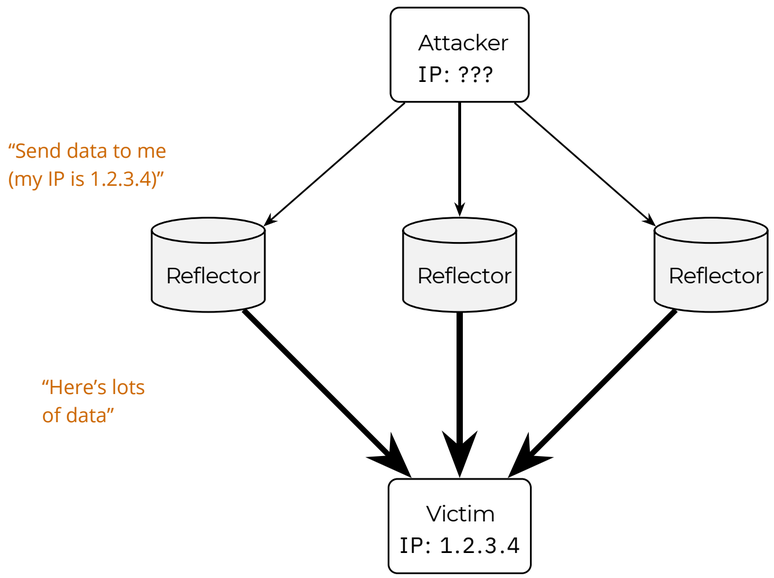
DDoS Amplification Honeypots

by Duncan Hill
Supervisor: Harm Griffioen

1 The Problem

Distributed Denial of Service (DDoS) amplification attacks:
Victim's network is overwhelmed with traffic.
Attackers use servers to amplify how big their attack can be, using servers that return bigger packets than they receive.



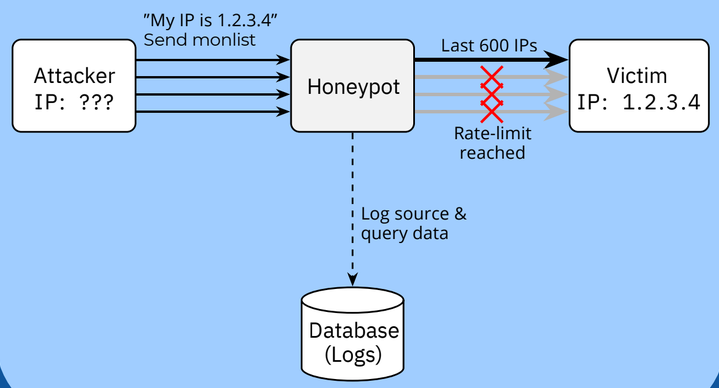
Network Time Protocol has this vulnerability.
Monlist returns last 600 IPs.
Largely fixed, but some servers still have it

2 The Questions

- Who is being targeted?
- When do attacks happen?
- What parts are still used?

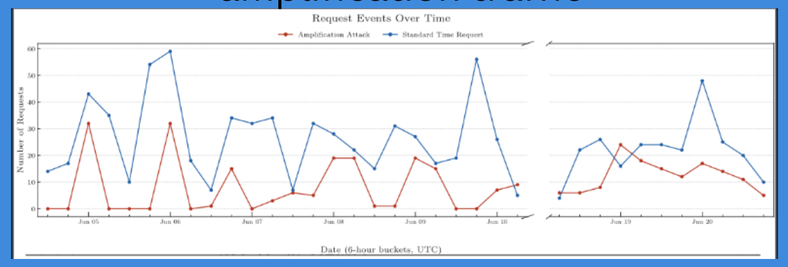
3 The Method

Honeypot pretends to be vulnerable server.
But, rate-limit traffic.



4 The Results

Succesful monitoring of NTP amplification traffic

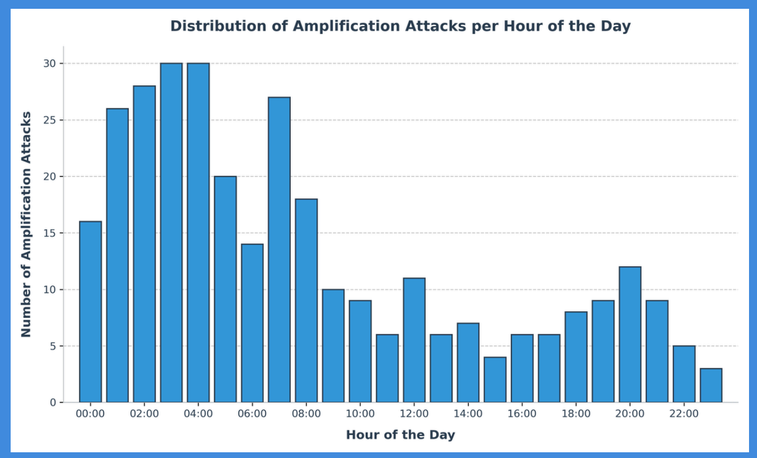


No large monlist request floods.
Due to small amplification

1203 total requests:
- 320 monlist
- 883 time

Monlist packets only sent to US and NL
Time requests mostly to sensors.

Nocturnal spike:



Future Work:
- Longer study
- Bigger amplification