사물인터넷 보호를 위한 방화벽 구현

이정희*, 김지원*, 신원*
*동명대학교 정보보호학과
e-mail:shinweon@tu.ac.kr

A Firewall System for IoT Environments

Jeong-Hui Lee*, Ji-Won Kim*, Weon Shin*
*Dept. of Information Security, Tongmyoung University

요 약

최근 다양한 사물인터넷 기기들이 출시되어 일상생활은 물론 다양한 환경에서도 널리 활용되고 있다. 이로 인해 기존의 사이버 위협들이 사물인터넷 환경에서도 고스란히 적용되어 심각한 위협으로 나타나고 있으나, 사물인터넷 기기를 대상으로 하는 침입차단과 대응은 부족한 실정이다. 본 논문에서는 사물인터넷 기기로 들어오는 패킷을 분석하여 사물인터넷 기기에 해당하는 이미 등록된 기능과 다른 이상행위를 하는 통신을 차단할 수 있는 방화벽 시스템을 개발한다. 이를 위하여 사물인터넷 환경을 구축하고, 오픈소스 공유기 환경에서 방화벽 시스템을 구현하였다.

1. 서론

최근 사물인터넷 기기들이 다양하게 개발되어 인터넷 및 네트워크에 연결됨에 따라 사이버 침해, 중요 정보 및 개인 정보 유출과 같은 기존 사이버 위협이 사물인터넷 환경에서도 심각한 위협으로 대두되고 있는 실정이다. 한편, 기존 네트워크 환경과 컴퓨터 시스템을 사이버 위협으로부터 보호하기 위한 안티바이러스(Anti-Virus), 방화벽(Firewall), 침입탐지시스템(Intrusion Detection System) 등 다양한 보안 시스템이 널리 적용되고 있다. 즉, 네트워크상의 통신 패킷 분석을 통해 사이버 공격을 탐지하고 보안 이벤트를 발생시키는 시스템으로 많은 기관에서 방화벽 또는 침입탐지시스템을 사용하고 있다. 그러나 이를 다양한 사물인터넷 환경과 스마트 기기에 직접 적용하기에는 다소 무리가 있다.

본 논문에서는 네트워크 보안의 가장 기본적인 침입차단의 개념을 사물인터넷 환경에 적용한 방화벽을 구현한다. 즉, 사물인터넷 환경에 방화벽을 접목시켜 사물인터넷 기기로 들어오는 통신을 분석하고 이상탐지의 경우 차단할 수 있는 시스템을 개발한다. 이를 위하여 본 논문에서는 사물인터넷 기기를 위한 어플리케이션 방화벽을 구현하고 세부 내용을 분석한 후 결론과 향후 연구방향에 대해 기술한다.

2. 사물인터넷 방화벽 구현

사물인터넷 기기용 방화벽 개발을 위하여 먼저 최소한의 사물인터넷 환경을 구성한다. 구축할 환경은 스마트 홈의 스마트 전구를 구축한다고 가정한다. 스마트 홈은 여러 사물인터넷 기기들을 공유기에 연결하여 외부 또는 내부에서 사물인터넷 기기를 제어할 수 있게 하여 사용자에게 편의성을 제공하는 개인 주택이라 할 수 있다. 스마트 전구, 부저, LCD 디스플레이는 스마트 홈 환경에서 외부 또는 내부의 On/Off 신호에 따라 각 기기를 켜고 끌 수 있는 시스템이다. 여기서 사물인터넷 기기는 공유기를 통하여 통신하는데, 본 논문에서 사용하는 공유기는 Raspberry Pi에 LEDE(Linux Embedded Development Environment)[1]라는 오픈소스 공유기 운영체제를 설치하여 기존 공유기의 동작을 대체할 수 있도록 구성한다. LEDE는 Linux 기반의 임베디드 운영체제로 opkg[2]라는 패키지 매니저를 이용하여 공유기와 방화벽 구축에 필요한 각종 패키지들을 편리하게 이용할 수 있다. Fig. 1은 제안하는 사물인터넷 방화벽 시스템의 개략적인 동작 방식을 보여준다.

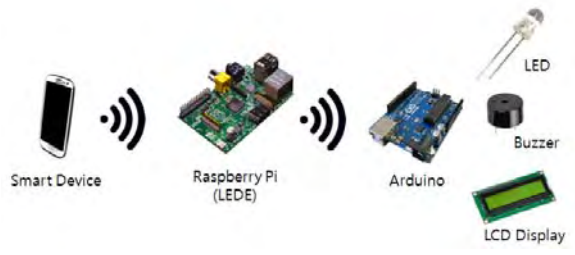

Fig. 1 Overview of the proposed IoT firewall

제어 대상이 되는 LED 스마트 전구와 부저, LCD 디스플레이는 Arduino와 직접 연결하여 구성한 뒤 Arduino Wi-Fi Shield를 이용하여 공유기(LEDE)와 통신할 수 있도록 설정한다. 여기서, Arduino가 Wi-Fi로 통신을 수행

할 수 있도록 Wi-Fi Shield를 사용해야 하는데 JSN270 Arduino Shield를 사용한다. 이를 통하여 Arduino를 공유기와 연결하여 외부 또는 내부에서 LED On/Off 신호에 LED가 동작을 할 수 있도록 구성한다. Fig. 2는 Raspberry Pi에 오프소스 공유기인 LEDE를 설치하여 운용하는 화면이다.

Fig. 2 LEDE screenshot

제안하는 방화벽은 공유기 내부에서 동작하는 Python 프로그램으로 만든다. LEDE에서 Python의 설치는 opkg를 이용하여 설치할 수 있고, python-netfilter 라이브러리를 이용해 Netfilter Table을 직접 제어할 수 있다. Netfilter[3]는 Linux 커널 내부의 네트워크 관련 모듈로, 다양한 네트워크 관련 연산을 핸들러 형태로 구현할 수 있도록 여러 가지 훅(Hook)을 제공한다. Fig. 3은 LEDE에서 python-netfilter를 이용하여 패킷을 후킹하는 소스 예이다.

```
from netfilter.rule import Rule,Match
from netfilter.table import Table

rule = Rule(
    in_interface='eth0',
    protocol='tcp',
    matches=[Match('tcp', '--dport 80')],
    jump='ACCEPT')

table = Table('filter')
table.append_rule('INPUT', rule)
```

Fig. 3 A hooking example by python-netfilter

Fig. 4는 제안 시스템의 세부 동작을 다이어그램으로 보여준다. 각 단계별 세부 동작을 살펴보면 python-netfilter 라이브러리를 이용하여 3계층 IP주소와 4계층 포트번호를 추출하여 각각 필터링을 수행하고 7계층에서 Python 프로그래밍을 통하여 정당한 명령인지를 확인한다. 모든 동작은 공유기에서 수행되며 공유기로 요청되는 패킷의 헤더와 페이로드를 분석하여 해당 페이로드가 정상적인 On/Off 기기 동작 페이로드인지 검증한다. 이를 위하여 사전에 DB를 구축하여 IP 주소, Port 번호, 페이로드에서 기기 및 사용자 인증 정보, MAC 주소와 정상적인 기기 동작 정보를 저장해둔다. 그리하여 DB에서 데이터를 조회하여 외부에서 온 요청과 비교하여 정상적인 동작과 일치하는 요청만을 서비스해주고 나머지 요청들은 전부 차단할 수 있게 한다.

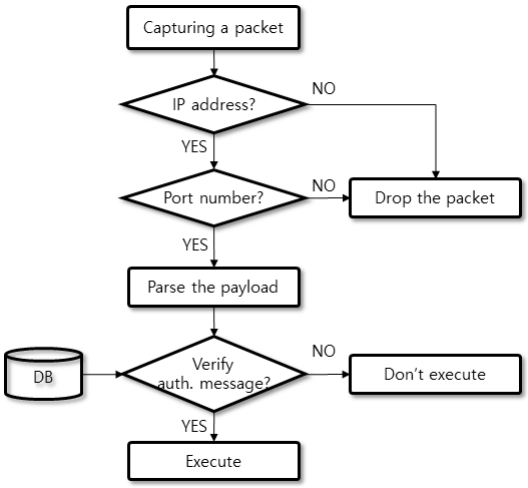

Fig. 4 Algorithm of the proposed system

Fig. 5는 이러한 과정에 따라 침입 여부를 판단하는 의사결정 트리를 보여준다.

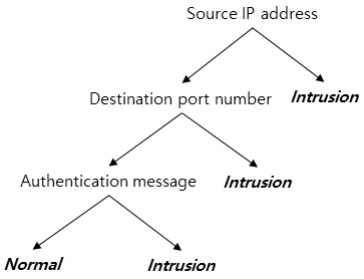

Fig. 5 Intrusion decision tree

여기서 사용하는 인증 메시지 Authentication Message는 다음과 같은 형태로 구성되어 있다. 이미 등록된 기기 ID와 사용자 ID, 사용자 패스워드 및 사용자 기기 MAC 주소의 해쉬값을 인증 정보로 사용한다. Fig. 6은 이러한 과정에 따라 침입 여부를 판단하는 인증 메시지에 대한 의사결정 트리를 보여준다.

$$Authentication\ Message = Device\ ID | User\ ID | Hash(PW | MAC\ address)$$

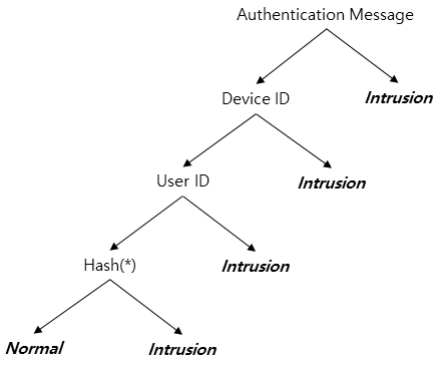

Fig. 6 Decision tree for authentication message

위와 같이 인증 메시지는 인증을 위하여 사용자 패스워드와 MAC 주소에 대한 해쉬값을 사용하는데, 암호기술 중 해쉬 알고리즘은 비밀정보의 일방향성을 보장하고 있으며 사물인터넷 환경에서 가장 단순하면서도 효율적인 방식으로 안전한 동작을 보장할 수 있다.

3. 결론

일반적으로 방화벽 또는 침입탐지시스템에서 침입을 탐지하는 방법으로는 2가지가 있다[4]. 첫째는 사용자가 등록한 문자열이 패킷 상에서 발견되었을 때, 보안 이벤트를 발생시켜 사용자에게 알려주는 오용탐지 방식이다. 둘째는 정상적인 통신 방식과 다른 형태의 통신이 나타났을 때, 보안이벤트를 발생시켜 사용자에게 알려주는 이상탐지 방식이 있다. 본 논문에서는 사물인터넷 기기 보호를 위한 방화벽 개발을 위해 Raspberry Pi와 Arduino로 사물인터넷 환경을 구축하였다. Raspberry Pi에 LEDE를 설치하여 공유기 환경을 구성하여 Arduino에 연결된 각종 기기를 On/Off 할 수 있도록 구현하였다. 여기에 Netfilter에 기반한 방화벽을 개발하여 정상적인 동작만을 전달시켜 주고, 나머지 동작들을 차단하도록 구현하였다.

본 연구 결과는 향후 반드시 등장할 사물인터넷 침입차단/탐지 시스템의 요구사항, 구현 방식과 동작 등의 분야에 기반 기술로 적용할 수 있을 것으로 예상된다. 향후 제안 시스템에서 구현된 이상탐지를 보다 확장하고, 다양한 사물인터넷 기기의 특성과 동작을 반영하여 오용탐지도 수행할 수 있는 침입탐지 시스템 구현을 위하여 지속적으로 연구 개발을 수행할 예정이다.

Acknowledgement

"본 논문은 부산광역시 재원으로 부산SW인재사관학교의 지원을 받아 연구되었음."

참고문헌

[1] OpenWrt Project: Welcome to the OpenWrt Project, http://openwrt.org/

[2] OpenWrt Project: Opkg Package Manager, http://openwrt.org/docs/guide-user/additional-software/opkg

[3] netfilter/iptables project homepage - The netfilter.org project, http://www.netfilter.org/

[4] Karthikeyan .K.R and A. Indra, “Intrusion Detection Tools and Techniques - A Survey ”, International Journal of Computer Theory and Engineering, Vol.2, No.6, pp.901-906, 2010