# Quantifiable Metrics of Home Router Security Using Open-Source Documents

Sreean Reddy Rikkala, Alexandria Simonson, Ryan King, Corey Mekelburg

*University of Nebraska at Omaha*

## Abstract

Consumer grade routers are critical devices in residential home networks that serve as the primary defensive layer against cyber threats. Despite their importance, consumers lack clear metrics to evaluate router security making it difficult for them to make informed choices when presented with numerous commercially available options. Faced with this difficulty, our research team proposed the question: what quantifiable metrics can be used to assess the security of home routers from openly available documentation? This research paper analyzes currently accepted cybersecurity best practices for consumer home routers and attempts to align controls in an objective and consistent grid that considers the default settings for each control. The produced grid is tested among our researchers by individually evaluating several routers and comparing the deviations between each researcher. Finally, suggestions are made for improvements to the grid and further areas of research towards securing consumer residential routers.

## Introduction

1. Iterate the importance of routers in a home network, backed up with the “80% of home networks have a router” statistic.1
2. Back up this argument with data regarding consumer network security literacy, including that “52% of survey respondents have never adjusted their router factory settings” and that “86% of survey respondents have never changed the router administrator password”.7
3. Examples of attacks using routers (botnets, data scraping, backdoor to network, etc.).

### Research Context

1. State our research question again and explain it as an aid to the consumer network security problem.
2. List our research methodology succinctly and the goals we hope to achieve.
   1. Evaluation Grid
   2. Criteria (different measurements)
   3. Categories (placing criteria into reasonable groups)
3. Explain the barriers to our methodology and testing:
   1. No physical access to routers
   2. Devices may be out of scope due to lack of documentation or documentation gated behind customer portals (ISP routers)
4. State our “success criteria”, or what we define as a successful outcome.
   1. Criteria that are consistently repeated.
   2. Criteria that can be evaluated objectively.

## Background

## Literature Review

1. Review Existing Frameworks
   1. NIST IR 8425A, CableLabs BCP, BSI TR-03148
2. Go Over CVSS model.
3. Go over previous attempts to assess router security (CIS Benchmarks, consumer router audits if applicable, research papers for different components [UI, wireless controls, default credentials]).
4. Additionally, pull from all sources in the “References” section of this document.
5. The literature review will reference criteria chosen in the next section to make the reasoning for each selection or omission clearer. Essentially, this builds a strong basis for our arguments in the next section.

## 4. Methodology

### 4.1 Research Approach

To develop an evaluation framework, we selected routers to review based on their relevance to U.S. consumers and their prevalence in the market. Our approach followed these steps:

1. Identify the Top U.S. ISPs: We began by identifying the largest internet service providers in the United States based on customer counts and sales data. This included Comcast (Xfinity), Charter Communications (Spectrum), AT&T, and Verizon. We scoped down this list to only include the top two – Xfinity and Charter.
2. Include ISP Local to Researchers: Cox Communications was included as a relevant ISP due to its prominence in the area where the researchers were conducting the study. Cox is a major regional ISP and a good comparison point.
3. Choose Compatible Third-Party Routers: Using ISP documentation and support portals, we reviewed the ISPs compatible routers and selected a few devices from each ISP to review. The devices that were selected were relatively new (past 5 years) to ensure there was publicly available data and they were devices in use.

This strategy ensured the evaluated devices were relevant to the Top U.S. ISPs while also ensuring they were a good representative of modern capabilities.

### 4.2 Criteria Selection Process

To ensure our security assessment framework is reliable and objective, we developed a process for selecting evaluation criteria. The process was guided by the following:

* Quantifiability: Each metric must be scorable between 0-10 using a defined rubric.
* Testability via Documentation: The metric must be able to be tested via publicly available documentation such as user manuals, support pages, CVE databases, and release notes.
* Alignment with Industry Standards: The metrics were selected from previously existing industry best practices, standards, or guidelines such as NIST IR 8425A, CableLabs BCP, and BSI TR-03148.
* Ability to Test Without Device Access: Metrics that couldn’t be tested without physical access to the device were excluded such as secure boot or runtime behavior.

### 4.3Metric Categories

As the primary research question focuses on evaluating router security using publicly available documentation, this section emphasizes only the security related metrics in the evaluation grid. Usability, performance, and cost were other domains assessed by the researchers, but they are out of scope for this paper.

The selected security metrics are organized by security categories:

1. Authentication & Access Control: Included default credentials settings, remote access settings, UPnP settings, and admin interface encryption and protection
2. Patch Management & Software Integrity: Included firmware update frequency, automatic security updates, known CVEs with and without patches, and secure wipe (Factory Reset).
3. Network Protection Features: Included firewall features, guest network isolation, DMZ settings, VPN settings, WPA3 and other wireless encryption support, parental controls, and logging and monitoring.

Each one of these metrics was chosen in alignment with best practices and based on its relevance to real world attack vectors. These categories range from preventative controls to reactive safeguards.

The metrics were intentionally chosen to be practical to verify without needing device access.

### 4.4 Weighing and Scoring

To maintain simplicity and ensure fairness across all evaluated metrics, we applied an unweighted scoring model to the selected security metrics. Each metric is scored on a scale of 0 – 10 and the overall security score is calculated by averaging the values. This method treats all security features as equally important which avoids potential bias that would be introduced by subjective weight assignments. This also allows for an easier interpretation of the results by typical consumers.

## Evaluation Grid

1. Brief description of the evaluation grid.
2. Explain that the grid was chosen to provide a repeatable and easily usable method for evaluating security features on a device.

### Explanation

1. Explain the grid’s categories and individual metrics.

### Trials Across Evaluators

1. Each research team member will analyze one or two routers independently.
2. Our individual results will be compared against each other and presented with visual data.
3. The results will determine the rest of our discussion including the conclusion; if our results do not match up, we will explain potential improvements to the criteria or grid.

## Limitations

1. Documentation from different routers have varying degrees of information
   1. Potentially include a quick snippet regarding security feature disclosure.
2. Certain features may not be possible to investigate. Additionally, some features may claim to be available on the device but not be implemented properly.
3. Data regarding CVEs and other vulnerabilities may no longer be relevant as technology progresses.
4. We were unable to test devices physically.

## Conclusion

1. Reiterate the importance of the work and our intended goal.
2. Recap our methodology and results.
3. Explain any shortcomings in our findings.
4. Make recommendations on how to continue research.

## References

**[1]** Parks Associates. Vast majority (80%) of us households have a home network router; 28% report intentions to purchase. Consumer Electronics Devices, Apr 2024.

**[2]** George Chalhoub and Andrew Martin. But is it exploitable? exploring how router vendors manage and patch security vulnerabilities in consumer-grade routers. In Proceedings of the 2023 European Symposium on Usable Security, EuroUSEC ’23, page 277–295, New York, NY, USA, 2023. Association for Computing Machinery.

**[3]** Marcus Niemietz and J¨org Schwenk. Owning your home network: Router security revisited. *arXiv preprint arXiv:1506.04112, 2015.*

**[4]** National Institute of Standards and Technology. Recommended cybersecurity requirements for consumer-grade router products. Technical Report Internal Report (IR) 8425A (Final), U.S. Department of Commerce, September 2024.

**[5]** Dragan Perakovic, Ivan Cviti´c, Tibor Kuljani´c, and Luka Brleti´c. Analysis of wireless routers vulnerabilities applied in the contemporary networks, 12 2018.

**[6]** Colin Stephenne, Felipe Gohring de Magalhaes, Frederic Cuppens, Jean-Yves Ouattara,

Militza Jean, Jose Fernandez, and Gabriela Nicolescu. Security assessment of a commercial router using physical access: a case study. In Proceedings of the 34th International Work-shop on Rapid System Prototyping, RSP ’23, New York, NY, USA, 2024. Association for Computing Machinery.

**[7]** Tofts, Alex. “Gap in Awareness Leaving Routers at Risk from Cyberattacks.” *Router Security Survey 2024*, Broadband Genie, 8 Oct. 2024, www.broadband.co.uk/broadband/help/router-security-research.

<https://www.cmcsa.com/static-files/9cd62cea-91c4-4ad7-a7dc-7eeaaa576c42>; <https://corporate.charter.com/newsroom/charter-announces-fourth-quarter-and-full-year-2024-results>; <https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2024/4Q24/4Q24_ATT_Financial_and_Operational_Schedules_and_Non_GAAP_Reconciliations.pdf>; <https://www.verizon.com/about/investors/quarterly-reports/4q-2024-earnings-business-update>; https://investors.alticeusa.com/news-events/press-releases/detail/212/altice-usa-reports-fourth-quarter-and-full-year-2024-results