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 also 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. The question arises: what quantifiable metrics can be used to assess the security of home routers from openly available documentation? Our research paper analyzes currently accepted cybersecurity best practices for consumer home routers and attempts to align controls in an objective and consistent grid that takes into account 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 on improvements to the grid and further areas of research towards securing consumer residential routers.

Contents

1 Introduction

This section will introduce, in more depth, the beginnings of our research and the goals we aim to achieve. It will introduce the topic, define some necessary terminology, and then expand upon our reasoning for proceeding with the research. It should discuss:

1. Why home routers were selected.
2. The restrictions on our research.
3. What we hope to accomplish.
4. Necessary terms.
5. Broad methodology.

=====DRAFT=====

Routers are the typical entry point into the home network for a large portion of the residential broadband customer base. These increasingly complex devices perform a variety of critical security functions as the core networking device in the typical consumer network. This trusted position on the network

makes it essential that the device is fortified against external threats.

However, an issue arises with the lack of quantifiable metrics that can be used consistently and objectively to evaluate the security of a home router device.

Consistent criteria must be chosen in such a way as to be repeatable across various types and designs of routers. Although there are many ways in which a manufacturer can create a router (modem pair, stand-alone router, broadband router, optical router, etc.), a consistent criterion would be able to perform across all variations without sacrificing accuracy in its measurement.

Similarly, a perfectly objective criterion would produce a measurement that is identical between various individuals who evaluate a given device. For example, if Evaluator A and Evaluator B used a perfectly objective criterion to measure a router, then that criterion would produce a measurement which is identical and free of any subjective experience. Of course, this is an almost impossible task; however, our research attempts to create metrics to this standard and verifies its consistency and objectiveness based on a small panel of evaluations.

Our criteria that we identify will have the requirement that they must be tested via open-source documentation that is readily available from the vendor or the companion ISP. This is to provide an easily reproducible and cost-effect evaluation method which would not require purchasing multiple routing devices.

=====END DRAFT=====

2 Literature Review

An analysis of current router security concerns, trends, and accepted measures.

This section will be a summarized literature review regarding currently active standards and measurements for home routers. The main documents that we will be pulling from are itemized here:

1. Recommended cybersecurity requirements for consumer-grade router products[4]
2. Owning Your Home Network: Router Security Revisited[3]
3. But is it exploitable? Exploring how Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers[2]
4. Analysis of Wireless Routers Vulnerabilities Applied in the Contemporary Networks[5]
5. Security assessment of a commercial router using physical access: a case study[6]
6. Press Release - Consumer Electronics Dashboard Home Networking Data[1]

3 Selecting Criteria

Choosing meaningful, objective, and consistent measurements for home router security

3.1 Goals of Criteria

This section will define the goals of our criteria more thoroughly. The intent for this section is to set the stage for the actual selection of our criteria. It will inform the reader of what drives each selection in the following section.

=====DRAFT=====

Criteria for data security is measured, categorized, matured, and delegated according to the needs of its use cases. For example, NIST is a data security standard developed by the U.S. military protect trade secrets. NIST CSF's observe the whole story of data, from the hardware supply chain to BC/DR governance to attacker countermeasures response plans. While the NIST measure can apply to small office / home (SOHO) routers, the scope of security can be scaled to a much smaller framework than that of a state nation.

This begs the question: What security standard can SOHO routers follow? There is no "One size fits all" data security compliance model. Instead, we must look at data security models, like NIST and FIPS, and extrapolate a list of hardening controls well-suited for SOHO routers.

=====END DRAFT=====

3.2 Categories

This subsection explains how each category was chosen. A category will be the high level overview for a group of criteria. This subsection will define the chosen categories in preparation for selecting criteria in the next section. It should make the definition and categorization of each selected criterion make sense in the next section.

3.3 Criteria

This is where each criterion will be selected along with the reasoning for its selection. Each criterion will have a category, a definition, and a reason for its selection with supporting evidence.

4 Evaluation Grid

Small description

4.1 Explanation

This will contain a visual representation of our grid. Although each criterion and category should have already been explained in the prior sections, this section will largely discuss how to use the grid and explain the scoring system. In essence, this section aims to fully describe each feature of the grid, its usage, and the interpretation of its results.

4.2 Trials Across Evaluators

This section may be on the chopping block, but we are not quite sure. It would involve each of us researchers completing evaluations of the same routers and then comparing our results. This would demonstrate, with a small sample size, the completion of our goal in creating an evaluation grid which contains consistent and objective criteria for scoring router security.

5 Conclusions

This is the conclusion, not too much to plan out here. It will be a rephrasing of our research question with the results that we achieved. Additionally, it will point out any shortcomings in

our work, where we believe additional research could be conducted, and any other necessary comments to close out the paper.

References

[1] Parks Associates. Vast majority (80 *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 Jörg 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 Cvitić, Tibor Kuljanić, and Luka Brletić. 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 Workshop on Rapid System Prototyping*, RSP '23, New York, NY, USA, 2024. Association for Computing Machinery.