Lightweight, Low-Rate Denial-of-Service Attack Prevention and Control Program for IoT Devices

Chi-Che Wu[1](✉), Wei Yang Wang[2], and Rung-Shiang Cheng[3]

[1] Department of Electrical Engineering,
National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan
jerry@gm.kuas.edu.tw
[2] Department of Information Management,
National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan
wyang@gm.kuas.edu.tw
[3] Department of Computer and Communication, Kun Shan University,
Tainan, Taiwan
rscheng@mail.ksu.edu.tw

Abstract. As information technology has become more advanced, the Internet of things (IoT) has evolved from being a mere concept to becoming a part of everyday life. IoT-based home appliance applications have matured, and numerous relevant software programs have been made commercially available. Therefore, IoT-created security issues have become an issue that must be addressed. Although DoS attacks are one of the most commonly used methods by hackers to attack target hosts, most mainframe computers are equipped with excellent DoS attack prevention and control programs. Nevertheless, most IoT devices do not have high computing power and are thus prone to DoS attacks. Therefore, this study examined the feasibility of using a lightweight, low-rate DoS attack prevention and control program in IoT devices with low computing power. The objective is to enable these devices to prevent and control DoS attacks.

Keywords: HTTP/2 · Denial-of-service attacks
Low-rate denial-of-service attacks · Information security

1 Introduction

In recent years, the Internet of things (IoT) has been widely used in smart homes and in the field of industrial control. IoT embodies the concept of creating a network in which everything is connected. For users, the IoT provides a novel way of interacting with devices. The interaction process includes collecting relevant data; The use of IoT in the field of industrial control is even more prevalent than that in smart homes. For instance, smart factories add numerous sensors to relevant equipment. When the equipment malfunctions, the networking devices send warning messages through wireless transmission to inform users of the abnormal situation, achieving early disaster prevention.

In general, devices connected to an IoT-based network contain a network component with data transmission capability. In addition, several sensors that have

Y.-B. Lin et al. (Eds.): IoTaaS 2017, LNICST 246, pp. 243–247, 2018.
https://doi.org/10.1007/978-3-030-00410-1_29

dissimilar goals or purposes are installed. These sensors are comparable to human senses and can be used to collect relevant data in surrounding environments.

2 Background Information

2.1 From the IoT to the WoT

The conventional IoT involves the use of numerous sensors that transmit related data to a cloud platform through a network device. Users who need to control or access relevant data can do so by connecting to the cloud platform and accessing inquired data. The Physical Web program introduced by Google in 2014 specified that all sensors and devices have URLs, which are the basis of connection in the web environment; these URLs are connected to physical devices to allow users to quickly control and use the devices.

2.2 Hypertext Transfer Protocol 2

The HTTP/2 request process differs from that of HTTP/1.1. For instance, HTTP/1.1 establishes 6–8 TCP connections to speed up the inquiry time, whereas HTTP/2 establishes only one TCP connection so as to reduce the burden on servers. After a TCP connection is established, browsers can establish multiple noninterfering streams and use the smallest unit frame to allocate the request content, facilitating browser–server communications (Fig. 1) [3–5].

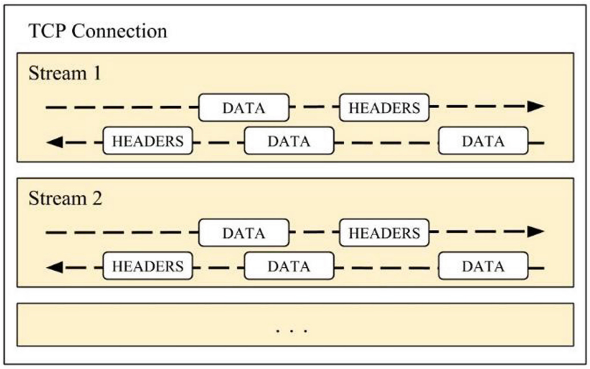

Fig. 1. HTTP/2 request submission process

2.3 DoS Attacks

Low-rate DoS attacks are a variation of DoS attacks; they attack by continuously sending a small number of network packets to attack server response times or buffer zones, causing depletion of server resources, resulting in service termination [6–8].

A study on low-rate DoS attacks on HTTP/2 services [1] confirmed that HTTP/2 security is at risk of low-rate DoS attacks. In such attacks, a virtual host using a type 1 ping and WINDOW_UPDATE frame defined by HTTP/2 attacks the virtual server. In the experiment of the aforementioned study, the degree of CPU depletion, size of the network packets received per second, and number of network packets received per second were used as a basis for assessing low-rate DoS attacks [1].

3 System Framework and Design

This study designed lightweight DoS-attack prevention and control programs for IoT devices that support WoT functions. Because RESTFul is the primary method for facilitating communication between devices, this study focused on designing a program that protects HTTP from low-rate DoS attacks.

HTTP/2 is the latest version of HTTP. Compared with HTTP/1.1, it has superior transmission capacity and lower power consumption. However, HTTP/2 is prone to low-rate DoS attacks. Thus, this study designed a defense mechanism in which the server firewall records the frames requested by users within a set time period (10 and 20 ms in this study) and identifies whether the frames are repeats and thereby pose a risk of a low-rate DoS attack. If the two criteria are met, the firewall initiates a filtering process (Fig. 2), which reduces the impact of the attacks on other users.

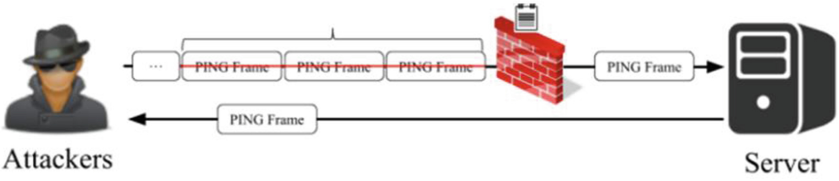

Fig. 2. Defense procedure

4 Performance Assessment

4.1 Average Time Required to Send and Receive Network Packets and the Final Network Packet Return Time

In this experiment, users were divided into two groups: attackers and legitimate users. The attackers initiated their attacks by continuously sending PING frames, whereas the legitimate users browsed webpages of all five types. A TCP connection was established every time a user visited a webpage. Once a connection was established, ten header frames were sent, which were then received and responded to in order to establish a new TCP connection. To prevent unclosed TCP connections from affecting the experimental results, signals indicating a closed TCP connection were sent to servers prior to completing new TCP connections. Users were required to wait 1 s before browsing the next webpage. Each experiment was performed 30 times (Fig. 3).

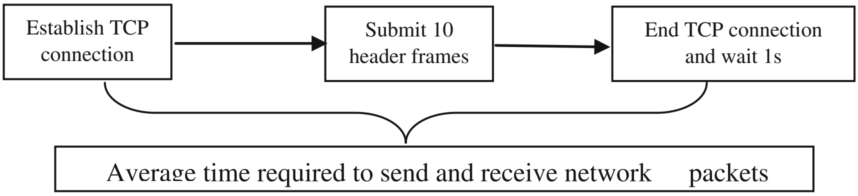
Establish TCP connection
Submit 10 header frames
End TCP connection and wait 1s
Average time required to send and receive network packets

Fig. 3. Experiment procedure

4.2 Experiment Results

Experiment was performed to verify whether introducing the defense mechanism could effectively reduce the effect of attackers on legitimate users' usage experience. Similarly to Experiment 1, measurements from the experimental trials were listed in ascending order, and the 10 middle values were averaged to plot Fig. 4. The two graphs reveal that the defense mechanism effectively lowered the risk of a successful attack.

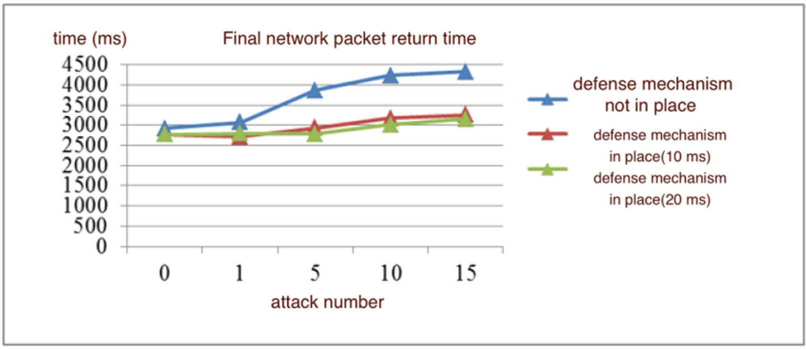

Fig. 4. Final network packet return time, with the defense mechanism used

5 Conclusion

HTTP/2 has special functions such as multiplexing and stream prioritization. However, although HTTP/2 has numerous advantages, studies have revealed that it also has several problems, one of which is its security. Therefore, this study conducted a series of experiments to explore this issue. The first experiment confirmed the existence threats to HTTP/2 security, which have also been identified in previous studies. Thus, the experimental results of this study offered two major contributions. The first is the revelation that the higher the number of attackers, the longer the amount of time is required for legitimate users to load webpages and that the effect is strongest when loading high-performance webpages. The second major contribution is the proposed defense mechanism that was verified in the second experiment; this mechanism can effectively reduce the effect of attackers on the usage experience of legitimate users.

References

1. Adi, E., et al.: Low-rate denial-of-service attacks against HTTP/2 services. In: 2015 5th International Conference on IT Convergence and Security (ICITCS), pp. 1–5. IEEE (2015)
2. Kuzmanovic, A., Knightly, E.W.: Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 75–86. ACM (2003)
3. Berners-Lee, T., Fielding, R., Frystyk, H.: Hypertext Transfer Protocol – HTTP/1.0, RFC 1945 (1996)
4. Fielding, R., et al.: Hypertext Transfer Protocol – HTTP/1.1, RFC 2616 (1999)
5. Chowdhury, S.A., Sapra, V., Hindle, A.: Is HTTP/2 more energy efficient than HTTP/1.1 for mobile users? PeerJ PrePrints **3**, e1571 (2015)
6. Grigorik, I.: Making the web faster with HTTP 2.0. Commun. ACM **56**(12), 42–49 (2013)
7. Varvello, M., et al.: To HTTP/2, or not to HTTP/2, that is the question. arXiv preprint arXiv:1507.06562 (2015)
8. Belshe, M., Thomson, M., Peon, R.: Hypertext Transfer Protocol Version 2 (HTTP/2), RFC 7540 (2015)