New Way To Protect WiFi Network From Hackers
-- Specification --

Henry V. Pham

This specification is based on the original document of the invention "**New Way To Protect WiFi Network From Hackers"** with a trademark named **WiFi[+]Secured,** which was resubmitted on 2024/02/27 with the **U.S. Patent Number PCT/US24/17533** and **International Patent Number PCT/IB2024/000110.** The first U.S. only submission was on 2021/07/01 with Patent Number **29/788,607** and a U.S. Trademark Serial Number **90795366.** This invention is invented to protect the existing WiFi routers from hackers with multiple hacking holes like VPN access via computers, WiFi SSID password scan by hacked apps, and from many other sources that could leak the WiFi password. The existing WiFi routers come with default WiFi SSID broadcasting which attract the hackers to gain access into WiFi network easier. And every wireless device needs WiFi access with online storage like cameras with online account are easily leaking the WiFi SSID and WiFi Password. The WiFi router should have a random WiFi SSID and a random Password label along with a wallet-card for factory-key and owner-key labels that come with the WiFi router package. The WiFi SSID, WiFi Password, factory-key and owner-key should be in scan-able-code, barcode, QR-code or G-CODE labels. The **Authentication Owner** key contains WiFi SSID, WiFi Password, and the owner-key. The **Authentication User** key contains **only** WiFi SSID and WiFi Password. The "Press-and-Scan" button will allow the users to scan the G-CODE labels to have the Network access. To scan the WiFi SSID and the WiFi Password from the label, the users need to press and hold the "Press-and-Scan" button while scanning the label. However, for the owners accessing procedure, the device OS or WiFi application will ask to scan the owner-key to have persistent owners WiFi Network access. For appliances and small devices or security cameras using WiFi Network, the devices' providers can have an application to assign WiFi Network access to the devices and must follow the same **WiFi+Secured** protocol with WPS feature supported for user friendly and convenience. This is the first step to secure data for entire world; www.TheCloudOSCenter.com contains the most recent and more details about the Cloud OS for the new **World of Computing Infrastructure Modern** to solve the Data Secured Puzzle.

Figure-1 below, from the original invention document, shows a use case follow diagram of the **New Way To Protect WiFi Network From Hackers** with the procedure of a normal use case follow diagram when the users first time try to gain access to the WiFi router. The use case diagram shows the owners pressed the "Press-and-Scan" button and scan the **Authentication User** key dot code or G-CODE label on the router with successfully Network access, the WiFi application will ask the owners to scan the owner-key. After the WiFi application scanned the owner-key, the device OS or WiFi application will confirm this owner-key with the router. If owner key is successfully confirmed, the accessed devices will have the **persistent Network access**. If the users do not have the owner-key or scan an invalid owner-key, the users will have a **temporary Network access** but this Network access will be clear or removed by the router after three hours of inactive. **The WiFi[+]Secured Router Reference** section on the last page of this specification document shows **Figure-R1** – WiFi[+]Secured Router Reference sample drawing which is the symbol WiFi[+]Secured protocol router overview of this invention; note that this drawing was not in the original invention document.

New Way To Protect WiFi Network From Hackers
-- Specification --

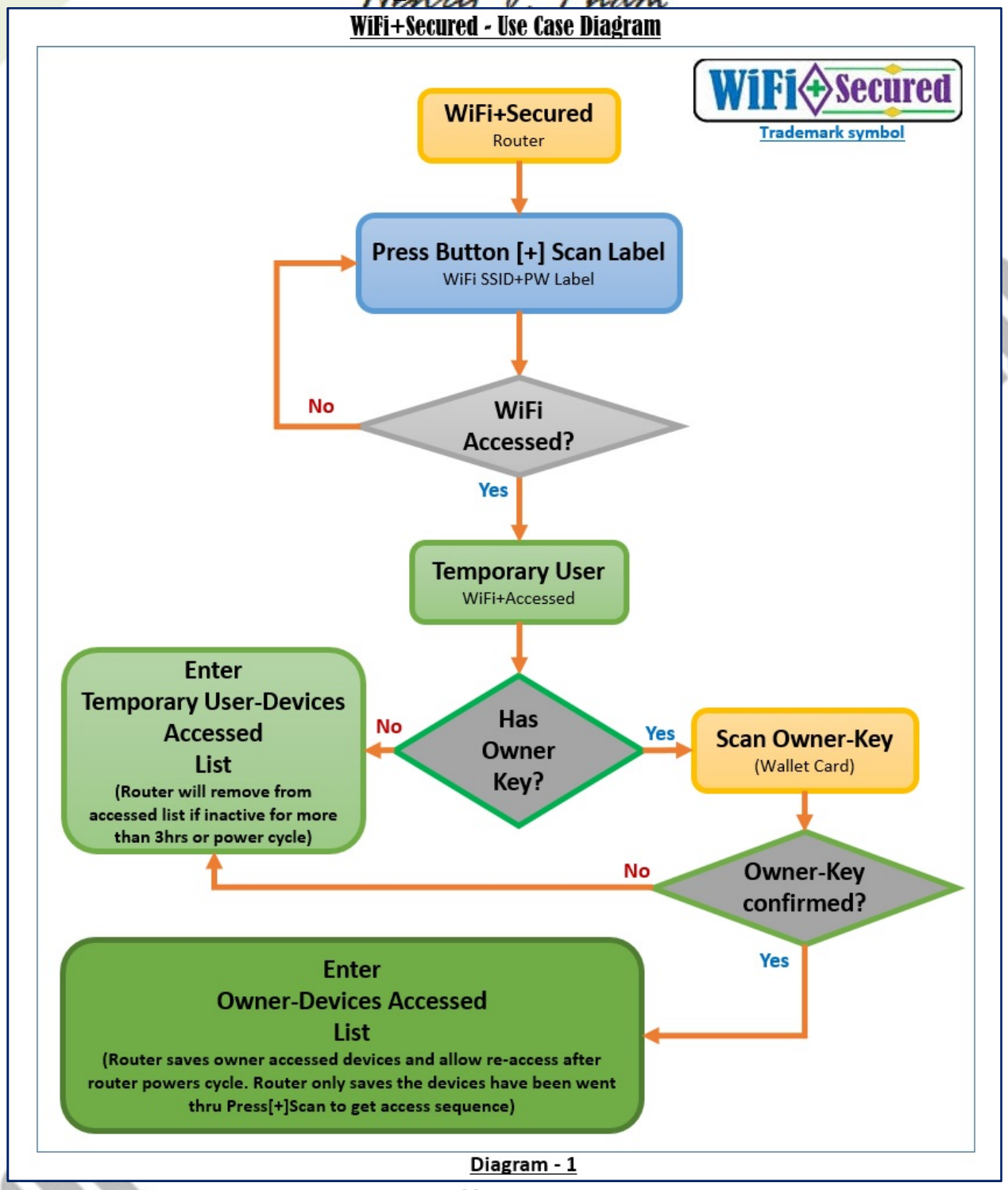


Figure-1: WiFi[+]Secured Use Case Diagram

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com

New Way To Protect WiFi Network From Hackers
-- Specification --

Henry V. Pham

Figure-2 from the original invention document shows a temporary user **Test Case 1** of the **New Way to Protect WiFi Network from Hackers** with the procedure to test **temporary accessed devices** with a power cycle to the WiFi router when the users first time (clean device) try to gain access to the WiFi router. The diagram shows that the device must be clean with no WiFi access yet, and then start with Press & Scan to have temporary access. After the test device has WiFi access and the WiFi router should add this device into the accessed list as expected. Then do a power cycle to the WiFi router, and confirm the test device has lost the WiFi access. This function is the WiFi router manufacture features needs to implement to ensure to pass this test case.

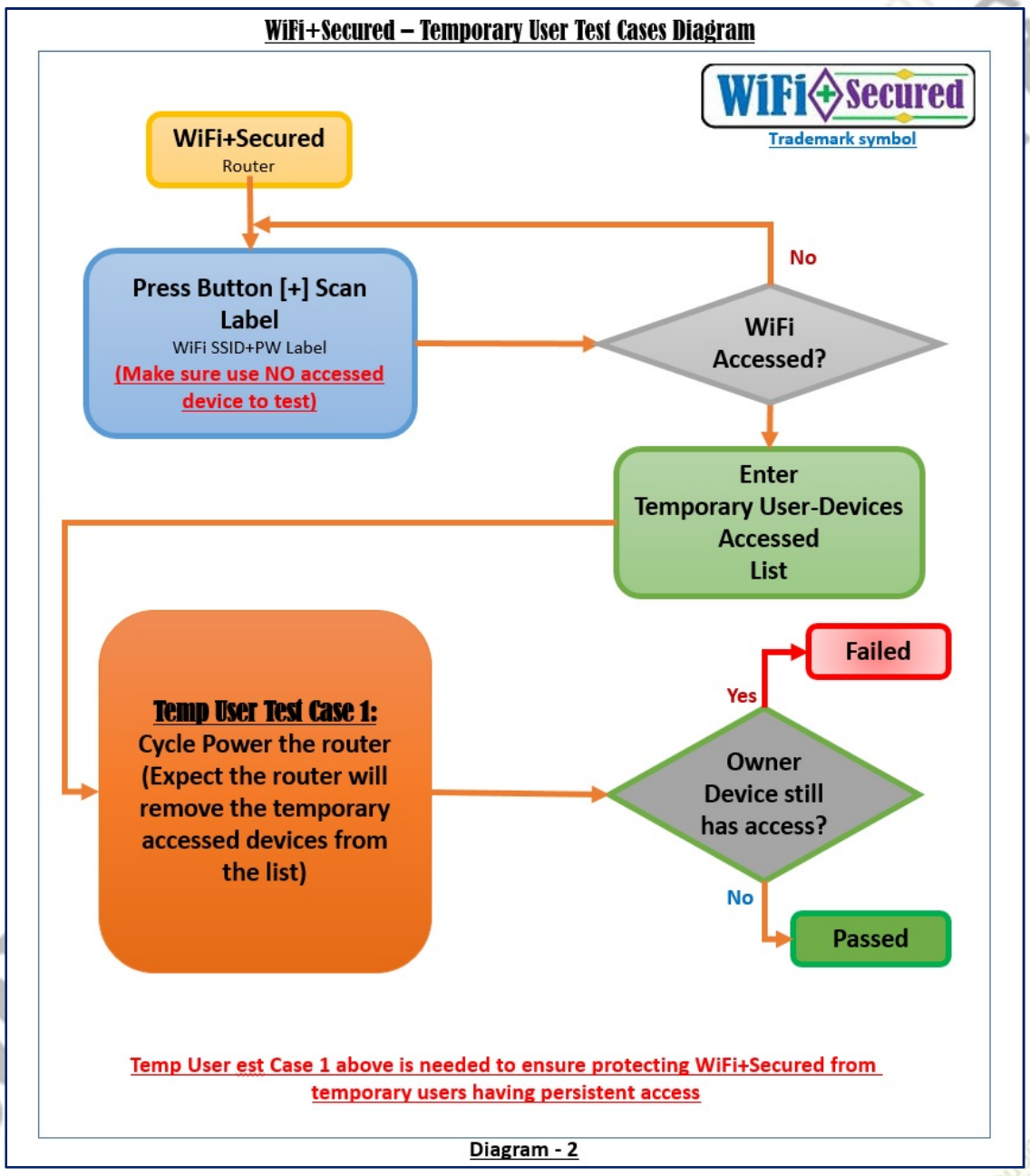


Figure-2: WiFi[+]Secured Temporary User Test Case-1 Diagram

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com

New Way To Protect WiFi Network From Hackers
-- Specification --

Henry V. Pham

Figure-3 from the original invention document shows a temporary user **Test Case 2** of the **New Way to Protect WiFi Network from Hackers** with the procedure to test **temporary accessed devices** with an inactivity timeout test when the users first time (clean device) try to gain access to the WiFi router. The diagram shows that the device must be clean with no WiFi access yet, and then start with Press & Scan to have temporary access. After the test device has WiFi access and the WiFi router should add this device into the accessed list as expected. Then turn off the test device and wait for 3 hours, and turn the test device back on to confirm the test device has lost the WiFi access. This function is the WiFi router manufacture features needs to implement to ensure to pass this test case. Note that the inactive timeout can be configured to 1h, 2h, and 3h if the manufacture provided; but the default inactive timeout should be 3 hours as required in this invention.

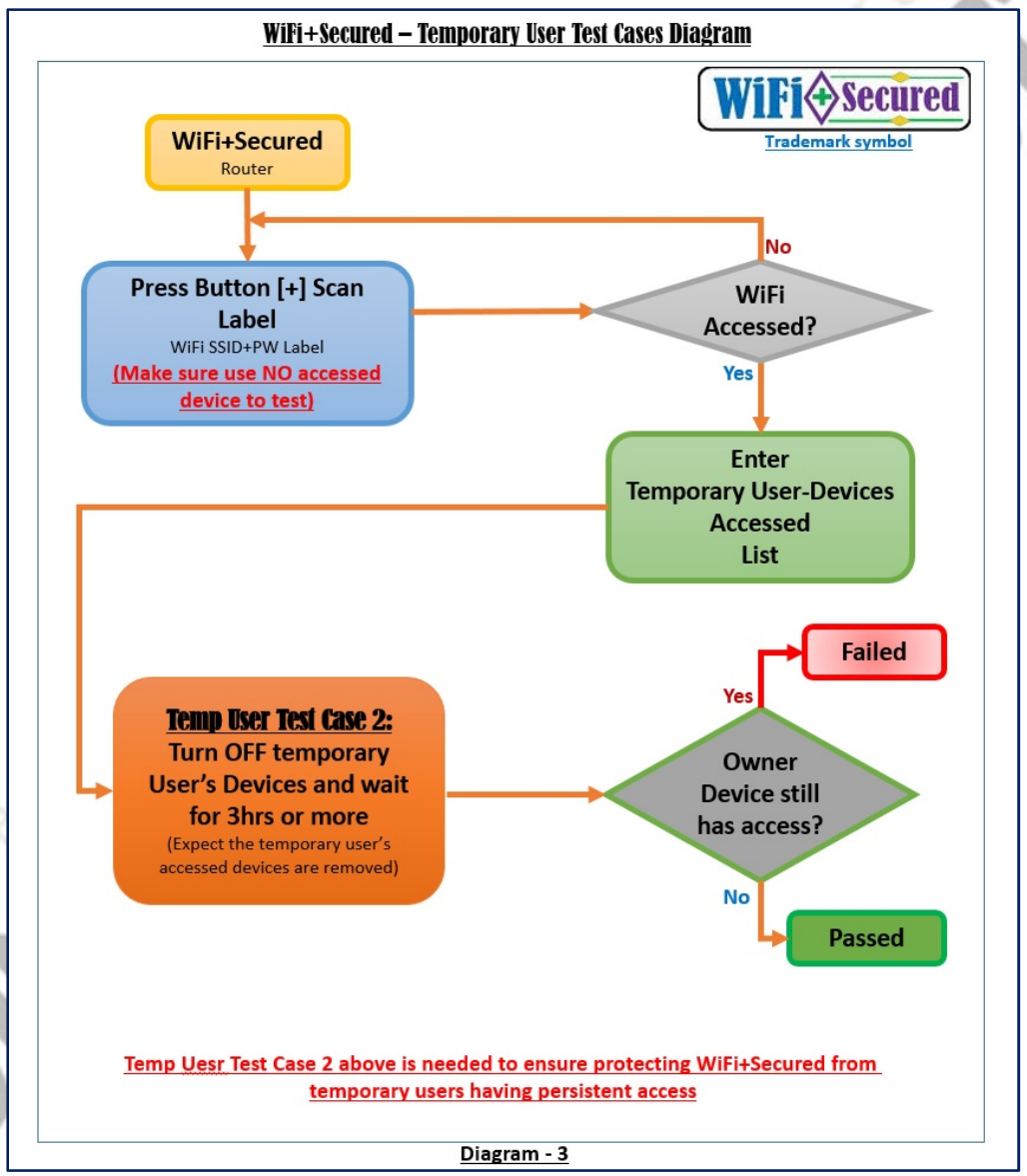


Figure-3: WiFi[+]Secured Temporary User Test Case-2 Diagram

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com

New Way To Protect WiFi Network From Hackers
-- Specification --

Figure-4 from the original invention document shows the owner test cases (**Power Cycle** and **Reprogram Owner Key**) of the **New Way to Protect WiFi Network from Hackers** with the procedure to test **owner accessed devices** with a power cycle to the WiFi router and reprogram Owner Key test when the owner devices already access to the WiFi router. With the procedures on the follow diagram below, after the owner test device already went through Press & Scan with owner key to have WiFi access, cycle power the WiFi router and confirm the owner device still have WiFi access to pass the **Test Case 1** in this figure. After the owner device passed test case 1 above, then reprogram the Owner Key with different code of new the SSID and WiFi Password which can be contained in a dot matrix code or G-CODE label for test case 2. After programmed the WiFi router with new WiFi SSID and WiFi Password, then confirm the test device should drop out of the WiFi access and make sure to reconfirm **Test Case 2** with a rebooting of the test device. The WiFi router manufacture should provide an application for the user to reprogram the SSID and WiFi Password. Note that the G-CODE Utility app already provides a text data combination of two text codes to generate a G-CODE Label to support reprogramming with new G-CODE Label that the users can do by themselves. The G-CODE Utility app and the G-CODE Invention documents are posted with details on the www.TheCloudOSCenter.com and www.TheGCODECreator.com.

Figure-5 from the original invention document shows the owner test cases (**Power Cycle** and **Reset Owner Key**) of the **New Way to Protect WiFi Network from Hackers** with the procedure to test **owner accessed devices** with a power cycle to the WiFi router and reset Owner Key test when the owner devices already access to the WiFi router. With the procedures on the follow diagram below, after the owner test device already went through Press & Scan with owner key to have WiFi access, cycle power the WiFi router and confirm the owner device still have WiFi access to pass the **Test Case 1** in this figure. After the owner device passed test case 1 above, then reset the Owner Key to confirm **Test Case 3** and expect the WiFi router reset to factory with default factory owner key and the test device lost out of WiFi access after reset. Then make sure to confirm the test device should drop out of the WiFi access and make sure to reconfirm **Test Case 2** with a rebooting of the test device

The WiFi router would come with a Reset Owner Key button, Press & Scan button and the trademark image symbol **WiFi[+]Secured** with U.S. Trademark Serial Number **90795366,** above or below the Press & Scan button with clear visibility to prove the users a certified **WiFi[+]Secured** protocol WiFi router. With this new invention, the Family-Client-Network and Business-Client-Network are worry-free from the hackers gaining access into their WiFi Networks. **WiFi+Secured** for Family-Client-Network are hidden from the neighbors and unwanted users. **WiFi+Secured** for Business-Client-Network are more secured and only allow access to the customers when they are in the business like Starbucks, Coffee stores, Restaurants, and small customer service businesses. This new **WiFi+Secured** Network protection will be even more secured for large business or corporate if they are sharing offices in the same building.

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com

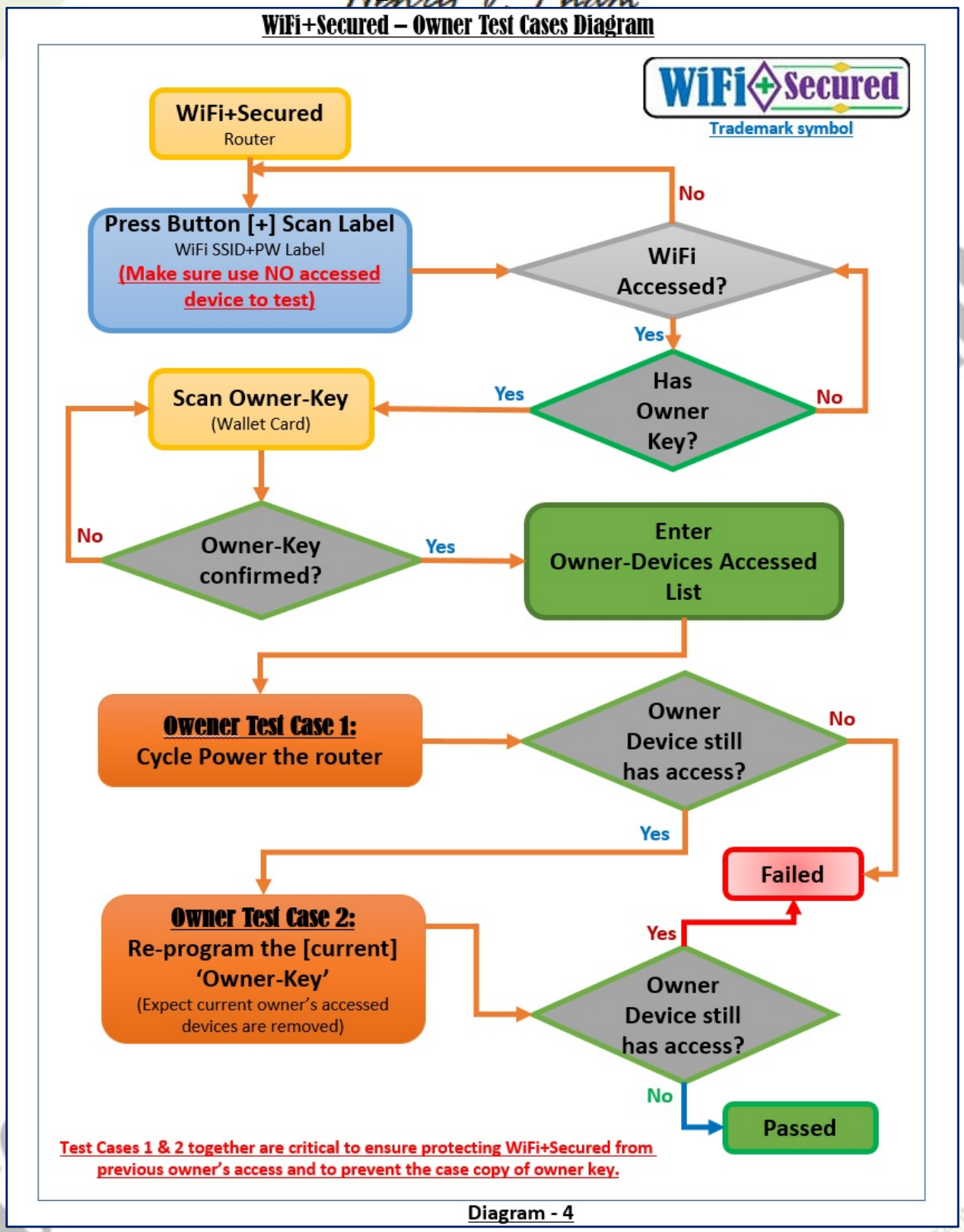


Figure-4: WiFi[+]Secured Test Case 1 & 2 Diagram

WiFi+Secured – Owner Test Cases Diagram

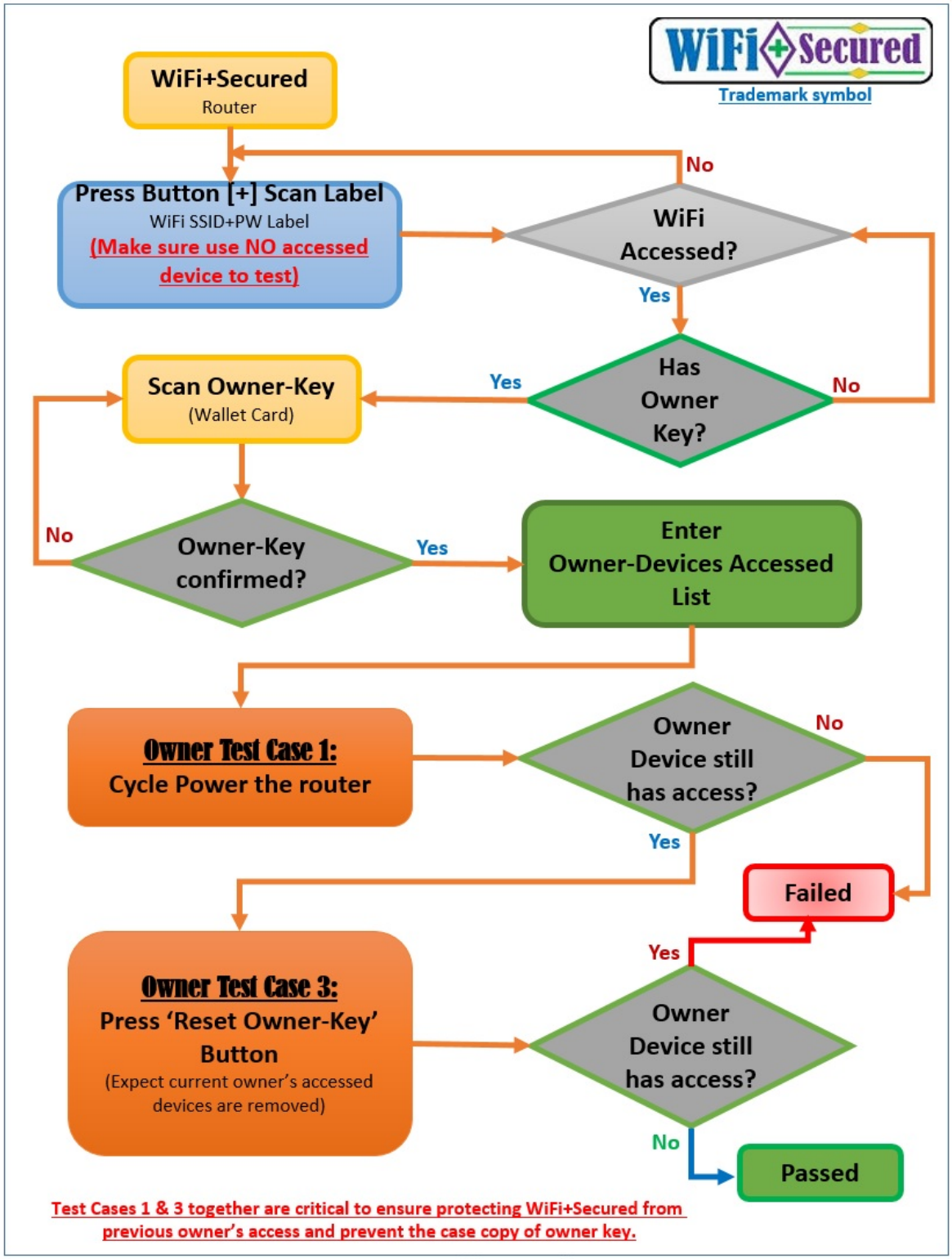


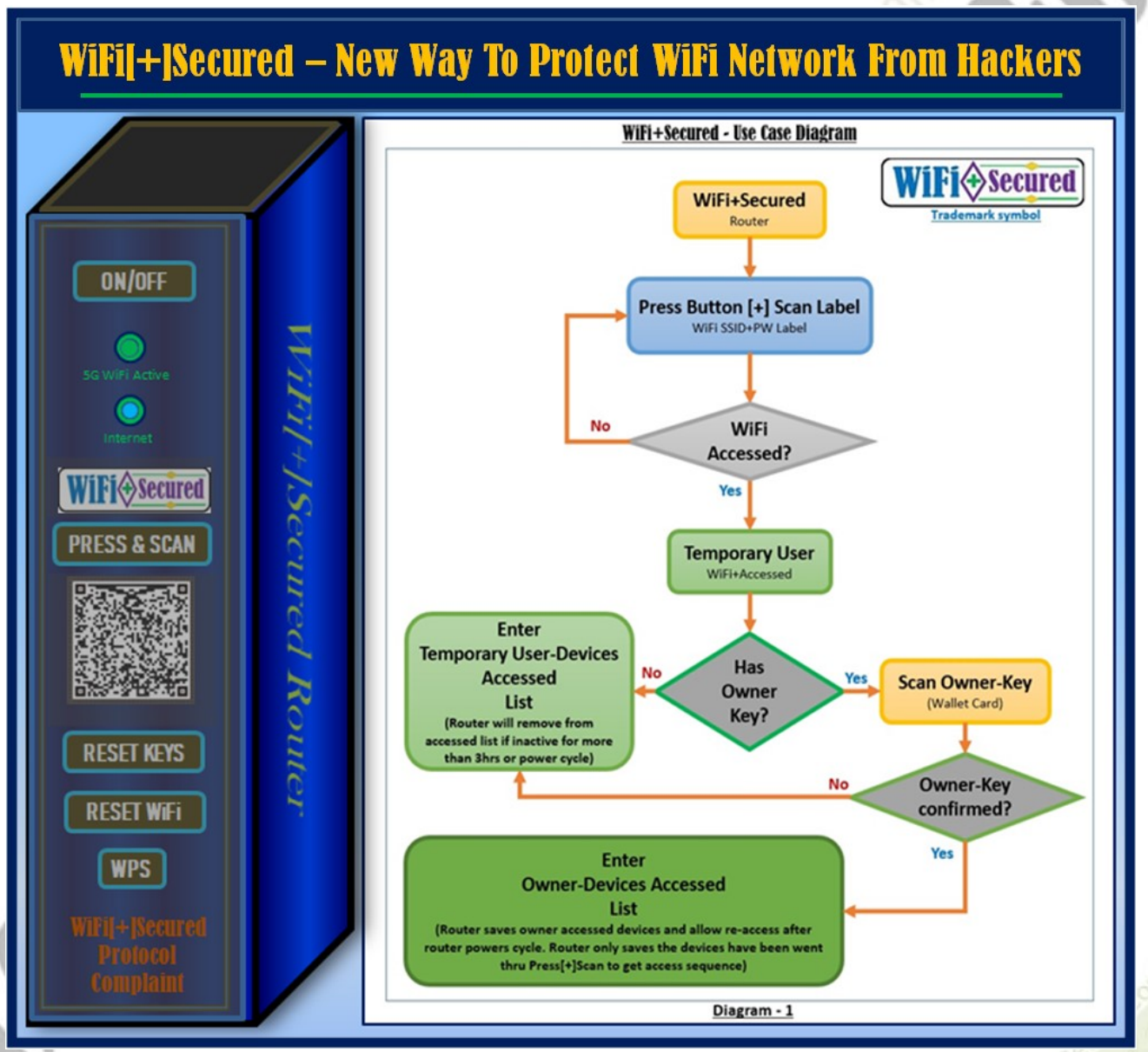
Diagram - 5

- Figure-5: WiFi[+]Secured Test Case 1 & 3 Diagram

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com

New Way To Protect WiFi Network From Hackers
-- Specification --
Henry V. Pham
WiFi[+]Secured Router Reference

1. The WiFi[+]Secured Router overview drawing below is the reference showing a sample WiFi router with 'Press & Scan' button to get WiFi access with the U.S Trademark **WiFi[+]Secured** symbol with U.S. Serial Number **90795366** along with other feature buttons of a standard WiFi router. The overview drawing also shows a use case diagram to show a complete signature of this invention drawing which is expected to show on the Patent Frame. This specification is based on the original document of the invention "**New Way To Protect WiFi Network From Hackers"** with the **U.S. Patent Number PCT/US24/17533** and **International Patent Number PCT/IB2024/000110.**



- Figure-R1: WiFi[+]Secured Router Reference

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com

2. This page shows the '**WiFi[+]Secured**' trademark symbol and the sample matrix labels one in QR code label as shown in the original invention document, and a GCODE label which contains the SSID and Security Key of the router. The combination SSID and Security Key in one label can be in pair key format separators like below; and this format is provided by **G-CODE Utility**, a java application which can be downloaded from these websites: **www.TheGCODECreator.com** or **www.TheCloudOSCenter.com.**

   These three sample combo-keys labels are shown in **GCODE Labels** in this page for references.

   [SSID12ADS64KGD772ADFADF3123613413]:[SKEY143da523ADFasdfsa7894SADe0kla!]
   (SSID12ADS64KGD772ADFADF3123613413):(SKEY143da523ADFasdfsa7894SADe0kla!)
   <SSID12ADS64KGD772ADFADF3123613413>:<SKEY143da523ADFasdfsa7894SADe0kla!>

   The below images are the WiFi[+]Secured trademark symbol and 3 sample of GCODE labels plus the original QR code label as shown in the original invention document.

HenryVPham@TheCloudOSCenter.com or henryvpham@gmail.com