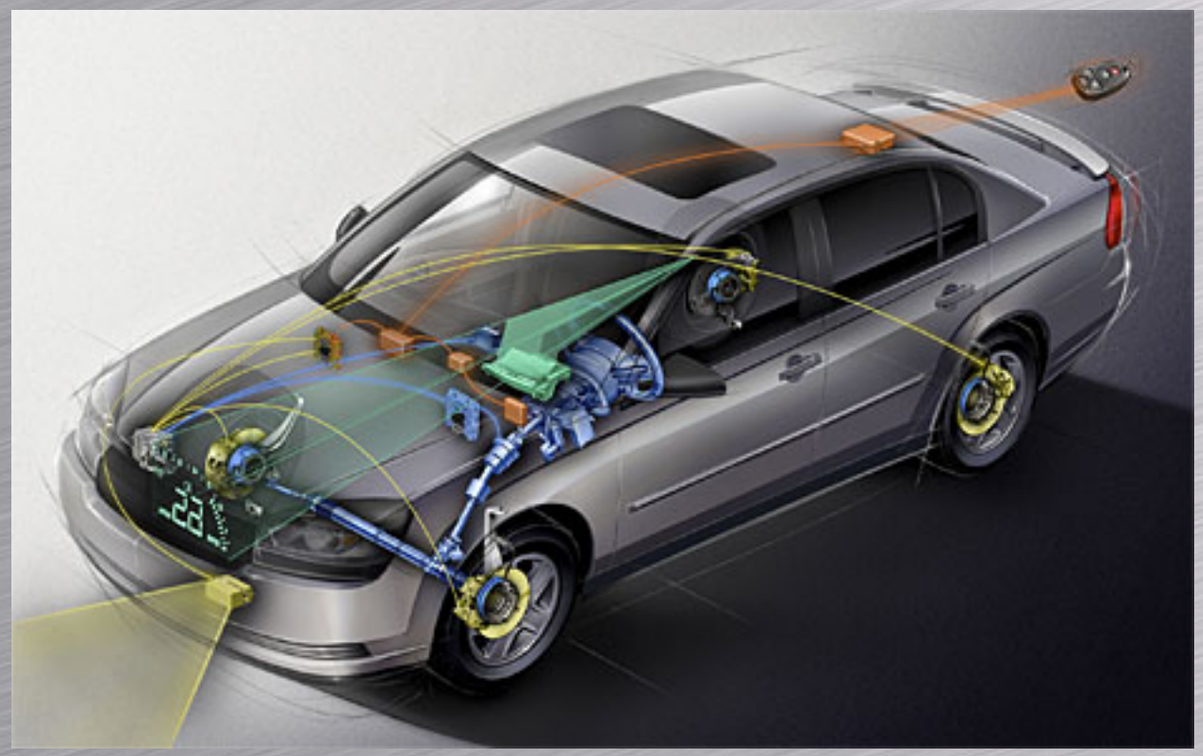
iSeeYou: Disabling the MacBook Webcam Indicator LED

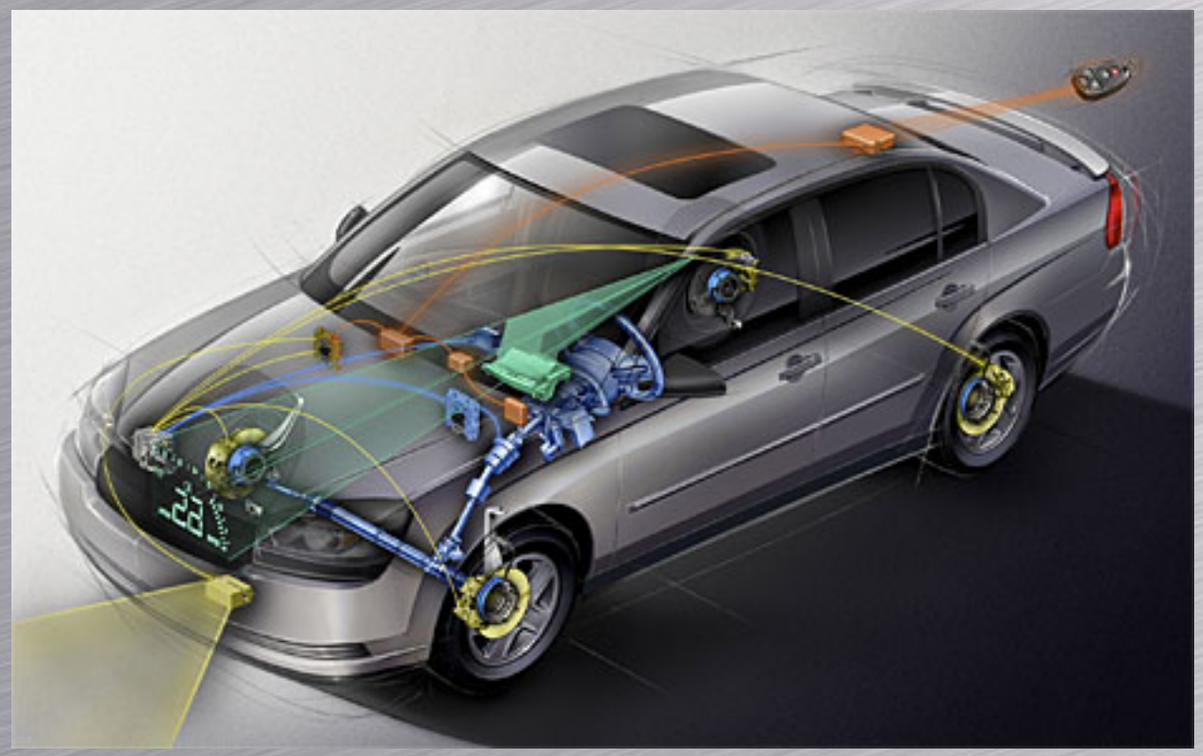
Matthew Brocker
Stephen Checkoway
Johns Hopkins University

Embedded Systems





Embedded Systems

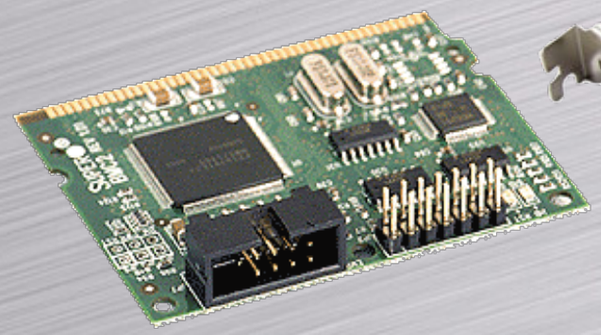






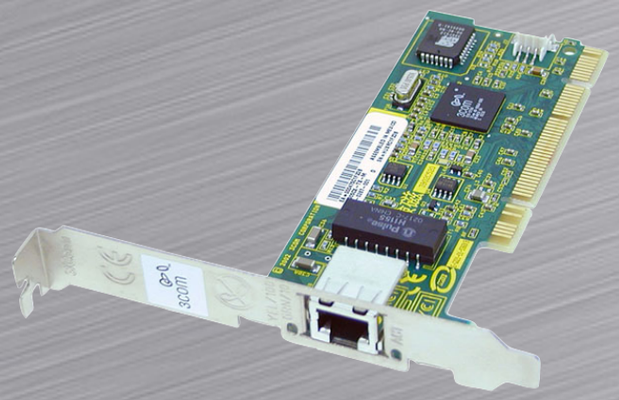
Processors all the way down









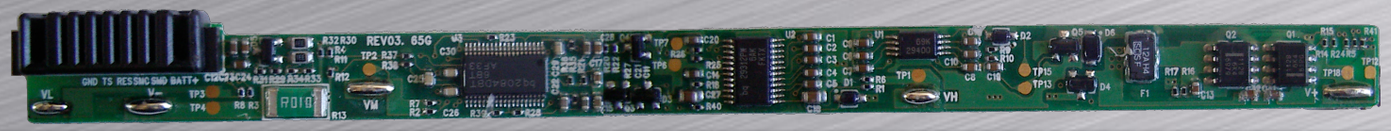












Toasters all the way down









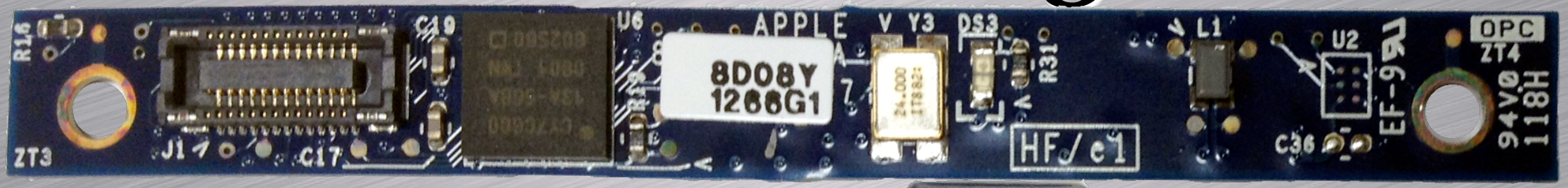


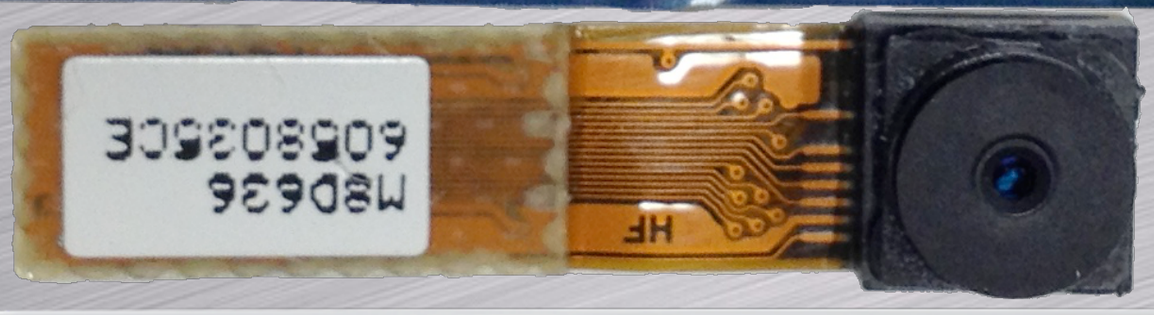






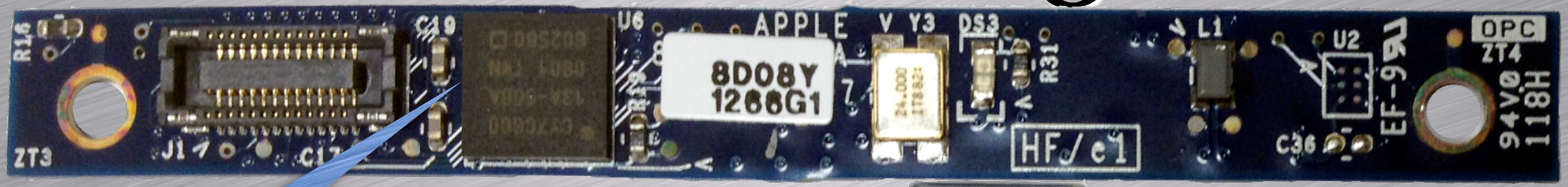
MacBook iSight



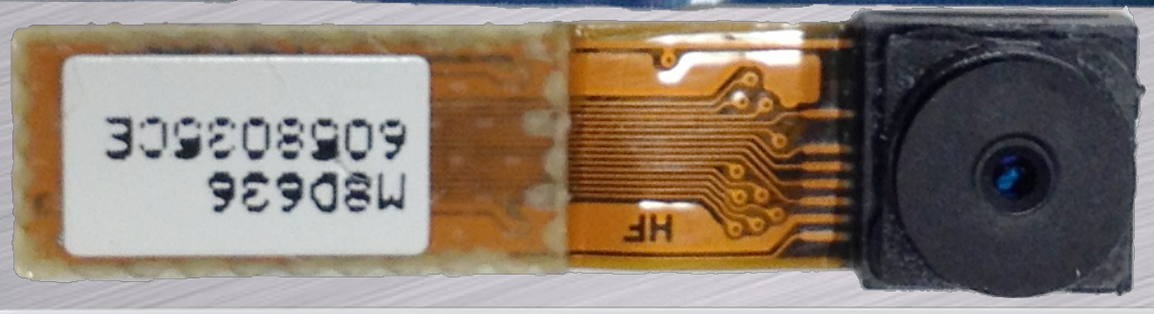




MacBook iSight

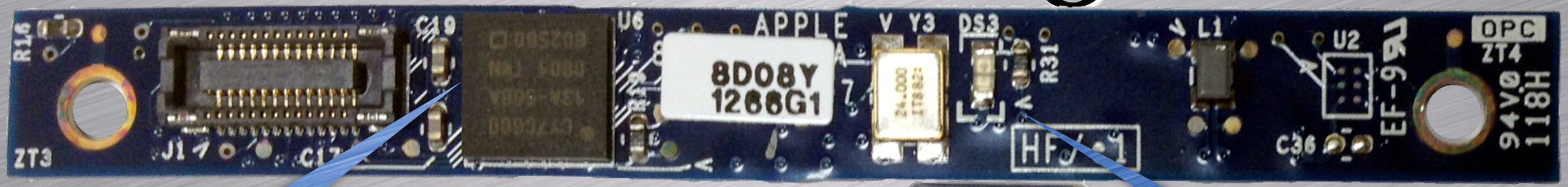


EZ-USB processor

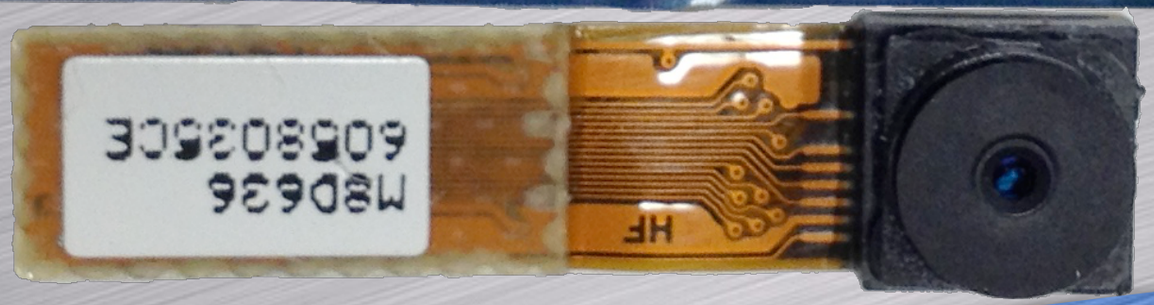




MacBook iSight



EZ-USB processor



LED



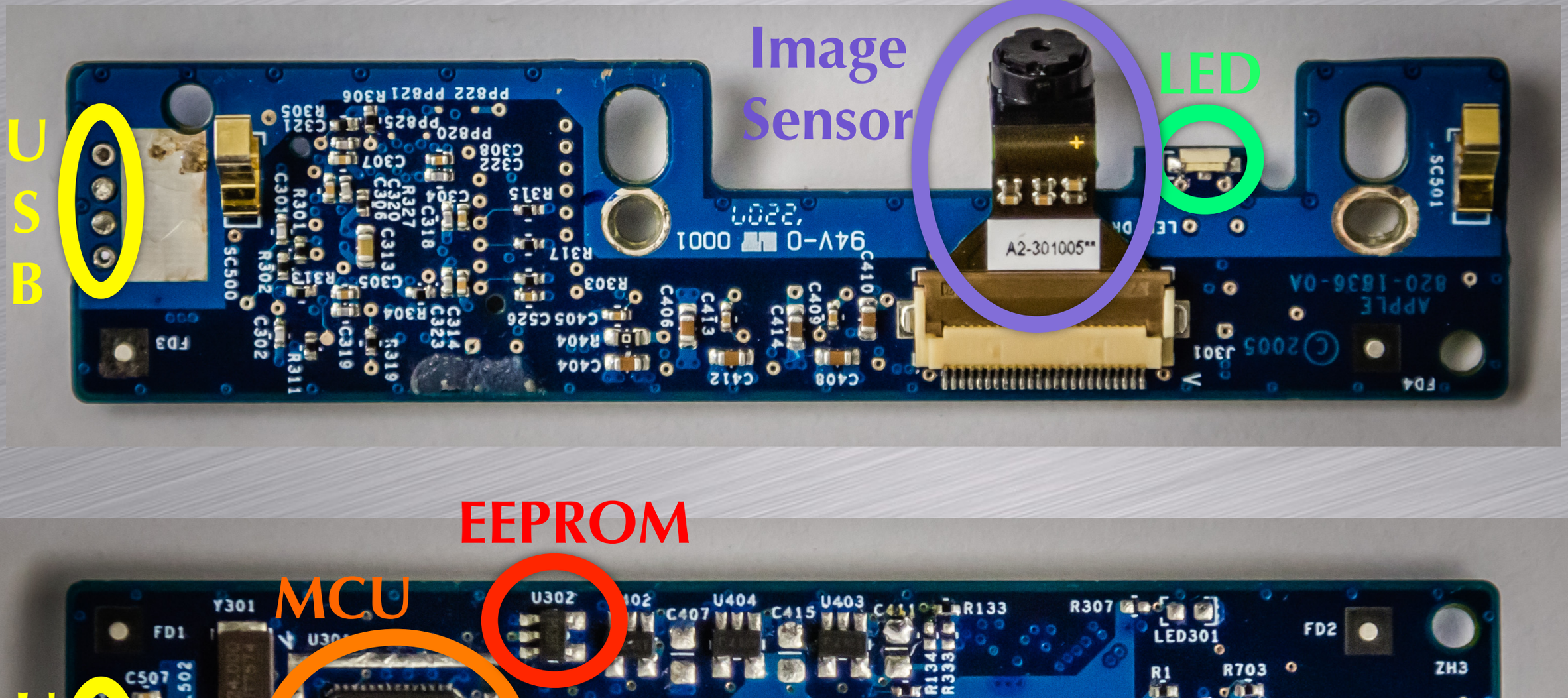
Okay. So what?

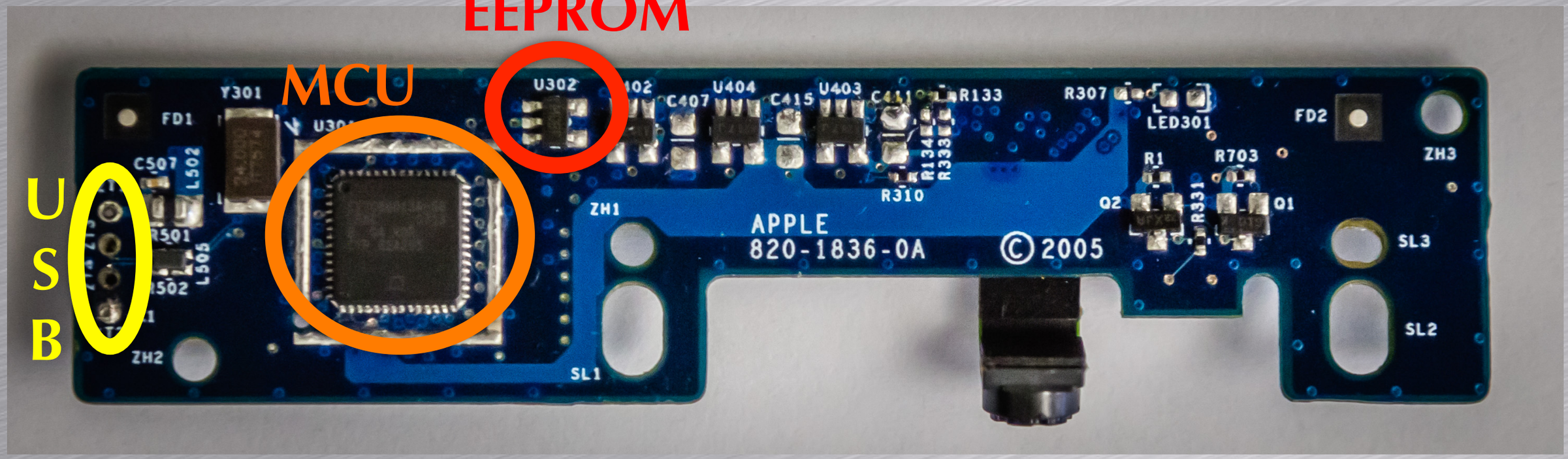
- Nation state actors
- Stalkers on the Internet
- Anyone who gives you a computer
- Biometric authentication using webcam

Can we turn the LED off while recording?

- Can malicious firmware control the LED?
- Can malicious software (on the host) replace the firmware

Hardware


USB
Image Sensor
LED
A2-301005**
APPLE
820-1836-0A
© 2005


EEPROM
MCU
USB
U302
Y301
FD1
ZH1
ZH2
SL1
SL2
SL3
ZH3
FD2
LED301
R307
R133
R310
Q1
Q2
APPLE
820-1836-0A
© 2005

Which one?

VGA Products

View All Imaging Products >>

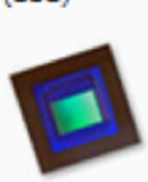
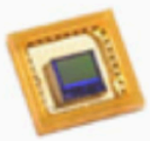
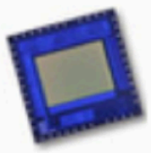
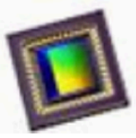
Part Number	Resolution	Pixel Size	Optical Format	Frame Rate	Maximum Data Rate	Power Consumption	Supply Voltage	Output	Shutter	Package	Application
NEW! MT9V012 	640H x 480V	3.6µm x 3.6µm	1/6 inch	30 fps (VGA), 60 fps (CIF)	13.5 megapixels per second (27 MHz master clock)	Active: 54mW (@ 30 fps VGA resolution) Standby: <10µA (In general light conditions)	2.50V–3.10V (Analog), 1.70V–3.10V (Digital and I/O)	10-bit	Electronic rolling shutter (ERS)	28-pin iBGA, die or wafer	Mobile PC Cam
	Product Flyer | Data Sheets | Request Info										
NEW! MT9V112 (SOC) 	640H x 480V	3.6µm x 3.6µm	1/6 inch	30 fps @ 27 MHz	12-13.5 megapixels per second (master clock, 24 MHz–27 MHz)	<78mW (@ 30 fps)	Digital I/O: 1.7V–3.6V Digital Core: 1.7V–1.9V, 2.5V–3.1V	10 bit, on-chip	Electronic rolling shutter (ERS)	36-pin iCSP, wafer or die	Mobile
	Product Flyer | Data Sheets | Request Info										
MT9V011 	640H x 480V	5.6µm x 5.6µm	1/4 inch (4:3)	30 fps at 27 MHz	13.5 MPS/27 MHz	70mW @ 2.8V, 20pF load, 27 MHz, 30 fps	2.8V	10-bit parallel	Electronic rolling shutter (ERS)	28-pin PLCC	Mobile PC Cam
	Product Flyer | Data Sheets | Request Info										
MT9V111 (SOC) 	640H x 480V	5.6µm x 5.6µm	1/4 inch (4:3)	15 fps @ 12 MHz (default) programmable up to 30 fps at 27 MHz	12 - 13.5 MPS/27 MHz	<80mW @ 2.8V, 15fps @12 MHz	2.8V±0.25V	10-bit, on-chip	Electronic rolling shutter (ERS)	44-Ball ICSP, wafer or die	Mobile PC Cam Automotive
	Product Flyer | Data Sheets | Request Info										
MT9V403 	659H x 494V	9.9µm x 9.9µm	1/2 inch	0-200 frames/sec. with source illumination at 550nm	66 MB/s (master clock 66 MHz)	130mW@ 200 fps	+3.3V	10-bit digital through a single port	TrueSNAP™ freeze-frame electronic shutter	48-pin CLCC	High Speed

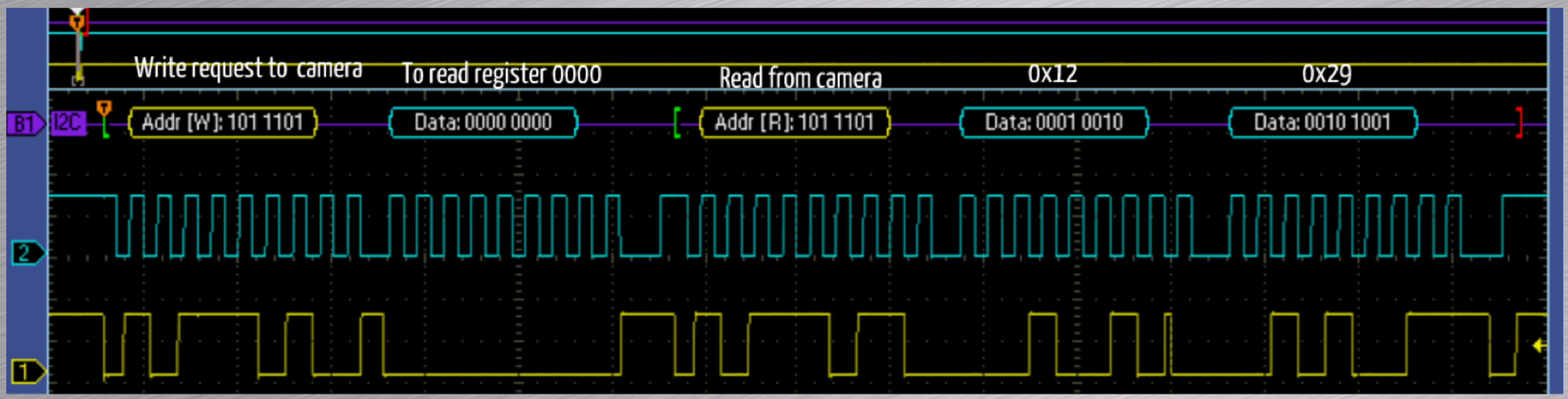
Image Sensor

MT9V112 : SOC VGA DIGITAL IMAGE SENSOR
Pixel Data Format

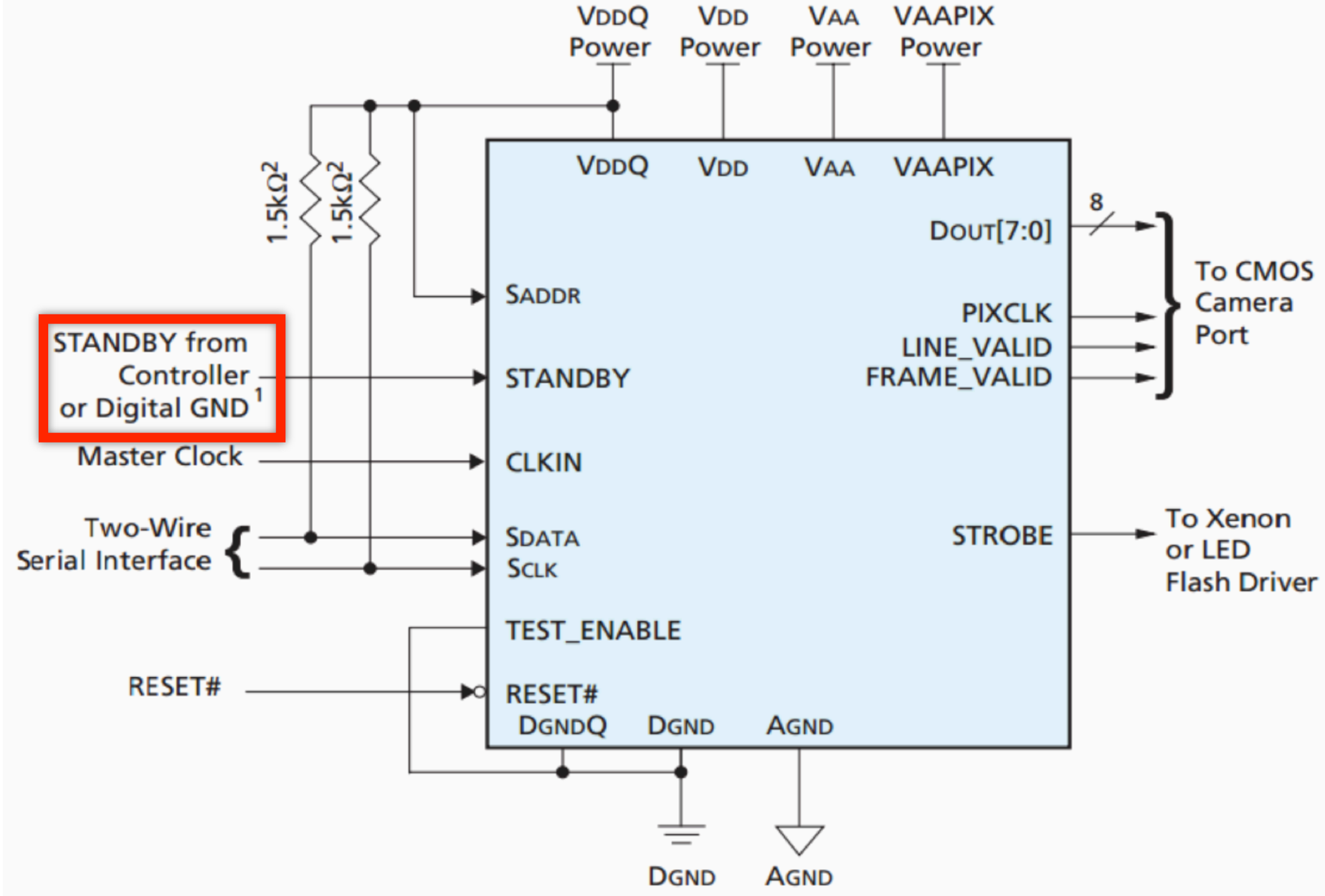
Sensor Core Registers

Table 12: Sensor Registers – Address Page 0

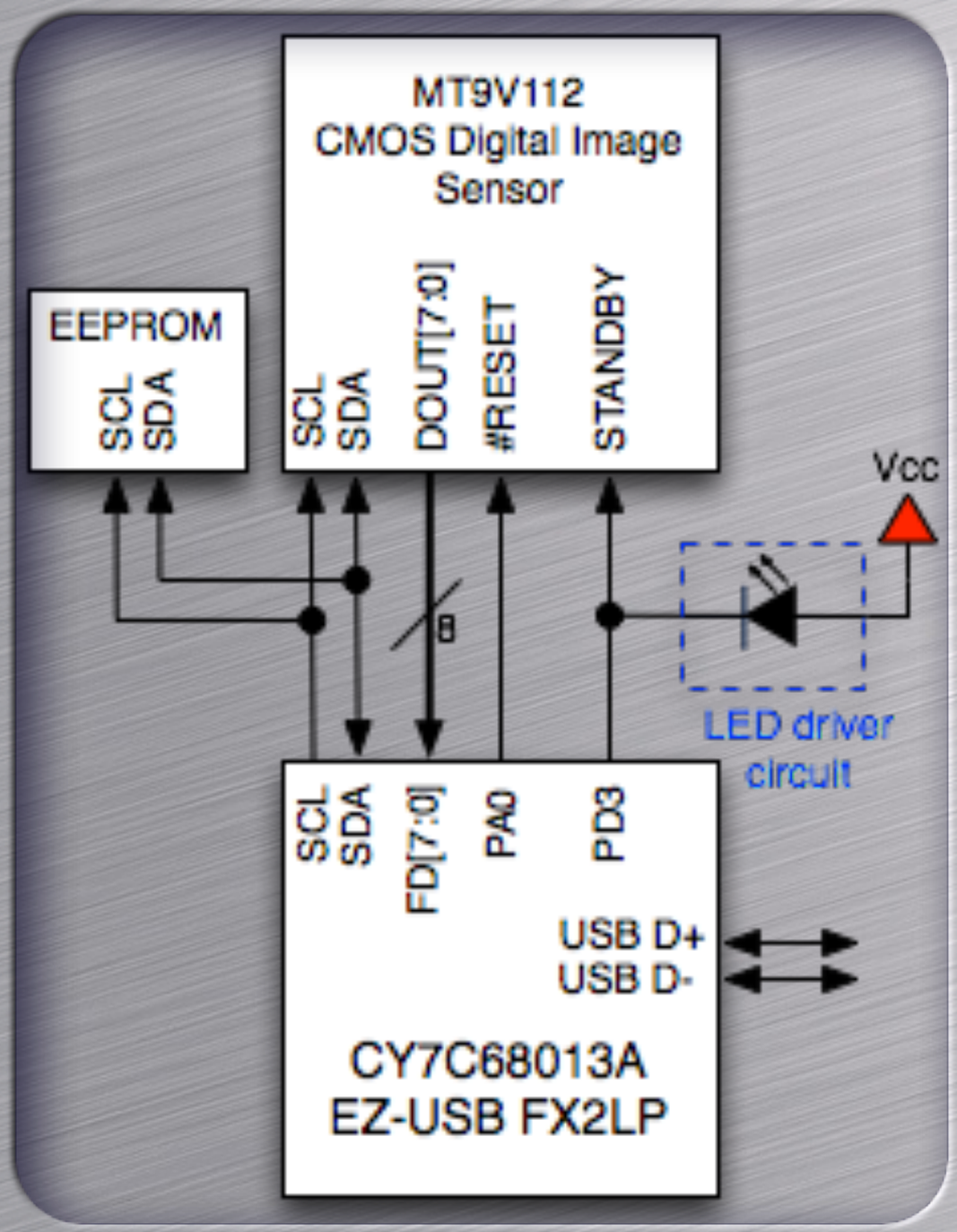
Register# Decimal (HEX)	Register Name	Data Format	Default Value Decimal (HEX)
0 (0x00)	Chip Version	0001 0010 0010 1001 (LSB)	4649 (0x1229)



Typical Configuration



iSight architecture



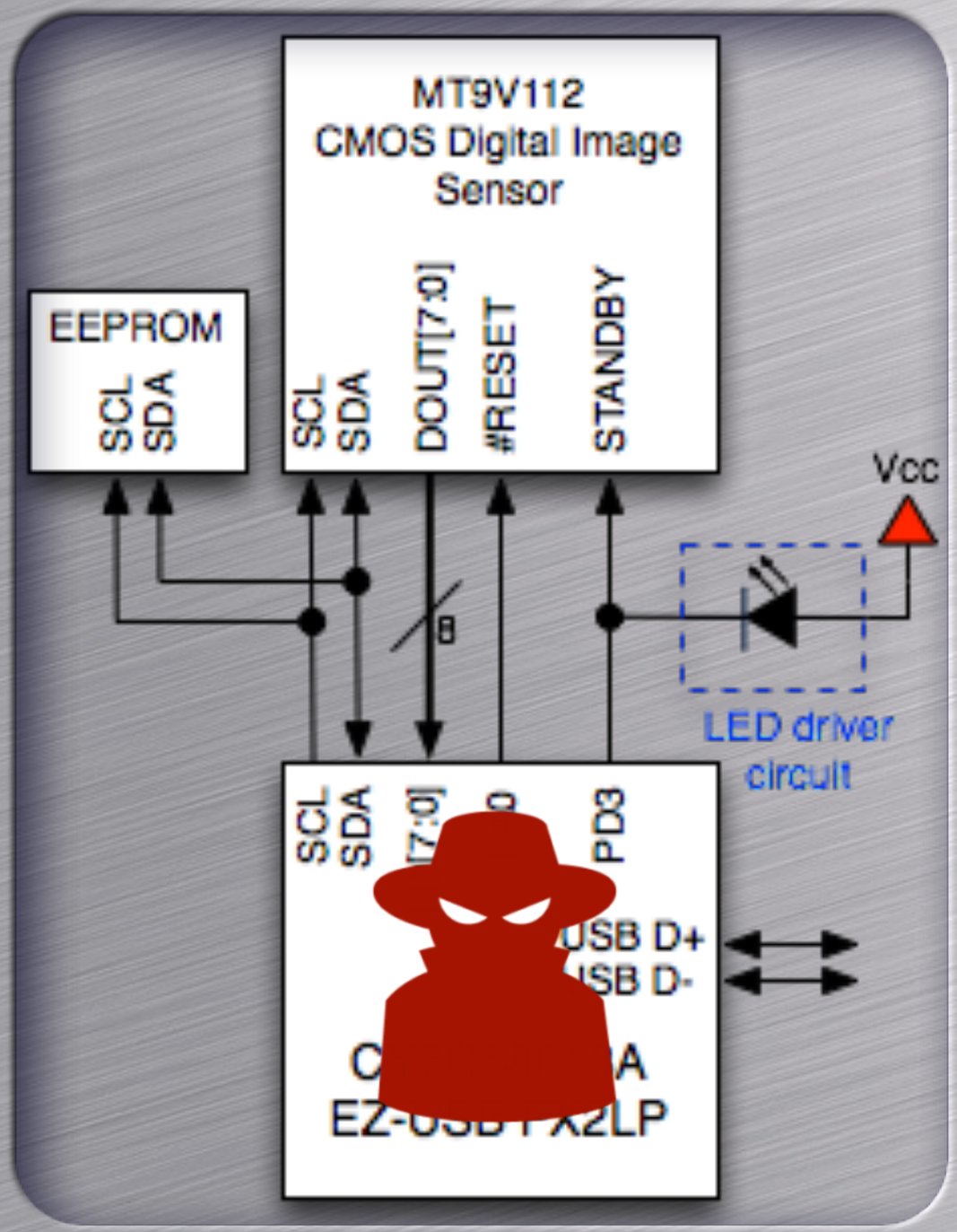
- USB connection to host
- Configure sensor via I^2C
- 16 byte I^2C EEPROM
- STANDBY=output disable
- PD3 also controls LED:

PD3	Output	LED
Vcc	Disabled	Off
Gnd	Enabled	On

RESET Register

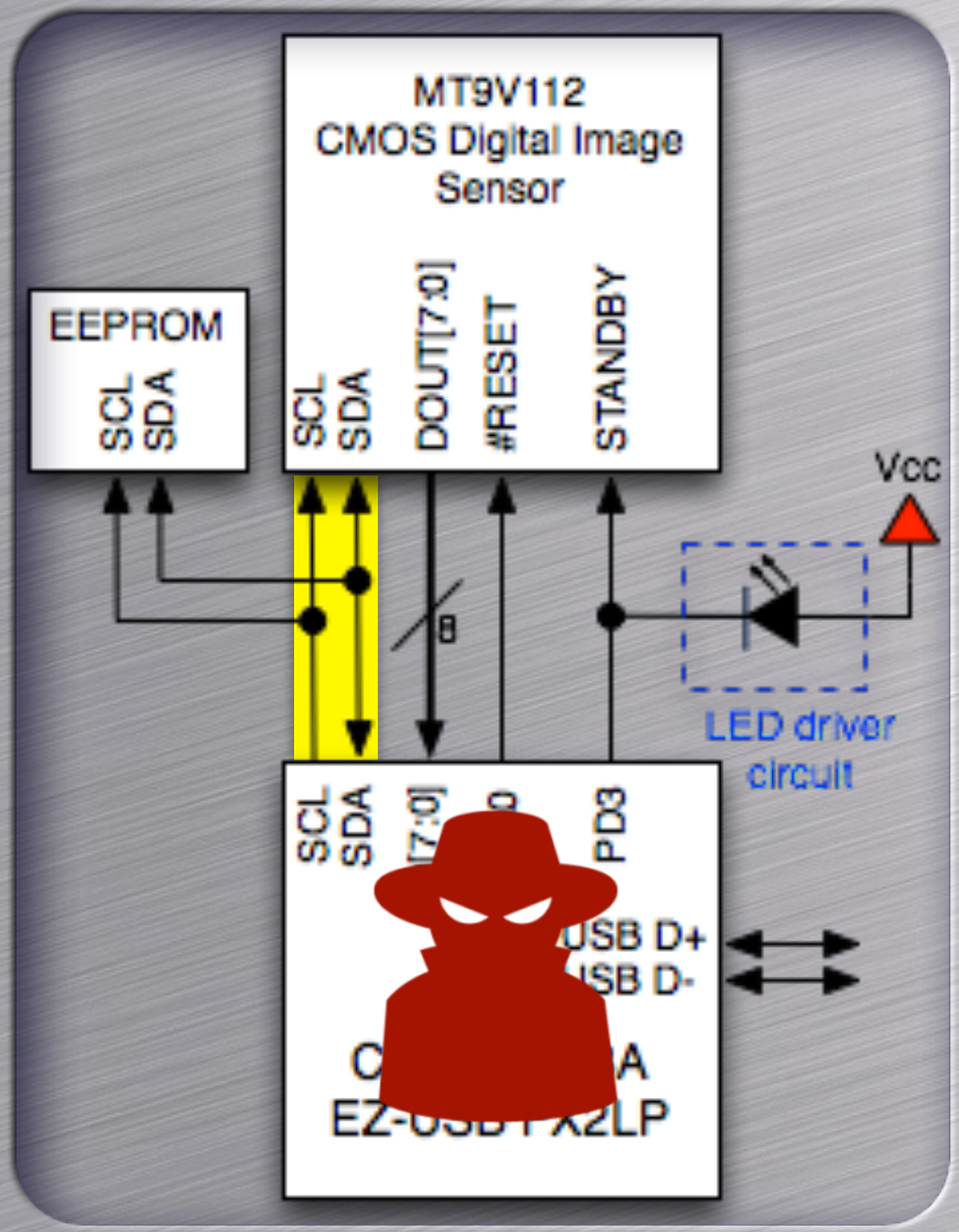
Bit Field	Description
Bit 7 Inhibit STANDBY	Setting this bit stops STANDBY from affecting entry to or exit from the low-power state.
Bit 6 Drive Signals	By default, asserting STANDBY causes the ball interface to enter High-Z. Setting this bit stops STANDBY from contributing to output enable control.

With malicious firmware



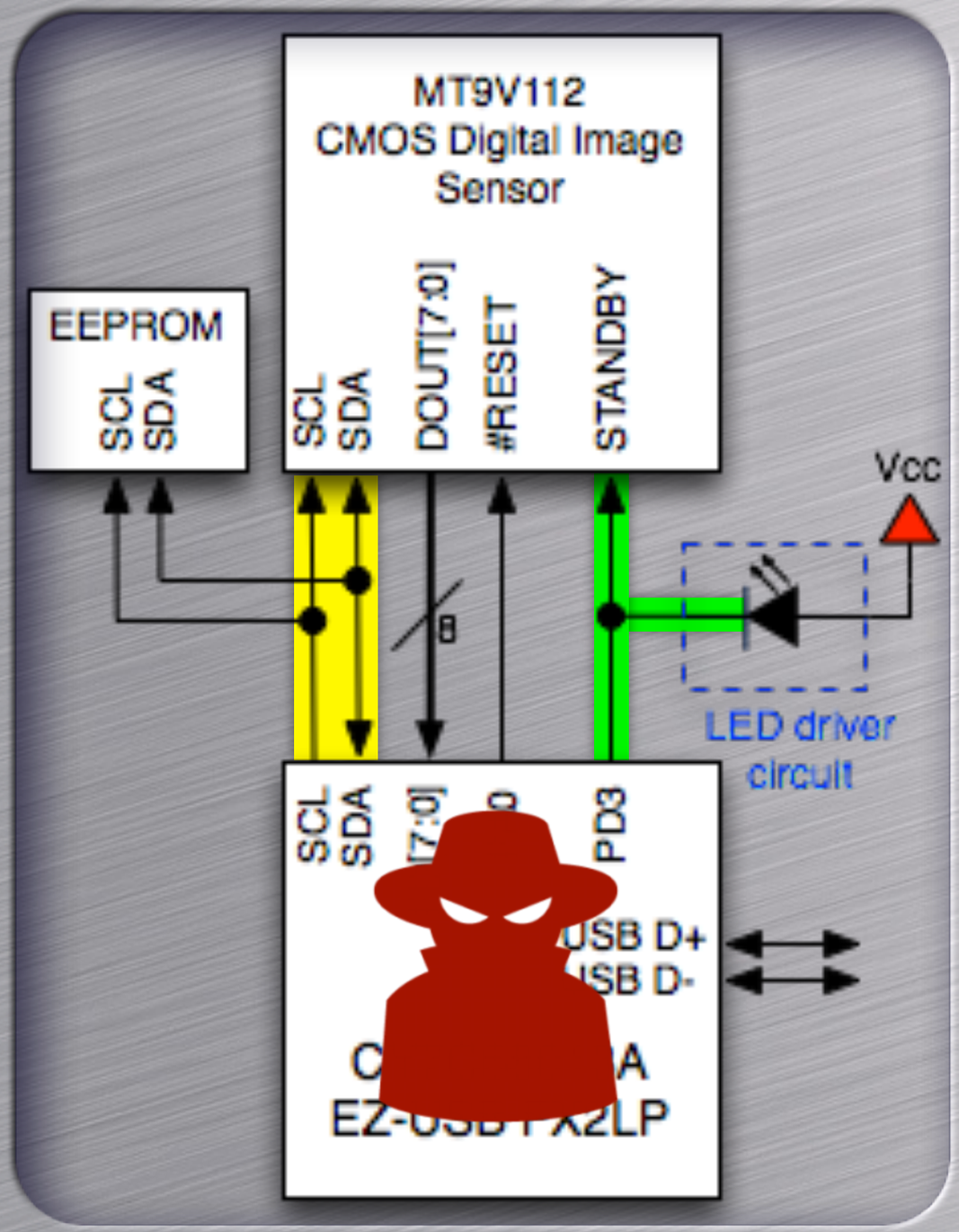
- Set RESET register via I^2C
- Control LED via PD3 (independent of Standby)

With malicious firmware



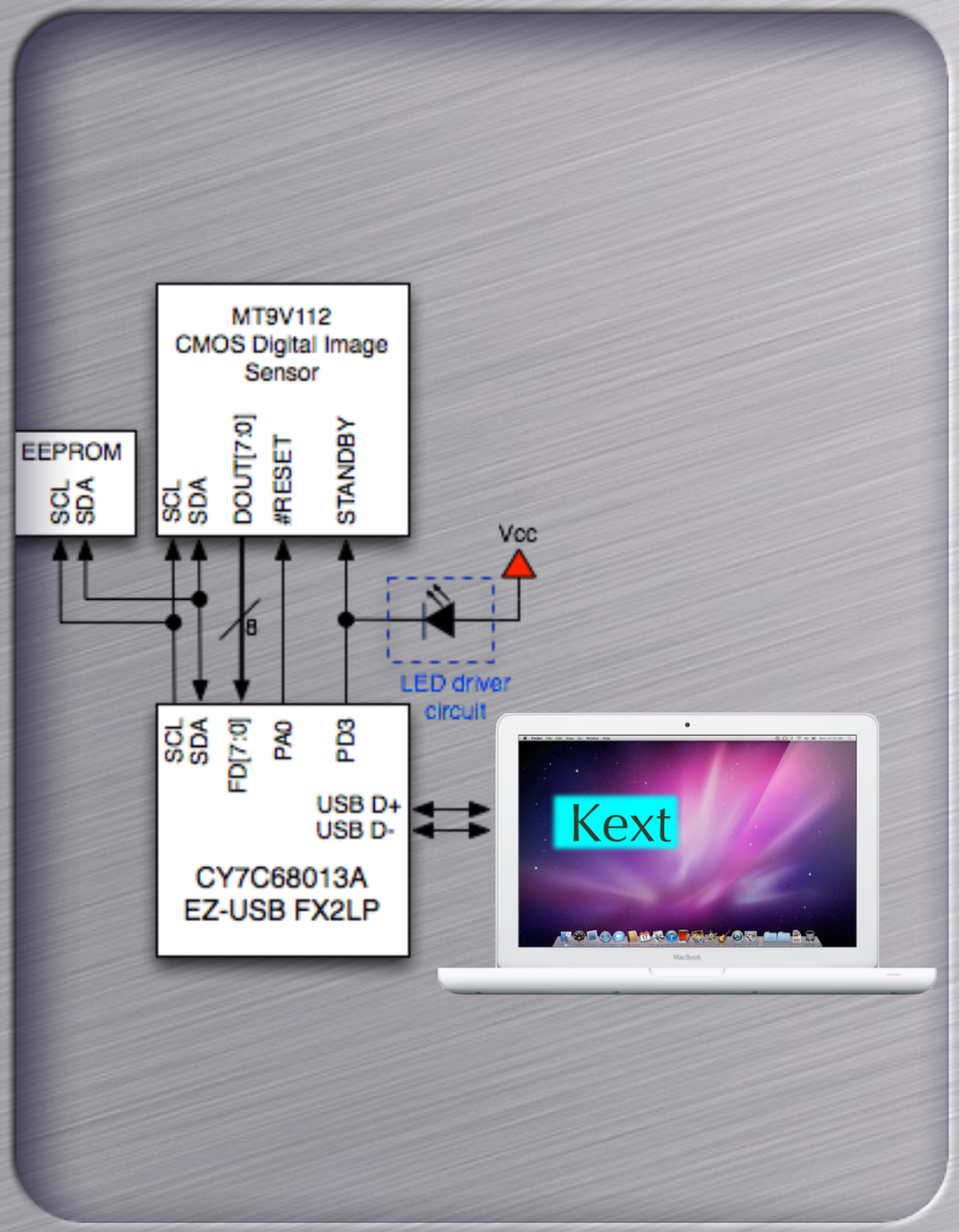
- Set RESET register via I²C
- Control LED via PD3 (independent of Standby)

With malicious firmware



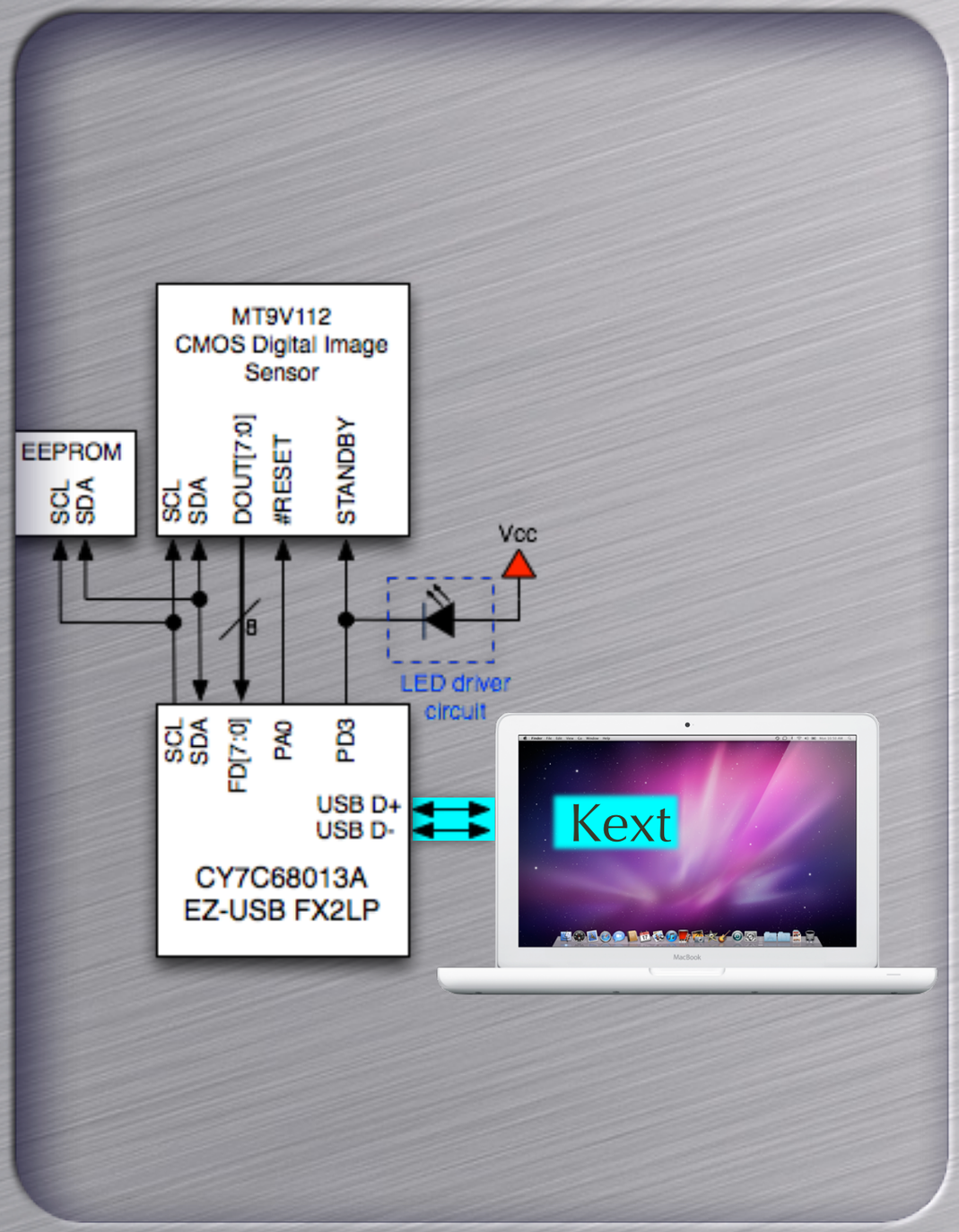
- Set RESET register via I^2C
- Control LED via PD3 (independent of Standby)

Firmware Load



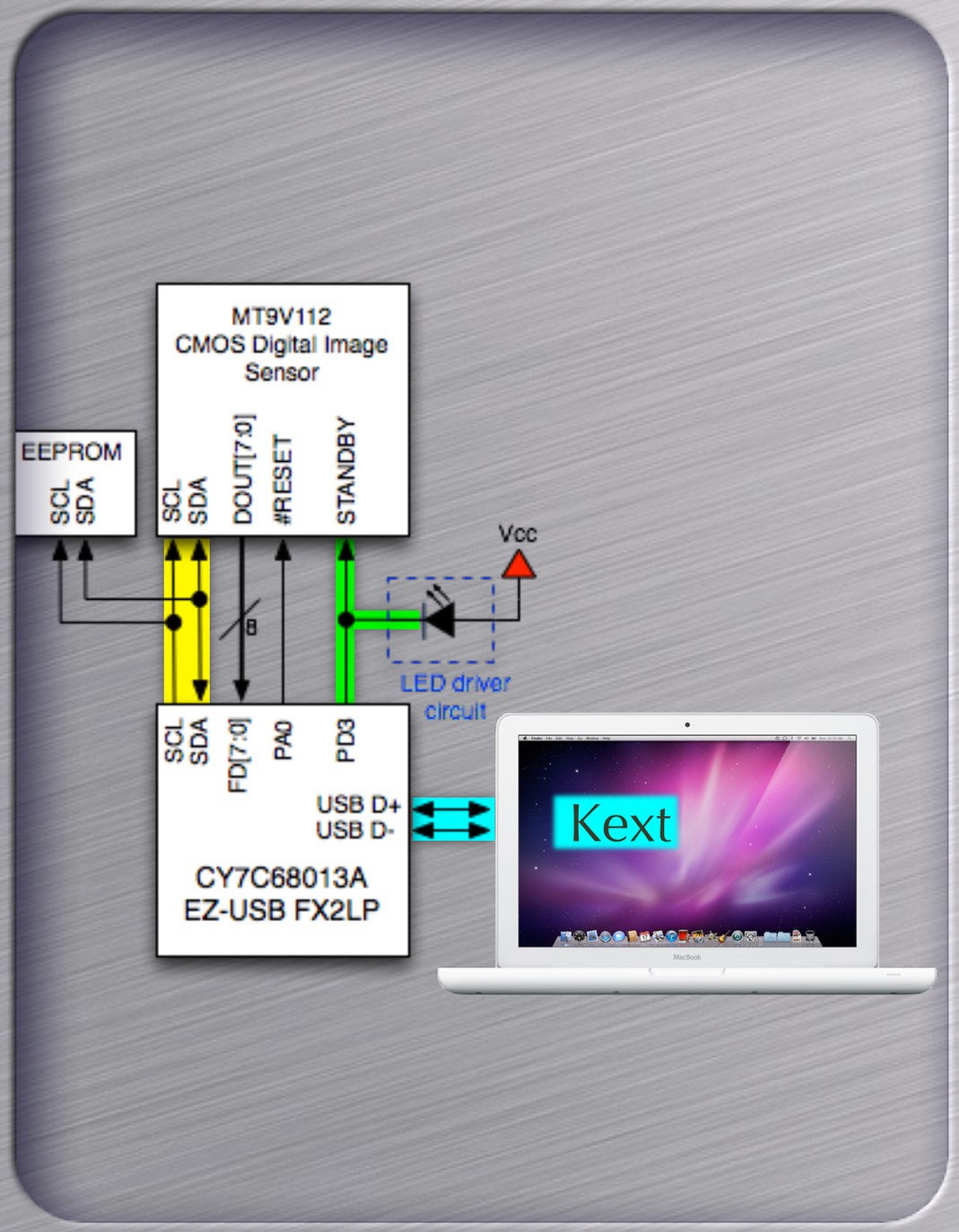
- Internal Hi-Speed USB bus
- AppleUsbVideoSupport kext
- Non-root process

Firmware Load



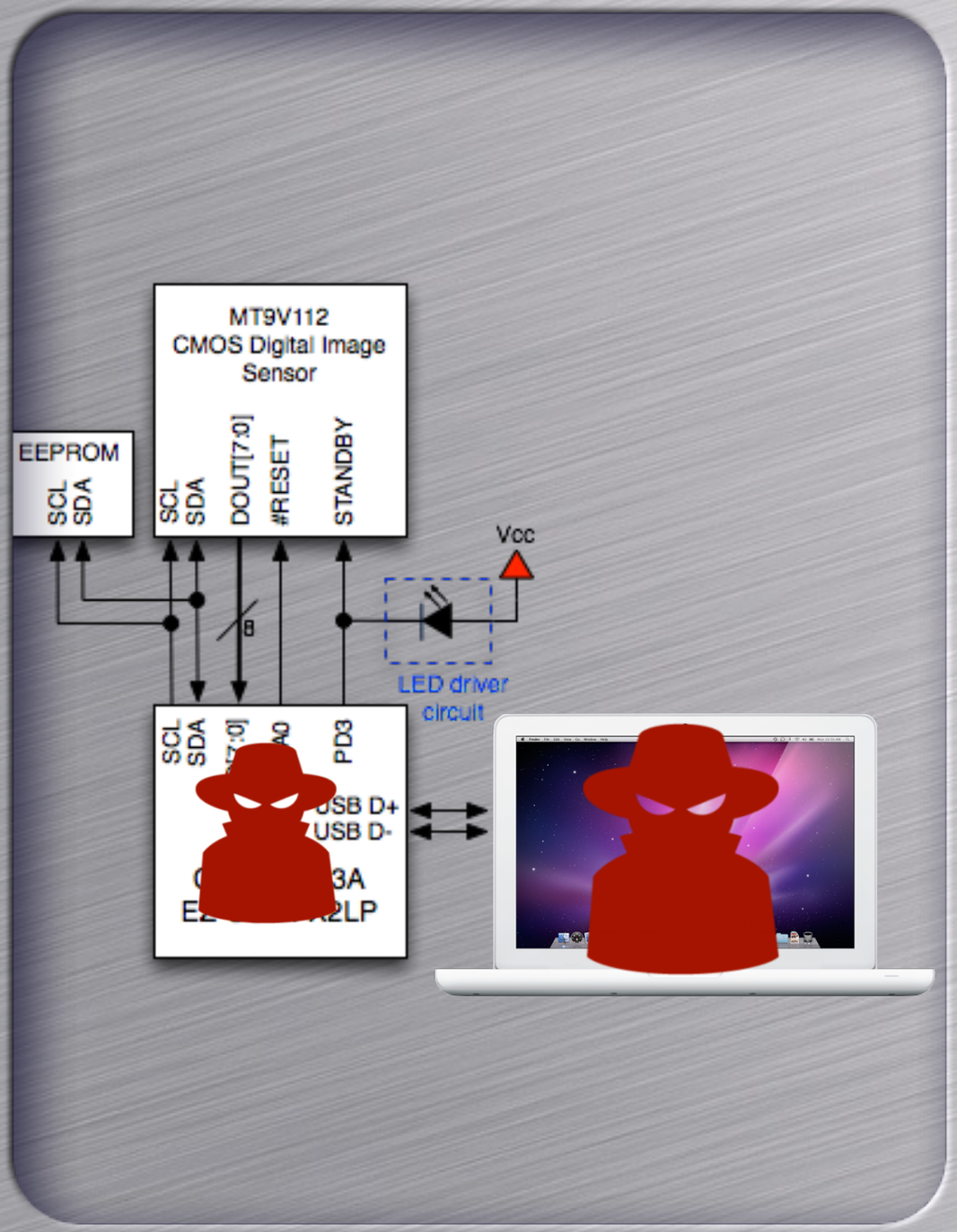
- Internal Hi-Speed USB bus
- AppleUsbVideoSupport kext
- Non-root process

Firmware Load



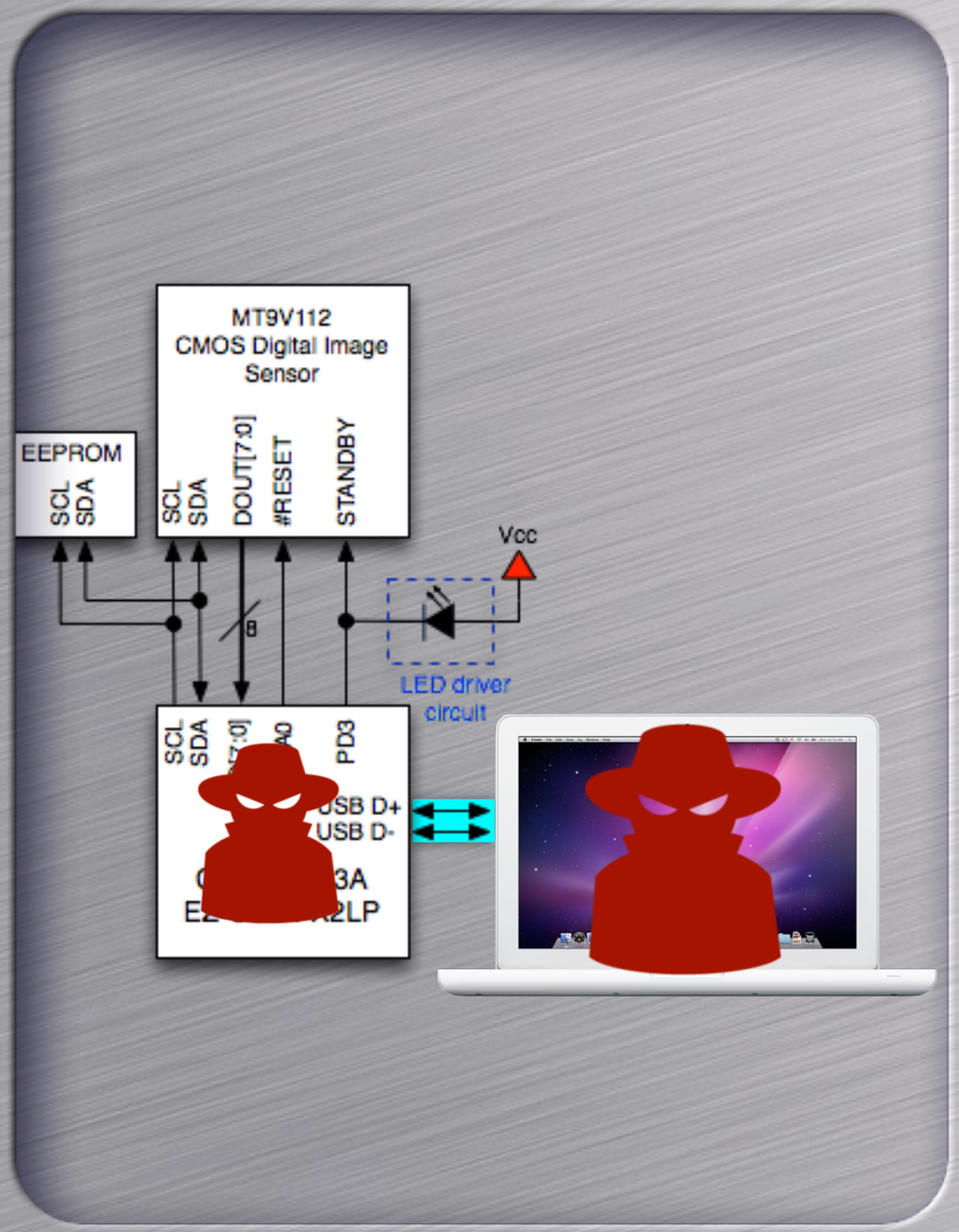
- Internal Hi-Speed USB bus
- AppleUsbVideoSupport kext
- Non-root process

Programming the EZ-USB



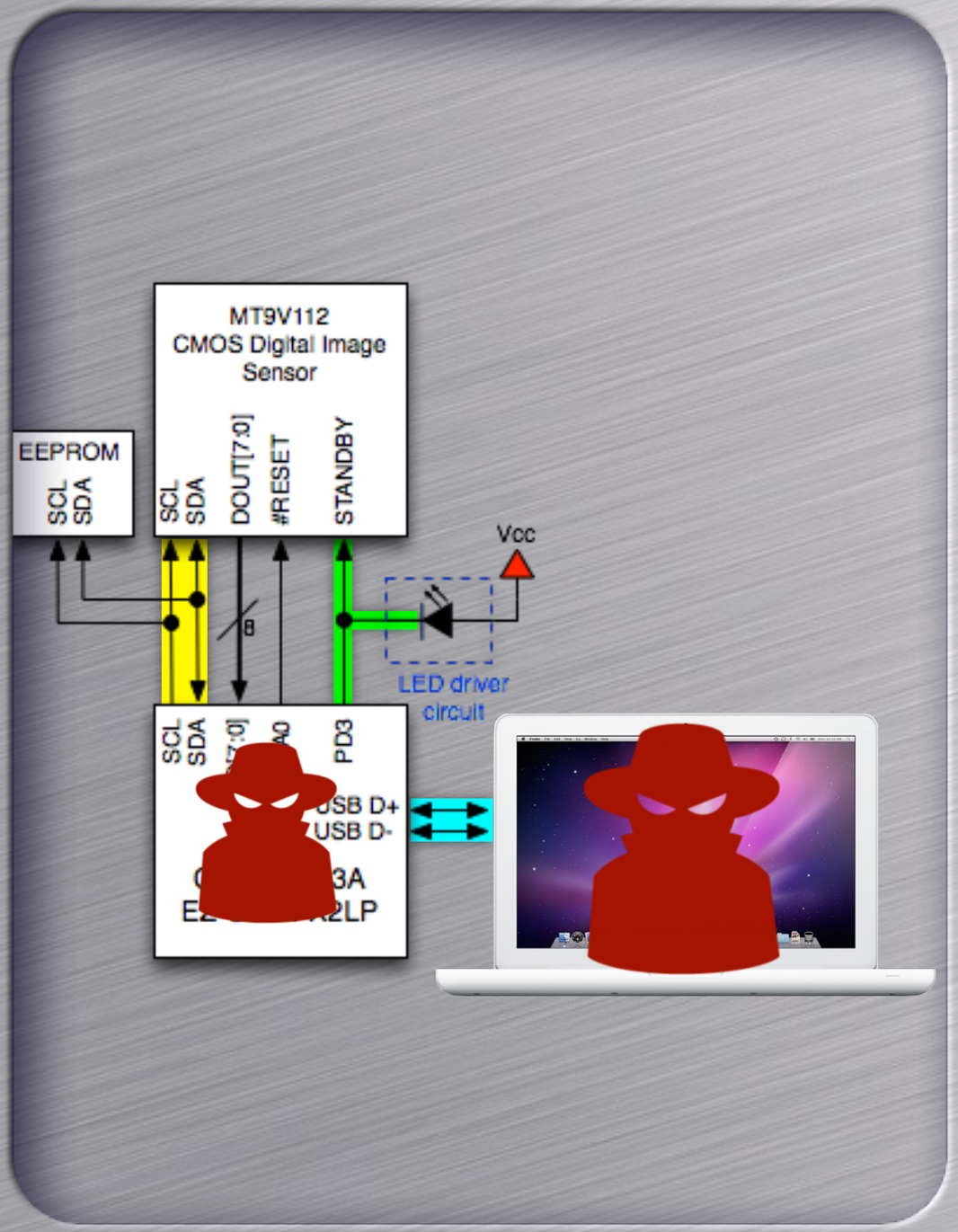
- Malware on host programs EZ-USB via USB
- EZ-USB sets RESET reg.
- LED under host control

Programming the EZ-USB



- Malware on host programs EZ-USB via USB
- EZ-USB sets RESET reg.
- LED under host control

Programming the EZ-USB



- Malware on host programs EZ-USB via USB
- EZ-USB sets RESET reg.
- LED under host control

Demo

What else can we do?

- Pretend to be a USB HID keyboard
- Break out of a Virtual Machine

Conclusions

- LED has privacy/security implications
- Software-circumventable defenses bad
- Processors in computer are vulnerable
- Security is a systems problem

Conclusions

- LED has privacy/security implications
- Software-circumventable defenses bad
- Processors in computer are vulnerable
- Security is a systems problem

Fin