Network Working Group
Internet-Draft
Intended status: BCP
Expires: November 15, 2012

S. Turner
IECA, Inc.
K. Patel
Cisco Systems
R. Bush
Internet Initiative Japan, Inc.

May 14, 2012

Router Keying for BGPsec
draft-ietf-sidr-rtr-keying-00

Abstract

BGPsec-speaking routers must be provisioned with private keys and the corresponding public key must be published in the global Resource PKI. This document describes two ways of doing so, 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."

This Internet-Draft will expire on November 15, 2012.

Copyright Notice

Table of Contents

1. Introduction

BGPsec-speaking routers must be provisioned with private keys and the corresponding public key must be published in the global RPKI (Resource Public Key Infrastructure). Note that the public key is published in the RPKI in the form of a certificate [I-D.ietf-sidr-bgpsec-pki-profiles]. This document describes two methods for generating the necessary public/private key-pair: router-driven and operator-driven.

In the router-driven method, the router generates its own public/private key-pair, uses the private key to sign a certification request [I-D.ietf-sidr-bgpsec-pki-profiles] (a PKCS#10 - includes the public key), and sends the certification request to the RPKI CA (Certification Authority). The CA returns a PKCS#7, which includes the certified public key in the form of a certificate, to the router and the CA also publishes the certificate in the RPKI.

The router-driven model mirrors the model used by most PKI subscribers. In many cases, the private key never leaves trusted storage (e.g., HSM (Hardware Security Model)). This is by design and supports CPs (Certification Policies), often times for human subscribers, that require the private key only ever be controlled by the subscriber to ensure that no one can impersonate the subscriber. For non-humans, this model does not always work. For example, when an operator wants to support hot-swappable routers the same private key needs to be installed in the soon-to-be online router that was installed in the soon-to-be offline router. This motivated the operator-driven model.

In the operator-driven model, the operator generates the private/public key-pair and sends it to the router in a PKCS#8 [RFC5958].

In both cases, the key pair is for algorithms defined in [I-D.ietf-sidr-bgpsec-algs]. The first version specifies ECDSA on the P-256 curve.

2. Terminology

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].

It is assumed that the reader understands BGPsec, see [I-D.lepinski-bgpsec-overview], [I-D.lepinski-bgpsec-protocol], the RPKI, see [RFC6480], and [I-D.ietf-sidr-bgpsec-pki-profiles].

3. Router-Generated Keys

For router-generated keys, the public/private keys are made by the router, a PKCS#10 is made by the router, and signed by the private key, and is transferred to the RPKI CA. The CA returns a PKCS#7, the operator transfers the PKCS#7 to the router, and the router picks the certificate out of the PKCS#7. Even if the operator can not get the private key off the router this still provides a linkage between a private key and a router.

4. Operator-Generated Keys

For operator-generated keys, the public/private keys are made by the operator with their RPKI management software. The private key pair MUST be as specified in [RFC5915], which supports ECDSA keys. That format MUST then be inserted to a PKCS#8 [RFC5958] along with the certificate. If the operator wants to ship the keys around they can use the .p8 file extension and optional PEM encoding also from [RFC5958].

EDITOR NOTE: One thing we should consider is whether the certificate needs to returned to the router like in the router-generated keys method. PKCS#8 supports including the certificate so it's not a big deal to add it if we do.

5. Provisioning a New Router

When commissioning a new router, the operator may use either of the above methods.

Using the Router-Generated Keys method, see Section 3, the operator decides on the AS number and the BGP RouterID of the router, logs on to the new router using the craft port, ssh, etc., and requests that the router generate a public/private key-pair and generate and sign (with the private key) a PKCS#10 request. The operator then off-loads the PKCS#10 request and uploads the request to their RPKI software management tools. The tools create and publish the RPKI Router-Key object for the public key, and return the PKCS#7. The operator uploads the PKCS#7 to the router which then extracts its certificate.

The router MAY use the PKCS#7 as an indicator that the certificate request was actually processed, and SHOULD verify that the issued certificate actually corresponds to the private key the router holds.

Using the Operator-Generated Key method, see Section 4, the operator

decides on the AS number and the BGP RouterID of the new router and uses their RPKI software management tools to generate the public/private key-pair and publish the public key in the RPKI. The tools also produce the PKCS#8 object which the operator then uploads into the new router via the craft port, ssh, NetConf, etc. The router installs the PKCS#8 and installs the public/private key-pair.

The router SHOULD verify that the issued certificate actually corresponds to the private key in the PKCS#8, i.e. the PKCS#8 is self-consistent.

6. 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 CLI 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, the 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 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 4.

7. 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 by a monkey in the middle. Hence transport security is strongly advised.

8. IANA Considerations

This document has no IANA Considerations.

9. References

9.1. Normative References

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

[RFC5915] Turner, S. and D. Brown, "Elliptic Curve Private Key Structure", RFC 5915, June 2010.

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

9.2. Informative References

[I-D.ietf-sidr-bgpsec-algs] Turner, S., "BGP Algorithms, Key Formats, & Signature

Formats", draft-ietf-sidr-bgpsec-algs-02 (work in progress), March 2012.

[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-03 (work in progress), April 2012.

[I-D.lepinski-bgpsec-overview]
Lepinski, M. and S. Turner, "An Overview of BGPSEC", draft-lepinski-bgpsec-overview-00 (work in progress), March 2011.

[I-D.lepinski-bgpsec-protocol]
Lepinski, M., "BGPSEC Protocol Specification", draft-lepinski-bgpsec-protocol-00 (work in progress), 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.

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