추가로 주어지게 하여 메시지 인증을 한다. 더 나아가 해시 함수를 활용하여 공격에 걸리는 시간을 증가시켜 해결할 것.

자동차 내부의 네트워크 이므로 빠른 처리속도를 위하여 공개키 암호화 방식의 전자 서명보다는 대칭 키 암호화 방식의 메시지 인증방식을 이용해야 한다. 그렇지만 기존의 메시지 인증 방식은 재전송공격을 막을 수 없다. 그렇기에 Timestamp값 혹은 challenge response 값 등을 활용하여 메시지 인증을 진행해야 한다. 추가로, 해시 함수를 통해 일정한 길이로 출력이 되도록 하여 위협원들이 공격에 걸리는 시간을 증가시킨다.

* 키 관리: 메시지 인증에 사용하는 키의 관리가 중요하기에 키 분배 단계에서 알맞은 설정을 진행한 후 차량 내부 네트워크에 가장 적합한 분배 방법인 KTC 방식으로 키를 분배해줌으로써 키를 관리하여 해결한다.

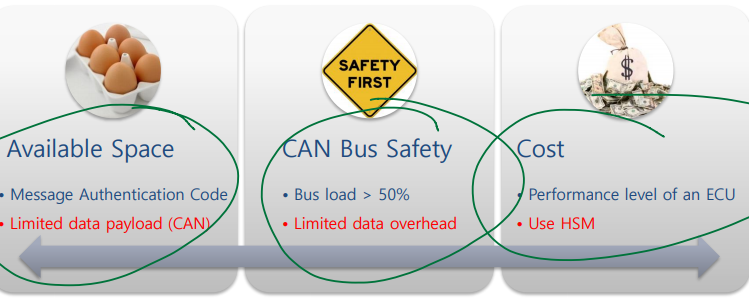
메시지 인증을 진행할 때, 키를 활용하는데 이 키의 관리가 매우 중요하다. 키는 생성, 분배, 저장, 취소, 갱신, 폐기 및 보관 등 다양한 프로세스를 거치는데, 특히 인증과정에서 사용하는 키는 키 분배 단계에서 설정을 해줘야 하는데, 마스터키를 이용하여 long-term 키를 만들고, 이를 기반으로 인증 키를 만들어 준다. 이후, 인증 키를 이용하여 short-term 키를 만들고, 이를 기반으로 세션 키를 만들어 주는 과정을 거친다. 이후 세션 키 설정을 한 후, 자동차 내부 네트워크는 UVO, bluelink 등 하나의 주체에 의해 관리가 되기 때문에 이에 걸 맞는 분배 방법인 KTC방식으로 분배를 해준다.

KTC 분배 방식이다. 자동차 네트워크에서는 UVO 등이 KTC의 역할을 수행한다.

**출처: 11주차 pdf**

1. 보안 조치를 위한 또 다른 보안 목적은 안 생기는가?

* CAN이 대중화가 될 수 있었던 큰 이유가 저렴한 가격이었기에, 경제 요소들 또한 보안과 더불어 고려할 수밖에 없기에 경제적인 목적이 발생한다. (가용성)

: CAN의 가용 데이터량와 안전을 위한 버스의 로드 율, 그리고 차에 탑재되는 ECU장비의 성능에 따라 달라지는 가격을 보안 요소들과 함께 고려를 해줘야 한다.

가용 데이터량은 메시지 인증과, 버스의 로드율은 보안과 기타 요소들의 전체적인 버스 사용량과,

가격은 특히 탑재되는 ECU장비의 성능과 관계가 있다. 출처:12주차 pdf

3. 자동차 외부 네트워크 보안 기술 설계

3-1 Keyless entry system의 취약점

키 리스 시스템, 흔히들 원격 키 리스 시스템이라 부르는 RKS(이하 RKS)는 전자 리모컨을 키로 사용하여 휴대용 장치에 의해 작동되거나 근접에 의해 자동으로 작동되는 잠금을 뜻한다. 특히나 자동차에 광범위하게 사용되는 RKS는 물리적인 접촉 없이 표준 자동차 키의 기능을 수행한다.

RKS의 취약점은, 13주차 수업시간에서도 ETH Zurich University의 해킹 사례에서도 볼 수 있었듯 LF RFID기술을 이용하여 전자 리모컨으로부터 쉽게 신호를 캐치하고, 더 나아가 100m ~ 400m가량의 상당한 원거리에 있는 키의 신호를 Relay하여 제어가 가능한데, 기본적으로 더 나은 보안을 제공하지 않고 있다는 점이다. 또한, 암호화를 진행하여도 신호 자체를 가져가기 때문에 기밀성과 무결성을 지키기가 어렵다.



RKS의 취약점을 이용하여 차를 절도하는 과정

3-2 Keyless entry system의 취약점 제거를 위한 방법

RKS의 취약점 제거를 위한 방법으로는 스티어링 잠금 장치나 휠 클램프와 같은 물리적인 장치를 추가적으로 장치하거나, RKS에 새로운 보안 조치를 취하는 방법이 있다. 전자의 물리적인 장치를 추가하는 것은, 편리하기 위해 사용하는 RKS에 오히려 불편함을 더하는 꼴이라 후자의 방법으로 RKS의 취약점을 제거하기 위한 보안 조치를 만들어야 한다.

휠 클램프의 모습.

3-3 Keyless entry system를 위한 정보보호 기능 설계

1. 보안 자산은 무엇인가?

* 보안 자산: 자동차와 운전자. 자동차의 제어가 제3자를 통해 이루어 진다면 운전자의 생명과도 직결될 수 있기 때문에 특히나 신경 써야 한다.

1. 보안 목적은 무엇인가?

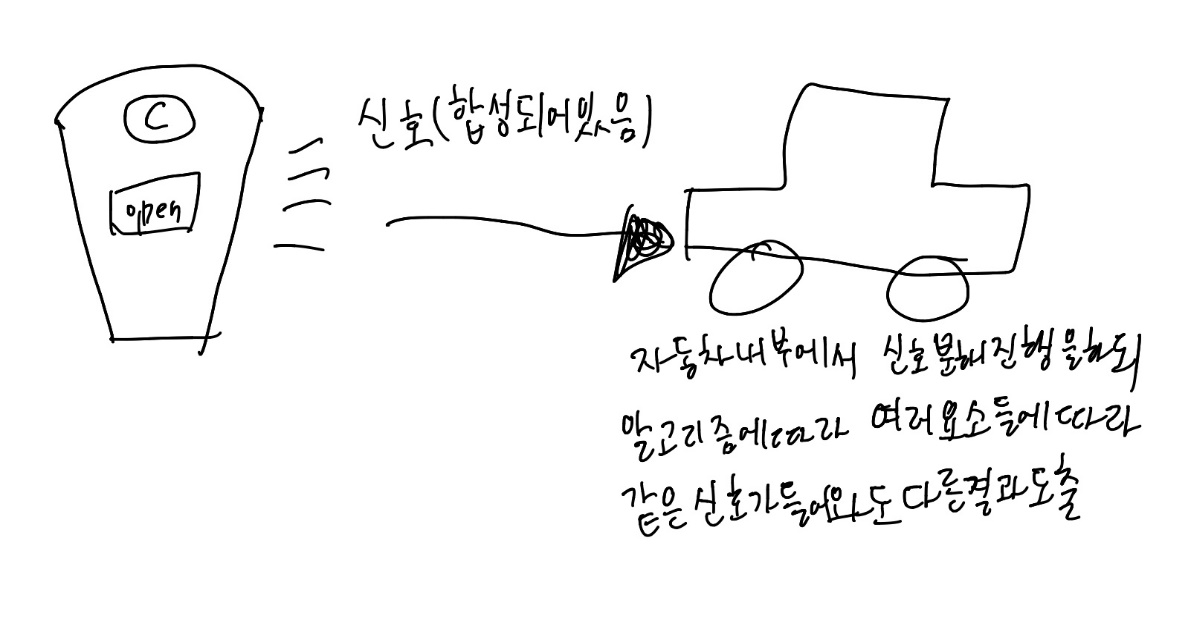
* 운전자의 생명과도 관계 있는 자동차 외부 네트워크의 부족한 인증 문제 등을 해결하여 운전자를 안전하게 지키면서, 동시에 RKS를 쓰는 이유인 필요할 때 언제든 서비스를 편리하게 이용할 수 있어야 한다는 가용성에 초점을 맞춘 보안체계를 확립하여야 한다.

1. 보안 요구사항은 무엇인가?

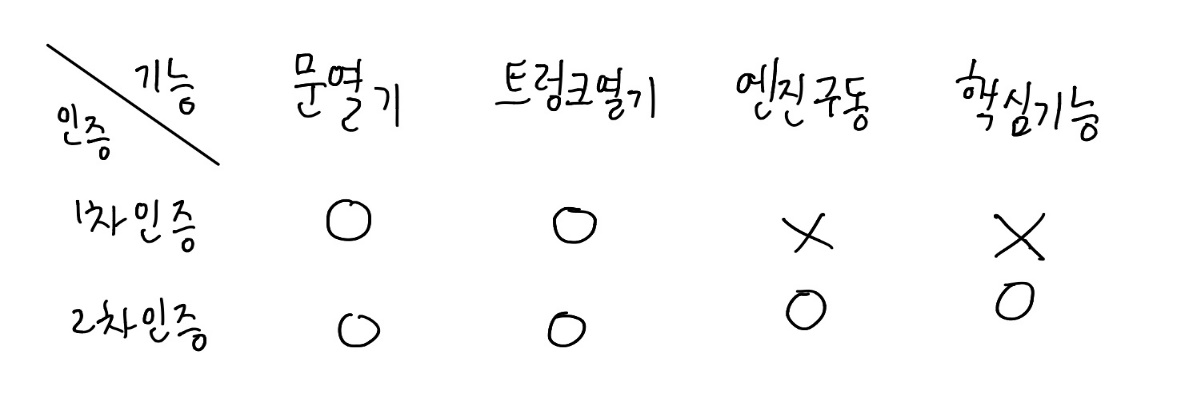
* RKS 신호 데이터의 합성응용(기밀성)
* 운전자 인증과 인가(인증)
* 필요할 때 사용할 수 있는 RKS(가용성)

1. 보안 조치는 어떻게 할 것인가?

* 기밀성: 신호의 합성을 활용하여 동일 키에서 나오는 신호여도 자동차 내부에서의 처리기관에서 소리 분해를 미리 짜인 알고리즘에 따라 진행하여 다른 결과값이 나오게 한다.

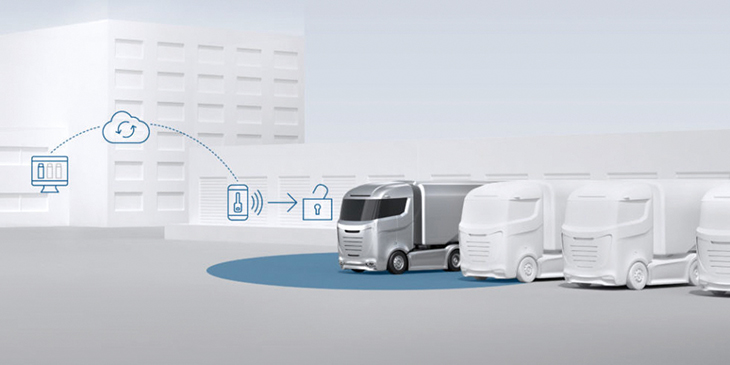
기존 신호 데이터의 기밀성을 지키기 위해서는 전자파차단 파우치나 알루미늄 호일 등으로 감싸 전자파를 차단하는 물리적인 방법이나 신호를 합성하고 자동차 내부에서 미리 짜인 알고리즘을 토대로 소리 분해를 진행하여 같은 전자파여도 접근 순서나 기타 다른 요소들에 따라 결과 값이 다르게 나오게 만들어 기밀성을 확보한다.

* 인증과 인가: 사용자 인증을 위해 신체특징기반 개체 인증을 사용한 2차 인증을 추가하고, 키와 2차 인증을 ACM 인가 조치에 따라 인증했을 때의 권한을 다르게 부여하여 핵심적인 활동을 하기 위해서는 2차 인증이 필요하도록 할 것이다.

단순히 키만으로는 운전자임을 인증할 수 없기 때문에 2차 인증 과정을 추가하고 각각의 단계에 따라 ACM 인가 조치를 취해 줄 것이다. 개체의 신원을 증명하기 위한 개체 인증에는 크게 인식기반, 소유기반, 생체기반 이렇게 3가지 인증 방식이 존재한다. 요즘 자동차에는 지문 인식 장비가 들어갈 수 있기 때문에 지문 같은 신체특징기반 개체 인증을 사용할 것이다. 2차 인증을 진행 하여야만 운전 등 핵심기능을 조종 및 제어할 수 있고, 평소의 키로는 문 열기 및 트렁크 관리와 같은 악용의 소지가 크지 않은 기능들을 사용이 가능하게 하여 보안을 향상시킬 수 있다.

인증 단계에 따른 기능 권한 ACM

* 가용성: 클라우드 기반 관리 시스템을 구축한 후, 핸드폰 어플리케이션과 NFC를 통하여도 안전하고 필요할 때 언제든 자동차에 접근할 수 있도록 구축한다.

현재 유행하고 있는 카쉐어링 서비스에서 사용하는 방법처럼, 보다 가용성을 높이기 위해서 단순히 키의 형태를 벗어나 클라우드 기반 관리 시스템을 토대로 스마트기기안에서의 조작을 통해 인증을 거친 후 제어가 가능하게 하고, 스마트 기기가 배터리가 없는 상황에서는 NFC를 통하여 제어가 가능하도록 하여 관련 문제 발생에도 대비를 한다.

클라우드 기반 플랫 매니지먼트 시스템 원리 출처: 보쉬

1. 보안 조치를 위한 또 다른 보안 목적은 안 생기는가?

* 보다 나은 가용성을 제공하기 위해 클라우드 기반의 시스템을 구축함에 따라 최근 특히나 유행하는 공격인 서비스 거부 공격에 대비하여 통신만 인터셉트 기능을 준비한다.

: 가용성 관련하여 최근 Dos 공격이 많아졌기 때문에 이를 대비하여 존재하지 않은 IP에서의 SYN 패킷 요청은 서버로 도달하지 못하게 하는 통신망 인터셉트 기능을 사용하여 서비스 거부 공격으로 인해 사용자들이 피해를 보지 않도록 대비한다.

1. 윤리적 딜레마

상황만 본다면 당시 상황에서 가장 책임소재가 큰 3번 10명이 있는 쪽으로 돌진하여야 한다는 것이 제 생각입니다만, 그 이전에 위와 같은 상황이 생기지 않도록 하는 것이 가장 중요하다고 생각합니다.

점차 바뀌어 가고 있는 무단횡단 사망 사고의 책임의 소재처럼 자율주행 자동차 사고 관련 제도를 충분한 공론화를 통하여 확실하게 마련하여 각 상황에서의 매뉴얼을 만들고, 일반 사람들의 무단횡단 관련한 인식을 바꾸는 것에 노력을 많이 해야 합니다.

또한, 자율주행 자동차가 자주 지나다니는 도로에는 실시간으로 도로 상황과, 문제 발생가능성이 있는 상황을 지켜보며 상황 발생시 빠르게 자율주행 자동차와 통신하여 보다 빠르게 자율주행 자동차가 잘 대응을 할 수 있도록 도와주는 시스템이 구축된다면 본 상황과 같은 사고를 보다 줄일 수 있을 것이라 생각합니다.

1. 참고 문헌 및 사이트 목록
2. 사이버보안 사고 사례 분석:

<https://www.e4ds.com/sub_view.asp?ch=1&t=0&idx=11556> – IoT 전망

<https://www.prnewswire.com/news-releases/ip-camera-market-to-cross-usd-20-bn-by-2025-global-market-insights-inc-300884454.html> - IP카메라 시장 전망

<https://www.sedaily.com/NewsVIew/1VQR9YSB83> - IoT장비 전망과 IoT보안 구멍관련

<https://itinformation.tistory.com/121> - 사례 참고 사이트 1

<https://newsis.com/view/?id=NISX20190201_0000548603> – 참고 사이트2

<https://news.joins.com/article/21950524> - 참고 사이트3

<https://www.itfind.or.kr/WZIN/jugidong/1914/file3018578133064757102-191401.pdf> -

5G 시대의 차세대 IoT 보안

1. 내부 네트워크 보안

<http://www.automotivereport.co.kr/news/articleView.html?idxno=1459> – CAN 표준의 취약점

1. 외부 네트워크 보안

<https://www.koreascience.or.kr/article/CFKO201714956117073.pdf> - 차량용 스마트키 취약점 분석과 해킹공격 대응방안

<https://patents.google.com/patent/KR101734947B1/ko> - 스마트 키 시스템 및 상기 시스템에서의 해킹 방지

<https://en.wikipedia.org/wiki/Remote_keyless_system> - Keyless entry system

<http://nara.kosmes.or.kr/mobile/view.html?sid=176&aid=5595&page=1&from=list> – 진화하는 자동차 보안기술

<https://peemangit.tistory.com/210> ㅡ Dos 공격법과 방어법