ISSN 2672-1562
VOL. 7

The 7th International Conference on
Next Generation Computing 2021

ICNGC 2021

Dates November 4(THU) ~ 6(SAT), 2021

Venue Gravel Hotel, Jeju, Korea

Organized by | 사단법인 한국차세대컴퓨팅학회 Korean Institute of Next Generation Computing

Sponsored by | IITP 정보통신기획평가원 Institute of Information & Communications Technology Planning & Evaluation · LG히다찌 · TRACOM · JDIA · JEJU NATIONAL UNIVERSITY Software Convergence Education Institute

Expert Fostering Program for New Industry Convergence Embedded System · AU MID-AIRC MR-IoT융합 재난대응 인공지능 연구센터 · 차세대 초지능 네트워크융합 고속연구단 BK21 FOUR AJOU UNIVERSITY

Auto-HRS: An Automated System Design for a Secure Home Router Environment

Se-Han Lee
SysCore Lab.
Sejong University
Seoul, Republic of Korea
sehands@sju.ac.kr

Sung-Kyu Ahn
SysCore Lab.
Sejong University
Seoul, Republic of Korea
yiimfn@gmail.com

Ki-Woong Park*
dept. of Information Security
Sejong University
Seoul, Republic of Korea
woongbak@sejong.ac.kr

***Abstract*—The Internet of Things (IoT) technology is a recent development, and subsequently, various application services have appeared. Accordingly, diverse smart environments based on wireless networks are being developed. Home routers, which are widely used to build a wireless network environment at home, are exposed to many security threats. Therefore, setting up a secure router environment has become an important issue. In this paper, we propose an automated home router security configuration system (Auto-HRS) for multiple home routers located in a wireless network environment both by network administrators and those who install and operate their domestic routers at home. Auto-HRS analyzes the configuration HTTP request-response message of the home router and stores the HTTP message corresponding to the secure router configuration. Subsequently, the stored HTTP message is used to generate a secure-environment-setting message and then send it to a home router to update the environment setting.**

Keywords—Home Router Security, IoT Security, Automated System, HTTP Request-Response Message

I. INTRODUCTION

In modern society, various Internet of Things (IoT) services have emerged concurrently with the rapid development of ICT technology. In particular, as smart home infrastructure is built, home appliances and electronic devices are connected to wireless networks to provide various services [1]. Recently, a service was introduced in which a lighting device, a temperature device, an intrusion alarm device, etc. in the home are connected through a smart home network for convenient use [2]. Tasks that are normally performed while moving about the home are now remotely performed using smart devices. In this smart environment, the devices commonly used for wireless network communication between various IoT devices are home routers.

However, many home routers have exposure to numerous security threats because security settings are not properly set up and are likely to cause personal information to be leaked [3]. As a result, setting up a safe home router environment is increasingly important.

To solve this problem, this paper proposes an automated home router security configuration system (Auto-HRS) for an administrator to install and operate a home router. The overall operation flow figure for the Auto-HRS proposed in this paper is shown in Fig. 1, and the operation sequence explanation "TABLE I" is as follows.

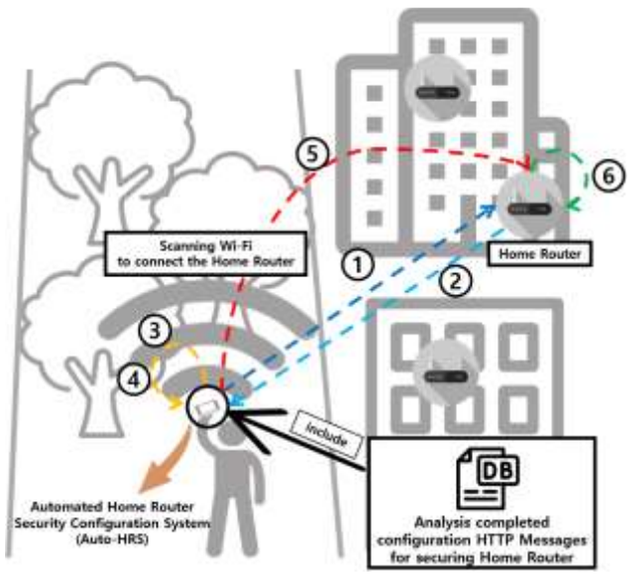

Fig. 1. A flow of automated home router security configuration system (Auto-HRS) operation

TABLE I. AUTO-HRS OPERATION SEQUENCE EXPLANATION

No.	Operation Order Description
1	A user who wants to check for security, requests configuration data using the Auto-HRS from the home router. (HTTP Request)
2	The Auto-HRS gets the configuration data from the home router. (HTTP Response)
3	Analyzing configuration data… Analysis Result: ***Not Secure!***
4	Generating HTTP Messages for secure configuration of the home router.
5	Sending HTTP Messages to the home router.
6	The home router updates the configuration.

This paper is structured as follows.

In Section II, we survey cases of router hacking and the prior research and development related to home-router security to analyze the contents and problems.

In Section III, we explain how the home-router configuration HTTP messages for the Auto-HRS are analyzed.

*Corresponding author

We explain the Auto-HRS configuration diagram in Section IV, and the conclusion and future research plans in Section V.

II. Related Work

A. A survey of router hacking incidents

'Switcher', a trojan malware, appeared in December 2016, [4] and uses Android devices to attack and infect home routers. Subsequently, it changes the DNS settings of the infected router so that the device connected to the router connects to a website that is controlled by a hacker.

In 2016, routers and other IoT devices were infected by the 'Mirai Botnet', and infected devices launched DDoS attacks on well-known websites [5]. In 2018, several routers were attacked by the 'Torii Botnet' and 'VPNFilter' malware [6].

A survey revealed that these cases were caused by inadequate router security settings. Consequently, the issue of setting up a secure router environment continually arises.

B. A survey of earlier research and development related to home router security

In the case of US Patent No. 'US 9,294,353 B2', the router setting information is verified using the hardware electrical signal for automatically setting the router environment. A new code is generated to set up the wireless network information based on verified information, and the router's SSID, password, and encryption method are automatically set up [7]. However, the system proposed by this patent must read the hardware electrical signal directly; therefore, an electrical signal analyzer is required.

Furthermore, a research team at Sejong University proposed a network system that safely operates IoT services using message queuing telemetry transport (MQTT) to protect the communication network between IoT devices on a smart home network [8]. However, this system only monitors the communication network packets of IoT devices and does not proceed with its own security settings for home routers.

C. The Defference between Auto-HRS and earlier research and development

In the patented system, a specific device is required to read the hardware electrical signals. The above-mentioned network system simply monitors the network packets.

However, the Auto-HRS analyzes HTTP Request-Response Messages generated by the home router, stores and modifies data related to the security settings, and uses it to set up a safe home router environment.

III. Analysis of the Home Router HTTP Request-Response Message for Auto-HRS

By analyzing the HTTP request-response message of the home router, a specific HTTP message type is found. In this study, we used ipTime A8004T, ipTime A3004NS-M, and ipTime A2004R to analyze HTTP messages for Auto-HRS [9].

The message for authenticating the home router's administrator account verifies that a new HTTP header is generated, and this header value is encoded in Base64 schemes. In addition, it was confirmed that the Wi-Fi settings and router security settings were configured using specific data values.

The HTTP Request-Response Message analysis was performed using 'Burpsuite [10]', a representative web proxy tool, and the process is shown in "Fig. 2." Several analyzed HTTP messages are shown in "Table II.

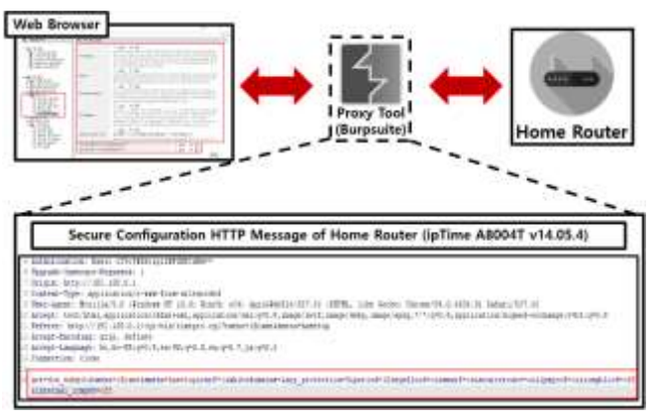

Fig. 2. Analysis the HTTP request-response message of the home router using Burpsuite

TABLE II. Example of the Home Router HTTP Request-Response Messages (ipTime A8004T v14.05.4)

Type	Analyzed HTTP Request-Response Messages
Admin Account Authentication	... Authorization: Basic bnNObGFkbWluOmRwc2RwdG14bGRwZg== ...
Admin Account Settings	POST /cgi-bin/timepro.cgi HTTP/1.1 ... act=save&tmenu=iframe&smenu=hiddenloginsetup &captcha_file=<captcha_file_name> &captcha_code=<captcha_code> &new_passwd=<password>&new_login=<id>
Router Wi-Fi Settings (2.4 GHz)	POST /cgi-bin/timepro.cgi HTTP/1.1 ... tmenu=iframe&smenu=hiddenwlsetup &wlmode=0&wlmodetxt=2g&action=allsubmit &...&SSID=<SSID>&...&personallist=wp2psk_aes &wpapsk=<Password>&...
Router Wi-Fi Settings (5 GHz)	POST /cgi-bin/timepro.cgi HTTP/1.1 ... tmenu=iframe&smenu=hiddenwlsetup&wlmode=1 &wlmodetxt=5g&action=allsubmit&... &SSID=<SSID>&...&personallist=wp2psk_aes &wpapsk=<Password>&...
Router Security Settings	POST /cgi-bin/timepro.cgi HTTP/1.1 ... act=dos_submit&tmenu=iframe&smenu=hasetup &csrf=1&whitedomains=&arp_protection=0&period=10 &synflood=on&smurf=on&sourceroute=on&ipspoof=on &icmpblock=off&internal_icmpbk=off

Currently, after the 'ipTime' vendor has patched its products, the home router administrator is authenticated using two methods: the HTTP method (old method) and the session method (new method). However, the HTTP method is still applicable. Therefore, it is possible to set up a secure router environment using the HTTP messages proposed in this study.

IV. Automated System Configuration

Figure 3 shows the overall configuration of the Auto-HRS proposed in this paper. The system detects the current home router. Next, it checks if the security setting of the target home router is correct and connects with the target home router.

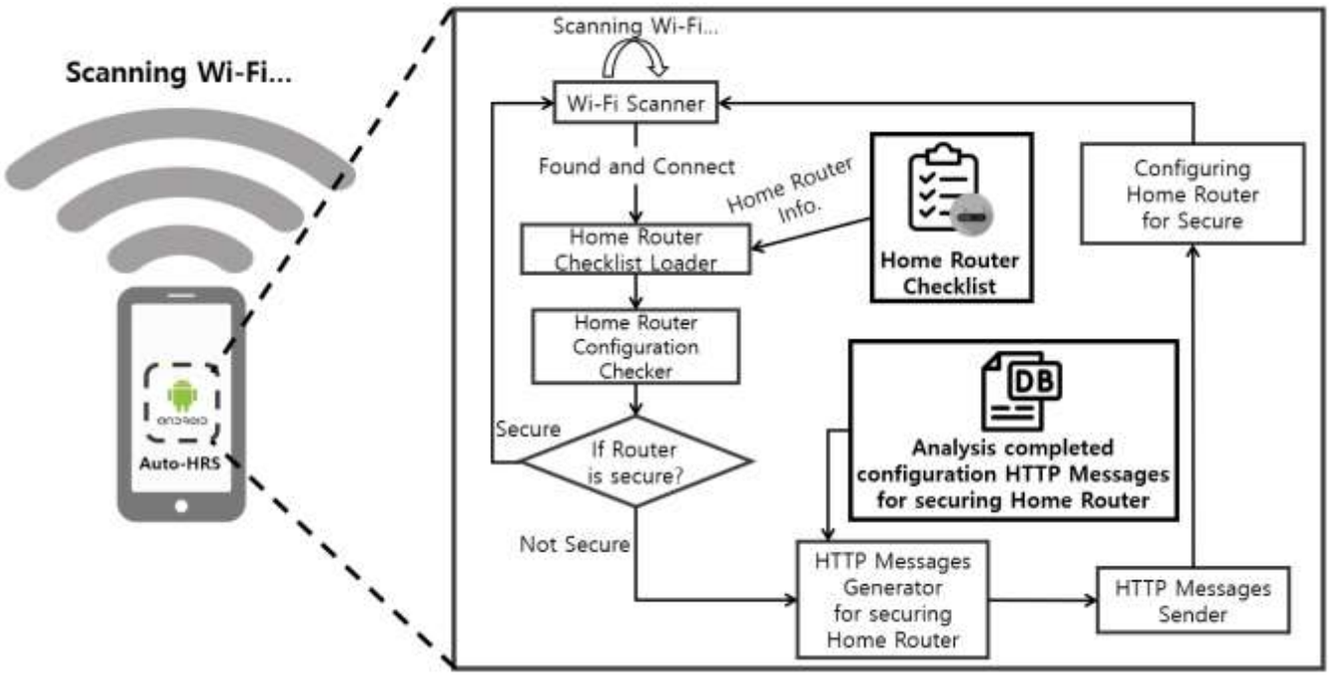

Fig. 3. Automated home router security configuration system (Auto-HRS) configuration diagram

After connecting, the system checks whether the current home router is secure. If the router is secure, it returns to its initial state and detects other home routers. If the router is not secure, it creates HTTP messages for secure configuration and sends them to the router. Subsequently, the router that receives the HTTP messages automatically completes the secure configuration.

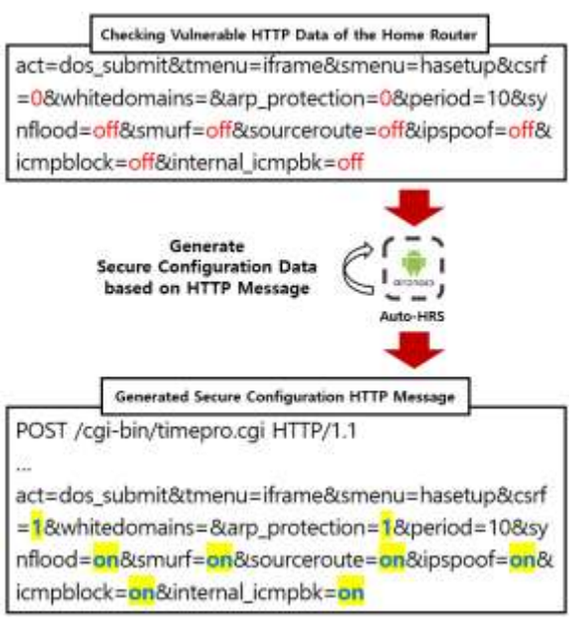

Fig. 4. Generate secure configuration HTTP message after changing unsafe router setting data to safe router setting data

V. Conclusion

The home router, which is one of the most commonly used devices in the IoT environment provides convenient wireless internet connectivity by establishing a wireless network. However, it is often exposed to hacking threats.

In this paper, we propose a system that enables a router manager to set up a safe home router environment easily when building a smart home IoT with a wireless network environment. We will later develop the system as an Android OS application for convenient use on smartphones.

Acknowledgment

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) (Project No. 2019-0-00426, 10%) and National Research Foundation of Korea (NRF) (No. NRF-2020R1A2C4002737, 90%) grants funded by the Korean government.

References

[1] A. K. Ray, A. Bagwari, “IoT based Smart home : Security Aspects and security architecture,” IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), pp.218-222, Apr. 2020.

[2] A. Osman, A. Wasicek, S. Köpsell, T. Strufe, ‘‘Transparent microsegmentation in smart home IoT networks,’’ Proceedings of the 3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge `20), June. 2020.

[3] Trend Micro Forward-Looking Threat Research (FTR) Team, “Securing Your Home Routers,” Trend Micro Research Paper, 2017.

[4] “Switcher hacks Wi-Fi routers, switches DNS,” Kaspersky Daily, Dec. 2016.

[5] M. Antonakakis et al., “Understanding the Mirai Botnet,” Proceedings of the 26th USENIX Security Symposium, pp.1093-1110, Aug. 2017.

[6] “Router Attacks Can Devastate Your Smart Home,” Avast Blog, Mar. 2019.

[7] Patrick Sewall, David Alan Johnson, “Configuring a wireless router,” United States Patent, US 9294353 B2, Mar. 2016.

[8] JS Baek, M. W. Kanampiu, CS Kim, “A Secure Internet of Things Smart Home Network: Design and Configuraton,” Applied Sciences, 11(14), 6280, 2021.

[9] ipTime, http://iptime.com/iptime/

[10] Burpsuite, https://portswigger.net/burp