IoT 디바이스의 보안 관제 설계를 위한 공개 보안 도구의 유형 및 적용 방안 분석

정준영○ 김병선 조진성

경희대학교 컴퓨터공학과

jjy920517@khu.ac.kr, ykbs0903@khu.ac.kr, chojs@khu.ac.kr

An Analysis on Types and Application of Public Security Tools for IoT Device Security Control Design

Junyoung Jung○ Byoungseon Kim Jinsung Cho

Department of Computer Science and Engineering

KyungHee University

요 약

IoT 디바이스들은 대부분 보안 이슈를 크게 고려하지 않고 제작되기 때문에 해킹, 웜 바이러스 등의 침해 사고에 항상 노출되어 있다. 이에 따라 IoT 환경 내 각 디바이스의 효과적 보안 침해 대응 및 다양한 보안 관제 기능을 제공할 수 있는 디바이스 보안 관제 시스템 적용이 필요하다. 이러한 보안 관제 설계를 위해서는 디바이스 취약점과 이상행위에 대한 충분한 사전 분석 및 검토가 기본적으로 선행되어야 한다. 본 논문에서 IoT 디바이스 보안 관제 설계를 위한 공개 보안 도구들의 유형 및 기능 분석을 수행하였고, 이를 통한 보안 도구들의 적용 방안을 분석한다.

1. 서 론

최근 IoT(Internet of Things) 시대의 도래와 함께 다양한 IoT 서비스 및 수많은 IoT 디바이스들의 출시가 가속화되고 있다. 하지만, 이러한 제조/개발 기업들의 성장 중심의 개발 집중화는 디바이스 보안 이슈를 크게 고려하지 않는 원인이 되었다. 이러한 원인은 IoT 디바이스에 보안 약점, 잠재적 보안 취약점으로 작용하여 해킹, 웜 바이러스, 프라이버시 침해, 제어 불능 등의 다양한 보안 위협을 심화시키고 있다[1].

실제로 최신 해킹 기법 및 이슈를 다루는 글로벌 보안 컨퍼런스 블랙햇(Black Hat) 2014에서는 자동차, 항공기, 가전, 의료기기에 대한 해킹 시연을 통해 주변의 모든 IoT 디바이스에 대한 해킹 가능성을 알렸다[2]. 또한, 2014년 정보보안업체 프루프포인트(Proofpoint)는 스마트TV, 냉장고, 홈 네트워크 라우터와 같은 약 10만개의 가전제품이 씽봇(Thingbot)이 되어 75만건 이상의 피싱/스팸 메일을 발송하는데 사용되었다고 밝혔다[3].

위 사례들은 결과적으로, 보안 기술의 충분한 검토 및 적용이 안 된 IoT 디바이스의 확산에 대한 위험성 및 보안 관제의 필요성을 시사한다. 이를 인지한 국제·국내 표준화 단체 및 정부 기관들은 IoT 디바이스 및 서비스의 보안 요구사항들을 제시하였다. 특히, 국내 미래창조과학부에서는 IoT 사이버 위협에 대응하기 위한 보안 관제 시스템 설계와 구축을 목표로 “사물인터넷 정보보호 로드맵”을 시행하고 있다[4].

한편 이러한 보안 관제 시스템의 효율적 설계를 위해서는 IoT 디바이스의 취약점과 이상행위에 대한 충분한 분석과 검토가 기본적으로 선행되어야 한다[5]. 이러한 작업을 지원하기 위해 다양한 보안 도구들이 존재하고 있지만, 각 도구들은 분석 범위와 제공 기능이 상이하여 목적에 따른 적절한 분석 및 탐지 도구를 선택하는 것이 중요하다.

본 논문에서는 먼저, 보안 도구로써 공개된 취약점 및 이상행위 탐지 도구들의 유형 및 기능 분석을 수행하였다. 또한, 분석 결과를 기반으로 IoT 디바이스 보안 관제 설계 시 기술 분야에 따른 보안 도구들의 적용 방안을 제시한다.

논문의 목차는 다음과 같다. 2장에서는 공개 취약점 분석 도구와 이상행위 탐지 도구에 대한 유형 및 기능을 소개한다. 3장에서는 IoT 디바이스 보안 관제 기술 분야에 따른 보안 도구들의 적용 방안을 기술하고, 4장에서는 결론을 맺는다.

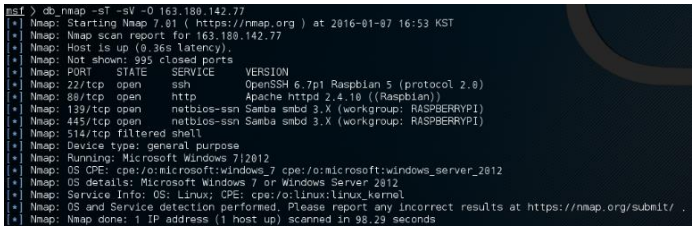
2. 공개 보안 도구 분석

2.1 취약점 분석 도구

취약점 분석은 보안 위협의 원인이 되는 디바이스의 취약 정보를 사전에 파악하기 위해 시스템 설계, 구현, 운영, 관리 측면에서의 취약점 존재 여부를 확인하는 작업을 의미한다. 이러한 작업을 위해 다양한 취약점 도구들이 존재하며, 본 장에서는 취약점 분석 도구의 목적별 분류 및 특징을

	도구명	역할(목적)
수동적 점검	nmap	포트 스캐닝
	OpenVAS	정보 수집
	John the Ripper	패스워드 점검
	Yasca	소스코드 분석
능동적 점검	Metasploit Framework	정보수집, 취약점 침투
	Inguma	정보수집, 취약점 침투
	SET	취약점 침투
	Aircrack-ng	WPA/WPA2-PSK크랙

[표 1] 취약점 분석 도구 분류



[그림 1] nmap을 이용한 타겟 포트 정보 수집 결과

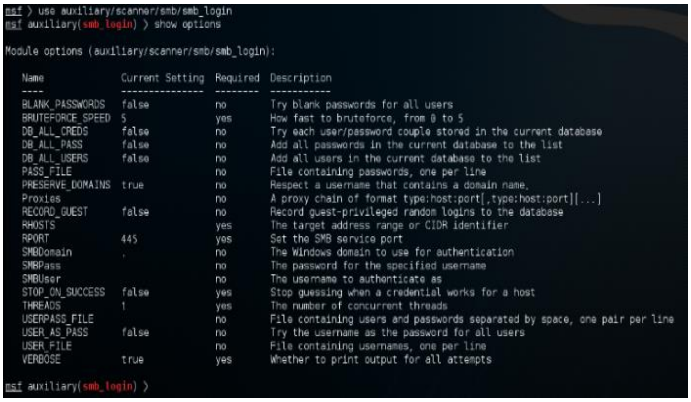
분석하였다.

[표 1]은 능동적/수동적 점검 방식에 따른 취약점 분석 도구들을 나타낸다. 수동적 점검은 시스템의 주요 파일이나 설정 사항의 점검을 통해 취약점을 찾는 방식이다. 수동적 점검의 예로는 시스템의 개방된 네트워크 포트를 체크하거나, 패스워드 파일의 보호 여부를 체크하는 방법 등이 있다. 능동적 점검은 모의 침투(exploit)를 통해 시스템의 취약점을 점검하는 방식이다. 이러한 침투 방식에는 무차별 대입 공격과 사회공학적 기법을 이용한 모의침투 등이 존재한다. 일반적으로 취약점 분석 도구들은 한가지의 도구를 단독적으로 사용하기보단 목적에 맞게 다양한 도구를 함께 사용한다. 즉, 수동적 점검 도구를 통해 시스템의 취약점을 예측한 후 능동적 점검 도구를 통해 예측된 취약점을 검증한다.

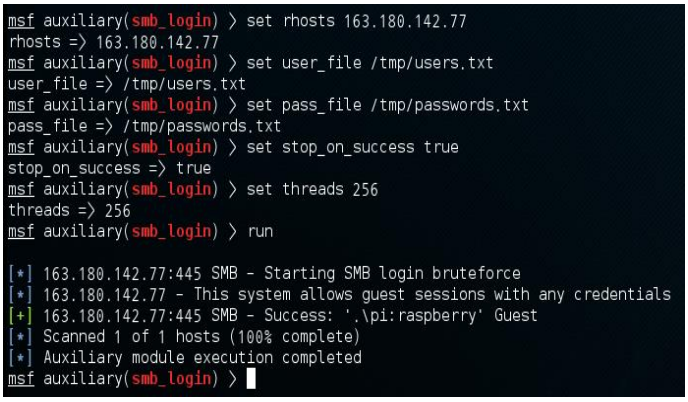
취약점 도구를 통한 모의 침투 시연에서는 COTS IoT 디바이스로 많이 활용되고 있는 Raspberry Pi model A(OS: Raspbian 8)를 타겟 디바이스로 사용하였다. 침투를 실행할 컴퓨터에 nmap을 설치하여 타겟 디바이스 정보를 수집한 후, MSF(Metasploit Framework)을 통한 취약점 분석을 수행한다.

nmap(v7.12)은 호스트나 네트워크를 스캐닝 할 때 사용되는 오픈 소스 분석 도구이며, 스캐닝한 시스템의 OS, 장치 종류, 서비스 버전, 방화벽 유/무 등을 파악하는 목적으로 활용된다. MSF(v4.11.5-2015121501)는 다양한 모듈을 사용하여 모의 침투를 할 수 있는 오픈 소스 취약점 분석 도구이며, 1517개의 침투 기능(exploits) 및 256개의 보조기능(auxiliary)을 통해 다양한 취약점을 이용한 침투와 정보를 수집할 수 있다.

일반적인 MSF의 모의 침투 수행은 총 4단계(정보수집, 모듈 로드, 옵션 설정, 공격 수행)로 구성된다. 먼저, '정보수집'에서는 nmap을 이용하여 [그림 1]와 같이 타겟의



[그림 2] MSF에서 모듈을 로드한 결과



[그림 3] 모듈 옵션을 설정하여 exploit에 성공한 화면

포트 정보를 수집하였다. 수집 결과를 통해 타겟 디바이스는 삼바(Samba; SMB 프로토콜)를 이용하고 있다는 것을 파악할 수 있으며, 파악된 정보를 토대로 침투에 사용할 모듈을 선택한다. 모듈의 선택은 RAPID7에서 제공하는 취약점 코드사전 (www.rapid7.com/db)를 통해 검색 가능하며, 본 연구에서는 SMB 프로토콜을 이용한 무차별 대입 모듈인 auxiliary/scanner/smb/smb_login을 사용하였다.

모듈 선택 후, [그림 2]과 같이 MSF에서 해당 모듈을 로드 후하고 옵션(타겟의 IP, User ID/PW 리스트)을 설정한다. 옵션 설정 후 침투(exploit)에 성공하였을 경우, [그림 3]와 같은 결과를 확인할 수 있다. 이러한 결과를 토대로 해당 디바이스는 SMB 프로토콜과 관련된 취약점이 존재하고 있으며, 포트스캐닝과 무차별 대입 공격에 안전하지 않다는 것을 파악할 수 있다.

2.2 이상행위 탐지 도구

이상행위 탐지 도구는 디바이스 내에서 동작하며 기존 시스템과 상이한, 사용자 접근이나 프로세스의 실행을 분석하여, 시스템 침해 사고에 대한 재빠른 대응과 피해 복구를 제공하기 위한 목적으로 활용된다. 또한, IoT 디바이스의 시스템 점검 기능을 수행한다. 대표적인 이상행위 탐지 도구는 [표 2]와 같다. 이 도구들은 특정한 한 개의 도구를 전적으로 신뢰하는 것은 매우 위험하기 때문에 복수개의 도구를 사용하는 것이 바람직하다.

기 능	도구명
파일 무결성 점검	Tripwire
	COPS
시스템 침입 흔적 조사	lsof
	chkrootkit
로그 분석	pacct

[표 2] 이상행위 탐지 도구 분류

Tripwire는 시스템에 설치된 후, 파일 속성, 접근 시간, 소유자 등의 데이터로 만든 정책에 따라 Linux 시스템 정보를 DB에 저장한다. 이 DB는 기준 DB가 되어, 차후 Tripwire 실행을 통해 새롭게 생성된 DB와 비교를 하게 된다. 비교 결과 기준 DB와 새로운 DB의 차이가 있다면 이 시스템의 파일이 변경되었다는 것을 알 수 있다.

lsof는 디렉토리나 파일시스템 내부의 특정파일을 사용하는 프로세스 확인, 특정 데몬/프로세스/유저가 사용하고 있는 파일 확인, 소켓 확인, 로그인 추적 등의 기능을 수행한다. 이 기능들을 사용하여 얻은 정보를 통해 관리자는 시스템 침입 흔적을 조사할 수 있다.

마지막으로 pacct는 사용자들의 접속시간, 이전 수행된 모든 명령어, 소프트웨어 입출력 수행시간, CPU 시간 등과 관련된 통계를 알 수 있는 도구이다. 이 도구를 사용하면 IoT 디바이스가 침투 당했을 경우, 신속하게 공격자가 수행한 정보를 알아 내어 대응할 수 있다.

이외에도 이상행위가 탐지되면 알림을 통해 관리자에게 안내를 해주는 도구, 비정상적인 권한의 변화를 감시하는 도구, 시스템의 패치 유·무를 점검하는 도구 등 다양한 이상행위 탐지 도구가 존재한다. 이러한 도구들을 사용하면 IoT 디바이스의 침해사고 모니터링과 대응이 가능하다.

3. IoT 디바이스 보안 관제 설계를 위한 보안 도구 적용 방안

IoT 디바이스 보안 관제는 아래와 같이 분야별 다양한 기술들이 존재하며, 적절한 보안 도구를 활용하여 분석 및 검토되어야 한다.

- ***저사양 디바이스의 특성을 반영한 경량 보안기술(백신, 암호화, 인증 등)***: 디바이스 타입, 운영체제, S/W 버전 등의 기본 시스템 정보는 OpenVAS와 MSF의 보조기능을 통해 수집할 수 있다. 또한, Yasca와 lsof를 활용하여 기존 기술의 소스코드 취약점 분석, 포트 점검을 수행할 수 있다.
- ***디바이스의 신뢰성 보장과 무결성 검증을 위한 센서/디바이스 보안패치 적용 기술***: tripwire, COPS 도구를 사용하여 디바이스 내 파일 무결성 검증 수행할 수 있으며, 이를 통한 신속한 보안패치가 가능하다.
- ***이기종 통신 네트워크 환경에 적합한 보안 기술***: IoT 디바이스는 WiFi, Bluetooth, NFC와 같은 이기종 통신 네트워크와 연결되어 사용된다. 따라서 Aircrack-ng를 사용하여 디바이스가 연결된 WiFi 네트워크의 안전성 검증을 해야 한다. Bluetooth, NFC 네트워크의 안전성 검증은 각각 bluesnarfer, mfoc를 통해 가능하다.
- ***안전한 개방형 플랫폼 이용 지침을 기반으로 한 디바이스/사용자 간 상호인증 키/신뢰 관리 기술***: 개방형 플랫폼의 취약점을 이용한 디바이스-서비스 간 허위 데이터 전송 등의 공격이 발생할 수 있다. 따라서 lsof를 통해 실행 중인 서비스가 참조하는 파일에 대한 정보와 특정 포트를 사용하는 서비스의 정보를 파악하여 대응할 수 있다.
- ***디바이스의 개인 정보 수집/추적 방지 및 개인 식별 정보 필터링 기술***: 디바이스가 수집한 정보의 중앙 집중 및 조합으로 사용자 신원 정보가 유출될 위협이 발생할 수 있다. 정보 유출을 판단하기 위해 losf와 pacct를 통한 특정 포트를 사용하는 프로세스 점검, 수행된 명령어 확인이 필요하다. 또한, 수집된 정보의 암호화는 John the Ripper를 이용하여 점검할 수 있다.
- ***대규모 기기, 네트워크에 대한 보안 상태 모니터링 및 감시 기술***: 가전, 의료기기 등 대규모 디바이스에 악성코드를 감염시켜 트래픽 폭증 공격을 하는 위협이 발생할 수 있다[2][3]. 따라서 2장에서 설명한 도구들을 통해 전체적인 점검이 필요하며 특히, 사회공학적 기법을 이용한 SET를 통해 특수한 목적으로 사용되는 IoT 디바이스의 취약점 분석이 가능하다.

4. 결론 및 향후 연구

본 논문에서는 취약점 분석 도구와 이상행위 탐지 도구의 유형을 조사 및 분석하였고 이 도구들의 기능이 IoT 디바이스 보안 관제 시스템에서 어떻게 활용될 수 있을지를 기술하였다. 향후 연구에서는 더 많은 도구를 사용 후 분석하여, IoT 디바이스에 최적화된 분석 도구를 개발할 예정이다. 최종적으로 이러한 분석도구를 이용하여 IoT 디바이스의 보안 안전성 검증을 할 수 있는 보안 관제 프로세스를 정립할 계획이다.

* “본 연구는 미래창조과학부 및 정보통신기술진흥센터(IITP)에서 지원하는 서울어코드활성화지원사업의 연구결과로 수행되었음” (R0613-16-1203)

참고 문헌

[1] 미래창조과학부, 세계최고의 스마트 안심국가 실현을 위한 사물인터넷(IoT) 정보보호 로드맵, p8, 2014

[2] Blackhat, https://www.blackhat.com/us-14/archi ves.html#cyber security-as-realpolitik

[3] Proofpoint, https://www.proofpoint.com/us/proof point-uncover s-internet-things-iot-cyberattack

[4] 미래창조과학부, 세계최고의 스마트 안심국가 실현을 위한 사물인터넷(IoT) 정보보호 로드맵, p23, 2014

[5] 김영진, 이수연, 권헌영, 임종인, 국가 전산망 보안관제업무의 효율적 수행방안에 대한 연구, 정보보호학회논문지, 19(1), p103-111, 2009