홈 IoT(Internet of Things) 장치에 대한 취약점 분류 체계 제시

이창민*, 이민규**, 서정택***

*가천대학교 컴퓨터공학과 (학부생)

**가천대학교 정보보호학과 (대학원생)

***가천대학교 컴퓨터공학부 (교수)

Proposal a Vulnerability Taxonomy for Home IoT Devices

Chang Min Lee*, Min Gyu Lee**, Jung Taek Seo***

*Department of Computer Engineering, Gachon University(Undergraduate student)

**Department of Information Security, Gachon University(Graduate student)

***Department of Computer Engineering, Gachon University(Professor)

요 약

홈 IoT에 대한 기술은 나날이 진화하고 있고, 홈 IoT 시장은 꾸준한 성장을 보여주고 있다. 홈 IoT의 발전으로 우리 생활의 모든 곳에 관여하고 있다. 그만큼 보안에 대한 중요성이 커지고 있지만, 정확하게 어떤 취약점이 존재하고 먼저 처리해야 하는 취약점이 어떤 것인지에 대해 알기는 쉽지 않다. 이에 본 논문에서는 부족한 홈 IoT 장치 취약점 분류에 대한 문제를 해결하기 위해, 홈 IoT 장치에 대한 취약점 분류 체계를 제시하고자 한다.

I. 서론

홈 IoT에 대한 관심이 급격하게 증가하고 있다. 일상생활과 IoT 장치들이 연결되어 편리함을 제공하고 있다. 그러나, 이 편리함은 오히려 보안 문제로 직결된다. 일상생활의 대부분이 IoT 장치와 연결되어 있어 IoT 장치에 의해 악의적으로 누군가에게 사생활이 노출되거나 다양한 공격을 받을 수 있다. 이러한 문제를 방지하기 위해, 홈 IoT 장치에 대한 보안 가이드도 존재한다. 국내에는 KISA의 'IoT 공통 보안가이드', '홈가전 IoT 보안가이드'가 있다. 다만, 현재 국내에서 제시되고 있는 보안 가이드에서는 어떤 취약점이 위험도가 높은지, 먼저 점검해야 할 취약점은 무엇인지에 대한 상세한 분류 체계가 제시되어 있지 않다.

본 논문에서는 홈 IoT 장치의 공개된 취약점들에 대해 수집한 뒤, 이를 각 분류에 맞게 재구성하여 취약점 분류 체계를 제시하려고 한다. 이를 통해, 홈 IoT 장치 도입 및 운용 시, 먼저 점검해야 하는 장치의 취약점을 쉽게 확인할 수 있고, 발생할 수 있는 위협에 대해 미리 제거할 수 있다는 효과를 가져올 수 있다.

II. 배경지식

2.1 홈 IoT

홈 IoT는 사물인터넷 기술과 홈 네트워크 기술을 결합하여, 가정 내 냉장고, 난방 장치 제어, 도어락 제어, 습도 조절 등의 각종 설비들을 하나의 네트워크로 연결되어 데이터를 주고받아 인공지능 기술을 통해 분석하고 학습한 정보를 사용자에게 제공하거나 스마트폰, 스마트워치 등을 활용하여 사용자가 제어할 수 있도록 하는 기술을 말한다[1, 2].

[그림 1]과같이 현재까지의 홈 IoT 변화가 이루지고 있다. 1세대는 홈 오토메이션으로 월패드 기반의 중앙제어를 제공하고, 2세대는 홈 네트워크로 모바일

[그림 1] 홈 IoT의 변화

기반의 원격제어가 가능해졌다. 3세대는 스마트 홈으로 AI 스피커 기반의 음성/이미지 인식이 가능해졌고, 현재 4세대의 인텔리전트 홈은 AI 기반의 자율제어 서비스를 제공하고 있다. 이러한, 빠른 변화를 통해 우리는 가정 내에서도 편리한 기능들을 제공받고 있다.

2.1 국내 홈 IoT 보안 가이드 현황

현재, 국내에서 제시하고 있는 홈 IoT 관련 보안 가이드는 대표적으로 KISA의 'IoT 공통 보안가이드', '홈가전 IoT 보안가이드'가 존재한다. 'IoT 공통 보안가이드'에서는 홈 네트워크에 대한 망분리 내용을 주로 다루고 있으며, '홈가전 IoT 보안가이드'에서 홈가전 IoT 장치에 대한 안전한 개발 가이드를 제시하고 있다.

2.1.1 KISA의 '홈가전 IoT 보안가이드'

KISA에서 제공하는 '홈가전 IoT 보안가이드'는 국내외 IoT 산업이 급격하게 성장함에 따라 IoT 장치 및 서비스에 대한 보안 위협 또한 급격하게 증가할 것으로 예상해 보안가이드를 제공한다. IoT 정보보호 로드맵을 따라, 7개의 보안원칙을 제시한 'IoT 공통 보안원칙'을 2015년 6월에 발표하였고, 이를 통해 'IoT 공통보안 가이드'가 제작되었다. 하지만, 'IoT 공통보안 가이드'는 특정 제품에 맞춘 설명을 제공하지 않기 때문에 세분된 가이드를 제공하기 위해, '홈가전 IoT 보안가이드'를 제공한다. 공통보안 요구사항을 SW 보안, 물리적 보안, 인증, 암호화, 데이터 보호, 플랫폼 보안 등 6가지 항목으로 분류하고, 보안요구사항을 설명한다.

실제 구현에 활용할 수 있도록 보안요구사항을 설명하고 있지만, 구체적으로 어떠한 취약점이 존재하고, 위험성이 높은지 등에 대한 내용이 언급되어 있지 않다.

제1절 '소프트웨어 보안'에서 2번 항목인 '알려진 보안취약점 점검 및 제거'에서 제시하는 보안 대책으로는 '홈가전 IoT 제품 및 유사 제품 유형에 관련하여 현재까지 알려진 보안취약점을 공개영역에서 조사한 후, 개발대상 제품에 해당 보안취약점이 존재하는지를 점검한 후 제거해야 함' 이라고 명시되어 있다. 본 논문에서는 2번 항목과 같이 구체적으로 명시되어 있지 않은 취약점에 대해 제품 항목별로 수집 및 분석을 통해 취약점 분류 체계를 제시한다. 알려진 보안취약점으로 특정 센서에 어떠한 형태의 취약점이 많이 발생하는지, 위험도가 높은지 등에 대한 평가를 진행하여 이후 위험도 순으로 배치해 먼저 점검해야 할 대상을 쉽게 파악할 수 있게 할 수 있다.

III. 홈 IoT 장치 취약점 분류 체계 제안

본 논문에서 제안하는 홈 IoT 장치 취약점 분류 체계는 KISA의 '홈가전 IoT 보안가이드'의 보안항목 구분에 따라 각 항목에 존재하는 CVE 취약점을 수집한 뒤, CVSS 점수를 취약점 개수로 나누어 총점을 구했다. 구해진 총계로 취약점 위험도에 대한 우선순위 구분이 가능하다. 제안한 취약점 분류 체계를 통해, 홈 IoT 장치를 설치 및 운용하는 자에게 먼저 점검하고 관리해야할 장치의 취약점을 제공할 수 있다. 또한, 취약점 분류 체계를 이용하면 기존에 존재하는 보안 가이드에 비해 취약점 항목을 상세하게 확인할 수 있으며, 취약점의 위험도를 직관적으로 확인할 수 있어 이를 통해, 위험도가 높은 장치의 추가적인 보안 취약점을 찾아볼 수 있게하는 가이드가 될 수 있다.

3.1 분류 항목 설정 기준

[표 1]에서 분류 기준은 센서 (스마트온도계 등의 센서), 제어 (전력 차단기, 조명 스위치 등 제어 제품), 중계 (홈 게이트웨이 등의 네트워크 제품), 촬영 (홈캠 등의 영상촬영 제품), 관리 (월패드, 앱/웹 등

[표 1] 홈 IoT 장치 취약점 분류 표

분류 기준	SW 보안	HW 보안	인증	암호화	데이터 보호	평균
센서	CVE-2020-3935 / 7.5	CVE-2020-9059 / 6.5	CVE-2018-11315 / 6.5 CVE-2020-9438 / 4.3	CVE-2020-3929 / 5.9 CVE-2019-9483 / 9.1	-	6.63
제어	CVE-2018-6692 / 10 CVE-2022-34753 / 8.8	-	CVE-2019-11896 / 7.1	CVE-2018-15124 / 10 CVE-2019-13598 / 10	-	9.1
중계	CVE-2023-21625 / 7.5	CVE-2021-20090 / 9.8	CVE-2017-8336 / 8.8	CVE-2023-1751 / 5.3	-	7.85
촬영	CVE-2019-2266 / 7.8 CVE-2019-10565 / 9.8	CVE-2018-3920 / 4.6	CVE-2018-20299 / 7.5	-	CVE-2019-10583 / 7.8 CVE-2019-10582 / 7.8	7.55
관리	CVE-2023-31761 / 7.5	-	CVE-2014-3394 / 5 CVE-2019-19163 / 8.8 CVE-2021-26638 / 9.8	-	-	7.77

관리기능 제공 제품)으로 분류한다. 취약점 분류 항목은 SW보안, HW 보안, 인증, 암호화, 데이터 보호, 물리적 보안으로 분류한다. 평균은 CVSS의 점수를 합한 후, 취약점 개수를 나눈 점수이다. [표 1]에서 취약점 뒤에 표시된 점수가 해당 취약점의 CVSS 점수를 의미한다.

IV.결론 및 향후연구

본 논문에서는 국내에 존재하는 홈 IoT 장치에 대한 보안 가이드의 세부적인 취약점 분류 체계 항목을 강화하기 위해 홈 IoT 장치 취약점 분류 체계를 제안한다. 이를 위해, 분류 기준으로 기존에 존재하는 KISA의 '홈가전 IoT 보안가이드'의 항목을 참조하였다.

향후연구 계획으로 분류 기준에 더 세부적인 장치들의 항목을 나눈 후, 더 많은 정보를 제공하기 위한 분류 체계를 제안할 예정이다. 취약점 수집에 대한 부분도 존재하는 취약점의 수를 늘려, 총계에 따른 위험도 선정의 신뢰성을 보완할 계획이다.

홈 IoT 장치 취약점 분류 체계를 통해, 발전하고 있는 스마트 홈 환경의 보안을 증가시키고, 홈 IoT 장치 사용자 및 설계자에게 안전하고 확실한 보안 체계를 제공하는 효과를 가져올 수 있다.

[참고문헌]

[1] KISA, "IoT 공통보안 가이드"

[2] KISA, "홈・가전 IoT 보안가이드"