**Breaking Down ISP Routers: Security & Privacy Insights**

Corey Mekelburg, Ryan King, Alexandria Simonson and Sreean Rikkala

November 14, 2025

**Introduction**

ISP routers are the most common routers used in modern households and small businesses nowadays. While these devices enhance connectivity and provide convenience, they also introduce significant security and privacy challenges for the end user. Many consumer networking devices like routers rely on users to manually configure their security settings, leaving networks exposed to different cyber threats due to misconfigurations and lack of technical knowledge, weak authentication mechanisms, and outdated firmware. Research from (Allifah, 2020) suggests that the lack of standardized security enforcement has led to widespread vulnerabilities, making it easier for attackers to exploit these devices. Since most consumers lack technical expertise, they often fail to apply proper security configurations, leaving their networks susceptible to data breaches and unauthorized access. By combining automation with informed decision-making like understanding what security features to look for, and how to choose the best router for their needs, users can better protect their networks against evolving cyber threats.

**Problem Statement**

Research from (Allifah, 2020) identifies several critical security challenges in routers. A primary concern is the over-reliance on user expertise for security configuration. demonstrate that current routers provide insufficient security guidance, making informed configuration choices difficult for average users. This finding is reinforced by (Haney, 2022) empirical study of 40 smart home users, which revealed that despite acknowledging security risks, users implement only basic security measures due to limited technical knowledge and also user reluctance.

Technical vulnerabilities compound these user-related challenges. From the research from (Jain, 2023) discovered that many ISP-provided routers contain unpatched security flaws, leaving entire networks vulnerable. The problem extends to data governance, as many devices collect extensive user data without transparent policies or automated privacy protections. (Sajjad, 2020) identified that even the Manufacturer Usage Description framework fails to address firmware vulnerabilities during initial setup, leaving devices exposed to various attacks from the moment of deployment.

**Evidence**

Empirical studies provide compelling evidence for the need for user guidance and acknowledgment of the real threat. (Haney, 2022) research revealed widespread implementation of inadequate security measures, primarily due to complex configuration interfaces, limited manufacturer guidance, inconsistent security standards across devices, and poor user understanding of security implications and has stated that cost is also one of the factors for security failure.

Technical analyses further support these findings. (Perera, 2021) demonstrated how default settings and manual security configurations in consumer routers create significant vulnerabilities, particularly during the initial setup phase. The threat landscape is especially concerning for IoT devices, as documented by (Sajjad, 2020), who found that traditional security frameworks fail to prevent automated attacks effectively. Research analyzing botnet variants discovered that routers with inadequate security controls enable attackers to launch large-scale attacks, while inconsistent security policies among device manufacturers exacerbate security risks.

**Solution**

Researchers have proposed various solutions focusing on automation and standardization. (Perera, 2021) NetBot solution demonstrates how automating initial configurations, vulnerability remediation, and compliance auditing can significantly reduce human error in router security. Key automation features include automated firmware updates, security configuration enforcement during onboarding, continuous vulnerability assessment, and default credential management.

Standardization efforts complement automation initiatives. (Jain, 2023) advocate for industry-wide standardization of security protocols, including mandatory automated firmware updates, standardized onboarding processes, transparent data governance policies, and automated security baseline enforcement. The enhanced MUD framework (eMUD) proposed by (Sajjad, 2020) demonstrates how automated security measures can be integrated into existing protocols, providing automated vulnerability assessments during setup, firmware verification before deployment, and standardized security policy enforcement.

**Conclusion**

This review demonstrates that ISP routers security requires a shift toward automated solutions and standardized practices. The evidence strongly supports the need for reducing user dependency on manual configuration while maintaining strong security postures. As the number of connected devices continues to grow, implementing automated security measures becomes increasingly critical for protecting consumer privacy and network integrity. Success will likely depend on automated security enforcement during device onboarding, standardized data governance practices, improved manufacturer transparency, and user-friendly GUI for necessary manual configurations.

**References**

Allifah, N. M., & Zualkernan, I. A. (2022). "Ranking Security of IoT-Based Smart Home Consumer Devices," IEEE Access, vol. 10, pp. 18352-18360. <https://doi.org/10.1109/ACCESS.2022.3148140>

Haney, J. M., Furman, S. M., & Acar, Y. (2022). "Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges," Proceedings of the International Symposium on Usable Security and Privacy (SOUPS). <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929479>

Perera, H. M. D. G. V., et al. (2021). "NetBot – An Automated Router Hardening Solution for Small to Medium Enterprises," IEEE IEMCON. <https://doi.org/10.1109/IEMCON53756.2021.9623186>

Sajjad, S. M., Yousaf, M., Afzal, H., & Mufti, M. R. (2020). "eMUD: Enhanced Manufacturer Usage Description for IoT Botnets Prevention on Home WiFi Routers," IEEE Access, 8, 164200-164220. <https://doi.org/10.1109/ACCESS.2020.3022272>

Jain, A., & Shete, P. (2023). "Accounting for the Unaccounted Vulnerabilities Found in Endpoint ISP SOHO Routers," IEEE International Carnahan Conference on Security Technology (ICCST). <https://doi.org/10.1109/ICCST59048.2023.10474274>

Feng, W., & Al-Muhtadi, J. (2002). "A General Security Infrastructure for Wireless Communication," Proceedings of the Joint International Conference on Wireless LANs and Home Networks (ICWLHN 2002) & Networking (ICN 2002). <https://www.researchgate.net/publication/269149051_A_GENERAL_SECURITY_INFRASTRUCTURE_FOR_WIRELESS_COMMUNICATION>