Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 9 pp. 504-509, 2019

https://doi.org/10.5762/KAIS.2019.20.9.504
ISSN 1975-4701 / eISSN 2288-4688

인터넷 와이드 스캔 기술 기반 인터넷 연결 디바이스의 취약점 관리 구조 연구

김태은[1*], 정용훈[2], 전문석[2]
[1]한국인터넷진흥원, [2]숭실대학교 컴퓨터학과

A Study on the Vulnerability Management of Internet Connection Devices based on Internet-Wide Scan

Taeeun Kim[1*], Yong Hoon Jung[2], Moon-Seog Jun[2]
[1]Korea Internet & Security Agency
[2]Dept. of Computer Science, SoongSil University, Seoul, South Korea

요 약 최근 무선 통신 기술과 소형 디바이스의 성능이 기하급수적으로 발전하였다. 이런 기술과 환경 변화에 따라 다양한 종류의 IoT 디바이스를 활용한 서비스가 증가하고 있다. IoT 서비스의 증가로 오프라인 환경에서 사용되던 소형 센서, CCTV 등의 디바이스가 인터넷에 연결되고 있으나, 많은 수의 IoT 디바이스는 보안 기능이 없고 취약한 오픈소스, SW를 그대로 사용하고 있다. 또한, 전통적으로 사용되던 스위치, Gateway 등의 네트워크 장비도 사용자의 주기적인 업데이트가 이루어지지 않아 수많은 취약점을 내포한 채 운영된다. 최근에는 IoT 디바이스의 간단한 취약점을 대상으로 대량의 봇넷(botnet)을 형성하여 DDoS 공격 등에 악용하는 사례가 늘어나고 있다. 본 논문에서는 Internet-Wide Scan 기술을 활용하여 인터넷에 연결된 대량의 디바이스를 빠르게 식별하고, 내포된 취약점 정보를 분석 및 관리하는 시스템을 제안한다. 또한, 실제 수집한 배너 정보를 통해 제안 기술의 취약점 분석률을 검증하였다. 향후 제안 시스템이 사이버 공격을 예방할 수 있는 기술로 활용 될 수 있게 자동화 및 고도화를 진행 할 계획이다.

Abstract Recently, both wireless communications technology and the performance of small devices have developed exponentially, while the number of services using various types of Internet of Things (IoT) devices has also massively increased in line with the ongoing technological and environmental changes. Furthermore, ever more devices that were previously used in the offline environment-including small-size sensors and CCTV-are being connected to the Internet due to the huge increase in IoT services. However, many IoT devices are not equipped with security functions, and use vulnerable open source software as it is. In addition, conventional network equipment, such as switches and gateways, operates with vulnerabilities, because users tend not to update the equipment on a regular basis. Recently, the simple vulnerability of IoT devices has been exploited through the distributed denial of service (DDoS) from attackers creating a large number of botnets. This paper proposes a system that is capable of identifying Internet-connected devices quickly, analyzing and managing the vulnerability of such devices using Internet-wide scan technology. In addition, the vulnerability analysis rate of the proposed technology was verified through collected banner information. In the future, the company plans to automate and upgrade the proposed system so that it can be used as a technology to prevent cyber attacks.

Keywords : Internet Wide Scan, Vulnerability Information Management, Device Management, Security Management, IoT Security

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임
(No.2016-0-00193, IoT 보안 취약점 검색·공유 및 시험 기술 개발)
*Corresponding Author : Taeeun Kim(KISA)
email: tekim31@kisa.or.kr
Received August 1, 2019 Revised September 4, 2019
Accepted September 6, 2019 Published September 30, 2019

1. 서론

최근 IT 환경은 IoT 서비스의 보급으로 인터넷에 연결되는 소형 디바이스의(CCTV, SmartHome, 등) 보급이 급격히 증가하고 있다. 2018년 IoT Analytics Research는 2018년 인터넷에 연결된 디바이스를 약 178억개로 분석하고 있으며, 2025년까지 인터넷에 연결되는 디바이스가 342억개 이상이 될 것이라고 전망하였다[1].

IoT 서비스 및 디바이스 수의 급격한 증가와는 반대로 보안에 대한 수준과 대안은 미흡하며, 이에 따른 인터넷 연결 디바이스의 취약점을 통한 사이버 위협은 늘어나고 있다. 네트워크, IoT 디바이스 등의 소형기기는 사용자가 최초 설치를 하고나면 주기적으로 펌웨어 업데이트 등의 관리를 하지 않아 오래된 취약점을 다량 보유하고 있어 주요한 공격 대상되므로 빠른 식별을 통한 업데이트, 격리(차단) 등의 예방조치가 필요하다[2].

취약한 디바이스는 개발의 편리함을 위해 보안 기능이 없거나 취약한 버전의 OS, 오픈소스, 통신 프로토콜 등을 사용하고 있다.

다음은 인터넷이 연결된 취약한 디바이스를 통해 이루어진 사이버 공격의 실제 사례이다. 2016년 프랑스의 웹 호스팅 업체(OHV)와 미국의 DNS 제공 업체(Dyn)를 공격하는 DDoS 공격이 발생하였다. 두 공격의 공통점은 PC를 감염시켜 공격 트래픽을 발생하던 기존 공격과는 다르게 CCTV, 공유기 등과 같은 소형 IoT 디바이스가 Botnet을 구성했다는 점이다. 위 공격은 인증이 취약한 CCTV 등을 'Mirai' 악성코드를 통해 감염 시켜 공격에 활용하였다. 이와 같이 감염된 디바이스에서 생성된 트래픽은 IP당 평균 1~30Mbps 크기의 트래픽을 총 1.5Tbps 규모로 전송하여 서비스를 이용하지 못하게 공격하였다. 'Dyn'의 경우는 공격을 통해 트위터, 넷플릭스 등 1,200 여개의 대형 사이트의 서비스가 정지되기도 하였다. 위 사이버 공격 사례들은 보안 기능이 없거나 인증에 필요한 비밀번호를 변경하지 않고 default password를 그대로 사용하는 취약한 IoT 디바이스로부터 시작되었다.

위와 같은 환경에서는, 기존 PC, 서버 등의 디바이스를 관리하는 방식과는 다른 기술이 필요하다. 본 논문에서는 다수의 디바이스를 빠르게 찾아 정보를 수집하는 'Internet-Wide Scan'과 알려진 취약점 정보를 활용 수집한 디바이스 정보에 알려진 취약점이 존재하는지 분석하는 '보안 취약점 정보 분석' 기술을 활용하여 사이버 공격을 예방할 수 있는 시스템 구조를 제안하고 성능을 검증한다. 또한 제안 기술은 사이버 공격의 사후 대응 관점보다는 사전 예방의 중요성을 강조하고자한다.

2. 관련 연구

2.1 인터넷 와이드 스캔 기술

기존의 네트워크 스캔 기술은 하나의 디바이스(단일 IP)를 대상으로 운영체제를 파악하고 열려있는 포트에 다량의 트래픽을 전송하여 디바이스 정보를 수집하였다. 또한 취약점 분석을 목적으로 공격적인 기법을 사용하여 디바이스의 취약점을 확인한다. 예를 들어 디폴트 패스워드 취약점을 확인하기 위해 잘 알려진 ID/PW를 대입해 보고, exploit 코드를 활용하여 디바이스를 직접적으로 공격 해 보기도 한다. 이러한 스캔 방식을 Active Scan이라고 하며 nmap, Nessus, Defensics 등과 같은 도구들이 있다. 하지만 인터넷에 연결된 다수의 원격지 디바이스를 점검하는 목적으로 사용하기에는 부적합하다. 점검하려는 디바이스로 공격적인 행위나 트래픽을 유발하므로 정상적인 동작을 할 수 없고, 디바이스가 다운되어 동작하지 못할 수 있다. 따라서 다수의 원격지 디바이스의 정보만을 빠르게 수집하기 위해 Passive Scan 기술이 활용되고 있다.

Passive Scan 기술은 디바이스 정보를 수집하기 위해 Active Scan과 같은 공격적인 방법을 사용하지 않는다. 이 도구들은 수집하려는 디바이스로 정상적인 통신 메시지를 보내고 돌아오는 응답 메시지에서 필요한 정보를 획득한다[3,4]. 또한 수집의 대상도 인터넷에 연결된 대부분의 디바이스가 대상이며, 주로 콘솔 서비스 등의 접속 배너 정보와 통신 트래픽의 헤더·바디 등의 정보를 고속으로 수집한다. 이러한 스캔 방식을 사용하는 서비스는 Shodan, Censys(ZMap), Masscan 등이 있다[5].

Shodan과 Censys는 디바이스 정보 수집량과 속도에서 차이점을 보인다. Shodan의 경우 IPv4 전체 대역의 정보가 갱신되는 주기가 4주인 반면 디바이스가 사용할 수 있는 모든 포트의 정보를 포함하고 있다. 하지만 Censys는 주요 포트를 기준으로 2주만에 업데이트가 되고 있다. Censys의 경우 IPv4 주소 대역 전체를 1개의 수집 probe를 사용하여 스캔 하였을 때 1:09:45 만에 디바이스의 alive 상태를 확인할 수 있다[6]. 하지만 Shodan과 Censys는 사용자가 검색한 키워드를 배너에서 단순 매칭 시켜주는 방식으로 분석가가 입력하는 제

품명 등의 키워드로 정확한 결과를 얻기 어렵다. 예를 들어 CCTV 키워드를 입력 하였을 때, CCTV를 판매하는 웹 사이트 바디의 키워드를 매칭 시켜 주기도 한다. 따라서 분석가는 검색 결과를 확인, 선별하는 추가적인 작업이 필요하다.

2.2 보안 취약점 정보 분석 기술

보안 취약점과 관련된 기술은 네트워크 스캔 기술과 같이 분석 대상(디바이스)에게 직접적인 공격 행위가 없는 기술을 대상으로 한다.

분석 대상에게 직접적인 행위를 하지 않는 기술을 '보안 취약점 정보 분석 기술' 이라고 분류한다. 요소 기술은 취약점 정보를 관리하기 위해 구조화된 DB를 구축하고, 구축한 취약점 정보를 활용하여 분석 대상의 정보와 연관성을 분석하는 기술들이 포함된다. 보안 취약점 정보는 여러 단체에서 각자의 기준에 따라 관리되고 있다. NVD(National Vulnerability Database)에서 관리하는 CVE(Common Vulnerabilities and Exposures)가 대표적이며 Bugtraq, VulDB, 디바이스·SW등의 제조사에서도 취약점 정보들을 관리한다[7]. 본 논문에서는 취약점 정보 분석 기술을 활용하여 인터넷에 연결된 다수의 디바이스를 관리하는 시스템을 제안 한다.

3. 디바이스 취약점 관리 시스템

본 장에서는 IPv4 주소 기반의 디바이스를 고속으로 검색하고 보안 취약점 정보를 식별하여 사이버 위협을 예방할 수 있는 시스템을 제안한다. 제안하는 시스템은 Passive 방식의 Internet-Wide Scan과 보안 취약점 정보 분석 기술을 활용한다.

3.1 제안 시스템의 구성

인터넷에 연결된 디바이스의 취약점 정보를 관리하기 위해 디바이스 정보 및 취약점 정보 수집 기술, 디바이스에 포함된 취약점 정보 분석 기술로 시스템을 구성하였다. 개발 시스템은 'Internet Wide Scan Module', 'Vulnerability Information Management Module', 'Devices Vulnerability Analysis Module', 'Interface Module' 총 4개의 기능 모듈을 개발하였다. 제안 시스템은 Fig. 1과 같은 논리적 구조이며 각각의 모듈은 시스템 성능을 최대화하기 위해 서로 다른 서버에서 동작한다.

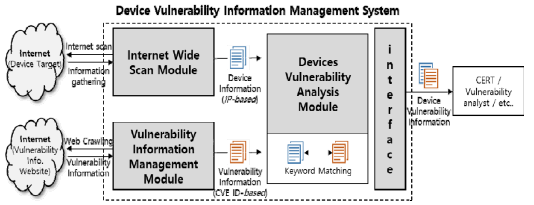


Fig. 1. Structure of Devices Vulnerability Management System

3.2 인터넷 와이드 스캔 모듈

인터넷에 연결된 디바이스의 정보를 수집하기 위해 'ZMap','ZGrab' 오픈소스를 개량하여 2가지 하위 모듈을 개발했다. 또한 2개의 수집 모듈에서 생성하는 스캔 트래픽을 관리하기 위해 트래픽 관리 모듈을 별도로 구현하고, DAG-CARD, PF-RING을 적용하여 성능을 향상시켰다. Internet Wide Scan Module의 구성은 Fig. 2와 같다.

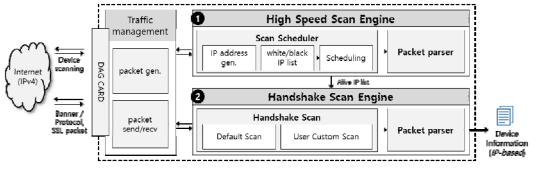


Fig. 2. Internet Wide Scan Module

❶ 디바이스를 고속으로 스캔하기 위한 'High Speed Scan Engine'은 디바이스의 연결 상태를 스캔하기 위한 스케줄러, 트래픽 파싱 기능을 수행한다.

스캔 스케줄러는 약 43억 개의 IPv4 주소를 스캔하기 위해 주소 목록을 생성한다. 스캔 IP주소 목록을 생성하는 과정은 Internet-Wide Scan 기술에서 중요한 역할을 한다. 스캔 IP주소 목록을 순차적으로 생성하게 되면 방화벽, IDS, IPS 등의 보안 장비에 비정상으로 탐지되고 더 이상 스캔을 할 수 없게 된다. 제안 시스템은 프로토타입 상태에서 주소 목록을 램덤하게 생성하기 위해 IP 주소를 10진수로 변환하여 순환하는 알고리즘을 개발하여 사용하였다. 하지만 실제 모듈 테스트에서 과도한 트래픽 발생으로 인해 보안 장비에 탐지되고, 패킷이 유실되는 현상이 발생하였다. 이와 같은 이슈를 개선하기 위해 Whois 정보를 기반으로 IP 할당 기관을 분류하고, 동일한 대역에 딜레이 타임을 적용한 스캔 스케줄러를 개발 하였다. 또한 스캔 스케줄러에는 Hit-rate 향상을 위한 White/Black List 기능도 적용하였다.

스캔 스케줄러에 의해 생성된 IP주소 목록으로 트래픽을 발생하면 인터 연결 디바이스로부터 응답 메시지(ACK)를 수신 할 수 있다. 응답한 디바이스의 포트 정보를 수집하기 위해 활성 IP List를 생성한다.

❷ 디바이스의 포트 별 정보 수집을 위한 'Handshake Scan Engine'은 ZGrab 오픈소스 같이 디바이스의 주요 포트를 대상으로 시스템 접속 배너, 암호 통신 정보, 패킷 헤더·바디 정보를 수집한다. 또한 다양한 추가 포트 정보를 수집하기 위해 사용자가 직접 포트와 데이터를 정의하거나, 트래픽 캡쳐(PCAP) 형태를 추출하여 임의의 프로토콜을 스캔하는 기능을 추가하였다. 따라서 디바이스 정보 수집 범위를 IPv4 전대역·전포트를 대상으로 확대하였다.

3.3 취약점 정보 수집 모듈

인터넷에 연결된 디바이스의 취약점 정보를 분석하기 위해 공개된 취약점 정보들을 수집하고, 분석이 가능하게 구조화 하는 기능이 필요하다. 취약점 정보 관리 모듈은 NVD에서 제공하는 파일화된 CVE 정보를 다운로드하여 CPE(Common Platform Enumeration), CWE(Common Weakness Enumeration), CVSS(Common Vulnerability Scoring System) 등의 정보를 구조화 한다. 현재까지 수집한 CVE 취약점 정보는 약10만개 정도이다.

하지만 취약점이 NVD에 등록되기까지 오랜 시간이 필요하며 다양한 취약점 정보를 얻기 위해서 정보 수집 채널의 확대가 필요했다. 추가적으로 Bugtraq, VulDB, Rapid7 등의 취약점 정보 사이트를 선정하여 업데이트 주기, 추가적인 취약점의 종류 등을 비교하였다. 그 결과 다양한 취약점 정보와 업데이트 주기가 빠른 Bugtraq, VulDB를 수집 대상으로 선정하여 웹 크롤링을 통해 취약점 정보를 수집한다.

취약점 정보는 CVE/non-CVE 분류로 정보를 수집하며, 하루 주기로 new/modified 정보를 업데이트한다. Bugtraq과 VulDB에는 각각의 취약점에 부여된 ID가 있고 연관된 CVE-ID가 포함되어 있다. 하지만 CVE에 등록되지 않은 새로운 취약점의 경우 '비정형 취약점 정보'로 분류하여 취약점 정보 유형을 분류하기 위한 가공을 한다.

3.4 디바이스 취약점 정보 분석 모듈

수집한 디바이스 정보에서 취약점의 존재를 확인하려면 디바이스 정보와 취약점 정보에 공통으로 들어있는 키워드 매칭이 필요하다. 'Devices Vulnerability Analysis Module'은 Fig. 3과 같이 2개의 하위 모듈로 구성된다. 첫 번 째는 디바이스 정보에서 제조사, 제품명과 같은 키워드를 찾아내서 CPE 정보를 식별하는 '디바이스 정보 분석' 모듈이며, 두 번 째는 디바이스 정보 분석 모듈에서 찾아낸 CPE를 통해 취약점 정보와 연결하는 '취약점 정보 분석' 모듈이다.

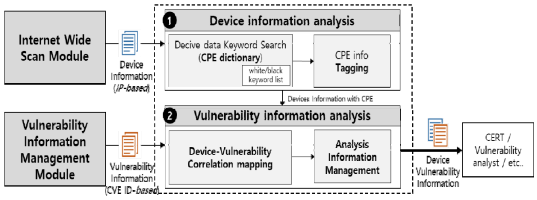


Fig. 3. Devices Vulnerability Analysis Module

❶ 디바이스 정보 분석 모듈은 디바이스를 스캔하여 수집한 배너, 응답 패킷의 payload(data), Handshake traffic 정보에서 CPE 정보를 식별한다. 식별하는 CPE 정보는 'CPE dictionary'에 정의된 표준화된 제품의 이름, 버전 등의 정보를 의미한다. CPE dictionary 정보와 디바이스 제품명 정보의 유사도 분석으로 정확도 80%이상의 결과를 CPE로 식별한다. 또한 CPE dictionary에 등록된 정보에 'a', 'login'과 같이 일반적으로 사용할 수 있는 단어가 포함되어 있어 디바이스를 식별하는데 많은 오류가 발생하였다. 이렇게 흔한 영어 단어나 특수한 키워드를 관리하는 White/Black List의 생성 및 관리 기능도 추가하였다. 마지막으로 식별한 디바이스의 CPE 정보에 사전에 정의 해둔 디바이스/제품 유형 정보를 태깅한다. 디바이스 유형 정보는 네트워크 장비, IoT 디바이스 등 6가지 유형으로 분류되며, IoT 디바이스는 IP Camera, NVR/DVR, 악성코드 감염 위험 디바이스 등 26가지의 제품 유형으로 추가 분류된다. 디바이스 정보 분석 예시는 Fig. 4와 같다.

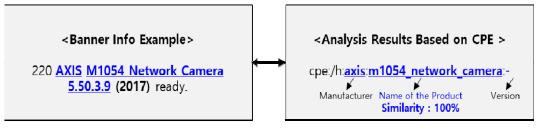


Fig. 4. Example of banner information analysis

❷ 취약점 정보 분석 모듈은 앞의 디바이스 정보 분석 모듈에서 식별한 디바이스의 CPE 정보와 취약점 정보

관리 모듈에서 수집한 취약점 정보에 포함된 CPE 정보를 매칭 분석한다. 디바이스 정보에서 CPE가 식별되었다면 취약점이 존재함을 의미 한다. 이렇게 매칭된 디바이스-취약점 정보는 국가 CERT, 취약점 분석가 등에게 공유하기 위해 json 형태로 생성/관리 된다.

4. 성능 실험 결과

'Devices Vulnerability Analysis Module'은 앞의 두 모듈에서 수집한 디바이스 정보, 취약점 정보를 매칭하여 디바이스에 포함된 취약점을 분석한다. 취약점 분석 성능 측정을 위해 사용된 데이터는 배너 분석을 통해 CPE 정보의 식별이 가능한 FTP, HTTP, SSH, TELNET 4종의 포트 정보를 사용하였다.

성능 측정은 수집된 디바이스 정보 중 제품명, 제조사, 버전 정보와 취약점 정보의 CPE 매칭 비율을 계산한다. CVE 취약점 정보에는 관련된 디바이스 정보를 CPE 형태로 포함하고 있어, CPE 식별을 통해 연관된 취약점 정보를 식별 할 수 있다.

$$\text{취약점 분석률}(\%) = \frac{CPE\text{정상 식별 수}}{\text{전체 배너 수}} * 100 \quad (1)$$

취약점 분석률은 수집된 전체 배너 수 에서 CPE를 정상적으로 식별한 비율을 계산한다. 프로토콜 4종의 데이터에서 각 10만개의 배너를 샘플링 했다. 샘플링 된 배너는 Unique한 배너 상위 1,000개를 기반으로 랜덤하게 선정하였다.(중복을 제외한 Unique 배너 Top 1,00 비율 : FTP - 69%, HTTP - 96%, SSH - 99%, TELNET - 82%)

취약점 분석률 실험은 배너 정보와 CPE의 매칭 임계값을 66%, 75%, 80%로 설정하여 분석 하였으며 결과는 Fig. 5, Table. 1과 같다.

취약점 분석률 실험 결과 배너정보의 정상 식별률은 평균 87.38% 으로 나탔으며, 4개의 프로토콜 모두 CPE 매칭 임계값을 80% 이상으로 설정하였을 때, 디바이스 정보에서 CPE를 정상으로 식별한 비율이 가장 높았다. 임계값이 낮은 경우에는 유사한 이름의 제품, 제조사 등이 과도하게 식별되는 오식별이 많이 발생함을 알 수 있다.

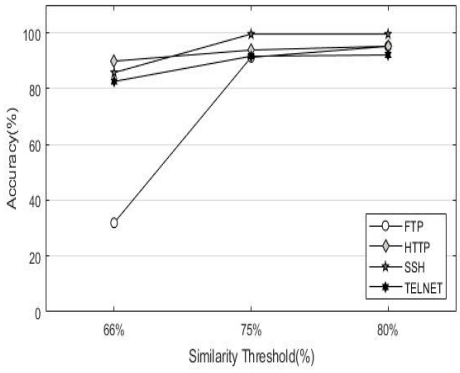


Fig. 5. The identification rate of the device information for CPE

Table 1. The result of the CVSS analysis for device information

Service	Similarity Threshold 66%	Similarity Threshold 75%	**Similarity Threshold 80%**	Average
FTP	31.9%	91.2%	95.2%	**72.8%**
HTTP	89.9%	93.9%	95.2%	**93%**
SSH	85.8%	99.6%	99.6%	**95%**
TELNET	82.6%	91.6%	92.1%	**88.8%**

5. 결론 및 향후 과제

최근 IoT 서비스의 확장으로 인터넷에 연결되는 디바이스 수가 급격하게 증가하고 있다. 하지만 소형 IoT 디바이스는 기존의 PC, 서버 등이 사용되던 환경과는 다르게 보안 관리가 쉽지 않다. 소형 IoT 디바이스는 직접적으로 백신과 같은 보안 프로그램의 설치가 어렵고 방화벽 등의 네트워크 환경 보안도 부족하다. 또한 취약한 오픈소스 SW, Cut-down OS를 사용하여 많은 취약점을 가지고 있다. 취약한 소형 디바이스는 대규모 DDoS 등과 같은 사이버 공격에 사용될 수 있다. 이와 같은 공격을 예방하기 위해서는 취약점의 주기적인 관리가 필요하다.

본 논문에서는 인터넷에 연결된 디바이스의 취약점을 관리하는 시스템의 구조를 제안하였다. 현재 개발된 시스템은 다양한 환경에서 비교 테스트를 계속 진행하고 있다. 기존 Internet-Wide Scan 기술은 많은 디바이스 정보를 빠르게 수집하는 방법에 초점을 두고 발전 중이다. 취약점 분석 전문가들은 이런 스캔 기술을 활용한 'Shodan' 등에서 제공하는 정보를 통해 디바이스의 취약

점을 발견하고 있다. 제안하는 시스템은 사람이 직접 인터넷 스캔 결과를 활용해 취약점을 분석하는 과정을 자동화하여 사이버 공격을 사전에 빠르게 예방하기 위한 기술이다. 향후 개발 시스템의 스캔 성능, 취약점 분석 등의 기능을 개선하여 사이버 보안 위협 대응을 위해 사용할 것이다.

References

[1] "State of the IoT 2018: Number of IoT devices now at 7B", IoT Analytics. Available online: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (accessed August 15, 2019).

[2] Ziegeldorf JH, Morchon OG, Wehrle K., "Privacy in the Internet of Things: threats and?challenges", *Security and Communication Networks*, Vol.7, No.12, pp.2728-2742, Jun. 2014. DOI: https://doi.org/10.1002/sec.795

[3] Auffret P., "SinFP, unification of active and passive operating system fingerprinting", *Journal in Computer Virology*, Vol.6, No.3, pp.197-205, Aug. 2010. DOI: https://doi.org/10.1007/s11416-008-0107-z

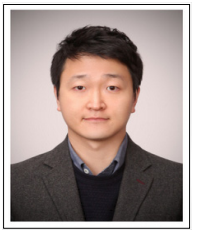
[4] Shamsi Z, Nandwani A, Leonard D, Loguinov D., "Hershel: single?packet OS fingerprinting.", *SIGMETRICS '14 The 2014 ACM international conference on Measurement and modeling of computer systems*, Vol.42, No.1, pp.195-206, June. 2014. DOI: https://dx.doi.org/10.1145/2591971.2591972

[5] Z. Durumeric, E. Wustrow, J. A. Halderman, "ZMap : Fast Internet-Wide Scanning and its Security Applications", *22nd USENIX conference on Security*, 2013.

[6] Anton V. Arzhakov, Irina F. Babalova, "Analysis of Current Internet Wide Scan Effectiveness", *Proceedings of 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, 2017. DOI: https://doi.org/10.1109/EIConRus.2017.7910503

[7] B. Genge, C. Enachescu, "ShoVAT: Shodan-based vulnerability assesment tool for Internet-facing services", Security & Communication Networks, 2015. DOI: https://doi.org/10.1002/sec.1262

김 태 은(Taeeun Kim) [정회원]



- 2005년 2월 : 백석대학교 정보통신학부 (공학사)
- 2007년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2007년 3월 ~ 현재 : 숭실대학교 컴퓨터공학과 박사과정
- 2013년 7월 ~ 현재 : 한국인터넷진흥원 책임연구원

〈관심분야〉
정보보안, 네트워크 보안, 융합 보안

정 용 훈(Yong Hoon Jung) [종신회원]

- 2006년 8월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2010년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2011년 3월 ~ 2014년 2월 : 서일대학교 조교수
- 2018년 8월 ~ 현재 : 바스랩 연구소장
- 현) 한국산학기술학회 상임이사

〈관심분야〉
네트워크 보안, 융합 보안

전 문 석(Moon-Seog Jun) [정회원]

- 1989년 2월 : University of Maryland Computer Science (공학박사)
- 1989년 3월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수

〈관심분야〉
네트워크 보안, 생체 인증