Building a Privacy-Preserving Smart Camera System

Yohan Beugin, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, Patrick McDaniel

PETS - July 11-15, 2022
Motivation

Motivation

Obscure providers’ incentives

Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns

By Deek Harwell
August 26, 2019 at 6:03 p.m. EDT

Senator blasts Amazon's Ring doorbell as an 'open door for privacy and civil liberty violations'

Sen. Ed Markey, D-Mass., called the lack of privacy protections "chilling."

Untrustworthy providers

Here's Anker's apology after 712 Eufy customers had camera feeds exposed to strangers

Eufy blames a software update and promises to do better
By Mitchell Clark | May 19, 2021, 3:00pm EDT

A Home Security Worker Hacked Into Surveillance Systems to Watch People Have Sex

By Lucas Ropek | 12/2/21 4:00PM | Comments (34)

Ring let employees watch customer videos, claim reports

'Unfiltered, round-the-clock live feeds from some customer cameras'
By Dari Deahl | @dari_deahl | Jan 10, 2019, 5:18pm EST
Goals

Smart camera systems need not compromise users' privacy.

How to:
1. Establish root of trust?
2. Manage the keys?

Features:
▶ Configuration
▶ Recording and Streaming
▶ Delegation
▶ Deletion
▶ Recovery
▶ Reset
Goals

Smart camera systems need not compromise users privacy.

Return control to users

Support commercial features
Goals

**Return control to users**

**Support commercial features**

How to:

1. Establish root of trust?
2. Manage the keys?

Features:

- Configuration
- Recording and Streaming
- Delegation
- Deletion
- Recovery
- Reset
Goals

Return control to users

Support commercial features

How to:
1. Establish root of trust?
2. Manage the keys?

Features:
- Configuration
- Recording and Streaming
- Delegation
- Deletion
- Recovery
- Reset
Establishing Root of Trust
Key Management

Seed key

$k_{ABCDEFGH}$
Key Management

Seed key

\[ k_{\text{ABCDEFGH}} \]

\[ k_{\text{ABCD}} \quad k_{\text{EFGH}} \]

\[ k_{\text{left}} = HKDF(k_{\text{parent}}) \]

\[ k_{\text{right}} = HKDF(k_{\text{parent}} \oplus 1) \]
Key Management

Seed key

\[ k_{ABCDEFGH} \]

\[ k_{ABCD} \]

\[ k_{AB} \]

\[ k_{CD} \]

\[ k_{EF} \]

\[ k_{GH} \]

\[ k_{left} = HKDF(k_{parent}) \]

\[ k_{right} = HKDF(k_{parent} \oplus 1) \]
Key Management

Seed key

\[ k_{ABCDEFGH} \]

\[ k_{ABCD} \]

\[ k_{AB} \]

\[ k_A \]

\[ k_{BC} \]

\[ k_B \]

\[ k_{CD} \]

\[ k_C \]

\[ k_{DE} \]

\[ k_D \]

\[ k_{EF} \]

\[ k_E \]

\[ k_{FG} \]

\[ k_F \]

\[ k_{GH} \]

\[ k_G \]

\[ k_{HG} \]

\[ k_H \]

\[ k_{left} = HKDF(k_{parent}) \]

\[ k_{right} = HKDF(k_{parent} \oplus 1) \]
Key Management

\[ k_{left} = HKDF(k_{parent}) \]
\[ k_{right} = HKDF(k_{parent} \oplus 1) \]

☞ Fine-grained delegation
CaCTUs

Camera system Controlled Totally by Users

Smart camera → Smartphone

- Initialization (3.2)
  System initialized

- Recording (3.3)
  Video frame encrypted and stored in cloud

- Factory reset (3.5)
  System uninitialized

- Streaming (3.3)
  Video streamed to smartphone until user exits

- Delegation (3.4)
  Owner shares encryption keys with a delegatee

- Deleting videos (3.5)
  Encryption keys deleted

- Access Recovery (3.6)
  Secrets recovered to new smartphone

- Factory reset (3.5)
  System uninitialized

- System initialized

- Uninitialized

- Initialized

- System initialized

- Video frame encrypted

- Streaming (3.3)
  Video streamed to smartphone until user exits

- Factory reset (3.5)
  System uninitialized

- System initialized
### Privacy and security analysis:

1. Right to not be seen
2. Right of sole ownership
3. Right to be forgotten

<table>
<thead>
<tr>
<th>Device Operation</th>
<th>Camera</th>
<th>Key Extraction</th>
<th>Frame Encryption</th>
<th>Signature</th>
<th>Upload</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average delay (ms)</td>
<td>0.05</td>
<td>0.03</td>
<td>4.0</td>
<td>8.8</td>
<td>662</td>
<td>204</td>
</tr>
<tr>
<td>Minimum delay (ms)</td>
<td>0.2</td>
<td>0.3</td>
<td>1.3</td>
<td>0.7</td>
<td>536</td>
<td>358</td>
</tr>
<tr>
<td>Maximum delay (ms)</td>
<td>2.2</td>
<td>0.6</td>
<td>1.6</td>
<td>2.8</td>
<td>365</td>
<td>475</td>
</tr>
</tbody>
</table>

**Table:**

Average delay during live stream at 480p (1000 frames)

- **Functional user evaluation**
  - Usable and simple
  - Fine-grained delegation
  - Sufficient quality
  - Improvements: latency and motion detection
Evaluation

Privacy and security analysis:

1. Right to not be seen
2. Right of sole ownership
3. Right to be forgotten

Performance evaluation

<table>
<thead>
<tr>
<th>Device</th>
<th>Operation</th>
<th>Delay</th>
<th>$\sigma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Key Extraction</td>
<td>0.05 ms</td>
<td>0.2 ms</td>
</tr>
<tr>
<td></td>
<td>Frame Encryption</td>
<td>4.0 ms</td>
<td>1.3 ms</td>
</tr>
<tr>
<td></td>
<td>Signature</td>
<td>8.8 ms</td>
<td>2.8 ms</td>
</tr>
<tr>
<td></td>
<td>Upload</td>
<td>662 ms</td>
<td>536 ms</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Download</td>
<td>204 ms</td>
<td>358 ms</td>
</tr>
<tr>
<td></td>
<td>Signature Verification</td>
<td>0.7 ms</td>
<td>0.5 ms</td>
</tr>
<tr>
<td></td>
<td>Key Extraction</td>
<td>0.03 ms</td>
<td>0.3 ms</td>
</tr>
<tr>
<td></td>
<td>Frame Decryption</td>
<td>0.6 ms</td>
<td>0.6 ms</td>
</tr>
</tbody>
</table>

Table: Average delay during live stream at 480 p (1000 frames)
Evaluation

Privacy and security analysis:

1. Right to not be seen
2. Right of sole ownership
3. Right to be forgotten

Performance evaluation

<table>
<thead>
<tr>
<th>Device</th>
<th>Operation</th>
<th>Delay</th>
<th>( \sigma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Key Extraction</td>
<td>0.05 ms</td>
<td>0.2 ms</td>
</tr>
<tr>
<td></td>
<td>Frame Encryption</td>
<td>4.0 ms</td>
<td>1.3 ms</td>
</tr>
<tr>
<td></td>
<td>Signature</td>
<td>8.8 ms</td>
<td>2.8 ms</td>
</tr>
<tr>
<td></td>
<td>Upload</td>
<td>662 ms</td>
<td>536 ms</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Download</td>
<td>204 ms</td>
<td>358 ms</td>
</tr>
<tr>
<td></td>
<td>Signature Verification</td>
<td>0.7 ms</td>
<td>0.5 ms</td>
</tr>
<tr>
<td></td>
<td>Key Extraction</td>
<td>0.03 ms</td>
<td>0.3 ms</td>
</tr>
<tr>
<td></td>
<td>Frame Decryption</td>
<td>0.6 ms</td>
<td>0.6 ms</td>
</tr>
</tbody>
</table>

Functional user evaluation

- Usable and simple
- Fine-grained delegation
- Sufficient quality
- Improvements: latency and motion detection

Table: Average delay during live stream at 480p (1000 frames)
Conclusion

No need to compromise users privacy:

1. Return full control to users:
   - Root of trust
   - Complete mediation

2. Support commercial functionality

3. Extensible to other IoT devices

Paper: Building a Privacy-Preserving Smart Camera System

Code: ☑️ https://github.com/siis/CaCTUs

✉️ yohan@beugin.org  🏡 https://yohan.beugin.org