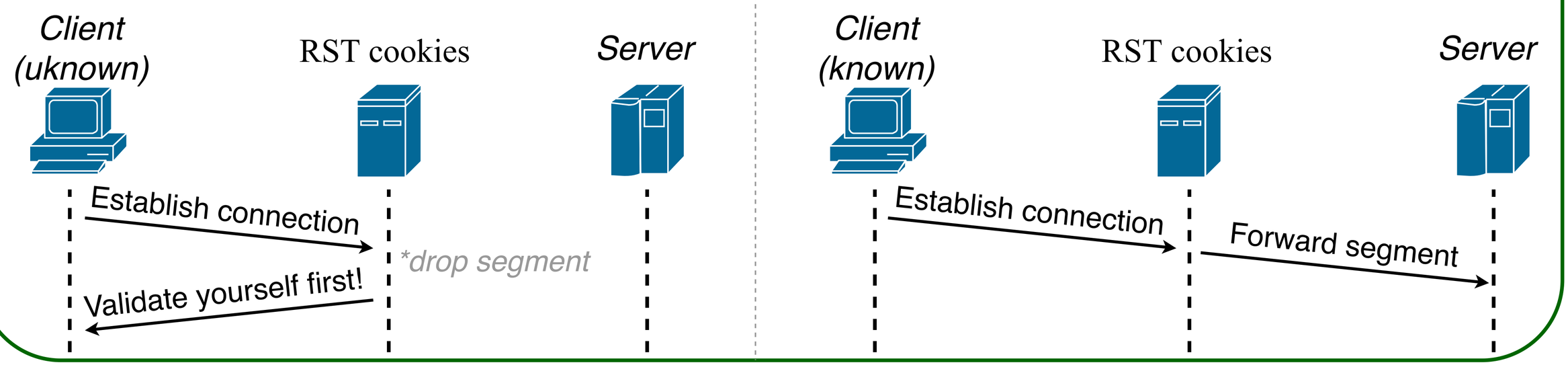
TCP Reset Cookies

Patrik Goldschmidt
xgolds00@stud.fit.vutbr.cz

#57

High-Level Overview



Why Should I Care?

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

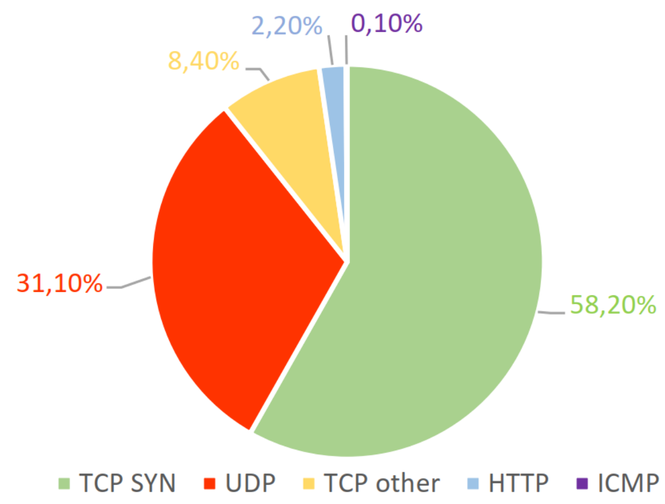


Figure 3: Distribution of DDoS attacks by type. Q4 2018. by Kaspersky Lab (DDoS report on securelist.com)

What Is It?

TCP Reset cookies is a heuristic DDoS mitigation technique, which utilizes the three-way-handshake mechanism. The main idea is to establish a security association with clients before allowing their connection requests. This is achieved by intentionally crafting an invalid SYN-ACK response to the first SYN received from a client.

Why Should I Use That?

- Blocks regular as well as more sophisticated DoS SYN Floods.
- Limits and blocks attackers who are somehow able to bypass the security mechanism.
- Able to create lists of both trusted and untrusted hosts.

How Does It Work?

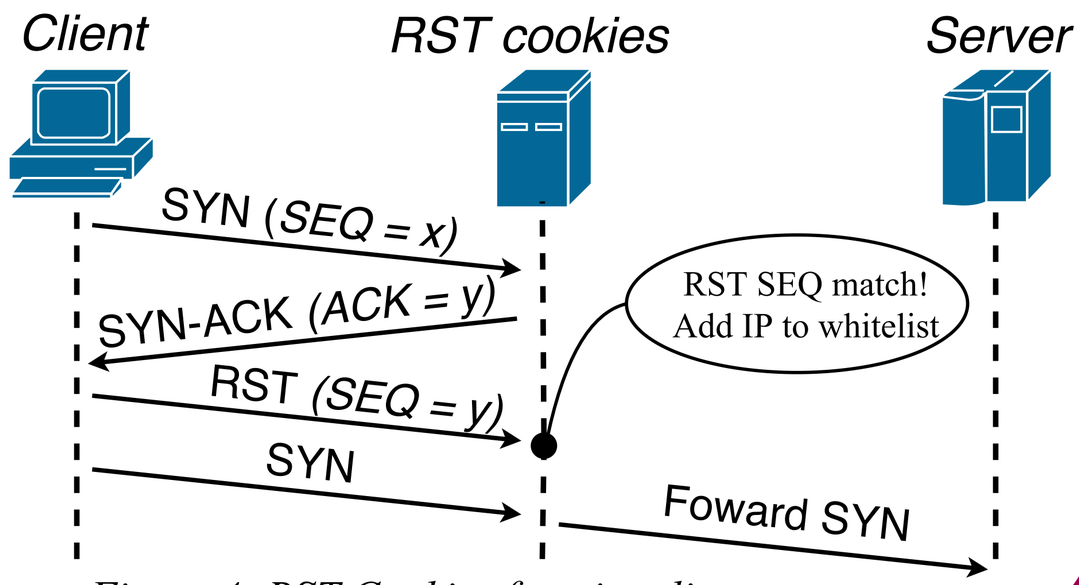


Figure 4: RST Cookies functionality

What Is The Cost?

- First attempt to establish a session always fails.
- And TCP SYN retransmission takes some time...
- Up to 1 second, dependend on the host OS.

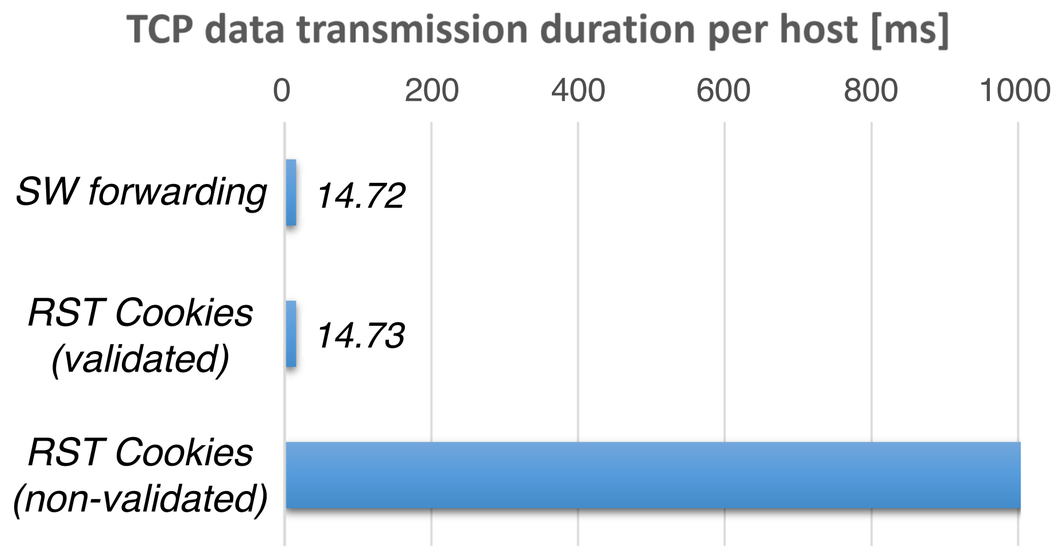


Figure 5: Transaction time performance comparison (Scientific Linux 7.4)

Where Does That Run?

Integrated into DDoS protection solution by CESNET, deployed on CESNET's backbone and NIX.CZ.