Title: Navigating the Threat Landscape of IoT: An Analysis of Attacks

Author: Shivansh Singh, Monika Sharma & Syed Akhter Hossain

Abstract: According to the International Telecommunication Union, a specialist body of the United Nations for ICTs, there were approximately 4.9 billion Internet users worldwide in 2021, and by 2023, this number had risen to over 5 billion. The rapidly increasing Internet is responsible for the expansion in the utilization of the connected devices. The Internet of Things ecosystem's expanding network of connected devices poses a significant cybersecurity risk. A leading company in IoT security order in their report revealed that in 2022, 42% of connected devices were either agentless or unagentable. According to the same report, this year's personal device count is two times higher, which raises the threat level. In Q4 of 2023, Cloudflare prevented over 5.2 million HTTP DDoS attacks. As per Microsoft's Digital Defense Report of year 2022, the company mitigated 1955 DDoS attempts on average every day in 2022, a 40% increase from the year before. User Datagram Protocol (UDP) spoof flood attacks increased from 16 to 55% in the first half of 2022, according to the same report. By 2025, there will likely be between 17 and 20 billion connected devices worldwide. As more devices are connected to one another, there are more potential entry points for cyberattacks. Every connected device can become a point of vulnerability that might be used to obtain unauthorized access, steal sensitive information, or launch serious cyberattacks. Furthermore, the diversity of IoT devices makes their security a burning issue. This paper presents a list of the most common attacks on each layer of the 5 layer architecture of the Internet of Things (IoT). This quick increase is due to the pervasive use of IoT devices in numerous businesses, homes, and essential infrastructures. IoT devices come in diverse designs, including self-driving cars, business sensors, medical equipment, and smart home products. Each type of device may have unique security requirements and vulnerabilities such as sensor spoofing, Gateway compromise, Business Logic attacks, Device Lifecycle Manipulation, and many more threats that must be addressed. Practical cybersecurity solutions addressing exclusively IoT devices is necessary. In this paper, we are focusing on security of 5 layers of IoT. Thus, this study provides a summary of the security challenges in each layer of Internet of Things. The goal is to identify weaknesses, open issues and suggest future directions to develop cybersecurity solutions for Internet of Things devices.

Keywords: IoT functioning, IoT threats, Device lifecycle manipulation, Business logic attacks, Middleware layer attacks, Business layer attacks

DOI: https://doi.org/10.1007/978-981-97-4149-6_3

https://link.springer.com/chapter/10.1007/978-981-97-4149-6_3