# 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 residential routers have a privileged multipurpose position as the gatekeeper of external threats and perform sensitive internal networking functions. This intermingling of external and internal functionalities places consumer networks as a valuable target for external threat actors. As such, it is essential that these devices utilize a wide variety of cybersecurity controls to ensure that the consumer's home network is properly protected. However, an issue arises when consumers are tasked with selecting routers that have implemented proper cybersecurity controls. The consumer must choose between relying on the ISP to provide and implement a secure router or purchasing and configuring their own. This task becomes increasingly difficult as the breadth of available devices and manufacturers grows. 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. State our research question again and explain it as an aid to the consumer network security problem.
4. 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)
5. 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

1. Reiterate router security importance.
2. 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)
3. Examples of attacks using routers (botnets, data scraping, backdoor to network, etc.).
4. Go over the need for assessment strategies for routers or need for consumer standards.

## Literature Review

## Related Work

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.

## Selecting Criteria

### Research Approach

1. Explain router selection process:
   1. 2 ISPs are the largest in the USA for consumers
      1. Comcast
      2. Charter
   2. 1 ISP is local to researchers
      1. Cox
2. Go over use of specification mining to get data:
   1. Information was pulled from ISP official documentation, support articles, product pages, and specification documents.
   2. CVE Databases.
   3. Public Firmware Notes.
3. Reliance on public data. No physical testing of devices was conducted.

### Criteria Selection

1. The Criteria were selected with these - Objectivity, Reproducability, Relevance, Alignment with Standards, Feasibility
2. Discuss Filtering of metrics from current industry standards
3. Go Over Inclusion and exclusion criteria
   1. Testable without access?
   2. Publicly available documentation?
   3. Is it something that is measurable or verifiable?
   4. Can data be found and tested consistently across routers?

### Metric Categories

1. Security
2. Usability
3. Performance
4. Cost
5. Briefly go over categories but clarify that for the focus of this paper is security metrics

### Weighing and Scoring

1. Weighing and Scoring
   1. Explain why certain metrics are weighed heavier than others
   2. Explain use of a weighted scoring model

### Goals of Criteria

1. Describe the goals/purposes/security impact of the metrics in the security grid
   1. Unique credentials
   2. Regular updates
   3. CVEs, etc
2. Connect goals to threats in the world]

### Categories

## 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.