Chapter III
An AAA Framework for IP Multicast Communication in Next Generation Networks

Prashant Pillai
University of Bradford, UK

Yim Fun Hu
University of Bradford, UK

ABSTRACT

IP multicast mechanisms provide efficient bandwidth consumption and distribution of high volume contents such as audio/video streaming, audio/video-on-demand and file sharing to multiple users. To commercially deploy multicast services in next generation networks it is important for Network Providers (NPs) to be able to control user access to the multicast content and to be able to account the multicast usage. This chapter compares some of the existing security mechanisms and highlights their inadequacies for providing efficient multicast security. The chapter then describes an AAA framework for IP multicast, which combines the IETF MSEC architecture with efficient AAA techniques to provide secure multicast content and to enable NPs to authenticate, authorise and provide efficient access control of end users requesting multicast content. This AAA framework also supports both post-paid and pre-paid accounting of users and allows the monitoring of session information like session duration and data volume for each multicast session.

INTRODUCTION

When an end user wants to access multicast content, he or she needs to send an Internet Group Management Protocol (IGMP) (Cain, 2002) *Join* message to its next hop router. Upon receiving the request, this router uses a multicast protocol such as Protocol Independent Multicast (PIM) (Estrin, 1998) for setting up a distribution tree so that the multicast data can be routed from the source to the receiver. As stated by Cain (2002), joining a multicast group is an "unprivileged operation", or in other words, in standard multicast operation, any end user (i.e. host device) is allowed to join any multicast group and gain access to multicast traffic without authentica-

tion. This implies that there is not a single mechanism defined to restrict access of the multicast traffic only to an authenticated and authorised set of users, or to inhibit un-authenticated users gaining access to multicast traffic, which are meant only for a specific user group. Hence NPs cannot limit or control the access to the multicast content making it impossible to account the users for their multicast service usages. In addition, these protocols do not enable the sender i.e. the Content Provider (CP) to know who is accessing the multicast data at any given time. Hence the sender cannot account users for the multicast usage, leading to an unclear business model for both the NP and the CP (Savola, 2005).

The traditional method of providing any form of accounting for multicast services is to associate it with security. In this mechanism, the multicast content is encrypted by the CP before transmission and the users who require access to this content have to request the security keys from the CP to decrypt the transmitted content. The CP may then charge these users to disclose the security keys to them. Though this provides a simple method in which the CP may charge users accessing the multicast content, it is merely a method to charge users once for providing the keys. This method does not provide the flexibility offered by standard Authentication, Authorisation and Accounting (AAA) protocols to allow access control by the NP, nor does it provide time and/or volume based pre-paid and post-paid charging. The Group Security Association and Key Management Protocol (GSAKMP) (Harney, 2006) and the Group Domain of Interpretation (GDOI) (Baugher, 2003) multicast security protocols based on the multicast security architecture (Baugher, 2005) defined by Internet Engineering Task Force (IETF) Multicast Security (MSEC) working group also use this traditional method for securing the multicast traffic. The biggest drawback with such a mechanism is that only the CP has the ability to control and charge the users. In a distributed architecture, the NP to which the user may be connected, has no control on the multicast usage and hence cannot charge the user for their network usage, making IP multicast service provision unattractive to the NP for commercial deployment. Since the NP has no control, a malicious user may send an IGMP *Join* message to join any multicast group with the intention to launch a Denial-of-Service attack.

AAA protocols such as RADIUS (Rigney, 2000) and Diameter (Calhoun, 2002) are being used very successfully and efficiently to ensure revenue generation for unicast by controlling the access to network resources. Similar AAA functionalities are also required for multicast services. Accounting multicast usage is most important for revenue generation in commercial networks. Hence it is required that the NP should be able to authenticate and authorise the user requesting access to the multicast content, measure the duration and volume of all multicast sessions and finally bill the user. In addition the multicast distribution trees should only be setup for authenticated users to prevent any denial-of-service attacks. This would prevent un-necessary network bandwidth consumption with data requested by an unauthenticated user.

Existing Multicast Security Mechanisms

The following sub-sections of the chapter describe some of the possible security architectures for securing multicast services by using existing multicast and security protocols.

IGAP

The Internet Group membership Authentication Protocol (IGAP) (Hayashi, 2003) (Hayashi, 2004) is based on the IGMP v2 protocol and is used for authentication of the join request sent by the multicast receiver to the first hop router. The protocol proposes to modify the IGMP v2 packet to include user specific information which can be used for authentication and accounting.

The procedure for user authentication using the IGAP protocol is shown in Figure 1where the user device initiates multicast access by sending an IGAP *Join* request to the IGAP router. This IGAP *Join* request consists of the group address of the multicast groups that the user is interested to receive data from and the user credentials, i.e. the username and password. If the Challenge-Response authentication mechanism is used, the process of requesting a *ChallengeID* and a subsequent response is added. On receiving this IGAP *Join* request, the IGAP router sends a RADIUS *Access-Request* to the backend RADIUS enabled AAA server. A Diameter enabled backend server may also be used. The AAA server can then authenticate the user and can then check the user profile to authorise the access request for the multicast content. If the user is a valid user and has the rights to