But is it exploitable? Exploring how Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers

GEORGE CHALHOUB, University College London and University of Oxford, UK
ANDREW MARTIN, University of Oxford, UK

Millions of consumer-grade routers are vulnerable to security attacks. Router network attacks are dangerous and infections, presenting a serious security threat. They account for 80% of infected devices in the market, posing a greater threat than infected IoT devices and desktop computers. Routers offer an attractive target of attacks due to their gateway function to home networks, internet accessibility, and higher likelihood of having vulnerabilities. A major problem with these routers is their unpatched and unaddressed security vulnerabilities. Reports show that 30% of critical router vulnerabilities discovered in 2021 have not received any response from vendors. Why?

To better understand how router vendors manage and patch vulnerabilities in consumer-grade routers, and the accompanying challenges, we conducted 30 semi-structured interviews with professionals in router vendor companies selling broadband and retail routers in the UK. We found that router professionals prioritize vulnerability patching based on customer impact rather than vulnerability severity score. However, they experienced obstacles in patching vulnerabilities due to outsourcing development to third parties and the inability to support outdated models. To address these challenges, they developed workarounds such as offering replacement routers and releasing security advisories. However, they received pushback from customers who were not technically capable or concerned about security. Based on our results, we concluded with recommendations to improve security practice in routers.

ACM Reference Format:
George Chalhoub and Andrew Martin. 2023. But is it exploitable? Exploring how Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers. In *The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 29 pages. https://doi.org/10.1145/3617072.3617110

1 Introduction

Consumer-grade routers are an essential part of the home network and provide the connection point for computers, tablets, and other network-enabled devices. They are the communication hub of the home, allowing users to access the internet, send and receive emails, work, shop and stay in touch with loved ones. Threats (e.g., remote access trojans) against routers have been increasing since the increase in home-working in 2020 due to the Covid-19 global pandemic [84]. According to a recent industry report by Symantec, routers have become a "hyper-scaling" security threat that accounts for over 75.2% of infected devices [67]. Trend Micro have reported that router family attacks (e.g., brute force attacks, remote command executions, access exploits) grew from five to 35 in just 3 years [88]. British consumer watchdog Which? revealed that at least 7.5 million UK residents use vulnerable routers [38].

This research was funded in whole or in part by InnovateUK [10028034]. For the purpose of Open Access, the authors have applied a CC BY public copyright license to any Authors Accepted Manuscript (AAM) version arising from this submission.

Manuscript submitted to ACM

Routers are one of the most attractive points of attack [62, 67]: they sit at the front gate of nearly every network and are the gateway to all internet-connected devices in the home [88]. A router is both an intermediary for almost all networking traffic and a line of defense from external attack (firewall); a compromised router therefore has the potential to both open the floodgates to new attacks and act as a jump off point for secondary attacks [76]. Because routers essentially control the network, they have an insidious ability to mount man in the middle attacks on entire portfolios of devices.

A major problem with routers is their outdated firmware and unpatched vulnerabilities [75]. A study by the Fraunhofer Institute for Communication examined 127 routers from seven major manufacturers and found vulnerabilities in all routers, where many routers tested had not received any security patch for 5 years [70]. In the US, the American Consumer Institute revealed that 83% of routers from popular brands have exploitable vulnerabilities [48]. These include malware, such as VPNFilter, which was thought to be sponsored by Russian military intelligence, and is estimated to have infected 500,000 routers worldwide. Other exploits which have taken advantage of a Universal Plug and Play vulnerability have infected at least 45,000 routers [12].

Despite the increased awareness of vulnerabilities found in routers and the numerous attack vectors, some vendor responses tend to be slow and in some cases, vague. Research from Kaspersky found that 30% of critical router vulnerabilities discovered in 2021 have not received any response from vendors (e.g., no patch or commentary) and 26% received only a comment from the vendor (e.g., most often including recommendations to contact customer support) [26, 46].

Researchers at Ben-Gurion University who presented critical router vulnerabilities at 13th USENIX Workshop on Offensive Technologies (WOOT) said [66]:

> "*We sent a draft of our findings to the manufacturers of the routers, [the] security response team notified us that they do not intend to fix the vulnerability we disclosed. None of the other router vendors responded to our disclosure.*"

In the United Kingdom, Sky took 18 months to patch a critical vulnerability affecting six million of its routers [41].

Prior work has broadly explored vulnerability management and patching in organizations [1, 10, 10, 17, 44, 50, 51, 55, 87, 89, 90]; but little is known about how router vendors prioritize and respond to security vulnerabilities, as well as their technical and non-technical challenges. To our knowledge, no qualitative study has been conducted on the *vulnerability management and patching practices of professionals in enterprise router vendors.*

Our overarching research question is: How do professionals in router vendor companies manage and address security vulnerabilities in consumer-grade routers?

To address our research question, we conducted a qualitative user study with 30 professionals (e.g., developers, engineers or managers) employed in enterprise router companies. Our aim was twofold: (1) understanding how router security vulnerabilities are evaluated, prioritized and remediated and (2) exploring the limitations and challenges of router vulnerability patching. We summarize our key findings below:

Router vendors prioritize patching vulnerabilities based on customer impact, rather than severity score: Router vendors developed their own prioritization processes (e.g., inferring context, deriving metrics) to patch router vulnerabilities. Vulnerabilities with the potential to impact customers (e.g., actively exploited in the wild) were prioritized over vulnerabilities declared with critical severity or zero-day vulnerabilities (§ 4.1).

Router vendors use third parties to develop routers, lacking direct control and autonomy over development: Router vendors outsourced router manufacturing (e.g., hardware, firmware development) to third-parties. When there was a need to patch vulnerabilities, vendors lacked direct control and autonomy over development processes, experiencing difficulties communicating with the original manufacturer (§ 4.2).

Router vendors offer free or discounted routers as a workaround to vulnerabilities that are difficult to patch: Router vendors experienced obstacles in patching vulnerabilities due to outsourced (e.g., firmware) and end-of-life routers (e.g., obsolete). As such, they developed workarounds such as offering discounted or free replacement routers to affected customers. In cases of end-of-life routers, vendors released security advisories to inform customers (§ 4.3).

Router vendors receive pushback from customers when attempting to upgrade routers: Despite efforts to upgrade routers through firmware or hardware upgrades, vendors experienced push-back from their users. They reported that some users were not technically capable to apply firmware or hardware upgrades, while others refused to upgrade outdated routers when they were sent free router replacement (§ 4.4).

The rest of the paper is structured as follows: we give an overview of relevant literature in Section 2. We describe our methods in Section 3. We present and discuss our results in Section 4 and Section 5, respectively. Finally, we present our recommendations in Section 6.

2 Literature Review

In this paper, we exclusively focus on 'consumer-grade routers', which we define as routers that are often located at homes or customer sites, are optimized for low cost and do not need hierarchical routing [37]. These routers can be obtained for free through ISP-provided routers (broadband router) or purchased through specific vendors (retail router). They are distinct from business and enterprise class routers, which often come with security plans [73].

2.1 Vulnerability Management and Patching

Vulnerability management and patching is a well-known challenge for product manufacturers [32, 72, 78]. Research shows that 70% of manufacturers fail to patch discovered vulnerabilities, and 30% fail to address vulnerabilities exploited in the wild, even when patches are available [8]. A common challenge is the number of vulnerabilities discovered. It is estimated that 150 vulnerabilities are discovered per week [58]. Evaluating vulnerabilities can be labor-intensive and tedious [4, 28, 60].

Another known challenge is the need to test patches before they are deployed in production environments [25]. Patches may interfere or be incompatible with existing system functionalities; and need to be thoroughly tested [71]. Organizations may not have the resources or expertise to properly evaluate patches and determine whether they are suitable for their environment [28]. In addition, patches may introduce new vulnerabilities [47, 56]. Moreover, a key challenge is that patch distribution is not standardized, and different vendors use different mechanisms to distribute patches [47, 86].

Finally, a major challenge is that the cost of patching can be high, especially in critical production systems [32]. Patching may require restarting or shutting down systems, which can incur downtime and lost productivity or revenue [6]. Patching may also fail and introduce unintended consequences, which would require systems to be rolled back to their pre-patch state, further increasing the cost of patching [54].

2.2 Vulnerability Management in IoT Devices

Vulnerability patching is more challenging in IoT devices than other technological solutions. IoT devices present a more complex IoT ecosystem that introduces security vulnerabilities from both edge and cloud [30]. Some IoT devices lack software updating capabilities, while other devices outlive the time period for which they receive updates [80]. As such, larger IoT firms tend to patch vulnerabilities only after rigorous testing, and out-of-cycle updates are triggered in emergency situations (e.g., exploitation) [42].

It is commonly agreed that IoT devices will inevitably be subject to security vulnerabilities and resolving these will not always be straightforward [11, 80]. For instance, Fernandes et al. discovered multiple privilege escalation vulnerabilities in common IoT devices and found that patching or mitigating these vulnerabilities will be difficult [30]. To address these challenges, researchers have developed new tools, frameworks and technical solutions with the aim to mitigate and address security vulnerabilities. For example, Simpson et al. [80], created a hub-based security manager in the router to intercept all communications and protect vulnerable devices. Wang et al. proposed Shield [92], a series of vulnerability-driven network filters for preventing known vulnerability exploits. Yu et al. proposed decentralized middleboxes to prevent unapproved communication between IoT devices in the home [94]. Similarly, Nighswander [65] proposed systems-level defenses and principles that can be deployed to secure critical GPS and dependent systems from vulnerabilities. Dixon et al. [24] presented HomeOS, a system that enforces data flow policies on IoT devices. Denning et al. offered a series of threats and case studies [21] and explored the secure development of household robots in [22].

Vulnerability management tools and programs tend to be more effective in theory than in practice [2, 39, 54, 71]. This can be due to organizations' limitations in terms of resources, budget, and personnel or a lack of understanding of the strategic limitations faced by the organizations in real-life context [60, 61, 72, 86]. Other factors include years of experience, mistakes, threat analysis, risk measurement, and regulations [35]. To address this gap, we explore the real-life challenges of vulnerability management in routers in order to derive recommendations tailored to the specific needs of router vendors.

2.3 Vulnerability Management in Routers

Routers are the most vulnerable internet devices, constituting 60% of all vulnerable internet-connected devices [69]. They have been exposed to critical vulnerabilities and repeatedly exploited for the past 10 years [93]. During 2020 and 2021, more than 500 router vulnerabilities were discovered [57].

There have been many efforts to improve router security [3, 36, 40, 45, 53, 76, 85]. For instance, Bitdefender Router Protection released Live Virtual Patching, a security platform for ISPs enabling live vulnerability patching in routers [79]. Despite recent advances in router security, vulnerability management and patching in routers seem to be lacking. Weidenbach and vom Dorp analyzed 127 routers of seven different large vendors in Europe; they described their results as '*alarming*'. They found security vulnerabilities in all routers, and that 46 had not received any security updates within the last year [70].

To our awareness, the identification and prioritization practices of router vendors are not well-known. To address this gap, we explicitly explore how router vendors identify and prioritize router vulnerabilities for patching.

2.4 Human Studies of Vulnerability Management

Numerous studies have explored the security needs and workflows of system administrators [14, 15, 17, 27, 44, 50, 51, 89, 90], their software upgrades and their security update behavior [55, 87]. Recent work has also looked into the role of ISPs in keeping IoT devices secure [52, 81].

Krombholz et al. [51] explored usability issues faced by system administrators trying to deploy the HTTPS protocol. Kraemer and Carayon [50] found that organizational structures and policies strongly influence how network administrators and security workers handle security. Chiasson et al. [17] created interface design principles to assist system administrators in diagnosing security challenges. Kandogan et al. [44] explored security stories and experiences of IT administrators. Velasquez and Weisband [89] found that informational and system factors influence system administrators beliefs and attitude, and also found that system administrators acquire knowledge through practice rather than certifications [90]. Crameri et al. [20] found that system administrators apply security patches on smaller systems before patching them in the product. Dietrich et al. [23] found that missed or delayed software updates cause most security misconfigurations.

More work has specifically targeted update processes in companies [9, 10, 59, 91]. For example, Vitale et al. [91] found that system administrators prioritize security and licensing over usability problems of updating systems, confirming Min Khoo and Robey [59]'s findings that in a corporate context, business needs rather than user requirements drive update decisions. In contrast, Blythe et al. [10] found that company employees don't feel responsible for security updates and rely on security experts to patch them. Li et al. [55] conducted an in-depth exploration of update processes of US-based system administrators and found that they apply software updates through five main stages, reporting several pain points. In a similar study with focus on German-based system administrators, Tiefenau et al. [87] confirmed most of Li et al.'s findings drawn from UK-based companies, thus representing a different culture.

More closely related to our work, Alomar et al. [1] conducted 53 interviews with predominantly US-based security practitioners tasked with vulnerability discovery or management. They found that organizations struggle with vulnerability remediation due to trust, communication, funding, and staffing issues. We expand on their findings by focusing on vulnerability management processes of professionals working in UK-based router vendor companies; focusing on a set of critically vulnerable devices (e.g., routers), and representing a different culture (e.g., UK-based).

3 Methods

From October 2022 until January 2023, we conducted a qualitative user study with professionals (e.g., security engineers, consultants, managers, senior executives) working in various UK-based router vendor companies. We conducted 30 semi-structured in-person and remote interviews, focusing on understanding vulnerability management and patching processes of router vendor companies, as well as the companies technical and non-technical limitations. Our institution's ethics committee approved this study (see Section 3.7).

We used Grounded Theory [83] for this study. As such, our data collection, data analysis, and theory development processes were iteratively conducted. We iteratively collected and analyzed data until we reached theoretical saturation – the point at which additional data adds no additional insight into our new theory (see Section 3.6).

We chose to investigate routers because they (i) are a hyper-scaling threat subject to increased security attacks, (ii) are a gateway to other devices in the home, (iii) have a significant portion of critical vulnerabilities that remain without any response from vendors.

3.1 Research Questions

Our work aims to address the following research question:

RQ. How do professionals in router vendor companies manage and address security vulnerabilities in consumer-grade routers?

To address our main research question, we explore the following sub-questions:

(1) How do professionals in router vendor companies evaluate, prioritize and remediate security vulnerabilities in consumer-grade routers?
(2) What are the technical and non-technical limitations that professionals experience when addressing router vulnerabilities?
(3) How do professionals deal with challenges and obstacles faced when addressing router vulnerabilities?

3.2 Recruitment

We used several means to recruit our participants, including advertising on Twitter, Reddit, Mailing Lists and Blogs. We also reached out to participants on Slack channels and LinkedIn. To diversify our sample, we aimed to interview senior managers and executives (e.g., CIO , CTO and CISO) who have likely made important decisions on security vulnerability management (See Appendix E). Since these are a hard-to-reach group [5, 29, 74], we used the snowball sampling method [33] to recruit some participants, and worked with a consultant advisor who had wider access to senior executives working in router vendor companies.

We aimed to recruit participants working at different companies, however, some participants were from the same company. When that was the case, they were not connected to each other and worked on different products. At the time of recruitment, interested participants were employees who were active at their company and responsible for the security, development, management or maintenance of a consumer-grade router product.

In addition, aimed to recruit UK-based participants with access to UK markets. In addition to selling products in the UK, three sold routers in the EU, two in the US and one in Germany.

We asked interested participants to complete an online screening questionnaire (see Appendix B). We received 165 complete responses. In addition to asking demographic questions, we asked participants to provide details on their employment as well as their company size. We describe the demographics of our participants in Table 1 in Appendix A.

3.3 Interview Procedure

We conducted semi-structured in-person and remote interviews with 30 professionals working at router vendor companies that sold consumer-grade routers (both broadband and retail routers). We interviewed participants using the funnel technique [13], starting with general questions and then drilling down to specific ones. We tailored our semi-structured interviews to our participant's roles, background and security experiences. We also asked follow-up questions or probed when appropriate.

We started the interview with general questions characterizing participants' role at their company (e.g., role, responsibilities), the type of routers they are focused on, and their user base. We then asked participants to describe how their routers get compromised (e.g., attack vectors and common security vulnerabilities) and how they keep them secured (e.g., security processes, security testing practices, security tools used). Moreover, we asked participants to describe how they discover (e.g., security scanners, user reports, bug bounty) and test their routers (e.g., third-parties, pen-testers) security vulnerabilities. Furthermore, we asked participants how they address and remediate vulnerabilities,

as well as how they prioritize patching (e.g., severity, zero-day vulnerabilities). We also asked participants to detail how they support users with infected routers (e.g., notifying users, applying patches, offering technical support). Finally, we asked participants about their challenges and limitations, as well as their appetite to adopt new interventions (e.g., hardware security, software engineering practices).

We conducted 15 interviews in-person (in secure locations in our institution) and 15 interviews remotely (on Microsoft Teams). In order to get rich data, we used open-ended questions, inviting participants to answer in their own words. Due to sensitivity of the interviews, three interviewees did not consent to being audio recorded; instead we took handwritten notes. We also audio-recorded and transcribed 27 interviews. Recorded interviews lasted for an average of 65 minutes. Our interview questionnaire can be found in Appendix D.

3.4 Pilot Study

To validate our initial interview questions (see Appendix D.7), we conducted a pilot study with six professionals. We recruited the pilot participants in a government-organized security-related networking event in October 2022. We distributed flyers about our pilot study, and had a booth where participants could sign up. Two researchers analyzed the pilot interviews. We used the findings to identify potential problems (e.g., adverse events, time) in advance prior to conducting the full-scale study. We didn't use the results from the pilot interviews, but we made the following changes:

- Recruitment process: We used snowball sampling to recruit hard-to-reach groups such as senior managers.
- Interview questions: We refined our script to reduce bias, improve quality and include more open-ended questions.
- Data analysis: We used grounded theory instead of thematic analysis due to in-depth & open-ended interviews.

3.5 Participant Demographics

Table 1 in Appendix A summarizes the demographics of our sample (n=30). We interviewed 23 male and seven female participants. Ages ranged from 29 to 52. 20 participants had a college (or undergrad degree) and 10 had a graduate (or postgraduate) degree. 15 participants were interviewed in person and 15 remotely.

We divided our participants (n=30) into four groups of stakeholders based on employment: managerial stakeholders (n=12), technical stakeholders (n=14) and consulting stakeholders (n=4). Out of 30 participants, 16 had roles directly related to security.

3.6 Data Analysis

We transcribed and analyzed all 30 semi-structured interviews using Grounded Theory, following Strauss and Corbin's procedure [83]. We used grounded theory because we were looking for patterns or trends in our interview data, which can help explain how or why phenomenons occur. Grounded theory can also lead to comprehensive and deep explanations [82].

Four researchers in total analyzed the transcripts. The primary researcher and a second researcher independently coded all interview transcripts. To verify the credibility of the initial codes, a third researcher cross-checked the codes against the interview transcripts. At the same time, a fourth researcher reviewed the initial codes and supporting quotes. The four researchers discussed any differences and generated a codebook of 216 codes. We then grouped the codes into themes (using axial coding; relating codes to each other through a combination of inductive and deductive thinking) and categories (using selective coding; selecting one category to be the core category, and relating all other categories to that category).

We observed data saturation [19, 34, 77] between the 28th and the 30th interview; i.e., no new codes emerged in interviews 28–30, and, hence, we stopped interviewing. After creating the final codebook (see Table 5 in Appendix F), we tested for inter-rater reliability. The initial coding had an agreement of 0.60 (average Cohen's kappa coefficient (κ) for all codes in our data). After cross-reviewing coding decisions, clarifying coding rules, and independently re-coding the utterances, inter-rater reliability increased to an acceptable level (average Cohen's (κ) was 0.83) [18]. The remaining disagreements were individually negotiated and resolved.

3.7 Research Ethics

The University of Oxford's Central University Research Ethics Committee (CUREC) reviewed and approved the study (C1B-22MT-COML-001). Prior to each interview, participants were briefed and signed an informed consent form explaining our study and data confidentiality practices. Due to the sensitivity of our interviews, we asked participants not to name specific people or sites so that the interviews will be anonymous to some degree.

All interviews were AES 256 encrypted and stored in a physical safe in our organization. Participants were thanked for their time with £100 in electronic store vouchers. In addition, participants were reimbursed for out-of-pocket expenses related to participation, including travel, meals, accommodation, and childcare. Participants could withdraw themselves and their data at any point, without loss of compensation, and without providing a reason. No participant withdrew.

3.8 Limitations

Our study has a number of limitations common to all qualitative research studies (e.g., [16]).

First, research quality depends on the interviewer's individual skills and might be influenced by their personal biases. Inexperienced interviewers may not be able to ask prompt questions or probe into situations that would result in missing gathering relevant data [49]. For instance, the depth of data collected is dependent on the interviewer's skill [43] and the quality of the questions asked [7]. To address this, one trained researcher, who was trained to conduct the interviews consistently and ask questions in an open and neutral way, conducted all 30 interviews.

Second, self-reporting bias is common in interview studies [31]. Some participants might have not responded accurately to our questions because they did not remember specific details. Other participants could have been concerned about the interviewer's perception of them and, therefore could have changed their answers in line with how they like to be perceived. To maximize validity and minimize self-reporting bias, we avoided leading questions and relied on open-ended questions, inviting participants to provide in-depth answers in their own words. Some of our participant answers were less detailed, however, we prompted participants to give full answers to all questions. In addition, we made assurances of confidentiality, verbally and through consent forms. We presented confidentiality agreements at the beginning of the data collection process. We discussed confidentiality at the outset to build trust and rapport with participants. We assured them that their audio recordings will be transcribed, anonymized and permanently deleted following their interview.

Third, security vulnerability management is a sensitive issue in router vendor companies. Our participants' corporate responsibilities, as well as their company's reputation, might have biased their responses. Many participants were not able to share confidential information about vulnerabilities, and could have stripped essential and valuable research data. For instance, P11 said "*I would have to be very careful what I say even though you say it's confidential.*" To mitigate this, we briefed our participants about our security and privacy measures, focusing on how we will encrypt their data and process it in accordance with the General Data Protection Regulation (GDPR).

Fourth, we note that ours is a qualitative study. We do not attempt to quantify our findings or draw conclusions or generalizable findings about a larger population. The focus of our qualitative work is about the richness of understanding rather than the generalizability. Our findings, emerging themes and discussion (e.g., patching based on impact, outsourcing, customer pushback, developing workarounds) coming from the grounded-theoretic analysis, would need to be tested in a follow-up confirmatory study with a larger population of global router vendors to assess their broader applicability and generalizability.

Fifth, senior router stakeholders (CTOs and CISOs) were notoriously hard to reach; as a result, we worked with a consultant advisor who could only connect us to participants based in the UK. As such, our study's population has a regional limitation and may not be representative of the global router vendor market. Future work should explore vulnerability management aspects with a broader population, such as examining differences between the UK router vendor population and other populations, or investigating specific aspects about the UK router vendor market that may have influenced our results.

4 Results

We detail the findings of our study in this section. We discuss our key findings organized according to the main themes of our analysis. The main themes are: Vulnerability Prioritization Processes (§ 4.1); Obstacles to Vulnerability Patching (§ 4.2); Workarounds for Patching Vulnerabilities (§ 4.3); User Pushback to Vulnerability Mitigation (§ 4.4).

We defined a '*router*' as a standalone device that connects two or more packet-switched networks or subnetworks. We distinguished between '*third party routers*' and '*ISP-provided routers*' during our analysis. We defined a '*third party router*' as a standalone router, obtained and managed independently, and often manufactured by a company that does not own the network provider. We defined an '*ISP-provided router*' as a fully managed router that is owned by the network provider and could include a combination of a router and a modem in a single device.

4.1 Vulnerability Prioritization Processes

Router vendors developed their own vulnerability prioritization processes by (i) adding more context to assess the risk arising from each vulnerability (§ 4.1.1), and (ii) deriving relevant metrics rather than relying on vulnerability scores (§ 4.1.2). Overall, they prioritized vulnerability patching based on the potential impact to their customers: vulnerabilities that were actively exploited in the wild were prioritized while patches that caused performance or downtime problems were delayed (§ 4.1.3).

4.1.1 Inferring Context to Measure Vulnerability Risk Participants (n=20) emphasized that inferring context is essential to understanding the risk of vulnerabilities. Participants reported different interpretations of understanding context when addressing vulnerabilities. Security Engineer P19 built a multi-dimensional map of all assets and entities in their organization in a graph database, which is then linked to existing security tools such as vulnerability scanners and endpoint detection and tools – which allowed them to better prioritize reported vulnerabilities. In contrast, Network Engineer P24 built a data model of all company assets and the relationships between them, which helps them accurately evaluate risk in a real-world context. They said:

> "*We do come across many vulnerabilities, but only 5-to-10% tend to be exploited. Many vulnerabilities seem critical when viewed in isolation, but they have inherently little value when they are put into context.*" (P24)

We list frequently reported contextual factors in Table 2 in Appendix A.

4.1.2 Deriving Metrics to Assess Vulnerability Severity Rather than rely on zero-day vulnerabilities or severity scores, participants (n=18) derived their metrics to assess the severity of vulnerabilities. Participants referred to severity scores to indicate that they avoided strict scoring frameworks (n=8), and put more emphasis on items not included in older versions of CVSS (n=10). Chief Technology Officer P20 explained:

> "*So just looking at vulnerabilities as a severity score is useful, but that really doesn't give us a genuine sense of the importance of that vulnerability. What we're always trying to do here is coming with the prioritization metric, how do we know what to work on next and how do we evidence what we've done is vital.*" (P20)

Other participants (n=15) reported that vulnerabilities being actively exploited in the wild tend to have higher severity ratings. Deputy CISO P11 explained:

> "*There is a difference between a vulnerability being declared and its impact being critical, versus a vulnerability being declared and being actively exploited in the wild at scale.*" (P11)

Similarly, Security Officer P09, who worked in a security incident team said that they look for evidence of publicly available proof-of-concept exploits or evidence of threat actors exploiting vulnerabilities before making key decisions. We list frequently reported metrics in Table 3 in Appendix A.

4.1.3 Patching Vulnerabilities Based on User Impact Participants (n=13) patched vulnerabilities based on the potential to impact router users. Patches for actively exploited vulnerabilities that exposed users to malicious code, malware, and data theft were prioritized; whereas patches that caused performance or downtime problems to routers were delayed. Senior Security Officer P07 explained:

> "*If a zero-day vulnerability or other critical issue arises, the first thing we do is assess the impact of that to the customer. Let's say it's a vulnerability that for some reason completely negates the firewall I mentioned before. It's an exploit which can compromise the router by knocking on a certain port in a certain way from the wider internet, and this tricks the router into doing something it shouldn't do. That would be an absolute critical vulnerability.*" (P07)

Chief information security officer P16 explained that they roll out patches in increments to their broadband router based on performance. They explained:

> "*There's an absolute catastrophe, we'll make a change, patch it, roll it out to 5% of the [broadband router brand], monitor the adoption, the device is crashed. Did they come back up successfully? If so, is performance impacted in any way? Is it doing what we expected it to do? Give it a few hours, depending on the severity, give it a few hours. The next 5%, the next 5%, and so on.*" (P16)

In summary, our participants believed that their vulnerability prioritization efforts and processes (e.g., inferring context, deriving metrics, patching based on user impact) were effective in managing security vulnerabilities in routers and achieving a robust security posture.

4.2 Obstacles to Vulnerability Patching

Router vendors outsourced routers' hardware and firmware development to third-parties, and weren't able to patch vulnerabilities promptly due lacking autonomy and control (§ 4.2.1). Furthermore, they weren't able to patch vulnerabilities in end-of-life (e.g., obsolete) routers (§ 4.2.2). Finally, router vendors weren't able to detect which customer routers are being exploited in the wild due not having access to customer data (§ 4.2.3).

4.2.1 Outsourcing Development to Third Parties Participants (n=22) outsourced hardware and firmware development to third-parties (i.e., offshore companies). When there was a need to patch vulnerabilities, they had limited control and autonomy (n=19), experienced communication issues (n=18), and lacked clear agreements with third-party manufacturers (n=3). Security Manager P01 whose company outsourced router firmware development to a partner in Asia said they collaborate to address vulnerabilities, but the team structure was not stable, stating that "*people come and go*". Participants reported communication barriers such as time zone differences, languages and cultural preferences and confidentiality needs. For instance, Security Engineer P03 faced obstacles fixing critical vulnerability in outsourced router firmware due to language differences. Other vendors lacked clear agreements with third-party manufacturers: IoT consultant P29 whose company outsourced hardware development to multiple third-parties explained they did not always have clear security-related quality assurance agreements. They said:

> "*When we get our routers built, obviously we didn't build them ourselves. We subcontract that out to various manufacturing houses across the world and we source the components from various manufacturers and then we've got the final systems integrator to put all the chips together, PCBs, all the plastic housing, everything. Some agreements are not too clear on patching, so the biggest challenge is incentivizing manufacturers to patch vulnerabilities once software is shipped.*" (P03)

We list reported communication barriers in Table 4 in Appendix A.

Some participants stressed that a potential solution would be the introduction of quality assurance contracts between domestic vendors and third-party vendors. Such contracts would ensure patching and security maintenance, as well as regular vulnerability assessments and other standard security practices.

We note that some challenges identified within the supply chain were specific to routers and were not seen in other IoT devices. Some participants envisioned routers as high-powered servers with many ethernet ports running not only routing software but, in some cases, even multiple containers; where their complexity expands the already ripe attack surface of other supply chain sides.

4.2.2 Inability to Support End-of-life Routers Participants (n=23) said that they are unable to patch vulnerabilities to routers due to reaching their end-of-life. From a vendor's point of view, an end-of-life (EOL) product is a product that has reached the end of its useful life and is no longer manufactured or supported. Therefore, its firmware, utilities, and website are no longer updated. Chief Executive Officer P15 explained:

> "*As per company policy, we don't release patches or workarounds to end-of-life routers. If the router is too old, we frankly tell them to throw it away and get a new one.*" (P15)

However, some participants (n=2) confirmed their support for critical firmware and security updates in EOL routers for a short period of time. Future work should explore why certain router vendors offer support to products that have reached EOL and how it would align with their business models. Other participants (n=14) cited the economic cost of supporting EOL routers to be high. For instance, Business Manager P27 stated that they have to focus their resources on supporting the latest models, rather than outdated ones. Other participants such as Security Consultant P05 were in favor of providing security patches to EOL routers, but said it is difficult for them to make their case. They said:

> "*It's hard to explain to the people who control the money, the purse strings to spend more. Especially when the people who govern finance never understand technology and how it works.*" (P05)

4.2.3 Not Knowing Which Routers are Being Exploited For regulatory and ethical reasons, participants (n=7) said they do not collect customer traffic (e.g., browsing habits). When zero-day or critical vulnerabilities emerged in routers,

it was sometimes difficult to know routers were actively being exploited. For instance, Security Lead P30 explained that compromised routers can redirect users to fake or unwanted sites, but they are difficult to detect since they don't access customer traffic. Similarly, Security Engineer P03 explained that it was difficult to track routers being exploited by authentication-bypass vulnerability due to not having access to HTTP traffic. Moreover, due to the limited data collected, Security Consultant P02 explained that it is impossible for them to determine which of their routers are being exploited. They said:

> "*There's absolutely no way to know it could be mining cryptocurrency. And yeah, there's no way to know. Maybe it'll get hot if the CPU is looping. So even if it was mining cryptocurrency and running at 100% CPU, you wouldn't even know.*" (P02)

In summary, our participants reported major obstacles to vulnerability patching in routers (e.g., end-of-life routers, outsourced development, not knowing which routers are exploited). Overall, our participants found that the vulnerability prioritization processes reported in Section 4.1 were helpful, but not sufficient in addressing these major obstacles. As a result, they developed workarounds, which will be discussed in the next section.

4.3 Workarounds for Patching Vulnerabilities

To address obstacles of vulnerability patching, participants developed several workarounds. Router vendors offered replacement routers (e.g., often newer models) for free or discounted rates when vulnerabilities couldn't be patched due to outsourcing (§ 4.3.1). Moreover, router vendors issued advisories (e.g., web pages) when vulnerabilities couldn't patched due to end-of-life routers (§ 4.3.2), provided mitigation advice when vulnerabilities couldn't be promptly fixed (§ 4.3.3) and forced firmware patches when users did not voluntarily install firmware updates (§ 4.3.4).

4.3.1 Offering Free or Discounted Routers Router vendors (n=3) developed workarounds for vulnerabilities that were difficult or impossible to patch. Users of routers that were still supported by vendors (e.g., have not reached end-of-life) were offered free or discounted replacement routers. Security Officer P09 explained dealing with a critical vulnerability that affected users who have not changed the router's default login credentials. However, they could not address the vulnerability in a small portion of routers because they had not manufactured it. As a result, they offered free replacement routers to their customers as part of a managed router service, which includes providing the router and hardware maintenance. They explained:

> "*A small portion of our routers were not made by us, when the problem happened, we offered to replace them for free.*" (P09)

Similarly, Security Engineer P03 explained that after a critical openSSL vulnerability emerged in the firmware of one router model that was soon to reach end-of-life, they decided to address the vulnerability in a newer model which was discounted to affected customers.

4.3.2 Releasing Security Advisories For routers that were no longer supported (e.g., reached end-of-life), vendors (n=6) released security advisories where they explicitly informed customers that they will not be patching the vulnerabilities. Chief Information Security Officer P26 explained that their company has implemented security vulnerability disclosure policies, which clearly address vulnerabilities in unsupported routers. They explained that they often release security advisories to vulnerabilities that can't be addressed when routers have reached end-of-life:

> "*If we're not addressing a vulnerability due to end-of-life, we will make it very clear that we didn't and won't introduce any updates.*" (P26)

Similarly, Security Manager P1 explained that their company does not provide support for discontinued routers, but has an official web page of legacy products which lists all products that have reached end-of-life.

4.3.3 Providing Mitigation Advice For vulnerabilities that could not be promptly patched, vendors (n=9) provided mitigation advice. They advised customers on how to mitigate these vulnerabilities. Vendors communicated this advice through formal communication channels, such as emails or Security Advisories (e.g., see Section 4.3.2). Network Engineer P14 reported that their routers were exposed to a remote code execution vulnerability that were incapable to promptly fix. They advised users to reset and disable remote management features of their routers in order to prevent any potential exploitation of the vulnerability. Similarly, Network Administrator P25 reported their routers were exposed to a remotely exploitable flaw that they were planning to address in the next software upgrade. To protect their customers, they advertised a workaround involving accessing the virtual machine of their router and editing code:

> "*When there is an available workaround, we usually tell customers what to do, in this case, open the VM and edit these files.*" (P25)

Similarly, Security Engineer P19 advised customers to block specific ports in order to avoid exploitation of a vulnerability.

4.3.4 Forcing Firmware Upgrades Participants (n=4) reported force-feeding routers with a firmware update when users did not install released firmware patches. Senior Consultant P05 received reports of a severely critical vulnerability affecting millions of routers. When they released a patch, most users did not update their router firmware. As a result, they forced an update on affected devices and alerted affected customers with notifications through management interfaces. They explained:

> *"People tend to think of their internet access line as one singular magic pipe. That's not the case. It's essentially four networks. The third and fourth networks we have are essentially maintenance and monitoring and diagnostics. That line is what we use to push down firmware updates. If it's critical, what we'll do is we will make a patch, we will rebuild the firmware, and we actually have the ability to push firmware updates out to our fleet on demand.*" (P05)

Similarly, IT Security Engineer P06 explained that they do force firmware updates for critical vulnerabilities that could disrupt internet access.

In summary, our participants developed workarounds (e.g., offering replacement routers, releasing security advisories, providing mitigation advice) to overcome obstacles to patching vulnerabilities. However, they reported user pushback, which we will describe in the next section.

4.4 User Pushback to Vulnerability Mitigation

Despite developing workarounds to address obstacles for vulnerability patching, participants reported pushback to vulnerability mitigation efforts. Not all routers upgrade their router hardware even when newer models are sent to their homes for free (§4.4.1). Moreover, router users that are not technically capable or family with technology tend not to install firmware updates or replacement routers (§4.4.2). Finally, participants expressed frustration that most of their router users are not concerned about router security (§4.4.3).

4.4.1 User Refusal to Upgrade Outdated Routers Participants (n=3) explained that some of their customers decide not to upgrade router devices even when new routers are offered for free or shipped. As a result, some customers end up with unsupported (e.g., end-of-life, discontinued) devices, depriving them of security patches. For example, Senior

Consultant P21, who works in a broadband router company explained that customers get free router replacements in their contract, but some elect not to upgrade:

> "*One thing I do know is that we do have a lot of legacy hardware still in the field or some customers, we'll send them a new [router] because their old one is out of support, and they elect not to switch the [router] over. Either because they don't want to or they don't know how, or they're afraid they'll break the internet, or whatever it is. We can see in our analytics dashboards that some customers are running hardware from 10 years ago, have chosen not to upgrade. I don't believe we support those devices anymore.*" (P21)

4.4.2 Technically Incapable to Upgrade Routers Participants explained that some of their customers do not have the technical expertise to upgrade their routers (whether it is a firmware or hardware upgrade). For example, CISO Advisor P12, working in broadband company explained that their customers are unable to replace their routers on their own, despite giving clear instructions:

> "*We'll send them the hardware, but they won't plug it in because they are not– even though we give them very clear instructions and we even color code the back of the [router] with the red, green, and yellow, and we have instructions inside saying, "Plug this cable into the green hole, plug this one into the red hole," people still don't do it just.*" (P12)

Moreover, Security Engineer P3 explained that a common challenge faced is that only their technically-competent or power users tend to upgrade the firmware of their routers.

4.4.3 Users Not Concerned About Router Security Participants (n=10) reported that router users are generally concerned about router security. As a result, efforts to improve the security of the routers (e.g., pushing hardware, firmware) are met with indifference. Chief Information Security Officer P10 explained:

> "*The average users just want to be connected to the Internet. Once they're connected to the Internet, they don't care anymore about the router. As long as you can breathe, you're not going to go for an annual physical.*" (P10)

Chief Technology Officer P08, explained that most of their customers are not concerned about security, and are not concerned with any features in their router's web management portal. They added:

> "*99% of our customers don't log in to the web portal on the [router] itself to actually do any user configuration. Maybe they do to change the WiFi password or the SSID, but that is rare. I'd say 1% example. Typically once they plug the internet in, they pull the little card off the back that has the SSID and the password, and that's it.* " (P08)

Other participants were frustrated, and mentioned that educating users about router security has not been successful. Privacy Engineer P04 said:

> "*Increase awareness, increase awareness, increase awareness, we have seen that for decades and it's not solving the problem.*" (P04)

In summary, our participants reported customer pushback (e.g., refusal to upgrade routers) to vulnerability mitigation efforts. We note that this finding is based on the perspectives of router vendors, which may offer limited insight into router customers. Future work should explore user perspectives and experiences in managing their router security.

5 Discussion

5.1 The Role of Regulation in Router Security

Given the lack of economic incentive for manufacturers to build better security into consumer-grade routers and the high number of vulnerable products in the market, we argue that government intervention is critical and necessary to improve vulnerability management and patching in routers.

In the UK, the landmark Product Security and Telecommunications Infrastructure Act 2022 has been recently passed [68]. Participant P05 said that the bill "*puts even more responsibility on telco providers to be responsible for the security and management of their devices in customers' homes.*" The new bill will prompt router manufacturers to refrain from using easy-to-guess default passwords, be more transparent to consumers about the length of time they will receive security updates, and create a better reporting public system for vulnerabilities. We argue that this legislation is a good first step; many consumer-grade routers fail to notify users if and when firmware updates become available, even though those updates are essential to patch security holes. Being more transparent about router upgrades to users is crucial.

Furthermore, our interviews imply that more is needed to better protect the security of consumer-grade routers. The average lifespan of consumer-grade routers is between three and five years. After consumer-grade routers reach end-of-life, our results show they do not receive any further support from the manufacturer (§4.2.2). Our results also show that users who are not technically capable are not unable or uninterested to upgrade obsolete routers.

Legislation could enforce an extended lifespan or a minimum guaranteed lifetime for consumer-grade routers. This would ensure that router users have access to security features for a more extended period. It may assist router customers who do not respond to security notifications from router vendors. Moreover, it would protect the security of populations who are not technically capable or vulnerable and are hesitant to upgrade to newer router models.

Moreover, just as data protection regulation requires companies to notify users of data breaches, legislation could also mandate more transparent communication with router customers. This could include clearly communicating the time, skill, and costs associated with remediating vulnerabilities. For example, router vendors could be required to clearly explain the implications of device replacement to customers, such as whether patches or replacements will maintain the network configuration or "reset" the home network. They could also indicate whether a vulnerability patch will cause downtime on the network, and explain the time costs associated with installing a patch.

Furthermore, while most routers provide security patches, not all are not automated and some require manual effort (often unbeknownst to consumers). Our results suggest that not all the users of consumer-grade routers have the skills to carry out firmware or software upgrades on their routers (§4.4.2). Legislation could require automatic updates by default in consumer-grade products.

In addition, reports show that some router vendors can be slow in patching vulnerabilities[1]. For example, in the US, a prominent broadband company did not fix a reported flaw in their routers for over two years [63]. While this may point to cultural differences in router companies, regulation could impose a legal obligation on routers vendors to correct known vulnerabilities within a certain time frame from their detection or announcement. This could include GDPR-like provisions where manufacturers have a specific window to respond to legal queries (e.g., 30 days).

We acknowledge that our proposed regulatory changes may have negative impacts, and could be significantly challenging (e.g., third-party dependencies). Future work should consider the potential consequences of our suggested changes, discuss the potential challenges, and the need for further research to determine the implications of our proposed changes.

[1]https://techcrunch.com/2019/05/22/tp-link-routers-vulnerable-remote-hijack/

5.2 ISP-Provided or Store-Bought Routers?

When UK households sign up for an Internet Service Provider (ISP), they usually receive a free router from their broadband provider[2] also known as a broadband router or an ISP-provided router. Some claim that store-bought (e.g., retail) routers are more secure than ISP-provided routers [64], and vice versa. As such, some users elect not to use store-bought routers while other users stick to their ISP-provided routers.

Participants (n=6) who worked at broadband router companies claimed that their routers come with additional security features from the ISP such as firewall, malicious traffic monitoring or automatic security updates. Conversely, participants (n=5) who worked at retail router companies claimed that their routers offered additional security features, extra controls, more stability and support for secure third-party firmware.

We argue that just having a broadband or retail router does not translate on its own into having a more secure router. It depends on the manufacturer having necessary security practices, processes and controls in place to ensure that routers are secure. This includes practices such as ensuring that router's firmware update and security patches are applied, changing default usernames and passwords and using encryption. Just like retail routers, broadband routers are not immune to security vulnerabilities or attacks (e.g., some experts suggest that they can be a prime target for intelligence agencies and criminal organizations[3]).

In addition, some router users report being unable to replace their ISP-provided router[4]. This can occur when ISPs either contractually prohibit users from using other routers or withhold connection data (e.g., authentication details for a PPPoE/VoIP connection). We argue that router users should have freedom of choice. If users elect not to use devices provided by their ISP, the ISP should (i) respect their decisions without repercussions and (ii) offer necessary support. This could lead to improved security practice in routers. For instance, if ISPs are slow to patch vulnerabilities in routers, users would have the option to use more secure routers.

5.3 Responsibilities between Vendors & Users

Our results show that responsibilities between routers and vendors and consumers are not clear. There are no clear boundaries to how far router vendors should go to protect their customers. Some participants did not know how far they should go to protect their users. Some broadband companies that offer router products as part of a managed router service go as far as sending technical staff to households in order to assist with replacing outdated hardware (§5.1). However, our results show that many router vendors struggle on drawing the line in protecting users.

Conversely, the responsibilities that the users have to make to protect their routers are not clear. Some router users expect their ISP to be fully responsible for their router security, regardless of whether they took any proactive steps (e.g., replacing hardware, upgrading firmware). Many responsibilities such as using firewall for protection, keeping firmware of the router upgraded, security physical access of the router, replacing end-of-life router are not clearly advertised to the user. We argue that future work is crucial to properly define the responsibilities boundaries between router vendors and users.

5.4 The role of Hardware in Preventing Router Vulnerabilities

Our participants stressed the need for development and implementation of security-focused hardware into routers. They explained that security-focused hardware which follows the principle of supporting limited and discretely defined

[2]https://www.cable.co.uk/broadband/guides/own-router/
[3]https://www.tomsguide.com/us/home-router-security,news-19245.html
[4]https://www.reddit.com/r/HomeNetworking/comments/zq0kba/isp_wont_allow_me_to_change_the_router/

functions is able to minimize the attack surface from router vulnerabilities. For instance, the ARM Morello program[5] seeks to prevent memory-based vulnerabilities on a hardware level. We argue that more work needs to explore how these hardware technologies could be deployed into routers in order to mitigate router vulnerabilities.

6 Conclusion

Consumer-grade routers are the gateway to the internet. All the traffic from every internet-connected device in the home goes via the router, so its security is paramount. Despite that, consumer-grade routers have been the '*low hanging fruit*' for cyber-criminals for many years. They are one of the most infected and attacked devices in the market. Routers are affected by a plethora of severe and critical security vulnerabilities that are unpatched or unaddressed by router vendors. Despite that, the vulnerability management and patching practices of router vendors have received little-to-no attention.

To address this gap, we conducted a semi-structured interview study with 30 full-time professionals (e.g., security engineers, senior managers and executives) in the UK working in router vendor companies selling both ISP-provided and retail routers. Based on our findings, we conclude with recommendations to the security of routers:

Develop Communication Tools between Users and Vendors: Our results show that not all router vendors have established communication means with users. We propose that future studies should explore how to create better communication tools for router users and vendors. These tools can be in the form of mobile applications or web interfaces. Such studies can explore how these tools can keep users informed about potential security vulnerabilities, devices that have reached end-of-life and available firmware patches.

Designing User-Friendly Security Interfaces for Routers: Our interviewees reported that some firmware updates and security patches require users to run command lines, start virtual machines and edit configuration files. This is non-tenable considering many router users lack technical skills or are unfamiliar with technology. Cyber security firm F-Secure stated that "*the user interfaces on many routers seem more like cruel jokes than anything else*". We argue for the need for a user study to better understand how we can better design interactive and user-friendly interfaces that allow users to manage the security of their routers. Such studies can attempt to create new user experiences where they can guide users through installing security patches or firmware updates.

Understanding the Attitude Concerns of Router Users: Our interviewees reported that router users did not elect to upgrade their consumer-grade routers, even when they are sent replacement routers for free and with clear instructions. Some participants speculated that router users were worried that upgrading their router might introduce connectivity issues. The attitudes and concerns of router users towards router vendor upgrades are not too well-known. There is a need for a user study to better understand the perceptions and preferences of router users towards hardware upgrades. This would help hardware vendors appreciate user preferences and refine their hardware upgrade strategies.

Acknowledgments

This work was supported by the Secure Networking by Design (SNbD) project with grant number 10028034. We are grateful to James Willison and John Moor from the IoT Security Foundation (IoTSF) for their significant assistance with participant recruitment. We are thankful to the anonymous reviewers for their valuable input. We are also thankful to Nick Allott from nquiringminds for their help with our study design.

[5]https://www.arm.com/architecture/cpu/morello

References

[1] Noura Alomar, Primal Wijesekera, Edward Qiu, and Serge Egelman. 2020. " You've got your nice list of bugs, now what?" vulnerability discovery and management processes in the wild. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 319–339.

[2] Henrique Alves, Baldoino Fonseca, and Nuno Antunes. 2016. Software metrics and security vulnerabilities: dataset and exploratory study. In *2016 12th European Dependable Computing Conference (EDCC)*. IEEE, 37–44.

[3] Kim Andersson and Patryk Szewczyk. 2011. Insecurity by obscurity continues: are ADSL router manuals putting end-users at risk. *Australian Information Security Management Conference* (Jan. 2011). https://doi.org/10.4225/75/57b52975cd8b4

[4] Ashish Arora, Chris Forman, Anand Nandkumar, and Rahul Telang. 2010. Competition and patching of security vulnerabilities: An empirical analysis. *Information Economics and Policy* 22, 2 (May 2010), 164–177. https://ideas.repec.org/a/eee/iepoli/v22y2010i2p164-177.html

[5] Rowland Atkinson and John Flint. 2001. Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social research update* 33, 1 (2001), 1–4. Publisher: Guildord.

[6] Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright, and Adam Shostack. 2002. Timing the Application of Security Patches for Optimal Uptime. *Proceedings of LISA'02: Sixteenth Systems Administration Conference*, 233–242.

[7] Peter Birmingham and David Wilkinson. 2003. *Using research instruments: A guide for researchers*. Routledge.

[8] B. Bloor. 2003. The patch problem: It's costing your business real dollars. *Baroudi Bloor* (2003). https://www.netsense.info/downloads/PatchProblemReport_BaroudiBloor.pdf

[9] John M. Blythe and Lynne Coventry. 2018. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior* 87 (Oct. 2018), 87–97. https://doi.org/10.1016/j.chb.2018.05.023

[10] John M. Blythe, Lynne Coventry, and Linda Little. 2015. Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 103–122.

[11] Brennen Bouwmeester, Elsa Rodríguez, Carlos Gañán, Michel van Eeten, and Simon Parkin. 2021. "The Thing Doesn't Have a Name": Learning from Emergent {Real-World} Interventions in Smart Home Security. 493–512. https://www.usenix.org/conference/soups2021/presentation/bouwmeester

[12] Matt Burgess. 2018. The IoT's security nightmare will never end. You can now search insecure cameras by address. *Wired UK* (Nov. 2018). https://www.wired.co.uk/article/internet-of-things-security-camera-search-location

[13] Charles F. Cannell, Peter V. Miller, and Lois Oksenberg. 1981. Research on interviewing techniques. *Sociological methodology* 12 (1981), 389–437.

[14] George Chalhoub and Ivan Flechais. 2022. Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 436 (nov 2022), 36 pages. https://doi.org/10.1145/3555537

[15] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 185–204. https://www.usenix.org/conference/soups2020/presentation/chalhoub

[16] George Chalhoub and Advait Sarkar. 2022. "It's Freedom to Put Things Where My Mind Wants": Understanding and Improving the User Experience of Structuring Data in Spreadsheets. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 585, 24 pages. https://doi.org/10.1145/3491102.3501833

[17] Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2007. Even experts deserve usable security: Design guidelines for security management systems. In *SOUPS Workshop on Usable IT Security Management (USM)*. 1–4.

[18] Jacob Cohen. 1960. A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement* 20, 1 (April 1960), 37–46. https://doi.org/10.1177/001316446002000104 Publisher: SAGE Publications Inc.

[19] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.

[20] Olivier Crameri, Nikola Knezevic, Dejan Kostic, Ricardo Bianchini, and Willy Zwaenepoel. 2007. Staged deployment in mirage, an integrated software upgrade testing and distribution system. *ACM SIGOPS Operating Systems Review* 41, 6 (Oct. 2007), 221–236. https://doi.org/10.1145/1323293.1294283

[21] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. 2013. Computer security and the modern home. *Commun. ACM* 56, 1 (Jan. 2013), 94–103. https://doi.org/10.1145/2398356.2398377

[22] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R. Smith, and Tadayoshi Kohno. 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing (UbiComp '09)*. Association for Computing Machinery, New York, NY, USA, 105–114. https://doi.org/10.1145/1620545.1620564

[23] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating System Operators' Perspective on Security Misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1272–1289. https://doi.org/10.1145/3243734.3243794

[24] Colin Dixon, Ratul Mahajan, Sharad Agarwal, A. J. Brush, Bongshin Lee, Stefan Saroiu, and Paramvir Bahl. 2012. An operating system for the home. In *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (NSDI'12)*. USENIX Association, USA, 25.

[25] M. Donner. 2003. Patch management-bits, bad guys, and bucks. *Secure Business Quarterly* 3, 2 (2003), 1–4.

[26] Edward G. 2022. Record-breaking number of router security flaws discovered in the last few years. https://atlasvpn.com/blog/record-breaking-number-of-router-security-flaws-discovered-in-the-last-few-years

[27] Anirudh Ekambaranathan, Jun Zhao, and George Chalhoub. 2023. Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 7, 2, Article 53 (jun 2023), 24 pages. https://doi.org/10.1145/3596267

[28] Gerhard Eschelbeck. 2005. The Laws of Vulnerabilities: Which security vulnerabilities really matter? *Information Security Technical Report* 10, 4 (2005), 213–219. Publisher: Elsevier.

[29] Jean Faugier and Mary Sargeant. 1997. Sampling hard to reach populations. *Journal of Advanced Nursing* 26, 4 (1997), 790–797. https://doi.org/10.1046/j.1365-2648.1997.00371.x

[30] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security Analysis of Emerging Smart Home Applications. In *2016 IEEE Symposium on Security and Privacy (SP)*. 636–654. https://doi.org/10.1109/SP.2016.44 ISSN: 2375-1207.

[31] Nigel G. Fielding. 2006. *The SAGE Dictionary of Social Research Methods*. SAGE Publications, Ltd. https://doi.org/10.4135/9780857020116

[32] Jose Fonseca and Marco Vieira. 2008. Mapping software faults with web security vulnerabilities. In *2008 IEEE international conference on dependable systems and networks With FTCS and DCC (DSN)*. IEEE, 257–266.

[33] Leo A. Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.

[34] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field methods* 18, 1 (2006), 59–82.

[35] Morey J. Haber and Brad Hibbert. 2018. *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations*. Apress. Google-Books-ID: vSpgDwAAQBAJ.

[36] Nikolai Hampton and Patryk Szewczyk. 2015. A survey and method for analysing SoHo router firmware currency. *Australian Information Security Management Conference* (Jan. 2015). https://doi.org/10.4225/75/57b697e7d9388

[37] David Heldenbrand and Christopher Carey. 2007. The Linux router: an inexpensive alternative to commercial routers in the lab. *Journal of Computing Sciences in Colleges* 23, 1 (Oct. 2007), 127–133.

[38] Hollie Hennessy. 2021. Millions of people in the UK at risk of using insecure routers - Which? News. https://www.which.co.uk/news/article/millions-of-people-in-the-uk-at-risk-of-using-unsecure-routers-afweT5A8CGNf

[39] Zhen Huang, David Lie, Gang Tan, and Trent Jaeger. 2019. Using safety properties to generate vulnerability patches. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 539–554.

[40] John Ioannidis and Steven Michael Bellovin. 2002. Implementing Pushback: Router-Based Defense Against DDoS Attacks. (2002). https://doi.org/10.7916/D8R78MXV

[41] Jane Wakefield. 2021. Six million Sky routers had serious security flaw. *BBC News* (Nov. 2021). https://www.bbc.com/news/technology-59332840

[42] Jose Nazario. 2027. The problem with patching in addressing IoT vulnerabilities. https://www.fastly.com/blog/problem-patching-addressing-iot-vulnerabilities

[43] Annabel Bhamani Kajornboon. 2005. Using interviews as research instruments. *E-journal for Research Teachers* 2, 1 (2005), 1–9.

[44] Eser Kandogan, Paul Maglio, and Eben Haber. 2012. *Taming Information Technology: Lessons from Studies of System Administrators*. OUP USA. Google-Books-ID: cJ36Q5HDPaYC.

[45] Emmanouil Karamanos. 2010. *Investigation of home router security*. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91107

[46] Kaspersky. 2022. 87 critical vulnerabilities discovered in routers in 2021. https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021 Section: Resource Center.

[47] Alex J. Kibe. 2018. *An Experiment to Determine the Effect of Ethical Hacking on It Administrator's Patch and Vulnerability Management Attitudes, a Case of a Leading Telecommunications Company*. Thesis. university of nairobi. http://erepository.uonbi.ac.ke/handle/11295/104505 Accepted: 2019-01-09T05:35:17Z.

[48] Mike Knight. 2019. Old Routers Are Targets For Hackers. https://reformit.co.uk/old-routers-are-targets-for-hackers/

[49] Benjamin Koskei and Catherine Simiyu. 2015. Role of interviews, observation, pitfalls and ethical issues in qualitative research methods. *Journal of Educational Policy and Entrepreneurial Research* 2, 3 (2015), 108–117.

[50] Sara Kraemer and Pascale Carayon. 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics* 38, 2 (March 2007), 143–154. https://doi.org/10.1016/j.apergo.2006.03.010

[51] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. 2017. "I Have No Idea What i'm Doing": On the Usability of Deploying HTTPS. In *Proceedings of the 26th USENIX Conference on Security Symposium* (Vancouver, BC, Canada) *(SEC'17)*. USENIX Association, USA, 1339–1356.

[52] Lorenz Kustosch, Carlos Gañán, Mattis van't Schip, Michel van Eeten, and Simon Parkin. [n. d.]. Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible. ([n. d.]).

[53] Gurjan Lally and Daniele Sgandurra. 2018. Towards a Framework for Testing the Security of IoT Devices Consistently. In *Emerging Technologies for Authorization and Authentication (Lecture Notes in Computer Science)*, Andrea Saracino and Paolo Mori (Eds.). Springer International Publishing, Cham, 88–102. https://doi.org/10.1007/978-3-030-04372-8_8

[54] Frank Li and Vern Paxson. 2017. A large-scale empirical study of security patches. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2201–2215.

[55] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. 2019. Keepers of the machines: Examining how system administrators manage software updates for multiple machines. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 273–288.

[56] Richard Lippmann, Seth Webster, and Douglas Stetson. 2002. The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 307–326.

[57] MARIA NAMESTNIKOVA. 2022. Router security report 2021. https://securelist.com/router-security-2021/106711/

[58] Lynda McGhie. 2003. Software patch management-the new frontier. *Secure Business Quarterly* 3, 2 (2003), 1–4.

[59] Huoy Min Khoo and Daniel Robey. 2007. Deciding to upgrade packaged software: a comparative case study of motives, contingencies and dependencies. *European Journal of Information Systems* 16, 5 (Oct. 2007), 555–567. https://doi.org/10.1057/palgrave.ejis.3000704

[60] Dongliang Mu, Alejandro Cuevas, Limin Yang, Hang Hu, Xinyu Xing, Bing Mao, and Gang Wang. 2018. Understanding the reproducibility of crowd-reported security vulnerabilities. In *27th USENIX Security Symposium (USENIX Security 18)*. 919–936.

[61] Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, and Tudor Dumitras. 2015. The attack of the clones: A study of the impact of shared code on vulnerability patching. In *2015 IEEE symposium on security and privacy*. IEEE, 692–708.

[62] Condé Nast. 2023. Your old router is an absolute goldmine for troublesome hackers. *Wired UK* (Jan. 2023). https://www.wired.co.uk/article/router-wifi-security-settings

[63] Nathaniel Mott. 2021. Virgin Media Routers Left VPN Users Vulnerable Since at Least 2019. https://uk.pcmag.com/security/135764/virgin-media-routers-left-vpn-users-vulnerable-since-at-least-2019

[64] South Florida Caribbean News. 2022. Why You Should Replace Your ISP's Router With A Store-Bought One? https://sflcn.com/why-you-should-replace-your-isp-router-with-a-store-bought-one/

[65] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley. 2012. GPS software attacks. In *Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12)*. Association for Computing Machinery, New York, NY, USA, 450–461. https://doi.org/10.1145/2382196.2382245

[66] Adar Ovadya, Rom Ogen, Yakov Mallah, Niv Gilboa, and Yossi Oren. 2019. Cross-Router Covert Channels.. In *WOOT@ USENIX Security Symposium*. https://www.usenix.org/system/files/woot19-paper_ovadia.pdf

[67] Brigid O'Gorman, Candid Wueest, Dick O'Brien, Gillian Cleary, Hon Lau, John-Paul Power, Mayee Corpin, Orla Cox, Paul Wood, and Scott Wallace. 2019. ISTR Internet Security Threat Report. *A Report published by SYMANTEC* 24 (Feb. 2019), 32. https://docs.broadcom.com/doc/istr-24-2019-en

[68] U. K. Parliament. 2022. Product Security and Telecommunications Infrastructure (PSTI) Bill. (2022). https://bills.parliament.uk/bills/3069

[69] Luana Pascu. 2019. The IoT threat landscape and top smart home vulnerabilities in 2018. *Bitdefender* (2019). https://www.bitdefender.com/files/News/CaseStudies/study/229/Bitdefender-Whitepaper-The-IoT-Threat-Landscape-and-Top-Smart-Home-Vulnerabilities-in-2018.pdf

[70] Peter Weidenbach and Johannes vom Dorp. 2020. Home Router Security Report 2020. *Fraunhofer Gesellschaft* (June 2020). https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

[71] Valentina Piantadosi, Simone Scalabrino, and Rocco Oliveto. 2019. Fixing of security vulnerabilities in open source projects: A case study of apache http server and apache tomcat. In *2019 12th IEEE Conference on software testing, validation and verification (ICST)*. IEEE, 68–78.

[72] Sam Ransbotham, Sabyaschi Mitra, and Jon Ramsey. 2012. Are markets for vulnerabilities effective? *Mis Quarterly* (2012), 43–64. Publisher: JSTOR.

[73] Broadband DSL Routers. 2014. Routers. *Westermo* (2014). https://rittbul.bg/resources/westermo_pb_100-3870_product_guide-4-24-27.pdf

[74] Georgia Robins Sadler, Hau-Chen Lee, Rod Seung-Hwan Lim, and Judith Fullerton. 2010. Research Article: Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & Health Sciences* 12, 3 (2010), 369–374. https://doi.org/10.1111/j.1442-2018.2010.00541.x

[75] Sam Bocetta. 2021. Hackers Targeting Router Devices: Is Your Household Vulnerable? https://www.networkcomputing.com/network-security/hackers-targeting-router-devices-your-household-vulnerable

[76] Christian Scully and Ping Wang. 2018. Router Security Penetration Testing in a Virtual Environment. In *Information Technology - New Generations (Advances in Intelligent Systems and Computing)*, Shahram Latifi (Ed.). Springer International Publishing, Cham, 119–124. https://doi.org/10.1007/978-3-319-54978-1_16

[77] Clive Seale. 1999. Quality in qualitative research. *Qualitative inquiry* 5, 4 (1999), 465–478.

[78] Youkun Shi, Yuan Zhang, Tianhan Luo, Xiangyu Mao, Yinzhi Cao, Ziwen Wang, Yudi Zhao, Zongan Huang, and Min Yang. 2022. Backporting Security Patches of Web Applications: A Prototype Design and Implementation on Injection Vulnerability Patches. In *31th USENIX Security Symposium (USENIX Security)*.

[79] Silviu Stahie. 2021. Virtual Patching Home Routers Before before Manufacturers Is the Way Forward. https://www.bitdefender.co.uk/blog/hotforsecurity/virtual-patching-home-routers-before-before-manufacturers-is-the-way-forward/

[80] Anna Kornfeld Simpson, Franziska Roesner, and Tadayoshi Kohno. 2017. Securing vulnerable home IoT devices with an in-hub security manager. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 551–556. https://doi.org/10.1109/PERCOMW.2017.7917622

[81] Nissy Sombatruang, Tristan Caulfield, Ingolf Becker, Akira Fujita, Takahiro Kasama, Koji Nakao, and Daisuke Inoue. 2023. Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT. In *USENIX Security Symposium. USENIX Association*.

[82] Anselm Strauss and Juliet Corbin. 1998. *Basics of qualitative research techniques*. Sage publications Thousand Oaks, CA.

[83] Anselm Strauss and Juliet M. Corbin. 1997. *Grounded theory in practice*. Sage.

[84] Suzanne Kernes Dawe. 2022. Lumen discovers new malware that targeted home-office routers for two years. http://news.lumen.com/2022-06-28-Lumen-discovers-new-malware-that-targeted-home-office-routers-for-two-years

[85] Patryk Szewczyk and Rose Macdonald. 2017. Broadband router security: History, challenges and future implications. *Research outputs 2014 to 2021* (Jan. 2017). https://doi.org/10.15394/jdfsl.2017.1444

[86] Xin Tan, Yuan Zhang, Chenyuan Mi, Jiajun Cao, Kun Sun, Yifan Lin, and Min Yang. 2021. Locating the Security Patches for Disclosed OSS Vulnerabilities with Vulnerability-Commit Correlation Ranking. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 3282–3299.

[87] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel Von Zezschwitz. 2020. Security, availability, and multiple information sources: Exploring update behavior of system administrators. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 239–258.

[88] Trend Micro. 2018. A Look Into the Most Noteworthy Home Network Security Threats of 2017. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-look-into-the-most-noteworthy-home-network-security-threats-of-2017

[89] Nicole F. Velasquez and Suzanne P. Weisband. 2008. Work practices of system administrators: implications for tool design. In *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology (CHiMiT '08)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/1477973.1477975

[90] Nicole F. Velasquez and Suzanne P. Weisband. 2009. System administrators as broker technicians. In *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology (CHiMiT '09)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/1641587.1641588

[91] Francesco Vitale, Joanna McGrenere, Aurélien Tabard, Michel Beaudouin-Lafon, and Wendy E. Mackay. 2017. High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 4242–4253. https://doi.org/10.1145/3025453.3025509

[92] Helen J. Wang, Chuanxiong Guo, Daniel R. Simon, and Alf Zugenmaier. 2004. Shield: vulnerability-driven network filters for preventing known vulnerability exploits. *ACM SIGCOMM Computer Communication Review* 34, 4 (Aug. 2004), 193–204. https://doi.org/10.1145/1030194.1015489

[93] Zhiqiang Wang, Yuqing Zhang, and Qixu Liu. 2012. A research on vulnerability discovering for router protocols based on fuzzing. In *7th International Conference on Communications and Networking in China*. 245–250. https://doi.org/10.1109/ChinaCom.2012.6417484

[94] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/2834050.2834095

A Relevant Tables

	Gender (Age)	Degree	Experience	Employment	Countries Served
P01	Male (40)	M.Sc.	8 years	Security Manager	UK
P02	Female (32)	B.Sc.	5 years	Security Consultant	UK
P03	Male (34)	M.Sc.	6 years	Security Engineer	UK
P04	Male (33)	Ph.D	4 years	Privacy Engineer	UK
P05	Male (43)	Ph.D	8 years	Senior Consultant	UK
P06	Male (29)	B.Eng.	4 years	IT Security Engineer	UK
P07	Female (37)	B.Sc.	7 years	Senior Security Officer	UK
P08	Male (44)	M.Sc.	10 years+	CTO	UK
P09	Female (35)	B.Sc.	5 years	Security Officer	UK
P10	Male (50)	B.Sc.	10 years+	CISO	UK
P11	Male (46)	B.Sc.	9 years	Deputy CISO	UK
P12	Male (42)	M.Sc.	10 years+	CISO Advisor	UK, US
P13	Male (30)	M.Sc.	4 years	Security Officer	UK
P14	Male (31)	B.Eng.	5 years	Network Engineer	UK
P15	Male (52)	B.Sc.	10 years+	CEO	UK, EU
P16	Male (48)	B.A.	10 years+	CISO	UK, EU
P17	Male (35)	B.Eng.	6 years	Hardware Engineer	UK
P18	Male (39)	B.Eng.	7 years	Network Engineer	UK
P19	Female (34)	B.Sc.	4 years	Security Engineer	UK
P20	Male (52)	B.Bus.	9 years	CTO	UK
P21	Female (41)	Ph.D	9 years	Senior Consultant	UK, Germany
P22	Male (39)	B.Sc.	7 years	Engineering Manager	UK
P23	Female (35)	B.Eng.	5 years	Security Manager	UK
P24	Male (32)	B.Eng.	4 years	Network Engineer	UK
P25	Male (38)	B.Sc.	7 years	Network Administrator	UK
P26	Male (46)	B.Bus.	10 years+	CISO	UK, EU, US
P27	Female (41)	M.Sc.	7 years	Business Manager	UK
P28	Male (37)	B.Sc.	5 years	Security Architect	UK
P29	Male (43)	M.Sc.	6 years	IoT Consultant	UK
P30	Male (39)	B.Sc.	7 years	Security Lead	UK

Table 1. Semi-structured interview participant demographics.

Contextual Details	Participant Count
User Harm	13
Confidential Data	8
Internet Environment	7
Business Value	5
Potential disruption	3

Table 2. Contextual factors used for vulnerability risk.

Metric	Participant Count
Actively Exploited in the Wild	15
Number of Affected Routers	13
Targeted by Threat Actor Groups	12
Remotely Exploitable	10
Potential High Lateral Movement	4

Table 3. Metrics Used to Assess Vulnerability Severity.

Contextual Details	Participant Count
Language and Cultural Differences	14
Time Zone Differences	10
Sending The Wrong Information	8
Need for Confidentiality	6
Misidentifying Stakeholders	5

Table 4. Communication Barriers to Outsourcing.

B Online Screening Questionnaire

(1) Select your gender:
- ◯ Male
- ◯ Female
- ◯ Other
- ◯ Prefer not to answer

(2) How old are you?
- ◯ ___
- ◯ Prefer not to answer

(3) What best describes your job at the company?
- ◯ Chief Analytics Officer (CAO)
- ◯ Chief Compliance Officer (CCO)
- ◯ Chief Data Officer (CDO)
- ◯ Chief Executive Officer (CEO)
- ◯ Chief Green Officer (CGO)
- ◯ Chief Human Resources Manager (CHRM)
- ◯ Chief Information Security Officer (CISO)
- ◯ Chief Information Security Officer Advisor (CISO Advisor)
- ◯ Chief Marketing Officer (CMO)
- ◯ Chief Security Officer (CSO)
- ◯ Chief Technology Officer (CTO)
- ◯ Hardware Engineer
- ◯ IT Security Engineer
- ◯ IoT Consultant
- ◯ Network Administrator

- ◯ Network Engineer
- ◯ Network Engineer
- ◯ Penetration Tester
- ◯ Privacy Engineer
- ◯ Security Architect
- ◯ Security Consultant
- ◯ Security Engineer
- ◯ Security Manager
- ◯ Security Officer
- ◯ Senior Consultant
- ◯ Senior Security Officer
- ◯ Other:

(4) How long have you been working at your company?

- ◯ 1 year or less
- ◯ 2 years
- ◯ 3 years
- ◯ 4 years
- ◯ 5 years
- ◯ 6 years
- ◯ 7 years
- ◯ 8 years
- ◯ 9 years
- ◯ More than 10 years

(5) What best describes your company?

- ◯ Consultant Company
- ◯ Product Company
- ◯ Service Company
- ◯ Platform Company
- ◯ Other:

(6) Select the types of routers that your company sells or produces:

- ☐ Home routers (a.k.a “consumer-grade routers”)
- ☐ Enterprise-grade routers (aka “business routers”)
- ☐ Broadband routers (a.k.a “ISP-provided routers”)
- ☐ Other:

(7) How many employees does your company or its subsidiary have in the UK?

- ◯ less than 25
- ◯ 26-50
- ◯ 51-100
- ◯ 101-250
- ◯ 251-500
- ◯ 501-1000

◯ More than 1000

C Pilot Interview Questions

(1) What company do you work for? What does the company do? What is your role in the company?
(2) Can you describe your responsibilities, in particular, in the development or security of routers?
(3) How do you discover or identify vulnerabilities in router products you are responsible for? How do you prioritize dealing with vulnerabilities?
(4) What are the typical challenges that you face when addressing security vulnerabilities in routers? Are there any challenges specific to routers that make them difficult to deal with?
(5) Is there anything that we could do to improve vulnerability discovery and remediation in routers? If so, please elaborate.

D Interview Guide

We describe below the script used for our semi-structured interviews. Some questions were asked in all interviews, whereas the remaining questions were chosen based on the current job title of the participant. We allowed participants to elaborate, share their thoughts, and ask any clarification questions.

D.1 Characterizations

(1) Would you tell us a bit about yourself?
(2) What is your role in the company that you work at?
  (a) When did you join the company?
  (b) What are your responsibilities?
  (c) What is your specific role in the development or the security of routers?
(3) What kind of router products do you develop?
  (a) Are there a specific router product that you focus on developing?
  (b) Can you describe your user base, clients, or customers?
  (c) How would you describe the typical customers that use your router products?

D.2 Securing Routers from Vulnerabilities

(1) Do your routers get compromised? Why/Why not? Are you aware of any attack vectors?
(2) What are the main causes of security vulnerabilities in your router products?
(3) Do you ensure that your routers are secure? If so, how? Is there a process? What does it look like?
(4) Do you conduct any tests to ensure that your routers are secure from vulnerabilities? If so, can you give more details?
(5) Do you use any tools to protect your routers from vulnerabilities?
(6) Do you ensure that your router products are free of security vulnerabilities? If so, how?
(7) Is security taken into consideration during the development of router products? If so, how?
(8) Are security requirements identified during the development of router products? If so, can you provide more details?
(9) Is anyone responsible for router security vulnerabilities or breaches? If yes, can you provide more details?

D.3 Discovering Vulnerabilities

(1) Do you have a process of discovering or identifying security vulnerabilities in your router products? If so, can you describe how the process looks like?
(2) Do you often search for vulnerabilities? Do you use any security scanners? Do you receive reports from users or third parties?
(3) Do you have a bug bounty rewards system for security vulnerabilities? Do you receive security reports from users?
(4) Do you test your routers for security vulnerabilities? If so, how and how often? Who is responsible for that?
(5) Do you deal with vulnerabilities? If so, can you describe the type and scale of vulnerabilities that you usually deal with?
(6) Do you evaluate or assess whether security vulnerabilities in routers are valid? If so, how?
(7) Do you evaluate or determine the severity of router vulnerabilities? If so, how?
(8) Do you stay up to date with the latest discovered vulnerabilities and attacks in routers? If so, how?

D.4 Remediating Vulnerabilities

(1) Do you usually address, remediate and solve router vulnerabilities that you are aware of? If so, how?
(2) Is anyone responsible for remediating vulnerabilities once they are discovered? Can you provide more details?
(3) Do you discuss the impact and severity of vulnerabilities with anyone? Does your discussions impact improving router security practices? Why/Why not?
(4) Do you prioritize router vulnerabilities that you deal with in your job? If so, how? How do you determine whether a vulnerability is worth looking into?
(5) Do discovered zero-day security vulnerabilities get more attention than other vulnerabilities? Why/Why not?
(6) Does every router vulnerability get the same attention? Why/Why not?
(7) Are there any vulnerabilities that you decide to ignore or dismiss? Why/Why not?
(8) How long on average do security vulnerabilities remain before receiving a patch?
(9) When do you consider a router vulnerability to be addressed or resolved?

D.5 Supporting Users

(1) Do you help or support users with infected routers? If so, how?
(2) Do you notify or inform customers when vulnerabilities are discovered in their routers? If so, how?
    (a) Do you publicize the information on your website(s)? If so, can you give more details?
    (b) Do you individually email users? If so, can you give more details?
(3) Do you offer any technical support or assistance to users with infected routers? If so, how does it look like?
(4) Do you help users with vulnerable routers that can't be patched or fixed (Why/Not)? If so, how do you help them?

D.6 Improving General Practices

(1) What are the biggest challenges or limitations you experience when you deal with router vulnerabilities? How do we think we can improve these challenges?
(2) What can we do to improve router vulnerability management practices?

(3) What different approaches (e.g., hardware security, software engineering, testing regimes) would you be open to address router vulnerability challenges?
(4) Do you use any third-party vulnerability management tools? Why/Why not?
(5) Do you wish there were any tools that would help you address security vulnerabilities in routers?

D.7 Concluding Remarks

(1) Do you think there is anything in the development of routers that can make it easier to mitigate or avoid router vulnerabilities?
(2) We have reached the end of the interview. Thank you for talking to us!
   (a) Do you have any questions?
   (b) Do you have any comments you want to add?

E Recruitment Material

A recruitment campaign has been featured on the IoT Security Foundation's website. A snapshot of this campaign can be accessed on the Internet Archive website.[6].

Understanding Gateway and Router Vulnerabilities

Routers, Vulnerabilities and Attacks

In recent years we've paid special attention to cyber-attacks which can be initiated remotely – from anywhere across the globe. This is because they can scale very easily and have impacts on specific targets, but can also wreak havoc with collateral damage on unintended victims. Of all the devices that are attached to a network – especially the Internet – routers and gateways are juicy targets for any threat actor.

Last year (June 8, 2022), Kaspersky reported 506 vulnerabilities had been discovered in routers – including 87 considered **critical** and incredibly *'most remain unpatched'*.

This clearly threatens the security of countless devices that are connected daily in offices, homes and in public places.

We're working on this through the activities of the ManySecured collaborative initiative and we'd like to know more about the problems that need addressing in this space.

Research

We are working with the University of Oxford, Department of Computer Science on a research study exploring this subject and we're looking for input from a range of stakeholders including consultants, router developers, engineers, managers etc., anybody who has a view. We are especially interested to talk to professionals who work in companies (of any size) that develop, manufacture, or sell router software/hardware.

One specific aim is to better understand the **challenges faced in vulnerability management** so we may further develop effective strategies and solutions to address these challenges e.g., through recommendations, best practices, tools and hardware security for memory safety.

The research is conducted via a simple interview process that should only last for approximately 30-45 minutes, conducted remotely at a date and time convenient to the participant. Oh, and all research data will be kept anonymous of course.

Can you or someone you know help us?

If you are interested to participate in the study or can suggest someone who would be glad to speak to us, please reach out and get in touch – we'll get you hooked up with our post-doc researcher *'George'*.

[6]http://web.archive.org/web/20230729122805/https://iotsecurityfoundation.org/understanding-gateway-and-router-vulnerabilities/

F CodeBook

Vulnerability Management	Obstacles	Workarounds	User Pushback
affected routers	automation challenges	ad hoc patching	annoyance when changing passwords
automatic upgrades	difficulty tracking	advertising fixes	cannot locate devices
business value	lack of visibility	discounted replacements	complaining about security measures
company assets	lacking necessary security	educating users	complaints about the complexity
company relationships	poor patch management	encouraging upgrades	complaints about the lack of transparency
confidential information	automatic hardware	forcing updates	concerned about internet access
critical vulnerability	cheaper production	free replacements	concerns about security
data model	chips manufacturers	informing users	concerns about slowing down internet
data theft	communication barriers	installing updates	cost of purchasing a new router
deriving heuristics	compatibility issues	listing legacy products	cost of updating existing router
deriving metrics	compromised routers	mitigation advice	cost prohibitive
downtime challenges	critical updates	monitor unpatched systems	difficulty of understanding the settings
financial value	cultural differences	network segmentation	disabled users
firewall	detecting infected routers	recalling hardware	disbelief in security measures
high vulnerability	development teams	removal of equipment	distrust on-screen reminders
inferring context	end-of-life (eol)routers	restricting features	does not see problems with unpatched routers
internet environment	explaining to finance teams	security advisoring	doubts about the integrity of patches
low vulnerability	failing to engage stakeholders	sufficient logging	elderly users
malicious code	false positives	use patching templates	fear of change
malware	firmware shipping	whitelisting	fear of creating an inconvenience for others
management reports	firmware updates	blocking ports	fear of introducing vulnerabilities
manual upgrades	high patching cost	business continuity plans	fear of losing internet connection
medium vulnerability	incentivizing manufacturers	centralized patching repository	fear of not being able to talk to relatives
monitoring patches	insufficient testing	change management processes	fear of unfamiliar change
network environment	lack of clear agreements	changing default credentials	frustration over security tasks
patch adoption	lack of resources	contacting customers	lack of control over router
performance problems	language differences	defense-in-depth approach	lack of digital literacy
potential disruption	legacy routers	disable unneeded configuration	lack of oversight over router
proof-of-concept exploits	limited autonomy	disable unneeded configurations	lack of proper contact channels
publicly available	limited control	hiring more engineers	lack of technical knowledge
real-world assets	manufacturers	incidental patching	lack of understanding of routers
remotely exploitable	miscommunicating progress	informal patching	low levels of confidence
router compromised	misidentifying stakeholders	install one-time only	misunderstanding settings
security tools	need for confidentiality	logical separation	not familiar with technology
threat actors	need for user input	manual patches	not following instructions
user environment	network complexity	notification alerts	not perceived as necessary
vulnerability assessment	not accessing customer traffic	offload patching to third-parties	not trusting manufacturer
vulnerability detection tools	obsolete routers	patching exceptions	physical limitations
vulnerability discovery	offshore companies	patching services from third parties	poor communication
vulnerability endpoint	old hardware	patching shortcuts	refusal to follow security protocols
vulnerability exploited	outsourcing firmware	patching-as-a-service	refusal to install security updates
vulnerability monitoring	quality assurance	practice incident response	resistance to providing information
vulnerability patching	sending wrong information	pre-defined patch cycles	too much effort
vulnerability prioritization	supported routers	pre-defined patch cycles	unable to install upgrades
vulnerability remediation	supporting eol briefly	quick patches	unable to remember credentials
vulnerability risk	system integrators	removing unsupported devices	unaware of patches
vulnerability risk factors	time-zone differences	replacing broadband router	unconcerned about security
vulnerability scanners	timely implementation	review hardware patching	unfamiliar with patches
vulnerability severity	unclear agreement	risk mitigation	unsure updates are safe
vulnerability severity scores	unclear translation	selecting patches	unused hardware
vulnerability widely exploited	unnecessary patching	temporary patches	unused web portal
zero-day vulnerability	unreachable teams	triage and action problems	inconvenience of security measures

Table 5. Codebook (Grounded Theory).