ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

AN EFFECTIVE METHOD OF TIME REQUIRED TO COMPROMISE A COMPUTER SYSTEM

V.Srimathi[1], R.Vishali[2], S. Brintha Rajakumari[3]

UG Student, Department of CSE, Bharath University, Chennai, India[1,2]

Assistant Professor, Department of CSE, Bharath University, Chennai, India[3]

Abstract: A cyber intrusion is a frequent assumption in the domain of cyber security and it follows the properties of a Poisson process. By the Poisson distribution the intrusion is well modeled and this process requires a high rate of time. This was also used with Pareto distribution of intrusion so that the rate of time required is slightly decreases with a better performance. Now we are used the chaos algorithm to determine the Time Taken to Compromise (TTC) by using this algorithm the time used for the performing a task in highly decreases. It shows the assumption of the Poisson process model might be suboptimal. The algorithm suggests that time to compromise decreases along the number of instruction of a system regarding this property. This paper clearly explains about the TTC by chaos algorithm.
Keywords: Invasive Software, Network Management, Risk Management.

I. INTRODUCTION

The effective method of time required to compromise a computer system depends on the assumptions regarding to its properties of failures in the systems and knowledge concerning how system failures behave in such situation critical to handle. Selecting the appropriate models for describing the number of failures in a system, and the time taken between failures, is of importance of the particulars as employment of an inappropriate statistical model that can result in improper project conclusions. In the business environment today where IT is a cornerstone of almost all the business, choosing appropriate models critical also to practitioners accurate reliability estimation as result of having used an inappropriate probability distribution can make an enterprise out of the business. this paper brings important insight into this aspect through examine of 5,602,097 malware alarms corresponding to 203,025 intrusions that has been held around 261,75computer systems of a large international companies between October 2009 and August 2012.

The paper is organized as follows. Section 2 describes the related work; section 3 describes statistical distributions. The chaos algorithm discussed in section 4. In Section 5 describes the implementation of the systems and finally concluded the paper in section 6.

II. RELATED WORKS

In the papers [1], [2], [3] that empirically examines distributions of cyber intrusions, properties of system failures, and the security awareness. In the paper[4],[5],[6] there are many kinds of efforts on modeling cyber intrusions, for example, to evaluate the security of a system. These analysis make many realistic to support their claims; a frequent one being that attacks, or intrusions, follows a Poisson process that the number of attacks or intrusions is well modeled by a Poisson distribution and that the time taken between such events is ideally distributed. In the paper [7, 8, 9] at the best of the author's knowledge, there is only one publication that an idea of the distribution of TTC using empirical information in data. The authors have observed that a total of 59 breaches, each of which them were categorized into one of six classes depending on the amount of hours taken to perform it [6].

In the paper [10-15], it is clear that there is a crucial difference between reliability and security. Particularly, the latter involves an actor with the intent of compromising an asset. Whatever, there are also similarities: Many security estimation models have been estimated based on models used for reliability developments.

Gives the lack of relevant theory in the cyber security domain, reliability studies pose a reasonable starting point for harvest potentially statistical distributions for examine Schroeder and Gibson studied many kinds of characteristics of 23,000 failures that had been held during 9 years and on 20 different systems that most being cluster solutions. In the paper [16,17,18] the basic information of malware are employees of the enterprise are required to utilize computer systems that are given through it. Each computer system is equipped with an antimalware solution provided by Symantec. When a malware is detected on a system by the local agent, the information data about the intrusion that is submitted to the central database is shown. In the paper [19], [20] it is the unique identification string of the compromised system, the IP of the compromised system, the time of the event, and the detected malware.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

III. ANALYZED STATISTICAL DISTRIBUTIONS AND TTC

There are three distributions that can be considered in terms of modeling the number of intrusions of a computer system— the Poisson (PO), normal (N), and log-normal (LN). These were all tested by Schroeder and Gibson [1] to model failure rate as a function of systems. While Schroeder and Gibson [1] did not concern cyber intrusions, it is common closely related study available, and that also the best possible start.

There are five statistical distributions that can be considered based on the related work—the exponential (EXP), log-normal (LN), Weibull (WBL), gamma (GAM), and the two-parameter Generalized Pareto (PAR)—in terms of degree of the fit to TTC of computers. EXP is mostly applied to model time between failures and has previously been shown to be a perfect fit for TTC. LN, WBL, GAM, and PAR were typically tested in studies regarding to the time between all the failures.

There are completely different metrics that may be applied to live however well a arrangement model determined knowledge and data. as an example, Kolmogorov-Smirnov, Crame´r-von Mises, Anderson-Darling, Shapiro-Wilk, and Chi sq.. This analysis utilizes the Akaike info criterion (AIC), a customary technique for ranking various models, to match the relative goodness of suited the distributions. AIC has several blessings compared to alternative goodness of- match metrics. The quantity of your time that the behavior of a chaotic system will be effectively expected depends on three things. In chaotic systems the uncertainty in an exceedingly forecast will increase exponentially with period of time. This suggests that in apply a Aic scores for the tested distributions concerning ttfc(exp, ln, par, and wbl) square measure given in table. The economic expert distribution is best match, with weibull receiving minor support, and gamma, log-normal and exponential receiving no support. The qq-plots in support the conclusion that economic expert is best match (with log-normal being the clearly worst fit). The analysis shows cdfs for ttfc in conjunction with the tested applied mathematics distributions. As are often seen, around ninety % of all intrusions need four hundred days or less a vary that all distributions except the log-normal square measure fairly match at modeling.

IV. CHAOS ALGORITHM

Chaos theory issues settled system whose behavior will in theory be expected. Chaotic systems area unit certain for a moment and so substantive prediction cannot be revamped AN interval of over two or three times the lyapunov time. The equations like,

$dx/dt=\sigma y-\sigma x,$ (1)
$dy/dt=\rho x-xz-y,$ (2)
$dz/dt=xy-\beta z.$ (3)

There are seven divisions in working systems which are mentioned below. They are Sender/ transmission, Network Sniffer, Router, Attack Classifier, Firecole, Rule Creation and Black Listing.

V. IMPLEMENTATION AND RESULT ANALYSIS

The following figure explains about the implementation that is used and the result analysis is shown. The front end process used in this algorithm is java swing and the platform used is jdk 1.6.The figure 1 shows the intrusion detection system of attack blocker was receiving the IP address, Router IP address and the sender password through it.The figure 2 shows us a router path to the user to connect the system along with our server. For connecting purpose it was also giving us a proxy server IP address for detection.

The figure3 shows us a clear way of connecting the client to our server and the required path for the connection. We can able to the codes which are mentioned in the screen shots that can directly leads the client's system to connect with server and protect the system from cyber intrusion so that our router path can be analyzed with each and every step.

Fig 1. Intrusion Detection System Attack Blocker(Client)

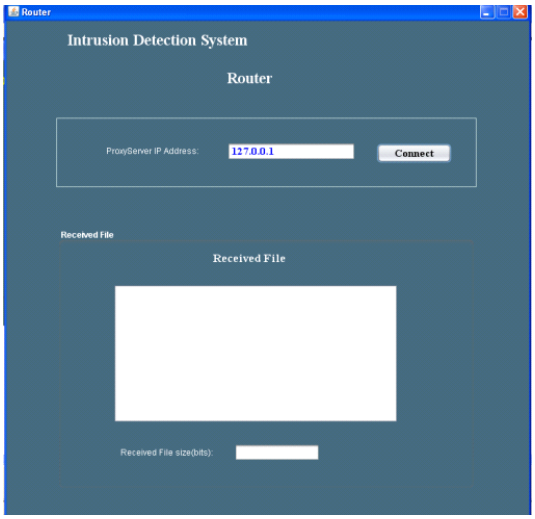

Fig 2.Intrusion Detection System (Router)

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

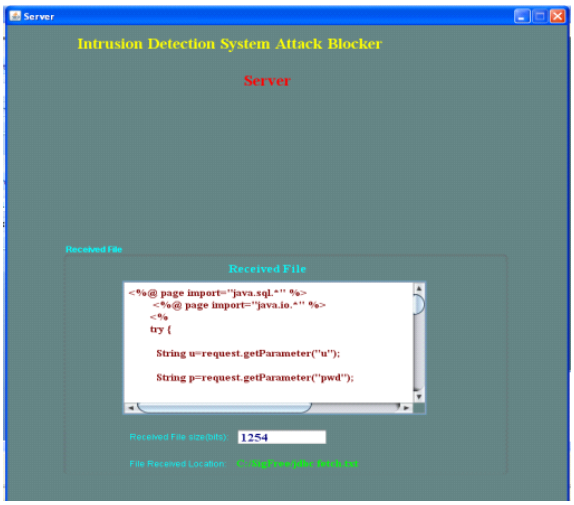

Fig 3. Intrusion Detection System

The figure4that the our software will start detecting our system. once it finds any cyber intrusion on the path of a router it detects the worm and gives alert to the user by proxy based sigfree.

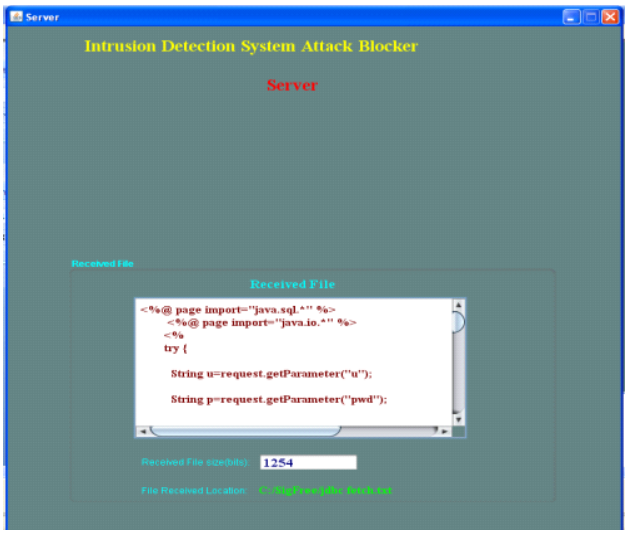

Fig 4. Intrusion Detection System Attack Blocker (Server)

The figure 5 indicates the work of the server to detect the worm and direct it to the some other path.

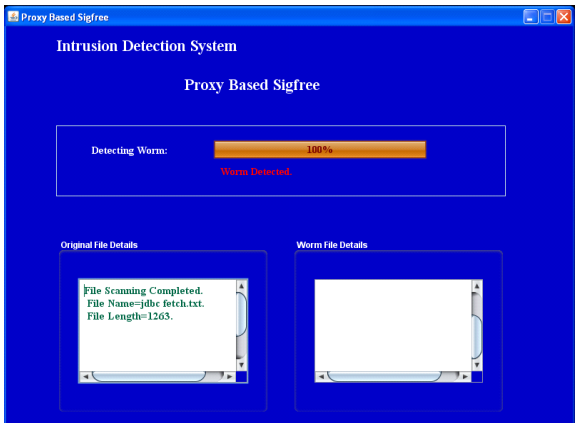

Fig 5. Proxy Based Sigfree

The figures 6 shows us the detection of worm from the path and direct it through the router of some other path and put them in a black list so that the file which is transferred by the user can reach.

This picture 6 shows us a final result of our work that the malware is detected and it has been directed to the black list.

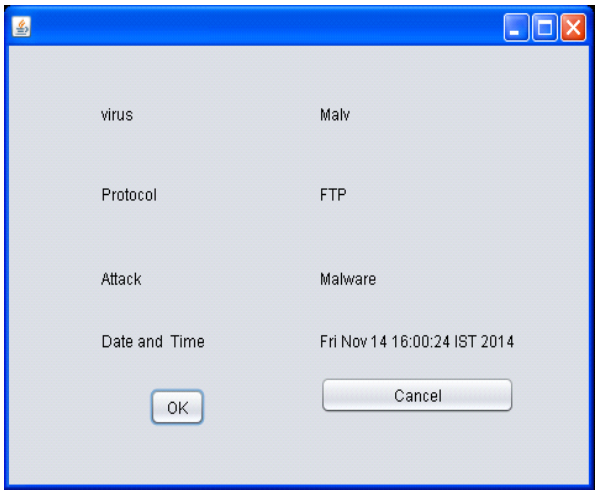

Fig 6. TTC Result

VI. CONCLUSION

In this paper, we have proposed a system where the network administrator will observe and analysis various types of attacking tendencies originating from variable source in network. This process basically understand the pattern and behavior of the hostile circumstances over the network and then it creates the profiles of the attackers based on this pattern analysis, which will protect the network system of the organization by blacklisting the origination of the resource profiling over the network itself thereby assuring the organizational network to be the most secure one in any future probability of network threats from those attackers.

Future analysis would have the benefit of any finding out these variables. Important results from this analysis also are the parameter estimates and therefore the range of compromised systems throughout the studied amount of your time, not solely on overall, except for workstations, servers, UNIX and Windows. These will be seen as a place to begin for an enterprise that has nonetheless to assemble such information.

REFERENCES

[1] B. Schroeder and G. Gibson, "A Large-Scale Study of Failures in High-Performance Computing Systems," IEEE Trans. Dependable and Secure Computing, vol. 7, no. 4, pp. 337-351, Feb. 2010.
[2] D. Nurmi, J. Brevik, and R. Wolski, "Modeling Machine Availability in Enterprise and Wide-Area Distributed Computing Environments," Proc. 11th Int'l Euro-Par Conf. Parallel Processing, pp. 612- 612, 2005.
[3] T. Heath, R. Martin, and T. Nguyen, "Improving Cluster Availability Using Workstation Validation," ACM SIGMETRICS Performance Evaluation Rev., vol. 30, no. 1, pp. 217-227, 2002.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

[4] D. Nicol, W. Sanders, and K. Trivedi, "Model-Based Evaluation: From Dependability to Security," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Oct. 2004.
[5] J. Conrad, "Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations," Proc. Fourth Workshop the Economics of Information Security, pp. 2-3, 2005.
[6] B. Madan, K. Go_seva-Popstojanova, K. Vaidyanathan, and K. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems," Performance Evaluation, vol. 56, no. 1, pp. 167-186, 2004.
[7] J. Ryan, T. Mazzuchi, D. Ryan, J.L. de la Cruz, and R. Cooke, "Quantifying Information Security Risks Using Expert Judgment Elicitation," Computers and Operations Research, vol. 39, no. 4, pp. 774-784, 2012.
[8] N. Schneidewind, "Cyber Security Prediction Models," R & M Eng. J. Am. Soc. for Quality, vol. 25, no. 4, 2005.
[9] M. McQueen, W. Boyer, M. Flynn, and G. Beitel, "Time-to-Compromise Model for Cyber Risk Reduction Estimation," Quality of Protection, vol. 23, pp. 49-64, 2006.
[10] D. Leversage and E. James, "Estimating a System's Mean Time-to-Compromise," IEEE Security and Privacy, vol. 6, no. 1, pp. 52-60, Feb. 2008.
[11] E. Jonsson and T. Olovsson, "A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior," IEEE Trans. Software Eng., vol. 23, no. 4, pp. 235-245, Aug. 1997.
[12] H. Okamura, T. Dohi, and S. Osaki, "Software Reliability Growth Model with Normal Distribution and Its Parameter Estimation," Proc. Int'l Conf. Quality, Reliability, Risk, Maintenance, and Safety Eng. (ICQR2MSE '11), pp. 411-416, 2011.
[13] P. Kapur, H. Pham, S. Anand, and K. Yadav, "A Unified Approach for Developing Software Reliability Growth Models in the Presence of Imperfect Debugging and Error Generation," IEEE Trans. Reliability, vol. 60, no. 1 pp. 331-340, Jan. 2011.
[14] J. Zheng, "Predicting Software Reliability with Neural Network Ensembles," Expert Systems with Applications, vol. 36, no. 2, pp. 2116-2122, 2009.
[15] C. Harteis, J. Bauer, and H. Gruber, "The Culture of Learning From Mistakes: How Employees Handle Mistakes in Everyday Work," Int'l J. Educational Research, vol. 47, no. 4, pp. 223-231, 2008.
[16] H. Holm, M. Ekstedt, and D. Andersson, "Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 6, pp. 825-837, Nov./Dec. 2012.
[17] B. Schneier, Secrets and Lies: Digital Security in a Networked World. Wiley, 2011.
[18] B. Fischhoff, P. Slovic, and S. Lichtenstein, "Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation," J. Experimental Psychology: Human Perception and Performance, vol. 4, no. 2, pp. 330-344, 1978.
[19] R. Ortalo, Y. Deswarte, and M. Kaaˆniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security," IEEE Trans. Software Eng., vol. 25, no. 5, pp. 633-650, Aug. 1999.
[20] D. Long, A. Muir, and R. Golding, "A Longitudinal Survey of Internet Host Reliability," Proc. 14th Symp. Reliable Distributed Systems, pp. 2-9, 1995.