VALKYRIE IDS

The General Project Overview

Document version 0.9 **(not for release)**
Updated on July 10th, 2003

Security Team of Poznań Supercomputing and Networking Center

Introduction

Security is a critical factor influencing a range of potential applications for every information technology. Although it seems obvious, it is a matter of recent years when the real problem of security was identified and initial attempts to find appropriate solutions were undertaken. Earlier it was common that security requirements were found less significant comparing to the functional ones. The security of an information system was often considered as just another functional component, sometimes optional, usually possible to be added at the end of a development process. And this approach failed.

Currently the security of the information system is usually one of the top priorities since the beginning of the design and development process. Such a great shift results mainly from a true assumption that besides its functionality, a system must also offer an appropriate level of security in order to be applied in a real environment. As a result, in most cases the analysis of security requirements is an unavoidable part of any design process today and security is being created during all further stages of implementation, deployment and maintenance of the information system. However, security problems still remain.

When information technologies became the networked ones, it turned out that available security mechanisms were not able to fulfill all requirements from new applications. Most of the current security methodologies (with the greatest example of firewalls) are based on placing limitations on accessing specific components of infrastructures, which is rather hiding the problem than solving it. These approaches are of very limited use in the context of new applications such as, for example, web services. This is the reason why new solutions for creating and efficient management of complex information infrastructures are continuously being searched, both in research and commercial areas. The intrusion detection systems and extensions of this concept are one of the most promising technologies in this field.

Intrusion Detection Systems

The main goal of the Intrusion Detection System is to detect in real time, all kinds of inappropriate users' activities such as attempts to breach system integrity, gaining unauthorized access to information or conducting denial of service attacks. Although the general concept of intrusion detection grew up in the mid 80s[1], these systems still belong mostly to the research and development area, where different approaches to solving the problem are continuously verified. Comparing to the research activities in this field, the commercially available systems still have to be considered as relatively simple solutions, definitely not fulfilling the requirements and hopes connected with IDS technologies.

[1] D. E. Denning, *An intrusion-detection model*, SRI International, IEEE 1986

There exists a significant diversity of approaches to creating Intrusion Detection Systems. The differences refer to general assumptions of required functionality as well as to solving specific technical problems. The overall taxonomy of IDSs may be presented using four main criteria: source of data, analysis method, reaction scheme and mode of operating. All these criteria as well as their most common values are illustrated in figure 1.

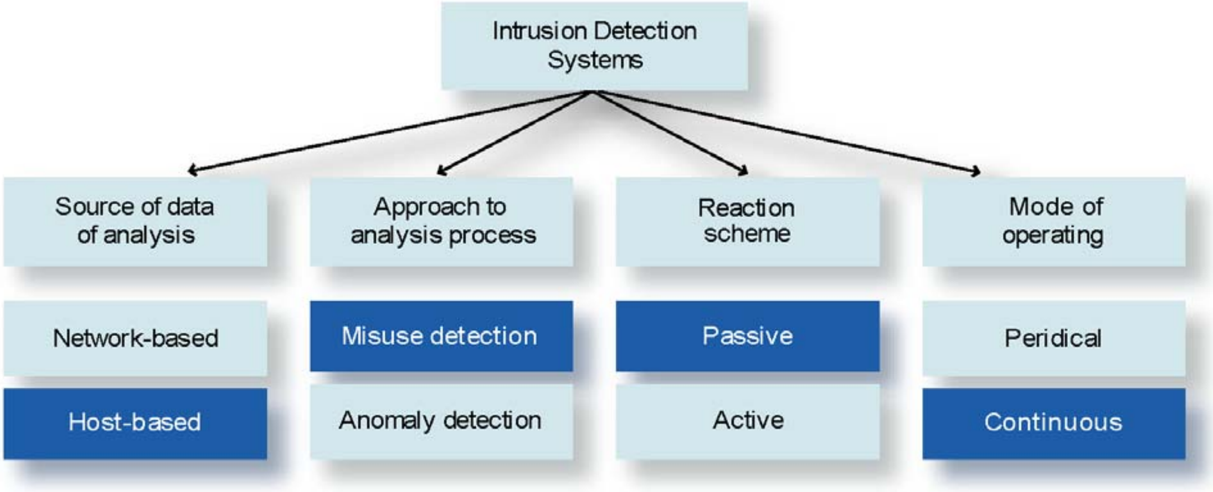


Figure 1 General taxonomy of Intrusion Detection systems[2]
(darken blocks refers to the profile of Valkyrie IDS)

Currently the Intrusion Detection Systems acquire data for analysis from two main sources: operating system (*host-based*) and network (*network-based*). In case of *host-based* solutions, data are provided by modules installed directly in protected resources, which are usually closely integrated with the kernel of operating systems. The acquired data are consistent and reliable, but this approach requires installing software components in every protected system. There is no such a requirement in case of *network-based* solutions, where information is gathered only in selected points of a protected network. However, the data of analysis are not so complete and often their usefulness is very limited, for example, when connections are encrypted.

The two main types of approaches can also be distinguished in the context of analysis methods applied for intrusion detection. The *misuse detection* methods are aimed at the detection of sequences in data, which match defined patterns of inappropriate behavior. These methods may be very efficient, yet their value strongly depends on the quality and completeness of pattern's database. The second type of approach, the *anomaly detection*, is based on an opposite concept. In these methods normal behavior is provided through the application of machine learning algorithms or through *a priori* definitions, and any deviation from such normal profiles are considered as inappropriate behavior. These methods can detect the unknown attack technique, yet they may be much more computationally expensive.

The reaction scheme of an IDS refers to types of actions that may be undertaken upon the detection of inappropriate behavior. According to the original concept of IDS, it should be aimed at detection and providing alert information, and therefore it may be considered as a *passive* solution. The *active* system is not only limited to providing such information, but should also automatically counteract and prevent an intrusion attempt from being successfully completed. Obviously, the *active* systems are more complex and require more reliable analysis

[2] H. Debar, M. Dacier, A. Wespi, *Towards a taxonomy of intrusion-detection systems*, Computer Networks, No. 31, 1999

methods, as it has to deal with *false positive* errors (when legitimate behavior is classified as anomalous and inappropriate).

The last taxonomy criterion describes the mode of the operating of a solution. Although it characterizes the operating of IDS as a complete system, it very often refers mostly to the analysis process, which is the most time consuming. Generally, the systems can be divided into *periodical,* where analysis is performed for example in the night-time, and *continuous*, which attempt to perform analysis and provide alert information in the real time. Obviously, the taxonomy of IDSs described here is very general and in practice there often exist systems that cannot be unambiguously classified upon all criteria. For example, an IDS solution may utilize different sources of information or analysis methods at the same time. In the context of this last criterion, a system may for example perform less expensive analyses continuously and more expensive ones in a periodical manner.

Architecture of Valkyrie IDS

The Valkyrie is an Intrusion Detection System created mainly upon experiences gained in the VALIS project conducted by the Security Team of Poznań Supercomputing and Networking Center since 1997. The Valkyrie shares the general architecture of VALIS using the modular and distributed approach, close integration with a kernel of protected operating systems, analysis process performed on selected and dedicated systems, and the possibility of monitoring whole protected infrastructure from a single, centralized Monitoring Console.

Comparing to the VALIS project, the Valkyrie system is less complex but more suited to fulfill the requirements of Sun based environments (better integration with a kernel of Solaris operating systems). The Valkyrie also does not have a capability of active intrusion prevention and currently is using only a single analysis method.

Basic Assumptions

The main goal of Valkyrie IDS is to efficiently provide valuable information about intrusion attempts undertaken in the complex, dynamic, and open environments, where traditional security mechanisms are hardly applied The efficiency in this context refers to optimized design of information gathering and analysis modules as well as to appropriate presentation of alerts in centralized manner.

Using the overall taxonomy of Intrusion Detection systems, Valkyrie IDS may be described as a *host-based* system (with components installed on protected systems), using *misuse detection* approach to analysis process (looking for defined attack patterns), *passive* (aimed at detection of attack only) and *continuous* (providing alert information in real time). On figure 1, the profile of Valkyrie IDS has been marked with darkened blocks.

The main requirements for the system high effectiveness of detection, low payload, and general flexibility. All those requirements significantly influenced the architecture of Valkyrie IDS as well as design and implementation of specific components.

Distributed Approach

The Valkyrie IDS is designed and implemented with modular and distributed architecture in mind. The system has been divided into several interrelated components, located in various points of the protected environment. For every environment protected using Valkyrie IDS, the three main logical points may be distinguished, these are respectively a protected resource, an analysis system, and monitoring console.

A protected resource is an system being monitored by the IDS. As the Valkyrie IDS is a *host-based* system, it requires installation of some software components in protected resource in order to gather data about its operating. This process is focused mainly on gathering and selecting data that may be critical from the security point of view, and sending them to network. As it is highly optimized, the overall computational payload on protected systems is reduced to acceptable level. The actual analysis process, which may be computationally expensive, is performed on an analysis system.

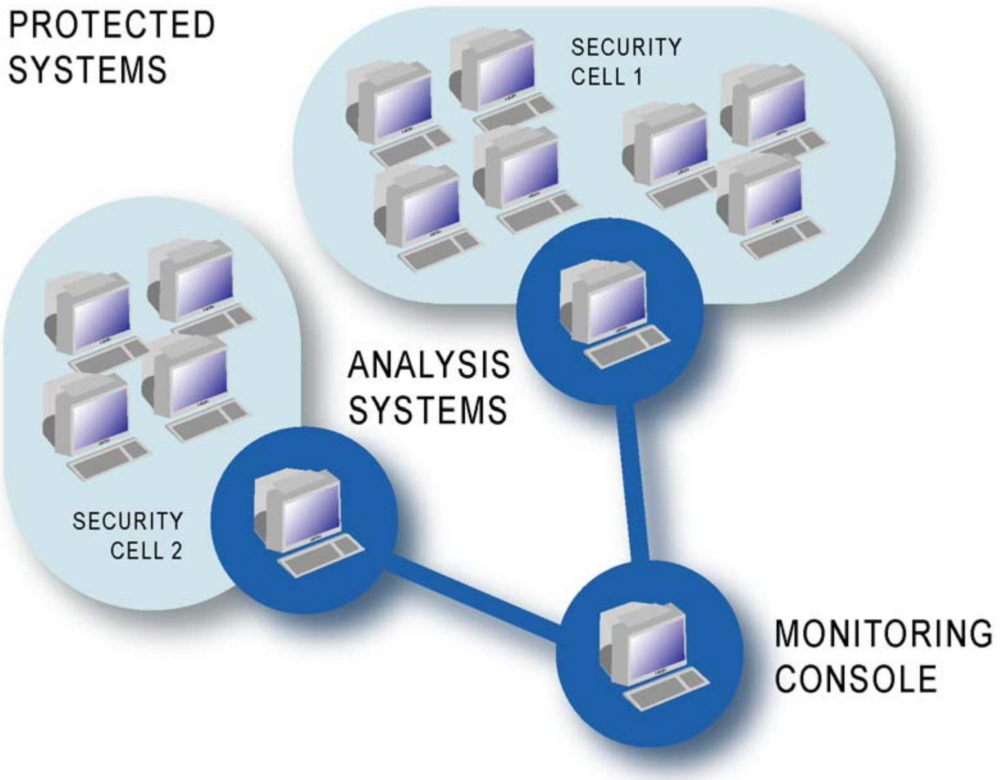


Figure 2 Modular and distributed architecture of the Valkyrie IDS

An analysis system is a computer dedicated to intrusion detection process. As the analysis process is performed on remote, tightly secure system, it is not affected by changes in state of protected system once data have been transferred through network. Currently only a single analysis module is used, but the general architecture enables introducing parallel analysis modules.

An analysis module can get receive and handle data from many protected resources. As the computational power of a single analysis system may not be sufficient, there can be used several independent analysis modules operating simultaneously. In such a case, a protected environment is divided into logical security cells, connected to specific analysis modules. Results of analysis from different security cells can be presented on the same monitoring console or be provided to another analysis module, performing alert management function (using different knowledge base). Therefore, it is possible to create a hierarchical structure of protected environment.

The overview of modular architecture used in the Valkyrie IDS is presented on figure 2.

Implementation

The Valkyrie IDS is currently prepared for working in computing environments built upon systems manufactured by Sun Corporation. However, it should be noticed that only data gathering components installed in protected resources are platform specific. The remaining modules are designed and implemented assuming requirement of high portability. The analysis module can be compiled and operate on most Unix systems. The monitoring console requires appropriate version of GTK window library.

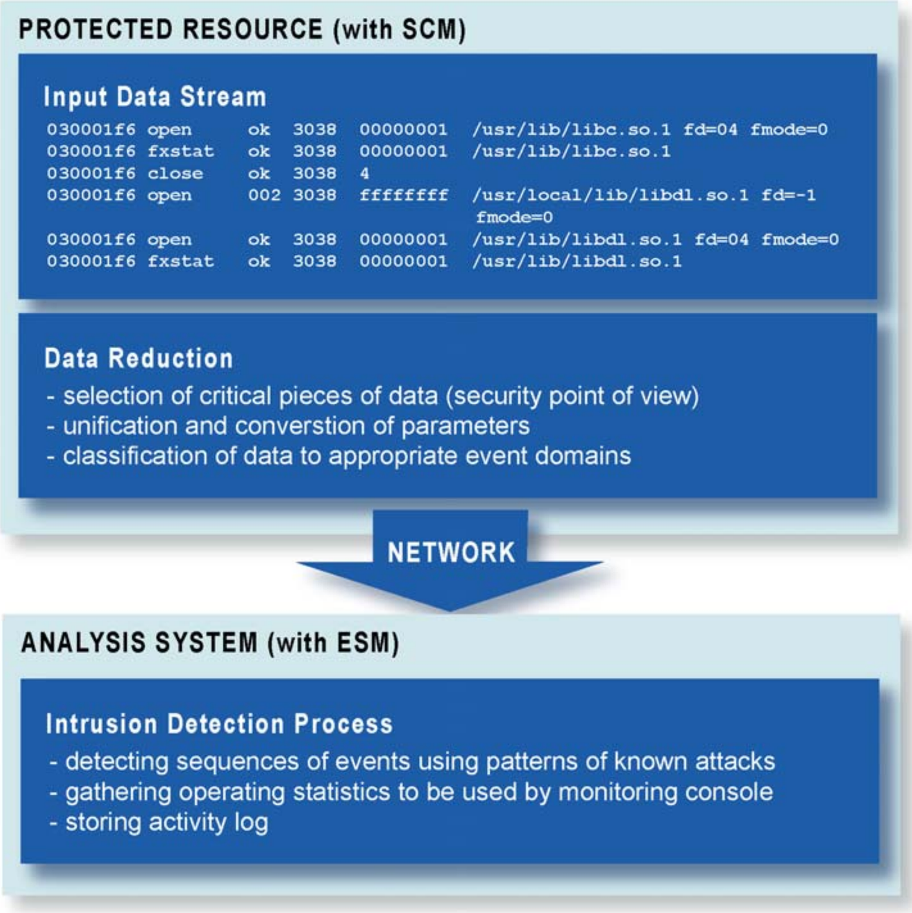
Components of Valkyrie IDS

For each of presented logical points of protected environment, an appropriate component of the Valkyrie IDS has been developed.

System Call Monitor (SCM)

The System Call Monitor (also referred as SCM) is the component responsible for gathering all significant data about operating of a protected resource. SCM is a low-level component, closely integrated with kernel of Solaris operating system. As it is able to monitor all operations performed by users' and system's processes, the component provides complete and reliable view of actions performed in a protected system. It is achieved through intercepting the system calls interface, which is the only way for users and application to perform operations at the operating system level.

During development of SCM, one of the most significant problem was amount of data gathered through monitoring of the operating systems, as it influenced not the overall system's performance but also network traffic (data must be transferred for analysis). The natural way for solving this problem is agile selection of data that are critical from the security point of view. In order to develop appropriate data selection technique, a series of analysis of modern attack techniques were performed. In result, the optimal group of system calls that have to be monitored was prepared. Additionally, it turned out that some other groups of calls have to be monitored only under special conditions and with different levels of details. For this reasons, the SCM was equipped with mechanism for dynamic changing range and detail level of monitored system calls.


PROTECTED RESOURCE (with SCM)
Input Data Stream

```
030001f6 open     ok  3038  00000001  /usr/lib/libc.so.1 fd=04 fmode=0
030001f6 fxstat   ok  3038  00000001  /usr/lib/libc.so.1
030001f6 close    ok  3038  4
030001f6 open     002 3038  ffffffff  /usr/local/lib/libdl.so.1 fd=-1
                                       fmode=0
030001f6 open     ok  3038  00000001  /usr/lib/libdl.so.1 fd=04 fmode=0
030001f6 fxstat   ok  3038  00000001  /usr/lib/libdl.so.1
```

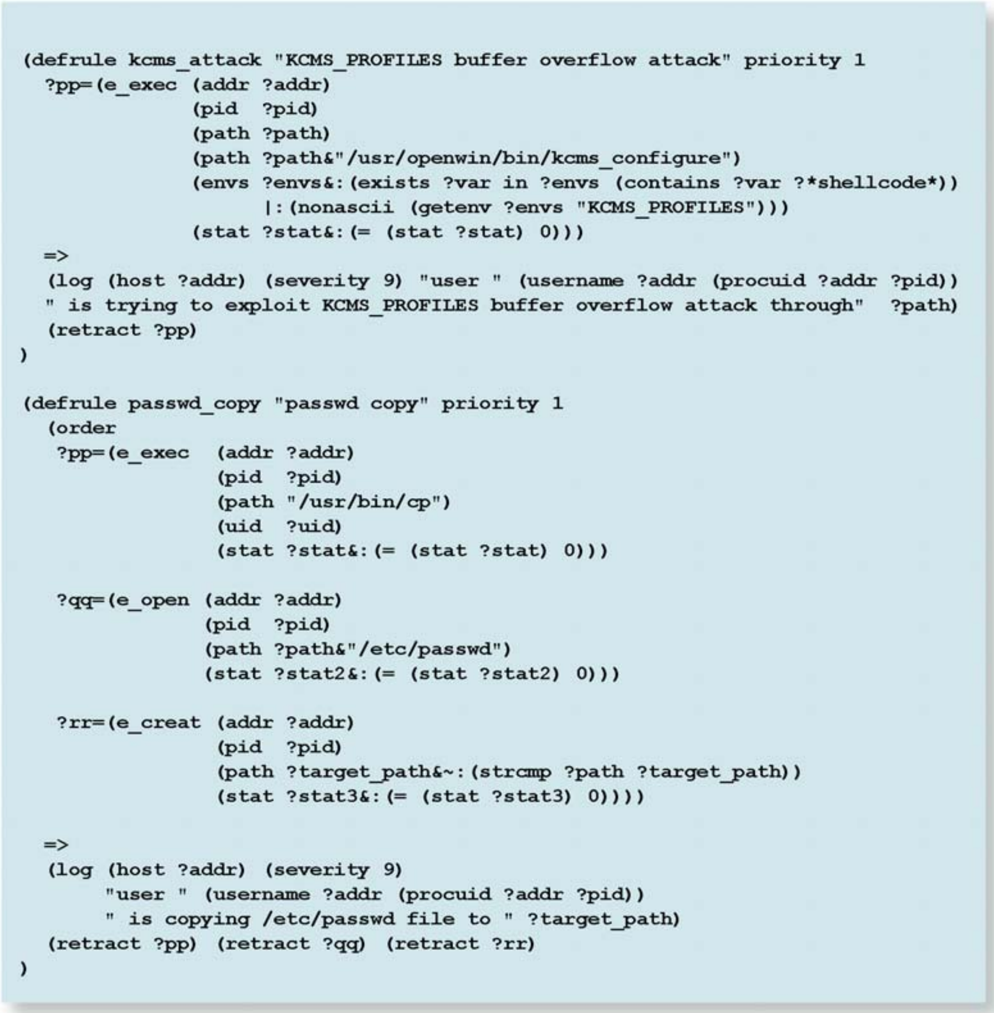
Data Reduction
- selection of critical pieces of data (security point of view)
- unification and converstion of parameters
- classification of data to appropriate event domains
NETWORK
ANALYSIS SYSTEM (with ESM)
Intrusion Detection Process
- detecting sequences of events using patterns of known attacks
- gathering operating statistics to be used by monitoring console
- storing activity log

Figure 3 Overall view at information gathering and analysis process in the Valkyrie IDS

The SCM is implemented as Kernel Loadable Module and is divided into several functional components. As the main requirements for this component were flexibility and performance, it is closely integrated with the kernel of Solaris operating system and therefore rather platform dependent.

Expert System Module (ESM)

The quality of Intrusion Detection System depends critically on effectiveness of applied analysis methods. Valkyrie IDS is currently using a single analysis module based upon *misuse detection* approach. The Expert Module System (ESM) uses predefined set of patterns in order to detect know types of attacks or various suspicious actions undertaken in the protected system. The ESM performs analysis based upon facts, which are sequences of events provided by the SCM or any other monitoring component. The facts are matched against rules stored is knowledge base, and appropriate action is selected upon result of this process. The general examples of rules are presented on figure 4. The first rule on the figure detects known buffer overflow attack against kcms_configure, while the second one detects an attempt to copy /etc/passwd file.



```
(defrule kcms_attack "KCMS_PROFILES buffer overflow attack" priority 1
  ?pp=(e_exec (addr ?addr)
              (pid  ?pid)
              (path ?path)
              (path ?path&"/usr/openwin/bin/kcms_configure")
              (envs ?envs&:(exists ?var in ?envs (contains ?var ?*shellcode*))
                    |:(nonascii (getenv ?envs "KCMS_PROFILES")))
              (stat ?stat&:(= (stat ?stat) 0)))
  =>
  (log (host ?addr) (severity 9) "user " (username ?addr (procuid ?addr ?pid))
  " is trying to exploit KCMS_PROFILES buffer overflow attack through"  ?path)
  (retract ?pp)
)

(defrule passwd_copy "passwd copy" priority 1
  (order
   ?pp=(e_exec  (addr ?addr)
                (pid  ?pid)
                (path "/usr/bin/cp")
                (uid  ?uid)
                (stat ?stat&:(= (stat ?stat) 0)))

   ?qq=(e_open (addr ?addr)
               (pid  ?pid)
               (path ?path&"/etc/passwd")
               (stat ?stat2&:(= (stat ?stat2) 0)))

   ?rr=(e_creat (addr ?addr)
                (pid  ?pid)
                (path ?target_path&~:(strcmp ?path ?target_path))
                (stat ?stat3&:(= (stat ?stat3) 0))))

  =>
  (log (host ?addr) (severity 9)
       "user " (username ?addr (procuid ?addr ?pid))
       " is copying /etc/passwd file to " ?target_path)
  (retract ?pp) (retract ?qq) (retract ?rr)
)
```

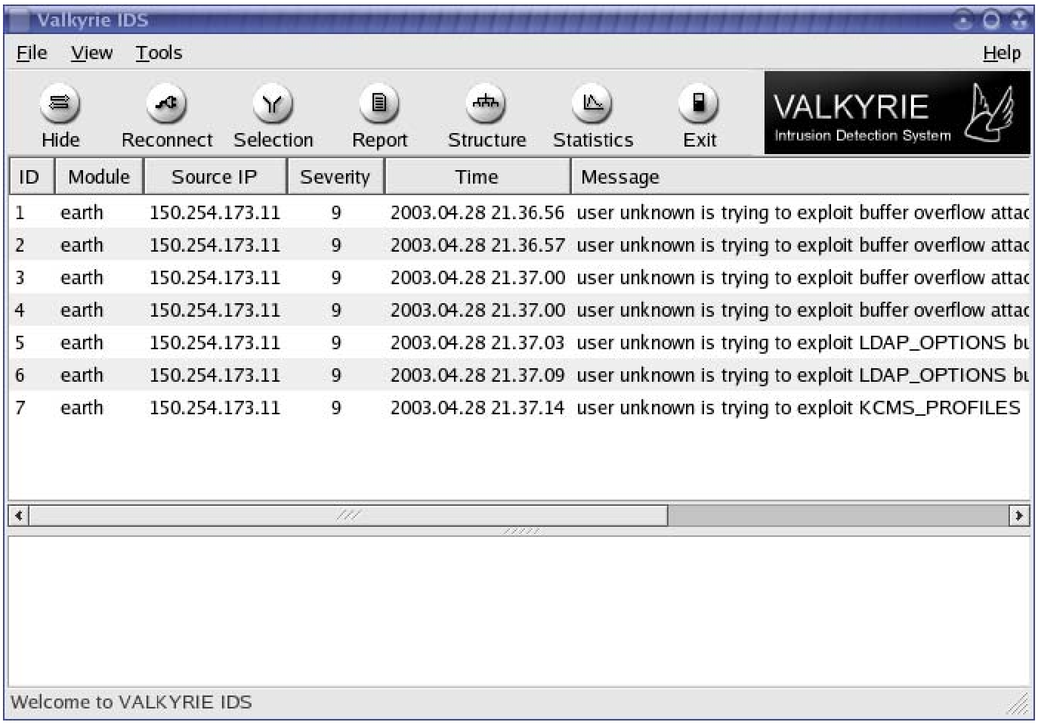
Figure 4 Examples of rules used in the analysis process performed by ESM

There can be distinguished to main parts of the ESM, the knowledge base and the inference engine. The knowledge base may be considered as a specific case of relational database. Obviously, effectiveness of the Valkyrie IDS strongly depends on completeness of knowledge base and its frequent updates. Currently, due to specificity of protected environment, the base contains general rules for attacks and suspicious behavior and rules specific for Solaris operating systems.

Monitoring Console (GUI)

The appropriate visualization and presentation of alert information is the last critical phase in operating of IDS. In order to enable easy monitoring of large and distributed infrastructure, the Valkyrie IDS is equipped with

Monitoring Console, which can be connected to multiply analysis modules and combine information from various sources. The main type of data received by Monitoring Console is message describing detection of specific sequence of events by the analysis module. Depending on severity of a message, it can be presented to security operator as a critical event (security alert) or just a warning about suspicious activity. The console may also present additional information about operating of analysis modules or specific protected resources.



ID	Module	Source IP	Severity	Time	Message
1	earth	150.254.173.11	9	2003.04.28 21.36.56	user unknown is trying to exploit buffer overflow attac
2	earth	150.254.173.11	9	2003.04.28 21.36.57	user unknown is trying to exploit buffer overflow attac
3	earth	150.254.173.11	9	2003.04.28 21.37.00	user unknown is trying to exploit buffer overflow attac
4	earth	150.254.173.11	9	2003.04.28 21.37.00	user unknown is trying to exploit buffer overflow attac
5	earth	150.254.173.11	9	2003.04.28 21.37.03	user unknown is trying to exploit LDAP_OPTIONS bu
6	earth	150.254.173.11	9	2003.04.28 21.37.09	user unknown is trying to exploit LDAP_OPTIONS bu
7	earth	150.254.173.11	9	2003.04.28 21.37.14	user unknown is trying to exploit KCMS_PROFILES

Welcome to VALKYRIE IDS

Figure 5 Screenshot of the main window of Valkyrie Monitoring Console

The Monitoring Console is currently implemented with use of GTK Toolkit for creating graphical user interfaces, version 2.x.

Summary

There do exist a need for new solutions and general security methodologies. Intrusion Detection Systems are about to play a critical role in securing complex computational infrastructures. They are not a replacement of currently applied technologies, like for example firewalls, but rather complementary solutions that can provide invaluable information about up-to-date state of protected environment. It is also highly probable that their application and meaning will be systematically increasing with technology progress and more demanding security requirements.

One of the most promising approaches to IDS problem seems to be based on using *host-based* systems in distributed security architecture with centralized management and possibility of using various analysis methods. The Valkyrie IDS is an example of such a solution.