DNS based DDoS mitigation solution

Schematic Diagram & Progress

Sukhun Yang

Seoul National University

August 18, 2023

Contents

Table of Contents

Architecture

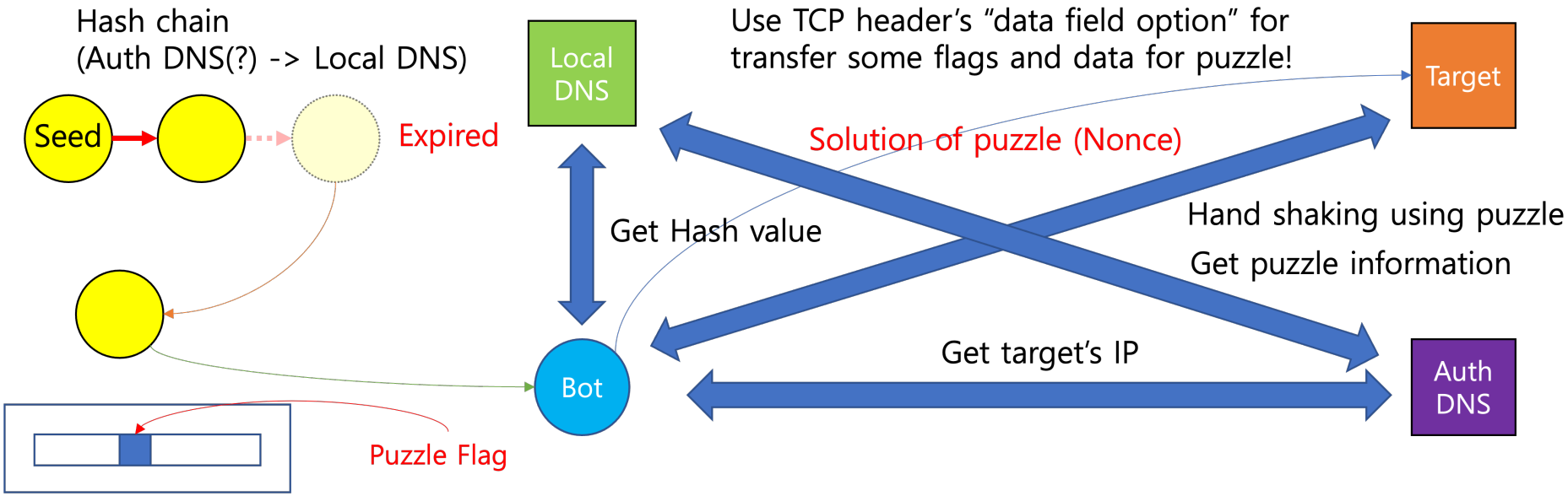


Figure 1: Architecture

Testbed

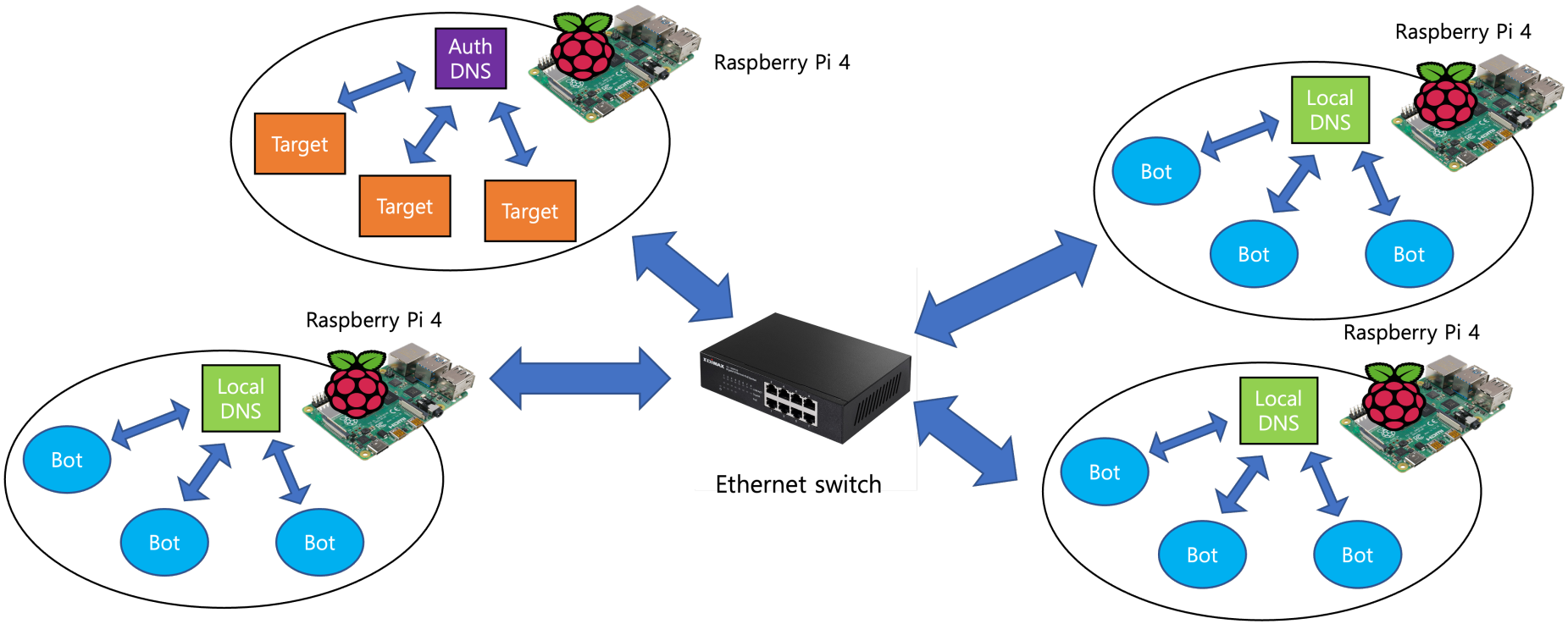
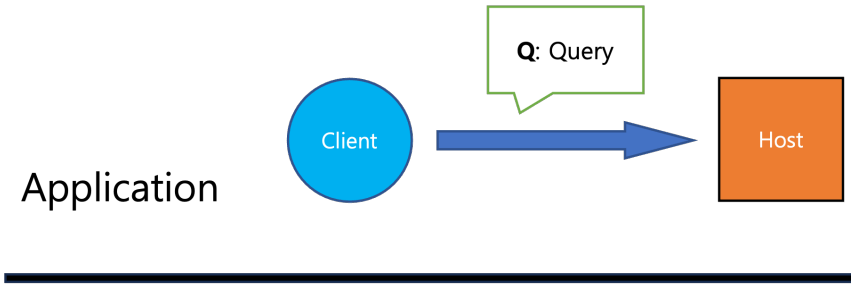


Figure 2: Testbed

Schematic Diagram



Schematic Diagram

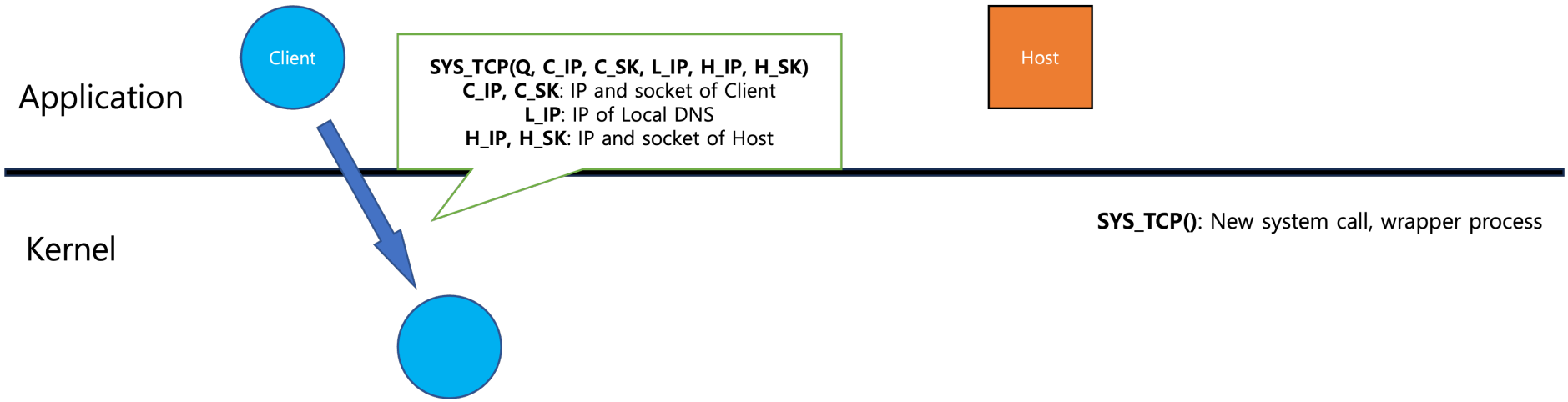
Application

Set **puzzle_flag** = 1!

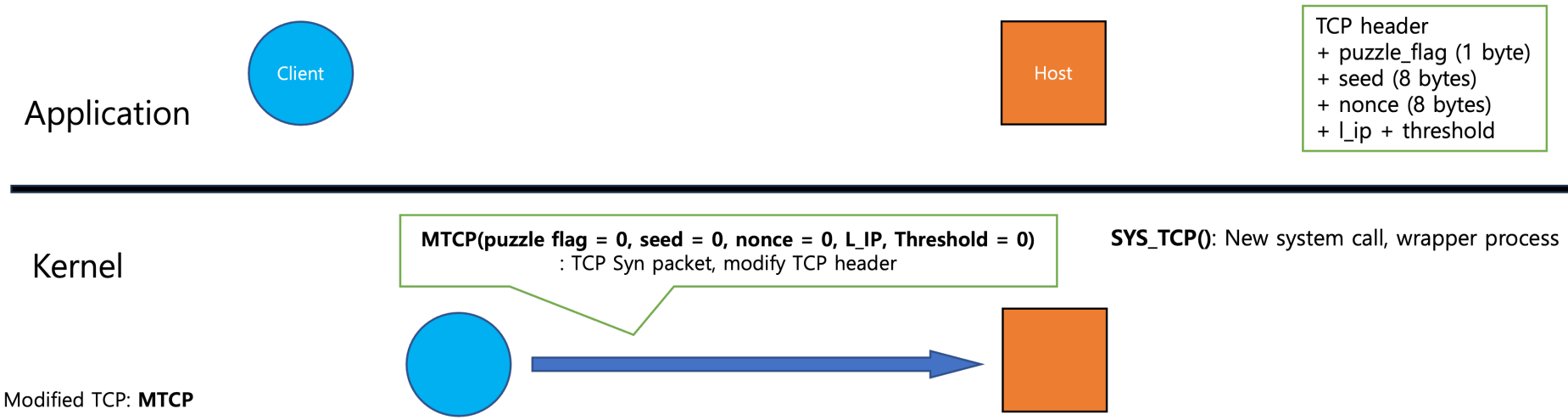
puzzle_flag = 0: without puzzle
puzzle_flag > 0: difficulty of puzzle

Kernel

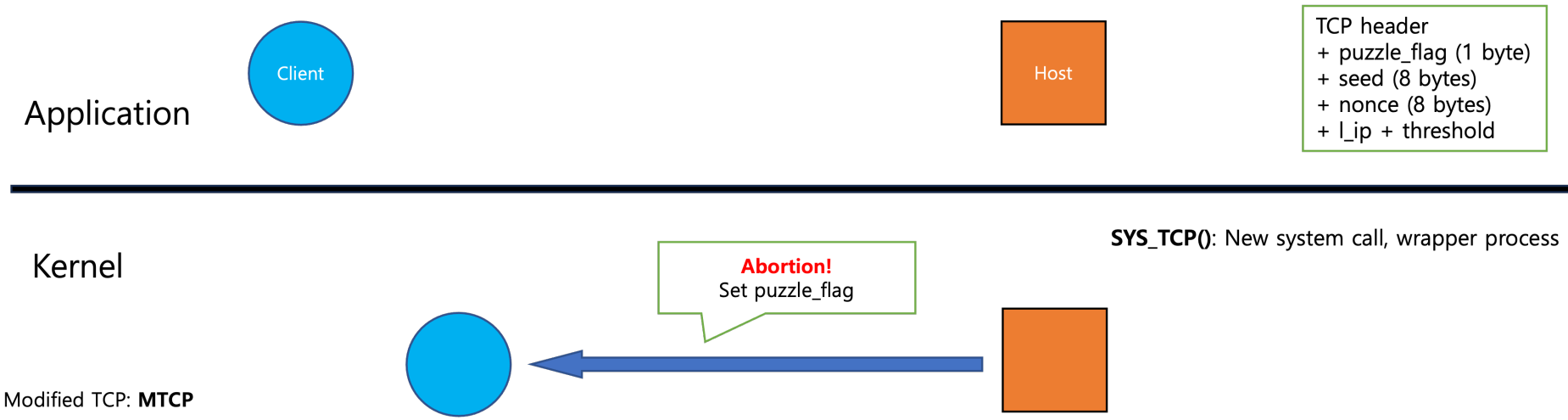
Schematic Diagram



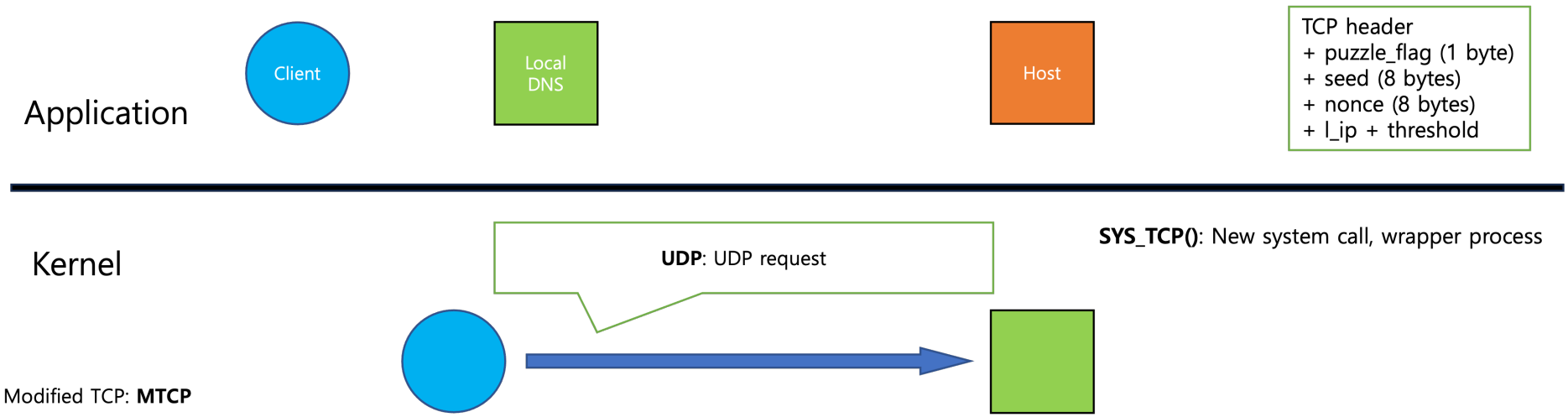
Schematic Diagram



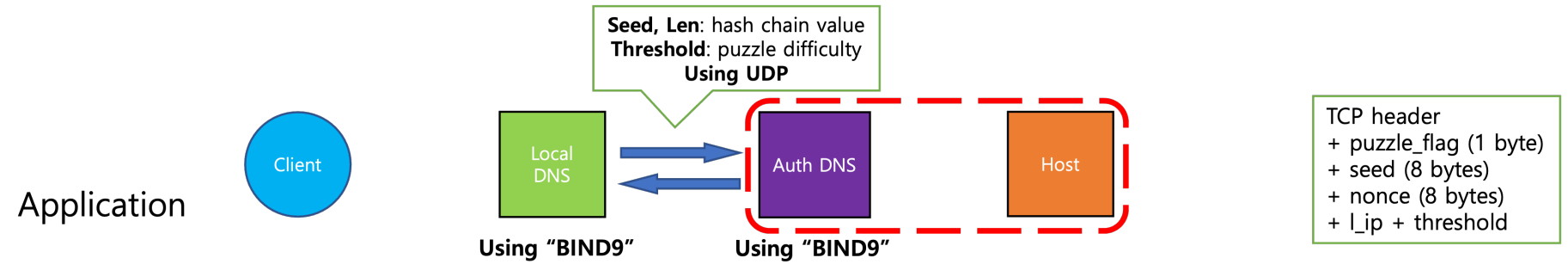
Schematic Diagram



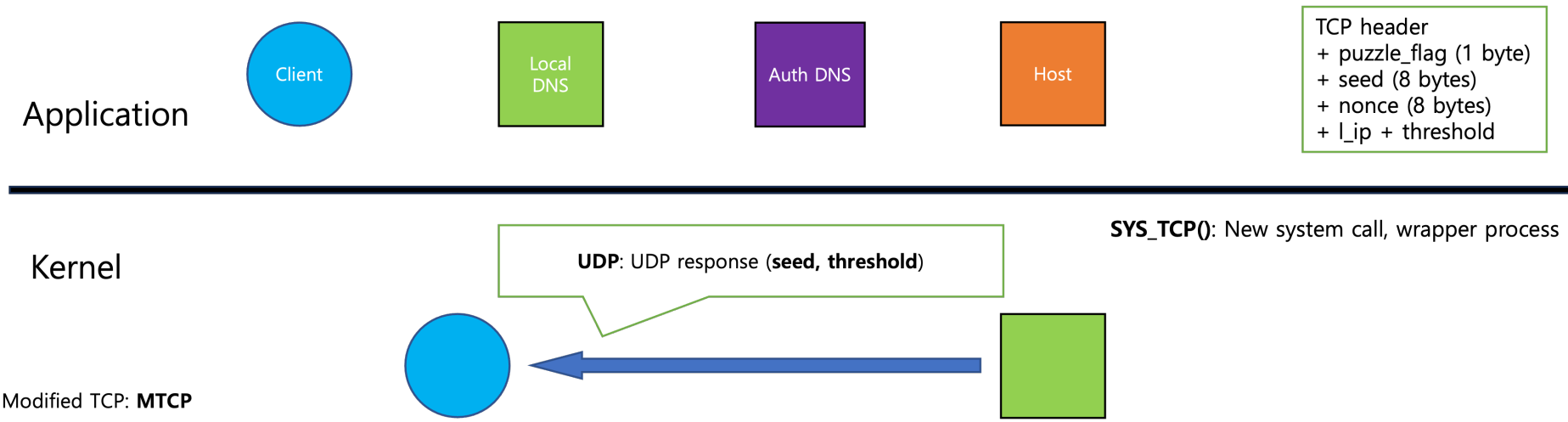
Schematic Diagram



Schematic Diagram

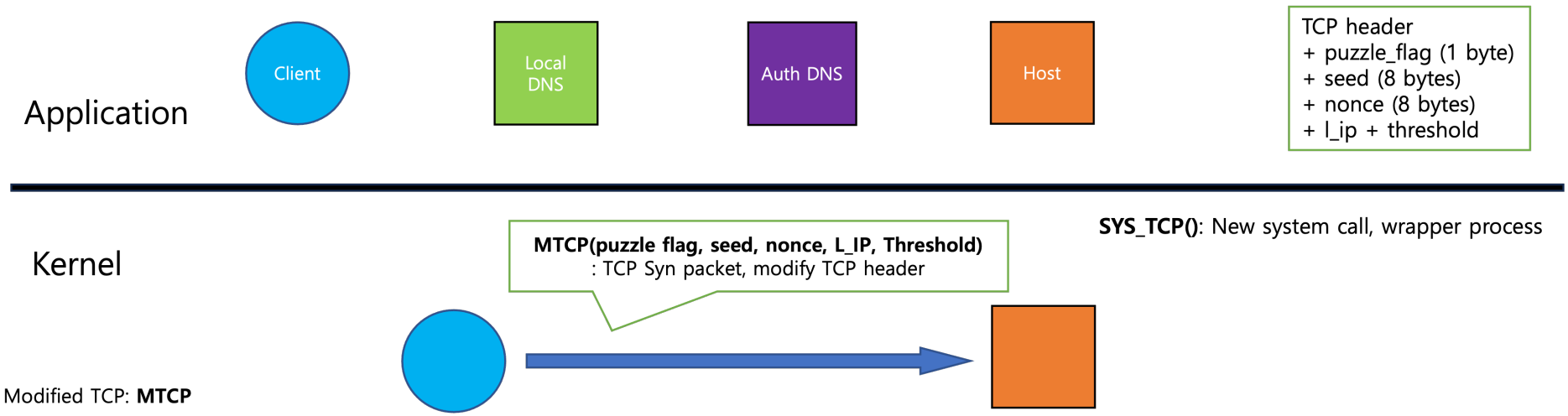


Schematic Diagram

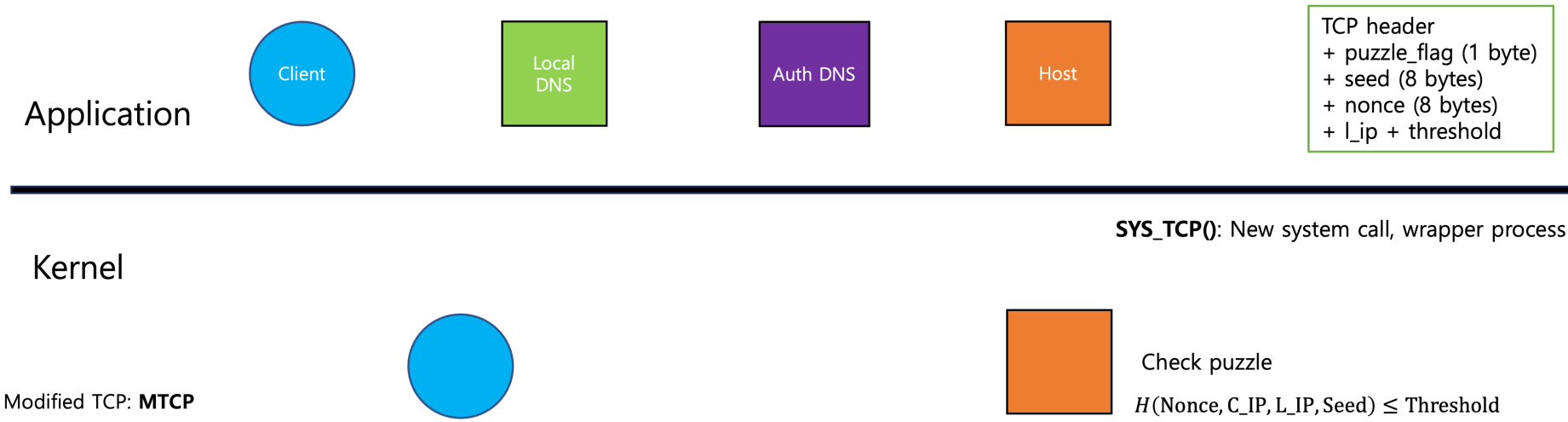


Schematic Diagram

Schematic Diagram



Schematic Diagram



Schematic Diagram

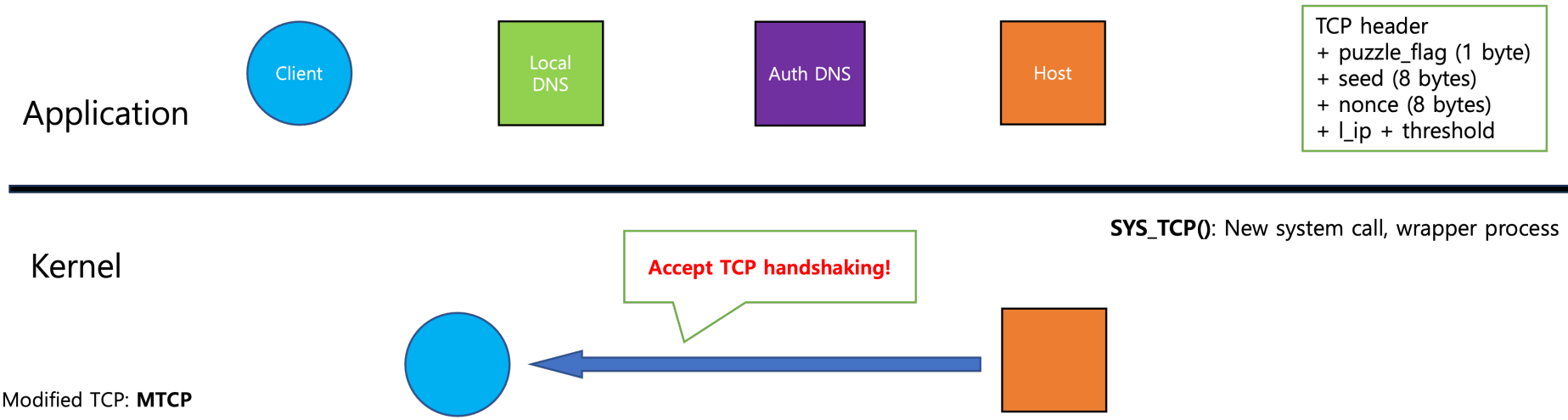


Table of Contents

Specification

Detailed parameters and values are appeared in above diagram.
The following is a brief summary of to-do list.

Let's talk detailed specification after today's meeting!

To-do list

Plan to make wrapper process as syscall at linux kernel

Client

- New syscall **SYS_TCP()** as wrapper process
- Modify TCP handshaking process in linux kernel

DNS

- UDP socket programming (**BIND9**) of local DNS and authoritative DNS

Host

- Autonomous system for control difficulties automatically

TCP header

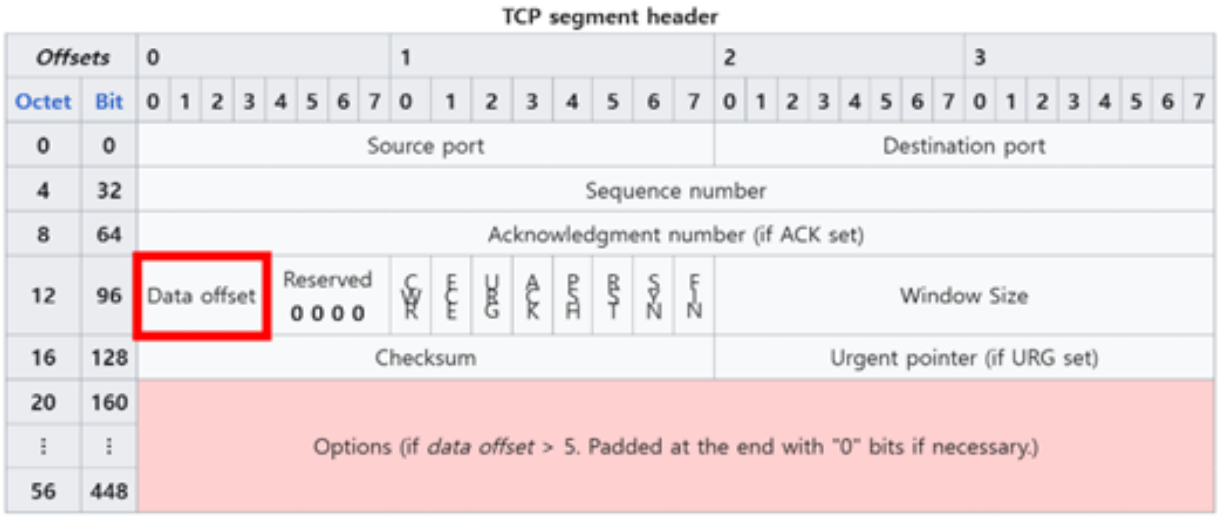


Figure 3: TCP segment header

Add '(u8) puzzle_type, (u32) threshold, nonce, local_dns_ip, seed'

Ipv4 packet flow

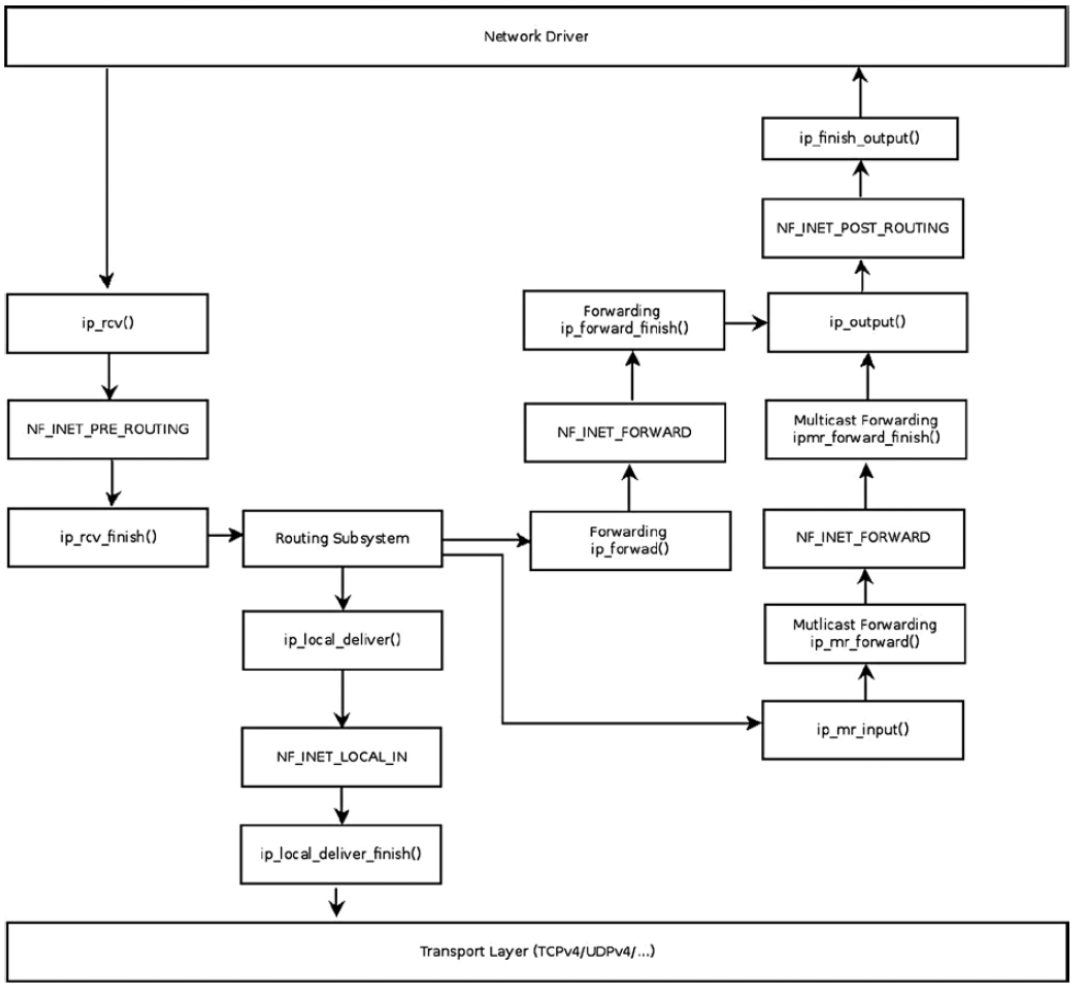


Figure 4: Ipv4 packet flow

TCP packet flow

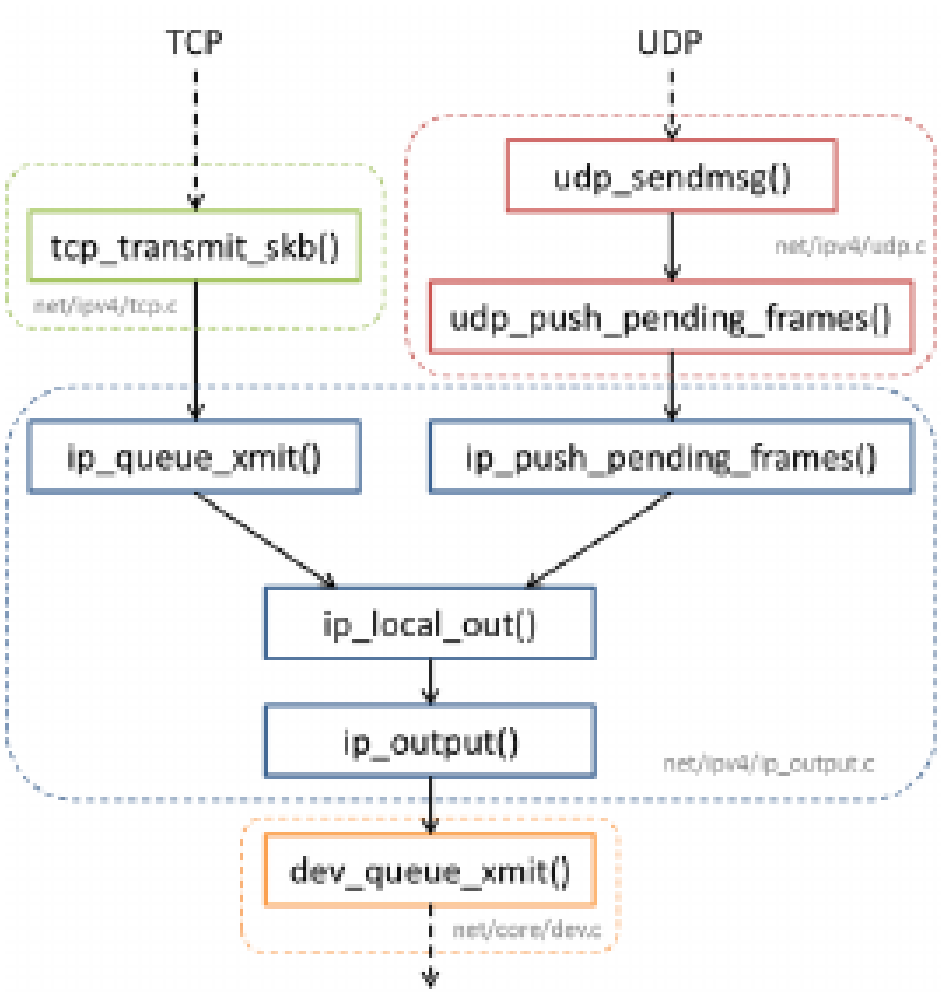


Figure 5: TCP UDP packet flow

TCP socket

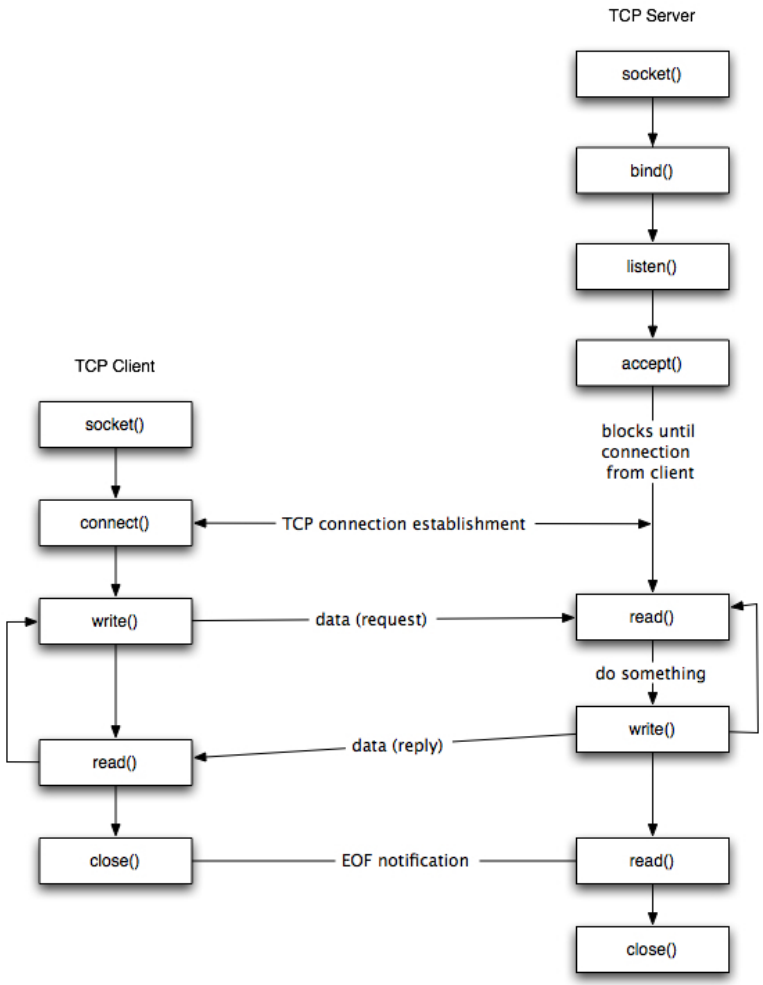


Figure 6: TCP socket

DNS socket programming

Local DNS & Authoritative DNS

Figure 7: BIND9 program

Table of Contents

Progress - Sukhun Yang

1. Devise schematic diagram
2. Modified linux kernel for TCP handshaking
3. Tried BIND9 program
4. Organize presentation slides

Source code

Currently Working Repository

https://github.com/Sagit25/DNS-based-DDoS-mitigation

⋆ Update basic modification of TCP kernel at 'ysh' branch!

⋆ If you leave your github ID, I will invite you as a collaborator!

Source Code

Table 1: Modified kernel part

net/ipv4/tcp_input.c	• TCP header parsing • tcp_rcv_state_process(): Check puzzle & nonce • tcp_rcv_synsent_state_process(): Add reset signal
net/ipv4/tcp_output.c	• Update TCP header writing

Source Code

Table 2: Modified kernel part

net/puzzle.c	• Add system calls • Puzzle hash function
net/ipv4/tcp_ipv4.c	• Change the order of function calls • tcp_v4_send_reset(): Add puzzle information

Plan - Sukhun Yang

- Complementary TCP handshaking process
- Implement wrapper process

Questions

Client

- Place of wrapper process

DNS

- Timing of update puzzle information
- Ownership of puzzle information

Host

- Place of autonomous system
- Data structures for storing dns information

Presentation Slides

Google Drive

Presentation slides folder

Progress - Jinyong Jun

Progress - Taehyun Kang