Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 5, 2016

R. Bush
IIJ Lab / Dragon Research Lab
S. Turner
IECA, Inc.
K. Patel
Cisco Systems

November 2, 2015

Router Keying for BGPsec
draft-ietf-sidr-rtr-keying-10

Abstract

BGPsec-speaking routers are provisioned with private keys in order to sign BGPsec announcements. The corresponding public keys are published in the global Resource Public Key Infrastructure, enabling verification of BGPsec messages. This document describes two methods of generating the public-private key-pairs: router-driven and operator-driven.

Requirements Language

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.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

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

These two sub-methods differ in where the keys are generated: on the router in the router-driven method, and elsewhere in the operator-driven method. Routers are required to support at least one of the methods in order to work in various deployment environments. Some routers may not allow the private key to be off-loaded while others may. While off-loading private keys would ease swapping of routing engines, exposure of private keys is a well known security risk.

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

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

The router-driven model mirrors the model used by traditional PKI subscribers; the private key never leaves trusted storage (e.g., Hardware Security Module). This is by design and supports classic PKI Certification Policies for (often human) subscribers which 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 used by the the soon-to-be offline router. This motivated the operator-driven model.

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

Useful References: [I-D.ietf-sidr-bgpsec-overview] gives an overview of the BGPsec protocol, [I-D.ietf-sidr-bgpsec-protocol] gives the gritty details, [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. Management / Router Communication

Operators are free to use either the router-driven or operator-driven method as supported by the platform. Regardless of the method chosen, operators first establish a secure communication channel between the management system and the router. How this channel is established is router-specific and is beyond scope of this document.

Though other configuration mechanisms might be used, e.g. NetConf (see [RFC6470]); for simplicity, in this document, the communication channel between the management platform and the router is assumed to be an SSH-protected CLI. See Appendix A for security considerations for this channel.

3. Exchanging Certificates

The operator management station can exchange certificate requests and certificates with routers and with the RPKI CA infrastructure using the application/pkcs10 media type [RFC5967] and application/pkcs7-mime [RFC5751], respectively, and may use FTP or HTTP per [RFC2585], or the Enrollment over Secure Transport [RFC7030].

4. Set-Up

To start, the operator uses the communication channel to install the appropriate RPKI Trust Anchor' Certificate (TA Cert) in the router. This will later enable the router to validate the router certificate returned in the PKCS#7.

The operator also configures the Autonomous System (AS) number to be used in the generated router certificate. This may be the sole AS configured on the router, or an operator choice if the router is configured with multiple ASs.

The operator configures or extracts from the router the BGP RouterID to be used in the generated certificate. In the case where the operator has chosen not to use unique per-router certificates, a RouterID of 0 may be used.

5. PKCS#10 Generation

The private key, and hence the PKCS#10 request may be generated by the router or by the operator.

5.1. Router-Generated Keys

In the router-generated method, once the protected session is established and the initial Set-Up (Section 4) performed, 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 is returned to the operator over the protected channel.

If a router was to communicate directly with a CA to have the CA certify the PKCS#10, there would be no way for the CA to authenticate

the router. As the operator knows the authenticity of the router, the operator must mediate the communication with the CA.

The operator adds the chosen AS number and the RouterID to send to the RPKI CA for the CA to certify.

5.2. Operator-Generated Keys

In the operator-generated method, the operator generates the public/private key pair on a management station and installs the private key into the router over the protected channel. Beware that experience has shown that copy and paste from a management station to a router can be unreliable for long texts.

Alternatively, the private key may be encapsulated in a PKCS #8 [RFC5958], the PKCS#8 is further encapsulated in Cryptographic Message Syntax (CMS) SignedData [RFC5652], and signed by the AS's End Entity (EE) 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 operator then creates and signs the PKCS#10 with the private key, and adds the chosen AS number and RouterID to be sent to the RPKI CA for the CA to certify.

6. Installing Signed Keys

The operator uses RPKI management tools to communicate with the global RPKI system to have the appropriate CA validate the PKCS#10 request, sign the key in the PKCS#10 and generated PKCS#7 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.

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

1. 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.

2. Returns the certificate to the operator's management station, packaged in a PKCS#7, using the corresponding method by which it received the certificate request. It SHOULD include the certificate chain below the TA Certificate so that the router can validate the router certificate.

In the operator-generated method, the operator SHOULD extract the certificate from the PKCS#7, and verify that the private key it holds corresponds to the returned public key.

In the operator-generated method, the operator has already installed the private key in the router (see Section 5.2).

The operator provisions the PKCS#7 into the router over the secure channel.

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 and whether or not the keys correspond; the mechanism is out of scope.

The router SHOULD also verify that the returned certificate validates back to the installed TA Certificate, i.e., the entire chain from the installed TA Certificate through subordinate CAs to the BGPsec certificate validate. To perform this verification the CA certificate chain 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.

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 the direct CA.

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].

7. 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.

7.1. Key Validity

It is critical that a BGPsec speaking router ensures that it is signing with a valid certificate at all times. To this end, the operator needs to ensure the router always has a non-expired certificate. I.e. the key used to sign BGPsec announcements always has an associated certificate whose expiry time is after the current time.

Ensuring this is not terribly difficult but requires that either:

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

2. The operator notes the expiry time of the certificate and uses a calendaring program to remind them of the expiry time, and/or

3. The RPKI CA warns the operator of pending expiration, and/or

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

It is advisable that expiration warnings happen well in advance of the actual expiry time.

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 helpful to notify a peer operator that one or more of their certificates are about to expire.

7.2. Key Roll-Over

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 and distributed 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 re-keyed (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, re-keying 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 well in advance of the operational certificate's expiry time.

7.3. Key Revocation

Certain unfortunate circumstances may occur causing a need to revoke a 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 Certificate Revocation List (CRL) as well as re-keying the router's certificate.

When 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 re-keying/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 other(s) are soon-to-be-operational, 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 next generation 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.

7.4. Router Replacement

Currently routers often generate private keys for uses such as SSH, and the private keys may not be seen or off-loaded from the router. 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 a protected session, e.g. SSH, NetConf (see [RFC6470]), SNMP, etc. This lets the operator upload the old private key via the mechanism used for operator-generated keys, see Section 5.2.

8. Security Considerations

The router's manual will describe whether the router supports one, the other, or both of the key generation options discussed in the earlier sections of this draft as well as other important security-related information (e.g., how to SSH to the router). After familiarizing one's self with the capabilities of the router, operators are encouraged to ensure that the router is patched with the latest software updates available from the manufacturer.

This document defines no protocols so in some sense introduces no new security considerations. However, it relies on many others and the security considerations in the referenced documents should be consulted; notably, those document listed in Section 1 should be consulted first. PKI-relying protocols, of which BGPsec is one, have many issues to consider so many in fact entire books have been written to address them; so listing all PKI-related security considerations is neither useful nor helpful; regardless, some boot-strapping-related issues are listed here that are worth repeating:

Public-Private key pair generation: Mistakes here are for all practical purposes catastrophic because PKIs rely on the pairing of a difficult to generate public-private key pair with a signer; all key pairs MUST be generated from a good source of non-deterministic random input [RFC4086].

Private key protection at rest: Mistakes here are for all practical purposes catastrophic because disclosure of the private key allows another entity to masquerade as (i.e., impersonate) the signer; all private keys MUST be protected when at rest in a secure fashion. Obviously, how each router protects private keys is implementation specific. Likewise, the local storage format for the private key is just that, a local matter.

Private key protection in transit: Mistakes here are for all practical purposes catastrophic because disclosure of the private key allows another entity to masquerade as (i.e., impersonate) the

signer; transport security is therefore strongly RECOMMENDED. The level of security provided by the transport layer's security mechanism SHOULD be commensurate with the strength of the BGPsec key; there's no point in spending time and energy to generate an excellent public-private key pair and then transmit the private key in the clear or with a known-to-be-broken algorithm, as it just undermines trust that the private key has been kept private. Additionally, operators SHOULD ensure the transport security mechanism is up to date, in order to addresses all known implementation bugs.

SSH key management is known, in some cases, to be lax [I-D.ylonen-sshkeybcp]; employees that no longer need access to routers SHOULD be removed the router to ensure only those authorized have access to a router.

Though the CA's certificate is installed on the router and used to verify that the returned certificate is in fact signed by the CA, the revocation status of the CA's certificate is rarely checked as the router may not have global connectivity or CRL-aware software. The operator MUST ensure that installed CA certificate is valid.

9. IANA Considerations

This document has no IANA Considerations.

10. References

10.1. Normative References

[I-D.ietf-sidr-bgpsec-algs]
Turner, S., "BGP Algorithms, Key Formats, & Signature Formats", draft-ietf-sidr-bgpsec-algs-04 (work in progress), March 2013.

[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-04 (work in progress), October 2012.

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

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

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

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

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

10.2. Informative References

[I-D.ietf-sidr-bgpsec-overview] Lepinski, M. and S. Turner, "An Overview of BGPSEC", draft-ietf-sidr-bgpsec-overview-02 (work in progress), May 2012.

[I-D.ietf-sidr-bgpsec-protocol] Lepinski, M., "BGPSEC Protocol Specification", draft-ietf-sidr-bgpsec-protocol-07 (work in progress), February 2013.

[I-D.ylonen-sshkeybcp] Ylonen, T. and G. Kent, "Managing SSH Keys for Automated Access - Current Recommended Practice", draft-ylonen-sshkeybcp-01 (work in progress), April 2013.

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

[RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys", BCP 86, RFC 3766, April 2004.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[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.

[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, DOI 10.17487/RFC7030, October 2013, <http://www.rfc-editor.org/info/rfc7030>.

Appendix A. Management/Router Channel Security

Encryption, integrity, authentication, and key exchange algorithms used by the secure communication channel SHOULD be of equal or greater strength than the BGPsec keys they protect, which for the algorithm specified in [I-D.ietf-sidr-bgpsec-algs] is 128-bit; see [RFC5480] and by reference [SP800-57] for information about this strength claim as well as [RFC3766] for "how to determine the length of an asymmetric key as a function of a symmetric key strength requirement." 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). Suggested minimum algorithms would be AES-128: aes128-cbc [RFC4253] and AEAD_AES_128_GCM [RFC5647] for encryption, hmac-sha2-256 [RFC6668] or AESAD_AES_128_GCM [RFC5647] for integrity, ecdsa-sha2-nistp256 [RFC5656] for authentication, and ecdh-sha2-nistp256 [RFC5656] for key exchange.

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.

Authors' Addresses

Randy Bush
IIJ / Dragon Research Labs
5147 Crystal Springs
Bainbridge Island, Washington 98110
US

Email: randy@psg.com

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

Email: sean@sn3rd.com

Keyur Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

Email: keyupate@cisco.com