

New Way to protect WiFi Network from Hackers - Claim

Henry V. Pham

The purpose of the 'New Way to protect WiFi Network from Hackers' invention is intended to replace existing WiFi Routers which are default configured with broadcasting WiFi SSID Names to provide access that attract hackers to get WiFi Passwords easily with a hacked WiFi Finder application and provide persistent access without users' acknowledgement. The 'WiFi[+]Secured' is the short name of this invention and would be used as a trademark label for the WiFi Routers that come with this "Press-and-Scan" to have access WiFi Secured Protocol and requires physical present of the users to have WiFi access. This invention provides the new WiFi Routers with protected WiFi Names and Passwords which would come in the Dot Matrix Label for temporary access key and the Dot Matrix Label Wallet Card for owner's persistent access key, and the users can just scan the label to have WiFi access. This claim shows the overview figure of this invention which was first submitted on 2021/07/01 with U.S. Only Patent Number 29/788,607; then re-submitted on 2024/02/27 with U.S. PCT/US24/17533 and International PCT/IB2024/000110 Patent Numbers, which can be used as the representing invention drawing to print on the patent frame and the following functions and features of this invention.

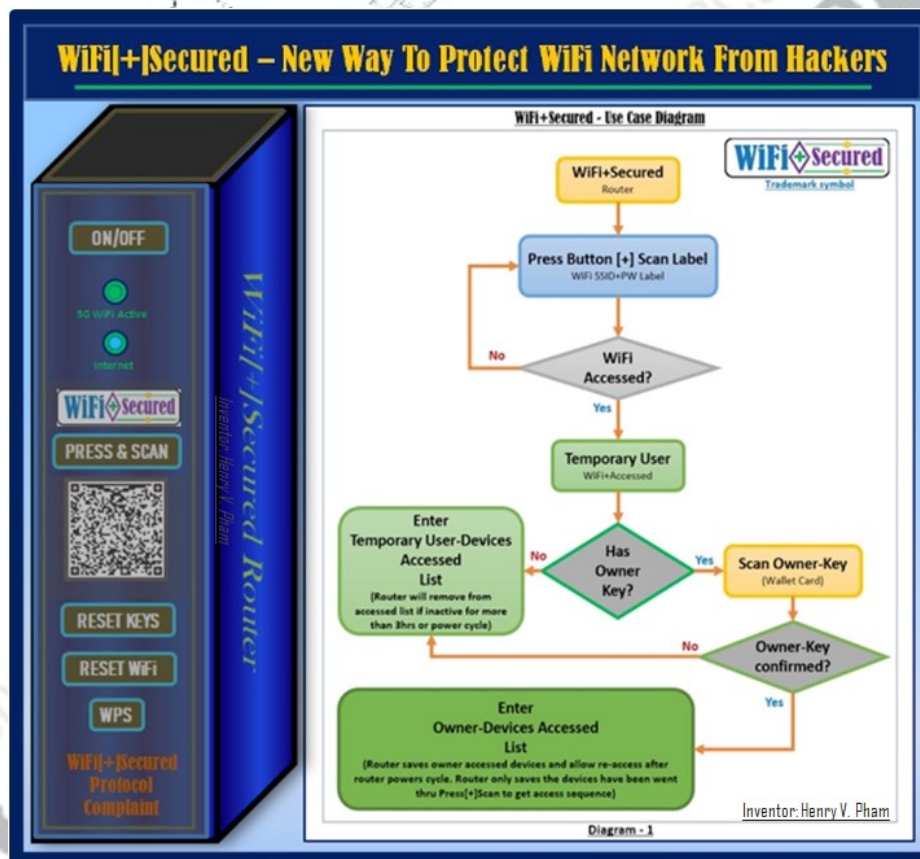


Figure-A: New Way to protect WiFi Network from Hackers -- Overview

1. The main apparatus for the WiFi[+]Secured, comprising:

The WiFi[+]Secured comes with 'Press-and-Scan' button to have WiFi access protocol with protected WiFi Names and Passwords with scan-able Dot Matrix Labels on the QR-Code or G-CODE labels. Wherein, the 'Press-and-Scan' button provides the users with secured method of scanning the code label while pressing this button to have WiFi access without lookup for WiFi Names on the smart devices; and the 'Press-and-Scan' to have access protocol requires physical present of the user instead of remotely gaining

New Way to protect WiFi Network from Hackers - Claim

access like the current wireless methods. The first scanning to have temporary access which would be timeout in 3 hours which is configurable from 1-3 hours; and the second scanning if owner Authentication Key is provided to have owner persistent access, would keep the connection persistently even the WiFi Routers got power outage.

2. The main operational apparatus for the WiFi[+]Secured, comprising:

The WiFi Router would check and remove the temporary accessed devices from the router after 3 hours of configured hours of inactive devices. The WiFi Names and Passwords are randomized and preprinted on the Dot Matrix Code user labels which would be combined into one label and visible for the users to scan; and the owner Authentication Key would also be the Dot Matrix Code which was recommended to be on a wallet card for more protected and easy to store for the owner. Wherein, when the user device is needed to have initial WiFi access, the user has to press the button and scan the WiFi Key label to have initial temporary access from the smart device WiFi application or WiFi Access Utility; the WiFi app would ask for owner Authentication Key to have further persistent access. The WiFi Router would allow and store the device into the persistent WiFi access list if the device is scanned and validated the owner Authentication Key; otherwise, the device would be allowed and stored into the temporary access list in the routers and would be remove after 3 hours of inactive for security purposes.

3. The WiFi[+]Secured Router buttons functioning apparatus of claim 1, further comprising:

The new WiFi[+]Secured Router would come with 'Press-and-Scan' button, 'RESET KEYS' button plus the 'WPS' button. Wherein, the 'Press-and-Scan' button would provide the function to scan the WiFi Name/SSID and Password for security purposes and convenience for the user without having to enter the password on the smart devices. The 'RESET KEYS' button would allow the users to reset the authentication keys before return, exchange or sale the router. The 'WPS' button which is already available and plus additional secured function by additional confirmation press of the button; the 1st press would provide initial temporary WiFi connection, and the 2nd press would provide the owner WiFi connection for persistent wireless access. This 'WPS' function would be provided to support setting up wireless access for small devices which may not able to use application for setup or configure the devices to have WiFi access.

4. The Dot Matrix Code label featuring apparatus of claim 2, further comprising:

The Dot Matrix Code can be printed on QR-CODE or G-CODE which contains WiFi Name/SSID and WiFi Password. Wherein, the label would contain both WiFi SSID and Password in one label with defined separator to provide one scan to have a complete authentication. The WiFi router manufacture should provide an application for the users to reprogram the SSID and WiFi Password. Note that the G-CODE Utility app already provided 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.

5. The WiFi[+]Secured for router supporting apparatus of claim 1 & 2, further comprising:

The 'WiFi[+]Secured' would be the label on the router that support this secured protocol and would be the first step to protect wireless data transferring from home or offices to datacenter or from

New Way to protect WiFi Network from Hackers - Claim

datacenter to home of offices and would be used for future with Cloud OS for high data secured infrastructure for entire world, and the 'WiFi[+]Secured' is the short name of this invention with the title 'New Way to Protect WiFi Network from Hackers'. Wherein, the trademark of the 'WiFi[+]Secured' would show the word 'WiFi' following a plus '+' symbol in diamond and following the word 'Secured' as shown in the overview figure and in the original invention document. This mark originally registered with U.S. Trademark WiFi[+]Secured symbol with U.S. Serial Number 90795366, and later re-registered on 2025/10/23 with U.S. Trademark Serial Number 99458763.

6. The WiFi SSID and Password format and usage apparatus of claim 2 & 3, further comprising:

The Dot Matrix Code labels would come with default factory keys, one wallet key card for owner key and user code label that contains factory for temporary access key; the label would contain WiFi SSID within its enclosed characters such as parentheses, square or angle bracket characters and separated by a special character as recommended in the original invention and specification documents. Wherein, the factory keys are the initial randomized with WiFi SSID and Password in one label and provided by the manufacturer; when the users re-programmed the new authentication keys, the factory keys would be disabled. The WiFi router manufacturers should provide application for the users to re-program the authentication keys for single or multiple routers at once, and the application to view and check for all the users showing on the temporary and permanent wireless access lists.

Inventor name: Henry Viet Pham

Email Address: HenryVPham@Gmail.com

Business Website: www.TheCloudOSCenter.com

Phone Number: 714-686-0927