BGPSEC Summary

PARSONS, Inc.

16 August 2016

Contents

1 Introduction

The BGPSEC software package is an open source implementation of the BGPsec Protocol, currently a work in progress [6] in the IETF SIDR working group. BGPsec provides path validation protections, providing comprehensive security for BGP. Path validation is a necessary step that prevents the origin validation protections [5] from being circumvented.

2 BGPSec Implementation

As part of developing and deploying a BGP security solution, this project produced a proof-of-concept implementation of the BGP Security (BGPsec) protocol [6]. The main goals for the implementation are:

- An open source, freely available reference implementation of the BGPsec protocol.
  - For academic study
  - For Internet Service Provider (ISP) internal use/testing

- A functional software router to provide operational experience and feedback into the protocol design.
- Proof-of-concept code suitable to support advancement of the BGPsec specifications within the Internet Engineering Task Force (IETF).
- A basis for future development and use of the protocol.

In order to fulfill these goals, a survey of open source routing software was conducted to determine both whether we should create our own software package or build off of one the existing software packages and which one to use if we chose to go with existing router software. The choice of the Bird Internet Router Daemon (BIRD) [1] software package determined the programming language used: C.

BIRD provides an implementation of Border Gateway Protocol (BGP) that includes origin validation. The BIRD origin validation relies on an external Route Origin Authorization (ROA) table that lists the authorized Autonomous System (AS) originators of a route to any prefix. A process external to BIRD is expected to populate that table, in order that the origin validation not be tied to any particular method of supplying that information.

The Resource Public Key Infrastructure (RPKI) is a source of the authorized AS originators information that is needed. It also provides the public router keys. Our BGPsec implementation provides the required external process, bird-rpki-client, which retrieves the authorized AS and prefix information from an RPKI cache and populates BIRD's internal ROA table. It also retrieves router public keys to make them available for the BGPsec code.

The build process was also determined by the choice of routing software: automake. The cryptographic code within the BGPsec implementation also requires OpenSSL libraries that support Elliptic Curve Digital Signature Algorithm (ECDSA). The bird-rpki-client requires a version of RTRlib that supports router key retrieval. A multi-user accessible source code version control system was created using git for code development. The implementation developers interacted with Secure Inter-Domain Routing (SIDR) Working Group [8] and the protocol developers to provide feedback for the protocol development.

3 Results: BGPSEC Implementation

The main result was the creation of functional software that implements the BGPsec protocol specification. The software has been shown to be functional in small test environments. It can negotiate and open BGPsec sessions between routers, send and receive BGP UPDATE messages with the BGPsec attribute, and check that the messages are cryptographically signed correctly. While BIRD supports multiple routing protocols including BGP, the code uses a modular design for the protocols supported. This in turn allowed us to limit most of the code changes to the BGP protocol module. Figure 1 on page 3 illustrates the BIRD architecture.

BGPsec adds security to BGP routing by providing two major protection features. One is path authentication. That is, BGPsec cryptographically authenticates that the series of AS's that a BGP prefix announcement claims to have passed through is accurate. The other feature is network

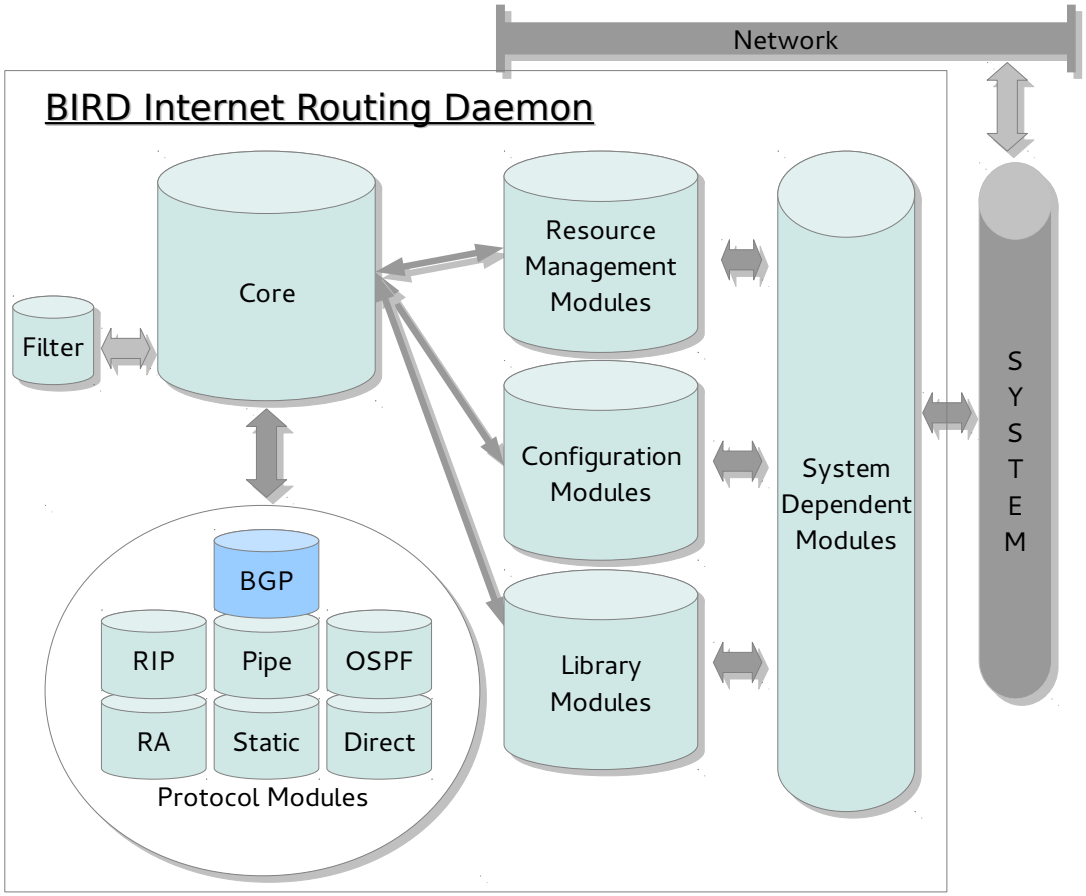

Figure 1: BIRD

prefix origin validation. Origin validation is validating that the AS which originated a network prefix is the valid holder of that prefix.

In order to provide path authentication, an additional BGP attribute, the BGPSEC_Path attribute, is added to a BGP Update message. The BGPSEC_Path attribute contains several values related to the AS_PATH attribute of the BGP Update message, and signature values that in turn authenticate the update message and its path. In order to support BGPsec within BIRD, we extended the BGP protocol module in BIRD's routing engine to support BGPsec attribute handling and to support the cryptographic signing and validation of data within the BGPsec attribute. The credentials, or keys, used to authenticate this data are garnered from the RPKI [5]. Figure 2 on page 4 shows an expansion of the BGPsec integration into the BGP protocol module in BIRD.

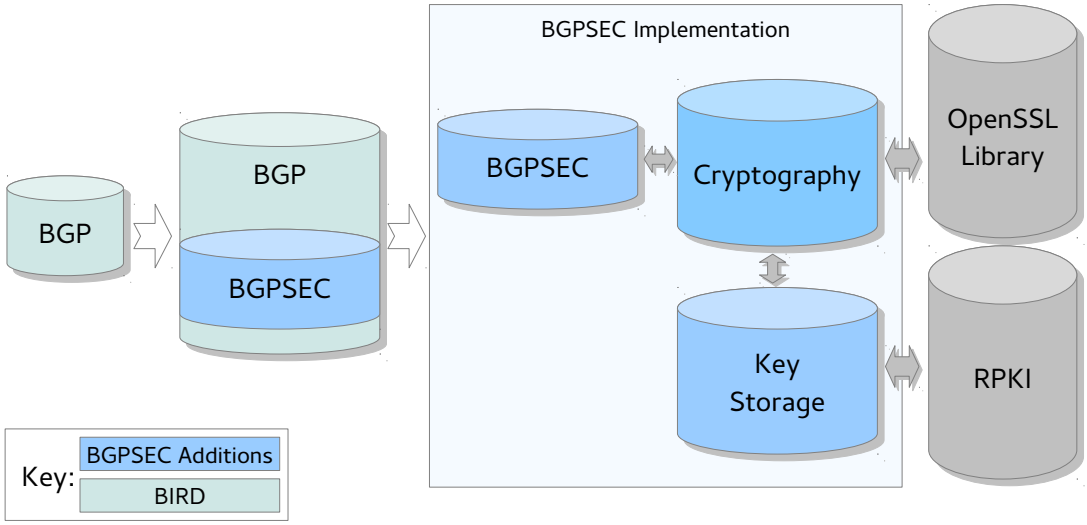

Figure 2: BGPSEC Implementation

In order to provide origin validation, the BIRD developers created an interface to create ROA tables that can be used to filter BGP prefixes based on the prefix's authorized originating AS number. The AS/Prefix data can be provided by the RPKI, but that data needs to be gathered and loaded into the ROA tables by a process outside of the BIRD daemon. RTRlib [7, 10] is an rpki-rtr client library for retrieving that data from an RPKI cache. Example client software for accessing that data was created by the RTRlib project as bird-rtrlib-cli. We in turn modified that code and provide a software client, bird-rpki-client, that can be used to populate the ROA tables in a running BIRD daemon.

Additionally, in order to authenticate the signatures within the BGPsec attribute, the signing router's public keys are needed. These keys are available from the RPKI. RTRlib also provides access to these router keys. The bird-rpki-client software was updated to download router keys and make them available to the BGPsec code within BIRD. An overview of the BIRD daemon with BGPsec and bgpsec-bird-client is shown in Figure 3 on page 5 below.

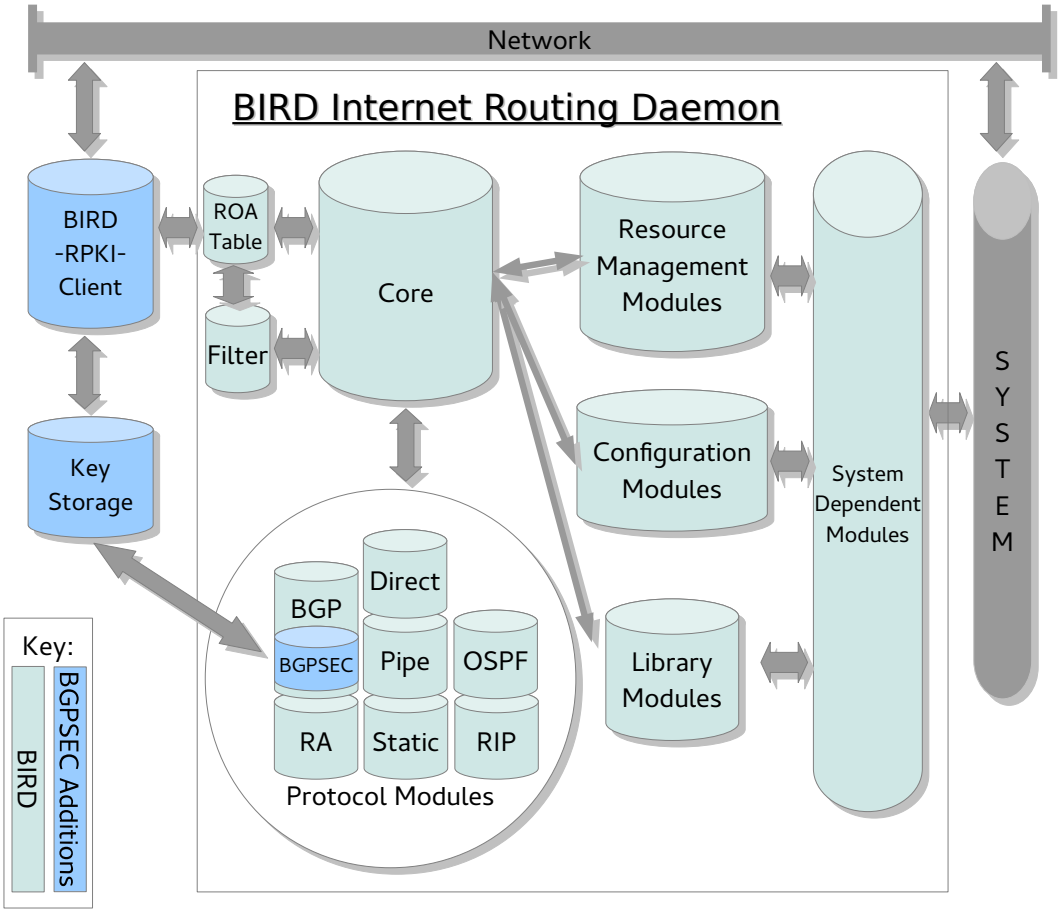

Figure 3: Overview of BGPSEC Implementation

There have been multiple releases of the software. The most current feature list follows:

- BGP capability negotiation for the use of BGPsec in a BGP session
- Creating and parsing of the BGPsec attribute in a BGP UPDATE message
- Generating and validating signatures within the BGPsec attribute
- Generating and processing the pcount field within the BGPSEC attribute. The pcount value is used to mimic the practice of prepending multiple copies of an AS number to an AS_PATH attribute. This is a common practice used in order to make a routing path less desirable.
- Ability to configure how Valid/Invalid BGPsec UPDATES are treated. Local policy can choose how to make use of the Valid/Invalid states in routing decisions.
- Use of RPKI-RTR protocol [2] to get ROA data from the local RPKI cache for Origin Validation within BIRD.
- Use of RPKI-RTR protocol [2] to get router public keys from the local RPKI cache to use for authenticating BGPSEC attribute signatures.

- Autonomous System Number (ASN) associated to router keys. Router keys are retrieved from the RPKI data by a combination of the router's ASN and the key identifier from the router's certificate.

4 Compliance with IETF SIDR Specifications

BGPSEC is compliant with the current BGPsec specification set in the SIDR working group, with two exceptions. The current BGPsec specification set includes:

- draft-ietf-sidr-bgpsec-protocol-17
  BGPsec Protocol Specification
  available at https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-17
- draft-ietf-sidr-bgpsec-algs-15
  BGPsec Algorithms, Key Formats, & Signature Formats
  available at https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-algs-15
- draft-ietf-sidr-bgpsec-pki-profiles-18
  A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests
  available at https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-pki-profiles-18

The first exception is that BGPsec does not support BGP confederations. The BIRD routing protocol package does not itself support confederations, so there the BGPsec implementation can not implement protections for that (missing) feature.

The second exception is that BGPsec does not support multiple cryptographic algorithms. There is presently no second algorithm defined, so there is no way to implement the (missing) second algorithm.

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

API Application Programming Interface. 7

AS Autonomous System
AS is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet. 2, 5, 7

ASN Autonomous System Number
ASN is the number associated to a AS. 6, 7

ASN.1 Abstract Syntax Notation One
ASN.1 is a language for describing structured information. 7

BGP Border Gateway Protocol
This is the routing protocol used to transfer reachability and routing information between Autonomous Systems (AS's) on the internet. 2, 5–7

BGPsec BGP Security
Additions to the BGP protocol to increase the security of the exchanged routing information. 1, 2, 5–7

BIRD The BIRD Internet Router Daemon is an open source routing software package [1]. 1, 2, 5–7

BPKI Business Public Key Infrastructure. 7

CA Certification Authority (x509)
An entity that issues digital certificates. The certificates are used to certify that the subject of the certificate owns the public key associated with the certificate. In the X.509 Public Key Infrastructure model, the CA is a trusted third party. That is, the owner of the certificate and the user, or relying party, of the certificate both trust the CA. 7

CMS Cryptographic Message Syntax
CMS is the IETF's standard for cryptographically protected messages. 7

ECDSA Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which operates on elliptic curve groups. The EC variant provides smaller key sizes for the same security level. This algorithm is used for signing and authenticating within the BGPSEC_path attribute in BGP UPDATE messages. 2, 7

GUI Graphical User Interface. 7

IANA Internet Assigned Numbers Authority
The IANA manages the DNS Root Zone, coordinates allocations from the global IP and AS number spaces, and serves as the central repository for protocol name and number registries used in many Internet protocols. 7

IETF Internet Engineering Task Force [4]

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. 1, 7

IRBE Internet Registry Back End. 7

IRDB Internet Registry Data Base. 7

IRR Internet Routing Registry
The union of world-wide routing policy databases that use the Routing Policy Specification Language. 7

ISP Internet Service Provider. 1, 7

ODBC Open Database Connectivity
ODBC is a standard programming language middleware API for accessing database management systems. 7

ORM Object-Relational Mapper
ORM is a programming technique for converting data between incompatible type systems in relational databases and object-oriented programming languages. In Django, the data models are defined as Python classes. 7

RIR Regional Internet Registries
Regional Internet Registries (RIRs) manage, distribute, and register public Internet Number Resources within their respective regions. 7

ROA Route Origin Authorization
A ROA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate routes to one or more prefixes within the address block. 2, 5, 7

RPKI Resource Public Key Infrastructure
A Public Key Infrastructure (PKI) used to support attestations about Internet Number Resource (INR) holdings. 2, 5–7

RPSTIR Relying Party Security Technology for Internet Routing
Pronounced ”rip-stir”. Using the global Resource Public Key Infrastructure (RPKI), RPSTIR securely generates a list of authorized prefix-origin AS pairs. This list can be used by the RPKI-RTR protocol, enabling routers to detect false origin announcements due to errors by network operators. 7

RRDP RPKI Repository Delta Protocol. 7

SIDR Secure Inter-Domain Routing (Working Group)
IETF Working Group that worked on creating BGPSEC [8]. 2, 7

SQL Structured Query Language
SQL is a query language used for managing data held in a relational database system. 7

ssh Secure Shell
SSH is a protocol for secure remote login and other secure network services over an insecure networks. 7

SSL Secure Sockets Layer
SSL is a protocol that provides communication security over the Internet. 7

SVN Apache Subversion (often abbreviated SVN, after the command name svn) is a software versioning and revision control system distributed as free software under the Apache

License. Developers use Subversion to maintain current and historical versions of files such as source code, web pages, and documentation. 7

XML Extensible Markup Language
XML is a markup language defined by the W3C[9] that defines a set of rules for encoding documents in a format that is human and machine readable. 7

YaML YAML Ain't Markup Language
YaML is a human-readable data serialization format. 7

GLOSSARY OF TERMINOLOGY

Apache Apache is a commercial grade web server package. 7

Django Django is a free and open source web application framework written in Python, that encourages rapid development and clean, pragmatic design. 7

ghostbuster An RPKI signed object which contains contact information for a person responsible for the RPKI repository in which the object appears. 7

irdbd A sample implementation of an IR database daemon. 7

left-right The left-right protocol is two separate client/server protocols over separate channels between the RPKI engine and the IR back end (IRBE). The IRBE is the client for one of the subprotocols, the RPKI engine is the client for the other. 7

MySQL a widely used and popular open source database package. 7

OpenSSL a widely used, open source implementation of many cryptographic features, including support for X.509 Public Key Infrastructure, XML, and many different cryptographic algorithms. 2, 7

PostgreSQL a powerful, open source object-relational database system, whose SQL implementation strongly conforms to the ANSI-SQL:2008 standard. 7

prefix a contiguous block of Internet addresses, called a prefix because all the addresses share the same initial bit pattern. 7

pubd The publication engine daemon. 7

rcynic The primary validation tool in the rpki.net package. 7

Relying Party The entity which retrieves RPKI objects from repositories, validates them, and uses the result of that validation process as input to other processes, such as BGP security. 7

rootd A separate daemon for handling the root of an RPKI certificate tree. 7

RouteViews Route Views is a project founded by Advanced Network Technology Center at the University of Oregon to allow Internet users to view global BGP routing information from the perspective of other locations around the internet. Originally created to help Internet Service Providers determine how their network prefixes were viewed by others in order to debug and optimise access to their network, Route Views is now used for a range of other purposes such as academic research. 7

rpki-rtr A protocol to deliver validated prefix origin data to routers. Described in RFC 6810 [2]. 7

rpki.net rpki.net is a project and website. The project provides a free, BSD License, open source, complete system for the Internet Registry or ISP. It includes separate components which may be combined to suit your needs. 7

rpkic A command line interface to control rpkid and pubd. 7

rpkid The main RPKI certificate issuance daemon. 7

rsync A file synchronization and file transfer program for Unix-like systems that minimizes network data transfer by using a form of delta encoding called the rsync algorithm. 7

rtr-origin rtr-origin is an implementation of the rpki-rtr protocol, including the rpki-rtr server, a test client and a utility for examining the content of the database rtr-origin generates. 7

RTRlib RPKI RTR Client C Library
The RTRlib is an open-source C implementation of the RPKI/Router Protocol client [7]. 2, 5, 7

subversion Apache Subversion (often abbreviated SVN, after the command name svn) is a software versioning and revision control system distributed as free software under the Apache License. Developers use Subversion to maintain current and historical versions of files such as source code, web pages, and documentation. 7

up-down A RPKI certificate provisioning protocol which is expressed as a simple request/response interaction, where the client passes a request to the server, and the server generates a corresponding response. Described in RFC 6492[3]. 7

X.509 an ITU-T standard for public key infrastructure (PKI) certificates and certificate revocation lists. 7

References

[1] BIRD Internet Routing Daemon. `http://bird.network.cz`.

[2] R. Bush and R. Austein. The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6810, January 2013.

[3] G. Huston, R. Loomans, B. Ellacott, and R. Austein. A Protocol for Provisioning Resource Certificates. RFC 6492, February 2012.

[4] IETF. The Internet Engineering Task Force. `http://www.ietf.org`.

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

[6] Matthew Lepinski (editor). BGPSEC Protocol Specification. IETF SIDR Working Group Internet Draft, June 2016.
`https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol/`.

[7] Joint project of the INET research group at the Hamburg University of Applied Sciences and the CST research group at Freie Universitt Berlin. Rtrlib - the rpki rtr client c library, June 2014. `rpki.realmv6.org`.

[8] SIDR. Secure Inter-Domain Routing, IETF Working Group.
`https://datatracker.ietf.org/wg/sidr/`.

[9] W3C. World Wide Web Consortium (W3C). `http://www.w3.org/`.

[10] Matthias Wählisch, Fabian Holler, Thomas C. Schmidt, and Jochen H. Schiller. Rtrlib: An open-source library in c for rpki-based prefix origin validation. In *Presented as part of the*

6th Workshop on Cyber Security Experimentation and Test, Washington, D.C., 2013. USENIX.