UNIVERSIDAD SIMÓN BOLÍVAR
BARRANQUILLA Y CÚCUTA - COLOMBIA | VIGILADA MINEDUCACIÓN
ACREDITACIÓN INSTITUCIONAL EN ALTA CALIDAD
RENOVACIÓN - 8 AÑOS • 2021 - 2029
Resolución 015867 - MINEDUCACIÓN

Ciberseguridad: Tipos de ataques y vulnerabilidades en IoT para el hogar

Alejandro Mario Arteta Peñaloza
202011222524
Miguel Andrés Jiménez Molina
202011221334
Andrés David Varela López
202011223844
Diego Andrés Telles Bertel
202011423929

Trabajo de Investigación del Programa Ingeniería de Sistemas

Tutor(es):

Paul Adolfo Sanmartín Mendoza

RESUMEN

En la creciente era de la Internet de las Cosas (IoT), donde la interconexión de dispositivos redefine nuestros hogares como "inteligentes", este artículo aborda exhaustivamente las vulnerabilidades y riesgos de seguridad asociados con la proliferación de dispositivos IoT en el entorno doméstico.

El análisis se inicia con una exploración detallada de las tecnologías de conectividad, como Zigbee, Wi-Fi, Bluetooth y RFID, destacando sus debilidades particulares, desde problemas de autenticación hasta riesgos de suplantación de identidad. Se examinan métodos cruciales para mitigar estos riesgos y fortalecer las defensas cibernéticas.

Se presenta un enfoque específico en casos notorios, como el ataque de la botnet Mirai en 2016, subrayando las consecuencias catastróficas de dispositivos mal configurados y contraseñas débiles. Este análisis sirve como fundamento para entender los peligros inherentes a la falta de actualizaciones de seguridad y la vulnerabilidad de dispositivos físicos en lugares accesibles.

El artículo continúa explorando dispositivos comunes en hogares inteligentes, como asistentes virtuales, tomacorrientes y bombillas inteligentes, destacando sus beneficios y, al mismo tiempo, exponiendo vulnerabilidades potenciales, desde la falta de autenticación sólida hasta la ausencia de cifrado de datos adecuado.

La sección final se centra en los ataques dirigidos a hogares inteligentes, que van desde robos de datos hasta ataques de denegación de servicio. Se proporcionan estadísticas alarmantes sobre la vulnerabilidad generalizada de los hogares digitales, con un énfasis particular en las debilidades de routers y la necesidad urgente de contramedidas.

El resumen culmina resaltando las medidas cruciales que deben tomar los usuarios, fabricantes y proveedores para proteger los hogares inteligentes. Desde cambios en las configuraciones predeterminadas hasta actualizaciones periódicas y la segmentación de redes, se presenta un conjunto de estrategias para salvaguardar la seguridad cibernética en la era IoT. Este artículo busca no solo informar sobre los desafíos, sino también proporcionar un marco integral para abordarlos y garantizar la seguridad en la revolución de los hogares inteligentes.

Palabras clave: **Vulnerabilidades, Internet de las cosas, Ciberseguridad, Casas inteligentes.**

ABSTRACT

This article delves into the vulnerabilities and security risks associated with the widespread adoption of Internet of Things (IoT) devices in home environments. Beginning with a detailed exploration of connectivity technologies such as Zigbee, Wi-Fi, Bluetooth, and RFID, the analysis highlights their specific weaknesses, ranging from authentication issues to identity theft risks. Crucial methods for mitigating these risks and strengthening cybersecurity defenses are examined.

The article then focuses on notorious cases, such as the Mirai botnet attack in 2016, emphasizing the catastrophic consequences of poorly configured devices and weak passwords. This analysis serves as a foundation for understanding the dangers of lacking security updates and the vulnerability of physically accessible devices.

Common devices in smart homes, including virtual assistants, smart outlets, and bulbs, are explored, outlining their benefits while exposing potential vulnerabilities, such as weak authentication and inadequate data encryption.

The final section concentrates on attacks targeting smart homes, spanning data theft to denial-of-service attacks. Alarming statistics on the widespread vulnerability of digital homes are provided, with a particular emphasis on router weaknesses and the urgent need for countermeasures.

The summary concludes by highlighting crucial measures for users, manufacturers, and providers to protect smart homes. From changing default settings to regular updates and network segmentation, a comprehensive set of strategies is presented to safeguard cybersecurity in the IoT era. This article aims not only to inform about the challenges but also to provide a comprehensive framework for addressing them and ensuring security in the smart home revolution.

KeyWords: **Vulnerabilities, IoT, Cybersecurity, Smart home**

REFERENCIAS

[1] N. Latto, “Riesgos de seguridad en el Internet de las cosas (IoT),” Riesgos de seguridad en el Internet de las cosas (IoT), Nov. 13, 2019. Accessed: Aug. 04, 2023. Available: https://www.avast.com/es-es/c-what-is-the-internet-of-things#topic-1

[2]B. K. Sovacool and D. D. Furszyfer Del Rio, “Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies,” *Renewable and Sustainable Energy Reviews*, vol. 120, no. 109663, Dec. 2019, doi: https://doi.org/10.1016/j.rser.2019.109663.

[3] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.

[4] A. Tomar, “Introduction to Zibgbee Technology,” Element14, Jul. 2011. https://eclass.uoa.gr/modules/document/file.php/DI367/%CE%A5%CE%BB%CE%B9%CE%BA%CF%8C/introduction-to-zigbee-technology.pdf

[5] Cisco, “What Is Wi-Fi?,” Cisco. Accessed: Aug. 11, 2023. https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html

[6] R. Shorey and B. A. Miller, "The Bluetooth technology: merits and limitations," 2000 IEEE International Conference on Personal Wireless Communications. Conference Proceedings (Cat. No.00TH8488), Hyderabad, India, 2000, pp. 80-84, doi: 10.1109/ICPWC.2000.905777.

[7] R. Want, "An introduction to RFID technology," in IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, Jan.-March 2006, doi: 10.1109/MPRV.2006.2.

[8] J. I. Iturbe Araya and H. Rifà-Pous, “Anomaly-based cyberattacks detection for smart homes: A systematic literature review,” *Internet of Things*, vol. 22, no. 100792, Apr. 2023, doi: https://doi.org/10.1016/j.iot.2023.100792.

[9] B. Tushir, Y. Dalal, B. Dezfouli and Y. Liu, "A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6282-6292, 15 April15, 2021, doi: 10.1109/JIOT.2020.3026023.

[10] Kaspersky, “What is a Botnet?,” Kaspersky.com, 2019. https://usa.kaspersky.com/resource-center/threats/botnet-attacks

(accessed Oct. 06, 2023).

[11] Kaspersky, "Defending Yourself from a Man in the Middle Attack," *www.kaspersky.com*, Oct. 30, 2017. https://www.kaspersky.com/resource-center/threats/man-in-the-middle-attack

[12]CrowdStrike, "What is a Brute Force Attack? Definition & Examples | CrowdStrike," crowdstrike.com, Jun. 01, 2022. https://www.crowdstrike.com/cybersecurity-101/brute-force-attacks/

[13] Kaspersky, "What is Spoofing?," *www.kaspersky.com*, Jan. 13, 2021. https://www.kaspersky.com/resource-center/definitions/spoofing

[14] U. Saxena, J. Sodhi and Y. Singh, "An Analysis of DDoS Attacks in a Smart Home Networks," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 272-276, doi: 10.1109/Confluence47617.2020.9058087.

[15] Kaspersky, "What is Zero Day Exploit?," *www.kaspersky.com*, Feb. 27, 2018. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

[16] R. C, "What is a deauthentication attack? - Atlas VPN," atlasvpn.com, Nov. 30, 2022. https://atlasvpn.com/blog/what-is-a-deauthentication-attack

[17] G. Kibirige and C. Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network," 2015. Available: https://arxiv.org/ftp/arxiv/papers/1505/1505.01941.pdf

[18] CrowdStrike, "Keyloggers: How They Work and How to Detect Them | CrowdStrike," crowdstrike.com, Feb. 02, 2023. https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/ (accessed Oct. 06, 2023).

[19] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 105–117, May 2020, doi: https://doi.org/10.1016/j.eij.2020.05.003.

[20] B. Krebs, "Some Basic Rules for Securing Your IoT Stuff," Krebs on Security, Jan. 17, 2018. Accessed: Aug. 04, 2023. Available: https://krebsonsecurity.com/2018/01/some-basic-rules-for-securing-your-iot-stuff/

[21] "Cybersecurity White Paper: EO Response," 2022, Pp 11-14, doi: https://doi.org/10.6028/nist.cswp.02042022-2.

[22] C. Bravo, "Botnet Mirai: ¿nuestros electrodomésticos pueden atacarnos?," www.welivesecurity.com, Aug. 04, 2023. https://www.welivesecurity.com/es/seguridad-iot/botnet-mirai-electrodomesticos-pueden-atacarnos/ (accessed Sep. 29, 2023).

[23] V. Ruiz, "Los ataques de la botnet Mirai, fuerte lección para colocar a la seguridad como un tema prioritario," LinkedIn, Jul. 13, 2023. https://www.linkedin.com/pulse/los-ataques-de-la-botnet-mirai-fuerte-lecci%C3%B3n-para-colocar-ruiz/ (accessed Sep. 29, 2023).

[24] Interactivadigital, "Riesgos de los asistentes virtuales y cómo evitarlos, Opinión | Interactiva," *InteractivaDigital.com*, Dec. 24, 2019. https://interactivadigital.com/opinion-marketing-digital/riesgos-de-los-asistentes-de-voz-y-como-evitarlos/ (accessed Aug. 27, 2023).

[25] T. DIS, "Dolphin attacks, and what they mean for digital assistants," *Thales blog*, Jun. 12, 2018. https://dis-blog.thalesgroup.com/iot/2018/06/12/dolphin-attacks-and-what-they-mean-for-digital-assistants/ (accessed Aug. 27, 2023).

[26] N. Carlini and D. Wagner, "Audio Adversarial Examples: Targeted Attacks on Speech-to-Text," 2018. Available: https://nicholas.carlini.com/papers/2018_dls_audioadvex.pdf

[27] E. Press, "Los enchufes inteligentes ponen en peligro la información guardada en la red doméstica," *www.europapress.es*, Jan. 12, 2019. https://www.europapress.es/portaltic/ciberseguridad/noticia-enchufes-inteligentes-ponen-peligro-informacion-guardada-red-domestica-20190112112934.html (accessed Aug. 27, 2023).

[28] R. Mitchell, "Smart homes can experience up to 12,000 attacks in a week," www.electropages.com, Jul. 22, 2022. https://www.electropages.com/blog/2022/07/smart-homes-can-experience-12000-attacks-week

[29] A. Husar, "IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities," www.cm-alliance.com, Oct. 25, 2022. https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities

[30] Kaspersky, "How safe are smart homes?," usa.kaspersky.com, Sep. 10, 2020. https://usa.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home

[31] Avast, "Avast Smart Home Security Report 2019," Feb. 2019. Available: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf

[32] Kaspersky, "Smart home technologies in real life," www.kaspersky.com, Feb. 25, 2023. https://www.kaspersky.com/blog/iot-survey-report-2023/

[33] Cyber Security Hub Editor, "A deep look into the ICS threat landscape," Cyber Security Hub, Jan. 30, 2023. https://www.cshub.com/iot/whitepapers/otiot-security-report-a-deep-look-into-the-ics-threat-landscape

[34] Locking Out Risks, & Homes, T. to S. (s/f). IoT Device Security. Trendmicro.com. Recuperado el 9 de octubre de 2023, de https://documents.trendmicro.com/assets/white_papers/IoT-Device-Security.pdf?_ga=2.157898169.2057653699.1696869221-199051684.1696869221

[35] Pranata, I., et al., December 2012. Securing and governing access in ad-hoc networks of internet of things. In: Proceedings of the IASTED International Conference on Engineering and Applied Science, Colombo, Sri Lanka, pp. 84–90. https://www.researchgate.net/publication/266629783_Securing_and_Governing_Access_in_Ad-Hoc_Networks_of_Internet_of_Things

[36] G. Gallopeni, B. Rodrigues, M. Franco, and B. Stiller, "A Practical Analysis on Mirai Botnet Traffic," IEEE Xplore, Jun. 01, 2020. https://ieeexplore.ieee.org/abstract/document/9142798

[37] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN : An Experimental Approach," Sensors, vol. 20, no. 3, p. 816, Feb. 2020, doi: https://doi.org/10.3390/s20030816.

[38] N. Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, Oct. 26, 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[39] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, "Foundational cybersecurity activities for IoT device manufacturers," May 2020, doi: https://doi.org/10.6028/nist.ir.8259.

[40] K. Boeckl et al., "Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks," Jun. 2019, doi: https://doi.org/10.6028/nist.ir.8228.