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 Drone Industry Association
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 교육연구단 BK21 FOUR AJOU UNIVERSITY

Time Interval Side-Channel for Authentication in an IoT Environment

Hye-Lim Jung
Department of Information Security
Sejong University
Seoul, South Korea
Hyello13@gmail.com

Sung-Kyu Ahn
Department of Information Security
Sejong University
Seoul, South Korea
yiimfn@gmail.com

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

***Abstract*—The fields to which IoT applies are widely found in domestic, industrial, national, and other facilities, where it serves various functions depending on the environment. However, most IoT systems communicate with servers and control IoT devices to function according to the server's requests and in this process, there is the threat of an IoT attack. Studies on security such as authentication systems as communication security techniques are undertaken to cope with it. However, systems with limited resources, such as IoT, require overhead to perform encryption operations for authentication. To solve this problem, the mechanism proposed in this paper performs authentication through subchannels and injects specific patterns into time stamps and time intervals to authenticate them. The mechanism does not use additional authentication solutions in limited hardware resource environments and performs authentication with physical timers and interval operations inside the system.**

Keywords-IoT system, Authentication, Side-channel, Network

I. Introduction

By using Internet protocols, IoT systems have become a key element in various fields such as electric devices, building management, and social and public infrastructure. IoT technology has been built into various infrastructures owing to the convergence of many IT technologies[1]. Yet, these infrastructures often utilize the client-server structure to issue central server commands to the IoT device. For example, in the case of home IoT, which is currently being commercialized, the information collected by the home IoT terminal sensors is transmitted to the server, the server analyzes these data, and uses a classic method of providing services to the user[2].

As IoT infrastructure develops into a terminal cluster, many servers and a plurality of devices process data simultaneously, providing complex IoT services[3]. Accordingly, security technologies targeting IoT platforms should be developed using IoT platforms. The security solution currently applied in IoT services uses a security solution targeting specific terminals or targeting infrastructures that provide specific services. However, as technology advances, solutions to defend against the threats to complex IoT infrastructure are limited when applying existing solutions because the existing solution is targeted at a single platform. It is a disadvantage that security solutions used in different devices must be integrated to apply them to a multi-server platform and terminal cluster infrastructure. This method is inappropriate for terminals where computing resources exist in various forms and interferes with normal service owing to the additional overhead in terminals that lack resources[4].

Therefore, to solve these problems, this study devises a safe and reliable communication authentication mechanism for heterogeneous data communication. The proposed mechanism uses a reverse-hash list based on a hash chain in the data transmitting and receiving process, thereby dividing the data into a specific number of "blocks" and generating a time interval between the transmission of the first and next data "blocks". The time interval pattern is confirmed by using the seed of the same hash chain in both the terminals transmitting and receiving data. The terminal receiving the data compares the transmission pattern of the data transmitted by the server or the other terminal with the interval data based on the hash chain. Thereby it authenticates that the data being received is transmitted from a normal server or terminal. Using this authentication method, the reliability of heterogeneous types of communication data can be secured. The terminal configured in the mechanism safely communicates with various terminals and servers. It minimizes the overhead by using a hardware timer inside a conventional terminal and an interval measurement mechanism in a data reception process.

II. Time interval side-channel

The proposed data authentication communication scheme is a communication mechanism between terminals and servers in a limited resource-limited environment. The mechanism transmits a data packet from a server in an IoT environment to control an IoT device and authenticates the data packet on the device-side that receives the data packet.

In the environment presented in this paper, the server divides the control data packets to be transmitted to the IoT device into "blocks". The divided control packet "blocks" are transmitted to the terminal according to a predetermined pattern.

In the device control data transmission process, the number of packets to be divided and the transmitted time intervals vary in all transmission processes. The mechanism constructs a hash chain based on seed data shared by each server and device before they start communication and creates a reverse hash data list to select the number of packets and

[*] Corresponding author

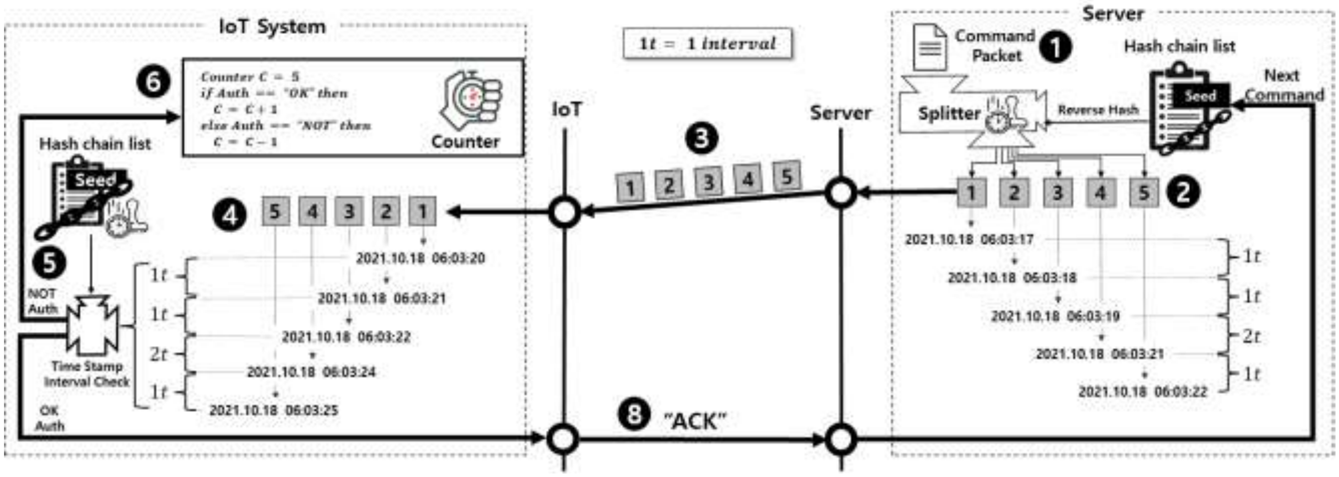

Fig.1. Structure and Communication Flow of the mechanism

time intervals. In this mechanism, based on the security policy of the device, it is assumed that the hash list generated by the seed is safe.

The device receives a packet transmitted from the server, checks the control command of the packet, and receives the next packet based on the number of packets and the time interval generated based on the list following a predetermined inverse solution. If the number of partitions and time intervals of the received data packets coincide with the number of partitions and time intervals generated based on the reverse-hash chain, the device certifies that the data are transmitted from a normal server.

However, if the device and server network environment is unstable or malicious users interfere during network communication, normal authentication between the server and the device cannot occur. To solve this problem, the terminal has a countdown mechanism in which the count decreases when the determined number of packets and intervals differ. The countdown mechanism was designed as a physical hardware counter inside the device. During non-normal communication, the count is deducted, and during normal communication the count data are initialized.

If abnormal data are received until the count is deducted, the server classifies the terminal as an abnormal device and interrupts the communication process. The IoT apparatus physically isolates the communication module. This neutralizes the attack on the device. To determine the presence of an unstable communication environment or external threat, the device and server perform heartbeat communication from time to time during a certain period to identify the status of communication environments and the presence of eexternal threats. The subchannel authentication mechanism presented in this paper does not use additional authentication solutions in environments with limited resources, such as IoT terminals.

III. Conclusion

The mechanism proposed in this paper is a side-channel technique that authenticates communications between IoT devices and servers. In this paper, we propose a mechanism to reduce the operations required for authentication between the server and the device. The server in this proposed mechanism has a seed value and the device has a seed value and a physical counter. The server and device seeds are similar and create a reverse-hash chain list based on the seed. The hash is read by the server and it designates the number of packets transmitted by the device and the time intervals between packets. The packets divided by the server are transmitted to the device according to the time intervals. In the device, the reverse-hash chain list created based on the seed and packets received from the server are compared. The number of packets received by the device from the server and the time interval of the timestamp recorded in the packet are compared. By considering the communication environment, a physical counter inside the device limits the opportunity for communication to prevent attacks. The proposed mechanism is designed to allow IoT devices to perform authentication operations with no overhead where hardware resources are limited.

Acknowledgment

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. 2019-0-00426,Development of active kill-switch and biomarker based defense system for life-threatening IoT medical devices, 10%) and National Research Foundation of Korea (NRF) (NO.NRF-2020R1A2C4002737, Intelligent Incident Investigation Platform for IoT CERT, 90%)

References

[1] Verma, Anurag, et al. "Sensing, controlling, and IoT infrastructure in smart building: a review." IEEE Sensors Journal 19.20 (2019): 9036-9046.

[2] Davis, Brittany D., Janelle C. Mason, and Mohd Anwar. "Vulnerability studies and security postures of IoT devices: A smart home case study." IEEE Internet of Things Journal 7.10 (2020): 10102-10110.

[3] Kuo, Yaw-Wen, et al. "Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications." IEEE Sensors Journal 18.12 (2018): 5187-5197.

[4] Pattar, Santosh, et al. "Searching for the IoT resources: fundamentals, requirements, comprehensive review, and future directions." IEEE Communications Surveys & Tutorials 20.3 (2018): 2101-2132.