RADIUS Usage for SNMP SSH Security Model
draft-narayan-isms-sshsm-radius-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 21, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract


Requirements Language
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Table of Contents

1. Introduction .............................................. 3
2. Problem Statement ......................................... 3
3. RADIUS Integration Mechanism .............................. 3
   3.1. RADIUS Authentication ............................. 3
   3.2. RADIUS Authorization .............................. 4
      3.2.1. SNMP Service Authorization .................. 4
      3.2.2. SNMP User Authorization ..................... 5
      3.2.3. RADIUS protocol operation ................... 5
      3.2.4. RADIUS Authorize-Only protocol operation ..... 6
   3.3. RADIUS Authorize-Only Requirements ................. 6
   3.4. Attribute Interpretation ............................ 7
4. SSHSM and RADIUS Binding .................................. 7
   4.1. Binding the authenticated Principal ............... 7
   4.2. SNMP Service Authorization ....................... 7
   4.3. SNMP User Authorization ............................ 8
5. IANA Considerations ........................................ 8
6. Security Considerations .................................... 9
7. Acknowledgements .......................................... 9
8. References ................................................ 9
   8.1. Normative References .............................. 9
   8.2. Informative References ......................... 10
8. Authors’ Addresses ........................................ 11
9. Intellectual Property and Copyright Statements .......... 12
1. Introduction

This memo describes the usage of the Secure Shell Security Model (SSHSM) with a RADIUS authentication system.

Integration of SSHSM with RADIUS will enable the use of a RADIUS server infrastructure for SNMP authentication, which would provide centralized management of user accounts instead of managing accounts on every SNMP engine. The RADIUS server also allows for a common identity to be shared across several management protocols thereby removing the need for separate maintenance, and thereby reducing administrative overhead.

2. Problem Statement

The Secure Shell Security Model [sshsm] describes a Security Model for SNMP using the Secure Shell protocol using a transport mapping [tmsm]. The Secure Shell protocol [RFC4251] provides a secure transport channel [RFC4253] with support for channel authentication [RFC4252] via local accounts and integration with various external authentication and authorization servers such as RADIUS, Kerberos, TACACS, etc. This document describes only RADIUS integration. SSHSM requires the SNMP protocol to continue to handle authorization of individual SNMP requests, this authorization can happen well after the SSH channel has been established and requires the SNMP engine to have knowledge of the SNMP securityName and any additional binding that is required for SNMP authorization.

The RADIUS protocol [RFC2865] is a widely deployed means of authentication and authorization for network access and administrative access to network devices. The RADIUS protocol does not have explicitly separate requests for authentication and authorization and all authorization information is communicated during the authentication exchange. This limits implementation and deployment options for integration of SSHSM with the RADIUS protocol. This memo specifies a method for integration of SSHSM with the RADIUS protocol.

3. RADIUS Integration Mechanism

3.1. RADIUS Authentication

The Secure Shell (SSH) Authentication protocol [sshsm] describes how SSH integrates with various types of authentication credentials and systems. This document describes how SSHSH will utilize RADIUS authentication, and optionally RADIUS authorization, provided through
the SSH authentication process. Existing SSH implementations have
been integrated with RADIUS Client implementations, and form the
basis for the requirements of SSHSM to utilize existing, deployed
authentication systems.

RADIUS currently provides authentication methods compatible with
username and password mechanisms, MD5 Challenge mechanisms,
Extensible Authentication Protocol (EAP) mechanisms, and HTTP Digest
mechanisms. SSH integration with RADIUS traditionally used the
username and password mechanism. Sometimes this integration is via
well known service APIs such as Pluggable Authentication Method
(PAM). RADIUS will indicate a successful authentication by returning
an Access-Accept message. An Access-Reject message indicates
unsuccessful authentication.

3.2. RADIUS Authorization

The RADIUS protocol [RFC2865] provides user authentication and
authorization. The user authentication portion is pretty
straightforward. Upon presentation of identity and credentials the
user is either accepted or rejected. The authorization portion may
be thought of as service provisioning. Based on the configuration of
the user’s account with the RADIUS Server, upon authentication the
Network Access Server (NAS) is provided with instructions as to what
type of service to provide to the user. When that service
provisioning does not match the capabilities of the NAS, or of the
particular interface to the NAS over which the user is requesting
access, RFC 2865 [RFC2865] requires that the NAS MUST reject the
access request.

RADIUS Servers will usually populate Access-Accept messages with one
or more service provisioning attributes. For a description of the
basic set of attributes, refer to [RFC2865]. RFC 2865 describes
service provisioning attributes for management access to a NAS, as
well as various terminal emulation and packet forwarding services on
the NAS. For SSH usage, RADIUS provisions management access service.
RFC 2865 defines two types of management access service attributes,
one for privileged access to the Command Line Interface (CLI) of the
NAS and one for non-privileged CLI access. [radman] describes further
RADIUS service provisioning attributes for management access to the
NAS, including SNMP access. When SSHSM is used with RADIUS
authorization, the SNMP-related attributes defined in this document
SHOULD be used to provision SNMP access over SSH, using SSHSM.

3.2.1. SNMP Service Authorization

The most common usage of SSH is to provide remote access to the
operating system prompt (a shell environment). Access to the shell
prompt is provided upon successful authentication. Authorization is implicitly provided by the access control mechanisms of NAS’s operating system, e.g. permissions to invoke certain programs or access certain files. In order to utilize RADIUS authorization, and to provide for enforcement of authorization levels when connecting directly to an SNMP engine, via SSH, an explicit form of authorization is required. The following RADIUS attributes will be used to authorize SNMPv3 over SSH;

1. Service-Type with a value of Framed-Management.

Refer to [radman] for a detailed description of these attributes. From the perspective of SSHSM, these two attribute and value pairs indicate that the SSH session is authorized to use SNMP over that session. It is a matter of implementation detail as to which component provides the authorization checking.

3.2.2. SNMP User Authorization

One additional level of user authorization is useful in conjunction with SNMPv3, and in particular with SSHSM. The SNMP architectural model provides for a modular access control mechanism. One such mechanism is the View-Based Access Control Method (VACM). The User-Based Security Method (USM) integrates with VACM, by mapping the user identity as defined in USM to access rights within VACM. When using RADIUS authentication and authorization with SSHSM, it is possible to achieve a similar mapping of user identity to access rights. Rather than using a locally stored mapping table, as is the case with USM, SSHSM may take advantage of access rights information provisioned by RADIUS. Typically, this access rights information will be implemented at the RADIUS Server based on the group membership status of the user account. The RADIUS attribute that communicates the access rights group name is the Management-Policy-Id attribute. This attribute contains a printable string, which comprises a policy or group name of local scope to the NAS. The NAS will require a mapping of the group name to the specific access control method, e.g. VACM. This mapping will need to be provisioned in non-volatile store on each SNMP engine, however it is unlikely to change very often and is likely to be related to a broad category of access rights, e.g. read-only, read-write, security-manager, network-manager, etc. This mapping mechanism is implementation specific.

3.2.3. RADIUS protocol operation

The RADIUS protocol operates, at the most simple level, as a request-response mechanism. RADIUS Clients, with the NAS, initiate a transaction by sending a RADIUS Access-Request message to a RADIUS
Server, with which the client shares credentials. The RADIUS Server will respond with either an Access-Accept message or an Access-Reject message. In many deployments, the RADIUS Server will be handling request from many different types of NASes with different capabilities, and different types of interfaces, services and protocol support. In order to support a diverse environment, and to provision the appropriate set of services, it is helpful if the RADIUS Server knows something about the access request in addition to the user’s identity and credentials. The RADIUS Client will often include attributes in the Access-Request message that indicate the nature of the service that the user is requesting, as a hint to the RADIUS Server. In the case of SSHSM, the RADIUS Client SHOULD include the following hint attributes in Access-Request messages:

1. Service-Type with a value of Framed-Management.

3.2.4. RADIUS Authorize-Only protocol operation

The RADIUS protocol inherently couples authentication with authorization. Authorization data, i.e. service provisioning attributes, are included in the Access-Accept message. Some other authentication and authorization protocols, such as TACACS, separate out the authorization phase from the authentication phase.

Dynamic RADIUS [RFC3576] allows re-authorization of existing NAS sessions by means of a Change of Authorization (CoA) request. In this instance, a CoA sequence is initiated by a RADIUS Server. It may be possible to use CoA request with SSHSM. This is a topic for further study. When RADIUS is used to provide Authorize-Only types of provisioning, such as with RFC 3576, there is an expectation that the original authentication for the NAS session was provided by RADIUS, and in fact provided by the RADIUS Server that initiates the CoA request. RFC 2865 requires that any RADIUS Access-Request with a Service-Type of Authorize-Only contain the State attribute that was obtained from the RADIUS Server during the initial authentication. This State attribute serves as a form of "cookie" between the server and client.

3.3. RADIUS Authorize-Only Requirements

The usage of RADIUS by SSHSM does not require that RADIUS be able to provide a separate authorization only phase, but it is different. One use case for separate authorization is where the initial SSH session authentication is provided by an authentication service, such as Kerberos, and subsequent session authorization is desired from RADIUS. The RADIUS protocol was not designed to act as an authorize-only service for use with other forms of authentication services.
The current restriction that RADIUS CoA request be accompanied by a State attribute from the original RADIUS authentication effectively prohibit this mode of operation. This is a topic that requires additional study.

3.4. Attribute Interpretation

If a NAS conforming to this specification receives an Access-Accept packet containing a Service-Type or Framed-Management-Protocol attribute which it cannot apply, it MUST act as though it had received an Access-Reject. [RFC3576] requires that a NAS receiving a Change of Authorization Request (CoA-Request) reply with a CoA-NAK if the Request contains an unsupported attribute. It is recommended that an Error-Cause attribute with value set to "Unsupported Attribute" (401) be included in the CoA-NAK. As noted in [RFC3576], authorization changes are atomic so that this situation does not result in session termination and the pre-existing configuration remains unchanged. As a result, no accounting messages should be generated.

4. SSHSM and RADIUS Binding

4.1. Binding the authenticated Principal

The Secure Shell Protocol server [RFC4251] will invoke RADIUS authentication as part of "ssh-userauth" service. The SSH engine would retain the user name field of the SSH_MSG_USERAUTH_REQUEST message as part of the SSH environment after successful authentication. As part of processing Incoming messages the SSHSM will query the SSH engine to extract the username and map it an appropriate securityName. This mapping will available in the Local Configuration Database (LCD) and by default the securityName is set to the user name that was authenticated by SSH.

4.2. SNMP Service Authorization

Service authorization for SNMP can be handled in two ways. Service Authorization can be handled by the SSH engine, the SSH engine must check whether the user has access to the SNMP service by verifying the values of the Service-Type and Framed-Management-Protocol attributes. In case the requested service is not available, the server should disconnect the session.

The other alternative is for SSHSM to perform the service authorization, this will require the SSH engine to retain the Service-Type and Framed-Management-Protocol attributes returned by the RADIUS server in the SSH environment. As part of processing
Incoming messages the SSHSM will query the SSH engine for the 
Service-Type and Framed-Management and authorize the SNMP service. 
This alternative is less efficient since the decision to the 
disconnect the session happens as part of processing the first 
incoming SNMP packet.

This memo recommends the use of the SSH engine for service 
authorization.

4.3. SNMP User Authorization

SNMPv3 provides granular user authorization via the View-Based Access 
Control Model (VACM), currently the securityName is used to bind the 
principal authenticated by the User Security Model (USM) to 
authorization provided by VACM. SSHSM can continue to rely on this 
model for user authorization but this model does present some 
management challenges when dealing with RADIUS.

The use of RADIUS protocol is allow central management of users to 
prevent the proliferation of users to thousands of managed entities. 
Using the securityName as a binding for authorization would require 
these centrally managed users or binding between these users and the 
SNMP securityName to be defined on all SNMP engines, this undermines 
the purpose of a central RADIUS server.

One alternative suggested by this memo is to use user groups managed 
by the RADIUS server to create binding the binding between SSHSM and 
VACM. This user group communicated in Management-Filter-ID can be 
mapped into a VACM groupName. The current VACM specification has the 
vacmanSecurityToGroupTable, this table maps a combination of 
securityModel and securityName into a groupName which is used to 
define an access control policy for a group of principals. The SNMP 
engine can use an alternative mapping that relies on the Management- 
Filter-ID, this mapping can be implementation specific.

The Management-Filter-ID for a particular securityName can be 
acquired during the SSH session establishment but it would need to be 
stored as part of the SSH environment which would require 
implementation specific extensions. The alternative is for SSHSM to 
use a RADIUS Authorize-Only request to acquire the 
Management-Filter-ID while processing the first incoming SNMP 
request.

5. IANA Considerations

This document makes no request of IANA.
Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

This specification describes the use of RADIUS for purposes of authentication and authorization. Threats and security issues for this application are described in [RFC3579] and [RFC3580]; security issues encountered in roaming are described in [RFC2607].

This document specifies a new attribute that can be included in existing RADIUS packets, which are protected as described in [RFC3579] and [RFC3576]. See those documents for a more detailed description.

A Framed-Management-Protocol or Management-Policy-Id attribute sent by a RADIUS server may not be understood by the NAS which receives it. A legacy NAS not compliant with this specification may silently discard the Framed-Management-Protocol or Management-Policy-Id attributes while permitting the user to access the SNMP engine. This can lead to users improperly receiving management access to the NAS.

7. Acknowledgements

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Kaushik Narayan
Cisco Systems Inc.
10 West Tasman Drive
San Jose, CA  95134
USA

Phone: +1 408-526-8168
Fax:
Email: kaushik_narayan@yahoo.com

David Nelson
Enterasys Networks Inc.
50 Minuteman Road
Andover, MA 01810-1008
USA

Phone: +1 978-684-1330
Fax:
Email: dnelson@enterasys.com