ISSN 2277-3061

Model-Based Tool-Assistance for Packet-Filter Design and its Future

Gurvinder Kaur[1], Dr. S.N. Panda[2], Dr. Dalvinder Singh Dhaliwal[3]

[1]Department of Computer Science and Engineering, RIMT, Mandi Gobindgarh (Punjab), India

Er.gurvinderkaur@gmail.com

[2]Department of Computer Science, RIMT, Mandi Gobindgarh (Punjab), India

Panda.india@gmail.com

[3]Department of Computer Science & Engineering, Bharat group of institutes, Sardoolgarh

dalvinder.dhaliwal@gmail.com

Abstract

Firewall is a device that secure the private network from unauthorized access. Model based tool assistance facilitate the design task and has contribute to the correctness of the filters. But the model based tool assistance approach is design time only does not manage actions at run time. So we shall propose model on run time auditing architecture to detect the attack while packet filtering in firewall technology. It is usually based on the log-files of the packet-filters.

Keywords*:* packet filtering; network access models; model based management

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 13, No. 1

editor@cirworld.com

www.cirworld.com, www.ijctonline.com

1. Introduction

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. At one time, most firewalls were deployed at network perimeters. This provided some measure of protection for internal hosts, but it could not recognize all instances and forms of attack, and attacks sent from one internal host to another often do not pass through network firewalls. Because of these and other factors, network designers now often include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to protect mobile devices that are placed directly onto external networks.

Threats have gradually moved from being most prevalent in lower layers of network traffic to the application layer, which has reduced the general effectiveness of firewalls in stopping threats carried through network communications. However, firewalls are still needed to stop the significant threats that continue to work at lower layers of network traffic. Firewalls can also provide some protection at the application layer, supplementing the capabilities of other network security technologies.

2. Packet Filtering

Packet filters, implemented on routers, filter on user defined content, such as IP address. They examine a packet at the network layer and are application independent. This allows them to deliver good performance and scalability. They are the least secure type of firewall. The reason is that they cannot understand the context of a given communication, making them easier for hackers to break . Packet filters have two choices with regard to outbound FTP connections. They can either leave the entire upper range of ports open (greater than 1023) to allow the file transfer session to take place over the dynamically allocated port, but exposes the internal network or they can shut down the entire upper range of ports to secure the internal network which blocks other services [2].

3. Objectives of the Study

1) Explore different working models of packet filtering technology in firewall technology.

2) Exploration of multiple parameters used in packet filtering technology.

3) Proposed model on run time auditing architecture to detect the attack while packet filtering in firewall technology.

4. An Analysis of Access Control Models and Model Based Management

A tool-assistance approach which itself is based on a combination of three approaches. Firstly, it applies object-oriented modelling as it is proposed by the Unified Modelling Language approach .

Secondly, they follow up the approach of model-based management supporting the development of systems for automated network, system and application management. The development starts with the design of a model of the system which should be managed.

Thereafter the model is refined. Additional information for the modelling of management objectives and functions is introduced.

Thirdly, the work is based on the notion of management policies and policy hierarchies .They propose a corresponding policy hierarchy for packet-filter design and represent the policy statements by model extensions. Accordingly, packet-filter design coincides with step-wise model and policy refinement. The tool-assistance is provided by an interactive design tool.

An implementation of the approach and a corresponding experimental design tool were developed which are particularly attended to configurations of *IPchains*, the packet-filtering extension of the Linux kernel [Lin99].Besides from the approaches already mentioned, our work is strongly related to role based access control RBAC [San96, Fer99] which had a forming influence on our abstract access control model. Moreover, the modelling is oriented at elements and views of the firewall reference model introduced in [Sch97].

In the sequel they first outline the approach of model-based management and give a short introduction into the Linux packet-filter kernel extension *IPchains*. Thereafter, we explain the system model with its three layers. The layers correspond to three levels of abstraction. Assignment and correlation elements connect the layers. The next section describes the process of interactive filter design. The initial model and the refining transformation steps are discussed. Then, a software tool supporting this design process is presented. Finally, the conclusion reports about the broader context of the work and particularly outlines pending extensions[3].

A. Access control models

Access control serves as the basis for many security related services and applications. It refers to the process of regulating access to protected data and resources based on pre-defined security policies. Security policy governs the behavior choice of the managed system without the need for a reimplementation. A security model provides a formal representation of the security policy and its working .There are three classic access control models: mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC). These models make a clear separation between authentication and authorization. While authentication is the process of verifying the identify of a subject; authorization refers to the process of granting privilege to that subject.

Mandatory access control grants access based on the regulations mandated by a central authority. It considers the processes operated on behalf of users as subjects, thus controlling the indirect access of information by execution of processes. The most common model of mandatory access control

is the multilevel security policy, where each subject and object is assigned to an access class and partial order is defined among those access classes. Authorization policies can be categorized into secrecy-based mandatory policies and integrity-based mandatory policies. These two models could be applied in a dual manner to achieve the protection of both confidentiality and integrity on information. Since mandatory policies enforce access control based on classification, assigning access classes to subjects and objects at the most appropriate granularity is not always an easy task. On the other hand, mandatory policies still remain vulnerable to covert channels, where information can be inferred through abnormal communication.

Discretionary access control grants access based on the identity of requesters. It also gives users the ability to pass their privileges to other users, where the granting and revocation of privileges is regulated by administrative policies. The access control matrix provides a basic framework for

describing DAC.

Role-based access control was proposed particularly for enterprise and corporate environment, where authorizations are granted to roles instead of individual users. This maps naturally to an organization's structure. A role represents a set of privileges that a user playing the role is granted to. Roles can be hierarchically organized to allow the propagation of access control privilege along the hierarchy.

In addition to the three classic models, credential-based access control has been proposed recently to address access control in open and dynamic scenarios, where clients and servers may not be known to each other in advance. The traditional separation between authentication and authorization cannot be applied anymore. Access control solutions need to answer which client can be granted access to the protected resource, as well as which server is qualified to provide this resource. Trust management was proposed as a solution for addressing access control in open systems[4].

B. Model based management

The concept of Model-Based Management was initially proposed by Luck et al.and later applied to the configuration of several security mechanisms such

as packet-filters and VPNs . This approach aims to support the policy based management by the use of an object-oriented model of the system to be managed. Based upon this model, a policy refinement can be accomplished such that configuration parameters for security mechanisms can be automatically derived.

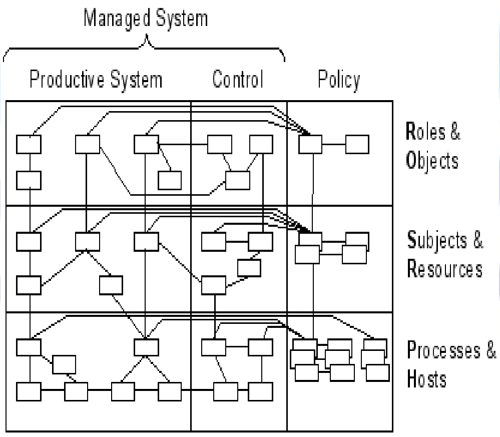

Fig. 1 Model Overview

The structure of the model is shown in Figure where three abstraction levels can be distinguished: Roles & Objects (RO), Subjects &Resources (SR), and Processes & Hosts (PH). Each level is a refinement of the superordinated level in the sense of a policy hierarchy". The uppermost level represents the business-oriented view of the network whereas the lowest level is related to the technical view. The vertical subdivisions differentiate between the model of the actual managed system (with productive and control elements) and the policies that regulate this system. This last category encompasses requirement and permission objects, each of which refers to the model components of the same level and expresses security policies.

The uppermost level (RO) is based on concepts from Role-Based Access Control (RBAC) . The main classes in this level are: Roles in which people, who are working in the modelled environment, act; Objects of the modeled environment which should be subject to access control; and Access Modes; i.e. the ways of accessing objects. The class Access Permission allows the performer of a Role to access a particular Object in the way defined by Access Mode.

The second level consists of a more complex set of classes. Objects of these classes represent: (a) people working in the modelled environment (User); (b) subjects acting on the user's behalf (Subject Types); (c) services in the network that are used to access resources (Services)|a service has references to all resources it is able to access; (d) the dependency of a service on other services (Service Dependency); and lastly (e) Resources in the network. The Service Permission class allows a subject to use a service to access a resource.

The SR level of layers a transition from the business-oriented view, represented in RO level, to a more technical perspective, which is service-based. This is accomplished by using a service-oriented management approach to achieve a relatively abstract view of the management system, which is hence defined from the standpoint of the services that the system will provide. As such, the system's internal structure is not expressed in the SR level, but rather in the third level (PH) of the model .

The lowest level (PH) is responsible for modelling the mechanisms that will be used to implement the security services defined in SR. Therefore, PH will have even more classes than before, representing for instance the Hosts, with their respective network Interfaces, and the Processes, that perform communicative actions relying on Sockets. Protocol Permissions allow the transition of packets between processes. Several other classes are also defined according to the supported mechanisms[5].

In the system modelling phase the filter designer successively considers the existing system on the three different levels of abstraction. On each level, he specifies the corresponding objects and their associations. Only those associations, however, are modelled which connect objects of the same abstraction level. Therefore, the three steps of system modelling can be performed separately. Thus, the designer can firstly concentrate on the role-based access control creating the RO-part of the model. He introduces objects of type *Role*, *Object*, *and AccessMode* as well as the connections between these objects. Thereafter, he designs the SR-part in terms of objects of type *User*, *Subject*, *Host*, *Resource*, and *Service*. Finally, the ND-part of the model directly

reflects the existing network structure[3].

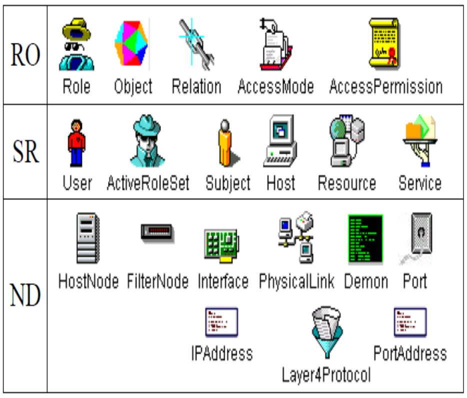

Fig. 2   Symbols for model classes

5. Research Problem Formulation

Model-Based Tool-Assistance for Packet-Filter Design   tool approach assisting in the design of *IPchains* packet filter configurations but this model is design time do not perform any action at run time.They developed a special tool that already provided a very helpful support, and also they study a more general modelling which additionally represents access control mechanisms and application gateways. In turn it supported the design of gateway-based firewall configurations and the tool could perform more specialized correctness checks. Their main aim was the integral modelling of all relevant security mechanisms and system components of a computer network in order to support a combined management of security services, security mechanisms, and network elements. Up to now, the tool is used at design time only. Their work therefore utilizes the layered model and the associations between the layers for the transformation of low-level log-statements into corresponding high-level reports[3]

6. Conclusion

Model based tool assistance for packet filter design is design time only .For managing actions at run time we shall propose an effective run time auditing architecture for the proper operations of packet filters. It is usually based on the log-files of the packet-filters and We shall explore multiple parameters used in packet filtering technology. Explore different working models of packet filtering technology in firewall technology.

REFERENCES

[1] Karen Scarfone ,Paul Hoffman,“Guidelines on Firewalls and Firewall Policy”, Recommendations of the National Institute of Standards and Technology,September 2009.

[2] Minho Sung and Jun Xu, “IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 14, NO. 9, SEPTEMBER 2003.

[3] Ingo Luck , Christian Schafer et al. “Model-Based Tool-Assistance for Packet-Filter Design”, POLICY 2001, LNCS 1995, pp. 120-136, 2001.

[4] Hang Zhao,“Security Policy Definition and Enforcement in Distributed Systems”,Graduate School of Arts and Sciences ,COLUMBIA UNIVERSITY.

[5] Joao Porto de Albuquerque, Heiko Krumm et al. “On Scalability and Modularisation in the Modelling of Network Security Systems”,Scholarship funding by the German Academic Exchange Service (DAAD).