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-keylabel 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 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 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.

New Way to protect WiFi Network from Hackers

- 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.
- 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.

New Way to protect WiFi Network from Hackers

- 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.

- 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 accessare 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 supportthe 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.

New Way to protect WiFi Network from Hackers

- 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.

- 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 thetemporary Network access with AuthenticationUser 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

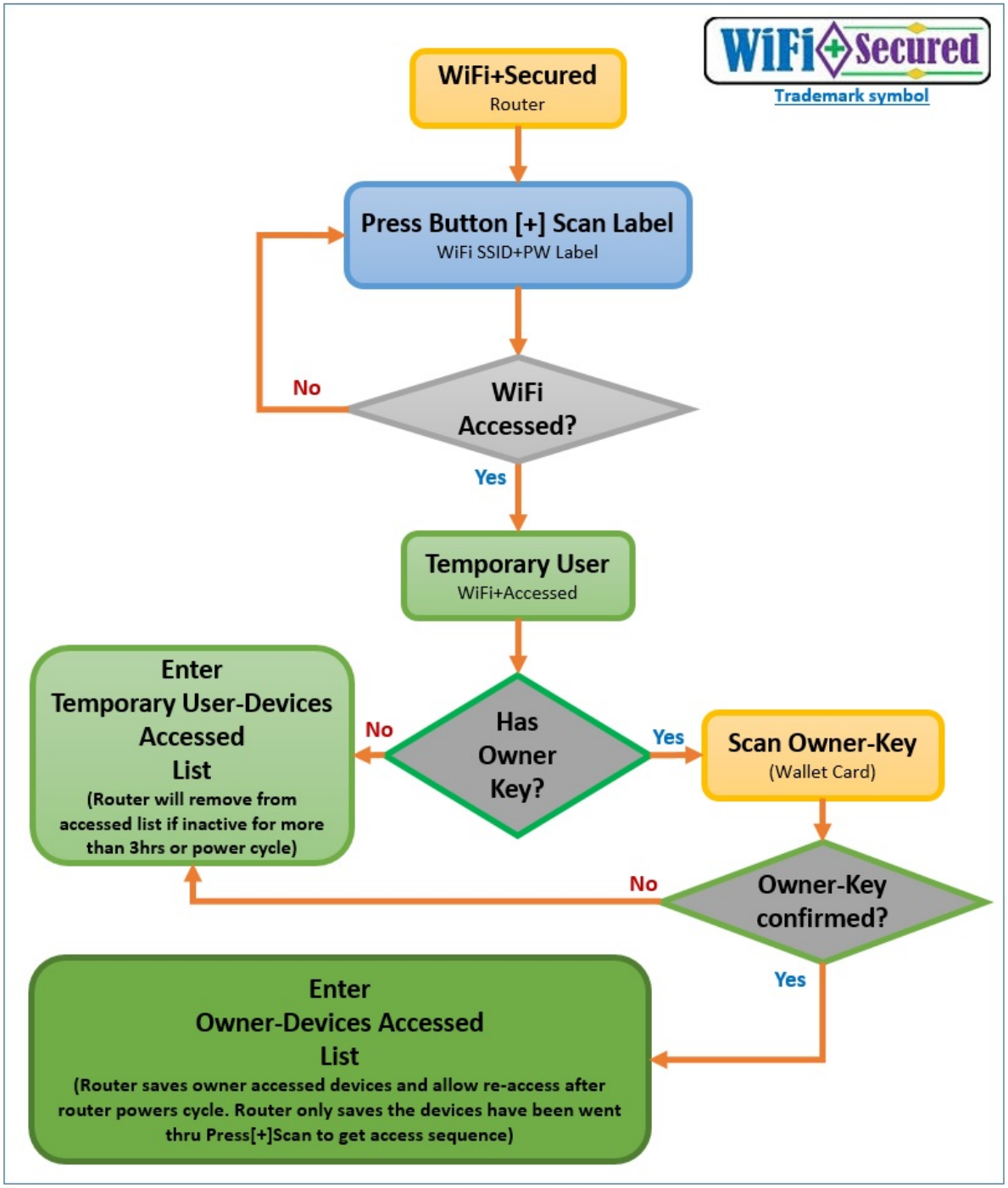

Diagram - 1

New Way to protect WiFi Network from Hackers

WiFi+Secured – Temporary User Test Cases Diagram

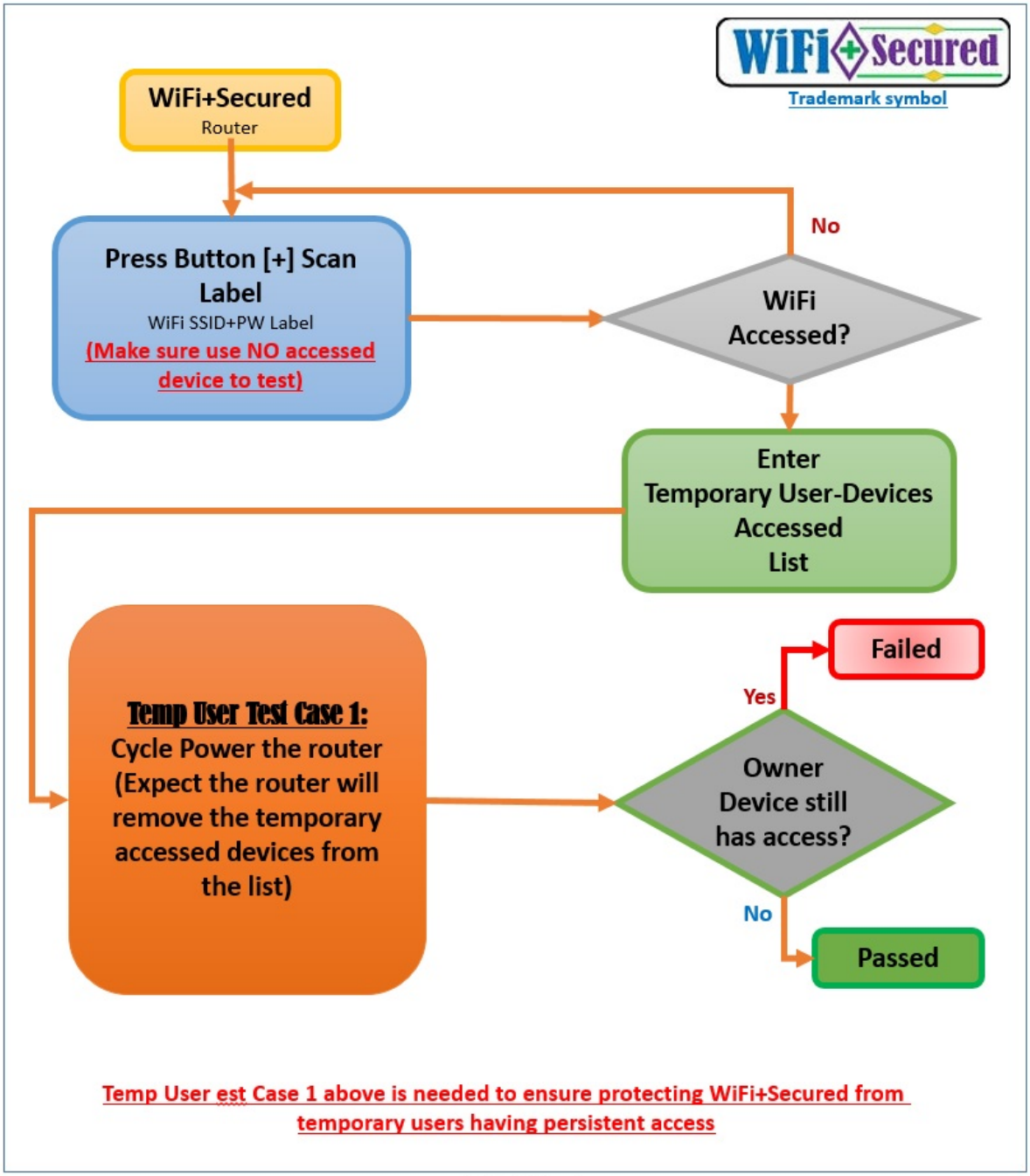

Diagram - 2

New Way to protect WiFi Network from Hackers

WiFi+Secured – Temporary User Test Cases Diagram

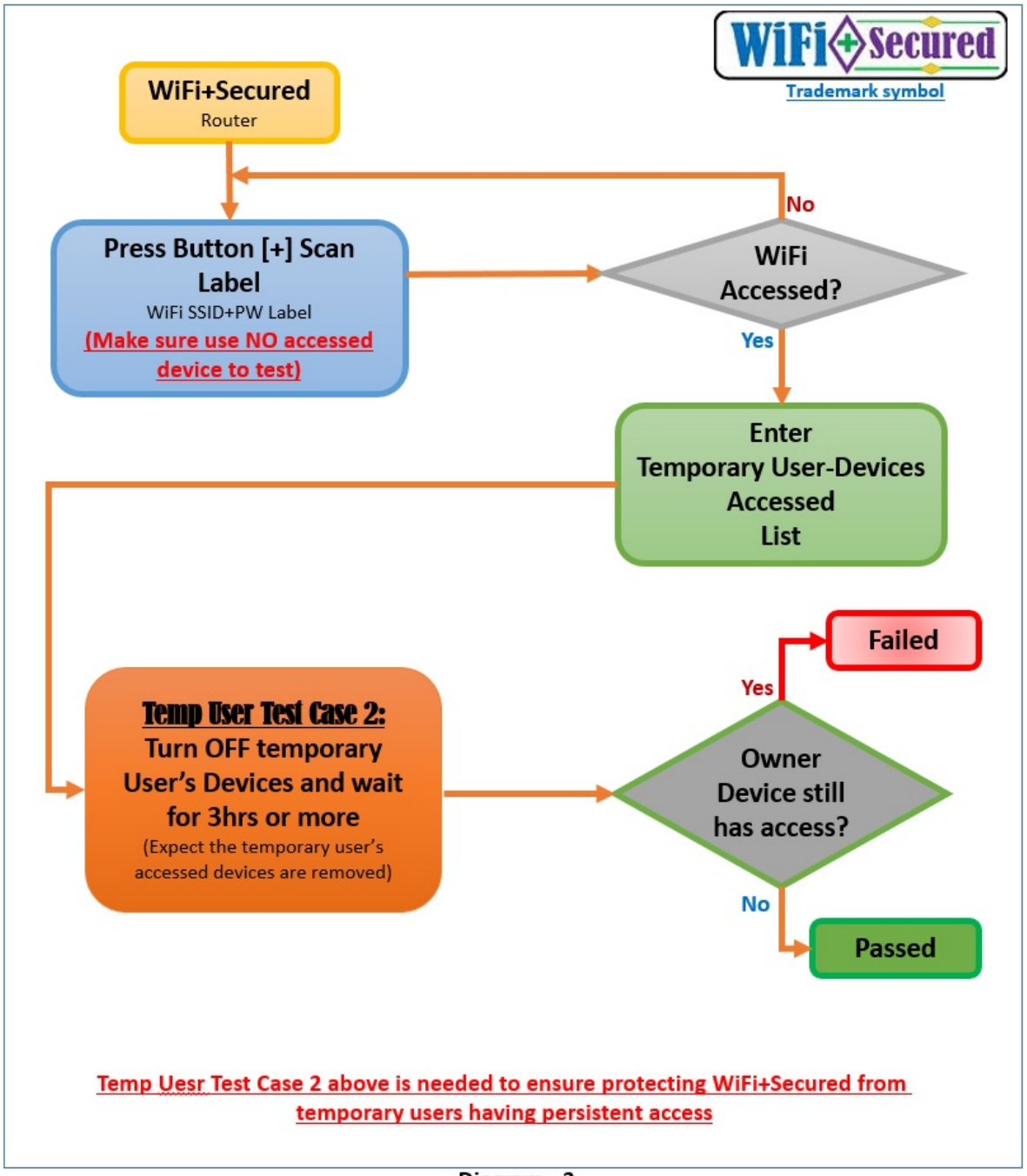

Diagram - 3

New Way to protect WiFi Network from Hackers

WiFi+Secured – Owner Test Cases Diagram

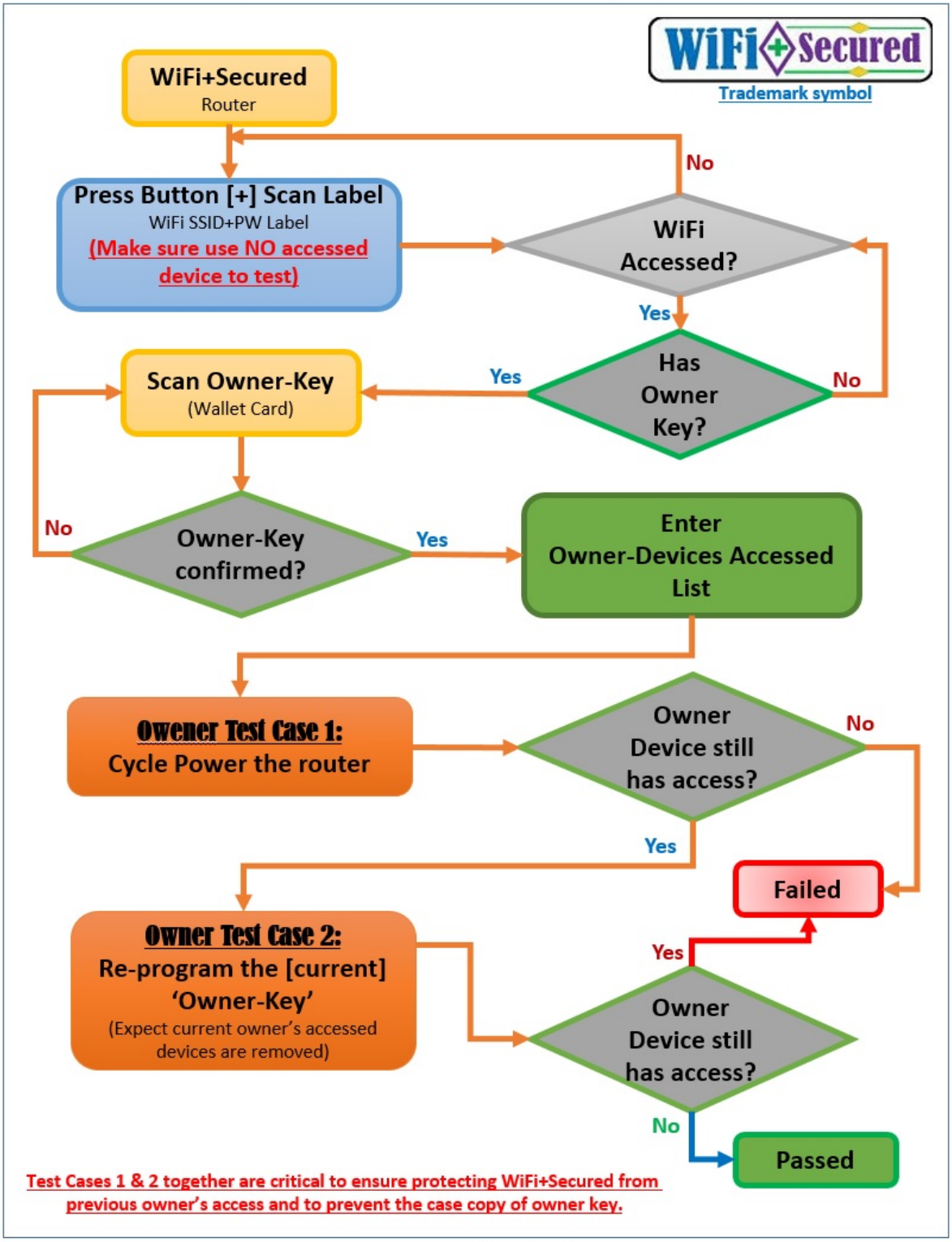

Diagram - 4

New Way to protect WiFi Network from Hackers

WiFi+Secured – Owner Test Cases Diagram

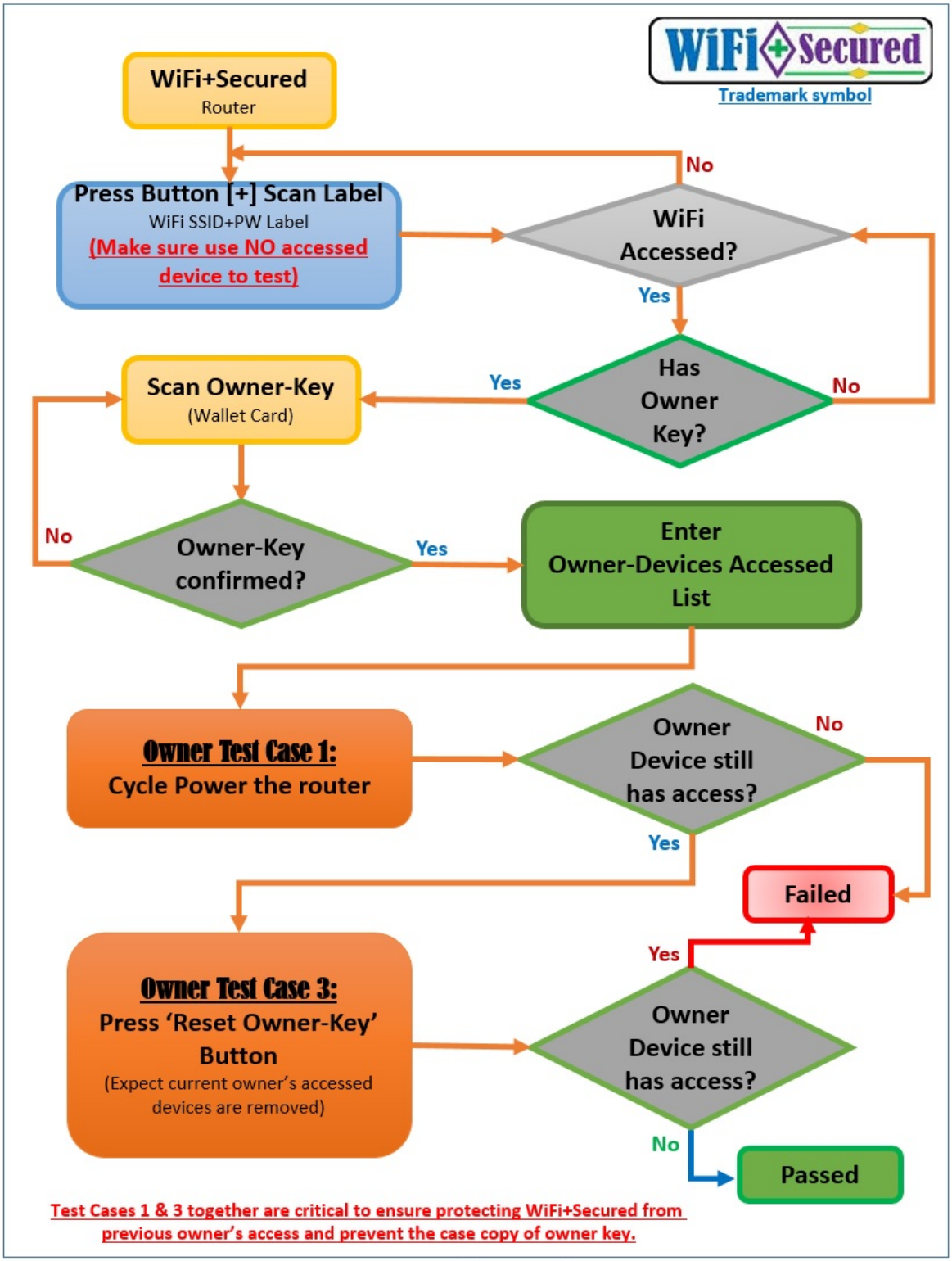

Diagram - 5

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 officesin 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.