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,

www.TheCloudOSCenter.com

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

www.TheCloudOSCenter.com

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

www.TheCloudOSCenter.com

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]:[SKEY143da523ADFasdfsa7894SADe0kla!]

(SSID12ADS64KGD772ADFADF3123613413):(SKEY143da523ADFasdfsa7894SADe0kla!)

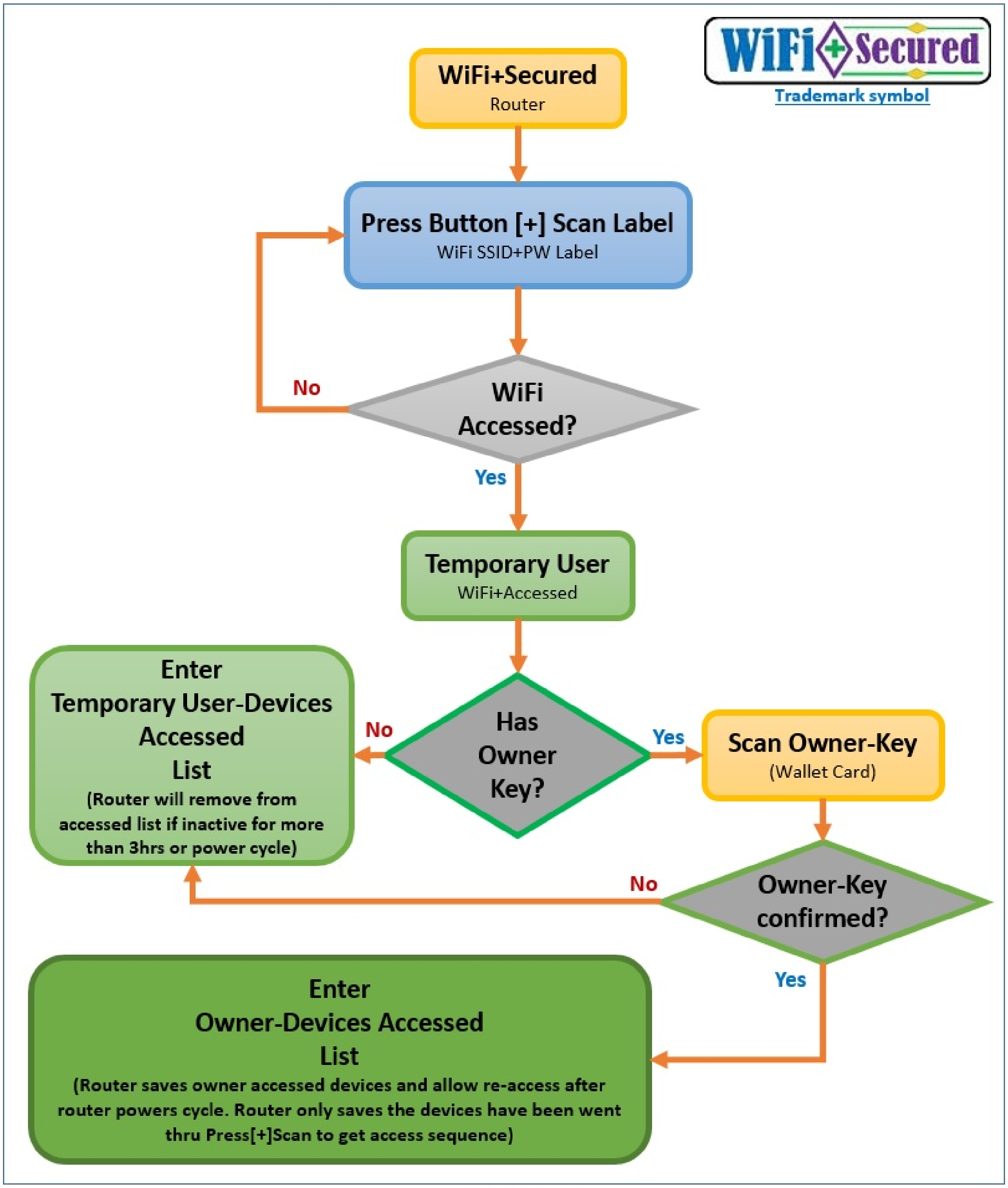
<SSID12ADS64KGD772ADFADF3123613413>:<SKEY143da523ADFasdfsa7894SADe0kla!>

www.TheCloudOSCenter.com

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

Henry V. Pham

WiFi+Secured - Use Case Diagram



WiFi Secured
Trademark symbol
WiFi+Secured
Router
Press Button [+] Scan Label
WiFi SSID+PW Label
No
WiFi Accessed?
Yes
Temporary User
WiFi+Accessed
Enter Temporary User-Devices Accessed List
(Router will remove from accessed list if inactive for more than 3hrs or power cycle)
No
Has Owner Key?
Yes
Scan Owner-Key
(Wallet Card)
No
Owner-Key confirmed?
Yes
Enter Owner-Devices Accessed List
(Router saves owner accessed devices and allow re-access after router powers cycle. Router only saves the devices have been went thru Press[+]Scan to get access sequence)

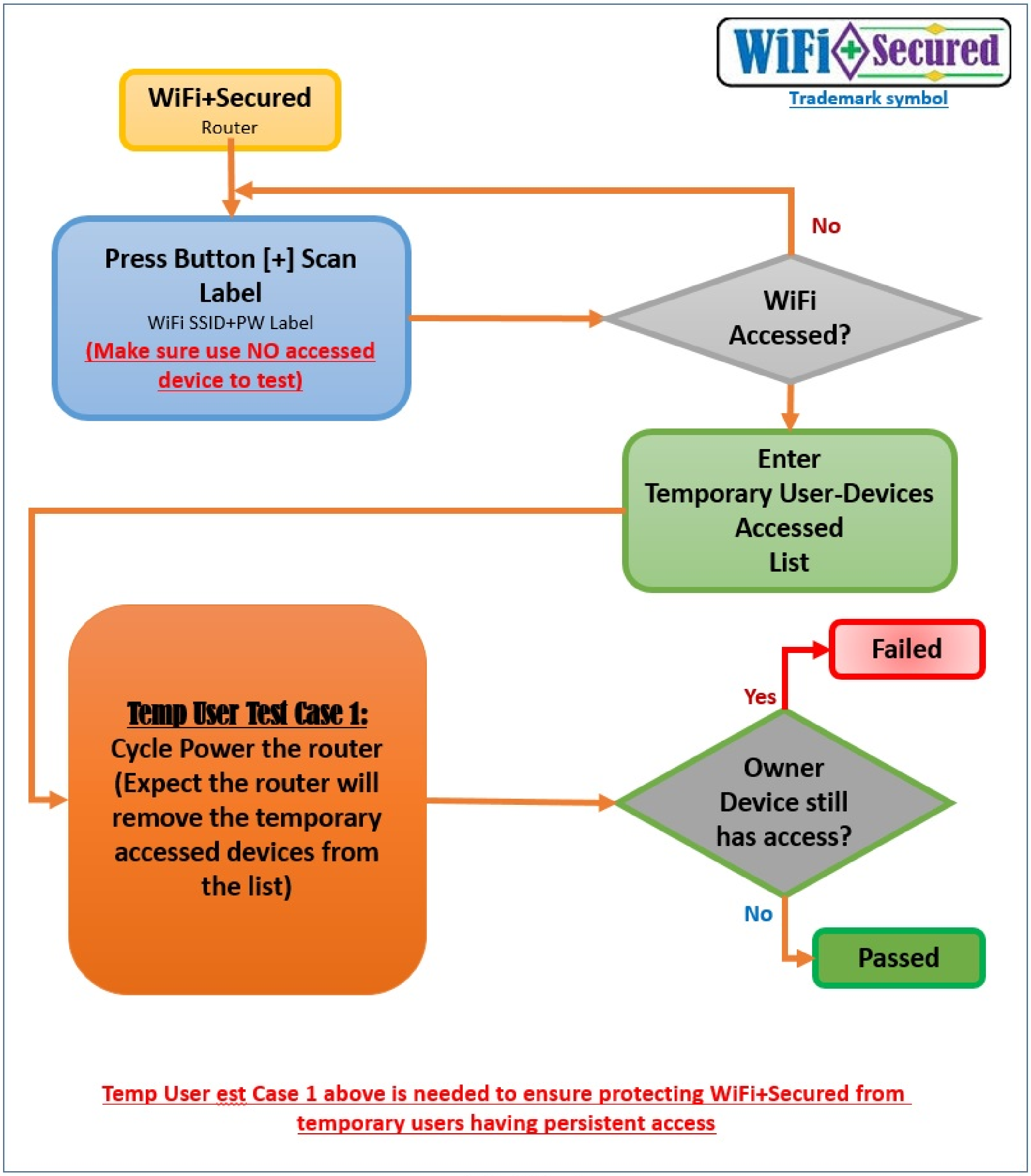
Diagram - 1

www.TheCloudOSCenter.com

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

Henry V. Pham

WiFi+Secured – Temporary User Test Cases Diagram


WiFi+Secured
Trademark symbol
WiFi+Secured
Router
Press Button [+] Scan Label
WiFi SSID+PW Label
(Make sure use NO accessed device to test)
No
WiFi Accessed?
Enter Temporary User-Devices Accessed List
Temp User Test Case 1:
Cycle Power the router (Expect the router will remove the temporary accessed devices from the list)
Yes
Failed
Owner Device still has access?
No
Passed

Temp User est Case 1 above is needed to ensure protecting WiFi+Secured from temporary users having persistent access

Diagram - 2

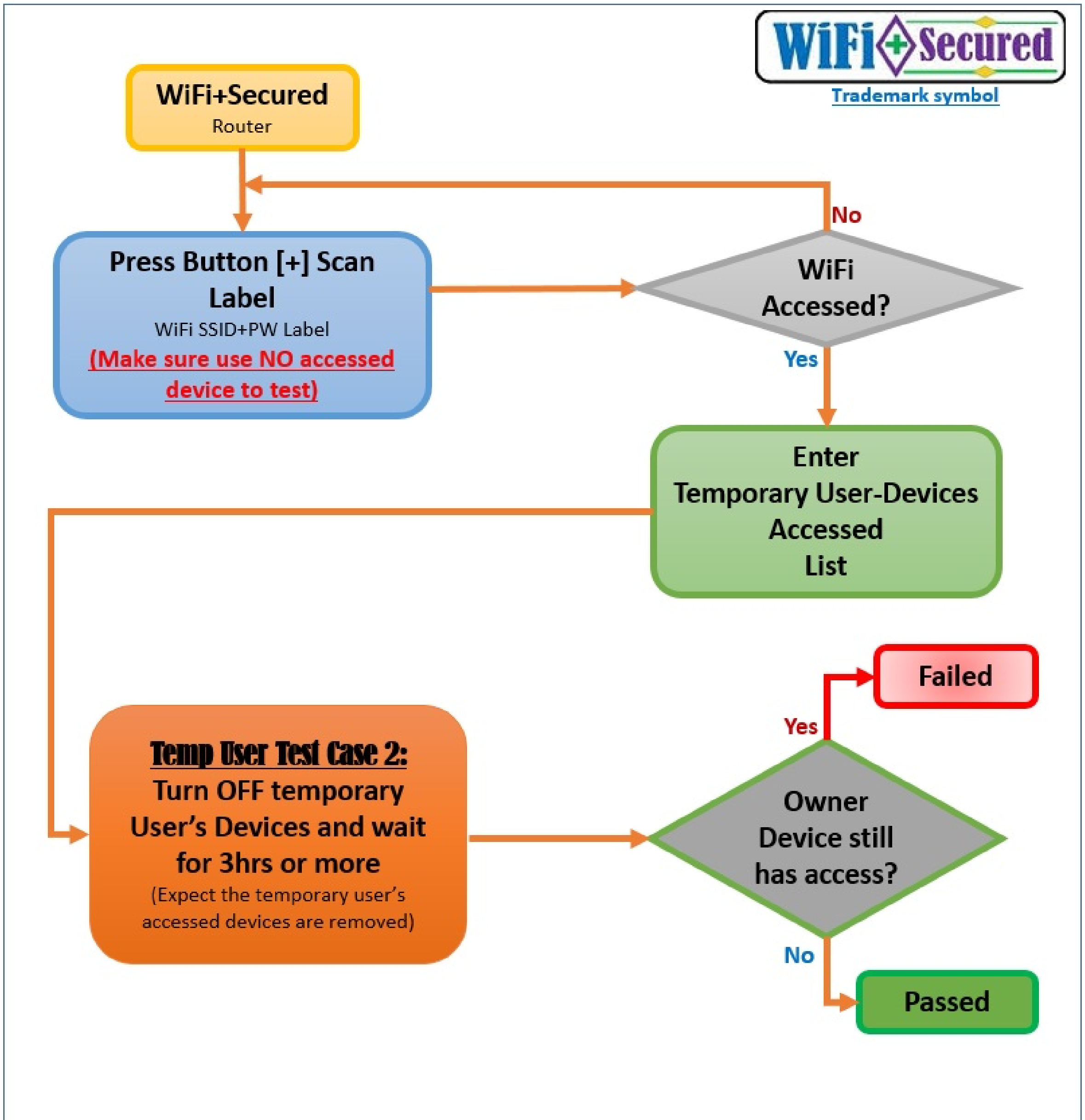
COPYRIGHTED

www.TheCloudOSCenter.com

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

Henry V. Pham

WiFi+Secured – Temporary User Test Cases Diagram


WiFi+Secured
Trademark symbol
WiFi+Secured
Router
No
Press Button [+] Scan Label
WiFi SSID+PW Label
(Make sure use NO accessed device to test)
WiFi Accessed?
Yes
Enter Temporary User-Devices Accessed List
Failed
Yes
Temp User Test Case 2:
Turn OFF temporary User's Devices and wait for 3hrs or more
(Expect the temporary user's accessed devices are removed)
Owner Device still has access?
No
Passed

Temp Uesr Test Case 2 above is needed to ensure protecting WiFi+Secured from temporary users having persistent access

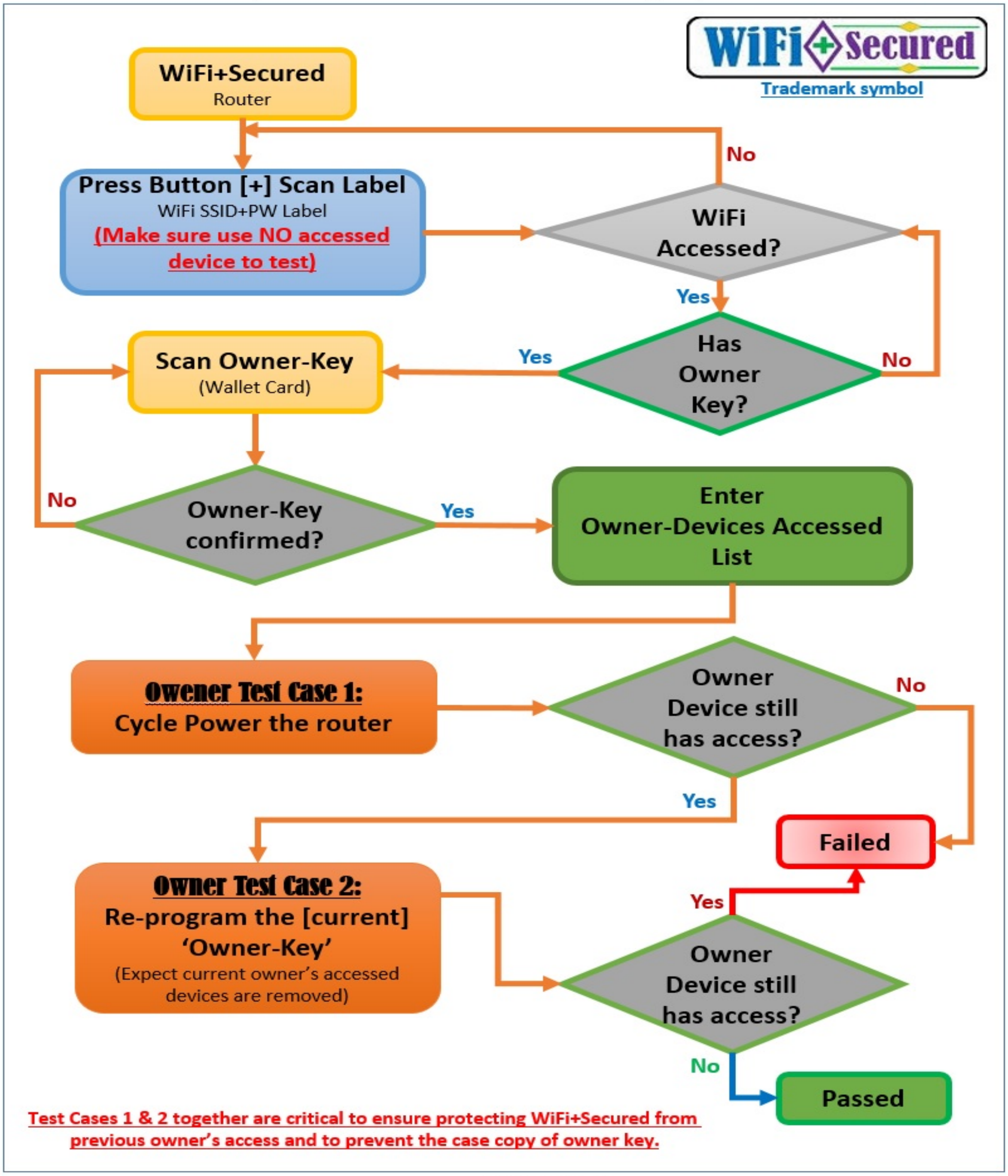
Diagram - 3

www.TheCloudOSCenter.com

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

Henry V. Pham

WiFi+Secured – Owner Test Cases Diagram



WiFi+Secured
Router
WiFi Secured
Trademark symbol
No
Press Button [+] Scan Label
WiFi SSID+PW Label
(Make sure use NO accessed device to test)
WiFi Accessed?
Yes
Has Owner Key?
No
Yes
Scan Owner-Key
(Wallet Card)
No
Owner-Key confirmed?
Yes
Enter Owner-Devices Accessed List
Owener Test Case 1:
Cycle Power the router
Owner Device still has access?
No
Yes
Failed
Owner Test Case 2:
Re-program the [current] 'Owner-Key'
(Expect current owner's accessed devices are removed)
Yes
Owner Device still has access?
No
Passed

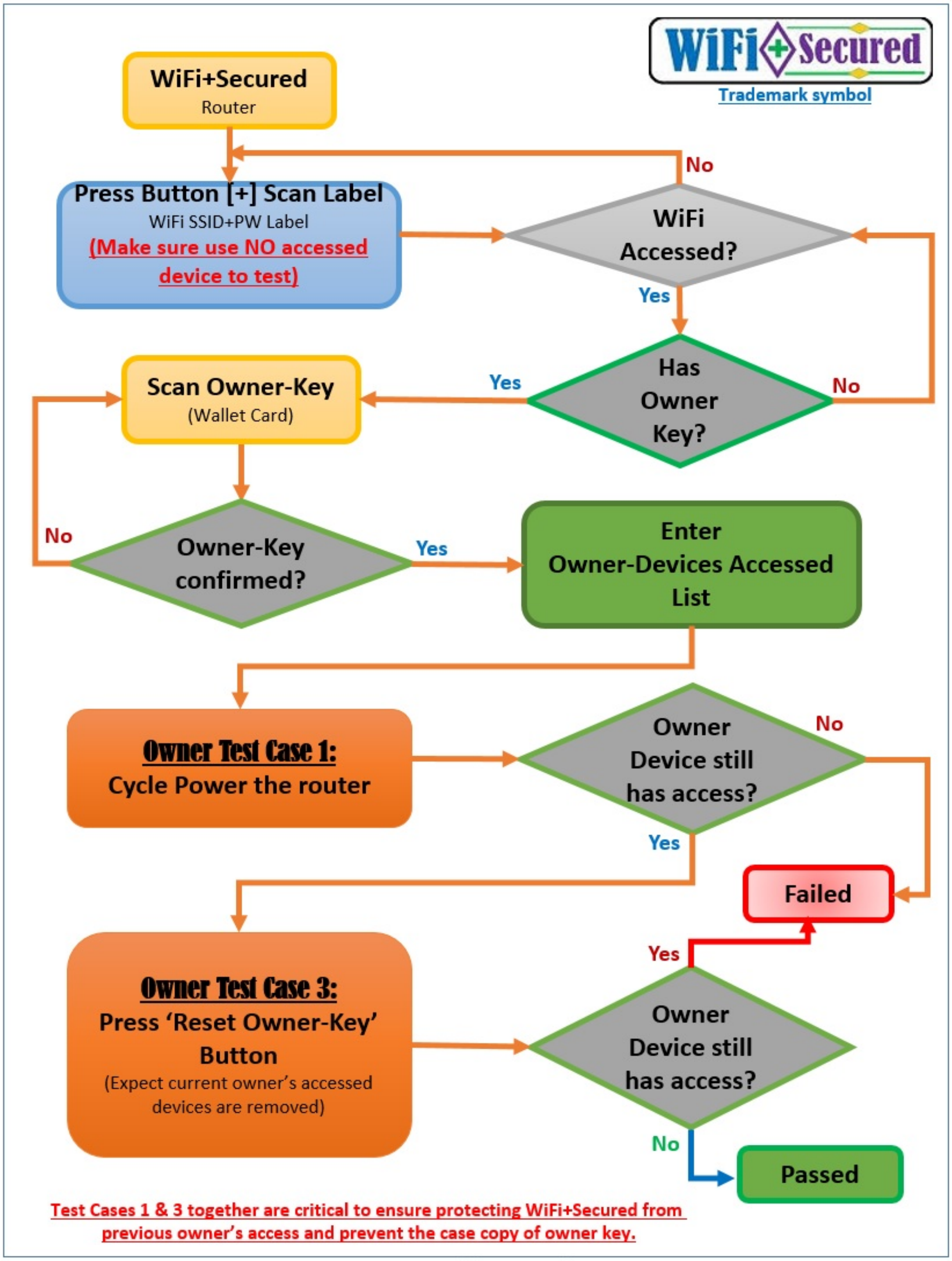
Test Cases 1 & 2 together are critical to ensure protecting WiFi+Secured from previous owner's access and to prevent the case copy of owner key.

Diagram - 4

CONFIDENTIAL

www.TheCloudOSCenter.com

WiFi+Secured – Owner Test Cases Diagram


WiFi+Secured
Trademark symbol
WiFi+Secured
Router
Press Button [+] Scan Label
WiFi SSID+PW Label
(Make sure use NO accessed device to test)
No
WiFi Accessed?
Yes
Has Owner Key?
Yes
No
Scan Owner-Key
(Wallet Card)
No
Owner-Key confirmed?
Yes
Enter Owner-Devices Accessed List
Owner Test Case 1:
Cycle Power the router
Owner Device still has access?
No
Yes
Failed
Yes
Owner Test Case 3:
Press 'Reset Owner-Key' Button
(Expect current owner's accessed devices are removed)
Owner Device still has access?
No
Passed

Test Cases 1 & 3 together are critical to ensure protecting WiFi+Secured from previous owner's access and prevent the case copy of owner key.

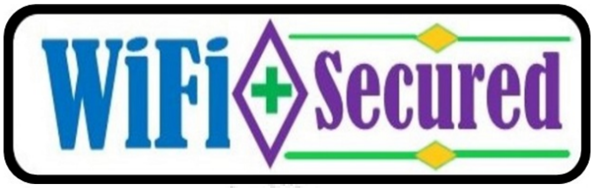
Diagram - 5

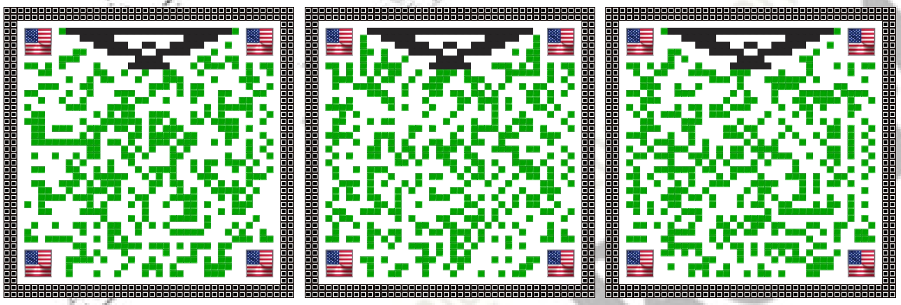
www.TheCloudOSCenter.com

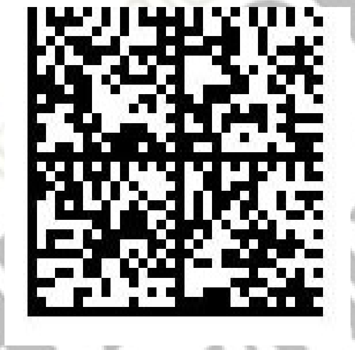
New Way to protect WiFi Network from Hackers (WiFi [+] Secured) -- Specification

Henry V. Pham

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.







COPYRIGHT PROTECTED
--HVPHAM
Henry V. Pham <Henry...@TheCloudOSCenter.com>
www.TheCloudOSCenter.com