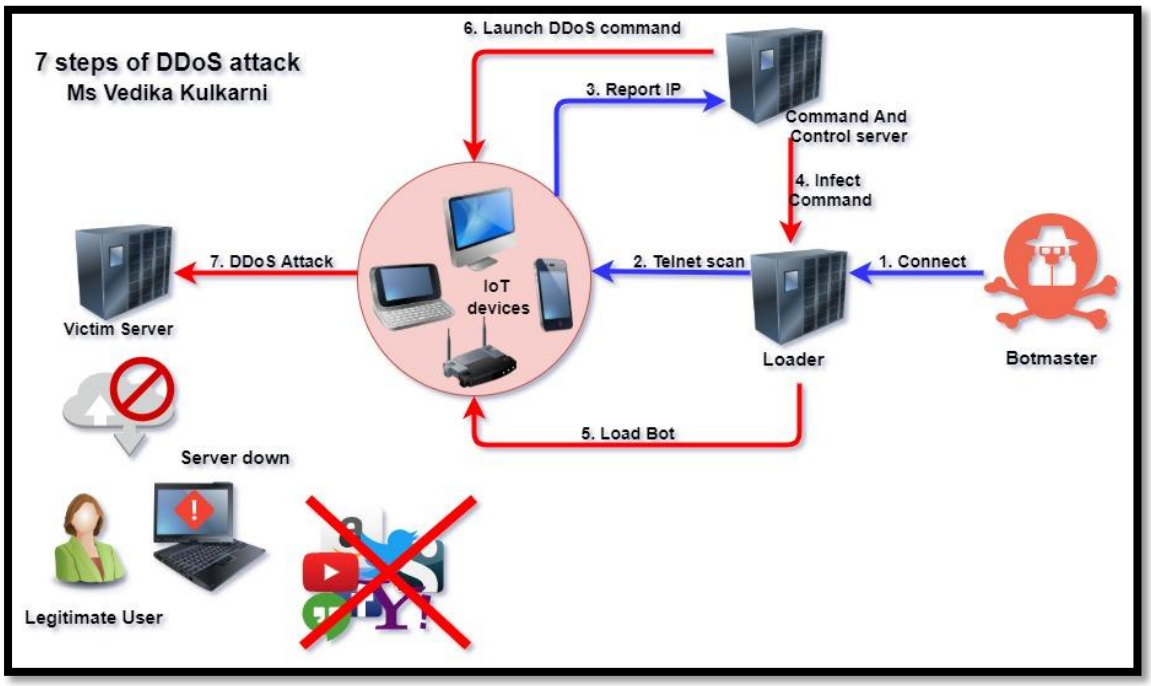
BLOCKCHAIN SOLUTION TO DDoS ATTACKS

Ms Vedika Kulkarni

INTRODUCTION:

Distributed-Denial-of-Service attack causes illegitimate traffic on the victim server due to which the service becomes unavailable to legitimate users. The attacker creates an army of bots. On his command, all the devices send requests to the victim server. The server gets overloaded due to which the genuine users are denied the service.

HOW THE ATTACK HAPPENS:



Consider Mirai botnet for example. A Mirai botnet attack unfolds in a seven-stage process:

(1) Mirai cracks into a weakly configured IoT devices by trying the 62 hardcoded username and password pairs.
(2) The bot sends the device details to the report server.
(3) The botmaster i.e. the attacker locates new targets through the Control and Command (CnC) server and by communication with report server through Tor.
(4) The botmaster loads an infected command in the loader.
(5) The loader loads this command into the target device which leads to installation of malware.
(6) After the device is configured, the attacker sends command using the CnC server to launch DDoS attack on the target server.
(7) The bots begin to attack the server in one of the several forms of DDoS attack.

IDENTIFICATION OF PROBLEM and OUTLINE OF THE SOLUTION:

Once the attacker gains access to the IoT device, he is able to perform communication with any server such as the report and CnC (Control and Command) server. My solution intends to solve this problem by preventing IoT device from communicating with unsafe IP addresses such as the CnC server and the report server.

TECHNICAL DETAILS:

There are three components in the system: the target IoT device, the devices connected to it and the IP addresses allowed to communicate with it, the Blockchain. Here are technical details of the **Blockchain component.**

Tools and Technologies:

- Public Blockchain platform – Bitcoin / Ethereum / Hyperledger Fabric
- CSPRNG Technology
- Elliptical Curve Multiplication Algorithm
- RSA Algorithm (Rivest-Shamir-Adleman)

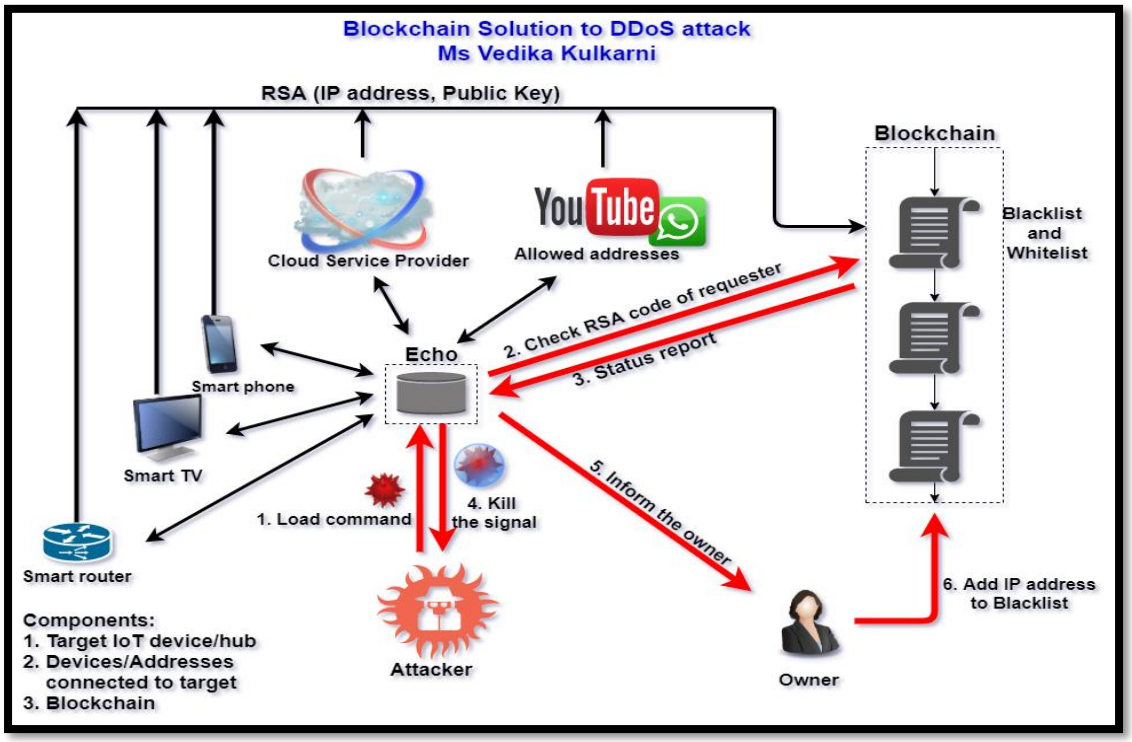
Feasibility of Implementation:

The proposed solution can be **easily implemented** without disturbing the **current architecture** of connected IoT devices. IoT devices are not required to do mining as the Bitcoin blockchain already has **dedicated miners**. Hence, IoT devices need not be modified.

SET UP:

1) The method will use **Bitcoin blockchain** as it is the most secure platform for communication till date. Other options that can be used are **Ethereum, Hyperledger** or a **private blockchain** (not recommended).
2) In any system, the IoT device/hub of interest is connected to other devices and sites. For example, the Amazon Echo can communicate with smart TV, smart speakers, smart router, etc as well as with the Cloud Service Provider (CSP) and selected sites.
3) The user will make a whitelist of all these allowed addresses. Only these are allowed to communicate with the device which will be targeted.
4) Owner is given a private key generated by the **Cryptographically secure pseudorandom number generator (CSPRNG) technology**. Public key can be derived by **Elliptic Curve Multiplication (ECM) algorithm.**
5) Each of the addresses in the whitelist is encrypted by the Public Key using **the RSA algorithm.** The owner will add this list of encrypted addresses to the blockchain.
6) Public key is visible to all and it does not need protection. It is stored on the IoT device/hub.

WORKING:



1) When attacker sends commands to the device to load the malware, the device will not instantly follow the command. It will encrypt the IP address of the requester (who sent the command) with the public key and then **check if it is in the whitelist of the user**.
2) If yes, then command will be executed. But if not present, then the device will **kill the command to load malware**. Thus, malware is not loaded.
3) Further the device will **automatically inform the owner** about this attempt. The owner can then add the IP address to the blacklist and store it on the blockchain. This will also help the other devices **globally** to stay alert of such IP address.
4) The advantage of encryption is that even though the encrypted form of IP addresses is visible to all, the attacker cannot figure out the IP addresses in whitelist. This is due to **strong encryption by RSA algorithm** due to which it is almost impossible to decrypt the code without the private key which is present only with the owner.
5) If the attacker tries to tamper with the whitelist stored on the blockchain, then it will not be mined as it is as invalid transaction. Only the owner has the rights to modify the list. Hence, the attacker's attempt will become unsuccessful and the owner will get informed automatically and immediately.

RSA ENCRYPTION ALGORITHM:

1) Convert the message M (IP address in our case) into an integer m by the **Padding Scheme Protocol**
2) If e is the public key then

$$C = m^e \pmod{n}$$ … C is the ciphertext (stored on blockchain)

RSA DECRYPTION ALGORITHM:

1) If d is the private key, then

$$m = C^d \pmod{n}$$

2) Given m, the original message M can be recovered by **reversing the padding scheme**.

REFERENCES:

1. https://en.wikipedia.org/wiki/RSA_(cryptosystem)
2. https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/
3. https://en.wikipedia.org/wiki/Blockchain
4. https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/
5. Aldoaies B.H., Almagwashi H.,Exploitation of the Promising Technology: Using BlockChain to Enhance the Security of IoT,(2018) 21st Saudi Computer Society National Computer Conference, NCC 2018, , art. no. 8593102
6. Li, Dongxing & Peng, Wei & Deng, Wenping & Gai, Fangyu. (2018). A Blockchain-Based Authentication and Security Mechanism for IoT. 1-6. 10.1109/ICCCN.2018.8487449.