Adaptive Profile Approach to Internal Attack Detection

V.I. Vasilyev
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: vasilyev@ugatu.ac.ru

T.R. Kashayev
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: kashayev@gmail.com

Abstract[1]

The rapid growing of number of internal attacks leads to the new security tools development. This paper describes the new approach to internal attack detection using adaptive users' profiles. Methods discussed here can improve the quality of attack detection and overall system performance.

1. Introduction

The importance of internal attack detection cannot be overestimated. This type of attack was exposed in 35% of interrogate companies (according to Deloitte & Touche auditing company) [1]. One can use different types of software tools to detect and prevent such attacks (examples are RealSecure, SecretNet, Symantec Enterprise Security Manager). However, there are a number of disadvantages that currently aren't resolved. The examples of these disadvantages include:

- complexity of installation and support;
- low efficiency against unknown attacks;
- high probability of misoperation;
- protection of perimeter only, not the objects inside the network.

An analysis shows that we can use two types of methods to detect inside attacks:

- correlated methods;
- signature methods.

The correlated methods include the static profiles and dynamic (or adaptive) profiles. The *static profiles* use reference user profile containing recorded typical user behavior. These profiles are permanent, i.e. the reference characteristics (ones recorded) stay intact. On the other hand, *dynamic profiles* contain characteristics that can be changed in time. This feature of dynamic profiles provides more accuracy in anomaly detection.

The signature methods use static signatures and dynamic (or adaptive) signatures of known attacks. These signatures are compared with user's behavior to detect attack-like actions. Whereas the *static signatures* are used without any modifications, the *dynamic signatures* are used as a base to create new possible attack patterns.

In-depth analysis has revealed that the problem of internal attack detection can be efficiently solved only by means of dynamic profiles and dynamic signatures.

There are two different ways of user's profile use:

- Building common users' profile;
- Building personal profile for each user.

We propose a combined approach to decrease the type 2 error (when the usual user's behavior considered as malicious). This approach use cluster analysis and fuzzy logic methods.

2. Using Adaptive Profiles for Internal Attacks Detection

The algorithm of this method can be described as follows:

1. At the first stage we run an initial system setup. During this process we create personal profiles for users and determine users' classes.

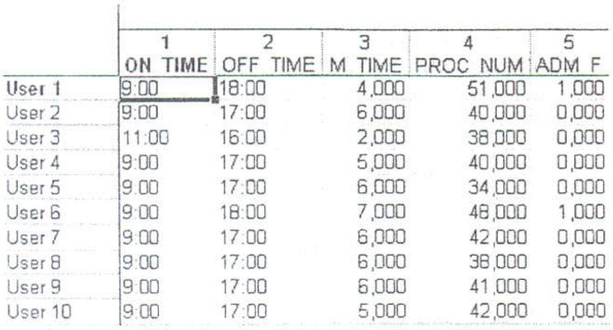
Each user of information system gets a set of characteristics which form its personal profile:

$P_i=\{x_{i1}, x_{i2}, \dots x_{in}\}$, $i=1\dots m$, where x_{ij} is the characteristic number i for user's number j, n – the total number of characteristics, m – the total number of users.

The example shows personal profiles of ten users of information system. These profiles consist of five characteristics (Fig. 1):

[1] *Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the CSIT copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Institute for Contemporary Education JMSUICE. To copy otherwise, or to republish, requires a fee and/or special permission from the JMSUICE.*

Proceedings of the 8th International Workshop on Computer Science and Information Technologies CSIT'2006
Karlsruhe, Germany, 2006



	1 ON TIME	2 OFF TIME	3 M TIME	4 PROC NUM	5 ADM F
User 1	9:00	18:00	4,000	51,000	1,000
User 2	9:00	17:00	6,000	40,000	0,000
User 3	11:00	16:00	2,000	38,000	0,000
User 4	9:00	17:00	5,000	40,000	0,000
User 5	9:00	17:00	6,000	34,000	0,000
User 6	9:00	18:00	7,000	48,000	1,000
User 7	9:00	17:00	6,000	42,000	0,000
User 8	9:00	17:00	6,000	38,000	0,000
User 9	9:00	17:00	6,000	41,000	0,000
User 10	9:00	17:00	5,000	42,000	0,000

Figure 1. Personal Users' Profiles (n=5, m=10)

- nominal time of login;
- nominal time of logout;
- average time of active work;
- average number of open processes;
- use of administrative authority.

We determine users' classes by means of cluster analysis [2].

As can be seen from Fig.2 there are two big classes of users {(User 1, User 6), (User 10, User 9, User 7, User 8, User 5, User 3, User 4, User 2)}. We calculate an average value of each characteristic

$$CP_i=\{cx_{i1}, cx_{i2},\ldots, cx_{in}\},\ i = 1, \ldots k,$$

where k is the total number of classes;

cx_{ij} – the averaged characteristic number j for class number i;

n – the total number of characteristics.

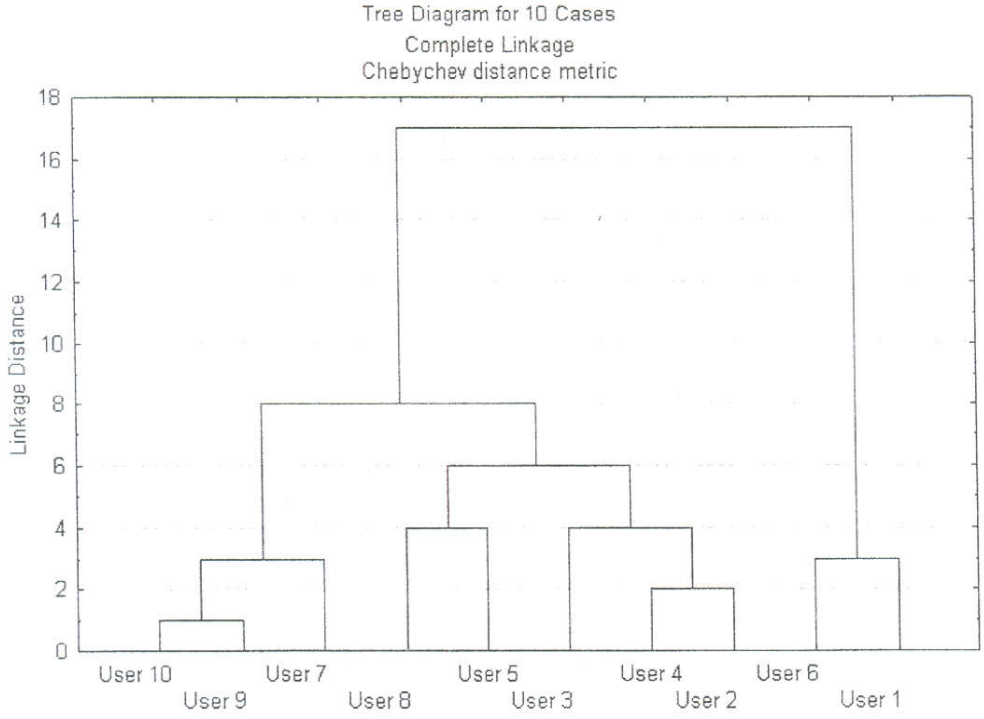


Figure 2. The Result of Cluster Analysis (Chebychev Distance Metric)

2. At the second stage we analyze user's behavior to detect anomaly.

During the work of user its personal profile characteristics are compared with current ones ($y_1, y_2, \ldots, y_n$) and with averaged characteristics of user's class. We propose a fuzzy logic method to determine whether user's behavior is suspicious [3].

1) We define a set of logical variables:

Difference between y_1 and x_1 = {small, medium, high}

Difference between y_1 and cx_1 = {small, medium, high}

...

Difference between y_n and x_n = {small, medium, high}

Difference between y_n and cx_n = {small, medium, high}

Degree of suspect behaviour = {small, medium, high}

2) Next we define rule base:

IF Difference between y_1 and x_1 = *Small* AND Difference between y_1 and cx_1 = *Medium* AND Difference between y_2 and x_2 = *High* AND … AND Difference between y_n and cx_n = *Small* THEN Degree of suspect behaviour = *Small;*

IF Difference between y_1 and x_1 = *Medium* AND Difference between y_1 and cx_1 = *Medium* AND Difference between y_2 and x_2 = *High* AND … AND Difference between y_n and cx_n = *Medium* THEN Degree of suspect behaviour = *Medium*…etc.

3) Now we can determine whether user's behaviour is suspicious by means of fuzzy logic method.

3. At the third stage we introduce corrections into user's profile to maintain its relevancy.

We propose the following structural scheme of profile analysis system.

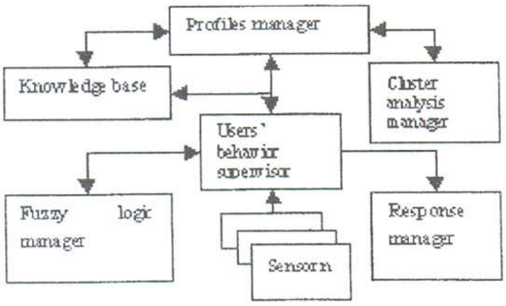


Figure 3. Profile Analysis System (Structural Scheme)

3. Profile Manager Software Implementation

The proposed software implementation of Profile Manager consists of four parts:

- Analysis Service
- Configuration Manager
- Profile Monitor
- Knowledge Base

Analysis Service is the system service that tracks user's behaviour in the system and makes corrections in user's profile.

Configuration Manager is the visual tool to set up the analysis service.

Profile Monitor is the visual tool that enables administrator to view the current profile statistics.

Knowledge base is a set of XML files that contain user's profiles in the following format:

```
<?xml version="1.0" encoding="utf-8"?>
<Header id="Active Audit Data" ver="1.0"/>
<Profile userid="MYPC\user1" created="20060525" local="MYPC" ver="14">
<Data sensor_id="1">9:00</Data>
<Data sensor_id="2">18:00</Data>
<Data sensor_id="3">4</Data>
...
</Profile>
<Profile userid="MYPC\user2" created="20060522" local="MYPC" ver="42">
<Data sensor_id="1">9:00</Data>
<Data sensor_id="2">17:00</Data>
<Data sensor_id="3">6</Data>
...
</Profile>
...
```

Using XML format eases data retrieval and raise versatility.

4. Conclusion

The current research task is to define the proper fuzzy logic variables and rules to get the relevant evaluation of user's behaviour. It is also important to define proper attacker's behaviour model which can be used to reveal weaknesses in system's structure and software implementation.

The proposed system has significant advantages over the current attack detection systems. It uses adaptive profiles to support relevancy of user's profile, two levels of user's behaviour analysis – personal profile analysis and user's class characteristics to decrease attack detection errors.

References

1. "2005 Global Security Survey". Deloitte & Touche Company, 2005.
2. Hartigan J.A. "Clustering Algorithms". John Wiley & Sons Inc., New York, USA, 1975.
3. Zadeh L.A., Kacprzyk J. "Fuzzy Logic for the Management of Uncertainty". John Wiley & Sons Inc., New York, USA, 1992.