CamShield: Securing Smart Cameras through Physical Replication and Isolation

Zhiwei Wang, Yihui Yan, Yueli Yan, Huangxun Chen*, Zhice Yang
ShanghaiTech University, *Huawei Theory Lab
Visual Sensors are Ubiquitous

- Smartphone
- TV
- Pet Monitor
- Drone
- Security Camera
- Refrigerator
- Vehicle
Google Disables Xiaomi Integration After Nest Hub Picks Up Random Camera Feed

A user’s Google Nest Hub was showing images from a random camera feed instead of his own Xiaomi smart IP security camera.

(Source: securitysales.com)
More

Buyer Beware: Used Nest Cams Can Let People Spy on You

UPDATED JUNE 20, 2019

After our story broke yesterday, Google sent us a statement for the problem.

(Source: nytimes.com)
Encryption alone is Insufficient

• We are not sure if the camera can be trusted (the prerequisite for encryption to take effect)
Root of Trust

Camera System

- Application
- Operating System
- Hardware
Trust-nothing Solution

• Mark Zuckerberg Tapes over His Webcam. Should We?
  • Secure but block everything

(Source: theguardian.com)
CamShield – Bolt-on Root of Trust

1. Protect Visual Privacy and Retain Functionalities.

2. Compatible with Existing Cameras.
CamShield – Approach

- Real Scenes
- CamShield
- CamShield App (Remote Review)
- Cloud Server (Video Analysis)
- Internet
- Smart Camera (Recording Video)
CamShield – Approach

• Approach: **Physical Replication and Isolation**
• Why the protection is trustworthy?
  ➢ **Isolation**
• How does the protection affect original camera functionalities?
  ➢ **Replication**
CamShield Hardware

- Smart Camera
- Visual Sensor
- Screen
- Lens
- Processing Unit
- Smart Camera
Hardware Prototype

Smart Camera

Visual Sensor
CamShield Software

- Region of Interest (ROI) Encryption
- Visible Light Communication (VLC) Data Path
CamShield Software

- Region of Interest (ROI) Encryption
- Visible Light Communication (VLC) Data Path
Whole-frame v.s. Partial Encryption

- **Whole-frame Encryption**: full protection, disallows cloud analysis.
- **Partial Encryption**: the cloud server can still extract information, like motions or gestures, from the unencrypted parts.
ROI Encryption Workflow

① ROI Detection (CV Algorithm)

② HEVC (H.265) Encoding (Tile-based)

③ ROI Encryption
ROI Configuration

- ROI Policies

<table>
<thead>
<tr>
<th>Index</th>
<th>ROI</th>
<th>Invert</th>
<th>Alg.</th>
<th>Time</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>all</td>
<td>F</td>
<td>/</td>
<td>all</td>
<td>F</td>
</tr>
<tr>
<td>2</td>
<td>none</td>
<td>F</td>
<td>/</td>
<td>all</td>
<td>F</td>
</tr>
<tr>
<td>3</td>
<td>face</td>
<td>F</td>
<td>mobile  net</td>
<td>all</td>
<td>T</td>
</tr>
<tr>
<td>4</td>
<td>body</td>
<td>F</td>
<td>opencv</td>
<td>all</td>
<td>F</td>
</tr>
<tr>
<td>5</td>
<td>text</td>
<td>F</td>
<td>opencv</td>
<td>work  days</td>
<td>F</td>
</tr>
</tbody>
</table>

Table of ROI Entries

- Configuration Interface

CamShield App

ROI Config Message

Via QR-Code

CamShield Device
CamShield Software

- Region of Interest (ROI) Encryption
- Visible Light Communication (VLC) Data Path
How to Transfer Encrypted Video?

• Risks
  • Isolation breaches
Visible Light Communication (VLC)

<table>
<thead>
<tr>
<th>Bits</th>
<th>Block Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>Blue</td>
</tr>
<tr>
<td>010</td>
<td>Green</td>
</tr>
<tr>
<td>011</td>
<td>Cyan</td>
</tr>
<tr>
<td>100</td>
<td>Red</td>
</tr>
<tr>
<td>101</td>
<td>Yellow</td>
</tr>
<tr>
<td>110</td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>Black</td>
</tr>
</tbody>
</table>

display content on the screen
captured by the smart camera
Decoding VLC Streams

- Lens Distortion
- Chromatic Distortion

Grid Preamble

Color Palette Preamble
CamShield App

Smart Camera (Recording Video)

Cloud Server (Video Analysis)

Internet

CamShield App (Remote Preview)

Preview
CamShield App

Smart Camera (Recording Video)

Cloud Server (Video Analysis)

CamShield App (Remote Preview)
Conclusion

• We propose an approach to secure visual sensing devices.

• Advantages
  • Bolt-on Solution: it is compatible with commercial cameras, and retains their functionalities.
  • Strong Protection: the shield device is not only logically but also physically isolated from the camera and the network, preventing it from many practical attacks.
Thank You!

Contact: Zhice Yang yangzhc@shanghaitech.edu.cn