논문 21-46-08-14 The Journal of Korean Institute of Communications and Information Sciences '21-08 Vol.46 No.08
https://doi.org/10.7840/kics.2021.46.8.1321

IoT 네트워크에서 보안위협 확산 방지를 위한 스마트 세그멘테이션 프레임워크 구현

임 재 덕◆, 손 선 경*, 김 정 녀°

Implementation of Smart Segmentation Framework for Preventing Security Threats Spreading in IoT Networks

Jae-Deok Lim◆, Seon-Gyoung Sohn*, Jeong-Nyeo Kim°

요 약

이동통신과 사물인터넷 발전에 따라 네트워크 연결 디바이스 증가 및 사물인터넷 서비스 대중화로 디바이스 취약점을 악용하는 보안사고가 급증하고 있다. 특히 제한된 자원 특성으로 보안이 취약한 디바이스들이 해커들의 공격 대상이 되고 있으며, 대표적인 것이 대규모 분산 서비스 거부(DDoS) 공격을 유발하는 Mirai 악성코드의 감염 확산이다. DDoS 공격 대응 방법 중 하나는 DDoS 공격 원인인 악성코드 확산 억제를 통한 대규모 사물봇넷 생성을 방지하는 것이다. 본 논문은 IoT 네트워크 내의 보안위협 확산을 억제하기 위해 디바이스 속성, 네트워크 정보, 서비스 유형 등을 기준으로 세그멘트를 정의하고, 보안위협 확산 여부에 따라 세그멘트 단위로 네트워크 접속을 자율적으로 통제하는 스마트 세그멘테이션 프레임워크에 대한 구현을 설명한다. 제안된 스마트 세그멘테이션 프레임워크는 Mirai 악성코드 감염 환경에서의 시험을 통해 악성코드 확산을 억제할 수 있음을 검증하였다.

Key Words : IoT security, segmentation, DDoS, botnet restraint, autonomous security enforcement

ABSTRACT

The advance of mobile communications and IoT networks has led to the proliferation of connected devices and the popularization of IoT services, however, security incidents exploiting vulnerabilities of IoT devices also continue to be increasing. The representative is malware infection such as Mirai creating massive IoT botnets and causing DDoS attacks. One way to weaken the intensity of DDoS attacks is to render the expansion of massive IoT botnets difficult by curbing the malware spreading. This paper describes the implementation of a smart segmentation framework that autonomously enforces security policy to segments for preventing the spread of threats within IoT networks. Segments are defined as security policy enforcing units and configured with the basis of IoT device attributes, network connection information, and IoT service types. We verified the framework can mitigate threat spreading by testing its functionality in an environment where Mirai malwares are spreading.

※ 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2018-0-00231, (IoT 2세부) IoT 인프라 공격 확산 방어를 위한 상황 적응형 보안 자율제어 기술개발)
◆ First Author : Information Security Research Devision, ETRI, jdscol92@etri.re.kr, 정회원
° Corresponding Author : Information Security Research Devision, ETRI, jnkim@etri.re.kr, 종신회원
* Information Security Research Devision, ETRI, sgsohn@etri.re.kr, 정회원
논문번호 : 202103-062-D-RN, Received March 15, 2021; Revised May 27, 2021; Accepted May 27, 2021

Ⅰ. 서 론

5G와 같은 이동통신 및 MQTT, CoAP 등 IoT 네트워크의 발전으로 다양한 디바이스의 네트워크 연결이 대중화되고 있으며, 이에 따라 네트워크에 연결된 디바이스 규모도 급격히 증가하고 있다. 하지만 네트워크에 연결된 디바이스가 증가할수록 네트워크 복잡도와 관리의 어려움은 증가하며 이는 사이버 공격 접점이 늘어나는 요인이 된다. 또한 원격 관리 및 제어 등을 위해 네트워크에 연결된 센서 및 액츄에이터 등과 같은 보안이 취약한 저사양 하드웨어 기반의 IoT 디바이스는 악의적인 공격자에 의한 사이버 공격 대상이 되고 있어 다양한 보안사고의 원인이 되고 있다[1].

특히, Twitter, Netflix, Paypal 등 수많은 인터넷 서비스 이용에 심각한 장애와 피해를 입힌 Dyn DNS 서비스 제공자에 대한 분산서비스거부 공격(DDoS)이 대표적인 IoT 네트워크에 대한 보안사고이다. 해당 사고는 보안이 취약한 디바이스에 침투한 Mirai 악성코드의 확산으로 생성된 대규모 사물봇넷을 통해 발생한 사고였으며 Mirai 악성코드는 지금도 변종이 꾸준히 발견되고 있다[2]. 이는 Mirai 악성코드가 다른 사물봇 악성코드에 비해 상대적으로 많은 기능을 가지고 있으며 소스 코드가 공개되어 있어 다른 모든 사물봇 악성코드의 제작에 직접적으로 영향을 주기 때문이다. 또한 최근의 IoT 악성코드 분석 및 분류 연구[3]를 보면 PC나 스마트 기기 등을 대상으로 한 악성코드가 IoT 디바이스를 목표로 한 악성코드에 포함되거나, 서로 다른 플랫폼에 감염될 수 있도록 악성코드들 간에 기능이 공유되거나, 감염된 IoT 디바이스에서 엔트포인트 디바이스를 공격 목표로 하는 기능도 발견되고 있어 IoT 네트워크 내부에서의 위협 확산 방지에 대한 대비가 필요함을 암시하고 있다.

대규모 디바이스의 연결로 IoT 네트워크 구조가 복잡해 짐에 따라 통신 트래픽 역시 기존의 계층적 구조에서의 상하 트래픽 이동(north-south movement)과 더불어 좌우 트래픽 이동(east-west movement)도 증가하고 있어 스위치, 라우터 등으로 구분된 전통적인 경계망이 허물어지고 있는 추세이고, 이에 따라 기존 네트워크 경계 보안 기술로 네트워크 내부에 침입한 보안위협에 대응하는 것에 한계가 발생한다[4-6]. 방화벽, IDS, IPS 등과 같은 전통적인 네트워크 경계 보안 기술은 주로 도메인 경계 지점에 위치하여 외부 네트워크에서 내부 네트워크로 침입하는 악성코드, 악의적 공격 행위 등의 위협에 대한 탐지 및 방어를 주된 목적으로 하고 있어 도메인 내부에 침투한 악성코드의 확산에 대해 효율적으로 대응하기가 어렵다[7]. 특히 디바이스 간 통신이 빈번하게 발생하는 IoT 환경에서는 내부 네트워크 영역 간 보호에 대한 요구가 증가하고 있다. 네트워크 내부 영역 보안을 위해 네트워크 일부 영역만 접속할 수 있게 하여 데이터의 접근을 제한하는 방법으로 서브넷, VLAN(Virtual LAN), 내부 방화벽 등과 같은 네트워크 세그멘테이션 기술이 적용되고 있지만, 정적인 특성으로 인해 경계망 내부에서 이동하는 트래픽에 대한 선택적 격리가 불가능하여 IoT 서비스에서처럼 디바이스가 동적으로 연결되는 환경에는 적합하지 않다[5].

디바이스에 침투한 보안위협 혹은 악성코드는 침투한 디바이스와 동일하거나 유사한 속성을 가진 다른 디바이스가 침투했을 때 이용한 보안취약점을 그대로 가지고 있을 확률이 높아 해당 디바이스를 대상으로 확산할 가능성이 매우 높다. 따라서 보안위협이 탐지되었고 해당 보안위협이 확산되고 있음이 확인되면 해당 보안위협이 발생한 디바이스와 동일한 혹은 유사한 속성을 가진 디바이스 그룹에 대해 사전에 네트워크 접근 통제를 집행하면 보안위협 확산을 완화할 수 있다. 특히, 이와 같은 디바이스 그룹에 대한 사전 네트워크 접근 통제 방법은 주변 디바이스에 악성코드를 감염시키면서 IoT 봇넷의 규모를 확장하는 Mirai 악성코드 같은 DDoS 공격을 유발하는 악성코드의 확산을 억제하는데 효과적이며 결국에는 DDoS 공격을 완화시키거나 규모를 축소할 수 있다.

본 연구는 IoT 네트워크에서 Mirai 악성코드와 같은 IoT 사물봇 악성코드의 행위를 탐지하고 탐지된 악성코드 정보를 기반으로 동일한 속성을 기준으로 구성된 세그멘트 단위로 네트워크 접속을 자율적으로 통제하여 네트워크 내에서의 악성코드 확산을 억제하는 스마트 세그멘테이션 프레임워크에 대한 구현을 설명한다. 세그멘트는 디바이스의 다양한 속성, 네트워크 연결 정보, 서비스 유형 등의 공통된 속성을 기준으로 디바이스가 등록될 시점에 자동으로 구성되는 단위이고, 보안위협 확산이 확인될 경우 보안위협이 확산될 세그멘트를 결정하여 사전에 보안통제정책을 적용함으로써, 보안위협이 통제된 세그멘트를 넘어 확산됨을 방지한다. 제안된 스마트 세그멘테이션 프레임워크은 Mirai 악성코드가 확산되는 환경[8]을 이용한 기능 시험을 통해 악성코드의 확산이 완화됨을 검증하였다.

Ⅱ. 관련 연구

IoT 디바이스의 증가로 복잡해진 IoT 네트워크의 보안을 위해 네트워크 관점이 아닌 디바이스 그룹으로 구성된 세그멘트 기반 개념을 이용한 보안 기술에 대한 연구가 진행되고 있다.

스마트홈에 적용된 마이크로 세그멘테이션 기술에 대한 연구[5]는 기존 네트워크 세그멘테이션의 정적인 단점을 극복하면서 네트워크 내부 영역에 대한 세부적인 접근 제한을 통해 공격 접점을 줄이는 방법으로 스마트홈 네트워크의 보안을 제공한다. 해당 연구에서는 네트워크 상에 연결된 스마트홈 디바이스를 식별하여 디바이스 기능과 보안성을 기준으로 디바이스 그룹으로 분류하고, 분류된 디바이스 그룹에 대해 그룹 간 접근에 대한 보안정책을 적용하여 격리함으로써 네트워크 내부 침입이 발생한 경우에 위협 범위를 그룹 내부로 제한하도록 한다.

구체적인 기술이나 구조를 제안하기보다는 세그멘트 개념을 이용하여 복잡하고 규모가 큰 IoT 네트워크 보안을 위한 추상적인 수준에서의 해결 방안을 제시한 연구도 있다[9]. 해당 연구에서는 IoT 네트워크에 대해 구현 독립적으로 보안위협을 방어할 수 있고 도메인 내의 보안 규정을 준수할 수 있는 개념적인 의미론적 제약을 기술하는 추상화 보안 패턴(Abstract Security Pattern)을 이용하여 IoT 네트워크를 보호하는 세그멘테이션 방법을 제안하였다. 복잡하고 규모가 큰 IoT 네트워크 보안을 위해 네트워크 환경 및 문제를 정의하고 문제에 대한 해결책을 추상적인 수준에서 일반화하여 제시한다. IoT 네트워크의 주요 문제는 서로 다른 제품 및 타입 등 수많은 이기종 IoT 디바이스들 특히 보안이 취약한 디바이스들이 다수 포함된 상황에서 중요한 디바이스들과 시스템들을 사이버 공격으로부터 어떻게 보호할 것인가로 정의한다. 이에 대한 해결책으로 관리자가 제대로 파악하고 있는 디바이스들을 작은 단위로 구분하여 세분화된 세그멘트 구조로 구성하여 관리하도록 하고, 이때 세그멘테이션은 조직 운영 목적과 구성 엔터티 간의 논리적 관계에 기반하여 전체 네트워크에 걸쳐 일관되게 적용되어야 함을 강조하고 있다.

Ⅲ. 스마트 세그멘테이션 프레임워크 구현

3.1 스마트 세그멘테이션 프레임워크 구조

스마트 세그멘테이션 프레임워크는 크게 스마트 세그멘테이션 매니저(이하 매니저, manager), 스마트 세그멘테이션 에이전트(이하 에이전트, agent), 스마트 세그멘테이션 관리 인터페이스(이하 관리 인터페이스, management interface)와 같이 세 가지 역할로 구분되어 그림 1과 같이 구성된다. 그림 1은 사물봇 확산을 방지를 위해 설계된 이전 연구의 스마트 세그멘테이션 프레임워크의 기본 구조[10]를 기반으로 확장된 구조이며, 추가된 기능과 보다 자세한 구현 방식을 제시한다.

매니저는 IoT 구성 중 관리서버 영역에서 동작하며 전체적인 스마트 세그멘테이션 운영에 필요한 다양한 설정 정보(디바이스, 세그멘트, 보안통제정책 정보 등)를 관리하고 스마트 세그멘테이션 운영에 필요한 기능을 제공하며 주요 기능은 다음과 같다.

- 세그멘트 관리(Segment management): 디바이스 및 IoT GW 관리, 디바이스 속성 기반 세그멘트 구성 관리, 세그멘트 보안 위험도 계산
- 도메인 네임 관리(Domain Name management): IoT 서비스 내에서 정상적으로 운영되는 시스템에 대한 도메인 네임(화이트리스트) 관리 및 에이전트 배포
- 위협정보 수신 및 분석(Receive & Analyze threat info.): 에이전트에서 제공하는 위협정보 수신, 분석주기 마다 수신된 위협정보 통계 생성, 분석주기 내 발생한 보안위협 분석(확산여부, 세그멘트별 보안위협 발생비율, 세그멘트별 보안위험도 등)
- 보안통제정책 생성(Policy construction): 분석된 보

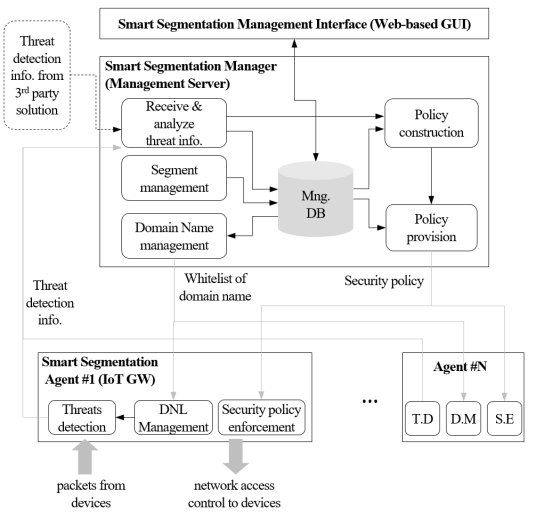

그림 1. 스마트 세그멘테이션 프레임워크 구조
Fig. 1. Smart segmentation framework architecture

안위협에 대해 통제할 세그멘트 결정 및 보안통제 정책 생성
- 보안통제정책 분배(Policy provision): 통제할 세그멘트 내 디바이스가 연결된 에이전트 결정, 보안통제정책 분배
- 세그멘테이션 관리 DB(Management DB): 세그멘테이션 관련 설정 및 상태 정보 관리

그림 1에서 점선박스로 표기된 외부 보안탐지 솔루션과의 상호작용은 본 구현에서 제공되는 보안위협 탐지 성능과 정보를 개선하기 위해 인터페이스 확장을 고려한 것으로 현재 추가로 연구개발 중인 부분이다.

관리 인터페이스는 매니저와 동일한 시스템이나 별도의 웹서버에서 동작하는 웹 기반 관리 인터페이스로 세그멘테이션 관리 및 운영에 대한 정보가 관리되는 데이터베이스를 통해 매니저와 상호작용하며, 다음과 같은 사용자 편의 관점에서 시각화 인터페이스를 제공한다.

- 디바이스 및 IoT GW 관리
- 세그멘트 구성 관리
- 도메인 네임 화이트리스트 관리
- 세그멘테이션 모니터링(보안위협 발생 및 통제 상태)

에이전트는 IoT 구성 중 엔드 디바이스가 네트워크에 연결되는 지점인 IoT GW에서 주로 동작하므로, 다수의 에이전트가 존재한다. 필요에 따라 GW가 아니더라도 엔드 디바이스의 네트워크 연결 통제가 필요한 지점에서 동작할 수 있으며, 다음과 같은 기능을 제공한다.

- 도메인 네임 목록 관리(DNL Mng.): 사물봇 악성코드 탐지의 기준이 되는 정상 시스템에 대한 도메인 네임(화이트리스트) 수신 및 로컬 관리
- 보안위협 탐지(Threats Detection): 사물봇 악성코드 DNS 쿼리 탐지 및 매니저로 탐지정보 전송
- 보안통제정책 집행(Security policy enforcement): 수신된 보안통제정책에 따른 세그멘트 기반 네트워크 연결 통제 수행

IoT 네트워크 환경에서 스마트 세그멘테이션의 동작 절차는 그림 2와 같이 초기 단계, 보안위협 탐지 단계, 보안위협 분석 단계, 보안통제정책 생성 단계, 보안통제정책 집행 단계로 진행되며, 다음 절에서 각

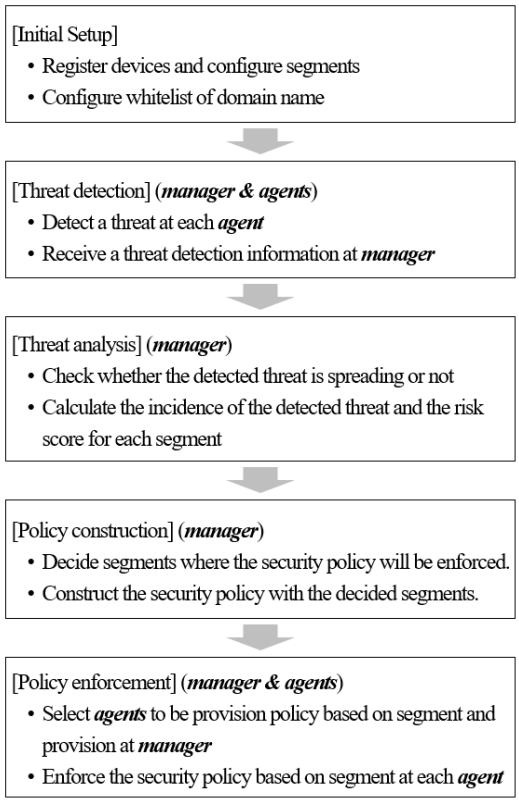

그림 2. 스마트 세그멘테이션 동작 절차
Fig. 2. Operational procedure of smart segmentation

단계별 세부 내용을 설명한다.

3.2 디바이스 등록 및 세그멘트 구성

스마트 세그멘테이션 운영을 위한 초기 설정 단계로 IoT 네트워크에 연결된 디바이스 등록 및 세그멘트 구성과 사물봇 악성코드 탐지에 기준이 되는 도메인 네임에 대한 화이트리스트 구성으로 진행된다. 디바이스 등록은 IoT 네트워크에 연결되는 디바이스에 대해 각종 속성 정보를 기술한 json 형식의 파일을 로딩함으로써 진행되며, 임의의 디바이스 속성을 기술한 json 파일 예시는 그림 3과 같다.

'*dev_value*' 속성은 조직에서 해당 디바이스가 얼마나 중요한지 즉, 얼마나 보호할 가치가 있는지에 대한 척도로 조직에 따라 임의로 지정하는 값이다. 속성 정보 설정에 명시되지 않았지만, 디바이스가 내재하고 있는 보안취약성 정보도 등록되며, 그림 4와 같은 절차로 국제 취약점 데이터베이스(NVD, National Vulnerability Database)에서 제공하는 공통 취약점 등급 시스템(CVSS, Common Vulnerability Scoring System) 점수를 획득하여 활용한다. NIST NVD에서

```
"devices":[
    {
        "device_id": "iG_SSS_GW01_D001",
        "device_name": "iG_SSS_GW01_D001",
        "device_type": "도어개폐기",
        "vendor": "akerun",
        "product": "smart_lock_robot",
        "os_ver": "linux_desktop",
        "ipv4_addr": "192.168.1.101",
        "mac_addr": "",
        "dev_se": "0",
        "gw_id": "iG_SSS_GW01",
        "gw_name": "iG_SSS_GW01",
        "service_id": "출입통제서비스",
        "dev_value": "2",
        "location": "안전관리팀"
    },
```


그림 3. 디바이스 등록에 사용되는 속성 정보 예시
Fig. 3. An example of device attributes used to be registered

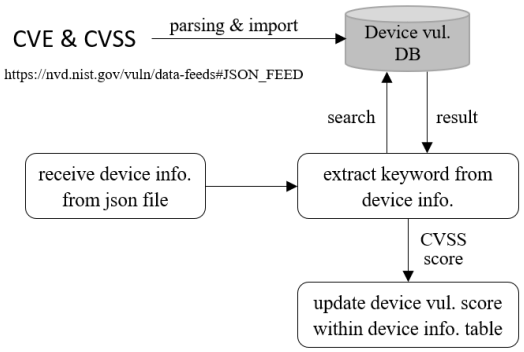

그림 4. 디바이스가 내재하고 있는 보안취약점 측정
Fig. 4. Device vulnerability measurement

제공하는 취약점 데이터 파일을 통해 CVE ID, 제품 유형(OS, 어플리케이션, 하드웨어), 벤더, 제품명, 버전, 공격벡터, 기밀성/무결성/가용성 영향력, 기본 점수, 기본 심각도 값을 추출하여 디바이스 보안취약점 DB를 구축한 후, 디바이스 등록 시 디바이스 속성 정보를 추출하여 CVSS 점수를 디바이스의 보안취약점 점수로 등록한다. 디바이스 중요도 및 CVSS 점수는 디바이스 등록 과정에서 디바이스의 위험도 계산에 활용되며 계산 방법은 세그멘트 위험도 계산 부분에서 설명한다.

세그멘트 구성은 디바이스가 등록되는 과정에서 디바이스 속성 기준으로 자동으로 구성되고, 크게 디바이스, 네트워크, 서비스 세그멘트로 구분된다. 디바이스 속성 정보가 같은 디바이스들로 구성된 디바이스 세그멘트가 대부분이고, 디바이스가 연결된 GW 기준으로 네트워크 세그멘트가 구성되며, 디바이스가 어떤 서비스를 목적으로 운영되는지에 따라 서비스 세그멘트가 구성된다. 본 논문에서 사용되는 디바이스 속성으로는 디바이스 타입(도어개폐기, 카드리더기, 출입통제제어기, 보안카메라 등), 제조사, 제품명, 운영체제 버전, HW 기반 보안모듈 장착 여부, 디바이스가 속한 서비스 종류(출입통제서비스 등) 등이 있다. 디바이스 세그멘트의 경우 같은 속성으로 구성된 디바이스 그룹 형태의 세그멘트로도 구성되고, 개별 디바이스에 대한 보안통제를 가능하도록 하기 위해 단독 디바이스로 구성된 "디바이스" 단일 형태의 세그멘트도 구성된다. 그림 5는 관리 인터페이스를 통해 디바이스 등록 및 세그멘트 자동 구성이 완료된 결과를 나타낸다.

상단 오른쪽은 등록된 디바이스의 개수, 격리된 디바이스 개수, 등록된 전체 디바이스에 대한 평균 위험도 정보가 표시되고, 상단 왼쪽은 오른쪽에 등록된 디바이스를 기준으로 구성된 세그멘트 정보가 표시된다. 총 204개의 세그멘트가 구성되어 있고, 정상상태 세그멘트, 격리된 세그멘트, 전체 세그멘트에 대한 평균 위험도 정보가 표시되어 있다. 구성된 세그멘트는 각 세그멘트를 구분하는 ID와 세그멘트 종류(구성 기준), 세그멘트의 위험도, 현재 보안통제상태, 세그멘트로 구성된 디바이스 개수 등의 정보를 확인할 수 있다.

세그멘트 위험도(S_R)는 세그멘트 내 디바이스 중요도(D_A) 평균($Avg(D_A)$), 세그멘트 내 디바이스 CVSS 점수(D_V) 평균($Avg(D_V)$), 세그멘트 내 보안

그림 5. 세그멘트 구성 결과
Fig. 5. Segments configuration result

위협 발생률(S_T)에 비중 상수(w_i)를 적용하여 계산된다. 개별 디바이스도 자신으로만 구성된 디바이스 세그멘트를 가지므로 디바이스 위험도는 디바이스 세그멘트에 대한 위험도로 구할 수 있다. 세그멘트 위험도(S_R)는 식 (1)과 같이 표현되고, 본 논문에 제시된 가중 상수값 및 개별 항목 값의 범위는 기능 시험을 위해 적절한 비율로 임의로 할당한 값으로 향후 조정이 필요한 부분이다.

$$S_R = w_1 Avg(D_A) + w_2 Avg(D_V) + w_3 S_T \qquad (1)$$

- $0 \le w_1 Avg(D_A) \le 2 \quad (w_1 = 0.4,\ 0 \le D_A \le 5)$
- $0 \le w_2 Avg(D_V) \le 3 \quad (w_2 = 0.3,\ 0 \le D_V \le 10)$
- $0 \le 10 w_3 S_T \le 5 \qquad (w_3 = 0.5,\ 0 \le S_T \le 1)$

세그멘트 위험도(S_R)는 디바이스 등록 시기에 보안위협 발생률이 적용되지 않은 값을 가지고, 보안위협이 탐지되었을 경우 적용되어 값이 갱신되고 보안통제 대상 세그멘트 결정 과정에 이용된다.

3.3 보안위협 탐지(사물봇 악성코드 행위 탐지)

본 논문에서 보안위협 탐지 범위는 사물봇 악성코드로 한정한다. 사물봇 악성코드는 C&C (Command and Control) 서버로부터 DDoS 명령을 수신하기 위해 C&C 서버와의 연결을 유지해야 하고, 공격자는 C&C 서버의 역추적을 피하기 위해 서버의 IP 주소를 수시로 변경한다. 그러므로 사물봇 악성코드는 공격 명령 수신을 위한 C&C 서버와의 상시 연결 상태를 유지하기 위해 주기적으로 DNS 서버를 통한 C&C 서버의 IP 주소를 획득해야 하며, 이는 사물봇 악성코드에 의한 DNS 쿼리가 반드시 발생함을 의미한다[11-12].

IoT 서비스에서의 디바이스는 크게 센서와 액츄에이터 역할의 디바이스들로 구성되어 있고, 센서에 의해 수집된 데이터가 전달되는 데이터 수집 시스템 혹은 액츄에이터에 제어 명령을 내리는 제어 시스템은 그 대상이 명백히 식별되어 있다. 따라서, IoT 서비스를 위해 운영되는 시스템을 제외한 관리되지 않은 시스템으로의 연결 시도는 C&C 서버로의 연결을 시도하는 사물봇 악성코드의 행위로 의심할 수 있다.

본 논문은 IoT 서비스에서 정상적으로 운영되는 시스템 서버의 도메인 네임으로 화이트리스트를 구성하고, 화이트리스트 이외의 도메인 네임에 대한 쿼리 행위를 사물봇 악성코드 행위로 간주한다. 또한 센서 및 액츄에이터 역할의 디바이스 외에 스마트 기기와 같이 연결 대상이 불특정한 디바이스는 사물봇 탐지 디바이스 대상에서 제외하는 예외 디바이스로 지정하여 사물봇 악성코드 오탐(false positive) 비율을 줄였다. 도메인 네임에 대한 화이트리스트 초기 설정은 매니저 인터페이스를 통해 IoT 네트워크에서 정상적으로 운영되는 시스템의 도메인 네임을 등록하고 등록된 도메인 네임을 모든 에이전트에게 배포하는 것으로 진행된다. 에이전트는 배포된 도메인 네임의 화이트리스트를 통해 사물봇 악성코드 행위를 탐지하는데 참조한다.

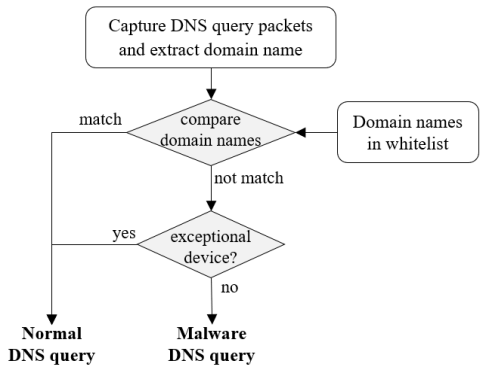

그림 6. 사물봇 악성코드 탐지 절차
Fig. 6. Procedure of malware detection

그림 6는 에이전트에서의 악성코드 탐지 절차를 나타낸다. 에이전트는 GW를 통과하는 DNS 쿼리 패킷을 캡쳐하여 쿼리 요청된 도메인 네임이 화이트리스트에 해당하는지 그리고 예외 디바이스로부터 전송된 패킷인지 확인하는 단계를 거쳐 악성코드를 판단한다.

악성코드로 판단될 경우 보안위협 식별정보(사물봇 악성코드), 탐지 에이전트 정보, DNS 쿼리 생성 디바이스 정보 및 요청한 도메인 네임 정보 등으로 보안위협 정보를 구성하여 매니저에게 전송한다.

3.4 보안위협 분석

보안위협 분석은 탐지된 보안위협 정보를 바탕으로 해당 보안위협의 확산 여부, 각 세그멘트에서의 해당 보안위협 발생률 및 위협도를 계산하는 과정이다. 해당 과정은 보안통제를 수행할 세그멘트 선택을 위한 선행 과정이다.

임의의 보안위협에 대한 확산 여부는 현재 분석 주기에서 발생한 해당 보안위협 수와 이전 모든 분석 주기에서 해당 보안위협 평균 발생 수의 비교를 통해 결정하며, 식 (2)과 같이 표현된다.

$$TS_{th_i} = N_{th_i\_t_n} - \frac{1}{n-1}\sum_{j=1}^{n-1}(N_{th_i\_t_j}) \quad (2)$$

TS_{th_i}는 보안위협 $i(th_i)$ 확산 여부, $N_{th_i_t_n}$은 현재 분석 주기(t_n) 내에서 발생한 th_i 발생 횟수, $N_{th_i_t_j}$는 임의의 분석 주기(t_j)에서 발생한 th_i 발생 횟수를 의미한다. 만약 TS_{th_i}가 0보다 크다면 즉, 이전의 모든 분석 주기에서의 th_i의 평균 발생횟수보다 현재 분석 주기에서 th_i의 발생 횟수가 더 많다면 th_i는 확산 중이라고 판단한다.

세그멘트 보안위협 발생률은 보안위협이 탐지될 때마다 세그멘트를 구성하는 전체 디바이스에 대한 해당 보안위협 발생 디바이스의 비율로 계산되며, 식 (3)와 같이 표현된다.

$$TI_{seg_k\_th_i} = N_{Dseg_k\_th_i\_t_n} / N_{Dseg_k} \quad (0 < k \leq N_s) \quad (3)$$

$TI_{seg_k_th_i}$는 세그멘트 $k(seg_k)$ 내 th_i 발생률, $N_{Dseg_k_th_i_t_n}$은 seg_k에서 현재 분석 주기(t_n)에 th_i가 발생한 디바이스 개수, N_{Dseg_k}는 seg_k를 구성하는 디바이스 개수, N_S는 전체 세그멘트 수를 의미한다.

위험도는 디바이스 등록 시 디바이스 및 세그멘트 위험도를 계산하는 식 (1)을 이용하여 보안위협 발생률을 적용하여 값을 갱신한다.

3.5 세그멘트 결정 및 보안통제정책 생성

보안통제정책이 적용될 세그멘트는 확산 여부에 따라 선택될 세그멘트 범위가 달라지지만 세그멘트가 선택된 후에는 선택된 세그멘트의 보안위협 발생률과 위험도가 각 임계치보다 높을 때 최종적으로 결정된다.

우선 보안위협 확산 상황이 아닐 경우, 보안위협 발생률이 가장 높은 세그멘트가 선택되고 선택된 세그멘트의 위험도가 설정된 임계치보다 높을 때 최종적으로 선택된다. 디바이스가 단독으로 세그멘트를 구성할 수 있으므로 보안위협이 발생한 디바이스 세그멘트가 보안위협 발생률 100%로 가장 높아 보안위협이 발생된 디바이스가 선택된다. 또한 위험도 임계치를 0.5로 설정할 경우 보안위협이 발생한 디바이스 세그멘트의 보안위협 발생률은 식 (1)에 의해 0.5가 되고 위험도도 0.5 이상이 되어 해당 디바이스가 최종적으로 보안통제정책 집행대상이 된다. 보안위협 확산 상황이 아닐 경우 보안위협이 발생한 디바이스만 통제할 수 있다.

보안위협 확산 상황일 경우, 보안위협 발생률이 설정된 임계치보다 높은 모든 세그멘트가 선택되고, 선택된 세그멘트 중 위험도가 설정된 임계치보다 높은 세그멘트가 최종적으로 선택된다. 보안위협 발생률 및 위험도 임계치가 높을수록 디바이스 그룹 단위의 세그멘테이션이 제한적으로 수행되고, 낮을수록 빈번히 수행된다. 확대된 범위에 대한 보안통제는 보안위협 확산 행위를 억제할 수 있지만, 정상적인 서비스에 영향을 줄 수 있으므로 조직에서 운영하는 보안정책 강도 및 서비스 가용성을 고려하여 임계치를 설정할 필요가 있다.

세그멘트 결정 후에는 세그멘트를 대상으로 네트워크 연결 통제를 위한 보안통제정책을 생성한다. 보안통제정책은 보안위협 특성에 따라 디바이스 그룹으로 구성된 디바이스 세그멘트, 디바이스 그룹과 특정 네트워크 속성(프로토콜, 포트)으로 구성된 네트워크 세그멘트, 네트워크 속성(프로토콜, 포트)으로만 구성된 서비스 세그멘트 형식으로 적용될 수 있다. 사물봇의 경우 악성코드 행위가 C&C 서버에 대한 DNS 쿼리, C&C 접속, 악성코드 로딩을 위한 악성코드 분배 서버(주로 웹서버)의 접속 등 다양한 네트워크 속성으로 동작하므로 디바이스 세그멘트 단위의 통제를 하도록 설정하였다.

3.6 보안통제정책 분배 및 집행

보안통제정책은 모든 에이전트에게 분배되지 않고, 보안통제 대상 세그멘트에 속한 디바이스가 연결된 에이전트에만 전달된다. 매니저는 보안통제정책을 전달할 에이전트 개수만큼 쓰레드를 생성하여, 각 쓰레드를 통해 보안통제정책을 에이전트에게 분배한다. 에이전트는 보안통제정책을 수신한 후 에이전트가 동작하는 GW 내 방화벽 규칙으로 치환되어 적용된다. 본 논문에서는 *iptables* 방화벽 프로그램을 이용하여 보안통제정책을 적용하였다.

3.7 스마트 세그멘테이션 관리 인터페이스

스마트 세그멘테이션 관리 인터페이스는 스마트 세그멘테이션 관리 및 상태 모니터링 기능을 제공하는 관리자용 시각화 기반의 웹 인터페이스이며 구성된 세그멘트에 대한 상태 모니터링을 위한 전체적인 형상은 그림 7과 같다. 그림 7에서 왼쪽에 위치한 각 사각형 박스는 세그멘트를 의미하고, 해당 박스를 클릭하면 그림 8과 같이 세그멘트 아래 구성된 디바이스를 확인할 수 있다. 세그멘트 바탕색은 세그멘트 위험

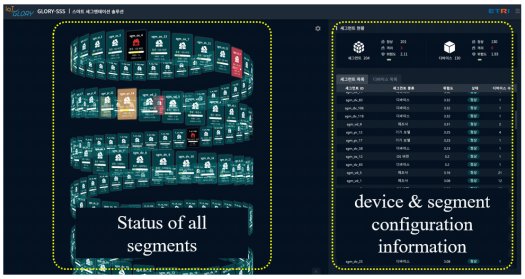

그림 7. 스마트 세그멘테이션 관리 인터페이스
Fig. 7. Smart segmentation management interface

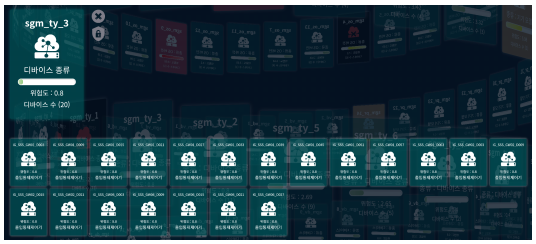

그림 8. 세그멘트를 구성하는 디바이스 정보
Fig. 8. Composed devices within a segment

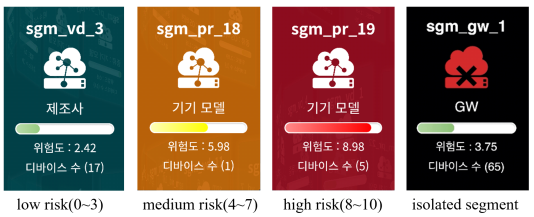

그림 9. 상태 정보에 따른 세그멘트 형상
Fig. 9. Segment appearance according to its status

도를 나타내고, 특히 검정색은 세그멘트가 보안통제정책에 의해 통제되었음을 나타낸다. 구체적인 이미지는 그림 9와 같다.

Ⅳ. 실험 및 결과

4.1 스마트 세그멘테이션 관리 인터페이스

스마트 세그멘테이션 프레임워크가 보안위협 확산 억제 기능을 제공하는지 검증하기 위해 그림 10과 같이 테스트베드를 구축하였다. 테스트베드는 매니저와 관리 인터페이스가 동작하는 Ubuntu Linux 기반 PC 서버와 에이전트가 동작하는 OpenWRT 기반 IoT GW 5대와 다양한 속성의 세그멘트를 구성하는 Raspberry Pi 3B+ 기반 IoT 디바이스 130대로 구성되었다. Mirai 악성코드의 위협 확산 환경을 위해 DNS 서버와 C&C 서버를 구축하였고, 한대의 C&C

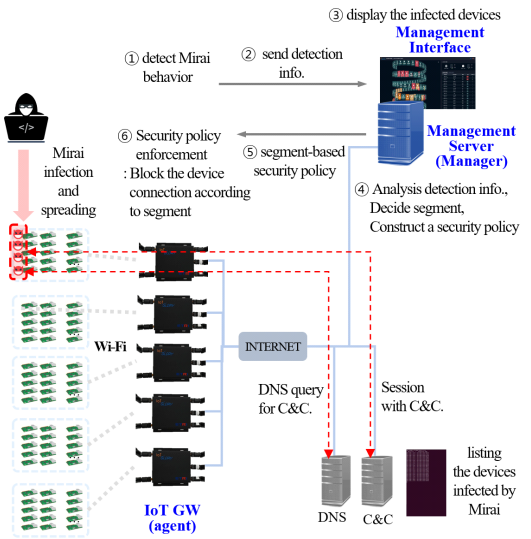

그림 10. Mirai 악성코드 동작 환경에서 스마트 세그멘테이션 기능 시험을 위한 테스트베드 구성
Fig. 10. Testbesd configuration for fundtional test of smart segmentation with Mirai malware

서버 내에 C&C 기능, HTTP 서버(악성코드 배포 서버), 로더가 동작한다. 130대 디바이스는 다양한 속성을 가지도록 그림 3과 같이 json 형식의 파일로 구성되어 등록되고, 등록 과정에서 속성값을 기준으로 자동 생성된 세그멘트에 포함된다.

하나의 디바이스는 속성에 따라 여러 개의 세그멘트에 구성될 수 있다. 본 실험에서는 디바이스 타입으로 도어개폐기, 카드리더기, 출입통제제어기, 보안카메라, 지문인식기 등을 설정하였고, 설치 위치로는 조직 부서 즉, 안전관리팀, 정보관리팀, 인사팀 등으로, 디바이스 제조사, 벤더, OS 버전 등은 CVE 정보를 기반으로 CVSS 점수를 참조할 수 있도록 디바이스에 임의로 설정하였다.

4.2 Mirai 악성코드 기반 세그멘테이션 기능 시험

스마트 세그멘테이션 프레임워크가 보안위협 확산 방지에 효과가 있는지 확인하기 위해, 디바이스 단위의 보안통제 시험과 세그멘트 단위의 보안통제 시험을 진행하였다. 디바이스 단위의 보안통제 시험은 Mirai 악성코드 행위가 탐지되면 해당 디바이스를 격리하고, 세그멘트 단위의 보안통제 시험은 보안위협 발생 시 해당 보안위협 분석 및 통계 정보를 통해 보안위협 확산이 예상되는 세그멘트를 격리한다. Mirai 악성코드는 IoT 네트워크에 침투되었다고 가정하고, 65대의 디바이스가 연결된 임의의 GW 영역 내 한 디

바이스에서 Mirai 악성코드를 실행시킨 후 감염이 확산되도록 하였다.

디바이스 단위 보안통제의 경우 보안위협이 탐지되면 탐지 정보를 기반으로 보안위협이 발생된 디바이스를 통제하므로 분석 주기 및 보안위협 발생률 및 위험도 임계치 값이 필요 없다. 세그멘트 단위 보안통제의 경우 보안위협 분석 및 세그멘트 결정 등과 관련하여 분석 주기 및 임계치 정보가 필요하고, 보안위협 확산 방지 효과를 빠르게 확인하기 위해 보안위협 확산 여부 결정에 대한 분석 주기는 30초, 보안위협 확산율 임계치는 0.3, 위험도 임계치는 0.3으로 설정하였다. Mirai 악성코드의 동작 및 악성코드 동작에 따른 세그멘테이션 과정은 그림 10에서 명시된 순서로 진행되고, Mirai 악성코드가 확산하는 환경에서 스마트 세그멘테이션 각 역할 별 동작 화면은 그림 11과 같다.

디바이스 단위 보안통제 수행 결과는 그림 12(좌)와 같으며, 65대 디바이스 중 51대가 감염되어 약 78.5%의 악성코드 확산율을 보였다. 악성코드 탐지 시점은 악성코드가 디바이스에 침투하여 C&C 서버와의 연결을 위한 DNS 쿼리 요청 시점이다. 이 시점은 인접 디바이스로의 감염이 진행되고 있는 시점으로 보안위협이 발생한 디바이스를 격리하더라도 C&C 서버와의 세션 연결을 차단할 수 있지만, 악성코드의 확산을 방지하지 못함을 알 수 있다.

세그멘트 단위의 보안통제 수행 결과는 그림 12(우)와 같으며, 65대 디바이스 중 23대가 감염되어 약 35.4%의 악성코드 확산율을 보이면서, 디바이스 단위의 보안통제와 비교하면 악성코드 확산율이 약 44% 정도 낮아졌다. 세그멘트 결정을 위한 분석 주기 동안 보안통제가 적용되지 않아 Mirai 악성코드의 확산 초

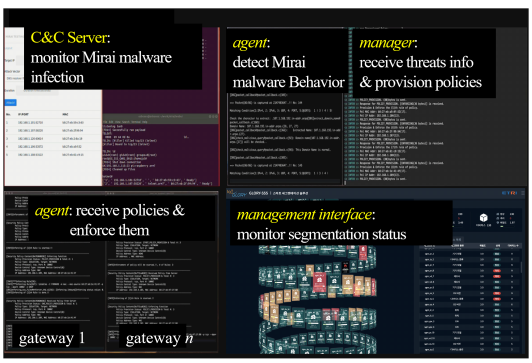

그림 11. Mirai 악성코드 환경에서의 스마트 세그멘테이션 시험 화면
Fig. 11. Snapshot of smart segmentation functional test using Mirai malware

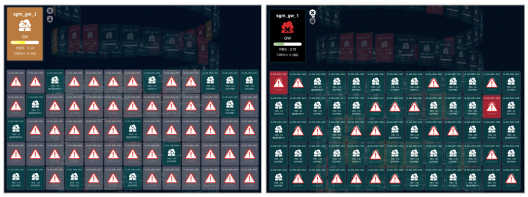

그림 12. 디바이스 단위(좌) 및 세그멘트 단위(우) 보안통제 상황에서의 악성코드 확산 결과
Fig. 12. Malware infection results under device unit(left) and segment unit(right) security control(isolation)

기에 일부 디바이스가 감염되는 상황은 불가피하지만 분석 주기 이후에는 디바이스 단위 보안통제에 비해 악성코드 확산이 크게 줄어드는 것을 확인할 수 있다. 이는 네트워크가 규모가 커질수록 디바이스 단위 통제의 경우 악성코드가 계속 확산될 수 있는 것에 비해 세그멘트 단위 통제는 일정 수준에서 확산을 차단할 수 있어 그 효과는 더욱 클 것으로 예상된다.

세그멘트 구성 상태와 설정값(확산주기, 보안위협 발생률 및 위험도 임계치), 그리고 악성코드 종류 및 확산 방법 등에 따라 확산 방지 성능은 달라질 수 있지만 본 시험 결과는 세그멘트 기반 보안통제 프레임워크가 IoT 네트워크에 침투한 보안위협 확산을 방지할 수 있음을 보여준다.

V. 결 론

본 논문은 IoT 서비스 특성에 기반한 Mirai 같은 사물봇 악성코드 행위를 탐지하고, 악성코드 감염 등의 보안위협 확산을 방지하기 위해 디바이스 속성 기반의 세그멘트 기반의 네트워크 접속을 통제하는 스마트 세그멘테이션 프레임워크에 대한 구현 방안을 제시하였다. 구현된 프레임워크는 IoT 네트워크 환경을 모사하여 구축하고 실제 보안사고를 일으킨 Mirai 악성코드 확산 기능을 재현하여 사물봇 악성코드 감염 확산 방지 및 사물봇 생성 억제가 가능함을 시험을 통해 검증함으로써, IoT 네트워크 환경에서 보안위협이 확산됨을 방지할 수 있는 세그멘트 기반 자율적인 보안통제가 가능한 프레임워크라는 점에서 의미를 가진다.

향후에는 현재 스마트 세그멘테이션 프레임워크의 기능 검증 수준의 성능을 고도화하기 위해, 보안위협 탐지 범위 및 성능 개선, 보안위협 확산 여부 판단 및 세그멘트 결정 알고리즘 고도화 등에 집중할 계획이며 현재 연구가 진행 중이다. 특히 최근 사이버 공격이 지능화됨에 따라 독자적인 솔루션만으로는 사이버

위협에 효과적인 대응이 어려워, 신속하고 효과적인 대응을 위해 사이버 위협 공유 체계 구축이 활발히 진행 중이며 이를 가능하도록 위협정보를 공유할 수 있는 STIX/TAXII 같은 표준화된 규격을 통해 위협정보 공유 체계가 만들어 지고 있다[13]. 이에 따라 표준화된 STIX/TAXII 표준 규격을 통해 고성능의 보안위협 탐지솔루션과의 연동을 통해 보안위협 탐지 성능을 높이고 확장된 보안위협의 탐지 결과를 제공받아 보안위협 분석, 세그멘트 결정 및 보안정책 생성의 고도화를 진행하고자 한다. 또한 세그멘트 단위의 격리는 보안위협이 발생하지 않은 디바이스에 대해 과도한 격리가 발생할 수 있고 이는 서비스 방해를 유발할 수 있어, 격리된 세그멘트 내 보안위협이 발생되지 않은 디바이스 해제 연구도 진행할 예정이다.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721-82743, Jun. 2019.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80-84, 2017.

[3] B. Vignau, R. Khoury, and S. Hallé, "10 years of IoT malware: a Feature-based taxonomy," *IEEE 19th Int. Conf. Softw. Quality*, 2019.

[4] Z. Kerravala, *To secure indudtrial IoT, use segmentation instead of firewalls* (2019). Retrieved Feb., 15, 2020, from https://www.networkworld.com/article/3437956/to-secure-industrial-iot-use-segmentation-instead-of-firewalls.html.

[5] A. Osman, A. Wasicek, S. Köpsell, and T. Strufe, "Transparent microsegmentation in smart home IoT networks," *3rd USENIX Workshops. HotEdge20*, Jun. 2020.

[6] A. Wasicek, "The future of 5G smart home network security is micro-segmentation," *Network Security*, vol. 2020, no. 11, pp. 11-13, Nov. 2020.

[7] S. Charfadine, O. Flauzac, F. Nolot, C. Rabat, and C. Gonzalez, "Secure exchanges activity in function of event detection with the SDN," *AFRICOMM 2018, LNICST*, vol. 275, pp. 315-324. Springer, Cham, 2019.

[8] S. Y. Hwang and J. N. Kim, "A study on the automated attack tool of IoT bot for verification about security technique of IoT device," *Conf. Info. Secur. and Cryptography*, 2019.

[9] E. Fernandez, N. Yoshioka, and H. Washizaki, "Abstract and IoT security segmentation patterns," in *Proc. Asian PLoP'19*, Tokyo, Japan, Mar. 2019.

[10] J. D. Lim, S. K. Sohn, and J. N. Kim, "Proposal of smart segmentation framework for preventing threats from spreading in IoT," in *Proc. ICTC2020*, pp. 1757-1759, Jeju Island, Korea, Oct. 2020.

[11] K. Alieyan, et al., "A survey of botnet detection based on DNS," *Neural Computing and Appl.*, vol. 28, no. 7, pp. 1541-1558, 2015.

[12] X. Li, J. Wang, and X. Zhang, "Botnet detection technology based on DNS," *Future Internet*, vol. 9, 2017.

[13] W. S. Lim, M. K. Yoon, and H. S. Cho, "KOSIGN: Cyber threat information sharing system from information protection products perspective," *J. KIISC*, vol. 28, no. 2, pp. 20-26, Apr. 2018.

임 재 덕 (Jae-Deok Lim)

1999년 2월 : 경북대학교 전자공학과 졸업

2001년 2월 : 경북대학교 전자공학과 석사

2013년 8월 : 충남대학교 컴퓨터공학과 박사

2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원

<관심분야> IoT 보안, 운영체제 보안, 네트워크 보안, 접근제어

[ORCID:0000-0001-6384-0056]

손 선 경 (Seon-Gyoung Sohn)

1999년 2월 : 전남대학교 전산학과 졸업

2001년 2월 : 전남대학교 전산학과 석사

2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원

<관심분야> IoT 보안, 보안관제, 위험관리

김 정 녀 (Jeong-Nyeo Kim)

1987년 2월 : 전남대학교 전산통계학과 졸업

2000년 2월 : 충남대학교 컴퓨터공학과 석사, 박사

1988년~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원

1996년 : OSF/RI 공동연구 파견(미국)

2005년 : Univ. of California, Irvine Post-Doc.

2015년~현재 : 과학기술연합대학원대학교(UST) ICT(정보보호공학)과 교수

<관심분야> IoT 보안, 모바일 보안, 보안 OS, 시스템·네트워크 보안 등

[ORCID:0000-0002-7134-0622]