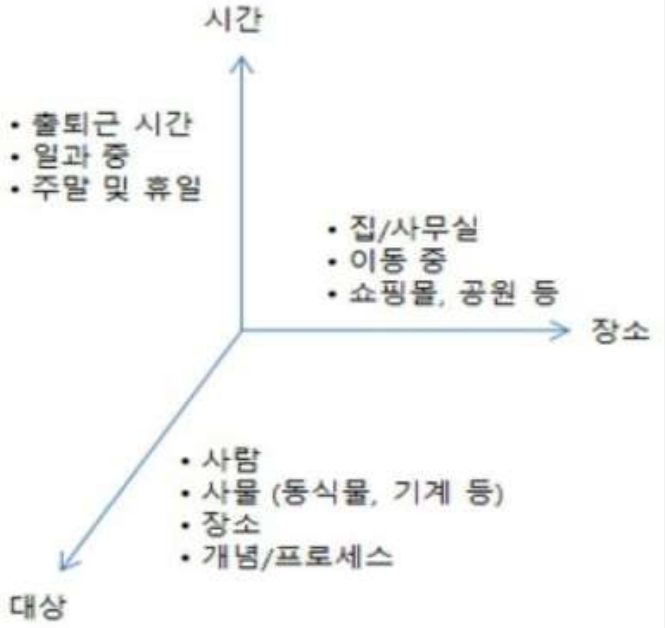
1.5 사물인터넷 보안

1.5.1 사물인터넷 보안개요

◆ 사물인터넷 보안 및 프라이버시 문제

- **다양한 사물들을 다양한 요소기술**(센싱, 통신 및 네트워킹, OS 및 임베디드 시스템, 플랫폼 기술, 빅 데이터 및 데이터마이닝, 웹 및 응용 서비스 기술 등)**을 이용하여 사물인터넷으로 연결되는 과정에서 보안 취약성 발생 가능함**
  - 사물인터넷 적용 대상은 다양한 사물과 물리적인 공간, 가상 시스템까지 확대해 나감
  - 사이버 공간에서의 해킹은 그대로 물리적인 공간의 위험으로 전이될 수 있음
- **사물인터넷 서비스는 처음부터 끝까지 일관된 방식으로 보안 및 프라이버시를 보장하는 것이 어려움**
  - 사물인터넷은 서비스의 주체가 공존하는 수평적 시장(horizontal market)으로, 보안 및 프라이버시 이슈에 소극적으로 대응하는 기업에 의해 문제가 발생할 수 있음

〈 사물인터넷 적용 대상의 확대 〉



※ 수직적 시장(vertical market)에서는 단일 기업이 서비스에 대한 보안 및 프라이버시 침해 문제에 대한 관리 및 대응이 가능함

1.5 사물인터넷 보안

1.5.1 사물인터넷 보안개요

구분	정보보호 패러다임의 변화	
보호 대상	PC, 모바일	가전, 자동차, 의료기기 등 모든 사물(Things)
대상의 특성	고성능, 고가용성을 가지는 운영환경	고성능, 고가용성 + 초경량, 저전력
보안 주체	ISP, 보안 전문업체, 이용자	ISP, 보안 전문업체, 이용자 + 제조사, 서비스제공자
보호 방법	별도의 보안장비, S/W 구현 및 연동	별도의 보안장비, S/W 구현 및 연동 + 설계단계부터 사물 내 보안 내재화
피해 범위	정보유출, 금전피해	정보유출, 금전피해 + 시스템 정지, 생명 위협

1.5 사물인터넷 보안

1.5.1 사물인터넷 보안개요

- IoT 기반 융합 서비스가 활성화 될수록 기하급수로 증가하게 될 IoT 연결 장치 (connected devices)들은 작게는 데이터를 수집하는 센서와 간단한 제어가 가능한 액츄에이터를 포함하여, 복수개의 센서와 액츄에이터를 갖는 이종 복합 시스템들까지 다양해진다. 따라서 기존 시스템 중심으로 설계된 인터넷 보안 기술로 안전과 프라이버시 보호를 수행하기에는 무리가 따른다.

  ➔ IoT 장치 및 서비스의 '설계–개발' 단계부터 보안과 프라이버시 보호 체계를 고려해야 함

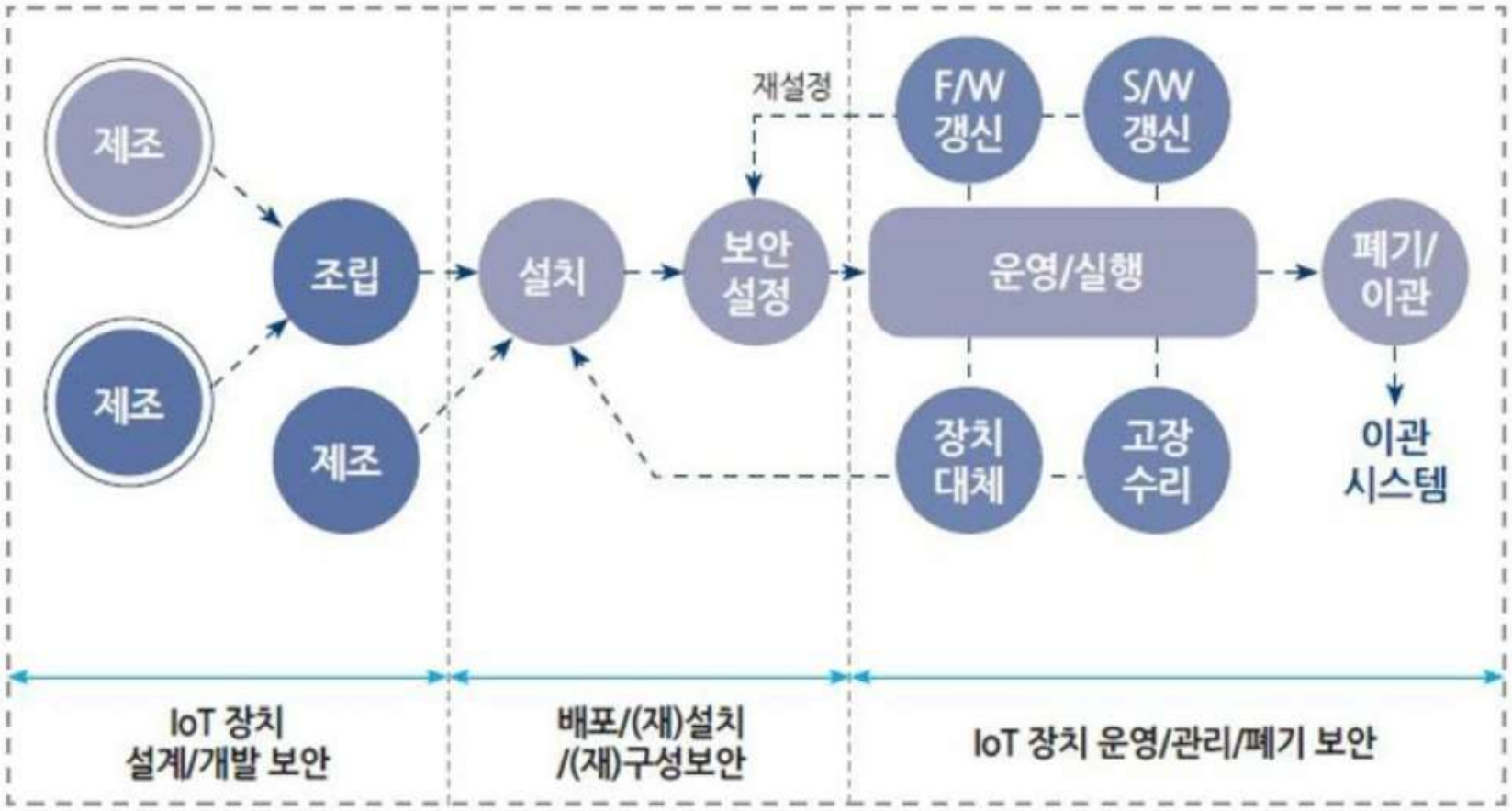
- IoT 장치를 '배포, 설치' 하는 단계에서도 사전에 잠재적 보안 위협을 차단할 수 있도록 해야 하며, 실사용이 이루어지는 '설정–운영–실행–폐기' 단계에서는 이 전 단계를 모두 고려하여 전주기적 침해 요소의 분석 및 대응 방안을 마련해야 한다.

  ➔ 즉, 보안의 잠재적 위협요소와 취약점을 전주기 단계에서 점검할 수 있는 기본적인 공통 보안 요구사항과 사용 주체별로 고려해야 하는 최소한의 보안 점검 항목이 필요함

1.5 사물인터넷 보안

1.5.1 사물인터넷 보안개요

IoT 장치의 전주기 단계별 보안 고려사항



※ F/W: Firmware, S/W : Software

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

단계별 보안 요구 사항	IoT 공통보안 7대 원칙
IoT 장치의 설계/개발 단계의 보안 요구 사항	(1) 정보보호와 프라이버시 강화를 고려한 IoT 제품 · 서비스 설계 (2) 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증
IoT 장치 배포/설치(재설치)/구성(재구성) 단계의 보안 요구 사항	(3) 안전한 초기 보안 설정 방안 제공 (4) 보안 프로토콜 준수 및 안전한 파라미터 설정
IoT 장치 및 서비스 운영/관리/폐기 단계의 보안 요구 사항	(5) IoT 제품 · 서비스의 취약점 보안패치 및 업데이트 지속 이행 (6) 안전한 운영 · 관리를 위한 정보보호 및 프라이버시 관리체계 마련 (7) IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

① 정보보호와 프라이버시 강화를 고려한 IoT 제품 · 서비스 설계

: “Security by Design” 및 “Privacy by Design” 기본 원칙 준수

‘Security by Design’ : IoT 제품 및 서비스의 설계 단계부터 보안을 내재화하고, 지속적인 대응을 수행하여 서비스 사용자 및 사업자의 자원 및 정보를 보호한다는 개념으로 다음을 포함한다.

- IoT 장치가 갖는 저전력/저성능 특성을 고려하여 기밀성, 무결성/인증, 가용성 등 정보 및 기기의 오용을 최소화하면서 경량화 할 수 있는 방안을 고려한다.
- IoT 서비스에서는 IoT 장치 및 정보에 대하여 서비스 운용환경에 맞는 장치의 접근권한관리, 종단간 통신보안, 무결성/인증 제공 등의 방안을 제공한다.
- 소프트웨어 보안 기술과 하드웨어 보안 기술의 적용을 적극 검토하고, 안전성이 검증된 표준 보안 기술을 활용한다.

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

'Privacy by Design' 은 IoT 제품 및 서비스의 설계 단계에서부터 프라이버시 침해 위협 요소를 분석하여 지속적으로 점검하고 침해가 발생하기 전에 선제적인 대응을 한다는 프라이버시 보호 개념이다. 프라이버시 강화는 IoT 서비스 제공에 필요한 최소한의 정보만을 취득하고, 사용자가 동의한 기간과 서비스 범위 내에서만 정보를 사용하여 개인의 민감한 정보를 보호하는 방안으로 다음의 고려사항들을 포함한다.

- IoT 장치와 IoT 서비스 운영 정책에 사용자의 프라이버시 보호 방법론을 기본으로 적용한다.
- IoT 장치가 수집하는 프라이버시 정보에 대하여 암호화 전송, 익명 저장 및 무결성/인증 방안 등을 포함한다.
- IoT 서비스는 수집된 프라이버시 정보에 대한 비식별화, 접근관리/인증, 기밀성, 안전한 저장 등에 대한 방안을 포함한다.
- IoT 서비스 제공자는 사용자에게 프라이버시 정보의 사용 범위 및 기간 등을 포함한 운영 정책을 가시화하여 투명성을 최대한 보장한다.

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

② 정보보호와 프라이버시 강화를 고려한 IoT 제품 · 서비스 설계
:시큐어 코딩, 소프트웨어, 어플리케이션 및 소프트웨어 보안성 검증 및 시큐어 하드웨어 장치 활용

◆ 시큐어 코딩 적용(1)

유형	내 용
이력 데이터 검증 및 표현	• 입력 데이터에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안 취약점 예) SQL 삽입, 자원 삽입, 크로스사이트 스크립트, 운영체제 명령어 삽입, LDAP 삽입, 디렉터리 경로 조작 등
보안기능	• 보안기능(인증, 접근제어, 기밀성, 암호화, 권한관리 등)을 부적절하게 구현할 시 발생할 수 있는 보안약점 예) 부적절한 인가, 중요한 자원에 대한 잘못된 권한설정, 취약한 암호화 알고리즘 사용, 사용자 중요정보 평문 저장(또는 전송)
시간 및 상태	• 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작하는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안 약점 예) 검사시점과 사용시점, 제어문을 사용하지 않는 재귀함수 등
에러처리	• 에러를 처리하지 않거나, 불충분하게 처리하여 에러 정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안약점 예) 오류 메시지를 통한 정보 노출, 오류 상황 대응 부재 등

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

◆ 시큐어 코딩 적용(2)

유형	내 용
코드오류	• 타입변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점 예) 널(Null) 포인터 역참조, 부적절한 자원 해제, 무한 자원 할당 등
캡슐화	• 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않는 사용자에게 데이터 누출이 가능해지는 보안약점 예) 제거되지 않고 남은 디버그 코드, 시스템 데이터 정보노출
API 오용	• 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점 예) DNS lookup에 의존한 보안결정

※ 보안은 오동작 또는 결함이 나타날 때에 추가할 수 있는 것이 아니다. 따라서 개발자는 장치와 관계없이 소스코드 구현단계부터 내재될 수 있는 보안 취약점을 사전에 예방하기 위해 시큐어 코딩을 적용해야 한다.

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

◆ 소프트웨어 보안성 검증

- IoT 제품 · 서비스 개발 시, 제품 및 서비스의 생산성을 높이고 품질을 향상시키기 위해 다양한 S/W를 활용할 경우, 현재까지 알려진 보안 취약점에 대한 보안성 검증을 수행하고 보안 패치를 반드시 적용해야 함
- 알려진 보안 취약점에 대한 보안성을 검증하기 위해 아래의 가이드라인 절차와 같이 수행하며, 참조사이트를 통해 알려진 취약점을 검색 · 대응함

유형	내 용
의존 S/W 열거	•사용한 오픈소스 S/W를 포함하여 의존성을 가지는 S/W들을 확인하고 열거해야 함 예) 오픈소스 프레임워크인 AllJoyn을 사용한다면, AllJoyn과 OpenSSL 등과 같이 AllJoyn을 사용하기 위해서 필요한 추가적인 S/W 및 library 등을 리스트로 열거해야 함
취약점 검색	•열거된 의존 S/W들에 대한 취약점을 검색해야 함 예) 의존S/W 열거단계에서 열거된 모든 S/W 및 library에 대한 취약점을 CVE, CWE, OWASP 등을 통해서 검색 수행
취약점/대응방법 열거	•S/W 별로 알려진 취약점을 열거 예) 열거된 S/W에 대한 CVE, CWE, OWASP 등에서 검색된 취약점 및 대응 방법을 항목별로 리스트에 열거
대응방법 반영	•알려진 취약점에 대한 대응절차에 따라 오픈소스 S/W에 반영하여 보완해야 함

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

◆ 시큐어 하드웨어 장치 활용

IoT 장치는 응용 서비스 종류에 따라 다양한 수준의 보안 강도를 필요로 한다. IoT 장치는 공격자에게 쉽게 노출될 수 있는 환경에 주로 설치되기 때문에 부채널 공격이나 펌웨어 코드 추출, 키 값 추출 등 다양한 하드웨어 보안 취약성을 갖는다. 이 때문에 하드웨어 보안성을 강화하기 위해 펌웨어/코드 암호화, 실행코드 영역제어, 역공학 방지 기법 등 다양한 하드웨어 보안 기법이 존재하며 이를 IoT 장치의 응용 환경에 따라 적절히 적용할 필요가 있다.

◆ 소프트웨어 보안 기술과 하드웨어 보안 기술 융합

소프트웨어 보안 기술과 하드웨어 보안 기술이 융합되는 경우, 소프트웨어 보안 기술과 하드웨어 보안 기술 간에 반드시 신뢰하는 접근 방법(단방향 및 양방향 인증) 기반의 안전한 보안 채널을 구성하여 전송 데이터에 대한 기밀성과 무결성 기능을 제공해야 한다.

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

③ 안전한 초기 보안 설정 방안 제공

: Secure by Default " 기본 원칙 준수

대부분의 경량화 장치들은 사용자 입출력 인터페이스(예, 디스플레이 장치나 입력 키패드 등)가 부재하거나 제한적이므로 설정 방안 제공이 중요함

- 제조사와 설치자가 IoT 장치의 초기 설정을 수행할 때, 보안 모듈과 파라미터는 안전하게 설정되어야 함(예, 국내 · 외를 사업 대상으로 하는 장치나 서비스의 경우 국제표준 권고 기준인 AES-128 이상의 보안 강도 준수)
- 서비스에서 강력한 암호와 무결성을 요구하는 경우 옵션 중 강한 암호를 기본으로 설정 (예, AE(Authenticated Encryption) 암호 모드 적용)
- 제조 시 기본으로 설정되어진 계정 이름과 패스워드를 설치 시 변경
- 응용 프로그램이 특정 기간이 지나면 암호 키와 인증 패스워드의 만료를 권고할 수 있는 옵션을 활성화하여 설정
- 장치 간, 장치와 인터넷 간에 암호화 통신을 사용하도록 기본 설정
- 다중 요소 인증이 옵션으로 제공될 경우 필요 시 활성화하여 설정
- 다중 사용자로 구성되는 서비스 환경에서는 최소한의 권한으로 초기 설정

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

④ 보안 프로토콜 준수 및 안전한 파라미터 설정
:통신 및 플랫폼에서 검증된 보안 프로토콜 사용 (암호/인증/인가 기술)

- 사물인터넷의 경우, 경량 장치들 간 및 경량 장치와 플랫폼 간의 정보 공유 시 적용 환경을 고려한 경량화 보안 프로토콜의 사용이 고려되어야 함
- 이러한 데이터 전송 보안 기술과 더불어 사용자의 인증 및 인증된 사용자의 접근 권한을 안전하게 관리하는 방식에서도 검증된 보안 프로토콜의 적용과 경량화를 고려해야 함

유형	내 용
네트워크	• 사물인터넷 서비스에서 주로 사용되는 통신/네트워크 접속 프로토콜에 적합한 보안 요구사항 만족
사물인터넷 전용 프로토콜	• 사물인터넷 표준 기구에서 표준화한 데이터 전송 프로토콜에서 권고하는 보안 요구사항 만족 • 프로토콜 간 연동 시 보안 취약성 해소 필요
사물인터넷 플랫폼	• 검증된 표준 기구에서 정의하고 있는 사물인터넷 플랫폼에서 요구하는 보안 요구 사항 만족
서비스 모델	• 서비스별로 다양한 보안 요구사항 및 보안관련 법/규제가 있을 수 있으며, 이를 만족시켜야 함 • 응용 서비스별 특성을 고려하여 맞춤형 보안 요구사항을 만족해야 함

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

⑤ IoT 제품 · 서비스의 취약점 보안패치 및 업데이트 지속 이행

- IoT 제품 제조사와 서비스 제공자는 IoT 제품 · 서비스에서 보안 취약점이 발견되면 이에 대한 분석을 수행하고, 보안 요구사항을 반영한 보안패치를 신속히 배포할 수 있도록 사후 조치 방안을 마련해야 함
  - ✓ 보안패치 및 업데이트 파일의 배포 과정에서 발생 가능한 위 · 변조 문제를 사전에 예방할 수 있도록 무결성 검증 기술을 적용해야 함
- 통신 채널을 활용한 업데이트 S/W의 전송 시 다음의 보안 서비스는 반드시 제공되어야 함

유형	내 용
네트워크	• 업데이트 서버와 IoT 장치 사이에 상호 인증 기능을 제공하여 위장 서버나 중간자 공격 등의 취약점에 대응할 수 있도록 함
사물인터넷 전용 프로토콜	• 저장 데이터(업데이트 설정 정보 파일: 예, conf, xml, ini 등)와 처리 데이터(주요 파라미터 관련 정보의 임시폴더나 설치 공간) 및 전송 데이터(업데이트 전송 정보)에 대하여 해커의 공격에 대비하여 암호화하여 저장/처리/전송해야 함 • IoT 제품 · 서비스의 보안 패치에 대한 코드 서명(Code Signing) 기법의 적용을 고려해야 함
사물인터넷 플랫폼	• 저장 데이터(업데이트 정보 파일), 처리 데이터(실행 파일) 및 전송 데이터(업데이트 전송 정보)에 대해 무결성 검사를 수행해야 함

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

⑥ 안전한 운영 · 관리를 위한 정보보호 및 프라이버시 관리체계 마련
: 사용자 정보 취득–사용–폐기의 전주기 정보의 보호 및 프라이버시 관리

- IoT 장치를 통해 다량의 개인정보가 수집 · 저장 · 전송될 수 있으며, 개인정보가 유출될 경우 심각한 프라이버시 침해 문제가 발생할 수 있음

  ➔ 따라서 최소한의 개인정보만 수집 · 활용될 수 있도록 개인정보보호정책 수립

- IoT 제품 · 서비스의 설계 및 개발이 완료되었다면 설계 시 수립된 보안위험 분석을 기반으로 안전한 운영과 관리를 위한 보안대책과 기술적 방안이 마련 되어야 함
- IoT 서비스의 운영 과정에 대한 안전한 정보보호 및 프라이버시 관리체계와 기술적 방안이 마련되어야 함
- 정보보호 관리체계는 IoT 서비스를 위한 유 · 무형 자산과 이에 대한 위험 식별, IoT 장치의 비인가 접근 및 도난 · 분실을 방지하기 위한 물리적 접근통제, 침해사고 발생 시 서비스 연속성이 유지될 수 있도록 백업 및 복구 절차 수립 등을 포함하고 있어야 함
- 설치 · 배포된 IoT 장치의 주기적인 보안 업데이트, 패치 적용, 폐기절차 등 사후관리 방안 등이 포함되어야 함

1.5 사물인터넷 보안

1.5.2 사물인터넷 공통 보안 7대 원칙

⑦ IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련
: 보안 사고에 대비한 침입탐지와 사고 시 분석 및 책임추적성 확보

- IoT 서비스는 다양한 유형의 IoT 장치, 유 · 무선 네트워크 장비, 플랫폼 등으로 구성되며, 각 영역에서 발생 가능한 보안 침해사고에 대비하여 침입탐지 및 모니터링이 수행되어야 함
  - ✓ 침해사고 발생 이후 원인분석 및 책임추적성 확보를 위해 로그기록을 주기적으로 안전하게 저장 · 관리해야 함
  - ✓ 단, 저전력 · 경량형 하드웨어 사양 및 운영체제가 탑재된 IoT 장치의 경우, 그 특성상 로그기록의 생성 · 보관이 어려울 수 있으므로, 이런 경우에는 서비스 운영 · 관리시스템에서 IoT 장치의 상태정보를 주기적으로 안전하게 기록 · 저장할 수 있어야 함

1.5 사물인터넷 보안

1.5.3 사물인터넷 분야별 보안 위협

① 칩벤더

- 일반적으로 보안시스템은 OS 및 펌웨어과 같은 상위 계층에서 동작함으로 하위계층의 마이크로칩과 같은 경우는 하드웨어 자체에서의 보안 시스템이 따로 구현되어 있어야만 함
- 이러한 하위계층인 칩의 경우 물리적인 접근으로 인한 공격을 통해 칩 내부의 회로 단계에서 보안 취약점이 발생 될 수 있음

명칭	공격 유형	보안 위협
부채널 공격	– 칩이 동작할 때, 변화하는 전력 소모, 열, 연산 소모 시간, 전자기파 등 부가적인 정보를 이용 – 부채널의 정보에 따라 시차 공격, 전력 분석 공격, 전자기파 분석 공격, 오류 주입 공격 등으로 분류	– 비밀 데이터 및 키 등의 주요 보안정보 추출 가능 – 공격 시 칩의 외부에서 접근 가능한 인터페이스만을 이용하기 때문에 상대적으로 적은 시간과 비용을 가짐으로 빠른 피해 확산이 가능
메모리 공격	– 메모리 내용을 추출하거나 복제, 변경 – 급속냉각, 메모리 연결버스의 데이터 관찰 삽입 및 추출	– 메모리 내의 정보를 획득할 수 있으며, 공격자의 악의적인 코드가 담긴 메모리로 교체하는 공격이 가능하고 전원이 차단된 비휘발성 메모리뿐만이 아닌 휘발성 메모리에도 공격이 가능
역공학을 통한 버스 프루핑 공격	– 칩의 패키지를 제거하고 칩의 각 층을 하나씩 제거 후, 칩 내부의 레이아웃을 통해 신호를 관찰하여 데이터 확인	– 메모리나 코어 등의 데이터를 획득하거나 연결된 버스의 회로 데이터를 분석하여, 지나는 데이터를 수집 및 분석하여 내부 코드를 추출할 수 있음

1.5 사물인터넷 보안

1.5.3 사물인터넷 분야별 보안 위협

② 모듈/디바이스

- 모듈/디바이스의 경우 무선 송수신칩+마이크로컨트롤러 및 일정의 프로세스를 갖추고 있기 때문에 데이터의 저장, 처리, 판단기능 및 네트워크 접속 능력을 가진 기기에 대하여 공격을 진행할 수 있어, 모듈/디바이스 자체의 오작동과 정보 유출이 가능함

명칭	공격 유형	보안 위협
악성코드, 바이러스	– 악성 코드, 바이러스 삽입을 통한 정보 위변조	– 기기 제어 흐름에 대한 정보 추출로 기기의 오작동을 일으킬 수 있으며, 내부에 저장된 정보 노출피해 발생 가능
코드 삽입 및 재사용 공격	– 비인증 관리 단말에 물리 혹은 논리적으로 접속하여 공격자의 코드를 시스템 내에 삽입	– 기기의 Root 권한 탈취 및 악의적 코드 실행으로 인하여 기기의 오작동발생 가능
제로데이 취약점	– 임베디드OS 및 미들웨어 기기 자체의 알려지지 않은 취약점을 통해 공격을 진행	– 기기의 인증정보, 개인정보 및 기타 저장정보에 대한 노출 피해 발생 가능

1.5 사물인터넷 보안

1.5.3 사물인터넷 분야별 보안 위협

③ 플랫폼/솔루션, 네트워크/서비스

- 플랫폼/솔루션과 네트워크/서비스에 대한 보안 위협은 유무선 네트워크가 연결된 시스템 혹은 서버, 소프트웨어로 이루어짐으로 상호 복합적인 보안 위협이 발생될 수 있음

명칭	공격 유형	보안 위협
비인가 접근	– ID/PW 대입공격 및 탈취로 인한 접근 이후 주변 장치 스캔 및 악성코드 삽입, 관리 시스템 해킹	– 연결된 여러 사물들의 상태 변경, 관리시스템에서의 내부 정보 변경을 이용한 상태 이상 발생
개인정보 탈취 및 정보유출	– 서버 및 통신 기기의 취약점을 이용한 관리권한 획득 및 백도어 설치	– 개인정보 유출로 인한 2차 피해 발생 가능 정보 자산에 대한 노출 위험
서비스 거부 공격 및 네트워크 공격	– MITM, 스니핑, DDoS와 같은 일반 네트워크 취약점이 IoT환경에 그대로 전이	– 정보유출 및 정상적 서비스를 방해하여 상태 이상 발생

1.5 사물인터넷 보안

1.5.4 사물인터넷 보안 요구 사항 및 대응 방안

① 칩벤더

- 칩벤더의 보안 취약점은 마이크로컨트롤러 자체에 존재함으로 IoT기기의 칩 생산시 이를 원천적으로 봉쇄하여야 함

MCU Developer의 보안강화

명칭	보안 요구사항 및 대응방안
부채널 공격	• 마스킹 – 연산 중간 과정에서 연산 값을 랜덤하게 만드는 방식으로 입력 값과 출력 값의 연관관계를 최대한 줄임 • 하이딩 – 연산 중간의 전력 소모량을 통일하거나 랜덤하게 만들어 전력변화에 대한 데이터를 측정하지 못하게 함
메모리 공격	PUF(Physical Unclonable Function) – 하나 이상의 키는 예측 불가능한 랜덤 값으로 생성하고 키를 메모리상에 저장하지 않으며, 추가적으로 키가 필요한 경우 이를 이용하여 암호화 후 메모리에 저장
역공학을 통한 버스 프루핑 공격	내부 구성 변경 – 키 생성 모듈이 암호 모듈 내부에 존재하도록 하여 키들이 버스를 통해 이동하지 않도록 구성

1.5 사물인터넷 보안

1.5.4 사물인터넷 보안 요구 사항 및 대응 방안

② 모듈/디바이스

- 모듈/디바이스는 임베디드 OS, 미들웨어 등 모듈/디바이스에 대한 상시 취약점 점검 및 제품의 지속적 업데이트 체계가 반드시 필요

명칭	보안 요구사항 및 대응방안
악성코드, 바이러스	– 지속적 정적 분석(바이너리/바이트코드 분석) 및 동적 분석(로깅 분석) – 정보의 암호화 관리 및 제품/단말의 상시 진단 – 외부로부터 유입되는 데이터로 인한 단말의 운영체제, 하드웨어 등이 영향을 받지 않도록 운영체제와 데이터를 논리적으로 격리
코드삽입 및 재사용 공격	– 기기의 개발 단계에서 시큐어 코딩을 적용하여 소스코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계, 구현함
제로데이 취약점	– 제품/단말의 지속적인 업데이트 지원 및 단말 상태 및 이벤트 관리 – 보안 정책에 맞추어 리소스와 서비스를 제공

1.5 사물인터넷 보안

1.5.4 사물인터넷 보안 요구 사항 및 대응 방안

③ 플랫폼/솔루션, 네트워크/서비스

- 모듈/디바이스는 임베디드 OS, 미들웨어 등 모듈/디바이스에 대한 상시 취약점 점검 및 제품의 지속적 업데이트 체계가 반드시 필요

명칭	보안 요구사항 및 대응방안
비인가 접근	– 위장 사물, 기능이 변조된 사물 등의 서비스 비인가 접속 차단, 기기 간 인증, 키 관리 및 접근 제어 사용
개인정보 탈취 및 정보유출	– 표준화된 암호화 기법을 사용하여 안전한 데이터 관리 – 망분리를 통한 데이터 영역과 통신 영역 분리
서비스 거부 공격 및 네트워크 공격	– IoT 게이트웨이 및 서버에 방화벽 및 보안 시스템을 구축하여 내부 기기 및 서비스에 영향을 미칠 수 없도록 함