References

[1] D.S.Bauer and M.E. Koblentz. NIDX - an expert system for real - time network intrusion detection. In Proceedings of the IEEE Computer Networking Symposium, pages 98-106,1988.

[2] A. Brignone. Fuzzy Sets: An answer to the evaluation of security systems? In Proceedings of Fourth IFIP TCII International Conference on Comp. Sec. (IFIP/Sec' 86), pages 143-151, Monte Carlo, Monaco, 2-4 Dec. 1986.

[3] H. Debar, M. Becker, and D. Siboni. A neural network component for an intrusion detection system. In proceddings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pages 240-250, 4-6 May 1992.

[4] R. O. Duda, P. E. Hart, and N. J. Nilsson. Subjective bayesian methods for rule based inference systems. In Proceedings of AFIPS,National Computer Conference, volume 45, pages 1075-1082, New York, June 7-10 1976.

[5] M. Esmaili, R. Safavi - Naini, and J. Pieprzyk. Computer intrusion detection: A comparative survey. Technical Report TR-95-07, Department of Computer Science, University of Wollongong, Australia, 1995.

[6] M. Esmaili, R. Safavi Naini, and J. Pieprzyk. Intrusion detection: A survey. In Proceedings of Twelfth International Conference on Computer Communication ICCC' 95, volume 1, pages 409-414, Seoul, Korea, 21-24 August 1995.

[7] J. Frank. Artificial intelligence and intrusion detections: current and future directions. In Proceedings of 17th National Computer Security Conference, volume 1, pages 22-33, Baltimore, Meryland, 11-14 oct 1994.

[8] P. Hajek, T. Havranek, and R. Jirousek. Uncertain Information in Expert Systems. CRC Press, Inc., 1992.

[9] S.J. Henkind and M.C. Harrison. An analysis of four uncertainty calculi. IEEE Transactions on Systems, Man, and Cybernetics, 18(5): 700-714, Sept./Oct. 1988.

[10] T. F. Lunt. IDES: An intelligent system for detecting intruders. In Proceedings of the symposium: Computer Security, Threat and Countermeasures, Rome, Italy, November 1990.

[11] J. L. O'Neill. Plausible reasoning. The Australian Computer Journal, 19(1): 2-15, February 1987.

and posterior Odds for C is:

$$\text{Odds } (C|B) = \text{IF } (C) \times \frac{PP_C}{1-PP_C}$$

and the posterior probability for C is:

$$P(C|B) = \frac{\text{Odds } (C|B)}{1+\text{Odds } (C|B)}$$

3-4- Intrusion Detection Example

Consider the following scenario"

In <file> - <anystring> % Creating a link to <file>

-<anystring> % file is a user's setuid script
% with # !/bin/ sh or # !/bin/csh
% in the first line

The network in Figure 2(b) can represent the above scenario. Suppose the current audit record contains a record showing that user has created afile. It is a definite piece of evidence, which corresponds to Create node in the network in Figure 2(b). Receiving this evidence, will change the posterior probabilities of Type (Link) and Type (Symb - Link) nodes.

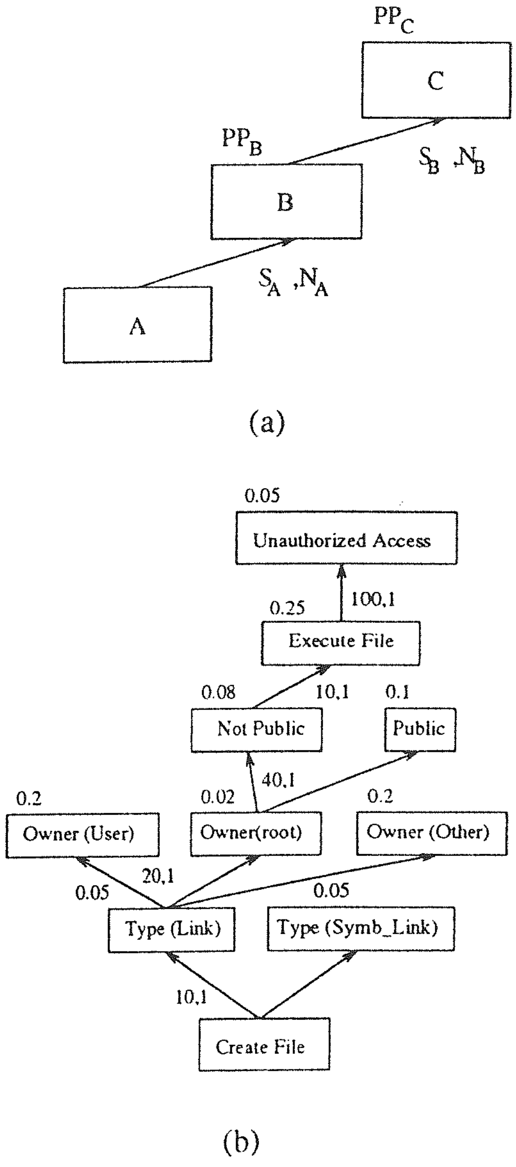
The prior Probability of Type (Link) is 0.05. Converting it to Odds we have

$$\text{Odds (Type)} = \frac{0.05}{1-0.05} = 0.0526$$

Propagating up the network posterior probability of Unauthorized Access would be 0.55. It means an increase of 0.5 in the probability of an intrusion to the system.

4 - Conclusion

In this paper we attempted to demonstrate the applications of AI techniques specifically Expert Systems in Intrusion Detection Systems. We also showed that how dealing with uncertainty probabilistically can allow the system to detect abnormality in the user behavior more efficiently. The use of Expert System technology allows certain intrusion scenarios to be specified much more easily and naturally than is the case using other technologies. However, expert system technology provides no support for developing models of intrusive behavior and encourages the development of *ad hoc* rules.



(a)

(b)

Figuer 2 : (a) General inference network (b) Network representing intrusion scenario

3-2-1- Plausible Relations

For plausible relations, assertions are combined using the odds-likelihood form of Bayes' rule, with modifications [8]. Bayes' rule can only be used where the evidence E (or~ E) is certain. In practice, E may be uncertain, because either E was declared by a user to be uncertain, or E was deduced from another plausible relation, using evidence E′ (say), yielding P (E | E′).

The problem of computing P (H|E) becomes one of computing (H | E′), which can be shown to be calculable (with assumptions) [4], from

$$P(H|E')=P(H|E)\times P(E|E') + P(H|{\sim}E)\times[1-P(E|E')].$$

If E (~E) is known with certainty, this formula produces consistent results. However, if E′ is irrelevant to E, then P (E| E′) = P(E), and the formula should produce a value for P(H| E′) which agrees with the expert's estimate of the prior probability P(H). This is unlikely, leading to the conclusion that P(H). P(E), P(H| E) and P(H| ~E) are not independent.

To solve this problem, we can use a piece-wise linear function of P(E | E′) to compute P(H| E) for each rule, with a way - point to ensure that P(H| E′) = P (H) when P(E| E′) = P (E) supplied by the expert. This is shown in Figure 1[4]. Converting to odds yields O(H| E′), and hence an *effective likelihood ratio*

$$L = \frac{O(H|E')}{O(H)}$$

can be computed for each rule. This ratio is dynamic, tending towards S as E is supported, and towards N as E is refuted (See Equations (2) and (3)). If n rules determine H, each with effective likelihood ratio L_i, the conditional independence assumption allows posterior odds on H to become.

$$O(H \mid E') = O(H) \times L_1 \times L_2 \times \dots \times L_n$$

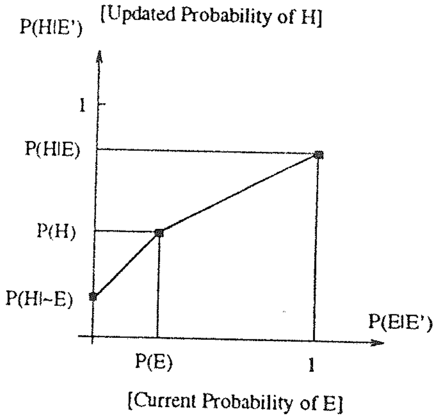


Figure 1 : Piece - wise linear function

3-3- A General Example

Consider the inference network in Figure 2(a):
PP's are prior probabilities for each piece of evidence.

If we receive the definite piece of evidence A, using sufficiency ratio S_A, then since prior probability for B is PP_B the Odds for B will be:

$$\text{Odds (B)} = \frac{PP_B}{1-PP_B}$$

and the posterior odds for B after receiving evidence A would be:

$$\text{Odds (B|A)} = S_A \times \text{Odds (B)}$$

This in turn, increases the odds on the next level in the inference network by a factor of S_B weighted by the degree to which B has increased from its prior probability. Then the posterior probability for B will increase based on the value of S_A.

$$P(B|A) = \frac{\text{Odds (B|A)}}{1+\text{Odds (B|A)}}$$

Propagating up the network, the odds increasing factor is:

$$IF(C) = S_B \times \frac{P(B|A) - PP(B)}{1-PP(B)}$$

3-1- Bayes' Theorem

Bayes' Theorem is based on probability theory, therefore has a sound mathematical background. It is not an ad-hoc method, as certainty factors are (MYCIN/EMYCIN). Bayes' Theorem calculates the probability of a cause, given an event, from the individual probabilities of the event and cause and from the probability of an event, given a cause, Bayes' Theorem is as follows:

$$P(C|E)=\frac{P(C)\times P(E|C)}{P(C)\times P(E|C)+P(\sim C)\times P(E|\sim C)} \quad (1$$

where "~" represents "not".

In implementation, Bayes' Rule is often converted to *odds* and *likelihood* ratios. Likelihood ratio is defined as (using H "*hypotheses*" instead of C "*cause*"):

$$L\ (E|H) = \frac{P(E|H)}{P(E|\sim H)}$$

Also, prior Odds on H is defined as:

$$O(H)=\frac{P(H)}{P(\sim H)}=\frac{P(H)}{1-P(H)}$$

If we use Bayes' equation with H (hypotheses) instead of C (cause), and divide both sides of it by P (~H| E),

$$\frac{P(H|E)}{P(\sim H|E)}=\frac{P(E|H)\times P(H)}{P(E|\sim H)\times P(\sim H)}$$

which is *Likelihood* × *Prior Odds*.

Likelihood ratio is the general name given to this type of ratio. If E is substituted by ~ E the ratio is referred to as the *Necessity Ratio*, and the original form is referred to as the *Sufficiencey Ratio.*

The *Posterior Odds* can be defined as:

$$O(H|E)=\frac{P(H|E)}{P(\sim H|E)}=L(E|\ H)\times O(H)$$

Sufficiency and Necessity Factors can be used in the knowledge base to give strength to belief in each hypotheses. This way, these factors are strengths in which the likelihood of an event E (evidence), influences the belief in another event H (hypothesis). The relationship can be defined as:

if E then H with strength ***Strength***

where strength and Strength are the necessity and sufficiency factors respectively. This can also be diagrammatically represented as:

$$E \xrightarrow[(N,S)]{} H$$

If we intend to investigate the hypothesis H, we collect evidence E to confirm or deny the hypotehsis. S tells how sufficient E is for H, and N tells how necessary E is for H. So, if E is true, then the greater the S is the more likely H is . But if E is false , then the lower the N is the less likely H is. The formulae for calculating these likelihood ratios are:

$$S=\frac{P(E|H)}{P(E|\sim H)} \qquad (2$$

$$N=\frac{P(\sim E|H)}{P(\sim E|\sim H)} \qquad (3$$

3-1-1- Inference Networks

An inference network model is often used to design the expert system when Bayesian methods are used for uncertainty. It shows the network of connections (relations) between evidence and hypotheses. The inference network usually includes the prior probabilities for each assertion being true and also the sufficiency and necessity ratios.

3-2- Logical Relations

For logical relations, the validity (truth or falsity) of a hypothesis, H is completely determined by the validity of its definition, using Zadeh's fuzzy - set formulae [11]. Therefore, if the validity of at least one of the defining assertions cannot be determined, then the probability of H may remain unchanged. If this is undesirable, then plausible relations may be used.

scenarios in its rule base. The IDS raises an alarm if observed activity matches any of its encoded rules. However, expert system technology provides no support for developing models of intrusive behavior and encourages the development of *ad hoc* rules.

Here, our interest is to extend the IDS paradigm to include specific models of proscribed activities. These models would imply certain activities with certain observables which could then be monitored. This would allow to actively search for intruders by looking for activities which would be consistent with a hypothesized intrusion scenarios. But the evidence can not always be matched perfectly to a hypothesized intrusion. Therefore, a determination of the likelihood of a hypothesized intrusion would be made based on the combination of evidence for and against it. The security of such an explicit model should be easier to validate. However, the system must be able to deal with information that can be uncertain. Various numerical calculi have been proposed as methods to represent and propagate uncertainty in a system. Among the more prominent calculi are *probabilistic* (in particular *Bayesian*) methods, the *evidence theory of Dempster - Shafer, fuzzy set theory*, and the MYCIN and EMYCIN calculi [9]. In this paper we look at the application of probabilistic reasoning in computer intrusion detection.

2-1- Proposed Extension

The IDS will include a model - based component which extends the IDS paradigm to include specific models of proscribed activities. Based on evidences received from audit trail, the system seeks additional evidence to conform or refute these models, which are stored in a knowledge base in terms of sequences of user behavior that constitute the scenario. As evidence is discovered which would support one of the other scenario models, that model would be added to the active set.

The system then predicts the next step in the scenario and translates this hypothesized behavior into the specific attributes and values of the audit data that would indicate that behavior. In other words, it figures out how the hypothesized behavior would show up in the audit record.

Using the top - down model - based reasoning approach, the models of intrusion can be used to decide what specific data should be examined next. These models allow the system to predict the action an intruder would take who is following a particular scenario. This in turn allows the system to determine specifically which audit data to be concerned with. If the relevant data does not occur in the audit trail, then the scenario under consideration is probably not occurring. If the system does detect what it was looking for, then it predicts the next step and will then examine only data specifically relevant to confirming the hypothesis of the posited intrusion, and so on until a conclusion is reached. Thus, a model - based system reacts to the situation, using only the data most appropriate to the given situation and context.

Model - based (probabilistic) reasoning supports a sound theory for reasoning under uncertainty. This technology allows uncertainty in the rules - whether the behavior implies something illegitimate - and uncertainty in the significance of the data.

3 - Probabilistic Reasoning

Security rules can be enforced to express which behavior is symptomatic for which threat and to evaluate the level of danger of a given threat. For each rule a weight table expressing the level of danger of the corresponding anomalies in terms of its occurrences and of the subject and object involved can be defined. Levels of danger of different anomalies can then be combined to express the probability of a given threat.

gaining entry into a system [1,2,3,10]. Many computer systems have some kind of security flaw that may allow outsiders (or legitimate users) to gain unauthorized access to sensitive information. In most cases, it is not practical to replace such a flawed system with a new, more secure system. It is also the case that it is very difficult, if not impossible, to develop a completely - secure system. Even a supposedly secure system can still be vulnerable to insiders misusing their privileges, or it can be compromised by improper operating practices. While many existing systems may be designed to prevent specific types of attacks, other methods to gain unauthorized access may still be possible. Due to the tremendous investment already made into the existing infrastructure of *open* (and possibly insecure) communication networks, it is infeasible to deploy new, secure, and possibly *closed* networks. Since the event of an attack should be considered inevitable, there is an obvious need for mechanisms that can detect outsiders attempting to gain entry into a system, that can detect insiders misusing their system privileges, and that can monitor the networks connecting all of these systems together.

The goal of any intrusion detection system must be to aid system security officers in the detection of penetration and abuse. The expert system should provide the knowledge of an "expert" security officer. This is a *minimum* standard of performance for an intrusion detection system. Humans generally do not do a very good job of audit trail analysis, since the volume of audit record data generated makes this a difficult and time consuming job. The set of penetrations or abuses detected by a security officer with the aid of the automated system should be a superset which would have been detected by the security officer unaided.

1-2- Behavior Classification

Classifying user or system behavior is a very hard problem. One problem is that only a small fraction of behavior is misuse; another is that often misuse looks like normal use, so it can be difficult to distinguish between intruders and normal users. As a result, classification can result in "false negatives", wherein an attacker is misclassified as a normal user. "False positive", where a normal user is classified as attacker, can also degrade productivity in the system being protected by invoking countermeasures unnecessarily. Finally all types of intrusive behavior can't be identified in advance.

Several AI techniques have been used to improve IDS classification performance. *Statistical anomaly detection* works on the assumption that many attackers behave differently from legitimate users, or that a system or a process behaves differently during an attack [5]. If a user is behaving abnormally it may indicate an attacker using that user's account. Expert systems encode policy statements and known attacks as a fixed set of rules. User behavior is matched to these rules to determine if an attack is under way. Rule- based systems create (discover) and manage rules corresponding to anomalous behavior.

2- Objective

Most of the current intrusion detection systems (IDS) are built on the concept of detecting anomalous behavior of users with respect to observed behavioral norms [5,6]. This approach may be likened to an unsupervised learning scheme for behavioral patterns with a subsequent pattern recognition approach to determining whether observed behavior falls inside or outside the pattern. In effect, a model of a user's behavior is generated based on observations, but it is difficult to relate the model to specific (and specially proscribed) activities. Thus, validation of the behavior of IDS' statistical algorithms may prove to be difficult.

Some intrusion detection systems also include an expert system component that attempts to encode known system vulnerabilities and attack

Computer Intrusion Detection and Incomplete Information

M. Esmaili R. Safavi - Naini J. Pieprzyk

Center for Computer Security Research
University of Wollongong, NSW 2522
Australia

Abstract

Intrusion Detection Systems (IDS) have previously been built by hand. These systems have difficulties in successfully classifying intruders, and require a significant amount of computational overhead making it difficult to create robust real-time IDS systems. Artificial Intelligence techniques (AI) can reduce the human effort required to build these systems and can improve their performance. AI has recently been used in Intrusion Detection (ID) for anomaly detection, data reduction and induction, or discovery of rules explaining audit data [7]. This paper demonstrates the application of probabilistic methods for dealing with uncertainty in Intrusion Detection Systems. We show that how dealing with uncertainty can allow the system to detect the abnormality in the user behavior more efficiently.

Keywords: *Artificial Intelligence application, Intrusion Detection, Bayesian Methods.*

1- Introduction

Intrusion Detection (ID) is the identification of attempted or ongoing attacks on a computer system or network. Issues in ID research include data collection, data reduction, behavior classification, papering and response. Although there are many significant open problems in ID research, we focus on behavior classification. *Classification* is the process of identifying attackers and intruders. Artificial Intelligence (AI) techniques have been used in many IDS to perform these important tasks [5].

In this paper, our aim is to propose an extension to the IDS paradigm to include specific models of proscribed activities. These models would imply certain activities with certain observables which could then be monitored. This would allow to actively search for intruders by looking for activities which would be consistent with hypothesized intrusion scenarios, But the evidence can not always be matched perfectly to a hypothesized intrusion. There fore, a determination of the likelihood of a hypothesized intrusion would be made based on the combination of evidence for and against it. The security of such an explicit model should be easier to validate. However, the system must be able to deal with information that can be uncertain or incomplete.

1-1- Background

Intrusion detection and *network security* are becoming increasingly more important in today's computer - dominated society. As more and more sensitive information is being stored on computer systems and transferred over computer networks, more and more *crackers* are attempting to attack these systems to steal, destroy or corrupt that information. While most computer systems attempt to prevent unauthorized use by some kind of access control mechanism, such as passwords, encryption, and digital signatures, there are several factors that make it very difficult to keep these crackers from eventually