Mobile Ad hoc Networking (MANET)
Internet-Draft
Updates: 7182 (if approved)
Intended status: Standards Track
Expires: January 23, 2015

C. Dearlove
BAE Systems ATC

July 22, 2014

Identity-Based Signatures for MANET Routing Protocols
draft-ietf-manet-ibs-00

Abstract

This document extends [RFC7182], which specifies a framework for, and specific examples of, integrity check values (ICVs) for packets and messages using the generalized packet/message format specified in [RFC5444]. It does so by defining an additional cryptographic function that allows the creation of an ICV that is an identity-based signature, defined according to the ECCSI (Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption) algorithm specified in [RFC6507].

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 23, 2015.

Copyright Notice

Table of Contents

1. Introduction

[RFC7182] defines ICV (integrity check value) TLVs for use in packets and messages that use the generalized MANET packet/message format defined in [RFC5444]. This specification extends the TLV definitions therein by defining two new cryptographic function code points that allow the use of an identity-based signature (IBS) as an ICV. An IBS has an additional property that is not shared by any of the previously specified ICVs, it not only indicates that the protected packet or message is valid, but also verifies the originator of the packet/message.

This specification assumes that each router (protocol participant) has an identity that may be tied to the packet or message. The router may have more than one identity, but will only use one for each ICV TLV. The cryptographic strength of the IBS is not dependent on the choice of identity.

Two options for the choice of identity are supported (the two code points allocated). In the first the identity can be any octet sequence (up to 255 octets) included in the ICV TLV. In the second, the octet sequence is preceded by an address, either the IP source address for a packet TLV, or the message originator address for a message or address block TLV. In particular, the second option allows just the address to be used as an identity.

Identity-based signatures, compared to the shared secret key ICVs specified in [RFC7182], allow identifying the originator of information in a packet or message. They thus allow additional security functions, such as revocation of an identity, and removing all information with a specific originator, if this is recorded - as it is for OLSRv2 [RFC7181], an expected user of this specification. When applied to messages (rather than packets) this can significantly reduce the damage that a compromised router can inflict on the network.

Identity-based signatures are based on forms of asymmetric (public key) cryptography - identity-based encryption (IBE). In terms of their use, IBE and IBS methods have a major advantage, and a major disadvantage, compared to more widely used public key cryptography solutions, such as RSA.

The advantage referred to is that each router can be configured once (for its key lifetime) by a trusted authority, independently of all other routers. Thus router A can connect to the authority (typically in a secure environment) to receive a private key, or can have a private key delivered securely (out of band) from the authority. During normal operation of the MANET, there is no need for the

trusted authority to be connected to the MANET, or even to still exist. Additional routers can be authorized, with no reference to previously authorized routers (the trusted authority must still exist in this case). A router's public key is its identity, which when tied to a packet or message (as is the case when using an address as, or as part of, the identity) means that there is no need for public key certificates or a certificate authority.

The disadvantage referred to is that the trusted authority has complete authority, even more so than a conventional certificate authority. Routers cannot generate their own private keys, only the trusted authority can do that. Through the master secret held by the trusted authority, it could impersonate any router (existing or not). When used for identity-based encryption (not part of this specification) the trusted authority can decrypt anything. However, note that the shared secret key options described in [RFC7182] also have this limitation.

There are alternative mathematical realizations of identity-based signatures. This specification uses one that has been previously published as [RFC6507], known as ECCSI (Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption). In common with other identity-based encryption/signature approaches, it is based on the use of elliptic curves. Unlike some, it does not use "pairings" (bilinear maps from a product of two elliptic curve groups to another group). It thus may be easier to implement, and more efficient, than some alternatives, although with a greater signature size than some. This specification allows the use of any elliptic curve that may be used by [RFC6507].

The computational load imposed by ECCSI (and, perhaps more so, other IBS methods) is not trivial, though depending significantly on the quality of implementation of the required elliptic curve and other mathematical functions. For a security level of 128 bits, the ICV data length is 129 octets, which is longer than for alternative ICVs specified in [RFC7182] (e.g., 32 octets for the similar strength HMAC-SHA-256). The signature format used could have been slightly shortened (to 97 octets) by using a compressed representation of an elliptic curve point, however at the expense of some additional work when verifying a signature, and loss of direct compatibility with [RFC6507], and implementations thereof.

The trusted authority is referred to in [RFC6507] as the KMS (Key Management Service). That term will be used in the rest of this specification.

2. Terminology

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

Additionally, this document uses the terminology of [RFC5444], [RFC6507], and [RFC7182].

3. Applicability Statement

This specification adds an additional option to the framework specified in [RFC7182] for use by [RFC5444] formatted packets and messages. It is applicable as described in [RFC7182], and subject to the additional comments in Section 6.

Specific examples of protocols for which this specification is suitable are NHDP [RFC6130] and OLSRv2 [RFC7181].

4. Specification

4.1. Cryptographic Function

This specification defines a cryptographic function named ECCSI that is implemented as specified as the "sign" function in Section 5.2.1 of [RFC6507]. To use that specification:

- The ICV is not calculated as cryptographic-function(hash-function(content)) as defined in [RFC7182], but (like the HMAC ICVs defined there) uses the hash function within the cryptographic function. The option "none" is not permitted for hash-function, and the hash function must have a known fixed length of N octets, as specified in Section 4.2.

- M in [RFC6507] is "content" as specified in in [RFC7182].

- ID, used in [RFC6507], is as specified in Section 4.3.

- KPAK, SSK and PVT, used in [RFC6507], are as specified in Sections 4.2 and 5.1.1 of [RFC6507], provided by the KMS.

The length of the signature is 4N+1 octets, as specified in [RFC6507], whose affine coordinate format (including an octet valued 0x04 to identify this) is used unchanged.

Verification of the ICV is not implemented by the receiver recalculating the ICV and comparing with the received ICV, as it is necessarily incapable of doing so. Instead the receiver evaluates the "verify" function described in Section 5.2.2 of [RFC6507], which may pass or fail.

To use that function M, KPAK, SSK and PVT are as specified above, while ID is deduced from the received packet or message, as specified in Section 4.3, using the <key-id> element in the <ICV-value>. This element need not match that used by the receiver, and thus when using this cryptographic function, multiple ICV TLVs differing only in their <key-id>, or in the choice of cryptographic function from the two defined in this specification, SHOULD NOT be used unless routers are administratively configured to recognize which to verify.

Routers MAY be administratively configured to reject a packet or message ICV TLV using ECCSI based on part or all of <key-id>; for example if this encodes a time after which this identity is no longer valid.

4.2. ECCSI parameters

Section 4.1 of [RFC6507] specifies parameters n, N, p, E, B, G, and q. The first of these, n, is specified as "A security parameter; the size in bits of the prime p over which elliptic curve cryptography is to be performed." For typical security levels (e.g., 128, 192 and 256 bits), n must be at least twice the required bits of security, see Section 5.6.1 of [NIST-SP-800-57].

Selection of an elliptic curve, and all related parameters, MUST be by administrative means, and known to all routers. This specification follows [RFC6507] with a RECOMMENDED selection to follow Appendix D.1.2 of [NIST-FIPS-186-4]. (Note that n in that document is q in [RFC6507].)

The parameter that is required by this specification is N, which is defined as Ceiling(n/8). The hash function used must create an output of size N octets. In particular for 128 bit security, and hence n = 256, N = 32, and the RECOMMENDED hash function is SHA-256. The signature (i.e. <ICV-data>) length is 4N + 1 octets, i.e., 129 octets for N = 32.

Note: [RFC6507] actually refers to the predecessor to [NIST-FIPS-186-4], but the latest version is specified here; there are no significant differences in this regard.

4.3. Identity

There are two options for the identity ID used by [RFC6507], which are indicated by there being two code points allocated for this cryptographic function, see Section 5.

- For the cryptographic function ECCSI ID is the element <key-id> defined in Section 12.1 of [RFC7182]. This MUST NOT be empty.

- For the cryptographic function ECCSI-ADDR, ID is the concatenation of an address (in network byte order) and the element <key-id> defined in Section 12.1 of [RFC7182], where the latter MAY be empty. For a packet TLV this address is the IP source address of the IP datagram in which this packet is included. For a message TLV or an address block TLV this address is the message originator address (the element <msg-orig-addr> defined in [RFC5444]) if that address is present, if not present and the message is known to have travelled only one hop, then the IP source address of the IP datagram in which this message is included is used, otherwise no address is defined and the message MUST be rejected. (Note that HELLO messages specified in NHDP [RFC6130] and used in OLSRv2 [RFC7181] always only travel one hop, and hence their IP source address SHOULD be used if no originator address is present.)

Note that this identity is formatted by [RFC6507], and thus does not need a length field incorporated into it by this specification.

5. IANA Considerations

IANA has, in accordance with [RFC7182], defined a registry for the cryptographic functions. IANA is requested to modify this allocation as indicated.

Value	Algorithm	Description	Reference
7	ECCSI	ECCSI [RFC6507]	This specification
8	ECCSI-ADDR	ECCSI [RFC6507] with an address (source or originator) joined to identity	This specification
9-251		Unassigned; Expert Review	

Table 1: Cryptographic Function Registry

6. Security Considerations

This specification extends the security framework for MANET routing protocols specified in [RFC7182] by the addition of an additional cryptographic function, in two forms according to how identity is specified.

This cryptographic function implements a form of identity-based signature (IBS), a stronger form of integrity check value (ICV) that verifies not just that the received packet or message is valid but that the packet or message originated at a router that was assigned a private key for the specified identity.

For a message the identity is, and for a packet it is recommended that it is, either the originator address of the router (i.e., an address unique to that router), or the originator address with additional information appended. The use of that additional information is outside the scope of this specification, a typical use may be to indicate an expiry time for signatures created using that identity.

In common with other forms of IBS, a feature of the form of IBS (known as ECCSI) used in this specification is that it requires a trusted authority (KMS) that issues all private keys, and has complete cryptographic information about all possible private keys. However to set against that, the solution is scalable, as all routers can be independently keyed, and does not need the KMS in the network. If no future keys will be required, then the KMS's master secret can be destroyed. As routers are individually keyed, key revocation (by blacklist and time expiry of keys) is possible, but is beyond the scope of this specification.

ECCSI is based on elliptic curve mathematics. This specification follows [RFC6507] in its recommendation of elliptic curves, but any suitable (prime power) elliptic curve may be used; this must be administratively specified. Implementation of this specification will require an available implementation of suitable mathematical functions. Unlike some other forms of IBS, ECCSI requires only basic elliptic curve operations, it does not require "pairings" (bilinear functions of a product of two elliptic curve groups). This increases the available range of suitable mathematical libraries.

7. Acknowledgments

The author would like to thank his colleagues who have been involved in identity-based security for ad hoc networks, including (in alphabetical order) Alan Cullen, Peter Smith and Bill Williams.

8. References

8.1. Normative References

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

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format", RFC 5444, February 2009.

[RFC6507] Groves, M., "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)", RFC 6507, February 2012.

[RFC7182] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 7182, April 2014.

8.2. Informative References

[NIST-FIPS-186-4] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS 186-4, July 2013.

[NIST-SP-800-57] National Institute of Standards and Technology, "Recommendation for Key Management - Part 1: General (Revision 3)", SP 800-57, Part 1, Revision 3, July 2012.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

Appendix A. Example

TBD.

Author's Address

Christopher Dearlove
BAE Systems Advanced Technology Centre
West Hanningfield Road
Great Baddow, Chelmsford
United Kingdom

Phone: +44 1245 242194
Email: chris.dearlove@baesystems.com
URI: http://www.baesystems.com/