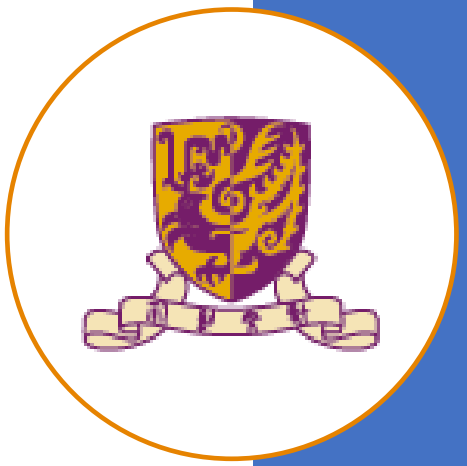
HOMESPY: The Invisible Sniffer of Infrared Remote Control of Smart TVs

Kong Huang[1], YuTong Zhou[1], Ke Zhang[1], Jiacen Xu[2], Jiongyi Chen[3], Di Tang[4], and Kehuan Zhang[1]

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



Kong Huang, Ph.D

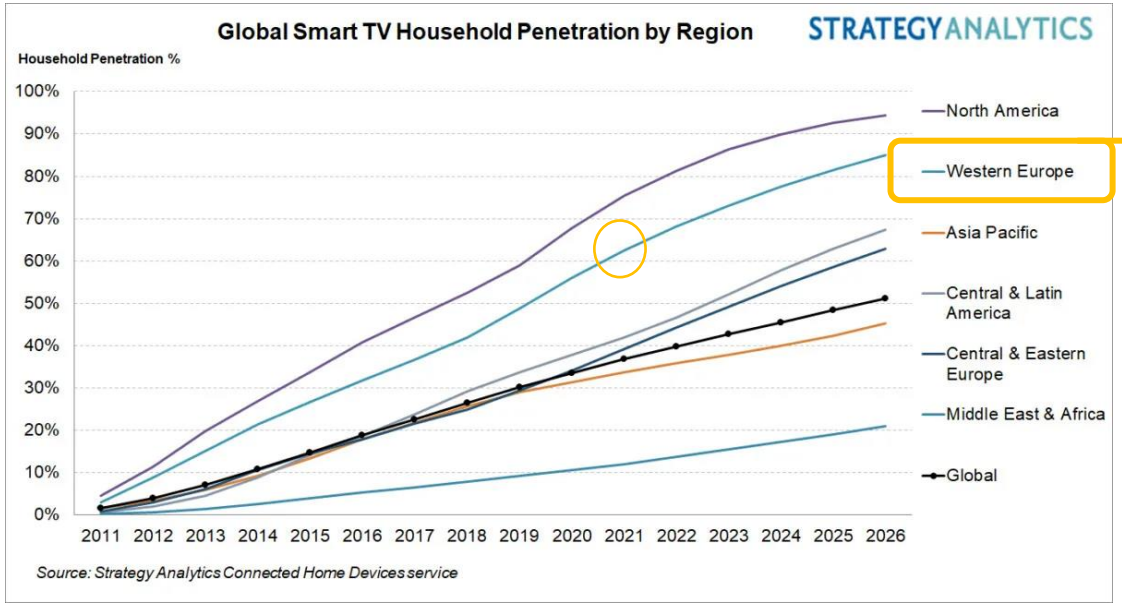
SVP, Head of Product & Technology

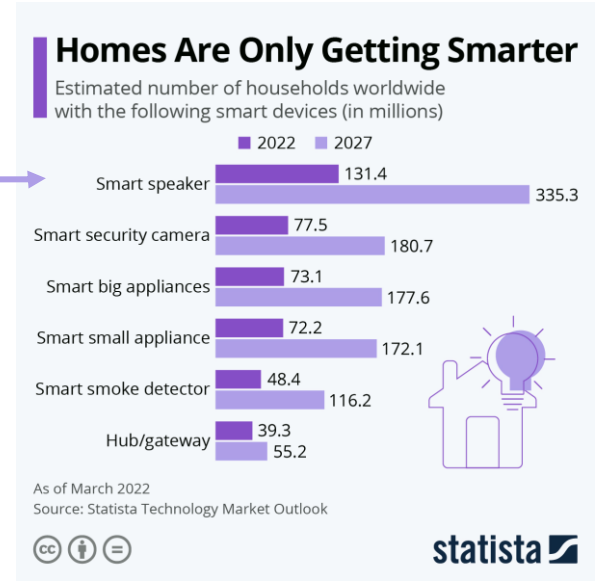
Consumer Business Group, HK Telecom

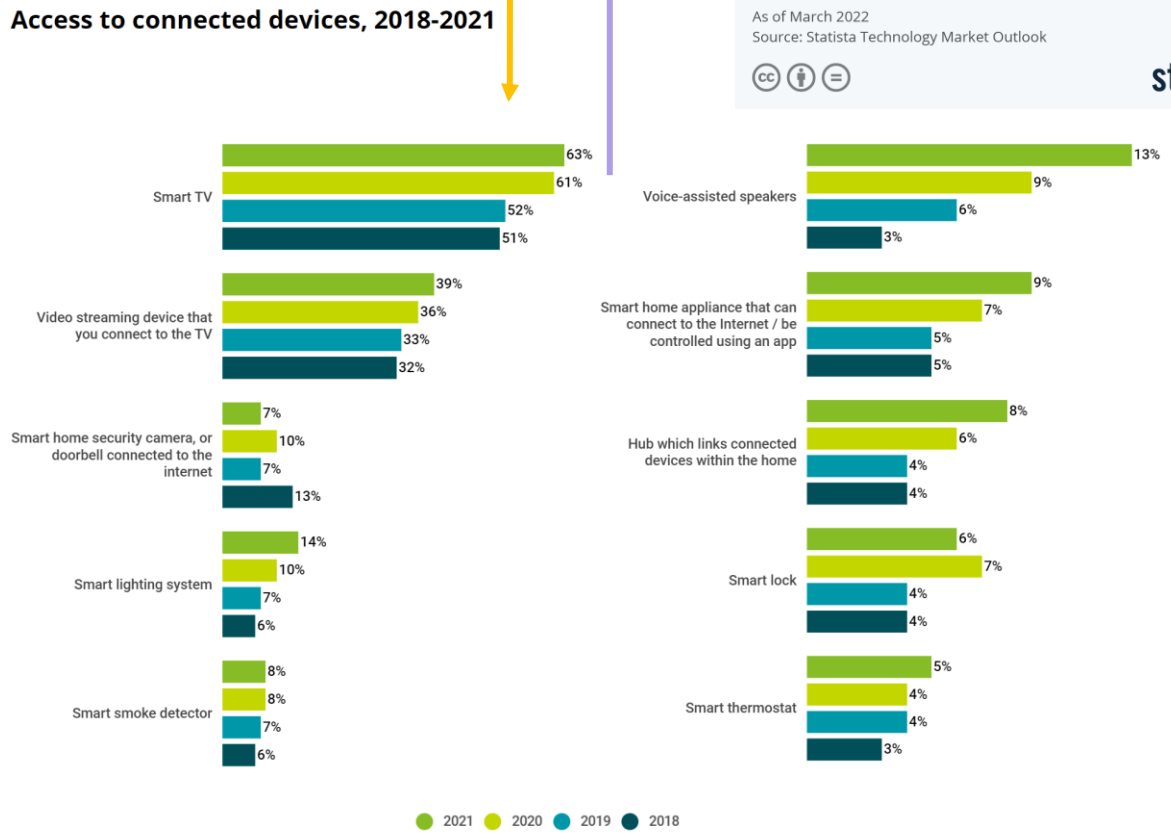
Motivation

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

Smart home device penetration

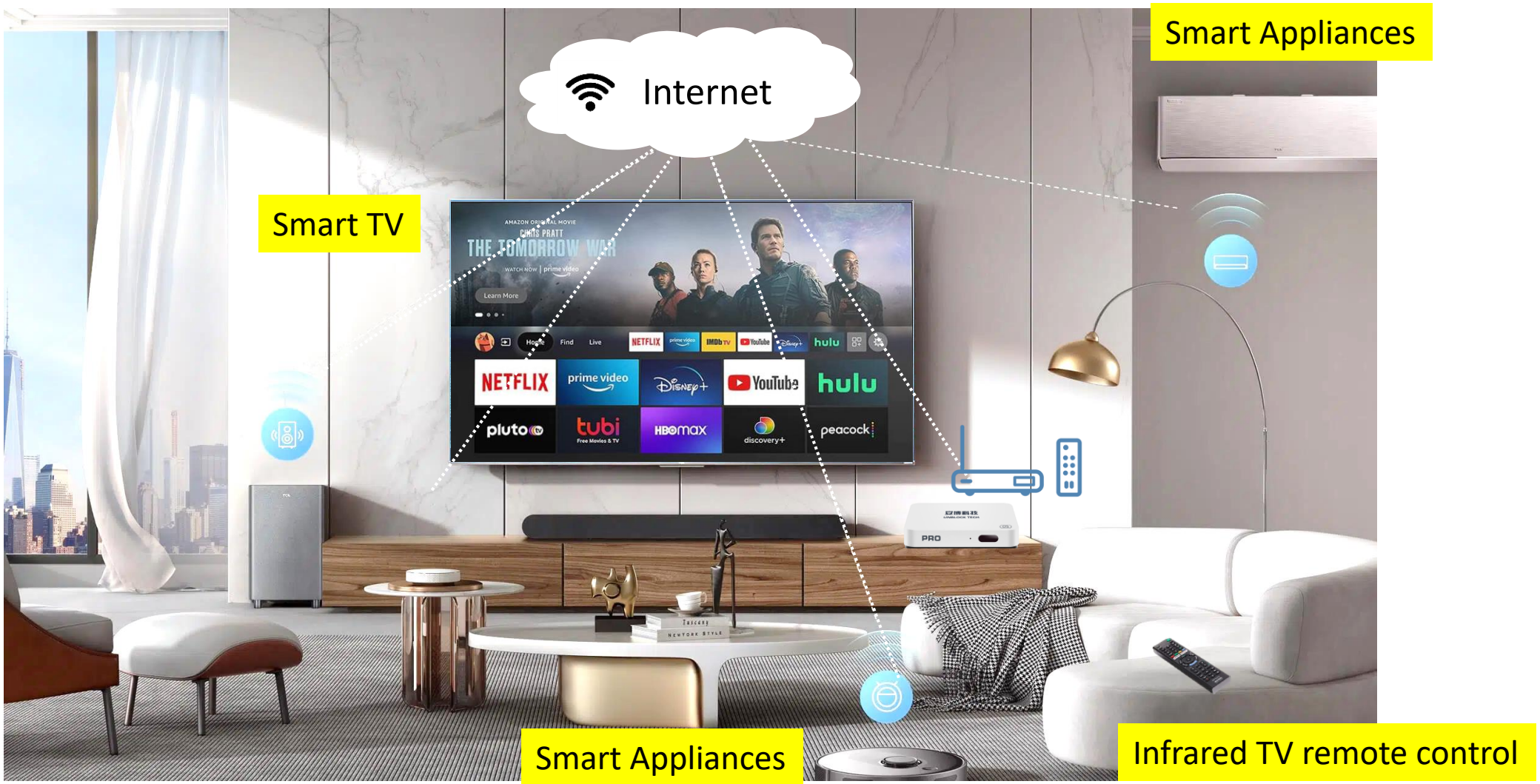






1. Smart TV Penetration over 50% by year 2026
2. Top 5 smart home devices in 2021:
   - Smart TV
   - Streaming device
   - Smart lighting
   - Voice assisted speaker
   - Smart appliance (e.g. air-conditioner)

Typical Smart Home



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

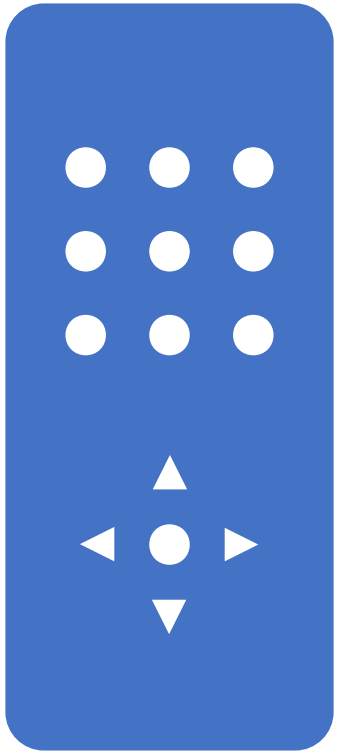
Identify activities in smart home analyzing network traffic

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

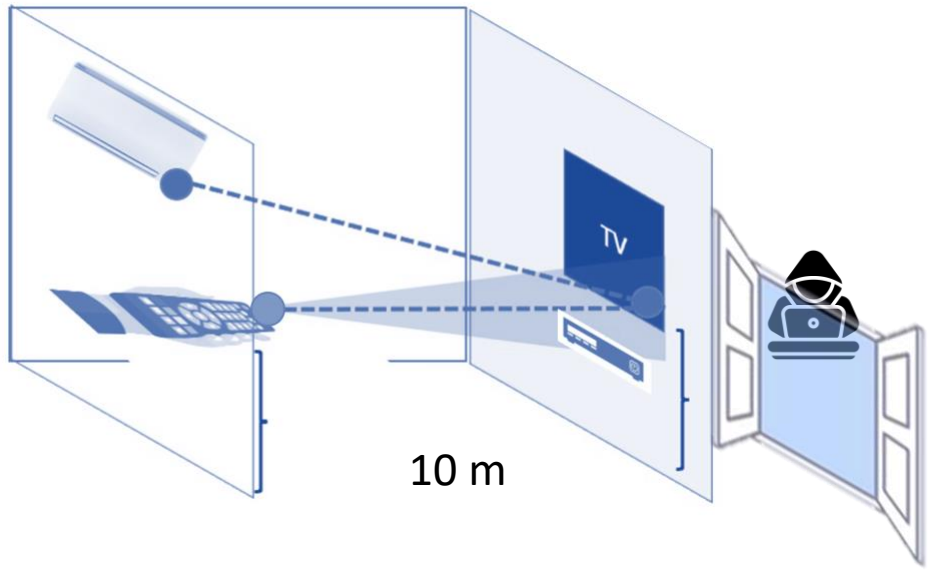
- Is it possible for an IoT device to sniff **smart TV** IR remote control signals, even when it is not on the path between TV and controller?
- What harm would it cause?

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



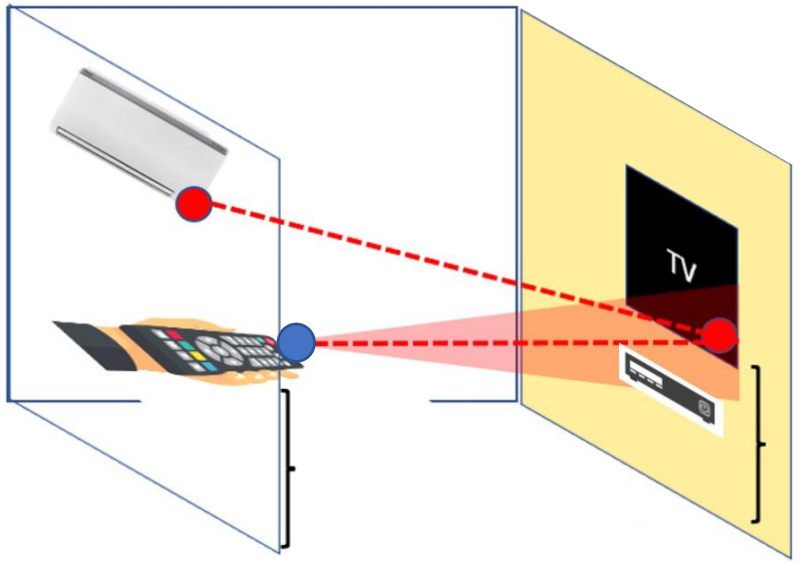
Attacker need to be close to the victim, and in the line-of-sight

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

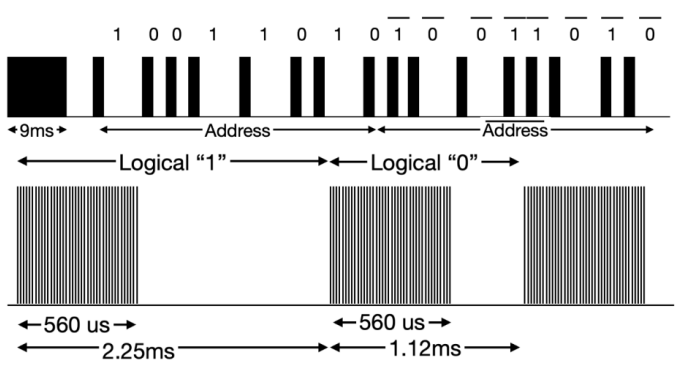


Figure 2.2: NEC protocol (top) and the modulation (bottom) at carrier frequency of 38kHz. [78]

NEC protocol

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

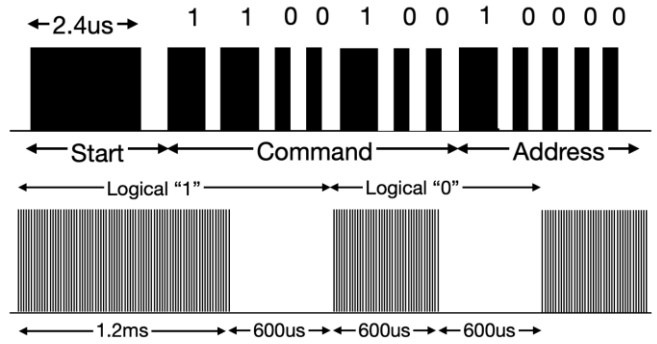


Figure 2.3: Sony SIRC protocol (top) and the modulation (bottom) at carrier frequency of 40kHz. [33]

Sony SIRC (12-bit)

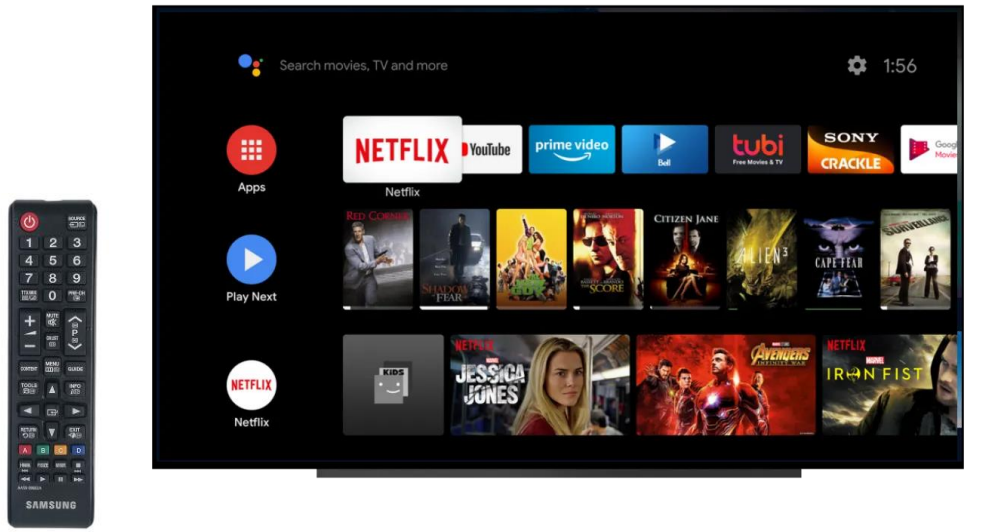
- Pulse width modulation
- Address and command are repeated every 45ms for as long as the key is held down
- **Unencrypted**

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.

App Name	Virtual Keyboard using Remote Controller	Mobile App	Web Service
Netflix	✓	✓	
YouTube	✓	✓	
Spotify	✓		✓
Apple TV	✓	✓	
Canal+	✓	✓	
Line TV	✓		
DAZN	✓		
Tencent Video/WeTV	✓		
BeIN Connect		✓	
Amazon Prime		✓	
HBO GO		✓	✓
Disney+			✓

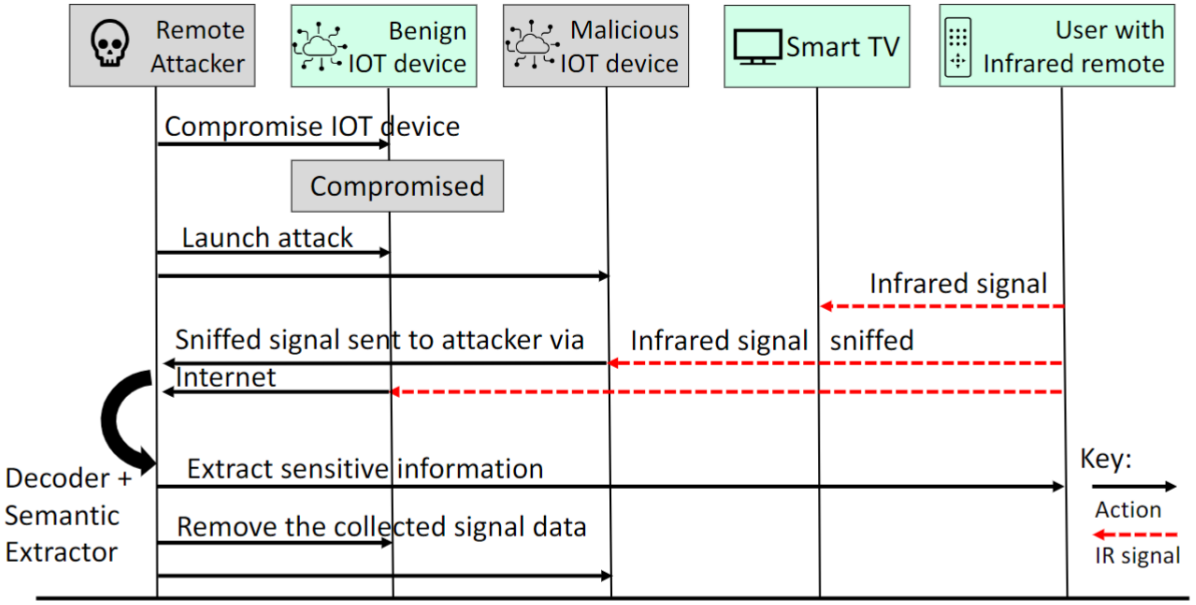
Table 2.2: Input methods of different smart TV Apps.



(a) YouTube App on Smart TV (b) Login screen of Google Account

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^{o}
- Raspberry-Pi as the prototype of the compromised IoT device

(a) IR Sniffer on Raspberry-Pi 3

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

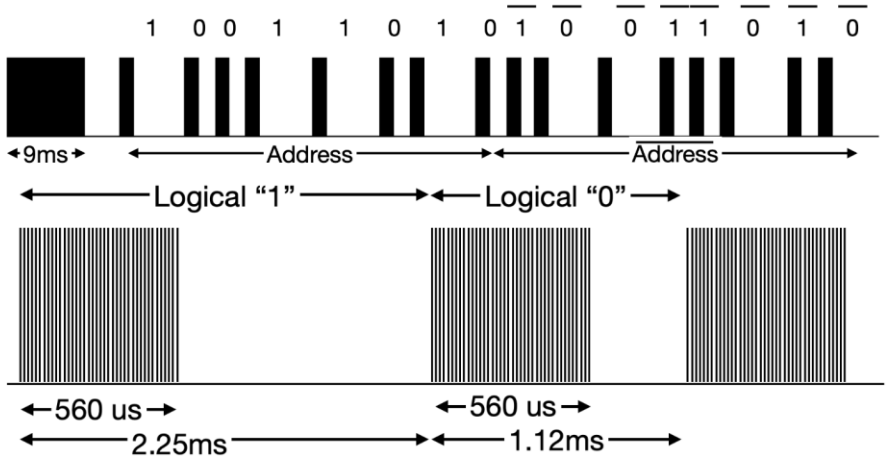


Figure 2.2: NEC protocol (top) and the modulation (bottom) at carrier frequency of 38kHz. [78]

ProntoHex Format:

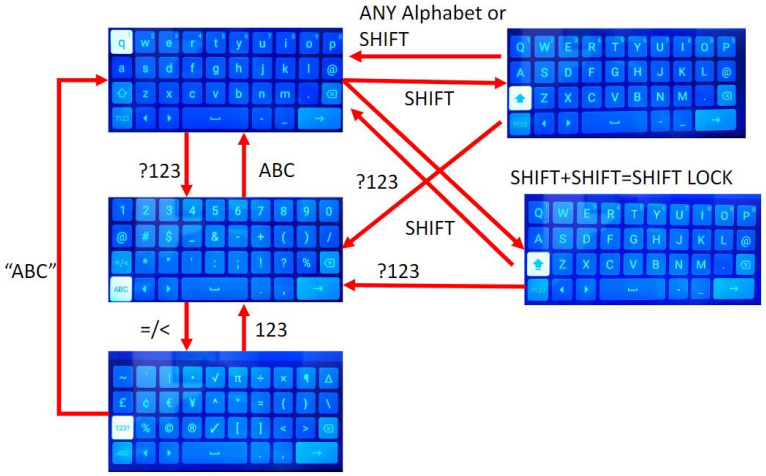
```
00ab 00ab
0015 003f 0015 0015 0015 0015 0015 003f 0015 003f 0015 0015 0015 003f 0015 0015
0015 0015 0015 003f 0015 003f 0015 0015 0015 0015 0015 003f 0015 0015 0015 003f
```

IR Raw Timing in microseconds:

```
4500 4500
560 1690 560 560 560 560 560 1690 560 1690 560 560 560 1690 560 560
560 560 560 1690 560 1690 560 560 560 560 560 1690 560 560 560 1690
```

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



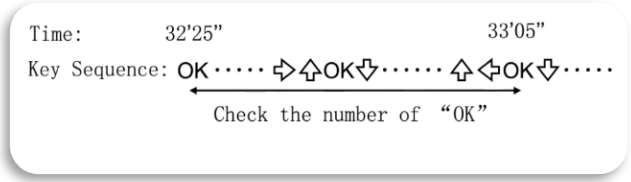


Figure 4.5: Layouts of android TV standard virtual keyboard.

Algorithm 4: Keyboard Information Extraction

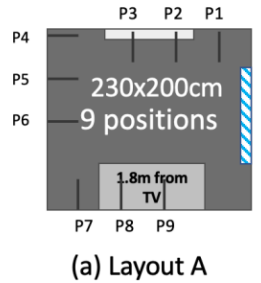
input : Sequence, Keyboard([page_number, y_position, x_postion])
output: Extracted private information candidates

```
candidates = []
// Establish the Keyboard position mapping
for p = 1...Keyboard.page_number do
    for y = 1...Keyboard[p].y_number do
        for x = 1...Keyboard[p,y].x_number do
            mapping[p-1,y-1,x-1] = Keyboard[p,y,x]
        end
    end
end
// Check each potential sequence and generate candidates
for i = 0 ... Sequence.length do
    position ← [0,0,0]
    data = Sequence[i:]
    message = ''
    for c in data do
        if c == 'BACK' then
            break
        else if c in ['UP','DOWN','LEFT','RIGHT'] then
            position = Change_position(position, c)
        else if c == 'OK' then
            if mapping[position] == 'ENTER' then
                candidates.append(message)
                message = ''
                position ← [0,0,0]
            else if mapping[position] == 'SHIFT' then
                if position.page == 1 then
                    position.page = 0
                else if position.page = 0 then
                    position.page = 1
            else if mapping[position] == 'NUMBER' then
                if position.page == 2 then
                    position.page = 0
                else if position.page = 0 then
                    position.page = 2
            else
                message += mapping[position]
    end
    candidates = Filter(candidates)
    return candidates
end
```

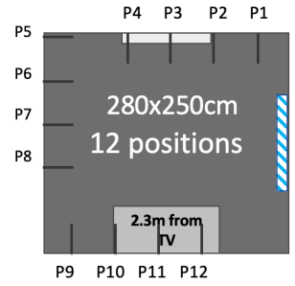
Experiment setup

(b) Setup of IR sniffer

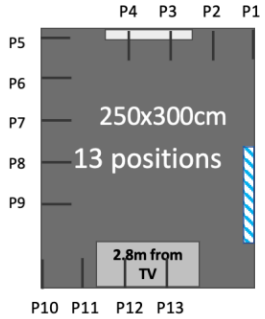
(c) Living room – Layout C



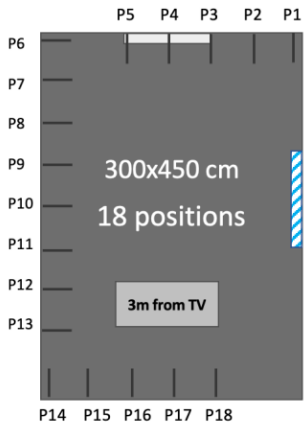
(a) Layout A



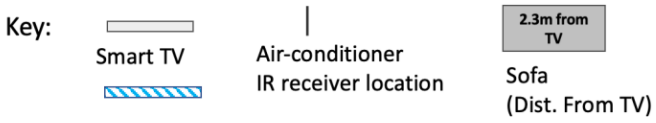
(b) Layout B



(c) Layout C



(d) Layout D



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.

TW and TH_{OK} to 300 (seconds) and 150

Evaluation result

IR Key sniffed	A	B	C	D
p1	10	6	10	10
p2	10	10	10	10
p3	10	10	10	10
p4	10	10	10	10
p5	10	10	10	10
p6	9	7	10	10
p7	10	10	8	10
p8	10	7	0	10
p9	10	10	0	10
p10	-	10	10	0
p11	-	9	10	0
p12	-	10	10	0
p13	-	-	10	0
p14	-	-	-	5
p15	-	-	-	10
p16	-	-	-	10
p17	-	-	-	10
p18	-	-	-	10
Extraction Accuracy	98.9%	90.8%	83.1%	75.0%
Missed	1.1%	9.2%	16.9%	25.0%

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

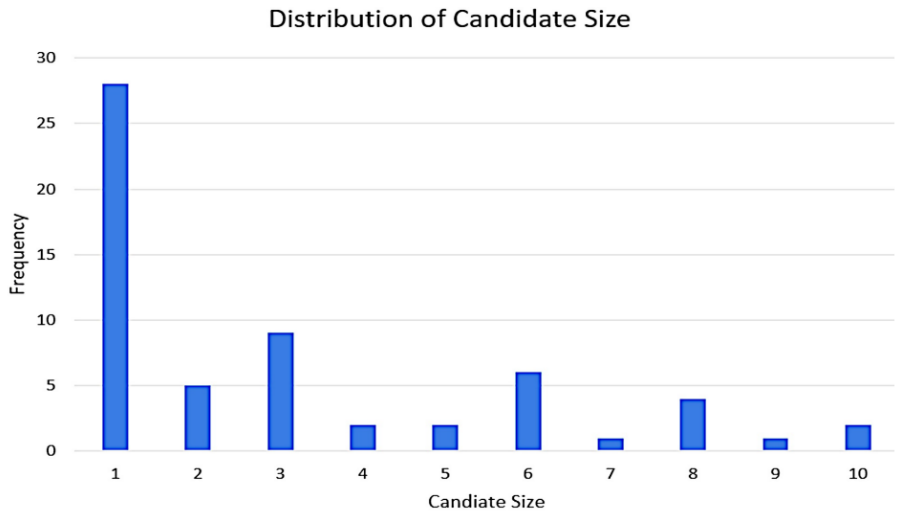


Figure 4.8: Distribution of candidate string sizes from HomeSpy.

User #	Top1	Top3	Top5
U1	17%	50%	58%
U2	75%	75%	75%
U3	58%	83%	100%
U4	33%	58%	67%
U5	50%	83%	83%
Mean	**47%**	**70%**	**77%**

Table 4.3: Accuracy of HomeSpy semantic extraction on the collected samples.

HomeSpy Attack Demo

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 wolfmight. 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/fu tg@ fvbx -wz_,
3. e m fc. f/fu tg@ 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 demonstrate a user watching linear free-to-air channel on smart TV. The IR sniffer will send the IR data to remote. The inference take effect when there is a direct input of number digit 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)
rthk.hk : TV|TIMETABLE

HK Open TV (Ch.76, 77)
香港開電視 Hong Kong Open TV (hkopentv.com)

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

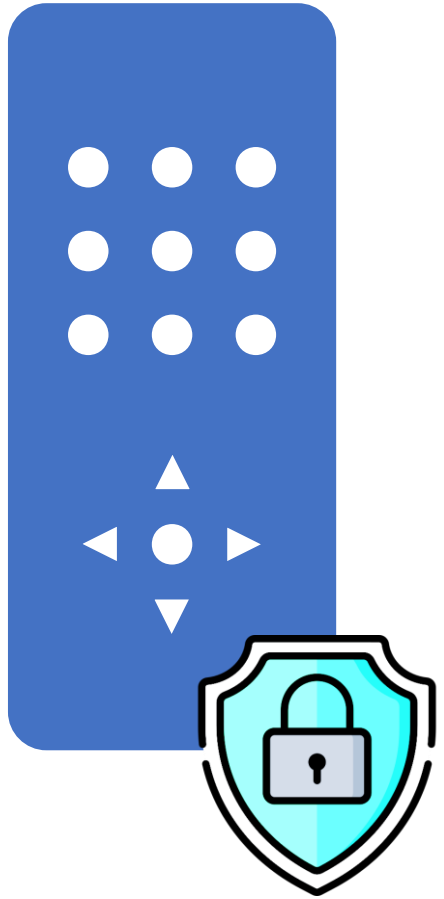
Or through 3rd party web/app:
香港電視節目表 HKTV EPG (網頁版) (jaffeling.com)

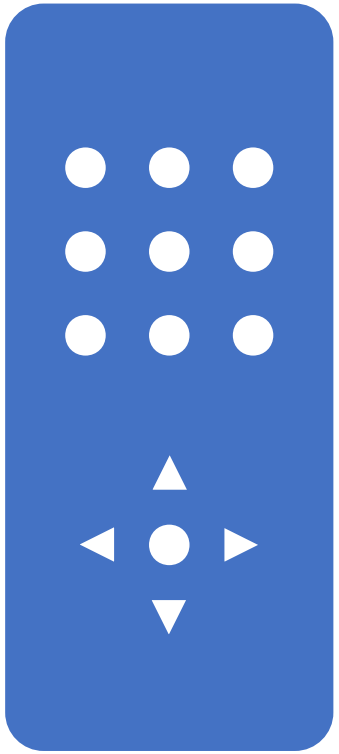
Discussions

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.

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

Kong Huang[1], YuTong Zhou[1], Ke Zhang[1], Jiacen Xu[2], Jiongyi Chen[3], Di Tang[4], and Kehuan Zhang[1]

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

Thank you!

Dr. Kong Huang (Keith)

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