Caer: IoT Firewall

Thinking about consumer security

$ whoami

Joyce Mellens

Hanzehogeschool Groningen, HBO ICT

Innovatiehuis Politie Noord NL

UvA OS3

~/iot

ubiquitous

valuable

opaque

/usr

complex environment

many wrong answers

/usr/problem

Users aren't doing what we need them to!

/usr/solution

training, awareness

UX, design

FUEL SHUT-OFF VALVE
OPEN
1 2
CLOSED

STEADY
OFF
RED AMBER
KEY

GEAR
UP
DOWN

ON LANDING LIGHTS OFF

ON

STEADY

FUEL BOOST PUMP

RECOGNITION LIGHTS

OFF

OFF
GREEN WHITE
KEY KEY

WARNING
NEVER EXCEED
147 MPH WITH
FLAPS DOWN

L R
ON
BOTH
OFF L L OFF
1 2
AAF TYPE
B-5

LEFT ENGINES

MASTER IGNITION SWITCH DOES
NOT DISCONNECT BATTERIES -
BATTERY SWITCHES LOCATED ON
GENERATOR PANEL.

RECOG. LIGHTS MAX.
GROUND OPERATING
TIME TEN (10) SEC.

COWL FLAP

LOCKED   LOCKED   LOCKED   LOCKED
CLOSE OPEN   CLOSE OPEN   CLOSE OPEN   CLOSE OPEN

RELIEF VALVE

NOTE:
PLACE ALL
VALVE HANDLES
IN LOCKED
POSITION AFTER
ACTUATING
THE FLAPS TO
DESIRED POSITION

SPEED
CONTROL

ENG. Nº 1   ENG. Nº 2   ENG. Nº 3   ENG. Nº 4

L R
ON
BOTH
OFF L L OFF
3 4
AAF TYPE
B-5

RIGHT ENGINES

uiux.pt

/usr/solution

training, awareness

UX, design

/usr/problem

~~Users aren't doing what we need them to!~~

We rely too much on the user

(doubly so for consumers)

/usr/solution

training, awareness

UX, design

simplicity, automation

~/caer

~/caer/network
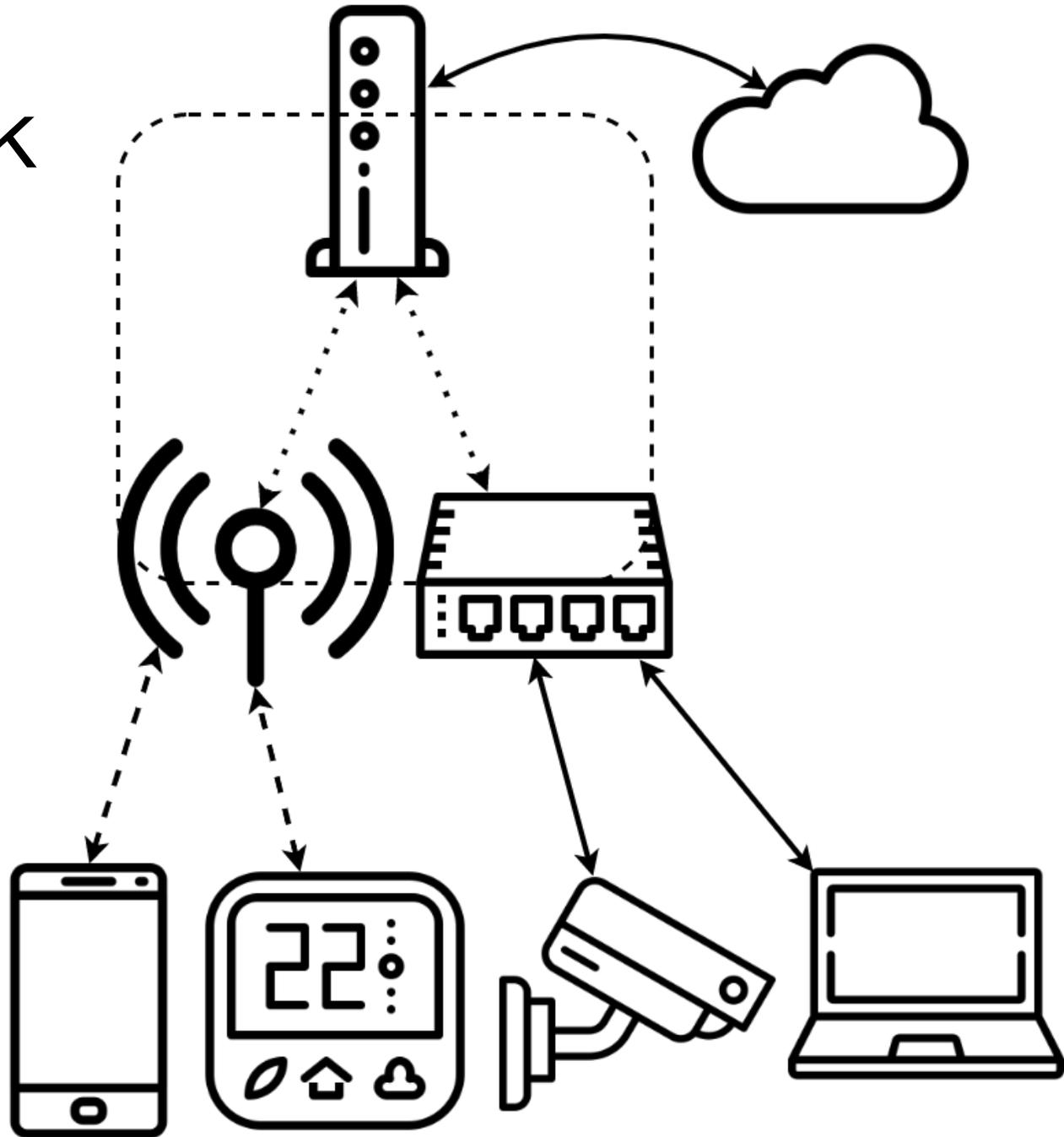
~/caer/network
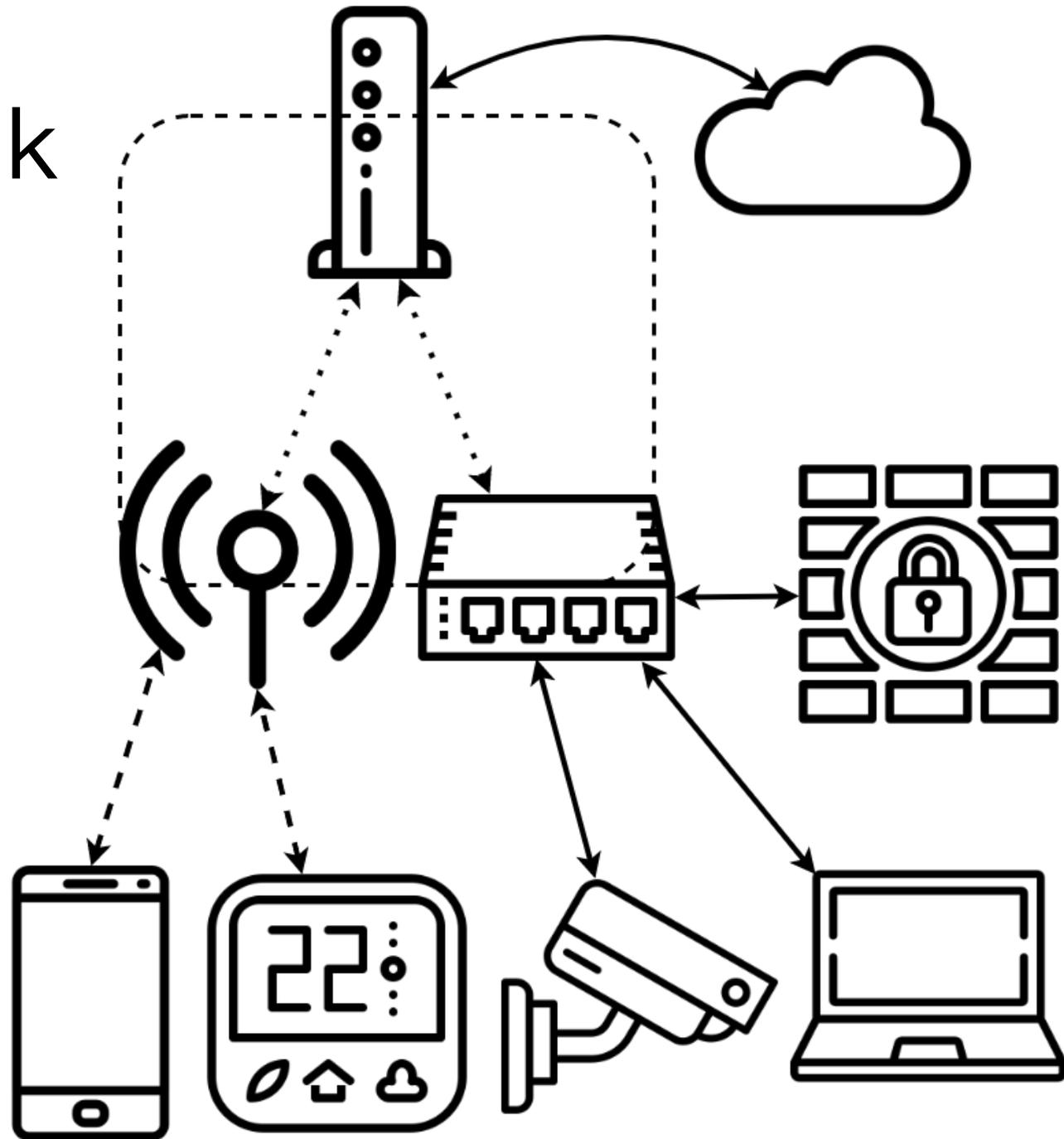
~/caer/dhcp

Subnet	Allocation
10.0.0.0/8	Home network
10.1.0.0/16	Regular devices
10.5.0.0/16	Quarantine
10.10.0.0/16	IoT subnet space
10.10.X.0/24	Individual IoT device subnets

~/caer/network

~/caer/network

10.0.0.1/8

10.0.0.10/8

10.1.0.12/16

10.1.0.13/16 10.10.3.2/24 10.10.4.2/24

Art by Chattapat, Freepik, Good Ware, iconixar,
kosonicon, prettycons, srip; via flaticon.com
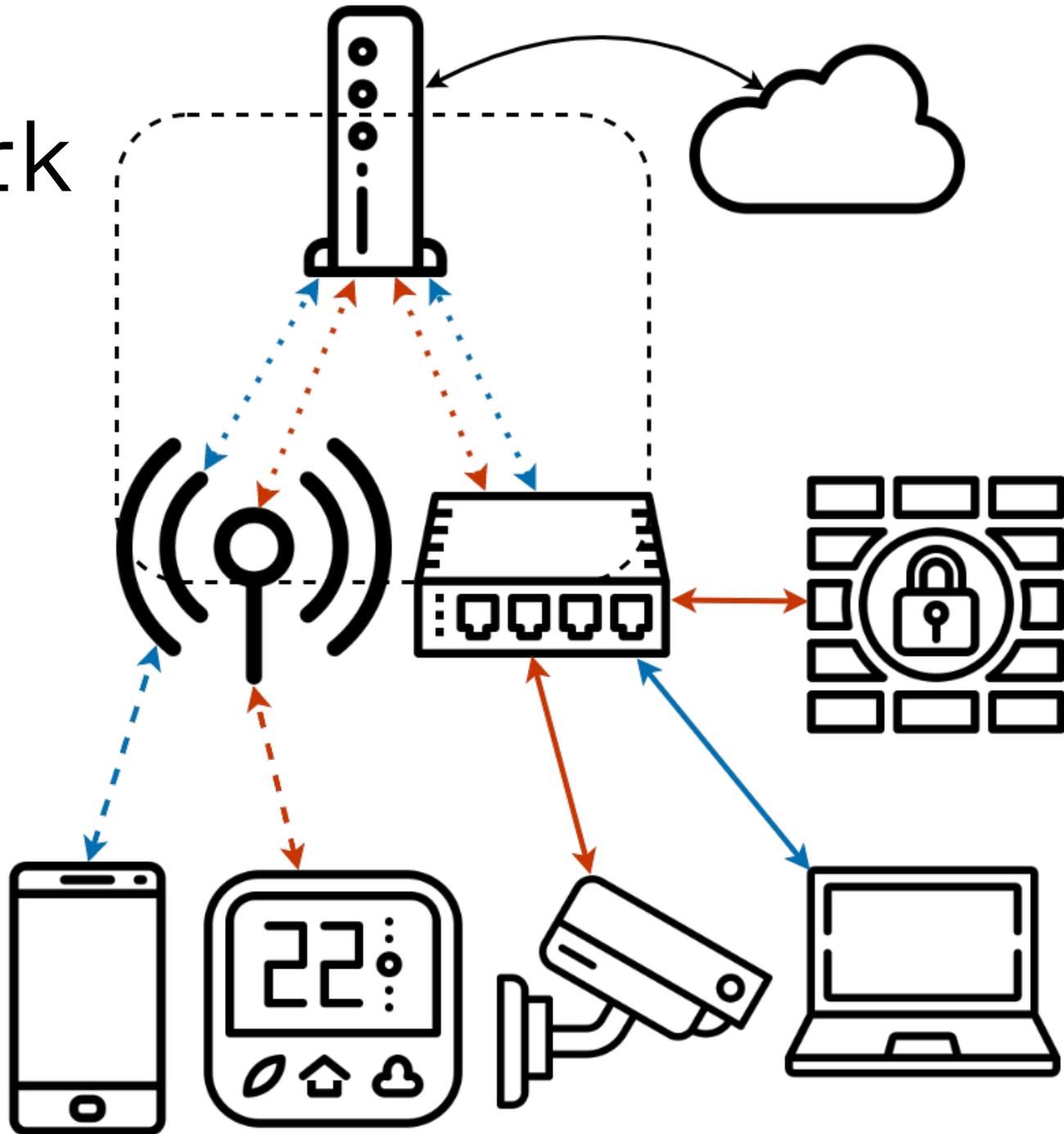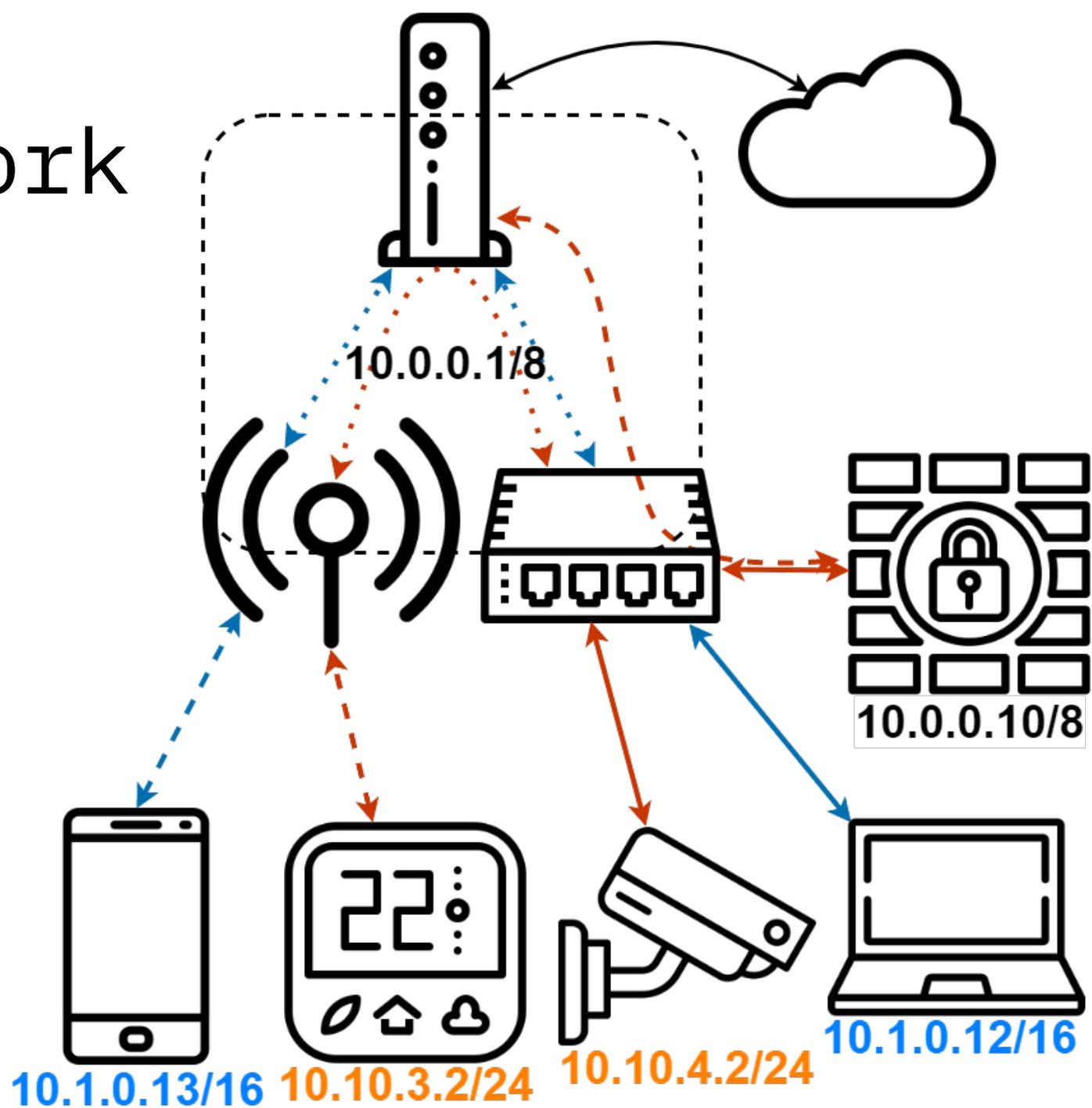
~/caer

IoT firewall

(near-)zero config

threat profile: botnet herders

          remote
          automated
          credential stuffing

~/caer/mfa

automated

periodic KeepAlive

client $\rightarrow$ server : $\{ip_c;time\}_{PSK}$

~/caer/core
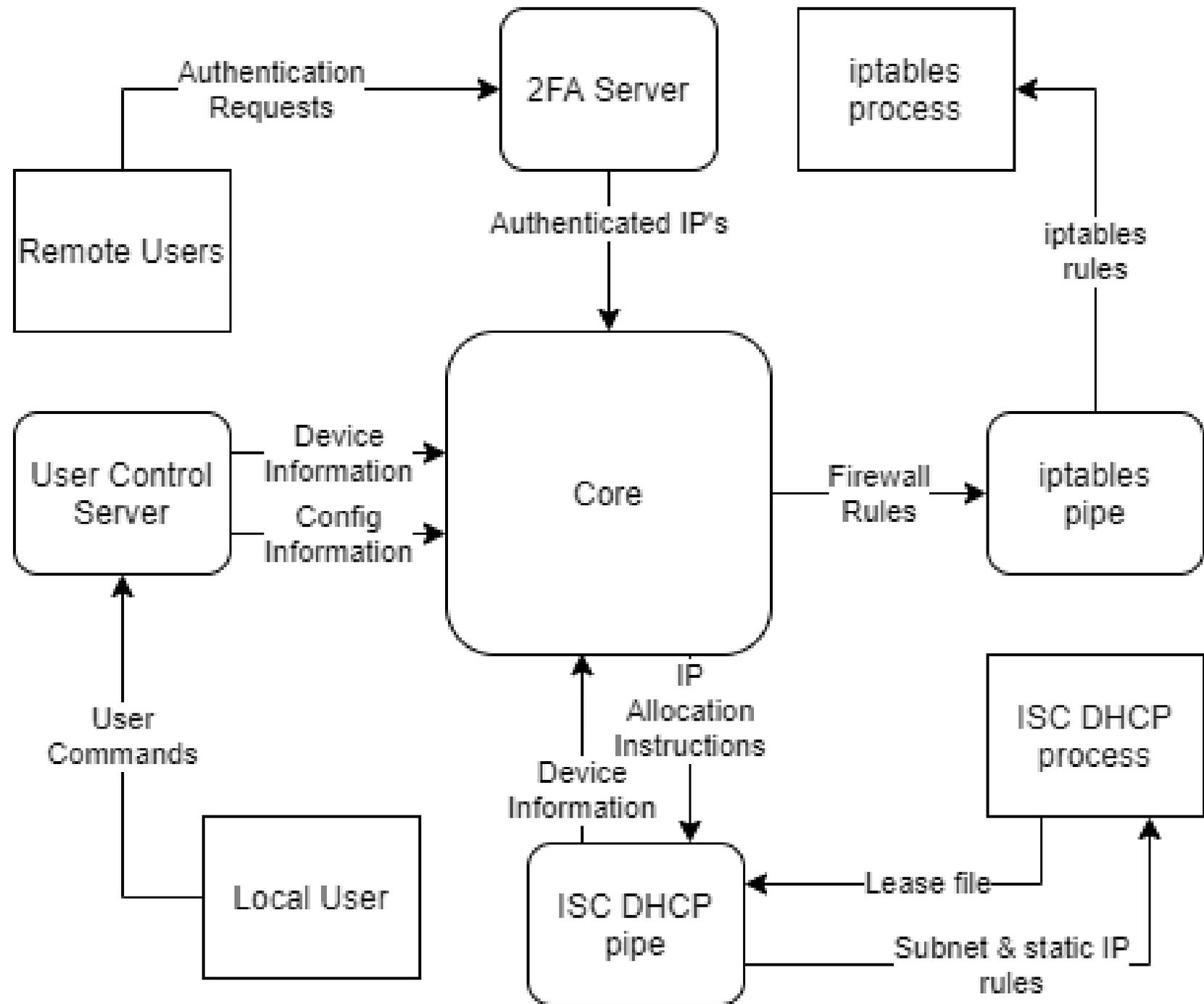
~/caer/market

open-source vs target audience

Hanzehogeschool entrepreneurship program

https://gitlab.com/jjmellens/caer