JPCAP, WINPCAP Approach For Intrusion Detection System

Padmini Rathore [#1], Nitin Jain [##2]

[#1] *M.Tech Scholar, Dept. Of Electronics & Telecom.Engg.*
Chouksey Engineering College, Bilaspur
Chhattisgarh, - India

[## 2] *Assistant Professor. Dept. Of Electronics & Telecom.Engg.*
Chouksey Engineering College, Bilaspur
Chhattisgarh, - India

Abstract- Over the past decade many anomaly-detection techniques have been proposed and/or deployed to provide early warnings of cyber attacks, particularly of those attacks involving masqueraders and novel methods. To date, however, there appears to be no study which has identified a systematic method that could be used by an attacker to undermine an anomaly-based intrusion detection system. This paper shows how an adversary can craft an offensive mechanism that renders an anomaly-based intrusion detector blind to the presence of on-going, common attacks. It presents a method that identifies the weaknesses of an anomaly-based intrusion detector, and shows how an attacker can manipulate common attacks to exploit those weaknesses.

Key Word: Anomaly, Signature, Intruders, Artificial Neural Networks (ANN), Genetic Algorithms (GA).

I INTRODUCTION

In recent years, a vast arsenal of tools and techniques has been accumulated to address the problem of ensuring the availability, integrity and confidentiality of electronic information systems. Such arsenals, however, are frequently accompanied by equally vast "shadow" arsenals of tools and techniques aimed specifically at subverting the schemes that were designed to provide system security. Although a shadow arsenal can be viewed negatively as a formidable threat to the security of computer systems, it can also be viewed positively as a source of knowledge for identifying the weaknesses of current security tools and techniques in order to facilitate their improvement. A small part of the security arsenal, and the focus of this work, is the anomaly-based intrusion-detection system. Anomaly-based intrusion-detection systems have sought to protect electronic information systems from intrusions or attacks by attempting to detect deviations from the normal behavior of the monitored system. The underlying assumption is that such deviations may indicate that an intrusion or attack has occurred (or may still be occurring) on the system. Anomaly detection – detecting deviations from normal – is one of two fundamental approaches used in systems that seek to automate the detection of attacks or intrusions; the other approach is signature-based detection. Anomaly. detection is typically credited with a greater potential for addressing security problems such as the detection of attempts to exploit new or unforeseen vulnerabilities (novel attacks), and the detection of abuse-of-privilege attacks, e.g., masquerading and insider misuse [1].

The promise of the anomaly-detection approach and its incorporation into a number of current automated intrusion-detection strategies (e.g., AT&T's Computer Watch, SRI's Emerald, Secure Net, etc. [1]) underscores the importance of studying how attackers may fashion counter-responses aimed at undermining the effectiveness of anomaly-based intrusion-detection systems. Such studies are important for two reasons: – to understand how to strengthen the anomaly-based intrusion-detection system by identifying its weaknesses; and to provide the necessary knowledge for guiding the design and implementation of a new generation of anomaly-based intrusion detectors that are not vulnerable to the weaknesses of their forebears. A number of approaches based on computing have been proposed for detecting network intrusions. The guiding principle of soft computing is exploiting the tolerance of imprecision, uncertainty, partial robustness and low solution cost. Soft computing includes many theories such as Fuzzy Logic (FL), Artificial Neural Networks (ANNs), Probabilistic Reasoning (PR), and Genetic Algorithms (GAs). When used for intrusion detection, soft computing is a general term for describing a set of optimization and processing techniques that are tolerant of imprecision and uncertainty. Soft computing is often used in conjunction with rule-based expert systems where the knowledge is usually in the form of if-then rules. Despite different soft computing based approaches having been proposed in recent years, the possibilities of using the techniques for intrusion detection are still underutilized [5-7].

Some early research on IDSs explored neural networks for intrusion detection. These can be used only after training on normal or attack behaviors, or combination of the two. Most supervised neural net architectures require retraining to improve analysis on varying input data, unsupervised nets, which offer greater adaptability, can improve their analysis capability dynamically [8]. The majority of currently existing IDS face a number of challenges such as low detection rates and high false alarm rates, which falsely classifies a normal connection as an attack and therefore obstructs legitimate user access to the network resources. These problems are due to the sophistication of the attacks and their intended similarities to normal behavior. More intelligence is brought into IDS by means of Machine Learning (ML). Theoretically, it is possible for a ML algorithm to achieve the best performance, i.e. it can minimize the false alarm rate and maximize the detection accuracy. However, this normally requires infinite training sample sizes (theoretically). In practice, this condition is impossible due to limited computational power and real-time response requirement of IDS. IDS must be active at any time and they cannot allow much delay because this would cause a bottleneck to the whole network [9].

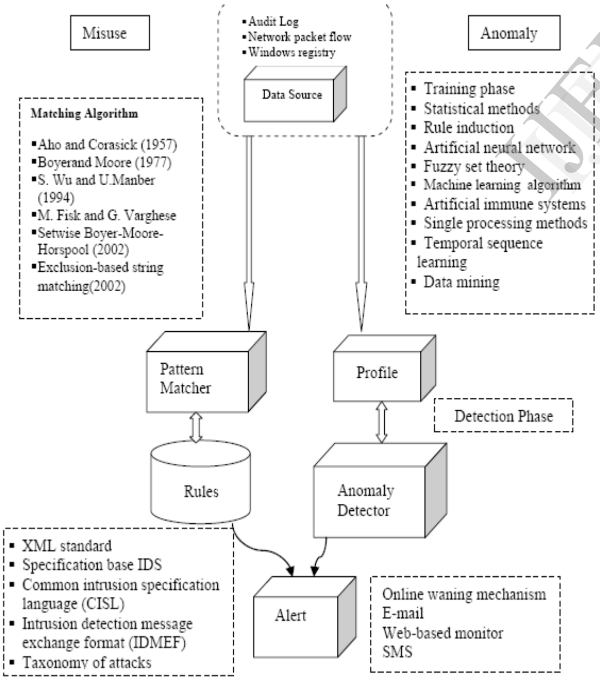


Fig. 1. The Flow Chart of Misuse Detectionand Anomaly Detection Application

To overcome low detection rate and high false alarm problems in currently existing IDS, we propose a hierarchical off line anomaly intrusion detection system using Distributed Time-Delay Artificial Neural Network to enhance the performance of intrusion detection for rare and complicated attacks. In this paper, we introduce anomaly intrusion detection system, this can detect network-based attacks using dynamic neural nets, and has facilities for training, testing, and tuning of dynamic nets for intrusion detection purpose.

II ANOMALY DETECTION TECHNIQUES

Anomaly detection is based on a host or network. Many distinct techniques are used based on type of processing related to behavioral model. They are: Statistical based, Operational or threshold metric model, Markov Process or Marker Model, Statistical Moments or mean and standard deviation model, Univariate Model, Multivariate Model, Time series Model, Cognition based, Finite State Machine Model, Description script Model, Adept System Model, Machine Learning based, Baysian Model, Genetic Algorithm model, Neural Network Model, Fuzzy Logic Model, Outlier Detection Model, Computer Immunology based, User Intention based

2.1. Statistical Models

2.1.1 Operational Model (or) Threshold Metric:

The count of events that occur over a period of time determines the alarm to be raised if fewer then “m” or more than “n” events occur. This can be visualized in Win2k lock, where a user after “n” unsuccessful login attempts here lower limit is “0” and upper limit is “n”. Executable files size downloaded is restricted in some organizations about 4MB.The difficulty in this sub model

2.1.2 Markov Process or Marker Model:

The Intrusion detection in this model is done by investigating the system at fixed intervals and keeping track of its state; a probability for each state at a given time interval Is. The change of the state of the system occurs when an event happens and the behavior is detected as anomaly if the probability of occurrence of that state is low. The transitions between certain commands determine the anomaly detection where command sequences were important.

2.1.3 Statistical Moments or Mean and Standard Deviation Model:

In statistical mean, standard deviation, or any other correlations are known as a moment. If the event that falls outside the set interval above or below the moment is said to be anomalous. The system is subjected to change by considering the aging data and making changes to the statistical rule data base. There are two major advantages over an operational model. First, prior knowledge is not required determining the normal activity in order to set limits; Second, determining the confidence intervals depends on observed user data, as it varies from user to user. Threshold model lacks this flexibility. The major variation on the mean and standard deviation model is to give higher weights for the recent activities.

2.1.4 Multivariate Model:

The major difference between the mean and standard deviation model is based on correlations among two or more metrics. If experimental data reveals better judicious power can be achieved from combinations of related measures rather than treating them individually.

2.1.5 Time Series Model:

Interval timers together with an event counter or resource measure are major components in this model. Order and interarrival times of the observations as well as their values are stored. If the probability of occurrence of a new observation is too low then it is considered as anomaly. The disadvantage of this model is that it is more computationally expensive is determining “m” and “n” .

2.2 Cognition Models:

2.2.1 Finite State Machine:

A finite state machine (FSM) or finite automation is a model of behavior captured in states, transitions and actions. A state contains information about the past, i.e. any changes in the input are noted and based on it transition happens. An action is a description of an activity that is to be performed at a given moment. There are several action types: entry action, exit action, and transition action

2.2.2 Description Scripts:

Numerous proposals for scripting languages, which can describe signatures of attacks on computers and networks, are given by the Intrusion Detection community. All of these scripting languages are capable of identifying the sequences of specific events that are indicative of attacks.

2.2.3 Adept Systems:

Human expertise in problem solving is used in adept systems. It solves uncertainties where generally one or more human experts are consulted. These systems are efficient in certain problem domain, and also considered as a class of artificial intelligence (AI) problems. Adept Systems are trained based on extensive knowledge of patterns associated with known attacks provided by human experts.

2.3 Cognition Based Detection Techniques:

Cognition-Based (also called knowledge-based or expert systems) Detection Techniques work on the audit data classification technique, influenced by set of predefined rules, classes and attributes identified from training data, set of classification rules, parameters and procedures inferred.

2.3.1 Boosted Decision Tree

Boosted Tree (BT), that uses ADA Boost algorithm [23] to generate many Decision Trees classifiers trained by different sample sets drawn from the original training set, is implemented in many IDS successfully[20, 21, 22]. All hypotheses, produced from each of these classifiers, are combined to calculate total learning error, thereby arriving at a final composite hypothesis.

2.3.2 Support Vector Machine

Support vector machines (SVM)) [24], reliable on a range of Classification tasks, are less prone to over-fitting problem, and are effective with unseen data. The basic learning process of the SVM includes two phases: 1) Mapping the training data from the original input space into a higher dimensional feature space, using kernels to transform a linearly non separable problem into a linearly separable one, 2) Finalizing a hyper plane within the feature space, with a maximum margin using Sequential Minimal Optimization (SMO) [25] or Osuna’s method .

2.3.3 Artificial Neural Network

Artificial Neural network (ANN) architectures (popular one being , Multilayer Perceptron (MLP), a layered feed-forward topology in which each unit performs a biased weighted sum of their inputs and pass this activation level through a transfer function to produce their output , are able to identify notreadily-observable patterns, however MLP is ineffective with new data. For general signal processing and pattern recognition problems, another branch of ANN that makes use of radial basis function, called The Modified Probabilistic Neural Network (related to General Regression Neural Network (GRNN) classifier and generalization of Probabilistic Neural Network (PNN)), was introduced by Zaknich. It assigns the clusters of input vectors rather than each individual training case to radial units.

2.4 Machine Learning Based DetectionTechniques

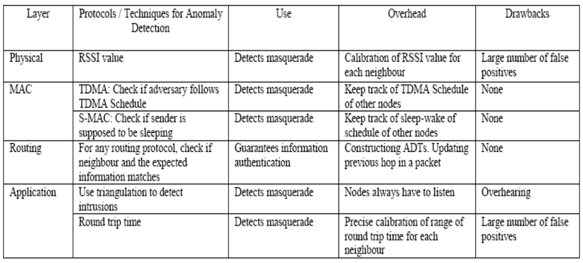
Machine learning techniques to detect outliers in datasets from a variety of fields were developed by Gardener (use a One-Class Support Vector Machine (OCSVM) to detect anomalies in EEG data from epilepsy patients [8A]) and Barbara (proposed an algorithm to detect outliers in noisy datasets where no information is available regarding ground truth, based on a Transductive Confidence Machine (TCM) .Unlike induction that uses all data points to induce a model, transduction, an alternative, uses small subset of them to estimate unknown attributes of test points. To perform online anomaly detection on time series data in, Ma and Perkins presented an algorithm using support vector regression. Ihler et al. present an adaptive anomaly detection algorithm that is based on a Markov-modulated Poisson process model, and use Markov Chain Monte Carlo methods in a Bayesian approach to learn the model parameters.

III CURRENT STATE OF ART

A new method that could achieve more accuracy than the existing six classification patterns (Gaussian Mixture, Radial Basis Function, Binary Tree Classifier, SOM, ART and LAMASTAR),called Hierarchical Gaussian Mixture Model[HMM] for IDM was put forward by M.Bahrololum et al[1]. Jiankun Hu and Xinghuo Yu et al [2] studied development of host-based anomaly intrusion detection, focusing on system call based HMM training. This was later enhanced with the inclusion of data pre-processing for recognizing and eliminating redundant sub-sequences of system calls, resulting in less number of HMM sub models. Experimental result on three public databases indicated that training cost can be reduced by 50% without affecting the intrusion detection performance. False alarm rate is higher yet reasonable compared to the batch training method with a 58% data reduction.R. Nakkeeran et al [3] proposed an anomaly detection system comprising of detection modules for detecting anomalies in each layer. The anomaly detection result of the neighbor node(s) is taken by the current node and its result in turn is sent to the neighbor node(s).Experimental results revealed increased detection rate and reduced false alarm positives, compared to other methods.

Jiong Zhang et al [4] proposed a new framework of unsupervised anomaly NIDS based on the outlier detection technique in random forests algorithm. The framework builds the patterns of network services over datasets labeled by the services. With the built patterns, the framework detects attacks in the datasets using the modified outlier detection algorithm, reducing the calculation complexity. This approach is independent of attack-free training datasets, but assumes that each network service has its own pattern for normal activities.

Ahmed Awad E. Ahmed et al [5] proposed a biometrics-based intrusion detector model to provide a lightweight and selfcontained module for detecting user identities misuse. System-calls and network traffic monitoring systems have to be combined to this detector to achieve the best solutions. Vijay Bhuse et al [6] proposed a technique to detect anomalies at all layers of a network stack in a sensor network, segregating the service at various levels. Physical layer intrusion is detected by using RSSI values of neighbors (dependant on background noise, weather conditions etc). Targeting MAC layer will work for schedule based and sleep/wake-up based MAC protocols while IASN protocol is aimed at the routing layer. Experiments show that IASN can be used for source initiated routing protocols, table driven routing protocols and data dissemination mechanisms like directed diffusion. The probability of detection increases linearly with the number of nodes running IASN. Nodes guard each other from masquerade at application layer. Depending on the resource availability, any combination of the above methods can be employed, as they are independent of one another. All techniques are energy efficient as they have very low false positive rates (except RSSI and round trip time) and low overhead. Using information theory measures, a model was put forward by Hossein M. Shirazi et al [7] that ranked 41 connection features performing normalization on each attack class. The main features of this are, ranking (relevant features for each attack class are selected and computing complexity is decreased) and features-selection (detection rate preserved, yet detection time decreased). Noisy and irrelevant features can be eliminated by running some detection models like SF- 5NN and SUS-5NN using only selected features. A combination of two detection engines(SF-KNN,SUS-KNN) based on best selected features and K-NN algorithm was proposed, that was much better(notably in detecting attacks like U2R, R2L) than approaches like traditional 5-NN, C4.5,C5. Experimentally, engines gave classification rates of 92.56%, 92.84% and false positive rates 2% and 4.52% respectively. Dayu Yang et al [8] introduced a method to apply Auto Associative Kernel Regression (AAKR) empirical modeling and the SPRT for SCADA system intrusion detection. In detecting anomalous behavior, this model is limited by two requirements - different indicators for different intrusion methods and managing a number of highly valuable variables identifying the optimal set of indicators for known and potential abnormalities is the future of this research.



Layer	Protocols / Techniques for Anomaly Detection	Use	Overhead	Drawbacks
Physical	RSSI value	Detects masquerade	Calibration of RSSI value for each neighbour	Large number of false positives
MAC	TDMA: Check if adversary follows TDMA Schedule	Detects masquerade	Keep track of TDMA Schedule of other nodes	None
	S-MAC: Check if sender is supposed to be sleeping	Detects masquerade	Keep track of sleep-wake of schedule of other nodes	None
Routing	For any routing protocol, check if neighbour and the expected information matches	Guarantees information authentication	Constructiong ADTs. Updating previous hop in a packet	None
Application	Use triangulation to detect intrusions	Detects masquerade	Nodes always have to listen	Overhearing
	Round trip time	Detects masquerade	Precise calibration of range of round trip time for each neighbour	Large number of false positives

IV Proposed Approach

` In this approach we are doing in two modules in first we are capturing the packets from systems those are connected in LAN such as WINCAP, JPCAP etc then in second module we are applying the anomaly based and signature based approach to detect abnormal packets(Intruders) from LAN.

References

[1] N. I. of Standards & Technology, An Introduction to Computer Security: The NIST Handbook, NIST, Ed. U.S. Department of Commerce, 2006.

[2] J. Grossklags, N. Christin, and J. Chuang, "Security and insurance management in networks with heterogeneous agents," in 9th ACM conference on Electronic commerce. New York, NY, USA: ACM, 2008, pp. 160-169.

[3] K. Labib, "Computer security and intrusion detection," Crossroads, vol. 11, no. 1, pp. 2-2, 2004.

[4] K. Ingham and S. Forrest, "A history and survey of network firewalls," University of New Mexico, Tech. Rep., 2002.

[5] R. Bace and P. Mell, "Nist special publication on intrusion detection systems," National Institute of Standards and Technology, Tech. Rep., 2001.

[6] M. T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," SIGMIS Database, vol. 38, no. 1, pp. 60-80, 2007.

[7] J. Graves, W. J. Buchanan, L. Saliou, and J. L. Old, "Performance analysis of network based forensic systems for in-line and out-of-line detection and logging," in 5th European Conference on Information Warfare and Security (ECIW), 2006.

[8] J. Hale and P. Brusil, "Secur(e/ity) management: A continuing uphill climb," J. Netw. Syst. Manage., vol. 15, no. 4, pp. 525-553, 2007.

[9] W. H. Baker and L. Wallace, "Is information security under control?: Investigating quality in information security management," IEEE Security and Privacy, vol. 5, no. 1, pp. 36-44, 2007.

[10] P. Fung, L. for Kwok, and D. Longley, "Electronic information security documentation," in ACSW Frontiers '03: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2003, pp. 25-31.

[11] J. Morrison, "Blaster revisited," Queue, vol. 2, no. 4, pp. 34-43, 2004.

[12] C. Miller, "The legitimate vulnerability market," in 6th Workshop on the Economics of Information Security, The Heinz School and CyLab at Carnegie Mellon University Pittsburgh, PA, USA, June 7- 8 2007.

[13] S. Peisert, M. Bishop, and K. Marzullo, "Computer forensics in forensis," SIGOPS Operating Systems Review, vol. 42, no. 3, pp. 112-122, 2008.

[14] S. Perry, "Network forensics and the inside job," Network Security, vol. 2006, pp. 11-13, 2006.

[15] D. K. Smetters and R. E. Grinter, "Moving from the design of usable security technologies to the design of useful secure applications," in Proceedings of the 2002 workshop on New security paradigms. New York, NY, USA: ACM, 2002, pp. 82-89.

[16] B. Woloch, "New dynamic threats require new thinking - "moving beyond compliance"," Computer law & security report, vol. 22, pp. 150 - 156, 2006.

[17] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, B. Fisher, and B. Fisher, "Towards understanding it security professionals and their tools," in SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security. New York, NY, USA: ACM, 2007, pp. 100-111.

[18] R. C. Newman, "Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities," in InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development. New York, NY, USA: ACM, 2006, pp. 68-78.

[19] Z.-Q. Wang, H.-Q. Wang, Q. Zhao, and R.-J. Zhang, "Research on distributed intrusion detection system," in 2006 International Conference on Machine Learning and Cybernetics, 2006.

[20] K. Buzzard, "Computer security - what should you spend your money on?" Computers & Security, vol. 18, pp. 322 - 334, 1999.

[21] S. M. Furnell and M. J. Warren, "Computer hacking and cyber terrorism: The real threats in the new millennium?" Computers & Security, vol. 18, pp. 28 - 34, 1999.

[22] S. Furnell and M. Papadaki, "Testing our defences or defending our tests: the obstacles to performing security assessment references," Computer Fraud and Security, vol. 1, pp. 8 - 12, 2008.

[23] C. Gates and C. Taylor, "Challenging the anomaly detection paradigm: a provocative discussion," in 2006 workshop on New security paradigms. New York, NY, USA: ACM, 2007, pp. 21-29.

[24] L. A. Hughes and G. J. Delone, "Viruses, worms, and trojan horses: Serious crimes, nuisance, or both?" Soc. Sci. Comput. Rev., vol. 25, no. 1, pp. 78-98, 2007.

[25] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A taxonomy ofcomputer worms," in WORM ’03: Proceedings of the 2003 ACM workshop on Rapid malcode. New York, NY, USA: ACM, 2003, pp. 11-18.