RouterCheck Test Plan

January 5, 2015

Sericon Technology Inc.
71 Marquette Ave.
Toronto, Ontario
M6A 1X8

Phone: 416.781.3988
E-mail: smithsa@sericontech.com

Contents

1 Introduction

RouterCheck is a tool for checking the security of home routers. It currently runs as an Android application and communicates with a server in the cloud to test all aspects of your network, both inside and out.

This document is used by Sericon Technology as a guide for how to test RouterCheck. Anyone interested in seeing how RouterCheck works can run the tests suggested here, and see how RouterCheck reacts when you configure something on your router that has a security implication.

1.1 Target Audience

This guide is meant for those people who wish to test RouterCheck. To get the most out of it, it is assumed that you have access to your router, can log into it, and have some familiarity with how to configure it.

It's also assumed that you've already installed RouterCheck on an Android device and know how to use it. If not, please see RouterCheck Installation and Usage .

1.2 Choosing a router to test

Okay, you should test what you have. Be aware though that some of what RouterCheck needs to do is figure out exactly which router it's interacting with (and frankly, that's a lot more difficult to do than it sounds). So for the best results, some routers will test better than others – use these guidelines:

1.2.1 Popular routers are better

If you use a popular router, or more importantly a popular brand, it's more likely we've tested it or at least something similar. We'd suggest choosing from one of these vendors:

- ASUS
- Belkin
- Buffalo

- D-Link
- Linksys
- Netgear
- TP-LINK
- TRENDnet
- ZyXEL

1.2.2 Basic Authentication > Web Form

The way that you log into a router will affect how RouterCheck will interact with it (because RouterCheck attempts to programmatically log in to see if you are using a bad password).

RouterCheck is much more successful with routers that use Basic Authentication (where the little login dialog is provided) rather than a web form (where there are form fields on the page). This will be changed in the future as we test more routers with web forms.

1.3 Note about configuring routers for the tests

Unfortunately, there are no standards at all about what a router's user interface should look like. What may be called **Open Ports** on one router may be called **Port Forwarding** on another. A setting on one router may be on the **LAN** tab and on the **Firewall** tab on another.

We've tried to be as generic as possible when describing what to do, but you may need to do a little router archeology to find the settings that you'll need to change. Your router's manual may be a good place to start. If you still can't figure it out, you might check a few nice websites such as:

- http://setuprouter.com/
- http://portforward.com/

One final thought: RouterCheck assumes that when it goes to a router's home page it will be confronted with a request for authentication (either Basic Authentication or a web form). Some routers do not provide this if someone is already logged in, instead it will simply put an error message up (we're looking at you Asus).

If things are working funny, you may want to log out of the router before you start to run RouterCheck.

2 Test Setup

2.1 Requirements

Before running RouterCheck ensure that you have the following:

- A connection to a network that you have permission to test on. This network should contain the router that will be tested.
- An Android device that runs at least Android 3.0 (Honeycomb). That means pretty much any reasonably modern device that runs Android. It's preferable to run RouterCheck on a tablet rather than a phone, and it's preferable to run RouterCheck in landscape rather than portrait orientation.
    - We've tested RouterCheck on several Android devices up to and including Android 5.0 (Lollipop).

2.2 Router Setup

Setting up your router to test RouterCheck is pretty easy if you keep it simple. When setting up the router ensure that

- There is connectivity to the internet
- There is only a single router running in your network. Do not cascade routers since the first router will be seen from inside the network and the second router will be seen from outside of the network. This provides you with an incomplete test, and will make it difficult to confirm that the things you'll change have really been changed.

3 The Tests

Each of these tests is designed to show how RouterCheck can determine that a vulnerability exists based on how the router has been configured. In each test, you are to change the configuration and then run RouterCheck to see whether that change was detected.

Not all tests will be available for all routers, since some of the configuration changes might not be supported by a given router.

3.1 External Access

In these tests, we want to see what happens when services on the router are exposed on the internet. While it's true that hackers don't necessarily need any services exposed to attack a network (e.g. the router is still vulnerable to infected computers within the firewall, CSRF attacks, etc.) providing an attacker with external access will only make his job easier. So, it's important to know exactly what is and isn't exposed on the network.

3.1.1 Remote Administration

Remote Administration is a convenience feature to allow the router to be administered from across the internet. It's highly dangerous since hackers are only a password guess away from being able to completely control everything that the router does (including easily downloading any malware that they want onto the device).

What To Do

Enable Remote Administration on the router. This feature is typically in the settings for *Administrator,* and may be called something like:

- Enable Remote Administration
- Enable Web Access From WAN

What To Expect

RouterCheck should be able to find an open port on 80, 8080, 443, 8443, or any combination of these depending on how the router works.

3.1.2 Ping

Ping is a simple network protocol to determine whether a device is up and running on the internet. In order for a device to be “pingable”, it must run a small service to respond to pings.

Ping is a great help when diagnosing problems with large servers, but there is very little reason that a home-based router should ever respond to a ping. However, many router vendors enable the ping service on their devices which are often used by hackers to help determine if there is a target at a given IP address to attack. This is a security vulnerability, and so, ping should always be turned off of the router if possible.

What To Do

Some routers allow you to turn ping on and off, others do not. The ones that do typically have this setting on the *WAN* or *Firewall* tab. The setting could be called something like:

- Respond Ping Requests From WAN

What To Expect

RouterCheck will report a warning when ping is on.

3.1.3 Open Ports

Opening or forwarding ports on your router’s firewall allows other computers on the internet to get access to services exposed by the computers on the network.

Opening ports can be dangerous, and should only be done by people who understand the security implications that it creates.

What To Do

Open a port on the router’s firewall and have it forwarded to a service running on one of the computers on the network. Ensure that the service is exposed on the internet, and if not, the port is not “truly” open.

Opening a port is a tricky thing to configure, so you might want to look at your router’s manual or at http://portforward.com/ to see what you need to do.

It’s probably wise to open a port on the router for a common service such as http, telnet, or ftp.

What To Expect

RouterCheck should report that the port is really open.

3.2 Administrator Password

The Administrator password is important because it allows you to log into the router and modify it in any way that you want. Hackers who take advantage of default or common passwords have an easy time exploiting the systems that they wish to attack.

RouterCheck tests the router for both the default password for the router model that it's testing, as well as a list of common passwords that hackers typically try when they attempt to break into a network.

3.2.1 Use Default Password

What To Do

Change the administrator's password (Not the WiFi password that's used to gain access to the network) to its default. If you don't know what the default password is, then look through the router's manual to find out or go to http://www.routerpasswords.com/.

Changing the password typically involves going to the *Administrator* page and typing in a new password.

If your router is already set up to use the default password, you should now feel shame.

What To Expect

RouterCheck will warn you that you are using a bad password.

3.2.2 Use Common Password

What To Do

Run the test as above, but instead of a default password, use a poorly-chosen common one such as:

- abc123
- qwerty

What To Expect

RouterCheck will warn you that you are using a bad password.

3.3 Connectivity

3.3.1 Disconnect the router from the internet

RouterCheck requires many resources on the internet for it to fully work. However, if the router does not have internet access, some of the local RouterCheck tests may still be run.

What To Do

Disconnect the router from the internet. This can easily be done by pulling out the cable leading to the modem.

WARNING: Disconnecting your router from the internet will knock everyone off of your network. Your spouse and/or children may not be so happy about this. So, if this test will negatively impact your life, it's better to skip it.

What To Expect

RouterCheck will run, but certain checks will not be done such as the search for open ports which is done by the RouterCheck Server.

3.4 WiFi Security

WiFi security provides encryption for data that is being transmitted between the device and the router. The password that controls this is the "WiFi password" that enables people to connect to your network.

In these tests we'll modify the way that the router uses WiFi security to see that RouterCheck informs you when you have insufficient security that can easily be broken. Currently, only WPA2 encryption should be used, as WPA and WEP have both been shown to be easily broken.

3.4.1 Turn off WiFi Security

Turn off WiFi security and try to run an open system that allows connections to be made without a password, or enable WEP that does require a password, but has been shown to not be secure.

What To Do

Turn off WiFi security by going to the *WiFi* or *Wireless* tab, and look for something called *Security* or *Authentication Method*. Change this to *None* or *Open System.*

What To Expect

RouterCheck will warn you that no security is being used.

3.4.2 Turn WPS on/off

WPS (WiFi Protected Setup) is a method that was created to enable people to easily set up their WiFi security. Unfortunately, the protocol was not so well thought through, and it contains some serious vulnerabilities that can allow hackers to easily connect to your router.

The level of support for WPS varies greatly between different routers. Some older routers will not support WPS at all. Others will support it by default and not allow you to change the settings. Some routers will allow you full control over whether WPS is being used. Unfortunately, many of these devices will ship with this set to *ON* by default.

What To Do

Disable WPS by going to the *WiFi* or *Wireless* tab, or perhaps there's a dedicated WPS tab, and look for how to turn it off. Note that some routers will not allow you to do this.

What To Expect

RouterCheck will warn you that WPS is being used.

3.5 DNS

Maintaining the integrity of a home network's DNS service is critical to that network's security. When hackers compromise this aspect of the network, they have free reign to launch additional attacks at will.

The most dangerous aspect of a compromised DNS system is that it's often very difficult to even diagnose that the system has been compromised.

Many routers have built-in DNS servers which hide the true source of any DNS resolution due to a lack of transparency. This means that even if you think you know where things are being resolved, it's often difficult to prove it, thereby creating a sense of doubt.

What To Do

Modify the DNS Server settings for the router and point them to a known and trusted DNS Server such as the Google DNS Server at 8.8.8.8.

What To Expect

Verify that RouterCheck sees this change and reports that things are okay. Be aware that if the DNS Server settings contain a local server on the router (e.g. the DNS settings look like 192.168.x.x) it will give a warning.

In the Future

Detecting a compromised DNS system is quite difficult, and is fertile ground for some research. We have some proprietary methods that are being developed that will make RouterCheck a very strong solution.

4 Other Things to Check

4.1 Router Information Found

RouterCheck will report on the vendor and model that it believes the router that it is testing is. Check to see that it's correct.

4.2 CVE Information

The CVE (Common Vulnerabilities and Exposures) database is used to inform the user what vulnerabilities his router has. The information that RouterCheck provides can be corroborated with the true database by going to https://cve.mitre.org/ and searching for the router model.