CAPPORT
IETF98 Hackathon

The Problem

- Captive Portals Suck
- Give all clients a consistent api/workflow to interact with capitve portals
- Minimize bad behaviour like hijacking https/man in the middle/etc
- Improve security

Planning

- Used architecture draft to guide at a high level
- Communicated over email ahead of time
- Used slack at hackathon to coordinate

What did we work with

- https://datatracker.ietf.org/doc/html/draft-donnelly-capport-detection
- https://datatracker.ietf.org/doc/draft-larose-capport-architecture
- https://tools.ietf.org/html/draft-wkumari-capport-icmp-unreach-01
- RFC 7710
- Coova Chilli https://github.com/coova/coova-chilli
- Flask (restful api framework)
- Wireshark (extended to read the new icmp messages)
- Tcpdump (extended to read the new icmp messages)

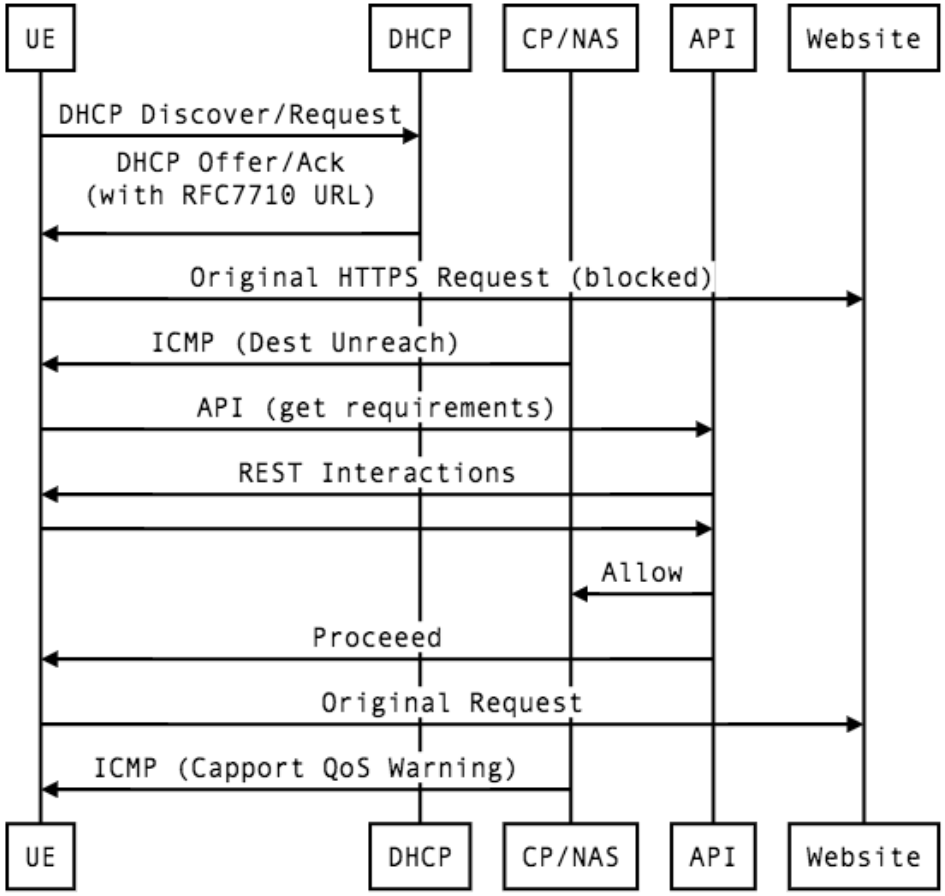
Achievements

- Achieved repeatable, automatic login to captive portal
- Extended tcpdump to support new icmp messages
- Extended wireshark to support new icmp messages
- Feedback for working group

How it works

- Coova-chilli
  - provides DHCP and captive portal
  - Sends ICMP Unreach with capport extension if blocked
  - Sends new ICMP Captive Portal Message to notify of throttling/etc
- Icmpd
  - Uses raw socket to get icmp
  - Spawns a python script to invoke login functionality of API automatically
  - IP hardcoded (should come from DCHP/RA-- RFC 7710)
- CAPPORT API Server
  - Provides REST interface to login/logout from captive portal
  - Calls coova-chilli CLI commands
- DHCP
  - Know how to do it client side (description on capport98 github)

How it works


UE
DHCP
CP/NAS
API
Website
DHCP Discover/Request
DHCP Offer/Ack
(with RFC7710 URL)
Original HTTPS Request (blocked)
ICMP (Dest Unreach)
API (get requirements)
REST Interactions
Allow
Proceeed
Original Request
ICMP (Capport QoS Warning)
UE
DHCP
CP/NAS
API
Website

Where to find the work

- Coova chilli: https://github.com/coova/coova-chilli
- Icmpd and DHCP: https://github.com/klarose/capport_98
- REST API: https://github.com/darshakthakore/capport-detection
- Wireshark: https://code.wireshark.org/review/#/c/20584/1
- Tcpdump: https://github.com/ThreadedThinking/tcpdump

Who did it?

- Kyle Larose (Sandvine)
- David Bird (Google)
- Darshak (Cablelabs)
- Alex Roscoe (Comcast)
- Remote:
  - Dave Dolson (Sandvine)
  - Alexis La Goulette
  - Vincent van Dam (Sandvine)

What did we find?

- Lots of discussion about:
  - Scope of API
  - Desired behaviour for different components
  - Security
  - Simplicity of solution
  - Usecases
- Identified real things to address in the WG