Working Group
Internet-Draft
Intended status: Informational
Expires: April 27, 2012

U. Chunduri
A. Tian
Ericsson Inc.,
October 25, 2011

Using IKEv2 with TCP-AO
draft-chunduri-karp-using-ikev2-with-tcp-ao-00

Abstract

This document analyzes the TCP based pairwise Routing Protocol (RP) requirements for IKEv2 Key Management Protocol (KMP). This document discusses the various authentication methods available for peer authentication in IKEv2 KMP and the specific Security Association (SA) requirements for IKEv2 protocol to protect the TCP based pairwise RPs.

Table of Contents

1. Introduction

Threat analysis for TCP based routing protocols (BGP [RFC4271], PCEP [RFC5440], MSDP [RFC3618] and LDP [RFC5036]) is detailed in [ietf-karp-routing-tcp-analysis]. KARP design guide [ietf-karp-design-guide] suggests various requirements and options for getting keys to protect the routing protocols and recommends using KMP to automate the key establishment and rekeying to protect the routing protocols.

This document analyzes the TCP based pairwise Routing Protocol (RP) requirements for IKEv2[RFC5996] Key Management Protocol (KMP).

One of the services provided by IKEv2 KMP is peer authentication. This happens before traffic keys are established between IKEv2 peers. As IKEv2 KMP provides a raft of authentications methods, Section 2 discusses various Symmetric, Asymmetric and EAP based KMP authentication options available for all TCP based routing protocols. This document also provides guidelines for designing suitable approach for routing environments.

This document analyzes one approach, which minimizes the changes for routing protocols (BGP, PCEP, MSDP and LDP) to be integrated with KMP. This document defines the interface between all TCP based pairwise routing protocols and the TCP-AO [RFC5925]. The interface between IKEv2 KMP and the TCP-AO for session parameter negotiation, key establishment and rekeying is also defined in Section 3.

Currently IKEv2 can establish only Security Association (SA) for IP Security (IPSec). Few extensions are needed for IKEv2 to establish SA for TCP based routing protocols that use TCP-AO. Section 4 discusses a brief summary of the extensions required for IKEv2 protocol for key establishment, traffic selectors negotiation and Security Association (SA) establishment for TCP based routing protocols.

1.1. 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 RFC 2119 [RFC2119].

1.2. Acronyms

EAP - Extensible Authentication Protocol

KDF - Key Derivation Function

KMP - Key Management Protocol (auto key management)

MKM - Manual Key management Protocols

NONCE - Number Once

2. Applicable Authentications methods

One advantage that IKEv2 provides is the largest selection of authentication methods suitable for various environments. The goal of this section is to look at various KMP authentications options available and recommend suitable options for deployment with routing protocols.

As some of the authentication mechanisms are optional in IKEv2, one mandatory authentication mechanism from the list below need to be selected for routing environments to ensure inter-operability and quicker adoption. This section attempts to summarize the available options and constraints surrounding the options.

2.1. Symmetric key based authentication

IKEv2 [RFC5996] allow for authentication of the IKEv2 peers using a symmetric pre-shared key. For symmetric pre-shared key based peer authentication, the deployments need to consider the following as per [RFC5996]:

1. Deriving a shared secret from a password, name, or other low-entropy source is not secure. These sources are subject to dictionary and social-engineering attacks, among others.

2. The pre-shared key should not be derived solely from a user-chosen password without incorporating another source of randomness.

3. If password-based authentication for bootstrapping the IKE_SA, then one of the EAP methods as described in Section 2.3 need to be used.

One of the IPsecME WG charter goals is to provide IKEv2 [RFC5996] a secure password authentication mechanism which is protected against off-line dictionary attacks without requiring the use of certificates or Extensible Authentication Protocol (EAP), even when using the low-entropy shared secrets. There are couple of documents which try to address this issue and the work is still in progress.

2.2. Asymmetric key based authentication

Another peer authentication mechanism for IKEv2 is with asymmetric key certificates or public key signatures. This approach will use the Public Key Infrastructure using X.509 (PKIX) Certificates. If this can be deployed for IKEv2 peer authentication, it will be one of the most secure authentication mechanisms. With this authentication option, there is no need for out-of-band shared key between the peers for mutual authentication.

Apart from RSA and DSS digital signatures for public key authentication provided by IKEv2, [RFC4754] introduces Elliptic Curve Digital Signature Algorithm (ECDSA) signatures. ECDSA provides additional benefits including computational efficiency, small signature sizes, and minimal bandwidth compared to other available digital signature methods.

2.3. EAP based authentication

In addition to supporting authentication using shared secrets and public key signatures, IKEv2 also supports authentication based on Extensible Authentication Protocol (EAP), defined in [RFC3748]. EAP is an authentication framework that supports multiple authentication mechanisms. IKEv2 provides EAP authentication since it was recognized that public key signatures and shared secrets are not flexible enough to meet the requirements of many deployment scenarios. For KARP KMP, EAP-Only Authentication in IKEv2 as specified in [RFC5998] can be explored.

By using EAP, IKEv2 KMP can leverage existing authentication infrastructure and credential databases, since EAP allows users to choose a method suitable for existing credentials. Routing protocols today use password based pre-shared key to integrity protect the routing protocol messages. The same pre-shared key can be used to bootstrap the KMP and as a potential authentication key in KMP. With appropriate password based EAP methods, stronger keys can be generated without using certificates.

For authenticating the nodes running routing protocols, EAP and the IKEv2 endpoints are co-located (no separate EAP server required). When EAP is deployed, authenticating the IKEv2 responder using both EAP and public key signatures could be redundant. EAP methods that offer mutual authentication and key agreement can be used to provide responder authentication in IKEv2 completely based on EAP.

Section 4 of [RFC5998] lists safe EAP methods to support EAP_ONLY_AUTHENTICATION. For routing protocols deployment, as EAP server is co-located with IKEv2 responder, channel binding capability

of the selected EAP method is irrelevant. Various qualified mutual authentication methods are listed in [RFC5998] and out of these, password based methods [RFC4746], [RFC5931], [RFC6124] can offer potential EAP alternative for pre-shared key only authentication.

Out of the list above, Encrypted Key Exchange (EKE) as described in [RFC6124] is relatively light weight and provides mutual authentication. This method also offers a secure and robust authentication, even with a operator provisioned weak password in the presence of a strong adversary.

3. Interfaces

Section 1.2 of TCP-AO [RFC5925] says "..we recommend the use of IPsec and IKE, especially where IKE's level of existing support for parameter negotiation, session key negotiation, or rekeying are desired." - but such interface is not defined. As IKEv2 [RFC5996] is being discussed as the potential KMP for routing protocols, this section defines the interface between IKEv2 KMP and TCP-AO. This section also analyzes the interface between TCP based routing protocols (BGP, LDP, MSDP, PCEP) and the TCP-AO module.

3.1. RP interface to TCP-AO

When a routing protocol is configured to use KMP (by not specifying the keys or through some other means), configured authentication algorithms and rekey life time is provisioned in the TCP-AO MKT. This can be achieved at the time of opening the socket. With this, the MKT created in TCP-AO contains all the configured information other than the keys to protect the underlying session.

3.2. TCP-AO interface to KMP

There needs to be a way to trigger the KMP to initiate negotiation with provisioned parameters, to rekey and to maintain the negotiated sessions. In this section, we define a common interface between TCP-AO and KMP that can be used by all TCP based routing protocols. (An alternative approach is to define an interface for each routing protocols to trigger KMP directly. This alternative is not of scope for this document.)

Following are the details of the interface between TCP-AO and KMP:

1. When the first SYN packet on the session is initiated, a trigger to negotiate the session specific parameters with all provisioned authentication algorithms and optionally key lifetime should be given to KMP.

2. A KMP session identifier need to be stored and should be used for rekeying the existing session.

3. MKT IDs as specified in Section 3.1 of TCP-AO [RFC5925], requires a SendID and a RecvID for each MKT, which are mutually agreed by the connection endpoints. These 1-byte quantities need to be part of MKT when the KMP key(s) are populated in MKT.

4. KMP negotiated authentication algorithm and optionally life time for traffic keys for each session, need to be populated in MKT.

5. Trigger may also be needed at the time of rekeying any particular session. Implementations can pro-actively negotiate new traffic keys before the life time of current traffic keys expire.

4. Extensions required for IKEv2 protocol

There can be two ways to derive a KMP that is suitable for TCP based routing protocols:

a. To create a new KMP for routing protocols based on IKEv2 as proposed in [mahesh-karp-rkmp].

b. Extend IKEv2 to make it suitable for TCP based routing protocols.

In this section, we would like to explore option b).

This section summarizes the extensions required for IKEv2 to negotiate non-ipsec SAs for tcp based routing protocols. Authors acknowledge, some of the items below are already discussed in KARP WG but the details presented here are different.

Routing protocols by deploying extended IKEv2 KMP, can continuously benefit from the new authentication methods and any other new features which might be added.

4.1. Non IPSec DOI

IKEv2 is designed for performing mutual authentication with the peer and establishing and maintaining Security Associations for IPSec. IKEv2 defined IKE_AUTH and CREATE_CHILD_SA exchange, consist of payloads, and processing guidelines for IPSec Domain of Interpretation (DOI) and this need to be generalized to exchange other protocol specific parameters.

IKEv2 CREATE_CHILD_SA exchange today can also be used to rekey the IKE SA and the master key. This document do not propose any changes

or extensions to re-establishing IKE SA through CREATE_CHILD_SA exchange.

4.1.1. Security Association Extensions

The Security Association (SA) payload, is used to negotiate attributes of a Security Association. This contains multiple proposals as configured in the routing protocol. Possible extensions to be made are:

1. Protocol ID, to be added in the proposal substructure with TCP-AO as new protocol.

2. Integrity Algorithm (INTEG), defined in the transform substructure need to be mandated for the new TCP-AO Protocol. Authentication algorithms as defined in [RFC5926] should be extended to the current list in IKEv2.

3. New transform type need to be created to represent the TCP-AO KeyIDs. Initiator KeyID represents the SendID and the Responder KeyID represents the RecvID in the TCP-AO MKT.

4. Diffie-Hellman group (D-H) transform type can be used for TCP_AO proposal as an optional transform.

5. Valid transform types for TCP-AO with mandatory and optional types need to be listed. Attribute negotiation rules need to be extended for TCP-AO protocol.

4.2. Simple Traffic Selectors Negotiation

The Traffic Selectors defined in IKEv2 [RFC5996] has huge potential to negotiate the particular traffic to be secured, agreeable to both initiator and responder. But for routing protocol SA, traffic selectors negotiation present a simple case and does not require any changes. A single connection or multiple connections with a different source port to be protected, can be negotiated with one CREATE_CHILD_SA exchange. The IP Protocol ID in the traffic selector field as defined in Section 3.13.1 of [RFC5996] can always be TCP for the routing protocol SAs.

The above is an attempt to summarize the brief list of changes with the approach and this section will be revisited further.

5. IANA Considerations

This document defines no new namespaces.

6. Security Considerations

This document does not introduce any new security threats for IKEv2 [RFC5925] or TCP-AO [RFC5996] protocol. For more detailed security considerations please refer the Security Considerations section of the KARP Design Guide [I-D.ietf-karp-design-guide] document as well as KARP threat document [I-D.ietf-karp-threats-reqs].

7. Acknowledgements

The authors would like to thank Joel Halpern for initial discussions and providing feedback on the document.

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.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, June 2010.

[RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, June 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC5998] Eronen, P., Tschofenig, H., and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2", RFC 5998, September 2010.

8.2. Informative References

[I-D.ietf-karp-design-guide]
Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", draft-ietf-karp-design-guide-02 (work in progress), March 2011.

[I-D.ietf-karp-routing-tcp-analysis]
Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP, and MSDP Security According to KARP Design

Guide", draft-ietf-karp-routing-tcp-analysis-00 (work in progress), June 2011.

[I-D.ietf-karp-threats-reqs]
Lebovitz, G., Bhatia, M., and R. White, "The Threat Analysis and Requirements for Cryptographic Authentication of Routing Protocols' Transports", draft-ietf-karp-threats-reqs-03 (work in progress), June 2011.

[I-D.mahesh-karp-rkmp]
Jethanandani, M., Weis, B., Patel, K., Zhang, D., and S. Hartman, "Key Management for Pairwise Routing Protocol", draft-mahesh-karp-rkmp-00 (work in progress), October 2011.

[RFC3618] Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)", RFC 3618, October 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

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

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4746] Clancy, T. and W. Arbaugh, "Extensible Authentication Protocol (EAP) Password Authenticated Exchange", RFC 4746, November 2006.

[RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 4754, January 2007.

[RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", RFC 5036, October 2007.

[RFC5440] Vasseur, JP. and JL. Le Roux, "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, March 2009.

[RFC5931] Harkins, D. and G. Zorn, "Extensible Authentication Protocol (EAP) Authentication Using Only a Password", RFC 5931, August 2010.

[RFC6124] Sheffer, Y., Zorn, G., Tschofenig, H., and S. Fluhrer, "An EAP Authentication Method Based on the Encrypted Key Exchange (EKE) Protocol", RFC 6124, February 2011.

Authors' Addresses

Uma Chunduri
Ericsson Inc.,
300 Holger Way,
San Jose, California 95134
USA

Phone: 408 750-5678
Email: uma.chunduri@ericsson.com

Albert Tian
Ericsson Inc.,
300 Holger Way,
San Jose, California 95134
USA

Phone: 408 750-5210
Email: albert.tian@ericsson.com