A Review on Computer Network Security System

Manjunath R ,Information Science and Engineering ,AIET ,Karnataka ,India

Mr. Pradeep Nayak, Information Science and Engineering ,AIET ,Karnataka ,India

Manish K, Information Science and Engineering ,AIET ,Karnataka ,India

Manoj M U, Information Science and Engineering ,AIET ,Karnataka ,India

Mohammed Adil, Information Science and Engineering ,AIET ,Karnataka ,India

Abstract

In this extensive study, we examine the vital components of thoughtfully designed wireless network security. To demonstrate how businesses can successfully adopt and maintain strong wireless security measures, we look at the foundational ideas of wireless security architecture, research safe wireless network design techniques, and analyse real- world case studies. The military, businesses, and individuals using personal computers now place a higher priority on network security. Security became a big concern with the introduction of the internet, and understanding the history of security helps to explain how security technology emerged . Numerous security vulnerabilities were made possible by the architecture of the internet. Machine Learning (ML)-based solutions that can identify intricate patterns in network traffic for a variety of network security issues have been put forth in a number of recent research projects. Network operators are hesitant to trust and use these "black-box" models in production environments, though, since they do not know how these models make judgements. Network security as a whole is a large and developing field. The scope of the study includes a brief history from the early days of the internet to the most recent advancements in network security. Background information about the internet, its vulnerabilities, online attack techniques, and security technology are crucial for comprehending the study being conducted today, and as such, they are examined.

Keywords: *Mitigation, Cryptography, Network, Security*

INTRODUCTION

With the introduction of the Internet and new networking technologies, the globe is becoming increasingly interconnected. Worldwide, there is a vast amount of government, business, military, and personal data on networking infrastructures. [1] The ease with which intellectual property can be obtained online has led to a growing need for network security. The necessity of safeguarding these networks is growing as more people begin to appreciate the ease and adaptability of wireless technologies. Our goal in writing this academic paper is to present a comprehensive examination of well-designed wireless network security. [2]The fundamentals of wireless security architecture, design techniques for building safe wireless networks, and practical examples showing these ideas applied successfully in business environments are all covered in our research. The network-security community has been experiencing increasing strain in recent years. In order to identify complex network traffic patterns for a variety of network security issues, recent research has shown that Artificial Intelligence (AI) and Machine Learning (ML) models are superior to more straightforward rule-based heuristics. In today's network use, user authentication is frequently not employed. [3] Anybody can access a network when they sign up without first obtaining user authentication. For transmission media (WEP), wireless access points are authenticated using wired equivalent privacy. [5] It is a laborious task for administrators to visit every client since the WEP key needs to be installed on every access point and every client access point. The WEP key can be found by looking at other client computers because it is static. [4] There are already a number of programs that can read the WEP key, enabling unauthorized. individuals to connect to the network and potentially damage any machines on it.[7]Only connection lines designated for staff are granted WEP authentication; in contrast, student connection lines (hotspots) use wireless access point transmission media without the need for authentication, making them accessible to all users. Cloud computing, machine learning, artificial intelligence (AI), and the industrial Internet of Things (IoT) have all developed quickly, which has made it easier for businesses and other economic entities to jump on the digital express train and encourage the steady and quick expansion of network capacity. Affected by the pandemic, a number of businesses have shifted to an online presence, which increases the risk of network security. We hope that this thorough analysis will provide insightful advice to academics and professionals alike in their search for practical solutions for wireless network security.[6] Businesses, governments, and individuals all place a high premium on network security as wireless networks spread more and further. It is essential to comprehend and put into practice methods for preserving strong wireless network security because the threat landscape is always changing.

LITERATURE REVIEW

INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

Organisations are deploying protected private networks, or intranets, out of fear of security vulnerabilities on the Internet. Security measures have been added to the Internet Protocol Suite at several tiers by the Internet Engineering Task Force (IETF). [8]Data units that are moved across the network can be logically protected thanks to these security measures. Internet security is standardised by the security architecture of the internet protocol, or IP Security. IP security, or IPsec, protects both the present IP version (IPv4) and the next generation (IPv6). Even while new methods, like IPsec, have been created to address the most well-known shortcomings of the internet, they don't seem to be enough. The Architectures of IPv4 and IPv6 In 1980, [9] IPv4 was designed to take the place of the ARPANET's NCP protocol. After twenty years, the IPv4 showed various shortcomings. With IPv4's inadequacies in mind, the IPv6 protocol was created. IPv6 is a new protocol architecture rather than a superset of IPv4. [10] There is too much to mention in regards to the design of the internet protocol. A detailed discussion is given of the key security-related components of the design. IPv4 Structure A few parts of the protocol produced issues while implementing it. Not all of these issues have to do with security.[11] To obtain a thorough understanding of the internet protocol and its weaknesses, they are mentioned. An address in the IPv4 architecture is 32 bits wide. As a result, the total number of PCs that can be online is restricted. A maximum of two billion computers can be linked to the internet using the 32-bit address. When the protocol was developed, it was not anticipated that going over that amount would be an issue. [12] The propagation of malicious code is facilitated by IPv4's limited address space. This protocol's routing is problematic since the routing tables' size keeps growing. The global routing tables might theoretically include up to 2.1 million entries.[11] Techniques for minimising the amount of entries in the routing table have been implemented. Today's numerous attacks are a result of the IPv4 protocol's lack of inbuilt security. [13] Although there are security protocols for IPv4, their adoption is not mandated. The protocol is secured by a particular method called IPsec.[27] IPsec uses cryptography to secure the packet payloads. The services of integrity, authentication, and confidentiality are offered by IPsec.[14] The competent hacker who might be able to crack the encryption scheme and get the key is not taken into consideration by this type of security. Upon the creation of the internet, the quality of service (QoS) was standardized based on the data being moved over the network.

BACKGROUND AND IMPORTANCE OF WIRELESS NETWORK SECURITY

The need for wireless network security has grown as the world's reliance on wireless communication expands. [15]Wireless networks include benefits like portability, flexibility, and scalability, but because of their open architecture and the simplicity with which hackers can intercept data transmissions, they also present special security concerns. [16]The need of safeguarding wireless networks is further highlighted by the rise in remote work, Internet of Things (IoT) devices, and the growing demand for seamless access. [26]To build, deploy, and maintain a secure wireless network, one must have a solid understanding of the fundamentals of wireless security.

[17]The fundamental ideas of wireless security, such as the CIA triad, authentication and authorization, and secure communication protocols, will be covered in this part. Ensuring the confidentiality, integrity, and availability of data exchanged across wireless networks is contingent upon the use of secure communication protocols. [18]These protocols usually use integrity-checking and encryption to guard against tampering and unauthorised access to data. In wireless networks, a few popular secure communication protocols. The total security posture of a wireless network is largely dependent on the wireless security architecture selected. [19]The function of network devices and components, centralised and decentralised designs, and the significance of integrating wireless security measures with current infrastructure will all be covered in this part.

CHALLENGES IN ML FOR NETWORK SECURITY

ML's Challenges for Network Security In addition to the trust issue that has already been raised, network security is a particularly difficult application domain for AI/ML for a variety of additional reasons. [20]Datasets that are specifically focused on cybersecurity and networking in general often include information on what is being communicated. 1538 Network Security Using AI/ML: The Emperor is not dressed. via a network offer insight into how networks facilitate such information exchanges, CCS '22, November 7–11, 2022, Los Angeles, CA, USA. Because of this, the datasets frequently give rise to grave privacy concerns particular to end users or expose provider-specific information that many businesses view as private and are thus reluctant to disclose. [21] Networking and cybersecurity datasets are usually composed of semantically rich content rather than human-recognizable images, and it often takes a significant amount of domain knowledge to properly label and unpack this content (e.g., network architecture, protocols, and standards). [22]The requirement for domain expertise eliminates labelling strategies that have been effectively employed in other fields, such as outsourcing (e.g., for labelling datasets that have been selected and made publicly available by for-profit self-driving car companies for academic use) or crowdsourcing[26] (e.g., for labelling photos that are included in open-source databases like ImageNet). [23]As a result, there are generally not enough datasets available to the public. Furthermore, because they were created artificially, came from small-scale testbed environments, or were so heavily anonymized that their overall utility was severely limited, the publicly accessible datasets typically lack the complexity of real-world settings. An much greater issue is the dearth of meticulously labelled data. [25]

CONCLUSION

Due to the fact that security is an ongoing concern, Service providers are required to develop a security plan since security is a continuous worry. Educating staff members on standard practices is a wise first step. Starting the process of implementing a security plan with the most obvious protections in place is essential. Additionally, you want to choose equipment capable of offering the most advanced security measures, like privileged-EXEC authentication and greater scalability than line-level. Incoming traffic restrictions, which include guarding against DoS attacks on router control processors, can also be implemented by administrators. Generally speaking, administrators ought to turn down unused and superfluous services, even if doing so implies turning off server functionality. Security of wireless networks is a crucial component of contemporary information technology and communication, with broad ramifications for both individuals and enterprises. This study has examined a number of topics related to well-architected wireless network security, such as future trends and challenges, technologies, case studies, security concepts, architectures, design techniques, and maintenance strategies. The main results of our study will be summarised, and the ramifications for academics and practitioners will be covered in this closing part. An essential component of contemporary information technology, well-architected wireless network security is a constant source of difficulty for both enterprises and researchers. We can make the digital world more safe and resilient for everyone by putting the ideas, approaches, and best practices covered in this research paper into practice. We introduce Trustee, a new framework that lets users assess how much they trust the black-box models that power machine learning (ML) solutions. We evaluate whether end users can trust published ML-based solutions from the literature in a number of use situations to show how Trustee functions in practice. We also discuss our findings and lessons gained. The scientific community has made a compelling case for increased reproducibility in recent years, as has the community for network research in particular. Much work needs to be done in order to achieve the goal of automating these tasks. Specifically, in order to statistically gauge the degree of trust that network operators and security experts have in a given black-box machine learning model that powers a suggested machine learning solution for a particular network security issue, we must include these parties in carefully crafted user studies.

REFERENCES

[1] Computer Network Security System, Ambarish Kumar Patel ,School of Computer Science , Anjaneya University Raipur C.G.

[2] J. B. Evans, W. Wang, and B. J. Ewy, "Wireless networking security: open issuesin trust, management, interoperation and measurement," Int. J. Secur. Netw., vol. 1, no. 1–2, pp. 84–94, Jan. 2006.

[3] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks," in Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications, Taormina-Giardini Naxos, Italy, 2003.

[4] M. Gajewski et al., "Two-tier anomaly detection based on traffic profiling of the home automation system," Comput. Networks, vol. 158, pp. 46–60, 2019, doi: 10.1016/j.comnet.2019.04.013.

[5] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: a tutorial,” IEEE Wirel. Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.
[6] J. M. Kizza, Guide to Computer Network Security. Springer International Publishing, 2013.
[7] M. K. Jain, “Wireless sensor networks: Security issues and challenges,” 2011.
[8] D. Boyle and T. Newe, “Securing wireless sensor networks: Security architectures,” J. Netw., vol. 3, no. 1, Jan. 2008.
[9] D. W. Apley and J. Zhu. 2020. Visualizing the effects of predictor variables in black box supervised learning models. Journal of the Royal Statistical Society: Series B (Statistical Methodology) 82, 4 (2020), 1059ś1086. https://doi.org/10.1111/rssb.12377arXiv:https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/rssb.12377
[10] G. Apruzzese, L. Pajola, and M. Conti. 2022. The Cross-evaluation of Machine Learning-based Network Intrusion Detection Systems. IEEE Transactions on Network and Service Management (2022), 1ś1. https://doi.org/10.1109/TNSM.2022. 3157344
[11] M. Arjovsky, L. Bottou, I. Gulrajani, and D. Lopez-Paz. 2020. Invariant Risk Minimization. arXiv preprint arXiv:1907.02893 (2020). arXiv:stat.ML/1907.02893
[12] D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, C. Wressnegger, L. Cavallaro, and K. Rieck. 2022. Dos and Dont’s of Machine Learning in Computer Security. In 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA. https://www.usenix.org/conference/usenixsecurity22/ presentation/arp
[13] V. Bajpai, A. Brunstrom, A. Feldmann, W. Kellerer, A. Pras, H. Schulzrinne, G. Smaragdakis, M. Wählisch, and K. Wehrle. 2019. The Dagstuhl Beginners Guide to Reproducibility for Experimental Networking Research. SIGCOMM Comput. Commun. Rev. 49, 1 (Feb. 2019), 24ś30. https://doi.org/10.1145/3314212.3314217
[14] Website of the P4 Language Consortium, https://p4.org/.
[15] .e P4 Language Specification, https://p4.org/p4-spec/p4- 14/v1.0.5/tex/p4.pdf.
[16] P4 Language Consortium, P4_16 Language Specification, P4.
[17] M. Shahbaz, S. Choi, P. Ben et al., “PISCES: A programmable, protocol-independent software switch,” in Proceedings of the 2016 ACM SIGCOMM Conference, pp. 525–538, Florianopolis, Brazil, August 2016.
[18] N. Zilberman, Y. Audzevich, G. A. Covington, and A. W. Moore, “NetFPGA SUME: toward 100 Gbps as research commodity,” IEEE Micro, vol. 34, no. 5, pp. 32–41, 2014.
[19] Behavioral model (bmv2), 2015, https://github.com/p4lang/ behavioral-model.
[20] Barefoot Tofino2, https://www.barefootnetworks.com/ products/brief-tofino-2/.
[21] N. McKeown, T. Sloane, and J. Wanderer, P4 Runtime-Putting the Control Plane in Charge of the Forwarding Plane, 2017, https://p4.org/api/p4-runtime-putting-the-control-plane-in-cha rge-of-theforwarding-plane.html.2017.
[22] J. B. Evans, W. Wang, and B. J. Ewy, “Wireless networking security: open issuesin trust, management, interoperation and measurement,” Int. J. Secur. Netw., vol. 1, no. 1–2, pp. 84–94, Jan. 2006.
[23] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, “Self-securing ad hoc wireless networks,” in Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications, Taormina-Giardini Naxos, Italy, 2003.
[24] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: a tutorial,” IEEE Wirel. Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.
[25] J. M. Kizza, Guide to Computer Network Security. Springer International Publishing, 2013.
[26] M. K. Jain, “Wireless sensor networks: Security issues and challenges,” 2011.
[27] D. Boyle and T. Newe, “Securing wireless sensor networks: Security architectures,” J. Netw., vol. 3, no. 1, Jan. 2008.
[28] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor network security: a survey,” IEEE Communications Surveys & Tutorials, vol. 11, no. 2, pp. 52–73, Second 2009.
[29] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, “Detecting wormhole attacks in delay-tolerant networks [Security and Privacy in Emerging Wireless Networks],” IEEE Wirel. Commun., vol. 17, no. 5, pp. 36– 42, Oct. 2010.
[30] J. P. Walters, Z. Liang, and W. Shi, “Wireless sensor network security: A survey,” Security in distributed, grid, 2007.