사물인터넷의 보안 실태에 관한 조사

고승원*, 박재경O
*한국폴리텍대학 사이버보안과,
O한국폴리텍대학 정보보안학과
e-mail: tonytony1714@gmail.com*, jakyPark@kopo.ac.krO

A Survey on the Security Vulnerability for Internet of Things

Seung-Won Ko*, Jae-Kyung ParkO
*Dept. of Cyber Security, Korea Polytechnics University,
ODept. of Information Security, Korea Polytechnics University

● 요 약 ●

최근 아파트의 월패드 해킹 사건과 같이 사물인터넷의 보안이 매우 심각한 상황이다. 사물인터넷은 자동화된 데이터 수집, 분석, 의사결정으로 효율성과 생산성 향상하고, 실시간으로 모니터링이 가능하면서 저비용으로 개발이 가능하다. 그리고 현재 인공 지능, 빅 데이터 및 클라우드 컴퓨팅 등 다양한 기술과 융합이 가능해 더욱 발전할 전망을 가지고 있다. 그러나 활용 범위가 갈수록 방대해지지만 현재 기술력으론 완벽한 보안을 실현하기가 어려운 것이 현실이다. 그리고 해킹의 대부분 직접적인 피해 당사자인 소비자들은 스마트홈이 주는 편의에 대해서만 알 뿐 보안 위협요소에는 잘 알지 못한다. 스마트홈의 보급이 빨라지고 있지만 정부 및 제조사에서 아직 스마트홈 보안에 관련한 홍보 및 교육이 따라가지 못하기 때문이다. 이러한 점을 보완하기 위해 본 논문에선 스마트홈의 보안 실태와 보안 요구사항에 대해서 다양한 방안을 살펴보고자 한다.

키워드: 사물인터넷(IoT), 보안 요구사항(Security Requirement), 취약점(Vulnerability), 위협요소(Threat Factor)

I. Introduction

최근 아파트의 월패드 해킹 사건과 같이 사물인터넷의 보안이 매우 심각한 상황이다. 사물인터넷은 자동화된 데이터 수집, 분석, 의사결정으로 효율성과 생산성 향상하고, 실시간으로 모니터링이 가능하면서 저비용으로 개발이 가능하다. 그리고 현재 인공 지능, 빅 데이터 및 클라우드 컴퓨팅 등 다양한 기술과 융합이 가능해 더욱 발전할 전망을 가지고 있다. 하지만 현재 기술력으론 완벽한 보안을 실현하기가 어려운 것이 현실이다. 그리고 해킹의 대부분 직접적인 피해 당사자인 소비자들은 스마트홈이 주는 편의에 대해서만 알 뿐 보안 위협요소에는 잘 알지 못한다. 스마트홈의 보급이 빨라지고 있지만 정부 및 제조사에서 아직 스마트홈 보안에 관련한 홍보 및 교육이 따라가지 못하기 때문이다. 이러한 점을 보완하기 위해 본 논문에선 스마트홈의 보안 실태와 보안 요구사항에 대해서 다양한 방안을 살펴보고자 한다.

II. Preliminaries

1. Related works

1.1 국내 동향

최근 사물인터넷의 사용량이 늘고 있고, 앞으로도 늘 전망이 크다. 그림 1은 2019년도부터 2021년까지의 사용량과 2030년까지의 사용량을 예측한 그래프다.

사물인터넷 환경의 취약점 종류를 살펴보자면 사물인터넷의 기반이 되는 임베디드 리눅스가 사용되기 때문에 다양한 취약점을 갖고 있다. 그림 2와 같이 펌웨어 패치 어려움과 악성코드 유포의 숙주로 악용, DDOS 공격 및 개인정보 유출, 디바이스의 집단적 기능 불능, 사용자 과실로 인한 피해로 5개 정도가 있다.

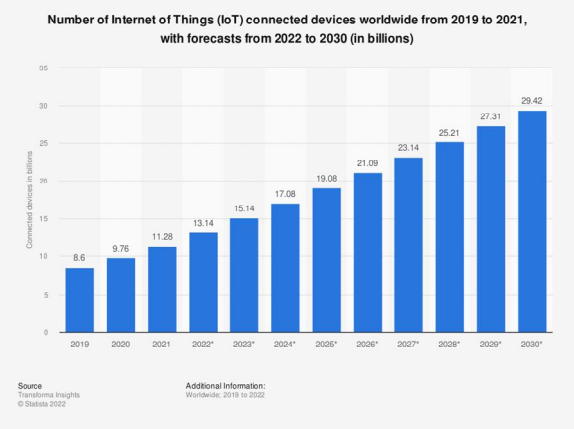

Fig. 1. Number of IoT connected devices worldwide 2019-2021, with forecasts to 2030

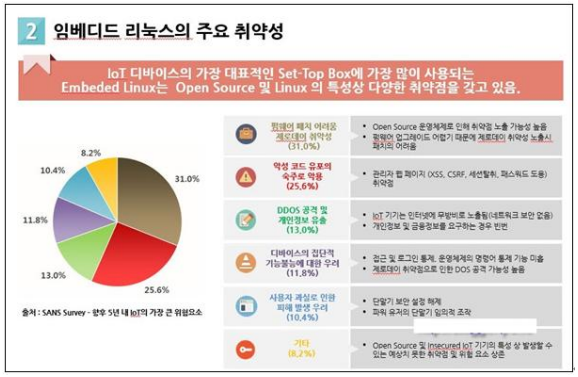

Fig. 2. Vulnerability in Embedded Linux

III. The Proposed Scheme

이를 통한 여러 공격 방법이 있는데, 표1과 같이 공격종류가 나뉘어 진다. 크게 물리 공격, 네트워크 공격, 소프트웨어 공격, 암호학 공격으로 총 4개로 나눌 수 있다.

Attack model	Features of attacks
Physical attack	Node Tampering, RF Interference, Node Jamming, Malicious Node InjectionMalicious Node Injection, PhysicalDamage,Social Engineering, SleepDeprivation Attack, Malicious Code Injection on the Node
Network attack	Traffic Analysis Attacks, Traffic Analysis Attacks, RFID Spoofing, RFID CloningRFID Unauthorized Access, Sinkhole Attack, Man In the Middle Attack, Denialof Service, Routing Information Attacks, Sybil Attack
Software attack	Virus and Worms, Spyware and Adware, Trojan Horse, Malicious Scripts, DOS
Cryptographic attack	Side Channel Attacks, Crypto analysis Attacks(Ciphertext Only Attack, KnownPlaintext Attack, Chosen Plaintext or Ciphertext Attack), Man In the MiddleAttack

사물 인터넷의 대표적인 예시인 스마트홈의 보안 요구사항을 보자면 인증, 암호화, 데이터 보호, 플랫폼 보안 등이 있는 것으로 조사되었다.

추가적으로 소프트웨어 설계 시 시큐어 코딩을 준수하며 오픈소스를 사용할 때 알려진 취약점이 있는지 주의하고 IoT 기기의 물리적 인터페이스를 제거하여 디버깅 및 데이터 유출을 예방해야 한다. 사용자들 같은 경우 보안 대책 방법이 5가지가 있다. 패스워드 설정, 암호화 설정, 접근제어 설정, 펌웨어 업데이트, IoT 보안 취약점 집중 신고 등이 있다.

그래서 위에서 살펴본 바와 같이 가장 중요한 요소는 아직 기술적인 요소들이 완벽하지 않으므로 사용자들이 보안에 대한 의식이 높아지는 것이 기본적인 조취를 취하는 최선의 방안이라고 판단한다.

IV. Conclusions

본 연구에서는 현재 IoT의 사용량을 통해 위험성을 알리고, 그에 관련한 공격 종류, 그리고 보안 대책을 통해 보안 강화를 할 것을 살펴봤다. 아직 기술의 한계로 인해 대처가 힘든 만큼 사용자들이 보안에 대한 의식이 높아지는 것으로 기본적인 조치를 취할 수 있다. 최근 월패드 하나만 공략에 성공하면 아파트 전체가 해킹당하기 쉬워지는 상태이기 때문에 사용자들의 보안 의식 강화와, 제조사와 업체가 제품 관리를 소홀하지 않도록 꾸준히 점검을 할 것을 권고한다.

REFERENCES

[1] Jung Tae Kim, "Analuses of Countermeasure of Vulnerability and Device Security on Internet of Things", Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociolgy, Vol. 7, No. 10, pp. 817-826, October 2017.

[2] Number of Internet of Things (IoT) connected devices world wide from 2019 to 2021, Statista, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[3] Home and home appliance IoT security guide, Kisa, https://www.kisa.or.kr/2060205/form?postSeq=3&page=2#fnPostAttachDownload

[4] Woo Young Yu, "An Analysis of Research Trends in IoT Security", Convergence Security Journal, Vol 18, pp. 61-67, March 2018.