RADIUS Usage for SNMP SSH Security Model
draft-narayan-isms-sshsm-radius-01.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 August 5, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

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. SSH and RADIUS authentication ........................ 4
   3.3. RADIUS Authorization ................................ 4
      3.3.1. SNMP Service Authorization ..................... 5
      3.3.2. SNMP User Authorization ......................... 5
      3.3.3. RADIUS protocol operation ....................... 6
      3.3.4. RADIUS Authorize-Only protocol operation ....... 6
   3.4. RADIUS Authorize-Only Requirements ................ 7
   3.5. Attribute Interpretation ............................ 7
   3.6. SSH Integration with RADIUS ........................ 7
4. IANA Considerations ...................................... 9
5. Security Considerations .................................. 9
6. Acknowledgements ....................................... 9
7. References .............................................. 9
   7.1. Normative References ............................... 9
   7.2. Informative References ............................. 10
Authors’ Addresses ........................................ 10
Intellectual Property and Copyright Statements ............ 12
1. Introduction

This memo describes the usage of the Secure Shell Security Model (SSHSM) with a Remote Authentication Dial-In User Service (RADIUS) authentication and authorization 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) [sshsm] describes a Security Model for SNMP using the Secure Shell protocol using a transport mapping [tmsm]. The Secure Shell protocol provides a secure transport channel with support for channel authentication [RFC4252] via local accounts and integration with various external authentication and authorization servers such as RADIUS, Kerberos, 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 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 RADIUS protocol provides authentication methods compatible with username and password mechanisms, MD5 Challenge mechanisms, Extensible Authentication Protocol (EAP) mechanisms, and HTTP Digest mechanisms. RADIUS will indicate a successful authentication by
returning an Access-Accept message. An Access-Reject message indicates unsuccessful authentication. SSH integration with RADIUS traditionally used the username and password mechanism.

3.2. SSH and RADIUS authentication

The Secure Shell (SSH) Authentication protocol [RFC4252] describes a generic authentication protocol and support multiple methods that can be used SSH servers to authenticate SSH clients, these methods include Public Key, Password and Host identity (hosts.equiv). The "password" method of SSH authentication primarily describes how passwords are acquired from the SSH client and transported to the SSH server, the interpretation of the password and validation against password databases is left to SSH server implementations.

SSH server implementations typically use the Pluggable Authentication Mechanism [pam] interface provided by operating systems such as Linux and Solaris to integrate with password based network authentication mechanisms such as RADIUS, TACACS+, Kerberos, etc. This document describes how SSHSM will utilize RADIUS authentication, and optionally RADIUS authorization, provided through the SSH authentication process. This document will rely of implementation specific integration of SSH and RADIUS to achieve these goals.

3.3. 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 on the RADIUS Server, and upon service "hint" attributes included in the Access-Request message, an Access-Accept message will provide the Network Access Server (NAS) with instructions as to what type of service teh NAS is 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 user’s 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.

### 3.3.1. 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.

### 3.3.2. 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.

### 3.3.3. 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 some cases, such as with EAP authentication methods, the RADIUS Server may respond with an Access-Challenge, in which case the RADIUS client will respond with another Access-Request. In many deployments, the RADIUS Server will be handling requests 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.

### 3.3.4. 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.

### 3.4. RADIUS Authorize-Only Requirements

The usage of RADIUS by SSHSM does not require that RADIUS be able to provide a separate authorization only phase, however it would be desirable to be able to do so. 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.

### 3.5. 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 packets should be generated.

### 3.6. SSH Integration with RADIUS

As mentioned in Section 3.2, the RADIUS client is often integrated with the SSH server using an intermediary such as Pluggable Authentication Modules (PAM) [pam]. It may also be integrated directly, and any such integration is a matter of implementaion. It is typical for host-based of the SSH server to use AAA services, such as RADIUS, simply for authentication. Any authorization is usually provided by the shell environment into which the remote user connects. For usage with SSHSM, there is no equivalent shell environment, and it may be useful for authorization data, e.g. RADIUS service provisioning attributes, to be utilized by the SSH server in making its decision to allow or deny an SSH connection. The RADIUS attributes of interest to SSHSM are described in Section 3.3.1 and Section 3.3.3. The ability of the SSH server to
use this kind of authorization information in session establishment is a matter of implementation. RADIUS clients export this type of information, and intermediate layers, such as PAM, provide mechanisms to pass these parameters through to the application that is using the AAA services, i.e. SSH.

Section 3.3.2 talks about the option of using RADIUS authorization information in an SNMP access control model, such as View-based Access Control Model (VACM). This option is the topic of current study. The modular SNMP architecture encourages models to restrict information that is shared across an Application Service Interface (ASI) to that which is model-independent. The Transport Mapping Security Model (TMSM) does use a cache, known as the tmStateReference, to keep information that is required by the underlying transport layer. It is possible, therefore, for an implementation of an access control model to make use of the content of the tmStateReference, in an implementation-dependent fashion, to obtain authorization parameters, passed to the TMSM by the underlying transport layer, e.g. SSH, which may have been received from an AAA service, e.g. RADIUS. Whether that is a recommended and secure practice, remains open for discussion.

Alternatively, the access control model could make use of AAA services directly, i.e. make calls to the RADIUS client, to obtain authorization information useful for access control. This is a second use case for an Authorize-Only operation in RADIUS. There are some practical limitations to that approach, however. The access control model identifies the principal requesting access by means of the securityName. When the access control information is configured in a local configuration store, as is the case with User-based Security Model (USM) and VACM, the access control model can look up the access rights in the local configuration store. If an access control model were to substitute a RADIUS authentication request transaction for the local lookup, it would need to take advantage of an Authorize-Only RADIUS operation, because the full authentication credentials are not available, just the securityName (User-Name). Currently, the RADIUS protocol prohibits the use of Authorize-Only operations unless they are tied to a previous, successful RADIUS authentication by means of a RADIUS State attribute. The only way an access control model would have access to the appropriate RADIUS State attribute would be for that information to be retrieved from a session-related cache, such as the tmStateReference. Thus, we degenerate to the previous alternative. Additional study is required.
4. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

5. 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 may be 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.

6. Acknowledgements

7. References

7.1. Normative References


July 2003.


7.2. Informative References


Authors’ Addresses

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

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

David Nelson
Independent contributor
72 Old Chester Road
Derry, NH  03038-4022
USA

Phone: +1 606-432-2796
Email: d.b.nelson@comcast.net
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).