NTNU
Norwegian University of Science and Technology

LIST: Lightweight Solutions for Securing IoT Devices against Mirai Malware Attack

Pallavi Kaliyar, Laszlo Erdodi, Sokratis Katsikas
Department of Information Security and Communication Technology
NTNU, Norway

Presented by: Pallavi Kaliyar, Post Doctoral Researcher, NTNU
17th October 2022

Our Contribution (1/2)

- First, In this paper we present a detailed analysis of the Mirai source code, which is publicly available on the git repository at GitHub since 2017. This analysis is important as it provides a more detailed description of the Mirai attack source code, i.e., what is the role of each Mirai source file in the execution of the Mirai attack.

- Our second contribution in this paper is the implementation of the Mirai code in a controlled environment, to show that although the Mirai attack has been long known, it is still very relevant, as a large number of devices are still vulnerable to it.

Contribution (2/2)

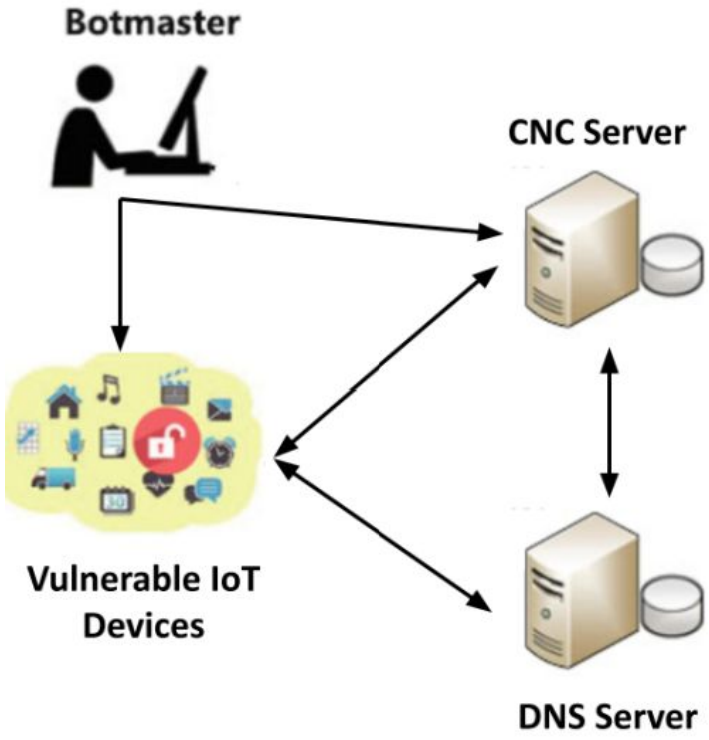
- Our third contribution in this paper is to propose three lightweight solutions to improve the security of IoT devices against Mirai and Mirai-like attacks. Contrary to previously proposed, state-of-the-art solutions, our solutions are applicable to both new and existing IoT devices, they do not require increased computational power, storage capability, or battery capacity, and they do not add any extra manufacturing cost to the devices.

DIFFERENT VARIANTS OF MIRAI

No.	Name	First Appearance	Exploit
1	Mirai original [5]	August 2016	Telnet 23/2323, brute force
2	Satori [10]	December 2017	Telnet 23/2323, Port 37215/52869, 2 exploits CVE-2014-8361 and CVE-2017-17215
3	Hajime [11]	March 2017	Telnet 23/2323, brute force, later closes the open ports
4	IoTroop [12]	October 2017	Vulnerability scanning instead of password brute-force
5	Okiru [13]	January 2018	IoT with RISC architecture, telnet default passwords 4 types of router exploits
6	Masuta, PureMasuta [14]	January 2018	EDB 38722 D-Link exploit
7	Jenx [15]	January 2018	2 exploits, CVE-2014-8361 and CVE-2017–17215
8	OMG [16]	March 2018	Make IoT a proxy server
9	Wicked [17]	June 2018	Port 80,81,8080,84433, new exploits, router exploits, cctv rce, CVE-2016-6277 command injection
10	Satori / 2018 [18]	July 2018	Android Debug Bridge (ADB) commands
11	Torii [19]	September 2018	Rich set of features for exfiltration of (sensitive) information, modular architecture capable of fetching and executing other commands and executables
12	Hakai, Yowai [20]	January 2019	Several hard coded exploits, ThinkPHP
13	Covid Mirai [21]	March 2020	TeamSpeak, Huawei default passwords
14	Satori – 2021 [22]	February 2021	Vantage Velocity field, Python script
15	Matryosh [23]	February 2021	Android Debug Bridge, TOR network is used

Mirai Attack Procedure

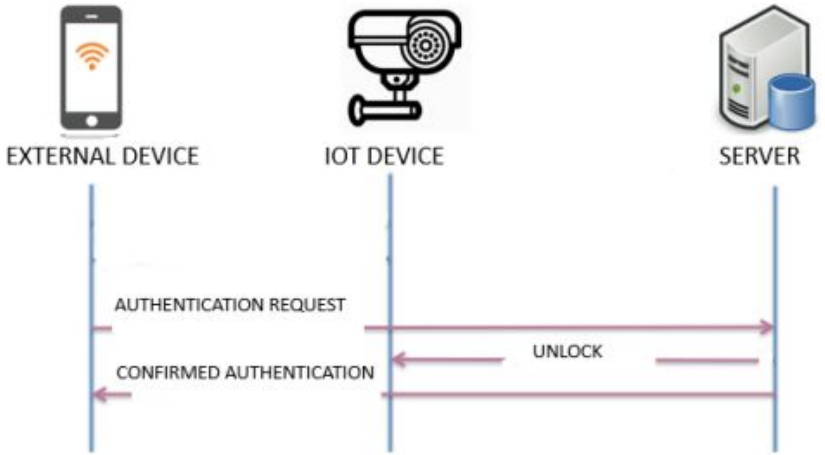
Figure here presents how to create a botnet made of IoT devices that a BotMaster/attacker can control to carry out a DDoS attack. Initially, the Command and Control (CNC) server starts scanning for IP addresses with port 23 (telnet) open to control the bots. When such devices are found, the attacker injects the malware code as it controls the shell, and then the bot's information (IP address, port, and authentication credentials



Proposed Solutions

Lightweight security solutions to mitigate Mirai Attack

1. **Secure Authentication**
2. **Biometric Authentication**
3. **Using One Time Password**



Conclusion

- In this paper we discussed how vulnerabilities of IoT devices can be exploited by a class of malware called Mirai, which creates a botnet of IoT devices.
- We presented a detailed analysis of the Mirai malware source code, and we implemented the Mirai attack using the same code, that is available on the Github.
- We believe that the Mirai attack is still very relevant and that resource-constrained IoT devices are vulnerable to it. We reviewed existing security solutions, whose take up in practice presents a number of difficulties.
- We proposed three new ones, that provide security without increasing the manufacturing cost of the devices.
- Our future research will focus on validating these solutions by means of extensive experimentation.

Thank you for your attention!

Any Queries?

https://sites.google.com/site/pallavikaliyar/