https://doi.org/10.33778/kcsa.2019.19.3.051

IoT 시대 기업 내부 네트워크의 가시성 확보를 위한 단말 식별 시스템 설계★

이 대 효*, 김 용 권**, 이 동 범**, 김 협***

요 약

본 논문에서는 사물인터넷(IoT) 시대의 안전한 기업 내부 네트워크 환경을 유지시키기 위하여 네트워크 가시성을 확보할 수 있는 단말 식별 시스템을 제안한다. 최근 기업 네트워크의 영역은 점점 더 넓어지고 복잡해지고 있다. 더 이상 데스크톱과 스마트폰뿐만 아니라 업무용 패드, 바코드스캐너, AP, Video Surveillance, 디지털 도어, 방범장치, 기타 IoT 장비 등 빠르게 증가하고 있으며, 이에 따라 보안위협 역시 증가하고 있다. 따라서 본 논문에서는 IoT 시대의 폭발적으로 증가하고 있는 단말을 식별할 수 있는 프로세스 및 모듈별 기능을 포함하는 단말 식별 시스템을 제안한다. 제안하는 시스템은 기업의 보안 관리자에게 다양한 단말의 정보 및 취약점 등을 제공하여 사내 네트워크에서 발생할 수 있는 잠재적인 사이버 위협뿐만 아니라 비즈니스 위협에 대응할 수 있는 종합적인 위협 관리 기능을 제공할 수 있다.

Device Identification System for Corporate Internal Network Visibility in IoT Era

Dae-Hyo Lee*, Yong-Kwon Kim**, Dong-Bum Lee**, Hyeob Kim***

ABSTRACT

In this paper, we propose a device identification system for network visibility that can maintain the secure internal net work environment in the IoT era. Recently, the area of enterprise network is getting huge and more complicated. Not only desktops and smartphones but also business pads, barcode scanners, APs, Video Surveillance, digital doors, security device s, and lots of Internet of Things (IoT) devices are rapidly pouring into the business network, and there are highly risk of security threats. Therefore, in this paper, we propose the device identification system that includes the process and module -specific functions to identify the exploding device in the IoT era. The proposed system provides in-depth visibility of the devices and their own vulnerabilities to the IT manager in company. These information help to mitigate the risk of the pot ential cyber security threats in the internal network and offer the unified security management against the business risks.

Key words : Device Identification System, Network Visibility, Enterprise Internal Network, IoT Security, BYOD

접수일(2019년 8월 13일), 수정일(1차: 2019년 9월 21일), 게재확정일(2019년 9월 26일)

★본 연구는 산업통상자원부 및 한국산업기술평가관리원의 산업기술혁신사업(우수기술연구센터(ATC))의 연구결과로 수행되었음(과제번호 : 10076453).

* GENIANS, INC. (주저자)
** GENIANS, INC. (공동저자)
*** GENIANS, INC. (교신저자)

1. 서 론

최근 정보통신기술(ICT, Information and Communications Technologies)의 발달로 일상생활에서 사물과 인터넷의 연결을 통한 다양한 서비스가 제공되고 있다. 현재 사물인터넷(IoT)은 다양한 분야에서 적용되고 있으며, 특히 기업 네트워크 환경에서 활발하게 사용되고 있다. IT 전문 시장조사 기관인 가트너(Gartner)는 2020년까지 260억 개 이상의 기기(단말)들이 상호 연결되어 다각적인 혁신과 사업기회가 기업에게 나타날 것이라고 전망하였다[1].

IoT 환경에서는 보다 많은 단말들이 다양한 통신방법으로 네트워킹에 참여하게 되며 상호간의 데이터 교환을 통하여 새로운 가치를 창출할 수 있게 된다. 하지만 다양한 이기종(heterogeneity) 단말 간의 유·무선 통신으로 사내 네트워크에서 발생할 수 있는 다각적인 보안 위협을 내포하고 있다[2,3]. 사내 네트워크의 영역은 더 넓어지고 복잡해지고 있다. 기업 네트워크는 더 이상 데스크톱과 스마트폰뿐만 아니라 업무용 패드, 바코드스캐너, AP(Access Point), Video Surveillance(IPTV 등), 디지털 도어, 방범장치, 기타 IoT(사물인터넷) 장비 등 빠르게 증가하고 있으며, 이에 따라 보안 위협 역시 증가하고 있다.

IoT 시대의 사이버 위협은 점차 고도화되어 가고 있으며, 복잡해지는 추세이다[4]. 이러한 기업 네트워크 환경에서의 사이버 위협을 쉽게 이해하고, 빠르게 대응하기 위해서는 네트워크의 가시성(Visibility)을 확보하고, 단말 식별의 개념을 제대로 이해하고 적용할 필요가 있다. 왜냐하면 폭발적으로 증가하는 단말 및 사용자로 인해 사내 네트워크의 가시성 확보가 사실상 어려운 환경으로 변하고 있기 때문이다. 또한 이렇게 증가하는 사이버 위협에 대한 우리의 대응은 한계가 존재하는 것이 사실이다.

본 논문에서는 네트워크 접근 제어(Network Access Control) 기술을 중심으로 기존 연구가 미비하였던 기업 네트워크 환경에서의 단말 가시성을 확보하고, 이를 통해 보안 관리자들이 보안 위협에 대응할 수 있는 단말 식별 시스템을 제안하고자 한다.

2. 관련 연구

2.1 IoT 시대의 네트워크 가시성(Visibility) 확보

최근 사물인터넷 환경은 다양한 산업 분야로 관련 기술 및 응용 범위가 확대되면서 빠른 속도로 진화하고 있다. 컴퓨터, 스마트폰, 태블릿 PC를 비롯하여 사물인터넷(IoT) 기기들의 연결은 불과 몇 년 사이에 큰 폭으로 증가되고 있다. 단말 증가에 따른 관리의 어려움과 동시에 관리되지 않은 단말의 잠재적인 보안위협 역시 크게 증가하고 있다. 이러한 상황에서 기업의 보안위협은 다양한 공격 대상과 유형으로 나타나고 있어, 기업 네트워크의 가시성 확보가 보안의 중요한 측면으로 강조되고 있다.

사물인터넷(IoT, Internet of Things)이란 통신, 계산 및 서비스 작업을 실현하기 위해 상호작용하고 협력할 수 있는 스마트 단말, RFID 태그, 자원이 제한적인 센서를 포함하는 모든 단말을 인터넷과 연결할 수 있는 기술이다[2,5,6]. 이러한 무선 전송 매체의 사용은 기존 무선 네트워크의 취약성을 내포하고 있어 위험성이 높으며, 지능형 지속 위협(APT) 등 보안위협에 따른 피해 규모는 보다 더욱 커질 것으로 전망된다[7]. 아래 표 1은 사물인터넷 환경에서의 보안위협을 세분화하여 정리한 것이다[8,9].

<표 1> 사물인터넷 관련 사내 보안위협

구분	세부내용
Application Program	인가되지 않은 서비스 및 사용자 접근, 데이터 위변조, 데이터의 기밀성 침해 등
Network	인증 방해, 정보유출, 서비스 거부, 데이터 위변조 등
Device	단말의 분실 및 물리적 파괴, 인가되지 않은 접근, 단말의 기밀성 및 무결성 침해 등

최근 들어 사물인터넷 환경에서의 기업은 사용자가 확인되지 않은 여러 단말 및 응용 프로그램을 광범위하게 실행할 수 있게 제작되었기 때문에 이를 식별할 수 있는 네트워크의 가시성 확보가 중요한 점으로 대두되고 있다[10]. 하지만 현재 기업 보안 관리자들은 네트워크 연결이 증가함에 따라 노출영역이 함께 확대되고, 다수의 IoT 기기는 저사양으로 별도의(임베디드 보안 기술 등)기술이 요구 되며, 개방형 플랫폼(리눅스 등) 기반 취약점 및 이를 이용한 공격이 용이하여 대응이 어려운 점 등을 겪고 있다.

글로벌 사이버 보안 기업인 트렌드마이크로(Trend Micro)는 2018년 보고서를 통하여 IoT 보안 위협에 대해 인식하고 있는 비율이 14% 이며, IoT 솔루션을 도입 및 운영하기 이전에 보안요구사항을 정의할 수 있는 비율은 37% 라고 기술하고 있다. 또한 기업에서 이루어지는 IoT 관련 공격의 절반이상(54%)이 사무실 기기를 대상으로 이루어지고 있다고 발표하였다.

(그림 1) IoT 보안위협 인식 조사(재인용)[13]

사내 비인가 단말을 통한 멀웨어(malware), 랜섬웨어(ransomware) 등 사내 자원의 탈취와 관련된 보안 위협들이 증가하고 있지만, 선행 연구에서는 위에서 기술한 위협에 대응할 수 있는 단말 식별 시스템에 관한 연구는 부족한 실정이다. 따라서 사물인터넷 환경에서 안전한 기업 네트워크의 유지를 위해 단말의 가시성을 확보할 수 있는 시스템 개발이 필요한 시점이다.

2.2 BYOD(Bring Your Own Device)와 기업 내부 네트워크 보안

ICT 기술이 발전함에 따라 많은 기업에서 직원들의 작업능력 및 업무효율성 향상, 편의성 증대를 지원하는 새로운 정책을 개발하기 시작하였다. 그러한 정책 중 하나가 바로 BYOD이다[3]. BYOD는 기업 콘텐츠 및 네트워크에 접근하기 위해 직원 소유의 단말을 업무에 활용하는 것이다[11].

기업은 BYOD 정책을 통해 업무효율을 높이고 비용을 절감하는 등 경제성, 개방성 및 다양성 측면에서 장점을 획득하였다. 하지만 이와 반대급부로 사내 네트워크에 다양한 단말을 통한 보안위협의 발생 가능성이 커진다. 직원들은 사무실뿐만 아니라 가정 등 기업 외부에서 단말을 사용하여 기업 내부 네트워크에 연결을 시도하거나 인가되지 않은 소프트웨어를 설치할 수 있다. 이 소프트웨어가 단말의 데이터를 탈취해 기업의 비밀정보가 범죄자의 불법적인 목적에 유출될 수 있어 기업 존속에 막대한 영향을 끼칠 수 있다. 이러한 위험성 때문에 일부 연구에서는 "Bring Your Own Danger" 로 불리기도 한다[12].

BYOD는 직원들의 업무효율성을 높여주었지만, 현재 기업 네트워크에 중대한 보안위협의 요소로 작용하고 있으며, 이를 식별하여 조치하는 것이 중요한 요인이 되고 있다.

3. 단말 식별 시스템 설계

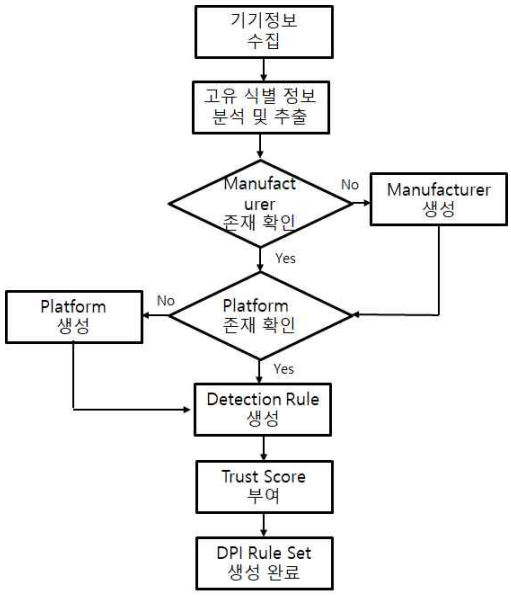
본 연구에서는 단말의 다양한 정보를 활용하여 기기 또는 단말을 식별하기 위한 시스템을 제안하고자 한다. 본 연구의 대상을 DPI(Device Platform Identification)으로 명명하였으며, 네트워크에 존재하거나 접속을 시도하는 다양한 단말의 정보를 수집 및 분석하여 단말을 식별, 분류하는 기술 및 시스템이다.

3.1 단말 식별 정책 도출 프로세스

본 연구에서는 Telnet, SNMP, MAC 등의 정보를 활용하여 기기 또는 단말을 식별하기 위한 식별 정책의 구성은 다음 표 2와 같으며, 개발 프로세스는 그림 2와 같다.

<표 2> 단말 식별 정책 구성

구분	내용
제조사 (Manufacturer)	기기 또는 단말에 대한 제조사를 식별할 수 있는 정보 그룹으로, Rule Set 생성 시 제일 먼저 고려되는 그룹
플랫폼 (Platform)	기기 또는 단말의 이름 및 정보를 식별할 수 있는 정보 그룹으로, 제조사 하위에 포함되는 그룹
탐지 규칙 (DR, Detection Rule)	기기 또는 단말을 식별하기 위한 Rule이 모여 있는 정보 그룹으로, 플랫폼 하위에 포함되는 그룹
신뢰도 점수 (Trust Score)	각각의 탐지 규칙에 부여되는 신뢰도 점수 그룹으로, 해당 점수가 높을수록 식별된 단말에 대한 정확도가 높음을 나타냄
취약점 정보 (CVE, CPE)	각 기기 또는 단말에 대한 CVE (Common Vulnerability & Exposure), CPE(Common Platform Enumeration)와 같은 취약점 정보가 매핑된 그룹으로, 플랫폼 하위에 포함되는 그룹



(그림 2) 단말 식별 정책 개발 프로세스

3.1.1 단말(기기) 정보 수집

단말 또는 기기 등 수집 대상으로부터 정보를 능동적 또는 수동적 방식으로 수집한다. 능동적 방법은 수집 대상에 패킷(Packet) 전송 등 작용 후 그 반작용을 수집, 관찰하는 방법이며 수동적 방법은 작용 없이 수집, 관찰하는 방법이다.

3.1.2 고유 식별 정보 분석 및 추출

수집된 정보에서 기기 또는 단말을 식별하기 위한 고유 식별 정보(Vendor, SNMP OID, MAC, SNMP Description, SMB OS, UPnP, Web Browser, DHCP, FTP, HTTP(S), DHCP 12 opt, FQDN, Telnet, Open port)를 기반으로 분석하여 추출한다.

3.1.3 제조사(Manufacturer) 존재 확인

3.1.2에서 분석된 고유 식별 정보에 해당되는 제조사가 존재하는지 확인하다. 만약 매치되는 제조사가 존재하지 않을 경우 신규로 생성한다.

3.1.4 플랫폼(Platform) 존재 확인

3.1.2에서 분석된 고유 식별 정보에 해당되는 플랫폼이 존재하는지 확인한다. 매핑되는 플랫폼이 존재하지 않을 경우 관련된 제조사에 신규로 생성한다.

3.1.5 탐지 규칙(Detection Rule) 생성

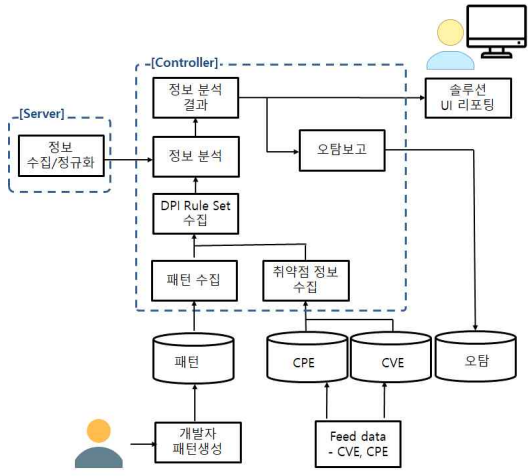
3.1.2에서 분석 및 추출된 고유 식별 정보를 기반으로 기기 또는 단말을 식별할 수 있는 탐지 규칙을 관련된 플랫폼에 생성한다.

3.1.6 신뢰도 점수(Trust Score) 부여

신뢰도 점수란 생성된 각각의 탐지 규칙에 부여하는 점수로, 높은 점수를 획득할수록 식별된 단말에 대한 정확도가 높다.

3.2 단말 식별 시스템 기능 설계

본 연구에서 DPI란 네트워크에 존재하거나 접속을 시도하는 다양한 단말의 정보를 수집 및 분석하여 단말을 식별하고 정확히 분류하는 기술 및 시스템을 의미한다. 이는 다음 그림 3과 같이 Server, Controller를 통해 기능이 동작한다.



(그림 3) 단말 식별 시스템 모듈별 기능 설계

3.2.1 서버(Server)

서버는 IoT 단말에서 정보를 수집하고, 정규화하여 컨트롤러로 전송하는 기능을 수행한다. 단말

정보 수집/정규화 모듈은 서버가 단말에서 정보를 수집하여 내부 정책에 따라 데이터를 정규화 하는 기능을 제공하는 모듈이다.

서버는 정보 수집 시 컨트롤러의 정책에 따라 능동적 수집 기능과 수동적 수집 기능으로 구분되며, 그 세부 내용은 표 3과 같다. 능동적 수집은 단말에 특정한 정보를 전송하고 회신되는 정보를 수집한다. 수동적 수집은 단말을 대상으로 어떤 정보도 전송하기 않고 서버로 전송되는 네트워크 트래픽을 분석하여 정보를 수집한다.

<표 3> 서버 수집 정보

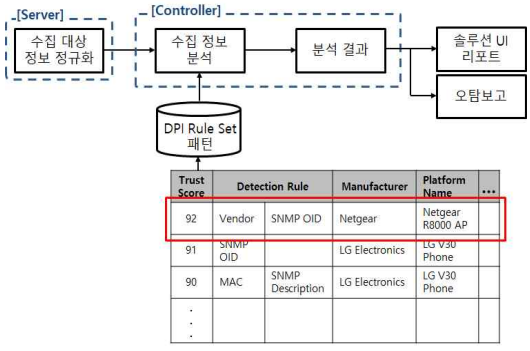
능동적 수집 정보 (Active Scan)	수동적 수집 정보 (Passive Scan)
FTP	FTP
Telnet	HTTP User-Agent
SNMP	SMTP
HTTP / HTTPS User-Agent	DHCP Fingerprinting
DHCP Fingerprinting	MAC Classification
MAC Classification	-
TCP Fingerprinting	-
Open Port	-
UPnP(Universal Plug & Play)	-
FQDN(Fully Qualified Domain Name)	-

3.2.2 컨트롤러(Controller)

컨트롤러(Controller)는 서버에서 수집한 기기 또는 단말의 정보패턴을 분석하여 기기 또는 단말을 식별하는 기능을 수행한다. 또한 정보 분석 모듈, 정보 분석 결과 모듈, DPI Rule Set 수집 모듈, 패턴 수집 모듈, 취약점 정보 수집 모듈로 구성되어 있다.

수집 정보 분석 모듈은 서버에서 전송된 수집 대상의 정보를 본 연구자들이 개발한 DPI Rule Set을 기반으로 매치하여 기기를 식별하는 기능을 제공하는 모듈이다.

다음 그림 4는 DPI Rule set을 통해 분석되는 프로세스를 도식화 한 것이다.



(그림 4) 수집정보 분석 프로세스

3.2.2.1 수집 대상 정보 정규화

서버에서 수집 대상 단말 또는 기기로부터 정보를 수집 및 정규화 하여 컨트롤러로 전송한다.

3.2.2.2 DPI Rule Set 정렬

본 연구자들이 개발한 DPI Rule Set에서 신뢰도 점수를 높은 순으로 정렬한다.

3.2.2.3 수집 정보 분석

3.2.1.1에서 수집된 정보와 3.2.1.2에서 정렬된 DPI Rule Set을 매치하여 수집 대상 단말 또는 기기의 정보를 분석한다. 매치 시 수집된 정보와 신뢰도 점수가 높은 순으로 탐지 규칙을 매치하며, 탐지 규칙이 모두 만족할 경우 해당 규칙과 매치된 플랫폼 이름으로 단말이 식별된다.

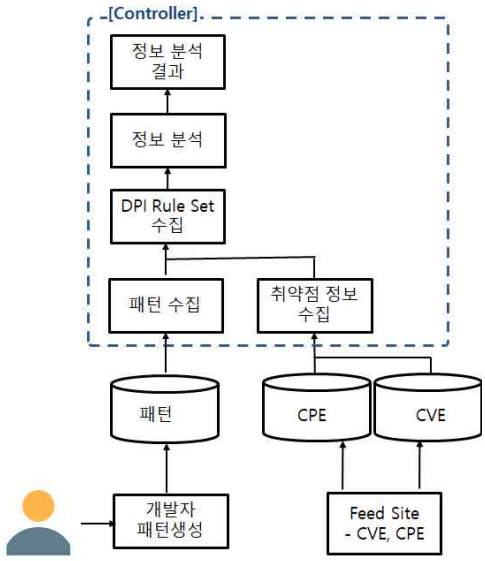
3.2.2.4 수집 정보 분석 결과

수집된 정보 분석 결과는 DPI Rule Set의 존재 여부에 따라 구분된다. DPI Rule Set이 존재하는 경우 일치하는 패턴에 명시된 이름(Platform Name)으로 기기가 식별되며, 관련된 기기 정보 및 취약점 정보를 솔루션 관리자 UI로 제공한다. 만약 일치하는 패턴을 찾지 못할 경우, 오탐 보고를 통해 오탐 보고 DB에

저장한다. 개발자는 저장된 오탐 보고를 기반으로 신규 DPI Rule Set을 개발한다.

3.2.2.5 DPI Rule Set 수집

DPI Rule Set 수집은 수집 대상 기기를 식별 및 분석할 수 있는 패턴 수집 및 취약점 정보를 수집하는 모듈로 아래 그림 5에서 컨트롤러(Controller)의 DPI Rule Set 수집 절차를 나타낸다.



(그림 5) 컨트롤러의 DPI Rule Set 수집 절차

패턴 수집 모듈은 연구자들이 개발한 DPI Rule Set를 수집하는 모듈로, 수집 대상 기기 또는 단말을 식별 및 분석하기 위한 패턴을 수집한다. DB에 저장된 패턴은 컨트롤러에서 주기적으로 동기화 작업을 통해 업데이트 한다.

취약점 정보 수집 모듈은 CVE 사이트에서 주기적으로 취약점 정보(CVE) 및 공통 플랫폼 목록(CPE) 정보를 수집하여 DB에 저장하며, 컨트롤러에서 주기적으로 동기화 작업을 통해 업데이트 한다.

마지막으로 수집된 취약점 정보를 통해 분석된 수집 대상 단말 또는 기기와 매치하여 취약점 정보를 제공한다.

4. 단말 식별 시스템 구현

4.1 단말 식별 시스템 제공 정보

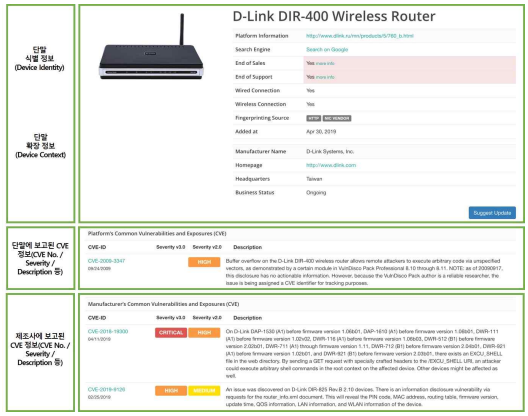
본 연구에서 설계된 시스템은 다음과 같은 단말의 관련 정보를 제공할 수 있다. 이를 정리하면 표 4와 같다.

<표 4> 단말 식별 시스템 제공 정보

구분	세부 정보
단말 식별 정보 (Device Identity)	-단말 제조사, 이름, 모델번호 -단말 사진 -네트워크 연결 방식(유선/무선) -단말 상세 정보 URL
단말 확장 정보 (Device Context)	-제조사 명칭 -제조사 홈페이지 URL -본사의 위치와 현재 사업 진행 여부 -제품 판매 종료(End of Sales) 여부 -제품 지원 종료(End of Support) 여부 -검색엔진 연결 URL
단말 위협 정보 (Device Risk)	-단말에 보고된 CVE 정보(CVE No. / Severity / Description 등) -제조사에 보고된 CVE 정보(CVE No. / Severity / Description 등)

4.2 단말 식별 시스템 관리자 UI 구현

본 연구에서 제안하는 시스템의 관리자 UI는 다음 그림 6과 같다.



(그림 6) 관리자 UI 구현 화면

4.3 기존 시스템과의 단말 식별결과 비교분석

본 연구에서 제안하는 시스템을 통한 단말 식별 결과를 핑거뱅크의 결과와 비교하였다. 핑거뱅크(Fingerbank, https://api.fingerbank.org)는 네트워크에 접속된 단말의 탐지와 정확한 식별을 위해 사용되는 시스템으로 Cisco, Nokia 등 다양한 기업에서 활용하고 있다. 핑거뱅크는 단말의 식별 및 탐지를 위하여 주로 DHCP fingerprinting 정보와 User-Agent 정보를 사용한다. Cisco, Meraki 등 AP(Access Control) 업체와의 협업 등을 주요 성공사례로 소개하고 있으며, 호텔 및 카페 등의 Guest WLAN 등에 해당 기술을 주로 활용하고 있다.

아래의 표 5는 DPI에서 식별 가능한 다양한 단말 중 전 세계적으로 5,500만대 이상 판매된 Samsung Galaxy S7을 기준으로 핑거뱅크와의 식별결과를 비교 및 분석한 내용이다.

<표 5> 제안 시스템(DPI)과 핑거뱅크 식별결과 비교

구분	DPI	핑거뱅크
탐지 근거	HTTP user-agent / MAC / NIC vendor / UPNP / DHCP / Hostname	MAC(OUI) / DHCP / HTTP user-agent
단말 식별 정보	제공 (Samsung Galaxy S7 phone)	부분 제공 (Galaxy S7)
단말 확장 정보	제공 (제조사 및 홈페이지 등)	미 제공
단말 위협 정보	제공 (CVE No. 등)	미 제공
사용 대상	B2B	B2C
사용 목적	자산 및 보안관리	통계 및 유관 서비스 제공
실제 탐지 내용		

위 표의 내용을 살펴보면 DPI가 핑거뱅크보다 상세한 탐지정보 및 부가정보를 제공하는 것을 확인할 수 있다. 이러한 결과 차이는 탐지 근거의 차이에 기인한 것으로 판단된다. 더불어 사용 대상 및 목적에 따라 결과의 편차가 발생할 수 있으나 본 연구의 대상이 기업 내 또는 기업 간 안전한 네트워크의 가시성을 확보할 목적으로 활용된다는 점에서는 DPI의 활용도가 더 높은 시스템이라 할 수 있다.

5. 결론 및 시사점

5.1 결론

본 연구에서는 사물인터넷 시대의 안전한 기업 네트워크를 유지하기 위한 단말 식별 시스템을 제안하였다. 기업 네트워크에 존재하거나 접속을 시도하는 다양한 이기종의 단말 정보를 수집하고 분석하였다. 이를 세분화하여 정리하면 다음과 같다.

첫째, 네트워크상의 다양한 단말로부터 능동적 또는 수동적으로 정보를 수집하는 프로세스를 정규화 하였다. 둘째, 정규화된 정보에 대하여 설정이 완료된 분석 규칙에 따라 분류한 후 신뢰도 점수를 부여하여 패턴을 분석하는 방법을 개발하였다. 마지막으로 패턴 분석의 결과에 기초하여 단말들의 식별 정보 및 위협 정보를 출력하는 단말 식별 시스템을 구현하고 분석하였다.

5.2 시사점 및 향후 연구

본 연구에서 구현된 단말 식별 시스템은 보안관리자에게 다음과 같은 시사점을 제공할 수 있다.

첫째, 기업 네트워크에 존재하는 다양한 단말 중 CVE 정보를 통하여 취약성이 보고된 단말 만을 빠르게 찾아 조치할 수 있다.

둘째, 제품 수명주기 관리(Life-cycle Management) 측면에서 판매가 중단되었거나(End Of Sales), 지원이 중단된(End Of Support) 단말을 찾아 업그레이드 및 교체 계획을 수립할 수 있다. CCTV와 같이 외형이 비슷하거나 제조사가 다양한 단말에 대하여 사진을 통해 정확히 대상을 인식할 수 있다. 비즈니스 위협 측면에서는 제조사의 사업 진행 계속 여부나 폐업 등의 정보를 확인하여 구매계획을 수립하는데 도움을 줄 수 있다.

셋째, SVA(Scan-less Vulnerability Assessm

ent) 측면으로 사내 네트워크에서 발생 가능한 잠재적인 위협 및 보안 사고를 사전에 예방할 수 있다. IoT 기기가 보유한 취약점을 별도의 스캔 없이 확인하고 대응할 수 있다. 제안된 시스템은 별도의 스캐너가 필요하지 않으며, 스캐닝으로 인한 네트워크 부하가 발생하지 않는 장점이 있다.

마지막으로 최근 사내 네트워크는 OA(IT)와 IoT가 혼용되어 운용되는데 DPI를 통해 OA와 IoT 기기를 정확히 분류할 수 있다. 이를 통해 네트워크를 분리하여 운영하는 것이 가능할 것이다.

보안관리자에게 다양한 단말 또는 기기의 정보 및 취약점 등을 제공하여 사내 네트워크에서 발생할 수 있는 잠재적인 사이버 위협뿐만 아니라 비즈니스 위협에 대응할 수 있는 종합적인 위협관리 기능을 제공할 수 있을 것이다.

향후 연구에서는 단말 식별 시스템에서 수집된 정보를 분석하여 DPI Rule Set을 고도화시키고, CVE, CPE와 같은 취약점 정보를 확장시키는 연구가 필요하다. 또한 식별 패턴을 클라우드(웹)에서 조회하여 단말을 식별할 수 있는 클라우드 기반의 단말 식별 시스템으로 확장할 수 있을 것이다.

감사의 글

본 연구는 산업통상자원부 및 한국산업기술평가관리원의 산업기술혁신사업(우수기술연구센터(ATC))의 연구결과로 수행되었음(과제번호 : 10076453).

참고문헌

[1] Gartner, “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020”, http://www.gartner.com/newsroom/id/2636073. Accessed 31 July 2019, 2011.

[2] Zhou, L., & Chao, H. C, “Multimedia traffic security architecture for the internet of things”, IEEE Network, Vol.25, No.3, pp.35-40, 2011.

[3] Shaji, R. S., Dev, V. S., & Brindha, T. “A methodological review on attack and defense strategies in cyber warfare”, Wireless Networks, Vol.25, No.6, pp.3323-3334, 2019.

[4] Park, W., Na, O., & Chang, H, “An exploratory research on advanced smart media security design for sustainable intelligence information system”, Multimedia Tools and Applications, Vol.75, No.11, pp.6059-6070, 2016.

[5] Atzori, L., Iera, A., & Morabito, G, “The internet of things: A survey”, Computer networks, Vol.54, No.15, pp.2787-2805, 2010.

[6] Kim, H., Kwon, H., & Kim, K. K, “Modified cyber kill chain model for multimedia service environments”, Multimedia Tools and Applications, Vol.78, No.3, pp.3153-3170, 2019.

[7] 전정훈, “사물 인터넷의 보안 위협 요인들에 대한 분석”, 융합보안논문지, 제15권, 제7호, pp.47-53, 2015.

[8] 최관, 김민지, “기업의 산업기밀정보 유출예방에 관한 연구: 사물인터넷 활용을 중심으로”, 융합보안논문지, 제17권, 제5호, pp.101-110, 2017.

[9] 한슬기, 김명주. “사물인터넷 기기 보안평가를 위한 기술요소 기반의 모델 설계 및 체크리스트 적용”, 융합보안논문지, 제18권, 제2호, pp.49-58, 2018.

[10] Cox, G, "Managing the risks of shadow IoT", Network Security, pp.14-17, 2019.

[11] Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A, "A review of bring your own device on security issues", Sage Open, pp.1-11, 2015.

[12] Disterer, G., & Kleiner, C, "BYOD bring your own device", Procedia Technology, Vol.9, pp.43-53, 2013.

[13] Trend Micro, “Trend Micro Research Finds Major Lack of IoT Security Awareness”, https://newsroom.trendmicro.com/press-release/commercial/trend-micro-research-finds-major-lack-iot-security-awareness. Accessed 31 July 2019, 2018.

[저 자 소 개]

이 대 효 (Dae-Hyo Lee)

2000년 2월 안양대학교
컴퓨터공학 학사
2009년 2월 성균관대학교 대학원
이동통신공학 석사
2012년 2월 KAIST 대학원
경영학(MBA) 석사
1999년 8월 ㈜어울림정보기술
2005년 3월 ㈜안랩
2009년 3월 ~ 현재
GENIANS, INC. 전략기획실 실장
email : dado@genians.com

김 용 권 (Yong-Kwon Kim)

1997년 2월 명지대학교
전자공학 학사
1999년 7월 ㈜어울림정보기술
2005년 2월 ~ 현재
GENIANS, INC. DevOps실 실장
email : kimpd@genians.com

이 동 범 (Dong-Bum Lee)

1995년 2월 성균관대학교
정보공학 학사
1995년 3월 두산정보통신(주)
1998년 1월 ㈜어울림정보기술
2005년 1월 ~ 현재
GENIANS, INC. 대표이사
email : dblee@genians.com

김 협 (Hyeob Kim)

2010년 2월 연세대학교
문헌정보학 학사
2014년 2월 연세대학교
정보시스템학 석사
2018년 8월 연세대학교
정보시스템학 박사
2014년 3월 ~ 현재 GENIANS, INC.
email : hyubiii@genians.com