**Deliverable #2: Hardware Breakdown and Component Research**

**Project: IoT Vulnerability Research Project**

**Participants:**

* Vikram Kher
* Varin Jaggi
* Tarik Wilkinson
* Patrick Kakooza
* Liza Moody
* Haoda Wang

**Introduction:**

For this deliverable, we first completed a hardware breakdown on the Laview camera. The hardware breakdown revealed a motor, camera module, and pcb board, among other things. We have provided some photos of the parts in this document. We additionally discovered a dataset on the camera module (“AK3918 HD IP Camera”). This dataset (found here: https://gzhls.at/blob/ldb/0/b/4/1/700cafec77419c2d7705f376c974b8d0ff72.pdf) seems to provide a wealth of information about how the camera’s hardware operates, including its encryption type. In future sprints, we would like to do more research on all of the chips on the pcb board. We will be clarifying tomorrow (2/7) with our stakeholder about what type of research on the components should be conducted.

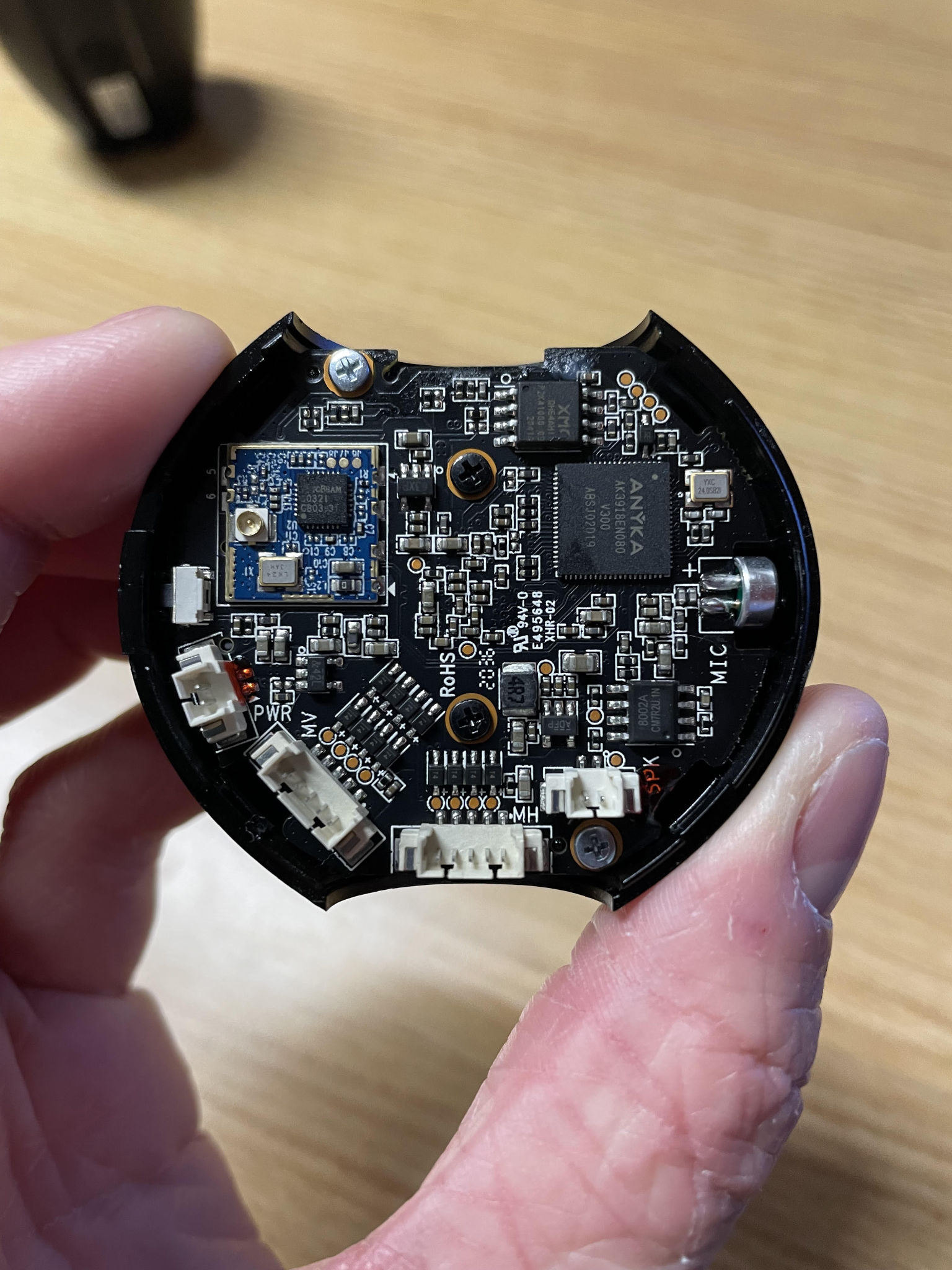
**Possible Attack Vectors:**

We tentatively hypothesize some possible attack vectors. It may be possible to gain control of the camera by changing the address which the bootstrap module points to. Then, when the processor of the camera is reset, a new set of instructions could be run. Another possible attack vector would be to somehow overtake how the timers work on the camera module. We might then be able to generate timer interrupts at will and thus effect the operation of the camera.

**Photo of the teardown progress:**



**Photo of Main PCB board:**



The following information was summarized or quoted from the specification document for the camera module (https://gzhls.at/blob/ldb/0/b/4/1/700cafec77419c2d7705f376c974b8d0ff72.pdf):

**Bootstrap Module:**

* When processor is reset, CPU cores get their first new instruction from address “32’0x0000,0000” from on chip ROM address space.

**RAM Controller:**

* 64mb DDR2
* Width of data bus is 16 bits

**Encryption:**

* “AES/DES/3DES Encryption module” encrypts video code stream.
* ”AES algorithm conforms with FIPS-197 standard.”
* “AES key length supports 128, 192, and 256 bits.”

**Features of Camera’s SoC:**

* **Anyka is the maker of the module**
* **(Information below is quoted from module spec)**
* ARM926EJ core, 16KB I cache and 16KB D cache
* advanced power management module
* supports little endian only
* Embedded 64MHz DDR2
* audio capability of MP3 encoder, ARM encoder, WAV encoder, Speex encoder
* MJPEG hardware encoder at 720p 30fps
* Multi-Stream encoding synchronously
* H.264 hardware encoder at 720p 30fps
* CCIR 601/CCIR 656 CMOS image sensor interface with programmable image size and
* smart scaling capability
* Ethernet MAC controller
* two ADCs for voice/music recording and battery measurement
* two Sigma-Delta DACs for stereo speakers
* built-in headphone driver
* I2S slave interface
* I2C master interface
* 2 UARTs, 1 has flow control
* rDA (under NEC protocol)
* ISP
* AES/DES/3DES Encrytion
* 2 SPI (master or slave operation)
* MMC/SD interface. MMC 4.2; SD 2.0
* SDIO interface, Version 1.1
* USB 2.0 HS Host/Slave
* 64 GPIOs, 7 dedicated, 57 shared with other pins
* JTAG supporting in-circuit debugging
* on-chip PLL and 32.768KHz RTC
* 5 PWMs
* 5 General Purpose timers
* 1 watchdog timer
* 1 RTC timer
* Four bootstrap modes, boot code saved in 32KB ROM
* package: 152-pin LFBGA”

**Timers:**

* 5 timers
* 26 bit down counter
* When timer reaches 0, the timer generates an interrupt

**CPU core:**

* Microprocessor called ARM926EJ from ARM Limited
* 32-bit ARM and 16 bit Thumb instruction sets
* Harvard cached architecture
* Contains memory management unit
* ”Separate instruction and data AMBA AHB bus interfaces”