IoT 디바이스 보안 메커니즘 설계

박재경*, 마명철O, 최상용*
*한국폴리텍대학교 서울강서캠퍼스 정보보안과
O숭실대학교 대학원 IT정책경영학과
e-mail: jakypark@kopo.ac.kr*, spike@kopo.ac.kr*, mcma@posod.co.krO

A Design of Secure Mechanism for IoT Devices

Jae-Kyung Park*, Myung-Chul Ma*, Sang-Young ChoiO
*Dept. of Information Security, Korea Polytechnics College
ODept. of Policy Management, Soongsil University

● 요 약 ●

본 논문에서는 IoT 디바이스를 안전하게 관리하고 인가되지 않은 접근과 같은 위협에 대응할 수 있는 보안 메커니즘을 제안한다. 이 메커니즘은 IoT 디바이스의 시스템 특징 및 네트워크 특징을 조합하여 개별적인 시그니처를 생성하고 이를 네트워크에서 지속적이고 주기적으로 검사를 수행함으로써 허가되지 않은 디바이스의 접근을 근본적으로 차단하는 방안이다. 본 논문에서는 제안한 메커니즘을 확인하기 위해 실험망을 구성하여 정상 IoT 디바이스와 비정상 IoT 디바이스를 정책적으로 구별하여 차단하여 보안 메커니즘의 우수함을 보인다.

키워드: 사물인터넷(Internet of Things), 보안 메커니즘(Security Mechanism), 시그니처(Signature), 비정상(Abnormal)

I. Introduction

최근 미래 IT 산업의 새로운 기회로 부상한 사물인터넷은 PC, 스마트폰 등 컴퓨터 단말을 넘어 모든 종류의 사물에 통신 기능을 접목해 사물들이 실시간으로 연결된 환경을 구축하는 개념으로 업계 및 학계에 매우 뜨거운 관심을 받고 있다. 또한 사물 인터넷 기술을 도입하는 기업이 증가하면서 환경 변화 및 관련 서비스도 급속히 증가하고 있다.

하지만, 사물인터넷은 모든 사물이 해킹의 대상이 되며 따라서 사이버보안에 대한 다양한 우려도 함께 증가하고 있는 실정이다. 현재 사물인터넷에 대한 근본적인 대안이 마련되지 못했고 보안에 대한 인식 자체도 매우 낮은 심각한 상황이다. 본 논문에서는 사물인터넷 디바이스에 적용가능한 보안 메커니즘을 제안하고자 한다.

II. Preliminaries

1. Related works

1.1 국내 동향

IoT에 대한 동향으로는 첫 번째 SoC(system On Chip)나 시큐어 OS를 탑재하여 IoT보안을 마련하는 연구 및 개발이 진행되고 있다. 하지만, 이는 기존에 개발되어 운영중인 디바이스에 적용하기에는 한계가 있다.

두번째로 참조제어 및 인증에 대한 방안이 있고 NAC(Netword Access Control)와 같은 제품을 통해 보안을 제공하고 있다. 하지만, 이는 IP나 MAC을 변경했을 경우 근본적으로 해결할 수 없는 단점을 가지고 있다. 또한 보안장비 즉 방화벽, IPS와 같은 장비와 연동하는 방안도 대안으로 제시하고 있으나 이는 별도의 장치나 S/W를 설치해야하며 스푸핑에 대한 근본적인 방안은 아닌 실정이다.

III. The Proposed Scheme

본 논문에서는 시도응답 방식을 사용하는 새로운 보안 메커니즘을 제안한다. 제안하는 메커니즘은 그림 1과 같이 설치된 후 서비스되기 이전 시점에 최초 IoT디바이스의 특성을 추출하기 위한 사전등록 절차를 거친다. 사전등록 절차를 거쳐 디바이스의 특징이 등록된 후에는 실시간 검사 모듈이 정기적으로 등록된 디바이스에 질의를 하고, 결과값을 등록된 값과 비교하여 정상디바이스 여부를 확인한다. 이 때 디바이스 확인을 위한 시그니처는 디바이스가 연결된 네트워크 정보, 디바이스의 시스템정보, 디바이스의 서비스 정보 등 공격자가 임의로 조작하기 힘든 정보를 사용하여 스푸핑과 같은 공격자의 위협에 안전한 강도를 제공한다.

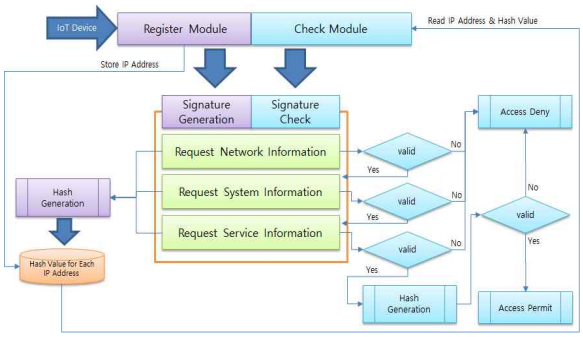

Fig. 1. Secure Mechanism

실험을 위한 환경은 그림2와 같다. 실험을 위한 대상으로 대표적인 IoT디바이스인 CCTV를 사용하였으며, 공격자는 CCTV와 같은 IP주소와 MAC주소를 사용하여 접근하였을 때, 비정상 디바이스로 인식하는지 여부를 점검하였다. 실험결과에서 "정상"이라고 표시된 부분은 "예상결과"대로 제안하는 메커니즘이 잘 동작하였음을 나타낸다.

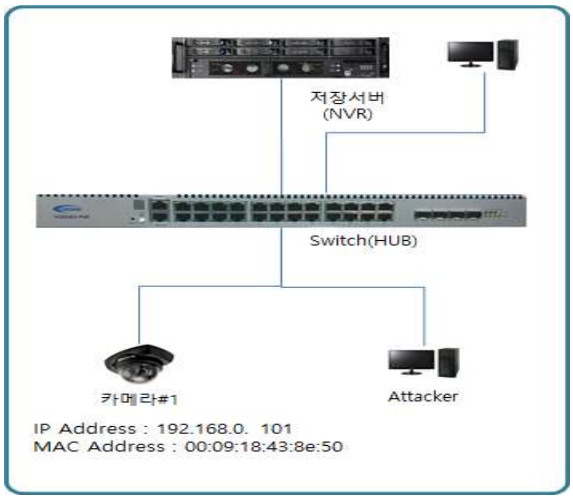

Fig. 2. Test Configuration

본 실험을 통해 두 개의 IoT 디바이스의 등록 및 검사의 결과는 다음의 표1 의 결과와 같다. 실험을 통해 제안하는 메커니즘이 비정상 디바이스를 잘 식별하는 것이 확인되었다.

Table. 1. Result Table

실험내용	예상결과	실험결과
등록모듈 검사	/reg디렉토리에 등록한 단말기의 IP Address와 시그니쳐 저장됨	정상
IP Address도용 단말기 차단	도용한 IP Address를 사용하여 연결하였을 때, 검사모듈 실행 후 도용한 IP Address가 차단규칙에 입력	정상
MAC Address 도용 단말기 차단	도용한 MAC Address를 사용하여 연결하였을 때, 검사모듈 실행 후 도용한 IP Address가 차단규칙에 입력	정상

IV. Conclusions

본 논문에서는 IoT 디바이스를 식별하고 검증할 수 있는 메커니즘을 제안하였다. 제안한 방법은 운영중인 IoT단말기의 변경 없이 쉽게 적용할 수 있어 IoT 환경에서 보다 안전한 IoT 서비스를 할 수 있을 것으로 기대한다. 또한, 등록을 위한 시그니쳐를 보다 정교하게 설정할 경우 해킹에 대한 보다 완전한 대응일 가능할 것으로 기대한다. 향후 다양한 IoT디바이스에 제안한 방법을 적용하기 위한 연구와 IoT 디바이스를 통제하는 운영장비 및 사용자 환경까지 확대할 수 있는 방안을 지속적으로 연구할 계획이다.

References

[1] AUTO-ID LABS. http://www.autoidlabs.org/. online, last visited 30. June 2011.

[2] E. Kim, D. Kaspar, N. Chevrollier, and JP. Vasseur. Design and Application Spaces for 6LoWPANs draft-ietf-6lowpan-usecases-09. Design and Application Spaces for 6LoWPANs draft-ietf-6lowpan-usecases-09, January 2011.

[3] BACnet. http://www.bacnet.org/. online, last visited 30. June 2011.

[4] DALI. http://www.dalibydesign.us/dali.html. online, last visited 25 Feb. 2011.

[5] ZigBee. http://www.zigbee.org/. online, last visited 30. June 2011. Security Challenges in the IP-based Internet of Things† 15