Router Keying for BGPsec
draft-ietf-sidr-rtr-keying-08

Abstract

   BGPsec-speaking routers are provisioned with private keys to sign BGP
   messages; the corresponding public keys are published in the global
   RPKI (Resource Public Key Infrastructure) thereby enabling
   verification of BGPsec messages. This document describes two ways of
   provisioning the public-private key-pairs: router-driven and
   operator-driven.

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."

1. Introduction

BGPsec-speaking routers are provisioned with private keys, which
allow them to digitally sign BGP messages. To verify the signature,
the public key, in the form of a certificate [I-D.ietf-sidr-bgpsec-
pki-profiles], is published in the RPKI (Resource Public Key
Infrastructure). This document describes two methods for
provisioning the necessary public-private key-pairs: router-driven
and operator-driven.

The difference between the two methods is where the keys are
generated: on the router in the router-driven method and elsewhere in
the operator-driven method. Routers are expected to support either
one, the other, or both methods to work in various deployment
environments. Some routers may not allow the private key to be off-
loaded while other routers may. Off-loading of private keys would
support swapping of routing engines which could then have the same
private key installed in the soon-to-be online engine that had
previously been installed in the soon-to-be removed card.

The remainder of this document describes how operators can use the
two methods to provision new and existing routers.

Note: [I-D.ietf-sidr-bgpsec-pki-profiles] specifies the format for
the PKCS #10 request and [I-D.ietf-sidr-bgpsec-algs] specifies the
algorithms used to generate the signature.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to
be interpreted as described in RFC 2119 [RFC2119] only when they
appear in all upper case. They may also appear in lower or mixed
case as English words, without normative meaning.

Readers are assumed to be familiar with the BGPsec protocol [I-
D.ietf-sidr-bgpsec-overview][I-D.ietf-sidr-bgpsec-protocol] and the
RPKI [RFC6480] as well as the BGPsec-specific PKI (Public Key
Infrastructure) specifications [I-D.ietf-sidr-bgpsec-pki-profiles][I-
D.ietf-sidr-bgpsec-algs].

3. Provisioning a New Router

Depending on the options supported by the new router, operators are
free to use either the router-driven or operator-driven methods.

Regardless of the method chosen, operators first establish a secure
communication channel (e.g., via SSH (Secure Shell)) between the
operator's management platform and the router to allow the operator
to securely use the Command Line Interface (CLI). How this channel
is established is router-specific and is not in scope of this
document. Though other configuration mechanisms might be used, e.g.
NetConf (see [RFC6470]), in the remainder of this document, the
secure communication channel between the server and the router is
assumed to be an SSH-protected CLI.

Encryption, integrity, authentication, and key exchange algorithms
used by the secure communication channel SHOULD be of comparable
strength to BGPsec keys, which currently is 128-bit, or stronger than
BGPsec keys. In other words for the encryption algorithm, do not use
export grade crypto (40-56 bits of security), do not use Triple DES
(112 bits of security), do use something like or better than AES-128:
aes128-cbc [RFC4253] and AEAD_AES_128_GCM [RFC5647]; for integrity
use something like hmac-sha2-256 [RFC6668] or AESAD_AES_128_GCM
[RFC5647]; for authentication use something like ecdsa-sha2-nistp256
[RFC5656], and; for key exchange use something like ecdh-sha2-
nistp256 [RFC5656].

Note that some routers support the use of public key certificates and
SSH. The certificates used for the SSH session are different than
the certificates used for BGPsec.   The certificates used with SSH
should also enable a level of security commensurate with BGPsec keys;
x509v3-ecdsa-sha2-nistp256 [RFC6187] could be used for
authentication.

3.1. Router-Generated Keys

In the router-driven method, once the SSH-protected CLI session is
established between the operator and the router, the operator issues
a command, or commands, for the router to generate the public/private
key pair, to generate the PKCS#10 request, and to sign the PKCS#10
with the private key. Once generated, the PKCS#10, which includes
the public key the router wants certified, is transmitted to the RPKI
CA for the CA to certify. This can be via a number of means, two of
which might be as follows:

   o Through the SSH-protected CLI session with the operator's RPKI
     management platform: The operator off-loads the PKCS#10 and
     uploads the request to the CA. If the CA is operated by an
     external entity, external network connectivity likely is
     required.

   o Between the router and the CA: The operator, through a command or
     commands, prompts the router to send/transfer the PKCS#10 request

to the CA over the network. Obviously for this to work, the
router requires network connectivity with the CA and if the CA is
operated by an external entity external network connectivity may
be required.

After the CA certifies the key, it does two things:

o Publishes the certificate in the Global RPKI. The CA must have
  connectivity to the relevant publication point, which in turn
  must have external network connectivity as it is part of the
  Global RPKI.

o Returns the certificate to the operator's management station or
  to the router, normally packaged in a PKCS#7, using the
  corresponding method by which it received the certificate
  request.

With network connectivity, the router and CA can exchange the
certificate request and the certificate using the application/pkcs10
media type [RFC5967] and application/pkcs7-mime [RFC5751],
respectively, with the FTP [RFC2585], the HTTP [RFC2585], or the EST
(Enrollment over Secure Transport) [RFC7030].

The router SHOULD extract the certificate from the PCKCS#7 and verify
that the private key it holds corresponds to the returned public key.
The router SHOULD inform the operator that the certificate was
received; by some mechanism which is out of scope of this document.
The router SHOULD inform the operator whether or not the keys
correspond, again by a mechanism which is out of scope for this
document.

The router SHOULD also verify that the returned certificate validates
back to a trust anchor. To perform this verification either the CA's
certificate needs to be installed on the router via the CLI or the
CA's certificate needs to be returned along with the router's
certificate in the PKCS#7. The router SHOULD inform the operator
whether or not the signature validates to a trust anchor; this
notification mechanism is out of scope. After performing these
checks, the router need not retain the CA's certificate because the
certificate is not transmitted as part of BGPsec messages.

Note that even if the operator cannot extract the private key from
the router, this signature still provides a linkage between a private
key and a router. That is the server can verify the proof of
possession (POP), as required by [RFC6484].

3.2. Operator-Generated Keys

In the operator-driven method, the operator generates the
public/private key pair and installs the private key into the router
over the SSH-protected CLI session. Note that cut/copy and paste
operations for keys over a certain sizes are error-prone.

The operator uses RPKI management tools to generate the keys, the
PKCS#10 certification request, the certificate, and the PKCS#7
certification response, as well as publishing the certificate in the
Global RPKI. External network connectivity may be needed if the
certificate is to be published in the Global RPKI.

Along with the PKCS#7, the operator returns the private key. The
private key is encapsulated in a PKCS #8 [RFC5958], the PKCS#8 is
further encapsulated in CMS (Cryptographic Message Syntax) SignedData
[RFC5652], and signed by the AS's EE (End Entity) certificate.

The router SHOULD verify the signature of the encapsulated PKCS#8 to
ensure the returned private key did in fact come from the operator,
but this requires that the operator also provision via the CLI or
include in the SignedData the RPKI CA certificate and relevant AS's
EE certificate(s). The router should inform the operator whether or
not the signature validates to a trust anchor; this notification
mechanism is out of scope.

The router SHOULD extract the certificate from the PKCS#7 and verify
that the private key corresponds to the returned public key. The
router SHOULD inform the operator whether it successfully received
the certificate; this mechanism is out of scope. The router should
inform the operator whether or not the keys correspond; this
mechanism is out of scope. The router SHOULD also verify the
returned certificate back to a trust anchor, but to perform this
verification either the CA's certificate needs to be installed on the
router via the CLI or the CA's certificate needs to be returned along
with the router's certificate in the PKCS#7. The router SHOULD
inform the operator whether or not the signature validates to a trust
anchor; this notification mechanism is out of scope. After
performing these checks, the router need not retain the CA
certificate.

Note: The signature on the PKCS#8 and Certificate need not be made by
the same entity. Signing the PKCS#8, permits more advanced
configurations where the entity that generates the keys is not CA.

4. Key Management

An operator's responsibilities do not end after key generation, key
provisioning, certificate issuance, and certificate distribution.
They persist for as long as the operator wishes to operate the

BGPsec-speaking router.

Paramount to maintaining a router that can be a continuous BPGsec speaker is ensuring that the router has a valid certificate at all times. To ensure this, the operator needs to ensure the router always has a non-expired certificate. That is the key used when BGP-speaking always has an associated certificate whose expiry time is after the current time.

Ensuring this is not terribly difficult but requires that either:

  o The router has a mechanism to notify the operator that the
    certificate has an impending expiration, and/or

  o The operator notes the expiry time of the certificate and uses a
    calendaring program to remind them of the expiry time. It is
    advisable that the expiration warning happen well in advance of
    the actual expiry time, and/or

  o The RPKI CA warns the operaor of pending expiration, and/or

  o Use some other kind of automated process to search for and track
    the expiry times of router certificates.

Regardless of the technique used to track router certificate expiry times, it is advisable to notify additional operators in the same organization as the expiry time approaches thereby ensuring that the forgetfulness of one operator does not affect the entire organization.

Depending on inter-operator relationship, it may be appropriate to notify a peer operator that one or more of their certificates are about to expire.

Routers that support multiple private keys also greatly increase the chance that routers can continuously speak BGPsec because the new private key and certificate can be obtained prior to expiration of the operational key. Obviously, the router needs to know when to start using the new key. Once the new key is being used, having the already distributed certificate ensures continuous operation.

Whether the certificate is rekeyed (i.e., different key in the certificate with a new expiry time) or renewed (i.e., the same key in the certificate with a new expiry time) depends on the key's lifetime and operational use. Arguably, rekeying the router's BGPsec certificate every time the certificate expires is more secure than renewal because it limits the private key's exposure. However, if the key is not compromised the certificate could be renewed as many

times as allowed by the operator's security policy. Routers that
support only one key can use renewal to ensure continuous operation,
assuming the certificate is renewed and distributed prior to the
operational's certificate expiry time.

Certain unfortunate circumstances exist when the operator will need
to revoke the router's BGPsec certificate. When this occurs, the
operator needs to use the RPKI CA system to revoke the certificate by
placing the router's BGPsec certificate on the CRL (Certificate
Revocation List) as well as rekeying the router's certificate.

When it is decided that an active router key is to be revoked, the
process of requesting the CA to revoke, the process of the CA
actually revoking the router's certificate, and then the process of
rekeying/renewing the router's certificate, (possibly distributing a
new key and certificate to the router), and distributing the status
takes time during which the operator must decide how they wish to
maintain continuity of operations, with or without the compromised
private key, or whether they wish to bring the router offline to
address the compromise.

Keeping the router operational and BGPsec-speaking is the ideal goal,
but if operational practices do not allow this then reconfiguring the
router to disabling BGPsec is likely preferred to bringing the router
offline.

Routers which support more than one private key, where one is
operational and the other(s) are soon-to-be-opertional, facilitate
revocation events because the operator can configure the router to
make a soon-to-be-operational key operational, request revocation of
the compromised key, and then make a new soon-to-be-operational key,
all hopefully without needing to take offline or reboot the router.
For routers which support only one operational key, the operators
should create or install the new private key, and then request
revocation of the compromised private key.

5. Other Use Cases

Current router code generates private keys for uses such as SSH, but
the private keys may not be seen or off-loaded via the SSH-protected
CLI session or any other means. While this is good security, it
creates difficulties when a routing engine or whole router must be
replaced in the field and all software which accesses the router must
be updated with the new keys. Also, any network based initial contact
with a new routing engine requires trust in the public key presented
on first contact.

To allow operators to quickly replace routers without requiring

update and distribution of the corresponding public keys in the RPKI,
routers SHOULD allow the private BGPsec key to be off-loaded via the
SSH-protected CLI, NetConf (see [RFC6470]), SNMP, etc. This lets the
operator upload the old private key via the mechanism used for
operator-generated keys, see Section 3.2.

6. Security Considerations

Operator-generated keys could be intercepted in transport and the
recipient router would have no way of knowing a substitution had been
made or that the key had been disclosed by a monkey in the middle.
Hence transport security is strongly RECOMMENDED. As noted in
Section 3, the level of security provided by the transport security
SHOULD be commensurate with the BGPsec key. Additionally, operators
SHOULD ensure the transport security implementation is up to date and
addresses all known implementation bugs.

All generated key pairs MUST be generated from a good source of non-
deterministic random input [RFC4086] and the private key MUST be
protected in a secure fashion. Disclosure of the private key leads
to masquerade [RFC4949]. The local storage format for the private
key is a local matter.

Though the CA's certificate is installed on the router and used to
verify the returned certificate is in fact signed by the CA, the
revocation status of the CA's certificate is not checked. The
operator MUST ensure that installed CA certificate is valid.

Operators need to manage their SSH keys to ensure only those
authorized to access the router may do so. As employees no longer
need access to the router, their keys SHOULD be removed from the
router.

7. IANA Considerations

This document has no IANA Considerations.

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.

   [RFC4086]   Eastlake 3rd, D., Schiller, J., and S. Crocker,
               "Randomness Requirements for Security", BCP 106, RFC 4086,
               June 2005.

   [RFC4253]   Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH)
               Transport Layer Protocol", RFC 4253, January 2006.

   [RFC5652]   Housley, R., "Cryptographic Message Syntax (CMS)", STD 70,
               RFC 5652, September 2009.

   [RFC5958]   Turner, S., "Asymmetric Key Packages", RFC 5958, August
               2010.

   [I-D.ietf-sidr-bgpsec-algs]
               Turner, S., "BGP Algorithms, Key Formats, & Signature
               Formats", draft-ietf-sidr-bgpsec-algs (work in progress).

   [I-D.ietf-sidr-bgpsec-pki-profiles]
               Reynolds, M., Turner, S., and S. Kent, "A Profile for
               BGPSEC Router Certificates, Certificate Revocation Lists,
               and Certification Requests",
               draft-ietf-sidr-bgpsec-pki-profiles (work in progress).

8.2. Informative References

   [I-D.ietf-sidr-bgpsec-overview]
               Lepinski, M. and S. Turner, "An Overview of BGPSEC",
               draft-ietf-sidr-bgpsec-overview (work in progress).

   [I-D.ietf-sidr-bgpsec-protocol]
               Lepinski, M., "BGPSEC Protocol Specification",
               draft-ietf-sidr-bgpsec-protocol (work in progress).

   [RFC2585]   Housley, R. and P. Hoffman, "Internet X.509 Public Key
               Infrastructure Operational Protocols: FTP and HTTP",
               RFC 2585, May 1999.

   [RFC4253]   Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH)
               Transport Layer Protocol", RFC 4253, January 2006.

   [RFC4949]   Shirey, R., "Internet Security Glossary, Version 2", FYI

                36, RFC 4949, August 2007.

    [RFC5647] Igoe, K. and J. Solinas, "AES Galois Counter Mode for the
               Secure Shell Transport Layer Protocol", RFC 5647, August
               2009.

    [RFC5656] Stebila, D. and J. Green, "Elliptic Curve Algorithm
               Integration in the Secure Shell Transport Layer",
               RFC 5656, December 2009.

    [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet
               Mail Extensions (S/MIME) Version 3.2 Message
               Specification", RFC 5751, January 2010.

    [RFC5967] Turner, S., "The application/pkcs10 Media Type", RFC 5967,
               August 2010.

    [RFC6187] Igoe, K. and D. Stebila, "X.509v3 Certificates for Secure
               Shell Authentication", RFC 6187, March 2011.

    [RFC6470] Bierman, A., "Network Configuration Protocol (NETCONF)
               Base Notifications", RFC 6470, February 2012.

    [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support
               Secure Internet Routing", RFC 6480, February 2012.

    [RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate
               Policy (CP) for the Resource Public Key Infrastructure
               (RPKI)", BCP 173, RFC 6484, February 2012.

    [RFC6668] Bider, D. and M. Baushke, "SHA-2 Data Integrity
               Verification for the Secure Shell (SSH) Transport Layer
               Protocol", RFC 6668, July 2012.

    [RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed.,
               "Enrollment over Secure Transport", RFC 7030, October
               2013.

Authors' Addresses

   Sean Turner
   IECA, Inc.
   3057 Nutley Street, Suite 106
   Fairfax, Virginia 22031
   US

   Email: turners@ieca.com

   Keyur Patel
   Cisco Systems
   170 West Tasman Drive
   San Jose, CA 95134
   US

   Email: keyupate@cisco.com

   Randy Bush
   Internet Initiative Japan, Inc.
   5147 Crystal Springs
   Bainbridge Island, Washington 98110
   US

   Phone: +1 206 780 0431 x1
   Email: randy@psg.com