ARTIFICIAL INTELLIGENCE TECHNIQUES IN INTRUSION DETECTION

Rasim M. Alguliev, Yadigar N. Imamverdiev

Azerbaijan National Academy of Sciences, Information-Telecommunication Scientific Centre, F.Agayev str., 9, Baku, AZERBAIJAN, ramiz@dcacs.ab.az

ABSTRACT

There is currently need for an up-to-date and thorough survey of the intrusion detection techniques. This paper presents a survey of artificial intelligence methods in the field computer and network security.

1. INTRODUCTION

This paper is a survey of artificial intelligence techniques in the intrusion detection domain. Some of the previous surveys of the field are [14, 30]. Summaries of the research areas covered in the intrusion detection techniques field are given by Lunt [30], who characterizes techniques as including expert systems, statistical detectors, neural networks, and model-based reasoning systems, and by Kumar, [21] who itemizes expert systems, model-based reasoning, state-transition analysis, and keystroke monitoring. Detection techniques are used to detect unusual behaviors, deviations from known-good behaviors, and known-bad behaviors. Several other summaries are also available [3, 6]. Most of these summaries are somewhat dated, and/or superficial, and the growing number of people taking interest in the field computer and network security calls for an up-to-date and thorough survey of the field. This paper presents such a survey.

Intrusion detection systems (IDSs) play an important role in achieving security of information systems. The goal of intrusion detection systems is to identify malicious behavior at different levels of granularity. The early intrusion detection research efforts realized the inefficiency of any approach that required a manual review of a system audit trail.

An intrusion can be defined as "any set of actions that attempt to compromise the integrity, confidentiality or availability" [16]. Intrusion detection is the process of identifying unauthorized usage of a computer system. The elements central to intrusion detection are: *resources* to be protected in a target system, i.e., user accounts, file systems, system kernels, etc; *models* that characterize the "normal" or "legitimate" behavior of these resources; *techniques* that compare the actual system activities with the established models, and identify those that are "abnormal" or "intrusive" [28].

There are many classification schemes of intrusions. In [5] Anderson presents a threat model that classifies threats as external penetrations, internal penetrations, and misfeasance and uses this classification to develop a security monitoring surveillance system based on detecting anomalies in user behavior. Another classification scheme presented by Smaha [37] provides a grouping of intrusions based on the end effect and the method of carrying out the intrusions. Intrusions can be categorized into two main classes based on their method of detection:

1. **Misuse intrusions** follow well-defined patterns of attack, that exploit weaknesses in system and application software. Such patterns can be precisely written in advance.
2. **Anomaly intrusions** are based on observations of deviations from normal system usage patterns. If the observed activity of a user deviates from the expected behavior, an anomaly is said to occur. For example, if user X only uses the computer from his office between 9 A.M. and 5 P.M., an activity on his account late in the night is anomalous and hence, might be an intrusion.

2. ANOMALY DETECTION VERSUS MISUSE DETECTION

The early research uncovered several features of the two main approaches, anomaly based and signature based intrusion detection.

Misuse detection systems encode intrusion signatures or scenarios and scan for occurrences of these, which requires prior knowledge of the nature of the intrusions. The most significant advantage of misuse detection approaches is that known attacks can be detected fairly reliably and with a low false positive rate. Misuse detection models can only detect known attacks and their slight variations. The key drawback of misuse detection approaches is that they cannot detect novel attacks against systems that leave different signatures. Therefore, the hope of providing effective defense against new attacks lies in anomaly detection models. Misuse detection is harder to automate since it requires applying many rules (as in NIDES [4]) or searching for many patterns (as in [22] and [36]); anomaly detection just requires calculating statistics and comparing them to norms.

In anomaly detection systems, it is assumed that the nature of the intrusions is unknown, but that the intrusion will result in behavior different from that normally seen in the system. Anomaly detection traditionally assumes that one can establish normal behavior patterns over time and use these patterns as profiles of normal system activity. The main difficulties of these systems are: intuition and experience is relied upon in selecting the system features, which can vary greatly among different computing environments; some intrusions can only be detected by studying the sequential interrelation between events because each event alone may fit the profiles; it may not be able to describe what the attack is and may have inability to identify the specific type of attack that is occurring. However, probably the most significant disadvantage of anomaly detection approaches is the high rates of false alarm. The anomaly detection tool does not really report intrusions but rather anomalous behavior. It is likely that non-intrusive behavior that falls outside the normal range will also be labeled as an intrusion. Another disadvantage is that the implementation can become computationally ineffective.

Few articles focus on the problems and limitations of anomaly detection. Helman and Liepins [17] made an attempt to quantify the powers and limitations of anomaly detection by creating a formal model for the detection process. Several papers describe approaches that address one or more problems, e.g. Warrender et al. [40] address the false alarm rate problem and Lane and Brodley [26] discuss both the false alarm rate problem and time to detection problem.

It was suggested [1, 31] that the two complimentary approaches of seeking anomalous activity should be employed in the same intrusion detection system, to better complement the relative strengths and weaknesses of the two approaches.

3. A Generic Intrusion Detection Model .

Many misuse and anomaly IDSs are based on generic intrusion detection model proposed by Denning [11].This paper was the first to propose the concept of intrusion detection as a solution to the problem of providing a sense of security in computer systems. This model is independent of the platform, system vulnerability, and type of intrusion. This model works as a rule based pattern matching system, which includes the following components: subjects, objects, audit records, profiles, anomaly records, activity rules. The task here is to develop a model or profile of the normal working state of a subject (e.g., user, file, privileged program, host machine and network) and to detect anomalous conditions as deviations from expected behaviors. A profile is the "signature or description of normal activity" of a subject or a group of subjects concerning an object or a group of objects. Behavior profiles may be built by performing statistical analysis on historical data [17], or by using rule-based approaches to specify behavior in terms of predictive pattern generation [22] or using state transition analysis [19]. Several statistical models are used to measure how anomalous the behavior is. Examples include the mean and standard deviation model, Markov process model, and time serial model. An activity rule describes what action will be taken under some conditions.

4. Some Shortcomings of Current intrusion Detection Systems

Jansen at al. [20] identify a number of functional and performance requirements for an intrusion detection system, but in general, intrusion detection system should continuously monitor network behavior, be fault tolerant (since it too may be the target of attack), be capable improving its detection capability by adapting to changes and receiving updated attack signatures, and accurately (i.e., with low false alarm rate) report anomalies or possible intrusions, supplying adequate information to deal with an intrusion. One of the most important characteristics for an intrusion detection system is its efficiency. An efficient intrusion detection system is able to correctly predict an attack as well as correctly recognize a normal operation. A difficult problem in anomaly intrusion detection is determining the correspondence between anomalous activity and intrusive activity. Two quantitative measurements are generally used to evaluate the efficiency of an intrusion detection system: a false positive rate and a false negative rate [21, 2]. A false positive rate is error rate when an intrusion detection system wrongly predicts normal behavior as an abnormal attack. Similarly, the false negative rate is error rate when an intrusion detection system marks an intrusion as a legal operation. A high false positive rate will seriously affect the performance of the system being detected. A high false negative rate will leave the system vulnerable to intrusions. When false negatives are not desirable, thresholds that define an anomaly are set low. This results in many false positives and detracts from the efficacy of automated mechanisms for intrusion detection.

Intrusion detection system must resist subversion. A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur. An intruder could use knowledge about the internals of an intrusion detection system to alter its operation, possibly allowing anomalous behavior to proceed. The intruder could then violate the systems operational security constraints. Another form of subversion error is fooling the system over time. Intruders may take some actions over a period of time. Each of these actions looks legal and safe if taken separately, but the sequence of these actions will compose a malicious intrusion. Intrusion detection system should have enough flexibility to generalize patterns, even over a period of time.

5. Research Issues in Intrusion Detection

Issues in ID research include data collection, data reduction, feature selection are problems behavior classification, reporting and response [14]. Many research labs: UC Davis Seclab, Purdue CERIAS/COAST, SRI, IBM Zurich GSAL, MIT Lincoln Labs, Columbia JAM, U. Idaho, NSWC, UNM, etc. and many DARPA sponsored projects devoted to intrusion detection research. The following advanced methods and techniques are being investigated by the intrusion detection research community:

- Cooperating detectors
- Statistical anomaly detection
- Machine learning
- Meta learning
- Computational immunology
- Quantitative evaluation of effectiveness
- Model-based detection
- Graphical detection
- Specification-based detection
- Thumbprint technique
- Software agents for intrusion detection
- Network and system instrumentation
- Network monitoring
- Signaling infrastructure detection
- Detection in high-speed networks
- Automated response
- Survivable active networks
- Planning and procedural reasoning

Data reduction consists of analyzing a collection of data in order to identify the most important components of the data, thereby reducing processing time, communication overhead and storage requirements. Different behavioral characteristics will generate different amounts of data. For example, an average user generates between 3-35 MB of audit data per day [14]. Data reduction is critical as the size of the profile impacts the time required for classification, as well as RAM and drive space overhead. [26] describe instance clustering approaches to the data reduction task. Empirically examined the data reduction performance of two clustering methods-an EM procedure K-centers and a greedy clustering technique based on a sequential selection of clusters.

It is often difficult to know which items from an audit trail will provide the most useful information for detecting intrusions. Determining the right measures is complicated because the appropriate subset of measures depends on the types of intrusions being detected. One set of measures will not likely be adequate for all types of intrusions. The process of determining which items are most useful is called feature selection in the machine learning literature. The set of optimal measures for detecting intrusions must be determined dynamically for best results. Genetic algorithms [16], neural networks [14] have been used for selection the most effective set of features for particular types of intrusions. For a survey of other feature selection techniques see [12].

Classification is the process of identifying attackers and intruders. In the simplest case, this is a binary decision problem. The data is classified as either normal (acceptable) or anomalous (and possibly intrusive). Data classification can be more complex, for instance, trying to identify the particular type of intrusion associated with anomalous behavior. AI techniques can be used to perform these important tasks.

6. Artificial Intelligence and Intrusion Detection Methods

Artificial Intelligence (AI) techniques have been around for many years now. They have been applied with varying degrees of success to a wide variety of problems. However, it is important to understand that AI is a very wide field that encompasses a diverse range of technologies and techniques. Artificial intelligence (AI) techniques have played an important role in both misuse detection and anomaly detection. The methods reported in the literature include rule based systems, neural networks, genetic algorithms, and data mining methods such as association rules and frequency episodes. AI techniques such as rule-based and feature-based classifiers can examine system activities to evaluate their legitimacy. Such systems can generalize from the data and adapt to evolving environments. Approaches include pattern-matching systems (expert systems, rule/model systems) and trained classifiers (decision trees, Bayesian classifiers, and neural networks) [14].

6.1. Machine Learning

Intrusion detection systems that are trained on system usage metrics use inductive learning algorithms. To simulate this learning process using a computer model is otherwise known as machine learning. Machine learning can be viewed as the attempt to build computer programs that improve performance of some task through learning and experience. The most commonly applied theory in many machine learning models is pattern classification.

In [23, 25] presented a machine learning approach to anomaly detection. Their system learn valid user profiles based on command sequences and compares current input sequences to the profile using a similarity measure. The system must learn to classify current behavior as consistent or anomalous with past behavior using only positive examples of the account's valid user. Empirical results demonstrate that this is a promising approach to distinguishing the legitimate user from an intruder.

This learning task possesses a number of difficulties not faced by traditional, static learning tasks and presents a number of research issues for both the machine learning and computer security communities, among which are learning from examples from only a single class, learning from discrete, non-metric time sequence data, online learning, and learning in the presence of concept drift [24].

Lee and others [28] adapted RIPPER to anomaly detection by using it to learn rules to predict system calls within short sequences of program traces. RIPPER – Repeated Incremental Pruning To produce Error Reduction – is a rule learning system developed by William Cohen [8]. It, like other rule learning systems, is typically used for classification problems.

6.2. Rule-Based Expert Systems

Rule-based expert systems have served as the basis for several systems including SRI's IDES (Intrusion Detection Expert System) [31], LANL's NADIR (Network Anomaly Detection and Intrusion Reporter) [34]. This systems encode an expert's knowledge of known patterns of attack and system vulnerabilities as production rules in the form if-then-else. A rule-based expert system will also facilitate the process of pattern matching. The efficiency of pattern matching is one of the most remarkable advantages for a rule-based expert system. The main disadvantage for a rule-based expert system is its "direct dependency" on audit data. An intrusion that deviates only slightly from a pattern derived from the audit data may not be detected or a small change in normal behavior may cause a false alarm. The acquisition of rules is a tedious and error prone process. This problem has generated a great deal of interest in the application of machine learning techniques to automate the process of learning the patterns. [29] describes an expert system development toolset called the Production-Based Expert System Toolset (P-BEST) and how it is employed in the development of a modern generic signature-analysis engine for computer and network misuse detection. For more than a decade, earlier versions of P-BEST have been used in intrusion detection research and in the development of some of the most well known intrusion detection systems.

6.3. Pattern Matching

Misuse Intrusion Detection has traditionally been understood in the literature as the detection of specific, precisely representable techniques of computer system abuse. Pattern matching is well disposed to the representation and detection of such abuse. Each specific method of abuse can be represented as a pattern and many of these can be matched simultaneously against the audit logs generated by the OS kernel. Using relatively high level patterns to specify computer system abuse relieves the pattern writer from having to understand and encode the intricacies of pattern matching into a misuse detector. Patterns represent a declarative way of specifying what needs to be detected, instead of specifying how it should be detected. [22] have devised a model of matching based on Colored Petri Nets specifically targeted fòr misuse intrusion detection. This paper presents a software architecture for structuring a pattern matching solution to misuse intrusion detection. In the context of an object oriented prototype implementation authors describe the abstract classes encapsulating generic functionality and the inter-relationships between the classes.

6.4. Neural Networks

Neural Networks in many ways better suits the demands and dynamic nature of the intrusion detection problem. Neural Networks have the ability to learn from an environment by applying an iterative process of adjustments to their internal structure. Neural Networks provide a robust approach to pattern learning and recognition that can model, generalize about, and classify many different types of input data where the exact nature of the input data is not known. An outstanding advantage of artificial Neural Networks is that they are highly tolerant of noisy data. Even an incomplete or inaccurate audit record will not prevent a neural network from detecting intrusions [7]. Neural Networks have been proposed as alternatives to the statistical analysis component of intrusion detection systems. The research group at SRI has experimented with the use of Neural Networks for intrusion detection [30]. Several IDSs that employ Neural Networks for on-line intrusion detection have been proposed in [10, 13, 39]. These systems learn to predict the next command based on a sequence of previous commands by a specific user. The neural network is trained on a set of representative command sequences of a user. The input to the net consists of the current command and the past *w* commands, where *w* is the size of the window of past commands. The output layer of the neural network conceptually consists of a single multi-level output that predicts the next command to be issued by the user. A multi layered feed forward network is used to capture program behavior patterns [15].

Neural Networks have also been proposed for use in the detection of computer viruses [10]. In [7] have been discussed the applicability of Neural Networks to the problem of misuse detection. For this experiment the specific type of neural net that was used was a Multi-Layer Perceptron.

Some disadvantages of this approaches are [7, 21]:

1. The topology and the weights assigned to each element of the net are determined only after considerable trial and error;
2. The size of the window is an important parameter: If *w* is too small, there will be many false positives; if it is set too high, the net will suffer from irrelevant data.

Some advantages of this approaches are [7, 21]:

1. The success of this approach does not depend on any statistical assumptions about the nature of the underlying data.
2. Neural Networks are highly tolerant of noisy data. Even an incomplete or inaccurate audit record will not prevent a neural network from detecting intrusions .
3. Neural Networks can automatically account for correlations between various measures that affect the output.

6.5. Data Mining

Data mining is extracting previously unknown, valid and actionable information from large databases [38]. The recent rapid development in data mining has made available a wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and database. Audit data can be formatted into a database table where each row is an audit record and each column is a field (system feature) of the audit records. Many recent approaches to intrusion detection have applied data mining techniques. These approaches build detection models by applying data mining algorithms to large data sets of audit data collected by a system. These models have been empirically proven to be very effective [28]. Two data mining methods, association rules and frequency episodes, have been proposed to mine audit data to find normal patterns for anomaly intrusion detection. An association rule specifies the correlation among different features. Agrawal and Srikant [38] have presented some fast algorithms to mine association rules, including algorithm Apriori. Mannila and Toivonen [33] have proposed an algorithm to discover simple serial frequency episodes from event sequences based on minimal occurrences. This algorithm can be used to discover inter-audit patterns. Lee, Stolfo and Mok [27, 28] have applied this method to the problem of characterizing frequent temporal patterns in audit data. A notable feature of the intrusion detection based on data mining is the support it offers for gathering and operating on data and knowledge sources from the entire observed system. However, one major drawback of data mining based approaches is that the data required for training is very expensive to produce. The mined rules or episodes are at the data level. This immediate dependency on data may limit the flexibility of intrusion detection.

Since many current IDSs are constructed by manual encoding of expert security knowledge, changes to IDSs are expensive and slow. In [28] a data mining framework proposed for adaptively building intrusion detection models. The central ideas are to utilize auditing programs to extract consistent and useful patterns of program and user behavior, and apply data mining programs to learn rules that accurately capture the behavior of intrusions and normal activities. These rules can then be used for misuse detection and anomaly detection. They proposed to use the association rules and frequent episodes computed from audit data as the basis for guiding the audit data gathering and feature selection process.

6.6. Fuzzy Logic

The advantage of using fuzzy logic is that it allows one to represent concepts that could be considered to be in more than one category (or from another point of view it allows representation of overlapping categories). There are two main reasons to introduce fuzzy logic for intrusion detection. First, many quantitative features are involved in intrusion detection can potentially viewed as fuzzy variables. The second reason to introduce fuzzy logic for intrusion detection is that security itself includes fuzziness. When using fuzzy logic, it is often difficult for an expert to provide "good" definitions for the membership functions for the fuzzy variables.

Luo have investigated [32] the integration of fuzzy logic with association rules and frequency episodes. The integration with fuzzy logic can produce more abstract and flexible patterns for intrusion detection, since many quantitative features are involved in intrusion detection and security itself is fuzzy. In experiments have been conducted to examine the utility of applying fuzzy association rules and fuzzy episode rules for off-line anomaly detection and real-time intrusion detection. Fuzzy association rules and fuzzy frequency episodes have used to extract patterns for temporal statistical measurements at a higher level than the data level. They have defined a modified similarity evaluation function which is continuous and monotonic for the application of fuzzy association rules and fuzzy frequency episodes in anomaly detection.

Recently, researchers started investigating techniques like artificial intelligence [18], autonomous agents [9], and mobile agent [20] architectures for detecting intrusions in network environment. Mark Crosbie and Gene Spafford [9] suggested the use of autonomous agents in order to improve the scalability, maintainability, efficiency and fault tolerance of an IDS. This idea fit well with the ongoing research on software agents in other areas of computer science.

Most recent work in the area of intrusion and anomaly detection has focused on architectures for the integration of multiple sensors. For example, EMERALD [35] combine the decisions of groups of highly specific base level sensors via a hierarchial decision-making process to yield a top level overview of the integrity of the monitored system. This type of approach is analogous to meta-learning schemes which boost the performance of multiple base-level "weak" learners through adaptive combination.

7. Conclusion

Anomaly detection methods were closely studied in the early 1980s and have since been used in some prototypes and products. Over the past twenty years, with particular emphasis during the last five, many intrusion detection techniques have been developed. Most of the available methods, however, were designed for specific applications, and each has its own idiosyncrasies. None of the intrusion detection approaches is sufficient alone- each addresses a different threat. A successful intrusion detection system should incorporate several of them. If we know the specific advantages and disadvantages of the different intrusion detection methods, we combine them more effectively and avoid using them for purposes for which they are not well suited. The unique advantage of anomaly detection may be utilized if it is complemented with other methods in order to cover its weaknesses.

REFERENCES

[1] Alguliev, R.M., About one algorithm of finding threats in accessing in a corporative network, *Izvestiya AS Azerbaijan*, Ser. of physics-technics and mathematics sciences, 6(1998), pp. 213-216.

[2] Alguliev, R.M., Theoretic-game model of acceptance of decisions by Seurity Administrator in struggle with threats in a corporative networks, *Reports of AS Azerbaijan*, 3-4 vol. LV (1999), pp.54-60.

[3] Alguliev R.M., Threats to corporative networks and formalization of it's relation with security mechanism, Review information, Ser. of Mejotraslevaya, Baku, Az Ssi STI, 2000

[4] Anderson D., T. Frivold, A.Valdes, Next-generation Intrusion Detection Expert System (NIDES): A Summary, SRI International Technical Report SRI-CSL-95-07.

[5] Anderson J. P.. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.

[6] Axelsson S., Research in Intrusion-Detection systems: A Survey. Technical Report 98-17, Department of Computer Engineering Chalmers University of Technology, SE-412 96 Gooteborg, Sweden, Dec. 1998. URL:http://www.ce.chalmers.se/sta /sax.

[7] Cannady J., Artificial neural networks for misuse detection. In Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), pages 443-456, October 5-8 1998. Arlington, VA.

[8] Cohen W.W., Fast effective rule induction. In Machine Learning: Proceedings of the 12th International Conference. Morgan Kaufmann, 1995.

[9] Crosbie, M., and Spafford E., Active Defense of a Computer System using Autonomous Agents. In Proceedings of the 18th National Information Systems Security Conference, pages 549-558, October 1995.

[10] Debar H., Becker M., and Siboni, D., A neural network component for an intrusion detection system. In Proc. *IEEE Symposium on Security and Privacy*, pages 240--250, Oakland, CA, 1992.

[11] Denning D., An Intrusion-Detection Model. – *IEEE Transactions on Software Engineering*, SE-13, No. 2, pp. 222-232. , February 1987

[12] Doak J., Intrusion detection: The Application of Feature Selection – A Comparison of Algorithms, and the Application of a Wide Area Network Analyzer. *Master's Thesis, Department of Computer Science, University of California*, Davis, 1992.

[13] Fox K.L., R.R. Henning, J.H. Reed, and R.P. Simonian. A neural network approach towards intrusion detection. In Proceedings of *the 13th National Computer Security Conference*, pages 125-134, Washington, D.C., October 1990.

[14] Frank, J. Artificial intelligence and intrusion detection: Current and future directions. In Proceedings of *the 17th National Computer Security Conference*, October 1994.

[15] Ghosh, A. K., Schwartzbard A., and Schatz M., Learning program behavior profiles for intrusion detection. In Proceedings of *the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, California, April , 1999.

[16] Heady, R., Luger, G., Macabe, A., and Servilla, M. The architecture of a network level intrusion detection system, *Technical Report CS90-20*, Department of Computer Science, University of New Mexico, Aug. 1990.

[17] Helman P., Liepins G., Statistical foundations of audit trail analysis for the detection of computer misuse, *IEEE Trans. on Software Engineering*, 19 (9) (1993) 886-901.

[18] Helmer, G.G., Wong, J.S.K., Honavar, V., Miller, L. Intelligent Agents for Intrusion Detection, Proceedings of *the IEEE Information Technology Conference*, Syracuse, NY, pp. 121-124, September 1998.

[19] Ilgun K., Kemmerer R.A., and Porras P.A.. State transition analysis: A rule-based intrusion detection system. *IEEE Transactions on Software Engineering*, 21(3), March 1995.

[20] Jansen, W., P. Mell, T. Karygiannis, and D. Marks, Mobile Agents in Intrusion Detection and Response. Proceedings of *the 12th Annual Canadian Information Technology Security Symposium*, Ottawa, Canada, June 2000.

[21] Kumar, S. Classification and Detection of Computer Intrusions. PhD thesis, Purdue University, West Lafayette, IN 47907, 1995.

[22] Kumar S., Spafford E., A Pattern Matching Model for Misuse Intrusion Detection, in: Proceedings of *the 17th National Computer Security Conference*, 1994, pp.11-21.

[23] Lane, T. and Brodley, C. E. Detecting the Abnormal: Machine Learning in Computer Security. Available as Technical Report ECE-97-1, January 1997, Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907.

[24] Lane, T, and Brodley, C. E. Sequence Matching and Learning in Anomaly Detection for Computer Security. In Proceedings of *the AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management*, pp 43-49. 1997.

[25] Lane, T, and Brodley, C. E. An Application of Machine Learning to Anomaly Detection. *20th Annual National Information Systems Security Conference*, vol 1, pp 366-380. 1997.

[26] T. Lane, and C. E. Brodley. Data Reduction Techniques for Instance-Based Learning from Human/Computer Interface Data Proceedings of *the 17th International Conference on Machine Learning*, pp. 519-526. 2000.

[27] Lee W., Stolfo S. J., and Mok K. W., Mining Audit Data to Build Intrusion Detection Models, In Proceedings of *the Fourth International Conference on Knowledge Discovery and Data Mining (KDD '98)*, New York, NY, August 1998

[28] Lee W., Stolfo S. J., and Mok K. W., A data mining framework for building intrusion detection models. In Proceedings of *the IEEE Symposium on Security and Privacy, 1999.*

[29] Lindqvist, U., and Porras P. A., Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST), Proceedings of *the 1999 IEEE Symposium on Security and Privacy*, Oakland, CA, May 9-12, 1999.

[30] Lunt T., A survey of intrusion-detection techniques. *Computers and Security*, 12, 4 (June 1993), 405-418.

[31] Lunt, T.F.,IDES: an intelligent system for detecting intruders. In Proceedings of *the Symposium: Computer Security, Threat and Countermeasures*, November 1990. Rome, Italy.

[32] Luo, J., Integrating fuzzy logic with data mining methods for intrusion detection. M.S. Thesis, Mississipi State University, 1999.

[33] Mannila, H., and Toivonen H., Discovering generalized episodes using minimal occurrences. In Proceedings of *the 2nd Conference on Knowledge Discovery and Data Mining*, Portland, Oregon, August, 1996, by AAAI Press 146-151.

[34] Mukherjee B., Heberlein L. T., and Levitt K. N., Network intrusion detection. *IEEE Network*, 8(3):26-41, May/June 1994.

[35] Porras P.A., and Neumann P.G., EMERALD: Event monitoring enabling responses to anomalous live disturbances. In Proceedings of *the 20th National Information Systems Security Conference*, pages 353-365, October 1997.

[36] Shieh, S., and Gligor V., A pattern-oriented intrusion-detection model and its applications. *Symposium on Security and Privacy*, Oakland, CA, May 1991, 327-342.

[37] Smaha S. E., Haystack: An intrusion detection system. *In Fourth Aerospace Computer Security Applications Conference*, pages 37-44, Tracor Applied Science Inc., Austin, Texas, December 1988.

[38] Srikant, R. and Agrawal, R. Mining generalized association rules. In Proceedings of *the 21st VLDB Conference,* Zurich, Switzerland, 1995.

[39] Tan K., The application of neural networks to UNIX computer security, in: Proceedings of *the IEEE International Conference on Neural Networks*, vol.1 (1995) pp.476-481.

[40] C. Warrander, S. Forrest, and B. Pearlmutter. Detecting intrusions using system calls: alternative data models. In *1999 IEEE Symposium on Security and Privacy*, pages 133-145, IEEE Computer Sosiety, 1999