Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 27, 2008

K. Narayan
Cisco Systems, Inc.
D. Nelson
Elbrys Networks, Inc.
February 24, 2008

Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models
draft-ietf-isms-radius-usage-02.txt

Status of this Memo

Copyright Notice

Abstract

This memo describes the use of a Remote Authentication Dial-In User Service (RADIUS) authentication and authorization service by Simple Network Management Protocol (SNMP) secure Transport Models to authenticate users and authorize creation of secure transport sessions. While the recommendations of this memo are generally applicable to a broad class of SNMP Transport Models, the examples

focus on the Secure Shell Transport Model.

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

1.1. General

This memo describes the use of a Remote Authentication Dial-In User Service (RADIUS) authentication and authorization service by Simple Network Management Protocol (SNMP) secure Transport Models to authenticate users and authorize creation of secure transport sessions. While the recommendations of this memo are generally applicable to a broad class of SNMP Transport Models, the examples focus on the Secure Shell Transport Model.

The RADIUS protocol is a widely deployed means of authentication and authorization for network access and administrative access to network devices. The RADIUS protocol enables centralized administration of user accounts and credentials thereby significantly improving manageability and scalability and reducing administrative overhead. The RADIUS protocol also provides the advantage of allowing a common identity to be used with or shared across disparate management protocols, since the other network management interfaces such as NETCONF are capable of authentication with the same RADIUS server.

In the context of this document, a Network Access Server (NAS) is a network device or host that contains an SNMP engine implementation, utilizing SNMP Transport Models. While it is customary in SNMP documents to indicate which subsystem performs specific processing tasks, in this document we leave such decisions to the implementer, as is customary for RADIUS documents, and simply specify NAS behavior. Such processing might be implemented in the secure transport module or in one or more modules of the SNMP engine.

1.2. RADIUS Operational Model

The RADIUS protocol [RFC2865] provides authentication and authorization services for network access devices, usually referred to as a Network Access Server (NAS). The RADIUS protocol operates, at the most simple level, as a request-response mechanism. RADIUS Clients, within 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.

RADIUS supports authentication methods compatible with plaintext username and password mechanisms, MD5 Challenge/Response mechanisms, Extensible Authentication Protocol (EAP) mechanisms, and HTTP Digest mechanisms. Upon presentation of identity and credentials the user is either accepted or rejected. RADIUS servers indicate a successful authentication by returning an Access-Accept message. An Access-

Reject message indicates unsuccessful authentication.

Access-Accept messages are typically populated with one or more service provisioning attributes, that control the type and extent of service provided to the user at the NAS. The authorization portion may be thought of as service provisioning. Based on the configuration of the user's account on the RADIUS Server, upon authentication the 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. 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. This memo describes specific RADIUS service provisioning attributes that are useful for use with secure transports and SNMP Transport Models.

RADIUS servers are often deployed on an enterprise- or organization-wide basis, covering a variety of disparate use cases. In such deployments, all NASes and all users are serviced by a common pool of RADIUS servers. In many deployments, the RADIUS Server will handle requests from many different types of NASes with different capabilities, and different types of interfaces, services and protocol support.

In order for a RADIUS server to make the correct authorization decision in all cases, the server will often need to know something about the type of NAS at which the user is requesting access, the type of service that the user is requesting, and the role of the user in the organization. For example, many users may be authorized to receive network access via a Remote Access Server (RAS), Virtual Private Network (VPN) server, or LAN access switch. Typically only a small sub-set of all users are authorized to access the administrative interfaces of network infrastructure devices, e.g. the Command Line Interface (CLI) or SNMP engine of switches and routers.

In order for the RADIUS server to have information regarding the type of access being requested, it is common for the NAS (i.e. the RADIUS client) to include "hint" attributes in the RADIUS Access-Request message, describing the NAS and the type of service being requested. This document recommends appropriate "hint" attributes for the SNMP Transport Model service type.

1.3. RADIUS Usage With Secure Transports

Some secure transport protocols that can be used with SNMP Transport Models have defined authentication protocols supporting several authentication methods. For example, the Secure Shell (SSH) Authentication protocol [RFC4252] supports multiple methods (Public Key, Password, Host-Based) to authenticate SSH clients.

SSH Server integration with RADIUS traditionally uses the username and password mechanism.

Secure transport protocols do not, however, specify how the transport interfaces to authentication clients, leaving such as implementation specific. For e.g., 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 often use the Pluggable Authentication Modules (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.

Secure transports do not typically specify how to utilize authorization information obtained from an AAA service, such as RADIUS. More often, user authentication is sufficient to cause the secure transport server to begin delivering service to the user. Access control in these situations is supplied by the application to which the secure transport server session is attached. For example, if the application is a Linux shell, the user's access rights are controlled by that user account's group membership and the file system access protections. This behavior does not closely follow the traditional service provisioning model of AAA systems, such as RADIUS.

1.4. SNMP Transport Models

The Transport Subsystem for SNMP [tmsm] defines a mechanism for providing transport layer security for SNMP, allowing protocols such as SSH and TLS to be used to secure SNMP communication. The Transport Subsystem allows the modular definition of Transport Models for multiple secure transport protocols. Transport Models rely upon the underlying secure transport for user authentication services. The Transport Model (TM) then maps the authenticated identity to a model-independent principal, which it stores in the tmStateReference. When the selected security model is the Transport Security Model (TSM), the expected behavior is for the securityName to be set by the TSM from the authenticated principal information stored in the tmStateReference by the TM.

The Secure Shell protocol provides a secure transport channel with support for channel authentication via local accounts and integration with various external authentication and authorization services such as RADIUS, Kerberos, etc. The Secure Shell Transport Model [sshtm] defines the use of the Secure Shell protocol as the basis for a Transport Model.

2. RADIUS Usage for SNMP Transport Models

There are three ways in which RADIUS may be used by SNMP Transport Models. These include (a) user authentication, (b) service authorization and (c) access control authorization. The first two items are discussed in detail in this memo, while the third item is a topic of current research, and beyond the scope of this document. This document describes the way in which RADIUS attributes and messages are applied to the specific application area of SNMP Transport Models.

User authentication for SNMP Transport Models has the same syntax and semantics as user authentication for any other network service. In the context of SNMP the "user" is thought of as a "principal" and may represent a host, an application or a human.

Service authorization allows a RADIUS server to authorize an authenticated principal to use SNMP over a specific secure Transport Model. This memo describes mechanisms by which such information can be requested from a RADIUS server and enforced within the NAS. The SNMP architecture, as described in RFC 3411, does not make a distinction between user authentication and service authorization. In the case of existing, deployed security models, such as the User-based Security Model (USM), this distinction is not significant. For the SNMP Transport Models and the SNMP Transport Security Model (TSM), this distinction is relevant, and perhaps important.

It is relevant because of the way in which SSH implementations have traditionally integrated with RADIUS Clients. Those SSH implementations traditionally seek to obtain user authentication (e.g. validation of a username and password) from an outside authentication service, often via a Pluggable Authentication Module (PAM) style interface. The service authorization in traditional SSH server implementations comes via the restrictions that the operating system (OS) shell (and file system, etc.) place on the user by means of access controls tied to the username or the username's membership in various user groups. These OS-style access controls are distinct from the service provisioning features of RADIUS. If we wish to use existing SSH server implementations, or slightly adapt them, for use with SNMP Transport Models, and we wish to support RADIUS-provisioned

service authorization, we need to be aware that the RADIUS service authorization information will need to be obtained by the relevant SNMP modules from the SSH module.

One reason that RADIUS-provisioned service authorization is important is that in many deployments the RADIUS server's back-end authentication database contains credentials for many classes of users, only a small portion of which may be authorized to access the management interfaces of managed entities (NASes) via SNMP. In the absence of RADIUS-provisioned service authorization, network management access may be granted to unauthorized, but properly authenticated, users.

Data object access control authorization in SNMP is handled by the Access Control Subsystem (ACS), instantiated as various Access Control Models. The SNMP architecture, as described in RFC 3411, explicitly mandates the separation of authentication and authorization operations in order to retain modularity of the SNMP system. The Abstract Service Interface (ASI) of the ACS uses method-independent parameters, including securityName, to determine access control rights. A detailed description of how an Access Control Model (ACM) might utilize the services of a RADIUS client to obtain access control policy information is the topic of current research, and beyond the scope of this document.

2.1. RADIUS Authentication for Transport Protocols

This document will rely of implementation specific integration of the transport protocols with RADIUS clients for user authentication.

It is RECOMMENDED that the integration of RADIUS clients with transport protocols utilize appropriate "hint" attributes in RADIUS Access-Request messages, to signal to the RADIUS server the type of service being requested over the transport session. Specific attributes for use with SNMP Transport Models are recommended in this document.

RADIUS servers, compliant to this specification, MAY use RADIUS hint attributes, as described herein, to inform the decision whether to accept or reject the authentication request.

2.2. RADIUS Authorization for Transport Protocols

In compliance with RFC 2865, NASes MUST enforce implicitly mandatory attributes, such as Service-Type, within an Access-Accept message. NASes MUST treat Access-Accept Messages that attempt to provision unsupported services as if they were an Access-Reject. NASes SHOULD treat unknown attributes as if they were provisioning unsupported

services. See [RFC5080] for additional details.

A NAS that is compliant to this specification, MUST treat any RADIUS Access-Accept message that provisions a transport protocol (e.g. SSH) that cannot be provided, and/or application service (e.g. SNMP) that cannot be provided over that transport, as if an Access-Reject message had been received instead. The RADIUS Service-Type attribute is the primary indicator of the service being provisioned, although other attributes may also convey service provisioning information. Specific attributes for use with SNMP Transport Models are recommended in this document.

For traditional SSH usage, RADIUS servers typically provision management access service, as SSH is often used to access the command line shell of a host system, e.g. the NAS. 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. These traditional management access services are not used with SNMP. [radman] describes further RADIUS service provisioning attributes for management access to the NAS, including SNMP access.

2.3. SNMP Service Authorization

The Transport Subsystem for SNMP [tmsm] defines the notion of a session, although the specifics of how sessions are managed is left to Transport Models. The Transport Subsystem defines some basic requirements for transport protocols around creation and deletion of sessions. This memo specifies additional requirements for transport protocols during session creation, and for session termination.

RADIUS servers compliant to this specification SHOULD use RADIUS service provisioning attributes, as described herein, to specify SNMP access over a secure transport protocol. Such RADIUS servers MAY use RADIUS hint attributes included in the Access-Request message, as described herein, in determining what, if any, service to provision.

NASes compliant to this specification MUST use RADIUS service provisioning attributes, as described in this section, when they are present in a RADIUS Access-Accept message, to determine whether the session can be created and MUST enforce the service provisioning decisions of the RADIUS server.

The following RADIUS attributes SHOULD be used, as hint attributes included in the Access-Request message to signal use of SNMP over a secure transport to the RADIUS server:

1. Service-Type with a value of Framed-Management.
2. Framed-Management-Protocol with a value of SNMP.
3. Management-Transport-Protection with a value of Integrity-Confidentiality-Protection.

Refer to [radman] for a detailed description of these attributes. From the perspective of the RADIUS Server, these attribute and value pairs indicate that the user is requesting to use SNMP over an SNMP Transport Model.

The following RADIUS attributes are used in an Access-Accept message to provision SNMP over a secure transport:

1. Service-Type with a value of Framed-Management.
2. Framed-Management-Protocol with a value of SNMP.
3. Management-Transport-Protection with a value of Integrity-Confidentiality-Protection.

Refer to [radman] for a detailed description of these attributes. From the perspective of the NAS, these attribute and value pairs indicate that the user is authorized to use SNMP using an SNMP Transport Model.

The following RADIUS attributes MAY be optionally used, to authorize use of SNMP over the default UDP transport protocol (no privacy):

1. Management-Transport-Protection with a value of No-Protection.

Refer to [radman] for a detailed description of this attribute. From the perspective of the NAS, this attribute and value pair indicates that the user is authorized to use SNMP using the default SNMP transport protocol, without a protected transport.

The following RADIUS attributes are used to limit the extent of a secure transport session carrying SNMP traffic, in conjunction with an SNMP Transport Model:

1. Session-Timeout
2. Inactivity-Timeout.

Refer to [RFC2865] for a detailed description of these attributes. From the perspective of the NAS, these attributes indicate session timeouts to be applied to the secure transport sessions. The Session-Timeout attribute indicates the maximum number of seconds that a session may exist before it is unconditionally disconnected. The Inactivity-Timeout attribute indicates the maximum number of seconds that a transport session may exist without any protocol activity (messages sent or received) before the session is

disconnected. These timeouts are enforced by the NAS.

2.4. SNMP Access Control Authorization

[radman] describes a RADIUS attribute that can be used for SNMP access control authorization, however, the details of how an SNMP Access Control Model, such as the View-based Access Control Model (VACM) [RFC3415], might utilize RADIUS authorization are the topic of current research, and beyond the scope of this document.

3. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Access-Request	Accept	Reject	Challenge	#	Attribute
0-1	0	0	0	1	User-Name [RFC2865]
0-1	0	0	0	2	User-Password [RFC2865]
0-1	0	0	0	4	NAS-IP-Address [RFC2865]
0-1	0-1	0	0	6	Service-Type [RFC2865]
0-1	0-1	0	0-1	24	State [RFC2865]
0	0-1	0	0	27	Session-Timeout [RFC2865]
0	0-1	0	0	28	Idle-Timeout [RFC2865]
0-1	0-1	0-1	0-1	80	Message-Authenticator [RFC3579]
0-1	0-1	0	0	TBA	Framed-Management-Protection [radman]
0-1	0-1	0	0	TBA	Management-Transport-Protection [radman]
0	0+	0	0	TBA	Management-Policy-Id [radman]

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present in a packet.
0+	Zero or more instances of this attribute MAY be present in a packet.
0-1	Zero or one instance of this attribute MAY be present in a packet.
1	Exactly one instance of this attribute MUST be present in a packet.

Note that this document does not describe the usage of RADIUS Accounting, nor Dynamic RADIUS Re-Authorization. Such RADIUS usages are not currently envisioned for SNMP, and are beyond the scope of this document.

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].

Additional security considerations for use of SNMP with secure Transport Models [tmsm] and the Transport Security Model [tsm] are found in the Security Considerations sections of the respective documents.

Note that if the SNMP Message Processing Module selects the SNMPv1 or SNMPv2c Security Model as the security model to use (because the message is SNMPv1 or SNMPv2), then securityName comes from the community name, as per RFC3584. This may not be what is expected when using an SNMP secure Transport Model.

Note that if the SNMP User-based Security Model is selected (because the SNMPv3 message contains a msgSecurityModel=USM), then securityName is determined using USM (after performing USM authentication). This may not be what is expected when using an SNMP secure Transport Model with an external authentication service, such as RADIUS.

The Message-Authenticator (80) attribute SHOULD be used with RADIUS messages that are described in this memo, as defined in [RFC3579].

6. Acknowledgements

The authors would like to acknowledge the contributions of David Harrington and Juergen Schoenwaelder for numerous helpful discussions in this space.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC4252] "The Secure Shell Authentication Protocol", 2005.

[radman] Nelson, D. and G. Weber, "Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management", draft-ietf-radext-management-authorization-02.txt (work in progress), February 2008.

[sshtm] Harrington, D. and J. Salowey, "Secure Shell Transport Model for SNMP", draft-ietf-isms-secshell-09.txt (work in progress), November 2007.

[tmsm] Harrington, D. and J. Schoenwaelder, "Transport Subsystem for the Simple Network Management Protocol (SNMP)", draft-ietf-isms-tmsm-11.txt (work in progress), November 2007.

[tsm] Harrington, D., "Transport Security Model for SNMP", draft-ietf-isms-transport-security-model-07.txt (work in progress), November 2007.

7.2. Informative References

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[RFC5080] Nelson, D. and A. DeKok, "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, December 2007.

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
Elbrys Networks, Inc.
75 Rochester Ave, Unit #3,
Portsmouth, NH 03801
USA

Phone: +1 (603) 570-2636
Email: d.b.nelson@comcast.net

Full Copyright Statement

Intellectual Property

Acknowledgment

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