ISSN No: 2348-4845

International Conference on Electronics, Communications and VLSI Circuits (ICECV-2015)

December 06, 2015 - Hyderabad, India.

Paper Published in IJMETMR, A Peer Reviewed Open Access International Journal.

# Policy Based Security and Network Management in Computer Networks

Anupoju Venkata Malleswara Rao [#1], Dr. Shaheda Akthar [*2]

[#] *Ph. D. Scholar, Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, Andhra Pradesh, India*

[*] *Lecturer in Computer Science, Department of Computer Science*

*Govt. College for Women, Guntur, Andhra Pradesh, India.*

## Abstract

Computer networks are ubiquitous in nature with a plethora of networking models that are suited to different organizations. However, security has been a concern in such networks besides managing network effectively. Mostly network security is based on the needs of the organization which used the network for secure communications. However, the actual implementation of security is achieved by defining policies that guide the policy management tool to take expert decisions. The policies when defined perfectly, the security can be most effective. Network administrators depend on traditional tools that can be used to monitor happenings in the network. However, when there are plenty of messages in the reports and network administrators need time to analyze and made decisions, they cannot prevent damage that has been caused already. Therefore a real time approach is desired for both network management and security in computer networks. We believe that policy based security and network management can help improve networks when the process is holistic and updated from time to time. This paper reviews literature that provides insights pertaining to policy based security and network management.

***Index Terms:*** *Network, security, security policy, security management, policy management, network management.*

## I. INTRODUCTION

Over a period of time computer networks evolved and being used across the globe. Right from the first network invented after Second World War, computer networks witnessed many changes from wired networks to wireless networks (different topologies for each network). These networks, though they are different from each other, show a common requirement that is security. Since security plays a crucial role in computer networks, it is to be given highest importance. Network security and network management are ever lasting issues that are to be addressed from time to time. Since the networks need to be protected, the automated applications need domain experts' inputs for protecting systems. It does mean that security systems might need user inputs. In other words, the security related policies are to be defined by users so that the security mechanisms can work well as per the requirements of the users. Thus policy management came into existence.

Security policies that are defined perfectly play a role in securing systems. No matter how good a security system is when policies are not defined correctly, it cannot guarantee fool proof security.

In this paper we review the literature on policy based security and network management in computer networks. As computer networks became diversified into Wireless Sensor Network (WSN), Mobile Ad Hoc Network (MANET), Vehicular Ad Hoc Network (VANET), and so on, it became essential to have a review of different computer networks and what are the policy based approaches employed in securing such networks. Our contributions in the paper include the review of the present state-of-the-art of policy based security and network management. The remainder of the paper is structured as follows. Section II provides various aspects of management of policies in communication/computer networks. Section III presents security policies for computer networks. Section IV concludes the paper besides providing directions for future work.

## II. MANAGEMENT OF POLICIES

According to Phanse, DaSilva [3] quality of Service (QoS) plays a vital role in computer networks. The network management here is required in order to handle network survivability, QoS robustness, and service differentiation. Policy based management is one of the promising methods that can be used to leverage QoS and network management. The policy distribution models can be either outsourced to third parties or can be built into the framework of the network. Response time and signalling overhead can be used as measures for enhancing network management. A policy based system should realize a robust architecture. Figure 1 presents important architectural elements of a policy – based system.

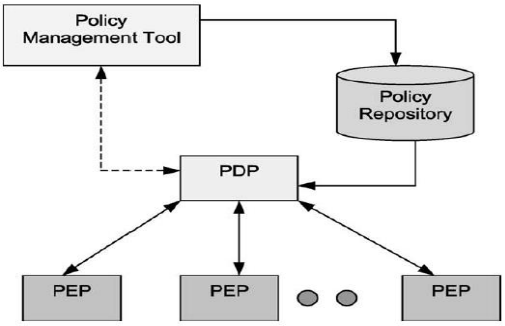

Fig.1 Overview of a policy-based system

As shown in Figure 1, it is evident that policy management tool (PMT) allows network administrator to define and manage security policies over network. PMT is ideally used by network administrator to monitor network and take necessary steps. The problems if any in the network can be identified using the policy-based system. The PMT determines the relationships among policies and the need for updating policies from time to time [3]. There is Policy Decision Point (PDP) is derived from multiple Policy Enforcement Points (PEP). The PEP is responsible to enforce given policy in the network. The policy dynamics are monitored by PDP server. PDP actually monitors the PEPs in order to ensure that there is thorough understanding between making well informed decisions. PEP also aware of policy changes and reports the same to PDP. The PDP has access to a wealth of knowledge that resides in the policy repository. The policy management tool interacts with PDP in order to know the policy dynamics and take appropriate decision [3]. There are two major models pertaining to policies namely provisioning model and outsourcing model are presented in Figure 2.

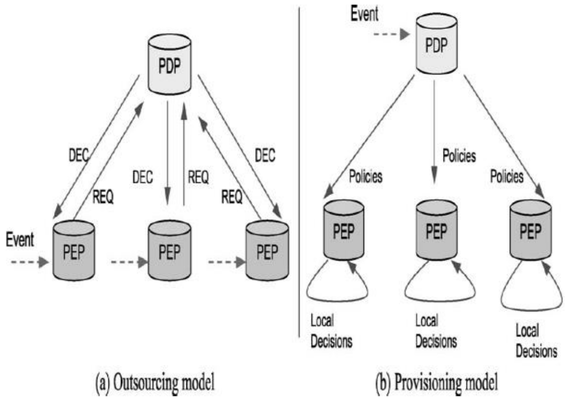

Fig. 2 Illustrates types of policy models [3]

As can be seen in Figure 2, it is evident that policies can be categorized into two models namely provisioning model and outsourcing model. In case of provisioning model, the local decisions are made on each PEP. However, the policies come from the PDP. On the contrary, the PDP takes decisions based on the request made by PEP. Therefore the outsourcing model is known as PEP-driven while the provisioning model is PDP driven. In case of provisioning the model is distributed in nature while the outsourcing model is centralized [3].

## 2.1Policy Based Content Delivery

Maclarty and Fry [4] explored active network architecture for policy – based content delivery. With respect to audio streaming to subscribers, it is possible to improve quality of service based on policies. Policy is nothing but the guidelines or rule sand regulations that are tailored towards a user of the network. User-based policies and the policy based content delivery with respect to live streaming can help increase QoS in computer networks. The user-centric policies that are defined with mutual agreement with end users can provide service providers an edge in maintaining quality of services. This will result in customer satisfaction, ease of content delivery and optimization of services. In case of distributed applications, the policies might be maintained in a remote server which is contacted to process every request in order to ensure that the service quality is not deteriorated. Dini et al. [5] explored policy – enabled mechanisms for handling challenges, expectations, and feature interactions in computer networks.

### 2.2 Resources Allocation Policies

An organization can achieve its strategic goals by assigning resources and managing them optimally. Resources include computing resources like storage, processing power, and so on. These sources can be allocated to increased number of users in a fashion that makes sense besides optimizing resource utilization. Gaining access to resources as per the privileges can also be integrated with resource allocation policies. It is also essential to monitor allocated resources using technologies. The technologies can also be used for ensuring security and controlling other applications and their user base with fool proof security and resource optimization.

### 2.3 Bandwidth Allocation Policies

Network management also involves bandwidth allocation. Towards this end, the bandwidth allocation policies play a vital role in ensuring quality of services. In packet-switched networks Hou et al. [6] proposed two bandwidth allocation policies. They are generalized max-min (GMM) and Weight-Proportional Max Min (WPMM). Available Bit Rate (ABR) became a norm to plan data transfer in distributed applications. The rate allocation mechanisms are in general and they do not consider or impose any special requirements on scheduling and buffering schemes. The experiments proved that the rate based feedback control when employed yielded in optimizing bandwidth allocation in computer networks.

## III. SECURITY POLICIES

The main purpose of security is to protect assets of an organization. Security risks are being increased due to the usage of computers, computer networks, Internet and other electronic computing resources. With the advent of Internet based e-Commerce applications there is ever increasing trend of online payments and thereby increased threats of security. The security risks are growing as computing facilities are growing. To overcome this problem different kind of security devices are introduced. Firewall is software of hardware solution that monitors incoming and outgoing packets from time to time. As the information security plays a vital role in safeguarding assets and intellectual properties of an organization, security risks became a common issue to be heard. The security risks include hacking data, data leakage, and defacement of web sites. Organizations need to take more care on information security as their assets are in the form of information resources. In fact information security needs to be given paramount importance. It is more important when businesses are connected to Internet there is growing interconnectivity in terms of devices and applications in a distributed environment. Such environment is vulnerable to security threats.

Security is crucial for all kinds of computer networks. Public Key Infrastructure (PKI) has been around for securing communications in networks. Lambrinoudakis et al. [7] explored PKI-based security policy for safeguarding e-Government services in distributed environment. The security requirements for communications include integrity, confidentiality, non-repudiation, source storage, logging, access control and authorization, identification and authentication. Management PKI services that are used in security services and the PKI and cryptographic services include camouflaging, TTP, encryption and digital signatures. The e-Government security requirements include availability, performance, management of privileges, authentication, logging, integrity, confidentiality, non-repudiation, anonymity, public trust, untraceability and secure storage.

### 3.1 Policy Languages

Policy languages have been around for network and security management. Policy driven management and policy driven security play a vital role in establishing fundamental security in computer networks. Han and Lei [8] made a review of such languages. The policy languages include PFDL, PDL, Ponder, CIM-SPL, KAOS, XACML, Rei, EPAL, P3P/APPEL, ASL and VALID. The features in the policy languages include ECA, XML, index, RBAC, Obligation, and Formalization. The policy driven management architecture is as shown in Figure 3.

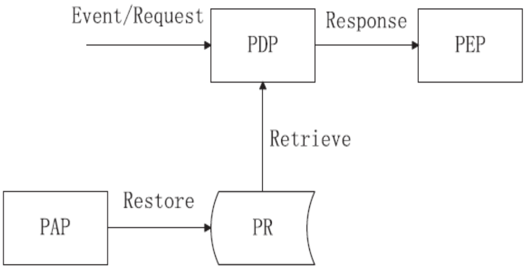

Fig.3 Illustrates policy-driven management architecture [8]

The policy – driven management is crucial in computer networks. PEP and PDP are for policy enforcement and policy decision making respectively. Policy Repository (PR) stored all policy related information. Policy authorization point (PAP) is responsible to restore policy repository. The PDP can take policy details from PR and take appropriate decisions based on the event or request. The PDP gives policy decisions to PEP while the PEP is responsible for enforcing such policy for high level of security in computer networks [8]. Gungor and Lambert [10] explored communication networks and managing them for automation of electric systems. In the process they proposed a structured mechanism that can be used to make effective decisions. Network management policies were also employed for designing water reservoir [12].

### 3.2 Integrating Policies with Intrusion Detection System

Network and security policies can be exploited by an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). According to Aydin, Zaim, and Ceylan [11] there are many kinds of IDS available. They are broadly classified into anomaly based and misuse based. The misuse-based IDS can identify any events that are not compatible with security and network policies. The anomaly based IDS, on the other hand, identifies abnormal activities involved in the system and considers such activities as potential attacks. There are many techniques used for anomaly detection such as genetic algorithms, neural networks, and data mining methods. Snort is an IDS which is widely used and based on misuse based approach.

### 3.3 Dynamic Modification of Policies

When network policies are changed dynamically, it is possible to have a system that can adapt to future requirements. Gorla and Pugliese [13] proposed a specification for access control model that enables dynamic modification of policies. The static and dynamic checking is possible by using policies that can be used to control access to computing resources. As the network security is ever changing phenomenon, it is essential to have new policies and modify existing policies to cope with new developments. Towards this end, the network system should have capabilities that can be leveraged to ensure fool proof security. It is more so in the highly distributed networks where different nodes located in various geographical places can be seamlessly integrated and policies can be enforced to have end to end security.

### 3.4 Agent Based Approach for Network Management

In case of distributed system, the network management becomes very complex. In spite of policies and monitoring applications, the network management is tedious task. Gavalas et al. [14] presents a hierarchical network infrastructure where agent – based approach is used for network management. Mobile Agent (MA) is the component that moves over network infrastructure and manages network in a scalable fashion. Distributed mobile agents that are code components are flexible and cost-effective to perform network monitoring activities. The mobile agents in distributed environment can fulfil many needs of network management. Mobile Ad Hoc Networks (MANETs) can be protected by using cluster based security schemes that are applied when a node leaves or joins network. The network security is based on policies that are used by clusters. The cluster communication is based on the policies defined.

## IV CONCLUSIONS & FUTURE WORK

In this paper we studied and reviewed various aspects of policy based security and network management in computer networks. Computer networks are diversified into different kinds to cater different services. In all such networks security has been an important concern that needs to be addressed. The security and network management issues are never ending problems.

Therefore they are to be handled from time to time. In tune with this they are to be changed based on the changing needs of the organizations besides vulnerabilities and threats envisaged. Moreover computer networks became wired and wireless and the security policies are different for both of them. Security policies are good only when the person who defines them has good knowledge. Nevertheless, security policies are playing a dominant role in abusive based protection mechanisms. This paper throws light into policy based security and network management dynamics by presenting the present state-of-the-art. This paper can be extended further to propose a framework that can guide framing policies and changing them dynamically for fool proof security of computer networks.

## REFERENCES

[1] Patrick Cohendet a,, Frieder Meyer-Krahmer. (2001). The theoretical and policy implications of knowledge codification. *ELsevier*. 30 . p.213-313.

[2] Dijiang Huang , Mayank Verma. (2009). ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks. *ELsevier*. 7 . p.1526–1535.

[3] Kaustubh S. Phanse, Luiz A. DaSilva. (2003). Addressing the requirements of QoS management for wireless ad hoc networks.*ELsevier*. 23 . p.1263–1273.

[4] G. MacLarty, M. Fry. (2001). Policy-based content delivery: an active network approach. *ELsevier*. 24 . p.12-17.

[5] Petre Dini a, Alexander Clemm b, Tom Gray c, Fuchun Joseph Lin d, Luigi Logrippo e, Stephan Reiff-Marganiec. (2004). Policy-enabled mechanisms for feature interactions: reality, expectations, challenges.*ELsevier*. 45 .p.56-60.

[6] Y. Thomas Hou a, Bo Li b, Shivendra S. Panwar c, Henry Tzeng d. (2000). On network bandwidth allocation policies and feedback control algorithms for packet networks. *ELsevier*. 34 .p.23-33.

[7] Costas Lambrinoudakisa, Stefanos Gritzalisa, Fredj Dridib, Gu¨nther Pernul. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *ELsevier*. 26 .p.25-34.

[8] Weili Han , Chang Lei. (2012). A survey on policy languages in network and security management. *ELsevier*. 56 . p.56-60.

[9] V.C. Gungor a, F.C. Lambert. (2006). A survey on communication networks for electric system automation. *ELsevier*. 50 . p.23-33.

[10] M. Ali Aydın ,A. Halim Zaim, K. Gökhan Ceylan. (2009). A hybrid intrusion detection system design for computer network security.*ELsevier*. 35 . p.56-60.

[11] A. Castellettia, D. de Rigoa, A.E. Rizzolib, R. Soncini-Sessaa, E. Weber. (2007). Neuro-dynamic programming for designing water reservoir network management policies. *ELsevier*. 15. p.977–1000.

[12] Daniele Gorla , Rosario Pugliese. (2009). Dynamic management of capabilities in a network aware coordination language. *ELsevier*. 78 .p.23-33.

[13] Damianos Gavalasa,b, Dominic Greenwoodc, Mohammed Ghanbarib, Mike O’Mahony. (2002). Hierarchical network management: a scalable and dynamic mobile agent-based approach. *ELsevier*. 38 .p.56-60.

[14] Vijay Varadharajan, Rajan Shankaran, Michael Hitchens. (2004). Security for cluster based ad hoc networks. *ELsevier*. 27 . p.25-34