Quantifiable Metrics of Home Router Security Using Open-Source Documents

Sreean Reddy Rikkala, Alexandria Simonson, Ryan King, Corey Mekelburg
University of Nebraska Omaha
May 12th, 2025

Abstract
Consumer grade routers are the primary defense between a home network and the open internet. The network and transport protocols set by the manufacturer are buried within router manuals across many network device websites, usually with vague explanations. There are no clear metrics to compare router security between different brands. Security-conscious consumers must make uninformed choices when presented with numerous commercially available options. To address this problem, 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 an array of router evaluations that normalizes deviations between each researcher. Finally, suggestions are made for improvements to the grid and further areas of research towards securing consumer residential routers.

Contents

1 INTRODUCTION

The resilience of a state nation is owed, in part, to information security of its numerous internet gateway devices that its population depends on. Consumer-grade routers are trusted with individual privacy and the integrity of networks hosted within homes and small businesses. With the growing popularity of remote work setups, smart homes, and satellite internet, router manufacturers have the responsibility of providing end-users the means to protect their networks from external threats. [14] [21]

Information security awareness has surged in recent years. Microsoft's Secure Future Initiative, as well as the US Executive Order on Improving the Nations Cybersecurity, have created market impacts covered by journalistic entities [2] [4]. The resulting rise in public awareness leaves many consumers anxious about their networking purchasing decisions.

Open resources online have formalized lists for security features and recommendations for home routers [15]. These documents often have a target audience of networking manufacturers and retailers. Such resources are not practical for everyday consumers because of their technical language and lengthy checklists. [10]

The purpose of the proposed research is to define security criteria for home routers that will aid cyber-conscious consumers in their home router purchasing decisions. To make the security criteria digestible for end users, it must be consolidated to show the most important security features, polymorphic across different types of routers, and repeatable so that security can be compared across devices. The router market has a diverse line of products from different manufacturers (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.

The security evaluations follow the contemporary format and guidelines for risk assessments. Research conducted in this paper is scoped to static analysis. The security evaluations can be adequately completed by utilizing user guides and white papers without much need for a dynamic analysis approach. Static analysis also keeps the methodology timely, cost-effective, and easily reproducible.

The proposed methodology has a handful of researchers collecting data in a model that is meant to compare data points. To minimize biases while grading routers, Krippendorff's Alpha Calculator was used to normalize the assessments among raters [19]. The result is a set of router security evaluations suitable for a PoC but with the accuracy of a production service that minimizes subjective experience.

A proof of concept (PoC) was made to demonstrate the proposed goal of aiding end users with router purchasing decisions. Simplicity was achieved by grading different routers on a security scale from one to ten. For technical users, the security evaluation of routers can be expanded to show granular security features that congregate

into the final score. The PoC was inspired by the website Tom's Hardware, where routers are rated out of five stars [16]. Our PoC prioritizes security, metrics, and comparability. It is also available as an open-source project [24].

2 BACKGROUND

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

2.1 Existing Standards

Several standards, guidelines, and compliance metrics are publicly available as open resources for security best practices on gateway devices. Most of these standards were written for public organizations handling nation resources, NIST and IMDA being examples [15] [17].

NIST 800-128 is a guide that meets requirements for U.S. federal systems but has a target audience of anyone who oversees system or information security management. This guide offers a four-phase Security-Focused Configuration Management to "enable security and facilitate the management of risk". [15] NIST IR 8425A scopes 800-128 into the context of home routers [22].

Some security guidelines are made open-sourced by private organizations who have tried and tested information standards recommended by NIST. In their issue of "*Gateway Device Security Best Common Practices*", CableLabs Security posted their best practices for routers and cable modems that are generally agreed upon by operators and manufacturers [25]. This work organizes robust guidelines like NIST, OWASP, and IEE, and compiles them into easily digestible "requirements" tables. The "*Initial/Out-of-Box Configuration Requirements*" table was especially useful for building our router evaluation matrix because these requirements tackle the authentication and admin access problems that commonly plague home routers. The "*Network Services and Listening Processes Requirements*" table was also critical for building the "security" section of our evaluation matrix by addressing default firewall configurations of home routers, and their encryption-in-transit protocols such as TLS. [25]

CableLabs is also referenced in the "*Recommended Cybersecurity Requirements for Consumer-Grade Router Products*" by authors Fagan et al [14]. In this report on home routers, four non-technical cybersecurity outcomes and requirements were suggested for router manufactures. The four requirements (documentation, information and query reception, information dissemination, and education and awareness) ensure cybersecurity assurance for a target audience of everyday consumers. [14]

Perhaps the most comprehensive list of requirements for routers is TR-124 by Broadband Forum. All 71 tables in their article "*Functional Requirements for Broadband Residential Gateway Devices*" build a global compliance for residential gateway devices. This superset of requirements provides security assurance for a full suite of voice, data, and video in broadband networks including home routers. [3]

Security requirements can gain credibility in the context of a threat model. In their paper "*BSI TR-03148: Secure Broadband Router*", researchers from Germany's Federal Office for Information Security defines security requirements for Small Office and Home Office (SOHO) routers [1]. While the other papers have a target audience for router manufacturers, this paper expands that target audience to end users as well. The user-friendliness of this paper is manifested through definition tables, diagrams, and a threat model. The threat model assumes an adversary is targeting a router from the public domain as well as from inside the local network. The paper demonstrates how contemporary security controls can thwart attacks from the adversary in the threat model. [1] This paper was crucial for helping communicate technical language to everyday users when publishing our results online.

2.2 Annotated Bibliography

European Telecommunications Standards Institute. (2020). Cyber security for consumer internet of things: Baseline requirements (ETSI EN 303 645 V2.1.1). *https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf*

This standard defines essential security requirements for consumer IoT products such as routers. It outlines 13 provisions including device password uniqueness, secure software updates, vulnerability disclosure handling, and exposed network service restrictions. The document is designed to serve as a baseline for manufacturers to ensure their devices meet minimum security standards. This paper references ETSI's baseline to inform the development of its security evaluation metrics. By using publicly available documentation to verify whether routers meet criteria such as unique default credentials or auto-update capabilities, this study aligns with ETSI's intent. The standard helps reinforce the legitimacy of the chosen metrics and supports the enabling of repeatable evaluations.

Costin, A., Zaddach, J., Francillon, A., & Balzarotti, D. (2014). A large-scale analysis of the security of embedded firmwares. Proceedings of the 23rd USENIX Security Symposium, 95–110. *https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/costin*

This research involved extracting and analyzing nearly over 30,000 firmware images from various embedded devices to identify vulnerabilities like hardcoded credentials, outdated libraries, and cryptographic misuse. It emphasizes the scale of insecure practices in consumer firmware and the risks posed by unpatched or poorly designed devices. While this paper uses firmware analysis, the results affirm many of the same risks identified in this study using documentation. Issues such as default passwords, lack of firmware updates, and insufficient patching are common across both approaches. This reference explains that many vulnerabilities detectable in code can also be inferred from public-facing documentation.

Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020). IoT device cybersecurity capability core baseline (NISTIR 8259A). National Institute of Standards and Technology. *https://doi.org/10.6028/NIST.IR.8259A*

This NIST publication establishes six core security capabilities that manufacturers must implement in IoT devices: device identification, secure configuration, data protection, logical access control, software updates, and awareness of the state of cybersecurity. It is designed to guide vendors toward producing secure, consumer-ready hardware. The evaluation grid of the paper closely reflects this NIST baseline in areas such as firmware update support, admin access controls, and device configuration defaults. By verifying these features through vendor manuals and support pages, the study applies NIST's guidance in a practical and accessible way. This makes the research both standards-aligned and user-focused.

OWASP. (2018). OWASP IoT Top 10: Security vulnerabilities and best practices. *https://owasp.org/www-project-internet-of-things/*

This guide lists the ten most common security vulnerabilities found in IoT devices, including weak/default passwords, insecure network services, lack of update capabilities, and insecure data transfers. It also offers mitigation strategies and practical recommendations to reduce risk in consumer-grade hardware. This source strengthens the foundation of the paper by validating the inclusion of key metrics such as default credential use, remote access configurations, and encryption standards. The Top 10 OWASP provides a theoretical checklist that complements the study's documentation-based approach and confirms that its focus areas are grounded in industry-recognized risks.

3 METHODOLOGY

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

3.1 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. The information gathered was taken from quarterly financial reportings from major ISPs in the United States, including Comcast (Xfinity), Charter Communications (Spectrum), AT&T, and Verizon. To determine the largest ISPs for our study, we aggregated the total number of consumer internet subscribers for each ISP.

ISP	Residential Subscribers
Comcast	29,373,000[12]
Charter	28,034,000[11]
AT&T	14,079,000[7]
Verizon	10,014,000[27]
Altice	3,999,900[5]

After collecting all of our data, 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; unfortunately, due to Cox's current position as a private entity, we are unable to provide an accurate subscriber count to attribute to them. The most recent data from 2020 states that they currently have 6.5 million total residential and commercial customers across 18 different states.[13]

(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.

3.2 Criteria Selection

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.

The evaluation criteria was inspired by the Verification Checklist from the article "*Security Requirements for Residential Gateways*" by Infocomm Media Development Authority [17]. The proposed methodology adds extra criteria recommended by CableLabs Security, such as published CVEs concerning the router and log monitoring [25].

3.3 Metric 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 [20] [8] [9]. The selected security metrics are organized by security categories:

(1) Authentication & Access Control: Included default credentials settings, remote access settings, port 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 preventive controls to reactive safeguards. The metrics were intentionally chosen to be practical to verify without needing device access.

3.4 Weighting 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. However, our scoring system did account for nuance in the application of a security control within individual criteria. Take, for example, the following criterion:

Measurement Criterion	Scoring Scale
Management GUI - HTTPS Enforced?	No - 0 or Yes -10

In this case, a router that enforces HTTP by default with the inability to enable HTTPS would be rated the same as a router which enforces HTTP by default but allows a consumer to manually enable HTTPS. These "middle-ground" cases give rise to a range of options available for scoring. In the aforementioned case, an option for "5" points is given for a router that has optional HTTPS capabilities.

3.5 Inter-Rater Reliability Assessment

To verify if our criteria is consistent and objective, the proposed standard was used to perform router evaluations and measure the reliability of the results. Different brands of routers were chosen to represent popular market choices and encapsulate the diversity of consumer routers available. Three routers were chosen for the reliability assessment: TP-Link AXE300, ASUS CMAX6000, and Motorola MT8733.

Each of the researchers performed an independent analysis of each of the three routers utilizing the evaluation grid containing the selected security criteria produced from initial research. The analysis had four requirements that each rater adhered to:

(1) The rater must work independently from other raters.

(2) The rater must notate ratings for which evidence could not be found in documentation.

(3) The rater must only utilize open-source documentation from the manufacturer (except for CVE Database).

(4) The rater must only use documentation which references the specific router being rated.

Prior to rating the routers, each researcher was trained in the grid and allowed to ask any questions regarding its format or markings to ensure the grid was used accurately and to the best of each rater's abilities. The results of each of these evaluations were combined and tabulated to represent the scoring of each router among all raters. These tables would later be used to calculate the reliability of the evaluation grid between raters for each individual router and its corresponding documentation. Below is an example of one such table used to calculate the inter-rater reliability of the evaluation grid against a single router model, the Motoral MT8733, using the 19 security criteria with four researchers as raters:

Criteria No.	Rater 1	Rater 2	Rater 3	Rater 4
1	10	10	10	5
2	NA	10	0	10
3	10	10	10	10
4	NA	NA	0	NA
5	10	10	10	5
6	NA	NA	0	0
7	NA	NA	10	5
8	10	10	10	10
9	5	7	7	6
10	7	10	10	7
11	10	10	10	10
12	3	3	3	0
13	NA	0	0	0
14	10	10	5	5
15	NA	10	10	10
16	10	10	10	10
17	7	NA	3	NA
18	10	NA	7	10
19	10	10	10	10

A full mapping of criteria numbers to names is available in the *Additional Materials* titled "Evaluation Grid.csv".

The method chosen to measure inter-rater reliability using the formatted data was Krippendorff's Alpha. Krippendorff's Alpha is a statistical measure of agreement among raters, and the value that the calculation produces, a reliability coefficient, can be used to determine the reliability for different individual raters to produce similar results when presented with the same subject material and evaluation criteria.[18] The value of Krippendorff's Alpha can be between -1 and 1, with the following interpretation:

- $\alpha < 0$: potential disagreement between raters, with disagreement increasing the closer it is to -1.
- $\alpha = 0$: an agreement that is no better than random chance.
- $\alpha > 0$: potential agreement between raters, with agreement increasing the closer it is to 1.

In the context of this research paper, the intent of using Krippendorff's Alpha is to determine if the chosen evaluation criteria is able to be consistently and objectively applied to open-source router documentation to provide a security "score". A perfectly objective scoring system with access to complete documentation of router security features and utilizing trained raters should have a reliability coefficient greater than 0.8 and nearing 1.

Krippendorff's Alpha was also chosen for its ability to interpret different data and for its allowance of the usage of missing or incomplete data in its calculations. In the evaluation of routers utilizing open-source documentation, this feature is essential when certain information cannot be found for different criteria and it allows for raters who failed to identify available criteria to input an empty value.

An essential component of the Krippendorff's Alpha's calculation is to determine the type of data being used by the raters. This data can be classified as nominal, ordinal, interval, or ratio.

- **Nominal** variables represent categorical labels where no inherent numerical value or order exists. In the context of rating, labels such as "wireless" or "wired" can be applied to the definition of an internet connection as exclusive categories that are meaningful only by name – hence the name "nominal", or "in name only".
- **Ordinal** values are defined by a rank, but their value between each ranking cannot be easily assigned or quantified. For example, when grading the quality of a trading card, a rater may assign a value of "Low", "Medium", or "High" to the card surface's printing quality based on certain characteristics. "High" is desirable, but its exact value is hard to quantify and the difference between "Medium" or "High" could be negligible.
- **Interval** metrics have a meaningful and equal quantitative difference between values, but there does not exist an absolute zero from which the metric can be compared. This means the ratio between these values are not meaningful. A common example for interval data is IQ – the difference between an IQ of 100 and 110 is the same as between 110 and 120, but an IQ of 120 is not "twice as intelligent" as an IQ of 60.
- **Ratio** metrics have similar properties to interval scales, but they also have an absolute zero point. This zero point allows for both differences and ratios to be interpreted in a meaningful way. Continuing the trading card example, the count of scratches on a card is a ratio variable – a card with 0 scratches has no damage, and a card with 10 scratches has twice as many as one with 5.

For the purposes of the evaluation grid, the **ordinal** type was used in Krippendorff's Alpha calculations. This decision was made since the order of the ratings for each criteria matter. Additionally, the distances between each assigned value is subjectively assigned as a general rating of security controls as opposed to a definite security value. Finally, the difference in security between different values is not directly equal to the same interval. For example, the difference between 0-5 is not necessarily always equal to the difference between 5-10 despite the same interval between ranges.

Krippendorff's Alpha was calculated using each router's combined data from all four raters. This data was inputted into the K-Alpha online calculator using the ordinal data type. The online calculator produced a reliability coefficient that indicated the extent of agreement among raters beyond chance.[19]

4 RESULTS

Initial results from the formed evaluation grid and trials, revisions to the grid, and data analysis.

Our efforts in researching various criteria and separating them into categories resulted in our final evaluation grid. The grid contains nineteen (19) total criteria across the three (3) categories. Due to the size of the evaluation grid, it has not been placed into the body of this paper. It can be viewed as a .csv file within the included *Additional Materials* titled "Evaluation Grid.csv". This grid was then used to perform a total of 18 analyses on 9 different consumer routing devices. These devices were from various manufacturers. In total, five different manufacturers were represented in our study: NETGEAR, TP-Link, ASUS, Motorola, and ARRIS.

Manufacturer	Router
ARRIS	G34
ARRIS	G54-Charter
ARRIS	G54-Comcast
ASUS	CMAX6000
Motorola	MT8733
Motorola	MG8702
NETGEAR	CAX30
NETGEAR	CBR750
TP-Link	AXE300

During our review, we noted that several security features are poorly documented or not documented at all within the router manufacturer's official documentation. This documentation included user manuals, device specifications, and publicly available FAQs provided by the manufacturer on their website. The absence of these security features in this documentation suggests that there is no ubiquitous standardization among manufacturers in regards to which information is necessary to disclose to users. In fact, of all routers evaluated using our grid, not a single device had a publicly available and labeled "security sheet" which documented core security features of the device. From the 19 criteria utilized in our analysis, these six (6) security criteria had the least information available regarding their usage or presence:

Criteria	NA Response Ratio
At-Rest Encryption	12/18
Admin Account Lockout	10/18
Management GUI HTTPS	4/18
Admin Password Length	4/18
Remote Management Protocols	4/18
VLAN Availability	4/18

This lack of information suggests that either the security criteria needs reevaluation, or that there exists a gap in information available to consumers regarding the security controls of the devices they purchase. We found that there was no clear correlation between the manufacturer of the device and the security features which were documented. Two routers from the same manufacturer can have highly variable documentation regarding the security features of the device. These conclusions are further compounded by the results of the Krippendorff's Alpha calculation for three routers which were individually evaluated by four separate raters. The results are as follows:

Router	Krippendorff's Alpha
TP-Link AXE 300	0.645
ASUS CMAX6000	0.503
Motorola MT8733	0.576

Krippendorff provided a general system for the estimate of reliability based on the produced alpha. This system is as follows:

- $\alpha = 1$ indicates perfect agreement among raters, where each rater recorded the same response.
- $\alpha >= 0.80$ is a generally acceptable level of agreement and can be considered reliable.
- α [0.67 - 0.79] can be considered the lower bound for acceptability.
- $\alpha < 0.67$ means there is poor agreement and the results can be considered unreliable.

It is important to note that Krippendorff states this should not be accepted as hard a truth due to various disciplines and data collection methods requiring varying levels of reliability For example, architectural data and engineering data may require much higher reliability to support an outcome.[18]. However, if we were to base our analysis purely off of these guidelines, our results can indicate three different scenarios, with a possible blend between them:

(1) The raters are unreliable.

(2) The evaluation grid as a whole is not reliable.

(3) The available documentation is unreliable.

Our interpretation of these results are that the available documentation for each router is limited and not standardized, even among the same manufacturer, which in turn produces evaluation results that are inherently unreliable across different routers and criteria. This makes it very difficult to produce evaluation criteria which can be used to consistently evaluate different router models on their security functionality. However, there are still some criteria which have more prevalence in open-source documentation than others that were able to be evaluated with consistency.

Through all nineteen (19) criteria, there were only two categories which had raters agreeing with each other on their evaluation across all routers: the presence of UPnP being enabled by default and the ability to securely wipe the router using factory resets. The following table includes a brief description of the security criteria and the number of router evaluations where all four (4) raters agreed on the scoring for that criteria. This table includes all entries above zero (0).

Security Criteria	Full Agreement
UPnP Enabled by Default	3/3
Factory Reset	3/3
Parental Controls	2/3
External Admin Interface	1/3
HTTPS Management GUI	1/3
Admin Password Complexity	1/3
Event Logging	1/3
DMZ Support	1/3
Disclosed Vulnerabilities	1/3

Similarly, this table presents the criteria for which there was **at least** a majority agreement (3/4) between raters for each router evaluation:

Security Criteria	Majority Agreement
UPnP Enabled by Default	3/3
Factory Reset	3/3
Default Credentials	3/3
External Admin Interface	3/3
Parental Controls	3/3
DMZ Support	3/3
Admin Password Complexity	2/3
Default Firewall	2/3
Event Logging	2/3
VLAN Support	2/3
Disclosed Vulnerabilities	2/3
HTTPS Management GUI	1/3
Admin Account Lockout	1/3
Wireless Security	1/3
DMZ Support	1/3

The sample size for our evaluations is quite small at three evaluations across four raters, so it cannot be overstated that these results need much more enrichment from further evaluations and studies. However, we can see that there is an immediate lack of consistency for evaluating router security through the use of materials directly available to the consumer. Out of all nineteen criteria, only six had at least a majority agreement across all raters through all evaluations.

In addition to this lack of information, our review of ISP approved routers using only this available documentation has shown that there are several security gaps and concerns, these include:

- Encryption at Rest: No public documentation confirmed support for encryption of data at-rest, suggesting that this feature is either unsupported or undocumented across reviewed routers.
- Short Support Lifespan: Many routers received firmware support for approximately two years, after which router support may no longer be provided, even if security vulnerabilities remain.
- Not Patched Known Vulnerabilities: Several devices still list unresolved CVEs from the past two years, with no mention of future patches in their documentation.
- Few Firmware Updates: The firmware update release vary widely. Many routers demonstrated irregular firmware updates or none at all.
- Poor Disclosure of Security Features: Manuals often lacked detailed information on security controls such as admin interface hardening, account lockout policies, default wireless security, or brute-force protections.

CVE Analysis Findings

Our security evaluation included analysis of documented CVEs for each of the evaluated routers. Among our findings, we discovered that the Netgear CBR750 was affected by CVE-2022-37337, a critical remote code execution vulnerability with a CVSS score of 9.1. The Arris G34 and G54 models (both Charter and Comcast versions) were impacted by CVE-2022-31793, a path traversal vulnerability that could expose sensitive configuration files.

For TP-Link devices, including the Archer AXE300, we found documentation of CVE-2024-21833, a command injection vulnerability. Motorola MT8733 was affected by a series of vulnerabilities (CVE-2022-4001/4002/4003) including authentication bypass and command injection flaws. This CVE analysis informed our "Known Vulnerabilities" criterion within the evaluation grid and significantly impacted the overall security scores of the affected devices.

Notably, we discovered that documentation regarding whether these vulnerabilities had been patched varied significantly between manufacturers, with some providing clear patch information while others offered no mention of remediation status.

Significance of CVE Analysis in Router Security Evaluation

The inclusion of CVE analysis in our evaluation methodology serves multiple critical purposes:

- Provides objective evidence of security flaws that have been independently verified and documented, adding credibility to our security assessments beyond the manufacturer's claims.
- Examining CVEs allows us to evaluate manufacturers' security response processes, how quickly vulnerabilities are acknowledged, addressed, and communicated to users.
- Our analysis revealed a significant gap between consumer information needs and manufacturer transparency. The average consumer has no practical way to discover these vulnerabilities when making buying decisions.

This finding directly supports our research question regarding what quantifiable security metrics can be reliably assessed from publicly available documentation, demonstrating that vulnerability history—despite being crucial for security evaluation—remains inaccessible to typical consumers without specialized knowledge.

5 CONCLUSIONS

This research intended to determine what quantifiable security metrics can be reliably assessed for consumer routers based on publicly available documentation. Using standards and best practices such as CableLabs Gateway Device Security BCP, BSI TR-03148, and NIST IR 8425, we were able to select security criteria that are important for consumer security and that can also be used for assessment without requiring physical access to the device [26].

To ensure the reliability of our evaluation criteria and rating method, we used a measurement of inter-rater reliability through Krippendorff's Alpha. Multiple raters each independently assessed the same sample set of routers from different manufacturers using the evaluation grid. From the results of these trials, the level of agreement among raters was measured. The results showed only mild agreement through the reliability coefficient; this highlighted inconsistency in router documentation regarding security controls and features provided by the device, and showed potential room for improvement in the evaluation grid.

Through this effort, we discovered that while certain security features can be confirmed via product manuals or the support sites, there were others that were rarely publicly disclosed - such as encryption at rest or account lockout policies. Lack of transparency creates a huge challenge for any consumer that is trying to determine the safety or security of their router [23]. We observed that:

- Firmware updates are infrequent or not documented well. Some documents did not include any information at all regarding how a device can be updated.
- Known CVEs can sometimes go un-patched with no fix timeline or statement from the manufacturer.
- Security support is often only guaranteed for two years after the routers release; however, many were receiving firmware updates for at least 4 years. Additionally, some manufacturers did not indicate any timeline for the life of the device.
- Manuals often did not include essential guidance on configuration or security features.

Future work could involve increasing the scope of security criteria for evaluation and experimenting with different evaluation methods. It may prove worthwhile to shift the focus from choosing an initial batch of criteria to instead documenting the security features that are publicly listed in each manufacturer's documentation. By categorically documenting these features, one would be able to easily identify which features are listed across devices and be able to highlight gaps in coverage. In addition, it would be beneficial to assess a larger swath of devices to ensure a more reliable data set. In order to better secure consumer routers, it is essential that consumers have the ability to be informed of the security features available on their devices [6].

Regardless of these limitations, our project was able to demonstrate that a standards backed, quantifiable security rating system can be achieved. Our findings from this project show that their is a greater need for regulatory guidance, pressure, and consumer advocacy to require manufacturers to be more transparent and disclose important security features. The data shows both what could be measured from publicly available data and what was lacking, showing the areas where more transparency and attention from the industry is needed.

6 AUTHOR CONTRIBUTIONS

This project was a collaborative effort. All contributors assessed routers and reviewed ISP documentation. The following outlines each contributor's primary responsibilities:

- Corey Mekelburg: Contributed to the "Introduction", "Methodology", "Results", and "Conclusion".
- Sreean Reddy Rikkala: Contributed to the background section, the CVE section of the results and conclusion.
- Alexandra Simonson: Wrote sections 3.1, 3.2, 3.3, 3.4, results, and conclusions sections of the paper.
- Ryan King: Contributed to the "Abstract", "Introduction", and "Background" sections.

REFERENCES

[1] Bsi tr-03148: Secure broadband router. *Federal Office for Information Security*, Digital Sicher BSI(Version 1.2), Jan 2023. www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03148/tr-03148.html.

[2] National cybersecurity strategy. *The White House Washington*, Mar 2023. bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[3] Tr-124: Functional requirements for broadband residential gateway devices. *The Broadband Forum*, Jul 2024. rg-device-requirements.broadband-forum.org/.

[4] Security future initiative. *Trust Center*, Microsoft, 2025. www.microsoft.com/en-us/trust-center/security/secure-future-initiative.

[5] Altice USA. Altice usa reports fourth quarter and full year 2024 results. 2024. investors.alticeusa.com/news-events/press-releases/detail/212/altice-usa-reports-fourth-quarter-and-full-year-2024-results.

[6] Parks Associates. Vast majority (80%) of us households have a home network router; 28% report intentions to purchase. *Consumer Electronics Devices*, Parks Associates, Apr 2024. www.parksassociates.com/blogs/press-releases/vast-majority-80-of-us-households-have-a-home-network-router-28-report-intentions-to-purchase.

[7] AT&T Inc. 4q24 financial and operational schedules and non-gaap reconciliations. 2024. 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.

[8] Scott Bradner and Jim McQuaid. Benchmarking methodology for network interconnect devices. *NetScout Systems*, Mar 1999.

[9] John Brooke et al. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996. digital.ahrq.gov/sites/default/files/docs/survey/systemusabilityscale

[10] 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*, volume Association for Computing Machinery of *EuroUSEC '23*, page 277–295, New York, NY, USA, 2023. 10.1145/3617072.3617110.

[11] Charter Communications. Charter announces fourth quarter and full year 2024 results. 2024. corporate.charter.com/newsroom/charter-announces-fourth-quarter-and-full-year-2024-results.

[12] Comcast Corporation. Fourth quarter 2024 earnings report. 2024. www.cmcsa.com/static-files/9cd62cea-91c4-4ad7-a7dc-7eeaaa576c42.

[13] Cox Communications. Company overview. 2024. newsroom.cox.com/company-overview.

[14] Fagan et al. Recommended cybersecurity requirements for consumer-grade router products. *NIST Internal Report*, Infocomm Media Development Authority, Oct 2020. www.imda.gov.sg/regulations-licences/regulations/consultations/consultation-papers/2020/security-requirements-for-residential-gateways.

[15] Johnson et al. Nist 800-128: Guide for security-focused configuration management of information systems. *Electrosoft Services, Inc.*, USA Department of Commerce(Version 1.2):i, 1–7, Oct 2019. 10.6028.
[16] Brandon Hill. Routers reviews. *Tom's Hardware*, Future US Inc, 2025. www.tomshardware.com/networking/routers/reviews.
[17] Infocomm Media Development Authority (IMDA). Security requirements for residential gateways. *Technical Specifications*, page Annex A, Oct 2020. www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf.
[18] Klaus Krippendorff. *Content Analysis: An Introduction to Its Methodology*, volume SAGE Publications. 4 edition, 2019. 10.4135/9781071878781.
[19] Giovanni Marzi, Mario Balzano, and Davide Marchiori. K-alpha calculator — krippendorff's alpha calculator: A user-friendly tool for computing krippendorff's alpha inter-rater reliability coefficient. *MethodsX*, 12:102545, 2024. 10.1016/j.mex.2023.102545.
[20] Jakob Nielsen. How to conduct a heuristic evaluation. *Nielsen Norman Group*, Nov 1995.
[21] Marcus Niemietz and Jörg Schwenk. Owning your home network: Router security revisited. *arXiv preprint arXiv:1506.04112*, 2015.
[22] 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. doi.org/10.6028/NIST.IR.8425A.
[23] Dragan Perakovic, Ivan Cvitić, Tibor Kuljanić, and Luka Brletić. Analysis of wireless routers vulnerabilities applied in the contemporary networks. pages 31–37, 12 2018. 10.18638/rcitd.2018.6.1.123.
[24] Sreean Rikkala. React website. *Breaking Down ISP Routers: Security Privacy Insights*, GitHub, 2025. github.com/SreeanRikkala/Breaking-Down-ISP-Routers-Security-Privacy-Insights/tree/main/react-website.
[25] CableLabs Security. Gateway device security best common practices. *CL-GL-GDS-BCP-V01-211007*, (V01), Oct 2021. www.cablelabs.com/specifications/CL-GL-GDS-BCP.
[26] 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*, volume Association for Computing Machinery of *RSP '23*, New York, NY, USA, 2024. doi.org/10.1145/3625223.3649279.
[27] Verizon Communications. 4q 2024 earnings and business update. 2024. www.verizon.com/about/investors/quarterly-reports/4q-2024-earnings-business-update.