International Journal of Engineering & Technology, *7 (3.33) (2018) 157-160*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Study on Development of IoT Software Vulnerability (Using Fake Information) Response System based on Artificial Intelligence

JangMook KANG[1], *CholeHee YOON[2], Jiho SHIN[3]

[1]Department of Big-Data Industrial Security, Namseoul University, Cheonan city 31020, Korea,
[2] Police Science Institute, Korean National Police University, Asan, Korea
[3] Police Science Institute, Korean National Police University, Asan, Korea
**Corresponding author E-mail:bertter@police.go.kr*

Abstract

The use of IoT devices such as wearable digital devices based on mobile devices is increasingly evident. In IoT-based environment, communication protocol of IoT category and lightweight special environment software are used instead of universal network configuration. Due to the operating structure of IoT, preparation of countermeasures to automatically analyze IoT software vulnerabilities based on artificial intelligence should be considered. Because of the rapid growth of IoT equipment and the expectation that there will be a sharp increase in the need to identify facts about vulnerabilities and improper use associated with IoT services naturally. It is necessary to apply artificial intelligence technology for classification and automatic collection and analysis of IoT vulnerabilities for wearable devices and smart home devices through artificial intelligence analysis technology. Sequentially, To acquire the data from the device, internal data and network data of the specified device after searching the protocol of the IoT device, it is possible to cope with IoT software vulnerability applying AI intelligence analysis method to related data. In this paper, we investigate software vulnerabilities in IoT environment and propose a technique to cope with ioT vulnerabilities through artificial intelligence.

Keywords: *IoT software vulnerabilities, Digital Forensics, Artificial intelligence*

1. Introduction

Through interconnection between humans, objects and services, IoT is interconnecting objects in an intelligent relationship through sensing, networking, and information processing, without human intervention. Recently, it has evolved into a concept of interacting with all information of reality and virtual world through intelligent communication between people, objects, objects and objects using mobile communication network. With the growth of mobile computing and network, various information is gathered and circulated through communication between machines without human substitution. As such, the rapid expansion of artificial intelligent IoT equipment and wearable digital devices is being developed for the benefit of people for a better life. However, crimes are taking place using vulnerabilities of software installed in IoT, and it is time to take measures to deal with dangerous situations.

Data generated from IoT mobile devices is collected / processed in a specific storage space in a high-speed network environment. Software security enhancement technology is required for safe operation. This is expanded to IoT devices based on network communication using various sensors have. It is very likely to be associated with crime because it exploits the fact that IoT technology, such as smartphones, artificial intelligent speakers, and smart lighting, is used to share information through synchronization with the platform. Therefore, it is necessary to use IoT digital forensic analysis technique to cope with software vulnerabilities and post - viewpoints to accommodate changes in wearable and smart home devices.

Table 1: IoT technically applied element classification

IoT technically applied element classification	Element	Description
Sensing	Context-aware sensor	Temperature / Humidity / Heat / Gas / Light / Ultrasonic Sensor
	Physical sensor	Remote Sensing, SAR, Radar, Position, Motion, Image Sensor
Wired communication	Ethernet	LAN environment based on 802.3 (xDSL, HFC, FTTH)
	BcN	Broadband network(service network, transmission network, subscriber network)
	PLC	Low-speed / low-capacity LAN communication technology based on power line
Wireless communication	WMAN	802.16 zone based on 3G / 4G / LTE
	WLAN	802.11 a / b / g / n, Wi-Fi Direct, WAVE
	WPAN	Bluetooth/Zigbee/UWB/RFID/6LoWPAN
Service interface	Semantic	Ontology-based, Resource / Property / Syntax structure
	Open API	Web services, lightweight transmission technology REST based, WOA based technology
	Cloud	Large scale distributed processing, Ha-

		doop, virtualization, resource management, security, SLA
Access control	NAC	802.1x, DHCP, authentication bypass, monitoring
	Copyright	DRM, watermarking, fingerprinting, CAS / DCAS
Encryption	Symmetric key based	DES, 3DES, AES, SEED, HIGHT, ECC
	Public Key Based	RSA, ECDSA, Diff-Hellman

Classification of objects related to artificial intelligence based IoT software vulnerabilities can be divided into services, platforms, networks, and devices. The IoT service is used in the fields of medical, manufacturing, defense, security, etc. for industrial, individual, and public areas. The IoT platform is used as a framework for communication of objects and services in the field of cloud information and service mashup. The most widely used field is IoT device, which uses intelligent smart sensing through IoT device as a communication-based network service using remote control and sensing. Through the intelligent IoT software vulnerability response system, it is possible to protect all the personal information of individuals in the smartphone, mobile and wearable device and protect the information that can be linked to the crime. IoT service is mainly a way that one computer (equipment / terminal) sends network data to another computer in Internet network. Therefore, internal information should be protected by minimizing software vulnerability inherent in IoT devices that are running.

2. Environment Analysis Related with IoT

2.1. Consumer’s Prior Knowledge of Functional Food

The artificial intelligence-based IoT software vulnerability technology level has a system and platform of self-access type for each telecommunication company that provides smart AI home service to IoT devices at the present stage. As a result, there has been no consideration of procedures and techniques for responding to vulnerabilities of IoT devices and analysis of vulnerabilities afterwards, and there is no technology or tool development at home or abroad. In general, the home network technology is composed of technologies constituting physical networks such as Ethernet, HomePNA, Radio Frequency (RF), and PLC (Power Line Communication), communication protocol technology between terminals, home appliances, sensors, and actuators constituting a home network, Middleware technology for mutual discovery, configuration and management between terminals on the network, and service technologies based on these middleware [1]. In the late 1990s, various home network standards for interoperability and interoperability of device families emerged, introducing LonWorks, CEBus, and UPnP (DLNA) for audio / video data networks, which are standards for home automation. However, due to the limitations of the network medium and the lack of convenience in comparison with the installation cost, consumers have been exposed [2]. Recently, a company providing a smart home service is developing the technology of analyzing the weaknesses of IoT related to the domestic market by utilizing the infrastructure for management and testing of its own network and devices. We are attempting to collect data from the IoT device centered on platform providers. However, there is not yet a tool for analyzing the specific IoT vulnerability in solution form due to legal institutional restrictions and privacy protection

Table 2: IoT service environment classification and security threats [3]

Category	IoT service environment classification	Security Threats	Description
Application	IoT Application	Information leakage, data forgery, denial of service	Industrial, personal and public domain applications IoT services - Medical, Manufacturing, Environment, Defense, Security, Market Application Platform
	IoT Platform		Framework for communication of things and services - IoT cloud information, IoT service mashup
Network	IoT Network	Wireless signal disturbance, information leakage, data forgery	Real-time IoT communication, service creation oriented network - IoT device remote control, IoT gateway
Device	IoT Device	Lost, Stolen, Physical	Intelligent Smart Sensing, Actuator HW Platform - Sensor, actuator module, wearable, health care

2.1. Development Status of Artificial Intelligent IoT

Standard competition for artificial intelligent IoT technology is accelerating, and artificial intelligent IoT standardization is being implemented in various aspects such as devices, networks, and services. It has been proposed to support multiple corporate standards or de facto standards rather than a single standard [1]. And artificial intelligence IoT software vulnerability related technical standard is trying, but it is the initial level, and it is expected that the weight will increase in the future.

Table 3: Artificial intelligent IoT service case

Category	Service	Service Platform
Artificial Intelligent Speaker Service	amazon echo Always ready, connected, and fast. Just ask. Roll over image to zoom in	• Amazon Echo • Google home • Apple HomeKit

2.2 IoT Technology Standardization Statuses

The artificial intelligence IoT platform is mainly managed by a company in order to provide a personalized service by interconnecting the devices installed in the home network so as to be able to interwork with people, things, objects and objects. In addition, standard and non-standard technologies are fragmented and technically mixed, and manufacturers and others have developed services and an open home IoT platform [3].

Table 4: IoT platform standardization group [4]

Category	Standardization	Summary
Standardization group	oneM2M	A consortium of eight major standards bodies (ETSI, TIA, ATUS, ARIB, TTC, CCSA, and TSDSI) from around the world, including Korea's TTA,
	OIC	Samsung, Intel, MediaTek, Dell,

		Broadcom, Atmel, etc. A consortium of standards for Internet service platforms
	AllSeen Alliance	Qualcomm and Linux Foundation led by Cisco, Microsoft and LG Electronics
	Thread Group	Intel, Atmel, Dell, Samsung Electronics, and other technology standards to ensure the connectivity of IoT devices
Standardization technology	CoAP	A lightweight RESTful-based application layer protocol developed for inter-object communication in the IETF CORE Working Group
	OMA LWM2M	The Internet standard for the management of Internet devices established by the OMA (Opan Mobile Alliance)

3. Onem2m IOT Software Vulnerability (Using Fake Information) Analysis and Countermeasures based on Artificial Intelligence

In order to address software vulnerabilities that operate artificial intelligent IoT devices, IoT device discovery and access ID discovery techniques are required. This is in accordance with the way the IoT service operates, and it must be possible to locate specific IoT devices for detection of abnormal behavior of IoT devices, which can be done based on scanning technology. Also, in order to check the connection information of the searched devices, techniques related to collection of evidence such as data acquisition and communication network data collection should be developed. Therefore, understanding of representative communication protocols and packets should be preceded. The following describes the communication protocol for oneM2M, which describes the configuration of IoT communication that occurs during communication to analyze technical vulnerabilities. In the OSI7 layer, the physical layer and the data link layer of IEEE 802.15.4, Bluetooth 4.0 Low Energy, RFID / NFC, WI-FI, 3GPP, 6LowPAN and zigbee, RPL, Ipv6, TCP, Shows the integration of the ONEM2M service layer.

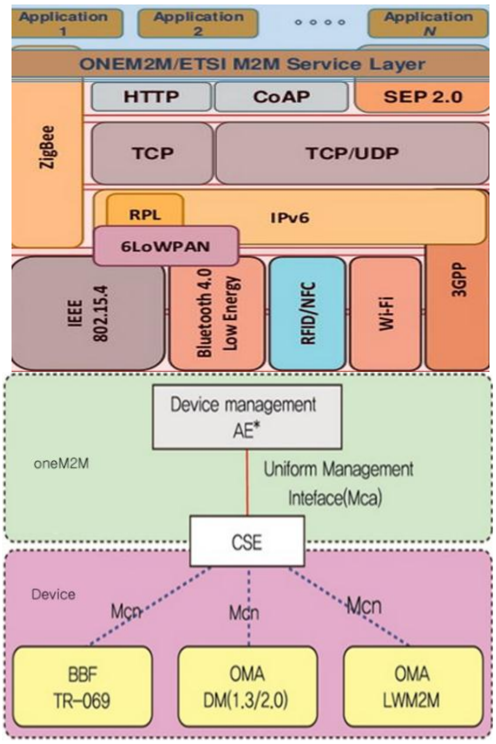
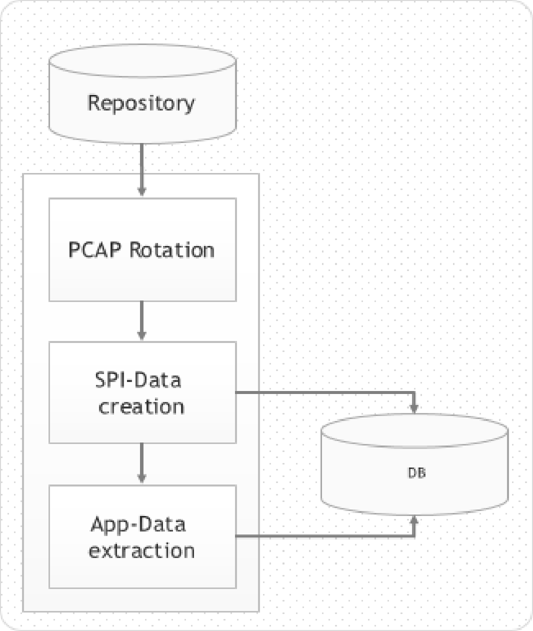
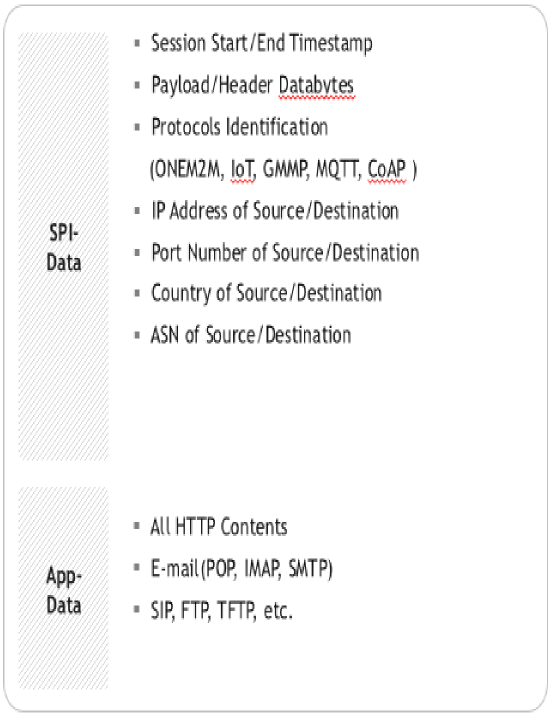


Fig. 1: oneM2M structure and network interworking structure [5] [6]

App-Data generated during IoT communication should be extracted and stored in the integrated DB. Session start point and timeline occurrence event can be collected for IoT devices to be started. Analysis of network communication payload is possible. This is data collection of communication of IoT usage protocol for vulnerability analysis that can occur in software. Finally, it leads to analysis of security vulnerability of IoT device connection number, receiving service, various personal information, occurrence time and data contents. All App-Data is then automatically classified and automated through Protocols identification and automatically classified as exposed to unusual activity. Next, after the IoT communication, the information of the communication process after searching and indexing can be inquired and retrieved through the Session Profiling Inspection and Application Data Inspection so that the SPI calculation for the connection to the network server and the application server can be inquired and retrieved. Progress can be made to detect IoT duplication terminals, IoT terminals to attempt DDos, and detection of abnormal services.





SPI-Data

- Session Start/End Timestamp
- Payload/Header Databytes
- Protocols Identification
  (ONEM2M, IoT, GMMP, MQTT, CoAP)
- IP Address of Source/Destination
- Port Number of Source/Destination
- Country of Source/Destination
- ASN of Source/Destination

App-Data

- All HTTP Contents
- E-mail(POP, IMAP, SMTP)
- SIP, FTP, TFTP, etc.

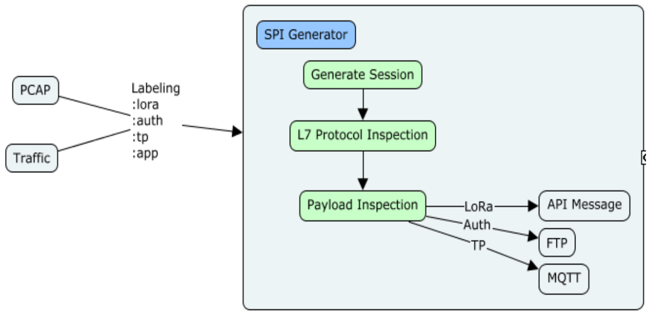


Fig. 2: Artificial intelligence application IoT communication SPI automation course

Fig. 2 illustrates the process of automatically classifying through Protocols identification and automatically classifying it as exposed to anomalous behavior. Generally, SPC-DATA is created by loading data for Pcap, which is stored in minutes, and detailed traffic is analyzed by AI.

For accurate analysis of traffic, extracting the application - data included in the payload and restructuring the data enables artificial intelligence risk analysis for IoT vulnerabilities.

4. Conclusion

In order to effectively analyze IoT software vulnerabilities based on artificial intelligence, we must focus on the development of automated analysis tools for the process of "collection → analysis → confirmation" of existing data. Collecting and analyzing IoT software standard APIs is required for data collection and analysis to address vulnerabilities in AI IoT devices. So far, the demand for software vulnerability analysis for IoT devices has not been very large. However, considering the demand for IoT devices, demand for software vulnerability analysis of wearable IoT devices based on mobile services will surge in the future.

From the technical point of view, it will be possible to develop and demonstrate techniques for instrument detection, path tracing, and anomaly detection through analysis of standard protocols for automated IoT detection and automated vulnerability analysis. In addition, it is expected that DDoS attacks on IoT devices, terminal detection techniques participating in communication, and repetitive abnormal packet generation behavior detection techniques are highly utilized. Sensing technology, wired / wireless communication network technology, and IoT service interface technology are closely related to each other, and software vulnerability analysis can be continuously developed.

Table 5: Classification of possible software vulnerabilities of IoT devices

Vulnerability point	object	Analysis method
privacy	Obtain financial information through IP camera hacking, smart TV hacking, Google class hacking	IoT network packet analysis
Smart Home	Real-time monitoring through robot cleaner, thermostat hacking, spy microchip, print document hacking, TV on-off remote control	Chip-off, J-TAG extraction and analysis
Network	Control platform hacking, set-top box, DDOS attack	M2M, Coap SPI analysis

In addition, a path trace tool and an anomaly detection tool are developed together. An additional automated IoT analysis system can classify and analyze data through inverse analysis of API that enables communication between IoT equipment and server. Another technology development methodology is to construct scenarios in which software vulnerabilities can occur in relation to IoT and develop corresponding countermeasures. Vulnerability analysis scenarios related to IOT devices can be divided into IOT device hacking, privacy problems, and network infringement. By developing detailed scenarios for each category and developing evidence collection and analysis techniques for each procedure, we can consider the demonstration method through simulations in the future test bed. The following figure considers continuous analysis and automation of IoT devices and software which are different from each other with the configuration for an automation system to cope with IoT software vulnerability applied with artificial intelligence.

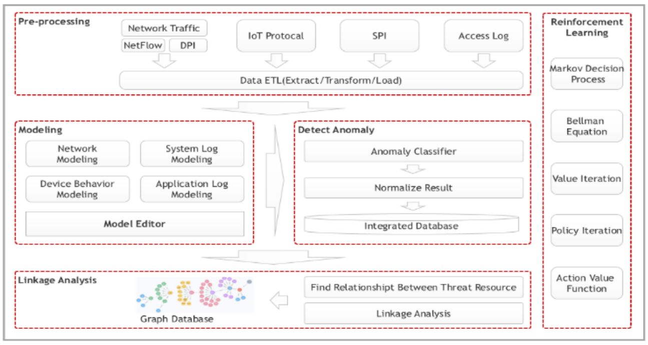


Fig. 3: Artificial Intelligence IoT Vulnerability Response System

It performs network traffic, DPI analysis, IoT protocol analysis and SPI in the pre-processed area, loads the stored log into the automated data base, classifies the anomaly according to the automated modeling, and finally classifies the IoT vulnerability. It is a countermeasure system that removes the risk after classifying enemy and network vulnerabilities. Systematic techniques of automated IoT risk management with artificial intelligence can be used to protect the proprietary information of an enterprise that leads to IoT related vulnerability analysis, development and collection tools and additionally to enter new IoT service. The development of the IoT software weakness response system based on artificial intelligence plays an important role in the creation of ecosystem of information protection. Analysis of artificial intelligent IoT software vulnerability will be able to create new markets such as various IoT related services and systems through the spread of security control, security industry and forensic related products in the future, and it will contribute to building social stabilization system.

Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.2018-0-00705, Algorithm design and software modeling for judge fake news based on artificial intelligence) This work was Supported by a Korea University Grant in 2015 (1.Mar.2015-28.Feb.2016)

References

[1] Son Young Seong, Park Joon Hee, Home IoT technology status and development direction. Journal of the Korean Institute of Communication Sciences (Information and Communication)., 32(4)(2015), 23-28.

[2] Park Joon-Hee, Home network middleware technology and standardization trend, Electronic communication trend analysis., 19 (5) (2004), 53-58.

[3] Jang Dae-il, Yu, Chang-hoon, IoT Software Mitch Network Vulnerability Assessment System Study, Journal of Digital Forensics., 11-3 (2017), 1-13.

[4] Kang Min Soo, IOT platform technology trend in the open direction, KEIT PD Report, 12 (2012), 201-219.

[5] Oh Seung Hoon, Trend of IoT device management standard protocol based on mobile communication, Analysis of electronic communication trend., 30 (2015), 2.

[6] EU Butler Project- Communication Issue., https://www.postscapes.com/internet-of-things-protocols/