# 基于可靠性理论的分布式系统脆弱性模型

冯萍慧, 连一峰, 戴英侠, 鲍旭华

冯萍慧, 连一峰, 戴英侠, 鲍旭华

(信息安全国家重点实验室(中国科学院 研究生院),北京  100049)

作者简介: 冯萍慧(1979－),女,浙江临海人,博士生,主要研究领域为脆弱性分析.连一峰(1974－),男,博士,副研究员,主要研究领域为网络安全.戴英侠(1942－),女,教授,博士生导师,主要研究领域为信息安全.鲍旭华(1977－),男,博士生,主要研究领域为入侵检测.

联系人: 冯萍慧  Phn: +86-10-88258551, Fax: +86-10-88258093, E-mail: phfeng@vip.sina.com, http://home.is.ac.cn

Abstract

After the analysis and comparison of the existing vulnerability analysis methods, a new vulnerability model of distributed systems based on reliability theory is proposed. First, it models vulnerabilities of distributed systems from the aspects of security-related factors. Then it utilizes the model checking method to build Vulnerability State Graph (VSG) of distributed systems to depict the complete process of exploitation of vulnerabilities. Finally, it introduces reliability theory to perform analysis and quantitative evaluation of vulnerabilities of distributed systems, which provides a theoretical evidence for security enhancement.

摘要

对现有的脆弱性分析方法进行分析和比较,提出基于可靠性理论的分布式系统脆弱性模型.针对影响分布式系统安全性的各项因素进行脆弱性建模,利用模型检验方法构造系统的脆弱性状态图,描述系统脆弱性的完整利用过程,引入可靠性理论对分布式系统的脆弱性进行分析和量化评估,

从而为增强分布式系统的安全性提供理论依据.

References:

[1] Dacier M, Deswarte Y, Kaaniche M. Quantitative assessment of operational security models and tools. Technical Report, 96493, LAAS, 1996.

[2] Ortalo R, Deswarte Y. Information systems security: Specification and quantitative evaluation. Technical Report, DeVa ESPRIT Long Term Research Project No.20072, the 2nd Year Report, LAAS-CNRS & INRIA, 1997. 561-584.

[3] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Trans. on Software Engineering, 1999,25(5):633-650.

[4] Swiler LP, Phillips C, Gaylor T. A graph-based network-vulnerability analysis system. Technical Report, SANDIA Report No. SAND 97-3010/1, 1998.

[5] Sheyner O. Scenario graphs and attack graphs [Ph.D. Thesis]. Pittsburgh: Carnegie Mellon University, 2004.

[6] Sheyner O, Haines J, Jha S, Lippmann R, Wing JM. Automated generation and analysis of attack graphs. In: Hinton H, Blakley B, Abadi M, Bellovin S, eds. Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 2002. 273-284.

[7] Jha S, Sheyner O, Wing JM. Minimization and reliability analyses of attack graphs. Technical Report, CMU-CS-02-109, Carnegie Mellon University, 2002.

[8] Cimatti A, Clarke E, Giunchiglia F, Roveri M. NuSMV: A new symbolic model verifier. In: Halbwachs N, Peled D, eds. Proc. of the 11th Conf. on Computer-Aided Verification (CAV'99). LNCS 1633, Trento: Springer-Verlag, 1999. 495-499.

[9] Jiang YX, Lin C, Qu Y, Yin H. Research on model-checking based on Petri nets. Journal of Software, 2004,15(9):1265-1276 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1265.htm

[10] Gansner ER, North SC. An open graph visualization system and its applications to software engineering. Software—Practice and Experience, 1999,30(11):1203-1233.

[11] Zeng SK, Zhao TD, Zhang JG, Kang R, Shi JY. A Design and Analysis. Tutorial of System Reliability. Beijing: Beijing University of Aeronautics & Astronautics Press, 2001 (in Chinese).

附中文参考文献:
[9] 蒋屹新,林闯,曲扬,尹浩.基于Petri网的模型检测研究.软件学报,2004,15(9):1265-1276. http://www.jos.org.cn/1000-9825/15/1265.htm

[11] 曾声奎,赵廷弟,康锐,石君友.系统可靠性设计分析教程.北京:北京航空航天大学出版社,2001.