To: INCITS Technical Committee T10
From: David L. Black, EMC
Email: black_david@emc.com
Date: November 4, 2008
Subject: SPC-4: IKEv2-SCSI Authentication (08-423r1)

1) *Revision history*

Revision 0 (Oct 29, 2008) First revision (r0)

Revision 1 (Nov 4, 2009) Major rewrite to put most of the added text in the model clause, plus reorganize affected portions of the model clause. (r1)

2) *Related documents*

spc4r16 – SCSI Primary Commands – 4
IETF RFC 4306 – Internet Key Exchange (IKEv2) Protocol
IETF RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
IETF RFC 5282 – Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol

3) *Overview*

Review of the IKEv2-SCSI specification has identified text that is incorrect when digital signatures are used for authentication. The erroneous text specifies that the recipient calculates the expected authentication value. This is applicable when a shared secret key is used for authentication (Shared Key Message Integrity Code), but is incorrect when a digital signature is used. This is because a digital signature is computed with the sender's private key, but the recipient checks it with the sender's public key. Asymmetric cryptography is used, so the recipient can check the signature, but cannot reproduce the signature on its own.

In considering how to correct this problem, a need has emerged for model clause material on IKEv2-SCSI authentication. This document proposes to add that model clause, where most of the corrections reside, and make the necessary changes elsewhere. This document also serves as a vehicle to make a couple of updates to Annex C, one of which has impacts elsewhere because it reflects IETF completion of standardization work motivated by IKEv2-SCSI.

Existing text is shown in **BLACK**, additions are shown in **GREEN**, text to be deleted is ~~**struck through in RED**~~ and comments (not to be included) are shown in **BLUE**.

Proposal:

2.5 IETF References

Remove RFC 3280 as it has been replace by RFC 5280

~~RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*~~

Add the following two references in the appropriate positions in the list of IETF RFCs:

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*

Editor: Please update all RFC 3280 references to reference RFC 5280.

5.14.4.3 ~~Handling of the Certificate Request payload and the Certificate payload~~ IKEv2-SCSI Authentication

5.14.4.3 becomes the new model material on IKEv2-SCSI authentication. The existing contents of 5.14.4.3 are moved to a subsection of 5.14.4.3. The existing contents of 5.14.4.5 are also moved to a subsection of 5.14.4.3.

5.14.4.3.1 Overview

IKEv2-SCSI authentication performs three primary security functions:

a) The application client and device server each establish an identity by demonstrating knowledge of a secret authentication key associated with that identity.
b) The application client demonstrates knowledge of the current device server capability information.
c) The application client and device server check the integrity of the current IKEv2-SCSI cryptographic command sequence (CCS). This prevents man-in-the-middle attacks on an IKEv2-SCSI CCS.

An IKEv2 SCSI authentication algorithm accomplishes these functions by generating and verifying a secure check value over specified input data. The input that is a concatenation of bytes that includes device server capability information and an appropriate portion of the IKEv2-SCSI parameter data from the Key Exchange step of the IKEv2-SCSI CCS.

A secret authentication key associated with an identity is used to generate a secure check value. IKEv2-SCSI conveys a secure check value in the AUTHENTICATION DATA field of the IKEv2-SCSI Authentication payload and conveys the associated identity in the IDENTIFICATION DATA field of the IKEv2-SCSI Identification payload. The recipient uses a verification key associated with the identity to validate correctness of the secure check value.

IKEv2-SCSI Authentication is bidirectional; both the application client and the device server perform authentication with each other. IKEv2-SCSI Authentication may be skipped when the application client and device server both agree to skip it during the Key Exchange step, see 5.14.4.6.

There are two classes IKEv2-SCSI Authentication methods:

a) Pre-Shared Key: The secret authentication key is also used as the verification key.
b) Digital Signature: The verification key and secret authentication key constitute a public/private key pair. The secure check value is a digital signature based on asymmetric cryptography.

Certificates and the IKEv2-SCSI Certificate payload may be used to provide verification keys for digital signatures to IKEv2-SCSI participants.

5.14.4.3.2 Pre-Shared Key Authentication

Pre-shared key authentication uses a single cryptographic algorithm to both generate and verify a secure check value. A pre-shared key is associated with an identity that is to be sent as IDENTIFICATION DATA in the Identification payload (see 7.6.5.3.4). The pre-shared key serves as both the authentication key and the verification key for the identity. The pre-shared key needs to be kept secret by both the application client and device server in order to avoid compromising IKEv2-SCSI security properties.

Generation of the secure check value shall consist of using the cryptographic algorithm and the pre-shared key associated with the identity to generate a secure check value for the specified input data.

Verification of the secure check value shall consist of using a verification key associated with the identification data received in the Identification payload from the other participant (see 7.6.3.5.4) and the specified input data to compute the expected contents of the AUTHENTICATION DATA field of the Authentication payload received from the other participant and comparing the expected contents of this field to the actual contents of the field. Verification is successful if the expected contents match the actual contents, otherwise verification is not successful.

The pre-shared key is provisioned and configured for use in the application client and device server by means outside the scope of this standard.

The contents of subclause 5.14.4.5 are moved to this location. Text that is unchanged from 5.14.4.5, except for relocation remains black.

~~If the Authentication payload (see 7.6.3.5.6) AUTHENTICATION DATA field contents are computed using pre-shared keys (e.g., if the applicable algorithm identifier is 00F9 0002h, Shared Key Message Integrity Code), then the~~ The following requirements for usage of pre-shared keys apply in addition to those found in RFC 4306:

a) A pre-shared key shall be associated with one identity;
b) The same pre-shared key shall not be used to authenticate both an application client and a device server;
c) Use of the same pre-shared key for a group of application clients or a group of device servers is strongly discouraged, because it enables any member of the group to impersonate any other member;
d) The means for provisioning pre-shared keys are outside the scope of this standard;
e) The pre-shared keys may be provisioned as follows:
    A) At the time of manufacturing;
    B) During device or system initialization; or
    C) Any time thereafter;

f) The following requirements from RFC 4306 apply to the interfaces for provisioning pre-shared keys:
   A) ASCII strings of at least 64 bytes shall be supported;
   B) A null terminator shall not be added to any input before it is used as a pre-shared key;
   C) A hexadecimal ASCII encoding of the pre-shared key shall be supported; and
   D) ASCII encodings other than hexadecimal may be supported. Support for any such encoding shall include specification of the algorithm for translating the encoding to a binary string as part of the interface;

and

g) Information about the size of the pre-shared key shall be stored at the same time that the pre-shared key is stored.

Editor: Please update cross-references to 5.14.4.5 to instead reference 5.14.4.3.2

5.14.4.3.3 Digital Signature Authentication

Digital signature authentication uses complementary signature and verification cryptographic algorithms to generate and verify a secure check value that is a digital signature. A public/private key pair is associated with the identity that is to be sent as IDENTIFICATION DATA in the Identification payload (see 7.6.5.3.4). The private key is used as the authentication key for the identity. The public key is used as the verification key for the identity. Each private authentication key needs to be kept secret in order to avoid compromising IKEv2-SCSI security properties.

Generation of the secure check value shall consist of using the private authentication key associated with the identity and the signature algorithm to generate a digital signature over the specified data.

Verification shall consist of using the public verification key associated with the identity received in the Identification payload from the other participant (see 7.6.3.5.4) and the specified input data to verify the digital signature received from the other participant as the contents of the AUTHENTICATION DATA field of the Authentication payload. Verification is successful if the digital signature is a valid digital signature over the specified data, otherwise verification is not successful.

The private authentication key is provisioned and configured for digital signature use by means outside the scope of this standard. If certificates are not used, the public verification key is also provisioned and configured for digital signature use by means outside the scope of this standard. If certificates are used, the public verification key is obtained from a certificate (see 5.14.4.3.4).

5.14.4.3.4 Certificates and Digital Signature Authentication

Certificates and the IKEv2-SCSI Certificate payload may be used to provide verification keys for digital signatures to IKEv2-SCSI participants. A certificate is a data structure that contains an identity, a public key for that identity and additional relevant information that may constrain use of the public key. A certificate is signed by a certification authority (CA), and that digital signature is part of the certificate data structure.

If the public key used to validate a digital signature is obtained from a certificate, the certification path from the certificate to a trust anchor should be validated (see RFC 5280); the digital signature check is not successful if the path cannot be validated, independent of whether the digital signature is valid. Certificates and trust anchors are provisioned and configured for use by means outside the scope of this standard.

Editors Note: Add CA to acronyms. May also need a certification authority definition.

A simple certificate use example is that an entity that trusts a CA uses the public key of the CA to validate a certificate presented as part of authentication; a successful validation establishes that the public key in the certificate is associated with the identity in the certificate, and that public key is then used to verify the security check value in the Authentication payload. In this example, providing a certificate as part of the IKEv2-SCSI Authentication step allows a single CA public key to serve as a trust anchor for verification of digital signatures for any identity that has been issued a certificate by the CA. This enables a single CA public key to be configured for authentication verification instead of configuring a public key for each identity. In full generality, multiple checks are involved in validating a certificate and the validation may traverse a certification path composed of multiple certificates, see RFC 5280.

The contents of Section 5.14.4.3 are moved here. Text unchanged except for location remains black.

As detailed in this subclause, a Certificate Request payload (see 7.6.3.5.5) in one set of parameter data requests the delivery of a Certificate payload (see 7.6.3.5.5) in the next set of parameter data transferred. The purpose of these IKEv2-SCSI protocol elements is as follows:

a) Each SA participant is allowed to require the delivery of a Certificate payload by the other SA participant for use in authentication; and
b) Each Certificate Request payload indicates the trust anchors (see RFC 4306) list used by the device server or application client when PKI-based Authentication is being used with certificates that are not self signed (see RFC ~~3280~~5280).

The presence of one or more Certificate Request payloads in the Key Exchange step SECURITY PROTOCOL IN command (see 5.14.4.8.3) parameter data indicates that the device server requires the application client to send a Certificate payload in the Authentication step SECURITY PROTOCOL OUT command (see 5.14.4.9.2).

The presence of one or more Certificate Request payloads in the Authentication step SECURITY PROTOCOL OUT command parameter list specifies that the application client requires the device server to send a Certificate payload in the Authentication step SECURITY PROTOCOL IN command (see 5.14.4.9.3).

If any Certificate payloads are included in the parameter data, the first Certificate payload shall contain the public key used to verify the Authentication payload. Additional Certificate payloads may be sent to assist in establishing a chain of trust from the certificate in the first payload to a trust anchor.

The application client and device server may use different authentication methods that require or do not require the use of Certificate payloads, and the presence or absence of Certificate Request payloads and Certificate payloads may vary in any of the commands described in this subclause.

Editor: Please update cross-references to 5.14.4.3 to instead reference 5.14.4.3.4

~~5.14.4.5 IKEv2-SCSI usage of pre-shared keys~~

The contents of section 5.14.4.5 are moved to 5.14.4.3.2 above. Remove this section, renumbering other sections (and cross-references to them) appropriately.

7.6.3.5.6 Authentication payload

In the middle of p.487 (after first numbered list):

When processing the Authentication step SECURITY PROTOCOL OUT command, the device server shall ~~compute the expected~~ verify the contents of the AUTHENTICATION DATA field by applying the algorithm specified by the ALGORITHM IDENTIFIER field in the SA_AUTH_OUT IKEv2-SCSI cryptographic algorithm descriptor in the IKEv2-SCSI SA Cryptographic Algorithms payload (see 7.6.3.5.12) in the Key Exchange step (see 5.14.4.8) as described in table 431 (see 7.6.3.6.6) and this subclause to the following concatenation of bytes:

No change to list of bytes to concatenate. Next change follows that list.

If the ~~expected~~ verification of the contents of the AUTHENTICATION DATA field ~~do not match actual contents of the AUTHENTICATION DATA field,~~ is not successful, then:

In the middle of p.488 (after first numbered list):

After GOOD status is received for the Authentication step SECURITY PROTOCOL IN command, the application client should ~~compute the expected~~ verify the contents of the AUTHENTICATION DATA field by applying the algorithm specified by the ALGORITHM IDENTIFIER field in the SA_AUTH_IN IKEv2-SCSI cryptographic algorithm descriptor in the IKEv2-SCSI SA Cryptographic Algorithms payload (see 7.6.3.5.12) in the Key Exchange step (see 5.14.4.8) as described in table 431 (see 7.6.3.6.6) and this subclause to the following concatenation of bytes:

No change to list of bytes to concatenate. Next change follows that list.

If the ~~expected~~ verification of the contents of the AUTHENTICATION DATA field ~~do not match actual contents of the AUTHENTICATION DATA field,~~ is not successful, then the application client should abandon the IKEv2-SCSI CCS and notify the device server that it is abandoning the IKEv2-SCSI CCS as described in 5.14.4.12.

7.6.3.6.2 Encryption algorithm (ENCR) IKEv2-SCSI cryptographic algorithm descriptor

Add "RFC 5282" as an additional Reference for the AES-CCM and AES-GCM rows in table 423.

7.6.3.6.6 IKEv2-SCSI authentication algorithm IKEv2-SCSI cryptographic algorithm descriptor

Add a new "Authentication Reference" column to table 431 between the Support and Reference columns (only these 3 columns are shown below), and rename the "Reference" column to "Algorithm Reference":

Description	Support	Authentication Reference
SA_AUTH_NONE	Optional	n/a
RSA Digital Signature with SHA-1 [a]	Optional	5.14.4.3.3
Shared Key Message Integrity Code	Optional	5.14.4.3.2
ECDSA with SHA-256 on the P-256 curve [a]	Optional	5.14.4.3.3
ECDSA with SHA-512 on the P-521 curve [a]	Optional	5.14.4.3.3
Vendor Specific	Optional	VS
Restricted	Prohibited	n/a
Reserved		

The reference in the Authentication Reference column specifies how the algorithm shall be used to generate and verify the contents of the AUTHENTICATION DATA field of the Authentication Payload.

C.1 IKEv2 protocol details and variations for IKEv2-SCSI

Modify item y) and add a new item ab) at the end of the list:

y) ~~The description of how combined mode algorithms are used in the Encrypted payload in this standard predates the definition of equivalent functionality in IETF standards.~~ IETF standards omit the Integrity transform instead of using AUTH_COMBINED;

ab) The critical (CRIT) bit is set to 1b in all IKEv2-SCSI payloads specified in this standard because they are required to be recognized by all implementations of IKEv2-SCSI. IETF RFC 4306 sets the Critical (C) bit to zero in all IKEv2 payloads specified in RFC 4306, but requires that all IKEv2 implementations recognize all payloads specified in RFC 4306.