iSeeYou:
Disabling the MacBook Webcam Indicator LED

Date: Sep 24/ 2014
Computer Science Department,
College of William&Mary
Email: wwtan@email.wm.edu
Is your webcam off?

“FBI has been able to covertly activate a computer’s camera without users knowing that.”

—Marcus Thomas, former assistant director of the FBI’s Operational Technology Division

Washington Post
Webcam-Spying

Cassidy Wolf, a 19-year-old Miss Teen USA, who fell victim to a webcam hacker.

– reported by Washington Post in 2013
A suburban Philadelphia school provided students MacBook laptops, which secretly recorded more than 30,000 images of those students’ daily life.
Solutions?
MacBook iSight

iSight from a 2008 MacBook
Webcam indicator LED
Can LED be turned off while recording?

- Can malicious firmware control the LED?
- Can malicious software (on the host) replace the firmware?
The authors found a way to activate iSight cameras without turning the LED light on.

Hackers webcam spying

LED indicator problem with both old and new MacBooks
Outline

Hardware

Architecture

Firmware

Software

Defense

Conclusion & Future Work Discussion
Hardware

Intel 8051-compatible microcontroller core
Outline

Hardware

Architecture

Firmware

Software

Defense

Conclusion & Future Work Discussion
iSight Architecture

- USB connection to the host
- EZ-USB configure image sensor via IIC
- 16 byte IIC EEPROM
- Standby connection (output disable)
iSight Architecture

PD3 controls STANDBY and LED

<table>
<thead>
<tr>
<th>PD3</th>
<th>STANDBY</th>
<th>LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Asserted</td>
<td>Off</td>
</tr>
<tr>
<td>Low</td>
<td>Deasserted</td>
<td>On</td>
</tr>
</tbody>
</table>
With Malicious Firmware

Set RESET register via IIC

Control LED via PD3
let LED be independent of STANDBY
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 register
- LED under host control
Demo

http://wapo.st/1eoJP9v

41 seconds
Washington Post video
What else we can do?
Approaches

- Apple deploys sandboxing tech: *App Sandbox*  
  (prevent applications inside the sandbox from accessing iSight)  
  but apps need to opt into the protection

- OS X kernel extension: *iSightDefender*  
  (modify the operation sys to prevent particular USB device requests,  
  block user space reprogramming attempts.)  
  but this is software-based defense, malware running as root  
  would have the ability to replace or modify kernel code
Outline

- Hardware
- Architecture
- Firmware
- Software
- Defense

Conclusion & Future Work Discussion
Conclusions

- LED has privacy/security implications
- Processors in computer are vulnerable
- Security is a systems problem
Future Works & Discussion

- Change hardware (Firmware can not be overwritten).
- Other security design?
- How about other web camera devices?
Back Up slides
## Narrow Down on 5 Image Sensors

### VGA Products

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Resolution</th>
<th>Pixel Size</th>
<th>Optical Format</th>
<th>Frame Rate</th>
<th>Maximum Data Rate</th>
<th>Power Consumption</th>
<th>Supply Voltage</th>
<th>Output</th>
<th>Shutter</th>
<th>Package</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW-MT9V012</td>
<td>640 x 480V</td>
<td>3.6μm x 3.6μm</td>
<td>1/6 inch</td>
<td>30 fps (VGA), 60 fps (CIF)</td>
<td>13.5 megapixels per second (27 MHz master clock)</td>
<td>Active: 54mW (© 30 fps VGA resolution)</td>
<td>2.5V-3.1V</td>
<td>10-bit rolling shutter (ERS)</td>
<td>28-pin IBGA, die or wafer</td>
<td>Mobile PC Cam</td>
<td></td>
</tr>
<tr>
<td>NEW-MT9V112 (SOC)</td>
<td>640 x 480V</td>
<td>3.6μm x 3.6μm</td>
<td>1/6 inch</td>
<td>30 fps @ 27 MHz</td>
<td>12-13.5 megapixels per second (master clock, 24 MHz-27 MHz)</td>
<td>&lt;78mW (© 30 fps)</td>
<td>1.7V-1.9V, 2.5V-3.1V</td>
<td>10-bit on-chip electronic rolling shutter (ERS)</td>
<td>36-pin ICSP, wafer or die</td>
<td>Mobile PC Cam</td>
<td></td>
</tr>
<tr>
<td>MT9V011</td>
<td>640 x 480V</td>
<td>5.6μm x 5.6μm</td>
<td>1/4 inch (4:3)</td>
<td>30 fps at 27 MHz</td>
<td>13.5 MPS/27 MHz</td>
<td>70mW @ 2.8V, 20pF load, 27 MHz, 30 fps</td>
<td>10-bit parallel electronic rolling shutter (ERS)</td>
<td>28-pin PLCC</td>
<td>Mobile PC Cam</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT9V111 (SOC)</td>
<td>640 x 480V</td>
<td>5.6μm x 5.6μm</td>
<td>1/4 inch (4:3)</td>
<td>15 fps @ 12 MHz (default) programmable up to 30 fps at 27 MHz</td>
<td>12-13.5 MPS/27 MHz</td>
<td>&lt;80mW @ 2.8V, 15fps @ 12 MHz</td>
<td>10-bit on-chip electronic rolling shutter (ERS)</td>
<td>44-Ball ICSP, wafer or die</td>
<td>Mobile PC Cam Automotive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT9V403</td>
<td>659 x 494V</td>
<td>9.9μm x 9.9μm</td>
<td>1/2 inch</td>
<td>0-200 frames/sec. with source illumination at 550nm</td>
<td>66 MB/s (master clock 66 MHz)</td>
<td>130mW@ 200 fps</td>
<td>3.3V</td>
<td>10-bit digital through a single port TrueSNAP™ freeze-frame electronic shutter</td>
<td>48-pin CLCC</td>
<td>High Speed</td>
<td></td>
</tr>
</tbody>
</table>
EZ-USB can query the chip version and then know the exact model of image sensor.