Networks Lab – DoS (Week 10)

Nikita Bogomazov

Innopolis University

n.bogomazov@innopolis.ru

March 28, 2019

For this task:

- We will discuss what is a Denial of Service attack & a way to counter it
- You will write a simple DoS tool (in any language you want (woohoo!))
- You will modify your torrent-node to mitigate a (D)DoS attack

Definition:

- DoS (Denial of Service) - resource exhaustion attack which leads to service unavailability.

DoS vs DDoS:

- DDoS is an attack in which multiple nodes spam a single service
- DoS can be done from a single node, but is easily mitigated

Why? Who?

- competitors trying to take down each other during crucial events to generate more profit
- gamers trying to influence events in multiplayer games
- hackers taking down services for fun and\or profit
- naive programmers writing poorly designed software which makes to much requests

How?

- software tools
- hire a botnet
- write your own poor tools

We will examine a variation of the SYN Flood attack

SYN FLood

- During a TCP 3-way handshake you only send first SYN and don’t continue the communication process
- By doing this your reserve resources on the server side and prevent it to process real users and request

Relating to your project:

- Your node sends & accepts multiple “SYNC” msgs all the time
- In most cases it is redundant because new nodes don’t enter the network with such frequency
- For any single node in the network such volume of msgs from other nodes can be considered as a DDoS attack and we need to do something with it

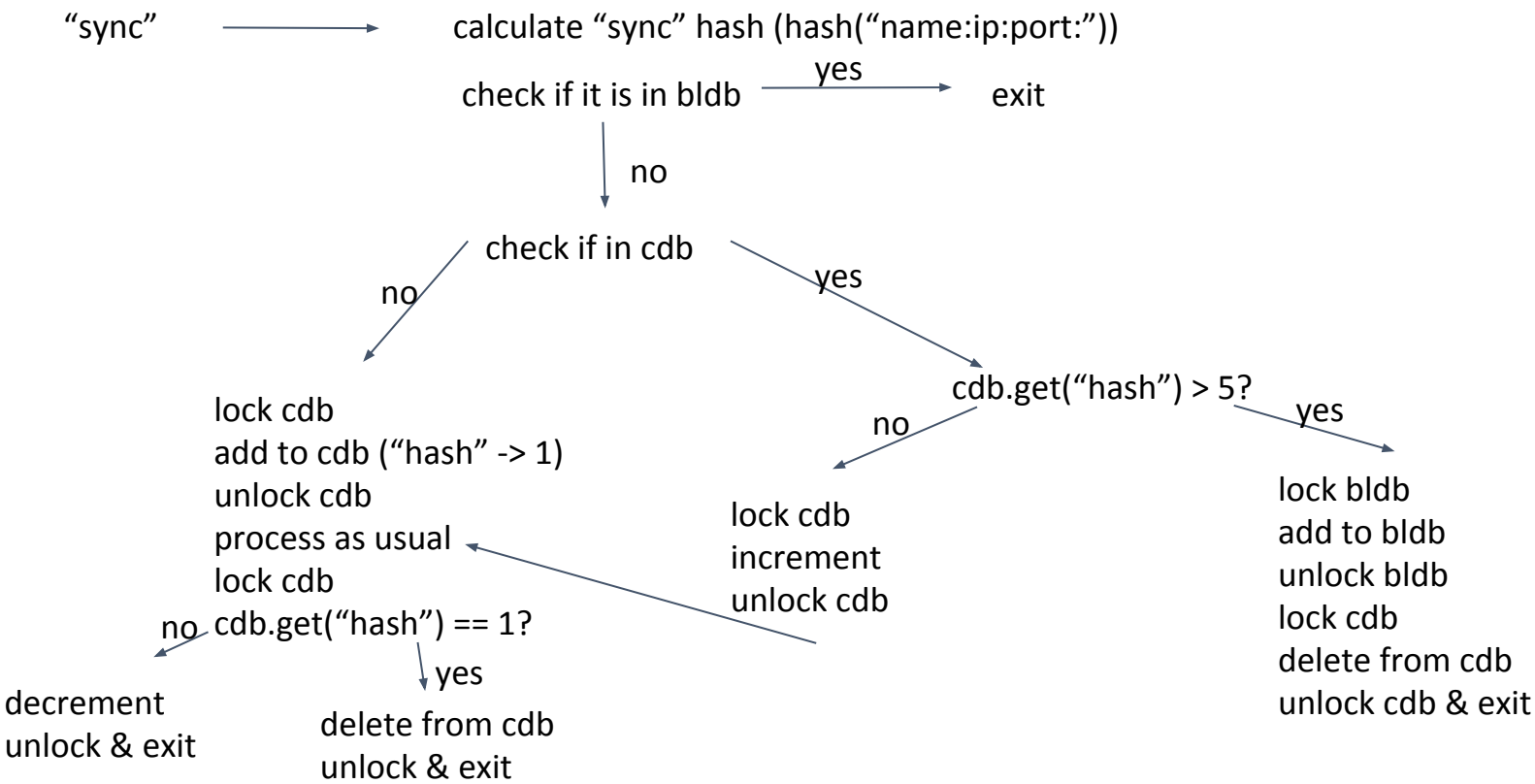
How to distinguish spammers in our network?

- First, we will limit the frequency with which we send messages to 5 - 10 sec
- With this in mind we can plan the counter measures to distinguish spammers
- For this we will include new data structures and modify the “sync” msg processing algorithm

Data Structures

- Known hosts db (kdb) will be still used to store the network map in our node (hashmap(“name:ip:port:” -> “file1,...”))
- Current db (cdb) will be used to store info about “sync” msg being processed from other nodes (hashmap(“name:ip:port:” -> n (number of “syncs” being processed now)))
- Blacklist db (bldb) to store nodes who are ignored (set(“name:ip:port:”))

Algorithm change:



Lab tasks:

- modify your code to send “sync”s once in 5-10 seconds
- modify your “sync” processing code according to the provided algorithm (1 point)
- create a small tool (in any language) to simulate a DoS attack on a given ip:port to test your (or any other) node (1 point)
- Submit an archive with: modified code, DoS tool code, report describing what you did, what you used and how to test it