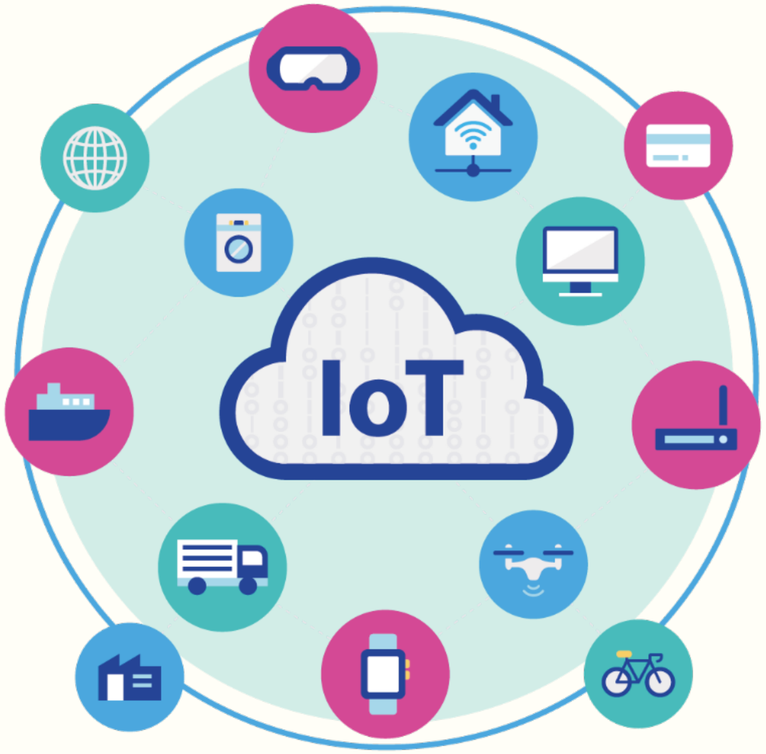
IoT 환경에서의 개인정보 보호

10조
김수연
전성배
윤건우
박성준

2024.12.04

목 차

IoT 란?



IoT 란?

Internet of Things의 줄임말로 인터넷을 통해 다양한 장치들이 서로 연결되어 데이터를 주고 받는 기술

종류

스마트 워치, 스마트 냉장고, CCTV, 홈캠, 로봇청소기, 스마트TV 등

IoT 보안 위협 사례

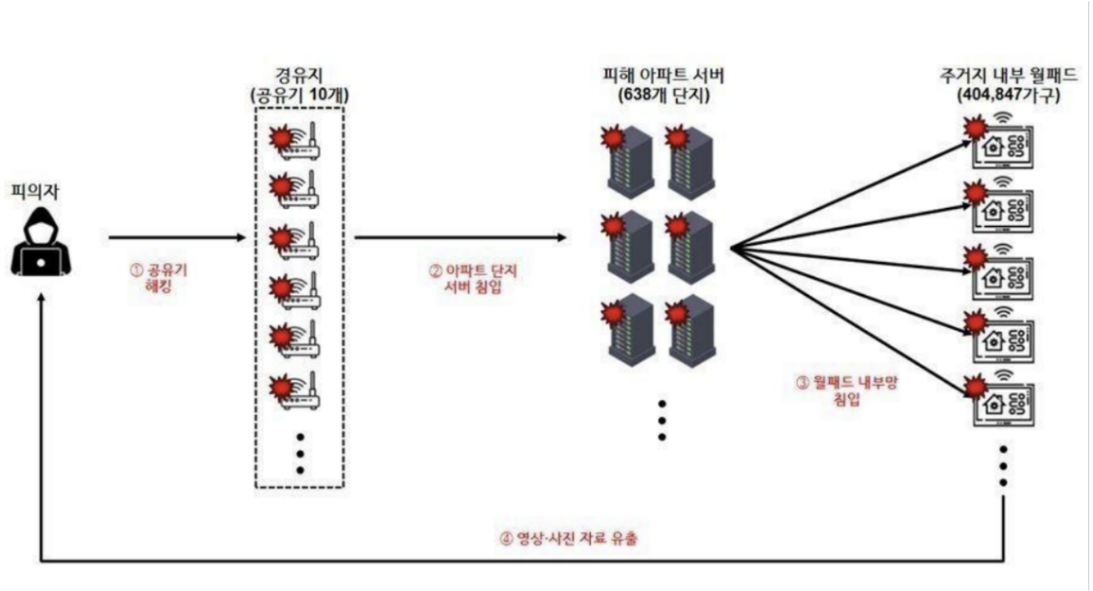
22년 40만 개 이상의 아파트 월패드 해킹

시사IN

사회

허술한 사물인터넷 보안, 40만 명의 사생활이 노출됐다

40만 개 넘는 가정용 월패드가 해킹돼 사생활이 유출됐다. 해외에서도 유사한 사건이 빈번히 일어난다. 전문가들 사이에서 사물인터넷의 취약한 보안이 논의된 것은 오래된 일이다.



먼저 식당이나 숙박업소 등의 인터넷 공유기를 해킹하여 일종의 '경유지'를 마련하고, 대부분 아파트의 세대 내 월패드는 하나의 망을 통해 중앙관리 서버에 연결되어 있는 점을 이용해 A씨는 중앙관리 서버에 침입해 악성 프로그램을 설치한 후, 이를 통해 가구별 월패드까지 접근

IoT 보안 위협 사례

2016년 인터넷 호스트 업체 Dyn DDos 공격

美 호스팅업체 DDoS 공격받아…미국 인터넷 주요 사이트 마비

김범수 기자

입력 2016.10.22. 18:18

미국 주요 인터넷 호스팅 서비스업체 '딘(Dyn)'이 연속적인 대규모 해킹 공격을 받아 트위터, 넷플릭스, 뉴욕타임스(NYT) 등 주요 사이특 마비되거나 서비스가 지연되는 일이 벌어졌다.

DDoS

DDoS 공격은 여러 대의 컴퓨터가 동시에 특정 웹사이트나 서버에 과도한 트래픽을 보내 과부하를 일으켜 정상적인 접속을 방해하는 사이버 공격
쉽게 말해, 너무 많은 사람이 한 번에 몰려 웹사이트가 다운되는 것과 비슷하다.

봇넷

봇넷은 해커가 감염시킨 여러 대의 컴퓨터나 기기를 네트워크로 연결해 하나의 그룹처럼 조종하는 것이다.
이를 통해 해커는 대규모 공격이나 불법 활동을 쉽게 수행할 수 있다.

문제 제기

우리나라에는 사물인터넷(IoT) 관련 명확한 법률이 제정되어 있지 않으며, 현재는 한국인터넷진흥원(KISA)과 미래창조과학부 등 기관에서 제공하는 가이드맵만 존재한다.

IoT 보안인증제도는 운영 중이지만, 2024년 10월 기준 대기업과 해외 기업의 인증 신청이 없고, 중소기업 참여도 저조하다.

이는 강제성이 부족한 자율적 제도 때문이며, 실효성을 높이기 위한 법적 기반과 강제적 참여 유도가 필요하다.

영국 PSTI 법

제조·수입·유통업체에기본 비밀번호 금지, 보안 업데이트 기간 공개, 취약점 보고 정책 의무화를 요구한다. 미준수 시 민사·형사처벌 등 제재가 있으며, 영국 시장에 제품을 공급하려면 반드시 준수해야 한다.

미국 IoT Cybersecurity Improvement Act of 2020

미국 연방 정부는 IoT 기기에 최소한의 보안 표준 준수를 의무화하고, 이를 위반한 계약 기업에는 계약상 불이익이나 법적 문제가 발생할 수 있다.

이 법은 연방 기관과 관련 계약업체에만 적용되지만, 민간 기업도 보안 모범 사례로 자발적으로 따를 수 있다.

기존 제도에 보안 항목을 추가

- 새로운 인증제도 신설보다 기존 인증제도 활용이 효율적
- 추가적인 제도적 복잡성 감소 및 실효성 강화
- 개선 방안:
  기존 인증제도에 IoT보안 항목 추가
  기술기준 및 사후관리로 나누어 조항 보완

지능형 홈네트워크 설비설치 기준

‘지능형 홈네트워크 설비 설치 기준’은 지능형 홈네트워크 설비의 설치 및 기술적 사항
에 관하여 위임 된 사항과 그 시행에 관하여 필요한 사항을 규정하고
'주택법' 제2조 제13호, '주택건설기준' 제32조 2에 근거하여 법적 구속력을 가진다.

제 14조의 2(홈네트워크 보안)
④ IoT기기 및 인프라에 대한 보안성 검토를 위한 체크리스트 점검을 실시해야 한다.

보안성검토를 위한 체크리스트

구분	항목	세부 내용
초기 설정 보안	안전한 인증 정보 강제	초기 설치 시 강력한 비밀번호 설정을 강제하는가?
		비밀번호 미설정 시 기기 작동을 제한하도록 설계되었는가?
	비밀번호 설정 인터페이스	직관적이고 사용자 친화적인 비밀번호 설정 인터페이스(NFCM QR코드, 버튼 등)을 제공하는가?
		비밀번호 설정 시 강도 검증 및 약한 비밀번호 경고 기능을 포함하는가?
보안 업데이트 및 유지관리	자동화된 업데이트 기능	보안 취약점 대응을 위한 자동 업데이트 기능 제공여부
		업데이트 과정에서 파일의 무결성 및 출처 인증이 보장되는가?
	업데이트 후 보안 강화	기존 설정보다 강화된 보안 옵션을 제공하는가?
		네트워크 분리 상태에서도 안전한 업데이트가 가능한가?
데이터 전송 및 기기 인증	데이터 전송 보호	TLS, DTLS 등의 암호화 프로토콜을 사용하여 데이터 전송을 보호하는가?
		데이터 암호화 키 관리가 적절히 이루어지고 있는가?
	기기 인증	IoT 기기가 상호 인증 기능을 지원하여 국가/국제 표준(ISO/IEC 등)을 준수하는가?
		기기 ID 또는 디지털 인증서를 통해 각 기기를 고유하게 식별하고 인증할 수 있는가?

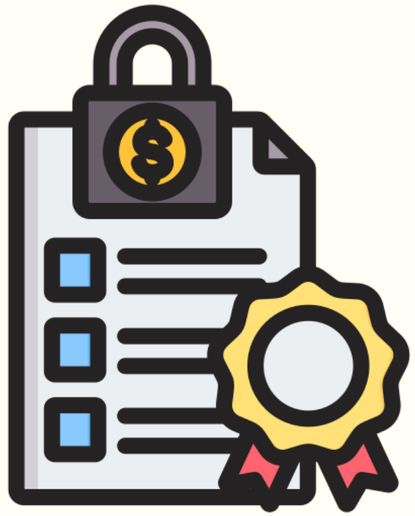
구분	항목	세부 내용
네트워크 및 장치 보안	DDoS 방어 기능	IoT 기기와 네트워크가 대량의 트래픽으로 인한 서비스 거부 공격(DDoS)을 탐지하고 방어할 수 있는가?
		DDoS 공격 방지를 위해 네트워크 트래픽 제한 및 필터링 설정이 가능한가?
		DDoS 완화 솔루션(예:클라우드 기반 DDoS 방어 서비스)을 활용하여 대규모 공격에 대비하고 있는가?
	봇넷 활동 탐지 및 차단	봇넷 활동(비인가 명령 실행, 이상 트래픽 전송 등)을 탐지하고 차단할 수 있는가?
		봇넷 활동 탐지를 위해 IDS/IPS(침입탐지/방지시스템) 또는 AI기반 분석 기술을 활용하고 있는가?
		홈게이트웨이와 단지서버가 IoT 기기의 원격 제어 명령을 감시하며 비인가 접근 시 즉각 차단할 수 있는가?
물리적 보안 및 유지관리	홈 게이트웨이 보안	홈게이트웨이가 데이터 통신의 안정성을 보장하는 보안 프로토콜을 준수하며, 안전한 파라미터가 설정되어 있는가?
		비인가 접근 시 자동으로 네트워크 차단 및 사용자에게 알림 제공이 가능한가?
법적 인증 및 보안 기준 준수	보안 인증 기준	IoT 기기가 국가가 정한 보안 인증 기준(예:IoT 보안 인증제)을 충족하는가?
		홈네트워크 IoT 기기가 보안 로그 관리 및 데이터 전송 보호 기능을 포함하는가?
	제조사의 보안 책임	제조사가 보안 기준에 부합하는 펌웨어 업데이트 기능과 보안 설정 강화 옵션을 제공하는가?

국제 표준 기구(IETF, oneM2M, OMA 등)는 TLS와 DTLS 기술을 IoT 환경에 적용할 것을 권고

DTLS 란?

UDP에서 데이터그램 기반 응용 프로그램에 사용하는 도청, 변조 또는 메시지 위조를 방지하도록 SSL/TLS와 같은 방식으로 통신할 수 있도록 보안을 제공하는 통신 프로토콜

IoT는 실시간 통신이 중요하기 때문에 UDP를 사용하는 DTLS가 적합



사후 관리

보안 결함 발생 시 리콜 및 대응 원칙

항목	세부내용
중대한 보안성 결함 시 리콜	타 디바이스 또는 네트워크 안전성을 위협하는 보안 결함 시 리콜해야 한다.
보안 취약점으로 인한 피해 대응	데이터 유출, 시스템 다운타임, 간접적 피해를 초래하는 보안 결함시 리콜해야 한다.
업데이트로 해결 가능한 경미한 결함	경미한 보안 결함은 소프트웨어 또는 펌웨어 업데이트로 해결해야 한다.
리콜 절차의 투명성	리콜 과정에서 사용자의 신체적, 재산적 피해를 최소화하기 위한 절차를 마련해야 한다.

감사합니다

참고문헌

<논문>
사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도 개선 방안
사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대응 방안
사물인터넷환경에서의 스마트홈 서비스 침해 위협 분석 및 보안 대책 연구

KISA 한국인터넷진흥원 - IoT 공통보안가이드