# IoT: Client Devices

Reverse Engineering

# Types of Firmware

## No Host

- No OS, services and operating code mixed
- Hard drives, USB, simple micro controllers
- BIOS, EFI/UEFI, etc.
- Smaller, simpler, less powerful

## Hosted

- Embedded Linux
- Have some kind of OS
- Userspace services on OS
- Larger, more complex, more powerful

# Reverse Engineering

## Why Reverse Engineering?

- See what others do
- Understand why
- Understand mistakes and avoid them!

## Start with downloadable images

- These don’t always exist

# Reversing a Device

## Scan the device

- Scan ports, monitor traffic examine protocols, dynamic analysis

## Running software

- We can run code using QEMU
- Real device better though

## All good things!

- We're not reverse engineers
- We just want to see the code

# What to Reverse?

## PUBLICLY AVAILABLE IMAGES

- Downloadable, we'll use TP-Link firmware images
- Saves you from extracting or buying the device

## NOTE: SHOULD YOUR FIRMWARES BE AVAILABLE?

- Controversial
- Hiding images is security by obscurity