IoT Device (Wi-Fi) Security Study

March 2020

hkpc 生產力局

HKCERT

Disclaimer

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Productivity Council (HKPC) reserve the right to amend the document from time to time without prior notice.

While we have made every attempt to ensure that the information contained in this document is obtained from reliable sources, HKCERT is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is intended to provide general information and for reference only. Reliance or use of this information shall be at the reader's own risk. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will HKCERT, HKPC or its partners, employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this document, or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Licence

Table of Contents

1. Background

The applications of the Internet of Things (IoT) are becoming more diverse with the rapid development of wireless technology. Each type of IoT devices need to adopt the appropriate wireless technology to suit its application requirements, with Wi-Fi being the most popular wireless networking due to its blazing fast transmission rate and easy deployment. Home and business areas are some common scenarios for Wi-Fi applications where users can easily connect a Wi-Fi network with a personal computer or mobile phone to access the Internet.

The most noticeable advantage of Wi-Fi is that it can meet the networking requirements of nearly all IoT devices. Many are Wi-Fi enabled, for example, Wi-Fi routers, network cameras and smart home appliances which are very common in our everyday lives. Yet their cyber security risk should not be neglected. Any IoT devices connecting to the Internet through Wi-Fi may encounter security threats from the Internet. At the same time, various kinds of security vulnerabilities are found in the authentication and encryption methods for Wi-Fi technology. Consequently, Wi-Fi security has attracted much attention from general users, IT operators and product developers.

For IoT devices, there are relatively few security protection programs. Also, users often ignore update patches of IoT devices that can substantially increase the security level of their devices, leaving them more vulnerable to cyber attacks. Attackers may use improper device configuration or vulnerabilities to launch attacks, triggering sensitive information disclosure and remote code execution.

Through security testing and research on Wi-Fi configuration and Wi-Fi enabled IoT devices, HKCERT hopes that the test results serve not only to clarify relevant security issues but also to help raise security awareness of general users and developers of IoT devices.

2. Wi-Fi Security Study

Wi-Fi is widely used in the realm of smart home. For instance, webcams and smart home appliances can be connected to the Internet through Wi-Fi in smart home settings, allowing users to use mobile phone applications or computer applications to monitor the devices (Fig. 2.1). An attacker can compromise the user's Wi-Fi network by cracking the passwords, etc., and then may launch attacks by using improper configuration or vulnerabilities of the device to trigger sensitive information disclosure or remote code execution.

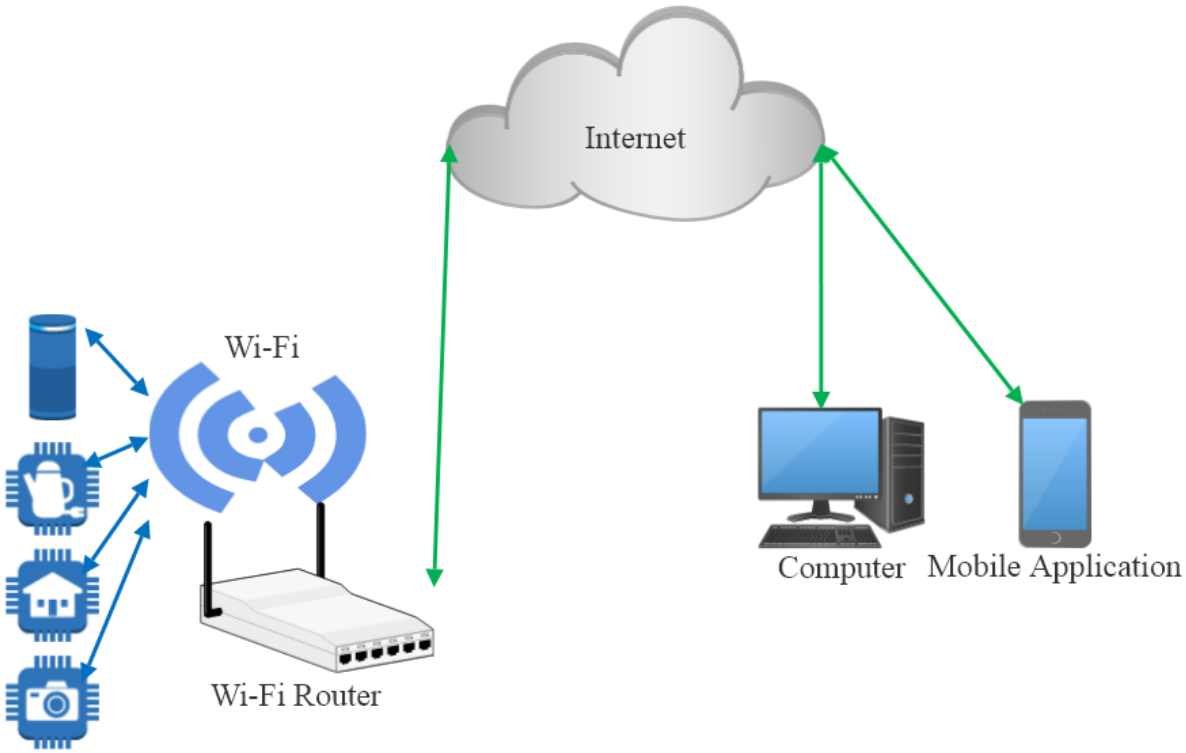

Fig. 2.1 Wi-Fi IoT devices use case

To ensure the security of Wi-Fi IoT environment and devices, the following two aspects need to be well-executed.

1. Correctly configure the Wi-Fi IoT environment to prevent networks from being hacked, while isolating the network of IoT devices from that used by computers and mobile phones; and
2. Ensure the security of Wi-Fi-connected IoT devices and patch device vulnerabilities in a timely manner

This article delineates security research on two aspects of configuring the Wi-Fi IoT environment and Wi-Fi IoT devices, followed by security advices for general users and developers about Wi-Fi IoT configuration and devices.

3. Security Study of Configuring Wi-Fi IoT Environment

In the context of Wi-Fi technology, security indicates two aspects:

1. Controlling who can connect to and configure the Wi-Fi network and equipment; and
2. Securing the data travelling wirelessly across Wi-Fi network from unauthorised view.

To achieve the above two aspects, authentication is required before IoT device can connect to the wireless network and the data transmitted wirelessly is encrypted. This article will introduce and analyse various authentication and encryption protocols, together with security recommendations for configuring Wi-Fi environment.

3.1 Security Analysis of Wi-Fi Authentication and Encryption Protocol

There are five types of Wi-Fi authentication and encryption methods, namely:

- Open Wi-Fi Networks;
- Wired Equivalent Privacy (WEP);
- Wi-Fi Protected Access (WPA);
- Wi-Fi Protected Access 2 (WPA2); and
- Wi-Fi Protected Access 3 (WPA3).

Among the above methods, WPA and WPA2 have two encryption methods: TKIP and AES. TKIP is mostly used with WPA. On the other hand, given that WPA2 requires the use of AES encryption algorithm, AES will have to be used with WPA2. The following table shows the security level and recommended level of various authentication and encryption methods.

Authentication and Encryption Method	**Security Level**	**Recommended Level**
Open Wi-Fi Networks	Insecure, without authentication and encryption, there is a possibility of data leakage and being attacked.	Not recommended.
WEP	Insecure, WEP passwords can be cracked in minutes by automated cracking tools.	Not recommended.
WPA/WPA2-TKIP	Insecure, TKIP allows an attacker to decrypt packets on the network and inject arbitrary data into the wireless network.	Not recommended.
WPA/WPA2-AES	Risky, this method carries the risk of brute force cracking of passwords. In addition, there are KRACK vulnerabilities and KrØØk vulnerabilities. The encrypted transmission of devices using affected Wi-Fi chips may be unauthorisedly decrypted, which may cause data leakage.	It is recommended before WPA3 becomes popular. Need to update patches in time to patch vulnerabilities.
WPA3	Secure. WPA3 fixes the vulnerabilities on WPA2. It can no longer be cracked by brute force, and it will not be affected by KRACK and KrØØk vulnerabilities.	It is recommended, but WPA3 is not yet universal.

Fig. 3.1.1 The security level and recommended level of Wi-Fi authentication and encryption methods

As stated in Fig. 3.1.1, while WPA3 is the most secure and recommended Wi-Fi authentication and encryption method, it is still in the early phase. Although Wi-Fi devices that support WPA3 are already on the market, and Windows 10, iOS 13 and Android 10 have added support for WPA3, most IoT devices do not support WPA3. Hence it is still recommended to use WPA2 + AES mode for the configuration of the Wi-Fi IoT environment currently.

WPA2 + AES carries the risk of brute force cracking of passwords, as well as vulnerabilities that may cause data leakage. HKCERT will perform security analysis on WPA2 + AES and provide security recommendations.

For IoT devices, there are relatively few security protection programs, with users often ignoring patches to update the software of the devices, making them more vulnerable to attacks. Attackers may invade vulnerable IoT devices, which in turn attacks computers and mobile phones in the same network. To avoid this situation, we recommend separating the network of IoT devices from that of the computers and mobile phones network when configuring the Wi-Fi IoT environment.

3.2 Security Analysis of WPA2+AES

Since WPA2 + AES passwords are vulnerable to brute force cracking, weak passwords may be successfully brute force cracked in a short period of time. WPA2 + AES password requires a minimum of 8 digits, but there is no complexity requirement. It is also common to use 8 digits as a password, such as using a phone number as a password. HKCERT used the test platform to brute force an 8-digit weak password which was successfully cracked within one minute (Fig 3.2.1). As such, using 8-digit weak password is not secure.

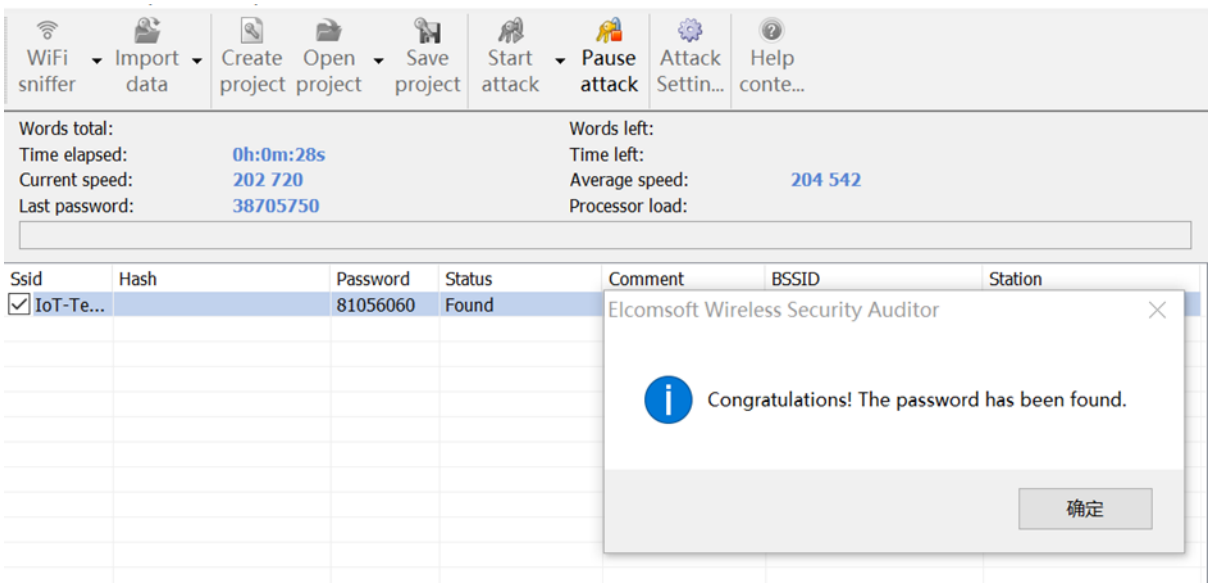

Fig. 3.2.1 Brute force WPA2+AES password

Wi-Fi Protected Setup (WPS) function is designed to solve the rather complicated steps of WPA / WPA2 authentication, but its PIN code can be cracked in one day because of its limited strength. Once the PIN code has been cracked, even if the user changes the Wi-Fi password, the attacker can still connect to Wi-Fi through the WPS PIN code. Device users are recommended to disable the WPS function or use the WPS push button connection function. The WPS push button connection function allows users

to press the button to turn on WPS when needed. Then when the connection is successful or the connection time limit is over, WPS will automatically turn off to prevent it from being brute forced.

In addition to the password brute force, there are two vulnerabilities named KRACK and KrØØk in WPA2+AES. Encrypted transmission of devices using vulnerable Wi-Fi chips are vulnerable to unauthorised access and decryption, which causes data leakage. Users need to update patches released by device vendors from time to time to fix the vulnerabilities.

3.2 Recommendations for Configuring Wi-Fi IoT Environment

The following are the security recommendations for the Wi-Fi IoT environment configuration for users:

- WPA3 authentication encryption method is recommended. However, before WPA3 is widely adopted, device users can still employ the WPA2 + AES authentication encryption method by using a large number of bits and more complex passwords, such as "dfgP94$Zwdngf!" with upper and lower cases characters, numerals and special characters;
- The function can only be connected by turning off the WPS function or using the WPS button;
- Pay attention to the vulnerability situation of Wi-Fi and update the patch to fix the vulnerability in time; and
- Separate the network of IoT devices from that used by computers and mobile phones.

4. Security Analysis of IoT Device (Wi-Fi)

Besides the security of the Wi-Fi IoT environment, the security of the Wi-Fi IoT device itself is another important factor affecting the degree of security when users are using Wi-Fi IoT devices. Even if an attacker compromises a user's Wi-Fi IoT network, the attack will not be able to launch further attacks as long as the devices in the network have no vulnerabilities. We use a Wi-Fi router, a smart diffuser (smart home), a control centre for home security monitoring system and a webcam to simulate a home Wi-Fi IoT environment (Fig 4.1.1). We cracked the Wi-Fi password by the method mentioned in the last section. Then we performed a security test on the IoT devices in the network to find vulnerabilities in the IoT devices. The following figure is a schematic diagram of our test.

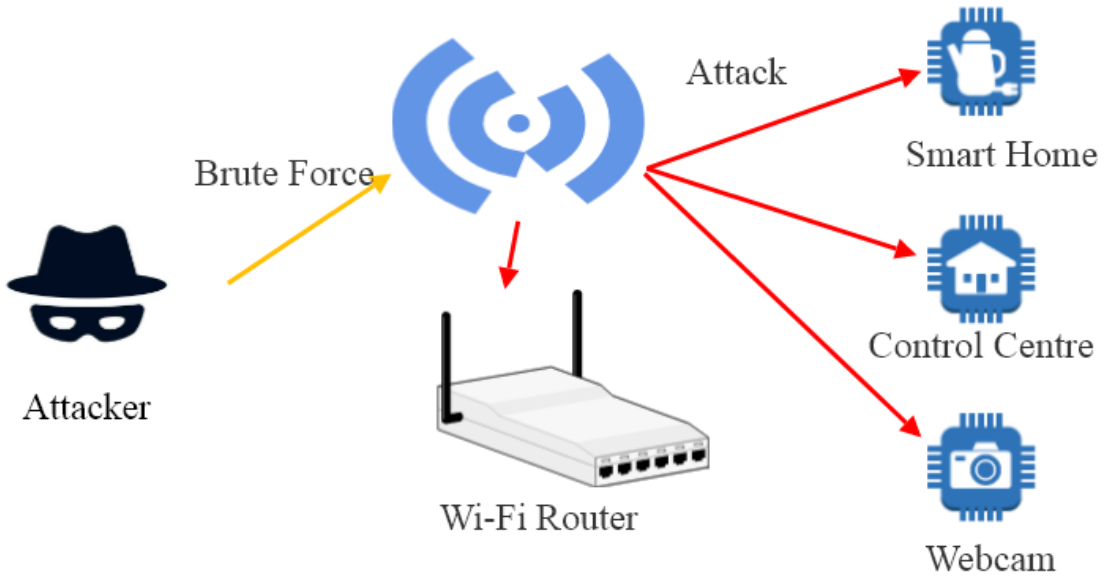

Fig. 4.1.1 IoT devices test schematic diagram

Through testing, we found three security vulnerabilities in Wi-Fi IoT devices:

- Device port weak management vulnerability
- Transmission without encryption vulnerability
- Device authentication weak management vulnerability

Below is our analysis of these three vulnerabilities.

4.1 Device Port Weak Management Vulnerability

IoT devices provide connection services through communication ports. We scanned the ports of the following IoT devices (Fig. 4.1.2) to identify which ports are open. The following table shows the open ports of tested devices.

Device	Open Port
Wi-Fi router	21, 22, 23, 53, 80, 2000, 8291
Smart diffuser	6668
Control centre	23, 53, 80
Webcam	80, 554, 2020, 8080, 8081, 8088

Fig. 4.1.2 IoT devices open ports

As seen from the table, except the smart diffuser, the other three devices have opened too many unnecessary ports by default and these open ports also have weak management vulnerabilities, allowing attackers to hack the device by attacking ports. Among them, we found a vulnerability in the Telnet service running on the control port 23 opened by the control centre. It allows direct login administrator account without a password. That is, if an attacker compromises the device, the attacker can execute malicious code remotely to turn it into a botnet. (Please Refer to Section 6.1 for test details)

4.2 Transmission without Encryption Vulnerability

The newly discovered KrØØk vulnerability will cause WPA2-AES encrypted data to be illegally decrypted, resulting in leakage of transmitted data. However, this vulnerability will only cause WPA2+AES encryption in Wi-Fi network failure and cannot decrypt data encrypted by the IoT device application. Therefore, encryption of IoT device transmission is very important, especially for devices transmitting sensitive information, such as webcams.

When we tested the webcam, we found that the transmission was not encrypted, and sensitive information, such as the device username and password, can be found in the transmitted data in plain text. An attacker can use the eavesdropped username and password to log in to the webcams for monitoring and operation. (Please refer to Section 6.2 for test details). We recommend using the HTTPS protocol in the device management interface instead of the unencrypted HTTP protocol.

4.3 Device Authentication Weak Management Vulnerability

Many IoT devices, such as Wi-Fi routers, network cameras, etc., have a management interface that uses an account password to log in. Users can log in to the management interface to manage the device, if an attacker breaks the device's account password and hacks into the device's management interface. It can trigger remote code execution and data leakage attacks. Therefore, IoT devices must have authentication protection measures, such as mandatory use of complex passwords, prevention of brute force attacks and two factor authentication, etc.

In the test, we found that the Wi-Fi routers and webcams had weak authentication management vulnerabilities. Some ports of these two devices do not have protection measures against brute force password cracking. We can obtain the device password through brute force cracking. Also, as there is no two-factor authentication protection in the devices, we can log in to the device's management interface through the cracked account password to monitor and operate. We used the Wi-Fi router as an example to demonstrate the brute force cracking process. (Please refer to Section 6.3 for details.)

4.4 Security Test Result and Risk Summary of Wi-Fi IoT Devices

Device	Port Weak Management Vulnerability	Transmission without Encryption Vulnerability	Authentication Weak Management Vulnerability	Security Risk
Wi-Fi router	Yes	No	Yes	There is a risk of being monitored and operated by the attacker, and the attacker can turn the device into a botnet.
Smart diffuser	No	No	Not applicable	If the user's device cloud account is stolen, the device can be controlled by an attacker.

Control centre	Yes	No	Not applicable	There is a risk of being completely controlled by attackers, causing the device to lose monitoring capabilities and become a botnet.
Webcam	Yes	Yes	Yes	There is a risk of leaking sensitive personal information.

Fig. 4.4.1 Security test result and risk summary of Wi-Fi IoT devices

4.5 Recommendations for Configuring and Designing Wi-Fi IoT Devices

End Users

- Change the default password when using the device for the first time;
- Close unnecessary ports when using the device for the first time;
- Password of device should be long and complex enough;
- Enable two factor authentication protection if this option is available;
- Check the device settings regularly. If settings are changed unexpectedly, reset the account of device immediately and keep on monitoring;
- Update firmware of device to the latest version; and
- Beware of security alerts of IoT devices.

Product Developer

- Apply Security by design to tighten security measures in product development life cycle;
- Enforce unnecessary network communication ports not open by default and perform identity authentication and permission management on open ports;
- Ensure the encryption of both data and password in transmission;
- Enforce change of default password for user using the webcam for the first time;
- Apply password complexity, e.g. at least 8 characters long and must include upper and lower cases characters, digits and special characters;
- Prevent brute force attack, e.g. lockup the account when password failed for 10 times;
- Equip two factor authentication protection on the device;
- Provide transparency on security vulnerabilities and continue to provide security patches for devices to patch critical vulnerabilities as soon as possible; and
- Use the self-assessment checklist of the HKCERT “IoT Security Best Practice Guidelines” to assess the product.

5. Summary

- Before WPA3 authentication and encryption method is widely applied, it is recommended to use WPA2 + AES. Please also note the Wi-Fi network needs to be properly configured and timely updated to patch vulnerabilities.
- Use WPA3 once it becomes popular.
- Separate the network of IoT devices from that used by computers and mobile phones.
- Developers should patch Wi-Fi vulnerabilities as soon as possible and release security patches.
- Developers can do more improvements, such as evaluating the product by referring to the HKCERT “IoT Security Best Practice Guidelines”.

6. Appendix – Security Test

6.1 Device Port Weak Management Vulnerability Security Test

We scanned the open ports of the control centre of a home security monitoring device through the test platform.

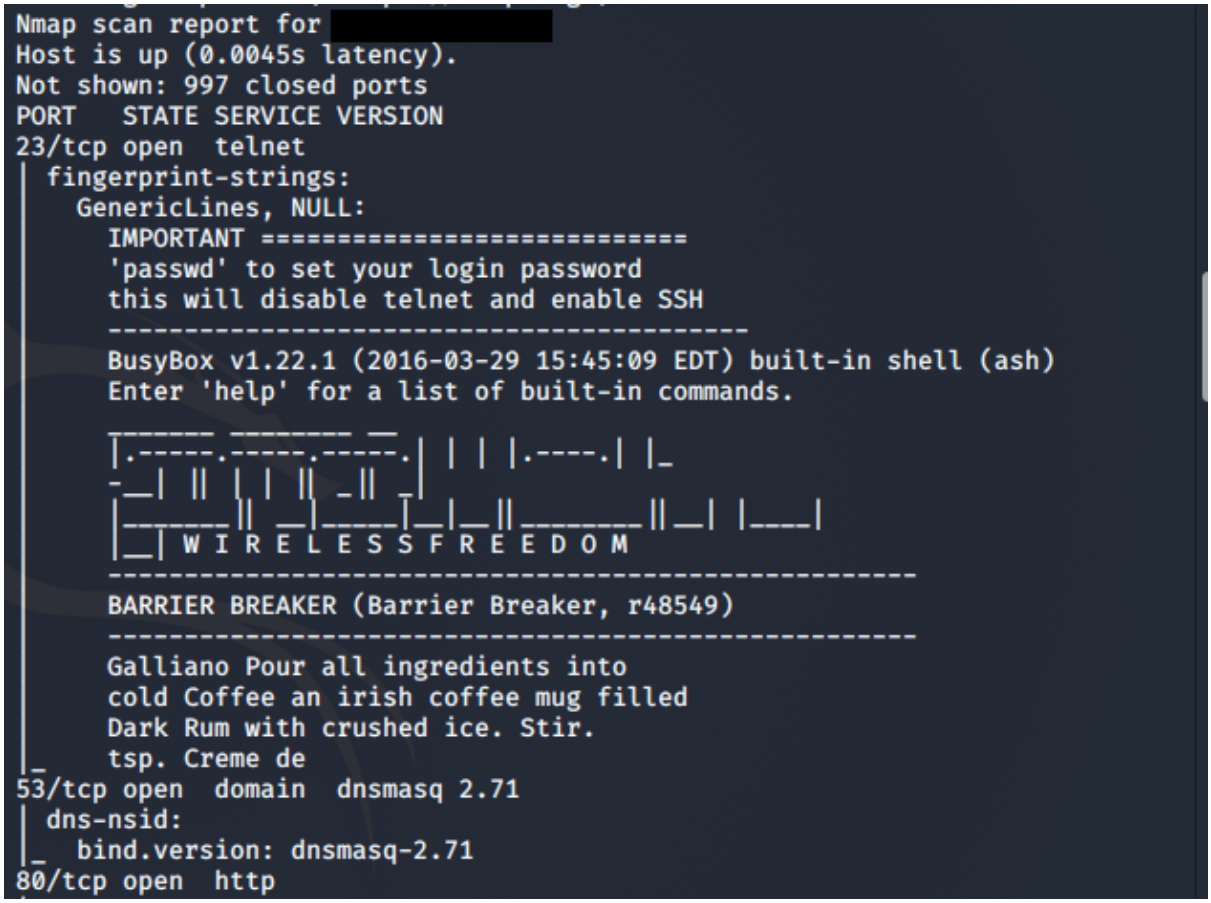

Fig. 6.1.1 Control centre open ports

As you can see, ports 23/53/80 are open. Port 23 is used for Telnet service. The data transmitted by traditional Telnet sessions is not encrypted, and sensitive information, such as account numbers and passwords, can be easily sniffed. We chose port 23 for testing.

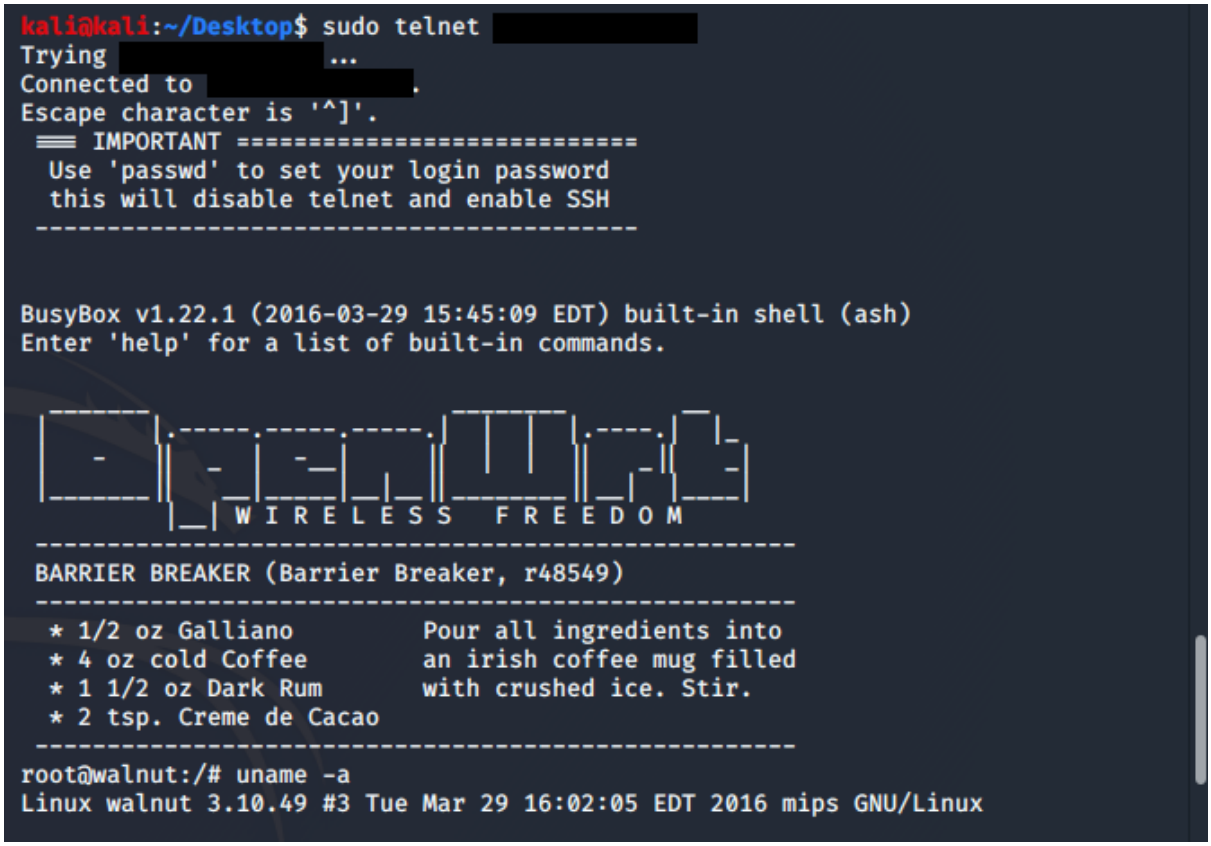

Fig. 6.1.2 Test against port 23

We used the telnet command to connect to the control centre. The default device password is empty. We can log in to the device without entering a password. It is a root account with the administrator privileges. The attacker can read, write data and execute code on the device. This vulnerability can be exploited by hackers easily. For instance, malware Mirai can be transmitted through port 23. Once the device is exposed to the Internet, it can be easily attacked, resulting in malware infection.

6.2 Transmission without Encryption Vulnerability Security Test

We used the mobile application to log in to the webcam, and sniffed the communication data between the mobile phone and the webcam through the test platform. Then it was found in the data that the webcam did not encrypt sensitive information such as device account password.

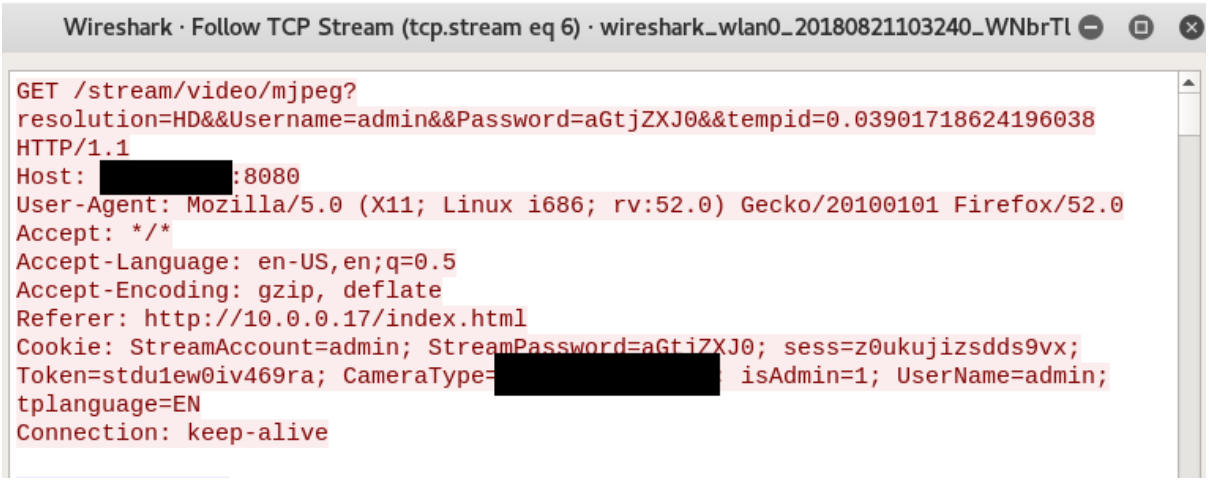

Fig 6.2.1 Plaintext transmission of webcam

The account and password of the webcam are transmitted in plain text. The password of the webcam is encoded with Base64, but base64 cannot provide any protection because it can be decoded by a decoding tool.

Fig 6.2.2 Retrieve password by decoding Base64

After decryption, we got the password of the webcam to log in to the management interface of the device for monitoring and operation.

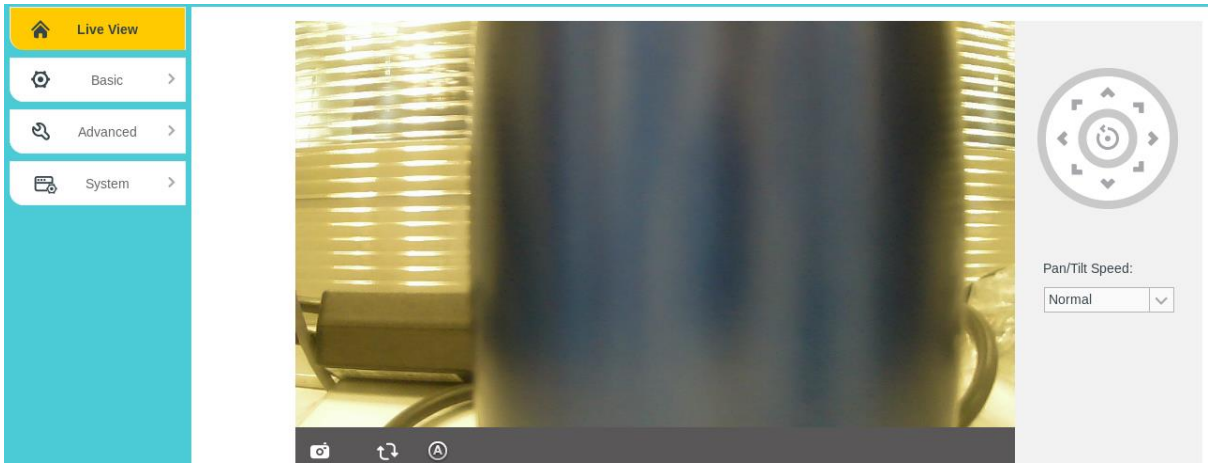

Fig 6.2.3 Log in to the management interface of the webcam for monitoring and operation

6.3 Device Authentication Weak Management Security Test

We scanned the open ports of the Wi-Fi router through the test platform.

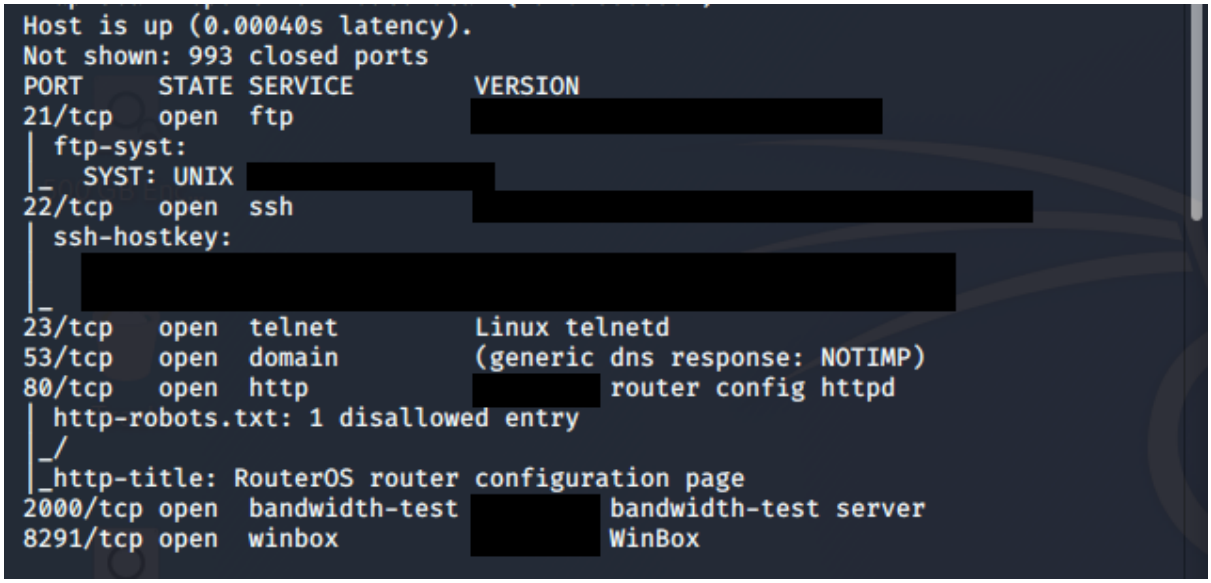

Fig 6.3.1 Wi-Fi router open ports

We searched and found that there is a brute-force vulnerability in port 8291 of this version of the firmware, which can be brute-forced by using a dictionary prepared in advance.

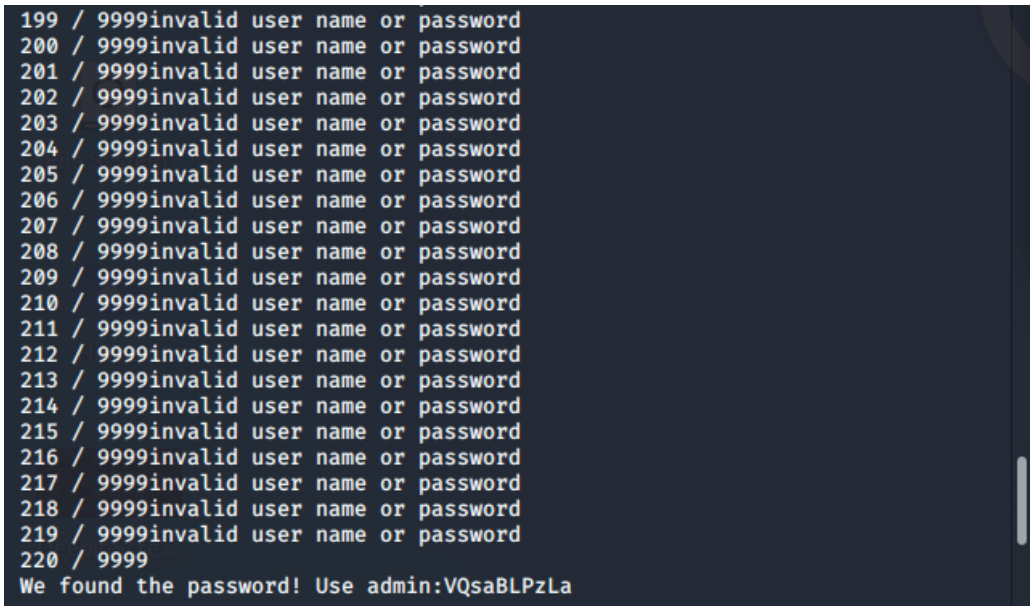

Fig 6.3.2 Brute force against port 8291

After cracking the password, we can use the cracked password to log in to the management interface of the Wi-Fi router for monitoring and operation.

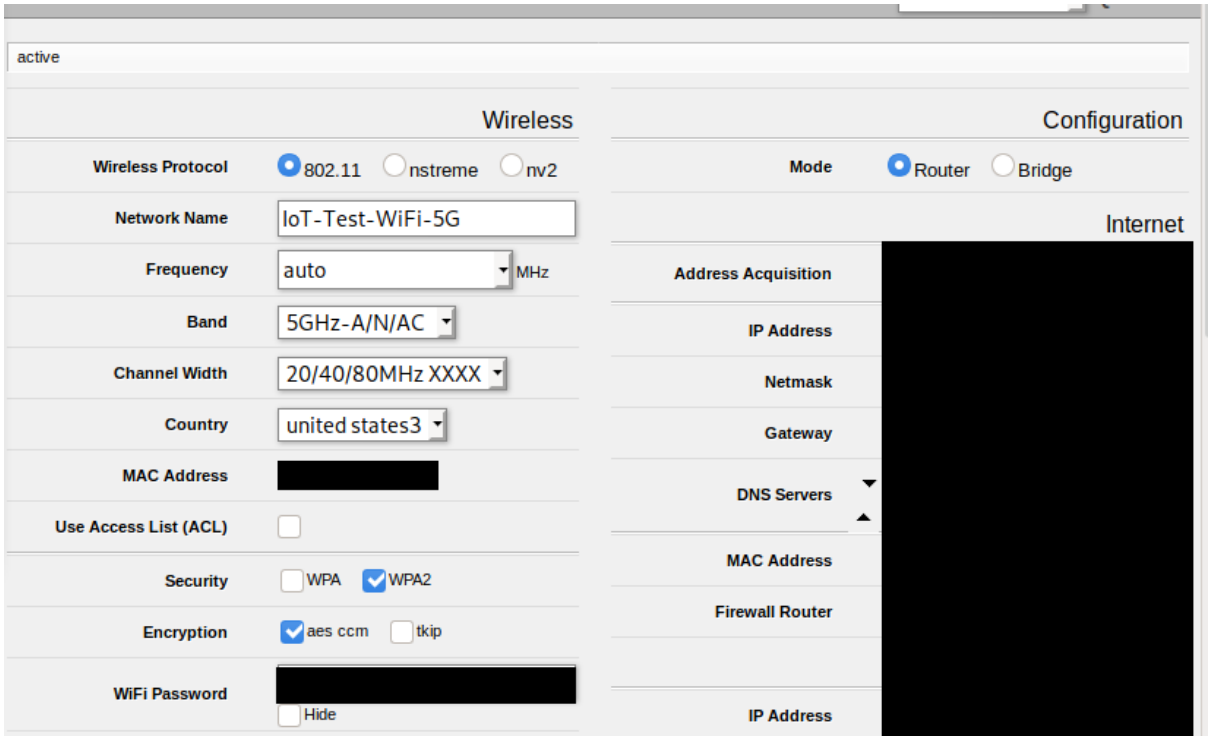

Fig 6.3.3 Log in to the management interface of the Wi-Fi router for monitoring and operation