The Real State of WiFi Security in the Connected Home

August 25, 2015

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

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

1 Abstract

Analyzing real-world data can teach us about the state of security in the connected home. RouterCheck, a tool for testing home router security, gathered real data from its large population of users around the world. We aggregated and analyzed this data, and we have developed insights and recommendations based on our findings.

We found that 85 percent of the home networks that were tested with RouterCheck had at least one vulnerability that could be avoided and fixed. Additionally, a tested network had on average 1.8 vulnerabilities. While the media reports on high-profile vulnerabilities that are found by security researchers, we believe that the typical home could benefit more by simply paying attention to the fundamentals of network security such as strong passwords and wireless encryption.

Additionally, we found that consumers who used a third-party security testing application like RouterCheck were able to fix their networking issues themselves. Users who tested their networks a second time showed a 20% drop in the number of vulnerabilities found.

2 Background and Methodology

Recently, computer security researchers have been very successful in finding new vulnerabilities in home networking equipment. The media have reported on high-profile bugs such as Misfortune Cookie[1] and NetUSB[2] and warned consumers about them. But how susceptible is the average home network to these problems? More importantly, how susceptible are home networks to lower-profile problems, such as poor passwords and open ports, and how do we mitigate these problems?

RouterCheck (www.RouterCheck.com) is a consumer tool that enables people without a computer security background to run a sophisticated security and vulnerability check of their home networks. It is currently deployed as an Android application[3], but it also communicates with a server in the cloud, so that the RouterCheck system views the same attack surface as a hacker.

After a check, RouterCheck presents the user with a list of vulnerabilities it found and instructions for fixing these problems. By aggregating the results from a large population of RouterCheck users, we can identify the true dangers in the connected home.

We collected the results presented in this document from RouterCheck users who checked their routers during May, June, and July of 2015. During that period, a diverse group of users in 133 different countries ran more than 24,000 individual checks.

Note: When RouterCheck tests a router, it does not gather any personally identifiable information about its users. In fact, personally identifiable information is not even available to RouterCheck.

3 Findings

We aggregated the results of the vulnerabilities found in the checks that users ran, and they are displayed in the graph below. On average, each user's check of a router resulted in 1.8 discovered vulnerabilities. We also found that 85 percent of the checks that were done discovered at least one vulnerability.

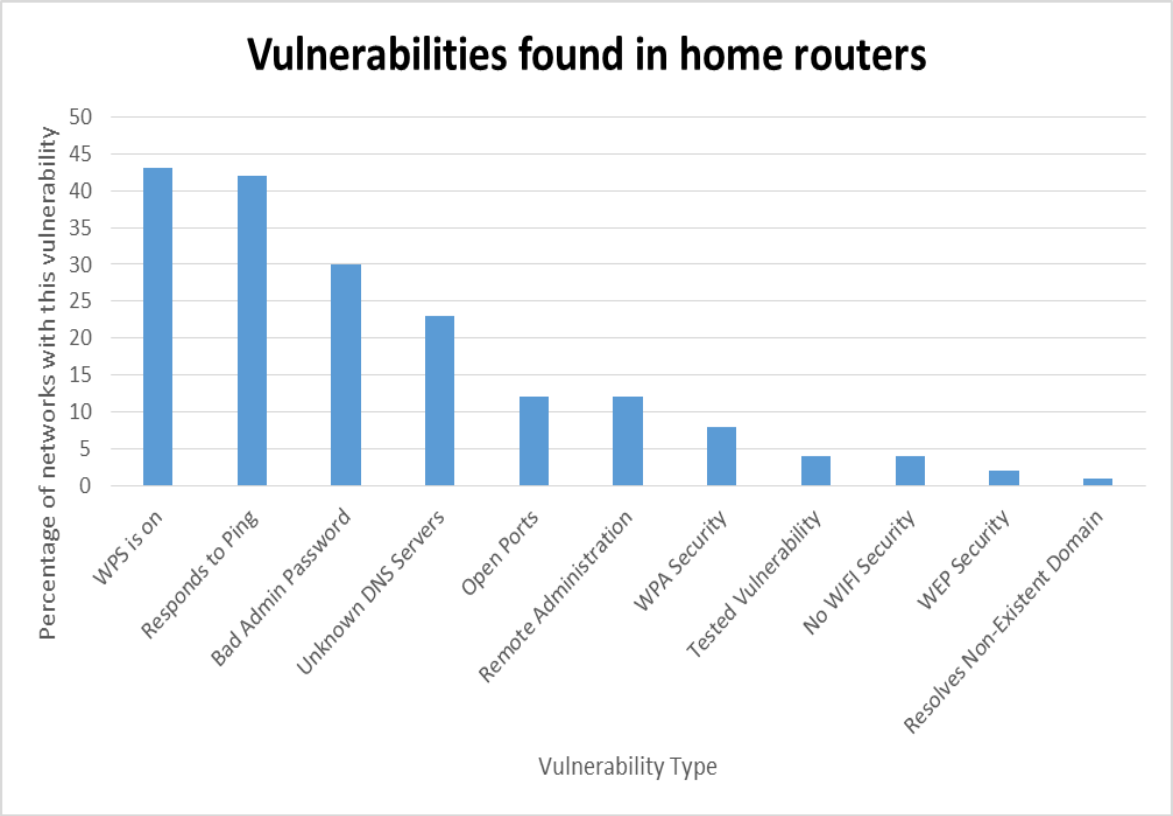

Figure 1- Graph showing the percentage of checks that found a certain class of vulnerability

3.1 Wireless Security

Wireless security prevents unauthorized devices from joining a home network. Currently, WPA2 is the only protocol that is considered to be sufficiently secure, because previous protocols (i.e. WEP[4], WPA[5]) have known vulnerabilities that enable unauthorized attackers to gain access to the network in a few hours at most. Wireless security protects users from attackers who are nearby.

RouterCheck determines the type of wireless security used in a network, and it has found the following insecure protocols in use:

- WPA: 8 percent
- No wireless security in use: 4 percent
- WEP: 2 percent

3.1.1 Insufficient Security

3.1.1.1 No security used

We were disturbed to see that 4 percent of the networks checked did not have any sort of wireless security at all. Upon further review, we realized that there are two different reasons why a network would have no security:

- **User ignorance and/or apathy**: We believe that many users either don't know or don't care about wireless security for their networks.
- **Guest Network**: Many routers allow a separate "Guest Network" to be run in parallel to the main network so that users can easily control what their guests do. Many of these networks don't use wireless encryption and instead request a password when first connecting.

Unfortunately, we have no way to distinguish between these two cases, although we believe that the majority of the cases are ignorance and apathy.

3.1.1.2 WEP and WPA

Although WEP and WPA have been obsolete for many years, they are still in use. We attribute some of this to older routers that do not have WPA2 available, but more importantly to users who do not know enough to understand the risks of each of the types of security. Vendors often do a poor job explaining the security options:

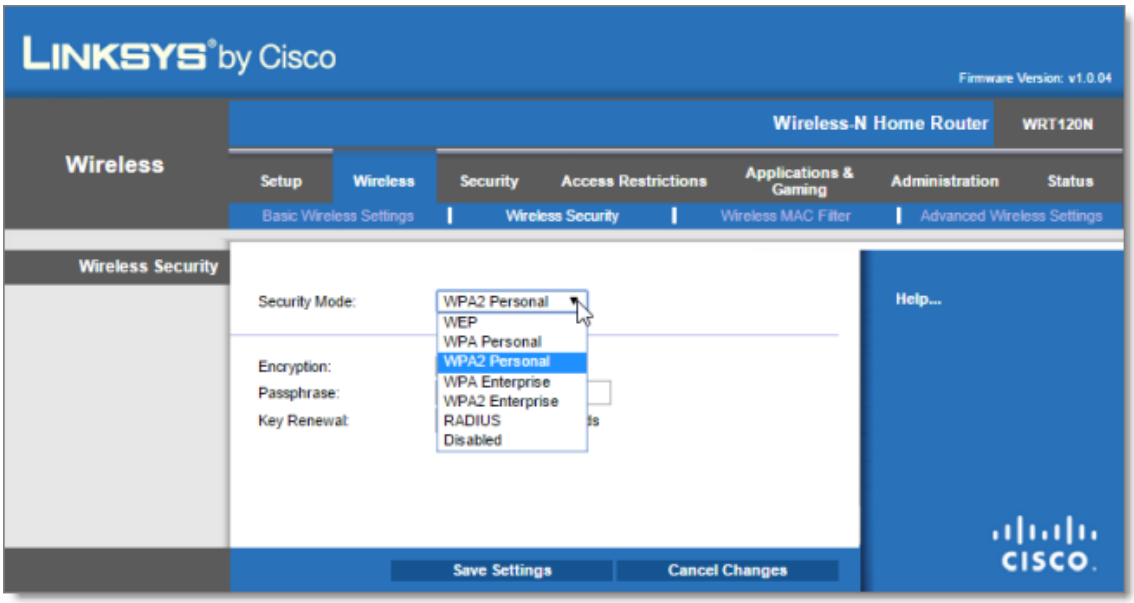

Figure 2- Setting the wireless security on a Linksys WRT120N

As we can see from the interface of a Linksys WRT120N router, users don't get a lot of help when it comes to router configuration. Choosing which of the 7 options to select for wireless security is very difficult if you don't know what the options mean. We believe that poorly designed interfaces such as this are responsible for the majority of poorly configured security for wireless routers.

3.1.2 WPS

WPS (WiFi Protected Setup)[6] is a system designed by the WiFi Alliance, and its support is mandatory for any device certified by that organization. WPS works alongside wireless security protocols like WPA2, and it exists solely to facilitate easier setting up of wireless security.

Unfortunately, in 2011 a serious flaw was found in this protocol, so that any router that actively uses WPS is susceptible to break-ins, even if WPA2 is also in use[7].

Forty-three percent of the routers that RouterCheck tested had WPS actively enabled.

3.2 Administrator Password

A router's administrator password prevents unauthorized users from accessing the router's administrator functions. A hacker who gains access to the administrator functions can do harm, such as modify the router's DNS settings, open ports on the router's firewall, or even run arbitrary code on the router itself. A compromised router

cannot protect the devices that it serves, and therefore we should treat any device on such a network as compromised too.

Many users falsely believe that since their router has no ports open to the WAN side of their network, this prevents a hacker from accessing the router's administrator interface and attempting to log in. This belief is incorrect: hackers can access the administrator interface from a CSRF[8] attack or from malware loaded onto a compromised device on the network. Therefore, a strong administrator password is vital to maintaining the security of every device on the network.

RouterCheck tests routers to determine whether the password is strong enough. However, this testing is not extensive. Since RouterCheck can determine the router's model, it can do a simple lookup for the default password and then test for it. It also tests for 25 other very common passwords (e.g. *password*, *qwerty*, *12345678*, etc.).

RouterCheck encounters routers using a poorly chosen password 30 percent of the time. Most of the time, these are default passwords that the user neglected to change. It's easy to dismiss this shocking number as "ignorant users", but we prefer to think of it as "poorly designed user experience".

3.3 External Connectivity

3.3.1 Open ports

Open or forwarded ports are dangerous because they give a remote hacker a foothold onto something within the home network to attack. A hacker who discovers an open port can see whether there are any known vulnerabilities to use against the application listening to that port.

Ports may be open for a variety of reasons, for example, to support a specific application such as a game, or to provide remote access to a device on the network, such as a NAS.

There are opened ports on 12 percent of the networks that RouterCheck tests. Opening a port on the router's firewall is not a trivial task, so it is unlikely that a complete novice would do this. However, there are now easy-to-use guides[9] available to help complete novices open ports for playing games, so this may be of concern.

3.3.2 Remote Administration

Remote Administration is a special case of an opened port. It is very dangerous, because this opened port to the internet leads directly to the router's administrator interface. Unfortunately, many users who unwisely enable Remote Administration also neglect to change their administrator password. This combination facilitates hackers breaking into their network from anywhere on the internet.

Twelve percent of the routers that RouterCheck tests have Remote Administration enabled.

3.3.3 Ping

Forty-two percent of routers that RouterCheck tests respond to a Ping on their WAN interface. Ping is often enabled by default on routers, but is generally an unnecessary protocol to support for a home network, so this creates a security exposure. Hackers sometimes use Ping to help locate targets: when a router does not reply to a Ping, a home network is harder for hackers to locate and identify.

3.4 Tested Vulnerabilities

RouterCheck actively tests for several high-profile vulnerabilities during a check. It typically does this by sending data to a specific port in a certain way and observing the response. We add tests for new vulnerabilities into the RouterCheck test suite as we discover them. We are also adding tests for older vulnerabilities. However, the list of actively tested vulnerabilities is not entirely comprehensive.

The most prevalent vulnerability found by RouterCheck was the Misfortune Cookie vulnerability, which was discovered at the end of 2014. Two percent of the routers that RouterCheck tested were susceptible to this vulnerability. Unfortunately, this is a very serious bug that easily allows attackers to gain administrator access to a router from across the internet. This is why it’s so important for users to be able to test for these problems, and be aware if their networks are at risk.

3.5 DNS Issues

From a security perspective, one of a home router's most important functions is managing the identities of the DNS Servers. When hackers compromise a router, they typically modify these settings, so that all internet queries are directed to a DNS Server that they control. From there, it’s easy to damage all the devices on the network.

3.5.1 Unknown DNS Server

RouterCheck determines whether a router's configured DNS Servers are commonly known. If not, they may be problematic. This is quite difficult to determine, because there are many DNS Servers on the internet and it is impossible to keep an up-to-date list of all of them. Furthermore, there is no way to comprehensively test whether a given DNS Server is being run by a hacker.

When RouterCheck encounters an unfamiliar DNS Server, it flags it as a warning to the user.

The RouterCheck developers are currently testing some innovative technology to better determine whether a given DNS Server is rogue. This technology will eventually be rolled into RouterCheck to provide users with improved performance and more specific recommendations.

RouterCheck encounters unknown DNS Servers in 23 percent of the routers it tests.

3.5.2 Resolves non-existent domain

When a DNS Server is confronted with a domain that does not exist, the correct behavior according to the DNS specification is to return NXDOMAIN. This means that the domain does not exist. Any other response means that the DNS Server does not implement DNS correctly.

Some DNS Servers perform DNS Hijacking[10], and they will return valid responses that point to advertising-laden resources. This is wrong for many reasons, and some security experts believe that this may create a security exposure.

RouterCheck issues a caution to the user when it finds a DNS Server configured to resolve non-existent domains. RouterCheck encounters this issue in one percent of the routers it tests.

4 Recommendations

Based on our analysis of the proceeding tests for how home routers are ***really*** being used in the real world, we can make the following recommendations.

4.1 Wireless Security

4.1.1 WPA2

Modern routers all support secure wireless protocols like WPA2, which is a positive step. However, the terminology and the lack of direction for the user makes it quite difficult for non-expert users to make the right choices for their wireless security.

Recommendation: Router interfaces should be more transparent so that users can better understand their choices.

Recommendation: If a router detects that a user has set the wireless security to an insufficient value, it should warn the user and explain the issue.

4.1.2 WPS

On many routers, WPS is often enabled by default, which is quite dangerous. Most routers with WPS support disabling this option. However, some routers have a user interface that appears to support disabling this option, yet WPS remains enabled. This behavior has been observed with Linksys routers.[11]

Recommendation: WPS should be disabled by default.

4.2 Passwords

4.2.1 Force users to change the password at installation time

A simple way that vendors can enforce better administrator passwords is by forcing them to set a new password the first time the router is being used. Since the router sits between the user and the internet, the router can divert any user web queries to a router configuration page that prompts the user to change the default administrator password before proceeding.

The open source third-party router firmware DD-WRT prevents users from continuing to use a router where the default password is unchanged.

Figure 3 - DD-WRT screen that forces users to change their administrator password.

Recommendation: Force users to create a non-trivial administrator password the first time the router is used.

4.2.2 Stop automated processes from guessing passwords

A significant problem with passwords is that a hacker has major advantages when trying to brute-force access a router by continuously guessing the password. A hacker's advantages are:

- Time
- Freedom from detection

A hacker who controls a device on the network through malware or some other means can try to guess the password of the router from that device. This guessing attack can last for 30 minutes or 30 days. The hacker does not need to use any resources to do this because the only processes at work are the infected device and the router.

Our tests show that a typical wireless home router can handle about a dozen login attempts per second. This means that if the device and router are left on continuously, the hacker can try 31 million different passwords every month.

The other reason that a hacker has unlimited time to try to break into routers from a compromised device is that there is no way to detect that anything is going on without resorting to tools that are not within the reach of the typical home user. This means that a virus loaded onto a computer in the kitchen can be set to brute force its way into the home's router, and this can go on for weeks without anyone being aware.

Router vendors must prevent this from happening.

4.2.2.1 Disallow unlimited login attempts

Websites do not allow unlimited and unconstrained login attempts, so why should home routers? Websites normally control login access several ways:

- Throttle the attempts by disallowing subsequent attempts until after a short wait. Alternatively, the response can simply be slowed down.
- Lock users out of their accounts after a number of failed attempts. This approach needs some sort of reset mechanism, such as email notifications or contacting a help desk. For obvious reasons, this is not a suitable solution for a home router.

Therefore, the simple way to shut down automated login attempts is to slow things down. After three failed attempts at logging in, make the wait times for subsequent attempts longer and longer. However, a real user must still be allowed to log in, and the automated process that is trying to guess the password by brute force must be prevented from creating a denial-of-service condition.

We are not aware of any routers that implement this mechanism.

Recommendation: Throttle the timing for responding to failed login attempts so that a very large number of attempts cannot be made.

4.2.2.2 Use CAPTCHA technology

One way to stop automated login attempts is to ensure that the entity trying to login to the router is indeed a person. This can be done by using CAPTCHA technology[12]. Some D-Link routers use this.

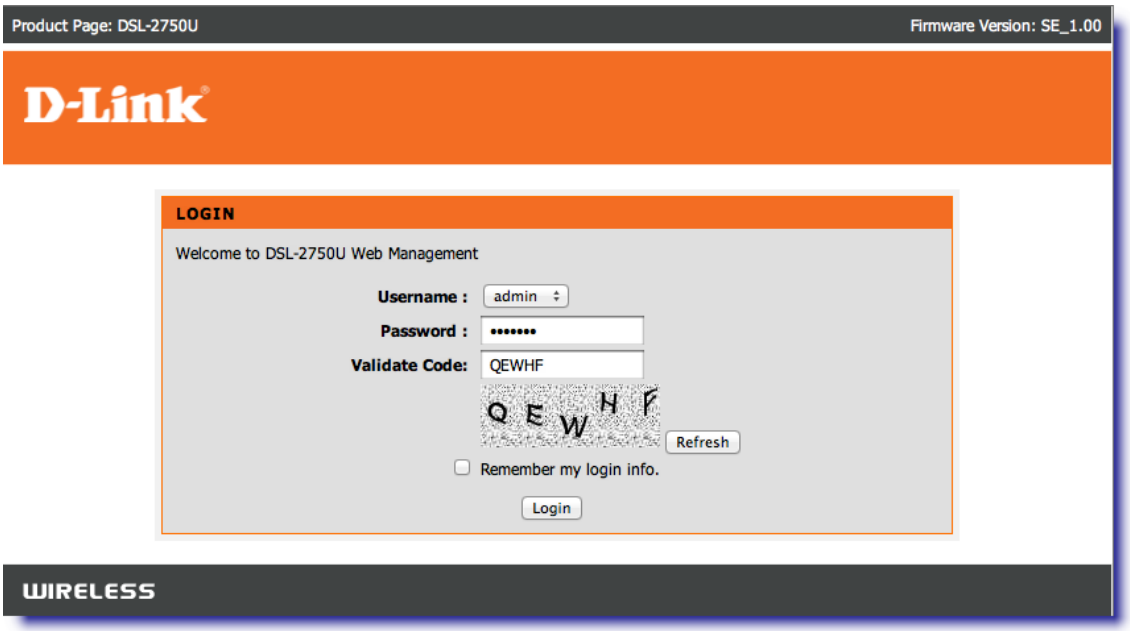

Figure 4 - CAPTCHA being used for login on a D-Link DSL-2750U

Unfortunately, CAPTCHA was not very well received when D-Link originally released support for it. One problem that happened was that researchers found ways to circumvent the system, and it was incorrectly reported as the CAPTCHA system being flawed.[13]

Recommendation: Despite the history, we still recommend using CAPTCHA because of its ability to slow down and stop automated processes. However, when using it, implementation and user interface are crucial.

4.3 Ping

We do not understand the purpose of having a home router respond to a Ping from across the internet. We could concoct a situation in which this behavior would be appropriate, but it certainly would not be meaningful for the vast majority of home internet users. Not responding to a Ping means that there is one less way for an attacker to determine that a given IP address is active, so this adds an extra measure of security.

Recommendation: Ping should be disabled by default.

5 Third-Party Testing

We believe that consumers need an independent third party tool that tests their home network from both inside **and** outside the firewall. As developers of RouterCheck, we may be a bit biased when we say this, but there are some very good reasons to support this:

5.1 Users fix the problems found by RouterCheck

Users who checked their router a second time with RouterCheck found fewer vulnerabilities 20 percent of the time. This happened because these users listened to the warnings that RouterCheck presented to them and fixed the underlying vulnerabilities that were found. By following RouterCheck's suggestions, they made their home networks safer.

The RouterCheck app comes integrated with RouterCheck Support. RouterCheck Support provides users with instructions for how to fix problems with their router. Since the RouterCheck app can determine the model of router and the nature of the problem, it can provide highly customized instructions.

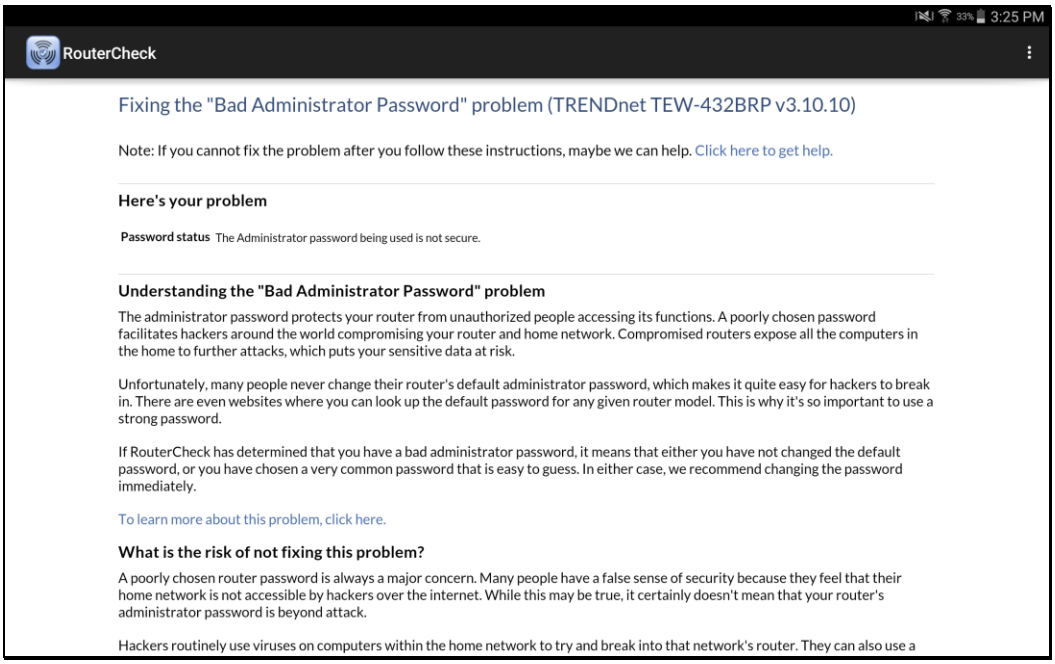

Figure 5 - RouterCheck Support provides customized instructions

Our data shows that users are not only consulting RouterCheck Support, but they are also following its instructions to resolve their issues.

5.2 Sometimes you need to hold the mirror up

We always feel optimistic whenever we see an article in a mainstream publication or newspaper that explains the dangers of the connected home to ordinary people. Unfortunately, we also know that these articles are often met with ignorance or apathy by the people reading them.

The problem is that articles only tell people what is theoretically wrong. By actually testing their networks, people can be shown: *Here's what's actually wrong and vulnerable in **your** network, and here's how to fix it*. Sometimes, people are only motivated to action when confronted with reality.

5.3 You can't trust the router's interface

If you want to determine whether a person is a liar or not you can't simply ask him – that would be unreliable. A better way is to observe his behavior and see what he really does.

Likewise, we cannot determine whether a router has been compromised simply by interacting with its user interface. If it's truly compromised, the user interface could tell us whatever the malware wants us to see. This is why a third-party tool like RouterCheck is so important. Instead of simply presenting the information gathered from the user interface, RouterCheck interacts with the router and reports on its actual behavior. If malware has modified the device, RouterCheck can determine this.

Additionally, we've seen that some routers contain bugs, so that some of the information in their user interfaces does not necessarily correspond with the reality of their configuration. Again, RouterCheck can see through this and offer suggestions on how to fix it.

5.4 Users require more information and explanation

Many of the vulnerabilities that we found could have been avoided had there been better information available to the user. A third-party tool can provide that explanation, and in fact do so in a way that is understandable to typical users.

A good example of this is WPS. Several RouterCheck users contacted us to thank us for pointing out the dangers of WPS and explaining them in an easy to understand format. If they had not used RouterCheck, they would not have known that WPS was problematic.

5.5 Some default configurations aren't good

Sometimes routers come pre-configured with harmful choices. For instance, turning on Ping and WPS by default seems like a bad idea to us.

Most users, even expert users, will configure their routers with a handful of custom settings and simply ignore the rest of the configuration. They just assume that "everything out of the box is safe". It is only when those bad choices are pointed out to users that they will take action to correct them.

5.6 ISPs can identify a coordinated attack

ISPs that supply their customers with equipment that contains a significant vulnerability are at risk of a so-called Hack of Mass Destruction[14]. A Hack of Mass Destruction occurs when a hacker can attack a large group of home networks that are easy to find and identify (as are ISP subscribers), and then compromise all of them based on the equipment's vulnerability.

RouterCheck can protect against such an attack when it's deployed to a large population of an ISP's subscribers. It can be run in a mode that can detect when a coordinated attack occurs against the ISP, and then alert that ISP so that the damage due to the attack can be contained.

6 Conclusion

As security researchers find new vulnerabilities in home routers, the media reports on them. This often makes users confused as to what to look for and how to mitigate any problems they think they may have.

However, RouterCheck demonstrates that the primary threats to home networks are not the complex vulnerabilities reported by the media. Rather, consumers systematically ignore calls for simple, common-sense security practices. This is the biggest threat to their security.

Users must understand the state of their networks before they can ensure that they are secure. While understanding how to log in to a router and view its status is important, this is not sufficient. Viewing a router's status from a third-party tool, such as RouterCheck, prevents a bug or a compromise in the router's firmware from providing an accurate picture. Therefore, third-party confirmation, which includes viewing the router from the same perspective as a hacker, is critical to router security.

Notes

[1] http://mis.fortunecook.ie/

[2] http://blog.sec-consult.com/2015/05/kcodes-netusb-how-small-taiwanese.html

[3] https://play.google.com/store/apps/details?id=com.Sericon.RouterCheck.client.android

[4] http://www.computerworld.com/article/2544215/security0/don-t-use-wep-for-wi-fi-security--researchers-say.html

[5] http://gizmodo.com/5078317/wpa-wi-fi-security-gets-cracked-your-network-is-no-longer-secure

[6] http://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup

[7] https://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/

[8] https://en.wikipedia.org/wiki/Cross-site_request_forgery

[9] http://portforward.com/

[10] http://www.dnsknowledge.com/whatis/nxdomain-non-existent-domain-2/

[11] http://www.40tech.com/2012/01/16/linksys-router-youve-got-security-problems/

[12] http://www.captcha.net/

[13] http://www.zdnet.com/article/d-link-routers-captcha-flawed-wpa-passphrase-retrieved/

[14] http://www.hackofmassdestruction.com/