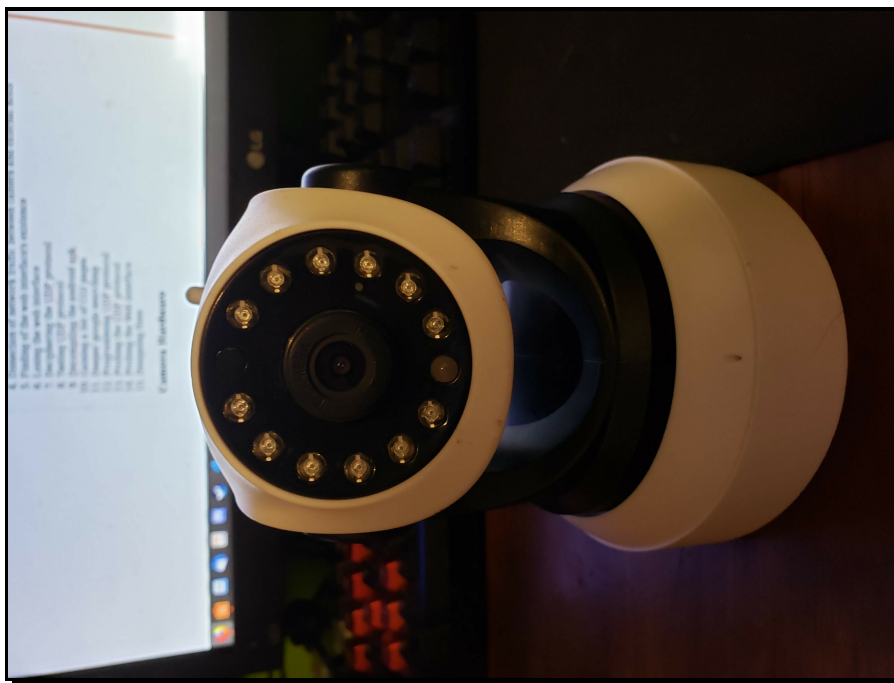


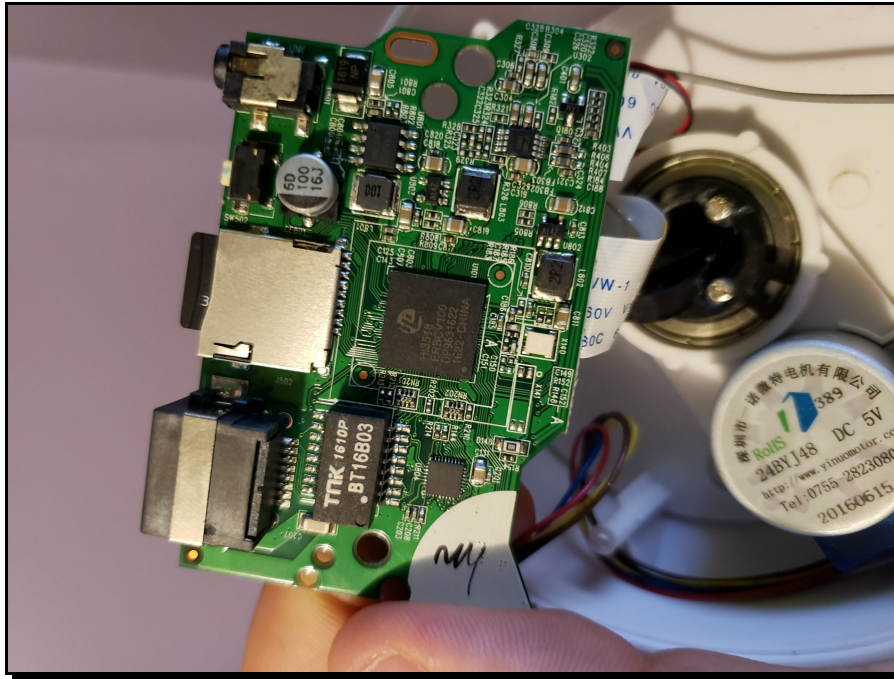
Date: 2019-09-03 Author: Ian Rash Index: #1

The camera itself has some pretty useful hardware, some which could be very easily taken advantage of with the right tools.

Just a couple simple Phillips screws and you are inside.







The processor it uses is a [HI3518](#) which apparently has already been hacked by other means. I quickly read through [this article](#) and unfortunately failed to locate any TX/RX pins I could solder into. I was a little disappointed by this, I had a spare [USB PL2303](#) lying around for just such an occasion.

When googling the HI3518 I noticed a website ispyconnect.com which seemed to be some sort of IP Camera database. I used their [website to search for my model of camera](#) and ended up finding out the company who manufactured it, [VStarCam](#). I want to point out, there is not a single marking anywhere on the device, including on the inside that would signify this to anyone. I also learned on this page that the camera can be potentially controlled by simple GET requests.

On one side of the board you can see an addon board where they added the wireless radio. (It's the blue PCB with the big silver square and the grey wire)

One other thing of note, the whole camera is powered by 5V DC, meaning you can power this thing off any USB port that can supply at least 1A. This is actually a pretty cool feature, because there are cheap USB battery backup options that could be used to augment the camera so it records even when the power is turned off.

---

TAGGED SKILLS:

[Security Research](#) [Reverse Engineering](#) [C](#)