Chapter 17
Security in IoT Devices

N. Jeyanthi
https://orcid.org/0000-0002-6141-5467
VIT University, India

Shreyansh Banthia
VIT University, India

Akhil Sharma
VIT University, India

ABSTRACT

An attempt to do a comparison between the various DDoS attack types that exist by analysing them in various categories that can be formed, to provide a more comprehensive view of the problem that DDoS poses to the internet infrastructure today. Then DDoS and its relevance with respect to IoT (Internet of Things) devices are analysed where attack types have been explained and possible solutions available are analysed. This chapter does not propose any new solutions to mitigating the effects of DDoS attacks but just provides a general survey of the prevailing attack types along with analysis of the underlying structures that make these attacks possible, which would help researchers in understanding the DDoS problem better.

INTRODUCTION

Distributed Denial of Service attacks pose an imminent threat to the internet infrastructure, where the frequency of these attacks have increased in recent times many folds. Attackers constantly modify their attacking techniques to work around defence mechanisms in place, leaving the researchers to play catch-up with them. There is no silver bullet solution to this problem because each attack fundamentally differs from the other with respect to the part of the network system that it attacks, the way it attacks, the resources with which it attacks etc. With so many variables in place it's tough categorise solutions to these problems.

DOI: 10.4018/978-1-7998-5348-0.ch017

Now coming to DDoS attacks and their relation to IoT devices we have a scenario where according to IDC, the IoT market will hit evaluation of $7.1 trillion in revenue by 2020. Gartner predicts the IoT devices base to expand to 26 billion units by 2020. This gives us a perspective on the importance of IoT in our futures but at the same time this technology is susceptible to exploitation because of the security gaps that exist in the communication technologies that these devices employ.

We hope that this survey would go a long way in simplifying the myriad categories of attacks that are possible, thereby helping the research community to direct their research towards specific targets, enabling this focussed effort to make a bigger impact.

TAXONOMY OF THE DDOS ATTACK METHODS

Classifying by Degree of Automation

1. **Manual Attacks:** The offender physically try to find inaccessible machines for susceptibility, splits them, then proposes the attack code, and after charges the outset of the attack (Mirkovic & Reiher, 2002). After all the actions, it leads to progression of semi-automated attacks of DDoS.
2. **Semi-Automatic Attack:** The DDoS Network comprises of handler and specialist slave machines. The select, misuse and taint stages are automated. In the utilization stage, the offender species the attack sort, on-set, span and the casualty by means of the handler to specialists. Attacker tries to set up scripts for scanning and fitting of the attack code, then he uses those machines to define the type of attack and the address of the victim (Mirkovic & Reiher, 2002).
3. **Direct Communication:** Attack in type is done through strong-coding of IP address of handler machines in the attack code that is later introduced on the agent side (Houle & Weaver, 2001). The agent and handler mechanisms need to know each other's ID keeping in mind the end goal to impart. Every operator then reports its status to the handlers, who store its IP address in a record for later correspondence (Mirkovic & Reiher, 2002).
4. **Indirect Communication:** Through this attack a level of duplicity is expanded for the serviceability of a DDoS network. Late attacks give the case of utilizing IRC channels for specialist/handler correspondence. The utilization of IRC administrations replaces the capacity of a handler, since the IRC channel offers adequate namelessness to the offender.
5. **Attacks with Random Scanning:** Every composed host inquiry random addresses within the IP address area (Paxson & Weaver, 2003). This probably creates a high traffic volume since several machines research the same addresses. (CRv2) performed random scanning.
6. **Attacks with Hit-list Scanning:** A machine acting hit-list scanning finds all addresses from an outwardly provided list (Paxson & Weaver, 2003). When it finds the harmful machine, it will send one-half of the initial hit-list to the receiver and keeps the other half of the hit-list. This method grants for nice propagation speed (due to exponential spread) and no collisions throughout the scanning section.
7. **Attacks with Permutation Scanning:** In this scanning method, major composed machines share a typical pseudo-random permutation of the IP address area; every IP address is structured to the index during this permutation. A machine starts finding by using the index got from its IP address as a start line. Whenever it sees an already infected machine, it chooses a brand new random begin point (Mirkovic, Prier & Reiher, 2002).