Exposed by Default: A Security Analysis of Home Router Default Settings

Junjian Ye
Nanjing University of Posts and Telecommunications
Nanjing, China
jjy470742953@gmail.com

Xavier de Carné de Carnavalet
The Hong Kong Polytechnic University
Hong Kong SAR, China
xdecarne@polyu.edu.hk

Lianying Zhao
Carleton University
Ottawa, Canada
lianying.zhao@carleton.ca

Mengyuan Zhang
Vrije Universiteit Amsterdam
Amsterdam, Netherlands
m.zhang@vu.nl

Lifa Wu
Nanjing University of Posts and Telecommunications
Nanjing, China
wulifa@njupt.edu.cn

Wei Zhang
Nanjing University of Posts and Telecommunications
Nanjing, China
zhangw@njupt.edu.cn

ABSTRACT

With ubiquitous Internet connectivity, home routers have become a cornerstone of our digital lives, often deployed with minimal changes to the factory default settings. However, if left unexamined, these settings can pose risks to user security and privacy. To systematically evaluate potential risks, we developed a threat model-based framework and conducted a comprehensive analysis of 40 commercial off-the-shelf home routers, representative of recent models across 14 brands. We surveyed 81 parameters and behaviors including default and *deep* default settings. We identified a variety of security flaws including the exposure of IPv6 local devices due to a lack of firewall protection, vulnerable Wi-Fi security protocols, open Wi-Fi networks and trivial admin passwords for "plug-and-play" routers, and unencrypted firmware update communications. We also discovered concealed WPS PIN support — at times associated with a trivial PIN. In total, we are reporting 30 exploitable vulnerabilities to the vendors. This paper highlights the need for heightened scrutiny of default router settings, providing valuable insights to both manufacturers and consumers for enhancing home network security. Our findings underscore the importance of meticulous device configuration, advocating for proactive measures from all stakeholders to mitigate the threats posed by insecure router default settings.

CCS CONCEPTS

• **Security and privacy → Network security**; *Embedded systems security*.

KEYWORDS

Home router, Default settings, Manual analysis

ASIA CCS '24, July 1–5, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0482-6/24/07…$15.00
https://doi.org/10.1145/3634737.3637671

ACM Reference Format:
Junjian Ye, Xavier de Carné de Carnavalet, Lianying Zhao, Mengyuan Zhang, Lifa Wu, and Wei Zhang. 2024. Exposed by Default: A Security Analysis of Home Router Default Settings. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), July 1–5, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3634737.3637671

1 INTRODUCTION

By the end of April 2023, the number of Internet users worldwide has reached 5.18 billion, accounting for 64.6% of the global population [53]. By 2019, most households in developed regions already had access to the Internet [62]. Traditionally, Internet access at home is provided by a modem together with a router to support a range of devices, from laptops to IoT devices, through wired or wireless communication. Home routers come with different characteristics and features and offer numerous customizable settings, e.g., Wi-Fi passphrase and protocol, admin password, remote control options, firewall, external storage support.

Numerous attacks target home routers, including botnet malware infections [3, 23, 39] and attacks on wireless protocol implementations [66, 69]. A body of research also aims at automating the discovery of vulnerabilities in routers from firmware images to uncover authentication issues [58], privilege escalation [15], command injection [33], and information disclosure [74]. However, a less studied issue stems from the quality of the settings being applied to the routers. For instance, home routers used to support the deprecated WEP (Wired Equivalent Privacy) protocol years after a powerful attack offering to recover the shared key was published [6, 20].

Nthala et al. [50] found many UK home users assume network devices are already secure when purchased, and can simply be plugged to work. This behavior is comparable and similar to interaction blindness [51] or banner blindness. A study by Ho et al. [24] has shown that users tend to keep default settings provided by the router's configuration wizard. Even for trained personnel (e.g. system administrators [40]), default settings are also important because they are either directly adopted or depict an important orientation. We consider the resulting configuration as the *initial default settings*. In turn, this configuration may not provide adequate security, e.g., leaving weak/well-known credentials unchanged. This will very likely be what the users end up with when using the router until

a future event brings attention to the router again. Therefore, any insecurity left in such initial default settings will possibly affect a large population. For instance, users may assume a secure connection when they are required to enter a "security key" before connecting but if the router's Wi-Fi security protocol defaults to a weak/vulnerable one (despite supporting stronger up-to-date protocols), the attacker can still eavesdrop on or intercept network traffic containing user sensitive data. This could be even worse than unprotected connection as the user is unaware and may take decisions based on wrong assumptions (e.g., otherwise sensitive transactions could have been avoided).

Concerns also arise from initially disabled features that, when activated by a single click, impose a multitude of additional default settings, which we term *deep default settings*. Similarly, as these settings become functional immediately upon activation, users are less likely to modify them. If overlooked, such settings could obscure a comprehensive security analysis of home router default settings. As an example, a typical feature which is usually disabled by default is guest network (to give temporary network access to a visitor). This disabled feature might not catch the attention of a security analysis but once enabled by the user (e.g., a friend drops by), guest network may default to improper settings and issues from the initial defaults would suddenly apply.

In this paper, we seek the answers to two questions: "*Will the default settings of home routers pose any security risks?*" (initial defaults) and "*Will the default settings of initially-deactivated features of home routers pose any security risks once activated?*" ("deep" defaults). Note that certain features may or may not be enabled by default, and thus we determine whether a feature is considered "deep" based on common practice (i.e., by most models). We clarify whether a feature is enabled by default if relevant in our results.

To answer these two questions, emulation-based large-scale analysis would appear to be a good choice because functional emulation of the firmware image is a promising direction to conduct security analyses (albeit with numerous challenges [17]). However, we found that it is inherently limited in its ability to yield *faithful* results. We show how the state-of-the-art emulators could not meet our requirements to retrieve the actual default settings in Section 3.1. Consequently, automating the analysis of merely available router firmware images is not a reliable method to survey their default settings. Moreover, a few popular brands obfuscate their firmware images in an attempt to thwart such analysis [56], not to mention a non-negligible number of router models do not even have available firmware images to be downloaded.

With emulation confirmed to be infeasible for our purpose, we purchased 40 home routers available at flagship stores on popular shopping platforms that still receive firmware updates in the past four years (2018–2022) to represent as many recent routers as possible. Based on our defined threat model of home routers (Section 2.1), we designed a comprehensive router default settings security analysis framework to analyze the selected home routers. By systematically testing the routers, we found insecure default settings and behaviors related to Wi-Fi security protocols, setup wizard, guest network, WPS, IPv6, TLS, router reset. We also found a hard-coded WPS PIN in a router allegedly not supporting WPS (this case is assigned a CNVD ID), as well as several instances of unprotected firmware update mechanisms (pending vendor acknowledgment).

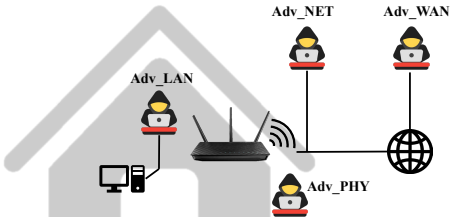

Figure 1: Threat model

Our main contributions are as follows:

- We introduce an 81-criteria security evaluation framework for default settings in home routers, with a focus on deep settings, while factoring in four types of adversaries.
- We demonstrate that firmware emulation has significant limitations as a solution to default setting analysis, and choose to conduct a comprehensive analysis with 40 real-world home routers using our proposed evaluation framework.
- We are the first to draw attention to what we call deep default settings in a security context, which take effect only when the corresponding feature is enabled and often neglected in regular security analysis, and we target such deep defaults in the conducted analysis.
- We uncover numerous security issues and shed light on weak default security protocols, incorrect implementation of TLS, improper configuration guidance for users, unencrypted firmware updates, IPv6 without NAT and default firewall, and concealed WPS support. We are currently reporting 30 exploitable vulnerabilities to the vendors (9 have been assigned CNVD/CVE IDs).

2 ANALYSIS SCOPE

This section defines the scope of our home router defaults analysis, which is twofold: the types of attacker capabilities (considered threats), and the individual router default settings which may lead to security implications if not properly set (considered features).

2.1 Threat Model

When a router is powered on and connected to the Internet, it may face potential threats from various adversaries. To better study the security implications of various default settings in home routers, we divide the adversaries into the following four types:

- Adv_WAN: Adversaries on the Internet. As the WAN interface of routers is exposed on the Internet, adversaries can discover open services (notably through specialized search engines e.g., Shodan [57], Zoomeye [77]) and try to exploit them.
- Adv_LAN: Adversaries in the LAN. Compromised user devices (e.g., by malware), or simply curious guests that are already connected to the router's local network have access to certain of the router's features. Also, adversaries who have managed to get connected to Wi-Fi (LAN) are included.
- Adv_PHY: Adversaries physically close to the router. The Wi-Fi signal coverage of the router is usually sufficient for adversaries to mount attacks to exploit wireless protocols from outside the user's home. For instance, adversaries in close proximity can attempt to break the security protocol to connect to Wi-Fi [63].

Table 1: Categories of settings considered and related threats

Categories of settings considered	Adv_LAN	Adv_PHY	Adv_NET	Adv_WAN	Common issues/vulnerabilities
Initial Defaults					
Wi-Fi and admin pass-phrase/word	✓	✓			Weak hard-coded default passphrases, lack of proper guidance for setting strong passphrases
Wi-Fi security protocol		✓			Support for outdated protocols (e.g. WEP, WPA, WPA2-TKIP)
WPS		✓			Hard-coded WPS PINs, absence of attempt rate-limiting
Local web access	✓				Absence of TLS and login attempt rate-limiting/CAPTCHAs
Firmware update mechanisms	✓		✓	✓	Absence or incorrect implementation of TLS or integrity verification
Exposed services	✓			✓	Concealed sensitive services (e.g. Telnet, FTP, UPnP, HTTP)
Deep Defaults					
Guest network		✓			The same issues as Wi-Fi, absence of isolation from main network
Remote web access			✓	✓	The same issues as local web access, self-signed TLS certificates
Telnet/SSH	✓			✓	Weak hard-coded default passphrases
IPv6				✓	Lack of IPv6 NAT or firewall
Cloud account			✓		Absence or incorrect implementation of TLS, lack of proper guidance for setting strong passphrases
App	✓		✓		Absence or incorrect implementation of TLS
UPnP	✓			✓	Vulnerable port mapping function
External storage	✓		✓	✓	Weak hard-coded default passphrases, absence or incorrect implementation of FTP over TLS
Reset	special case				Incomplete reset

- Adv_NET: Adversaries on the network path. Adversaries such as the ISP can passively eavesdrop on the outgoing traffic and mount man-in-the-middle attacks to tamper with traffic. Such adversaries are in line with the Dolev-Yao model [13], where they are capable of accessing arbitrary messages sent on the network, only limited by cryptographic capabilities, e.g., can't break encryption with a high-entropy key.

Curious router manufacturers/vendors may also threaten users' security and privacy e.g., by implementing backdoors; we do not consider them in our threat model.

2.2 Risk-Prone Features Under Consideration

Home routers, as the bridge between the home network and the internet, come with a range of features. While these features enhance user experience, they also introduce potential security vulnerabilities. Below, we provide a list of features of home routers with a track record of security issues. We categorize them based on our threat model in Table 1. This serves as the motivation for our analysis.

Wi-Fi and admin passwords/passphrases. Wi-Fi password is the password required for users to connect to the Wi-Fi of the router, while admin password is required to log in to the management page of the router. Passphrases could be preset and printed on the router's label. Lorente et al. [37] found that certain routers generate default Wi-Fi passphrases based on their MAC addresses (e.g. CVE-2012-4366), making them predictable to Adv_PHY. Niemietz et al. [48] found 10 routers with weak default admin passphrases. Adv_LAN may conduct brute-force attacks to crack them and control routers.

Wi-Fi security protocol. Wi-Fi is a Wireless Local Area Network (WLAN) technology based on the IEEE 802.11 standard [29]. Due to the open nature of wireless communications, wireless devices communicate through encryption protocols such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and more recently WPA3 (standardized in 2018). Vulnerabilities and flaws have been discovered in WEP [6, 20], WPA and WPA2 (based on TKIP [59, 65, 66], e.g., CVE-2017-13086), and WPA3 [64, 67] (e.g. CVE-2019-9494 and CVE-2020-24586). Thus, when checking router default settings, only WPA2-CCMP and updated implementations of WPA3 are considered secure choices in this paper.

WPS. Wi-Fi Protected Setup (WPS) is a simplified Wi-Fi connection method. Typically, users can either enter an 8-digit PIN displayed by the router or press a WPS button physically or in a management page (PBC) to connect to Wi-Fi without entering the passphrase. The PIN method brings additional security risks as it lets attackers attempt to connect at any time, and flaws were found in the design of the PIN verification that lower the number of attempts needed to find the correct PIN to a mere 11,000 [25, 27, 69] (e.g. CVE-2016-1206 and CVE-2020-15023). Hard-coded WPS PIN is also a serious issue because it can be exploited by Adv_PHY to connect to the Wi-Fi and access the LAN easily (e.g. CVE-2013-5037). Countermeasures include a significant timeout period between failed attempts.

Local web access. A router's management webpage is normally accessible by anyone on the LAN side including via Wi-Fi, though access restrictions can be configured. Devices on the LAN side could be infected by malware that tries to access the router's configuration. The authentication mechanism should resist malicious login attempts. Besides the weak admin password issue mentioned above, relying on an unencrypted HTTP connection by default can also help Adv_LAN obtain the admin password by ARP spoofing [72] and log in to the management page [22, 27, 48] (e.g. CVE-2020-9420). Similar to WPS, login attempt rate-limiting and CAPTCHAs are also necessary for countering brute-force attacks (e.g. CVE-2021-38474).

Firmware update mechanisms. Routers receive firmware updates that can fix security vulnerabilities and improve security. There are three ways to update router firmware: automatic update, user-initiated update and manual update. Automatic update means that the router will check and automatically update to the latest version at regular intervals. User-initiated update means that users can click on the "check firmware version" or "update firmware" buttons in the management page to trigger the same process. Both of the above methods need to interact with servers on the Internet. If HTTPS is not employed or the TLS certificate is not properly validated, Adv_NET may tamper with the update files through man-in-the-middle (MITM) attacks and downgrade router firmware [5, 70] (e.g. CVE-2020-10925 and CVE-2020-15498). Lack of authentication and integrity verification allows attackers to potentially write malicious firmware into the router (e.g. CVE-2014-2718) [10].

Exposed services. Each exposed service increases the attack surface [38] of home routers. In particular, a service exposed on the WAN interface will be indexed by search engines such as Shodan and might be scrutinized by malicious individuals. It poses a permanent risk to users if the exposed service cannot be disabled through a setting. Adv_LAN and Adv_WAN can discover the open ports on routers' LAN and WAN interfaces, respectively, and exploit vulnerabilities to attack routers [35].

Guest network. A guest network is a separate wireless SSID advertised by the router with limited functionalities and targeted for a user's guests. The network usually provides isolation from other clients of the main network, inter-client isolation, and prevents guests from accessing the management webpage [27]. There are two types of guest networks: open networks without Wi-Fi password that instead leverage a captive portal to ask for the guest password after users connect to it; and secured network protected by the guest Wi-Fi password. The former type may carry various security risks [26] while the latter type is similar to the main Wi-Fi network and relies on the default Wi-Fi security protocols [19].

Remote web access. Remote web access is a feature that allows users to access management pages from the WAN side. It should be disabled by default because it exposes web interfaces to the internet, which can bring security risks [45, 60] (e.g. CVE-2012-2440). The security concerns for remote web access are similar to local web access [27] (e.g. CVE-2013-6918). In addition, when users remotely access management pages with HTTPS, routers act as TLS servers and users may still be vulnerable to MITM attacks if the certificates provided by routers are self-signed [9].

Telnet and SSH. Telnet and SSH are commonly used protocols for remote management. Routers support them for remote debugging; Therefore, they tend to hide the status of Telnet and SSH (the default usernames and passwords of these services) from the users. However, the manufacturers may employ weak hard-coded passwords [35] (e.g. CVE-2016-10177, CVE-2018-10532, and CVE-2022-38452) for such services. The Mirai botnet, which was once used for large-scale DDoS attacks, also infects devices by attempting Telnet and SSH logins with a static set of passwords [39].

IPv6. In IPv4, Network Address Translation (NAT) is a mechanism that is often seen as necessary due to the scarcity of global IPv4 address space. Though not a primary purpose of NAT, it provides a "better-than-nothing" security boundary as well by translating and masking private IP addresses, thereby making it more challenging for outside attackers to initiate connections to internal devices [34]. IPv6 eliminates the need for NAT thanks to globally unique addresses, making internal hosts directly reachable via the internet and poses new security risks. RFC 4864 [34] recommends home routers apply IPv6 stateful packet filtering that "conforms to the user expectations already in place" [73] with IPv4 NAT. One remaining barrier for attackers is to find active hosts within the large IPv6 address space [28, 44], especially due to (partially) random 64-bit suffixes in certain settings [47].

Cloud account. Certain router manufacturers provide cloud account services for users. These accounts can be bound with routers and their companion apps for remote access and management or used for Dynamic DNS (DDNS). Therefore, account password strength requirements should be very strict. Similar to firmware update, routers also need to communicate with servers when users log in to their cloud accounts; a process that could be vulnerable to MITM attacks [2].

App. To facilitate accessing and managing the router, manufacturers develop companion apps for their routers. These apps can be bound to routers or manufacturer accounts and communicate with routers directly by Wi-Fi or through a server from the Internet. Wi-Fi is used near the router and only vulnerable to Adv_LAN (e.g. CVE-2022-23000). If users want to rely on the app to remotely control the router, the manufacturer's server needs to be involved to forward packets to the router. Similar to firmware update, Adv_NET can control the router by hijacking the packets between the router and the server [2, 31] (e.g. CVE-2022-41540).

UPnP. Universal Plug and Play (UPnP) is an architecture for easy and robust connectivity of many sorts of devices in homes, offices, and elsewhere [43]. For routers, UPnP can help peer-to-peer software in the LAN access the Internet more smoothly by automatically configuring port mapping. Esnaashari et al. [16] found that adversaries can exploit UPnP to carry out MITM attacks by adding port mappings.

External storage. External storage is a feature that supports users to access the content in USB devices connected to the router. Generally, there are three different access methods: SMB-based, web-based over HTTP or HTTPS, and FTP-based. SMB is limited to file sharing within the local area network (LAN), while the latter two methods support remote access. For FTP, Kumar et al. [35] discover a number of devices support FTP with weak hard-coded credentials (e.g. CVE-2022-46637) or without authentication (e.g. CVE-2008-1268). Strong credentials are also necessary for SMB-based and web-based access methods. Additionally, similar to remote web access, properly implemented TLS is important for remote web-based and FTP-based access methods to prevent attacks from Adv_WAN and Adv_NET.

Reset. Router refurbishment and second-hand router trading are very common. Usually, users reset routers to dispose of their sensitive data. However, there may be residual data in the router due to improper implementations of the reset function. Hard reset means pressing and holding the physical "RESET" button, while soft reset means clicking the "reset to factory default settings" button in the management page. For a soft reset, routers may offer different reset options to help users dispose of their data selectively, which may result in users unintentionally retaining sensitive information. Additionally, sensitive information may remain on the flash memory after a device reset [21, 36], which allows adversaries to recover the previous owner's data from second-hand devices.

3 ANALYSIS DESIGN

We justify below why firmware emulation is unfit for our task. We then describe our methodology to extract default settings from real routers and measure their behaviors. We not only collect the settings shown in the web management page, but also verify whether critical settings are properly applied. In doing so, we also launch active tests such as port scanning.

3.1 An Attempt with Emulation

An intuitive choice for large-scale firmware analysis would be emulation, with both minimal cost and better flexibility. We show why it is not the case for our purpose. We found that only Firmadyne [7] and FirmAE [33] can automatically run router firmware without hardware information or manual configuration. So, we chose FirmAE as it is an improved version of Firmadyne with a

Table 2: Outcome of 320 emulated images with FirmAE

Emulation outcome			Count
Failed			3
Appears "successful"	**No access to management page**	"Unable to connect"	41
		404 error	37
		"Page not found"	3
		Blank page	33
		"The connection was reset"	6
		Infinite waiting	9
		Jump to the official website	12
		Others*	10
	Disrupted setup wizard	Cannot login or set password	16
		"Cable is unplugged"	56
		"Require admin privilege"	5
		Infinite waiting	8
		"Invalid MAC address"	1
		"Searching PVC"	1
Appears "functional"			79
Total			320

*Examples include 400 error, 500 error, "Time out", "Unsupported browser", "Checking JavaScript support", Blank, "Need upgrade".

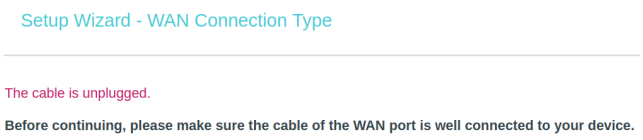

Figure 2: The error page of TP-Link TL-WR940N

79.36% success rate. We tested the firmware images of 320 routers FirmAE claims to support, and tabulated the results in Table 2. We identified two main types of issues that prevent us from relying on emulation altogether.

Non-functional emulation. The definition of "successful" emulation varies with purposes. FirmAE assumes that as long as the host can successfully ping the IP address of router's LAN interface, the emulation is successful (which is why there are only 3 failed cases in Table 2). However, in numerous cases we cannot access the management page or complete the initial setup, let alone extract the default settings. Through our investigation, the main reasons for these failures are the lack of important information from flash or NVRAM storage, incorrect speculation about network interfaces, and the lack of customized Linux kernel hardware drivers. For instance, the setup wizard was interrupted for TP-Link TL-WR940N due to an error: "The cable is unplugged" as shown in Figure 2. This error is due to the Web application relying on `ioctl()` to obtain the connection status, as shown in Listing 1. FirmAE was unable to provide a correct response because its Linux kernel (which is not the original one) did not support the private command code `0x89F7`. We can add this command into the Linux kernel of FirmAE and return 1 to allow the setup wizard to continue; however, this approach does not generalize to other routers.

Default values not in the firmware. Table 2 shows 79 routers out of 320 (24%) appear to be functional during the emulation. However, those "functional" emulated firmware images still suffer from other

```
int wanIsConnected(int a1) {
  // ...
  char v1[16] = "eth0";
  int v2 = socket(2, 1, 0);
  if ( v2 == -1 ) {
    perror("Socket creation faild\n");
    return 0;
  }
  strncpy(v3, v1, 16);
  v4 = ioctl(v2, 0x89F7, v3); // query SIOCGLINKSTATUS
  if ( v4 >= 0 ) {
    // ...
  }
  else {
    perror("SIOCGLINKSTATUS");
    close(v2);
    return 0;
  }
}
```

Listing 1: Decompiled code of the funtion that returns the cable status in the firmware of TP-Link TL-WR940N

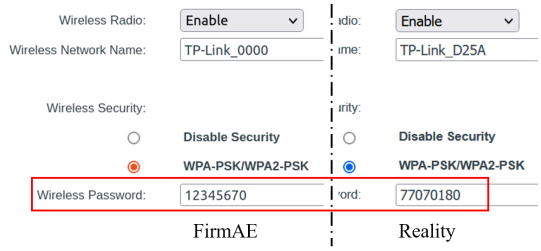

Figure 3: The Wi-Fi configuration page of TP-Link TL-WR940N in FirmAE and a real device

issues primarily due to the absence of required values normally found in flash.

This issue is more critical than failed firmware emulation. Discrepancies in default settings between successful setup wizards and actual devices may go unnoticed, compromising the accuracy of the analysis. For instance, after we fixed the error mentioned above in TP-Link TL-WR940N, the setup wizard proposes the default Wi-Fi passphrase `12345670`. However, as shown in Figure 3, a physical router running this firmware proposes a less-trivial passphrase: `77070180`. We confirmed by reverse-engineering the firmware image that in the absence of a value in flash, the passphrase will fall back to `12345670`. See Appendix A for more details.

In conclusion, missing important information in the firmware images makes it impossible for emulators to properly emulate real devices while preserving realistic default settings. Due to this intrinsic limitation, we resorted to purchasing physical routers.

3.2 Overview and Analysis Environment

To conduct a comprehensive analysis of both the LAN and WAN sides of the router, we build an analysis environment based on real routers. We first interpose the WAN interface of the router to observe outgoing traffic, provide a realistic network configuration to the router (especially with regard to IPv6), and conduct port scanning. Our position is thus representative of Adv_WAN and Adv_NET. Then, we connect to the Wi-Fi network of the home

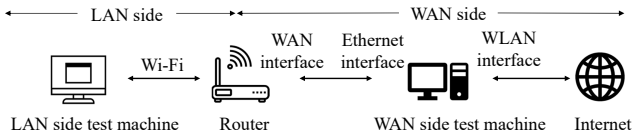

Figure 4: Environment setup in the analysis framework.

router to access the web management page, complete the setup wizard, and conduct further analysis from the perspective of Adv_LAN and Adv_PHY; see illustration in Figure 4.

Based on this environment, we designed a comprehensive router default settings security analysis framework according to Section 2. This is a minimal security testing framework that may not cover all potential security issues (which is also impossible), but routers should pass these tests to ensure a minimal level of security. This framework can be divided into two stages: initial analysis and deep analysis. The initial analysis is concerned about obtaining the initial defaults of the router, while the deep analysis focuses on the sensitive features supported by the router, after we enable them.

The tested items are listed in Table 1 with their potential exploiters. Additionally, we designed a report template containing 81 items to fill in the analysis results based on this analysis framework, as shown in Table 4 in Appendix C.

3.3 Setup Wizard

Routers may not be fully operational after getting plugged in for the first time. In this case, users will be invited to manually visit the management page of the router, or automatically redirected there by their browser. In Appendix B, we show an example of a setup wizard in Figure 6.

Our initial approach involves connecting to the router's Wi-Fi network with the credentials provided on the router's label. We evaluate whether the router can be plug-and-play, disregarding instances where routers that could be plug-and-play include a "quick setup" guide that, despite recommendations, is not necessary for completing the setup process.

The setup wizard guides users to configure the network, set the Wi-Fi and admin passwords, and update firmware. We expect users may try to avoid making decisions and simply click "next" or "skip" when possible. When users without necessary knowledge have to make decisions, visual hierarchical design [52] can affect their decisions. Therefore, when a page of the setup wizard requires to take an action, e.g., update the router firmware now, we can use the principle of visual hierarchy to infer the buttons that manufacturers want users to click on and the behavior of most real users, see illustrations in Figures 5a, 5b. Our goal is to complete the setup wizard as the average user and record default settings and behaviors.

3.4 Initial Settings Analysis

After completing the setup wizard (if any, and when necessary), we traverse all management pages of the router and record the settings for sensitive features and whether these features are enabled by default. We also verify whether Wi-Fi settings are applied correctly and perform a port scan on both the LAN and WAN sides to detect exposed services. We discuss these tested items as follows.

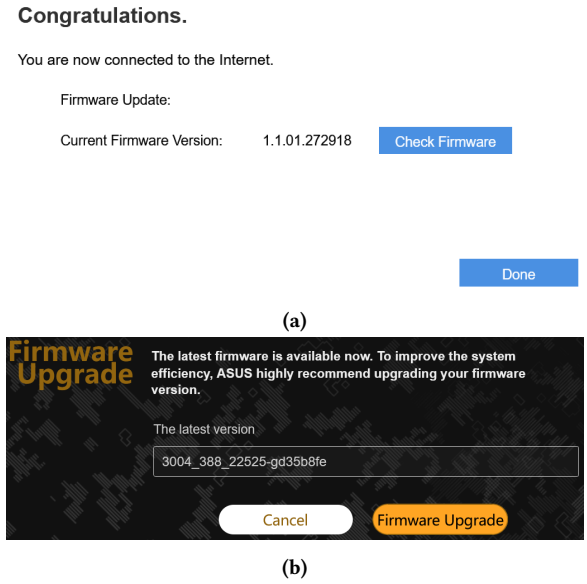

Figure 5: Setup Wizard inviting the user to check for and apply firmware update now: (a) skip is the user's most likely choice ("Done"); (b) proceed is the user's most likely choice ("Firmware Upgrade")

Wi-Fi and admin passwords/passphrases. We first record the default password/passphrase in each router (if any, and usually provided on the label) to evaluate their strength. Then, to check whether routers can guide users to set strong passwords/passphrases, we record whether changing the default password is required and try to set the shortest and simplest password that can be accepted during password change to test strength requirements. Routers may also offer a password strength meter (informative only).

Wi-Fi security protocol. We record the default security protocol set to protect Wi-Fi communications. Sometimes, a hybrid mode is supported to provide backward compatibility with older client devices. We also measure the effective protocols supported by the router by examining beacon frames sent by the router. Beacons carry information about the supported WPA version ciphersuite (TKIP or CCMP). We check both the main and guest networks as well as all frequency bands (2.4 and 5GHz).

WPS. WPS PIN is vulnerable to brute force attacks. We can extract the status of WPS from the beacon frames advertised by the router to verify its support for WPS PIN and whether the status is "Configured" (functional) or "Locked" (non-functional) [1]. In the former case, we attempt to record and test the given PIN (printed on the label or available in the relevant configuration page) or launch a brute-force attack leveraging Reaver [61] when no PIN is known to check the usability of WPS. We also detect whether a rate-limiting mechanism is in place, imposing restrictions on brute-force attacks.

Local web access. We first record the protocol employed to access the management page (HTTP or HTTPS, and TLS version), which could allow adversaries (Adv_LAN), when vulnerabilities exploited, to eavesdrop on the traffic and learn sensitive information such as

the admin password. Then, we also measure countermeasures to brute-force login attempts, through rate-limiting or CAPTCHAs.

Firmware update mechanisms. During the setup wizard, we record whether routers notify or force users to update the firmware as a one-time action, or if the router indicates it is running the latest version (so we cannot test which way it is). If the setup wizard is not required, this step can be skipped by users. Automatic update can help users update firmware regularly, so we check whether it is enabled by default in the management page. For user-initiated update, we run Wireshark and mitmproxy [8] to capture firmware update packets and check whether TLS is correctly implemented. In addition, we also check whether the firmware update will modify or reset the router settings without prompting the user, which may cause the user's security settings to become invalid.

Exposed services. To discover hidden services (not mentioned in the management page), we leverage Nmap [49] to scan for the router's open ports and corresponding services and their versions on the WAN and LAN interfaces. To speed up scanning of 65,535 ports, we run Nmap in parallel on smaller port ranges.[1]

3.5 Deep Settings Analysis

After completing the initial analysis, we have collected default settings about all generally-supported features. Next, we focus on deep defaults, which often require an action to turn on the corresponding features.

Guest network. We record the type of the guest network first. If it is protected by a Wi-Fi security protocol, we will investigate its Wi-Fi configurations and passphrase requirements as mentioned earlier. To test the privileges of the guest network, we check whether we can log in to the management page as an administrator from the guest network.

Remote web access. Remote management via the Internet usually requires the help of companion apps or remote web access. In the case of remote web access, the public IP address of the router's WAN interface with a designated port number allows access to the management page from the WAN side directly. As with local web access, we can examine the security of remote web access the same way, but with additional considerations since it is exposed to the Internet. We also check whether the TLS certificate of the router is self-signed. If the subject and issuer of a certificate are the same, it means that this certificate is self-signed. Additionally, we record the version of TLS because older versions may have known vulnerabilities.

Telnet/SSH. Adv_WAN and Adv_LAN can exploit Telnet or SSH to access the terminal of the router if it is not configured properly. We can check whether Telnet or SSH is enabled by default on the LAN or WAN interfaces of the router according to management pages and the results of port scanning. If the router supports Telnet or SSH, we try to connect to it and check whether a username and password are required to login and whether the default username and password are weak.

IPv6. The security of IPv6 depends on whether the IPv6 addresses of connected devices are generated by the router, whether they are predictable, whether IPv6 NAT is leveraged by default, and whether the IPv6 firewall blocks IPv6 packets from the WAN side. We leverage `dhcpd6` and `radvd` to build a virtual stateless DHCPv6 environment to assign IPv6 address to the router and capture traffic between the router and the connected device when connecting to the router's Wi-Fi. Then, we can find out whether the router employs SLAAC, stateful DHCPv6 or stateless DHCPv6 to assign IPv6 addresses. Only in the stateful DHCPv6 IPv6 addresses are generated by the router, and in the other two methods IPv6 addresses are generated by the device itself. We can record the WAN IPv6 addresses and MAC addresses of the router and connected devices to check whether the generated addresses are predictable. Usually, the generation algorithms of different devices are different.

To check whether IPv6 NAT is leveraged by default, we can ping the Internet from the LAN side and compare the source IPv6 addresses of ping request packets captured on the LAN side and WAN side. If they are different, it means that the router employs NAT, and the IPv6 address of the device is only used in the LAN, so the adversary cannot directly connect to the device with the IPv6 address. When there is no NAT, we set up a simple Web server on the LAN side and try to access it based on the IPv6 address of the WAN side to check whether an IPv6 firewall that blocks incoming connections from the Internet is enabled by default. If not, it means that the connected devices are being exposed to the Internet, bringing potential security risks to users. To check the blocking range of the firewall, we can deploy the server on the common port 80 and the private port 8000 for testing.

Cloud account. If the cloud account is compromised, the bound router may be controlled by adversaries. Therefore, there is a need to examine its password strength requirements. Additionally, we capture login packets and check whether the password of the account can be intercepted by Adv_NET.

App. We capture the traffic between the router and the server to check whether HTTPS is employed and the TLS certificate is validated properly when binding the app with the router and leveraging the app to remotely manage the router.

UPnP. The main security risk of UPnP comes from the port forwarding function. PortMapper [32] can be leveraged to detect whether the router supports UPnP port forwarding and whether new port mappings can be added.

External Storage. To prevent exposure of the user's private data stored in the external storage, we check whether authentication is enabled and verify the strength of default passwords. Additionally, for remote FTP, we capture the traffic on the WAN side when leveraging FileZilla [18] to connect to the FTP server on the router's WAN interface. Similar to remote web access, the captured traffic allows us to validate whether the remote FTP traffic is encrypted by TLS and whether the router's TLS certificate is valid. We also record the version of TLS. Remote storage access over HTTPS also relies on TLS for secure communication over the Internet, so we apply the same evaluation methods to assess its security.

[1] `nmap -sV -T5 -p 1-100`, then `-p 101-1000`, `-p 1001-5000`, etc.

Reset. We check what information will be retained after a device reset. Given the data extraction cost, we do not consider the sensitive information left in the flash chip of the router, but only focus on the information available in the management page, including Wi-Fi SSID & password, admin username & password, cloud account, third-party accounts (e.g., DDNS, VPN, PPPoE, email, and FTP) and logs. Additionally, the binding status between the companion app and the router is also sensitive, and it is necessary to ensure that the router is automatically unbound from the app when reset. We can reset the router after modifying and recording all sensitive information. If the router offers different reset options, we will record them and select the default recommended options. Thereafter, we try to skip the setup wizard and check whether such sensitive information is retained and whether we can still use the app to remotely manage the router. If the wizard cannot be skipped, we will pay additional attention to whether the sensitive information is kept as default values in the setup wizard. Note that we consider the reset feature as a special case as it is expected to restore to the default settings (which is our focus) and may pose a security risk; however, it does not map to any of our four types of adversaries.

4 ANALYSIS RESULTS

We analyzed 40 home routers based on a selection detailed in Section 4.1, by following our analysis framework (Section 3). The routers were running the factory firmware unless the setup wizard explicitly recommends updating the firmware before continuing, mimicking common user behaviors. The factory version will also run for a period of time until the router automatically updates the firmware (if supported).

We share below the essential findings from the analysis. The key results are summarized in Table 3 by brand and model (we have anonymized the models with unpatched vulnerabilities for ethical reasons). We found a total of 46 potential vulnerabilities (marked with "!!" in Table 3), out of which, we have confirmed 30 to be exploitable in the latest version and reported them to manufacturers or CNVD/CVE (marked with "*" in Table 3). More information about our vulnerability reporting will be updated at https://github.com/YjjNJUPT/AsiaCCS2024_vul_report. The detailed results are tabulated in Appendix C.

It is noteworthy that our analysis may have covered only a small portion of all available routers on the market. Our research objective is to understand trends to help manufacturers improve home router security, rather than guiding consumers in choosing a router.

4.1 Router Selection

Home routers are diverse in vendors, regional markets, popularity, and firmware filesystems. Due to the prohibitive cost of buying all available router models, we choose to evaluate a selection of commercially off-the-shelf routers that can reflect both popularity and diversity.

Brands included in our selection are from both the global market [41] and, in consideration of the huge user base in China, the Chinese market [76]. We purchased the routers from Amazon US, Taobao, and JD (two largest online shopping platforms in China), which we believe are representative of what most end users are exposed to. We selected 40 home routers (for scale, 35 routers were purchased in a previous study [30]) according to their series names, regions, price range, and popularity, under a budget of $3,000 USD. Although some of them are not the latest models, they still received updates in recent years and appear to be popular on those platforms. Consumers might buy them especially since they may be cheaper and thus more attractive. Therefore, including them is essential to reflect the actual status of the router market.

4.2 Key Findings

4.2.1 Finding 1: IPv6 support without firewall. 37 routers support IPv6 (but only 25 can work) and 11 of them have it enabled by default. Nearly all of the routers with a functional IPv6 stack do not implement IPv6 NAT (24/25), as expected. However, 5 of them also do not implement an IPv6 firewall to block incoming connections from the internet by default. Adv_WAN can directly reach devices located in the local network using their (public) IPv6 address. This behavior is a violation of RFC 4864 [34], and dangerous in a home network environment as it exposes printers, IoT and other devices that are not designed to be publicly reachable. Two of the 5 routers enable IPv6 by default and can simply work as plug-and-play, leaving customers of IPv6-enabled ISPs exposed out of the box.

Worse, a router implements stateful DHCPv6 and attributes full IPv6 addresses to connected devices by following simple and predictable suffixes such as "1000", "1001", "1002". Fortunately, this router does not enable IPv6 by default.

The other 4 routers rely on stateless DHCPv6 to assign IPv6 addresses to devices, which means that the IPv6 addresses are generated by the devices themselves rather than the routers. Note that modern operating systems generate random interface IDs [12, 47], making it difficult for adversaries to predict the IPv6 address of a specific computer. However, we cannot guarantee that all devices, especially IoT devices, can generate an unpredictable IPv6 address for themselves.

We are working with the affected vendors to fix these vulnerabilities. At present, two of them have been assigned CVE IDs (CVE-2023-41603 and CVE-2023-41604) and D-Link has released a hotfix for D-Link R15.

4.2.2 Finding 2: Insecure Wi-Fi security protocols still supported by default. 13 routers still support WPA (version 1) with AES-CCMP encryption by default. Although AES-CCMP is relatively secure, it is susceptible to KRACK attacks [65, 66] that can replay and decrypt packets. More worryingly, 2 routers still support the outdated TKIP encryption by default, a protocol vulnerable to both replay and forgery of packets via KRACK attacks. Out of the 40 routers we purchased, 17 do not support WPA3, while the remaining 23 routers do not default to WPA3 although supported. This shows a slow adoption of new standards among router manufacturers.

Furthermore, we encountered a router that initially supports WPA/WPA2-PSK-(TKIP|CCMP) before the setup wizard finishes then transitions to only supporting WPA2-PSK-CCMP. However, it is functional without the setup wizard, and thus could run with less secure configuration in a plug-and-play scenario.

4.2.3 Finding 3: Insecure default se ings for plug-and-play. Plug-and-play functionality allows users to start enjoying their router

Table 3: Summary of potential and confirmed security issues from our analysis of 40 routers

Brand	Model name	Has IPv6 NAT disabled	Has IPv6 firewall disabled	Uses predictable IPv6 address	Supports WPA v1	Supports TKIP encryption	Does not require setup wizard	Offers open Wi-Fi by default	Offers no or weak admin pwds	Supports configured WPS	Uses PIN hidden from users	Accepts WPS PIN attempts	Does not rate-limit PIN attempts	Uses Hard-coded PIN	Checks version info insecurely	Downloads FW image insecurely	Has insecure app remote mgmt	Does not change Wi-Fi/admin pwd	Allows open Wi-Fi to remain	Offers open guest network	Allows open Wi-Fi/admin pwd	Supports WPA v1	Supports TKIP encryption	Allows guests to access mgmt page	Leaves sensitive info after reset
360	T—	-	-	-	!	-	-	-	-	-	-	-	-	-	!!	-	-	!	-	!	-	-	-	-	-	-
ASUS	R—	!	-	-	-	-	!	-	!	!	-	!	-	-	-	!!*	-	-	-	-	-	-	-	-	-	-
ASUS	T—	-	-	-	-	-	-	-	-	!	-	!	-	-	-	!!*	-	-	-	!	-	-	-	-	-	-
ASUS	T—	-	-	-	-	-	-	-	-	!	-	!	-	-	-	!!*	-	-	-	!	-	-	-	-	-	-
D-Link	D—	!	-	-	!	!	!	-	!	!	!	-	-	-	!!*	-	-	-	!	!	-	-	-	-	-	-
D-Link	D—†	!	-	-	!	-	-	-	-	!	-	!	-	-	!!	-	-	!	-	!	-	-	-	-	-	-
D-Link	D—	-	-	-	-	-	!	-	!	!	-	-	-	-	-	-	-	-	-	!	-	-	!!*	-	-	-
D-Link	R15	!	!!*	-	-	-	!	-	-	!	!	!	-	!!*	-	-	-	-	-	-	-	-	-	-	-	-
H3C	N—	!	-	!	-	-	-	-	-	!	!	-	-	-	!!*	!!*	-	!	-	!	-	-	-	-	-	-
HUAWEI	AX3 Pro	!	-	-	-	-	-	-	-	!	!	-	-	-	-	-	-	-	-	!	-	-	-	-	-	-
HUAWEI	WS7002	!	-	-	-	-	-	-	-	!	!	-	-	-	-	-	-	-	-	!	-	-	-	-	-	-
Linksys	E—	!	-	-	-	-	-	-	-	!	-	!	-	-	-	!!*	-	-	-	C	-	-	-	-	-	-
Linksys	E—	-	-	-	-	-	-	-	-	!	-	!	-	-	!!	!!*	-	-	-	C	-	-	-	-	-	-
Linksys	E—	!	-	-	-	-	-	-	-	!	-	!	-	-	-	!!*	-	-	-	C	-	-	-	-	-	-
Linksys	E—	-	-	-	-	-	-	-	-	!	-	!	-	-	!!	-	-	-	-	C	-	-	-	-	-	-
Linksys	EA5800	-	-	-	-	-	-	-	-	!	-	!	-	-	-	-	-	!	-	C	-	-	-	-	-	-
Linksys	MR6350	-	-	-	-	-	!	-	!	!	-	!	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Linksys	W—	!	-	!	-	-	-	-	-	!	-	!	-	-	!!	-	-	-	-	-	-	-	-	!!*	-	-
Mercury	X30G	!	-	!	!	-	-	-	-	-	-	-	-	-	-	-	-	!	!	!	-	-	-	-	-	-
Netcore	N—	-	-	-	!	-	-	-	-	!	!	!	-	-	!!*	!!*	-	!	-	!	-	-	-	-	-	-
Netcore	N—	!	-	-	!	!	!	!	-	!	!	!	-	-	!!*	!!*	-	-	-	-	!	-	-	-	-	-
Netcore	N—	!	-	-	!	-	!	-	-	!	!	!	-	-	!!	-	-	-	-	-	!	-	-	-	-	!!*
Netcore	P—	!	!!*	-	!	-	!	!	-	!	!	-	-	-	!!	-	-	-	-	!	-	-	-	-	-	-
NETGEAR	R6120	-	-	-	-	-	-	-	-	!	-	!	-	-	-	-	-	!	-	!	-	-	-	-	-	-
NETGEAR	R—†	-	-	-	-	-	-	-	-	!	-	!	-	-	!!	!!	-	!	-	!	-	-	-	-	-	-
NETGEAR	RAX40	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	!	-	!	-	-	-	-	-	-
NETGEAR	R—	-	-	-	-	-	-	-	-	-	-	-	-	-	!!	-	-	!	-	!	-	-	-	-	-	-
NETGEAR	R—	-	-	-	-	-	-	-	-	-	-	-	-	-	!!	-	-	!	-	!	-	-	-	-	-	-
Ruijie	X—	!	-	!	!	-	-	-	-	-	-	-	-	-	!!*	!!*	!!*	-	-	!	-	-	!!*	-	-	-
Tenda	A—	-	-	-	-	-	!	!	-	!	-	!	-	-	!!	!!	!!*	-	-	!	-	-	-	-	-	-
Tenda	A—	!	!!*	-	-	-	!	!	-	!	-	!	-	-	!!	!!	!!*	-	-	!	-	-	-	-	-	-
Tenda	F3	-	-	-	!	-	!	!	!	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TP-Link	Archer-AX23†	!	-	-	-	-	-	-	-	!	-	!	-	-	-	-	-	!	-	!	-	-	-	-	-	-
TP-Link	T—	!	!!*	!	!	-	-	-	-	-	-	-	-	-	-	-	-	!	!	!	-	-	-	-	-	-
TP-Link	T—	!	!!*	-	-	-	-	-	-	!	-	!	-	-	-	-	-	!	-	!	-	-	-	-	-	-
TP-Link	TL-WR940N†	!	-	-	!	-	-	-	-	!	-	!	-	-	-	-	-	!	-	-	-	-	-	-	-	-
TP-Link	TL-XDR3010	!	-	!	!	-	-	-	-	-	-	-	-	-	-	-	-	!	!	!	-	-	-	-	-	-
Xiaomi	4—	!	-	!	!	-	-	-	-	!	!	-	-	-	!!*	!!*	-	!	-	-	-	-	-	-	-	-
Xiaomi	Redmi AX3000	!	-	!	-	-	-	-	-	!	!	-	-	-	-	-	-	!	-	-	-	-	-	-	-	-
ZTE	A—	!	-	-	!	-	!	-	!	!	!	!	-	-	-	-	-	-	-	!	-	-	-	-	-	!!
Total	40 routers	24	5	8	15	2	12	5	6	31	12	23	0	1	18	14	3	18	3	23	4	1	3	2		

Legend: "!" indicates the presence of an issue/feature that may be a prerequisite for security issues (e.g. no IPv6 NAT is not a vulnerability by itself unless IPv6 firewall is not working). "!!" indicates the presence of a potential vulnerability and "*" means we have confirmed it to be exploitable in the latest version. "C" under "Open guest network" represents a captive portal. "†" marks the 4 routers purchased between Dec 2021 and Oct 2022 for preliminary (other routers were purchased in Oct 2022, Feb 2023 and May 2023).

without accessing the management page or completing the setup wizard, which poses security risks. Out of the 12 plug-and-play routers studied, 5 lack a default Wi-Fi password, making the Wi-Fi network open and vulnerable. Furthermore, if the setup wizard is never completed, accessing the management page will redirect to this wizard that lacks any admin password in two routers, or expects simple passwords, e.g., "admin", "password", in 4 routers. Adv_LAN could easily take control of the router in such cases. Finally, 5 other routers ask for the Wi-Fi passphrase as an initial admin password, which Adv_LAN might already know.

4.2.4 Finding 4: WPS PIN still supported by default, sometimes with unknown PINs. Despite the known susceptibility of the WPS PIN authentication method to brute-force attacks, 31 routers appear to still support this feature as advertised by a "Configured" status. The concern is heightened as 12 of these routers do not tell users the expected PIN.

Out of these 31 "configured" routers, 23 routers can theoretically be cracked as reaver can successfully complete several WPS PIN attempts. To prevent brute force attacks, all of them get locked after several failed WPS PIN attempts, but the locking time varies among routers. Seven routers are only locked for 1 minute per failure and one router is only locked for 2 minutes. Other routers are locked for a long time and difficult to crack.

As brute-forcing is time-consuming, we only cracked D-Link R15 successfully. We find that the hidden WPS PIN code of this router is very simple. We purchased another router of the same model and confirmed the PIN works successfully, meaning that it is hard-coded and likely to be the same for all such routers, which is a serious vulnerability. We reported this issue to D-Link and received a confirmation. At present, this vulnerability has been assigned a CNVD ID (CNVD-2023-59339) and D-Link has fixed it by a hotfix.

4.2.5 Finding 5: TLS not used when needed or without certificate validation. Several routers were found to communicate with servers over HTTP instead of HTTPS when checking firmware versions or downloading firmware update files. This practice exposes routers to MITM attacks. In addition, certain routers failed to validate TLS certificates properly.

Checking firmware version, performing firmware update, binding to the companion app and remote management with the app all require routers to communicate with servers on the Internet. We find that 7 routers rely on HTTP to check firmware version and 7 rely on HTTP to download firmware update files. Moreover, among routers that do leverage TLS, 9 of them do not validate TLS certificates properly for version checking, and 5 routers when downloading update files. Adv_NET can easily replace update files to downgrade the router or write malicious firmware into the router, if no further integrity or authenticity check is performed.

Also, a router did not perform certificate validation when being remotely managed by the companion app, i.e., Adv_NET can use a self-signed certificate to intercept traffic between the router and the server and carry out MITM attacks. Additionally, we find that two routers implement a custom protocol over TCP to check firmware version, perform update and communicate with the companion app server, but sensitive information is transmitted in plaintext, which leads to information being exposed on the internet to Adv_NET.

External storage and remote web access also require the TLS protection. However, we can only find two routers employing non-self signed TLS certificates: one served a public certificate for a real domain, and leaked the key in firmware, however this problem has already been fixed in later versions of the firmware; the other one includes an untrusted certificate issued by "ZTE-ROOT-CA", which is not better than self-signed certificates. In addition, we find one Linksys router employing an expired self-signed TLS certificate after we update its firmware. The incorrect use of TLS certificates may result in Adv_NET being able to conduct MITM attacks. DDNS can alleviate this issue as it attaches the router to a domain name and could facilitate the issuance of browser-trusted certificates; however, it is always disabled by default.

4.2.6 Finding 6: Setup wizards fail to guarantee strong passwords. Although 28 routers require users to complete the setup wizard, 18 of them do not force users to set Wi-Fi or admin passwords during the setup wizard. Similarly, all 11 routers with optional setup wizards fail to enforce the change of either passwords. After going through all setup wizards, 4 routers end up not having a default Wi-Fi password and do not force users to set it (i.e., Wi-Fi network remains open). The same applies to admin passwords for two routers. If the user is not paying attention, these routers may run without a password. Additionally, two routers employ "admin" as the default admin password and do not require users to change it, which is also insecure. We also find that 10 routers employ the Wi-Fi password as the admin password by default and inconspicuously remind users during the setup wizard. If Adv_LAN can obtain the Wi-Fi password, he can also access the management page and control such routers easily.

10 routers require users to set both Wi-Fi and admin passwords, but the requirements for password strength are very low. All of the selected routers only require users to set a Wi-Fi password that contains more than 8 characters and don't have any other requirement. In this case, users may prefer to set 8-digit numeric passwords [68], which are not so difficult for Adv_PHY to crack. In addition, there are 8 routers that do not even have any admin password strength requirements.

4.2.7 Finding 7: Poorly protected guest network. As guest network is an optional feature, only one router has it enabled by default, which might be why not much attention has been given to the security of this feature. However, we find that 23 routers do not enforce a Wi-Fi security protocol by default, which means that the guest network is open if the user simply enables it by a click. Among the routers that enable Wi-Fi security protocols by default, we also find 4 routers support WPA and one of them still support TKIP by default.

In addition, 5 routers offer a captive portal with an open (unencrypted) Wi-Fi configuration by default. Those routers' strength requirements only impose a 4 character minimum limit and their login interfaces do not seem to limit password attempts.

To protect the main network, the guest network is generally isolated from the host network. However, 3 routers allow access to the management page from the guest network, unnecessarily exposing the router to (untrusted) guests. Among them, a "plug-and-play" router has "password" as default admin password, which makes it even more vulnerable.

Given these heterogeneous results, we note that a standard definition of the characteristics of "guest networks" is missing.

4.2.8 Finding 8: Reset options requiring user diligence. It is common for routers to support resetting through the management page by clicking on a button, which is also known as soft reset. We find 2 routers retaining sensitive information after reset. One retains logs. The other one is still bound with the companion app after reset and the app can remotely manage the router. This may undermine user privacy when second-hand routers are traded.

Additionally, we find 7 routers provide different reset options for users to keep some data, but enable them by default. If the user is not aware, some sensitive information may be retained. For example, 2 routers have "Preserve network configuration when restoring factory settings" enabled by default and will retain Wi-Fi passwords after reset. If users reset the router in this way, sensitive information will remain in the router.

4.3 Discussion

In this section, we discuss the security implications of home router default settings from the perspective of various types of adversary and provide recommendations to make home routers more secure.

Adv_WAN. The security of IPv6 has not received sufficient attention from manufacturers, compared to its predecessor. As shown in Finding 1, an attacker on the Internet could directly access devices on the local network of the 5 routers without IPv6 NAT and firewall with their public IPv6 addresses, if no other protection in place.

Although none of the analyzed routers leave any port open on the WAN interface by default, certain features that are initially disabled may pose security risks from the Internet when turned on without changes to the related default settings. For remote web access, our analysis reveals that 5 routers employ the insecure HTTP protocol as the default option. Even for the routers that support the TLS protocol, Finding 5 indicates that it is not implemented properly. Regarding remote FTP, authentication passwords are required by all 10 routers supporting this feature. However, only one router implements TLS encryption for FTP traffic. On a positive note, we observed that only ASUS routers support SSH, and no router enables Telnet or UPnP on the WAN interface.

Recommendation. To defend against Adv_WAN, manufacturers should avoid exposing unnecessary services on the WAN interface, and only support TLS-based services when needed. If IPv6 is required, an IPv6 firewall should be enabled and properly configured to reject inbound connections by default, as it is the current behavior in IPv4 (either due to a firewall or a NAT).

Adv_LAN. Although the LAN is not as exposed to the Internet as the WAN side, its security still needs attention. Adv_LAN (e.g., compromised devices) is likely to try to access the management page first because this is the easiest way to control the router. As shown in Finding 6, the setup wizard does not always guide users to set a strong password and accessing the management page may not even require a password in the case of plug-and-play (Finding 3).

To mitigate brute force attacks, 25 routers rate-limit the login attempts to the management page, and 4 routers support CAPTCHA. However, all of the analyzed routers choose HTTP as the default protocol for web access, which means that Adv_LAN can eavesdrop the password when users log in to the management page.

When analyzing the open ports of the LAN interface, we discovered that 2 routers have an open but undocumented Telnet service, while 4 routers have an undocumented SSH service. However, only one router allows connection with the admin password, with limited functionality. Our speculation is that the Telnet/SSH service might be intended for debugging purposes and was not fully removed or disabled thereafter. Additionally, we observed that all routers supporting Telnet/SSH in the management page have these services disabled by default and utilize the admin password for login, which is relatively secure.

Adv_LAN can exploit UPnP to mount MITM attacks by adding port mappings [16]. Unfortunately, 18 routers have UPnP enabled by default on the LAN interface and support adding port mappings, making them vulnerable to Adv_LAN.

If Adv_LAN is interested in compromising user privacy, external storage would be a good target. In our analysis results, 10 routers do not enable authentication for SMB and 6 routers do not enable authentication for local FTP by default. 5 routers support local HTTP/HTTPS access and none of them enable authentication by default. Also, 3 routers use very weak default credentials for SMB and local FTP (2 "admin/admin" and 1 "user/password").

Recommendation. To defend against Adv_LAN, manufacturers should make the setup wizard mandatory and enforce password strength requirements and leverage proper meters to guide users to set a strong password. Rate-limiting should be employed to counter brute-forcing. Manufacturers also need to protect services on the LAN interface (e.g., restrict/disable UPnP port mapping, and authenticate users from Telnet/SSH and external storage). Home router users should set a strong admin password, disable unnecessary services, or when necessary, enable them with strong authentication.

Adv_PHY. Adversaries physically close to the router can receive Wi-Fi signals and their main goal is usually to become Adv_LAN. As shown in Finding 2, routers still employing insecure Wi-Fi security protocols by default will be vulnerable to KRACKs. Findings 3 and 6 also indicate weak Wi-Fi authentication on certain routers. The guest network is even less protected according to Finding 7. In addition, WPS PIN is one of the WPS modes we confirmed to be insecure in Finding 4, but still sometimes supported.

Recommendation. To prevent Adv_PHY, manufacturers should employ WPA3 as the default Wi-Fi security protocol and guide users to set a strong Wi-Fi password via the setup wizard for both host and guest networks. Manufacturers also need to ensure that the guest network is isolated from the host network. In addition, support for WPS PIN and the relevant code should also be removed to prevent undesired effects. Home router users should select WPA3 and set strong passwords for the host and guest networks.

Adv_NET. Adversaries already able to plug into the network communication between the router and the Internet can mainly be prevented by the TLS protocol from implementing MITM attacks. However, Finding 5 indicates that TLS is not always implemented properly. This means that Adv_NET can eavesdrop on and tamper with packets between the router and servers/clients when users update firmware, leverage the companion app to remotely manage

the router, or remotely access the management page or the external storage over the Internet.

We find 8 routers using custom protocols to communicate with their servers and 2 of them do not encrypt the packets because we are able to extract key information (e.g., Wi-Fi passwords) when remotely modifying the settings via the companion app.

Recommendation. To counter Adv_NET, manufacturers should rely on TLS with browser-trusted certificates and validate it properly to encrypt the traffic between routers and servers/clients.

Ways forward. Despite the various issues being case-specific, our generalized vision is that both the initial and the deep default settings need to be secure. In particular, with the motivation and assumption mentioned in Section 1, i.e., end users tend to leave default settings as is, the burden to improve is first on device manufacturers, e.g., certain settings are not always shown, not to mention updatable in the management page (hence not an action users are able to take). This is further reflected in our observation that in certain cases after a firmware update, the default settings become more secure, which means that the security of default settings is gradually receiving attention from manufacturers. Still, as the last line of defense, security awareness among users should also be enhanced to be vigilant on the defaults, not just to ignore and skip.

Although we believe these 40 routers can represent the majority of routers in the current international and Chinese home router markets, the results may not accurately profile the actual situation, as our selection methods are not based on all the routers in active use (about which we do not have access to the information). Nonetheless, our results can be considered an approximation of the actual situation and help researchers better understand potential risks of home router default settings.

5 RELATED WORK

In this section, we revisit several previous efforts similar or comparable to our work.

IoT security analysis. Wang et al. [71] and Zhao et al. [75] conducted large-scale security analyses of IoT devices on the Internet. They leverage search engines such as Shodan [57] and Zoomeye [77] or custom search tools [11] to test active IoT devices on the Internet, which means only devices with exposed services (open ports) to the Internet were covered in the analysis. They focus on the distribution information of device firmware versions and known vulnerabilities on the Internet without covering other types of attackers discussed in Section 2.1.

Taking a step further, there are also projects/studies focusing on IoT devices in home networks. For instance, Kumar et al. [35] analyzed the user's home network information collected by Avast's tool called Wi-Fi Inspector (where users could upload their scan results for insecure IoT devices), and found that many IoT devices employed weak passwords on FTP and Telnet, and default admin passwords that were left unchanged by users. Alrawi et al. [2] systematized the literature for home-based IoT security and, similar to our work, evaluated 45 IoT devices and proposed mitigation recommendations based on an abstract model that segments IoT deployments into components, including the IoT device, the companion mobile app, the cloud endpoints, and the associated communication channels.

Although home routers are also a type of IoT devices, the security implications of their default settings is tightly coupled with the users' perception and usage habits and how they use the routers — involving sociotechnical factors. Therefore, a tailored study like ours is necessary. Nonetheless, these aforementioned studies can still be good references for evaluating home router security.

Router security analysis. Visoottiviseth et al. [70] proposed an emulation-based firmware analysis tool that can perform both static and dynamic large-scale analyses for router firmware. It includes several open-source automated tools to test the security of passwords, SSL, web application and firmware update to find vulnerabilities in the router firmware. However, emulation-based analysis is limited to only router models with publicly available firmware and subject to potential low fidelity as we demonstrated in Section 3.1. Along this direction, similar to our work, Jeitner et al. [30] and Niemietz et al. [48] chose to evaluate real-world home routers, but they only focus on the DNS service or web interface of routers. Currently, there is no comprehensive security assessment work for the default settings of various features of home routers.

Human-computer interaction. To understand the impact of UI design on user behavior, research in human-computer interaction such as visual hierarchy [14, 52], dark pattern [42, 46] and banner blindness [4, 51] has received immense attention. In addition to Web page/advertising design, these paradigms can also be applied to improve device setup wizards. Prange et al. [54] studied the effect of "nudges" based on the Protection Motivation Theory in the setup wizard of smart home devices on increasing users' motivation to employ effective threat prevention. Ho et al. [24] performed a city-wide survey and several interviews and found that home router users commonly adopt the default settings provided by the setup wizard. They designed and implemented a new set of configuration steps to secure routers, but only considered password management and MAC address filtering.

6 CONCLUSION

In this paper, we brought attention to the various security-related default settings of home routers, and designed a comprehensive router default settings security analysis framework and leveraged it to analyze 40 home routers from the global and Chinese markets. To our surprise, although our analysis methodology is quite straightforward (we merely verify whether the settings and basic functions are configured properly), we found numerous security issues, resulting in up to 30 exploitable vulnerabilities. We discussed potential improvements for users and especially manufacturers to make home routers more secure. Although default settings have received gradual attention from manufacturers, e.g., we noticed improvements after a firmware update, there is still a long way to go according to our findings. This framework can also be applied to analyze home routers from other sources (such as ISPs [55]), which are popular in certain regions. We hope our analysis can shed some light on the user-centric security research of home routers in the community.

ACKNOWLEDGMENTS

This work is supported by the National Key Research and Development Program of China with 2019YFB2101704.

REFERENCES

[1] Wi-Fi Alliance. 2020. Wi-Fi Protected Setup Specification v2.0.8. https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_Protected_Setup_Specification_v2.0.8.pdf.

[2] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. 2019. SoK: Security Evaluation of Home-Based IoT Deployments. In *IEEE Symposium on Security and Privacy (S&P'19)*. 1362–1380.

[3] Baran, Guru. 2019. New Mozi P2P Botnet Attacks Netgear, GPON, D-Link and Huawei Routers Using Weak Passwords and Some Known Exploits. https://gbhackers.com/new-mozi-botnet/.

[4] Jan Panero Benway. 1998. Banner Blindness: The Irony of Attention Grabbing on The World Wide Web. In *Human Factors and Ergonomics Society Annual Meeting (HFES)*, Vol. 42. 463–467.

[5] Meriem Bettayeb, Qassim Nasir, and Manar Abu Talib. 2019. Firmware Update Attacks and Security for IoT Devices: Survey. In *Annual International Conference on Arab Women in Computing (ArabWIC'19)*. 1–6.

[6] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. 2003. Security Flaws in 802.11 Data Link Protocols. *Communications of the ACM (CACM'3)* 46, 5 (2003), 35–39.

[7] Daming D. Chen, Manuel Egele, Maverick Woo, and David Brumley. 2016. Towards Automated Dynamic Analysis for Linux-based Embedded Firmware. In *Network and Distributed System Security Symposium (NDSS'16)*. 1–16.

[8] Aldo Cortesi, Maximilian Hils, Thomas Kriechbaumer, and contributors. 2010. Mitmproxy: A Free and Open Source Interactive HTTPS Proxy. https://mitmproxy.org/ [Version 9.0].

[9] Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. 2014. A Large-scale Analysis of the Security of Embedded Firmwares. In *USENIX Security Symposium (USENIX Security)*. 95–110.

[10] Ang Cui, Michael Costello, and Salvatore J Stolfo. 2013. When Firmware Modifications Attack: A Case Study of Embedded Exploitation. In *Network and Distributed System Security Symposium (NDSS'13)*. 1–13.

[11] Ang Cui and Salvatore J. Stolfo. 2010. A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-area Scan. In *Annual Computer Security Applications Conference (ACSAC'10)*. 97–106.

[12] Joseph Davies. 2007. The Cable Guy IPv6 Autoconfiguration in Windows Vista. https://learn.microsoft.com/en-us/previous-versions/technet-magazine/cc137983(v=msdn.10)?redirectedfrom=MSDN.

[13] Danny Dolev and Andrew Yao. 1983. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory (TIT)* 29, 2 (1983), 198–208.

[14] Doaa Farouk Badawy Eldesouky. 2013. Visual Hierarchy and Mind Motion in Advertising Design. *Journal of Arts and Humanities* 2, 2 (2013), 148–162.

[15] Mohamed Elsabagh, Ryan Johnson, Angelos Stavrou, Chaoshun Zuo, Qingchuan Zhao, and Zhiqiang Lin. 2020. FIRMSCOPE: Automatic Uncovering of Privilege-Escalation Vulnerabilities in Pre-Installed Apps in Android Firmware. In *USENIX Security Symposium (USENIX Security)*. 2379–2396.

[16] Shadi Esnaashari, Ian Welch, and Peter Komisarczuk. 2013. Determining Home Users' Vulnerability to Universal Plug and Play (UPnP) Attacks. In *International Conference on Advanced Information Networking and Applications Workshops (WAINA'13)*. 725–729.

[17] Andrew Fasano, Tiemoko Ballo, Marius Muench, Tim Leek, Alexander Bulekov, Brendan Dolan-Gavitt, Manuel Egele, Aurélien Francillon, Long Lu, Nick Gregory, Davide Balzarotti, and William Robertson. 2021. SoK: Enabling Security Analyses of Embedded Systems via Rehosting. In *ACM Asia Conference on Computer and Communications Security (ASIACCS'21)*. 687–701.

[18] FileZilla. 2023. FileZilla - The Free FTP Solution. https://filezilla-project.org/.

[19] Jason Fitzpatrick. 2022. Use a Wi-Fi Guest Network? Check These Settings. https://www.howtogeek.com/832507/use-a-wi-fi-guest-network-check-these-settings/.

[20] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. In *Annual International Workshop on Selected Areas in Cryptography (SAC'1)*. 1–24.

[21] Dennis Giese and Guevara Noubir. 2021. Amazon Echo Dot or the Reverberating Secrets of IoT Devices. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'21)*. 13–24.

[22] Baptiste Gourdin, Chinmay Soman, Hristo Bojinov, and Elie Bursztein. 2011. Toward Secure Embedded Web Interfaces. In *USENIX Security Symposium (USENIX Security)*. 17–32.

[23] Hilt, Stephen and Merces, Fernando. 2021. VPNFilter Two Years Later: Routers Still Compromised. https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.

[24] Justin T. Ho, David Dearman, and Khai N. Truong. 2010. Improving Users' Security Choices on Home Wireless Networks. In *Symposium on Usable Privacy and Security (SOUPS'10)*. 1–12.

[25] Chris Hoffman. 2013. Wi-Fi Protected Setup (WPS) is Insecure: Here's Why You Should Disable It. https://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/.

[26] Michael Horowitz. 2015. Linksys Smart Wi-Fi Makes A Stupid Guest Network. https://www.computerworld.com/article/2940566/linksys-smart-wi-fi-makes-a-stupid-guest-network.html.

[27] Michael Horowitz. 2015. Router Security. https://www.routersecurity.org/checklist.php.

[28] Amanda Hsu, Frank Li, and Paul Pearce. 2023. Fiat Lux: Illuminating IPv6 Apportionment with Different Datasets. In *ACM international conference on Measurement and modeling of computer systems (SIGMETRICS'23)*. 1–24.

[29] IEEE. 2021. IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)* (2021), 1–4379.

[30] Philipp Jeitner, Haya Shulman, Lucas Teichmann, and Michael Waidner. 2022. XDRI Attacks - and - How to Enhance Resilience of Residential Routers. In *USENIX Security Symposium (USENIX Security)*. 4473–4490.

[31] Davino Mauro Junior, Luis Melo, Harvey Lu, Marcelo d'Amorim, and Atul Prakash. 2019. Beware of the App! On the Vulnerability Surface of Smart Devices through their Companion Apps. arXiv:1901.10062 [cs.CR]

[32] kaklakariada. 2015. UPnP PortMapper. https://github.com/kaklakariada/portmapper.

[33] Mingeun Kim, Dongkwan Kim, Eunsoo Kim, Suryeon Kim, Yeongjin Jang, and Yongdae Kim. 2020. FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis. In *Annual Computer Security Applications Conference (ACSAC'20)*. 733–745.

[34] Eric Klein, Gunter Van de Velde, Ralph Droms, Tony L. Hain, and Brian E. Carpenter. 2007. Local Network Protection for IPv6. https://www.rfc-editor.org/info/rfc4864.

[35] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. 2019. All Things Considered: An Analysis of IoT Devices on Home Networks. In *USENIX Security Symposium (USENIX Security)*. 1169–1185.

[36] Peiyu Liu, Shouling Ji, Lirong Fu, Kangjie Lu, Xuhong Zhang, Jingchang Qin, Wenhai Wang, and Wenzhi Chen. 2023. How IoT Re-using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT Devices. In *IEEE Symposium on Security and Privacy (S&P'23)*. 1845–1861.

[37] Eduardo Novella Lorente, Carlo Meijer, and Roel Verdult. 2015. Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers. In *USENIX Workshop on Offensive Technologies (WOOT'15)*. 1–13.

[38] Pratyusa K Manadhata and Jeannette M Wing. 2010. An Attack Surface Metric. *IEEE Transactions on Software Engineering (TSE'10)* 37, 3 (2010), 371–386.

[39] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *USENIX Security Symposium (USENIX Security)*. 1093–1110.

[40] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. 2022. "As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication. In *Symposium on Usable Privacy and Security (SOUPS'22)*. 483–501.

[41] MarketWatch. 2023. Home Wireless Router Market Size 2023-2030 | Detailed Analysis of Market Size and Growth Rate. https://www.marketwatch.com/press-release/home-wireless-router-market-size-2023-2030-detailed-analysis-of-market-size-and-growth-rate-2023-05-08.

[42] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In *Conference on Human Factors in Computing Systems (CHI'21)*. 1–18.

[43] B.A. Miller, T. Nixon, C. Tai, and M.D. Wood. 2001. Home Networking with Universal Plug and Play. *IEEE Communications Magazine (IEEE COMMUN MAG)* 39, 12 (2001), 104–109.

[44] Austin Murdock, Frank Li, Paul Bramsen, Zakir Durumeric, and Vern Paxson. 2017. Target Generation for Internet-wide IPv6 Scanning. In *Internet Measurement Conference (IMC'17)*. 242–253.

[45] David Murphy. 2020. You Need to Lock Down Your Router's Remote Management Options. https://lifehacker.com/you-need-to-lock-down-your-routers-remote-management-op-1842525275.

[46] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces. *Queue* 18, 2 (2020), 67–92.

[47] Dr. Thomas Narten, Richard P. Draves, and Suresh Krishnan. 2007. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. https://www.rfc-editor.org/info/rfc4941.

[48] Marcus Niemietz and Joerg Schwenk. 2015. Owning Your Home Network: Router Security Revisited. arXiv:1506.04112 [cs.CR]

[49] Nmap. 2023. Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/.

[50] Norbert Nthala and Ivan Flechais. 2018. Rethinking Home Network Security. In *European Workshop on Usable Security (EuroUSEC'18)*. 1–11.

[51] Timo Ojala, Vassilis Kostakos, Hannu Kukka, Tommi Heikkinen, Tomas Linden, Marko Jurmu, Simo Hosio, Fabio Kruger, and Daniele Zanni. 2012. Multipurpose Interactive Public Displays in the Wild: Three Years Later. *Computer* 45, 5 (2012), 42–49.

[52] James O'Flaherty. 2012. Hierarchy – What Do You Want People to See? Where Do You Want Them to Go? https://www.datadial.net/blog/hierarchy-what-do-you-want-people-to-see-where-do-you-want-them-to-go/.

[53] Petrosyan, Ani. 2023. Number of Internet and Social Media Users Worldwide as of April 2023. https://www.statista.com/statistics/617136/digital-population-worldwide/.

[54] Sarah Prange, Niklas Thiem, Michael Fröhlich, and Florian Alt. 2022. "Secure Settings Are Quick and Easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. In *International Conference on Advanced Visual Interfaces (AVI'22)*. 1–9.

[55] Z. Cliffe Schreuders and Adil M. Bhat. 2013. Not all ISPs equally secure home users: An empirical study comparing Wi-Fi security provided by UK ISPs. In *International Conference on Security and Cryptography (SECRYPT'13)*. 1–6.

[56] Ax Sharma. 2020. D-Link Blunder: Firmware Encryption Key Exposed in Unencrypted Image. https://www.bleepingcomputer.com/news/security/d-link-blunder-firmware-encryption-key-exposed-in-unencrypted-image/.

[57] Shodan. 2023. Shodan. https://www.shodan.io/.

[58] Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. 2015. Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware. In *Network and Distributed System Security Symposium (NDSS'15)*. 1–15.

[59] Chris McMahon Stone, Tom Chothia, and Joeri de Ruiter. 2018. Extending Automated Protocol State Learning for the 802.11 4-Way Handshake. In *European Symposium on Research in Computer Security (ESORICS'18)*. 325–345.

[60] Patryk Szewczyk and Rose Macdonald. 2017. Broadband Router Security: History, Challenges and Future Implications. *Journal of Digital Forensics, Security and Law (JDFSL'17)* 12, 4 (2017), 55–74.

[61] t6x. 2015. reaver-wps-fork-t6x. https://github.com/t6x/reaver-wps-fork-t6x.

[62] Taylor, Petroc. 2023. Households with Internet Access Worldwide 2019, by Region. https://www.statista.com/statistics/249830/households-with-internet-access-worldwide-by-region/.

[63] Erik Tews and Martin Beck. 2009. Practical attacks against WEP and WPA. In *ACM conference on Wireless network security (WiSec'09)*. 79–86.

[64] Mathy Vanhoef. 2021. Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. In *USENIX Security Symposium (USENIX Security)*. 161–178.

[65] Mathy Vanhoef and Frank Piessens. 2017. Key reinstallation attacks: Forcing nonce Reuse in WPA2. In *ACM SIGSAC Conference on Computer and Communications Security (CCS'17)*. 1313–1328.

[66] Mathy Vanhoef and Frank Piessens. 2018. Release The Kraken: New Kracks in the 802.11 Standard. In *ACM SIGSAC Conference on Computer and Communications Security (CCS'18)*. 299–314.

[67] Mathy Vanhoef and Eyal Ronen. 2020. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *IEEE Symposium on Security and Privacy (S&P'20)*. 517–533.

[68] Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. 2022. A Large-scale Analysis of Wi-Fi Passwords. *Journal of Information Security and Applications (JISA'22)* 67 (2022), 103190.

[69] Stefan Viehböck. 2011. Brute Forcing Wi-Fi Protected Setup. https://www.cs.cmu.edu/~rdriley/330/papers/viehboeck_wps.pdf.

[70] Vasaka Visoottiviseth, Pongnapat Jutadhammakorn, Natthamon Pongchanchai, and Pongjarun Kosolyudhthasarn. 2018. Firmaster: Analysis Tool for Home Router Firmware. In *International Joint Conference on Computer Science and Software Engineering (JCSSE'18)*. 1–6.

[71] Dingding Wang, Muhui Jiang, Rui Chang, Yajin Zhou, Baolei Hou, Xiapu Luo, Lei Wu, and Kui Ren. 2021. A Measurement Study on the (In)security of End-of-Life (EoL) Embedded Devices. arXiv:2105.14298 [cs.CR]

[72] Sean Whalen, Sophie Engle, and Dominic Romeo. 2001. An Introduction to ARP Spoofing. https://api.semanticscholar.org/CorpusID:59638215.

[73] James Woodyatt. 2011. Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service. https://www.rfc-editor.org/info/rfc6092.

[74] Yu Zhang, Wei Huo, Kunpeng Jian, Ji Shi, Longquan Liu, Yanyan Zou, Chao Zhang, and Baoxu Liu. 2019. SRFuzzer: An Automatic Fuzzing Framework for Physical SOHO Router Devices to Discover Multi-Type Vulnerabilities. In *Annual Computer Security Applications Conference (ACSAC'19)*. 544–556.

[75] Binbin Zhao, Shouling Ji, Wei-Han Lee, Changting Lin, Haiqin Weng, Jingzheng Wu, Pan Zhou, Liming Fang, and Raheem Beyah. 2022. A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. *IEEE Transactions on Dependable and Secure Computing (TDSC'22)* 19, 3 (2022), 1826–1840.

[76] ZOL. 2023. 2023 Wireless Router Brand Rankings. (in Chinese) https://top.zol.com.cn/compositor/227/manu_attention.html.

[77] Zoomeye. 2023. Zoomeye. https://zoomeye.org/.

A SOURCE OF DEFAULT WI-FI PASSWORD IN TP-LINK TL-WR940N

```
int sub_4A2844(){
  //...
  int v1 = 0;
  if ( usrconf_bManufactory() > 0){
    HTTP_DEBUG_PRINT("ucWlan.c:722", "load Manufactory configure!");
    *(dword_5F0460 + 0xE0) = getMFWLAN_chan_width();
    if ( readPinFlash() < 0 || !swWlanWpsCheckPIN(dword_5F046C + 8, v61) ){
      *(dword_5F046C + 0x8) = '1234';
      *(dword_5F046C + 0xC) = '5670';
    }
    sscanf(dword_5F046C + 0x8, "%d", &v1);
    *(dword_5F0460 + 0xD0) = v1 % 9 + 2; // save pwd to dword_5F0460
    // Finally, "12345670" is saved to dword_5F0464
    //...
  }
}
// sub_44AD58 call swWlanSecurityCfgGet to set httpWlanSecCfg_newForAp from dword_5F0464
int sub_46AC18(int a1, int a2){
  //...
  int v1[95],v2[120],v3[84];
  if ( !httpGetEnv(a2, "Next") ){
    if ( !httpGetEnv(a2, "Return") ){
      memcpy(v1, &httpWlanBasicCfg_newForAp, sizeof(v1));
      memcpy(v2, &httpWlanModeCfg_newForAp, sizeof(v2));
      memcpy(v3, &httpWlanSecCfg_newForAp, sizeof(v3));
      OUTPUT_ARRAY_HEAD(a2, "wzdWlanInf", 0, 1);
      //...
      writePageParamSet(a2, "\"%s\",", (const char *)&v3[40]);
      //...
      // wzdWlanInf[17] get default password from httpWlanSecCfg_newForAp
    }
  }
}
// Finally, WzdWlanRpm.htm get default password from wzdWlanInf[17]
```

Listing 2: Decompiled code of the funtions that set default Wi-Fi password from Flash in the firmware of TP-Link TL-WR940N

B AN EXAMPLE OF SETUP WIZARD

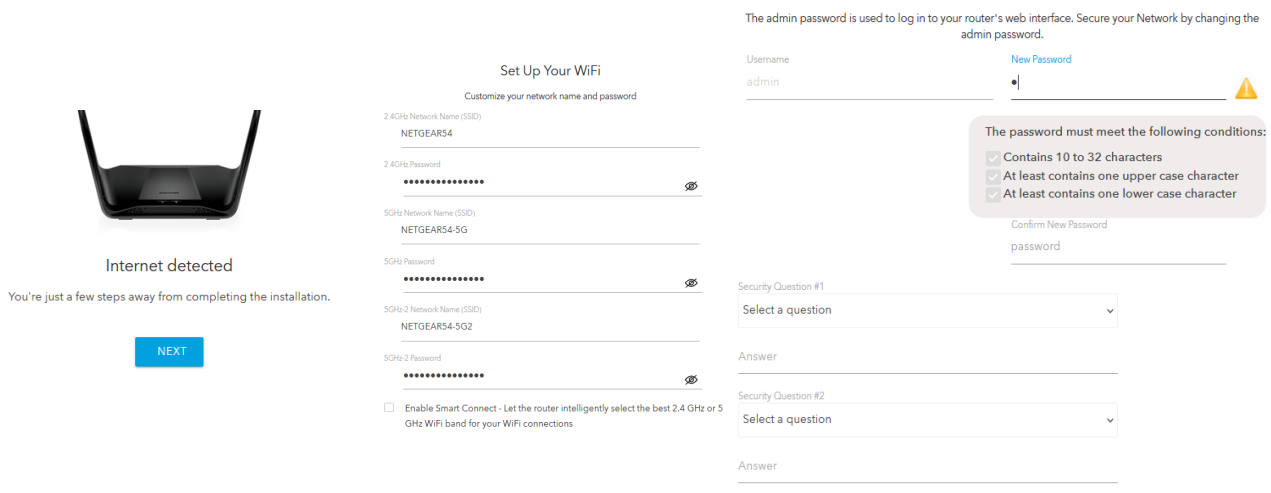

Figure 6: Setup Wizard detecting the Internet and configuring network automatically (Left), guiding user to set Wi-Fi password (Middle), guiding user to set administration password (Right)

C STATISTICS OF ANALYSIS RESULTS

Table 4: The statistical results of analysis results. The statistical results of each item are in parentheses after it.

Items	Attributes	Situations				
Wi-Fi security protocol	Default Wi-Fi security protocols	WPA/WPA2-TKIP&CCM (2)	WPA/WPA2-CCMP (13)	WPA2-CCMP (25)		
	Consistency between UI and reality	Not consistent (0)	Consistent (40)			
Setup wizard	Plug and play	Supported (12)	Not supported (28)			
	Skip setup wizard	No setup wizard (1)	Supported (8)	Not supported (31)		
Wi-Fi and administration password settings	Default Wi-Fi password	NULL (19)	Same as WPS PIN (3)	Randomly generated (18)		
	Must change Wi-Fi SSID	No (32)	Yes (7)			
	Must change Wi-Fi password	No (18)	Yes (21)			
	Wi-Fi password strength meter	No (21)	Yes (18)			
	Wi-Fi password strength requirements	At least 8 characters (5)	8-16 characters (1)	8-32 characters (2)	8-63 characters (31)	
	Default admin password	NULL (22)	Hard-coded (6)	Same as Wi-Fi password (10)	Randomly generated (2)	
	Must change admin username	No (36)	Yes (3)			
	Must change admin password	No (15)	Yes (24)			
	Admin password strength meter	No (19)	Yes (20)			
	Minimum length of admin password	1 character (8)	5 characters (7)	6 characters (13)	8 characters (10)	10 characters (1)
	Admin password strength requirements	At least one number (3)	At least one letter (1)	At least 2 types of characters (3)	Upper and lowercase letters (2)	No more than two identical characters in a row (5)
Firmware update	Setup wizard reminds users to update	No (28)	Force update (1)	Remind update (5)	Remind update/recommend (4)	Latest (2)
	Automatic update	Not supported (12)	Disabled (6)	Enabled (22)		
	Trigger self update	Not supported (3)	Supported (37)			
	Settings change or reset after update	Can't update firmware (17)	No (23)	Yes (0)		
	Communication security (check version)	HTTPS/no validation (9)	HTTPS/validation (19)	HTTP (7)	Custom Protocol/plaintext (2)	Custom Protocol/encoded (0)
	Communication security (download firmware)	Can't update firmware (17)	HTTPS/validation (9)	HTTP (7)	HTTPS/no validation (5)	Custom Protocol (2)
Open ports	The number on the WAN	0 (40)	1-5 (0)	5+ (0)		
	The number on the LAN	0 (0)	1-5 (22)	5+ (18)		
Local web access	HTTP/HTTPS support	Only HTTP (21)	Only HTTPS (0)	HTTP&HTTPS (19)		
	Limit for password attempts	No (15)	Yes (25)			
	CAPTCHA	No (36)	Yes (4)			
Telnet	Telnet support on UI	Not supported (37)	Disabled (3)	Enabled (0)		
	Telnet (LAN, WAN)	Not supported (35)	Only LAN (5)	Only WAN (0)	LAN&WAN (0)	
	Default username/password	Unknown (1)	Hard-coded (0)	Same as admin password (4)	Randomly generated (0)	
SSH	SSH support on UI	Not supported (37)	Disabled (3)	Enabled (0)		
	SSH (LAN, WAN)	Not supported (33)	Only LAN (4)	Only WAN (0)	LAN&WAN (3)	
	Default username/password	Unknown (1)	Hard-coded (0)	Same as admin password (6)	Randomly generated (0)	
UPnP	UPnP support on UI	Not supported (1)	Disabled (8)	Enabled (31)		
	Add UPnP port mapping (LAN)	Can't connect (8)	Can't add (11)	Can add (20)		
	Add UPnP port mapping (WAN)	Can't connect (39)	Can't add (0)	Can add (0)		
Guest network	Guest network support on UI	Not supported (3)	Disabled (36)	Enabled (1)		
	Default guest password	NULL (23)	Hard-coded (8)	Randomly generated (6)		
	Must change guest password	No (36)	Yes (1)			
	Guest password strength meter	No (30)	Yes (7)			
	Guest password strength requirements	4-32 characters (5)	At least 8 characters (2)	8-16 characters (1)	8-63 characters (29)	
	Default Wi-Fi security protocols	Open (28)	WPA/WPA2-TKIP&CCMP (1)	WPA/WPA2-CCMP (3)	WPA2-CCMP (5)	
	Guest network mode	Captive portal mode (5)	Normal mode (32)			
	Can access management page	No (34)	Yes (3)			
WPS	WPS support on UI	Not supported (13)	Push button (27)	Client PIN code (19)	Router PIN code/disabled (0)	Router PIN code/enabled (16)
	WPS status	"No" (6)	"Not Configured" (0)	"Locked" (3)	"Configured" (31)	
	Can find WPS PIN code on the label or UI	No (21)	Yes (19)			
	Feasibility of brute force attack	No (8)	Yes (23)			
	Limit for WPS PIN code attempts	No (0)	Yes (23)			
IPv6	IPv6 support on UI	Not supported (3)	Disabled (26)	Enabled (11)		
	IPv6 addresses assignment method	SLAAC (0)	Stateful DHCPv6 (12)	Stateless DHCPv6 (25)		
	IPv6 NAT	IPv6 can't work (12)	No (24)	Yes (1)		
	IPv6 firewall	IPv6 can't work (12)	Not block (5)	Block (20)		
External storage	External storage support on UI	Not supported (27)	Supported (13)			
	SMB	Not supported (0)	Disabled/no authentication (1)	Disabled/authentication (1)	Enabled/no authentication (9)	Enabled/authentication (2)
	Local HTTP access	Not supported (8)	Disabled/no authentication (0)	Disabled/authentication (0)	Enabled/no authentication (5)	Enabled/authentication (0)
	Local HTTPS access	Not supported (8)	Disabled/no authentication (0)	Disabled/authentication (0)	Enabled/no authentication (5)	Enabled/authentication (0)
	Local FTP	Not supported (0)	Disabled/no authentication (6)	Disabled/authentication (5)	Enabled/no authentication (0)	Enabled/authentication (2)
	Remote HTTP access	Not supported (13)	Disabled/no authentication (0)	Disabled/authentication (0)	Enabled/no authentication (0)	Enabled/authentication (0)
	Remote HTTPS access	Not supported (8)	Disabled/no authentication (0)	Disabled/authentication (5)	Enabled/no authentication (0)	Enabled/authentication (0)

Table 4: The statistical results of analysis results. The statistical results of each item are in parentheses after it.

Items	Attributes	Situations				
	Self-signed TLS certificate (HTTPS)	No (1)	Yes (4)			
	Version of TLS (HTTPS)	v1.2 (1)	v1.3 (4)			
	Remote FTP	Not supported (3)	Disabled/no authentication (0)	Disabled/authentication (10)	Enabled/no authentication (0)	Enabled/authentication (0)
	Self-signed TLS certificate (FTP)	Not over TLS (9)	No (0)	Yes (1)		
	Version of TLS (FTP)	Not over TLS (9)	v1.2 (0)	v1.3 (1)		
	Default username/password	Hard-coded (3)	Same as admin password (10)	Randomly generated (0)		
Cloud account	Cloud account support on UI	Not supported (35)	Supported (5)			
	Minimum length of account password	6 characters (8)	8 characters (3)	10 characters (2)		
	Account password strength requirements	At least one number (7)	At least one special character (2)	At least 2 types of characters (2)	Upper and lowercase letters (7)	
	Supported functions of cloud account	Web access (3)	App (13)	DDNS (3)		
	Communication security (login account on UI)	HTTP (0)	HTTPS/no validation (0)	HTTPS/validation (5)	Custom Protocol/plaintext (0)	Custom Protocol/encoded (0)
Companion App	App support on UI	Not supported (11)	Supported (29)			
	Supported communication methods	Over Wi-Fi (29)	Over the Internet (25)			
	Remotely manage the router	Not supported (4)	Disabled (3)	Enabled (22)		
	Communication security (bind)	HTTP (0)	HTTPS/no validation (0)	HTTPS/validation (23)	Custom Protocol/plaintext (2)	Custom Protocol/encoded (0)
	Communication security (remote management)	HTTP (0)	HTTPS/no validation (1)	HTTPS/validation (16)	Custom Protocol/plaintext (2)	Custom Protocol/encoded (6)
Remote web access	Remote web access support on UI	Not supported (24)	Disabled (16)	Enabled (0)		
	HTTP/HTTPS support	Only HTTP (5)	Only HTTPS (10)	HTTP&HTTPS (0)	Set by users (1)	
	Self-signed TLS certificate (HTTPS)	No (2)	Yes (12)			
	Version of TLS (HTTPS)	v1.2 (8)	v1.3 (6)			
Reset	Reset options	Not supported (33)	Supported (7)			
	Retain sensitive information after reset	No (31)	Yes (9)			