Adaptive DDoS Protection

Patrik Goldschmidt
xgolds00@stud.fit.vutbr.cz

#34

What Is It All About?

- DDoS attacks are frequent cybersecurity threats.
- Here at BUT FIT, organization CESNET develops a software to protect against them.
- Currently, 4 different mitigation methods against SYN Flood attacks are implemented.
- Methods differ in required resources and in the ability to protect against various attack variants.
- Therefore, a mechanism to switch between them and choose the most optimal one is required.

Why Should I Care?

- Bad guys like to DDoS (Cisco prognosis - 14.5M attacks p.a by 2022).
- TCP is a popular target.

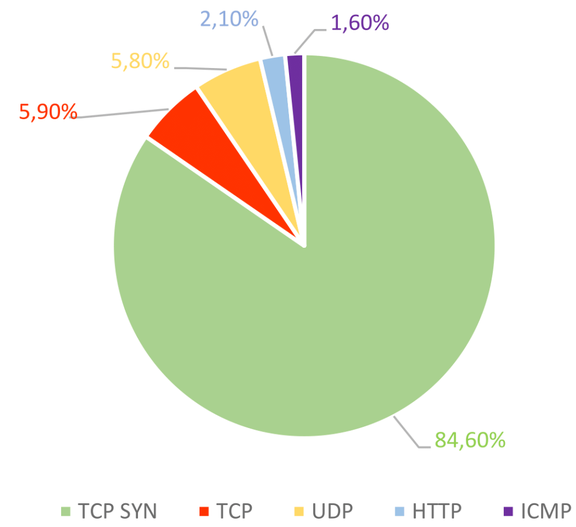

Figure 1: Distribution of DDoS attacks by type. Q4 2019. by Kaspersky Lab (DDoS report on securelist.com)

Mitigation - "SYN Cookies"

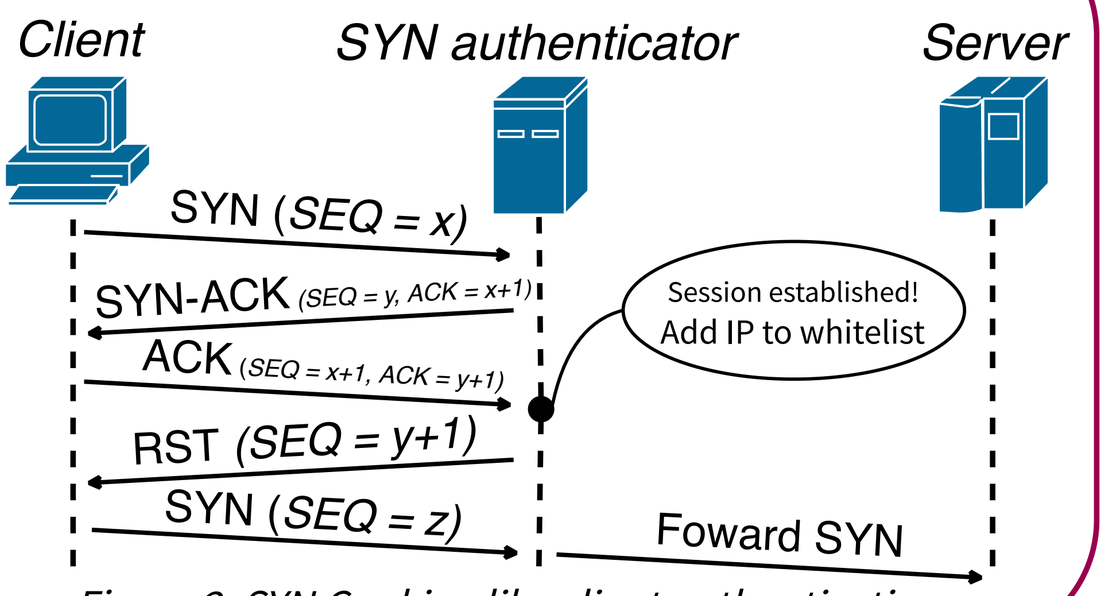

Figure 2: SYN Cookies-like client authentication

Mitigation - Reset Cookies

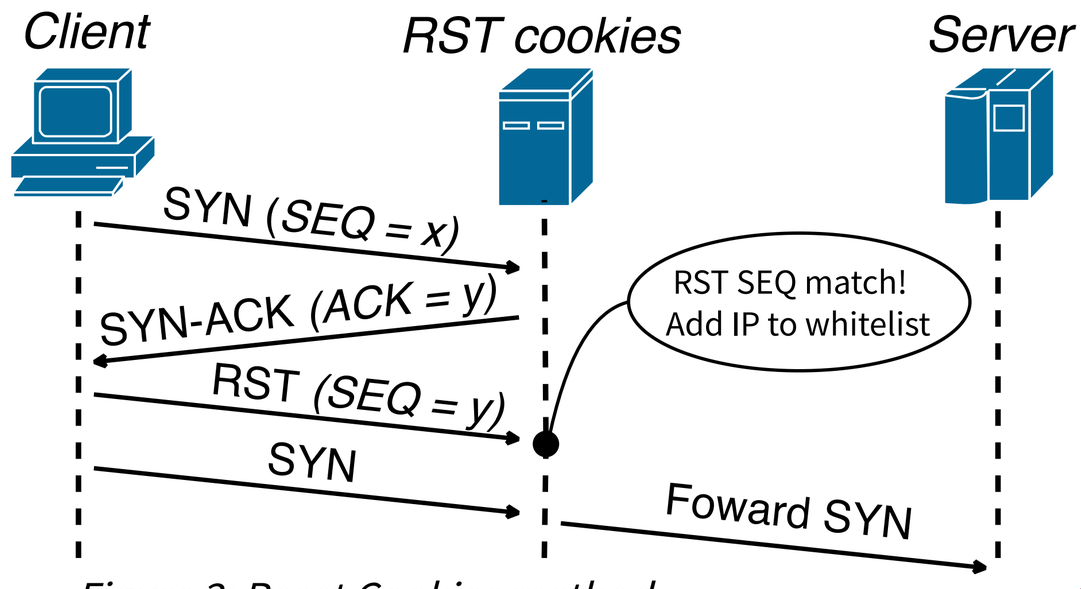

Figure 3: Reset Cookies method

MITIGATION - SYN DROP (ACKS = 0)

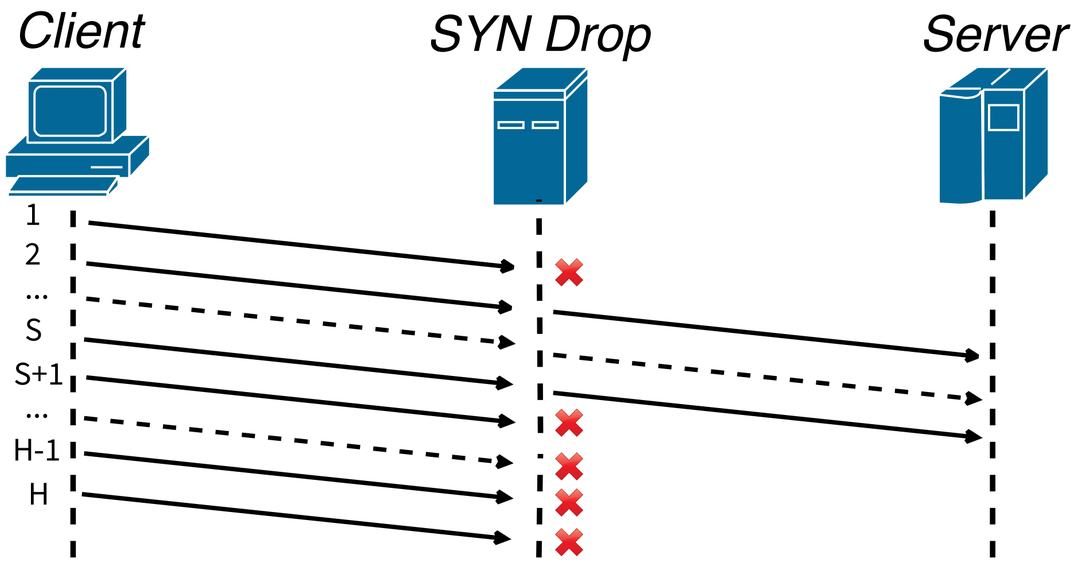

Figure 4: SYN Drop method

Deciding Which Method To Use

- Goal: Mitigate the attack as best as possible without the end-user noticing.
- Approach: Choose a method able to mitigate the attack with the smallest impact on the end-user.
- Realization:
  - Rate the methods based on the end-user impact.
  - Monitor the network to detect the attack type.
  - Select a suitable method with the best rating.
  - Monitor the mitigation process and react.

More Information

- Part of the CESNET's security research project.
- Offers for students, information for enterprises.
- Contact: tmc-info@cesnet.cz.