

DNS based DDoS mitigation solution

Issue

Sukhun Yang

Seoul National University

August 19, 2023

Contents

- 1 Diagram
 - Case 1: Accept
 - Case 2: Abort
- 2 Issue

Table of Contents

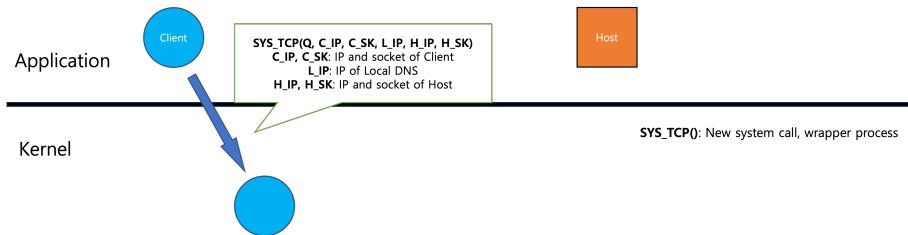
- 1 Diagram
 - Case 1: Accept
 - Case 2: Abort

- 2 Issue

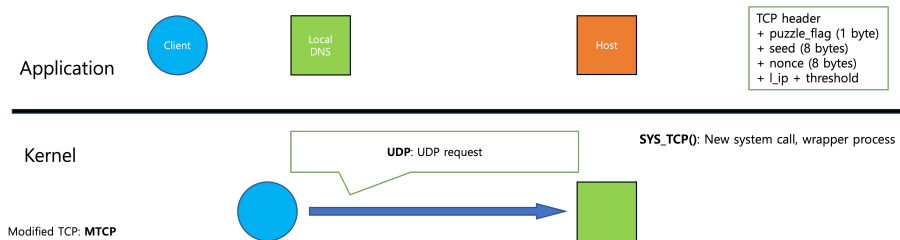
Puzzle policy

Assumed that the puzzle policy already exists.

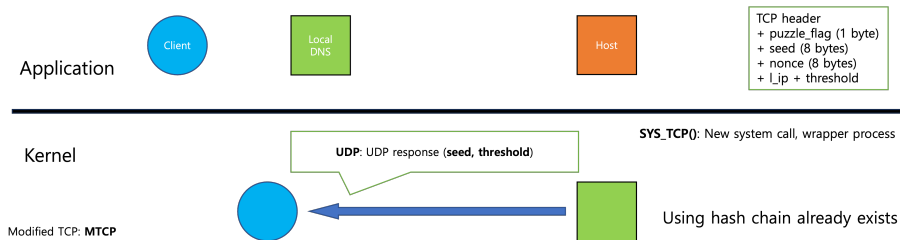
Case 1: Accept



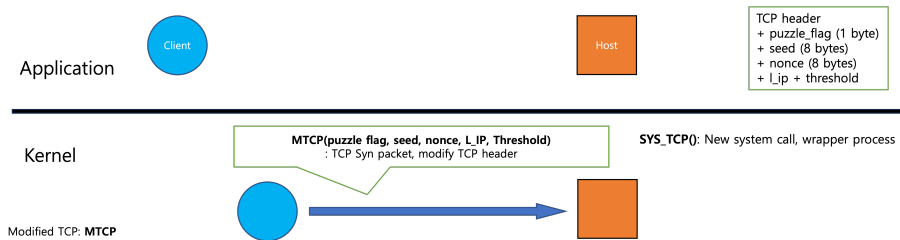
Case 1: Accept



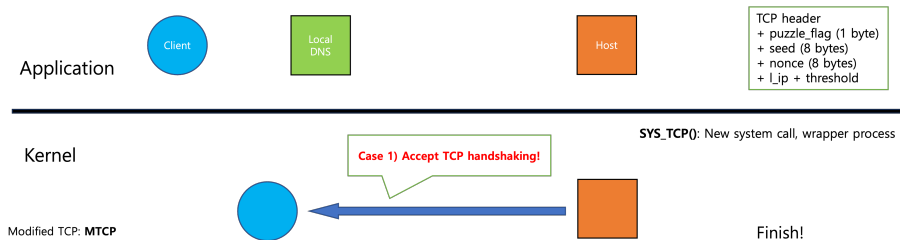
Case 1: Accept



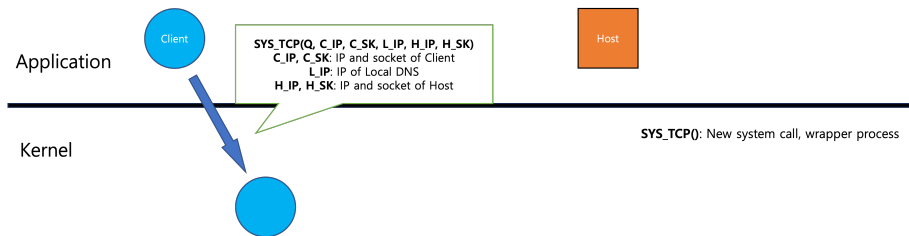
Case 1: Accept



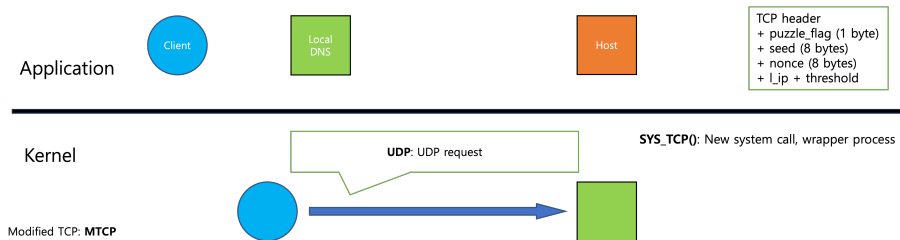
Case 1: Accept



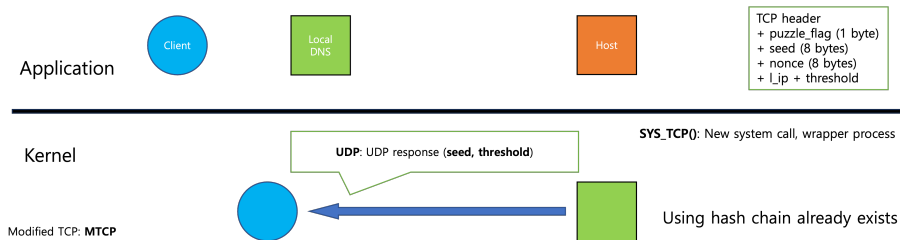
Case 2: Abort



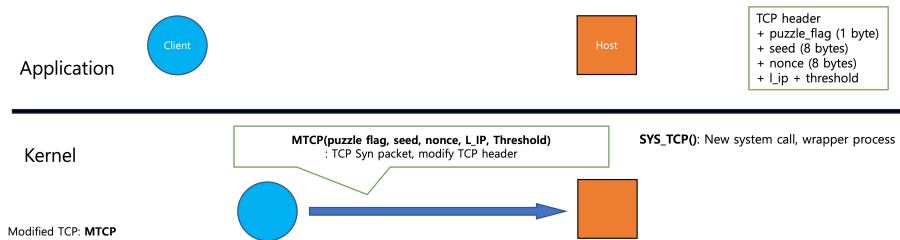
Case 2: Abort



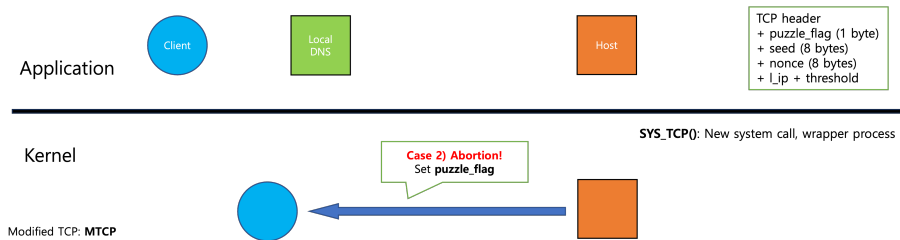
Case 2: Abort



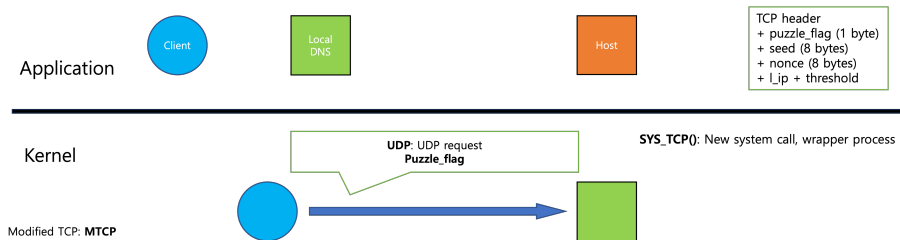
Case 2: Abort



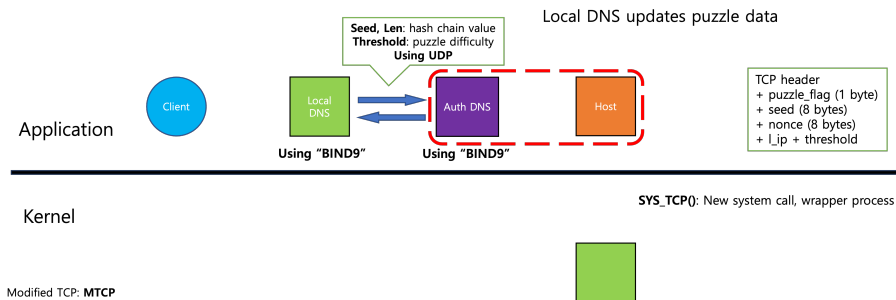
Case 2: Abort



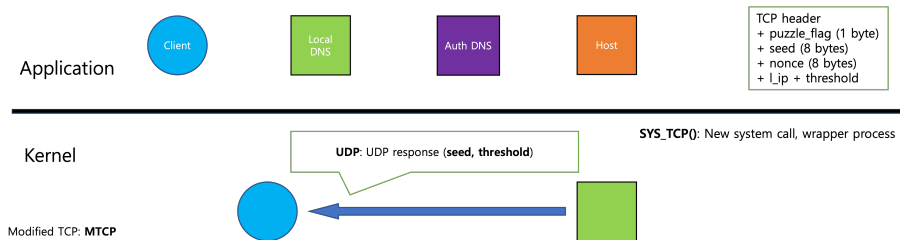
Case 2: Abort



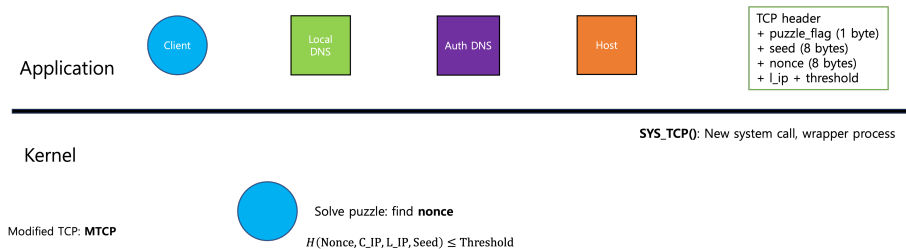
Case 2: Abort



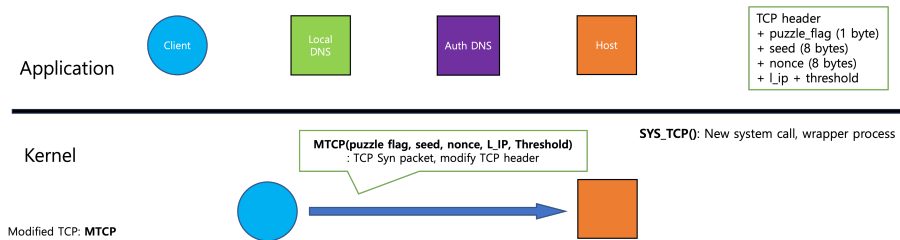
Case 2: Abort



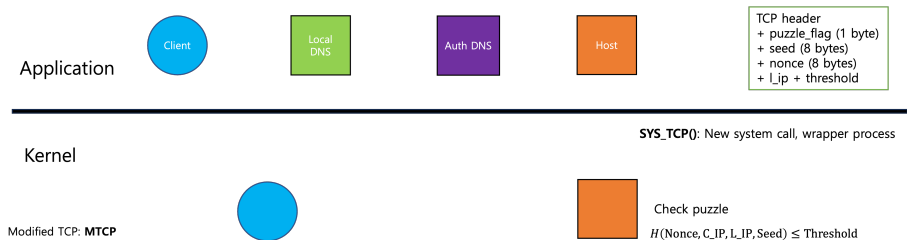
Case 2: Abort



Case 2: Abort



Case 2: Abort



Case 2: Abort

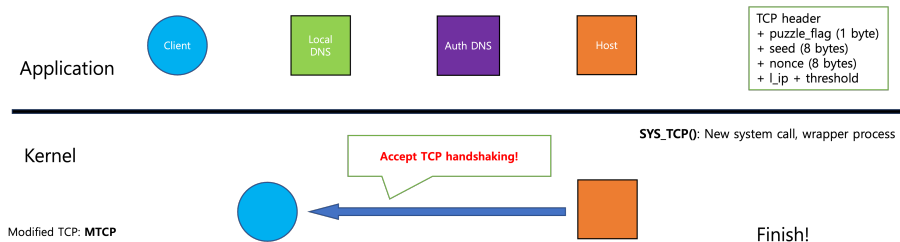


Table of Contents

- 1 Diagram
 - Case 1: Accept
 - Case 2: Abort

- 2 Issue

Questions

Timing of update puzzle information

- Client → Local DNS
- Local DNS → Authoritative Name Server

Issue

- Case 1: Client get exist puzzle from Local DNS → Accept TCP 3-way handshaking
 - Case 2: Client get exist puzzle from Local DNS → Abort TCP 3-way handshaking → Client request puzzle to Local DNS → Local DNS get puzzle from Auth. NS → Local DNS send puzzle to Client → Accept TCP 3-way handshaking
- ① If there is an overlapping period, then corresponds to Case 1 because handshaking accepts
 - ② Local DNS updates puzzle information only when Aborted (Case 2)
 - ③ If there is an overlapping period, the puzzle is not updated in the current diagram