

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

**Title of
Invention**

NEW WAY TO PROTECT WIFI NETWORK FROM HACKERS

As the below named inventor, I hereby declare that:

This declaration
is directed to:

☐

The attached application, or

☒

United States application or PCT international application number 29/788,607

filed on 7/01/2021

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: PHAM, HENRY VIET

Date (Optional): 8/05/2021

Signature: Pham.Henry.V

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**FIRST VERSION SPECIFICATION
PAPER SUBMISSION**

Specification

I, Henry Viet Pham have invented a new design for a 'New Way to Protect WiFi Network from Hackers' as set forth in the following specification:

Figure-1 is a 'WiFi[+]Secured - Use Case Diagram' of a WiFi[+]Secured protocol showing my new design;

Figure-2 is a 'WiFi[+]Secured – Temporary User Test Case 1 Diagram' thereof;

Figure-3 is a 'WiFi[+]Secured – Temporary User Test Case 2 Diagram' thereof;

Figure-4 is a 'WiFi[+]Secured – Owner Test Case 1&2 Diagram' thereof; and

Figure-5 is a 'WiFi[+]Secured – Owner Test Case 1&3 Diagram' thereof;

I claim: The ornamental design for a '**New Way to Protect WiFi Network from Hackers**' as shown.

WiFi+Secured - Use Case Diagram

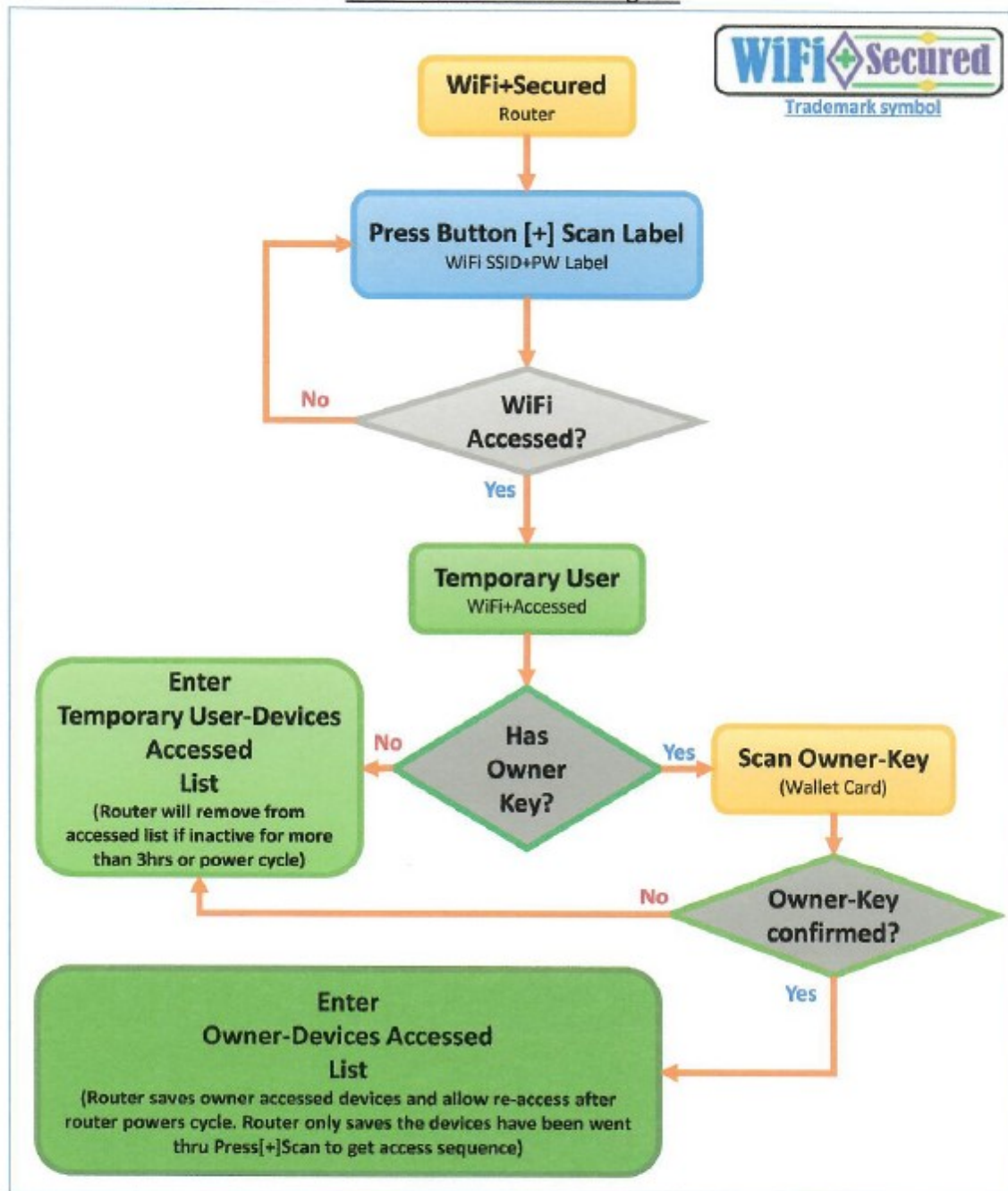


Figure - 1

WiFi+Secured – Temporary User Test Cases Diagram

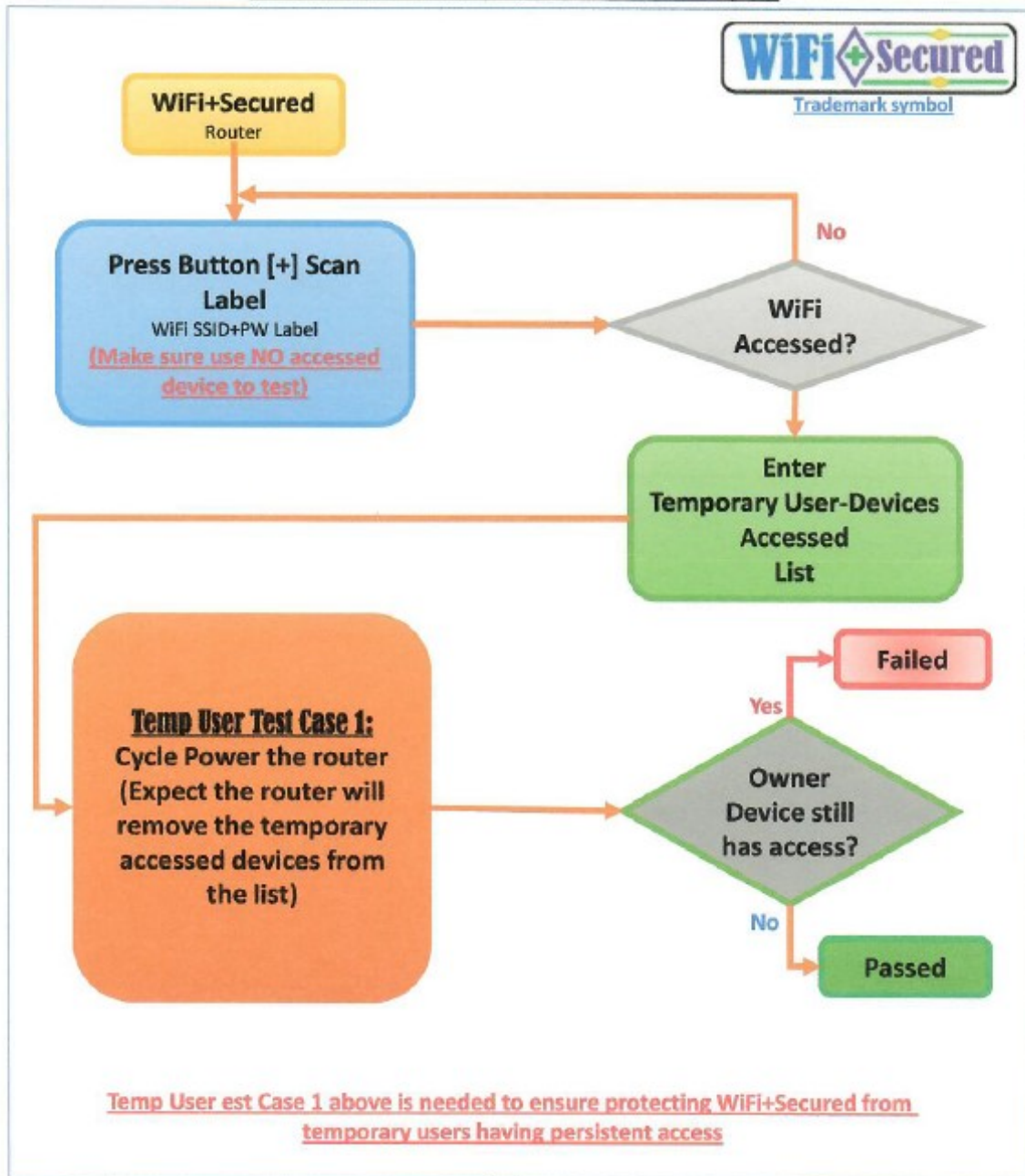


Figure - 2

WiFi+Secured – Temporary User Test Cases Diagram

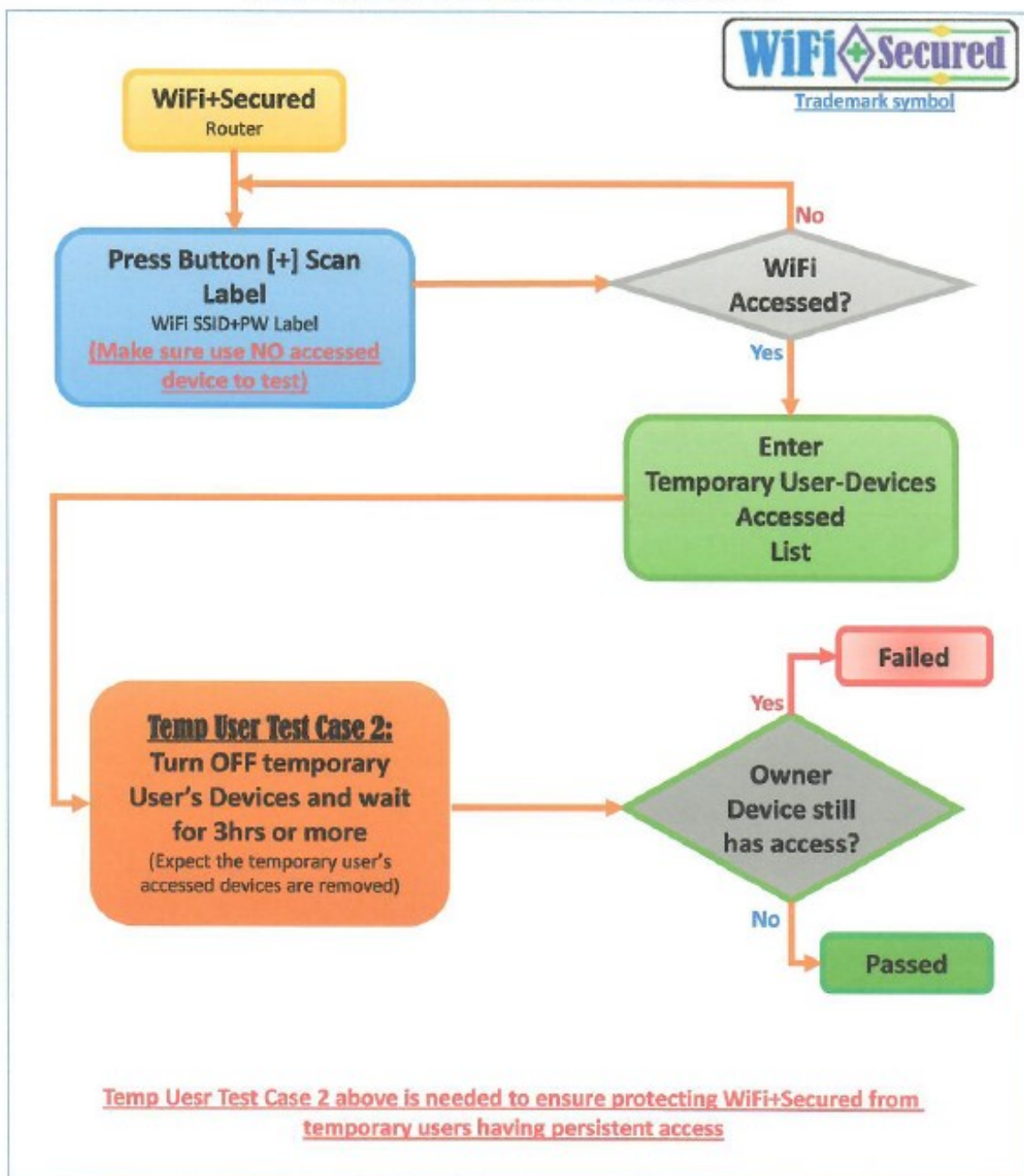


Figure - 3

WiFi+Secured – Owner Test Cases Diagram

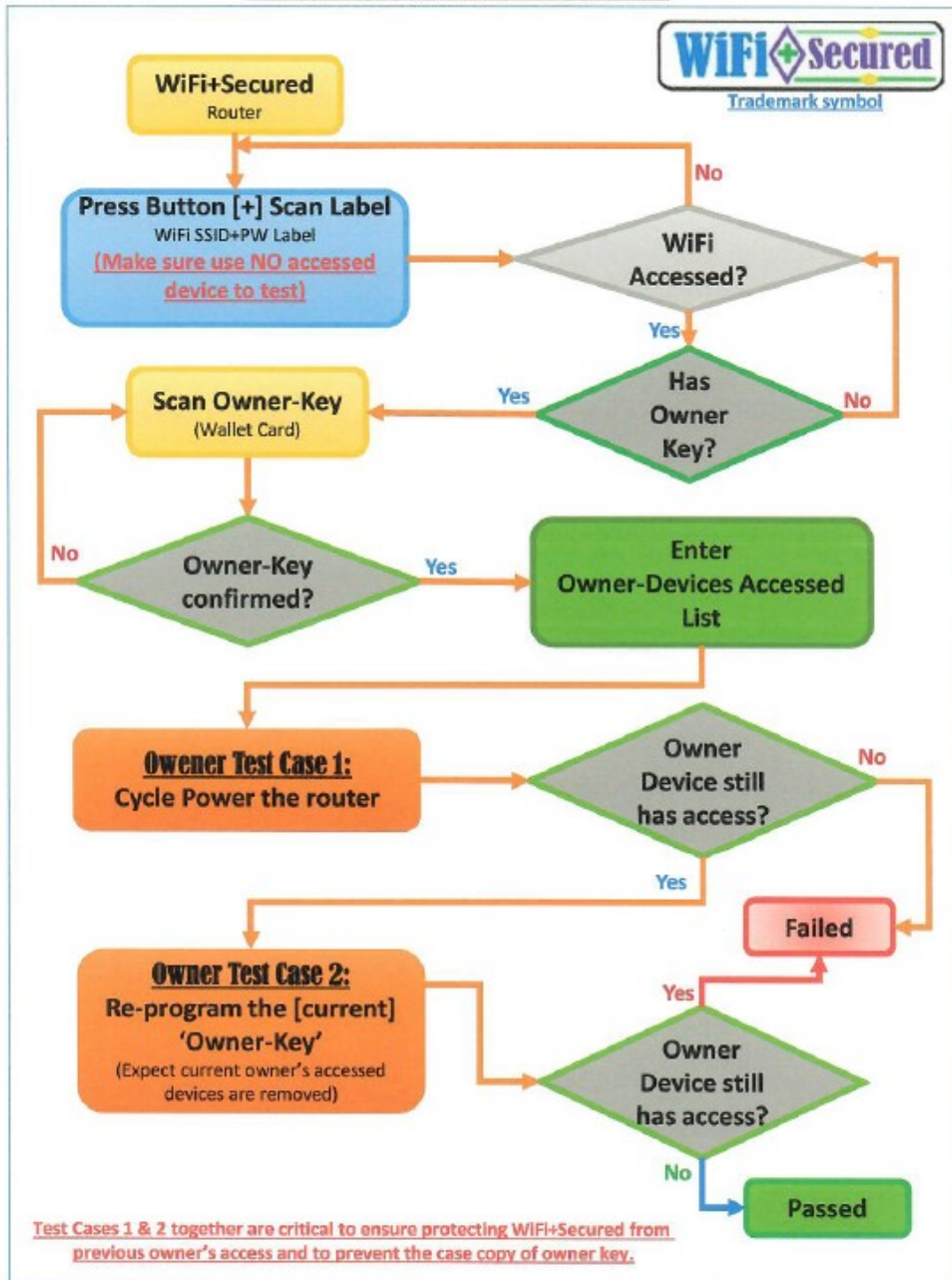


Figure - 4

WiFi+Secured – Owner Test Cases Diagram

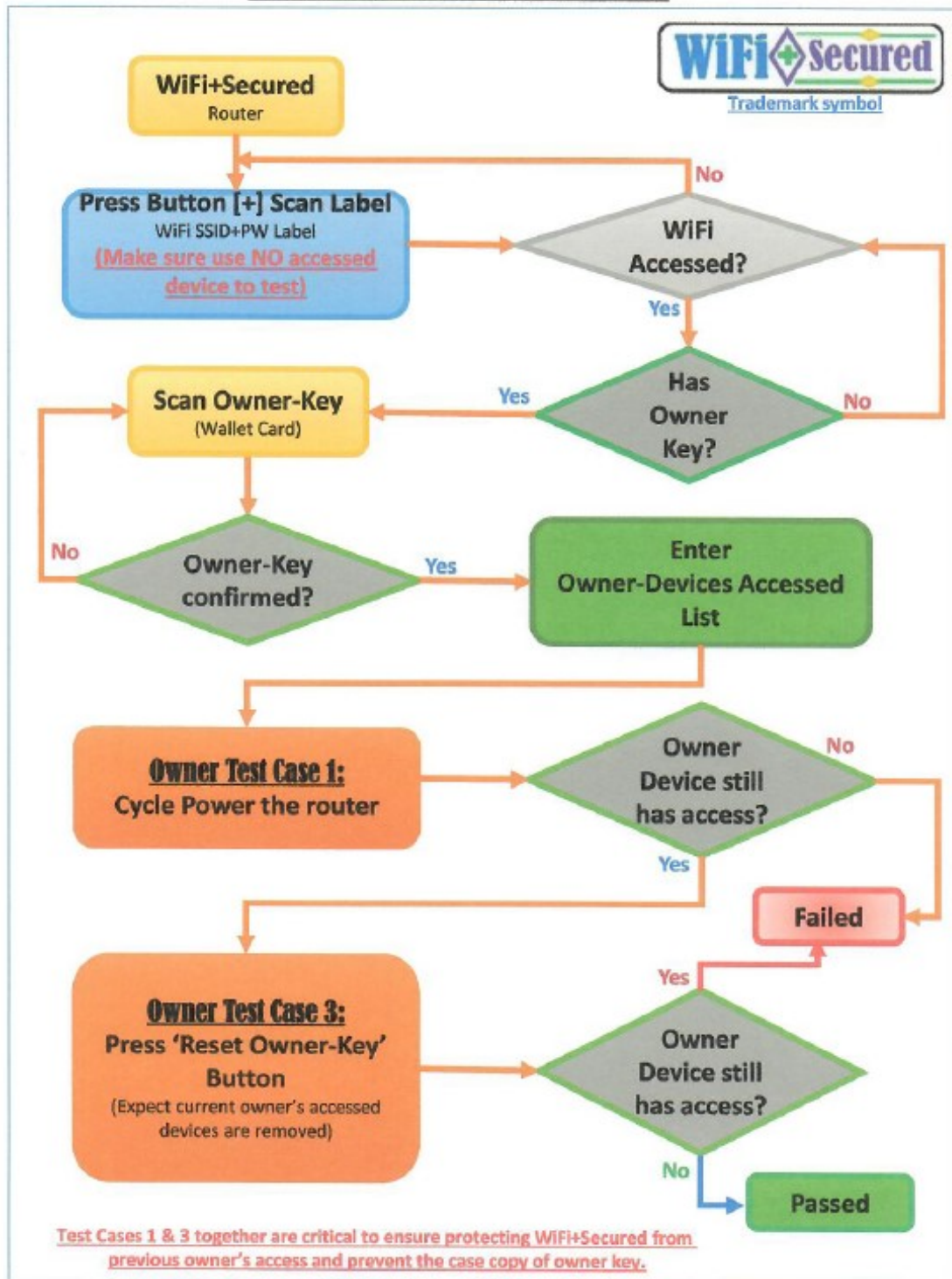


Figure - 5

**FINAL VERSION INVENTION DOCUMENT
PAPER SUBMISSION**

REPLY:

Office Action Summary

Application No.
29/786,607

Applicant(s)
Pham, Henry Viet

Examiner
RICHARD E CHILCOT

Art Unit
2916

AIA (FITF) Status
Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.130(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- ☐ A declaration(s)/affidavit(s) under 37 CFR 1.130(b) was/were filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 1 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the Patent Prosecution Highway program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☒ The specification is objected to by the Examiner.
- 11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ____.
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date ____.
- 4) ☐ Other: ____.

New Way to protect WiFi Network from Hackers

There are many different ways to hack into the current WiFi Network. And the current WiFi routers are difficult to setup for non-Network experience people. The current WiFi routers are default with visible WiFi name (SSID), and this will attract the hackers to hack into the WiFi router to have Network access.

I introduce the new way to protect the WiFi Network [**WiFi+Secured**] completely from the hackers with the new WiFi router **Press-and-Scan-to-Access**. This new WiFi router **Press-and-Scan-to-Access** will provide the owners and users an invisible WiFi SSID and the WiFi Password without the user inputs.

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 label 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 a persistent owners WiFi Network access. For appliances and small devices

New Way to protect WiFi Network from Hackers

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.

The whole idea of this new WiFi Network protection here is to have a button pressed while scanning the WiFi SSID and the Password to have access to prevent unwanted users from outside of the house or business accessing the WiFi Network. This idea also applies to the WiFi Extenders. The "Press-and-Scan" button should be close to the WiFi SSID and Password label. For more extensible Network like business, a separate wireless device has a "Press-and-Scan" button and an Authentication keys label provided to replace the routers with "Press-and-Scan" button and the labels that are hidden from the users. The device OS or WiFi application should only show the desired name but not the WiFi SSID even this is a random SSID.

With the above idea, the users must be next to the WiFi router to have WiFi Network access. After the owners pressed the "Press-and-Scan" button and scan the **Authentication User** key 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

New Way to protect WiFi Network from Hackers

or removed by the router after three hours of inactive. When the device OS or WiFi application of the owners try to access after they have completely went through the owner authentication procedure, the owners' device OS or WiFi application must send to the router the **Authentication Owner** key to ask for the router permission to have access. If the router received the owner-key is not valid, then the router will reject the access.

In summary, the following key items and functions that are required a new router must have to comply with the new WiFi+Secured protocol:

- ❖ The new router package should have a wallet-card with **factory-key** and **owner-key** label, and a **random WiFi SSID** and **random WiFi Password** label.
- ❖ The new router should have a **"Reset Owner Key"** button. When the router is reset to factory key, the factory-key become the default owner-key.
- ❖ The new router should have a **"Press and Scan"** button. This button will allow the users to scan the G-CODE labels for the Authentication keys to have the Network access. 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 owner-key and factory-key will be on a wallet-card for the owner access only.

New Way to protect WiFi Network from Hackers

- ❖ The owners have the rights to program their own owner-key, WiFi SSID and WiFi Password. When setting up the WiFi Network, the owners will be asked to have their owner-key, and the Authentication User key to be programmed to their router. After the Network is completely setup and running, the owners can reprogram their own Authentication keys every six months or so for their own security purposes. This feature can be provided through the router application or an application that can program all the routers at once. The owners can print and use their own G-CODE labels for the Authentication keys and stick them to the router or at a Press-and-Scan-to-Access point.
- ❖ The router application should provide a feature for the owners to remove an accessed device from the accessed devices list. This feature prevents the previous owners or unwanted users accessing to the WiFi Network.
- ❖ The new router should always check and validate the owner-key for the accessing devices, then reject and remove the devices that have incorrect or old owner-key.
- ❖ The new router should always check and remove the accessed devices from the temporary accessible list for the devices that have been inactive for three hours or more. The **temporary accessed devices** are the devices in the temporary Network access that are allowed access but without the owner-key.

New Way to protect WiFi Network from Hackers

- ❖ When cycle power the router, the router should always remove and clear all the temporary accessed devices. But the owner accessed devices in the persistent Network access are always allowed to access when power is back on.

The following key items, functions or procedure that are required the device OS and the WiFi application to support the new router to comply with the new WiFi+Secured protocol:

- ❖ Provide the users with a default Network name with a random number like "TempNetwork<random#>", and allow the users to rename it to their desired Network name. This desired Network name will be shown on the WiFi list instead of the current way showing the WiFi SSID.
- ❖ Then the WiFi application will ask the users to press the "Press-and-Scan" button to scan the WiFi SSID and WiFi Password. The device will have WiFi Network access at this point with the Authentication User access not the Authentication Owner access yet.

New Way to protect WiFi Network from Hackers

- ❖ Owner step, this is the owner-access-procedure and optional for the temporary users. The WiFi application will ask the users to scan the owner-key with an option owner access. The WiFi application will confirm this owner-key with the router. If successfully confirmed, the device OS or WiFi application will have a full Authentication Owner key with three parameters (WiFi SSID, WiFi Password and the owner-key). The idea of having Owner Key and must be following Press-and-Scan to get access is to prevent the case of copied or stolen Owner Key to gain WiFi access at any time. If the users do not have the owner-key or scan an invalid owner-key, the users will have the temporary Network access with Authentication User key with two parameters (WiFi SSID and WiFi Password) but the Network access will be clear or removed by the router after three hours of inactive.

New Way to protect WiFi Network from Hackers

WiFi+Secured - Use Case Diagram

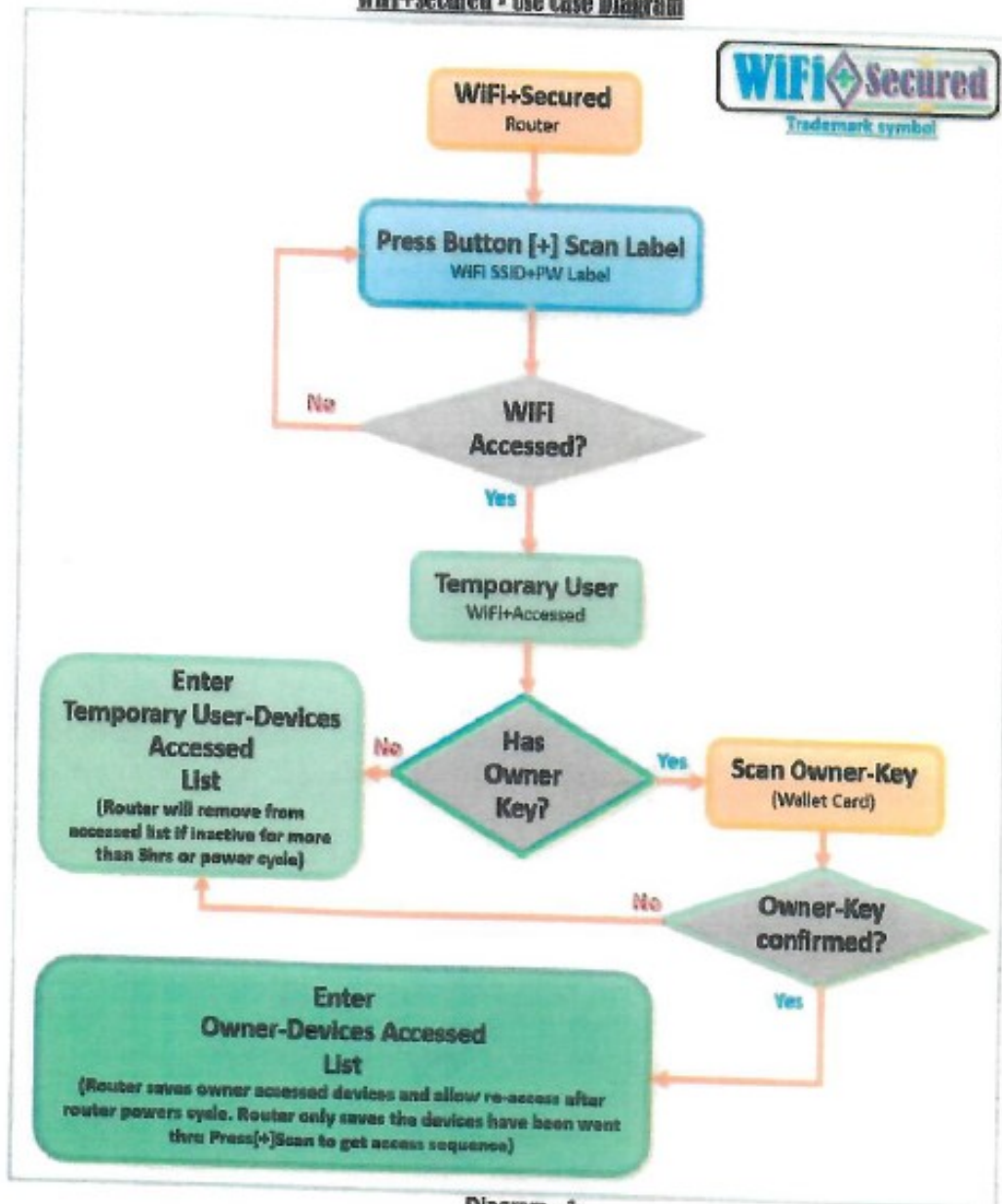


Diagram - 1

New Way to protect WiFi Network from Hackers

WiFi+Secured – Temporary User Test Cases Diagram

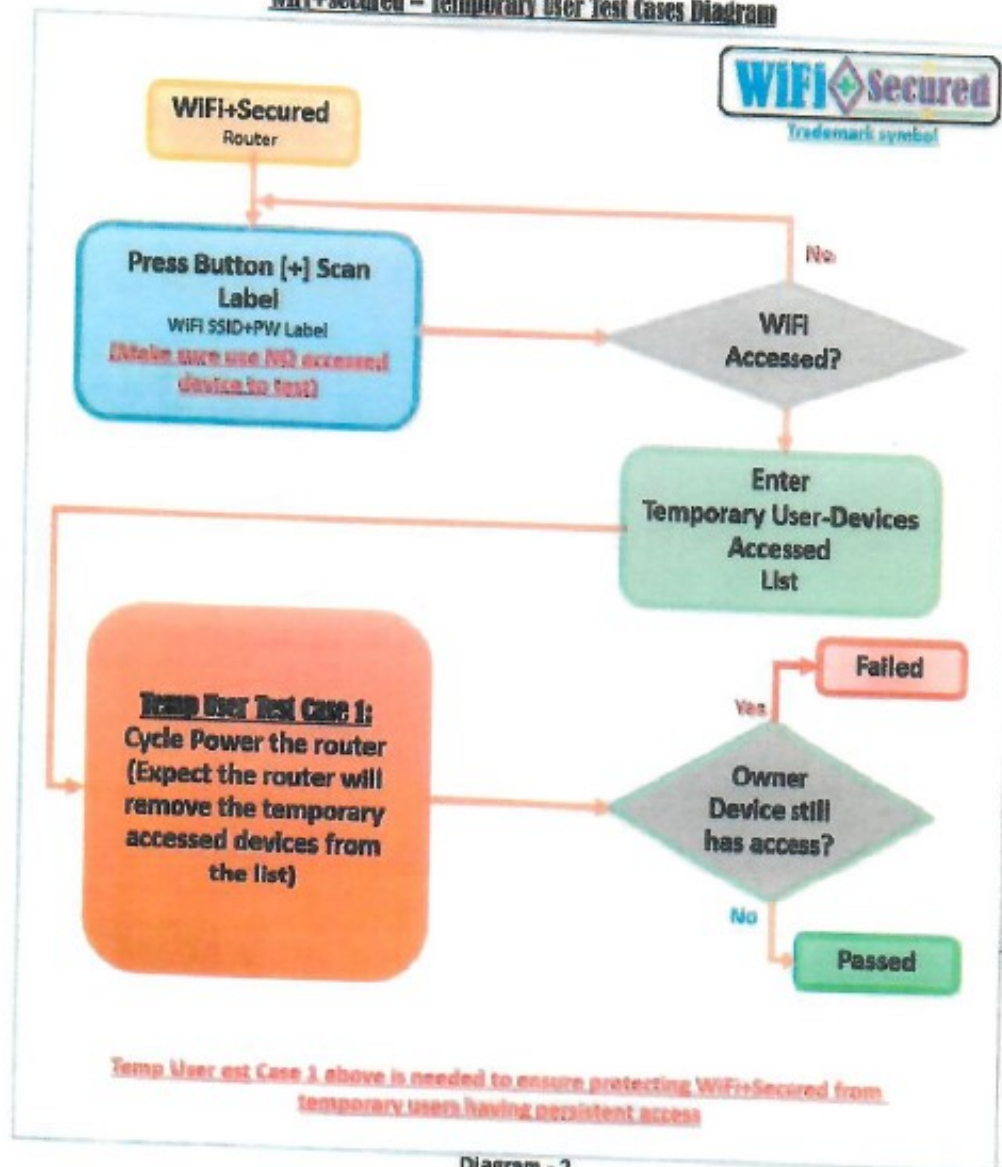
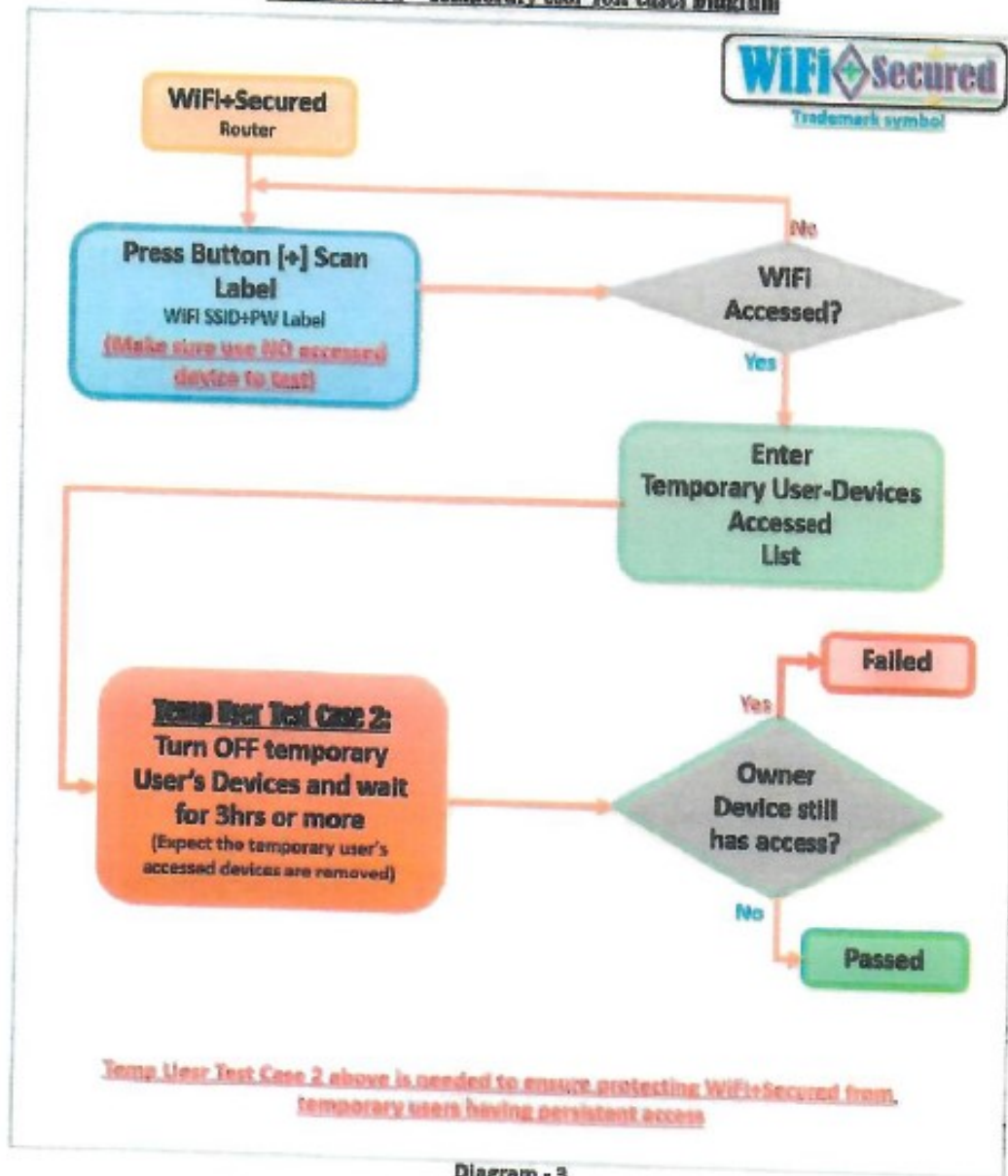


Diagram - 2

New Way to protect WiFi Network from Hackers

WiFi+Secured – Temporary User Test Cases Diagram



New Way to protect WiFi Network from Hackers

WiFi+Secured – Owner Test Cases Diagram

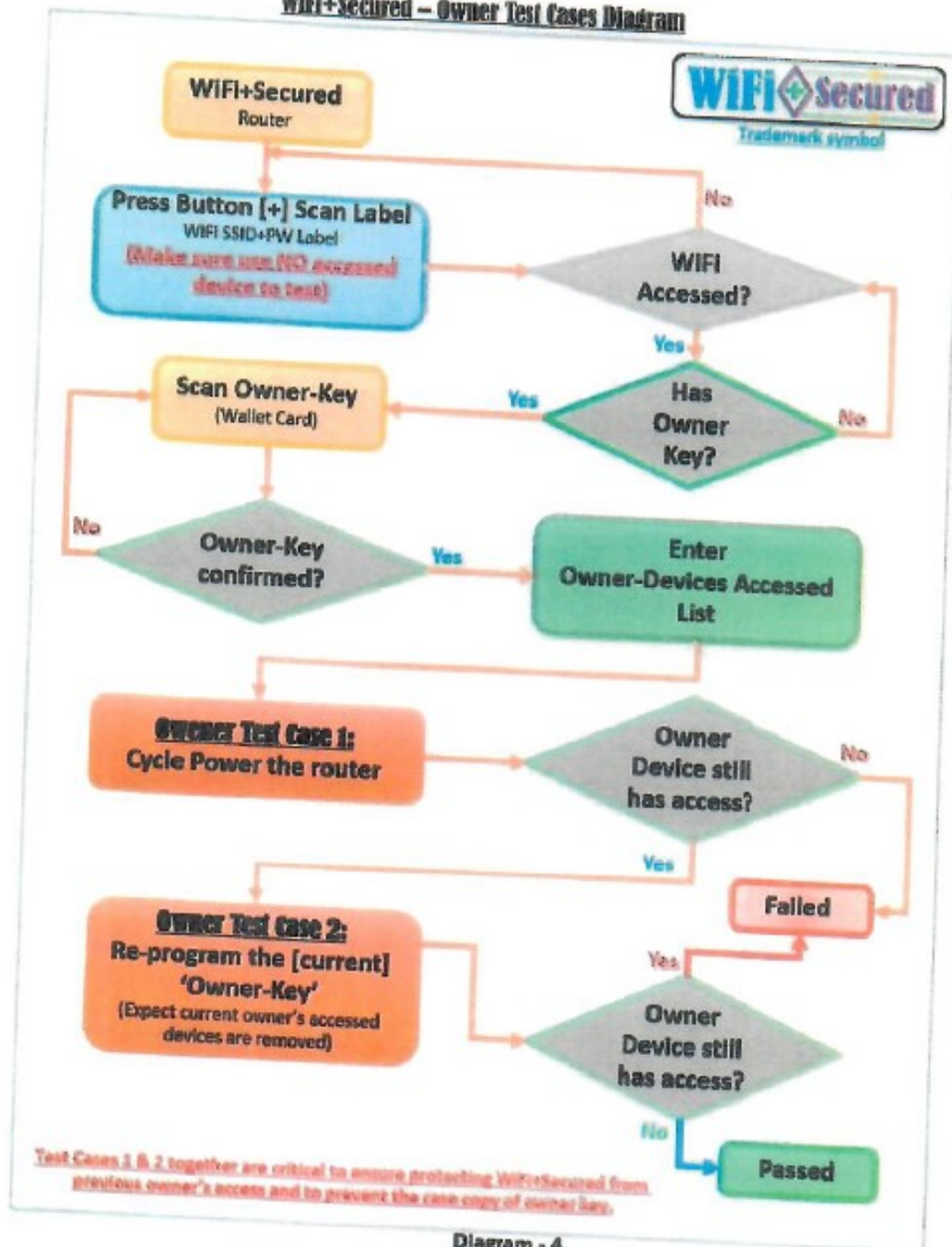


Diagram - 4

New Way to protect WiFi Network from Hackers

WiFi+Secured – Owner Test Cases Diagram

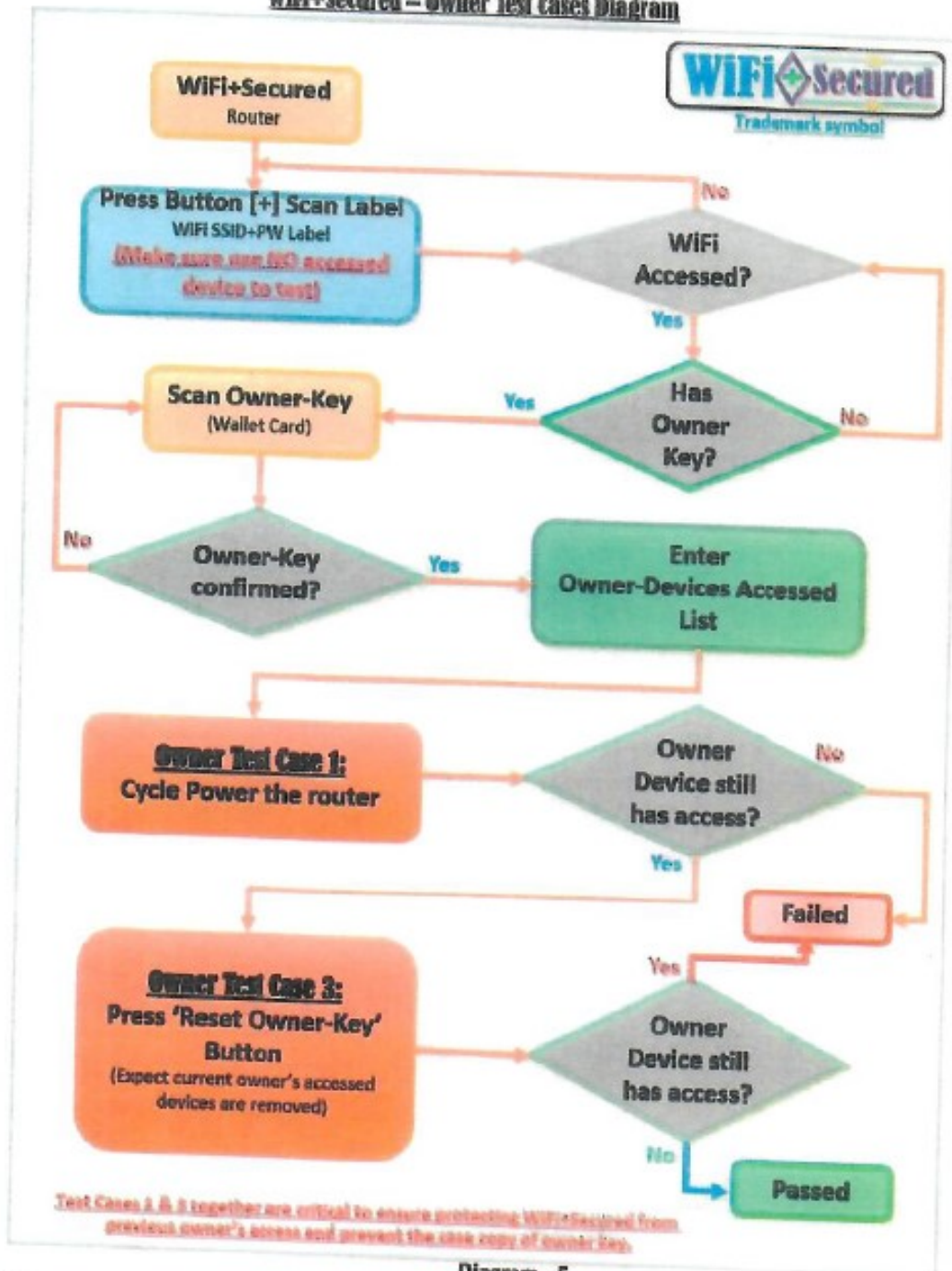


Diagram - 5

New Way to protect WiFi Network from Hackers

With this new idea, 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 corporates if they are sharing offices in the same building.

A standard trademark below is for new routers with this new secured protocol to help customers and users identify the new **WiFi+Secured** protocol should have the Trademark and WiFi-Access-Label like below. The trademark and the WiFi-Access-Label should be printed right below the "Press-and-Scan" button. The WiFi security option should always be set to the highest security option "WPA2" or higher.

Notice: The QR code below is just a sample code label, and can could be replaced by other code labels like Barcode or G-CODE labels.



**FINAL VERSION SPECIFICATION &
INVENTORSHIP CLAIM
PAPER SUBMISSION**

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Claim

I, Henry Viet Pham as a sole inventor with the USPTO customer number 183405, claim the inventor-ship for the invention with the title, "New Way to protect WiFi Network from Hackers" with the US Application Number 29/788,607 which was first submitted online on 07/01/2021 with 7 pages document, and then resubmitted by paper with some updates of 5 (five) more diagrams with total of 12 pages long as requested by USPTO on 08/07/2021. Also, the live video proof of identification process via ID.me was conducted on 03/22/2022; which was proved of my personal identity with live conference and proof of Passport and Photo ID.

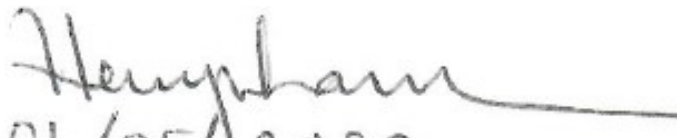
This invention was created for the purpose of prevent hacking to be described below for the ornamenting purpose of this invention. The current Wireless devices providers or routers broadcast SSID everywhere; especially when sharing the same work building or offices, and anyone can able to try to gain WiFi access from remotely. Any smart devices like smart cameras or camera systems, the users have to provide SSID and WiFi pass code to the mobile applications or through a web application via setup procedure. These provide a high hacking potential, and the hackers can able to gain access from remotely. There is no way to prevent with the current procedure of providing or access WiFi network for current smart devices. These problems lead to this invention to prevent hacking to WiFi networks from remotely is required the users have to be physically next to the router to have WiFi access. Physically right next to the router with 'Press-and-Scan-to-Access' is the only way to prevent un-authorized remote accesses for WiFi networks of any access points.

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Claim

In this claim, I, Henry V. Pham provide the original invention document, the Electronic Acknowledgement Receipt (online submission on 07/01/2021) and the paper Acknowledgement Receipt (paper resubmission on 08/07/2021) along with my personal Passport and Photo ID as a proof for patent of this invention. The followings are the items which attached in this package.

- 1) Original Invention Document, title "New Way to protect WiFi Network from Hackers" -- (12 pages).
- 2) Electronic Acknowledgement Receipt (1st submission) -- (2 pages).
- 3) Paper Acknowledgement Receipt (resubmission) -- (3 pages).
- 4) The specification of invention, title "New Way to protect WiFi Network from Hackers" -- (10 pages).
- 5) Personal Identification; copy of Passport and Photo ID -- (on page 3 of this claim).

Signature:



Date:

01/05/2023

Inventor name: Henry Viet Pham

Home Address: 805 S. Hilda Street, Anaheim CA 92806

Email Address: HenryVPham@Gmail.com

Phone Number: 714-686-0927

Personal Passport & Photo ID



7/1/2021

Submission Receipt - Submissions - Patent Center - USPTO


**UNITED STATES
PATENT AND TRADEMARK OFFICE**

**UNITED STATES
PATENT AND TRADEMARK OFFICE**

Print

Email

Save as...

 P.O. Box 1450
 Alexandria, VA 22313-1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

 APPLICATION #
29/788,607
 RECEIPT DATE / TIME
07/01/2021 04:57:44 PM ET
 ATTORNEY DOCKET #
 -

Title of Invention

New Way to protect WiFi Network from Hackers

Application Information

APPLICATION TYPE	Design - Nonprovisional Application under 35 USC 171	PATENT #	-
CONFIRMATION #	1396	FILED BY	Henry Pham
PATENT CENTER #	60230912	FILING DATE	-
CUSTOMER #	-	FIRST NAMED INVENTOR	Henry Viet Pham
CORRESPONDENCE ADDRESS	Henry Viet Pham 805 S Hilda St Anaheim, CA 92806 US	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGE S	DESCRIPTION	SIZE (KB)
generatedADS60230912.pdf	5	Application Data Sheet	120 KB
New Way to protect WiFi Network from Hackers.pdf	7	Abstract	84 KB

Digest

DOCUMENT	MESSAGE DIGEST (SHA-512)
generatedADS60230912.pdf	C3751C40C58AE9E55F5174EF81F4F0B7699FAA97F0EF266D479E8BC57CDD4C668022073CE026B4D3DC8B0A6379A6875A2E5B95EE64F08BA05C12FFAA364843C8
New Way to protect WiFi Network from Hackers.pdf	5883E3DF31EE44B3DA2D3BB60091734E694C6A2CB43BFD485657FD8E02D646C82E723555418F1D9742C37D2305B91865312B204FAE7C5819759F9629C1D99E29

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<https://patentcenter.uspto.gov/wi/submissions/9db3fc8-ae40-401d-9c0a-9194dfb0a9db/submission-receipt?category=NewSubmissions>

7/1/2021

Submission Receipt - Submissions - Patent Center - USPTO

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b) (d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

**FINAL VERSION SPECIFICATION
PAPER SUBMISSION**

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

I, Henry Viet Pham invented the WiFi secured protocol for router with the invention title, "**New Way to protect WiFi Network from Hackers**"; shorten name in Trademark application shown as '**WiFi[+]Secured**' with the Trademark serial number '**90795366**'. This invention was intended to protect the WiFi network with simple sequence protocol "Press-and-Scan-to-Access"; this requires the routers to implement a button for users to press and scan a WiFi Keys (SSID & Security Key) label to get access.

All wireless devices providing internet access like Wireless Routers, Wireless Access Points, and WiFi Extenders are required to have this protocol implemented to protect WiFi network. The '**WiFi[+]Secured**' trademark symbol was designed to adhesive as a sign-symbol on the routers or access points to show the users the routers or access points are implemented with this protocol. The routers are required to have 'Press-and-Scan-to-Access' button, 'Reset Keys' button, and the '**WiFi[+]Secured**' label; along with a wallet card for random factory key (part of the key could be router info and serial number) and a random owner key.

The followings 5 diagrams shows below are the original diagrams from the invention document. The original document was submitted on 07/01/2021 with 7 pages, and then later resubmitted with 5 diagrams with total of 12 pages with additional author name and date at footer of each page for document's author and date identification. These diagrams will show the regular procedure use cases, and provide test cases to identify and confirm the routers,

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

Wireless access points or wireless access provider devices have this protocol implement correctly.

The Diagram-1 below shows the use case for both temporary (guest) users and owner users. When users press and hold 'Press-and-Scan-to-Access' button while scanning the WiFi SSID-Key label, if the SSID-Key is scanned successfully, the routers will allow the users to have WiFi access as a temporary access. This process requires the users have to be physically next to the routers; and router SSID should be invisible; no needs to broadcasting SSID like currently. Next step, the WiFi application will ask for owner key which can be a wallet key for easy secure storage, if the users have owner key and can be scanned in successfully, then the users will have persistent WiFi access. Persistent access will allow the users to have access when the routers have power cycles or after reboots. However, this step requires the phones, tablets, computers or smart devices that need WiFi access to have a function to support additional scanning for owner key. If the users don't have owner key, they only have guest or temporary access. These temporary access devices will be hold for maximum of 3 hours of inactive, and then the routers will remove the temporary access devices from the access list. This inactive timeout can be configured from 1 (one) hour to 3 (three) hours depends on customer requirements. With guest or temporary access, if the temporary access devices are inactive for the defined timeout or the routers have been rebooted, then these devices are required to press and scan SSID-Key label again to have access. The routers are required to have an application for the users to

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

reprogram new SSID and Keys from new labels, and to view and manage the routers. The SSID and Keys are randomized or defined by users which will be the keys code in dot matrix labels; the labels can be the GCODE labels.

The **Diagram-2** below shows the test case when temporary devices already have WiFi access, then the router is powered cycle to confirm the temporary devices are removed from the router's access list and the devices are no longer have WiFi access. The diagram shows the sequence with a new (no WiFi access) device which goes through a process to get temporary access, then cycle power the router. This test expects the device will no longer have WiFi access after the power cycle of the router.

The **Diagram-3** below shows the test case when temporary devices already have WiFi access, then the devices go offline (powered OFF) to confirm the temporary devices are removed from the router's access list after the inactive timeout. The diagram shows the sequence with a new (no WiFi access) device which goes through a process to get temporary access, then power OFF the device. This test expects the device will no longer have WiFi access when turning back ON after the device powered OFF longer than the inactive timeout.

The **Diagram-4** below shows the test case when the owner devices already have owner WiFi access, then the router is powered cycle to confirm the owner devices are still having WiFi access; then the router is reprogrammed with new owner key and expected the

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

device will no longer have WiFi access. The diagram shows the sequence with a new (no WiFi access) device which goes through a process to get owner access, then goes through 2 owner test cases; test with router power cycle, and test with router reprogrammed with new owner key.

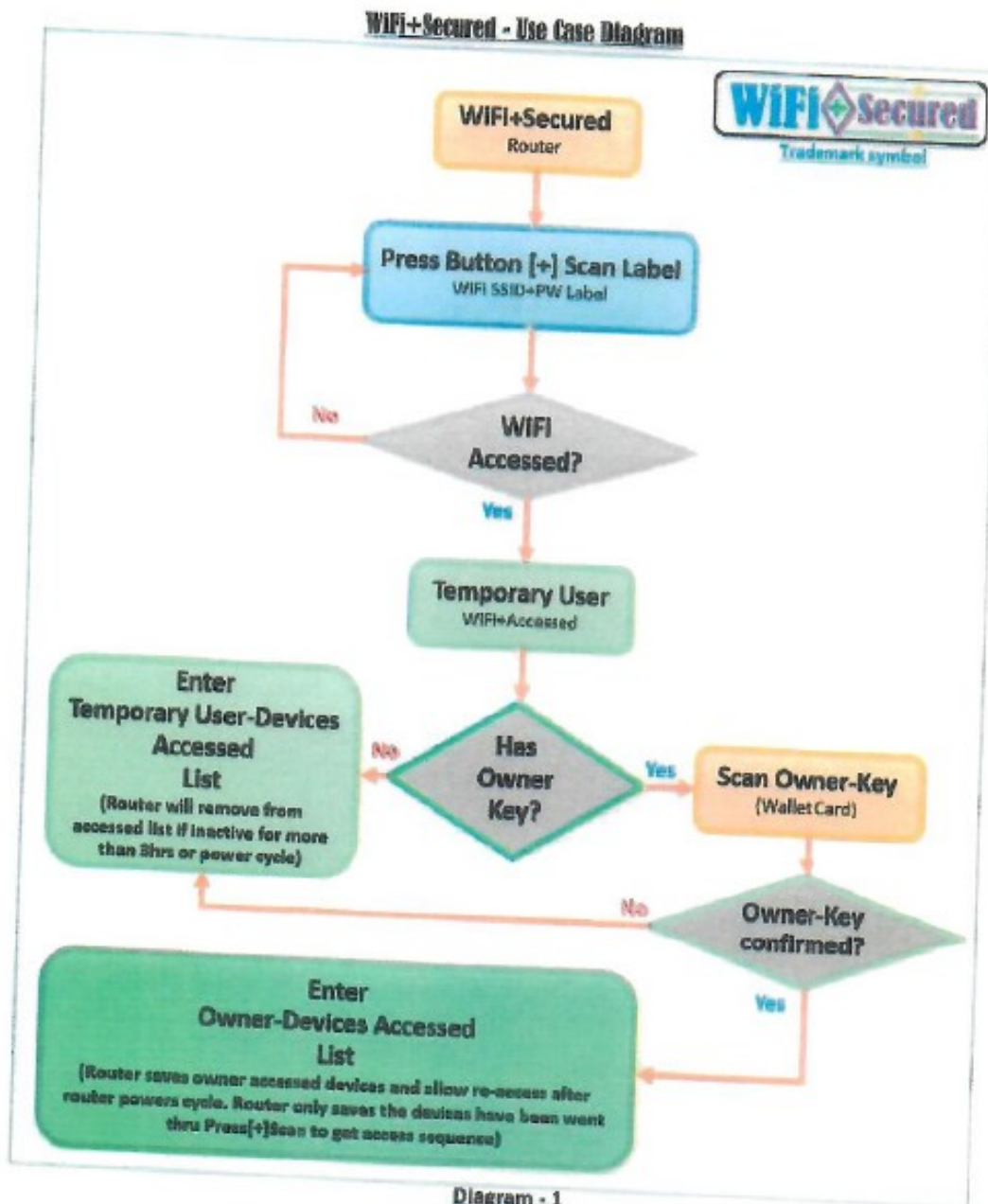
The Diagram-5 below shows the test case when the owner devices already have owner WiFi access, then the router is powered cycle to confirm the owner devices are still having WiFi access; then the router is reset the owner key or all keys and expected the device will no longer have WiFi access. The diagram shows the sequence with a new (no WiFi access) device which goes through a process to get owner access, then goes through 2 owner test cases; test with router power cycle, and test with router reset the keys with new owner key.

The last 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 my website www.TheGCODECreator.com

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

```
[SSID12ADS64KGD772ADFADF3123613413]:[SKEY143da523ADFasdfs7894SADe0kla!]  
(SSID12ADS64KGD772ADFADF3123613413):(SKEY143da523ADFasdfs7894SADe0kla!)  
<SSID12ADS64KGD772ADFADF3123613413>:<SKEY143da523ADFasdfs7894SADe0kla!>
```

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification



New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

WiFi+Secured -- Temporary User Test Cases Diagram

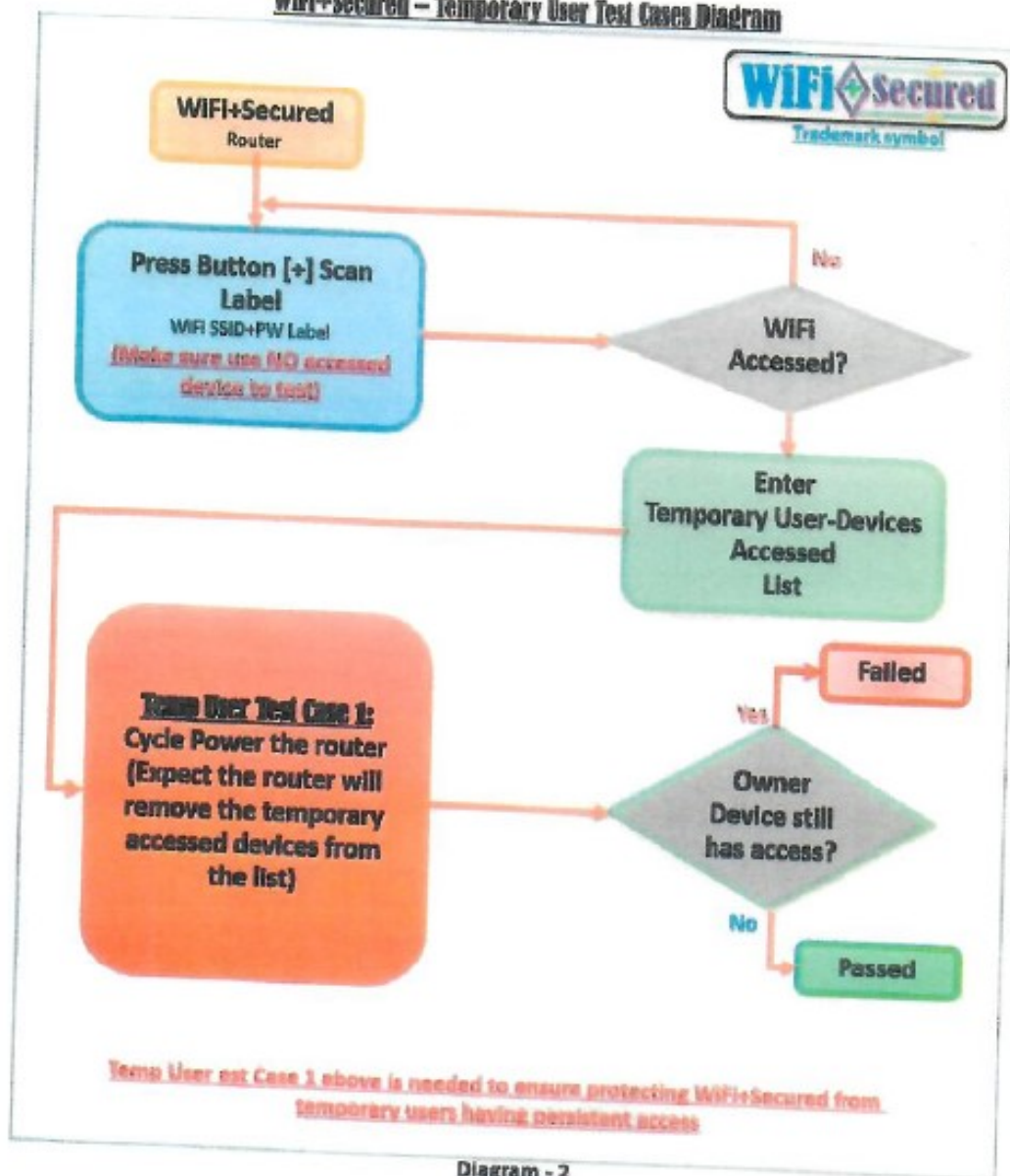


Diagram - 2

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

WiFi+Secured -- Temporary User Test Cases Diagram

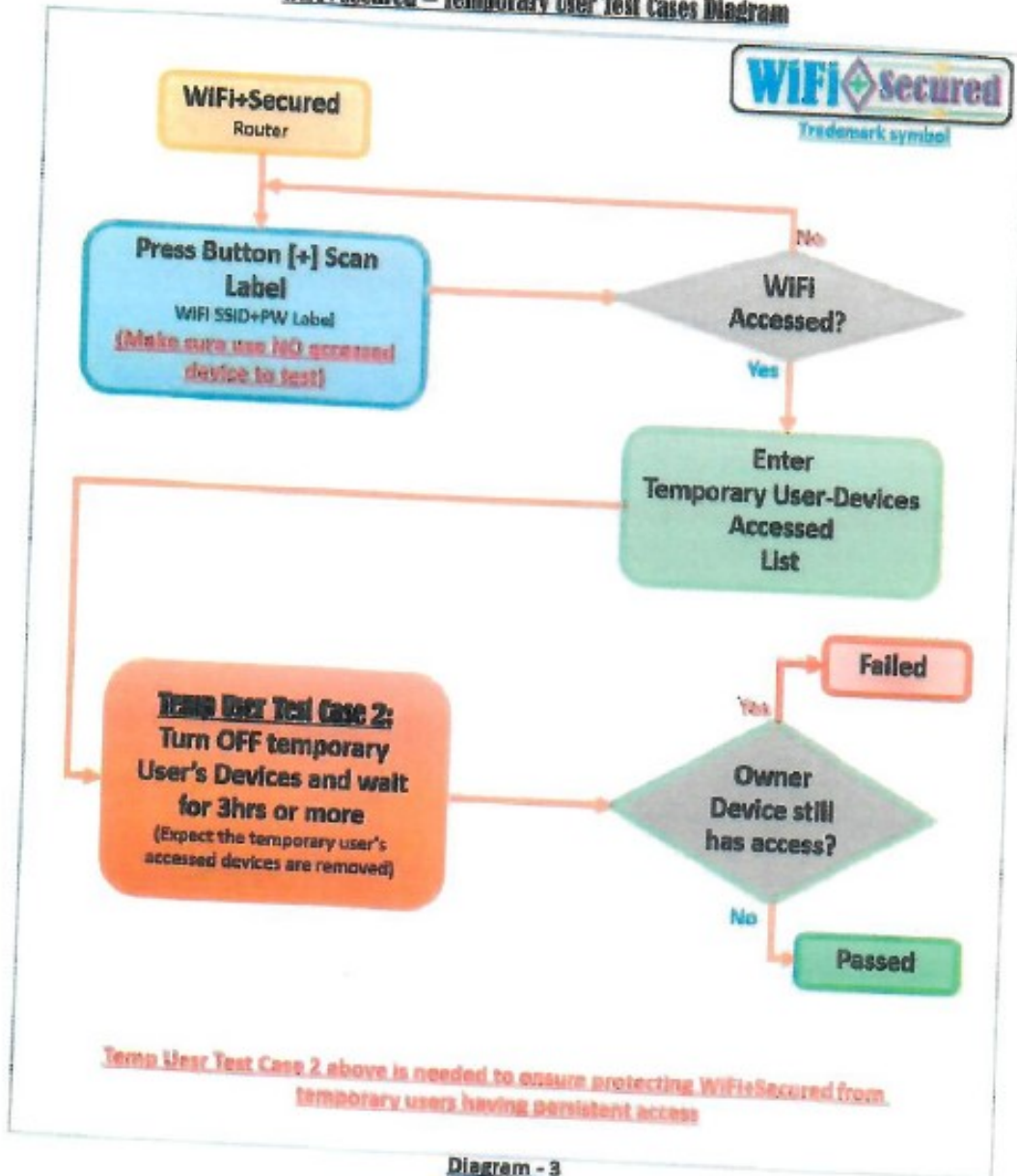


Diagram - 3

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

WiFi+Secured -- Owner Test Cases Diagram

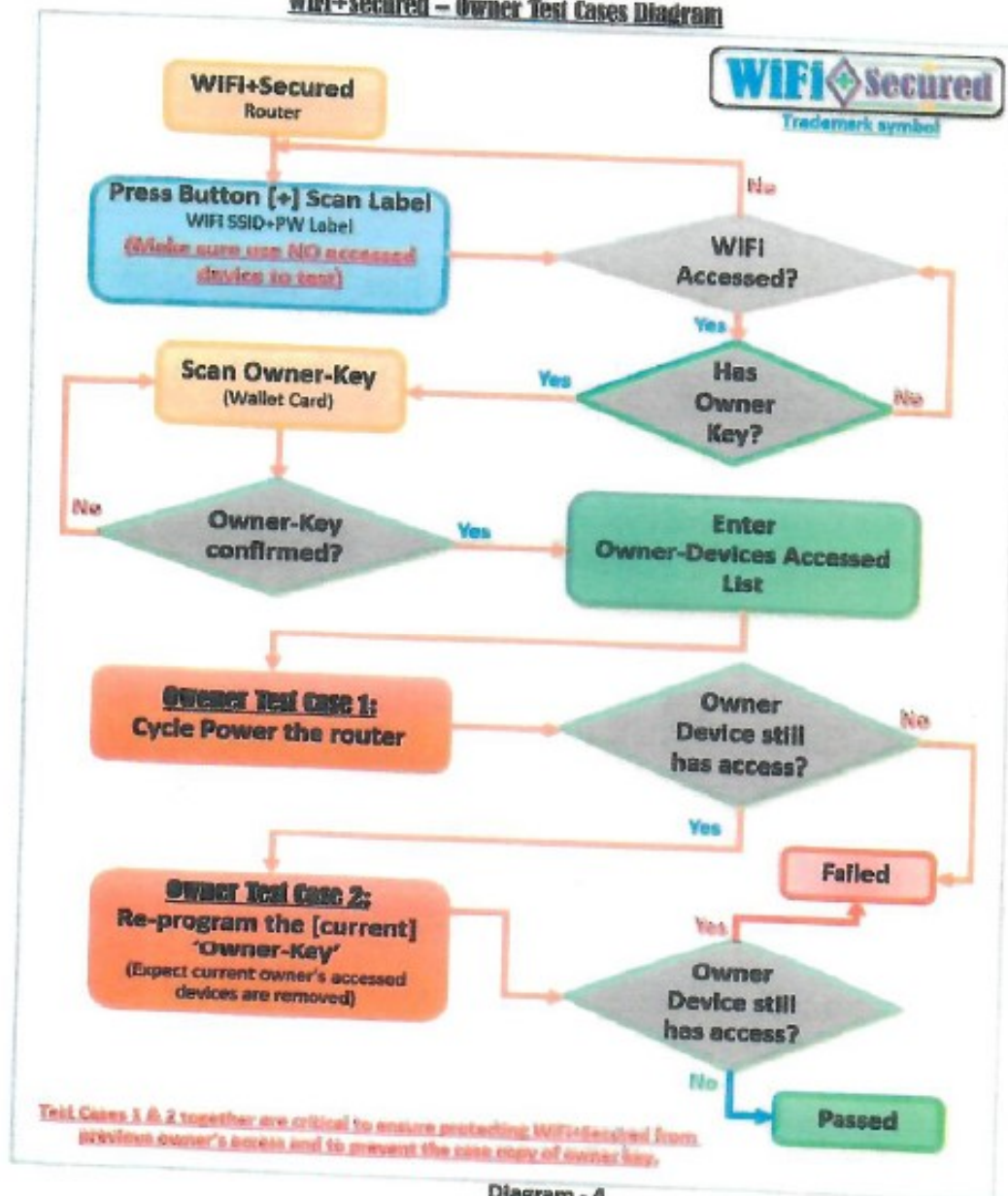
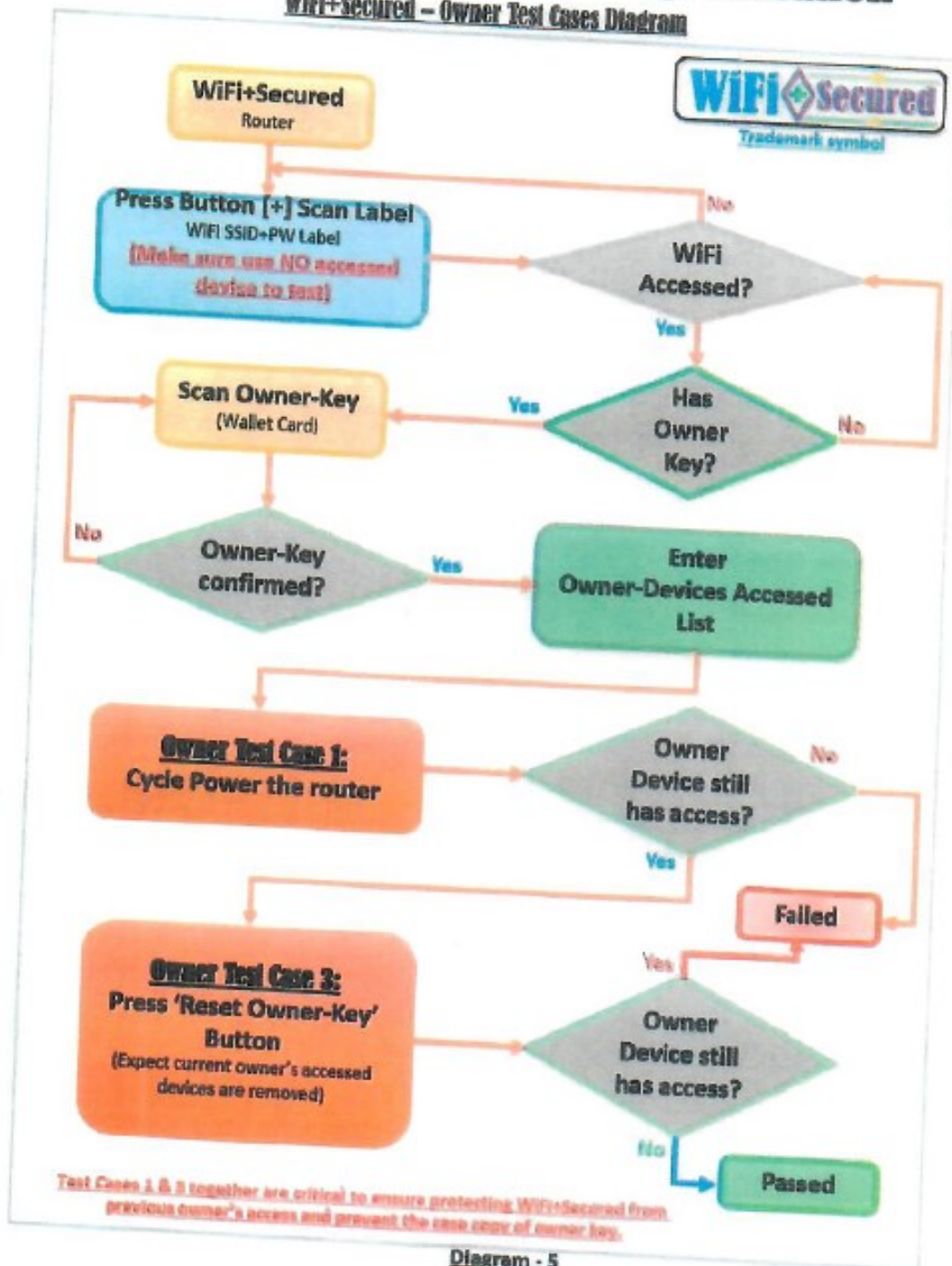


Diagram - 4

New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

WiFi+Secured -- Owner Test Cases Diagram



New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

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.





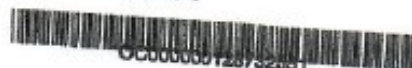
UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 3716(a) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
29/788,607	08/07/2021	2913	1020		1	1

Henry Viet Pham
805 S Hilda St
Anaheim, CA 92806

CONFIRMATION NO. 1396
FILING RECEIPT



Date Mailed: 08/29/2021

Receipt is acknowledged of this non-provisional design patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Henry Viet Pham, Anaheim, CA;

Applicant(s)

Henry Viet Pham, Anaheim, CA

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/28/2021

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 29/788,607**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

Way to protect WIFI Network from Hackers

Preliminary Class

D14

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process simplifies the filing of patent applications on the same invention in member countries, but does not result in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.