IoT measuring of UDP-based Distributed Reflective DoS Attack

Ladislav Huraj, Department of Applied Informatics, University of SS. Cyril and Methodius Trnava, Slovakia, *e-mail*: ladislav.huraj@ucm.sk
Marek Šimon, Department of Applied Informatics, University of SS. Cyril and Methodius Trnava, Slovakia, *e-mail*: marek.simon@ucm.sk
Tibor Horák, Institute of Applied Informatics, Automation and Mechatronics, Faculty of Materials Science and Technology in Trnava, Slovak University of Technology in Bratislava, Trnava, Slovakia, *e-mail*: tibor.horak@stuba.sk

Abstract. IoT devices and their fast growth on the Internet cause many cyber-attacks problems. The number of compromised IoT devices can be used by DDoS (Distributed Denial of Service) attackers to imitate valid request packet or to form illegal request packet to the victim with a spoofed source IP addresses to hide themselves, meanwhile giving rise the system collapse, the obstruction of network/traffic, or disrupting of the victim Internet operation. In this article is demonstrated a specific kind of DDoS attack involving usually accessible IoT devices the UDP-based Distributed Reflective DoS Attack (DRDoS). The packets are flooded by the attacker to the IoT device as a reflector with a source IP address set to the IP address of the victim who obtains the reflected replies and can be overloaded. To examine this kind of attack, there has to be four representatives of heterogeneous IoT devices involved: an IP camera, a smart light-bulb, a network printer, and a small singleboard computer Raspberry Pi. This article illustrates the possibility of the IoT devices to be integrated into DRDoS attack and to flood a network as well as their potential to form a targeted attack on a particular victim machine.