홈·가전 IoT 보안가이드

2017. 7

IoT 보안얼라이언스 Internet of Trust

홈가전 IoT 보안가이드

2017. 7

IoT 보안얼라이언스

홈·가전 IoT 보안가이드

CONTENTS

홈·가전 IoT 보안가이드

제1장 개요

제1절 배경 및 필요성
제2절 목적 및 구성

제1장
개요

제1절 배경 및 목적

IDC 조사에 따르면, 세계 사물인터넷(Internet of Things, 이하 IoT) 시장은 2017년 현재 8천억 달러 규모에서 2021년에는 1조 4천억 달러 규모로 성장할 것으로 전망되며, 보안 하드웨어 및 소프트웨어 시장도 각각 연평균 15.1% 및 16.6% 성장할 것으로 예상[1]된다. 국내 IoT 시장은 2017년 4월말 기준으로 7,367억 원 규모[2]에서, 2020년에는 17조 1천억 원 규모로 무려 연평균 38.5% 성장할 것으로 전망[3]하고 있다. 그리고 세계 스마트홈 시장은 2020년까지 약 430억 달러 규모로, 국내 시장은 약 13억 2천만 달러(약 1조 5천억 원) 규모로 성장할 것으로 예측하였다. 국내외 IoT 산업의 급격한 성장과 비례하여 IoT 기반의 다양한 제품 및 서비스에 대한 보안위협 역시 급격히 증가할 것으로 예상되며, 이에 따라 글로벌 IT 리서치 기관인 가트너에서는 전 세계 IoT 보안 지출 규모가 2018년에는 5억 4,700만 달러에 달할 것으로 예측하였다.

이와 같은 IoT 산업의 성장을 지원하기 위해 미국, 유럽, 일본, 중국 등 각 나라에서는 IoT 산업 육성 및 활성화 정책과 더불어 사이버 공격으로부터 안전한 서비스 제공을 위한 IoT 정보보호 정책을 추진하고 있다.

국내에서는 2009년 10월, 방송통신위원회가 최초로 IoT 분야의 국가경쟁력 강화 및 서비스 촉진을 위한 '사물지능통신 기반구축 기본계획'을 발표한 데 이어 2013년 6월, 과학기술정보통신부에서 IoT를 인터넷

1 IDC Worldwide Semiannual Internet of Things Spending Guide, 2016H2

2 http://www.newstomato.com/ReadNews.aspx?no=757487

3 사물인터넷(IoT) 관련 유망산업 동향 및 시사점(현대경제연구원, 16-24(통권 662호), 2016.7.11)

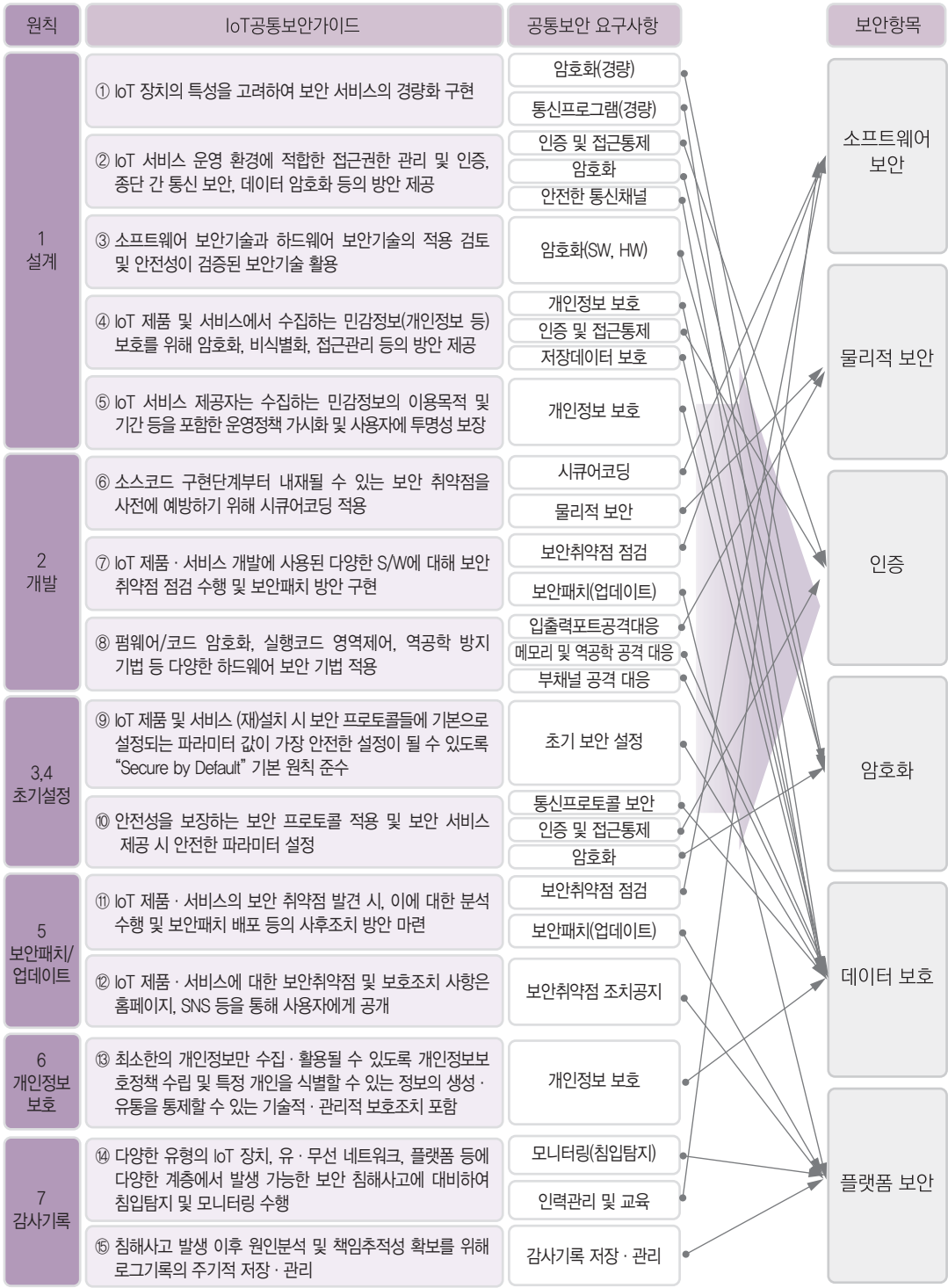
신산업분야의 주요 기술로 선정하고 이에 따른 중장기 발전계획인 '인터넷 신산업 육성방안'을 발표하였으며, 2014년 5월에는 정부관계부처 합동으로 '초연결 디지털혁명의 선도국가 실현을 위한 IoT 기본계획' 을 발표하였다.

또한, IoT 위협의 범국가적 대응을 위해 같은 해 10월, '사물인터넷 정보보호 로드맵'을 수립하고, ICT와 산업 간 융합으로 인해 발생 가능한 안전위협에 대응하기 위해 'K-ICT 융합보안 발전전략'을 2016년 4월 발표하였다.

IoT 정보보호 로드맵에 따라, IoT 제품의 보안내재화를 위해 IoT 하드웨어와 소프트웨어 전반에 걸쳐 준수해야 할 7개의 보안원칙을 제시한 'IoT 공통 보안원칙' 이 2015년 6월 발표되었다. 이에 따라 ICT 융합 제품 및 서비스 설계 시 개발자 등이 자율적으로 활용 가능한 'IoT 공통보안 가이드' 가 이듬해 9월 개발되었으나 IoT 공통보안 가이드는 특정 제품에 맞춘 설명을 제공하지 않기 때문에 분야별로 세분화된 가이드 제공이 필요하였다.

본 가이드에서는 IoT 공통보안 가이드의 공통보안 요구사항을 소프트웨어 보안, 물리적 보안, 인증, 암호화, 데이터 보호, 플랫폼 보안 등 6가지 보안항목으로 분류하고 IoT 제품 개발자 및 제조사들이 개발단계부터 보안을 고려하여 안전하게 개발할 수 있도록 요구사항을 구체화하여, 실제 구현에 활용할 수 있도록 보안요구사항을 세부적으로 설명하였다.

• IoT공통보안가이드 보안항목과 홈·가전 IoT 보안가이드의 연관관계 •



제2절 가이드 목적 및 구성

목적	– 홈 · 가전 IoT 제품 개발자 및 제조사가 개발 단계에서부터 보안을 고려하여 안전하게 개발할 수 있는 가이드 제공
대상	– 홈 · 가전 IoT 제품 개발자 및 제조사
범위	– 스마트TV, 스마트 냉장고, 디지털 도어락, 월패드, 공유기 · 게이트웨이 등 실생활에 사용되고 있는 홈 · 가전 IoT 제품 * 기술발달 수준에 따라 향후 범위 확대
구성	**– 제1장 개요** 제1절 배경 및 필요성 제2절 목적 및 구성 **– 제2장 주요 보안 위협** **– 제3장 보안항목 구분** 제1절 제품 유형 및 보안요구사항 제2절 보안항목 제3절 제품 유형별 필요기능 **– 제4장 공통 보안항목 및 대응방안** 제1절 소프트웨어 보안 제2절 물리적 보안 **– 제5장 유형별 보안항목 및 대응방안** 제1절 인증 제2절 암호화 제3절 데이터보호 제4절 플랫폼 보안
활용	**(개발자)** 자체적으로 보안 취약점 진단 및 개선조치 시 활용 **(시험자)** 보안취약점 보유여부 진단 및 개선권고 시 활용 **(기타)** 홈 · 가전 IoT 제품 보안취약점에 대한 이해수준 제고

홈·가전 IoT 보안가이드

제2장 주요 보안위협

제2장

주요 보안위협

스마트홈이란 주거 환경에 ICT를 융합하여 국민의 편익과 복지증진, 안전한 생활이 가능하도록 하는 인간 중심적인 스마트라이프 환경을 말한다. 이러한 스마트홈 인프라는 가전제품들과 센서 등이 이종의 유무선 네트워크 및 프로토콜로 연결되어 있으며, 이를 위한 운영체제(OS) 및 소프트웨어들이 혼재되어 있다. 따라서 스마트 홈에 사용되는 홈 · 가전 IoT 제품은 컴퓨팅 능력, 네트워크 연결 등을 필요로 하며, 이로 인해 기존 가전제품과 달리 다양한 보안 위협이 존재한다. 최근 발생한 홈 · 가전 IoT 제품 관련 보안사고는 다음과 같다.

• 최근 홈 · 가전 IoT 제품 관련 보안사고 동향 •

2010 4월 트렌드넷의 웹 기반 모니터링카메라 단말기인 시큐어뷰어가 촬영한 동영상이 온라인 상에 노출되는 사건 발생

펌웨어 업데이트 버전 상용화 시 고객의 로그인 계정 정보를 인터넷상으로 평문으로 전송하면서 동영상을 전송저장하여 발생. 또한 트렌드넷 전용 모바일 앱이 고객의 로그인 정보를 지속적으로 단말기에 저장하여 보안에 취약한 구조임

2013 8월 美 라스베이거스에서 스마트TV에 탑재된 카메라를 해킹해 사생활 영상 유출 시연

2014 1월 보안서비스업체프루프포인트는 '13년말부터 '14년초까지 10만대 이상의 스마트 TV, 스마트 냉장고 등 가정용 장비에 감염된 Thingbots을 통해 총 75만건 이상의 피싱과 스팸 메일 발송됐다고 발표

3월 보안컨설팅 업체인 Team Cymu는 해커들이 D-Link, Tenda, Micronet, TP-Link 등이 제조한 약 30만 개의 공유기를 해킹했다고 경고

9월 블랙펄 시큐리티는 로봇청소기 원격조종을 위해 필요한 앱의 인증방식 취약점과 로봇 청소기에 연결되는 AP의 보안 설정상 취약점 등을 악용하여 로봇청소기에 탑재된 카메라로 실시간 모니터링 가능에 대해 해킹 시연 (ISEC 2014)

2014 ~ 2016 2014년에 CIA는 英 MI5와 함께 개발한 것으로 보이는 TV 악성코드(Weeping Angel)를 해킹에 활용하여 TV전원을 끄더라도 방에서 들리는 소리를 수집한 뒤 인터넷을 통해 CIA서버로 전송하거나, TV에 저장된 WIFI 비밀번호를 복구하는 방식으로 WIFI 사용자 이름과 비밀번호를 해킹

2017 3월 스위스 보안 업체는 디지털 비디오 방송-지상파(DVB-T) 수신기가 해킹코드가 삽입된 신호를 수신하면, TV에 내장된 웹브라우저의 취약점을 이용해 권한을 탈취하여 기능 제어 가능 발표
(스마트TV 관련 시중 제품의 85% 이상이 방송전파를 이용한 해킹에 노출)

홈 · 가전제품 등 일상생활로 IoT 서비스가 확산되면서 PC 외에도 가정용 무선공유기를 비롯해 냉난방 공조장비 등 인터넷에 연결된 모든 제품(IoT)에 대한 공격이 현실화되었다. 분산서비스거부(DDoS) 공격은 가정에서 주로 많이 쓰는 무선 공유기가 대상이 되는데, 보통 이러한 무선 공유기는 기본적인 보안 솔루션인 안티바이러스도 설치되지 않을 뿐 아니라 관리 주체도 불분명하다. 게다가 대부분의 사용자는 무선 공유기 초기 설정을 변경하지 않은 상태로 사용한다. 최근 무선 공유기 해킹 사고가 빈발하면서 일부 제조사가 보안을 강화하고 있지만 여전히 대부분의 가정이 사이버 위협에 노출된 상태다. IoT 시대에는 인터넷에 연결되는 제품이 기하급수적으로 늘어나므로 인터넷에 연결되는 냉장고, 청소로봇 등 모든 홈 · 가전 IoT 제품이 해킹 대상이 될 수 있다. 또한 IoT 제품은 일반 ICT 시스템과 달리 보안기술을 적용하기 어려워 상대적으로 보안에 취약하다는 문제점이 있다.

홈 · 가전 IoT 제품 유형별 주요 보안위협은 다음과 같다.

• 제품 유형별 주요 보안위협 •

유형	주요 제품	주요 보안위협	주요 보안위협 원인
멀티미디어 제품	스마트TV, 스마트 냉장고 등	• PC 환경에서의 모든 악용 행위 • 카메라/마이크 내장 시 사생활 침해	• 인증 메커니즘 부재 • 강도가 약한 비밀번호 • 펌웨어 업데이트 취약점 • 물리적 보안 취약점
생활가전 제품	청소기, 인공지능 로봇 등	• 알려진 운영체제 취약점 및 인터넷 기반 해킹 위협 • 로봇청소기에 내장된 카메라를 통해 사용자 집 모니터링	• 인증 메커니즘 부재 • 펌웨어 업데이트 취약점 • 물리적 보안 취약점
네트워크 제품	홈캠, 네트워크 카메라 등	• 사진 및 동영상을 공격자의 서버 및 이메일로 전송 • 네트워크에 연결된 홈캠 등을 원격으로 제어하여 임의 촬영 등 사생활 침해	• 접근통제 부재 • 전송데이터 보호 부재 • 물리적 보안 취약점
제어제품	디지털 도어락, 가스밸브 등	• 제어기능 탈취로 도어락의 임의 개폐	• 인증 메커니즘 부재 • 강도가 약한 비밀번호 • 접근통제 부재 • 물리적 보안 취약점
	모바일 앱(웹) 등	• 앱 소스코드 노출로 IoT 제품 제어기능 탈취	• 인증정보 평문 저장 • 전송데이터 보호 부재
센서 제품	온/습도 센서 등	• 잘못된 또는 변조된 온 · 습도 정보 전송	• 전송데이터 보호 부재 • 데이터 무결성 부재 • 물리적 보안 취약점

홈·가전 IoT 보안가이드

제3장 보안항목 구분

제1절 제품 유형 및 보안요구사항
제2절 보안항목
제3절 제품 유형별 필요기능

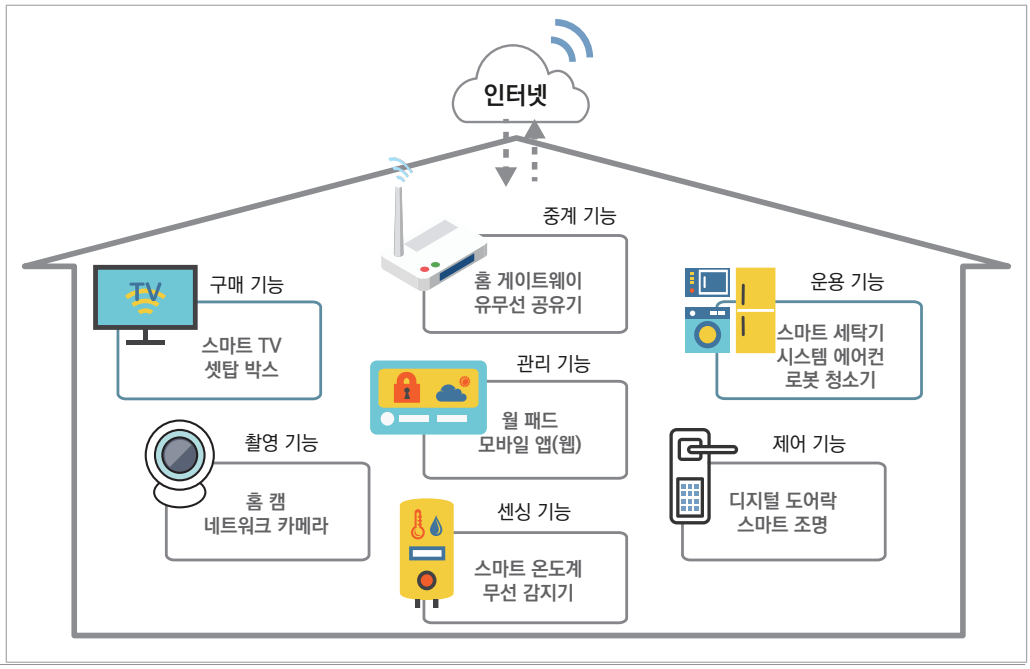
제3장

보안항목 구분

제1절 제품 유형 및 보안요구사항

홈 · 가전 IoT 제품은 지능화된 가전제품이 네트워크를 통해 서로 연결되어 정보를 공유하므로 소비자에게 새로운 가치를 제공한다. 제품에 장착된 센서는 댁내의(집 내부) 빛, 온도, 동작, 습도 등의 정보를 수집하며, 이러한 정보를 이용하여 난방, 보안, 조명 시스템 등을 거주자에게 알맞게 조정하여 쾌적한 환경을 제공한다. 또한 컴퓨터나 스마트폰과 같은 장치를 이용하여 언제 어디서든 인터넷을 통해 제품을 모니터링 및 제어할 수 있다.

• 홈 · 가전 IoT 제품 유형 예시 •



이러한 홈 · 가전 IoT 제품은 집안에 설치된 홈 · 가전제품(부록2 참조)이 무선 네트워크 통신을 기반으로 제공하는 기능 및 서비스에 따라 다음과 같은 유형으로 분류할 수 있으며, 제품의 특성에 따라 2개 이상의 유형에 포함될 수 있다.

유형	세부 설명	대상제품
센싱	**(정의)** 열, 빛, 온도, 압력, 습도 등 여러 종류의 물리적인 양이나 변화를 감지, 검출하거나 판별, 계측한 정보를 전송하는 제품 **(보안성)** 센싱 정보의 무결성 및 진위 여부, 인가된 수신자 **(보안위협)** 센싱 정보 위 · 변조, 위장	스마트온도계 등 센서
제어	**(정의)** 등록된 센서로부터 전송된 정보 또는 인가된 사용자의 조작 명령에 따라 통제하고 조정하는 제품 **(보안성)** 제어 명령어의 무결성 및 진위 여부, 인가된 사용자 접근, 인증정보 기밀성 및 무결성 **(보안위협)** 제어 명령어 위 · 변조, 위장, 인증정보 유출 · 도용	디지털 도어락, 스마트 전력 차단기, 스마트 조명 스위치 등 제어 제품
중계	**(정의)** 홈 네트워크의 댁내망과 사업자망을 상호 접속하거나 중계하는 제품으로, 홈 · 가전 IoT 제품의 송 · 수신 데이터를 중계하는 역할 수행 **(보안성)** 홈 · 가전 IoT 제품으로 송신하는 데이터의 기밀성 및 무결성, 송수신 데이터 저장 금지, 인가된 송 · 수신자, 정책설정을 위한 인가된 사용자 접근, 인증정보 기밀성 및 무결성 **(보안위협)** 중계 데이터 유출 및 위 · 변조, 위장	홈게이트웨이 등 네트워크 제품
구매	**(정의)** 양방향 통신을 기반으로 홈쇼핑 또는 영화 등 컨텐츠 구매 기능을 제공하는 제품 **(보안성)** 인가된 사용자 접근, 구매에 필요한 중요 정보(인증정보, 개인정보, 금융정보 등)의 기밀성 및 무결성 **(보안위협)** 중요정보 위 · 변조, 위장	스마트TV, 셋탑박스 등 구매 기능을 제공하는 제품
촬영	**(정의)** 댁내에 설치된 네트워크 카메라를 통하여 영상을 촬영하여 저장하거나 촬영한 영상정보를 네트워크 통신채널로 전송하는 제품 **(보안성)** 개인영상(정지영상 포함)의 기밀성, 인가된 사용자의 저장 영상 접근, 인가된 수신자, 인증정보 기밀성 및 무결성 **(보안위협)** 개인영상 유출, 위장	홈캠(웹캠) 등 영상촬영 제품
관리	**(정의)** 네트워크 통신을 이용하여 다양한 유형의 홈 · 가전 IoT 제품을 관리(설정 · 조회 · 제어 등)하는 제품 **(보안성)** 등록된 관리대상 제품(센싱, 제어 등 유형 제품), 인가된 사용자 접근, 인증정보 기밀성 및 무결성 **(보안위협)** 위장, 보안설정 임의 변경	월패드, 모바일 앱(웹) 등 관리기능 제공 제품
운용	**(정의)** 홈 · 가전제품의 고유 기능을 수행하는 제품으로 네트워크에 연결되어 원격으로 관리 가능 **(보안성)** 인가된 사용자 접근 **(보안위협)** 위장, 임의 접근 · 사용	스마트 냉장고, 스마트 세탁기, 시스템 에어컨 등

홈 · 가전 IoT 제품은 다음과 같은 세부 보안요구사항을 만족해야 한다. 홈 · 가전 IoT 제품이 제품 개발 및 관리 시 적용해야 하는 공통 보안항목으로는 소프트웨어 개발보안, 물리적 보안이 있으며, 각 보안항목에 대한 보안요구사항은 아래 표와 같다.

유형	소프트웨어 개발보안	물리적 보안
센싱	• 시큐어코딩 • 알려진 보안약점 및 취약점 제거 • 최신 3rd party 소프트웨어 사용	• 물리적 인터페이스 차단
제어		
중계		
구매		
촬영		
관리		
운용		

홈 · 가전 IoT 제품이 기능 및 서비스 측면에서 고려해야 하는 유형별 보안항목으로는 인증, 암호화, 데이터 보호, 플랫폼 보안이 있으며, 각 보안항목에 대한 보안요구사항은 다음과 같다.

유형	인증	암호화	데이터 보호	플랫폼 보안
센싱	• IoT 제품 간 상호인증	• 안전한 암호 알고리즘 사용 • 안전한 암호키 관리	• 안전한 통신채널 • 저장 및 전송 데이터 보호	• 안전한 업데이트
제어	• 인증 및 접근통제 • IoT 제품 간 상호인증	• 안전한 암호 알고리즘 사용 • 안전한 암호키 관리	• 안전한 통신채널 • 저장 및 전송 데이터 보호	• 설정값 및 실행코드 무결성 검증 • 안전한 업데이트 • 감사기록
중계				
구매			• 안전한 통신채널 • 저장 및 전송 데이터 보호 • 개인정보 보호	
촬영				
관리				
운용		• 안전한 암호 알고리즘 사용 • 안전한 암호키 관리	• 안전한 통신채널	• 안전한 업데이트 • 설정값 및 실행코드 무결성 검증(권고)

제2절 보안항목

홈 · 가전 IoT 제품의 하드웨어 및 소프트웨어 개발 단계에 공통적으로 적용되어야 하는 공통 보안항목과 홈 · 가전 IoT 제품의 기능적 유형에 따라 차등적으로 적용해야 할 보안항목을 다음과 같이 구분하였다.

공통 보안항목은 개발단계에서 공통적으로 요구되는 항목이며, 유형별 보안항목은 제품이 가진 기능적 유형 및 다루는 정보의 중요도에 따라 선별적으로 요구되는 보안항목이라고 볼 수 있다.

공통 보안항목 • 소프트웨어 보안, 물리적 보안

유형별 보안항목 • 인증, 암호화, 데이터보호, 플랫폼 보안

가. 보안항목

1) 공통 보안항목

홈 · 가전 IoT 제품은 공통적으로 다음과 같은 보안속성을 고려해야 한다.

유형	소프트웨어 보안	물리적 보안
센싱	보안취약점의 원인이 제거된 안전한 소프트웨어 개발 보안패치가 적용된 최신 3rd party 라이브러리 사용	물리적 인터페이스에 대한 인가된 사용자 접근
제어		
구매		
촬영		
중계		
운용		
관리		

2) 유형별 보안항목

홈 · 가전 IoT 제품별 주요 기능을 기반으로 요구되는 보안항목은 다음과 같다.

유형	인증	암호화	데이터 보호	플랫폼 보안
센싱	인가된 수신자 센싱 정보 진위성	무결성	센싱 정보 무결성	안전한 업데이트
제어	인가된 사용자 접근, 제어 명령어 진위성	기밀성, 무결성	제어 명령어 무결성 인증정보 기밀성 · 무결성	안전한 업데이트 제어기능 관련 주요 설정값 · 실행코드 무결성 제어기능 수행 적절성 추적
구매	인가된 사용자 접근	기밀성, 무결성	중요정보 기밀성 · 무결성	안전한 업데이트 구매기능 관련 주요 설정값 · 실행코드 무결성 구매기능 수행 적절성 추적
촬영	인가된 사용자의 저장 영상 접근 인가된 수신자	기밀성, 무결성	개인영상(정지영상 포함) 기밀성 인증정보 기밀성 · 무결성	안전한 업데이트 촬영기능 관련 주요 설정값 · 실행코드 무결성 영상접근 수행 내역 추적성
중계	인가된 송 · 수신자 인가된 사용자 접근	기밀성, 무결성	송 · 수신데이터 기밀성 · 무결성 송수신데이터 저장 금지 인증정보 기밀성 · 무결성	안전한 업데이트 중계기능 관련 주요 설정값 · 실행코드 무결성 중계기능 수행 적절성 추적
운용	인가된 사용자 접근	–	–	안전한 업데이트 운용기능 관련 주요 설정값 · 실행코드 무결성
관리	등록된 관리대상 제품 인가된 사용자 접근	기밀성, 무결성	인증정보 기밀성 · 무결성	안전한 업데이트 관리기능 관련 주요 설정값 · 실행코드 무결성 관리기능 수행 내역 추적성

나. 보안항목별 보안위협

각 보안항목별로 해당되는 보안요구사항 및 보안위협은 다음과 같다.

보안항목	보안요구사항	관련 주요 보안위협
소프트웨어 보안	• 시큐어코딩 • 알려진 보안취약점 점검 및 제거 • 최신 3rd party 소프트웨어 사용	• 소프트웨어 결함 등 보안약점으로 인한 보안취약점 원인 제공 • 알려진 보안취약점 악용 • 3rd party 소프트웨어의 보안취약점 악용
물리적 보안	• 물리적 인터페이스 차단	• 물리적 보안 취약
인증	• 인증 및 접근통제 • IoT 제품간 상호 인증	• 인증 메커니즘 부재 • 강도가 약한 비밀번호 • 접근통제 부재
암호화	• 안전한 암호 알고리즘 사용 • 안전한 암호키 관리 • 안전한 난수 생성 알고리즘 사용	• 취약한 암호알고리즘 • 취약한 암호키 길이 • 낮은 엔트로피
데이터 보호	• 안전한 통신채널 • 저장 및 전송 데이터 보호 • 개인정보 보호	• 전송데이터 보호 부재 • 인증정보, 암호키, 개인정보 등 중요정보 평문 저장
플랫폼 보안	• 설정값 및 실행코드 무결성 검증 • 안전한 업데이트 • 감사기록	• 데이터 무결성 부재 • 펌웨어 업데이트 취약점 • 보안사고 추적 불가능

다. 보안항목별 해당 제품

각 보안항목별로 해당되는 제품은 다음과 같다.

보안항목		해당 제품
소프트웨어 보안	시큐어코딩	프로그램이 가능한 제품
	알려진 보안취약점 점검 및 제거	프로토콜, API, 패키지, 오픈소스 등과 펌웨어 또는 운영체제를 사용하는 제품
	최신 3rd party 소프트웨어 사용	펌웨어 또는 운영체제 및 애플리케이션 소프트웨어에 3rd party 소프트웨어를 사용하는 제품
물리적 보안	물리적 인터페이스 차단	외부에 인터페이스(USB, RS232, 메모리카드 포트 등 외부접근포트)가 존재하거나, 개발 및 고장 수리 등을 위해 외부기구(예, 외부 덮개 등)를 해체 후 내부 PCB에 메모리 및 MCU[4]에 접근 가능한 포트가 존재하는 제품
인증	인증 및 접근통제	유 · 무선접속, 제품 설치시 인증이 필요한 제품
	IoT 제품간 상호인증	IoT 제품 간 연결 시 인증이 필요한 제품
암호화	안전한 암호 알고리즘 사용	민감 정보를 저장하거나 IoT 제품 간 통신 시 암호화 통신이 요구되는 제품
	안전한 암호키 관리	민감 정보를 저장하거나 IoT 제품 간 통신 시 암호화 통신이 요구되는 제품
	안전한 난수 생성 알고리즘 사용	암호키 생성, 분배, 상호 인증 등 안전한 난수 사용이 요구되는 제품
데이터 보호	안전한 통신채널	IoT 제품 간 암호화 통신이 요구되는 제품
	저장 및 전송 데이터 보호	IoT 제품 간 암호화 통신이 요구되며, 고유식별정보, 금융정보, 신체식별정보, 식별코드, 사진 등 개인정보를 처리 · 저장 · 전송하는 제품
	개인정보보호	고유식별정보,금융정보,신체식별정보,식별코드,사진 등 개인정보를 처리 · 저장 · 전송하는 제품
플랫폼 보안	설정값 및 실행코드 무결성 검증	설정값 및 거래 등 무결성 검증이 필요한 제품 (스마트TV/셋톱박스 등 결제 관련 암호키 관리가 필요한 제품 등)
	안전한 업데이트	유무선 통신 및 내 · 외부포트를 이용하여 업데이트가 가능한 제품
	감사기록	보안기능이 구현된 제품

4 MCU (Micro Controller Unit) : 집적 회로 안에 프로세서와 메모리, 입출력 버스 등의 컴퓨팅 요소를 내장한 소형 컨트롤러

제3절 제품 유형별 필요기능

홈 · 가전 IoT 제품은 유형에 따라 다음과 같은 세부 보안요구사항을 고려해야 한다. 센싱 제품은 기본적으로 제품 간 상호인증, 정보의 무결성을 요구하며, 제어 기능이 있는 제품의 경우 인증 및 무결성과 함께 제어정보에 대한 기밀성을 고려해야 한다. 구매 기능이 포함된 제품은 인증정보의 무결성 그리고 결제정보 등에 대한 기밀성 및 무결성을, 촬영기능이 제공되는 경우 개인정보 보호 관점으로 촬영정보에 기밀성을 고려해야 한다. IoT 제품을 원격으로 운용하는 경우 사용자 인증을, 관리 기능이 있는 제품의 경우 설정 정보의 무결성 및 기밀성, 사용자에 대한 인증 · 인가 등 강한 보안성을 요구할 수 있다. 이를 기반으로 아래와 같이 IoT 제품의 기능적 유형에 따라 보안항목별 최소 보안요구사항을 제시하고자 한다.

그러나 각각의 제품이 다루는 정보의 종류 · 의존성 · 민감성, 보안위협의 악용가능성, 보안사고 시 파급효과 등 위험분석 결과와 각각의 제품이 제공하는 기능 및 서비스의 복잡도 · 융합 정도에 따라 아래에서 제시한 보안요구사항 일부가 제외되거나 추가될 수 있다.

가. 센싱

보안항목	보안요구사항	필요기능
소프트웨어 보안	• 시큐어코딩	• 센서 소프트웨어 시큐어코딩 • 불필요한 서비스 비활성화 • 난독화 적용 컴파일
	• 알려진 보안약점 및 취약점 제거	• 보안취약점 점검 · 제거
	• 최신 3rd party 소프트웨어 사용	• 최신 3rd party 소프트웨어 사용
물리적 보안	• 물리적 인터페이스 차단	• 외부 입출력 포트 비활성화 • 내부 디버그 포트 비활성화 • 외부 조작 확인 및 분해 방지 메커니즘
인증	• IoT 제품 간 상호인증	• 상호인증
암호화	• 안전한 암호 알고리즘 사용	• 안전한 암호 알고리즘 사용
	• 안전한 암호키 관리	• 안전한 암호키 저장
데이터 보호	• 안전한 통신채널	• 안전한 통신채널 제공
	• 저장 및 전송 데이터 보호	• 전송 데이터 보호(무결성)
플랫폼 보안	• 안전한 업데이트	• 신뢰할 수 있는 업데이트 서버 • 업데이트 파일의 부인방지 및 무결성 제공 • 안전한 업데이트 기능 제공 • 펌웨어 분석 방지 기능 제공

나. 제어 및 중계

보안항목	보안요구사항	필요기능
소프트웨어 보안	• 시큐어코딩	• 제어 · 중계 소프트웨어 시큐어코딩 • 불필요한 서비스 비활성화 • 난독화 적용 컴파일
	• 알려진 보안약점 및 취약점 제거	• 보안취약점 점검 · 제거
	• 최신 3rd party 소프트웨어 사용	• 최신 3rd party 소프트웨어 사용
물리적 보안	• 물리적 인터페이스 차단	• 외부 입출력 포트 비활성화 • 내부 디버그 포트 비활성화 • 외부 조작 확인 및 분해 방지 메커니즘
인증	• 인증 및 접근통제	• 제품의 초기 인증정보 변경 • 사용자 인증 • 인증정보 보호 • 안전한 비밀번호 사용 • 접근통제
	• IoT 제품 간 상호 인증	• 상호인증
암호화	• 안전한 암호 알고리즘 사용	• 안전한 암호 알고리즘 사용
	• 안전한 암호키 관리	• 안전한 암호키 생성 · 전송 · 저장 · 파기
	• 안전한 난수 생성 알고리즘 사용	• 안전한 난수발생기 사용
데이터 보호	• 안전한 통신채널	• 안전한 통신채널 제공 • 안전한 세션관리
	• 저장 및 전송 데이터 보호	• 전송데이터 보호 • 저장데이터 보호 • 메모리 공격 및 역공학 공격 대응(선택)
플랫폼 보안	• 설정값 및 실행코드 무결성 검증	• IoT 제품 주요 설정값 및 실행코드 무결성 검증
	• 안전한 업데이트	• 신뢰할 수 있는 업데이트 서버 • 업데이트 파일의 부인방지 및 무결성 제공 • 안전한 업데이트 기능 제공 • 펌웨어 분석 방지 기능 제공
	• 감사기록	• 감사기록 생성(제어기능 수행 결과, 보안기능 수행 내역 등) • 감사기록 보호

다. 구매

보안항목	보안요구사항	필요기능
소프트웨어 보안	• 시큐어코딩	• 구매 소프트웨어 시큐어코딩 • 불필요한 서비스 비활성화 • 난독화 적용 컴파일
	• 알려진 보안약점 및 취약점 제거	• 보안취약점 점검 · 제거
	• 최신 3rd party 소프트웨어 사용	• 최신 3rd party 소프트웨어 사용
물리적 보안	• 물리적 인터페이스 차단	• 외부 입출력 포트 비활성화 • 내부 디버그 포트 비활성화 • 외부 조작 확인 및 분해 방지 메커니즘
인증	• 인증 및 접근통제	• 제품의 초기 인증정보 변경 • 사용자 인증 • 인증정보 보호 • 안전한 비밀번호 사용 • 접근통제
	• IoT 제품 간 상호 인증	• 상호인증
암호화	• 안전한 암호 알고리즘 사용	• 안전한 암호 알고리즘 사용
	• 안전한 암호키 관리	• 안전한 암호키 생성 · 전송 · 저장 · 파기
	• 안전한 난수 생성 알고리즘 사용	• 안전한 난수발생기 사용
데이터 보호	• 안전한 통신채널	• 안전한 통신채널 제공 • 안전한 세션관리
	• 저장 및 전송 데이터 보호	• 전송데이터 보호 • 저장데이터 보호 • 메모리 공격 및 역공학 공격 대응 • 부채널 공격 대응(선택)
	• 개인정보 보호	• 개인정보 비식별화 조치
플랫폼 보안	• 설정값 및 실행코드 무결성 검증	• IoT 제품 주요 설정값 및 실행코드 무결성 검증
	• 안전한 업데이트	• 신뢰할 수 있는 업데이트 서버 • 업데이트 파일의 부인방지 및 무결성 제공 • 안전한 업데이트 기능 제공 • 펌웨어 분석 방지 기능 제공
	• 감사기록	• 감사기록 생성(구매기능 수행 결과, 보안기능 수행 내역 등) • 감사기록 보호

라. 촬영 및 관리

보안항목	보안요구사항	필요기능
소프트웨어 보안	• 시큐어코딩	• 구매 소프트웨어 시큐어코딩 • 불필요한 서비스 비활성화 • 난독화 적용 컴파일
	• 알려진 보안약점 및 취약점 제거)	• 보안취약점 점검 · 제거
	• 최신 3rd party 소프트웨어 사용	• 최신 3rd party 소프트웨어 사용
물리적 보안	• 물리적 인터페이스 차단	• 외부 입출력 포트 비활성화 • 내부 디버그 포트 비활성화 • 외부 조작 확인 및 분해 방지 메커니즘
인증	• 인증 및 접근통제	• 제품의 초기 인증정보 변경 • 사용자 인증 • 인증정보 보호 • 안전한 비밀번호 사용 • 접근통제
	• IoT 제품 간 상호 인증	• 상호인증
암호화	• 안전한 암호 알고리즘 사용	• 안전한 암호 알고리즘 사용
	• 안전한 암호키 관리	• 안전한 암호키 생성 · 전송 · 저장 · 파기
	• 안전한 난수 생성 알고리즘 사용	• 안전한 난수발생기 사용
데이터 보호	• 안전한 통신채널	• 안전한 통신채널 제공 • 안전한 세션관리
	• 저장 및 전송 데이터 보호	· 전송데이터 보호 • 저장데이터 보호 • 메모리 공격 및 역공학 공격 대응(선택)
	• 개인정보 보호	• 개인정보 비식별화 조치
플랫폼 보안	• 설정값 및 실행코드 무결성 검증	• IoT 제품 주요 설정값 및 실행코드 무결성 검증
	• 안전한 업데이트	• 신뢰할 수 있는 업데이트 서버 • 업데이트 파일의 부인방지 및 무결성 제공 • 안전한 업데이트 기능 제공 • 펌웨어 분석 방지 기능 제공
	• 감사기록	• 감사기록 생성(영상정보 전송 내역, (영상정보 저장시) 접근 내역, 관리기능 수행내역, 보안기능 수행 내역 등) • 감사기록 보호

마. 운용

보안항목	보안요구사항	필요기능
소프트웨어 보안	• 시큐어코딩	• 구매 소프트웨어 시큐어코딩 • 불필요한 서비스 비활성화 • 난독화 적용 컴파일
	• 알려진 보안약점 및 취약점 제거	• 보안취약점 점검 · 제거
	• 최신 3rd party 소프트웨어 사용	• 최신 3rd party 소프트웨어 사용
물리적 보안	• 물리적 인터페이스 차단	• 외부 입출력 포트 비활성화 • 내부 디버그 포트 비활성화 • 외부 조작 확인 및 분해 방지 메커니즘
인증	• 인증 및 접근통제	• 제품의 초기 인증정보 변경 • 사용자 인증 • 인증정보 보호 • 안전한 비밀번호 사용 • 접근통제
	• IoT 제품 간 상호 인증	• 상호인증
암호화	• 안전한 암호 알고리즘 사용	• 안전한 암호 알고리즘 사용
	• 안전한 암호키 관리	• 안전한 암호키 저장
데이터 보호	• 안전한 통신채널	• 안전한 통신채널 제공
플랫폼 보안	• 안전한 업데이트	• 신뢰할 수 있는 업데이트 서버 • 업데이트 파일의 부인방지 및 무결성 제공 • 안전한 업데이트 기능 제공 • 펌웨어 분석 방지 기능 제공
	• 설정값 및 실행코드 무결성 검증(선택)	• IoT 제품 주요 설정값 및 실행코드 무결성 검증

홈·가전 IoT 보안가이드

제4장 공통 보안항목 및 대응방안

제1절 소프트웨어 보안
제2절 물리적 보안

제4장

공통 보안항목 및 대응방안

홈 · 가전 IoT 제품에 공통적으로 적용해야 하는 보안항목은 다음과 같으며, 세부 보안요구사항은 다음 절에서 안내하고자 한다.

보안항목	보안요구사항
소프트웨어 개발보안	• 시큐어코딩 • 알려진 보안취약점 점검 및 제거 • 최신 3rd party 소프트웨어 사용
물리적 보안	• 물리적 인터페이스 차단 – 외부 입출력 포트 비활성화 – 내부 입출력 포트 비활성화 – 외부 조작 확인 및 분해 방지 메커니즘

제1절 소프트웨어 보안

1. 시큐어코딩

가. 개요

홈 · 가전 IoT 제품 설계 단계에서부터 홈 · 가전 IoT 제품 보안가이드(및 IoT 공통보안가이드)의 보안항목을 고려하여 제품을 설계하고, 보안취약점의 원인인 보안약점(Weakness)을 최소화하여 안전하게 구현하는 것을 목적으로 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① **홈 · 가전 IoT 제품의 소프트웨어 및 모바일 앱 구현시 소프트웨어 개발보안 가이드와 같은 시큐어코딩 가이드를 참고하여 안전하게 구현해야 함**

적용방안

- 소스코드 보안약점 분석도구를 이용하여 소스코드 또는 바이트코드에 대한 보안약점을 점검하여 제거

시큐어코딩이 적용되지 않은 스마트 홈 · 가전 제품의 경우 입력 데이터 검증 및 표현, 보안 기능, 시간 및 상태, 에러 처리, 코드오류, 캡슐화, API 오용 등에서 보안 취약점이 발생할 수 있으며, 특히 공유기, IP 카메라, 앱 등의 XSS 취약점을 이용하여 사용자 정보를 모으기 위한 1차 공격이 이루어지는 경우가 있어 필터링 적용이 필요하다.

버퍼오버플로우, 시스템 명령 취약점은 침해사고뿐만 아니라 신고포상제를 통해 가장 많이 조치되고 있는 취약점 중 하나이다. 주로 파라미터, 사용자 입력 값의 길이, 데이터 값을 필터링 없이 받아서 시스템 함수 인자로 바로 대입하여, PC의 주요 설정을 변조하는 등의 문제를 많이 발생시킨다.

이에 대응하기 위해서는 DirBuster, Cross Fuzz 등의 퍼징 툴을 이용하여 취약점에 대한 사전 점검을

진행하는 것이 필요하며, 설계 및 개발 단계에서 시큐어코딩을 적용하여야 한다. 다음은 최근 주로 발생하는 명령어 삽입, 버퍼 오버플로우 등에 대한 시큐어코딩 예시이다.

• 입력데이터 검증 및 표현에 대한 보안 약점 대응 방안 예시 •

보안 약점	운영체제 명령어 삽입
설명	외부 입력이 시스템 명령어 실행 인수로 사용될 때, 적절한 처리 없이 사용되는 경우 발생하는 보안 약점이다. 일반적으로 명령 인수나 스트림 입력 등 외부 입력을 사용하여 시스템 명령어를 생성하는 프로그램에서 발생하며, 이러한 경우 외부 입력 문자열에 대한 검증 혹은 필터링이 없을 시 공격자가 원하는 명령어 실행이 가능하게 된다.
안전한 코딩 기법	외부 입력이 직접 또는 문자열 복사를 통하여 함수에 직접 전달되는 것은 위험하다. 미리 적절한 후보 명령어 리스트를 만들고 선택하게 하거나, 위험한 문자열의 존재 여부를 검사하는 과정을 수행하여야 한다.

보안 약점	버퍼 오버플로우
설명	할당되는 버퍼의 한계치를 넘는 경우 발생하는 보안 약점
안전한 코딩 기법	– 프로그램이 버퍼가 저장할 수 있는 것보다 많은 데이터를 입력하지 않는다. – 프로그램이 버퍼 경계 밖의 메모리 영역을 참조하지 않는다. – 프로그램이 사용할 메모리를 적절하게 계산하여 로직에서 에러가 발생하지 않도록 한다. – 입력에 대해서 경계 검사(Bounds Checking)를 한다. – strcpy()와 같이 버퍼 오버플로우에 취약한 함수를 사용하지 않는다.

시큐어코딩에 대한 세부적인 사항은 행정안전부 및 한국인터넷진흥원의 소프트웨어 개발보안 가이드를 참고한다.

② 불필요한 서비스 비활성화를 기본 값으로 설정해야 함

적용방안

- 불필요한 외부 접속 포트(Telnet, FTP, UPnP, SNMP) 등의 서비스 비활성화를 기본 값으로 설정
- 외부 접속 포트를 사용할 경우 비밀번호 설정, 접근 IP 제한 등의 추가적인 보안 조치 수행

③ 컴파일러 옵션을 활용하여 난독화 등의 메모리 보호 기법을 적용해야 함

적용방안

- 모바일 앱의 경우 난독화 등의 메모리 보호 기법을 적용
- IoT제품 애플리케이션의 경우 버퍼오버플로 방지를 위한 기법(예: ASLR, NX, Stack Smashing Protector 등)을 적용

모바일 앱의 경우 공격자가 메모리 해킹을 통해 관리자 권한을 탈취할 수 있는 데이터를 수집할 수 있다. 이에 스마트 홈 · 가전 제품 개발 시, 컴파일러 옵션을 활용하여 난독화 등의 메모리 보호 기법을 적용해야 한다.

현재 안드로이드 운영체제에서는 ProGuard, Dex Guard, Android Env 등을 이용하여 난독화가 가능하다. ProGuard는 안드로이드 SDK를 통해 난독화를 지원하며, 변수명 변경 등의 간단한 난독화 기능을 무료로 이용할 수 있다. Dex Guard는 ProGuard의 유료 버전으로, ProGuard보다 보안성이 향상된 난독화 기능을 제공한다. Android Env는 안드로이드 상용 난독화 도구로, 단순 함수명 변경뿐 아니라 프로그램 플로우 셔플 등의 난독화를 지원한다. 이 중 무료로 제공되는 프로그램인 ProGuard는, build.gradle 파일에 소스 코드를 삽입하는 방식으로 난독화를 적용할 수 있다. 다음은 ProGuard를 통한 난독화 적용 소스 코드 예시이다.

ProGuard를 이용한 난독화에 대한 세부적인 사항은 안드로이드 개발자 사이트의 이용자 가이드를 참고한다.

• ProGuard를 통한 난독화 적용 소스 코드(JAVA) •

```
buildTypes {

  release {
     minifyEnabled true
     proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
  }
}
```

컴파일러의 난독화 옵션을 적용할 시, 공격자가 기능을 파악하지 못하도록 함수 명, 배열명 등이 의미 없는 문자열로 변환된다. 아래 표는 컴파일러 난독화 옵션 적용 전 · 후의 예시이다.

• 컴파일러 난독화 옵션 적용 예시(JAVA) •

- 컴파일러의 난독화 옵션 적용 예시(전)

```
public Car(TrackPosition pos, Color drawColor, {
        this.pos_ = pos;
        this.drawColor_ = drawColor;
        this.eraseColor_ = eraseColor;
        this.gasPedal_ = gasPedal;
        int[] xs = new int[4];
        int[] ys = new int[4];
        this.poly_ = new Polygon(xs, ys, 4);
```

- 컴파일러의 난독화 옵션 적용 예시(후)

```
public a(h paramh, Color paramColor1, Color paramColor2{
        this.a = paramh;
        this.b = paramColor1;
        this.c = paramColor2;
        this.e = paramb;
        int[] arrayOfInt1 = new int[4];
        int[] arrayOfInt2 = new int[4];
        this.d = new Polygon(arrayOfInt1, arrayOfInt2, 4);
```

모바일 앱 보안성 검증에 대한 세부적인 사항은 행정안전부의 모바일 대국민 전자정부서비스 취약점 점검 가이드를 참고한다.

IoT 애플리케이션의 경우, IoT 제품의 운영체제 설정 또는 애플리케이션 컴파일 시 버퍼오버플로우로 인한 공격 위험성이 있다면 이를 방지하기 위한 기법(예: ASLR, NX, Stack Smashing Protector 등)을 적용한다.

메모리 보호 기법	설명	적용 예시
ASLR(Address Space Layout Randomization)	메모리 공격을 어렵게 하기 위해 스택이나 힙, 라이브러리 등의 주소를 랜덤으로 프로세스 주소 공간에 배치함으로써 실행할 때마다 데이터의 주소를 바꿈	다음 중 2번 값을 적용 randomize_va_space=0 : ASLR 해제 randomize_va_space=1 : 랜덤 스택 & 랜덤 라이브러리 설정 randomize_va_space=2 : 랜덤 스택 & 랜덤 라이브러리 & 랜덤 힙 설정
NX(No-eXecute)	데이터 영역에서 코드가 실행되는 것을 막는 기법.	gcc 옵션에 "-z execstack"이 포함되지 않도록 하여 컴파일
SSP(Stack Smashing Protector)	함수 진입 시 스택에 리턴 주소와 프레임 포인터 정보를 저장할 때 정보를 보호하기 위해 특정한 값(canary)을 기록	gcc 옵션에 -fstack-protector을 추가하여 컴파일

다. 대상

모든 유형의 제품에 적용된다.

라. 참고자료

1) CWE(Common Weakness Enumeration) 사이트, cwe.mitre.org

2) 행정안전부, 한국인터넷진흥원, "소프트웨어 개발보안 가이드", 11-1311000- 000330-10 (발간등록번호), 2017년 1월

3) 행정안전부, 한국인터넷진흥원, "모바일 전자정부서비스 앱 소스코드 검증 가이드라인", 11-1312000-000057-01 (발간등록번호), 2015년 12월

4) SEI CERT Coding Standards (C, C++, Android, Java, Perl), www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

5) IT보안인증사무국(소스코드 보안약점 분석도구), www.itscc.or.kr/certifyProd_list.asp

6) SAMATE(SW Assurance Metrics & Tool Evaluation) 사이트, samate.nist.gov/index.php/Tool_Survey.html

5) 안드로이드 개발자 사이트, developer.android.com/studio/build/shrink-code.html#configuring

2. 알려진 보안취약점 점검 및 제거

가. 개요

홈 · 가전 IoT 제품을 구성하는 소프트웨어가 기존에 알려진 보안취약점을 갖는 프로토콜, 라이브러리, API, 패키지, 오픈소스 등을 사용하여 개발되었을 경우 제반 펌웨어, 운영체제도 보안에 취약할 수 있기 때문에 제품을 점검하여 보안취약점을 제거해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① **홈 · 가전 IoT 제품 및 유사 제품 유형과 관련하여 현재까지 알려진 보안취약점을 공개영역(예, KrCERT, CVE, NVD, SecurityFocus, 논문 등)에서 조사한 후, 개발대상 제품에 해당 보안취약점이 존재하는지를 점검한 후 제거해야 함**

적용방안

- CVE, NVD와 관련된 점검규칙을 보유한 상용 또는 신뢰할 수 있는 공개용* 보안취약점 점검도구(스캐너)를 사용하여 개발대상 제품의 보안취약점 점검 및 제거
  * 지속적으로 보안취약점 점검규칙이 업데이트되고, 널리 사용되는 도구
- 최신버전 및 보안패치가 적용된 3rd party 라이브러리(예, openssl 등), 운영체제(예, Linux, Android 등) 사용
- 외부 시험기관 등을 통해 보안취약점을 점검하여 보안취약점 제거 조치

다. 대상

모든 유형의 제품에 적용된다.

라. 참고자료

1) KISA인터넷보호나라 & KrCert 사이트, www.krcert.or.kr

2) CVE(Common Vulnerabilities and Exposures) 사이트, cve.mitre.org

3) NVD(National Vulnerability Database) 사이트, nvd.nist.gov

4) SecurityFocus 사이트, www.securityfocus.com

5) 공개용 SSL 라이브러리 사이트, www.openssl.org

6) 공개용 SSH 라이브러리 사이트, www.openssh.org

7) IT보안인증사무국(취약점 점검도구), www.itscc.or.kr/certifyProd_list.asp

8) SAMATE(SW Assurance Metrics & Tool Evaluation) 사이트, samate.nist.gov/index.php/Tool_Survey.html

3. 최신 3rd party 소프트웨어 사용

가. 개요

홈 · 가전 IoT 제품 개발 및 서비스 운영환경에 사용되는 3rd party 소프트웨어(운영체제, 라이브러리, 모듈 등 공개용 및 상용 소프트웨어)는 최신 보안패치가 적용된 최신 버전을 사용해야 한다. 출시된 홈 · 가전 IoT 제품에서 사용되는 3rd party 소프트웨어에 심각한 결함이나 보안취약점에 대한 보안패치를 적용해야 하는 경우 신속하게 업데이트를 수행해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① (개발 단계) 3rd party 소프트웨어는 최신 보안패치가 적용된 최신 버전을 사용하여 제품을 개발해야 함

적용방안

- 제품 개발에 사용되는 3rd party 라이브러리 및 모듈은 최신 보안패치가 적용된 최신 버전을 사용해야 함
- 제품 연동 및/또는 구동·운용을 위해 사용되는 3rd party 소프트웨어는 최신 보안패치가 적용된 최신 버전을 사용하여야 하며, 사용자(관리자) 매뉴얼에 안전한 운영환경을 제시하여야 함

② (출시 후) 제품에 적용된 3rd party 소프트웨어와 관련하여 심각한 보안취약점 발생하여 긴급하게 보안패치가 필요한 경우, 최신 버전의 3rd party 소프트웨어를 기반으로 보안패치를 개발하여 신속하게 배포해야 함

적용방안

- 최신 보안사고 및 보안취약점 동향(KrCERT, CVE 등)을 파악하고 제품에 적용된 3rd party 소프트웨어 보안패치 정보를 주기적으로 모니터링하여 보안사고 발생 시 최신 버전을 적용한 보안패치를 개발하여 배포해야 함
- 보안패치 파일 배포는 본 가이드의 '안전한 업데이트 기능 제공'의 보안대책을 따름
- 검증된 보안제품(예, 침입방지시스템, 안티바이러스제품 등) 사용 및 최신 룰(rule) 적용을 통해 대응해야 함

다. 대상

3rd party 소프트웨어를 사용하는 모든 유형의 제품에 적용된다.

마. 참고자료

1) KISA인터넷보호나라 & KrCert 사이트, www.krcert.or.kr

2) CVE(Common Vulnerabilities and Exposures) 사이트, cve.mitre.org

3) NVD(National Vulnerability Database) 사이트, nvd.nist.gov

4) SecurityFocus 사이트, www.securityfocus.com

5) 공개용 SSL 라이브러리 사이트, www.openssl.org

6) 공개용 SSH 라이브러리 사이트, www.openssh.org

7) 리눅스 커널 사이트, www.kernel.org

8) 마이크로소프트社 소프트웨어 업데이트 사이트, support.microsoft.com

9) MySQL 소프트웨어 사이트, www.mysql.com

10) SQLite 소프트웨어 사이트, www.sqlite.org

11) 공개 소프트웨어 포털 사이트, www.oss.kr

제2절 물리적 보안

1. 물리적 인터페이스 차단

1.1 외부 입출력 포트 비활성화

가. 개요

외부에 노출된 포트는 종류와 기능 식별이 쉽고, 별도의 접속 도구를 사용하지 않고도 쉽게 접근이 가능하기 때문에 공격 대상이 되기 쉽다. 이에 따라, 홈 · 가전 IoT 제품의 불필요한 외부 인터페이스는 제거해야 한다.

나. 보안대책

① USB, RS232, Ethernet, SD Card 슬롯 등 제품 운영에 불필요한 포트는 제거하거나 비활성화하여 비인가된 외부 접근을 근본적으로 차단해야 함

적용방안

- USB, RS232, Ethernet포트로 운영체제(OS) 펌웨어에 접근하지 못하도록 함
  ※ 필요 시 비인가된 접속을 방지하기 위한 인증 기능 구현(비밀번호는 본 가이드의 '비밀번호 강도 보안요구사항' 참조)
- 업그레이드를 위해 SD Card를 이용하여 접속 시 아이디/비밀번호 확인 등 인증절차를 거친 후 업그레이드하도록 구현

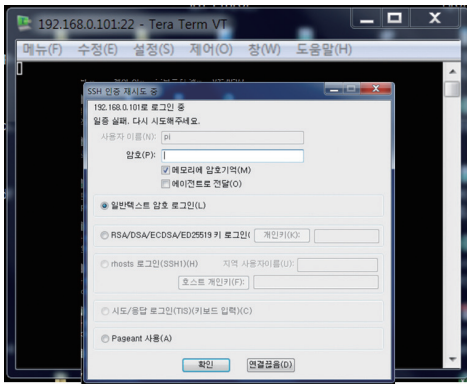
다. 예시

디지털 도어락의 외부 인터페이스를 제거하고, 웹캠의 이더넷(ethernet)은 SSH 접속을 이용함으로써 비인가된 접근을 방지한다.

• 디지털 도어락 / 웹캠 비인가 접속 방지 예시 •

디지털 도어락 외부 인터페이스 제거

웹캠 Ethernet 비인가 접속 불가 (SSH 접속)



라. 대상

- **특징** 운영체제(OS) 관리자 접근, 외부 인터페이스를 이용한 업그레이드
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) Internet of Things (IoT) Security Testing Framework(ICSA Labs, Document Version 2.0, October 26, 2016)

2) ICT 융합 제품 · 서비스의 보안 내재화를 위한 IoT 공통보안 가이드 (IoT 보안얼라이언스, 2016.09)

1.2 내부 입출력 포트 비활성화

가. 개요

홈 · 가전 IoT 제품의 내부 입출력 포트(예: UART, JTAG 등)를 통해 펌웨어 추출 및 파일 시스템 분석을 통한 정보검색을 방지하기 위해 입출력 포트에 대한 접근통제를 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 개발 버전 PCB와 양산 버전 PCB 변경으로 입출력 포트(예, UART, JTAG 등)를 완전히 제거하거나 비활성화하여 제품을 출시해야 함

적용방안

- (UART) 제품 소스코드에서 UART 비활성화 설정
- (JTAG) IC업체에서 제공하는 메모리 관련 보호 도구로 JATG 비활성화 설정
- (UART, JTAG 등 입출력포트) 쉽게 식별되지 않도록 포트 식별 난독화 적용*

[포트 식별 난독화* 고려사항]

- 주요 부품간 통신 라인의 내층 설계
- JTAG, UART 등 입출력 포트의 실크인쇄 삭제로 포트 식별을 어렵게 함
- Lead type MCU는 CAN 적용하여 IC에 직접 접근을 어렵게 함
- 주요 IC의 레이저 마킹 삭제로 IC 의 데이터 시트의 수집을 어렵게 함 (데이터 시트 수집으로 디버깅 포트 및 통신 포트 정보 취득 쉬움)
- 디버깅을 위해 JTAG 등 포트를 테스트 포인트로 구현하고, 위치 분산으로 접근을 어렵게 함
- 단순 핀수 증가하는 것은 지양
- 디버깅 접속을 위한 자체 접속도구 활용

- (USB, UART, JTAG 등 입출력포트) 콘솔 접속 시 비인가된 접속을 방지하기 위한 인증 기능 구현(비밀번호는 본 가이드의 '비밀번호 강도 보안요구사항' 참조)

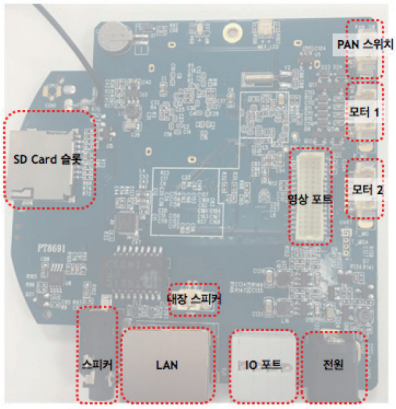
다. 예시

양산 제품은 내부 입출력 포트 또는 디버깅 포트를 완전히 제거하여 하고, 업데이트나 고장수리를 위해 내부 포트를 유지할 경우, JTAG 포트 비활성화 또는 패스워드를 사용해 접근을 통제하도록 한다.

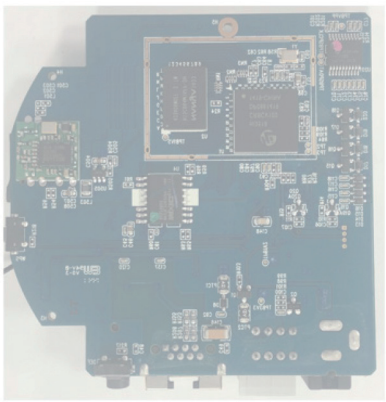
① 개발 버전 PCB와 양산 버전 PCB 변경으로 입출력 포트(JTAG)를 완전히 제거한 제품 예시

• 웹캠 제품의 하드웨어 보드 예시 •

JTAG 포트 미구현(앞면)



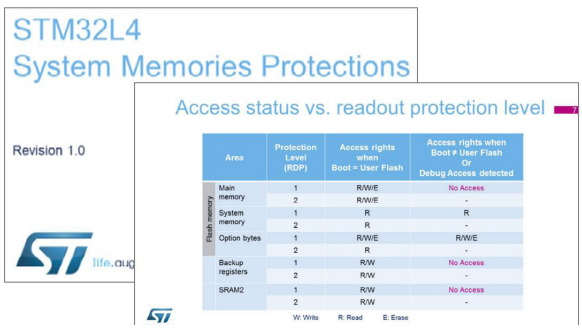
JTAG 포트 미구현(뒷면)



② JTAG 포트 제거 불가시 JTAG 비활성화 파라미터를 설정한 예시

(JTAG 비활성화 예시1) ST Micro사 STM32L4 계열 제품에서 지원하는 시스템 메모리 접근 보호 기능은 ST Micro사에서 제공하는 STLink Tool을 이용하여 설정이 가능하다.

• ST 사 메모리 셋팅 테이블 및 STlink 도구 •


STM32L4
System Memories Protections

Revision 1.0

Access status vs. readout protection level

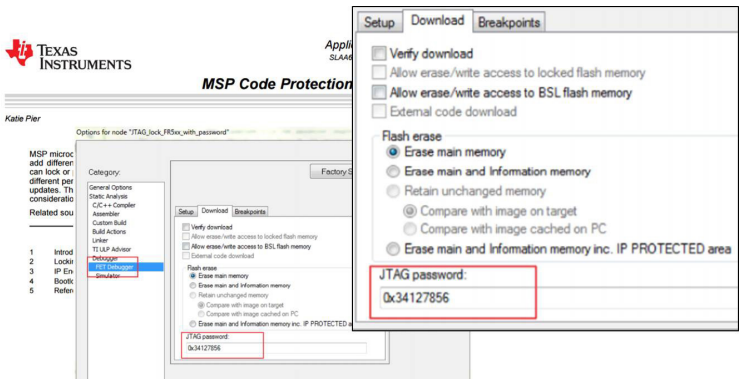
Area		Protection Level (RDP)	Access rights when Boot = User Flash	Access rights when Boot ≠ User Flash Or Debug Access detected
Flash memory	Main memory	1	R/W/E	No Access
		2	R/W/E	-
	System memory	1	R	R
		2	R	-
	Option bytes	1	R/W/E	R/W/E
		2	R	-
	Backup registers	1	R/W	No Access
		2	R/W	-
	SRAM2	1	R/W	No Access
		2	R/W	-

W: Write R: Read E: Erase

출처 :http://www.st.com/

(JTAG 비활성화 예시2) TI사의 MSP 계열 제품에서 지원하는 JTAG 및 메모리 접근에 대한 Protection 기능 지원에 대한 내용이다.

• TI 사 MSP Family 제품 Code protection 기능 •



출처: http://www.ti.com/

라. 대상

- **특징** 운영체제(OS) 관리자 접근, 내부 인터페이스를 이용한 디버깅 및 업그레이드
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트온도계, 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) ST사 STM32L4 계열 System Memory Protection 및 STlink 도구 정보
www.st.com/content/ccc/resource/training/technical/product_training/08/4c/83/1b/56/bd/45/34/STM32L4_System_SYSCFG.pdf/files/STM32L4_System_SYSCFG.pdf/jcr:content/translations/en.STM32L4_System_SYSCFG.pdf

2) TI 사 MSP Family 제품 Code protection 정보
www.ti.com/lit/an/slaa685/slaa685.pdf

3) Internet of Things (IoT) Security Testing Framework(ICSA Labs, Document Version 2.0, October 26, 2016)

4) ICT 융합 제품 · 서비스의 보안 내재화를 위한 IoT 공통보안 가이드 (IoT 보안얼라이언스, 2016.09)

1.3 외부 조작 확인 및 분해 방지 메커니즘

가. 개요

일반적으로 하드웨어에 대한 보안 취약점은 하드웨어의 데이터 버스와 제어신호 등에 대한 직접적인 접근 가능성에 의해 발생 가능하다. 디바이스 내부 접근을 위한 데이터 버스로의 직접 접근은 제품의 외부 조작 및 분해를 통해 가능하기 때문에 디지털 도어락, 웹캠과 같은 홈 · 가전 IoT 제품은 조작 확인(Tamper Proofing) 또는 분해 방지 메커니즘을 구현해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 물리적 탐침을 방지하고 비인가 조작을 탐지하여 대응하는 기능을 구현해야 함

적용방안

- 조작방지(Tamper Proofing) 솔루션을 도입하여 비인가 조작을 탐지하고, 비인가 조작 탐지 시 주요키 및 민감 데이터 초기화 수행

  ※ 초기화가 어려울 경우, 제품을 비활성화하여 운영을 못하도록 함

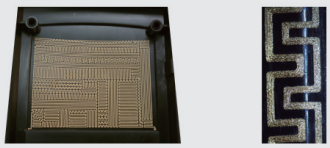
- 특수 제작된 스크류 및 제품 몰딩으로 분해 방지 메커니즘을 구현하거나, 외관 분해 확인을 위하여 파괴 테이프 등을 이용하여 분해 시도 확인 도구로 사용 가능

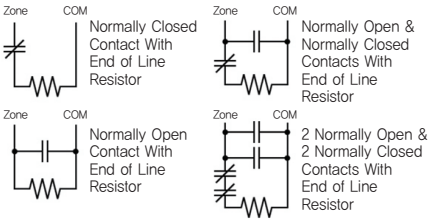
다. 예시

LDS(Laser Direct Structuring) 공법을 이용한 패턴 구현 및 응용 회로와 특수 스크류 등을 적용하여 외부 조작방지 메커니즘을 도입한다.

• 월패드에 적용된 외부조작 방지 메커니즘 •

Tamper Protection Mesh 회로





Tamper Protection 스크류

분해 확인 파괴 테이프

라. 대상

- **특징** 암호연산(암호키 저장), 인증정보(비밀번호 등) 저장, 제품에 대한 높은 접근성
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트온도계, 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) Internet of Things (IoT) Security Testing Framework(ICSA Labs, Document Version 2.0, October 26, 2016)

2) ICT 융합 제품 · 서비스의 보안 내재화를 위한 IoT 공통보안 가이드 (IoT 보안얼라이언스, 2016.09)

제5장 유형별 보안항목 및 대응방안

제1절 인증
제2절 암호화
제3절 데이터보호
제4절 플랫폼 보안

제5장

유형별 보안항목 및 대응방안

홈 · 가전 IoT 제품 유형별로 적용해야 하는 보안항목은 다음과 같으며, 세부 요구사항은 다음 절에서 안내하고자 한다.

보안항목	보안요구사항	
인증	• 인증 및 접근통제	– 제품의 초기 인증정보 변경 – 사용자 인증 – 인증정보 보호 – 안전한 비밀번호 사용 – 접근통제
	• IoT 제품간 상호 인증	– 상호인증
암호화	• 안전한 암호 알고리즘 사용	
	• 안전한 암호키 관리	– 안전한 암호키 생성 – 안전한 암호키 전송 – 안전한 암호키 저장 – 안전한 암호키 파기
	• 안전한 난수 생성 알고리즘 사용	
데이터 보호	• 안전한 통신채널	– 안전한 통신채널 제공 – 안전한 세션관리
	• 저장 및 전송 데이터 보호	– 전송데이터 보호 – 저장데이터 보호 – 메모리 공격 및 역공학 공격 대응 – 부채널 공격 대응
	• 개인정보 보호	
플랫폼 보안	• 설정값 및 실행코드 무결성 검증	– IoT 제품 주요 설정값 및 실행코드 무결성 검증
	• 안전한 업데이트	– 신뢰할 수 있는 업데이트 서버 – 업데이트 파일의 부인방지 및 무결성 보장 – 안전한 업데이트 기능 제공 – 펌웨어 분석 방지 기능 제공
	• 감사기록	– 감사기록 생성 – 감사기록 보호

제1절 인증

1. 인증 및 접근통제

1.1 제품의 초기 인증정보 변경

가. 개요

홈 · 가전 IoT 제품의 초기 비밀번호 설정을 그대로 사용하는 경우, 이를 악용한 '미라이 악성코드' 등에 노출될 수 있다. 이를 예방하기 위해 초기 설치 단계와 재설치 단계에서 초기 인증정보(아이디, 비밀번호 등)를 필수적으로 변경하도록 하여 비인가된 사용자의 임의 접근이나 DDoS 공격을 방지한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① (출시 단계) 홈·가전 IoT 제품 개발 및 제조 시 제품별로 서로 다른 초기 인증정보(예: 비밀번호 등)를 설정·주입하여 출시해야 함

적용방안

- 제품에서 사용자 등록정보(예, 사용자의 전화번호, 이메일 등)를 기반으로 한 개별 인증정보를 생성하여 제품별로 다른 인증정보를 사용자에게 전송하여 사용하도록 함
- QR코드, NFC태그 등을 활용하여 초기 인증정보를 대체할 수 있도록 하며, 제품 포장 박스보다는 제품의 외관에 부착하여 해당 인증정보가 외부로 공개되는 것을 제한

② (사용 단계) 최초 설치(및 재설치) 단계에서 사용자로 하여금 초기 인증정보 변경을 강제하도록 함

적용방안

- 초기 인증 후 인증정보를 변경하는 입력창을 띄워 사용자가 반드시 인증정보를 변경하는 단계를 거치도록 함
- 제품에서 생성한 인증정보를 사용자 보유수단(예, 스마트폰 등)으로 전달(예, NFC, BLE 등)하여 제품 접속 시 인증수단으로 사용하도록 함

다. 예시

월패드 제품 설치 시, 아래와 같이 제품의 초기 인증정보 입력 후 인증정보를 필수적으로 변경하도록 해야 한다.

• **월패드 제품의 최초 인증정보 입력 및 변경 예시** •

제품 설치 시 초기 인증정보 입력

초기 인증정보 입력 후 인증정보 변경 강제

라. 대상

- **특징** 관리자 설정 기능, 인증절차 후 접근
- **유형** 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “2016년 Mirai 악성코드 동향”, 2016년 12월, www.boho.or.kr

1.2 사용자 인증

가. 개요

홈 · 가전 IoT 제품의 설정 및 제어 기능에 접근할 때 사용자 인증 기능이 없거나 취약한 경우 비인가된 사용자 접근을 가능하게 하므로 보안취약점을 유발할 수 있다. 따라서 홈 · 가전 IoT 제품의 설정 및 제어 기능 수행 시 사용자 인증을 반드시 거치도록 해야 하며 사용자 인증 우회를 방지해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 홈 · 가전 IoT 제품의 설정 및 제어 등의 관리 서비스나 개인정보 등의 민감 정보에 접근 시 사용자 인증을 수행해야 함

적용방안

- 아이디/비밀번호* 기반으로 사용자 인증 수행

  * 비밀번호를 유추하거나 해킹하지 못하도록 안전한 비밀번호 사용
- 제품에서 생성한 인증정보를 사용자 보유수단(예, 스마트폰 등)으로 전달(예, SMS, NFC 등)하여 인증 번호를 입력하거나 제품을 터치하는 방식 등으로 인증 수행

② 잘못된 인증정보를 통한 반복된 인증 시도(예, Brute Force 공격)에 대해 인증을 제한하는 기능을 수행해야 함

적용방안

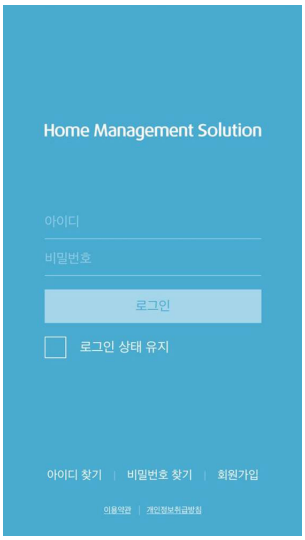
- 잘못된 인증정보를 통한 인증 시도 시 인증 시도 횟수를 제한하고 제한된 시도 횟수 초과 시 일정시간 동안 계정 잠금(비활성화)
- 비활성화된 계정은 인가된 관리자가 사용자 요청 및 확인을 통해 잠금해제 수행
- 캡챠(CAPTCHA) 방식 등과 같은 자동입력방지 문자와 같은 기능을 적용하여 로봇을 이용한 자동화된 반복 시도 방지

다. 예시

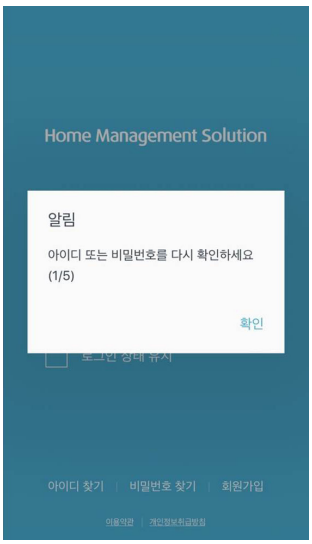
월패드 설정 및 제어를 위해 사용자가 개인 단말(앱)을 이용하여 접근을 시도하면 사용자 인증을 요구한다. 해당 월패드는 사용자 인증을 위하여 아이디/비밀번호 메커니즘을 이용하며 잘못된 인증정보를 통한 인증 시도 횟수를 제한하고 있다.

• 월패드 제품의 인증 수행 및 잘못된 인증 시도에 대한 횟수 제한 예시 •

월패드 설정 및 제어 기능 접근 시 사용자 인증 수행



잘못된 인증정보를 통한 인증 시도 반복 횟수 제한



라. 대상

- **특징** 관리자 설정 기능, 인증절차 후 접근
- **유형** 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “비밀번호 선택 및 이용안내서”, 2010년 1월

2) 한국인터넷진흥원, “암호이용안내서”, 2010년 1월

3) 캡챠(CAPTCHA) 방식, developers.google.com/recaptcha/ 및 captcha.com

1.3 인증정보 보호

가. 개요

홈 · 가전 IoT 제품의 비밀번호를 하드코딩하거나 비밀번호를 포함한 인증정보 입력 시 평문으로 표시되는 경우 인증정보가 노출되어 비인가된 사용자의 접근을 허용할 수 있다. 또한, 인증실패 피드백에 인증실패 사유를 구체적으로 제시하는 경우 인증 방식의 안전성 혹은 보안강도가 낮아질 수 있다. 따라서 인증 과정에서 관련된 정보 제공을 최소화하고, 인증정보를 안전하게 보호하기 위한 다양한 방안을 적용해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 홈 · 가전 IoT 제품 및/또는 소스코드에 비밀번호를 하드코딩하거나 평문으로 저장하지 않아야 함

적용방안

- 인증정보(예, 비밀번호, PIN 등) 저장 시 평문 혹은 단순 인코딩하여 저장하지 않고, SHA2 이상의 보안강도를 가진 일방향 해시함수을 사용하여 저장하고, DB접속과 같이 인증정보가 필요한 경우 AES 등으로 암호화하여 저장
  * 예) SHA2 이상의 보안강도를 가지고 있는 일방향 해시함수(예. SHA- 224/256/384/512)를 이용하여 별도의 파일에 저장하고, 솔트(salt)를 사용하여 동일한 인증정보를 다른 해시값으로 표현되도록 해야 함
- 인증정보가 필요한 경우, 사용자 입력을 받아 사용

② 인증정보 입력 시 정보 보호를 위해 평문으로 표시되지 않도록 해야 함

적용방안

- 비밀번호 등 인증정보 입력 시 '*'문자 등을 이용하여 인증정보가 평문으로 표시되지 않도록 함

③ 인증 실패 이유에 대한 피드백(예, 아이디 오류, 비밀번호 오류 등)을 제공하지 않아야 함

적용방안

- 아이디/비밀번호 방식의 경우, 인증 실패의 원인이 아이디 오류인지 비밀번호 오류인지 등 특정 실패원인을 유추할 수 없도록 피드백(예, 인증이 실패하였음) 정보 제공

④ 인증정보 재사용을 방지해야 함

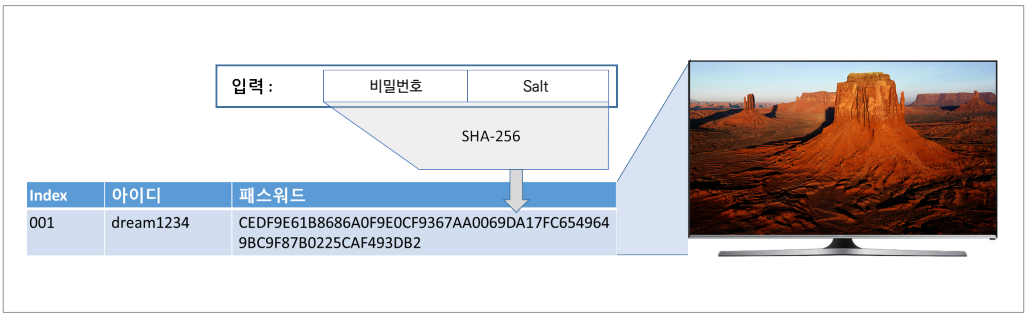
적용방안

- 인증세션에 타임스탬프 등을 적용하여 인증세션을 재사용하는 것을 방지
- 일회용 비밀번호(OTP) 사용

다. 예시

월패드와 같은 홈 · 가전 IoT 제품 내에 비밀번호 저장 시 솔트를 적용한 인증정보의 해시값을 저장한다.

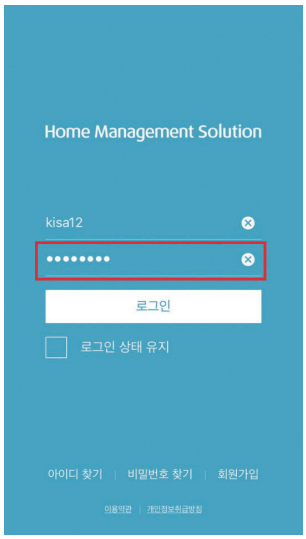
• 월패드 제품의 인증정보 저장 시 솔트를 적용한 인증정보의 해시값 저장 •



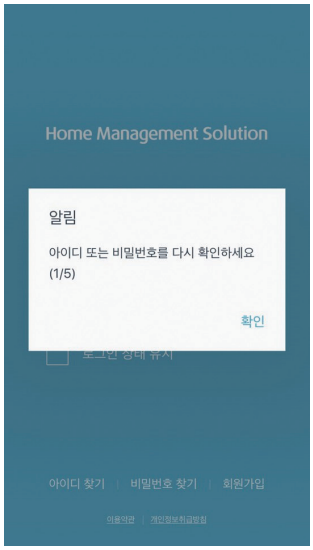
사용자 개인 단말을 통해 월패드에 접근하여 인증정보(비밀번호)를 입력 시 아래와 같이 인증정보가 마스킹되어 표시된다. 또한 인증 실패 시 실패원인을 유추할 수 없는 팝업창이 출력된다.

• **월패드 제품에 인증정보 입력 시 마스킹 출력 및 실패 시 팝업창 예시** •

비밀번호(인증정보) 입력 시 평문 출력 방지

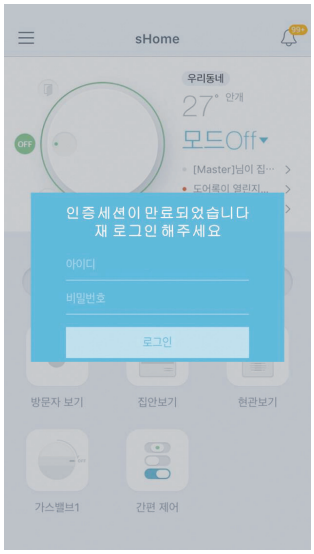


인증 실패 시 대한 인증정보에 대한 추측이 불가한 팝업창



월패드 제품의 사용자 인증 후 일정 시간 동작이 없으면 세션이 만료되며, 재 인증을 요청한다.

• **월패드 제품의 사용자 인증 후 세션 타임아웃 예시** •



라. 대상

- **특징** 관리자 설정 기능, 인증절차 후 접근
- **유형** 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2013년

2) 한국정보통신기술협회, “일회용 패스워드(OTP) 알고리즘 프로파일”, www.tta.or.kr/data/ttas_view.jsp?rn=1&rn1=Y&rn2=&rn3=&pk_num=TTAK.KO-12.0193&nowSu=4&standard_no=&kor_standard=otp&publish_date=&section_code=&acode1=&acode2=&scode1=&scode2=&order=publish_date&by=desc&totalSu=14

1.4 안전한 비밀번호 사용

가. 개요

홈 · 가전 IoT 제품 사용 및 관리를 인가된 사용자로 제한하기 위해 아이디/비밀번호 메커니즘 기반의 접근통제 기능을 구현 시, 비인가된 사용자의 접근을 방지할 수 있도록 추측이 어려운 비밀번호를 설정하도록 지원해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 안전한 비밀번호를 설정할 수 있도록 지원해야 함

※ 단, 아이디 없이 비밀번호만 입력하고 입력 문자가 숫자로 제한되는 제품(예, 디지털 도어락)의 경우, 비밀번호(또는 PIN)는 충분한 자리수의 숫자가 입력될 수 있도록 해야 한다.

적용방안

- **(공통적용)** 비밀번호가 동일한 문자로 구성되지 않아야 하며, 한자리와 같이 짧은 길이의 비밀번호를 허용하지 않도록 해야 함
- **(공통적용)** 비밀번호 재설정 시 이전 비밀번호가 재사용되지 않아야 하며, 유추하기 쉬운 비밀번호(예, admin, root, pass 등)를 허용하지 않아야 함
  ※신규 비밀번호와 이전 비밀번호 체크 및 허용하지 않는 비밀번호 체크 기능을 구현하거나 또는 사용자 설명서에 주의사항으로 기술하여 신규 비밀번호를 이전 비밀번호와 동일하게 설정하거나, 유추하기 쉬운 비밀번호를 설정하지 않도록 유도
- **(원격 모바일 앱/웹)** 모바일 앱 또는 웹을 통해 원격으로 홈·가전 IoT 제품에 접속하는 경우, 모바일 앱/웹에 로그인하기 위한 비밀번호는 영문자, 숫자, 특수문자를 포함하여 8자리 이상으로 설정하도록 해야 함
- **(콘솔)** JTAG 등 디버그포트를 통해 홈·가전 IoT 제품에 접속하는 경우, 콘솔로 로그인하기 위한 비밀번호는 영문자, 숫자, 특수문자를 포함하여 8자리 이상으로 설정하도록 해야 함
- **(콘솔)** 홈가전 IoT 제품의 부트로더(예: U-boot, CFE, ARMBoot 등)에서 제공하는 관리자 메뉴에 비밀번호를 설정하거나 디폴트로의 접근을 비활성화해야 함
- **(직접 접속)** 제품 화면으로 직접 접속하거나 BLE 등 근거리 무선통신으로 접속이 제한된 모바일 앱으로 접속하여 잠금설정을 해제하려는 경우, 잠금해제를 위한 비밀번호는 영문자, 숫자, 특수문자를 포함하여 일정길이 이상으로 설정하도록 해야 함
- **(대체)** 제품에서 생성한 인증정보를 사용자 보유수단(예, 스마트폰, 스마트키 등)으로 전달(예, NFC, BLE 등)하여 근거리에서 제품 접속 시 인증수단으로 사용하도록 함

※ (참고1) 미라이 악성코드에서 사용한 아이디 및 비밀번호

아이디	비밀번호	아이디	비밀번호	아이디	비밀번호
root	(none)	root	jvbzd	admin	123456
root	admin	root	anko	admin	54321
root	root	root	zlxx.	admin	meinsm
root	user	root	ikwb	admin	7ujMko0admin
root	pass	root	vizxv	admin1	password
root	system	root	xmhdipc	administrator	1234
root	default	root	juantech	Administrator	admin
root	dreambox	root	xc511	user	user
root	realteck	root	7ujMko0vizxv	guest	guest
root	1111	root	7ujMko0admin	guest	12345
root	1234	admin	(none)	service	service
root	12345	admin	admin	support	support
root	123456	admin	admin1234	supervisor	supervisor
root	666666	admin	smcadmin	ubnt	ubnt
root	888888	admin	pass	tech	tech
root	00000000	admin	password	mother	fucker
root	klv123	admin	1111	666666	666666
root	klv1234	admin	1111111	888888	888888
root	Zte521	admin	1234		
root	hi3518	admin	12345		

출처: www.ciokorea.com/news/31449

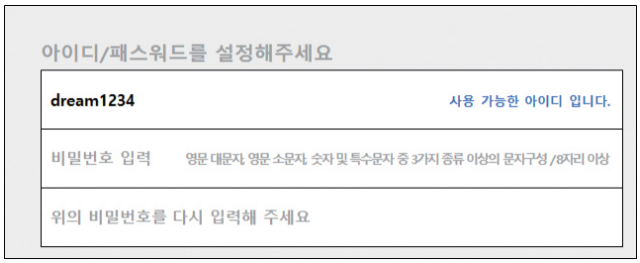
※ (참고2) 안전한 비밀번호 및 취약한 비밀번호 조건(출처: KISA 암호이용안내서)

구분	안전한 비밀번호 조건	취약한 비밀번호 조건
문자 구성 및 길이	• 3가지 종류 이사의 문자 구성으로 8자리 이상의 길이로 구성된 비밀번호 • 2가지 종류 이상의 문자 구성으로 10자리 이상의 길이로 구성된 비밀번호 ※ 문자 종류는 알파벳 대문자와 소문자, 특수문자, 숫자의 4가지임	• 2가지 종류 이하의 문자구성으로 8자리 이하의 길이로 구성된 비밀번호 • 문자구성과 관계없이 7자리 이하 길이로 구성된 비밀번호 ※ 문자 종류는 알파벳 대문자와 소문자, 특수문자, 숫자의 4가지임
특정 정보 이용 및 패턴	• 한글, 영어 등의 사전적 단어를 포함하지 않은 비밀번호	• 한글, 영어 등을 포함한 사전적인 단어로 구성된 비밀번호 ※ 스펠링을 거꾸로 구성한 비밀번호도 포함
	• 널리 알려진 단어를 포함하지 않거나 예측이 어렵도록 가공한 비밀번호 ※ 널리 알려진 단어는 컴퓨터 용어, 기업 등의 특정 명칭 그대로 사용하는 경우 ※ 속어, 방언, 은어 등을 포함하는 경우	• 널리 알려진 단어로 구성된 비밀번호 ※ 컴퓨터 용어, 사이트, 기업 등의 특정 명칭으로 구성된 비밀번호도 포함
	• 사용자 ID와 연관선이 있는 단어구성을 포함하지 않는 비밀번호	• 사용자 ID를 이용한 비밀번호 ※ 사용자 ID 혹은 사용자 ID를 거꾸로 구성한 비밀번호도 포함
	• 제3자가 쉽게 알 수 있는 개인정보를 포함하지 않은 비밀번호 ※ 개인정보는 가족이름, 생일, 주소, 휴대전화번호 등을 포함	• 제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 비밀번호 ※ 가족이름, 생일, 주소, 휴대전화번호 등을 포함하는 비밀번호
	–	• 패턴이 존재하는 비밀번호 ※ 동일한 문자 반복 : aaabb, 123123 ※ 키보드 상에서 연속한 위치에 존재하는 문자들의 집합: qwerty, asdfgh ※ 숫자가 제일 앞이나 제일 뒤에 오는 구성의 비밀번호 : security1, may12 • 숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 비밀번호 ※ 영문자 'O'를 숫자 '0'으로, 영문자 'l'를 숫자 '1'로 치환 등의 비밀번호 • 특정 인물의 이름을 포함한 비밀번호 ※ 사용자 또는 사용자 이외의 특정 인물, 유명인, 연예인 등의 이름을 포함하는 비밀번호 • 한글의 발음을 영문으로, 영문단어의 발음을 한글로 변형한 형태의 비밀번호 ※ 한글의 '사랑'을 영어 'SaRang'으로 표기, 영문자 'LOVE'의 발음을 한글 '러브'로 표기
기타	• 해당 시스템에서 사용자가 이전에 사용하지 않고 이전 비밀번호와 연관성이 있는 단어구성을 포함하지 않은 비밀번호	• 시스템에서 예제로 제시되는 비밀번호 • 시스템에서 초기 설정된 비밀번호 • 해당 시스템에서 사용자가 이전에 사용했던 비밀번호

다. 예시

① 홈 · 가전 IoT 제품이 사용자 인증 방식으로 아이디/비밀번호 메커니즘을 사용할 때 안전한 비밀번호를 사용 및 설정하도록 한다.

• 아이디/ 비밀번호 설정 화면 •



② 홈 · 가전 IoT 제품의 UART를 물리적으로 연결하여 키 입력을 하더라도 관리자 메뉴가 활성화되지 않도록 한다.

적용 전	적용 후
U-Boot 2010.12-rc2 (Dec 30 2013 - 16:51:46) Cores: ARM 432 MHz DRAM: 256 MiB Bad block table found at page 65408, version 0x01 Normal Booting... Hit any key to stop autoboot: 0 DM365 EVM #	U-Boot 2010.12-rc2 (Dec 30 2013 - 16:51:46) Cores: ARM 432 MHz DRAM: 256 MiB Bad block table found at page 65408, version 0x01 Normal Booting...

라. 대상

- **특징** 관리자 설정 기능, 인증절차 후 접근
- **유형** 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 미라이 IoT 봇넷에서 활용한 61가지 비밀번호, www.ciokorea.com/news/31449

2) 한국인터넷진흥원, “암호이용안내서”, 2010년1월

1.5 접근통제

가. 개요

홈 · 가전 IoT 제품을 설정 혹은 제어하거나 제어 대상 제품을 등록하는 등의 중요한 기능에는 인가된 사용자(관리자)만 접근할 수 있도록 허용해야 중요 기능 오용을 방지할 수 있다. 따라서 일반 사용자에게는 중요기능 설정에 접근할 수 없도록 최소한의 사용 권한만 허용해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 관리자 권한이 일반 사용자에게 부여되지 않아야 함

적용방안

- 중요 기능(예, 제어 앱 설치 스마트폰 등록, 제어대상 웹캠 등록, 업데이트 서버 설정, 스마트TV에서 컨텐츠 구매 기능, 디지털 도어락에서 스마트키 등록 등) 접근·사용은 사용자 인증 후 인가된 관리자/사용자로 제한
- 제품 사용 주체(Subject)의 권한과 접근·사용 대상인 객체(Object)의 보안 등급을 정의하여 RBAC (Role Based Access Control)과 같은 접근통제모델 기반의 접근통제 수행
- 제품을 구매한 사용자만 물리적으로 접근 가능하도록 물리적으로 통제 가능한 공간에 설치. 단, 무선통신(근거리 포함)으로 접속하여 설정하지 못해야 함

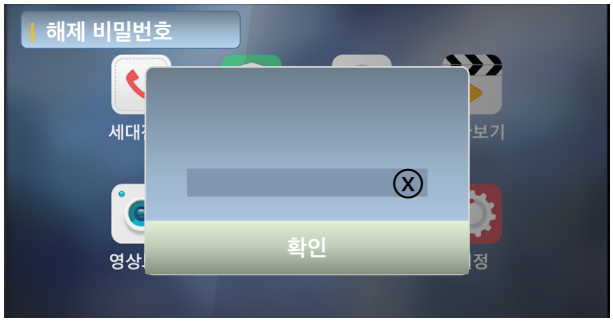
  ※ 예) 디지털 도어락 비밀번호 설정 또는 스마트키 등록을 위한 물리적 버튼을 문 안쪽에 설치

다. 예시

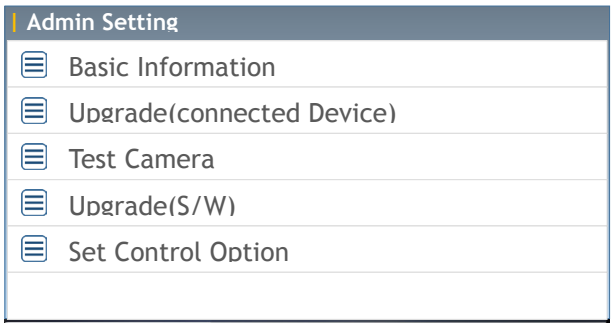
월패드 제품에서 관리자 권한을 가진 주체가 접근할 수 있는 기능에 일반 사용자는 접근할 수 없도록 한다.

• 관리자 페이지는 사용자 인증과는 다른 패스워드로 설정 •

관리자 페이지 로그인



관리자 페이지



라. 대상

- **특징** 관리자 설정 기능, 인증절차 후 접근
- **유형** 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “접근통제기반 개인정보관리 모델 연구”, 2007년11월

2) Ferraiolo, D.F. and Kuhn, D.R., “Role-Based Access Control” (PDF). 15th National Computer Security Conference: 554 – 563., Oct. 1992

3) Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E., “Role-Based Access Control Models” (PDF). IEEE Computer. IEEE Press. 29 (2): 38 – 47, Aug. 1996

2. IoT 제품 간 상호인증

2.1 상호인증

가. 개요

홈 · 가전 IoT 제품 간 상호인증 없이 상호 연결이나 데이터 전송을 허용할 경우 비인가된 사용자에 의해 제품이 제어되거나, 개인정보 등 민감정보가 유출될 수 있다. 이에 따라, 홈 · 가전 IoT 제품 간 데이터를 전송하거나 제어를 위해 연결을 수행하는 경우 상호인증을 수행해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 홈 · 가전 IoT 제품 구성요소간 또는 제품간 민감정보를 전송하거나 제어를 위한 연결 시도 시 상호인증을 선행해야 함

적용방안

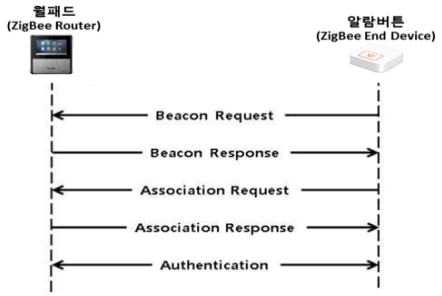
- 공개키암호 방식의 개인키를 이용한 상호인증 수행
  ※ 제조사(또는 서비스제공자)는 홈·가전 IoT 제품 제조 직후 주입되는 초기 암호키(PSK, Pre-Shared Key)를 안전하게 관리해야 하며, 초기 암호키 주입 시 인가된 직원이 안전한 장소에서, 안전한 방법으로 주입할 수 있도록 관리해야 함
- 보안속성 값(UID, Key 등), 보안칩 기반의 상호인증 수행
- 경량통신프로토콜인 CoAP 또는 L2M2M에 DTLS 적용하여 데이터 전송
- 경량통신프로토콜인 MQTT에 TLS 적용하여 데이터 전송
- 사전 등록된 서버*로 접속하여 서버에서 인증코드를 발급받아 인증하는 방식 사용
  * 서버 정보(예, IP 등)가 저장된 제품은 서버 정보에 대한 무결성을 보장해야 함
- 매뉴얼 방식으로 사용자가 상호인증(A↔B) 대상 제품(A)에 로그인 하여 상호인증 대상 제품(B)을 등록하고, 등록된 제품(B)으로 전송(예, SMS, BLE, NFC 등)된 인증코드를 입력하여 상호인증 수행

다. 예시

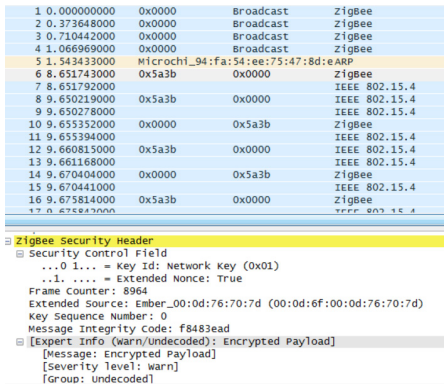
사용자 개인 단말(앱)을 통해 홈캠(웹캠)에서 취득한 정보(영상 데이터)를 요청할 때 홈캠(웹캠)은 사용자 개인 단말로 사용자 인증을 수행하도록 한다.

• ZigBee기반 월패드와 알람버튼의 등록 시 상호 인증 예시 •

ZigBee Secured 네트워크 상호 인증 절차



월패드와 알람버튼 인증 로그



라. 대상

- **특징** 세션 또는 채널을 통한 네트워크 통신, 관리자 설정 기능, 인증절차 후 접근, 유무선 상호 인증 및 데이터 통신, 전송 데이터 암호화
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 월패드, 홈캠(웹캠) 등 모든 홈·가전 IoT 제품

마. 참고자료

1) IETF RFC 7252 Constrained Application Protocol

2) Example : DTLS CoAP Server, github.com/cetic/6lbr/wiki/Example-:-Dtls-Coap-Server

3) OMA LightweightM2M V1.0 Overview,
www.openmobilealliance.org/wp/overviews/lightweightm2m_overview.html

4) IoT Standards, iot.eclipse.org/standards/

5) MQTT, mqtt.org

6) MQTT-TLS, github.com/hirotakaster/MQTT-TLS

제2절 암호화

1. 안전한 암호 알고리즘 사용

가. 개요

보안강도가 낮은 암호알고리즘을 사용하는 경우 데이터에 대한 암호문을 키 정보 없이도 짧은 시간 안에 복호화 할 수 있다. 그러므로 안전하게 데이터를 보호하기를 위해서는 국내에서 권고하는 암호알고리즘을 사용하거나 요구되는 보안강도 이상의 암호키 길이를 가진 암호알고리즘을 사용하여야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① **MD5(자체 결함 발생), DES, SHA-1(키 길이 보안강도가 낮음) 등 사용을 피하고, AES, ARIA, SEED, RSA 등 국제표준으로 등재된 표준 암호알고리즘 또는 국가정보원에서 안전성을 보증하는 검증 대상(ARIA, SEED, LEA, KCDSA, EC-KCDSA 등) 알고리즘을 선정하여 적용해야 함**

• 국내 권고 암호 알고리즘(112bit 기준) •

대칭키 암호 알고리즘	공개키 암호 알고리즘			해시 함수	
	키 공유	암 · 복호화용	전자서명용	메시지 인증, 키 유도, 난수생성용	단순해시, 전자서명용
국내 : SEED, ARIA, HIGHT 국외 : AES, 3TDES	DH, ECDH	RSAES-OAEP	RSASSA-PSS KCDSA ECDSA EC-KCDSA	SHA-224/256/384/512	SHA-224/256/384/512

출처: 암호 알고리즘 및 키 길이 이용 안내서, KISA, 2013

• 안전한 암호키 길이 •

보안 강도	대칭키 암호	해쉬 함수	공개키 암호				암호 알고리즘 안전성
			인수분해	이산대수		타원곡선 암호	
				공개키	개인키		
112bit	112	112	2048	2048	224	P–224/B–233	~2030년
128bit	128	112	3072	3072	256	P–256/B–283	2030년 이후
192bit	192	192	7680	7680	384	P–384/B–409	
256bit	256	256	15360	15360	512	P–512/B–571	

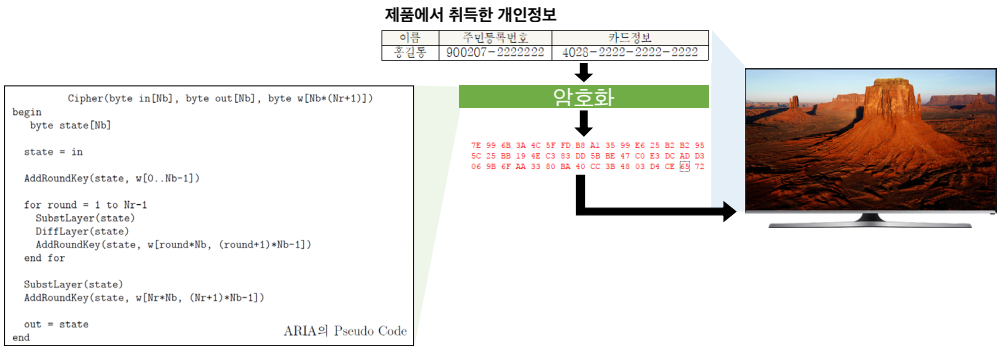
출처: 암호 알고리즘 및 키 길이 이용 안내서, KISA, 2013

적용방안

- 공개된 코드 사용 및 자체구현 시 검증을 위해 테스트벡터로 정확하게 구현되었는지 필수적으로 확인
- 저용량 제품에 대한 경량화 암호알고리즘(LEA, HIGHT 등) 사용
- 안전성이 검증되지 않은 암호알고리즘 또는 키 길이가 포함되는 경우 기본 설정값(Default)을 비활성화(Disable)로 설정
  * 안전성이 검증된 암호알고리즘 사용

다. 예시

암호알고리즘 ARIA를 사용하여 제품에서 취득한 개인정보(주민등록번호, 카드정보 등)를 암호화하여 사용하거나 저장한다.



라. 대상

- **특징** 금융, 개인정보 등 민감한 정보에 대한 기밀성 유지 및 데이터 진위, 출처 확인 등을 위한 무결성 수행, 데이터 기밀성/무결성을 위해 암호알고리즘 사용
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) 암호알고리즘 및 암호키 길이 선택 가이드
www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=82&ST=&SV=, 암호_알고리즘_및_키_길이_이용_안내서_2013.pdf

2) AES 구현 참고자료
csrc.nist.gov/groups/STM/cavp/block-ciphers.html

3) TDES 구현 참고자료
csrc.nist.gov/groups/STM/cavp/block-ciphers.html

4) ARIA 구현 참고자료
seed.kisa.or.kr/iwt/ko/bbs/EgovReferenceDetail.do?bbsId=BBSMSTR_000000000002&nttId=39&pageIndex=1&searchCnd=&searchWrd=

5) SEED 구현 참고자료
seed.kisa.or.kr/iwt/ko/sup/EgovSeedInfo.do

6) LEA 구현 참고자료
seed.kisa.or.kr/iwt/ko/sup/EgovLeaInfo.do

7) Digital signature 구현 참고자료
csrc.nist.gov/groups/STM/cavp/digital-signatures.html

8) Hash 구현 참고자료
csrc.nist.gov/groups/STM/cavp/secure-hashing.html

2. 안전한 암호키 관리

2.1 안전한 암호키 생성

가. 개요

안전하게 암호키가 생성되지 않을 경우 암호화된 데이터의 기밀성이 보장되지 않으므로 안전성이 검증된 방법으로 암호키를 생성해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 암호화 연산에 사용되는 암호키는 안전하게 생성해야 함

적용방안

- 암호키 생성에 필요한 난수는 안전한 난수발생기(RBG)를 이용해서 생성(예, KS X ISO IEC 18031)
- 초기 키는 제품별로 다른 키 사용이 원칙이나, 공통 키를 사용할 경우 서비스 이용 전에 제품마다 다른 키로 갱신하여 사용
- 초기 암호키는 인가된 직원이 안전한 장소에서 안전한 방법으로 주입할 수 있도록 관리
- 공개키 암호알고리즘을 위한 키 생성 시 개인키 소지자(사용자)가 직접 공개키-개인키 쌍을 생성하거나 신뢰할 수 있는 기관에서 공개키-개인키 쌍을 생성하여 안전한 방법으로 개인키 소지자(사용자)에게 전달
- 디지털서명 알고리즘(DSA, KCDSA, EC-DSA, EC-KCDSA)용 공개키 쌍 생성 시 KS X ISO IEC 14888-3 또는 안전한 난수발생기를 통해 생성
- 대칭키 암호알고리즘을 위한 키 공유 시 키를 공유할 실체 간 안전한 프로토콜을 통해 키를 공유하거나 신뢰할 수 있는 기관에서 키를 생성하여 안전한 방법으로 배포
- 검증된 암호키 관리 솔루션 사용

다. 예시

안전한 난수를 사용하여 암호키를 생성하고, 표준기반 키생성 함수를 사용한다. 또한, 인가된 관리자가 인가된 장소에서 안전하게 키를 주입한다.

라. 대상

- **특징** 금융, 개인정보 등 민감한 정보에 대한 기밀성 유지 및 데이터 진위, 출처 확인 등을 위한 무결성 수행, 데이터 기밀성/무결성을 위해 암호알고리즘 사용
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 암호키 관리 안내서
www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=83&ST=total&SV=, 암호키 관리 안내서.pdf

2) PKCS #5 v2.1 : Passowrd-Based cryptoraphy standard
www.emc.com/collateral/white-papers/h11302-pkcs5v2-1-password-based-cryptography-standard-wp.pdf

3) Key Derivation Using Pseudorandom Functions Validation System
csrc.nist.gov/groups/STM/cavp/documents/KBKDF800-108/kbkdfvs.pdf

4) Recommendtaion for Password-Based Key Derivation
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

2.2 안전한 암호키 전송

가. 개요

암호키 전송 시 전송 오류 등으로 키가 변경되는 경우 IoT 제품의 암호 기능이 정상 동작하지 않을 수 있으며, 중간자 공격 등으로 의도하지 않은 키가 전송되는 경우 보안에 취약할 수 있으므로 안전하게 암호키를 전송해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 다음을 고려하여 안전하게 암호키를 전송해야 함

- 암호키에 대한 분배는 안전성이 검증된 분배 방법 사용
- 전자서명 등을 이용하여 전송되는 키의 출처를 확인할 수 있어야 함
- 전송된 암호키의 변경·변조 여부를 확인할 수 있도록 무결성 검증 메커니즘 제공
- 암호키의 기밀성 유지를 위해 다른 키로 암호화하여 전송
- 암호키 수신 후 무결성 검증 결과 무결성이 손상된 경우, 해당키는 사용할 수 없도록 파기

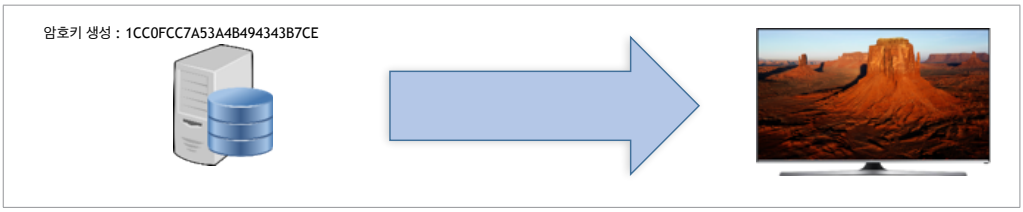
적용방안

- 암호키에 대한 분배는 안전성이 검증된 분배 방법 사용
  예) (U)SIM AKA, ECDSA 기반 ECDH, TLS/DTLS, Security API 등
- 암호키를 Online으로 전송할 경우에는 출처를 알 수 있는 안전한 방법(전자서명, HSM 등)으로 전송하고, Offline으로 주입(전송)할 경우에는 안전한 장소에서 인가된 관리자에 의해서만 수행
- 암호키 전송 시 일반적으로 무결성을 보증하기 위해 해시값(SHA2)을 사용해야 하지만 저사양 IoT 제품의 경우 CRC32 등을 이용하여 위·변조 여부를 확인
- 암호키 전송 시 안전하게 공유된 공개키·비밀키로 암호화하여 전송하거나 저사양 IoT 제품의 경우 여러 조각으로 분리하여 전송함으로써 전체 키에 대한 접근을 불가능하도록 함

다. 예시

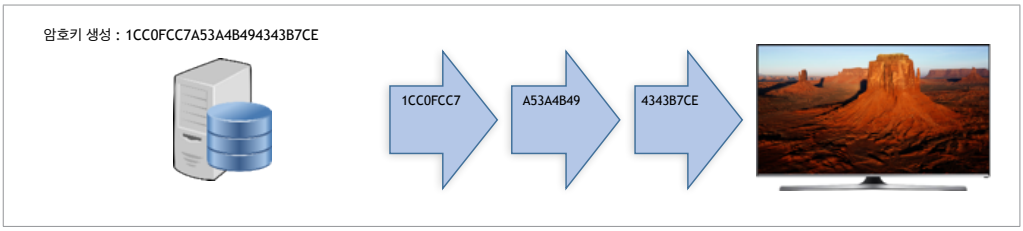
월패드에서 사용하는 암호키를 분배할 때, 키 암호화용 키를 생성하여 공유 후 암호화하여 전송하거나 키를 분산하여 전송함으로써 키를 보호한다.

• 암호키 단순 전송 방식 •



• 암호키 암호화 전송 •

• 암호키 분산 전송 •



라. 대상

- **특징** 금융, 개인정보 등 민감한 정보에 대한 기밀성 유지 및 데이터 진위, 출처 확인 등을 위한 무결성 수행, 데이터 기밀성/무결성을 위해 암호알고리즘 사용
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 암호키 관리 안내서
www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=83&ST=total&SV=, 암호키 관리 안내서.pdf

2.3 안전한 암호키 저장

가. 개요

암호화에 사용되는 암호키 노출 시 주요 정보에 대한 기밀성 및 무결성이 훼손 될 수 있으므로 암호키를 안전하게 관리해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 다음 사항을 고려하여 안전하게 암호키를 관리해야 함

- 모든 암호키는 가용성 및 무결성, 기밀성을 보장받을 수 있도록 저장
  ※ 공개키는 기밀성이 반드시 보장될 필요는 없음
  ※ 암호키 관련 데이터(예, SEED값)에 대한 무결성, 기밀성 필요
- 암호키는 (물리적/논리적)비인가된 접근으로부터 보호
  ※ 대칭키 및 개인키를 하드웨어 보안 방식으로 저장 시 KS X ISO/IEC 19790의 보안수준 2 이상을 따르는 안전한 모듈에 보관
  ※ 대칭키 및 개인키를 소프트웨어 보안 방식으로 저장 시 분산 저장 혹은 Random Pool을 사용하여 안전하게 보관
- 데이터의 중요도, 노출 위험도, 노출 시 위험 수준 등에 따라 사용되는 암호키의 사용기간 및 유효기간을 설정
  ※ 중요하고 민감한 데이터일수록 키의 사용기간을 짧게 설정
- 사용기간이 만료된 키 또는 키에 대한 무결성 오류 발생 시 해당키 사용 중지

적용방안

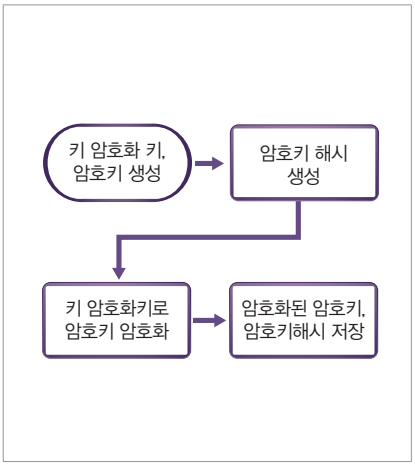
- 외부 키 관리 서버(CKMS, Cryptogram Key Management System)를 활용하여 외부에서 암호키 관리

- 공개키, 개인키를 안전한 암호모듈 외부에 보관하는 경우 키 암호화 또는 암호키에 대한 물리적 보호
- 무결성 검증에 대해 암호화 메커니즘이 불가한 경우 비암호화 메커니즘 수행(CRC32 등)
- 검증된 암호키 관리 솔루션 사용

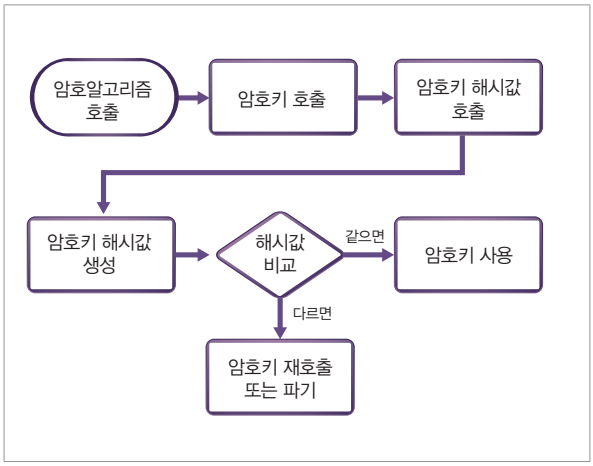
다. 예시

대칭키 및 개인키는 KS X ISO/IEC 19790의 보안수준 2 이상을 따르는 안전한 모듈에 보관하고, 암호키 저장 시 해시값을 생성하고, 호출 및 사용 시 해시값을 비교하여 암호키가 변조되지 않았음을 확인한다.

• 암호키 생성 시 •



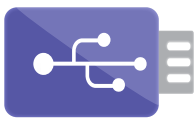
• 암호키 호출/사용 시 •



모든 대칭키, 개인키는 저장된 상태에서 기밀성이 유지되어야 하고 (물리적/논리적) 비인가된 접근으로부터 보호되어야 한다.

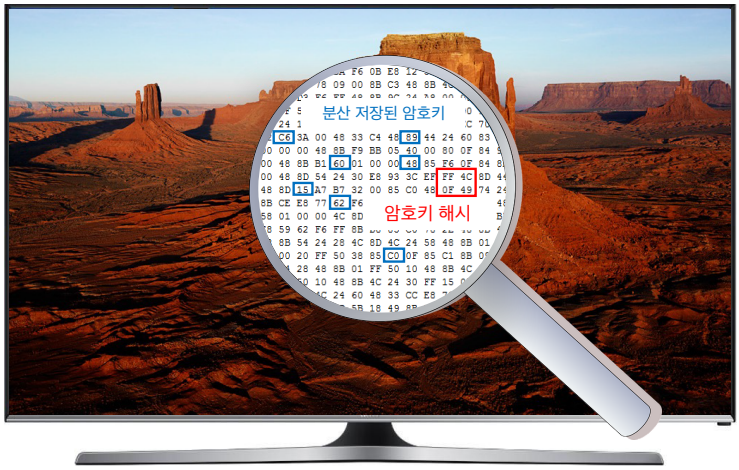
– 폐쇄형 IC 플랫폼과 개방형 IC 플랫폼 기반의 탐침 기능이 탑재된 하드웨어 보안 카드 및 칩인 Secure Element(PUF, USIM, eSIM, eSE, TEE, TPM, 보안MCU, 보안 SoC 등)를 이용한 하드웨어 보안 방식으로 시크릿(secret) 정보(Key, 보안속성 값 등)를 위하여 안전한 저장소에 저장

• USB 토큰 •



• 스마트카드 •

– 국내외 표준/가이드 문서/보안표준에 준하는 SW 보안방식 기반 암호키에 대한 관리 및 접근통제방법 (예, 암호키 분산 저장, Random Pool 등)을 사용



라. 대상

- **특징** 금융, 개인정보 등 민감한 정보에 대한 기밀성 유지 및 데이터 진위, 출처 확인 등을 위한 무결성 수행, 데이터 기밀성/무결성을 위해 암호알고리즘 사용
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) 암호키 관리 안내서
www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=83&ST=total&SV=, 암호키 관리 안내서.pdf

2.4 안전한 암호키 파기

가. 개요

암호키가 저장소, 메모리 등에 남아있는 경우 암호키의 탈취 및 주요 데이터 노출의 위험이 있으므로 사용 기간이 만료된 암호키 혹은 사용 후 메모리에 남아있는 암호키는 반드시 삭제해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 다음을 고려하여 안전하게 암호키를 파기해야 함

- 사용이 만료된 개인키 및 대칭키는 즉시 파기
- 키 생성을 위한 파라미터 및 암호키 등은 사용 후에 메모리를 다른 값으로 채우거나 임시파일을 영구 삭제하여 복구 불가능하도록 해야 함

적용방안

- 메모리 또는 기억장소에서 암호키에 대한 삭제가 불가능할 경우 임의의 값을 계속 저장하여 기존 키 정보를 찾을 수 없도록 함
- 검증된 암호키 관리 솔루션 사용
- 본 가이드 “물리적 보안“절을 참조하여 대응할 수 있음‘

다. 예시

안전성이 검증된 암호키 삭제 방법 중 대표적인 소프트웨어 보안 방식은 키가 저장된 메모리를 ‘0’ 등의 특정 문자로 채운 후 해당 메모리를 해제한다. 참고로, DoD 5220.22-M(또는 DoD 5200.28-STD)에 따르면 키 정보를 완전삭제하기 위해서는 최소 3회 이상의 덮어쓰기 등을 하는 것으로 기술되어 있다.

하드웨어 보안(SE, HSM) 방식은 적법한 접근 권한을 얻은 후 Delete 명령을 통하여 파일 구조 혹은 DB에 저장된 키 정보를 삭제한다.

라. 대상

- **특징** 금융, 개인정보 등 민감한 정보에 대한 기밀성 유지 및 데이터 무결성, 출처 확인 등을 위한 무결성 검증 수행, 데이터 기밀성을 위해 암호알고리즘 사용
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 암호키 관리 안내서
www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=83&ST=total&SV=, 암호키 관리 안내서.pdf

3. 안전한 난수 생성 알고리즘 사용

가. 개요

난수 생성 알고리즘은 암호화 및 키 공유 등에 사용되는 키를 생성하기 위해 사용된다. 예측 가능하거나 연관성이 존재하는 난수들은 보안성이 위협받을 수 있다. 따라서 난수성이 검증된 난수 생성 알고리즘을 사용해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 난수 생성 시 국내외 표준에 따른 안전한 난수 발생기를 이용하여 난수를 생성해야 함

적용방안

- PRNG (Pseudo-Random Number Generator) 사용
  - 거의 실물과 같은 수준의 random seed를 기반으로 한 난수
- 검증된 난수 발생기 솔루션 사용

다. 예시

홈캠(웹캠)에서 난수 생성 알고리즘을 사용하여 암호키를 생성하는 경우 국내외 표준을 따르는 안전한 난수 생성 알고리즘을 사용하여 암호키를 생성한다.

라. 대상

- **특징** 금융, 개인정보 등 민감한 정보에 대한 기밀성 유지 및 데이터 무결성, 출처 확인 등을 위한 무결성 검증 수행, 데이터 기밀성을 위해 암호알고리즘 사용, 암호키 생성 등 난수 사용
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) ISO/IEC 18031, “Information technology — Security techniques — Random bit generation”, 2011년

2) NIST SP 800–90A, “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”, 2015년 10월

3) KS X ISO/IEC 18031:2013, “정보기술－보안기술－난수 발생기”, 2013년 12월

제3절 데이터 보호

1. 안전한 통신채널

1.1 안전한 통신채널 제공

가. 개요

홈 · 가전 IoT 제품에서 전송되는 중요 데이터를 제3자가 도청 및 위 · 변조하는 것을 방지하기 위해 안전한 암호화 통신채널을 제공해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① (Bluetooth) BLE(Bluetooth Low Energy)는 BLE 4.0/4.1과 낮은 버전의 제품은 보안모드 1의 보안레벨 3(암호화된 인증 페어링)을 적용하고, BLE 4.2 제품 및 서비스는 보안모드 1의 보안레벨 4(암호화된 저전력 보안연결 인증)를 적용해야 함

• BLE 보안모드 단계 •

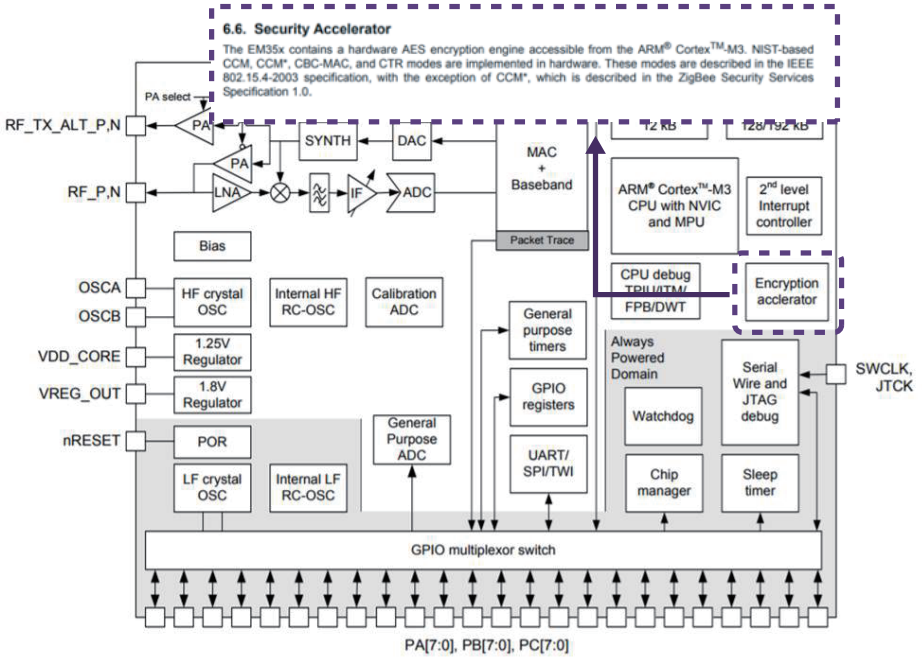
보안레벨진위	LE(저전력) 보안 모드 1	LE(저전력) 보안 모드 2
1	보안 없음 (인증 및 암호화 없음)	데이터 서명을 통한 인증되지 않은 페어링
2	암호화되지 않은 페어링	데이터 서명을 통한 인증된 페어링
3	암호화된 인증 페어링	–
4	128비트 강도 암호화키로 암호화된 저전력 보안연결 인증	–

출처: https://www.bluetooth.org

② (Zigbee) ZigBee의 CCM 운영모드를 AES-CBC-MAC-128(보안강도 128비트 이상의 메시지인증) 또는 AES-CCM-128(보안강도 128비트 이상의 암호화 및 메시지인증)로 선택적으로 사용해야 함

* IEEE 802.15.4 Security 128-bit AES을 지원하는 IC 사용

• SILICON LABS 사 ZigBee IC : AES Encryption 지원 •



③ (Z-Wave) Z-Wave 인증을 받고 S2(시큐리티 2) 프레임워크를 적용해야 함

- Z-Wave S2(시큐리티 2) 프레임워크의 주요 특징
  - AES 128bits
  - ECDH(Elliptic Curve Diffie-Hellman) 기반의 안전한 키 교환
  - 인증된 배포로 “man-in-the-middle” 공격 벡터 제거
  - 안전한 TLS 1.1 터널을 통해 모든 Z/IP 트래픽에 대해 Z-Wave 터널링 제공

④ (WiFi) WPA2 방식을 적용하고, WPA2-PSK의 경우 초기 무선랜 인증 시 4-way 핸드쉐이킹 단계의 무선 패킷 수집을 통해 비밀키 유추가 가능한 문제가 있으므로 비밀키는 특수문자를 포함한 임의의 문자를 사용하여 최대한의 자리수를 사용항목

• 무선인증방식 •

항목	Static WEP Key	Dynamic WEP Key	WPA v1	WPA v2
보안키	WEP(24Bit IV)	WEP(24Bit IV)	TKIP(48Bit IV)	CCMP
암호화 알고리즘	RC4	RC4	RC4	AES
암호화 비트	20/128 Bit	128 Bit	128 Bit	128 Bit
보안레벨	하(매우취약)	중/상	상	최상

⑤ (SSL/TLS) TLS 최신 버전(예: TLS 1.2)을 사용하고, 안전한 암호 알고리즘 조합 적용

• SSL/TLS 프로토콜 버전별 안전성 •

암호			프로토콜 버전					
종류	알고리즘	강도 (bits)	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (Draft)
블록암호 및 연산모드	AES GCM	128, 256	N/A	N/A	N/A	N/A	Secure	Secure
	AES CCM		N/A	N/A	N/A	N/A	Secure	Secure
	AES CBC		N/A	N/A	Depends on mitigations	Secure	Secure	N/A
	Camellia GCM	128, 256	N/A	N/A	N/A	N/A	Secure	Secure
	Camellia CBC		N/A	N/A	Depends on mitigations	Secure	Secure	N/A
	ARIA GCM	128, 256	N/A	N/A	N/A	N/A	Secure	Secure
	ARIA CBC		N/A	N/A	Depends on mitigations	Secure	Secure	N/A
	SEED CBC	128	N/A	N/A	Depends on mitigations	Secure	Secure	N/A
	3DES EDE CBC	112	Insecure	Insecure	Insecure	Insecure	Insecure	N/A
	GOST 28147–89 CNT	256	N/A	N/A	Insecure	Insecure	Insecure	–
	IDEA CBC	128	Insecure	Insecure	Insecure	Insecure	N/A	N/A
	DES CBC	056	Insecure	Insecure	Insecure	Insecure	N/A	N/A
		040	Insecure	Insecure	Insecure	N/A	N/A	N/A
	RC2 CBC	040	Insecure	Insecure	Insecure	N/A	N/A	N/A
스트림 암호	ChaCha20–Poly1305	256	N/A	N/A	N/A	N/A	Secure	Secure
	RC4 RC4	128	Insecure	Insecure	Insecure	Insecure	Insecure	N/A
		040	Insecure	Insecure	Insecure	N/A	N/A	N/A
None	Null	–	N/A	Insecure	Insecure	Insecure	Insecure	Insecure

출처: https://en.wikipedia.or

⑥ **(기타) 안전한 통신 채널 제공을 위한 특정 프로토콜 규격을 사용하고 있지 않은 경우 상호인증 및 키 일치(공유)를 수행 후 안전한 구간 암호화 수행**

적용방안

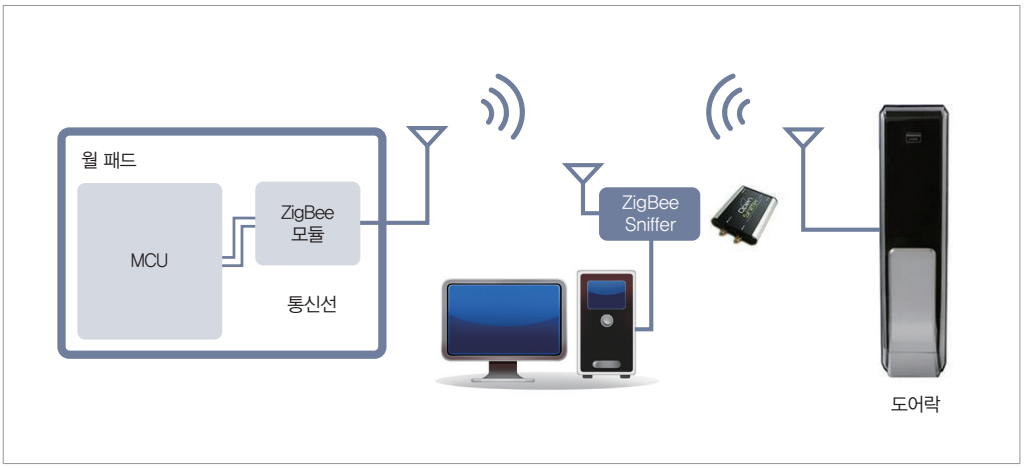
- 다른 무선통신 프로토콜을 적용하는 경우, 안전한 암호화 알고리즘을 사용하도록 설정하여 통신채널 제공
- 전송데이터에 대해 기밀성(예, AES, SEED, ARIA, LEA, HIGHT 등 안전한 암호알고리즘 사용) 및 무결성(예, SHA2 등 안전한 해시알고리즘 사용) 보호대책 적용하여 전송

다. 예시

다음은 홈 · 가전 IoT 제품에서 월패드와 디지털도어락 간의 안전한 통신채널 제공에 대한 예시로, 암호화를 적용한 ZigBee 무선통신 채널을 기반으로 월패드와 디지털도어락간 통신을 수행한다.

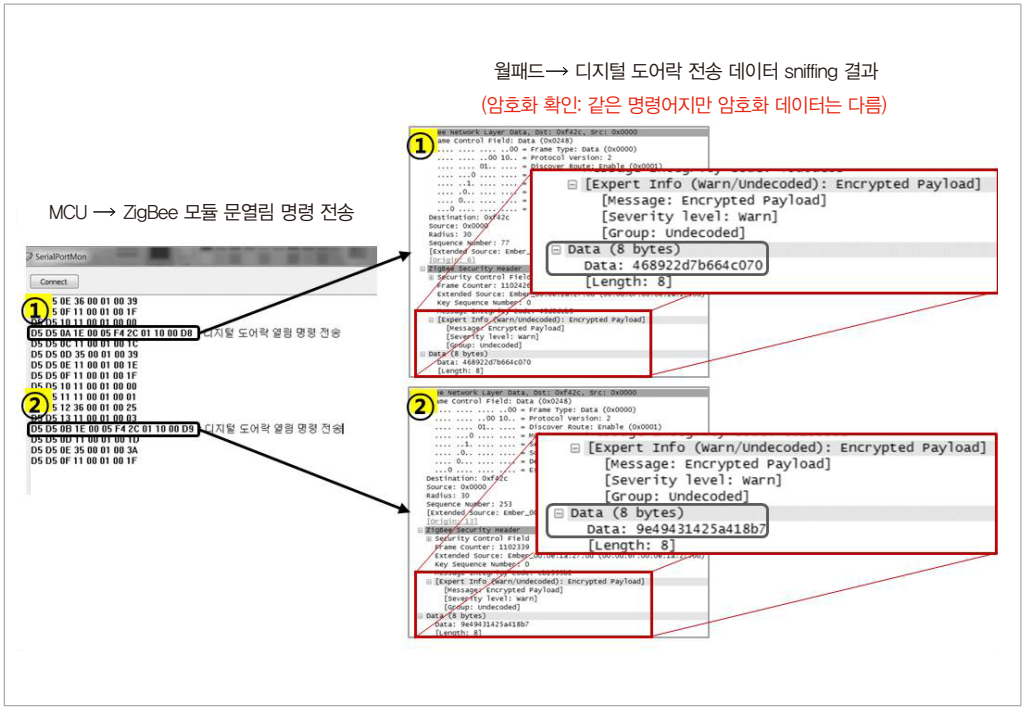
월패드와 디지털도어락 간 통신 패킷을 스니핑 도구를 이용하여 도어락 열림 명령어가 암호화되어 있는지를 확인할 수 있다.

• **월패드와 디지털 도어락 통신 구간 암호화 예시** •



월패드에서 디지털도어락으로 전송되는 제어 명령어(예, 열림)는 암호화되어 전송되고, 반복 전송되는 동일한 제어 명령어에 대해 이전과 다르게 암호화된 값이 전송되고 있음을 확인할 수 있다. 또한 ZigBee 무선통신에서 암호화에 IEEE 802.15.4 보안 모드는 적용하지 않고, ZigBee 보안 기능을 사용하고 있음을 확인할 수 있다.

• 월패드와 디지털 도어락간 암호화를 적용한 무선통신 분석 예시 •



라. 대상

- **특징** 유무선 상호 인증 및 데이터 통신, 전송 데이터 암호화
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트온도계, 디지털도어락, 스마트TV, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) Bluetooth 사이트, www.bluetooth.org

2) NIST Special Publication(SP) 800–121 Rev.2,"Guide to Bluetooth Security", 2017년 5월

3) Zigbee alliance 사이스, www.zigbee.org

4) Z-Wave 사이트, z-wave.sigmadesigns.com, z-wavealliance.org/z-wave-alliance-announces-new-security-requirements-z-wave-certified-iot-devices/

5) 방송통신위원회, KISA,"무선랜 보안 안내서", KISA안내 · 해설 제2010-12호, 2010년 1월

6) IETF RFC 5246 (The Transport Layer Security Protocol Version 1.2), tools.ietf.org/html/rfc5246, en.wikipedia.org/wiki/Transport_Layer_Security

7) SSL/TLS 프로토콜 정보, en.wikipedia.org/wiki/Transport_Layer_Security

8) 3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 14)

9) NIST FIPS 186-2 X9.62 & X9.63, SEC2

10) SW(구간 암호화) 국가정보원 사이트, http://www.nis.go.kr/AF/1_7_3_3/list.do

1.2 안전한 세션관리

가. 개요

홈 · 가전 IoT 제품은 인가된 사용자임을 구분하기 위하여 세션ID를 사용한다. 순차적으로 증가하는 값이나 패턴 분석이 가능한 값, 단순값 등 예측 가능한 세션ID 를 사용하는 경우, 세션하이재킹과 같은 공격으로 인가되지 않은 사용자가 시스템을 사용할 수 있게 된다. 또한 연결이 종료된 세션정보가 삭제되지 않는 경우 비인가된 사용자에 의해 해당 연결이 재사용될 수 있으며, 중요정보에 접근하거나 중요기능을 악용하는 문제가 발생할 수 있다. 이에 따라, 세션ID에 대한 안전한 관리가 필요하다.

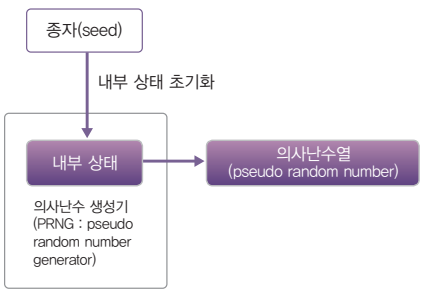
나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 세션ID는 최소 128비트의 길이로 생성되어야 하며, 안전한 난수 알고리즘을 적용하여 예측이 불가능한 값을 사용해야 함

세션 구성을 위해 사용되는 난수생성기는 다음과 같은 의사난수 생성기를 사용할 수 있다.

[의사난수 생성기 구조 예시]

구조	설명
	• 내부 상태 = 메모리값 • 내부 상태에 의해 다음에 생성할 의사난수가 정해지므로 내부 상태가 공격자에게 알려지지 않게 하여야 함 • 외부에서 주어지는 종자(seed)는 의사난수 생성기의 내부상태를 초기화함

적용방안

- 웹서버나 웹 애플리케이션 플랫폼에서 제공하는 세션 ID 사용
- 하드웨어로 구성된 의사난수 생성기를 통해 세션 ID 구성

② **세션 인증 시마다 주기적으로 세션ID를 바꾸어야 하며, 일정 시간이 지난 후에 세션ID를 폐기해야 함**

세션 만료에 대한 ASP, JSP 적용 방안은 다음과 같다.

• ASP

- 접속자별로 세션을 생성하여 사용자의 정보를 각각 저장할 수 있는 Session 오브젝트를 사용하여 타임아웃 기능을 구현한다.
- Session 오브젝트는 페이지의 접근을 허가하거나 금지할 때 또는 사용자별로 정보를 저장할 때 많이 사용하며 접속자의 브라우저에서 쿠키기능을 지원해야 Session 오브젝트의 사용이 가능하다. 다음과 같은 설정이 적용될 경우 사용자가 로그아웃할 때 세션은 바로 삭제되며, 로그아웃하지 않고 10분 동안 웹 서버로의 요청이 없을 경우에도 세션은 종료된다.
  예) Session.Timeout = 10

[ASP의 세션 관련 항목 예시]

구분		설 명
Property	SessionID	사용자마다 갖게 되는 고유한 세션값
	Timeout	세션이 유지되는 시간
Method	Abandon	강제로 세션을 소멸시키는 함수
Event	Onstart	각각의 사용자가 처음 방문할 때 발생
	Onend	사용자의 세션이 끝나는 시점에 발생

• JSP

- 세션타임아웃기능을 구현하는 방법은 session.getLastAccessedTime() 를 이용하여 세션의 마지막 접근 시간으로부터 일정 시간 이내에 다시 세션에 접근하지 않은 경우 자동으로 세션을 종료하도록 구현한다.
- 세션의 타임아웃은 두 가지 방법으로 설정할 수 있다.

  (1) web.xml 파일에서 〈session-config〉 태그를 사용하여 타임아웃을 지정하는 방법

  (2) session 기본 객체가 제공하는 setMaxInactiveInterval() 메소드를 사용

  〈% session.setMaxInactiveInterval(600); %〉

적용방안

- 주기적으로 세션ID를 재할당하고 세션 정보를 삭제하도록 함
  ※ (Java언어) session.invalidate() 메소드를 사용하여 세션에 저장된 정보 삭제
- 웹 브라우저 종료로 인한 세션종료는 서버 측에서 인지할 수 없기 때문에, 일정시간 동안 사용되지 않는 세션 정보는 강제적으로 삭제하도록 함
- 로그인 성공 시 로그인 전에 할당받은 세션ID는 파기하고 새로운 값으로 재할당

③ 홈 · 가전 IoT 제품은 세션에 마지막으로 접근한 시간으로부터 일정 시간 동안 동작이 없을 경우 세션 잠금을 하고, 재접속 시 재인증을 수행해야 함

적용방안

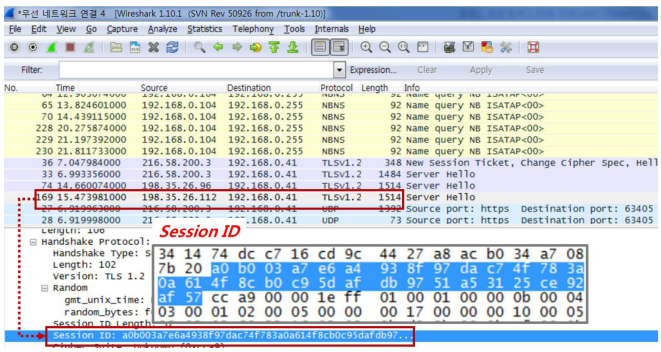
- 세션이 마지막으로 접근한 시간 이후 일정 시간* 동안 동작이 없을 경우 세션 종료
  * 제조사에서 일정 수준의 시간을 기본값으로 설정하여 출시하고, 사용자에 의해 변경할 수 있도록 구현 가능
  ※ (참고) "전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드"에서는 세션타임아웃을 중요기능의 경우 2~5분, 위험도가 낮은 기능의 경우 15~30분으로 설정하는 방안에 대해 설명하고 있음

다. 예시

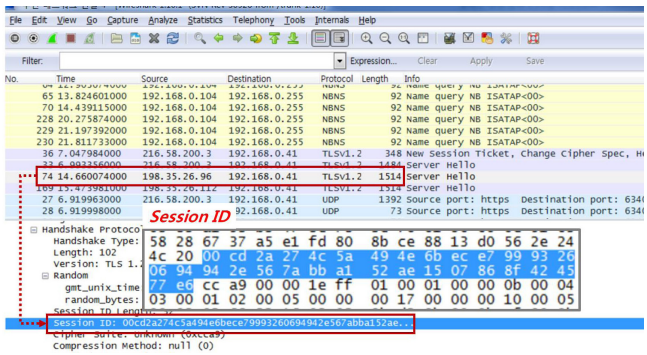
웹캠은 서버 등에 연결할 때마다 세션 ID를 새롭게 랜덤으로 생성함으로써 세션 ID를 예측하는 것을 방지하고 재사용 공격 등에 방어해야 한다.

• 웹캠 제품의 최초 인증정보 입력 및 변경 예시 •

설치 시

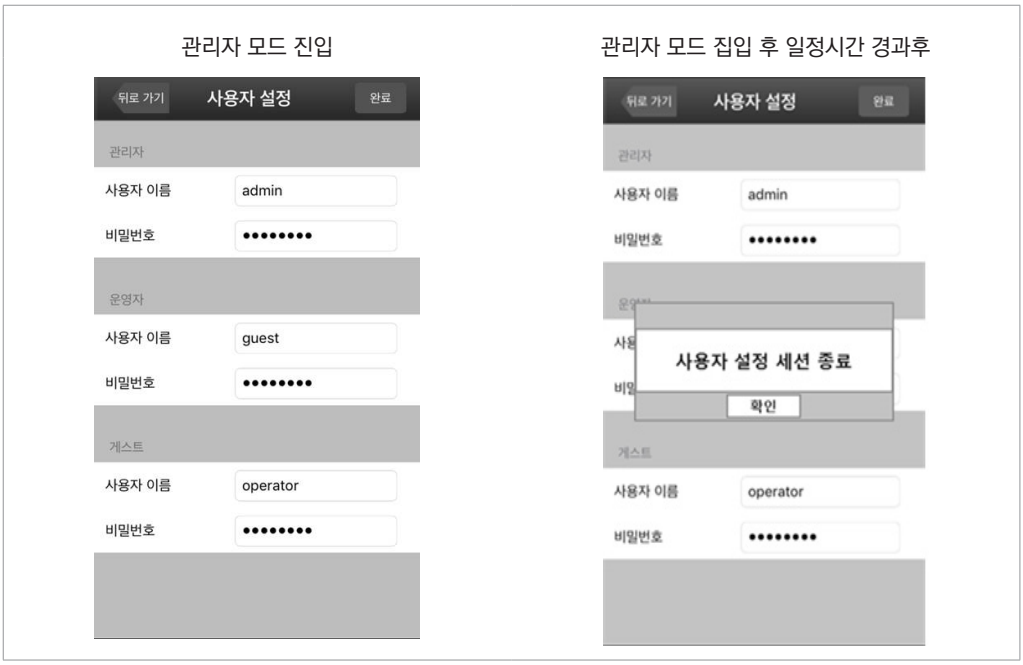


운용 시



월패드 등 관리자 모드가 별도로 있는 제품은 관리자 모드 진입 후 일정시간 동안 동작이 없을 경우 자동으로 세션을 종료하고 메시지로 알려야 한다.

• 관리자 모드 진입 후 자동 세션 잠금/종료 예시 •



라. 대상

- **특징** 세션 또는 채널을 통한 네트워크 통신, 관리자 설정 기능, 인증절차 후 접근, 유무선 상호 인증 및 데이터 통신, 전송 데이터 암호화
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “홈페이지 취약점 진단 · 제거 가이드”, 2013년 12월
www.kisa.or.kr/public/laws/laws3_View.jsp?mode=view&p_No=259&b_No=259&d_No=49&ST=T&SV=

2) 행정안전부, 한국인터넷진흥원, “전자정부 SW 개발 · 운영자를 위한 소프트웨어 개발보안 가이드”, 2017.

2. 저장 및 전송 데이터 보호

2.1 전송데이터 보호

가. 개요

홈 · 가전 IoT 제품에서 전송되는 중요정보(예, 인증정보, 제어정보, 센싱정보 등)가 외부로 유출되어 임의로 도용(재사용 등)되거나 위 · 변조되는 것을 방지하기 위해 중요정보를 보호하고 안전하게 전송할 수 있는 방안을 고려해야 한다.

나. 보안대책

홈 · 가전 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 인증정보, 개인정보 등 민감정보 전송 시 기밀성 및 무결성을 보장해야 함

적용방안

- 안전한 암호알고리즘(AES, LEA, HIGHT, SHA2(224/256/384/512) 등) 사용
  ※ 본 가이드의 '암호화' 내용 참조
- 안전한 통신채널을 사용하여 전송
  ※ 본 가이드의 '안전한 통신채널 제공' 내용 참조

② 제어정보 및 센싱정보 전송 시 무결성을 보장해야 함

적용방안

- 안전한 해시알고리즘(SHA2(224/256/384/512) 등) 사용
  ※ 본 가이드의 '암호화' 내용 참조
- 안전한 통신채널을 사용하여 전송
  ※ 본 가이드의 '안전한 통신채널 제공' 내용 참조

③ 제어정보 및 전송 시 재생 공격을 방지해야 함

적용방안

- 송신 측에서 타임스탬프, 시퀀스를 추가하고 전체 데이터를 서명해야 함
- 수신 측에서 서명을 검증하고 타임스탬프 및 시퀀스의 재사용 여부를 확인해야 함

④ 펌웨어, 제품 제어 정보 등 전송 시 중간자 공격을 방지해야 함

적용방안

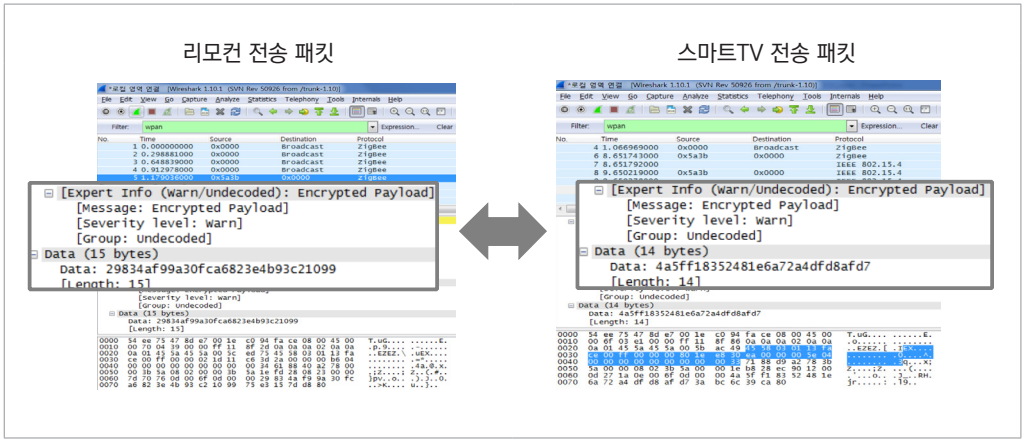
- 서버에 CA 서명을 받은 인증서 및 개인키를 설치해야 함
- IoT 제품에서 서버와 통신 시도 시 서버 인증서의 진위를 검증 후 통신해야 함

다. 예시

ZigBee 통신 시 ZigBee 표준에 따른 암호화 통신을 해야 하며 802.15.4 표준에 따른 암호화 통신을 추가로 적용하여 전송데이터를 보호해야 한다. 다음 그림은 월패드와 알람버튼 간 통신 데이터의 암호화 형식을 보여 주고 있다.

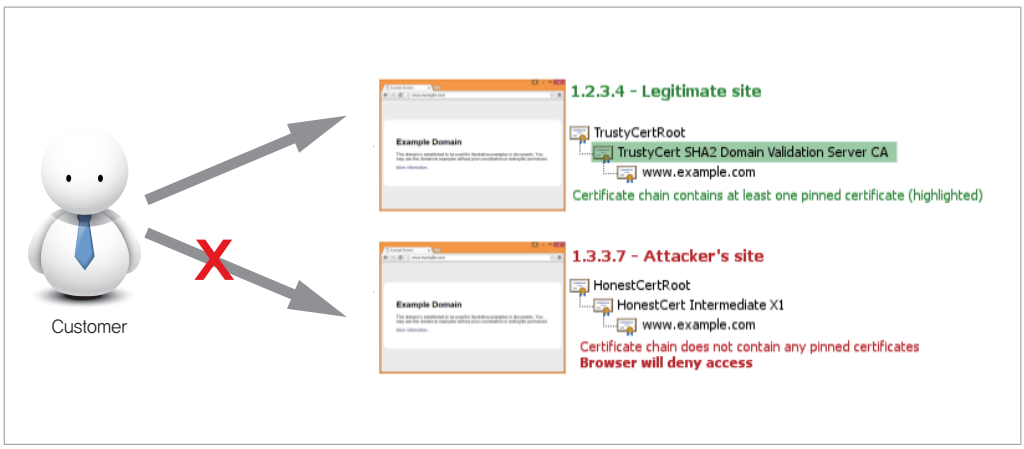
• 웹 캠 제품의 최초 인증정보 입력 및 변경 예시 •

• ZigBee 통신 암호화 통신 패킷 •



TLS를 이용하여 전송 구간을 암호화 하더라도 공격자가 프록시 도구를 이용하여 중간자 공격을 할 수 있는 네트워크 구간이 존재한다면 기밀성이 보장되지 않는다. 또한 IoT 제품이 수신한 공개키 정보가 다르거나 공개키 서명자가 신뢰 목록에 없는 경우 중간자 공격의 가능성이 있다. 브라우저와 달리 IoT 제품에는 이러한 기능이 자동으로 제공되지 않으므로, 제품에서 TLS 통신을 구현할 경우 서버 인증서를 검증하여 신뢰할 수 있는 경우에만 통신을 수락하는 로직을 추가해야 한다.

• 중간자 공격 방지 매커니즘 •



라. 대상

- **특징** 유무선 상호 인증 및 데이터 통신, 전송 데이터 암호화
- **유형** 센싱(무결성), 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) Bluetooth 사이트, www.bluetooth.org

2) NIST Special Publication(SP) 800-121 Rev.2,"Guide to Bluetooth Security", 2017년 5월

3) Zigbee alliance 사이스, www.zigbee.org

4) Z-Wave 사이트, z-wave.sigmadesigns.com,
z-wavealliance.
org/z-wave-alliance-announces-new-security-requirements-z-wave-certified-iot-devices/

5) 방송통신위원회, KISA,"무선랜 보안 안내서", KISA안내 · 해설 제2010-12호, 2010년 1월

6) IETF RFC 5246 (The Transport Layer Security Protocol Version 1.2),
tools.ietf.org/html/rfc5246, en.wikipedia.org/wiki/Transport_Layer_Security

7) SSL/TLS 프로토콜 정보, en.wikipedia.org/wiki/Transport_Layer_Security

8) Certificate Pinning, https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

2.2 저장데이터 보호

가. 개요

홈 · 가전 IoT 제품 내부에 저장되는 중요데이터(설정파일, 암호키, 인증정보 등)가 유출될 경우 악용될 우려가 있으므로 비인가된 접근 및 변경으로부터 보호해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① IoT 제품의 보안을 손상시킬 수 있는 중요정보*는 기밀성 및 무결성이 보장되어야 함

중요정보 예시

- 데이터를 암호화하기 위한 평문과 암호문으로 된 비밀키, 개인키, 공개키
- 비밀번호 또는 개인식별번호(PIN)와 같은 인증 데이터
- 제품이 수집한 사용자 민감 데이터
- 기타 제품 운영 관련 중요 정보
  (예 : 제품의 설정 값(IP/MAC값), 보안정책, 감사 사건과 감사 데이터 등)

• 보안강도에 따른 대칭키 암호 알고리즘 분류 •

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPY(유럽)	국내
112 비트 이상	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 3TDEA KASUMI Blowfish	SEED HIGHT ARIA-128/192/256
128 비트 이상	AES-128/192/256	AES-128/192/256 Camellia-128/192/256 MISTY1	AES-128/192/256 KASUMI Blowfish	SEED HIGHT ARIA-128/192/256
192 비트 이상	AES-192/256	AES-192/256 Camellia-192/256	AES-192/256 Blowfish	ARIA-192/256
256 비트 이상	AES-256	AES-256 Camellia-256	AES-256 Blowfish	ARIA-256

출처: 암호 알고리즘 및 키 길이 이용 안내서 2013

• 보안강도에 따른 메시지인증/키유도/난수생성용 해시함수 분류 •

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPY(유럽)	국내
112 비트 이상	SHA–224/256/384/512	SHA–256/384/512	SHA–224/256/384/512 Whirlpool	SHA–256/384/512
128 비트 이상	SHA–256/384/512	SHA–256/384/512	SHA–256/384/512 Whirlpool	SHA–256/384/512
192 비트 이상	SHA–384/512	SHA–384/512	SHA–384/512 Whirlpool	SHA–384/512
256 비트 이상	SHA–512	SHA–512	SHA–512	SHA–512

출처: 암호 알고리즘 및 키 길이 이용 안내서 2013

적용방안

- 국제 표준인 AES를 포함하여 국내 표준인 ARIA, SEED 등의 대칭키 암호 알고리즘 기반으로 데이터 암/복호화
- IoT 운영환경에 맞은 경량 암호 알고리즘 LEA, HIGHT 활용 가능

[국내 경량 암호 알고리즘 표준]

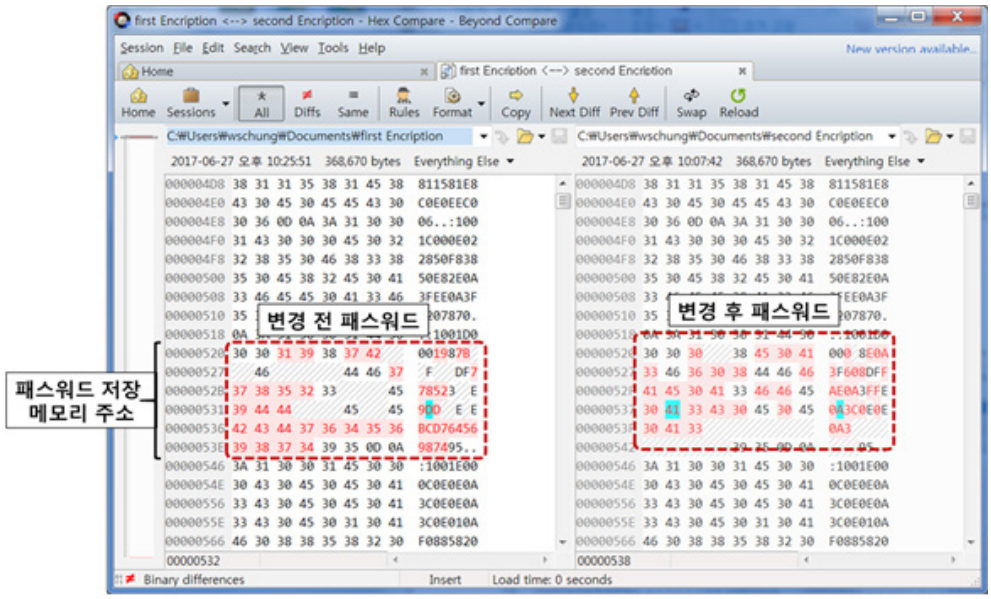
표준	암호알고리즘
TTAS.KO–12.0040/R1	HIGHT 암호 알고리즘
TTAS.KO–12.0233	LEA 암호 알고리즘

- HMAC 혹은 CMAC을 이용 데이터의 무결성을 확인
- 데이터 저장 시 해시 함수(SHA-2, SHA-3 등)나 PBKDF2 알고리즘이용 MAC Tag(인증 값) 저장

다. 예시

• 월패드 관리자 패스워드의 암호화 저장 •

외부 인터페이스로 전송된 데이터 암호화 저장



라. 대상

- **특징** 암호연산(암호키 저장), 인증정보(비밀번호 등) 저장, 제품에 대한 높은 접근성
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 암호 알고리즘 및 키 길이 이용 안내서 2013 (KISA, 2013.01)

2.3 메모리 공격 및 역공학 공격 대응

가. 개요

홈 · 가전 IoT 제품 메모리는 위치에 따라 Off-SoC 메모리와 On-SoC 메모리로 나눌 수 있으며, 메모리의 종류에 따라 휘발성 메모리와 비휘발성 메모리로 나뉜다. 메모리 공격이란 메모리 내의 내용을 추출하거나 복제, 변경하는 공격 방식이다. 역공학 공격은 홈 · 가전 IoT 제품 내부에 구성된 부품 중 집적회로(IC) 또는 메모리 패키지를 제거하고 각 층을 하나씩 제거하여 레이아웃을 찍은 후 획득한 레이아웃을 분석하여 민감 정보를 탈위하는 방식을 의미한다. 홈 · 가전 IoT 제품은 기능과 성능에 따라 이러한 공격에 적절히 대응해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 중요 데이터(암호키 포함)를 안전하게 저장하여 메모리 공격으로부터 보호되어야 함

적용방안

- 암호키는 외부공격에 대응 가능한 방법으로 Secure Element (USIM, Secure microSD, TPM 등) 적용과 PUF(Physical Unclonable Function) 등을 연동하여 사용
- 본 가이드의 “외부 조작 확인 및 분해 방지 메커니즘”을 적용하여 공격에 대응
- 소프트웨어적 메모리 공격 대응방안은 본 가이드의 “안전한 암호키 관리”, “저장 및 전송데이터 보호” 참조

② 제품 내부의 부품 중 역공학 공격대상이 되는 집적회로(IC)나 메모리는 물리적 접근방지 메커니즘이 구현되어야 함

적용방안

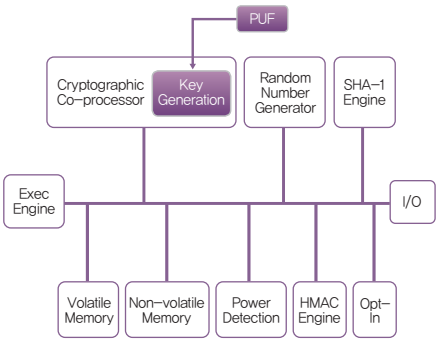
- PUF 사용하여 집적회로 내부통신 시 탈취 가능한 키 값 보호
- 소프트웨어 수준의 대응 방안은 본 가이드 “안전한 암호키 관리”, “저장 및 전송데이터 보호” 참조
- 물리적 대응 방안은 본 가이드 “외부 조작 확인 및 분해 방지 메커니즘”참조
- (접근 가능 시) 물리적 접근 시도 탐지시 제품이 동작하지 않거나 정상 동작하지 않아야 함

다. 예시

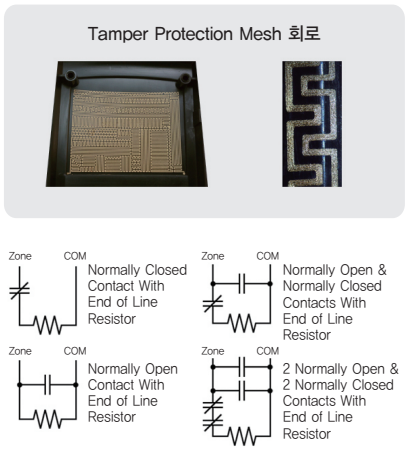
스마트TV와 월패드에 PUF를 적용하여 데이터 키 값을 보호할 수 있으며, 외부 조작 방지 메커니즘을 구현하여 물리적 공격에 대응한다.

• 스마트TV와 월패드에 적용된 물리적 공격 대응 메커니즘 •

PUF IC 적용 구조



외부 조작 방지 메커니즘



라. 대상

- **특징** 암호연산(암호키 저장), 인증정보(비밀번호 등) 저장, 제품에 대한 높은 접근성
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 하드웨어 칩 기반 보안시스템 및 해킹동향 (정보와 통신, 2014.5)

2) https://www.ecnmag.com/article/2012/04/robust-hardware-security-devices-made-possible-laser-direct-structuring

3) https://www.structuredhomewiring.com/SecuritySystem/TamperProofWiring/

2.4 부채널 공격 대응

가. 개요

제품 내부의 보안모듈이 구동되면서 발생하는 다양한 부채널 정보(Side Channel Information)로부터 보안모듈의 암호키를 크랙킹하는 공격을 방어해야 한다. 공격에 사용되는 대표적인 부채널 정보로는 보안모듈 구동 시간, 전력 소모량, 전자파 신호, 오류에 대한 출력 값 등이 있다.

• 부채널 공격법 분류 •

대분류	소분류	내용
침투 공격	tampering 공격 방법	De-Packing
		Layout Reconstruction
		Manual Micro-probing
		Using Advance Beam 기술(ion Beam 등)
		중요 데이터와 메모리 Reading
		EEPROM 수정
준침투공격	오류주입 공격, FI (Fault Injection)	전자기파 오류주입(EMFI, Electro-Magnetic Fault Injection) 암호연산 시 전자기파를 주사하여 오동작을 발생시킴으로써 암호키 정보 획득
		광확 오류주입(OFI, Laser Fault Injection) 암호연산 시 Laser를 주사하여 오동작을 발생시킴으로써 암호키 정보 획득
		차분 오류 분석(DFA, Differential Fault Analysis) 발생한 오류를 통계적 분석을 통해 암호키 정보 획득
비침투 공격	Glitch Attacks	암호연산 시 비정상 전력, 비정상 클록 등을 주사하여 오동작을 발생시킴으로써 암호키 정보 획득
	부채널 분석	시차 분석 공격 (Timing Analysis Attacks) 암호키 관련 연산 처리시간을 이용한 통계적 분석
		단순 전력 분석(SPA, Simple Power Analysis) 전력소모 정보에 대한 형태 분석을 통해 암호키 정보 획득
		차분 전력 분석(DPA, Differential Power Analysis) 암호키 관련 연산의 전력소모 정보에 대한 통계적 분석
		고차원 차분 전력분석(HO-DPA, High Order Differential Power Analysis) 다구간의 전력소모 정보를 이용하여 DPA 수행
		차분 전자파 분석(DEMA, Differential Electro-Magnetic Analysis) 암호키 관련 연산의 발생 전자기파 정보에 대한 통계적 분석

※ 세부 내용은 '부채널 공격 취약성 평가 방법론 및 기준 개발(KISA-WP-2009-0065)' 참조

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 제품의 성능과 하드웨어 보안성을 고려하여 부채널 공격 정보에 대한 다양한 공격에 대응하는 수준별 보안 기법을 적용하여 구현해야 함

적용방안

- 다음과 같은 한국인터넷진흥원의 '부채널 공격 취약성 평가 방법론 및 기준 개발'내용을 참조하여 제품에 적용 가능한 기법 적용

■ 물리적 대응 기법

- **난수 클락 시그널** : 비침입 공격에 대해서는 특정 명령이 실행될 때 각각을 예상해야 한다. 각 클락으로 같은 입력이 들어오면, 프로세서는 항상 리셋 후에 같은 명령을 C 클락 사이클로 실행한다. 따라서 확실한 방어를 위하여, 관찰 가능한 동작과 오퍼레이션 간에 난수 시간의 지연을 삽입하는 것이다. 공격자가 상호 상관관계 분석을 하는 경우도 있기 때문에 클락 사이클 레벨에서의 타이밍 난수를 도입한다.
- **난수 멀티 쓰레드** : 알고리즘 실행 결정을 어렵게 하기 위한 명령 레벨로 랜덤 연산에 멀티 쓰레드 스케줄링을 더한다.
- **강한 저주파수 센서** : 저주파수의 경우, 버스 관찰이 용이하기 때문에 저주파수 센서가 존재하는 제품은 센서를 비활성화하여 공격에 대응한다.
- **파괴적 테스트 회로** : 생산 공정에서 마이크로 컨트롤러의 테스트를 위한 회로가 불활성인 상태로 테스트 후에도 칩 상에 남아있어, 공격자는 이 회로의 FIB나 마이크로프로빙으로 접속해 모든 메모리 내용을 덤프하는 것이 가능하다. 따라서 테스트 회로는 완전하게 파괴한다.
  - 프로그램 카운터의 제약 : 프로그램 카운터를 주소 패턴 생성으로서 악용하는 것, 또는 분기나 호출, 리턴 명령이 실행되는 프로세서를 리셋하는 Watchdog 카운터를 없애는 방식은 많은 트랜지스터를 요구하게 된다. 이를 위해서 주소공간 모두가 사용하는 프로그램 카운터를 제공하지 않는 것이 유효하다. 16비트의 프로그램 카운터는 7비트의 오프셋 카운터와 16비트의 세그먼트 레지스터로 설정한다.
- **최상층의 센서 메쉬** : 실제로 회로상의 센서 메쉬를 형성한 금속층은 어떠한 신호도 전달하지 않는다. 그러나 결함이 있는 메쉬도 존재하여, 메모리 초기화를 소프트웨어가 실행하도록 한다.

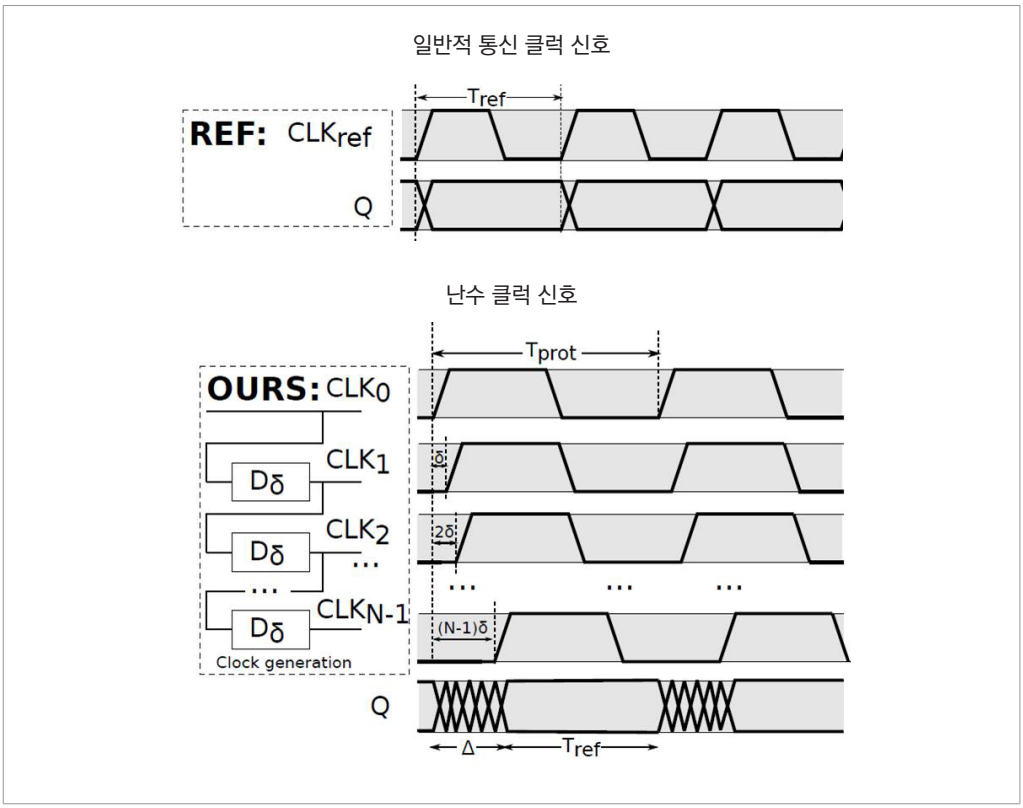
■ 소프트웨어적 대응 기법

- **중간값 Masking** : 부채널 분석 공격기법은 부채널 정보와 실제 연산값 간의 관련성에 기반한 공격방법이므로 실제 연산값에 난수(Masking) 값을 씌워서 연산을 수행하므로써 수집된 부채널 정보와 암호키 정보간의 관련성을 제거하는 대응 기법이다.
- **Shuffling 연산 기법** : 부채널 분석 공격기법은 부채널 정보와 실제 연산값 간의 관련성에 기반한 공격방법이므로 일부 연산의 순서를 랜덤하게 섞어서 수행함으로써 수집된 부채널 정보와 암호키 정보간의 관련성을 낮추는 대응 기법이다.
- **암호연산 출력값 검증** : 오류주입으로 인해 발생한 오류값을 그대로 출력하는 경우 공격자에게 암호키 관련정보를 제공하게 되므로 동일한 평문, 동일한 암호키로 암호연산을 n회 수행하여 n번의 암호문이 동일하면 암호문을 사용하고 동일하지 않으면 오류주입 수행된 것으로 판단하여 암호문을 삭제하고 다시 암호화를 수행한다.

다. 예시

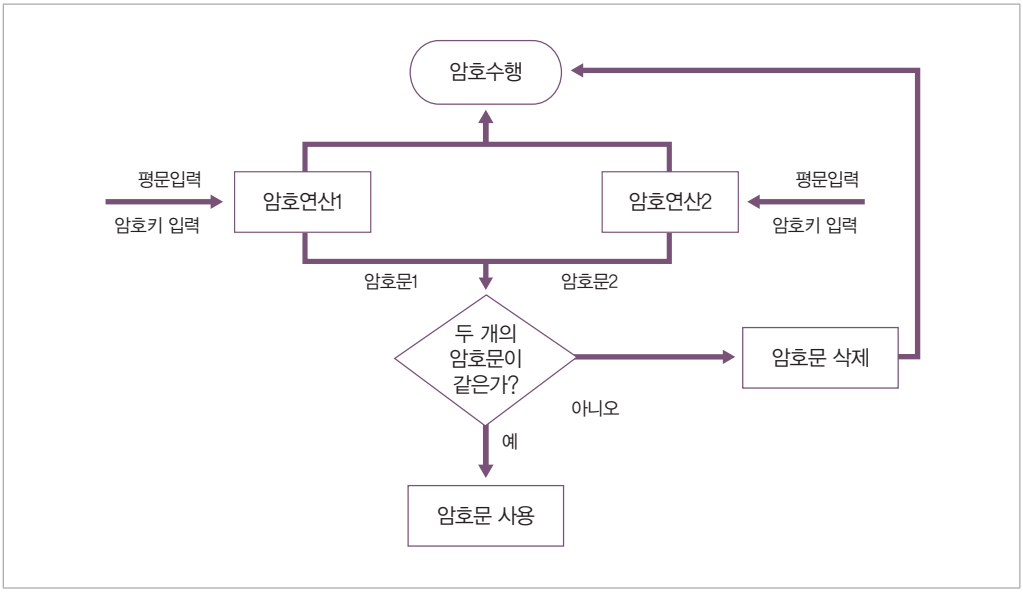
차분 전력 분석 및 차분 전자기파 분석을 위해서는 암호키 연산 시점을 균일한 시점으로 정렬을 수행해야 하며, 난수 클락 시그널을 사용할 경우 균일한 시점에 정렬되는 것을 방해함으로써 공격을 어렵게 할 수 있다.

• 난수 클락 시그널 구현 예시 •



암호연산 중에 오류주입 소스(전자기파 또는 Laser 등)로 인해 오류가 발생하게 되면 두 개의 암호문이 서로 다른 출력값을 가지게 되므로 해당 암호문을 삭제 후 암호연산을 재수행 함으로써 오류주입으로 인한 암호키 정보의 유출을 차단할 수 있다.

• 암호연산 출력값 검증 예시 •



라. 대상

- **특징** 암호연산(암호키 저장), 인증정보(비밀번호 등) 저장, 제품에 대한 높은 접근성
- **유형** 구매
- **적용 대상 제품** 스마트TV 등 홈·가전 IoT 제품

마. 참고자료

1) An EDA-Friendly Protection Scheme against Side-Channel Attacks(UC Riverside Previously Published Works, 2013.01)

2) 부채널 공격 취약성 평가 방법론 및 기준 개발(KISA-WP-2009-0065)

3) 보안 칩에서 중요키의 공격(부채널 공격 중심) 기술 동향(The Magazine of the IEIE, 전자공학회지 2016.7)

3. 개인정보 보호

가. 개요

홈 · 가전 IoT 제품에서 처리 · 전송 · 저장되는 개인정보가 외부에 평문으로 노출되지 않도록 안전하게 관리해야 한다.

• 개인정보 종류 •

분류	개인정보 종류
고유식별정보	주민번호, 여권번호, 운전면허번호, 외국인등록번호
민감정보	사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정 치적 견해, 병력(病歷), 신체적 · 정신적 장애, 성적(性的)취향, 유전자검사정보, 범죄 경력정보 등 사생활을 현저하게 침해할 수 있는 정보
개인식별정보	이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 생년월일, 성별 등
개인관련정보	학력, 직업, 키, 몸무게, 혼인여부, 가족상황, 취미 등
인증정보	비밀번호, 바이오정보(지문, 홍채, 정맥 등)
신용정보/금융정보	신용정보, 신용카드번호, 계좌번호 등
의료정보	건강상태, 진료기록 등
위치정보	개인 위치정보 등
자동생정정보	IP정보, MAC주소, 사이트 방문기록, 쿠키 (cookie) 등
가공정보	통계성 정보, 가입자 성향 등
제한적 본인식별정보	회원번호, 사번, 내부용 개인식별정보 등

출처: 소프트웨어 개발보안 가이드(2017.1., 행정안전부/KIS)

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 홈 · 가전 IoT 제품에 다루는 개인정보는 비식별화 조치를 통해 안전하게 관리되어야 함

• 개인정보 예시 •

[홈·가전 IoT 제품(예, 스마트TV 등)를 이용한 금융거래 시 요구될 수 있는 개인정보]
- 고유식별정보 : 주민등록번호, 여권번호, 외국인등록번호, 운전면허번호
- 금융정보 : 통장계좌번호, 신용카드 번호

[홈·가전 IoT 제품(예, 스마트TV, 월패드, 모바일 앱 등) 사용자 인증시 요구될 수 있는 개인정보]
- 신체 식별정보 : 지문, 음성, 홍채 등
- 식별코드 : 고객번호, 아이디 등

[홈·가전 IoT 제품(예, 홈캠(웹캠), 카메라 부착 제품 등)에서 처리될 수 있는 개인정보]
- 사진 : 정지사진, 동영상, CCTV 영상 등

출처: 개인정보 비식별 조치 가이드라인(2016.6.30., 관계부처합동)

적용방안

- 개인정보 비식별 조치 가이드라인'에서 제시하는 개인정보 비식별화 기술을 적용

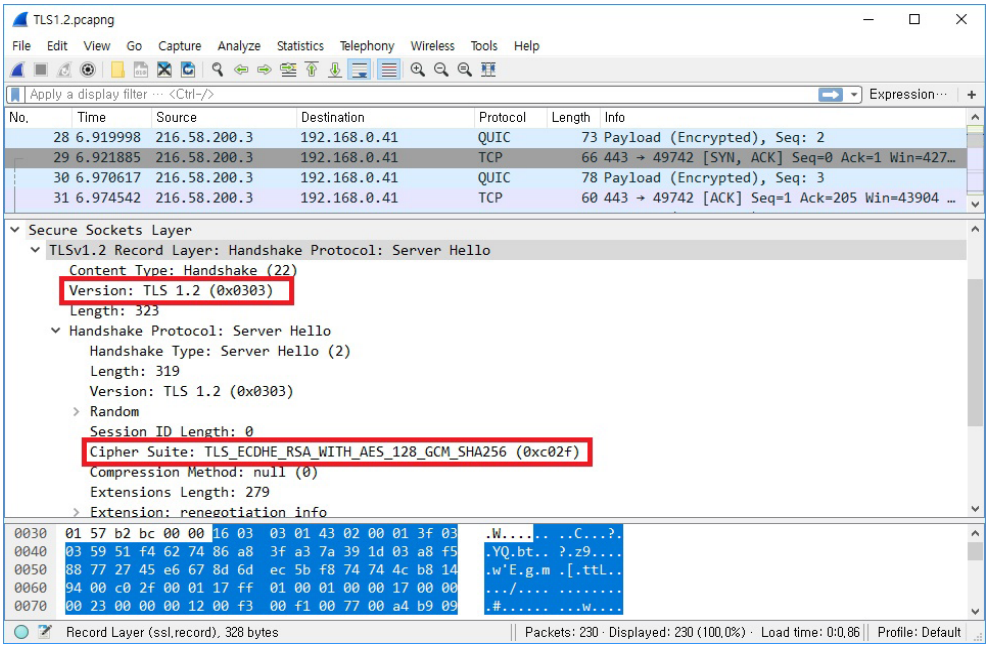
[국내 경량 암호 알고리즘 표준]

처리 기법	비식별화 조치		세부기술
	처리 前	처리 後	
가명 처리	홍길동, 35세, 서울 거주, 한국대 재학	임꺽정, 30대, 서울 거주, 국제대 재학	·휴리스틱 가명화 ·암호화 ·교환방법
총계 처리	임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm	물리학과 학생 키 합 : 660cm, 평균키 165cm	·총계처리 ·부분총계 ·라운딩 ·재배열
데이터 삭제	주민등록번호 901206-1234567	90년대 생, 남자	·식별자 삭제 ·식별자 부분삭제 ·레코드 삭제 ·식별요소 전부삭제
데이터 범주화	홍길동, 35세	홍씨, 30~40세	·감추기 ·랜덤라운딩 ·범위 방법 ·제어 라운딩
데이터 마스킹	홍길동, 35세, 서울 거주, 한국대 재학	홍○○, 35세, 서울 거주, ○○대학 재학	·임의 잡음 추가 ·공백과 대체

- 안전성을 보장하는 보안 프로토콜(HTTPS, SSL/TLS, CoAP(DTLS), Security API 등)을 이용하여 전송
- 검증된 종단간 암호화 솔루션 적용
- 저장 시 안전한 암호알고리즘 적용

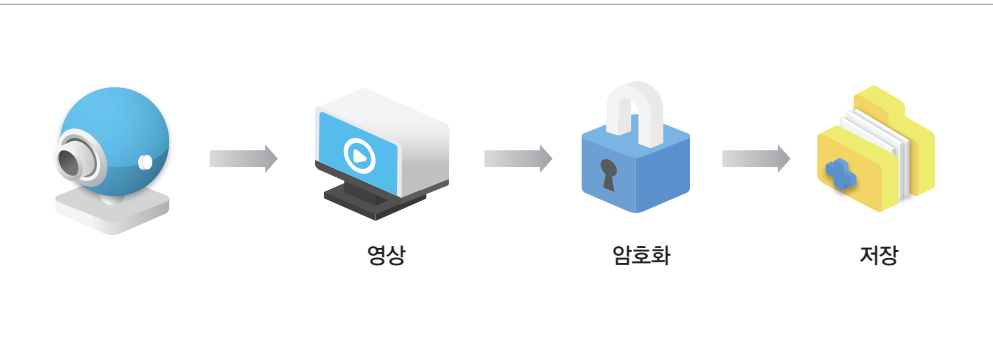
다. 예시

홈 · 가전 IoT 제품을 통해 수집된 개인정보 전송 시 통신 프로토콜 TLS 1.2를 사용하여 전송한다.



홈캠(웹캠) 제품에서 수집된 영상정보 저장 시 이를 암호화하여 저장되도록 한다.

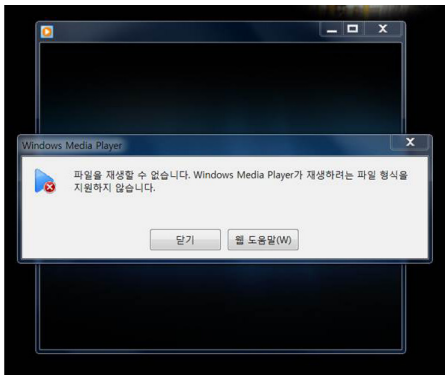
• 홈캠(웹캠) 제품의 개인영상정보 암호화 저장 예시 •



• 암호화 영상 저장에 따른 결과 •

암호화 전 영상 출력

암호화 후 영상 출력



라. 대상

- **특징** 개인 정보(고유식별정보, 금융정보, 사진, 동영상 등) 처리·저장·전송
- **유형** 구매, 촬영, 관리
- **적용 대상 제품** 스마트TV, 홈캠(웹캠), 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 개인정보 보호법, www.law.go.kr

2) 관계부처합동, “개인정보 비식별 조치 가이드라인”, 2016년6월30일

3) 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2013년 1월

4) 행정안전부, 한국인터넷진흥원, “소프트웨어 개발보안 가이드”, 11-1311000-000330-10(발간번호), 2017년 1월

1. 설정값 및 실행코드 무결성 검증

1.1 IoT 제품 주요 설정값 및 실행코드 무결성 검증

가. 개요

홈 · 가전 IoT 제품의 정상동작을 보장하기 위해, 주요 설정값 및 실행코드에 대한 무결성을 검증해야 하며, 무결성 오류(위 · 변조 발생) 발생 시, 대응방안을 고려해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 제품 시동 시 및 주기적으로 주요 설정값 및 실행코드에 대한 무결성 검증을 수행해야 함

• 보안강도에 따른 단순해시/전자서명용 해시함수 •

보안강도	NIST(미국)	CRYPTREC(일본)	ECRYPT(유럽)	국내
112비트 이상	SHA-224/256 SHA-384/512	SHA-224/256 SHA-384/512	SHA-224/256 SHA-384/512 Whirlpool	SHA-224/256 SHA-384/512
128비트 이상	SHA-256 SHA-384/512	SHA-256 SHA-384/512	SHA-256 SHA-384/512 Whirlpool	SHA-256 SHA-384/512
192비트 이상	SHA-384/512	SHA-384/512	SHA-384/512 Whirlpool	SHA-384/512
256비트 이상	SHA-512	SHA-512	SHA-512	SHA-512

출처: 암호 알고리즘 및 키 길이 이용안내서)

적용방안

- (점검대상) 제품 구동에 영향을 미치는 설정값, 보안기능 및 제품의 중요 기능(예, 구매, 제어, 전송 등)과 관련된 실행코드
- 점검대상으로 설정된 설정값 및 실행코드에 대한 해시값을 기반으로 시동 시 및 주기적으로 재 생성된 해시값 비교를 통해 무결성 검증을 수행
- 무결성 검증은 128비트 이상의 보안강도를 가진 해시함수, HMAC, CMAC 등 사용
- 해시함수 사용 시 무결성 검사 대상코드를 변조한 후에 해시를 재계산하여 덮어쓰기가 가능하므로, 해시값 변경 방지를 추가로 고려해야 함

② 무결성 검증 실패 시 적절한 대응행동을 수행해야 함

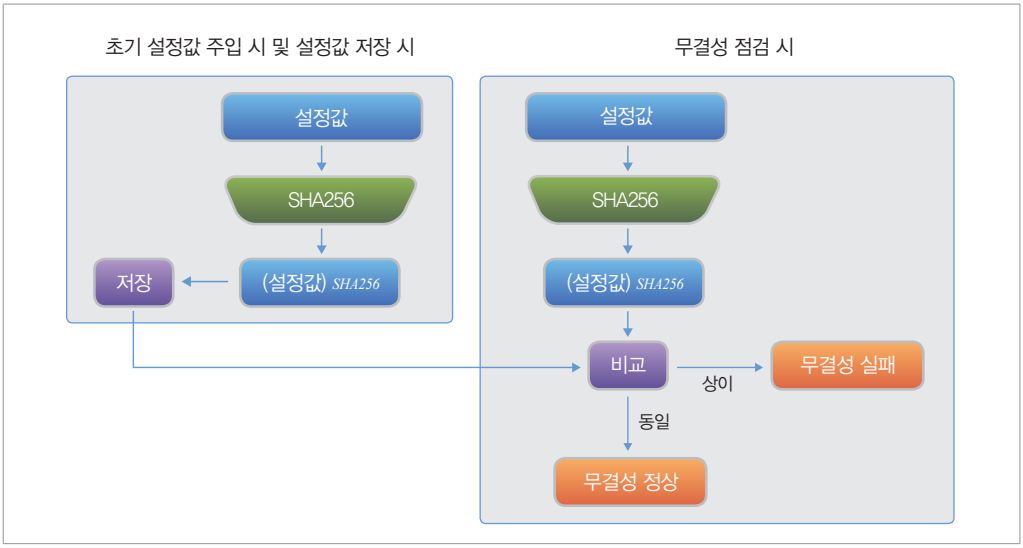
적용방안

- 관리자에게 알림(예, 이메일, 팝업 등)
- 무결성 오류 이전 설정값 및 실행코드로 복구
- 제품에서 제공하는 기능 잠금 또는 서비스 중단
- 암호키 등 중요정보 삭제
- 공장초기화 수행 등

다. 예시

홈 · 가전 IoT 제품은 초기 설정값 주입 시 및 설정값 저장 시 해시값을 생성해야 한다. 무결성 점검 시 설정값에 대한 해시값을 새로 생성하여 저장된 해시값과의 일치 여부를 확인한다.

• 홈·가전 IoT 제품의 설정값에 대한 무결성 점검 절차 예시 •



또한 월패드 제품의 무결성 점검 기능을 아래와 같이 제공할 수 있다. 시동 시 및 주기적으로 무결성 점검을 수행하도록 하고 있으며, 무결성 실패 시 관리자에게 알림을 제공하고 있다.

• 월패드 제품 시동 시 무결성 점검 수행 및 무결성 실패 시 관리자 알림 예시 •

라. 대상

- **특징** 암호연산(암호키 저장), 인증정보(비밀번호 등) 저장, 제품에 대한 높은 접근성
- **유형** 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2013년

2. 안전한 업데이트

2.1 신뢰할 수 있는 업데이트 서버

가. 개요

홈 · 가전 IoT 제품의 안전한 업데이트를 위해 신뢰할 수 있는 업데이트 서버를 통해 업데이트가 수행되어야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 홈 · 가전 IoT 제품은 업데이트 서버 주소에 대한 무결성을 보장해야 함

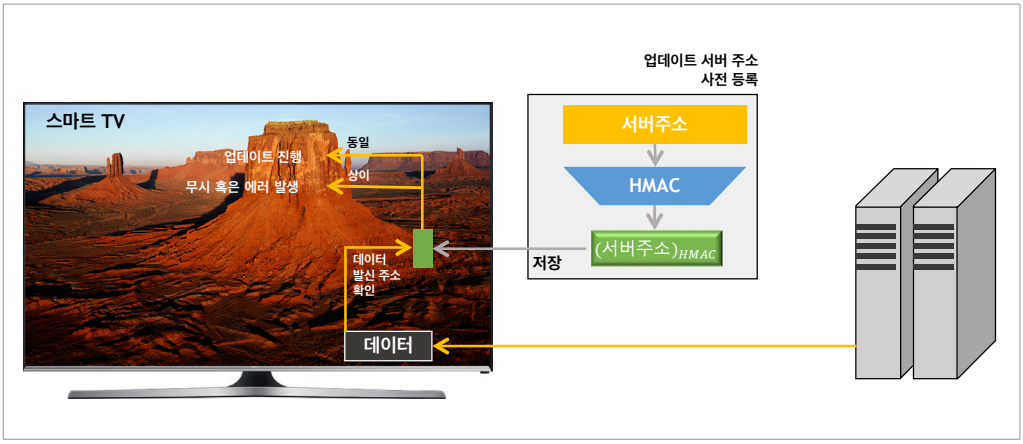
적용방안

- 업데이트 서버 주소(예, 1.1.1.1)의 비인가된 변경을 방지 및 탐지하기 위해 서버 주소에 대한 MAC값을 생성하여 비교
- 업데이트 서버 정보를 도메인으로 제공할 경우 전자서명 된 인증서사용

다. 예시

스마트TV 제품 등과 같이 실행파일 및 펌웨어 업데이트를 지원하는 경우 업데이트 서버 주소에 대한 MAC값을 보관하고, 업데이트 시 전송된 데이터의 발신지 주소를 확인하여 사전에 저장된 업데이트 서버 주소와 동일한 경우 업데이트를 진행한다.

• 스마트 TV 제품 소프트웨어 업데이트 절차 •



라. 대상

- **특징** 온라인을 통한 소프트웨어 업데이트 기능을 사용
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) OWASP IoT Top 10 (OWASP. 2014, www.owasp.org)

2.2 업데이트 파일의 부인방지 및 무결성 보장

가. 개요

홈 · 가전 IoT 제품의 안전한 업데이트를 위해 업데이트 파일에 대한 진위 여부 및 무결성을 검증한 후 업데이트를 수행해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 제조사는 업데이트 파일 배포 시 전자서명을 통해 배포자 및 무결성을 검증할 수 있도록 해야 함

적용방안

- 펌웨어의 변조 및 무결성 보장을 위해 업데이트 파일의 해시값에 전자서명을 적용하고, 시큐어부트를 적용
- 펌웨어 파일에 대한 무결성 검증 시 단순 해시로 무결성 확인

② 제조사는 업데이트 파일 배포 시 HMAC, CCM, GCM, CBC 방식을 통해 배포자 및 무결성을 검증할 수 있도록 해야 함

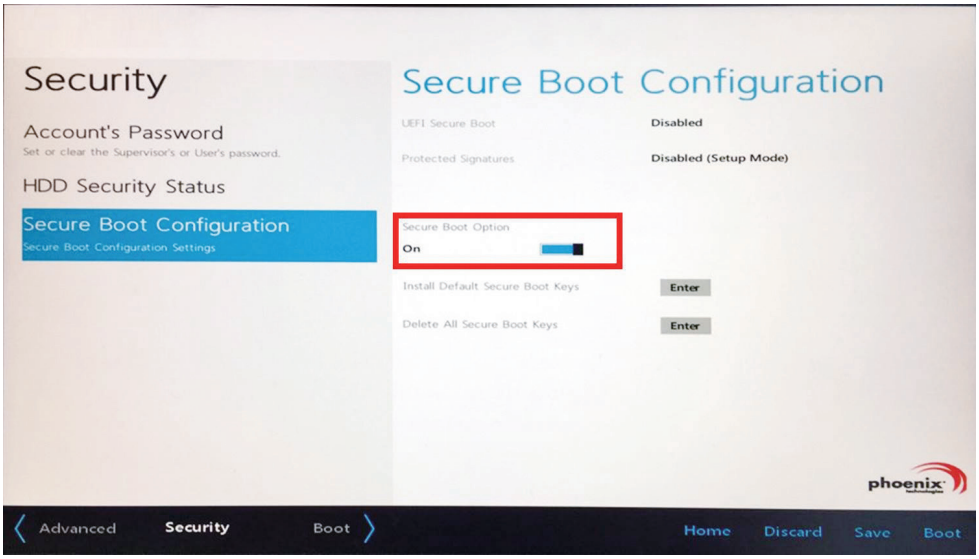
적용방안

- 펌웨어의 변조 및 무결성 보장을 위해 업데이트 파일에 대한 해시값에 제각 단말별 고유한 키로 HMAC, CCM, GCM, CBC 방식을 이용하여 무결성 검증
- 펌웨어 파일에 대한 무결성 검증 시 단순 해시로 무결성을 확인

다. 예시

스마트TV 제품에 시큐어부트를 적용하여 모든 OS 로더를 허용하는 BIOS를 사용하지 않고, 인정된 OS 로더만을 허용하는 UEFI 등을 지원하는 하드웨어를 사용하고 있다.

• 스마트TV의 시큐어부트 옵션을 제공하는 Windows 10 OS 사용 •



월패드 제품에서 펌웨어 업데이트 시 새로운 펌웨어에 대해 무결성 침해 여부를 확인한다.

• 패드 제품 업데이트 파일 무결성 검증 예시 •

라. 대상

- **특징** 온라인을 통한 S/W 업데이트 기능을 사용
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “악성코드 유포 탐지기술 현황 조사 및 발전모델 연구”, 2015.12

2) 한국인터넷진흥원, “사물인터넷 소형 스마트 홈 · 가전 보안 가이드”, 2016.12

2.3 안전한 업데이트 기능 제공

가. 개요

안전한 홈 · 가전 IoT 서비스를 지속적으로 제공하기 위해서는 인가된 사용자에 의해 안전한 업데이트를 수행하도록 해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 업데이트 수행 전 인가된 사용자(및 관리자)에 의해 업데이트 수행이 진행되는지 여부를 확인하기 위해 사용자 인증을 수행해야 함

적용방안

- 중요 업데이트(예, 보안패치 등) 발생 시, 제조사 홈페이지(SNS 등 포함)에 공개, 제품 팝업, 고객에게 이메일·SMS 발송 등 사용자에게 알릴 수 있는 다양한 수단을 제공해야 함
- 업데이트 수행 전 인가된 사용자(및 관리자) 여부를 확인할 수 있는 인증 기능 제공(예, 아이디/비밀번호, PIN 입력, 소유자 보유 카드 태깅, 생체인식 등)

② 인가된 사용자에게 업데이트 기능을 제공해야 함

적용방안

- 제품 소유자 또는 제조사 직원(및 A/S기사 등)이 업데이트 파일을 외부 인터페이스(예, USB 등)를 통해 수동으로 주입
  ※ 제품 설명서에 업데이트 방법 또는 제조사 연락처를 제공해야 함
- 업데이트 알림 기능 구현을 통해 사용자가 확인 후 자동으로 업데이트 수행

다. 예시

디지털도어락 제품에서 업데이트 전용 포트로 연결 시 관리자 비밀번호를 입력하도록 구현될 수 있다.

• 디지털도어락 제품의 펌웨어 업데이트 •

라. 대상

- **특징** 온라인을 통한 소프트웨어 업데이트 기능을 사용
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “악성코드 유포 탐지기술 현황 조사 및 발전모델 연구”, 2015.12

2) 한국인터넷진흥원, “사물인터넷 소형 스마트 홈 · 가전 보안 가이드”, 2016.12

2.4 펌웨어 분석 방지 기능 제공

가. 개요

펌웨어는 제조사 사이트에서 다운로드 하거나, IoT 제품에서 직접 추출 또는 전송 구간 스니핑을 통해 획득할 수 있다. 펌웨어 파일에는 부트로더, 운영체제, 라이브러리, 애플리케이션, 설정 파일, 키 파일, 펌웨어 업데이트 스크립트, 버전 정보, 소스 코드, 서명값 등이 포함되어 있어, 공개된 역공학 도구를 통해 해당 파일(중요 로직이나 키 정보 등 포함)를 추출할 수 있다. 이에 따라 적절한 수준의 펌웨어 보호 기법을 적용해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 펌웨어 전체를 암호화를 적용해야 함

적용방안

- 펌웨어를 관리 서버에 등록하는 시점에 암호화하고 암호키는 별도로 관리

② 패키지 구성 요소 중 중요 정보를 선별하여 암호화 또는 난독화를 수행해야 함

적용방안

- IoT 제품의 인증용 키, 메시지 노출 방지를 위한 암호화
- 개인키 평문 노출 방지를 위한 패스워드 적용
- 소스코드(예: asp, php, asp 등) 및 설정(예: *conf, *.cfg, *.sh, *.ini 등)값 평문 노출 방지를 위한 암호화 또는 난독화
- DRM 권한 체크, 애플리케이션 실행 권한 체크 로직의 리버스 엔지니어링 방지를 위한 시큐어코딩, 패킹

다. 예시

방안	적용 전	적용 후
개인키에 패스워드 적용	-----BEGIN RSA PRIVATE KEY----- MIIEpAIBA... -----END RSA PRIVATE KEY-----	-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,F81CB322AE5B46DB ZENHWuiugV... -----END RSA PRIVATE KEY-----
메시지 노출방지를 위한 암호화	Case Tamper Event.,Case Connected.. 43 61 73 65 20 54 61 6D 70 65 72 20 45 76 65 6E 74 2E 2E 43 61 73 65 20 43 6F 6E 6E 65 63 74 65 64 2E 2E	` e §æ½x U & i n ? (h … 60 E8 A7 E6 BD 78 DB 26 ED 6E 88 28 68 F4 5B A9 BF 9E 32 C9 B0 68 27 14 1A B9 05 9A CC 5C A9 82 FF FB FA CA 7B 3E 60 74 3A 1E 8C A9 3C 77 1E 2F

라. 대상

- **특징** 온라인을 통한 소프트웨어 업데이트 기능을 사용
- **유형** 센싱, 제어, 구매, 촬영, 중계, 운용, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 스마트 냉장고, 월패드 등 모든 홈·가전 IoT 제품

마. 참고자료

1) OWASP Firmware Analysis, https://www.owasp.org/index.php/IoT_Firmware_Analysis

2)LG CNS, 기업 담당자가 읽어야 할 사물인터넷 보안 대응 방안, http://blog.lgcns.com/1462

3. 감사기록

3.1 감사기록 생성

가. 개요

사용자의 금전적 손실, 사생활 침해, 안전(방범 등) 등에 영향을 미칠 수 있는 기능 및 서비스를 제공하는 홈 · 가전 IoT 제품의 경우 사용자 접근 및 로그인, 보안기능 수행, 중요 기능(구매 등) 수행 등에 대한 감사기록 생성 기능을 구현하여 홈 · 가전 IoT 제품의 이상행위를 탐지 및 추적할 수 있도록 해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 제품 설정 및 동작에 대한 감사기록(로그)을 생성해야 함

적용방안

- (감사대상) 사용자 로그인 성공/실패, 제품 설정 변경 내역, 기능 수행 내역(보안기능 포함) 등
  ※ 비밀번호, 암호키 등 민감한 정보는 감사기록에 포함되지 않아야 함
- 감사기록은 사건발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 작업내역 및 결과(성공/실패) 포함 고려
- 인가된 사용자가 해석하기에 적합하도록 감사기록을 생성하고, 검토할 수 있는 기능 제공
- 정확한 시간정보 생성을 위해 신뢰할 수 있는 타임스탬프 제공(예, NTP 등)

② IoT 제품이 저사양인 경우, 제품 설정 및 동작에 대한 감사기록(로그)을 생성 후 서버로 감사기록을 전송해야 함

적용방안

- 인가된 사용자가 해석하기에 적합하도록 감사기록을 생성하고, 서버로 감사기록을 전송
- 서버와 연결이 불가할 경우
  - 인가된 사용자에게 통보(예, 팝업, 이메일 등) 수행
  - 오래된 감사기록 덮어쓰기 수행

다. 예시

스마트TV 제품에서 사용자가 발생시킨 사건에 대해 감사데이터를 생성하며 관리자가 이를 조회 및 관리할 수 있는 기능을 제공하고 있다.

• 스마트 TV 제품의 감사데이터 관리 페이지 •

일시	사건 유형	주체	작업 내역 및 결과
2017-06-28 11:38:52	사용자로그인	manager	로그인성공
2017-06-28 11:46:28	제품설정변경	manager	사용자단말등록
2017-06-28 11:47:02	제품제어	manager	도어락오픈

라. 대상

- **특징** 민감정보 및 제어정보, 보안 접근, 인증 기반 관리자 로그인, 사용정보 수집
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “침해사고 분석 절차 안내서”, 2010.01.

2) 한국인터넷진흥원, “IoT 공통보안가이드”, 2015.09

2) 한국인터넷진흥원, “IoT 공통보안원칙”, 2015.09

3.2 감사기록 보호

가. 개요

감사기록의 유실 및 비인가된 변경(삭제 포함)에 대비하기 위해 감사기록을 보호하는 장치를 마련해야 한다.

나. 보안대책

홈 · 가전 IoT 제품에 따라 다음 보안대책을 선별하여 적용할 수 있다.

① 감사기록은 비 인가된 삭제 또는 변경이 발생하지 않도록 보호되어야 함

적용방안

- 감사기록을 삭제 또는 변경할 수 있는 UI를 제공하지 않아야 함

② 감사기록 저장 및 백업 기능을 제공해야 함

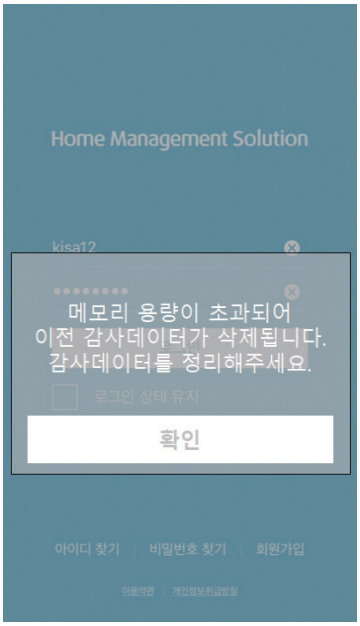
적용방안

- (내부저장소 사용) 감사증적의 크기가 지정된 한도를 초과할 경우
  - 인가된 사용자에게 통보(예, 팝업, 이메일 등)
  - 오래된 감사기록 덮어쓰기 등
- (외부저장소 사용) 홈게이트웨이, 클라우드 이용
- (공통) 감사기록 백업 및 복구 기능 제공

다. 예시

월패드 제품에서 사용자에 의한 사건 발생으로 감사데이터 생성 시 감사증적의 크기가 지정된 한도를 초과할 경우, 사전에 정의한 방식에 따라 관리자에게 통보하고 오래된 감사레코드의 덮어쓰기를 수행하도록 한다.

• 월패드 제품에서 감사증적 크기 초과 시 인가된 사용자에게 제공되는 팝업창 •



라. 대상

- **특징** 민감정보 및 중요 제어, 보안 접근, 인증 기반 관리자 로그인, 사용정보 수집
- **유형** 제어, 구매, 촬영, 중계, 관리
- **적용 대상 제품** 스마트TV, 디지털도어락, 홈캠(웹캠), 홈게이트웨이, 월패드 등 홈·가전 IoT 제품

마. 참고자료

1) 한국인터넷진흥원, “침해사고 분석 절차 안내서”, 2010.01

2) 한국인터넷진흥원, “IoT 공통보안가이드”, 2015.09

2) 한국인터넷진흥원, “IoT 공통보안원칙”, 2015.09

부록

부록1

약어 및 용어정의

가용성 정당한 사용자가 정보 시스템의 데이터 또는 자원을 필요로 할 때 부당한 지체 없이 원하는 객체 또는 자원으로의 접근 및 사용을 보장해 주는 성질

개인식별번호 PIN(Personal Identification Number)으로, 식별확인을 할 수 있는 문자와 숫자가 조합된 기호로 된 식별 번호를 의미함. 현금 자동 지급기와 같은 장치에 대한 접근 관리를 위해 개인에게 부여된 개인 식별 번호 등이 있음

개인키 비대칭 암호알고리즘에서 사용되며 하나의 개체(개인키를 사용하는 주체)와 유일하게 결합되는 암호키로 공개되어서는 안됨. 비대칭 서명 시스템에서는 서명을 위해 사용됨

공개키 비대칭 암호알고리즘과 함께 사용되며, 하나의 개체(공개키를 사용하는 주체)와 유일하게 결합되는 암호키로 공개가 가능함. 비대칭 서명 시스템에서는 서명 검증을 위해 사용됨

기밀성 중요 정보가 인가되지 않은 상대방에게 노출되지 않음을 보장해 주는 성질로, 허가 받은 사용자가 아니면 내용에 접근할 수 없어야 함. 기밀성의 보증을 위하여 일반적으로 암호화(encryption)가 사용됨

난수 정의된 범위 내에서 무작위로 추출된 수를 말하며, 다음 생성될 수에 대한 예측이 불가능함. 불규칙한 자연현상(동전의 앞뒷면, 주사위 눈금) 등과 같은 진난수(True Random Number)와 수학적으로 진난수에 가깝게 생성하는 의사난수(Pseudo Random Number)로 나뉨

난수 발생기 암호연산, 통신, 인증 등 암호응용을 위해서 특정한 제한 조건에 따라 일련의 난수를 발생시키기 위한 프로그램이나 하드웨어를 칭함

내부인터페이스 제품 내부 회로기판에 구성된 통신포트로 디버깅, 펌웨어다운로드, 내부 파일 추출 등이 가능

대칭키 송 · 수신자가 암 · 복호화를 할 때 같은 키를 쓰는 알고리즘. 메시지를 일정한 크기(블록)로 나누어 암 · 복호화하는 블록 암호 방식과 한 번에 한 비트 또는 한 바이트를 암호화하는 스트림 암호 방식이 있음

댁내망 다양한 유무선 기술을 적용하여 댁내의 개인용 컴퓨터(PC), 가전제품, 제어제품, 각종 시설 등은 물론

휴대전화, 개인 휴대 정보 단말기(PDA) 등을 통합한 네트워크로 외부의 공중 네트워크와 접속되기도 함

도용 남의 정보를 몰래쓰는 행위

도청 비인가된 사용자, 컴퓨터 또는 프로그램이 전송 정보를 불법적으로 가로채는 것으로, 송수신되는 정보의 변경을 포함하지 않고, 정보의 수신만을 의미

무결성 네트워크를 통해 송수신되거나 시스템에 보관되어 있는 데이터가 불법적으로 변경되거나 삭제되지 않도록 보장하는 성질. 데이터 및 네트워크 보안에 있어서 정보가 인가된 사람에 의해서만 접근 또는 변경이 가능하다는 확실성

미라이 악성코드 IoT 제품을 대상으로 하는 악성 코드로, 미라이(Mirai) 악성코드는 주로 카메라, DVR 등 인터넷에 연결된 제품들을 감염시켜 봇넷을 만든 후 대량의 트래픽을 유발시키는 디도스(DDoS) 공격을 함. 미라이(Mirai)는 '미래(未來)'라는 뜻의 일본어로, 2016년 5월 처음으로 발견되었음

민감정보 누출이나 훼손되었을 때 정보의 소유자에게 부정적 영향이 발생하며 시스템의 계속적 운영이 불가능해지고 상당한 양의 자원을 다시 생성해야 하는 상황을 유발하는 정보

보안강도 암호 알고리즘의 보안성을 비트(Bit)로 표기한 일종의 평가지표로 암호키 또는 알고리즘의 취약성을 찾아내는데 필요한 계산량을 의미함. 예) 112 보안강도란 2^{112} 번의 연산을 해야 암호키 또는 알고리즘의 취약성을 알아낼 수 있음을 의미

보안성 권한이 없는 사람 또는 시스템은 정보를 읽거나 변경하지 못하게 하고, 권한이 있는 사람 또는 시스템은 정보에 대한 접근이 거부되지 않도록 정보를 보호하는 소프트웨어의 능력

보안요구사항 식별된 보안위협에 대응하기 위한 요구사항

보안위협 자산에 손실을 발생시키는 원인이나 행위

보안취약점 시스템 또는 프로그램에 내재되어 있는 버그(잘못된 부분)를 의미하며, 해커는 이를 악용해 시스템에 침입하여 정보 유출, 시스템 파괴 등 유발

부채널 공격 비밀정보를 이용한 연산과 관련 부채널 정보를 이용하여 비밀정보를 추측함으로써 암호 알고리즘이나 암호키 등의 보안강도를 낮추는 공격

부채널 정보 암호 알고리즘 등이 비밀정보(암호키 등)를 사용하여 동작하는 동안 발생하는 부가정보(전력 소모량, 전자파 발생량 등)을 말하며, 이러한 부가정보는 비밀정보에 따라 달라지므로 비밀정보에 대한 정보가 포함될 수 있음

비밀번호 보안을 위하여 미리 약정하여 쓰는 개인 고유의 문자열을 의미함

비휘발성 메모리 전력이 끊어져도 저장 정보가 유지되며 전력이 공급되면 다시 저장된 정보를 사용할 수

있는 기억 매체

사물인터넷 여러 네트워크를 통해 인터넷에 연결되어 있는 여러 장치 어플라이언스 등을 총칭하는 개념

사업자망 기업이나 기관이 개인이나 회사들에게 인터넷에 접속할 수 있도록 서비스를 제공하는 네트워크

상호인증 두 개체가 서로 상대방의 신분을 확인하는 절차로 서로간에 신뢰성을 요구할 때 사용됨. 예) 서버–클라이언트 간 인증, 접근 사이트–사용자 간 인증

설정파일 응용 프로그램을 설치할 때 사용자가 선택한 시스템 구성 요소의 조건이나 설정한 특성 등을 보관한 파일

솔트 비밀번호 저장 시 비밀번호의 해시값을 변환하는 데 사용되는 무작위 문자열. 다른 사용자가 동일 시스템 내에서 동일한 비밀번호를 사용하더라도 유일하게 식별함으로써 충돌을 방지하기 위해 해시 알고리즘에 적용되며, 또한 해커들이 비밀번호를 사용해 시스템에 잠입하는 것을 어렵게 하기 위해 해시 알고리즘에 적용됨

스니핑 해커가 네트워크상에서 송수신되는 패킷을 수집하여 비밀번호 등을 알아내는 해킹 기법

스마트 홈 집안의 다양한 가전제품들이 네트워크로 연결되어 원하는 서비스를 제공하는 집

암호키 암호연산(암 · 복호화, 인증코드 연산, 서명 생성, 서명 검증 등)을 실행하기 위한 암호 알고리즘에 사용되는 매개변수

외부인터페이스 제품 외부에 노출되어 있는 통신포트로 디버깅, 펌웨어다운로드, 내부 파일 추출 등이 가능

운영모드 대칭키 암호 알고리즘을 이용하여 임의의 크기를 갖는 데이터를 암 · 복호화하기 위해 적용하는 블록 암호의 운영 방식을 칭함

위변조 위조(보안공격의 하나로 비인가자들이 시스템에 대한 위조물을 삽입하는 것)와 변조(보안공격의 하나로 비인가자들의 불법적인 접근뿐만 아니라 불법적인 변경 행위)를 아울러 이르는 말

위장 한 실체가 시스템에 접근하고자 할 때, 정상적으로 허가받은 다른 실체인 것처럼 흉내 내어 시스템에 접근을 시도하는 행위

위협원 자산에 불법적인 접근, 변경, 삭제 등 위협을 일으키는 인가되지 않은 외부 실체

의사난수 발생기 'Pseudo Random Number Generator(PRNG)'로, 초기값을 이용하여 정해진 메커니즘에 따라 수학적으로 진난수에 가까운 의사난수를 생성하는 프로그램이나 하드웨어를 칭함

인가된 관리자 식별 및 인증을 성공으로 완료한 실체로서, 운영 및 관리를 수행할 수 있는 권한이 부여된 관리자

인가된 사용자 보안정책에 따라 기능을 실행할 수 있는 사용자

인가된 수신자 메시지(예, 센싱 정보)를 전달받거나 발신한 메시지에 대한 전달 결과 보고를 전달받는 허가된 사용자(또는 IT실체)

인증정보 인증을 위해 검증자가 요청하는 객체를 식별할 수 있는 정보로, 인증 정보에는 아이디, 비밀번호, 인증서 등이 포함됨

재생 공격 이전에 전송된 메시지를 다시 사용하는 위장 공격으로, 시간이나 순서에 따른 유효성을 검출할 수 있도록 순서 번호나 타임스탬프, 또는 도전/응답 등으로 방어할 수 있음

전자서명 데이터의 출처 또는 무결성을 확인할 수 있도록 암호 알고리즘으로 계산된 첨부값을 의미함. 데이터 생성자만이 가지고 있는 개인키를 이용하여 전자서명을 수행하면 수신자는 해당값을 통해 데이터 생성자 확인 및 제 3자에 의한 데이터 위조로 여부를 검증함

중간자 공격 통신하고 있는 두 당사자 사이에 들키지 않게 끼어들어 당사자들이 교환하는 통신내용을 바꾸거나 도청하는 공격 기법

진난수 발생기 'True Random Number Generator(TRNG)'로, 불규칙적인 자연현상(노이즈 등)을 숫자로 변환해 난수를 생성하며, 컴퓨터 기술의 발달로 인해 의사난수의 패턴이 노출되는 경우가 있으며, 더 강한 난수성이 요구 되는 곳에 사용됨

진위성 주체나 자원이 진짜임을 보장하는 성질로, 사용자, 프로세스, 시스템 및 정보와 같은 실체에 적용됨

테스트벡터 암호 또는 해시 알고리즘에 대한 구현의 정확성을 확인하기 위해 예시로 주어진 입 · 출력 값들을 의미하며, 주어진 입력값들을 이용하여 알고리즘을 수행하면 그에 맞는 출력값이 생성되어야 함

해시값 임의의 길이의 입력 메세지를 고정된 길이의 출력값으로 압축시키는 알고리즘의 결과값을 의미함

해시 알고리즘 임의의 길이의 문자열을 고정된 길이의 이진 문자열로 매핑하여 주는 알고리즘. 해시 알고리즘은 데이터의 무결성, 인증, 부인 방지 등에 사용됨

휘발성 메모리 전원을 끊으면 기억하고 있던 정보가 없어지는 성질의 기억 매체

AES 'Advanced Encryption Standard'의 약자로, AES는 2001년 미국 국립표준기술연구소(NIST)가 기존의 암호표준을 대체하기 위해 채택한 128비트의 블록 크기를 가지는 새로운 암호 표준임. 128, 192, 256비트의 키 길이 처리가 가능한 대칭키 암호 알고리즘

ARIA 'Academy, Research Institute, Agency'의 약자로, ARIA는 경량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘. 128, 192, 256비트의 키 길이 처리가 가능한 대칭키 암호 알고리즘이다. 국내에서 개발되었으며 국내 표준으로 지정된 암호 알고리즘

CMAC 'Cipher-based Message Authentication Code'의 약자로, CMAC은 암호를 기반으로 한 메시지 인증 코드임

HIGHT 'HIGh security and light weigHT'의 약자로, HIGHT는 RFID, USN 등과 같이 저전력 · 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 2005년 KISA, ETRI 부설연구소 및 고려대가 공동으로 개발한 64비트 블록암호 알고리즘. 128비트의 키 길이 처리가 가능한 대칭키 암호 알고리즘으로, 2006년 12월 정보통신단체표준(TTA)으로 제정되었으며, 2010년 12월 ISO/IEC 국제 블록 암호 알고리즘 표준으로 제정되었음

HMAC 'Hash-based message authentication code'의 약자로, HMAC은 해시를 기반으로 한 메시지 인증 코드. 반복적인 암호화 해시 기능을 비밀 공용키와 함께 사용하며, 체크섬을 변경하는 것이 불가능하도록 한 키 기반의 메시지 인증 알고리즘

JTAG 'Joint Test Action Group'의 약자. 임베디드 시스템 개발 시에 사용하는 디버깅 장비로 개발 시 통합한 회로로 사용되는 IEEE 1149.1의 일반적인 이름

LEA 'Lightweight Encryption Algorithm'의 약자로, LEA는 빅데이터, 클라우드 등 고속 환경 및 모바일기기 등 경량 환경에서 기밀성을 제공하기 위해 개발된 128비트 블록암호 알고리즘. 128, 192, 256비트의 키 길이 처리가 가능한 대칭키 암호 알고리즘으로, LEA 규격 및 운영모드는 국내 TTA 표준으로 제정되었음

PBKDF2 'Password-Based Key Derivation Function 2'의 약자로, 비밀번호 저장 시 무차별 대입 공격에 대응하기 위해 솔트 및 난수 생성기를 적용하여 구현하는 키 유도함수

PUF 'Physically Unclonable Function'의 약자. 일종의 난수 발생 장치로 직접 회로의 예측 불가능한 지연 성분을 이용한 디지털 기기 복제 방지 기술

RS232 'Recommended Standard-232'의 약자. 모뎀과 데이터 단말 장치를 접속하는 직렬 통신 인터페이스

SEED SEED는 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 2월 한국인터넷진흥원과 국내 암호전문가들이 순수 국내기술로 개발한 128비트 블록 암호 알고리즘. 128, 256비트의 키 길이 처리가 가능한 대칭키 암호 알고리즘으로, SEED 128은 1999년 9월 정보통신단체표준(TTA)으로 제정되었으며, 2005년에는 국제 표준화 기구인 ISO/IEC 국제 블록암호알고리즘, IETF 표준으로 제정되었음

SHA2 SHA2는 안전한 해시 함수로 SHA-224, SHA-256, SHA-384, SHA-512의 4종을 통칭함

SHA3 SHA-3는 SHA-2를 대체하기 위해 미국 국립표준기술연구소(NIST)가 2015년 8월에 발표한 안전한 해시 함수

SSH 'Secure Shell'의 약자. 보안 등급이 낮은 네트워크상에서 보안 등급이 높은 원격 접속 개시나 데이터

전송을 수행하고 암호 통신을 이용해서 다른 컴퓨터에 접속한 다음 명령을 실행하거나 파일 조작하는 프로토콜

Tamper Proofing 조작 방지로, 소프트웨어에서 워터마크 삭제 등과 같이 소프트웨어가 불법으로 변경되었을 경우, 그 소프트웨어가 정상 수행 되지 않게 하는 기법

TLS 'Transport Layer Security'의 약자. 인터넷상에서 데이터의 도청이나 변조를 막기 위해 사용되는 보안 소켓 계층(SSL: Security Sockets Layer) 프로토콜 보다 보안성이 강화된 프로토콜

TPM 'Trusted Platform Module'의 약자. 암호화된 키, 패스워드, 디지털 인증서 등을 저장하는 안전한 저장 공간을 제공하는 보안 모듈

UART 'Universal Asynchronous Receiver/Transmitter'의 약자. 컴퓨터의 비동기 직렬 통신을 처리하는 프로그램 또는 병렬 데이터의 형태를 직렬 방식으로 전환하여 데이터를 전송하는 컴퓨터 하드웨어의 일종

USB 'Universal Serial Bus'의 약자. 범용 직렬 버스로 주변 기기 등을 개인용 컴퓨터(PC) 또는 IoT 제품에 접속하기 위한 인터페이스

USIM 'Universal Subscriber Identity Module'의 약자. 가입자 정보를 탑재한 심(SIM) 카드와 범용IC카드(UICC)가 결합된 형태로써 사용자 인증, 과금, 로밍 등 가입자 정보를 담고 있는 스마트카드

Zigbee 2.4GHz, 915MHz, 868MHz 주파수 대역을 사용하는 무선 통신 기술

Z-Wave Zensys사와 Z-Wave 얼라이언스에서 개발한 상호운용성을 가지는 무선 통신 프로토콜

부록2

홈 · 가전 IoT 제품 유형

글로벌 전자제품 제조사 제품과 IoT 제품 전문웹사이트 정보를 기반으로 스마트 홈에 설치 · 운영되고 있는 홈 · 가전 IoT 제품 총 76종을 선정하여 다음과 같이 9가지 유형으로 분류하였다.

유형	홈 · 가전 IoT 제품
멀티미디어 제품	스마트TV, 셋톱박스(스마트박스), 게임기, 홈시어터(사운드바), 빔프로젝터, 디지털액자, 스마트스피커
주방가전 제품	냉장고, 오븐, 전기밥솥, 정수기, 식기세척기, 김치냉장고, 커피메이커
생활가전 제품	스마트 홈 인공지능 로봇, 애완동물 모니터링, 카메라, 유아용 모니터링 제품 및 카메라, 스마트 리모컨, 제스처 리모컨, 스마트 잔디깍이, 스마트 혈압측정기, 스마트 맥박측정기, 스마트 혈당측정기, 세탁기, 건조기, 공기정화기, 로봇청소기, 안마의자, 산소발생기, 가습기, 의류 스타일러, 스마트 차고문 제어기, 스마트 프로판, 가스통 게이지, 스마트 스프링쿨러, 스마트 활동량 측정기, 스마트 생활패턴 분석기, 스마트 운동량 분석기, 스마트 체중계, 스마트 애완동물Feeder, 스마트 조명, 무선전동 블라인드, 스마트 블루투스 버튼, 스마트 화분, 모니터링제품, 소모품 자동주문제품(세제 등), 스마트 전동칫솔, 스마트 컵, 수면패턴 분석 및 도우미
계절가전 제품	에어컨, 전기히터, 스마트 보일러, 선풍기
가구	스마트 침대, 스마트 의자, 스마트 책상
네트워크 제품	네트워크 카메라, 스마트 라우터, 가정용 방화벽, 스마트 게이트웨이, 월패드(IHD), 영상통화 IP 전화기, 유무선 공유기
제어제품	디지털 도어락, 스마트 환기구 제어기, 스마트 조명 스위치, 스마트 전력차단기, 스마트 가스차단기, CO2센서
센서제품	화제감지 센서, 인감 센서, 창문개폐센서, 온/습도센서, 조도센서
센서+제어제품	스마트 콘센트, 스마트 전력검침기, 스마트 가스검침기

홈 · 가전 IoT 제품으로 분류할 수 있는 76종에 대해 실제 제품화하여 출시된 제품(2017년 6월 기준, 아래 표 참조)을 조사하여 IoT 제품의 시스템 사양을 기반으로 등급(Class)을 구분하고, 현재 적용된 기능 및 기술을 확인하였다.

홈 · 가전 IoT 제품	관련 제품 주소
스마트TV	http://www.lge.com, http://www.samsung.com
셋톱박스(스마트 박스)	https://www.apple.com/tv/
스마트 냉장고	http://www.lge.com, http://www.samsung.com
스마트홈 인공지능 로봇	http://www.lge.com, https://madeby.google.com/home/
애완동물 모니터링 카메라	http://www.anygate.co.kr/sub/detail.asp?idx=484
유아용 모니터링 제품 및 카메라	https://www.summerinfant.com/monitoring
네트워크 카메라	http://www.uplusiotshop.com/MMall/
스마트라우터	https://www.getcujo.com/, www.lge.com
가정용 방화벽	https://www.getcujo.com/
스마트 게이트웨이	https://rainforestautomation.com/rfa-z114-eagle-200/
월패드(IHD)	http://www.hyundaitel.co.kr/new/main/main.asp
게임기	http://www.xbox.com/ko-KR/xbox-one-s
스마트 오븐	https://juneoven.com/
스마트 전기 밥솥	https://www.uplus.co.kr/ent/iot/IotRiceCookerInfoCC.hpi
스마트 김치냉장고	http://www.dayou-winia.com
스마트세탁기	http://www.lge.com, http://www.samsung.com
스마트 건조기	http://www.lge.com, http://www.samsung.com
로봇 청소기	http://www.lge.com, http://www.samsung.com
스마트 리모컨	http://www.logitech.com/en-us/product/harmony-elite
제스처 리모컨	http://singlecue.com/
스마트 차고문 제어기	https://garageio.com/
스마트 잔디깍이	http://www.husqvarna.com/us/products/robotic-lawn-mowers/
스마트 혈압 측정기	https://ihealthlabs.com/
스마트 맥박 측정기	https://ihealthlabs.com/
스마트 혈당 측정기	https://ihealthlabs.com/
스마트 체중계	http://www.inbody.com/kr/product/InBodyH20B.aspx
스마트 에어컨	http://www.lge.com, http://www.samsung.com

홈 · 가전 IoT 제품	관련 제품 주소
스마트 전기 히터	https://www.balmuda.com/jp/smartheater/
스마트 보일러	http://www.rinnai.co.kr/
영상통화 IP 전화기	https://www.ipecs.co.kr/site/ericssonlg_ko/menu/159.do
유무선 공유기	http://iptime.com/iptime/
스마트 콘센트	http://www.dawondns.co.kr/views/product-b3.php
디지털 도어락	http://www.egateman.co.kr
무선 화제감지 센서	https://shop.leeo.com/
스마트 전력 차단기	http://www.schneider-electric.com.au/en/faqs/FA285554/
스마트 가스 차단기	http://www.soosanht.com/product/iot/
홈시어터(사운드 바)	http://www.lge.com, http://www.samsung.com
블루투스스피커	http://www.lge.com, http://www.samsung.com
빔 프로젝터	http://www.lge.co.kr/lgekor/product/media/minibeam/productDetail.do?cateId=1340&prdId=EPRD.310498#featureBtnsWrap
디지털 액자	https://mementosmartframe.com/
스마트 정수기	http://www.coway.co.kr/Product/Detail/?prodDispNo=162
스마트 식기 세척기	http://www.bosch-home.com/us/smart-dishwashers.html
스마트 커피메이커	https://nestle.jp/brand/nba/abouti/, http://www.mrcoffee.com/
스마트 공기정화기	http://www.lge.com, http://www.samsung.com
스마트 안마의자	http://www.bodyfriend.co.kr/mall/goods/goods_view.asp?goods=272&category=9&word=&asc=2&sorting=0&top_size=9
스마트 가습기	http://www.idea3.co.kr/page/page.php?pg_idx=110&thismenucode=3_sub010601
의류 스타일러	http://www.lge.com
스마트 프로판 가스통 게이지	http://www.iotlist.co/search?utf8=%E2%9C%93&terms=+propane+
스마트 스프링쿨러	http://www.rachio.com/
스마트 버튼	https://flic.io/
스마트화분모니터링제품	http://global.parrot.com/au/products/flower-power/
소모품 자동 주문 제품 (세제 등)	https://aws.amazon.com/ko/iotbutton/
스마트 활동량 측정기	https://misfit.com/fitness-trackers/misfit-shine-2

홈 · 가전 IoT 제품	관련 제품 주소
스마트 애완동물 Feeder	http://www.petnet.io/
스마트 전동 칫솔	https://www.kolibree.com/en/
스마트 컵	https://www.myvessyl.com/vessyl/
수면 패턴 분석 및 도우미	https://eightsleep.com/
스마트 조명	http://www.lge.com, http://www.samsung.com
무선 전동 블라인드	https://www.teptron.com/page/vertical-blinds
스마트 선풍기	http://m.post.naver.com/viewer/postView.nhn?volumeNo=4472729&memberNo=15460786&vType=VERTICAL
스마트 침대	https://www.sleepnumber.com/home
스마트 의자	http://www.duoback.co.kr/c_mbuy/?p_url=detail&p_id=CA001CB034CC001P002072
스마트 책상	http://www.magice.co/portfolio/ergo-desk/
스마트 환기구 제어기	https://keenhome.io/
무선 CO2 센서	http://trueyes.co.kr/airq
스마트 조명 스위치	http://www.lutron.com/en-US/Products/Pages/WholeHomeSystems/Homeworksqs/Overview.aspx
스마트 전력 검침기	http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170528005453
스마트 가스 검침기	http://www.soosanht.com/product/iot/
무선 온/습도 센서	https://nest.com/thermostat/meet-nest-thermostat/
무선 조도 센서	http://www.lutron.com/en-US/Products/Pages/Sensors/RadioPowrSavrDaylightSensor/Overview.aspx
무선 인감 센서	http://www.lutron.com/en-US/products/Pages/sensors/occupancy-vacancy/wirelessradiopowrsavr/overview.aspx
무선 창문 개폐 센서	http://www.rayhomeiot.com/
스마트 자물쇠	http://www.trionshop.com/
스마트 샤워기	http://www.us.kohler.com/us/Moxie-Showerhead-Wireless-Speaker/article/CNT120100003.htm
스마트 젓가락	http://www.homecrux.com/2014/09/05/20290/smart-chopsticks-check-freshness-of-food-youre-about-to-eat.html
스마트 미러(거울)	https://www.himirror.com/us_en/product/himirror

홈 · 가전 IoT 제품의 시스템 사양 기반의 등급(Class), 기능 및 기술은 다음과 같이 정의할 수 있다.

가. 등급(Class)

IETF RFC7228(Terminology for Constrained-Node Networks), ENISA(유럽네트워크정보보호원)의 'Security and Resilience of Smart Home Environments', TTA(한국정보통신기술협회)의 '사물인터넷 제품 등급 분류 및 보안 요구사항(TTAK.KO-12.0298)'에서 정의된 각각의 등급 분류를 의미하며, 시스템 사양을 확인하여 점검할 수 있다.

관련 보안항목 • 암호화 보안항목(경량화 적용 고려)

나. 개인정보 · 인증정보 · 센싱정보의 생성 · 저장 · 전송여부

제품이 개인정보, 인증정보, 센싱정보를 다루는지 여부를 의미하며, 제품의 기능과 동작을 고려하여 점검할 수 있다.

※ (예) 네트워크 카메라(웹캠)는 개인영상 촬영 후 실시간으로 전송되거나 저장 후 전송될 수 있기 때문에 개인정보의 생성 · 저장 · 전송이 해당될 수 있으며, 무선인터넷에 인증절차 후 접속하기 때문에 인증정보의 생성 · 저장 · 전송도 해당될 수 있다. 그리고, 사람의 움직임에 따라 촬영을 시작하는 기능이 구현될 수 있기 때문에 센싱정보의 수집 · 저장 · 전송 또한 해당될 수 있다.

관련 보안항목 • 인증, 암호화, 데이터 보호 보안항목

다. 무선통신

제품이 Wi-fi, Zigbee, Z-wave, BLE 등 무선통신 기능을 지원하는지를 의미하며, 시스템 사양 및 통신 프로토콜을 기반으로 점검할 수 있다.

관련 보안항목 • 데이터 보호 보안항목

라. OS(운영체제)

제품에 운영체제가 탑재되는지 여부를 의미하며, 시스템 사양을 기반으로 점검할 수 있다.

※ (참고) TTA 등급 분류 중 운영체제에 대한 구분이 반영된 '등급1'이상에 해당하는 제품들이 운영체제를 탑재한 제품으로 분류될 수 있으나 메모리(Flash 등) 크기 등을 고려하였을 때 TTA 등급분류 '등급2'이상이 적절할 것으로 판단되어 '등급2'이상인 제품에 대해서만 운영체제가 탑재될 수 있다고 표시하였다.

관련 보안항목 • 인증, 플랫폼 보안 보안항목

마. 웹 · 앱 연동

제품이 웹 또는 스마트폰 등의 앱(app)과 연동되는지 여부를 의미하며, 제품 기능을 기반으로 점검할 수 있다.

※ (참고) 최근 제품의 성능 및 기능 개선으로 기존에 웹 또는 앱과 연동되지 않던 제품들이 Wi-Fi 등 무선통신을 기반으로 스마트폰 등 모바일 단말기와 연동되는 경향성을 띄고 있다.

관련 보안항목 • 인증, 데이터 보호 보안항목

바. 업데이트 기능

제품의 유 · 무선 통신방식을 이용하여 제품의 업데이트 기능 제공 여부를 의미하며, 제품 제조사 지원내용을 기반으로 점검할 수 있다.

※ (참고) 소모품 개념의 저가 · 저성능 센서의 경우 업데이트에 대한 요구사항이 없었으나, IoT 제품의 성능 및 가격이 높아지고 보안위협이 증가하면서 보안패치 적용을 위한 업데이트 기능이 탑재되고 있다. OTP(One Time PROM) 메모리를 사용하지 않는 IoT 제품들을 제외한 대부분의 IoT 제품들은 유 · 무선 통신을 기반으로 원격 업데이트가 가능해지고 있다.

관련 보안항목 • 플랫폼 보안 보안항목

사. 물리적 I/F(인터페이스)

제품의 중앙처리장치 또는 메모리에 접근 가능한 내 · 외부 인터페이스 유무를 의미하며, 시스템 인터페이스 사양을 기반으로 점검할 수 있다.

※ (참고) 대부분의 IoT 제품은 물리적 내 · 외부 인터페이스를 보유하고 있다.

관련 보안항목 • 물리적 보안 보안항목

위에서 정의한 홈 · 가전 IoT 제품별 등급(Class)과 적용 기능 및 기술은 다음과 같이 조사되었으나, 조사된 내용이 모든 홈 · 가전 IoT 제품을 대표하지 않기 때문에 조사에 포함되지 않은 타 제조사 제품은 아래 조사된 내용과 상이할 수 있다. 또한, 향후 기술 발전에 따라 제품 등급이 상향 조정될 수 있으며, 다양한 기능 및 기술이 적용될 수 있다.

스마트홈가전 · IoT제품	등급(CLASS)			처리/저장/전송			무선 통신	OS	웹/앱 연동	업데이트 기능	물리적 I/F
	RFC	ENISA	TTA	개인정보	인증정보	센싱정보					
스마트TV	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/전송	●	●	●	●	●
셋톱박스 (스마트 박스)	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	–	–	●	●	●	●
스마트 냉장고	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/전송	●	●	●	●	●
스마트홈 인공지능 로봇	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	●	●	●	●
애완동물 모니터링 카메라	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	●	●	●	●
유아용 모니터링 제품 및 카메라	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	●	●	●	●
네트워크 카메라	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	●	●	●	●
스마트라우터	Class 2	HC	등급 3	–	처리/저장/전송	–	●	●	●	●	●
가정용 방화벽	Class 2	HC	등급 3	–	처리/저장/전송	처리/저장/전송	●	●	●	●	●
스마트 게이트웨이	Class 2	HC	등급 3	–	처리/저장/전송	–	●	●	●	●	●

스마트홈가전 · IoT제품	등급(CLASS)			처리/저장/전송			무선 통신	OS	웹/앱 연동	업데이트 기능	물리적 I/F
	RFC	ENISA	TTA	개인정보	인증정보	센싱정보					
월패드(IHD)	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	●	●	●	●
게임기	Class 2	HC	등급 3	처리/저장/전송	처리/저장/전송	–	●	●	●	●	●
스마트 오븐	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 전기밥솥	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 김치냉장고	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 세탁기	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 건조기	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
로봇 청소기	Class 2	HC	등급 2	–	처리/저장/전송	처리/저장/전송	●	●	●	●	●
스마트 리모컨	Class 2	HC	등급 2	–	처리/저장/전송	–	●	●	●	●	●
제스처 리모컨	Class 2	HC	등급 2	처리	처리/저장/전송	처리/전송	●	●	●	●	●
스마트 차고문 제어기	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 잔디깎이	Class 2	HC	등급 2	–	처리/저장/전송	–	●	●	●	●	●
스마트 혈압 측정기	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 맥박 측정기	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 혈당 측정기	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 체중계	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 에어컨	Class 2	HC	등급 2	처리/저장	처리/저장/전송	처리/저장/전송	●	●	●	●	●
스마트 전기 히터	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
스마트 보일러	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
영상통화 IP 전화기	Class 2	HC	등급 2	처리/저장/전송	처리/저장/전송	처리/저장/전송		●	●	●	●
유무선 공유기	Class 2	HC	등급 2	–	처리/저장/전송	–	●	●	●	●	●
스마트 콘센트	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
디지털 도어락	Class 2	HC	등급 2	처리/저장/전송	처리/저장/전송	–	●	●	●	●	●

스마트홈가전 · IoT제품	등급(CLASS)			처리/저장/전송			무선 통신	OS	웹/앱 연동	업데이트 기능	물리적 I/F
	RFC	ENISA	TTA	개인정보	인증정보	센싱정보					
무선 화제감지 센서	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 전력 차단기	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
스마트 가스 차단기	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
홈시어터 (사운드 바)	Class 2	HC	등급 2	–	처리/저장/전송	–	●	●	–	●	●
블루투스 스피커	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	–	●	●
빔 프로젝터	Class 2	HC	등급 3	–	처리/저장/전송	–	●	●	●	●	●
디지털 액자	Class 2	HC	등급 2	처리/저장/전송	처리/저장/전송	–	●	●	●	●	●
스마트 정수기	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 식기세척기	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 커피메이커	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 공기정화기	Class 2	HC	등급 2	–	처리/저장/전송	처리/저장/전송	●	●	●	●	●
스마트 안마의자	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●
스마트 가습기	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
의류 스타일러	Class 2	HC	등급 2	–	처리/저장/전송	–	●	●	●	●	●
스마트 프로판 가스통 게이지	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 스프링쿨러	Class 2	HC	등급 2	–	처리/저장/전송	–	●	●	●	●	●
스마트 버튼	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 화분모니터링 제품	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/저장/전송	●	–	●	●	●
소모품 자동 주문 제품 (세제 등)	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 활동량 측정기	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 애완동물 Feeder	Class 2	Class 2	등급 1	–	처리/저장/전송	–	●	–	●	●	●

스마트홈가전 · IoT제품	등급(CLASS)			처리/저장/전송			무선 통신	OS	웹/앱 연동	업데이트 기능	물리적 I/F
	RFC	ENISA	TTA	개인정보	인증정보	센싱정보					
스마트 전동 칫솔	Class 1	Class 1	등급 0	처리/전송	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 컵	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
수면 패턴 분석 및 도우미	Class 2	Class 2	등급 1	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 조명	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
무선 전동 블라인드	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
스마트 선풍기	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
스마트 침대	Class 2	Class 2	등급 1	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 의자	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 책상	Class 2	Class 2	등급 1	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	–	●	●	●
스마트 환기구 제어기	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
무선 CO2 센서	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 조명 스위치	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 전력 검침기	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 가스 검침기	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
무선 온/습도 센서	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	–	●	●
무선 조도 센서	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	–	●	●
무선 인감 센서	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	–	●	●
무선 창문 개폐 센서	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	–	●	●
스마트 자물쇠	Class 1	Class 1	등급 0	처리/저장/전송	처리/저장/전송	–	●	–	●	●	●
스마트 샤워기	Class 1	Class 1	등급 0	–	처리/저장/전송	–	●	–	●	●	●
스마트 젓가락	Class 1	Class 1	등급 0	–	처리/저장/전송	처리/전송	●	–	●	●	●
스마트 미러 (거울)	Class 2	HC	등급 2	처리/저장/전송	처리/저장/전송	처리/저장/전송	●	●	●	●	●

부록3

주요 홈 · 가전 IoT 제품 개발 시 고려 보안항목 예시

본 예시는 가이드 작성시 검토된 제품의 분석 결과로 보안항목이 적절하게 포함되어 있는 5개 제품을 선별하여 각 제품에 해당하는 보안항목을 제시하고 있다. 적용 보안항목은 “필수”와 “조건부”그리고 “예외”로 구분되며, “조건부”의 경우 해석이 필요하고, 해석의 사례로는 ‘보안항목 적용이 필요한 저사양의 제품인 경우’또는 ‘특정 라이브러리의 사용여부’로 구분하여 보안항목 해당여부를 판단한다. 아래 표에 선별된 제품이 모든 제품을 대표할 수 없고 사례로만 제시하고 있음을 고려해야 한다.

대상제품	포함 기능 유형	비고
스마트TV	센싱, 제어, 구매, 촬영, 중계, 운용, 관리	
디지털 도어락	제어, 운용	
스마트 세탁기	운용	
스마트 콘센트	운용	
창문개폐센서	센싱, 제어	

구 분		스마트TV	디지털 도어락	스마트 세탁기	스마트 콘센트	창문 개폐 센서	비 고
소프트웨어 보안	시큐어코딩	●	●	●	●	●	–
	알려진 보안취약점 점검 및 제거	●	●	●	●	●	–
	최신 3rd party 소프트웨어 사용	●	●	●	●	●	최신 3rdparty 소프트웨어적용 시 필수 고려 항목
물리적 보안	물리적 인터페이스 차단	●	●	●	●	●	–
인증	인증 및 접근통제	●	●	●	–	–	–
	상호인증	●	●	●	●	●	–
암호화	암호연산	●	●	●	●	●	–
	암호 키 관리	●	●	●	●	●	–
데이터 보호	안전한 통신채널	●	●	●	●	●	–
	저장 및 전송데이터 보호	●	●	▲	▲	▲	• 암호키 : 필수 • 데이터 중요도에 따라 선별적 적용 가능
	개인정보 보호	●	●	–	–	–	–
제품 플랫폼	설정 값 및 실행코드 무결성 검증	●	●	–	–	–	–
	안전한 업데이트	●	●	●	●	●	–
	감사기록	●	●	–	–	▲	게이트웨이 또는 제어 제품 (월패드)에 감사기록 저장 가능

부록4

하드웨어 보안기술과 소프트웨어 보안기술의 동시 사용 시 보안 고려사항

출처: IoT 공통보안 가이드

저성능의 IoT 제품에서 높은 수준의 보안 기능을 제공하기 위하여, 소프트웨어 보안기술과 하드웨어 보안 기술(서버단 HSM, SE 등)을 함께 적용하는 경우가 존재할 수 있다. 이와 같은 경우에 대한 사례로는, 주로 보안을 위해 추가적으로 요구/소모되는 리소스를 하드웨어로 구성하여 공급하거나, IoT 제품 및 서비스의 데이터 암·복호 화에 사용하는 키, 인증정보, 카드번호, 결재정보, 개인정보 등의 민감한 데이터를 물리적으로 분리하여 저장할 수 있도록 하는 경우가 일반적이다. 이때 소프트웨어 보안 기술은 주로 IoT 제품의 메인 MCU에 올라가게 되며, 하드웨어 보안 기술은 MCU 주변의 하드웨어 모듈로 장착되어 한 보드에 올라 메인 MCU와 하드웨어 보안 모듈간의 통신은 Serial로 I2C, UART, SPI 등을 통해 이루어진다.

실제, IoT 제품(Host)에 하드웨어 보안 모듈과 소프트웨어 보안 모듈 간 내부 상호 통신(ISO 7816 APDU) 방식을 사용하여 융합보안 서비스를 제공 하는 경우에는, IoT 서비스와 IoT 제품 내부의 보안수준을 고려하여 신뢰할 수 있는 접근방법(단방향 및 양방향 인증)을 통해, SW 및 HW기반 보안 기술 간 안전한 내부(제품내 인사이드) 보안 채널을 구성할 수 있다.

이를 통해 실제 전송되는 데이터에 대한 기밀성과 무결성을 제공함으로써, 하드웨어 보안모듈에서 저장된 키를 보안채널을 통하여 안전하게 호출 및 사용이 가능하다.

홈가전 IoT 보안가이드

인 쇄 2017년 7월 인쇄
발 행 2017년 7월 발행

발행처 한국인터넷진흥원
발행인 백기승
주 소 (58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원
TEL. 1544-5118 / FAX. 405-5209 / www.kisa.or.kr

제 작 호정씨앤피(02-2277-4718)

홈·가전 IoT 보안가이드

과학기술정보통신부
KISA 한국인터넷진흥원
IoT Internet of Trust 보안얼라이언스