數位遊戲嵌入式系統之高安全技術研究

吳佳鑫、曹偉駿

E-mail: 382061@mail.dyu.edu.tw

摘 要

隨著網路發展，數位線上遊戲與大型電玩直至目前，由不被重視而轉為現代人的消遣娛樂，故數位遊戲產業漸趨蓬勃發展，因而安全議題逐漸顯得重要。在數位遊戲產業面臨的安全議題中，除了駭客攻擊外，尚有機器人外掛的公平性破壞，以及通訊封包截取後竊改。機器人外掛以及封包被竊取後的破壞影響，輕則可令遊戲廠商損失慘重，重則可令數位遊戲乏人問津甚至面臨倒閉的危機。綜觀目前數位遊戲產業的安全機制，皆無法同時兼具低成本與高安全性，致使目前相關安全機制無法普及。 本論文研究目的是要讓玩家與廠商即使未具安全概念也可保障其利益，故本研究開發具高度隱藏特性之Rootkit技術來達到數位遊戲嵌入式系統之通訊資料的保護。雖然現有的Rootkit都是被駭客利用來作各種系統攻擊，以令使用者無所查覺，但正所謂「水可載舟亦可覆舟」，Rootkit就如雙面刃可用於不法也可用於正途，因而本論文是首先植基於Rootkit的隱藏特性以保護數位資料封包的傳輸，其作法是採用隱藏能力強大之DKOM (Direct Kernel Object Manipulation) 技術將遊戲資料藏於設備機台的Windows Embedded 作業系統內，讓不法者無法截取資料、製作外掛機器人與進行相關的攻擊，以有效保障數位遊戲使用者與廠商的權益。本研究所提出的防護方法，因採用軟體方式建構且具有隱藏功能，以及完全不需要硬體搭配，故有極低的建置成本與極高的安全特性，因而非常有助於數位遊戲產業的發展。

關鍵詞 : 數位遊戲、系統安全、嵌入式系統、Rootkit、Windows作業系統

目錄

參考文獻

[1] MIC 產業情報研究所，全球遊戲市場與趨勢， http://www.iii.org.tw/about/1_7_5_1.asp, May 19, 2013.

[2] 蔣妤羚，線上遊戲身份認證機制安全性之研究，樹德科技大學資訊管理系碩士論文，2008。

[3] 陳冠中，「天堂」遊戲參與者之動機、沉迷與交易行為關係之研究，國立中正大學企業管理研究所碩士論文，2002。

[4] ?豐加密小精靈， http://www.hsbc.com.tw/1/2/Mis c/popup-tw/pib-tw/security-device/about, May 2, 2013.

[5] 暴風雪魔獸世界官網， http://tw.battle.net/wow/zh/, May 23, 2013.

[6] 智冠科技， http://www.soft-world.com/news_sw/sw /sw1010921.htm, May 23, 2013.

[7] 17173.com, 17173China ’ s Online Games ’ Users Research report 2009, Technical Report of ESET, 2010.

[8] Black Hat USA, http://www.blackhat.com/us-13/, May 20, 2013.

[9] B. Bencs ’ ath , G. P ’ ek , L. Butty ’ an and M. F ’ elegyh ’ azi, The Cousins of Stuxnet: Duqu, Flame and Gauss, Future Internet, pp. 971-1003, 2012.

[10] H. Chen , The Single-Chip Solution of Embedded USB Encryptor, IEEE International Conference on Information Theory and Information Security (ICITIS), pp. 42-45, Dec, 2010.

[11] Y. Y. Chen, Design of Web Intervention to Influence Youth Behavior Toward Online Gaming, International Symposium in Information Technology (ITSim),Vol. 3, pp. 1368 – 1371, 2010.
[12] Y. C. Chen, P Chen, R. Song and L. Korba, Online Gaming Crime and Security Issue Cases and Countermeasures from Taiwan, National Research Council of Canada, 2004.
[13] Y. C. Chen, J. J. Hwang, R. G. Song, G. Yee and L. Korba, Online Gaming Cheating and Security Issue, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05),Vol. 1, pp. 518 – 523, 2005.
[14] CurrPorts - Monitoring Opened TCP/IP network ports / connections, http://www.nirsoft.net/utils/cp orts.html, May 15, 2013.
[15] L. Duflot, Using CPU System Management Mode to Circumvent Operating System Security Functions, CanSecWest Applied Security Conference. Vancouver, 2006.
[16] Diagnosing Memory Problems on Your Computer,
http://windows.microsoft.com/en-US/windows7/Diagnosing-memory-problems-on-your-computer, May 15, 2013.
[17] E. Florio and K. Kasslin, Your Computer is Now Stoned (Again!): the Rise of MBR Rootkits, Technical Report of Symantec, 2008.
[18] Ganesan R., An Independent Verification of Errors and Vulnerabilities in SaaS Cloud, Dependable Systems and Networks Workshops (DSN-W), Proceedings of the International Conference on IEEE/IFIP 42nd, pp. 1-6, 2012.
[19] M.M. Kermani and M. Zhang, Raghunathan A. and Jha N.K., Emerging Frontiers in Embedded Security, Proceedings of the International Conference on VLSI Design and 12th Embedded Systems (VLSID), pp. 203 – 208, Jan, 2013.
[20] A. J. Kornecki, J. Zalewski and W. F. Stevenson, Availability Assessment of Embedded Systems with Security Vulnerabilities, 34th IEEE Software Engineering Workshop (SEW), pp. 42 – 47, June, 2011.
[21] B. Khan, Security Analysis of Firewall Rule Sets in Computer Networks, Fourth International Conference on Emerging Security Information Systems and Technologies (SECURWARE), pp. 51 – 56, 2010.
[22] N. Kumar and V. Kumar, Vbootkit: Compromising Windows Vista Security, Black Hat USA Conference, 2012.
[23] S. King, SubVirt: Implementing Malware with Virtual Machines, Proceedings of the IEEE Symposium on Security and Privacy, pp. 327, 2006.
[24] L. Lin, A Study on China's Online Games Development Trend, Proceedings of the International Conference on Mechanic Automation and Control Engineering (MACE), pp. 1725 – 1728, 2010.
[25] Q. Lu, Compound Security Event Detection System Research and Implementation, Networking and Distributed Computing (ICNDC), pp. 175 – 178, 2011.
[26] X. Lan, Y. C. Zhang, C. Yang and M. K. Zhang, An Investigation of Online Game Bots in China, Proceedings of the International Conference on E-Product E-Service and E-Entertainment (ICEEE), pp. 1 – 5, 2010.
[27] Y. Ma, W. Jiang, N. Sang and P. Pop, SAFCM: A Security-Aware Feedback Control Mechanism for Distributed Real-Time Embedded Systems, Proceedings of the IEEE 18th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), pp. 340 – 349, Aug, 2012.
[28] A. Matrosov, E. Rodionov, D. Harley and J. Malcho, Stuxnet Under the Microscope, Technical Report of ESET, 2010.
[29] M. Myers and S. Youndt, An Introduction to Hardware-assisted Virtual Machine (HVM) Rootkits, White Paper of Crucial Security, 2007.
[30] G. McGraw, Guest Editors' Introduction: Securing Online Games: Safeguarding the Future of Software Security, Security & Privacy, IEEE, Vol. 7, pp. 11 – 12, 2009.
[31] Network socket, http://en.wikipedia.org/wiki/Net work_socket, May 20, 2013.
[32] B. Pablo and F. G. Daniel, Rootkits Survey A Concealment Story, Department of Informatics University of Oviedo, 2010.
[33] D. Quist and V. Smith, Detecting The Presence of Virtual Machines Using The Local Data Table, White Paper of Offensive Computing, 2006.
[34] X. M. Qin, Study on Causes and Strategies of Online Game Addiction Among College Students, Proceedings of the International Conference on Multimedia Technology (ICMT), pp. 1 – 4, 2010.
[35] J. F. Ruiz, R. Harjani, A. Mana, Desnitsky V., Kotenko I., Chechulin A. and Parallel, A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components, Proceedings of the 20th Euromicro International Conference on Distributed and Network-Based Processing (PDP), pp. 261 – 268, Feb, 2012.
[36] J. Rutkowska and A. Tereshkin, IsGameOver, Anyone?, Invisible Things Lab, 2007.
[37] J. Rutkowska, Subverting Vista Kernel for Fun and Profit, http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf, May 20, 2013.
[38] C. P. Su, J. H. Lee, S. C. Seo and B. K. Kim, Proceedings of the 12th International Conference on Assuring software security against buffer overflow attacks in embedded software development life cycle,Advanced Communication Technology (ICACT), pp. 787 – 790, Feb. 2010.
[39] M. Serb, Using MTMs to Secure Electronic Signatures Generation, Proceedings of the International Conference on Communications (COMM ' 09), pp. 315 – 318, 2012.
[40] W. J. Tsaur, S. R. Wu and J. X. Wu, Windows Rootkits Stealth Technologies in Cloud Computing, Proceedings of CISC, Taiwan, 2012.

[41] W. J. Tsaur, Strengthening Digital Rights Management Using a New Driver-Hidden Rootkit, IEEE Transactions on Consumer Electronics, Vol. 58, pp. 479 – 483, 2012.
[42] The QQ Fantasy main culprits, http://it.sohu.com/20 070201/n247970507.shtml, May 29, 2013.
[43] TCPView, http://technet.microsoft.com/en-us/sysin ternals/bb897437.aspx, May 15, 2013.
[44] The IntelR Processor Diagnostic Tool for Windows, http://www.intel.com/support/tw/motherboards/desktop/sb/CS-032037.htm, Oct 15, 2012.
[45] F. Wecherowski, A real SMM Rootkit: Reversing and Hooking BIOS SMI Handlers, Phrack Magazine, Vol. 13, Issue 66, 2009.
[46] M. Wang, General Survey on Massive Data Encryption, Proceedings of the International Conference on Computing Technology and Information Management (ICCM ' 08), pp. 150 – 155, 2012.
[47] R. Wojtczuk and J. Rutkowska, Attacking SMM Memory Via Intel CPU Cache Poisoning, White Paper of Invisible Things Lab, 2009.
[48] S. Wang, Analysis and Application of Wireshark in TCP/IP Protocol Teaching, Proceedings of the International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), Vol. 2, pp. 269 – 272, 2010.
[49] S. D. Webb, Cheating in Networked Computer Games: A Review, Proceedings of the 2nd International Cconference on Digital interactive media in entertainment and art, 2007.
[50] Y. Yang, Y. H. Liu and T. X. Song, The Internet of Things Based on Embedded Mode Design, Proceedings of the International Conference on Internet Technology and Applications, pp. 1 – 4, Aug, 2010.
[51] Y. Danger, S. Guilley, S. Bhasin and M. Nassar, Embedded systems security: An evaluation methodology against Side Channel Attacks-Souissi, Proceedings of the Conference on Design and Architectures for Signal and Image Processing (DASIP), pp. 1 – 8, Nov, 2011.
[52] S. Yanan, An Identity Authentication Mechanism Based on Timing Covert Channel, Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 832 – 836, 2012.
[53] J. Yan, An Investigation of Cheating in Online Games, IEEE Security & Privacy, Vol. 7, Issue: 3, pp. 37 – 44, 2009.
[54] J. Yan, Security Design in Online Games, Proceeding of 19th Annual Computer Security Applications Conference, pp. 286 – 295, 2003.
[55] IceSword, http://www.softpedia.com/get/System/Sy stem-Info/IceSword.shtml, Apr. 23, 2013.
[56] Rootkit Unhooker, http://www.antirootkit.com/soft ware/RootKit-Unhooker.htm, Apr. 12, 2013.
[57] Gmerek P, http://www.gmer.net/, Apr. 13, 2013 [58] Microsoft Security Essentials, http://www.microsof t.com/security_essentials, Apr. 29, 2013 [59] G. Jacob, H. Debar, and E. Filiol, Behavioral Detection of Malware: from A Survey Towards An Established Taxonomy, Journal Computer Virology, 2008.
[60] D. Wagner, Mimicry Attacks on Host-Based Intrusion Detection Systems, Proceedings of the 9th ACM conference on computer and communications security, 2002.
[61] G. Hoglund, Rootkits: Subverting the Windows Kernel, Addison-Wesley, 2005.
[62] Gmer, http://www.gmer.net/, Apr. 18, 2013.
[63] B. Blunden, The Rootkit Arsenal, Wordware Publishing, 2009.
[64] B. Cogswell and M. Russinovich, Rootkitrevealer, http://technet.microsoft.com/en-us/sysinternals/bb897445, Apr. 14, 2013.
[65] M. Russinovich, Rootkit Reveale, http://technet.mic rosoft.com/en-us/sysinternals/bb897445.aspx, Apr. 18, 2013.
[66] U.S. Patent No. 11/271327. Washington, DC: U.S., Patent and Trademark Office, 2010.