Healthcare Security System using IP Hiding methods

Yong Kyu Park, Lee Hak Joon and Yong Gyu Jung*

InnogsKorea, inc., Innoplex 203, Yangsan-ro 57-5, YoungDeoungPo-gu, Seoul, 07271, Korea.

*Eulji University, Department of Medical IT, 553 Sanseong-Daero, Sujeong-gu, Seongnam-si, Gyeonggi-do, 13135, Korea.

(*Corresponding Author)

Abstract
In the medical field, IoT era has come, and a lot of so-called healthcare products and services have been created which carry out health management system through IoT devices. The healthcare service provided by the general enterprises or the telemedicine service provided by the hospital as a pilot service is composed of an IoT device for collecting data and a service server for collecting and analyzing collected information. In this paper, we propose a medical information system that protects a service server against hacker attacks by preventing the IP of the service server from being exposed even if the IoT device as a client is hacked in the data transmission. Through this study, it is possible to safely keep the information of the service server which is inevitably exposed to the threat of the hacker due to lack of resources among the components of the Healthcare System.

Keywords: healthcare service, protecting server, hacker attacks, preventing IP, IoT device,

INTRODUCTION
In the medical field, IoT era has come, and a lot of so-called healthcare products and services have been created which carry out health management system through IoT devices. World-class companies such as Samsung Electronics, LG Electronics, Sony, Huawei and Xiaomi are equipped with GPS in their smart watches and smart bands to measure distance traveled and provide calorie and momentum calculations by measuring heart rate. In the case of Xiaomi, Mi Scale is introducing a smart scale that provide weight management services continuously. So far, companies have been providing healthcare functions as a way to promote their IoT devices.

However, many hospitals are developing services and systems to utilize IoT devices as a means of telemedicine. It is being attempted to provide Healthcare devices to patients who need constant management, and to periodically collect data and manage doctors in charge. Although it is still a trial service level, it is expected that such an attempt will become an important medical service in the future.

The above-mentioned healthcare service provided by the general enterprises or the telemedicine service provided by the hospital as a pilot service is composed of an IoT device for collecting data and a service server for collecting and analyzing collected information. In this paper, we propose a medical information system that protects a service server against hacker attacks by preventing the IP of the service server from being exposed even if the IoT device as a client is hacked in the data transmission.

PROBLEMS AND SOLUTIONS
A Healthcare System or a telemedicine system that is currently being operated or scheduled to be installed, collects the patient's status through the IoT type Healthcare device, transmits the status to the service server via the Internet, and the doctor checks the status of the patient through the service server. The problem of the current Healthcare System can be summarized by the threat of the service server exposure due to the hacking of the client, the DDoS attack of the service server caused by the hacking of the client, and malfunction of the Healthcare System due to the theft and change of the data packet.

As mentioned in the previous issue, the problems of the current Healthcare System are diverse. Once the service server exposes and changes the data due to IP exposure and packet theft, the following method can be suggested as a solution to these problems.

In order to solve the problem of data exposure and change, the Internet communication between the healthcare IoT device serving as a client of the Healthcare System and the service server is made to use the encrypted communication. Encryption communication can be done in various ways, but the most common method is to use SSL. Generally, in the Healthcare System, since the communication between the client and the service server uses the communication using the TCP protocol, even if an IoT device that can use a lot of system resources can’t use the encrypted communication. Of course, you can build your own encryption system, but if you use Internet communication in the Internet as a standard way, using SSL is an effective way.
However, even with SSL, it is possible to prevent data exposure and change, but the service server’s IP exposure can’t be secured. Due to the structure of packet, SSL can exist in the TCP, so it can’t protect the IP address of the service server in the IP header existing outside the TCP. As a general method, there is no way to prevent the IP exposure of the service server. There is no way to connect the service server to the service server only through the relay system without introducing the IP of the service server directly to the client through the introduction of the relay system. To do this, a proxy server is generally used to hide the IP of the service server. In this study, we design and develop a service server security infrastructure system that does not directly affect service server even if IP information is exposed due to hacking of clients or data packets through IP concealment of service server through relay system.

DEVELOPMENT, RESULTS AND DISCUSSION

As mentioned in section 2.2, there is no way to introduce a relay system in order to prevent exposure of IP of service server. In other words, the service server can access only through the relay system. That is, only the relay system knows the IP of the service server, and the client knows the IP of the relay system, not the IP of the service server. As a method of creating a relay system, a proxy server is made as a relay system, and the information of the service server is registered in the corresponding proxy server so that the proxy server transmits the data received from the client to the service server.

To do this, the client must return the IP address of the relay server (proxy server) instead of service server by DNS. It is necessary to finish setting the IP to be allocated to the domain of the service server to the IP of the proxy server in advance in the DNS setting. Alternatively, the client may have an IP address of the proxy server instead of the IP address of the service server (generally, the IP address of the service server is obtained through the domain). When DNS returns a proxy server’s IP address for a service server's IP request, it does not return the IP of one proxy server but distributes two or more proxy servers using the load balancing function of DNS.

For example, as shown in Figure 1, when the service server is connected to a.com, if it is original, when the client requests the IP address of a.com, DNS sends 50.120.74.152, which is the IP address of the a.com service server. However, since the DNS is set to 100.50.5.101, which is the IP address of the proxy server that uses IP of a.com as the proxy server, the client will respond to the IP address of the proxy server when requesting the IP address of a.com. And the proxy server has set up information on service server of a.com.

A client that receives the IP address of the proxy server from the DNS sends its healthcare-related information to the proxy server. The proxy server connects the service server using the IP of the a.com service server and transmits the data received from the client again to the service server. The service server receives the data from the proxy server and returns the response to the proxy server, and the proxy server transmits the response received from the service server to the client. In this way, the client can send and receive data to the service server through the relay system without using the IP of the service server.

Even if the hacker hacked the client and intercepted the packet to communicate with the service server, the hacker could not access the IP of the service server because the packet has only the proxy server’s IP (100.50.5.101). And DDoS attacks, it attacks the proxy server instead of the service server. Therefore, even if the proxy server itself has a problem, it does not affect the service server. Therefore, the service server has not a hindrance from the attack of the hacker, can be prevented. Because the proxy server itself is a problem, a client connecting to the proxy server may have a connection failure, but a client connecting to another proxy server (another proxy server assigned through the load balancing function of DNS) is not adversely affected.
EXPERIMENT AND RESULTS

In order to verify the contents of this study, the environment of experiment was constructed as shown in Figure 2.

This study is the communication between IoT product and service server, but in the test for verification, it is done on PC, not IoT product. In order to check the packet, we installed Wireshark on the client, the 1st proxy server and the 2nd proxy server to check the packet. I set tt.com as a domain for testing, and the client's host file that tt.com sends to 192.168.100.10 which is the IP of the 1st proxy server. NginX of the 1st proxy server stores the IP of the client which is confirmed when the packet is received in NginX for all the packets to which the target IP belongs, and when it is exported back to the 2nd proxy server, the IP of the already set service server (192.168.100.51) as the target IP, and stores the Inner IP packet in which the IP of the client is set as the source IP, and sets the IP header, and then customized it so that it can be transferred to the 2nd proxy server. In the 2nd proxy server, NginX is customized so that the Outer IP header is removed from the packet whose source IP is the IP of the 1st proxy server and the protocol is IPIP, and the Inner IP packet in the packet is directly transferred to the target IP of the Inner IP header.

CONCLUSION

Through this study, it is possible to safely keep the information of the service server which is inevitably exposed to the threat of the hacker due to lack of resources among the components of the Healthcare System. Even if the hacker hacked the client and intercepted the packet to communicate with the service server, the hacker could not access the IP of the service server because the packet has only the proxy server's IP and DDoS attacks, it attacks the proxy server instead of the service server. Therefore, even if the proxy server itself has a problem, it does not affect the service server. Therefore, the service server has not a hindrance from the attack of the hacker, can be prevented. Because the proxy server itself is a problem, a client connecting to the proxy server may have a connection failure, but a client connecting to another proxy server (another proxy server assigned through the load balancing function of DNS) is not adversely affected. Using this method, the service server can check the information of the client, so that the administrator can take action on the client, which is a problem when a problematic client occurs.

Financial support: This research was supported by Bio & Medical Technology Development Program (Research on demonstration of prognostic and diagnostic systems for aging related diseases), through the National Research Foundation of Korea (NRF), funded by the Ministry of Science and ICT (2016M3A9B6904246 ).

REFERENCES