Your broadband router is not as secure as you think it is

December 9 2015, by Patryk Szewczyk And Nikolai Hampton

Your broadband router might not look like much, but it's your first line of defence against cyber attack. Credit: Matt J Newman/Flickr, CC BY-SA

Between your home network and the internet sits your broadband router. This humble device is often overlooked, yet it is also your first line of defence against hackers, malware and viruses.

It's easy to assume that the latest firmware for your router will provide protection against cyber threats. However, our new research has found

that even the latest broadband router firmware remains dangerously vulnerable to attack.

Firmware is the operating system and software that controls all the features of your router, from the blinking lights and configuration options, to advanced network security features. Similar to any desktop operating system, firmware can contain thousands of system files, any of which may contain security vulnerabilities.

Just like any software you would install on your laptop or personal computer, it needs to be maintained and updated frequently to mitigate known security vulnerabilities. Unfortunately, we have found that even the latest firmware contains security holes.

Obsolete software

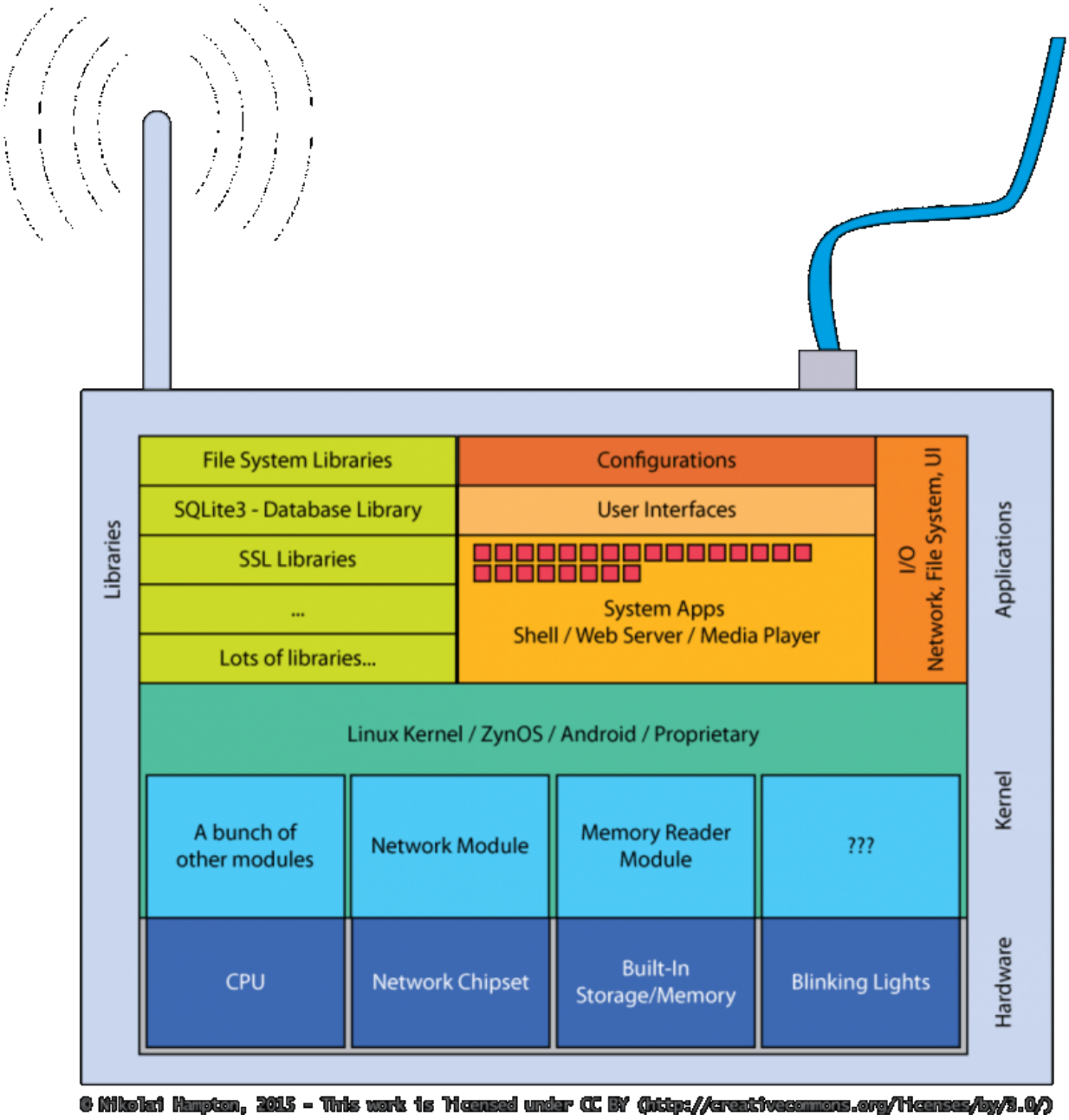
To test how secure these devices really are, we extracted the firmware from 37 currently available broadband routers. We then reverse engineered the firmware to analyse components such as the operating system, system libraries and executable files. This allowed us to construct a comprehensive database of devices, software versions and known vulnerabilities.

We found that 90% of the components analysed were more than six years old. In every firmware we found obsolete software with known security issues, regardless of the manufacturer or release date.

Old software may not sound like a big deal. However, security experts agree that all developers should start from a solid base, building upon well maintained and up-to-date software components.

Yet many people probably don't realise that critical security vulnerabilities identified a decade ago are still present. Cyber threats

evolve rapidly, and six months is a long time, two years an eternity, and a decade – well, you get the picture!



A simple overview of what makes your router go. Credit: Nikolai Hampton, CC BY

Obsolete components often have security issues that are so well known that common security testing tools and hacking software even incorporate their exploits into simple "point-and-click" interfaces. So old firmware components are a major concern.

It's not just routers

Internet of Things (IoT) and smart devices are also powered by firmware. If the pattern we have found continues, then it won't be long before we find a piece of malware that can infect your internet enabled refrigerator.

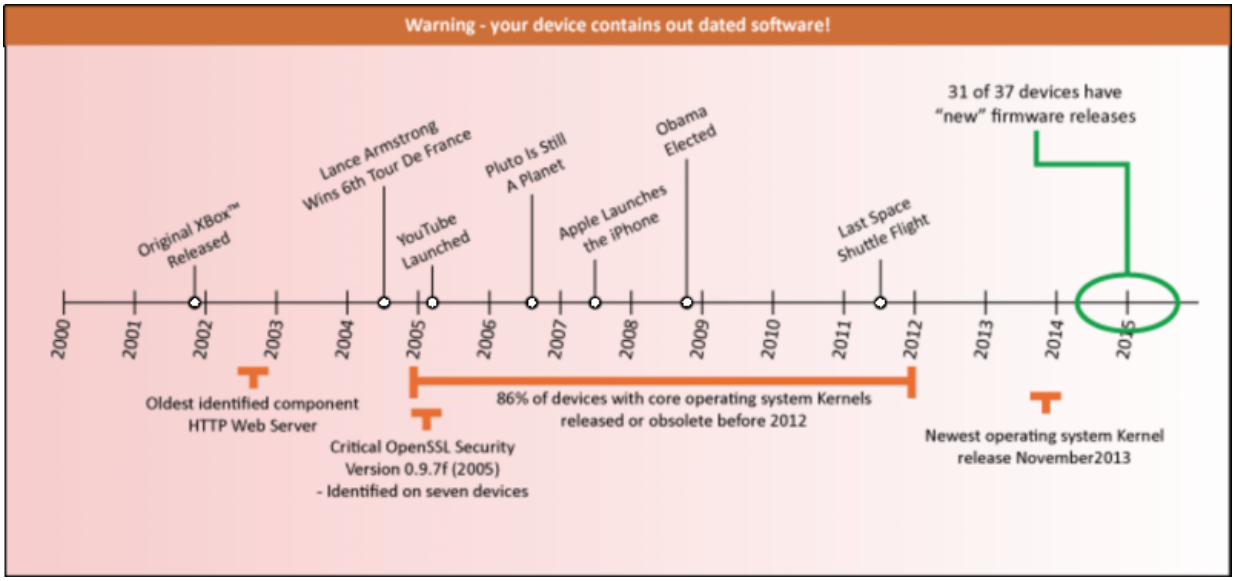
Our latest research has started "cracking open" IoT devices. The first device examined was a 2015 internet enabled security camera that had an obsolete operating system and key security components from 2008.

While alarming, our research does not suggest that consumer routers are being attacked frequently or on a large scale. It does, however, indicate an environment where attacks are likely to increase in frequency and severity in the near future.

So you can follow best cyber security practices and still fail to be adequately protected. You may also have a false sense of security if you believe the latest firmware will provide adequate protection. In reality, the core components of most router firmware are built on open source software released up to a decade ago, and (on many occasions) maintained by part-time enthusiasts rather than professionals.

Broadband routers are clearly vulnerable to a range of cyber security threats and manufacturers have little incentive to improve their firmware development practices at the moment. The lack of transparency, accountability and user education breeds an environment that rewards first-to-market devices with multimedia capabilities or stylish antennas,

rather than robust security.



Timeline of selected significant software components - a historic perspective. Credit: Nikolai Hampton, CC BY

How can you protect yourself?

Our research does not suggest that all firmware updates are a waste of time. The problem is the lack of transparency; we simply don't know what is included in our device firmware.

The best advice remains keeping all of your devices up-to-date.

You can also get better protection by using a multi-layer defences, such as virus scanners and firewalls. The Windows operating system comes with built-in services, including Windows Defender and Windows Firewall. You should make sure that these services are installed, up-to-

date and running as a matter of priority.

Third-party anti-virus scanners can help, but some people may find them more intrusive than beneficial. Third party products can also contain unwanted programs and tool bars that can slow your computer or internet connection. You should read a range of product reviews before deciding on what software to trust.

The problem can only be truly fixed by manufacturers. Consumers and IT professionals must demand better security, but without further independent device analysis, many people won't be equipped to understand the security issues or implications. This is an area that needs serious attention.

We have proposed a range of long term solutions, including a security star rating system, to help users understand how their device compares. We are hopeful that the industry, security experts and end-users can work together to achieve meaningful security improvements, before the threat of mass cyber attacks becomes an every day reality.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation