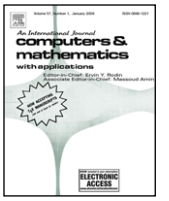
Computers and Mathematics with Applications 60 (2010) 176–186

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa



A universal access control method based on host identifiers for Future Internet

Hongchao Wang [a], Hongke Zhang [a], Chi-Yuan Chang [b], Han-Chieh Chao [b,c,*]

[a] National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, 100044, Beijing, China

[b] Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan

[c] Institute of Computer Science & Information Engineering and Department of Electronic Engineering, National Ilan University, I-Lan, Taiwan

ARTICLE INFO

Keywords:
Access control
Access protocol
Security
Host identifier
Authentication

ABSTRACT

There have been many security events in the Internet. Many of them are due to arbitrary access permissions to the network resources of the malicious users, especially their free sending packets to anywhere in the network. However, current existing solutions such as ingress filtering and network firewalls cannot solve the problem of malicious access to the network flexibly and effectively. In this paper, we present an efficient access control method based on host identifiers, in which a safe and bidirectional authentication process is introduced whenever the host begins to access the network. Meanwhile, all the succeeding information exchanges between the host and the network can be controlled through the encrypt scheme negotiated during the access authentication process. Through analysis and experiments, we find that the proposed method has the following merits. First, our method has the capability to support various end-nodes to access the Internet in a uniform way. Second, with our method, end-nodes and the core network can establish a mutual trustworthy relationship to avoid any spoof from the other side. Third, our method can support host mobility very well.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

Access control (AC) is a security mechanism to protect certain resources or services from illegal access. It is an important component in the security of modern information and communication systems [1]. As for the network, AC is adopted to control the users who want to access the network and avail the services of the network. It is the first doorsill and plays an important role in the network security.

At the time the current Internet was designed, network nodes were assumed to be trustful to each other. With the rapid development of the Internet, however, some network users become threatening and malicious, as envisioned by the Denial-of-Services (DoS), spam information, identity spoof, etc.

According to the report [2], there were 1813 incidents received by CNCERT/CC in the first half of 2007. More than 60% of the incidents could be avoided, if the network had a perfect access control mechanism. Therefore, how to control the large number of potential malicious users to access the network has become a puzzle requiring urgent solutions.

Although some access control mechanisms [3–5] have been proposed, they are not enough to support security, mobility and PnP (Plug and Play) applications in Future Internet. Furthermore, the wireless channels are easy to access and the internet protocols are open to all users. This makes it easy for the third party to capture the packets and analyze the contents, even juggle or clone the data and spoof the opposite side to acquire some important information.

* Corresponding author at: Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan. Tel.: +886 3 9357400 251; fax: +866 3 9354238.

E-mail address: hcc@niu.edu.tw (H.-C. Chao).

0898-1221/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2009.12.031

In Future Internet, both end-nodes and core networks should be protected from spoof or illegal access and a mutual trustful environment should be set up between them [6]. Moreover, Future Internet should permit various kinds of end-nodes such as Personal Computer (PC), Personal Digital Assistant (PDA), Mobile Phone (MP), Telephone, and Sensor Node (SN) to access the network. In other words, the size of Future Internet will be bigger and there will be more malicious users in Future Internet. Besides, Future Internet should support host mobility in the global scope. However, there is no good access control method to support various kinds of end-nodes to access the network in a uniform way and control the mobile nodes to access the network flexibly and efficiently in the global scope. Hence, in order to satisfy the requirements of Future Internet, a new access control mechanism is needed.

The main contribution of this paper is a universal access control method based on host identifiers for Future Internet. In the view of the network information exchange, the proposed method has the following characteristics. First, it is a network protocol which can prevent the unregistered or malicious users from accessing and using the network. Meanwhile, it can limit the speed of users' sending packets to an appropriate level. Second, it is based on the host identifier which is abstracted from the hardware information of the host, and it has a universal formation for all the nodes that can access the future network. Third, the proposed method contains a bidirectional authentication processes that can assure a mutual trustworthy environment to be established between the host and the network. At last, the method has a coordination mechanism between different access points which makes the future network support the host mobility very well.

The rest of this paper is organized as follows. Section 2 briefly presents related work. We present our access control method in Section 3, followed by the security analysis of the method in Section 4. In Section 5, we present results from experimental tests. Finally, we outline concludes and future work in Section 6.

2. Related work

Due to the importance of the access control in the network, there have been some researchers to develop the access control models or new network architectures to make the network be more secure and reliable.

Ingress Filtering [7] is a typical scheme to implement network access control. This method requires Internet Service Providers and organizations at the edge to apply filters limiting the source addresses allowed on incoming packets to those specifically allowed in the stub networks. If there were 1/4 of networks not applying Ingress Filtering, the whole network would still be insecure. In addition, the strict binding of IP, MAC and physic Port will restrict mobility of end-nodes exceedingly.

Context-based access control schemes [8,9], can partly solve the access control problem flexibly. But they are still one-way authentication, or they need to take up more memory space or consume more compute resources. What is more, some simple sensor nodes in Future Internet are difficult to satisfy the requirements. Kulkarni et al. [10] propose a context-aware role-based access control model for pervasive computing applications. However, it is directed against the programming framework.

Forstall et al. [11] point out an access control management scheme based on the profile associate to the media device. When the media device is connected to a host computer system, if the media device has a development profile, the integrated development environment on the host computer system can access the media device. Otherwise, if the device only has a personal profile, the integrated development environment is prevented from accessing the device. It is a very well access control method to protect the copyrights of the software. When the device has the ability to exchange information with others, its network behavior still cannot be controlled.

IP Security [12–14] can provide authentication and protection in the network layer. However, it needs to spend a long time on encryption and decryption. It is mainly used to solve the end-to-end security, but it is not fit for secure network access control. Host Identity Protocol [15] can reduce certain types of Denial-of-Service (DoS) attacks. However, it emphasizes to solve the mobility and enhance the end-to-end security in communication process, and its performance could not satisfy the need of mobile node's fast handoff among different access points.

Bao et al. [16] propose a light-weight encryption schemes for multimedia data and high-speed networks. However, it is an encrypt/decrypt scheme to protect the data integrity, reliability and availability running the end systems. But, its high-speed and light-weight encrypt scheme is valuable for our design the access control method in future networks.

In addition, from Secure and Scalable Internet Routing Architecture [17], Locator/ID Separation Protocol [18], which are the candidates of the Future Internet architecture, we can find that the separation of accessing and routing is the trend. This mechanism can enhance the security of the core part of the Internet efficiently. But, at the edge of the network, especially in the access network, there should have a good access control mechanism to provide high security for the whole network.

This paper considers access control in the network layer and proposes a universal access control method based on host identifiers. In the following sections, the paper presents the specific process of access control and its implementation in the universal network [19].

3. A universal access control method based on host identifiers

By analyzing and studying the technology of access control in traditional telecommunication and Internet deeply and systematically, we summarize the commonness of various access control mechanisms and design the Universal Access Control Method Based on Host Identifiers.

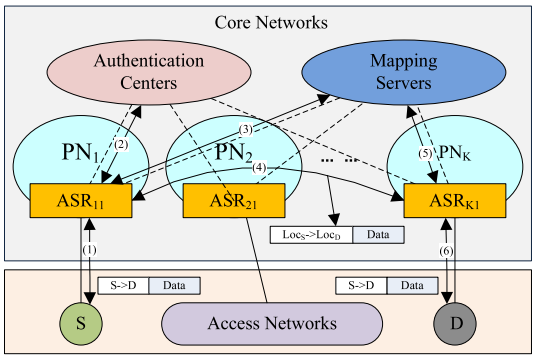


Fig. 1. The universal network model.

Our approach can be separated into two parts: one is the registration process, and the other is the authentication process. That is to say, if one end-node wants to access the network, it must register its identity information which can differ itself from others into the Authentication Center, which stores the registered information of every end-node in the registration process firstly. When an end-node attempts to use the network to communicate with others, it should finish the authentication process firstly before the communication.

In addition, we design the handover process to support the mobility of end-nodes and encryption process to prevent the threat of sniffer and clone from the third party in our method. The specifics of all the processes will be described in the following sections.

3.1. Terms

In order to illustrate our approach clearly, some important terms are given as follows:

- ***End-nodes***: generally refer to the various network terminals that can access the network, for example, PC, Telephone, MP, and SN.
- ***Accessing and Switching Router (ASR)***: responsible for providing the service of network access to end-nodes, authenticating end-nodes that want to access the network, assigning and maintaining the mapping relations between the accessing identifiers and the routing identifiers for the end-nodes which have passed the authentication, meanwhile mapping the identifiers of the packets and forwarding the packets in the network layer.
- ***Authentication Center (AUC)***: responsible for recording the information about the accessing identifiers and identity information of end-nodes, authenticating end-nodes when they try to access the network, and providing some necessary information about encryption between end-nodes and ASRs.
- ***Mapping Server***: responsible for restoring the mapping relations between AID and RID, and provides the service of resolving the mapping relations between AIDs and RIDs to the ASR, when the ASR has no caches of the mapping relations. It is located in the core networks and works with RIDs as the network identifiers.
- ***Accessing Identifier (AID)***: the identity of a host or router located in access networks. It is a network layer identifier. A host or router in access networks has one or more globally unique AID(s) which will not change under moving.
- ***Routing Identifier (RID)***: the locator of a host node. RID is also a network identifier. It is used in the core networks, and indicates the topological location of the host node in the network. RIDs of a host node are assigned by each accessing and switching router (ASR) to which the host node attaches.
- ***Host Identifier (HI)***: a kind of unreadable information which can indicate a unique end-node. It can be considered as a kind of host identity.

3.2. Overview of the universal network model

Before the specifics of the proposed access control method, we first introduce the universal network. The universal network is designed for the Future Internet that allows various kinds of terminals to access in a uniform way. It divides the whole network into two parts, access network and core network. The access network and the core network are in completely separated routing spaces. A mapping service is used to bridge them. Its structure and a simple communication process can be shown as Fig. 1.

As shown, the core network consists of a lot of provider networks (PNs), mapping servers and authentication centers. End hosts are located at access networks that connect with provider networks through accessing and switching routers (ASRs) at borders of provider networks. Whenever a source S wants to communicate with a destination D, it must pass the access authentication process among the source S, ASR and AUC through step (1) and (2) identified in the figure. Of course, the destination D also needs the network access permission to finish the communication. After the authentication processes, the ASR_{11} and ASR_{k1} will allocate routing identifiers to S and D and register the mapping relations to the mapping server,