{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 173
-
Number 8

Year of Publication: 2017

Authors:

Olubadeji Bukola, Adetunmbi A. O.

10.5120/ijca2017914214

{bibtex}2017914214.bib{/bibtex}

Abstract

Security of information is of utmost importance to any organization or individual, which depend on computer system or internet for business transaction or source of information or research. Many viruses are able to recognize certain anti-virus software, and respond differently to such software than to programs designed for other purposes. Some viruses go after the databases stored by anti-virus products. Some viruses simply go after anti-virus products, trying to erase them. Immune systems also face this daunting control challenge. On the one hand, there is need to minimize damage from pathogens, without wasting energy and resources, but on the other must avoid initiating or perpetuating autoimmune responses.

Several preventive measures including identification and authentication, logic access control, audit trails, digital signature and firewalls have been developed for the purpose of information security on system. As a result of inadequacies of these measures intrusion detection was introduced to complement these techniques and hence guarantee full protection of computing resources. Detection system is the process of identifying and detecting unauthorized access or

abnormal incursions, actions and events in the system, which provides information for timely counter measures.

This paper presents a systematic approach to intrusion detection using machine learning techniques to purging in order to avoid autoimmunity on network. Machine learning is an automatic process of extracting hidden or interesting knowledge from data in order to generate its own rule based on the given set of data. In this paper rough set theory will be used as a mathematical tool to deal with imprecise and insufficient knowledge, finding hidden patterns in data and reduce dataset [12]. Appraisal of the shortcomings of the current intrusion detection systems (IDS) will be pointed out and the international knowledge discovery and data mining tools (KDD99) are used for benchmarking intrusion detection used, with the designing of rough-set model.

References

1. Adetunmbi A. O., Falaki S. O., Adewale O. S. and Alese B. K. (2008). Network Intrusion Detection Based on Rough Set and K-Nearest Neighbour. International Journal of Computing and ICT Research, 2(1).
2. Anderson, J.P.(1980). Computer Security threat monitoring and surveillance, Technical report, James P. Anderson co. Box 42, Fort Washington.
3. Apache (2002). “Apache Chunk Buffer Overflow Attack”.
4. Byunghae-Cha, K.P. And Jaittyun, S. (2005). Neural Networks Techniques for Host anomaly Intrusion Detection using Fixed Pattern Transformation. ICCSA 2005, LNCS 3481, 254-263
5. Balasubramanuyan, J.S, Garcia-Fernadez, J.O., Isaacoff, D., Spafford, E., and Amboni,D.(1998) An architecture for intrusion detection using autonomous agent 14th Annual computer security conference(ACSAC’’98), pages 13-24’ IEEE. Computer society.
6. Cobb, S. (1996) The NASA GUIDE TO PC AND LAN security, McGraw-Hill Book Company
7. Cuppens F. and Ortalo R. (2000). “LAMBDA: A Language to Model a Database for Detection of Attacks”, In Proceedings of the Third International Workshop on the Recent Advances in Intrusion Detection (RAID’2000),Toulouse, France.
8. Dacier M, Deswarte Y and Kaâniche M. (1996). “Models and Tools for Quantitative Assessment of Operational Security”, in 12th International Information Security Conference (IFIP/SEC'96), (S.K. Katsikas and D. Gritzalis,Eds.), 177-186, Chapman & Hall, Samos (Greece).
9. Jiawei and Micheline, K.(2006) Data Mining: Concepts and techniques, second edition, Elsevier inc.
10. Kendall, K. (1999) A database of computer attacks for the evaluation of intrusion detection systems, Masters thesis, Massachusetts institute of technology, USA.
11. Krakauer, D.C. and Plotkin, J.B. (2005) Principles and parameters of molecular robustness. In Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies (Jen, E., ed.), pp. 71–103, Oxford University Press
12. Krakauer, D.C. (2005) Robustness in biological systems: a provisional taxonomy. In Complex Systems Science in Biomedicine (Deisboeck, T.S. and Kresh, Y., eds), pp. 185–207, Plenum

13. Matzinger, P. (1998) An innate sense of danger. Semin. Immunol. 10, 399–415
14. Pawlak, Z. (1982) Rough sets: international journal of computer and information science, vol. 11. No.5, pp. 341 - 356. 1982
15. Schmidt-Hempel, P. (2005) The evolutionary ecology of insect immune defense. Annu. Rev. Immunol. 50, 529–551
16. Slagel, M. (2001) the design and implementation of MAIDS (Mobile Agent for Intrusion Detection System) Master's creative Component paper, Iowa state university, Ames Iowa.
17. Sundaram, A. (1996). An Introduction to Intrusion detection.
18. Spafford, E. (1989): internet worm program: an analysis ACM Communication Review, 19(1) 17-57.

Index Terms

Computer Science Security

Keywords

Autoimmunity, Purging, Intrusion detection, Rough Set Theory