29

An attack detection system for secure computer systems - Design of the ADS

I. Kantzavelou and A. Patel
Computer Networks and Distributed Systems Research Group
Department of Computer Science, University College Dublin
Belfield, Dublin 4, Ireland, tel. +353-1-7062476, fax +353-1-2697262, ioanna@teia.ariadne-t.gr, apatel@ccvax.ucd.ie

Abstract

Attack Detection Systems for secure computer systems are an approach to enhancing the security of a computer system. In the past, they aimed at only providing a trail which could be useful in determining how a system was breached and who was responsible for this breach. More recently, attack detection systems have become automated tools which analyse audit data captured from a system, detect attacks as they take place and take measures to prevent further damage to the target system. The Attack Detection System (ADS) discussed in this paper is a real-time attack detection system which allocates points to users who are attempting to attack the target system, detects attacks by examining the number of points each user has been given, and takes countermeasures according to this number of points.

Keywords

Attack Detection, Event Monitoring, Event Analysis, Attack Counteraction, User Profiles, Neural Networks, Expert Systems, Real-Time Detection, Rule-Based Attack Detection System.

1 INTRODUCTION

The growing spread of computer networks and distributed systems has created a number of threats(ISO 7498-2 1989,Pfleeger 1989,ECMA TR/46 1988) to the security of these systems. The main source of these threats is users who use methods of attack(Christmas 1992) to damage a system. Due to the fact that the use of security mechanisms has proved insufficient to protect a computer system from such threats, the use of an attack detection system seems to be an advanced solution for many organisations and institutions. Such a system should be able to log all events of a computer system, and analyse them in order to detect attacks.

S. K. Katsikas et al. (eds.), *Information Systems Security*

2 THE CONCEPT OF ATTACK DETECTION

The attack detection systems are an approach to enhancing the security of a computer system. These systems are based on the auditing of events that take place on a computer system. They aim to provide a trail which could be useful in determining how the system was breached and who was responsible for this breach. However, they do not prevent breaches(ISO 7498-2 1989).

Essentially, the attack detection area comprises the following four aspects: the *event monitoring*, the *event analysis*, the *attack detection* and the *counteraction* aspect.

- The *Event Monitoring* includes the capture of the events of a computer system by a specific module called an *audit trail*, and the recording and storing of these events in special files in a predetermined format. Each record of those files represents an event called an *audit record*.
- The *Event Analysis* covers the division between the security relevant and security irrelevant events. Examples of such security-relevant events are unsuccessful attempts to read, write, or delete a file.
- The *Attack Detection* forms the central part of the system including the characterisation of the suspicious security relevant events as attacks.
- The main responsibility of the automatic *counteraction* is to decide upon and to take the proper action when an attack is detected. Actions may be of three kinds: *immediate*, *temporary* and *long term* actions(ISO 7498-2 1989). An example of an *immediate action* may be to enforce an immediate abort of operations. An example of a *temporary action* is to disable a terminal for one day. Finally, an example of a *long term actions* may be the introduction of an entity into a "black list" denying him any further access to the system.

Computer system audit trails are analysed with the use of automated tools. These automated tools first attempt to isolate security relevant events, so that they can reduce the large volume of audit data. Subsequently, they examine the security relevant audit records to detect actual attacks. This examination may take place after the attack or in real-time. The following types of audit data examination are relevant for security purposes(Lunt 1993):

- in-depth off-line (after-the-fact) examination of audit data
- real-time testing of audit data, so that an immediate action is possible
- subsequent examination of the audit data for damage assessment

The examination of audit trails involves the analysis of the users activities of a computer system. Anderson(Anderson 1980) has attempted a categorisation of users upon whom attention should be focused in an audit trail examination, as follows:

- *external penetrators*: unauthorised users who wish to damage a system, or the interest of the organisation owning a system.
- *internal penetrators*: authorised users of a system who are not authorised for the use of resources accessed. This category also includes masquerades who operate under another user's identity, and clandestine users who evade auditing and access controls.

- *misfeasors*: authorised users of a computer system and of the resources they access, but who misuse their privileges.

The detection of attacks carried out by the user categories described above requires the use of attack detection techniques. A survey of the existing techniques is presented in the next section.

3 ATTACK DETECTION TECHNIQUES

The design and implementation of an attack detection system requires the use of appropriate techniques which will achieve the goals of such a project. In recent years, many research groups and institutions have developed and experimented with different methods of detecting attacks. Three attack detection techniques have gained favour: *user profiles*(Lunt 1993), *neural networks*(Lunt 1990), and *expert systems*(Jackson 1991,Snapp 1991).

3.1 User profiles

The user profiles technique aims at distinguishing users from one another. This approach is based on user patterns of computer system usage, and on the fact that user behaviour characteristics may be used to discriminate between normal user behaviour and departures from it.

In particular, a user's pattern consists of a number of measures, such as file usage, compiler usage, day of use, etc., which are profiled for the user. A statistical model processes the data collected for each user for each measure, thus this technique is termed a statistical technique. These statistics form a user's historical profile. As the behaviour of a user changes slightly, his profile is updated to match his new behaviour. According to this approach, an attack detection system compares the profiles of users against their behaviour. If a significant departure from the historical profile appears, then the system becomes suspicious of the user.

In addition to the measures described above, the user profiles technique can be used to examine other user characteristics related to user's keyboard use. A user's keyboard activity includes measures like typing speed, typing errors, etc.

3.2 Neural Networks

Due to the fact that a user's behaviour is very complex, and observation and detection of departures from the normal activity of a user is quite difficult, the technique described in the previous subsection may cause a significant number of false alarms. These alarms can mislead the statistical algorithms used for this detection approach, so that undetected attacks can pass through a system. Neural networks have been used in recent years in an attempt to progressively replace the user profiles technique(Denault 1993). Laurene Fausett(Fausett 1994) defines neural networks as follows:

> *Neural networks are information processing systems inspired by biological neural systems but not limited to modelling such systems. They consist of many simple processing elements joined by weighted connection paths. A neural net*

produces an output signal in response to an input pattern; the output is determined by the values of the weights.

One of the areas in which neural networks are currently being applied is the general area of pattern recognition(Pao 1989). The user profiles technique described in the previous section falls into this general area. Teresa Lunt(Lunt 1990) has attempted a description of the problems that neural networks seem to solve if used in replacement to the user profiles technique:

The need for accurate statistical distributions

In some cases statistical methods require the use of assumptions about the underlying distributions of user behaviour, such as a Gaussian distribution of deviations from a norm. Invalid assumptions may lead to a high false-alarm rate. Neural networks do not require such assumptions, thus a neural network approach can increase the reliability of an attack detection system.

Difficulty in evaluating detection measures

The selection of a set of intrusion-detection measures as well as the evaluation of their effectiveness for characterising user behaviour has been proved quite difficult(Lunt 1993). Regarding the evaluation process, a measure may seem to be ineffective when considered for all users, but may be useful or totally effective for some particular user. A neural network can serve as a tool which helps the evaluation process of various sets of measures.

High cost of algorithm development

The revising of old statistical algorithms and building new software is a time consuming procedure. In addition, it is costly to reconstruct existing statistical algorithms and to modify the software which implements them. Neural network implementation has proved easier to maintain and adopt(Lunt 1993).

Difficulty in scaling

The use of a statistical approach causes new problems when the number of users to be monitored is large, e.g. thousands of users. Therefore, the need for methods which will be used to assign individuals to groups on the basis of similarity of behaviour, becomes apparent. Such a method results in the need to maintain group profiles instead of a profile for each user. Although there are a number of characteristics that could assist this grouping, such as job title, shift, responsibilities, etc., this approach may prove inadequate. A neural network could be used to classify users according to their actual observed behaviour, thus making group monitoring more effective.

Although the neural network technique seems to be promising for intrusion detection systems, Lunt believes that a neural network approach cannot simply replace a statistical-based approach(Lunt 1993).

3.3 Expert Systems

The expert systems technique uses traditional expert system technology which simply includes the codification of the knowledge of experts in intrusion detection into the form of rules. These

rules are maintained into a rule base and are used to examine the audit data for suspicious activity.

Several projects have adopted the expert system technique to fill some of the gaps in the statistical-based approach. For example, in the Intrusion Detection Expert System (IDES) approach(Lunt 1992), the rule base contains encoded information about known system vulnerabilities, reported attack scenarios and intuition about suspicious behaviour. These rules do not depend on past user or system behaviour. An example of such a rule might be that more than three unsuccessful login attempts for the same user identity within five minutes is to be treated as a penetration activity.

Although the expert system technique can be used to fill some of the gaps in the statistical-based technique, it also has two limitations(Lunt 1993). The first limitation is that the rules have information about known vulnerabilities and attacks, but not about unknown ones, and the second one is that an activity which does not trigger a rule will pass undetected.

In summary, an expert system approach can be proved efficient in detecting intrusion activities on a computer system, only if the rule base is comprehensive enough to detect a large number of attempted attacks.

4 THE ATTACK DETECTION SYSTEM (ADS)

The Attack Detection System (ADS) discussed in this paper is a real-time attack detection system which allocates points to users who are attempting to attack the target system, detects attacks by examining the number of points each user has been given, and takes countermeasures according to this number of points. In particular, the ADS provides the following services(Kantzavelou 1994):

- The ADS detects attacks which result from the selected types of threats: *disclosure* and *corruption of information*, *unauthorised use* and *misuse of resources*, *unauthorised information flow*, and *denial of service*(Kantzavelou 1995).
- The ADS protects itself against attacks.
- The Attack Detection System provides two separate user interfaces. One addresses the needs of the Security Officer of the target system, who needs to access the ADS in order to monitor its activities. The second interface is used by the Administrator of the ADS, who is able to modify the ADS in order to make it more effective and accurate.
- The Security Officer's interface displays detected attacks in real-time, is easy to use, and is application independent.
- The Attack Detection System Administrator's interface is protected from breaches. This assures that the ADS is protected from any unauthorised changes. In addition, it is easy to use, and application independent.

In addition, the ADS has a number of characteristics which provide supplementary services. These are(Kantzavelou 1994):

- The ADS is a real-time system.
- The ADS allows its Administrator to modify system parameters in order to improve the effectiveness and accuracy of the ADS.

- The ADS is an application independent system because its design allows the installation of the ADS on other computer platforms.
- The ADS is composed of a number of modules. This facilitates modification, testing and maintenance of this system.

4.2 Technical approach

The technical approach used for the development of the Attack Detection System is based on a method of points allocation(Kantzavelou 1994). This method has the following four aspects which are depicted also in Figure 1:

- *a user causes events using the target system*
- *an unsuccessful event has a number of points*
- *a certain amount of points makes up a suspicion zone*
- *a suspicion zone decides a certain countermeasure to protect the target system*

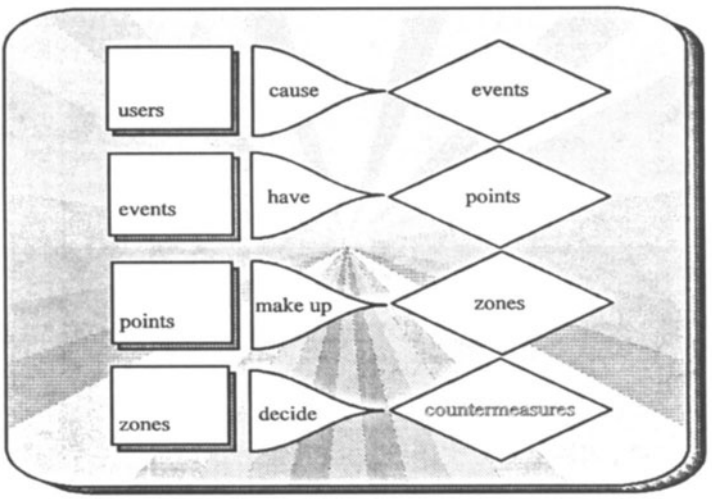

Figure 1 The point allocation method of the Attack Detection System

Each security relevant event which occurs has a number of points associated with it. In the case where a *user* initiates an event which fails, the user is allocated the number of points which are associated with the event.

Repeated failures will lead to a user accumulating a substantial number of points. The amount of points associated with a user are utilised as a measure of suspicion by the Attack Detection System (ADS). A user is placed in one of four suspicion *zones*, depending on how

many points he has. These four zones have been distinguished by the use of a colour range from *yellow* to *black*. This colour range represents the degree of suspicion as described:

1. The ***YELLOW*** zone characterises users as slightly suspicious. They might be novices, future attackers, or bona fide users making occasional mistakes.
2. The ***ORANGE*** zone characterises users as possible attackers.
3. The ***RED*** zone characterises users as attackers who have already attempted to damage the system and its resources.
4. The ***BLACK*** zone characterises users as severe attackers.

When the ADS detects an attack, the *countermeasure* which is selected and carried out depends on the suspicion zone of the user. Users in higher suspicion zones (i.e. RED and BLACK) will have more severe countermeasures used against them.

In conclusion, the Attack Detection System modules which are presented in the next section, apply this method in order to detect attacks.

4.3 The Attack Detection System modules

The Attack Detection System (ADS) uses two data bases and carries out six main functions. Therefore, it was decided that the Attack Detection System will composed of six modules and two data bases(Kantzavelou 1994). These are:

1. *Event Reception Module (ERM)*
2. *Event Data Base (EDB)*
3. *Event Data Base Manager (EDBM)*
4. *Rule Base (RB)*
5. *Rule Base Manager (RBM)*
6. *Attack Detection Module (ADM)*
7. *Security Officer Interface Module (SOIM)*
8. *Management Interface Module (MIM)*

Description of the role of each module or data base in the Attack Detection System is provided below. Figure 2 depicts the overall design of the Attack Detection System and the links between its components.

1. The *Event Reception Module (ERM)* is the bridge between the target system and the Attack Detection System. It is responsible for collecting the target system activities, called *audit data*, filtering the audit data which are of potential relevance from a security point of view, and converting the security relevant audit data into a special format.
2. The *Event Data Base (EDB)* is the storage of the audit data collected by the Event Reception Module. It includes a number of files that are required for the ADS operations.
3. The *Event Data Base Manager (EDBM)* maintains the Event Data Base (EDB). It is responsible for reading and writing audit data in the EDB.
4. The *Rule Base (RB)* contains rules that characterise the state of the Event Data Base which constitute an attack.

5. The *Rule Base Manager (RBM)* maintains the Rule Base (RB). It is responsible for reading, writing, updating, and deleting rules from the RB. In addition, it is responsible for checking new rules against the construction of the RB, and for keeping a backup of the RB before any changes.
6. The *Attack Detection Module (ADM)* is the heart of the Attack Detection System. It is responsible for analysing and examining the audit data stored in the Event Data Base, and detècting attacks using the Rule Base. When an attack is detected, the Attack Detection Module decides what action to take to protect the system from further attacks, and performs the chosen action.
7. The *Security Officer Interface Module (SOIM)* provides a link between the Security Officer of the target system and the Attack Detection System. It allows him to install the ADS, to view detected attacks, and to view audit data stored in the Event Data Base.
8. The *Management Interface Module (MIM)* provides the interface between the Attack Detection System Administrator and the Rule Base (RB). It allows him to view the contents of the Rule Base, and to change the RB in order to make the Attack Detection System more effective and accurate.

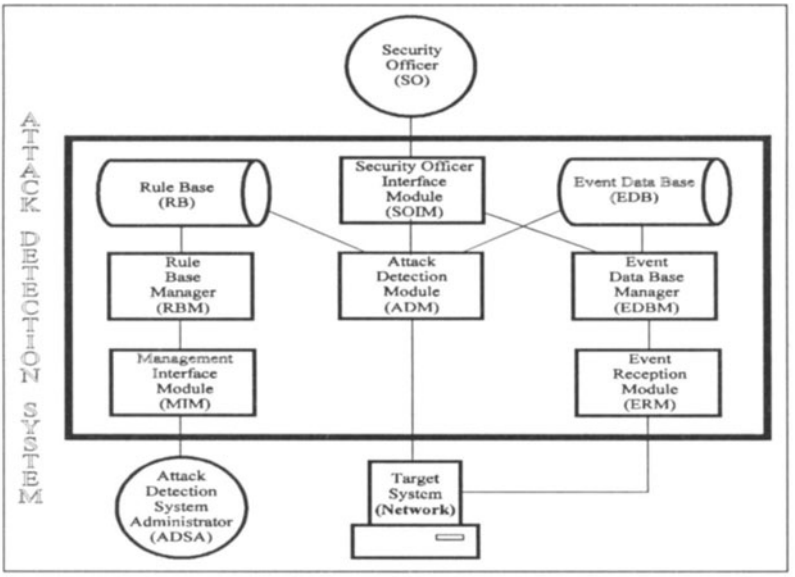

Figure 2 Modules and Data Bases of the Attack Detection System

4.4 Outline of the Attack Detection System functions

The modules of the Attack Detection System presented in the previous section carry out a number of functions. The six main functions that are conducted by the corresponding modules are(Kantzavelou 1994):

- ***Event Collection*** performed by the *Event Reception Module*
- ***Event Data Base Maintenance*** performed by the *Event Data Base Manager*
- ***Attack Detection*** performed by the *Attack Detection Module*
- ***Rule Base Maintenance*** performed by the *Rule Base Manager*
- ***Rule Base Access*** performed by the *Management Interface Module*
- ***Attack Detection System Access*** performed by the *Security Officer Interface Module*

An outline of the above functions is provided in the following:

Event Collection (Event Reception Module)

The Event Reception Module (ERM) monitors and collects the target system activities, called the *audit data*. When it collects audit data of a user's activity, it sends it to the Event Data Base Manager to store it in the Event Data Base. Subsequently, the ERM analyses the audit data in order to determine whether it is security relevant, and sends the security relevant audit data to the Event Data Base Manager to store it. Finally, the ERM formats the security relevant audit data characterising each of them by an action type which indicates the attempted or the succeeded action.

Event Data Base Maintenance (Event Data Base Manager)

The Event Data Base Manager maintains the Event Data Base by performing a number of functions. It stores audit data and security relevant audit data in the Event Data Base, when the Event Reception Module sends it. It also retrieves and sends records of audit data to the Security Officer when he requests them.

Attack Detection (Attack Detection Module)

The Attack Detection Module (ADM) analyses and examines the security relevant audit data received from the Event Data Base Manager, and when it detects an attack, it selects and takes an action to protect the target system from further attacks.

In order to perform these operations, the ADM retrieves records of audit data from the Event Data Base for a user, and creates a new record which contains information about the general behaviour of this user. Then, it retrieves the rule which characterises the state of the general user behaviour from the Rule Base, and compares the information against this rule. The comparison will show if this user acts suspiciously or not. In the case of an attack it decides what action to take to protect the system, and performs the action.

Furthermore, the ADM checks whether sensitive resources have been accessed and informs the Security Officer about detected attacks and resources accessed.

Rule Base Maintenance (Rule Base Manager)

The Rule Base Manager maintains the Rule Base by performing a number of operations. It creates new rules, updates existing rules, deletes rules, keeps backups of the Rule Base before any change, and retrieves rules to display them to the Attack Detection System Administrator.

Rule Base Access (Management Interface Module)

The Management Interface Module provides the interface that is required to access the Rule Base. The Attack Detection System Administrator uses this interface to view the contents of

the Rule Base, to change rules, to create new rules and to delete rules from the Rule Base. This interface co-operates with the Rule Base Manager.

Attack Detection System Access (Security Officer Interface Module)

The Security Officer Interface Module provides the interface that is required to access the Attack Detection System. The Security Officer of the target system can install the ADS, view detected attacks, and view the contents of the Event Data Base. This interface co-operates with the Attack Detection Module and the Event Data Base Manager.

5 CONCLUSION

The growing spread of computer networks and distributed systems has generated a number of threats to the security of these systems. Users may use various methods of attack to damage a system. The use of an attack detection system may usefully supplement other security mechanisms in many organisations and institutions. This paper has described the design of such a system, the Attack Detection System (ADS).

The ADS is a real-time system which collects information about user activities from the Target System and filters it in order to discover security relevant events. Subsequently, it examines these events against the Rule Base and allocates points to users whose behaviour is suspicious. According to the number of points a user has been given, the ADS selects and takes actions to protect the target system. In addition, the ADS is itself protected against attacks.

In conclusion, no attack detection system works as a panacea for a computer system, and the ADS is not perfect.

6 REFERENCES

Anderson, J P *Computer Security Threat Monitoring and Surveillance*, Technical report, James P. Anderson Co., Fort Washington, Pennsylvania (1980).

Christmas, P *Network Security Manager*, Elsevier Advanced Technology, UK (1992).

Denault, M, Gritzalis, D, Karagiannis, D, Spirakis, P *Intrusion Detection: Approach and Performance Issues of the SECURENET System* (submitted 1993).

ECMA TR/46, *Security in Open Systems - A Security Framework*, European Computer Manufacturers Association (1988).

Fausett, L *Fundamentals of Neural Networks: Architectures, Algorithms, and Applications*, Prentice Hall International Inc. (1994).

ISO 7498-2, *Information processing systems - Open Systems Interconnection: Basic Reference Model - Security Architecture*, ISO (1989).

Jackson, K A, Dubois, D H and Stallings C A *'An Expert System Application for Network Intrusion Detection' Proc. of the 14th National Computer Security Conference*, USA (1991).

Kantzavelou, I *An Attack Detection System for Secure Computer Systems*, M.Sc. Thesis, 1994.

Kantzavelou I, Patel A *'Issues of Attack in Distributed Systems - A Generic Attack Model', Proc. of the Joint Working Conference IFIP TC-6 TC-11 and Austrian Computer Society*, September 20-21, 1995, Graz, Austria, pp. 1-16.

Lunt, T F, Tamaru, A, Gilham, F, Jagannathan, R, Neumann, P G, Jalali, C, *'IDES: A Progress Report' Proc. of the 6th Annual Computer Security Applications Conference*, Tuscon, Arizona (1990).

Lunt, T, Tamaru, A, Gilham, F, Jagannathan, R, Jalali, C, Neumann, P, Javitz, H, Valdes, A, Garvey, T *A Real - Time Intrusion Detection Expert System*, Final Technical Report, SRI Computer Science Laboratory (1992).

Lunt, T *'A survey of intrusion detection techniques' Computers & Security*, Vol 12 No 4 (June 1993) pp 405-418.

Pao, Y H *Adaptive Pattern Recognition and Neural Networks*, Addison Wesley, New York (1989).

Pfleeger, C *Security in Computing*,, Prentice-Hall International Editions (1989).

Snapp, S R, Brentano, J, Dias, G V, Goan, T L, Heberlein, L T, Ho, C-L, Levitt, K N, Mukherjee, B, Smaha, S E, Grance, T, Teal, D M and Mansur, D *'DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype' Proc. of the 14th National Computer Security Conference*, USA (1991).

7 BIOGRAPHIES

Ioanna Kantzavelou is a member of the Computer Networks and Distributed Systems Research Group held in the Computer Science Department of University College Dublin (Ireland). She received an M.Sc. by research (security in computer networks) degree at UCD in 1994, and she has worked on Secure Environment for Information Systems in MEDicine (SEISMED) project in UCD, and on a numerous other projects in the industry and other universities. Her interests are security in information systems and especially in medical information systems.

Ahmed Patel received his M.Sc. and Ph.D. in Computer Science from Trinity College Dublin in 1977 and 1984, respectively. From 1978-82, he was responsible for developing the Irish Universities Data Network and from 1982-85 he developed EuroKom computer conferencing and electronic mail service used by R&D projects in Europe. At UCD he is a lecturer in Computer Science, and head of CNDSRG, and centre director of Teltec Ireland. He is involved in various multi-national R&D projects in ESPRIT, RACE/ACTS, INFOSEC, AIM, COST and the Irish national IT and Telecommunications programmes. His main research interests include network management, security, protocols, performance evaluation, intelligent networks, CSCW and open distributed processing systems. He has published many technical papers and co-authored two books on computer network security and one book on group communications. He is a member of the Editorial Advisory Board of the Computer Communications and Collaborative computing Journals.