# 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.
2. (citation needed) Back up this argument with data regarding consumer network security literacy.
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. Why is router security critical
2. Barriers to testing
   1. No physical access
   2. Locked-down devices or lack of documentation
3. Examples of attacks using routers (botnet)
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 attempt to assess router security (CIS Benchmarks, consumer router audits if applicable)

## Selecting Criteria

### Research Approach

1. 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
2. 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. Show the grid and explain the security metric

### Explanation

### Trials Across Evaluators

1. Walk through one or two routers to apply scoring and show matrix or chart visual

## Limitations

1. Reliance on public documentation
2. Lack of ability to verify certain security features
3. CVE data change
4. No hands on user testing or penetration testing.

## Conclusion]