Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining

Harjit Singh, Steven Furnell, Benn Lines and Paul Dowland

Network Research Group, Department of Communication and Electronic Engineering,
University of Plymouth, Drake Circus, PLA 8AA, United Kingdom
{hsingh, sfurnell, blines, pdowland}@plymouth.ac.uk

Abstract. The continuous growth of computer networks, coupled with the increasing number of people relying upon information technology, has inevitably attracted both mischievous and malicious abusers. Such abuse may originate from both outside an organisation and from within, and will not necessarily be prevented by traditional authentication and access control mechanisms. Intrusion Detection Systems aim to overcome these weaknesses by continuously monitoring for signs of unauthorised activity. The techniques employed often involve the collection of vast amounts of auditing data to identify abnormalities against historical user behaviour profiles and known intrusion scenarios. The approach may be optimised using domain expertise to extract only the relevant information from the wealth available, but this can be time consuming and knowledge intensive. This paper examines the potential of Data Mining algorithms and techniques to automate the data analysis process and aid in the identification of system features and latent trends that could be used to profile user behaviour. It presents the results of a preliminary analysis and discusses the strategies used to capture and profile behavioural characteristics using data mining in the context of a conceptual Intrusion Monitoring System framework.

Keywords

Data Mining, Intrusion Detection Systems, Knowledge Discovery, Behavioural Profiling, Intelligent Data Analysis.

1 Introduction

The increasing reliance upon IT and networked systems in modern organisations can have a calamitous impact if someone deliberately sets out to misuse or abuse the system. Systems may be affected by internal and external categories of abuser, as a result of both mischief and malice, leading to a range of undesirable consequences for the affected organisations (e.g. disruption to activities, financial loss, legal liability and loss of business goodwill). A recent study conducted by the US Computer Security Institute (CSI), in collaboration with the FBI, reported that 70% of respondent organisations had detected unauthorised use of their computer systems in the previous 12 months [1] – which represented an 8% increase on previous findings from 1999. The level of reported incidents highlights the paucity of security measures in current systems and, hence, the need for more comprehensive and reliable approaches. In particular, it can be suggested that traditional user authentication and access controls (e.g. passwords and user/group-based file permissions) are not sufficient to prevent determined cases of abuse or re-occurrence, in the case of successfully breached account(s), and misuse occurring from a legitimate user. Having passed the frontline controls and having the appropriate access privileges, the user may be in the position to do virtually anything without being further challenged. However, appropriate monitoring and analysis of user activity within an active session may potentially reveal patterns that appear abnormal in relation to their typical behaviour, or which are compatible with the sign of recognised intrusion scenarios. It is from this perspective that many Intrusion Detection Systems (IDS) have been conceived. Various IDSs [2, 3] have been proposed, which generally can be categorised based on the data source, audit trails or network traffic data, and intrusion model employed, anomaly detection or misuse detection model. The approaches used are generally focused on providing continuous monitoring and involve analysing vast amounts of audit trails, which in an eight-hour period can amount to 3-35MB [4] of data generated.

There is an increasing need for a more coherent paradigm for audit processing in terms of automating the data analysis stages. The current trend of network components providing audit trail or audit logs provides the foundation for IDSs to explore database automated match and retrieval technologies. This can be seen in audit processor components for instance the SecureView in the Firewall-1 using Data Mart to store the audit trails [5]. This available information could be used for security audit trail analysis in IDSs by utilising the technology in the data analysis stages. The need to eliminate the manual and ad-hoc approaches in the data analysis stages in IDSs is attracting interest in applying Intelligent Data Analysis (IDA) techniques. In this paper is discussed the potential of Data Mining (DM) algorithms and techniques as an IDA tool. We use DM to automate the data analysis process in identifying system features and latent trends for classifying user behaviour from the collected audit trails. DM is a rapidly expanding field which, has been exploited in lucrative domains such as the financial [6] and communications [7] sectors. Although some reported work has been carried out to analyse network traffic data [8, 9], none has been carried out in analysing host-based audit trails using DM for the purpose of user authentication, which is the focus of this research work.

2 Data Mining

Data Mining can be described as a collection of techniques and methodologies used to explore vast amounts of data in order to find potentially useful, ultimately understandable patterns [10] and to discover relationships. DM is an iterative and interactive process, involving numerous steps with many decisions being made by the user. The fundamental goals of data mining are finding latent trends in data, which enable prediction and description [11] of the analysis phases. Different algorithms are optimised based on the predefined DM task. This involves deciding whether the goals of the DM process are classification, association, or sequential [10]. Classification has two distinct meanings. We may aim to classify new observations into classes from established rules or establishing the existence of classes, or clusters in data [12]. Association attempts to generate rules or discover correlation in data and is expressed: X => Y, where X and Y are sets of items. This means that an event or a transaction of a database that contains X tends to contain Y. Sequential looks at events occurring in a sequence over time or time-ordered sequences. This could be expressed through the following: for E ? N, E is a set of event types and an event is a pair (A, t), where A ? E is an event type and t represents the time of the event or occurrence of an event. This is followed by predefined sets of possible intrusion classes where, C is a set of intrusion classes and I ? C, I is an intrusion type, hence for example: 90% of the time, if the event (A, t) occurs, it is followed by intrusion type I. The subsequent process, once the DM task is defined can be derived from the four main activities; *selection*, *pre-processing*, *data mining and interpretation*, also known as post-processing [12].

3 Classification of User Behaviour

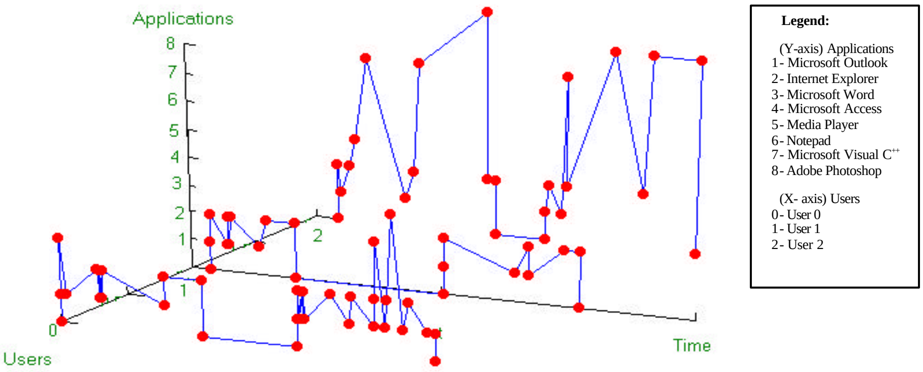


Figure 1. Graphical representation of applications run by users

Distinguishing user behaviour patterns and classifying it as normal or intrusive is a subtle task. Furthermore exploring the vast amount of audit trail data often yields a small fraction of intrusion or misuse. Besides managing these tasks, IDSs have to limit the errors that could occur from misclassification of user behaviour such as false positive or false negative errors. Therefore, it is essential to ensure that accurate profiles of users are established in order to improve the accuracy of intrusion classification. Hence the need to gather as much information as possible pertinent to a user's interaction with the system in order to distinguish between similar behavioural patterns of users that could occur. Auditing the applications that users run could for instance provide a distinctive pattern of the user's interaction with the system as depicted in ***Figure 1***. Users patterns once identified could be incorporated into an anomaly detector framework in conjunction with other key indicators of user behaviour in order to identify unauthorised access when compared against this distinctive usage patterns. Hence it is essential to collect as much information as possible regarding such behavioural indicators in order to correlate the possibility of intrusion.

4 Methodology

We use DM to extract latent patterns or models of user behaviour from the collected audit trail. This is then reflected in the DM algorithm classifiers (e.g. through rule induction) to recognise deviation, if it occurs, from normal use. This approach is based on the assumption that a user's behaviour has regularity and that using the classifiers this behaviour can be modelled. Using this analogy, anomalous behaviours can then be categorised as a possible unauthorised user or use of that system. The audit trail data analysed was collected from networked computers on a participating local area network (LAN) using an independent agent installed locally in order to audit user interaction with the system. This is based on the assumption that users performing their regular tasks will impose similarly regular demands upon system resources. Hence system features involved for continuous monitoring of user interaction with the system such as resource usage, process-related information such as creation, activation and termination, etc, is audited. Similar system features have been used in other published work [2]. However, previous work was focused on statistical and neural network analysis. A user's behaviour profile can be uniquely identified by: <user name, absolute time, date, hostname, $\text{event}_{1,\ldots,}$ event_n >, which is the semantic used for the audit trail where, $\textit{events}_{n,}$ denotes the system features being monitored.

4.1 Data Mining audit trail

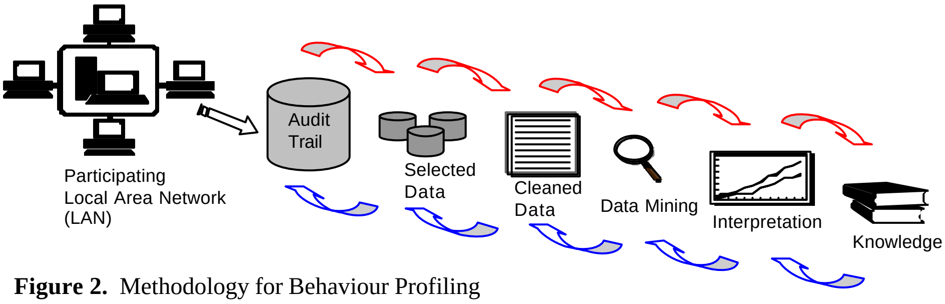
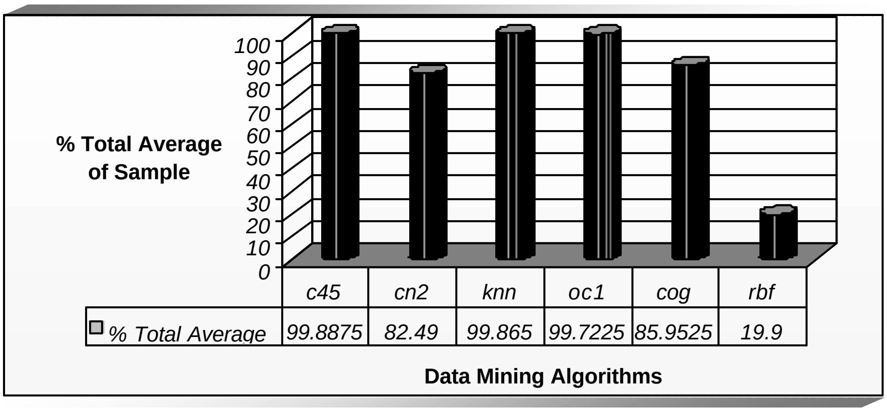


Figure 2. Methodology for Behaviour Profiling

The methodology used is derived from the four main activities of DM; selection, pre-processing, data mining and interpretation, and is as depicted in ***Figure 2.*** The collected audit trail is split into various sample sizes. These subsets form the target data sets, which will undergo the analysis to identify patterns and to tes t specific hypotheses. The cleaned data, containing both categorical and numerical data, is then subjected to analysis by the DM algorithms. There are a wide variety of DM techniques available, each of which performs more accurately over certain characteristic data sets (e.g. numerical or categorical) and is also relative to the number of variables or attributes and classes. The Intelligent Data Analysis (IDA) Data Mining Tool [13] is used to analyse the sample data sets which incorporates algorithms from the fields of Statistical, Machine Learning and Neural Networks. Six algorithms, k-NN, COG, C4.5, CN2, OC1 and RBF were chosen for this investigative work. For the purpose of this work, the data sets were split into ratios of 9:1, 8:2 and 7:3, hence into two parts, which is a commonly used technique known as train and test. The algorithm or classifier is subjected initially with the training set and then the classification accuracy is tested using the unseen data set or testing set. The results give an indication of the error rate (or false positives) and the overall classification accuracy of the trained algorithms.

5 Results

The initial results obtained from the analysis as depicted in ***Figure 3***, suggest that Machine Learning and Statistical-based algorithms are better for these types of data sets. C4.5 and OC1 decision tree based algorithms in particular, out performed the CN2 rule-based and RBF algorithms. The classification accuracy obtained, using k-NN in comparison to C4.5, shows some significance for further investigative work despite the slower classification times observed. Amongst the statistical algorithms, k-NN faired better then COG but is slower in comparison to the classification times observed. The classification accuracy obtained overall depicts RBF classification accuracy as inverse proportional to the sample sizes. These results support other reported work [12]. In addition to the consistency in classifying the data sets and the overall average classification accuracy, our initial investigations also identified that C4.5 has overall quicker train and test time and outputs explicit rules.



	c45	cn2	knn	oc1	cog	rbf
▢ % Total Average	99.8875	82.49	99.865	99.7225	85.9525	19.9

Figure 3. Total percentage average classification accuracy of selected Data Mining algorithms

6 Discussion and conclusion

The classification accuracy obtained suggests that DM techniques could be integrated into an IDS framework in order to provide a mechanism to detect intrusions. The approach used in these initial trials has shown the potential that DM techniques can be used to detect anomalies or intrusions through the behaviour model generated by the DM algorithm's classifiers. The high classification accuracy obtained and fast response time exhibited in classifying the user behaviour by some of the DM algorithms further demonstrates the potential of applying DM techniques within a real-time application for identifying intrusions [14]. Another important element identified is the interpreted rules obtained from the data mining process. The systems features outlined by the classifiers to detect anomalous behaviour can be used to detect known intrusions. The results so far have been based around the classifiers used that are optimised to classify either new observed user behaviour into classes from established rules or establishing the existence of classes using the DM algorithms. While this has been the fundamental goal in our approach, another important aspect of identifying user behaviour from frequent patterns developing over time has yet to be addressed.

References

1. Computer Security Institute, "2000 CSI/FBI Computer Crime and Security Survey", Vol. 6, No.1, SPRING-2000.
2. T.F. Lunt, "IDES: an intelligent system for detecting intruders", Proc. of the Computer Security, Threat and Countermeasures Symposium, November 1990 Rome, Italy.
3. B. Mukherjee, L.T. Herberlein and K.N. Levitt "Network Intrusion Detection", IEEE Network-1994, Vol. 8, No. 3, 26-41.
4. J. Frank, "Artificial Intelligence and Intrusion Detection: current and future direction", Proc. of the 17th National Computer Security Conference, October 1994.
5. E.G. Amoroso, "Intrusion Detection: an introduction to internet surveillance, correlation, traps, trace back, and response", Intrusion.Net-1999, ISBN 0-9666700-7-8.
6. C. Westphal and T. Blaxton, "Data Mining Solution, Methods and Tools for Solving Real-World Problems", Wiley-1998, ISBN 0-471-25384-7, 531-585.
7. R. Sasisekharan and V. Seshadri, "Data Mining and Forecasting in Large-Scale Telecommunications Networks", IEEE Expert Intelligent Sy stems and Their Applications-1996, Vol.11, No.1, 37-43.
8. W. Lee and S. Stolfo, "Data Mining Approaches for Intrusion detection", Proc. 7th USENIX Security Symposium, 1998.
9. C. Warrender, S. Forrest, B. Pearlmutter, "Detecting Intrusion Using Calls: alternative data models", Symposium on Security and Privacy, 1999.
10. U. M. Fayyad, "Data Mining and Knowledge Discovery: making sense out of data", IEEE Expert-1996, Vol.11, No.6, 20-25.
11. P Adriaans and D. Zantinge, "Data Mining", Addison-Wesley-1998 , ISBN 0-201-40380-3.
12. D. Michie, D.J. Spiegelhalter and C.C. Taylor, "Machine Learning, Neural and Statistical Classification", Ellis Horwood-1994, ISBN 0-13-106360-X, 136-141.
13. H. Singh, K.E. Burn-Thornton and P.D. Bull, "Classification of Network State Using Data Mining", Proc. of the 4th IEEE MICC & ISCE '99,Malacca, Malaysia, Vol.1, 183-187.
14. S.M. Furnell and P.S. Dowland, "A Conceptual Architecture for Real-time Intrusion Monitoring", Information Management & Computer Security-2000, Vol. 8, No. 2, 65-74.