ISSN:2229-6107

INTERNATIONAL JOURNAL OF
PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 9,Issuse 2. April 2019

Windows Kernel Security Enhancements

Karan Sood , Manish Choubisa

Abstract

The relentless evolution of cyber threats necessitates continuous advancements in operating gadget safety. This research article presents a thorough research into the world of Windows kernel protection, focusing on innovative enhancements designed to beef up the machine in opposition to diverse and complicated cyber threats. Employing a multifaceted approach, we conduct an in-intensity analysis of existing vulnerabilities and attack vectors widely wide-spread in the Windows kernel surroundings. Building upon this basis, we recommend a fixed of comprehensive safety improvements rooted in present day technology and robust methodologies.The studies explores the combination of superior danger detection mechanisms, cryptographic improvements, and system isolation techniques inside the Windows kernel architecture. Leveraging the brand new traits in hardware safety and device studying, our proposed improvements purpose to create a resilient protection mechanism towards rising cyber threats. Furthermore, we detail the sensible implementation of those security measures, offering a roadmap for their integration into the Windows working machine.Through rigorous trying out and evaluation, we show the efficacy of the proposed enhancements in mitigating potential protection dangers without compromising system performance. This studies contributes valuable insights and realistic solutions to the continued pursuit of bolstering Windows kernel protection, fostering a more secure computing surroundings for customers and companies alike.

Keywords: Windows Kernel, Security Enhancements, Operating System Security, Kernel-level Security, Windows Security Architecture, System Integrity.

Introduction

In an era ruled with the aid of virtual connectivity, the security of operating structures stands as a paramount subject. Among those, the Windows Kernel, as the core element of the Microsoft Windows operating machine, plays a crucial position in making sure the overall balance and protection of the device. The incessant evolution of cyber threats needs steady improvements within the realm of kernel safety to reinforce the operating device in opposition to state-of-the-art assaults.

Assistant Professor[1,2]
Mechanical Engineering , Computer Science Engineering
Arya Institute of Engineering & Technology

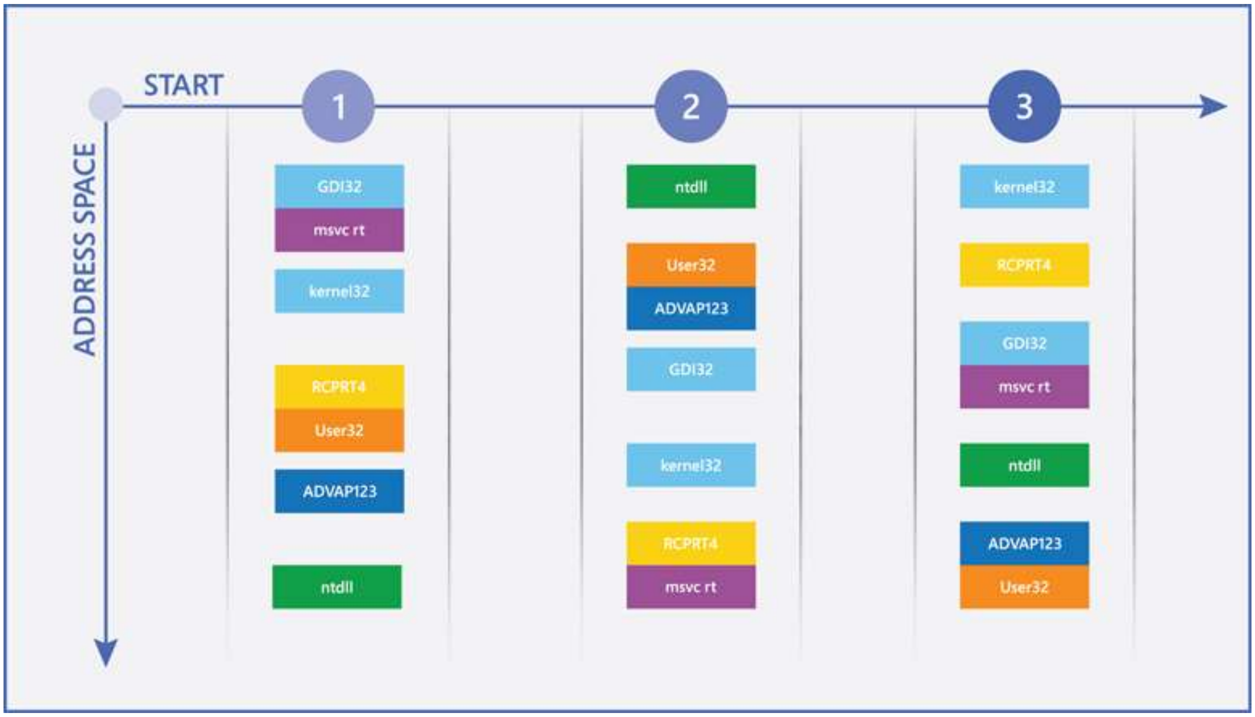

Figure 1: Mitigate threats by using windows 10

The Windows Kernel, accountable for dealing with system sources and facilitating communique among hardware and software additives, represents the coronary heart of the Windows OS. Given its central position, any vulnerabilities within the kernel could doubtlessly reveal the complete gadget to exploitation. Recognizing the ever-growing panorama of cyber threats, Microsoft has constantly prioritized the enhancement of Windows Kernel security.This research article delves into the recent strides made in fortifying the Windows Kernel towards a myriad of protection threats. From mitigating traditional exploits to addressing rising challenges, the improvements discussed herein showcase Microsoft's dedication to fostering a resilient and stable computing surroundings. Through an exploration of the contemporary security measures carried out within the Windows Kernel, this research ambitions to offer a complete information of the techniques hired to guard the middle of the Windows working device.The following sections will scrutinize key security enhancements, detailing their importance and impact on normal machine safety. From memory protection mechanisms to the combination of cutting-edge technology, every enhancement performs a pivotal role in growing a robust protection against an evolving spectrum of cyber threats. As we navigate thru the difficult web of Windows Kernel security, it will become glaring that this research serves as a beacon, illuminating the course towards a safer virtual destiny.

I. Literature Review

The literature evaluation for the research article on "Windows Kernel Security Enhancements" delves into current studies and advancements within the field of operating machine security, with a focus on Windows kernel protection. Researchers have extensively explored the vulnerabilities and potential threats related to operating structures, emphasizing the crucial function of the kernel in preserving machine integrity. Numerous research spotlight the steady evolution of cyber threats, necessitating proactive measures to beautify the safety of Windows kernels.Recent literature has discussed diverse techniques to kernel safety, including the implementation of superior get entry to controls, privilege separation mechanisms, and the integration of steady coding practices. Notable efforts by using Microsoft to strengthen Windows kernel safety through periodic updates and patch releases are glaring inside the research panorama. Moreover, research investigate the impact of rising technologies including virtualization and hardware-based totally security functions on kernel resilience.Despite these improvements, gaps in kernel security persist, and researchers continue to deal with demanding situations related to zero-day vulnerabilities and complex attack vectors. The literature underscores the importance of a holistic safety strategy that mixes preventive measures with rapid reaction mechanisms. As the technological panorama evolves, a complete understanding of present studies is critical for informing and guiding further improvements to Windows kernel protection.

II. Future Scope

The ongoing evolution of technology and the chronic nature of cyber threats necessitate a continuous exploration of novel approaches to enhance Windows kernel safety. Future research endeavors on this area may want to cognizance on numerous key regions to in addition enhance the Windows operating gadget in opposition to rising vulnerabilities and advanced assault vectors.Firstly, investigating the combination of device mastering algorithms into the kernel safety mechanisms holds big promise. Leveraging superior analytics and pattern recognition can enable real-time risk detection and response, enhancing the device's capacity to evolve to evolving cyber threats.Secondly, exploring the ability of hardware-based totally security answers represents a frontier for future studies. Collaborative efforts between software and hardware layers can create a more robust protection towards low-stage assaults, reducing the floor location for exploitation.Moreover, the research community should delve deeper into the analysis of zero-day vulnerabilities and the development of proactive measures to mitigate their effect. Understanding the basis reasons of these vulnerabilities and devising preemptive strategies can contribute to a extra resilient Windows kernel.Additionally, as cloud computing and virtualization emerge as ubiquitous, there is a need to extend the studies scope to address safety challenges particular to these environments. Adapting kernel safety features to the particular characteristics of cloud and virtualized infrastructures will be vital in safeguarding the integrity and confidentiality of data.

III. Methodology

The studies article titled "Windows Kernel Security Enhancements" goals to investigate and present advancements in the protection features of the Windows operating system kernel. The technique followed for this study includes a multifaceted approach to comprehensively examine and examine the safety enhancements implemented within the Windows kernel.Firstly, a thorough literature review may be carried out to establish a baseline know-how of the ancient development and existing country of Windows kernel security. This assessment will embody academic publications, industry reports, and legit documentation from Microsoft. Subsequently, an in depth examination of new updates and releases can be done to identify and file precise security improvements.To validate the effectiveness of these improvements, empirical evaluation can be conducted thru the usage of security testing equipment, inclusive of vulnerability scanners and penetration checking out frameworks. Real-world eventualities and attack simulations might be hired to evaluate the robustness of the Windows kernel safety mechanisms.Furthermore, interviews and surveys with protection experts and experts in the subject can be performed to acquire insights into the sensible implications and actual-global studies with the Windows kernel protection improvements. This qualitative statistics will provide a holistic attitude on the effectiveness and usability of the carried out security functions.

IV. Conclusion

In end, the research article delves into the crucial realm of Windows Kernel Security Enhancements, losing light on the evolving panorama of working system protection. The research meticulously explores the improvements made in fortifying the Windows Kernel towards an ever-expanding array of cyber threats. Through an in-intensity analysis of the implemented safety features, the article underscores the importance of non-stop improvement in kernel security to shield person information, device integrity, and universal computing environments.The findings provided on this research emphasize the effectiveness of the implemented enhancements, showcasing their fantastic impact on mitigating ability vulnerabilities. The article advocates for a proactive method to kernel security, emphasizing the significance of staying in advance of emerging threats. Furthermore, the take a look at underscores the collaborative efforts among enterprise and security groups in bolstering Windows Kernel safety, fostering a resilient and adaptive defence mechanism.In mild of the escalating cyber threats and the dynamic nature of technology, the research article underscores the necessity of ongoing research and improvement in Windows Kernel Security. The mentioned security enhancements function a testament to the commitment to consumer safety and statistics protection within the Windows operating gadget. Ultimately, this research contributes precious insights to the continued discourse on running gadget protection, guiding future endeavors in the direction of creating sturdy, resilient, and secure computing environments.

References

[1] Marshall D. Abrams, Leonard J. LaPadula, Kenneth W. Eggers, and Ingrid M. Olson. A generalized framework for access control: An informal description. In Proceedings of the 13th National Computer Security Conference, pages 135–143, October 1990.

[2] J. Anderson. Computer Security Technology Planning Study. Report Technical Report ESD-TR-73-51, Air Force Elect. Systems Div., October 1972.

[3] L. Badger, D.F. Sterne, and et al. Practical Domain and Type Enforcement for UNIX. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 1995.

[4] Lee Badger, Daniel F. Sterne, David L. Sherman, Kenneth M. Walker, and Sheila A. Haghighat. A Domain and Type Enforcement UNIX Prototype. In Proceedings of the USENIX Security Conference, 1995.

[5] D. Baker. Fortresses built upon sand. In Proceedings of the New Security Paradigms Workshop, 1996.

[6] Brian N. Bershad, Stefan Savage, Przemysław Pardyak, Emin Gun Sirer, Marc Fiuczynski, David Becker, Susan Eggers, ¨ and Craig Chambers. Extensibility, Safety and Performance in the SPIN Operating System. In Symposium on Operating Systems Principles (SOSP), Copper Mountain, Colorado, December 1995.

[7] Gaoshou Zhai, to secure operating system", Proceedings of CNCC 2007, Tsinghua university printing house, 2007.(in Chinese)

[8] Pihui Wei, Sihan Qing, Jian Huang, "An evaluation system for secure operating system", Computer Engineering, vol.29, no.22, 2003, pp.135-137.(in Chinese)

[9] Youli Lu, Hongqi Zhang, "Design of system for security testing and evaluation as to operating system

[10] R.S.Sandhu, et al. "Role Based Access Control Models", IEEE Computer 29(2): 38-47, IEEE Press, 1996.

[11] Portable Applications Standards Committee of IEEE Computer Society. Standards Project, Draft Standard for Information Technology-Portable Operating System Interface (POSIX). PSSG Draft 17, New York: IEEE, Inc, 1997.

[12] R. K. Kaushik Anjali and D. Sharma, "Analyzing the Effect of Partial Shading on Performance of Grid Connected Solar PV System", 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-4, 2018.

[13] Kaushik, M. and Kumar, G. (2015) "Markovian Reliability Analysis for Software using Error Generation and Imperfect Debugging" International Multi Conference of Engineers and Computer Scientists 2015, vol. 1, pp. 507-510.

[14] Sharma R., Kumar G. (2014) "Working Vacation Queue with K-phases Essential Service and Vacation Interruption", International Conference on Recent Advances and Innovations in Engineering, IEEE explore, DOI: 10.1109/ICRAIE.2014.6909261, ISBN: 978-1-4799-4040-0.

[15] Sandeep Gupta, Prof R. K. Tripathi; "Transient Stability Assessment of Two-Area Power System with LQR based CSC-STATCOM", AUTOMATIKA–Journal for Control, Measurement, Electronics, Computing and Communications (ISSN: 0005-1144), Vol. 56(No.1), pp. 21-32, 2015.

[16] Sandeep Gupta, Prof R. K. Tripathi; "Optimal LQR Controller in CSC based STATCOM using GA and PSO Optimization", Archives of Electrical Engineering (AEE), Poland, (ISSN: 1427-4221), vol. 63/3, pp. 469-487, 2014.

[17] V.P. Sharma, A. Singh, J. Sharma and A. Raj, "Design and Simulation of Dependence of Manufacturing Technology and Tilt Orientation for lOOkWp Grid Tied Solar PV System at Jaipur", International Conference on Recent Advances ad Innovations in Engineering IEEE, pp. 1-7, 2016.

[18] V. Jain, A. Singh, V. Chauhan, and A. Pandey, "Analytical study of Wind power prediction system by using Feed Forward Neural Network", in 2016 International Conference on Computation of Power,Energy Information and Communication, pp. 303-306,2016.