HOMESPY: The Invisible Sniffer of Infrared Remote Control of Smart TVs

Kong Huang¹, YuTong Zhou¹, Ke Zhang¹, Jiacen Xu², Jiongyi Chen³, Di Tang⁴, and Kehuan Zhang¹

¹The Chinese University of Hong Kong,
²University of California, Irvine,
³National University of Defense Technology,
⁴Indiana University Bloomington

Kong Huang, Ph.D
SVP, Head of Product & Technology
Consumer Business Group, HK Telecom
Motivation

HOMESPY: The Invisible Sniffer of Infrared Remote Control of Smart TVs

© Copyright 2023
1. Smart TV Penetration over 50% by year 2026
2. Top 5 smart home devices in 2021:
   - Smart TV
   - Streaming device
   - Smart lighting
   - Voice assisted speaker
   - Smart appliance (e.g. air-conditioner)
Typical Smart Home

Smart TV

Internet

Smart Appliances

Infrared TV remote control
It is important to understand more about the smart home devices’ security implications and how to protect them.
Security and privacy issues in smart home

Identify activities in smart home analyzing network traffic
Sniffing of Wi-Fi signal to infer user activities
Eavesdropping on wireless transmission of sensors
Inferring video watched on TV using ambient light sensors of mobile phone
Instructing voice assistant to make payments or unlock homes through malicious voice commands
Observations and key questions

• Is it possible for an IoT device to sniff smart TV IR remote control signals, even when it is not on the path between TV and controller?

• What harm would it cause?
Traditional IR control use case

- IR is a line-of-sight communication with a range within 10 meters, the attacker needs to stay close to the victim => high cost of attack
- Main use is to change channels, the information carried is insensitive => low value of privacy data

⇒ The IR communication at home is safe and secure, to the extent that no data protection is needed
Revisit security of IR communication

• IR communication is **NOT** a security threat because
  
  • IR is a line-of-sight communication with a range within 10 meters
  
  • The signal strength will be weakened after a single reflection
  
  • The information carried is insensitive

• Build a prototype HOMEspy to show a new IR sniffing attacking

  • IR could be sniffed by a commercial off-the-shelf (COTS) receiver not in the line-of-sight and even after reflection
  
  • Smart home or IoT device with IR receiving capability makes remote attack feasible
  
  • Sensitive login/payment information is entered using IR remote control on smart TV using a virtual keyboard
Infrared remote control

IR transmitter of remote control
IR receiver of the smart home device

**NEC protocol**
- Pulse distance modulation
- Address and command are transmitted twice
- **Unencrypted**

**Sony SIRC (12-bit)**
- Pulse width modulation
- Address and command are repeated every 45ms for as long as the key is held down
- **Unencrypted**
Smart TV

• 4 major functions:
  • Free-to-air channels (built-in tuner)
  • Video output through HDMI
  • Settings (Wi-Fi, Login - user name/password, PINs)
  • Smart TV Apps (Entertainment, gaming, shopping, etc.)

<table>
<thead>
<tr>
<th>App Name</th>
<th>Virtual Keyboard (using Remote Controller)</th>
<th>Mobile App</th>
<th>Web Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netflix</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>YouTube</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Spotify</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Apple TV</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canal+</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Line TV</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAZN</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tencent Video/WeTV</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BeIN Connect</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Prime</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HBO GO</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Disney+</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Table 2.2: Input methods of different smart TV Apps.

Figure 2.4: YouTube app and login screen.
Adversary model

1. Gain control of an IoT device with power by an attacker
   ⇒ Many smart devices support IR
   ⇒ Vulnerable IoT device is prevalent

2. Position of the device to sniff the IR signal
   ⇒ No line-of-sight assumption

3. Decode the IR command and extract information
   ⇒ No prior knowledge of the TV brands and protocols
IR Sniffer

• Commercial off-the-shelf (COTS) IR receiver module using VS1838B
  • A shorter distance of 20 meters
  • A low cost (less than USD 0.1@)
  • Reception angle +/- 45°

• Raspberry-Pi as the prototype of the compromised IoT device

(a) IR Sniffer on Raspberry-Pi 3

© Copyright 2023
IR Command Decoder

• Collect from IRDB + Remote Central DB
• The codes are in ProntoHex format which uses a pair of 4-digits hexadecimal numbers to represent an on/off sequence.
• Convert ProntoHex format into IR raw timing sequence using MakeHex and irgen.
• Result: 75,901 IR codes for 1,303 devices
Semantic Extractor

- Assume the more challenging remote with D-Pad only
- Virtual keyboard is bought up at the same initial position “q”
- Assumed character length (email, password) and time window for virtual keyboard sequence using empirical study and previous works to classify valid entry, and we prune the sub-sequence with “OK” at ENTER key.
- Filter out candidates with known PIN or email characteristics

Figure 4.5: Layouts of android TV standard virtual keyboard.
Each participant is asked to complete the following tasks:

- **Task 1**: entering 10 email-based login credentials (i.e., email addresses and passwords) and 2 phone-number-based login credentials (i.e., phone numbers and passwords), using a virtual QWERTY keyboard as shown in Fig. 4.9-i;
- **Task 2**: entering 50 PIN code with 4-digits, using the number pad layout as shown in Fig. 4.9-v;
- **Task 3**: navigating on the YouTube app for 10 minutes, with an IR remote controller.

$T_W$ and $TH_{OK}$ to 300 (seconds) and 150
## Evaluation result

<table>
<thead>
<tr>
<th>IR Key sniffed</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>p1</td>
<td>10</td>
<td>6</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>p2</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>p3</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>p4</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>p5</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>p6</td>
<td>9</td>
<td>7</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>p7</td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>p8</td>
<td>10</td>
<td>7</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>p9</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>p10</td>
<td>-</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>p11</td>
<td>-</td>
<td>9</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>p12</td>
<td>-</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>p13</td>
<td>-</td>
<td>-</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>p14</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td>p15</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>p16</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>p17</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>p18</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
</tr>
</tbody>
</table>

**Extraction Accuracy**

<table>
<thead>
<tr>
<th></th>
<th>98.9%</th>
<th>90.8%</th>
<th>83.1%</th>
<th>75.0%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed</td>
<td>1.1%</td>
<td>9.2%</td>
<td>16.9%</td>
<td>25.0%</td>
</tr>
</tbody>
</table>

![Distribution of Candidate Size](image)

*Figure 4.8: Distribution of candidate string sizes from HOME Spy.*

### Table 4.2: The accuracy of HOME Spy IR sniffer (ratio of correct sniffed keys and pressed keys).

<table>
<thead>
<tr>
<th>User #</th>
<th>Top1</th>
<th>Top3</th>
<th>Top5</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1</td>
<td>17%</td>
<td>50%</td>
<td>58%</td>
</tr>
<tr>
<td>U2</td>
<td>75%</td>
<td>75%</td>
<td>75%</td>
</tr>
<tr>
<td>U3</td>
<td>58%</td>
<td>83%</td>
<td>100%</td>
</tr>
<tr>
<td>U4</td>
<td>33%</td>
<td>58%</td>
<td>67%</td>
</tr>
<tr>
<td>U5</td>
<td>50%</td>
<td>83%</td>
<td>83%</td>
</tr>
<tr>
<td><strong>Mean</strong></td>
<td><strong>47%</strong></td>
<td><strong>70%</strong></td>
<td><strong>77%</strong></td>
</tr>
</tbody>
</table>

*Table 4.3: Accuracy of HOME Spy semantic extraction on the collected samples.*
HomeSpy attack on email login of Youtube app on smart TV

The video demonstrate a login using YouTube app on Sony TV. The user’s login is 
tdemars16@gmail.com and password is wolfmighet. The IR sniffer is located at the back of the sofa  
(the position of smart air-conditioner is the same as p13 in layout C in Fig.9 of the paper. The IR  
sniffer send the captured data to remote attacker through internet. The candidate list of email and  
password is shown in the blue console at the bottom right corner of the video and listed below for  
reference:

1. tdemars16@gmail.com/wolfmight
2. r. fc.f/fuf@g@ fvbx -wz_
3. em fc. f/fuf@g@ fvbx -wz_
4. qya&&@&8%9?/wolfmight,
5. ya&&@&8%9?/wolfmight,
6. a&&@&8%9?/wolfmight

Total 6 candidates (before applying common email and password rules)
HomeSpy Attack Demo

HomeSpy attack on content being watched on smart TV

The video demonstrates a user watching linear free-to-air channel on smart TV. The IR sniffer will send the IR data to remote. The inference takes effect when there is a direct input of numerical digits that match the free-to-air channel number in a specific location. Based on time of capture, and the IP location of the smart air-conditioner, the attacker could infer the TV channel and TV program that the victim is watching, the result is shown on the blue console at the bottom right corner of the video. Subsequent capture of CH+ or CH- key on the remote will be captured to infer the navigation of the channel list and therefore able to know the final channel number and the program that the victim is watching.

In the demo:
The 12 free-to-air channel in HK:

Digital TV: Full Digital TV Broadcast

The EPG of each channel can be found per TV broadcaster website:

RTHK (Ch. 31, 32, 33)

HK Open TV (Ch. 76, 77)

TVB (Ch. 81, 82, 83, 84, 85)

Jade (81) - EPG - myTV SUPER

J2 (82) - EPG - myTV SUPER

TVB News Channel (83) - EPG - myTV SUPER

Pearl (84) - EPG - myTV SUPER

TVB Finance & Information Channel (85) - EPG - myTV SUPER

Viu TV (Ch. 96, 99)

ViuTV

ViuTV

Or through 3rd party web/app:

香港網絡電視 HKTV EPG (網頁版) (jftv105.com)
Discussions

Securing IR communications

• Encryption requires some form of exchange of messages between TV and remote. It is hard as IR is one-way communication.

• Two-way communications require extra hardware or the user’s help.
  • If the message is too long, inconvenience to the user
  • If the message is too short, no guarantee against a brute-forcing attack

➔ It is difficult to deploy security mechanism considering the trade-off between usability and security
Contributions:

- **Re-examination of IR remote control security.** We have developed a HOMESPY attack and evaluated its performance.

- **A new IR sniffing attack.** An IoT device sitting in the same room can sniff IR signals at home, and attackers can derive sensitive information via semantic extraction techniques.

- **New threat to smart home security.** Smart IoT devices support IR for compatibility with universal remote controllers, creating an ongoing threat to smart home security through the invisible IR vulnerability.
Thank you!

Dr. Kong Huang (Keith)

E-mail: keith.k.huang@gmail.com