RADEXT Working Group
INTERNET-DRAFT
Category: Informational
Expires: January 11, 2012
11 July 2011

D. Nelson (Editor)
Elbrys Networks, Inc.

Crypto-Agility Requirements for Remote Dial-In User Service (RADIUS)
draft-ietf-radext-crypto-agility-requirements-07.txt

Abstract

This memo describes the requirements for a crypto-agility solution for Remote Authentication Dial-In User Service (RADIUS).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and 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 January 11, 2012.

Table of Contents

1. Introduction

1.1. General

At the IETF-66 meeting, the RADIUS Extensions (RADEXT) Working Group was asked by members of the Security Area Directorate to prepare a formal description of a crypto-agility work item, and corresponding charter milestones. After consultation with one of the Security Area Directors, Russ Housley, text was initially proposed on the RADEXT WG mailing list on October 26, 2006:

> The RADEXT WG will review the security requirements for crypto-agility in IETF protocols, and identify the deficiencies of the existing RADIUS protocol specifications against these requirements. Specific attention will be paid to RFC 4962 [RFC4962].
>
> The RADEXT WG will propose one or more specifications to remediate any identified deficiencies in the crypto-agility properties of the RADIUS protocol. The known deficiencies include the issue of negotiation of substitute algorithms for the message digest functions, the key-wrap functions, and the password-hiding function. Additionally, at least one mandatory to implement cryptographic algorithm will be defined in each of these areas, as required.

This document describes the features, properties and limitations of RADIUS crypto-agility solutions, as well as defining the term "crypto-agility" as used in this context, and providing the motivations for this work.

The requirements defined in this memo have been developed based on e-mail messages posted to the RADEXT WG mailing list, which may be found in the archives of that list. The purpose of framing the requirements in this memo is to formalize and memorialize them for future reference, and to bring them explicitly to the attention of the IESG and the IETF Community, as we proceed with this work.

1.2. 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].

A RADIUS crypto-agility solution is not compliant with this specification if it fails to satisfy one or more of the MUST or MUST NOT statements. A solution that satisfies all the MUST, MUST NOT, SHOULD, and SHOULD NOT statements is said to be "unconditionally

compliant"; one that satisfies all the MUST and MUST NOT statements but not all the SHOULD or SHOULD NOT requirements is said to be "conditionally compliant".

1.3. Publication Process

RADIUS [RFC2865] is a widely deployed protocol that has attained Draft Standard status based on multiple independent interoperable implementations. Therefore it is desirable that a high level of interoperability be maintained for crypto-agility solutions.

To ensure that crypto-agility solutions published on the standards track are well specified and interoperable, the RADEXT WG has adopted a two phase process for standards-track publication of crypto-agility solutions.

In the initial phase, crypto-agility solutions adopted by the working group will be published as Experimental. These documents should contain a description of the implementations and experimental deployments in progress, as well as an evaluation of the proposal against the requirements described in this document.

The working group will then select proposals to advance on the standards track. Criteria to be used include evaluation of the proposal against the requirements, summary of the experimental deployment experience and evidence of multiple interoperable implementations.

2. A Working Definition of Crypto-Agility

Crypto-Agility is the ability of a protocol to adapt to evolving cryptography and security requirements. This may include the provision of a modular mechanism to allow cryptographic algorithms to be updated without substantial disruption to fielded implementations. It may provide for the dynamic negotiation and installation of cryptographic algorithms within protocol implementations (think of Dynamic-Link Libraries (DLL)).

In the specific context of the RADIUS protocol and RADIUS implementations, crypto-agility may be better defined as the ability of RADIUS implementations to automatically negotiate cryptographic algorithms for use in RADIUS exchanges, including the algorithms used to integrity protect and authenticate RADIUS packets and to hide RADIUS Attributes. This capability covers all RADIUS message types: Access-Request/Response, Accounting-Request/Response, CoA/Disconnect-Request/Response, and Status-Server. Negotiation of cryptographic algorithms MAY occur within the RADIUS protocol, or within a lower layer such as the transport layer.

Proposals MUST NOT introduce generic new capabilities negotiation features into the RADIUS protocol or require changes to the RADIUS operational model as defined in "RADIUS Design Guidelines" [RFC6158] Section 3.1 and Appendix A.4. A proposal SHOULD focus on the crypto-agility problem and nothing else. For example, proposals SHOULD NOT require new attribute formats and SHOULD be compatible with the guidance provided in [RFC6158] Section 2.3. Issues of backward compatibility are described in more detail in Section 4.3.

3. The Current State of RADIUS Security

RADIUS packets, as defined in [RFC2865], are protected by an MD5 message integrity check (MIC), within the Authenticator field of RADIUS packets other than Access-Request [RFC2865] and Status-Server [RFC5997]. The Message-Authenticator Attribute utilizes HMAC-MD5 to authenticate and integrity protect RADIUS packets.

While RADIUS does not support confidentiality of entire packets, various RADIUS attributes support encrypted (also known as "hidden") values, including: User-Password (defined in [RFC2865] Section 5.2), Tunnel-Password (defined in [RFC2868] Section 3.5), and various Vendor-Specific Attributes, such as the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes (defined in [RFC2548] Section 2.4). Generally speaking, the hiding mechanism uses a stream cipher based on a key stream from an MD5 digest. Attacks against this mechanism are described in "RADIUS Support for EAP" [RFC3579] Section 4.3.4.

"Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms" [RFC6151] discusses security considerations for use of the MD5 and HMAC-MD5 algorithms. While the advances in MD5 collisions do not immediately compromise the use of MD5 or HMAC-MD5 for the purposes used within RADIUS absent knowledge of the RADIUS shared secret, the progress toward compromise of MD5's basic cryptographic assumptions has resulted in the deprecation of MD5 usage in a variety of applications. As noted in [RFC6151] Section 2:

> MD5 is no longer acceptable where collision resistance is required such as digital signatures. It is not urgent to stop using MD5 in other ways, such as HMAC-MD5; however, since MD5 must not be used for digital signatures, new protocol designs should not employ HMAC-MD5.

4. The Requirements

4.1. Overall Solution Approach

RADIUS crypto-agility solutions are not restricted to utilizing technology described in existing RFCs. Since RADIUS over IPsec is

already described in "RADIUS and IPv6" [RFC3162] Section 5 and [RFC3579] Section 4.2, this technique is already available to those who wish to use it. Therefore, it is expected that proposals will utilize other techniques.

4.2. Security Services

Proposals MUST support the negotiation of cryptographic algorithms for per-packet integrity/authentication protection. Proposals also MUST support per-packet replay protection for all RADIUS message types. Crypto-agility solutions MUST specify mandatory-to-implement cryptographic algorithms for each defined mechanism.

Crypto-agility solutions MUST avoid security compromise, even in situations where the existing cryptographic algorithms utilized by RADIUS implementations are shown to be weak enough to provide little or no security (e.g. in event of compromise of the legacy RADIUS shared secret). Included in this would be protection against bidding down attacks. In analyzing the resilience of a crypto-agility solution, it can be assumed that RADIUS requesters and responders can be configured to require the use of new secure algorithms in the event of a compromise of existing cryptographic algorithms or the legacy RADIUS shared secret.

Guidance on acceptable algorithms can be found in [NIST-SP800-131A]. It is RECOMMENDED that mandatory-to-implement cryptographic algorithms be chosen from among those classified as "Acceptable" with no known deprecation date from within this or successor documents.

It is RECOMMENDED that solutions provide support for confidentiality, either by supporting encryption of entire RADIUS packets or by encrypting individual RADIUS attributes. Proposals supporting confidentiality MUST support the negotiation of cryptographic algorithms for encryption.

Support for encryption of individual RADIUS attributes is OPTIONAL for solutions that provide encryption of entire RADIUS packets. Solutions providing for encryption of individual RADIUS attributes are REQUIRED to provide support for improving the confidentiality of existing encrypted (sometimes referred to as "hidden") attributes as well as encrypting attributes (such as location attributes) that are currently transmitted in cleartext.

In addition to the goals referred to above, [RFC4962] Section 3 describes additional security requirements, which translate into the following requirements for RADIUS crypto-agility solutions:

Strong, fresh session keys

RADIUS crypto-agility solutions are REQUIRED to generate fresh session keys for use between the RADIUS client and server. In order to prevent the disclosure of one session key from aiding an attacker in discovering other session keys, RADIUS crypto-agility solutions are RECOMMENDED to support Perfect Forward Secrecy (PFS) with respect to session keys negotiated between the RADIUS client and server.

Limit key scope

In order to enable a NAS and RADIUS server to exchange confidential information such as keying material without disclosure to third parties, it is RECOMMENDED that a RADIUS crypto-agility solution support X.509 certificates for authentication between the NAS and RADIUS server. Manual configuration or automated discovery mechanisms such as NAI-based Dynamic Peer Discovery [RADYN] can be used to enable direct NAS-RADIUS server communications. Support for end-to-end confidentiality of RADIUS attributes is OPTIONAL.

For compatibility with existing operations, RADIUS crypto-agility solutions SHOULD also support pre-shared key credentials. However, support for direct communications between the NAS and RADIUS server is OPTIONAL when pre-shared key credentials are used.

4.3. Backwards Compatibility

Solutions MUST demonstrate backward compatibility with existing RADIUS implementations. That is, an implementation that supports both crypto-agility and legacy mechanisms MUST be able to talk with legacy RADIUS clients and servers (using the legacy mechanisms).

While backward compatibility is needed to ease the transition between legacy RADIUS and crypto-agile RADIUS, use of legacy mechanisms is only appropriate prior to the compromise of those mechanisms. After legacy mechanisms have been compromised, secure algorithms MUST be used, so that backward compatibility is no longer possible.

Since RADIUS is a request/response protocol, the ability to negotiate cryptographic algorithms within a single RADIUS exchange is inherently limited. Prior to receipt of a response, a requester will not know what algorithms are supported by the responder. Therefore, while a RADIUS request can provide a list of supported cryptographic algorithms which can be selected for use within a response, prior to the receipt of a response, the cryptographic algorithms utilized to provide security services within an initial request will need to be pre-determined.

In order to enable a request to be handled both by legacy as well as

crypto-agile implementations, a request can be secured with legacy algorithms was well as with attributes providing security services using more secure algorithms. This approach allows a RADIUS packet to be processed by legacy implementations as well as by crypto-agile implementations, and does not result in additional response delays. If this technique is used, credentials used with legacy algorithms MUST be cryptographically independent of the credentials used with the more secure algorithms, so that compromise of the legacy credentials does not result in compromise of the credentials used with more secure algorithms.

In this approach to backward compatibility, legacy mechanisms are initially used in requests sent between crypto-agile implementations. However, if the responder indicates support for crypto-agility, future requests can use more secure mechanisms. Note that if a responder is upgraded and then subsequently needs to be downgraded (e.g. due to bugs), this could result in requesters being unable to communicate with the downgraded responder unless a mechanism is provided to configure the requester to re-enable use of legacy algorithms.

Probing techniques can be used to avoid the use of legacy algorithms in requests sent between crypto-agile implementations. For example, an initial request can omit use of legacy mechanisms. If a response is received, then the recipient can be assumed to be crypto-agile and future requests to that recipient can utilize secure mechanisms. Similarly, the responder can assume that the requester supports crypto-agility and can prohibit use of legacy mechanisms in future requests. Note that if a requester is upgraded and then subsequently needs to be downgraded (e.g. due to bugs), this could result in the requester being unable to interpret responses, unless a mechanism is provided to configure the responder to re-enable use of legacy algorithms.

If a response is not received, in the absence of information indicating responder support for crypto-agility (such as pre-configuration or previous receipt of a crypto-agile response), a new request can be composed utilizing legacy mechanisms.

Since legacy implementations not supporting crypto-agility will silently discard requests not protected by legacy algorithms rather than returning an error, repeated requests can be required to distinguish lack of support for crypto-agility from packet loss or other failure conditions. Therefore probing techniques can delay initial communication between crypto-agile requesters and legacy responders. This can be addressed by upgrading the responders (e.g. RADIUS servers) first.

4.4. Interoperability and Change Control

Proposals MUST indicate a willingness to cede change control to the IETF.

Crypto-agility solutions MUST be interoperable between independent implementations based purely on the information provided in the specification.

4.5. Scope of Work

Crypto-agility solutions MUST apply to all RADIUS packet types, including Access-Request, Access-Challenge, Access-Reject, Access-Accept, Accounting-Request, Accounting-Response, Status-Server and CoA/Disconnect messages.

Since it is expected that the work will occur purely within RADIUS or in the transport, message data exchanged with Diameter SHOULD NOT be affected.

Proposals MUST discuss any inherent assumptions about, or limitations on, client/server operations or deployment and SHOULD provide recommendations for transition of deployments from legacy RADIUS to crypto-agile RADIUS. Issues regarding cipher-suite negotiation, legacy interoperability and the potential for bidding down attacks, SHOULD be among these discussions.

4.6. Applicability of Automated Key Management Requirements

"Guidelines for Cryptographic Key Management" [RFC4107] provides guidelines for when automated key management is necessary. Consideration was given as to whether or not RFC 4107 would require a RADIUS Crypto-Agility solution to feature Automated Key Management (AKM). It was determined that AKM was not inherently required for RADIUS based on the following points:

- RFC 4107 requires AKM for protocols that involve O(n^2) keys. This does not apply to RADIUS deployments, which require O(n) keys.
- Requirements for session key freshness can be met without AKM, for example, by utilizing a pre-shared key along with an exchange of nonces.
- RADIUS does not require the encryption of large amounts of data in a short time.
- Organizations already have operational practices to manage

existing RADIUS shared secrets to address key changes required as a result of personnel changes.

- The crypto-agility solution can avoid use cryptographic modes of operation such as a counter mode cipher that require frequent key changes.

However, at the same time, it is recognized that features recommended in Section 4.2 such as support for perfect forward secrecy and direct transport of keys between a NAS and RADIUS server can only be provided by a solution supporting AKM. As a result, support for Automated Key Management is RECOMMENDED within a RADIUS crypto-agility solution.

Also, automated key management is REQUIRED for RADIUS crypto-agility solutions that use cryptographic modes of operation that require frequent key changes.

5. IANA Considerations

This document makes no request of IANA.

6. Security Considerations

Potential attacks against the RADIUS protocol are described in [RFC3579] Section 4.1, and details of known exploits as well as potential mitigations are discussed in [RFC3579] Section 4.3.

This specification describes the requirements for new cryptographic protection mechanisms, including the modular selection of algorithms and modes. Therefore, the subject matter of this memo is all about security.

7. Acknowledgments

Thanks to all the reviewers and contributors, including Bernard Aboba, Mary Barnes, Pasi Eronen, Dan Romascanu, Joe Salowey and Glen Zorn.

8. References

8.1. Normative References

[NIST-SP800-131A]
Barker, E. and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST SP-800-131A, January 2011.

[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.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

[RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, July 2007.

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

[RFC6158] DeKok, A., "RADIUS Design Guidelines", BCP 158, RFC 6158, March 2011.

8.2. Informative References

[RADYN] Winter, S. and M. McCauley, "NAI-based Dynamic Peer Discovery for RADIUS over TLS and DTLS", Internet draft (work in progress), draft-ietf-radext-dynamic-discovery-03, July 2011.

[RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

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

[RFC5997] DeKok, A., "Use of Status-Server Packets in the Remote Authentication Dialin User Service (RADIUS) Protocol", RFC 5997, August 2010.

Author's Address

David B. Nelson
Elbrys Networks, Inc.
282 Corporate Drive, Unit 1
Portsmouth, NH 03801
USA

Email: d.b.nelson@comcast.net