Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.3, Jun. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.3.537

사물인터넷 기기 침해사고 데이터 수집 방안 연구*

이 종 범,[1†] 엄 익 채[2‡]
[1,2]전남대학교 시스템보안연구센터 (대학원생, 교수)

A Study on Data Acquisition of IoT Devices Intrusion*

Jong-bum Lee,[1†] Ieck-Chae Euom[2‡]
[1,2]System Security Research Center in Chonnam National University
(Graduate student, Professor)

요 약

사물인터넷(Internet of Things)기술이 발전함에 따라 다양한 분야에서 사물인터넷 기기를 활용하고 있다. 하지만 이는 새로운 사이버 공격 표면이 되었고 기존 사이버 침해사고를 염두하지 않았던 산업까지 영향을 미치는중이다. 침해사고 발생 이후 사후처리, 피해확산 방지 등이 중요하지만 이에 관련된 표준이나 가이드라인이 부족하여 대응하기 어려운 현황이다. 따라서 본 논문에서는 이러한 침해사고 대응을 위해 침해사고 데이터 수집 절차를 정립하고 수집 가능한 데이터를 제시하여 범용적인 사물인터넷 기기의 침해사고 데이터 수집 방안을 개선하였다. 또한 실험을 통해 데이터 수집 절차의 효율성과 타당성을 증명하였다.

ABSTRACT

As Internet of Things (IoT) technology evolves, IoT devices are being utilized in a variety of fields. However, it has become a new surface of cyber attacks and is affecting industries that did not previously consider cyber breaches. After a intrusion occurs, post-processing and damage spread prevention are important, but it is difficult to respond due to the lack of standards and guidelines. Therefore, in order to respond to such incidents, this paper establishes an incident data collection procedure and presents the data that can be collected to improve the intrusion data acquisition method for general IoT devices. In addition, we proved the efficiency and feasibility of the data collection procedure through experiments.

Keywords: IoT, Forensics, Acquisition, Intrusion, Procedure

I. 서 론

사물인터넷은 현재 우리 주변 차량, 집, 공공, 산업 등 여러 분야에서 활용될 뿐만 아니라 일상생활에서 빠질 수 없는 필수 요소가 되었다. 하지만 대부분의 사물인터넷 기기가 한번 설치되면 수년, 수십 년 동안 별도의 교체 없이 사용되고 또한 사용량이 급격히 증가함에 따라 사물인터넷의 보안 위협이 각종 분야에 상속되며 침해사고의 피해 또한 증가하고 있다[1].

특히 사물인터넷 기기의 대부분은 리눅스(Linux) 기반 OS를 사용하고 있으므로 악성코드에 쉽게 감염되는 특성을 보인다. 공격자는 이를 통해 손쉽게 사물인터넷 기기에 악성코드를 감염시키고 네트워크 내 다른 기기들 또한 전파하여 최종적으로 봇넷을 구축하고 사용자들에 피해를 준다.

Received(03. 13. 2023), Modified(05. 08. 2023), Accepted(05. 08. 2023)
* "이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임"(IITP-2022-0-01203)
* 본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No.2106061)
† 주저자, znsfisn1595@gmail.com
‡ 교신저자, iceuom@jnu.ac.kr(Corresponding author)

사물인터넷 기기 관련 대표적 침해사고인 미라이(mirai) 봇넷은 최고 감염 기기 수가 약 60만대로 대부분 취약한 암호를 사용하는 사물인터넷 기기를 대상으로 발생한 멀웨어이다. 미라이 봇넷에 감염된 사물인터넷 기기는 특정 사이트의 서비스를 가용하지 못하도록 할 수 있으며 파급력이 상당했던 멀웨어이지만 해당 멀웨어는 오픈소스로 공개되었을 뿐만 아니라 멀웨어 코드의 재사용성 또한 높아 미라이 봇넷을 바탕으로 다양한 변종 멀웨어가 개발되어 침해사고를 발생시키는 중이다.

미라이 봇넷은 최근에도 활동 중으로 2022년 10월 마인크래프트(Minecraft) 서버인 Wynncraft에 2.5T bps 수준의 서비스 거부 공격을 약 2분 동안 지속하였으며 비트 레이트 관점에서 보았을 때 가장 큰 공격이라고 밝혔다.

이렇듯 사물인터넷 기기에 침해사고가 발생하면 기기 용도에 따라 금전적 피해, 개인정보 유출 등 다양하고 큰 피해가 발생할 수 있다. 하지만 이러한 침해사고 관련 대응책, 표준 등이 명확하지 않으며 이로 인해 침해사고 발생 시 대처하기 어렵다. 또한, 사물인터넷 기기는 메모리 및 처리능력이 제한되어있어 기기 간 통신을 캡처, 모니터링 및 분석하기 어렵다.

따라서 본 논문에서는 국내외 침해사고 대응 절차 및 관련 연구와 사물인터넷 기기의 특성을 고려한 하드웨어 기반 사물인터넷 기기 침해사고 데이터 수집 방법 및 절차를 제시한다.

II. 관련 연구

2.1 사물인터넷 기기 침해사고 사례

2016년 테슬라(TESLA)의 스마트폰 차량 제어 시스템에 대한 취약점으로 인해 자동차 위치 노출, 차량 잠금 해제 등 여러 가지 보안 취약점이 발견되었다. 또한, 중국의 보안회사인 킨 시큐리티 랩(Keen Security Lab)에서는 테슬라 차량의 무선 공유기에 악성코드를 심어 차량과 멀리 떨어진 곳에서도 차량 원격 조종이 가능하다고 설명하였다[2].

2021년 국내 638개 아파트단지, 약 40만 가구의 월 패드가 해킹되어 시민들의 일상생활이 노출된 경우가 발생하였다. 이는 펌웨어 업그레이드 도중 발생하는 취약점을 이용하거나 월 패드 서버에서 검증을 수행하지 않아 발생하는 인증 우회 취약점 등을 통해 권한을 획득하였으며 최종적으로 해당 가구 내 월 패드 내부 카메라들의 영상을 탈취하여 다크웹에 판매되는 경우가 발생하였다[4].

2019년 전 세계 72개국의 사물인터넷 기기 약 11,700여 대가 모지(Mozi) 봇넷에 감염된 것이 확인되었다. 이는 변경되지 않은 기본 암호 또는 쉬운 암호 등을 사용해서 감염되는 경우가 대부분이며 이를 통해 전파를 시도하였다. 모지 봇넷의 운영자는 2021년 체포되었지만, 해당 봇넷이 P2P 네트워크를 기반으로 동작하기 때문에 체포된 이후에도 여전히 전파되고 있다고 밝혔다[5].

이 외에도 Fig.1.과 같이 다양한 사물인터넷 기기

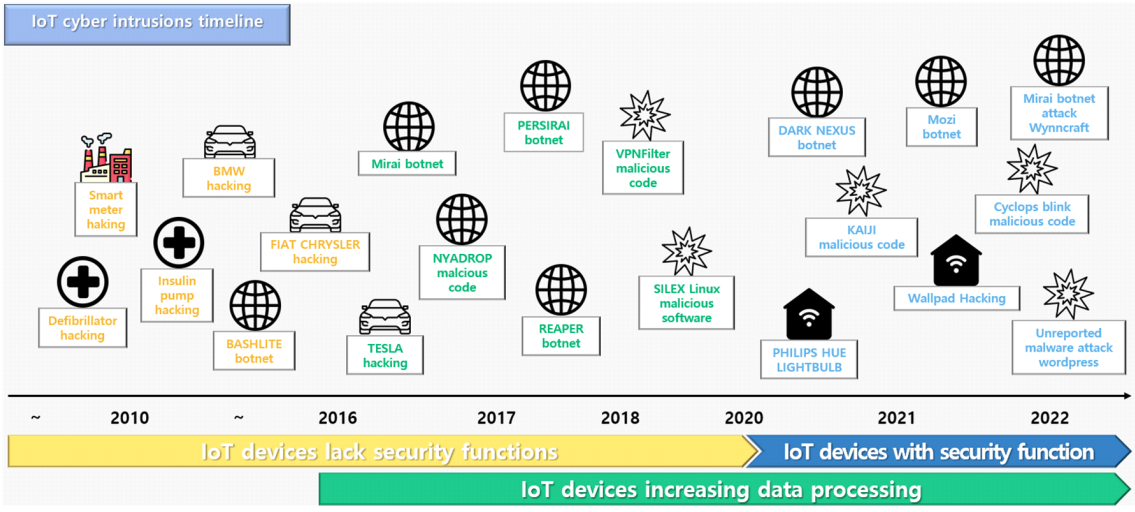

Fig. 1. Timeline of IoT device Incident Case

침해사고 사례가 꾸준히 발생하고 있다[6-9]. 다양한 사물인터넷 기기에 다양한 취약점들이 발견됨에 따라 단일 대상뿐만 아니라 네트워크에 연결된 다양한 기기들까지 추가로 피해를 볼 수 있다. 침해사고 발생 이후 피해확산 방지를 위해 침해사고 발생 시 신속한 분석 절차가 이루어져야 한다.

하지만 사물인터넷 기기 자체에 저장이 가능한 메모리의 용량이 적어 기록되는 로그도 많은 정보를 담지 못한다.

2.2 국내외 침해사고 대응 절차 분석

국내 침해사고 대응 절차에는 한국인터넷진흥원의 침해사고 분석 절차 안내서가 있다. 해당 안내서는 침해사고를 총 7단계로 나누었으며 단계별로 해야 할 일들을 설명하고 있고 운영체제별 침해사고 분석 기술을 다루고 있으며 주요 해킹사고별 분석 사례를 예시로 들고 있다. 하지만 이 안내서의 마지막 최신 개정이 2010년이기 때문에 추가적인 정보가 필요할 수가 있다. 해당 모델의 경우 사건 발생 직후에는 효율성이 뛰어나지만, 사고 발생 탐지가 안될 경우에는 모델의 효율성이 떨어지게 된다. 또한, 국내에서 대표적인 안내서임에도 불구하고 사물인터넷 기기에 대한 대응 방안 및 분석 방법이 부족하다.

국외자료 중 미국 국립표준 기술연구소(NIST)의 SP 800-61에서는 침해사고 대응 가이드를 2012년에 개정하여 발표하였고 준비, 탐지 및 분석, 감염제거 및 복구, 사후활동 총 4단계의 침해사고 대응 생명주기를 제시하였다[11]. 침해사고에 효율적으로 대응하기 위해 각 생명주기 단계별로의 활동을 상세히 기술한다. 탐지 및 분석단계는 모든 공격 경로들을 기술하였다. 감염제거 및 복구단계에서는 침해사고 이후 다른 자산에 피해 전이를 막기 위한 격리와 봉쇄가 필수적이며 사전에 제정된 전략과 절차를 통해 쉽게 대응할 수 있음을 설명하였다. 하지만 이 가이드는 개정된 지 10년이 지났기 때문에 침해사고 절차의 최신화가 필요하다. 이 외에도 여러 가이드와 표준들이 있지만 광범위한 사물인터넷에 관련된 표준이나 대응 가이드는 부족하다[12-18]. 관련 표준 및 가이드라인에 대한 내용은 table 1.과 같다.

최근 사물인터넷 침해사고 데이터 수집에 관한 연구 동향을 살펴보면 사물인터넷 기기 자체에 저장이 가능한 메모리의 용량이 적어 기록되는 로그도 많은 정보를 담지 못한다. 증거 데이터가 사물인터넷 장치에서 발견된다고 하더라도 암호화되어 저장되거나 비표준 형식으로 저장되어있을 가능성이 커 디코딩이 가능한 형식으로 변환하고 읽어야 한다.

대부분의 사물인터넷 기기들은 리눅스 기반의 운영체제로 이루어져 있고 리눅스를 변조한 운영체제를 사용하기 때문에 호스트 및 네트워크 데이터를 수집하는데 있어서는 큰 문제가 되지 않지만, 하드웨어적으로 접근하여 데이터를 수집하기는 어려움이 크다. 만약 침해사고 현장에 도착하여 증거를 수집하는 과정 중 전원 연결이 차단된 사물인터넷 기기의 데이터를 수집하기 위해서는 하드웨어 인터페이스를 통해 증거를 수집해야 하므로 하드웨어적 데이터 수집방법은 필수적이다.

Table 1. Cyber intrusions guides and standards

Agency	Guides and standards	Explanation
KISA	Cyber intrusions analysis procedure guide[12]	Analysis and Response Guide for cyber intrusions guide by Operating System
TTA	TTAK.KO-12.0058 R1 [13]	Digital evidence collection preservation guidelines
	TTAK.KO-12.0059 R1 [14]	Mobile device forensics guidelines
ISO/IEC	ISO/IEC 27037 [15]	Guidelines for identifying, collecting, acquiring, and preserving digital evidence
	ISO/IEC 27043 [16]	Incident investigation principles and procedures
NIST	NIST SP 800 - 61 [11]	Computer security incident handling guide
	NIST SP 800 - 86 [17]	Forensic Techniques Incident Response Integration Guide

2.3 사물인터넷 침해사고 데이터 수집 관련 연구

Malek Harbawi 외 1명은 디지털 증거는 사이버 관련 범죄에서 사건과 관련된 결정을 하는 데 중요한 역할을 한다고 설명하며 사물인터넷 기기에 대한 디지털 증거 수집 절차를 제시하였다[18]. 해당 절차는 7단계로 나누어져 있지만, 절차의 내용이 상당히 큰 범위를 가지고 있어 세부적이지 못하다는 단점이 있다.

이진오 외 1명은 사물인터넷기술의 발전으로 가정에 보급률이 증가함에 따라 다양한 보안사고 및 범죄가 발생하지만, 사물인터넷 기기 분석 및 보안과 관련된 연구가 매우 적어 사물인터넷 기기 데이터 획득에 관한 연구가 필요하다 설명하였다. 또한, 해당 연구에서는 스마트 TV, 스마트 카메라, 스마트 도어락에 대해 메모리 칩오프 방식을 선택하여 데이터 획득을 시도하였다. 이를 통해 추출된 각 메모리 데이터를 시그니처 기반을 통해 분석하는 도구를 개발하여 제시하였다[19]. 해당 논문에서는 데이터 수집을 위한 방법만 있고 세부적인 절차는 존재하지 않는다.

Maria Stoyanova 외 4명은 사물인터넷 기기에 데이터 처리량이 한정되어있어 침해사고 이후 포렌식 절차를 진행하기 위해 어려움이 있다고 밝히며 포렌식의 중요성을 강조하였다. 따라서 이를 위한 정책, 기술적 문제에 대해 해결방안을 제시하였다. 또한, 디지털 포렌식 분야에서 과거와 현재의 이론적 모델의 생명주기에 대한 비교 등을 제시하여 차이점 설명 및 사물인터넷 포렌식에 대한 마인드맵을 제시하였다[20]. 다음 table 2.은 관련 연구에 대한 정량적인 비교표이다.

table 2.은 침해사고 데이터 수집 관련 논문들을 비교한 표이다. 실질적인 절차 및 데이터 획득 방안 등이 여전히 부족한 현황이다. 또한, 사물인터넷 기기 특성상 침해사고 이후 비활성화 상태의 침해사고 기기에 전원을 공급하는 것은 주변 네트워크에 대한 위협, 예를 들어 봇넷에 감염되어 악성 파일이 롬에 저장될 경우 기기 재부팅 시 주변 네트워크로 전파될 가능성이 크다. 따라서 본 논문에서는 이러한 비활성화 상태에서 다양한 접근 방법을 통한 데이터 수집 방안을 제시하고 실증을 통해 절차의 타당성을 입증한다.

Table 2. Compasion with related studies

	Malek Harbawi [18]	Jin-O Lee [19]	Maria Stoyanova [20]
IoT froensic process	O	X	O
hardware technology	X	O	X
Analyze in the disabled state	X	O	X

III. 침해사고 데이터 수집 절차

사물인터넷 기기에서의 침해사고 발생 이후 데이터를 획득하기 위한 절차는 Fig.2.과 같다.

3.1 디버깅 포트 및 메모리 칩 식별

사물인터넷 기기에서 침해사고 데이터를 획득하기 위한 가장 좋은 방법은 디버깅 포트 및 메모리 덤프를 통한 방법이 있다. UART, JTAG는 사물인터넷 기기에서 범용적으로 사용되는 디버깅 포트이며 접근성이 용이하다. 또한, 사물인터넷 기기의 대다수는 MCU를 사용하여 개발되기 때문에 메모리 덤프를 통한 접근은 가장 확실한 방법이 될 수 있다[21].

3.1.1 디버깅 포트 식별

UART는 사물인터넷 기기에서 범용적으로 사용되는 디버깅 포트로서 기기의 정보, 예를 들어 커널, OS 메시지, 하드웨어 정보 등을 수집할 수 있으며 이를 통해 데이터 수집 범위 등을 결정하여 분석할 수 있다. UART는 4핀 배열로 구성되며 사용 및 구현이 간편하여 사물인터넷에서 범용적으로 사용된다. 이를 식별하기 위해서는 육안을 통해 4핀 배열을 확인하거나 제조사의 Datasheet를 통해 확인하는 방법이 있다. 4개의 핀은 VCC, Ground, Rx, Tx로 구성되며 이를 식별하기 위해서는 통전 테스트 등의 방법이 있다[22].

JTAG는 하드웨어 디버깅의 표준으로 이를 이용하여 메모리 덤프, 펌웨어 획득 등이 가능하게 되며 이를 통해 시스템의 접근 권한, 환경 구성, 데이터 저장 위치 등을 파악할 수 있다. JTAG는 8핀, 14핀 20핀 등의 구성으로 이루어져 있으며 핀 종류가 많은 만큼 육안으로 식별하기는 쉽지 않다. 또한, 핀

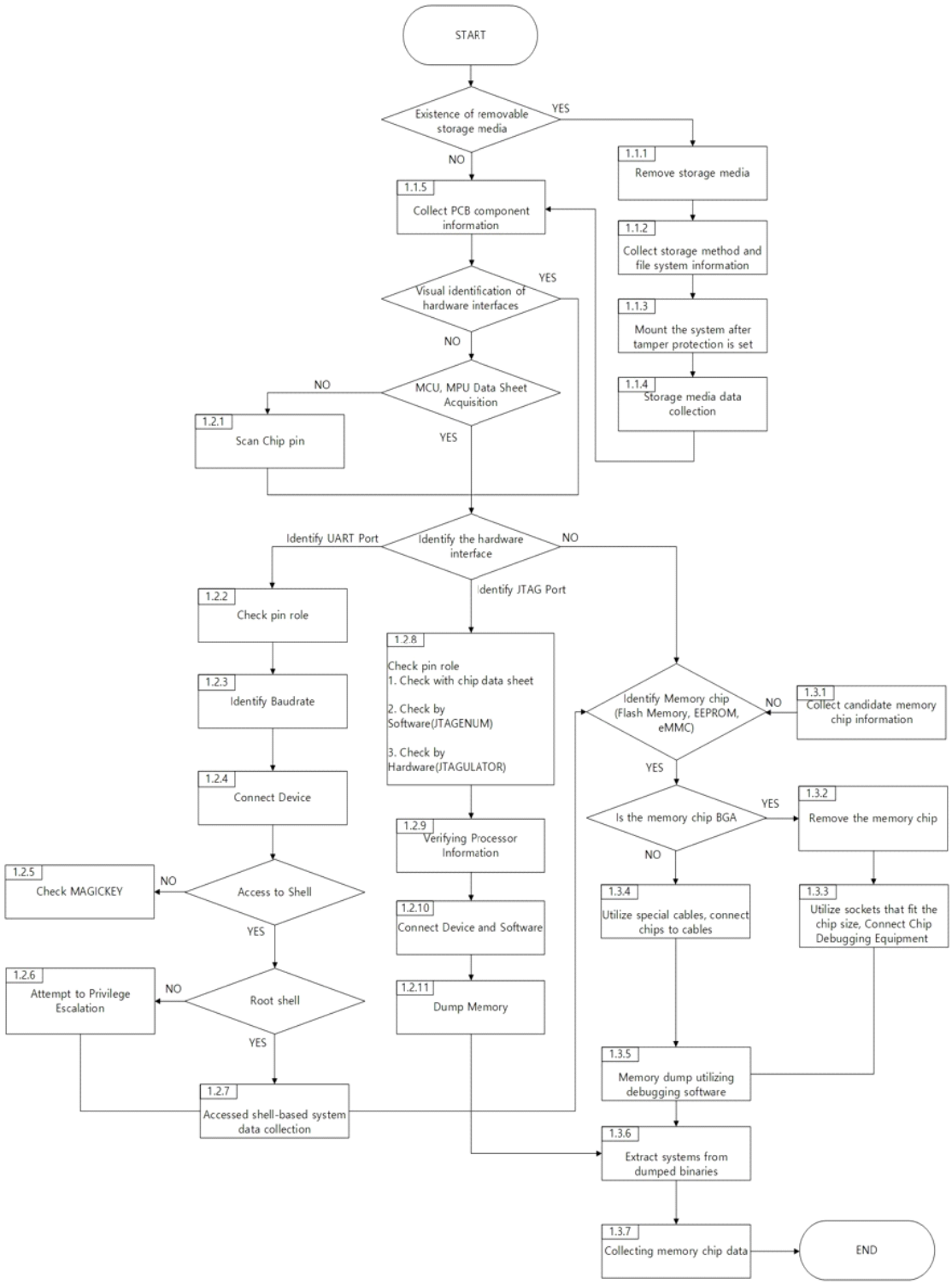

Fig. 2. Acquisition procedure of hardware based intrusion data

이 숨겨져 있거나 핀이 돌출되어있지 않은 경우 납땜 작업이 필요할 수 있다. 여기서 JTAG를 육안으로 식별하지 못한다면 제조사의 Datasheet 또는 BOM(Bills of Material)을 통해 식별하여 파악해야 한다.

3.1.2 메모리 칩 식별

사물인터넷 기기에서 메모리 칩은 펌웨어 및 적은 용량의 데이터들이 저장되는 공간으로 추가적인 저장 장치가 없다면 대부분 메모리 칩에 저장된다. 메모리 칩을 통해 침해사고 데이터를 획득할 경우 사물인터넷 기기의 핵심인 펌웨어와 추가적인 데이터들을 획득할 수 있어 확실한 방법이지만 메모리 칩에 물리적인 힘을 가하여 메모리에 손상을 입히거나 핀이 돌출되어있지 않아 메모리 칩을 탈거해서 분석해야 한다. 따라서 하드웨어의 손상은 불가피하다.

메모리 칩을 식별하기 위해서는 PCB에 적혀진 칩의 부품 번호 또는 코드를 찾거나 Datasheet, 웹사이트 및 포럼과 같은 온라인 커뮤니티를 통해 찾을 수 있다. 추가로 제조사의 BOM을 획득할 수 있는 경우 더욱 쉽게 식별할 수 있다.

Table 3. Identifications by different type

Type	Identifying method	kind of connecting pins
UART	Visual identification, PCB identifier, Datasheet, 4 pin array voltage, measurement	4pins, 10pins (VCC, Ground, Rx, Tx)
JTAG	Check the voltage of the candidate terminal, Datasheet, BOM	ARM 20 pins, STDC 14 pins, OCDS 16 pins, ARM 14 pins, TI 14 pins, ARM CoreSight 20 pins, ARM CoreSight 10 pins (TDI, TDO, TCK, TMS, TRST)
Memory	Visual identification, BOM, Datasheet, Opensource	8 pins, 10 pins, 12 pins, 16 pins, BGA 24 ball, etc. (CS, DO, GND, DI, CLK, VCC)

3.2 침해사고 데이터 수집

3.2.1 UART를 통한 데이터 수집

UART를 통한 데이터 수집은 사물인터넷 기기의 전반적인 정보를 획득하는 방법으로서 기기별로 상이하지만, 특정 기기는 관리자 권한 쉘을 실행할 수 있는 경우가 있으며 이를 통해 모든 파일에 접근할 수 있다. 하지만 대부분 보호된 쉘을 사용하기 때문에 Magic Key를 통한 Escape 방법을 강구하거나 기기의 정보를 획득한 뒤 다음 절차로 넘어가야 한다.

UART를 통해 사물인터넷 기기 정보에 접근하기 위해서는 전송 속도를 식별해야 한다. 전송 속도는 주로 9600, 57600, 115200 등을 사용하지만 정확한 전송 속도를 식별하기 위해서는 신호분석기를 사용해야 한다. 식별된 전송 속도를 활용하여 Putty 등과 같은 연결 프로그램을 사용하면 쉘에 접근할 수 있다. 쉘은 psh, 관리자 등의 쉘에 접근할 수 있는데 psh의 경우 Magic Key를 찾아내어 일반 쉘로 접근할 수 있다.

접근한 쉘을 통해 기기의 데이터 송수신 정보, 부팅 정보, 오류 메시지, 기기의 설정값 등 다양한 정보를 획득할 수 있으며 이를 통해 취약한 부분을 발견하거나 침해사고 발생 가능성 등을 유추 가능하며 데이터의 저장 위치 등의 정보들을 얻을 수 있다 [23].

3.2.2 JTAG를 통한 데이터 수집

JTAG를 통한 데이터 수집은 사물인터넷 기기의 펌웨어, 기기 구성 정보, 메모리 정보 등 다양한 정보들을 수집할 수 있으며 TDI, TDO, TMS, TCK, TRST 총 5가지의 핀을 사용하여 연결하여 사용한다.

사물인터넷 기기에서 JTAG에 접근하기 위해서는 기기의 프로세서를 식별해야 한다. 프로세서에 따라 연결 가능한 분석 장비가 달라지며 이에 맞는 장비를 선택하여 연결을 시도해야 한다. 또한, 분석 장비에 연결 시 클럭 속도 설정, 프로세서와 분석 장비 간 호환성에 주의해야 한다. JTAG에 연결 이후 획득

가능한 데이터는 메모리에 포함된 데이터, 데이터 구조, 프로세서 상태, 레지스터 상태 등 기기의 정보 대부분에 접근할 수 있다.

3.2.3 메모리 칩을 통한 데이터 수집

디버깅 인터페이스를 식별하지 못했을 경우 메모리 칩을 통한 데이터 수집을 수행해야 한다. 이는 사물인터넷 기기에 대한 정보를 정확하게 얻는 방법으로서 소형 사물인터넷 기기의 경우 추가적인 저장장치 없이 사용하므로 유일한 저장장치는 메모리 칩이다. 따라서 메모리 칩의 정보를 획득한다면 기기의 모든 정보를 획득할 수 있다[24].

메모리 칩은 핀이 돌출된 방식과 BGA(Ball Grid Array) 방식이 있는데 BGA 방식의 경우 메모리 칩 데이터를 획득하기 위해 메모리를 탈거해야 하며 이는 기기의 영구적인 손상을 준다[25]. 메모리 칩을 탈거했다면 해당 메모리 칩에 맞는 소켓과 분석 도구를 사용하여 분석할 수 있다. 하지만 이와 같은 도구들은 높은 비용을 요구하기 때문에 본 논문에서는 낮은 비용의 도구들로 높은 효율성과 정확한 침해사고 데이터를 수집할 수 있는 방법을 제시한다.

메모리 칩이 노출되어있는 경우 테스트 클립 및 특수 케이블 등을 통해 연결을 시도하며, 외부에 노출된 핀과 테스트 클립을 연결한 뒤 분석 장비와 연결하여 메모리 칩의 데이터를 덤프할 수 있다. 덤프한 데이터는 바이너리 파일이기 때문에 binwalk와 같은 도구를 사용하여 분석할 수 있으며 이를 통해 침해사고 데이터를 식별 및 추출할 수 있다[26].

각 디버깅 포트 및 메모리 칩 접근을 통해 수집 가능한 침해사고 데이터는 table 4.와 같다.

Table 4. Collectable data depending on type

Type	Connect Tools	Collectable data
UART	Jumper cable, Connecting software, USB to Serial	Kernal, OS Message, Error message, Bootloader, Command Shell,
JTAG	JTAG interface connecter (ex. Buspirate), Jumper cable, JTAGulator	Device Firmware, Device configuration, Memory contents, Processor state
Memory	ROM Writer, Hook Cable, Soic Test Clip	Event log, Configuration setting, Sensor data, etc.

IV. 절차에 따른 침해사고 데이터 수집 실증

4.1 침해사고 가정

하드웨어 기반 사물인터넷 기기 침해사고 데이터 수집 절차를 실증하기 위해 사물인터넷 기기에 대해 침해사고 데이터 수집을 진행하였다.

대상 기기는 H사의 IP카메라이며 Mirai 봇넷을 감염 시켜 데이터를 수집한다. 하지만 Mirai 봇넷 특성상 감염 시 메모리에만 상주하기 때문에 전원 종료 시 악성코드 또한 같이 사라지기 때문에 Mirai 봇넷에 대한 데이터는 남아있지 않았다.

IP카메라는 별도의 저장장치 없이 운영할 수 있으므로 바로 덮개 제거를 통해 데이터 수집 절차를 진행한다.

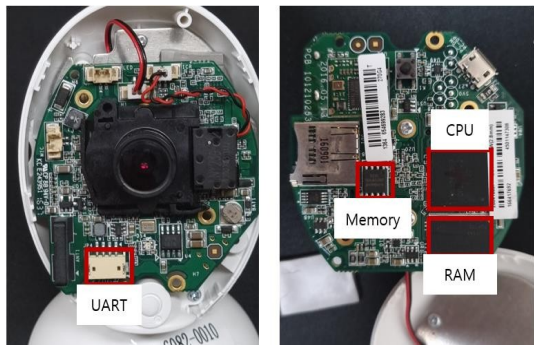

Fig. 3. Components of ip camera

4.2 침해사고 데이터 수집 절차 실증

IP카메라의 덮개를 제거하여 인터페이스를 식별한다. 덮개를 제거하면 전면에 렌즈와 UART, 후면에 Memory, RAM, CPU가 존재한다. 하지만 JTAG는 식별되지 않았기 때문에 절차 실증이 불가능 하므로 우선으로 식별된 UART에 대해 접근을 시도한다.

IP카메라의 UART의 핀 식별을 위해 멀티테스터를 사용하여 Fig.3.의 왼쪽부터 GND, Tx, Rx, VCC 핀이라는 결과를 도출했다. 각 핀을 USB to Serial에 연결하여 분석 장비와 연결한 결과 보호된 쉘에 접근 가능하였으며 해당 쉘에서 IP카메라의 환경변수, 파일 시스템 등과 같은 하드웨어 정보들을 수집할 수 있지만 침해사고에 관련된 데이터들은 수집할 수 없었다. 따라서 메모리 칩을 통해 데이터 수집을 시도하였다.

해당 메모리는 SOIC 방식으로 칩 핀이 돌출되어 있어 SOIC test clip과 같은 케이블을 통해 메모리 덤프를 수행한다. 여기서 SOIC test clip은 테스트용이기 때문에 완전하지 않으며 접촉 불량이 생기는 경우가 다수이기 때문에 신중하게 다뤄야 한다. SOIC test clip과 분석 장비를 연결하기 위해 Fig.4.과 같이 아두이노를 사용하였다. 아두이노에 연결할 핀들은 메모리 핀의 CS, IO0, IO1, GND, VCC이다. 각 핀을 파악하기 위해서는 BOM 또는 메모리 칩 위에 출력되어있는 식별자를 통해 해당 메모리의 핀 정보를 파악할 수 있다.

이렇게 각 핀을 식별한 뒤 아두이노에 연결하였을 때 IP카메라의 전원이 들어와야 정상적으로 연결된 것이며 전원이 들어오지 않을 때 해당 메모리 칩에 연결이 정확히 되었는지 확인한 뒤 재시도한다. 이후 메모리 덤프를 위해 tty와 전송 속도를 해당 기기에 맞게 설정한 뒤 flashrom 명령어를 통해 메모리 덤프가 가능하다.

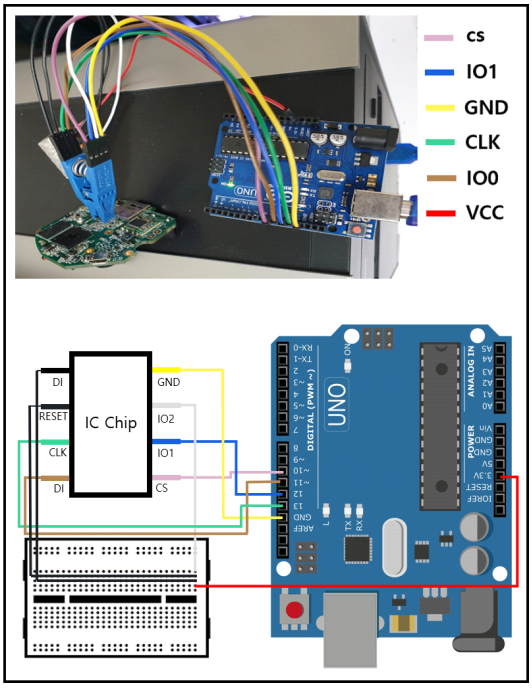

Fig. 4. Memory connection with arduino and SOIC test clip

메모리 덤프 이후 해당 메모리 파일을 분석하기 위해 binwalk 도구를 사용하여 시스템 정보를 확인한다. IP카메라의 경우 CramFS의 파일 시스템을 사용하는 중이었으며 추가로 도구를 사용해 추출 과정을 진행하였다. 추출 진행 시 파일의 크기를 중점으로 두었다. Fig. 5.는 IP카메라의 메모리 덤프를 수행한 뒤 덤프 파일을 binwalk를 통해 분해하여 확인한 파일 구조이다.

덤프된 파일을 추출하면 첫 번째로 CramFS파일을 확인할 수 있다. 이를 통해 리눅스 명령어를 사용할 수 있고 71C9B를 추출해보면 .cpio 확장자를 가진 파일을 확인할 수 있으며 이를 통해 파일 시스템 디렉터리를 파악할 수 있다. 파일을 추출하는데 있어서 가장 크게 눈여겨 봐야 할 것은 파일의 크기이다. 파일의 용량을 통해 파일 시스템을 추출하기 위해 어떤 파일을 추출해야 하는지, 유의미한 데이터인지 파악할 수 있다.

이후 추출한 파일을 마운트하면 일반 리눅스 디렉터리 구조와 해당 시스템에서 사용하는 busybox 명령어, 사용하는 프로토콜의 종류, /etc/passwd 파일, 쉘의 종류 등 해당 사물인터넷 기기의 다양한 호스트 데이터들을 수집할 수 있다. 수집 가능한 데이터 중 일부인 /etc/passwd는 Figure.6.과 같다.

이렇게 메모리를 통해 침해사고 데이터를 수집하는데 가장 주의해야 할 점은 우선 메모리 손상 방지이다. 메모리가 손상되면 더 이상 기기를 사용할 수

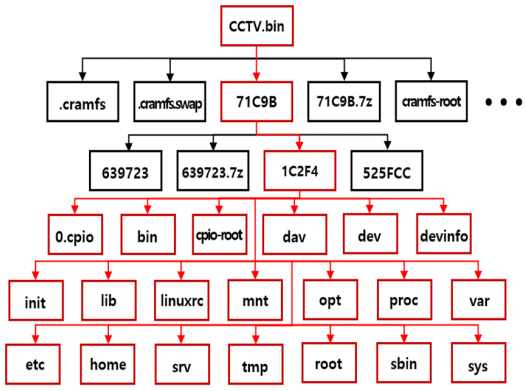

Fig. 5. Structure of memory file in IP Camera

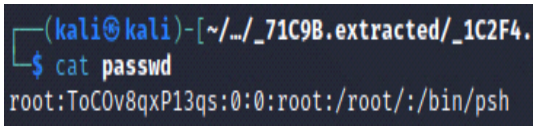

Fig. 6. Acquiring a password

없을뿐더러 공격 및 공격자 식별을 위한 침해사고 데이터를 수집할 수 없기 때문이다.

4.3 침해사고 데이터 수집 방안

기존 침해사고 데이터 수집 절차는 침해사고 발생 전부터 보고서 작성까지 침해사고 전 주기를 다루고 있기 때문에 침해사고 데이터 수집에 관한 세부적인 절차는 부족하다. 또한 사물인터넷 기기에 침해사고 발생 이후 특히 비활성화 상태에서 데이터 수집은 저장매체가 따로 존재하지 않는 경우, 기기의 보안을 위해 디버깅 인터페이스가 존재하지 않는 경우 등 다양한 조건을 고려해야 한다. 따라서 침해사고 데이터 수집 및 식별을 위해 기존 연구에 보다 세부적인 절차를 추가하였으며 이를 통해 다양한 환경 및 조건 속에서 명확하게 데이터를 수집할 수 있다.

V. 결 론

사물인터넷 기기에서 침해사고가 발생하기 전 보안을 강화하는 것이 우선순위이지만 기기 특성에 따라 한번 설치하면 오랫동안 업데이트 없이 사용되기 때문에 침해사고 발생 이후 대응 방안은 매우 중요하다. 또한, 사물인터넷 기기들은 다양한 취약점이 발생하고 오픈소스로 공개됨에 따라 취약점을 통해 침투한 뒤 주변 네트워크에 악성 행위를 하는 일은 비교적 쉬운 일이 되었다. 따라서 침해사고가 발생한 사물인터넷 기기에 전원을 공급하는 것은 주변 네트워크에 악영향을 끼치는 행위이며 이를 방지하며 침해사고 데이터를 수집하기 위해서는 비활성화 상태에서 조사해야 한다.

본 논문에서는 다양한 사물인터넷 기기에 대한 여러 침해사고 사례를 살펴보며 국내·외 침해사고 대응 절차 동향의 최신화 필요성에 관해 설명하고 사물인터넷 침해사고 데이터 수집의 한계에 관해 기술하였다. 이에 비활성화 상태에서 하드웨어 디버깅 인터페이스를 통한 침해사고 데이터 수집 절차 및 방법을 세부적으로 제시하였으며 실증을 진행하여 해당 절차의 효율성을 입증하였다.해당 절차와 방법을 통해 낮은 비용으로 높은 효율을 도출해낼 수 있을 것이며 공격자의 악성 행위, 아티펙트 등을 획득하여 공격자의 IP주소 및 신원파악 등이 가능할 것이다. 하지만 디버깅 인터페이스가 비활성화 되어있으며 메모리 덤프 데이터 또한 암호화 되어있는 경우 제시한 절차를 적용하여도 침해사고 데이터를 수집할 수 없기 때문에 이에 대한 연구가 필요하다.

References

[1] M.S. Mazhar, et al. "Forensic Analysis on Internet of Things (IoT) Device Using Machine-to-Machine (M2M) Framework," Electronics, vol. 11, no. 7 Apr. 2022.

[2] S. Nie, L. Liu, and Y. Du, "FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS," Black Hat USA, Jul. 2017.

[3] A. Dalvi, S. Maddala, and Divya Suvarna, "Threat Modelling of Smart Light Bulb," In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1 - 4, Aug. 2018.

[4] Jeon Jeong-Hoon, "A Study on the Response to Smart Home Attacks," The Society of Convergence Knowledge Transactions, 10(2), pp. 109-118, Jun. 2022.

[5] T. T, et al. "A comprehensive study of Mozi botnet. International Journal of Intelligent Systems,"Wiley Online Library, vol. 37, no. 10, pp. 6877-6908, Feb. 2022

[6] D. CHOI, "IoT (Internet of Things) based Solution Trend Identification and Analysis Research," 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), pp. 252-258, Sep. 2022.

[7] P. Legg, et al. ""Hacking an IoT Home": New opportunities for cyber security education combining remote learning with cyber-physical systems," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-4, Jul. 2021
[8] A. Banafa "Three major challenges facing iot," IEEE Internet of things, pp. 26-67, Mar, 2017
[9] N. M. Karie, N. M. Sahri, P. H. Dowland, "IoT Threat Detection Advances, Challenges and Future Directions.," 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), pp. 22-29, May. 2020.
[10] Kang Min-Sup, "Design of AES-Based Encryption Chip for IoT Security," The Institute of Internet, Broadcasting and Communication, 21(1), pp. 1-6, Feb. 2021.
[11] P. Cichonski, et al. "computer security incident handling guide," NIST Special publication 800-61, Aug. 2012.
[12] KISA, "Cyber instrusions analysis procedure guide", 2010-8, Jan. 2010
[13] Lee Sang-Jin, et al. "Computer Forensics Guideline," TTAK.KO-12.0058/R1, Dec. 2007.
[14] Han Jae-hyeok, et al. "Guidelines on Cellular Phone Forensics," TTAK.KO-12.0059/R1, Dec. 2020.
[15] A. Ajijola, P. Zavarsky, R. Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIS T SP 800-101 Rev. 1 :2014 and ISO/IEC 27037:2012," World Congress on Internet Security (WorldCIS-2014), pp. 66-73, Feb. 2015.
[16] A. Valjarević, H. Venter, and Petrović, "ISO/IEC 27043:2015 - Role and application," 2016 24th Telecommunications Forum (TELFOR), pp. 1-4, Nov. 2016.
[17] K. Kent, et al. " Guide to Integrating Forensic Techniques into Incident Response," Special Publication 800-86, Aug. 2006.
[18] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," 2017 5th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-6, Apr. 2017.
[19] Lee Jin-O and Shon Tae-Shik "Acquisition of artifacts used for criminal investigations through smart home appliances and IoT devices forensics," Journal of Digital Forensics, 16(2), Jun, 2022
[20] M. Stoyanova, et al, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues", IEEE Communications Surveys & Tutorials, vol. 22, no. 2, Jan. 2020
[21] Z. Kazemi, et al. "Hardware Security Evaluation Platform for MCU-based Connected Devices: Application to healthcare IoT," 2018 IEEE 3rd International Verification and Security Workshop (IVSW), pp. 87-92, Oct. 2018.
[22] K. Rosenfeld and R. Karri. "Attacks and Defenses for JTAG," IEEE Design & Test of Computers, vol. 27, no. 1, pp. 36-47, Feb. 2010
[23] C. Kelly, et al. "Testing And Hardening IoT Devices Against the Mirai Botnet, " 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1-8, Jun. 2020
[24] J. Seo, S. Lee, and T. Shon, "A study on memory dump analysis based on

digital forensic tools," Peer-to-Peer Networking and Applications, vol. 8, no. 4, pp. 694-703, Jun. 2013.
[25] J. Sitek, et al. "Investigations of temperature resistance of memory BGA components during multi-reflow processes for Circular Economy applications," 2017 21st European Microelectronics and Packaging Conference (EMPC) & Exhibition, pp. 1-7, Sep. 2017
[26] Y. Ma, et al. "SVM-based instruction set identification for grid device firmware," 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), pp. 214-218, May 2019

〈저자소개〉

이 종 범 (Jong-bum Lee) 학생회원
2022년 2월: 호남대학교 정보통신공학과 졸업
2022년 3월~현재: 전남대학교 정보보안협동과정 석사과정
〈관심분야〉 산업제어시스템 보안, IoT 보안, 디지털포렌식

엄 익 채 (Ieck-Chae Euom) 종신회원
2003년 8월: 전남대학교 컴퓨터정보학부 학사 졸업
2015년 2월: 한국과학기술원 소프트웨어대학원 석사 졸업
2019년 2월: 전남대학교 정보보안협동과정 박사 졸업
2019년 10월~현재: 전남대학교 시스템보안연구센터 소장, 데이터사이언스대학원 교수
〈관심분야〉 제어시스템보안, 스마트그리드 보안, 원자력 보안, 취약점 분석, 차세대인프라 보안, 스마트시티·공장 보안, AI기반 이상징후 탐지, 지능형 보안