Computer Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Potential risk of IoT device supporting IR remote control

Zheng Zhou[a], Weiming Zhang[a,*], Shangbin Li[b], Nenghai Yu[a]

[a] Key Laboratory of Electromagnetic Space Information of the Chinese Academy of Sciences, University of Science and Technology of China, China
[b] Key Laboratory of Wireless-Optical Communications of the Chinese Academy of Sciences, University of Science and Technology of China, China

ARTICLE INFO

Article history:
Received 29 July 2018
Revised 8 November 2018
Accepted 12 November 2018
Available online xxx

Keywords:
Internet of things (IoT)
Infrared (IR)
Remote control
Covert channel
Data exfiltration
Air-gapped

ABSTRACT

Infrared (IR) remote control technology is widely applied in daily human life. IR remote control signals are a simple, safe and reliable resource that can help to control nearby electrical appliances. With the development of Internet of things (IoT) technology, an increasing number of IoT devices supporting IR remote control access the Internet. In this paper, a malicious IR hardware module (MIRM) is made. The MIRM is implanted into a keyboard in an air-gapped network to control nearby IoT devices to leak sensitive data out. In our attack experiments on a smart TV set-top box, the rate of the covert channel can reach 3.15 bits/s. The potential risk that IoT devices can be exploited maliciously to leak sensitive data is revealed. Finally, a list of countermeasures is presented to enhance security of IR remote control and eliminate such covert channels.

1. Introduction

With the development of the Internet of things (IoT), an increasing number of devices can access the Internet. "For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide [1]." Furthermore, "267 billion US dollars will be spent on IoT technologies, products, and services [2]." This greatly promoted the development of home automation. When connected with the Internet, home devices are an important constituent of IoT. To providing convenience to users, many smart appliances inherit infrared (IR) remote control function that have been widely utilized on conventional non-IoT appliances. There are many advantages of IR remote control. However, the main weak point of IR remote control is that no authentication or identification is needed to control an appliance. It is not a matter to conventional appliance without accessing the Internet. But for a smart appliance, the risk of being exploited to build covert channels requires consideration.

As a method to leak sensitive data, the definition of *covert channel* was given by Lampson in 1973 to refer to those channels that are not used for normal communication [3]. He found that the shared resources could be abused by processes with different privilege levels to circumvent the security mechanism. With the development of network technology, many new types of covert channel have been found in the past twenty years. Zander et al. [4] surveyed the network covert channels in different types of network protocols in 2007.

To protect against the threats of network covert channels, physical isolation is conducted in top-secret organizations to keep networks with high security levels separated from less-secure networks and the Internet. This type of isolation is known as *air-gapped*. However, an air-gapped network is still not sufficiently safe to eliminate data leakage. Numerous methods for breaching air-gapped networks have been proposed over the last ten years.

Side channels and covert channels are two kinds of channels that can be exploited to attack an air-gapped system. A side channel is used to obtain information by receiving passively the signal emitted from the target system. Whereas, if a covert channel is exploited by an attacker, he/she must compromise both sides of it. Therefore, it is a necessary step to infect the target system in an air-gapped network [5–7].

Infecting air-gapped networks can be accomplished, as demonstrated by incidents such as Stuxnet [8] and Agent.Btz [9] etc. There are two directions of data leakage: *infiltration* and *exfiltration*. Infiltrations of air-gapped networks include the following general methods:

- Supply chain attack [10]: The attacker installed malware on PCs before the users received them.
- Attacks on update procedure [11]: The attacker insert malware into the offline upgrade packages before the users copied them onto the air-gapped network.

* Corresponding author.
E-mail addresses: zhou7905@mail.ustc.edu.cn (Z. Zhou), zhangwm@ustc.edu.cn (W. Zhang), shbli@ustc.edu.cn (S. Li), ynh@ustc.edu.cn (N. Yu).

https://doi.org/10.1016/j.comnet.2018.11.014
1389-1286/

- Portable media-based attacks [12]: The attacker infected the OS of an air-gapped PC by copying a virus or worm to portable media storage devices.

Once the malware has been activated on an air-gapped PC, the next step is to build an air-gapped covert channel through which to leak sensitive data.

Several methods to bridge air gaps were proposed in the past decade. Four main kinds of covert channels were built: *electromagnetic* covert channels, *acoustic* covert channels, *thermal* covert channels and *optical* covert channels. Generally, electromagnetic covert channels are imperceptible to humans. However, they can be detected with electronic reconnaissance equipment. And they even are the key points of traditional security safeguards. Acoustic covert channels are novel security threats to an air-gapped network, especially the covert channels via ultrasonic wave. However the capacity of such covert channels is too limited due to the carrier frequency with normal acoustic devices in PC. And as mentioned in Section 4.1 in [13], high power ultrasonic wave is also a threat to human safety. Thermal covert channels have good covertness, but they are still unstable to transmit data on a distance of several centimeters. Compared with above-mentioned covert channels, optical covert channels have both high covertness and rates. The source and sink devices become more against the background of IoT. Therefore, optical covert channels are the most commonly utilized methods.

An optical covert channel can leak data via IR signals that is invisible to humans. In 2016, Lopes and Aranha [14] presented a malicious flash disk to leak data via IR signals with a transmit rate of 15 bits/s.

However, two factors must be considered by attackers when building an air-gapped covert channel.

First, like all other air-gapped covert channels, the IR optical covert channels mentioned above are restricted by their effective distances. Hence, a *malicious insider* is needed to help fulfill data exfiltration. A malicious insider uses a signal receiver to capture sensitive data at a feasible distance.

For example, Lopes' prototype [14] requires a malicious insider to hold a receiver to obtain the IR signals. Nevertheless, this requirement is difficult to achieve in locations with high secrecy levels. Therefore, the conditions allowing a malicious insider are not satisfied at all times.

Second, the method to add the extra function for the aim system to leak data must be considered. In Lopes' prototype [14], an IR transmitter is hidden in the shell of a USB (Universal Serial Bus) flash disk. Clearly, this scenario is only feasible in locations where a USB flash disk is permitted.

By contrast, IoT devices that support IR remote control functions are at greater risk. No malicious insider is needed since the devices can access the Internet directly. In other words, the pervasive IoT devices can serve as malicious insiders under certain conditions. Meanwhile, the hardware configuration of the computers in an air-gapped network can be customized maliciously to send IR remote control commands to control these IoT devices by a supply chain attack [10] or malicious maintenance. Therefore, the introduction of IoT devices supporting IR remote control has dramatically changed the way to breach air-gapped networks.

In our prototype, a novel malicious IR hardware module (MIRM) implanted previously into a keyboard is designed and developed, via which an IR optical covert channel can be established to leak data. The keyboard with an MIRM is shown in Fig. 1. Exploiting the weak points of IR remote control, the MIRM studies the IR surroundings of the air-gapped network and finds the IoT devices supporting IR remote control. Once an available type of appliance is found, the MIRM would modulated the sensitive data into IR remote control commands, and send them at an appropriate time.

Fig. 1. HP keyboard embedded with malicious hardware.

Because the IR signals are usually used for their original purpose, it is very difficult to distinguish between the real signals created by a remote controller by a human and the fake signals modulated from an IR light-emitting diode (LED) by the MIRM, which decreases the probability of detection.

Generally, we found that the precondition that both sides of the channel must be compromised to build a covert channel is not necessary any more against the background of IoT. Once an attacker knows the hardware configuration of the IoT device, he/she can exploit it to leak data by involving supply chain attacks etc. In other words, the attacker makes a nearby smart device peripheral equipment of an air-gapped computer.

The contributions of our research are as follows:

- A potential risk that IoT devices supporting IR remote control can be exploited to leak sensitive data from an air-gapped network with malicious IR hardware module is revealed.
- A set of malicious IR hardware module is designed and developed to verify the existence of such threats.

The rest of the paper is organized as follows. Related works are described in Section 2. The technological background is given in Section 3. Our prototype is proposed in Section 4. Experimental results and evaluations are described in Section 5. Section 6 presents a discussion on our prototype. Countermeasures are given in Section 7, and conclusions are drawn in Section 8.

2. Related work

Among wireless communication technologies for IoT, Bluetooth and WiFi are used to remotely control the smart home appliances. WiFi is a high energy consumption way. Hence, a WiFi controller is usually a virtual one in smart phone app. Therefore, Bluetooth is another common technology for remote control besides IR. The security mechanism to identify a user is Secure Simple Pairing (SSP) introduced into Bluetooth v2.1. Plenty of research on security of SSP has conducted since 2007.

In 2007, Chang and Shmatikov [15] analyzed the numeric comparison association model in SSP by using the ProVerif cryptographic protocol verifier. In 2009, Suomalainen et al. [16] presented a taxonomy of protocols for creating security associations in personal networks and made use of this taxonomy in surveying and comparing association models proposed in several emerging standards. Also in 2009, Lindell [17] proved that the numeric comparison association model in the Bluetooth standard v2.1 is secure under appropriate assumptions regarding the cryptographic functions used. In 2010, Haataja Toivanen [18] proposed two new Man-In-The-Middle (MitM) attacks on Bluetooth SSP. In 2012, Phan Mingard [19] conducted the detailed analysis of SSP for all its MitM-secure models in Bluetooth standard v4.0. Also in 2012, Barnickel et al. introduced an MitM attack on the Passkey Entry method [20], where an attacker can prevent the pairing process to successfully complete and the user uses the same PIN twice. In 2016, Gajbhiye

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014

et al. [21] presented the simulation and security analysis of Bluetooth Pairing protocol for the numeric comparison association using Elliptic Curve Diffie-Hellmen protocol in the network simulator NS2. In 2018, Sun et al. [22] proposed MitM attacks on SSP in Bluetooth standard v5.0 and gave corresponding countermeasures.

On the other hand, research to attack the air-gapped networks have been conducted for twenty years. IoT devices serve as receivers in more and more attack models.

In 1985, Van Eck introduced a method [23] to eavesdrop electromagnetic radiation from TV set with normal antenna. Smulders studied an eavesdropping attack [24] on electromagnetic radiation from RS-232 cables in 1990. In 1997, Ling et al. [25] researched the electromagnetic leakage and protection for the CRT monitor of a computer. Kuhn and Anderson proposed a method [26] to transmit information covertly using electromagnetic radiation in 1998. And in 2004, Kuhn [27] continued his research with flat-panel displays. Guri et al. introduced AirHopper [28], a type of malware, to leak data between a mobile phone and a nearby computer using an FM radio module in 2014. Guri et al. introduced malware called GSMem [29], which leaks data via electromagnetic radiation generated by the bus of computer memory, in 2015. Guri et al. proposed USBee [5], which can be used to leak data via electromagnetic radiation generated by a USB cable, in 2016. In 2016, Matyunin et al. used the magnetic field sensor in mobile device to build a covert channel [7].

In 2013, Hanspach and Goetz used acoustic devices, i.e., the speakers and microphones of a notebook computer, to build a covert channel [6]. Malley Choo [30] introduced covert communication via inaudible sounds in 2014. Lee et al. [31] used a loudspeaker as an acoustical input device and developed a speaker-to-speaker covert channel in 2015. Guri et al. introduced DiskFiltration [32], a new method to send acoustic signals without speakers, in 2016.

In 2011, Zander et al. [33] studied the capacity of temperature-based covert channels. In 2015, Guri et al. introduced BitWhisper [34] to build a unique bidirectional thermal covert channel via the heat radiated by another adjacent computer. In 2017, Mirsky et al. proposed HVACKer [35] to build a one-way thermal covert channel from an air conditioning system to an air-gapped network. Thermal covert channels in multi-core CPUs have also been studied. Mast built a thermal covert channel in multi-cores [36] with a transmission rate of 12.5 bits/s in 2015. Bartolini studied the capacity of a thermal covert channel in multi-cores [37] in 2016. Selber proposed UnCovert3 [38], a new thermal covert channel in multi-cores with a rate of 20 bits/s, in 2017.

Optical covert channels are the most commonly utilized channel. In addition to IR LEDs, normal LEDs are often used in optical covert channels. Loughry and Umphres studied exfiltration via LED indicators [39] in 2002. And also in 2002, Kuhn [40] researched optical time-domain eavesdropping risks of CRT displays. Sepetnitsky et al. proposed a covert channel prototype [41] for leaking data to the camera in a smart phone via the monitor's power status LED indicator in 2014. Shamir presented a cover channel to breach an air-gapped network [42] with a light-based printer in 2014. Guri et al. presented LED-it-GO [43] to leak data via hard drive LED indicators in 2017. Zhou et al. introduced a prototype [44] for leaking sensitive data to a network surveillance camera via the status LED indicators on a keyboard in 2018.

3. Background

3.1. Infrared transmission

IR radiation was discovered in 1800 by William Herschel. IR radiation is used in industrial, scientific and medical applications, especially in short-range wireless communication. IR is the most common method for the remote control of appliances. More than ten IR transmission protocols exist [45]: ITT, NEC, Nokia NRC, Sharp, Philips RC-5, Philips RC-6, Philips RECS-80, Sony SIRC, etc. The protocols are used to prevent surrounding IR from interfering with remote control signals.

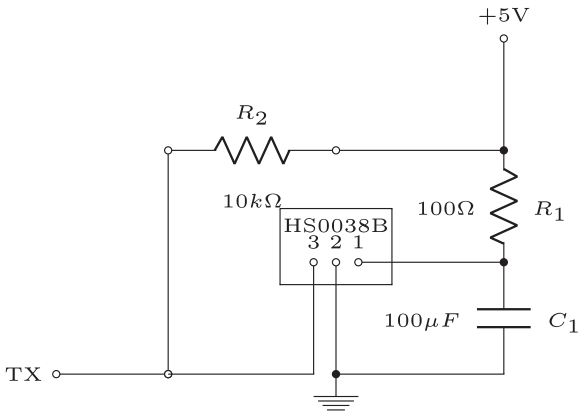

Fig. 2. Circuit used by HS0038B to receive an IR signal.

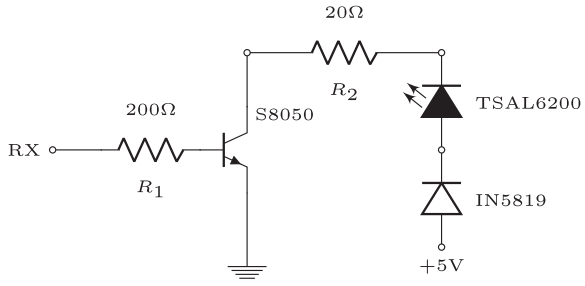

Fig. 3. Amplifier circuit to send an IR signal.

The carrier wave is the key index to distinguish the correct signal to receive. For example, the IR sensor HS0038B made by Vishay Telefunken can receive signals in the carrier frequency range of 35–41 kHz, with peak detection at 38 kHz. Therefore, an HS0038B can receive all transmission protocols at 38 kHz.

The HS0038B circuit is shown in Fig. 2. Resistor R_1 is a current-limiting resistor, and resistor R_2 is a pull-high resistor that is used to maintain a high level on node TX when no IR signal is received by HS0038B. Capacitor C_1 is a filter capacitor that maintains a constant voltage for HS0038B. A low-level signal is output on node TX when any IR signal is received.

Meanwhile, the IR diodes TSAL6200 can be used in an amplifier circuit.

In Fig. 3, the IR LED is TSAL6200. IN5819 is a normal diode that protects triode S8050 from an inverse voltage by mistake. Resistors R_1 and R_2 are both current-limiting resistors. IR diode TSAL6200 sends IR radiation when a high-level signal is received by node RX.

3.2. Raspberry Pi

Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and developing countries [46]. Raspberry Pi serves well as a controller for the IR sensor and transmitter, and it can easily exchange data with an IR sensor, IR transmitter and air-gapped computer via its general-purpose input/output (GPIO) bus.

The Raspberry Pi boots its OS when a power supply is available. Then, it continuously receives signals from the IR sensor via the GPIO bus.

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014

3.3. USB adapter

A USB adapter is a type of protocol converter that is used for converting USB data signals to and from other communications standards. Most commonly, USB data signals are converted to either RS (Recommended Standard)-232, RS-485, RS-422, or TTL (Transistor-transistor logic)-level serial data.

In our prototype, a USB-TTL adapter is used to simulate a serial port on the air-gapped computer. Any device linking the port with correct parameters can receive or send data with TTL-level signals.

4. Attack model

In the attack model, an MIRM is made and implanted into a keyboard with a supply chain attack or a malicious maintenance. Then, the MIRM can be used to attack several IoT devices support IR remote control.

4.1. MIRM

The precondition of attack on those IoT devices supporting IR remote control is to make an MIRM with feasible size and capability. The MIRM is composed of the following:

- A USB-TTL adapter that can simulate a serial port on the air-gapped computer;
- A Raspberry Pi that can
  - Record the IR signals from an IR sensor via GPIO,
  - Study the surrounding IR signals,
  - Make the type and brand of nearby electrical appliances clear,
  - Receive sensitive data from the air-gapped computer via TTL,
  - Modulate sensitive data into IR remote control commands, and
  - Send IR remote control commands to IR LED via GPIO.

The MIRM is linked to the USB port on the computer in a hidden way. In our prototype, the module is embedded in a USB keyboard. Hence, a USB hub is also needed to provide two USB ports for the MIRM and the keyboard.

The malware seeks the sensitive data on the computer and sends them to the MIRM via a USB-TTL adapter. The MIRM studies the IR surroundings of the air-gapped network. The type and brand of the electrical appliances can be judged by checking a signal table. Once a suitable appliance is found, the MIRM modulates the sensitive data into IR remote control commands and sends them to the appliance at the proper time. Then, the IR signals exfiltrate out of the air-gapped network. Because of the variety of electrical appliances, the modulation forms of the signal are different.

The hardware configuration is as follows:

IR transmitter and receiver: An IR LED TSAL6200 is used to replace the normal LED indicator for Scroll Lock, which is seldom used. An HS0038B IR sensor serving as an IR signal sniffer can hide itself behind the translucent plastic panel on a keyboard or anywhere and can receive optical signals easily. The circuits to control sensor and transmitter are redesigned as shown in Fig. 4 to decreases the size into 1.9 cm $\times$ 2.6 cm.

Raspberry Pi: Among all Raspberry Pi versions, Raspberry Pi Zero has the smallest size: 6.5 cm $\times$ 3.0 cm $\times$ 0.5 cm. Hence it can be embedded into a normal-sized keyboard.

Others: A USB hub and a USB-TTL adapter are needed.

Hardware host object: A model KU-1156 HP keyboard, as shown in Fig. 5, is used as the host object to accommodate all the malicious hardware: HS0038B, TSAL6200, their circuit board, Raspberry Pi Zero, a USB-TTL adapter and a USB hub.

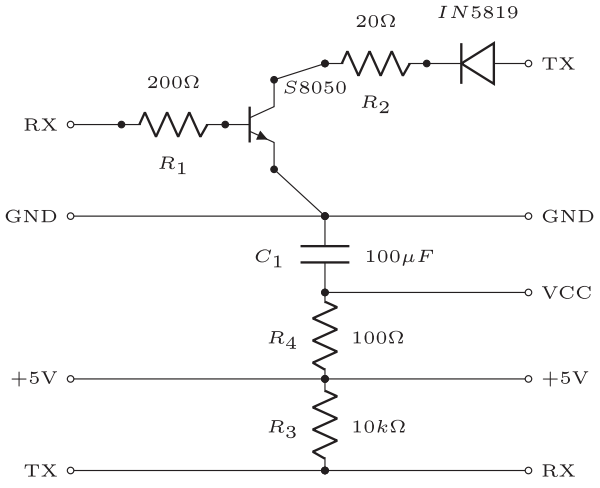

Fig. 4. Circuit for both TSAL6200 and HS0038B.

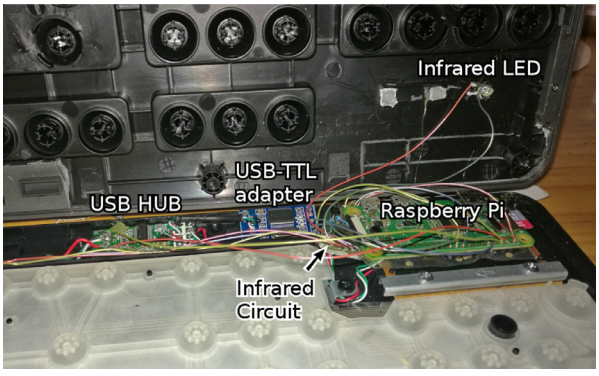

Fig. 5. Inside the keyboard with MIRM.

A website is required to receive the covert data and stores them in an SQLite database. The website is written in Django and can be accessed by the TV box.

To be compatible with more IR transmission protocols, our prototype is designed to record and replay a signal's waveforms directly rather than analyzing its code. The IR signals are detected and are compared with known waveforms to judge their protocols and the brands of the appliances. The results of these assessments are stored in a database that can be queried by the MIRM.

Except studying the IR surroundings, the receiver can also be used to watch for any exceptional situation during the procedure of sending remote control commands. If a received IR signal is different from the sent signal, that means another party has sent an IR command. It is almost certain that the party is a controller held by a person. Therefore, it is not a suitable time to build a covert channel, and the sending procedure is halted immediately.

Finally, a malware is also required to be activated on the air-gapped computer. The malware can fetch sensitive data on the air-gapped network, and send sensitive data to the MIRM via TTL.

4.2. Attack on smart TV box

An attack flow diagram is shown in Fig. 6. Sensitive data, such as credit card numbers, passwords and encryption keys, are sent to the MIRM via TTL-level signals by the malware. The MIRM converts the TTL-level signals into IR remote control commands and send them to a nearby TV box. The TV box is controlled by those commands and forwards the exfiltrating data to a website on the Internet. The exfiltrating data are obtained by accessing the log file of the website. Then, the restored sensitive data can be obtained.

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014

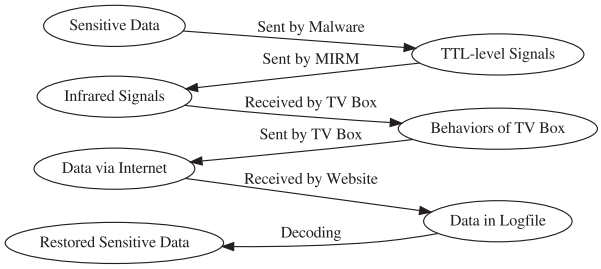

Fig. 6. Attack flow diagram via TV box.

4.2.1. Scenario

In our prototype, a smart TV box serves as the receiver. We assume that there is a TV set with a network smart set-top box in the same room as an air-gapped computer. This scenario is common in system control rooms and command centers. A row of computers are placed in the center of the room. Their screens, keyboards and mice are placed on a desk, and their main boxes are settled under the desk. Several panel TV sets are hung on the wall in front of the operators. Some of the panels are used to display the key status information of the systems they control. One of the panels is used to broadcast news about the situation from public media in real time [47].

Because Android is the most popular mobile OS, an increasing number of TV sets and TV boxes ship Android to enrich the functionality and provide a better experience to users. As a required function, the network browser can access websites on the Internet. Naturally, the browser can be control by an IR remote controller.

Therefore, if the appliance is a smart TV set, the signal can be modulated into a serious of IR remote control commands to visit a malicious website with a long URL that involves the sensitive data.

4.2.2. Hardware configuration

TV Box: A 2nd generation Skyworth Network Set-Top Box Q+, which is one of the most popular TV set-top boxes in China, is used.

4.2.3. Conversion from text to remote control commands

When text data are sent from the air-gapped computer to the TV box via the MIRM, a conversion algorithm is needed to convert the words, which are composed of numbers and letters, into a series of remote control commands.

The users of a TV box cannot input text directly using a remote controller. The buttons on the controller of the Skyworth TV box are shown in Fig. 7. A user can input words using a few buttons, such as “up”, “down”, “left”, “right” and “ok”. An input method editor (IME) app, such as Baidu TV IME, is set to active to provide help to the user.

Meanwhile, as shown in Fig. 8, Baidu TV IME has four keyboards in English mode: *lowercase letters, uppercase letters, numbers* and *symbols*. Therefore, four data tables record the locations of every byte. Then, a path from a byte to another can be calculated by considering the difference in their locations. The initial locations of the former three keyboards are always “q”, “Q” and “1”. A conversion algorithm is proposed, and its brief pseudo codes are listed in Algorithm 1.

4.3. Attack on other smart devices

Similar attack experiments are conducted on some other IoT devices. In all these experiments, the sensitive data are encoded into a serial of device statuses. Then these statuses are received by accessing the control panel of a smart home app.

Fig. 7. Controller of a TV box.

Fig. 8. Keyboards in baidu TV IME.

4.3.1. Smart air-conditioner

Smart air-conditioners have become the mainstream of air-conditioners market. A consumer can turn on his living room air-conditioner via the Internet before coming home. The temperature and running mode can be accessed and controlled with an app on his mobile phone. A smart air-conditioner can also be controlled by an IR remote controller. Therefore, the sensitive data can be modulated into a serial of configuration statuses that can be easily read by an attacker who accesses a control panel of the air-conditioner via an app.

In our experiments, the model of the smart air-conditioner is TCL KFRd-25GW/JD13. The remote controller and the control panel on app are shown in Fig. 9 .

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014

As a result, we found that the minimum time interval between two commands is about 2 s. The status of temperature, fan speed and work mode can be set at the same time since the command code is a status code. There are 320 status codes that can be transmitted. Therefore, the capacity of this cover channel can reach 4.16 bits/s.

4.3.2. Smart electric fan

In our experiments, the model of the smart electric fan is GREE FL-09X62Bha. The remote controller and the control panel on app are shown in Fig. 10.

The minimum time interval between two commands is about 0.5 s. Four buttons: "Swing", "Mode", "+" and "−" can be used to send covert message. Therefore, the capacity of this cover channel is 4 bits/s.

4.3.3. Robot sweeper

The model of the robot sweeper in our experiments is ECVRCS DEEBOT DJ35. The remote controller and the control panel on app are shown in Fig. 11.

The minimum time interval between two commands is about 2 s. Only one button: "Pause" on the remote controller can be used to send covert message. The sensitive data can not be encoded directly. Therefore, the rate of this cover channel is very low.

Algorithm 1 Calculate IR Remote Control Commands of a Path from *src* to *dst*.

```
Input: src, dst are valid keyboard positions.
Output: cmd = Path(src, dst)
  cmd ← Empty
  if src.kbd ≠ dst.kbd then
    (Tmp, src) ←MvKbd(src, dst)
    cmd ← cmd + Tmp
  end if
  return cmd+Mv(src, dst) + " ok"

  function Mv(src, dst)
    cmd ← Empty
    if src.row ≠ dst.row then
      offset ← src.row − dst.row
      if offset > 0 then
        cmd ← cmd+ " up"×offset
      else
        cmd ← cmd+ " down"×|offset|
      end if
    end if
    if src.column ≠ dst.column then

    offset ← src.column − dst.column
    if offset > 0 then
      cmd ← cmd+ " left"×offset
    else
      cmd ← cmd+ " right"×|offset|
    end if
  end if
  return cmd
end function

function MvKbd(src, dst)
  cmd ← Empty
  if dst.kbd = 0 then
    if src.kbd = 1 then
      cmd ← cmd+Mv(src, Pos("cap"))
    end if
    if src.kbd = 2 then
      cmd ← cmd+Mv(src, Pos("Bk2"))
    end if
    if src.kbd = 3 then
      cmd ← cmd+Mv(src, Pos("Bk3"))
    end if
    src ← Pos("q")
  end if
  if dst.kbd = 1 then
```

(*continued*)

Algorithm 1 (*continued*)

```
    if src.kbd = 0 then
      cmd ← cmd+Mv(src, Pos("CAP"))
    end if
    if src.kbd = 2 then
      cmd ← cmd+Mv(src, Pos("Bk2"))
    end if
    if src.kbd = 3 then
      cmd ← cmd+Mv(src, Pos("Bk3"))
    end if
    src ← Pos("Q")
  end if
  if dst.kbd = 2 then
    if src.kbd = 0 then
      cmd ← cmd+Mv(src, Pos("12-0"))
      src ← Pos("1")
    end if
    if src.kbd = 1 then
      cmd ← cmd+Mv(src, Pos("12-1"))
      src ← Pos("1")
    end if
    if src.kbd = 3 then
      cmd ← cmd+Mv(src, Pos("PgUp"))
      src ← Pos("PgDn")
    end if
  end if
  if dst.kbd = 3 then
    if src.kbd = 0 then
      cmd ← cmd+Mv(src, Pos("12-0"))
      src ← Pos("1")
    end if
    if src.kbd = 1 then
      cmd ← cmd+Mv(src, Pos("12-1"))
      src ← Pos("1")
    end if
    cmd ← cmd+Mv(src, Pos("PgDn"))
    src ← Pos("PgUp")
  end if
  return (cmd, src)
end function
```

Fig. 9. Controller and control panel of air-conditioner.

5. Experimental results and evaluations

5.1. Existence of covert channel

To verify the existence of such a covert channel, in one of our experiments attacking on TV box, the string "Keyboard-

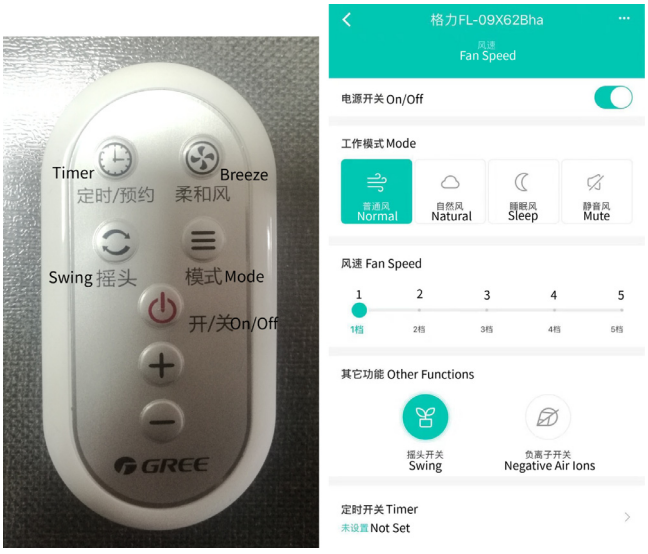

Fig. 10. Controller and control panel of electric fan.

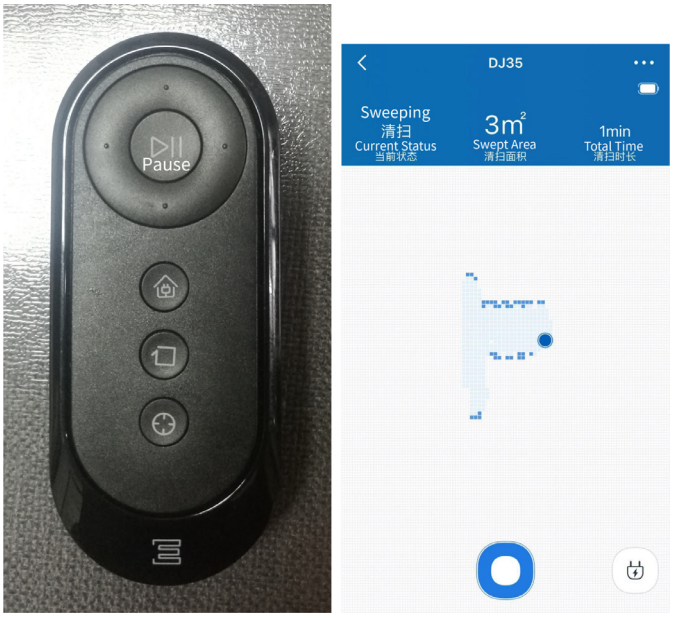

Fig. 11. Controller and control panel of robot sweeper.

isOKon20180104Thankyou USTC" with the length of 34 bytes was sent. First, a series of commands was sent to change the input source of the TV set and order the TV box to open the browser app. A total of 9 s was required to fulfill this procedure. Then, we waited 10 s for the start of the app. Second, commands were sent to input a prefix in the URL textbox. The prefix was used to indicate the protocol and the site address. A total of 173 commands were sent in this procedure in 39 s. Third, the payload of 34 bytes was sent, which required 68 s. Finally, commands were sent in 4 s to close the browser app, return the interface back to the home setting, and change the input source of the TV set. The total transmission time was 130 s.

As a result, the website was accessed by the TV box, and the access time and covert data were found in our database:

```
15|2018-01-04 07:02:17.652151|KeyboardisOKon20180104ThankYouUSTC
```

It is slow to transmit 34 bytes in 130 s. Therefore, a quantitative analysis on the maximum rate of such channels will be given in the next Subsection by measuring the maximum emitting rate of IR remote control commands encoded with NEC standard, and by studying the feature of IME on the TV box.

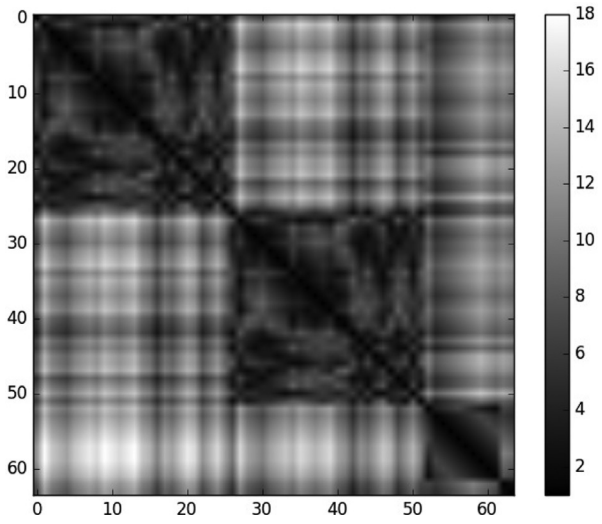

Fig. 12. Command numbers for moving from one byte to another.

5.2. Throughput

As shown in Fig. 12, the command numbers for moving from one byte to another byte according to the conversion algorithm were calculated. The axis values from 0 to 63 stand for bytes "A"～"Z", "a"～"z", "0"～"9", "–" and "_", which can be used to encode data with a modified Base64 for URL [48]. The numbers vary. The smallest is 1 when the next byte is the same as the current. The largest is 18, when the bytes are located on different keyboards and are far from the button used to change the keyboard, such as moving from "5", "6", "7" to "B", "J", "N".

The procedure to input a text can be considered to be a Markov process with 64 states. The transition probability matrix can be calculated based on the statistics of the input texts. Then, the average moving numbers can be obtained by a given matrix. Finally, the rate of the covert channel can be determined.

According to Information Theory, the rate can be defined by the following equation.

$$R = \frac{nH(X)}{t} = -\frac{n}{t}\sum_{x_i \in X} P(x_i)\log P(x_i) \tag{1}$$

where R is the rate, $H(X)$ is the information entropy of source X, x_i is a codeword of X, $P(x_i)$ is the probability of emergence of x_i , n and t indicate that there are n codewords of X transmitted in the channel in t s.

When all 64 bytes are used with the same probability $P(x_i) = (1/64)$, such as when the data are encoded with Base64, the average moving number is 8.442871. One byte has $-\log_2(1/64) = 6$ bits of information in Base64. Additionally, we measured that it costs 0.225433526 s to send a remote control command successfully, so the rate is $6/(8.442871 \times 0.225433526) = 3.152409248$ bits/s.

5.3. Bit error rate

The bit error rate (BER) cannot be measured directly since the minimum transmission unit is not a bit but a command. Therefore, we can measure the command error rate (CER) of the covert channel. The CER is the statistical probability of a transmission error.

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014

To transmit a byte, a group of commands is sent to form a group of independent issues. Therefore, the byte error rate (BYER) can be calculated with the following equation.

$$\mathrm{BYER} = 1 - (1 - \mathrm{CER})^n \tag{2}$$

where n is the average command number of a letter.

Then, the BER can be calculated from the BYER via the following equation.

$$\mathrm{BER} = 1 - \sqrt[m]{1 - \mathrm{BYER}} \tag{3}$$

where m is the information bits number of a byte.

The CERs were measured with a TSAL6200 and a 2nd generation Skyworth Network Set-Top Box Q+ at a series of distances. The measurements show that the statistical probability is nearly zero within a distance of 10 m, which is close to the upper bound indoor distance in an office room. When the transmitter is not in sight of the receiver, the IR signals are transmitted via reflections. Office environments contain an abundance of smooth reflective surfaces, such as walls and glass, which improve the transmission quality of IR signals. Therefore, the BER can be considered to be zero in our scenario.

6. Discussion

In this section, we still take TV box for example to discuss the necessary conditions of existence, error handling and rate improvement methods to increase the availability of this type of covert channel.

6.1. Necessary conditions of existence

The necessary conditions of the existence of such covert channels are:

- There is at least one IoT device that supporting IR remote control function.
- There is at least one remote controller that is frequently used to send IR signals that can be studied by the MIRM.
- There is adequate space in the keyboard to contain all parts of the MIRM.

6.2. Error on remote control commands

When a string is input, any error occurring in the transmission of remote control commands is fatal because the position of any subsequent byte depends on the position of the previous one. If there is not a pause to reset the position, an incorrect position will impact all subsequent bytes.

To help users input text, Baidu TV IME introduced the function "ring shift" to make the moving of highlighted byte faster. The function "ring shift up" is not available when some bytes are already typed into the top row of the IME interface. The highlighted area stays on the fist alternative item, regardless of how many 'up's are clicked. Hence, this phenomenon can be exploited to pause the input procedure. An array of commands: "up, up, up, up, ok" can match all positions on the keyboard. Then, the new position is always the initial position ("q" or "Q") on the current keyboard. A pause is used to reset the position to avoid continuous errors.

6.3. Modified encode algorithms

As mentioned in 5.2 of Section 5, the average moving number per bit is $8.442871/6 = 1.407145167$. Therefore, a simple bit encode algorithm must be built to decrease the average.

We note that the highlighted letter is always "q" when the IME app is activated. The bit information can be encoded as shown in Table 1, and the state transition graph is shown in Fig. 13.

Table 1
Encoding with two states.

Bit	State transition
0	"q → q" or "w → w"
1	"q → w" or "w → q"

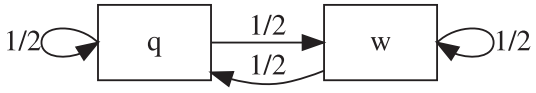

Fig. 13. State transition graph with two states.

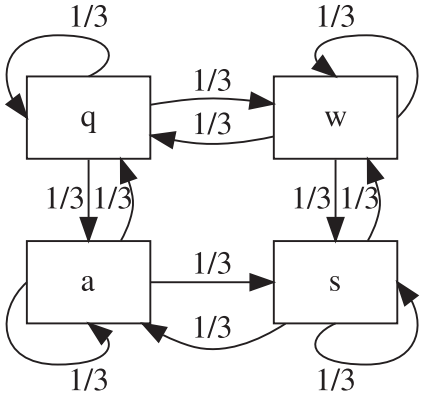

Fig. 14. State transition graph with four states.

With this encode algorithm, the average moving number per bit is $(1/2) \times 1 + (1/2) \times 2 = 1.5$. The number is close to, but not better than, the value of the original algorithm. Nevertheless, the error probability of one letter is decreased considerably for a smaller average moving number per bit.

The new encode algorithm is given in Table 2, and the state transition graph is shown in Fig. 14.

With the new encode algorithm, the average moving number per bit is $[(1/8) \times 2 + (4/8) \times 3 + (3/8) \times 4)]/3 = 1.083333333$, and the rate can reach $1/(1.083333333 \times 0.225433526) = 4.094674556$ bits/s.

The disadvantage of the two modified algorithms is that the URL may be too long.

7. Countermeasures

All countermeasures are divided into two parts: countermeasures for IR remote control and countermeasures against covert channels.

There are two methods in countermeasures for IR remote control. The first method is to avoid to use IR remote control. Because no authentication or identification in any IR remote control protocols, this is a radical way to eliminate risk. However, it would cost a lot to replace all remote controllers with Bluetooth-enabled ones. Furthermore, an IR controller is more power efficient than a Bluetooth controller; The second method is to give a prompt tone for every received command. There are prompt tones on air-conditioners, electric fans and robot sweepers. While in order not to affect the viewing effect of video program, a TV set-top box has no prompt tone. The prompt tones can cause users' awareness. However, the method can not hold back an over-night attack.

The types of potential countermeasures against covert channels are threefold: design countermeasures, procedural countermeasures and technical countermeasures.

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014

Table 2
Encoding with four states.

Bits	State transitions
000	"q → q, q → q" or "w → w, w → w" or "s → s, s → s" or "a → a, a → a"
001	"q → q, q → w" or "w → w, w → s" or "s → s, s → a" or "a → a, a → q"
010	"q → q, q → a" or "w → w, w → q" or "s → s, s → w" or "a → a, a → s"
011	"q → w, w → w" or "w → s, s → s" or "s → a, a → a" or "a → q, q → q"
100	"q → w, w → q" or "w → s, s → w" or "s → a, a → s" or "a → q, q → a"
101	"q → w, w → s" or "w → s, s → a" or "s → a, a → q" or "a → q, q → w"
110	"q → a, a → a" or "w → q, q → q" or "s → w, w → w" or "a → s, s → s"
111	"q → a, a → q" or "w → q, q → w" or "s → w, w → s" or "a → s, s → a"

Table 3
Cost and effect of countermeasures.

Countermeasure	Type	Cost	Effect	Shortcomings
Avoid to use IR remote control	Design	High	Good	High cost
Give prompt tones for IR commands	Design	Low	Normal	Can not stop over-night attacks
Banning web browser apps from a TV Box	Design	Low	Good	Bad image to consumers
Set a network security enforcement	Design	High	Good	High cost
Banning Internet from a smart air-conditioner	Proc.	Low	Good	Inconvenience to user
Covering the unused LEDs	Proc.	Low	Poor	Inconvenience to user
IR signal monitoring with hardware	Tech.	High	Normal	Difficult to find
Redundant device detection	Tech.	Low	Normal	Difficult to find
Power detection	Tech.	High	Good	Requires professional tools

Design countermeasures can increase the difficulty of exploitation of the appliances receiving IR commands. Web browser apps are banned in some TV set-top boxes, such as Tmall MagicBox, a popular TV box brand in China. Nevertheless, the market occupancy of Tmall MagicBox has been decreasing since the manufacturer banned all the third-party apps from their boxes. Another choice is to set a stronger security enforcement [49] for all IoT devices to restrict their network activities. However, it would cost a lot when the number of IoT devices is small.

Procedural countermeasures include banning the Internet access from a smart air-conditioner and covering unused LEDs, which are easy to apply methods; however, they can inconvenience users.

Technical countermeasures include IR signal monitoring with hardware, redundant device detection and power detection. The aim of the first is to sniff the IR signals by a set of IR receivers. Nevertheless, it is difficult to find the covert channel since the covert channel is not in operation at all times. Additionally, it is difficult to distinguish the behavior of a normal remote controller and that of an MIRM when human behaviors are simulated exactly. The second one technique is used to physically detect the existence of MIRM. The last method performs detection by measuring the power consumption of the hardware.

A summary of all countermeasures is presented in Table 3.

8. Conclusions

In this paper, a malicious IR hardware module (MIRM) was designed and developed to covertly leak sensitive data from an air-gapped network by exploiting the weak point that no authentication or identification in IR remote control protocols. The MIRM can control the IoT device supporting IR remote control such as smart TV set-top boxes, smart air-conditioners, smart electric fans and robot sweepers etc. An attack model was introduced to build a covert channel with a smart TV set-top box controlled by IR remote control signals sent by an MIRM embedded in the keyboard. The potential risk that IoT devices can be exploited maliciously to leak information was revealed. A conversion algorithm to convert from a text string to a set of remote control commands was designed to send text data to the TV box through the covert channel. The result of experimentation showed that the rate can reach 3.15 bits/s. the necessary conditions of existence, error handling and rate improvement methods to increase the availability of such covert channels were discussed. Finally, countermeasures for IR remote control and countermeasures against covert channels were presented.

Data availability

All data are provided within the paper and its supporting information.

Web resources

Demo Video: https://youtu.be/2eQdivwDk9o
Research Site: https://home.ustc.edu.cn/~zhou7905/IREXF

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under grants U1636201 and 61572452.

We thank Prof. David Barrera honestly for his warmhearted guide on the writing of the paper.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.comnet.2018.11.014.

References

[1] A. Nordrum, Popular Internet of Things Forecast of 50 Billion Devices by 2020 is Outdated, 2016. (https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated). [Online; accessed 30-September-2017].
[2] L. Columbus, Internet of Things Market to Reach $267b by 2020, 2017. (https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#39038c66609b). [Online; accessed 30-September-2017].
[3] B.W. Lampson, A note on the confinement problem, Commun. ACM 16 (10) (1973) 613–615, doi:10.1145/362375.362389.
[4] S. Zander, G. Armitage, P. Branch, A survey of covert channels and countermeasures in computer network protocols, IEEE Commun. Surv. Tut. 9 (3) (2007) 44–57, doi:10.1109/COMST.2007.4317620.
[5] M. Guri, M. Monitz, Y. Elovici, Usbee: air-gap covert-channel via electromagnetic emission from usb, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2016, pp. 264–268.

[6] M. Hanspach, M. Goetz, On covert acoustical mesh networks in air, J. Commun. 8 (11) (2013) 758–767, doi:10.12720/jcm.8.11.758-767.
[7] N. Matyunin, J. Szefer, S. Biedermann, S. Katzenbeisser, Covert channels using mobile device's magnetic field sensors, in: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016, pp. 525–532, doi:10.1109/ASPDAC.2016.7428065.
[8] D. Kushner, The Real Story of Stuxnet, 2013. (https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet). [Online; accessed 9-Apirl-2018].
[9] F-Secure, Worm:w32/agent.btz Description, 2008. (https://www.f-secure.com/v-descs/worm_w32_agent_btz.shtml). [Online; accessed 14-October-2018].
[10] L. Urciuoli, T. Männistö, J. Hintsa, T. Khan, Supply chain cyber security–potential threats, Inf. Secur. 29 (1) (2013).
[11] C. Kasmi, J.L. Esteves, P. Valembois, Air-gap limitations and bypass techniques:command and control using smart electromagnetic interferences, in: Bot Conf., 2015.
[12] P. Walters, The Risks of Using Portable Devices, 2012. Carnegie Mellon University. Produced for US-CERT, a government organization. Retrieved from http://www.us-cert.gov.
[13] M.A. Hanson, Health Effects of Exposure to Ultrasound and Infrasound: Report of the Independent Advisory Group on Non-Ionising Radiation, Health Protection Agency, 2010.
[14] A.C. Lopes, D.F. Aranha, Platform-agnostic low-intrusion optical data exfiltration., in: International Conference on Information Systems Security & Privacy(ICISSP), 2017, pp. 474–480.
[15] R. Chang, V. Shmatikov, Formal analysis of authentication in bluetooth device pairing, in: FCS-ARSPA07, 2007, pp. 45–61.
[16] J. Suomalainen, J. Valkonen, N. Asokan, Security associations in personal networks: a comparative analysis, in: F. Stajano, C. Meadows, S. Capkun, T. Moore (Eds.), Security and Privacy in Ad-Hoc and Sensor Networks, Springer, Berlin, Heidelberg, 2007, pp. 43–57.
[17] A.Y. Lindell, Comparison-based key exchange and the security of the numeric comparison mode in bluetooth v2.1, in: M. Fischlin (Ed.), Topics in Cryptology – CT-RSA 2009, Springer, Berlin, Heidelberg, 2009, pp. 66–83.
[18] K. Haataja, P. Toivanen, Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures, IEEE Trans. Wireless Commun. 9 (1) (2010) 384–392, doi:10.1109/TWC.2010.01.090935.
[19] R.C.-W. Phan, P. Mingard, Analyzing the secure simple pairing in bluetooth v4.0, Wireless Pers. Commun. 64 (4) (2012) 719–737, doi:10.1007/s11277-010-0215-1.
[20] J. Barnickel, J. Wang, U. Meyer, Implementing an attack on bluetooth 2.1+ secure simple pairing in passkey entry mode, in: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 17–24, doi:10.1109/TrustCom.2012.182.
[21] S. Gajbhiye, M. Sharma, S. Karmkar, S. Sharma, Design, implementation and security analysis of bluetooth pairing protocol in ns2, in: 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 1711–1717, doi:10.1109/ICACCI.2016.7732294.
[22] D.-Z. Sun, Y. Mu, W. Susilo, Man-in-the-middle attacks on secure simple pairing in bluetooth standard v5.0 and its countermeasure, Pers. Ubiquit. Comput. 22 (1) (2018) 55–67, doi:10.1007/s00779-017-1081-6.
[23] W. Van Eck, Electromagnetic radiation from video display units: an eavesdropping risk? Comput. Secur. 4 (4) (1985) 269–286.
[24] P. Smulders, The threat of information theft by reception of electromagnetic radiation from rs-232 cables, Comput. Secur. 9 (1) (1990) 53–58.
[25] L. Ling, N. Yan, Z. Hongjin, The electromagnetic leakage and protection for computer, in: 1997 Proceedings of International Symposium on Electromagnetic Compatibility, 1997, pp. 378–382, doi:10.1109/ELMAGC.1997.617167.
[26] M.G. Kuhn, R.J. Anderson, Soft tempest: hidden data transmission using electromagnetic emanations, in: International Workshop on Information Hiding, Springer, 1998, pp. 124–142.
[27] M.G. Kuhn, Electromagnetic eavesdropping risks of flat-panel displays, in: International Workshop on Privacy Enhancing Technologies, Springer, 2004, pp. 88–107.
[28] M. Guri, G. Kedma, A. Kachlon, Y. Elovici, Airhopper: bridging the air-gap between isolated networks and mobile phones using radio frequencies, in: 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), IEEE, 2014, pp. 58–67.
[29] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, Y. Elovici, Gsmem: data exfiltration from air-gapped computers over GSM frequencies, in: 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 849–864.
[30] S. OMalley, K.-K. R. Choo, 2014. Bridging the Air Gap: Inaudible Data Exfiltration by Insiders, 20th Americas Conference on Information Systems (AMCIS 2014), Association for Information Systems, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2431593.
[31] E. Lee, H. Kim, J.W. Yoon, Various threat models to circumvent air-gapped systems for preventing network attack, in: International Workshop on Information Security Applications(WISA), Springer, 2015, pp. 187–199.
[32] M. Guri, Y. Solewicz, A. Daidakulov, Y. Elovici, Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('Diskfiltration'), Springer International Publishing, Cham, pp. 98–115. doi:10.1007/978-3-319-66399-9_6.
[33] S. Zander, P. Branch, G. Armitage, Capacity of temperature-based covert channels, IEEE Commun. Lett. 15 (1) (2011) 82–84.
[34] M. Guri, M. Monitz, Y. Mirski, Y. Elovici, Bitwhisper: covert signaling channel between air-gapped computers using thermal manipulations, in: IEEE 28th Computer Security Foundations Symposium (CSF), 2015, IEEE, 2015, pp. 276–289.
[35] Y. Mirsky, M. Guri, Y. Elovici, Hvacker: bridging the air-gap by manipulating the environment temperature, Magdeburger J. zur Sicherheitsforschung 14 (2017) 815–829. Retrieved August 18, 2017
[36] R.J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, S. Capkun, Thermal covert channels on multi-core platforms, in: 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 865–880.
[37] D.B. Bartolini, P. Miedl, L. Thiele, On the capacity of thermal covert channels in multicores, in: Proceedings of the Eleventh European Conference on Computer Systems, ACM, 2016, p. 24.
[38] M. Selber, P.D.L. Thiele, Uncovert3: Covert Channel Attacks on Commercial Multicore Systems, 2017.
[39] J. Loughry, D.A. Umphress, Information leakage from optical emanations, ACM Trans. Inf. Syst. Secur. 5 (3) (2002) 262–289, doi:10.1145/545186.545189.
[40] M.G. Kuhn, Optical time-domain eavesdropping risks of crt displays, in: Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on, IEEE, 2002, pp. 3–18.
[41] V. Sepetnitsky, M. Guri, Y. Elovici, Exfiltration of information from air-gapped machines using monitor's led indicator, in: 2014 IEEE Joint Intelligence and Security Informatics Conference, 2014, pp. 264–267, doi:10.1109/JISIC.2014.51.
[42] A. Shamir, Light-Based Printer Attack Overcomes Air-Gapped Computer Security, 2014. (https://www.scmagazineuk.com/light-based-printer-attack-overcomes-air-gapped-computer-security/article/541140/). UK, SG SC Magazine, [Online; accessed 18-September-2017].
[43] M. Guri, B. Zadov, Y. Elovici, LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED, Springer International Publishing, Cham, pp. 161–184. doi:10.1007/978-3-319-60876-1_8.
[44] Z. Zhou, W. Zhang, Z. Yang, N. Yu, Optical exfiltration of data via keyboard led status indicators to ip cameras, IEEE Internet Things J. (2018) 1, doi:10.1109/JIOT.2018.2842116.
[45] S. Bergmans, Sb-Projects - Ir Index, 2017. (https://www.sbprojects.net/knowledge/ir/index.php). [Online; accessed 10-July-2018].
[46] Raspberry Pi, 2012. (https://www.raspberrypi.org/). [Online; accessed 26-December-2017].
[47] Wikipedia, Network Operations Center - Wikipedia, 2018. (https://en.wikipedia.org/wiki/Network_operations_center). [Online; accessed 2-October-2018].
[48] S. Josefsson, The Base16, Base32, and Base64 Data Encodings, RFC Editor, 2003.
[49] D. Barrera, I. Molloy, H. Huang, Standardizing IoT Network Security Policy Enforcement, in: Workshop on Decentralized IoT Security and Standards (DISS), 2018, 2018, p. 6, doi:10.14722/diss.2018.23007.

Zheng Zhou received his B.S. degree and M.S. degree in 2001 and 2007 respectively from Information Engineering University, Zhengzhou, China. He is now pursuing the Ph.D. degree in University of Science and Technology of China. His research interests include steganography, covert channels and cyberspace security.

Weiming Zhang received his M.S. degree and Ph.D. degree in 2002 and 2005 respectively from Information Engineering University, Zhengzhou, China. Currently, he is a professor with University of Science and Technology of China. His research interests include multimedia security, information hiding, and privacy protection.

Shangbin Li received his B.S. and Ph.D. degrees in physics from Zhejiang University, Hangzhou, China, in 1996 and 2003, respectively. He was a postdoctoral researcher in optical engineering in Zhejiang University from 2003 to 2005, and then the senior optoelectronics engineer/R&D manager/R&D director in a few high-tech companies including Amertron Technology. Since 2013, he has been on the faculty of University of Science and Technology of China (USTC). His research interest lies in the LED-LED visible light communication, blue-LD based white light sources for joint lighting and optical wireless communications, quantum communication and quantum information processing.

Nenghai Yu received his B.S. degree in 1987 from Nanjing University of Posts and Telecommunications, M.E. degree in 1992 from Tsinghua University and Ph.D. degree in 2004 from University of Science and Technology of China, where he is currently a professor. His research interests include multimedia security, multimedia information retrieval, video processing, information hiding and security, privacy and reliability in cloud computing.

Please cite this article as: Z. Zhou, W. Zhang and S. Li et al., Potential risk of IoT device supporting IR remote control, Computer Networks, https://doi.org/10.1016/j.comnet.2018.11.014