**Annotated Bibliography**

Allifah, N. M., & Zualkernan, I. A. (2022). Ranking Security of IoT-Based Smart Home

Consumer Devices. *IEEE Access, 10*, 18352-18360. <https://doi.org/10.1109/ACCESS.2022.3148140>

Allifah and Zualkernan (2022) propose a ranking methodology for evaluating the security risks of smart home consumer devices using a Analytic Hierarchy Process. Interesting insights on how IoT-based smart home devices like security cameras, smart speakers, and home automation systems pose security risks due to exposure to cloud-based services and mobile applications with known vulnerabilities. The authors speak that current consumer devices provide little information about their security levels, making it difficult for users to make informed choices. Their methodology systematically ranks devices based on network security, application security, and exploitable services, revealing that network security is the primary driver of smart home security. Consumers lack clear guidance on the security risks of IoT devices, making informed security decisions challenging.

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*](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929479)

Haney et al. (2022) examines that the privacy and security concerns of smart home users through in-depth interviews with 40 participants. The study finds that while many users acknowledge security risks, their mitigation efforts are simplistic and ineffective due to a lack of technical knowledge and limited configuration options provided by ISP manufacturers. Key concerns include unauthorized data collection, weak authentication mechanisms, and unpatched vulnerabilities. The authors argue that manufacturers should provide clearer security guidance and implement standardized security features such as default privacy settings, secure firmware updates, and user-friendly security tools. Many smart home users fail to implement effective security measures, either due to a lack of awareness or the complexity of available options.

Perera, H. M. D. G. V., Kasthuriarachchi, D. N. W., Samarasekara, K. M., Abeywardena, K. Y.,

Hewamanna, I. U. K., & Yapa, K. (2021). NetBot – An Automated Router Hardening Solution for Small to Medium Enterprises. *IEEE IEMCON.* <https://doi.org/10.1109/IEMCON53756.2021.9623186>

The study by the author highlights the vulnerabilities in consumer routers due to weak default settings, lack of firmware updates, and poor security policies. NetBot automates initial configurations, vulnerability remediation, compliance auditing, and rollback procedures, reducing the burden on IT administrators. The authors say that automating security settings can significantly improve network security and minimize human error in router configurations. SMEs often lack expertise in securing routers, leading to misconfigurations that create network vulnerabilities.

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>

The authors examine IoT botnet threats targeting home WiFi routers and propose eMUD, an enhanced version of the Manufacturer Usage Description protocol. The study identifies that the current MUD framework fails to address firmware vulnerabilities before deploying network policies, allowing IoT devices to be compromised even with security controls in place. eMUD improves IoT security by incorporating vulnerability assessments, firmware testing, and authentication mechanisms into the MUD framework. The authors also propose blockchain-based threat intelligence sharing to enhance collaborative defense mechanisms among IoT manufacturers. The existing MUD framework does not address firmware vulnerabilities before issuing security profiles, leaving IoT devices exposed to botnet attacks.

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>

Jain and Shete (2023) analyzes various security vulnerabilities in ISP-provided SOHO routers, revealing unpatched firmware issues, default credentials, and insecure network configurations. The study demonstrates how attackers can exploit these weaknesses to compromise entire subnets, making ISP networks highly vulnerable. The authors highlight the lack of vendor accountability in issuing security patches and providing transparency to users. The paper proposes industry-wide standardization for SOHO router security, mandatory firmware updates, and security transparency measures for ISPs. Many ISP-provided routers have unpatched security flaws, leaving entire networks vulnerable to attacks.

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*](https://www.researchgate.net/publication/269149051_A_GENERAL_SECURITY_INFRASTRUCTURE_FOR_WIRELESS_COMMUNICATION)

Feng and Al-Muhtadi (2002) discuss the security weaknesses in wireless communication networks, highlighting the risks of unauthorized access, user tracking, and data interception. The authors propose IRIS i.e., Inter-Realm Infrastructure for Security, a general-purpose security framework designed to enhance wireless communication security by integrating authentication, encryption, and secure routing mechanisms. The study emphasizes the need for dynamic security protocols to adapt to evolving cyber threats in mobile and wireless networks. Wireless communication suffers from security gaps due to its open nature and lack of dynamic, adaptable security measures.