Logan Herodes
Cybersecurity
Fall 2019

How Safe is Your Router?

Abstract:

Nearly everyone in the United States has a personal network in their home being run from a router on which they do everything they could imagine on the internet. Terrifyingly, many routers are insecure out of the box, meaning that home networks are vulnerable to a plethora of attacks from nefarious individuals. But, is there such a thing as a more secure router? How do you pick one? And, once you have your network, how do you ensure that nobody is using it to attack you?

In this paper I will delve into the risks associated with different routers and home network setups. I do not plan to look at the massive risks posed by the internet of things, but more at what an individual can do to ensure that when they are browsing, banking, playing or surfing at home they are protected.

Introduction:

A wifi router is a device that allows users to wirelessly connect to a network, most commonly and dangerously the Internet. Routers are becoming more and more commonplace in the world, with nearly every individual, small business, coffee shop or anywhere else that could be imagined. An insecure router could spell disaster for many different people at a time. In an instance of a home router being hacked, an entire family's privacy could be lost or identities could be stolen. Were a router hacked at a business or coffee shop, all the traffic present on the network that is going through the router could be captured to a malicious person's computer.

In the case of a router, it can often be configured to encrypt traffic by requiring a username and password to access the network or it can be opened to the public and allow anyone to have access. Routers often also allow specific administrators to have configuration ability over the network in most cases, which in most cases come preset by the factory from which the router came. Routers also collect all of the traffic that is sent through it to the internet, which means that all data that is uploaded or downloaded is collected at some level in the packets that are transmitted through the router.

To the Community:

As I walk around campus or to most major locations in the city nowadays I am constantly seeing options to connect to open networks around me. I began to wonder how dangerous it would be to use this seemingly free internet access even though it was running through a router I could not access. As I began to investigate, I started to consider people's home networks which were often visible to the public as well as you

walk by their home or apartment building. Thinking like a hacker cause me to realize that if something so visible was dangerous, there could be significant risks associated, especially given that most people have a router and personal network at home but absolutely no idea what either of those things actually do.

Router security is extremely important. *Everybody* has a router. Nearly everybody has their own internet connection of some kind. If these devices really are vulnerable, a malicious person could inflict serious harm on an extremely widespread group of victims. Further, nearly every business nowadays has offices with many routers inside and many employees connected to routers at a given time. For a company, having a vulnerable network could spell financial disaster or pose privacy risks to employees, clients or stakeholders of any kind. Given that routers are such a widespread and necessary device for so many people, educating both router manufacturers and the general populace on how to ensure their security is extremely important.

Specific Risks:

The specific risks on an insecure to a person or business are significant and ubiquitous. An article from Norton Security explains some of the risks: “If your Wi-Fi network isn’t secured properly — a public IP address, no unique Wi-Fi password — you could be letting anyone with a wireless-enabled device gain access. You might not be worried about someone using your wireless connection, but the real risk is exposing sensitive information you send and receive — your emails, banking information, and maybe even your smart home’s daily schedule — to cybercriminals.” (Norton Security) An insecure router could allow a hacker to steal your traffic history and its contained data, like usernames or passwords sent to any site accessed through the router. Further, a hacker could look at and possibly take control of any devices connected to the router. As the Internet of Things becomes more popular, more and more devices get connected to more routers every day. It is imperative that people be aware of the risks of insecure routers so that they become aware of why they should take the time to secure their routers at home and in their business.

Insecurities and Vulnerabilities:

Firmware issues commonly plague internet routers. Routers are relatively cheap to manufacture and can be made even cheaper if security is overlooked. Buggy code is often deployed in routers and leads to a significant number of the vulnerabilities found in routers. An article from darkreading.com states “Research conducted by the American Consumer Institute Center for Citizen Research indicates that the routers commonly found in homes are huge security vulnerabilities for consumers and their employers. The center's analysis shows that of 186 sampled routers, 155 (83%) were found vulnerable to potential cyberattacks. Most of the vulnerabilities were in router firmware,

according to the researchers, with the sheer number of vulnerabilities caused by a combination of a reliance on open source projects for code and a lack of vigorous patching and update policies on the part of the vendors." (Dark Reading) As stated here, routers often have problems in the code that makes them run; the problem is that often times, manufacturers do not spend a great deal of time updating old routers as it is to their benefit to have you buy a new one, so many known vulnerabilities go unpatched in routers. If companies focused more on security, there would likely be less insecurity among internet routers and they may not have to worry as much about patching if they spent more time doing it right the first time. As a community, demanding more secure routers could influence companies. However, for now, the only defence against buggy code that is unpatched is to throw away the old router when a vulnerability is discovered and get a new one. If a patch exists, it should be installed immediately.

Another flaw of routers is that many people do not change the default username and password that come coded in the router. These username and password pairs are often set at the time of manufacturing, and should be changed when the router is set up. A strong password should be used as well, because a device as visible as a router has a higher chance of getting attacked in general. Cracking a complicated password is extremely difficult for a hacker; cracking a simple, commonly used or default password can take a hacker just seconds in some cases. If an unwanted person is able to access your router, not only could they steal your internet and cause your internet to slow down, they could steal all of the traffic that is sent over the router. Many routers contain administrative usernames and passwords that are also set at the time of manufacturing and are often the same for every device. If a hacker gains access to a network or joins an open network and is able to enter default administrative credentials, the hacker could take control of the whole network. In this case, a hacker could download all of the traffic flowing through the router, change the credentials needed to log into the wifi, or take control of devices connected to the router in some cases. The fix to this type of vulnerability is simply to change the admin username and password and the network name and password to something complicated so it is harder for a hacker to crack.

Defenses:

Many of the issues detailed above can be defended against in relatively simple ways; ensuring strong username and password combinations on routers and networks during setup is step one. This is a fix to many issues that takes an additional five minutes of setup. Further, ensuring that the network the router is distributing is encrypted is important. This is usually a feature that can be turned on or off during setup. Typically, open networks are unencrypted, which is why they do not need a password to access. In general, it is dangerous to use or operate an open network, especially at home or in a business because anyone will be able to access the network

without credentials. In the case where a router is insecure because of firmware issues, the only defense is awareness. It is important to keep up to date about issues facing different types of routers and keeping tabs on which routers are affected by which issues. If you happen to own an insecure router, either search for a firmware update or, in the unfortunate and common case where no such patch exists, throw the router away and get a new one. Although this seems like an expensive approach, an insecure router could lead to issues that cause significantly more than a few dollars worth of damage.

It is also possible to monitor traffic that comes through a router if you are an admin. Using this information, it is possible to monitor the traffic going over a network to ensure it is coming from known IP addresses or devices and blocking it if it is not. This is commonly done by businesses on secured networks to ensure that only internal company parties are accessing the internet and any routers in the building. Monitoring a network can be time consuming even if done programmatically, but is a good way of ensuring that only known devices are accessing the network. Further, with a PC or laptop it is often possible to connect to the internet with a wired connection. Not only is this faster than using a router, it will defend against the vulnerabilities of routers mentioned above.

Conclusion:

Routers are ubiquitous and necessary; they allow large numbers of people to conveniently connect to the internet. However, they contain a number of potential risks to users in a business or personal context. It is possible to improve a routers security, but it takes a bit of effort in some cases. It is important to invest in a high-quality router that has no history of vulnerabilities and keep it up to date with patches. During setup, ensure that strong and complicated username and password combinations are used as well. With a small amount of involvement, it is possible to have a decently secure router and home network.

Sources:

- “Netgear Vulnerability Calls for Better Router Security across Businesses and Homes.” *Netgear Vulnerability Calls for Better Router Security across Businesses and Homes - Güvenlik Haberleri - Trend Micro TR*, www.trendmicro.com/vinfo/tr/security/news/vulnerabilities-and-exploits/netgear-vulnerability-calls-for-better-router-security-across-businesses-and-homes.
- “Router Bugs Flaws Hacks and Vulnerabilities.” *Router Security*, routersecurity.org/bugs.php.

- Schubert, Christina. “Router Security: How to Setup WiFi Router Securely.” *Router Security: How to Setup WiFi Router Securely*, us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html.
- Staff, Dark Reading. “Most Home Routers Are Full of Vulnerabilities.” *Dark Reading*, Dark Reading, 5 Oct. 2018, www.darkreading.com/network-and-perimeter-security/most-home-routers-are-full-of-vulnerabilities/d/d-id/1332987.
- Wagenseil, Paul. “Your Router's Security Stinks: Here's How to Fix It.” *Tom's Guide*, Tom's Guide, 11 Nov. 2018, www.tomsguide.com/us/home-router-security,news-19245.html.