RPSTIR Summary

PARSONS, Inc.

16 August 2016

Contents

1 Relying Party Security Technology for Internet Routing (RPSTIR)

RPSTIR is an open source implementation of the Relying Party (RP) functions in the RPKI, including an implementation of the RPKI-RTR protocol [2], as well as a stringent set of tests to prove a relying party implementation is correctly detecting errors in PRKI certificates. A relying party implementation passing these stringent tests can be used to rigorously test a CA's compliance with the RPKI specifications.

2 Software: RPSTIR

The PARSONS team member Raytheon BBN Technologies created an open-source release of the Relying Party Security Technology for Internet Routing (RPSTIR, pronounced "rip-stir").

RPSTIR provides relying party tools to retrieve and verify Resource Public Key Infrastructure (RPKI) objects contained in the world-wide system of RPKI repositories.

RPSTIR helps network operators detect and reject accidental, false route origin advertisements, thus reducing the likelihood of inadvertent Internet address space hijacking.

RPSTIR synchronizes with the global RPKI repository system, verifies the data, and extracts a list of authorized prefix-origin AS pairs. This list is precisely the information a router requires in order to detect false BGP origin announcements.

RPSTIR implements the RPKI to Router Protocol (rpki-rtr, RFC6810[2]), allowing routers to communicate with RPSTIR to verify route origin announcements and detect false origin announcements due to errors by network operators (e.g., the Pakistan Telecom hijack of YouTube address space [7]).

RPSTIR also implements the local trust anchor management [5].

Figure 1, below, shows the overview of the RPSTIR architecture.

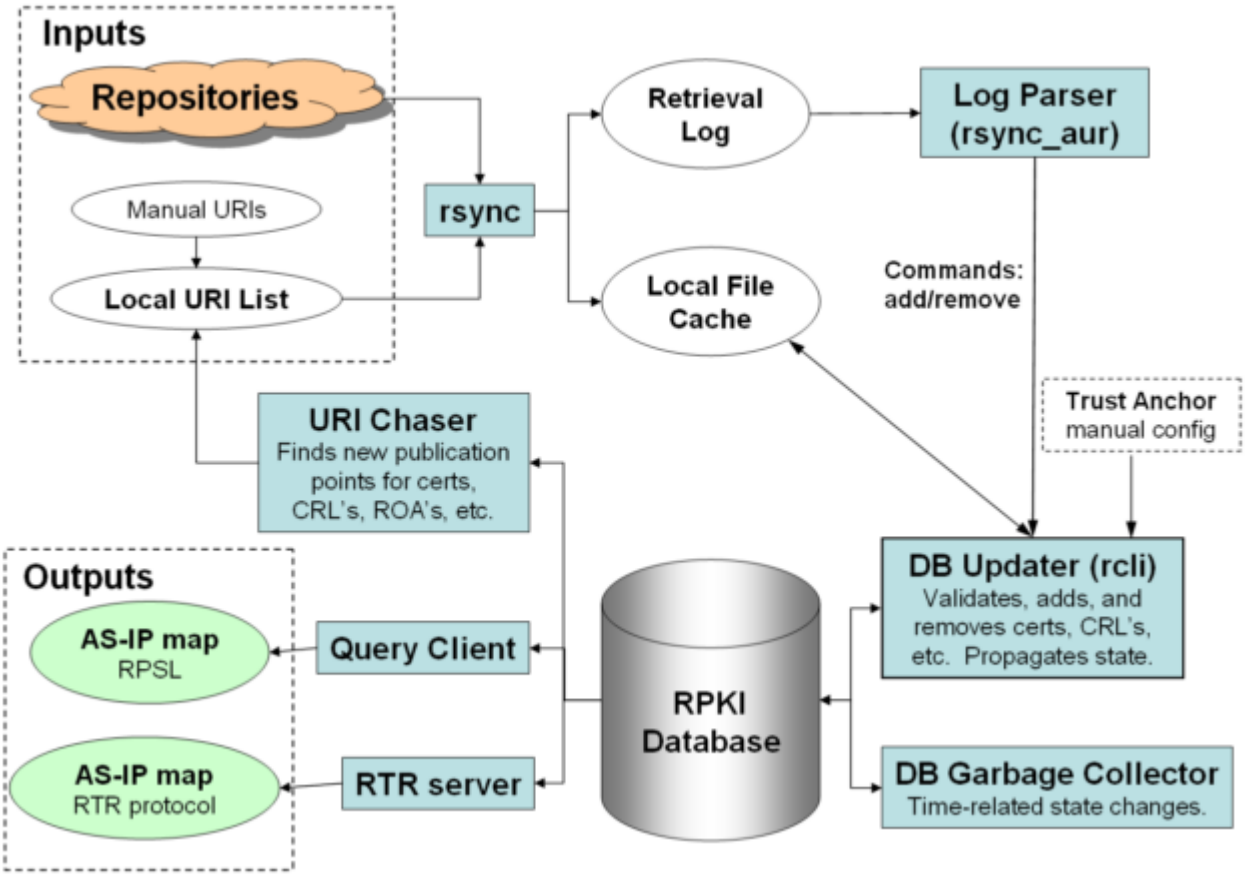

Figure 1: Overview of RPSTIR Implementation

The RPSTIR software is composed of several components.

2.1 RPKI synchronization and local caching.

The *rpstir-synchronize* utility of RPSTIR uses the rsync protocol to synchronize with the global RPKI repository system and create a local rsync file cache. The utility must be run periodically to keep it in sync with the global RPKI. Users must configure their system using Cron or another time based job scheduler to run *rpstir-synchronize* at an interval appropriate for their system.

After the local file cache has been synchronized, the *rsync_aur* utilty parses the sychronization log file and passed updated configuration information to the *rcli* utility. The *rcli* utility validates the RPKI objects and extracts a list of authorized prefix-origin AS pairs to a local RPKI database cache. This local database cache can be queried using the *rpstir-query* utility.

2.2 RTR Server; Route Origin Verification.

RPSTIR implements the RPKI to Router Protocol (rpki-rtr, RTR), which creates flexibility in the deployment of RPKI in a network. Using the rpki-rtr protocol, RPSTIR can be hosted anywhere in the router's network, sparing the router the burden of the synchronization and cryptographic validation. RPSTIR would produce the local RPKI database cache and act as an rpki-rtr server. Routers could communicate with the RPSTIR rpki-rtr server to retrieve the list of authorized prefix-origin AS pairs, and use that information to verify route origin announcementa and detect false origin announcements.

The *rpstir-rpki-rtr-update* utility updates the local rpki-rtr cache and should be called after *rpstir-synchronize*.

RPSTIR also offers an Routing Policy Specification Language (RPSL) output option, enabling operators to generate route filters compatible with existing, deployed router and operations software.

2.3 Compliance Tools.

RPSTIR provides fine-grained, stringent compliance tests for relying party code. These test cases can be used to test any relying party implementations for compliance with published RFCs and Internet-Drafts, testing that compliant RPKI objects pass the tests and non-compliant objects fail. Additionally, relying party software that passes the tests can be used to test the output of a CA, to ensure that the CA is producing compliant products.

3 Software Dependencies.

RPSTIR depends on several other open source packages.

- **MySQL:** MySQL is used for the the local RPKI database cache.
- **OpenSSL:** OpenSSL is used for cryptographic libraries for X.509 certificates.

- **ODBC mySql Connector:** ODBC (Open Database Connectivity) is a standard programming interface (API) for accessing database, used to connect with the local RPKI database cache.
- **rsync:** Rsync is used to synchronize a local file cache of global RPKI data.
- **Python:** Python is a programming language that lets you work quickly and integrate systems more effectively.
- **Netcat:** Netcat is a networking utility which reads and writes data across network connections.
- **Cryptlib:** Cryptlib is a library which provides implementations of complete security services via a simple high level programming interface (API).
- **cURL:** cURL is a command line tool and library for transferring data with Universal Resource Locator (URL) syntax (e.g. HTTP, FTP, etc).
- **OpenSSH:** OpenSSH provides utilities and libraries for Secure Shell (SSH) access.

3.1 Results: RPSTIR

RPSTIR provides a production quality implementation of the relying party tools necessary to use the RPKI.

RPSTIR is offered under the BSD open source license model, so everyone is free to modify RPSTIR to suit individual needs or incorporate it into other products.

Features include:

- Fine-grained ASN.1-level diagnostics for debugging RPKI repositories
- Both RPSL and diagnostic output
- Top-down and bottom-up certification path discovery
- Flexible database architecture (based on MySQL)
- Efficient parallel download of RPKI objects
- Implementation of the Local Trust Anchor functionality [5] for mitigation of CA errors
- Implementation of the server for the rpki-rtr protocol
- statistics collection of the RPKI over time, including incremental updates and multiple simultaneous statistics collections.
- Support for adding files from an existing local cache. In the future, this could be used to quickly deploy additional relying party machines without requiring each to synchronize individually with the global RPKI repository system

4 Compliance with IETF SIDR Specifications

The SIDR published specifications of the RPKI are available at https://datatracker.ietf.org/wg/sidr/documents/. The RPSTIR implementation is compliant with the specifications relevant to the RPKI relying party role, including:

RFC6487 (A Profile for X.509 PKIX Resource Certificates),
RFC6482 (A Profile for Route Origin Authorizations (ROAs)),

RFC6486 (Manifests for the Resource Public Key Infrastructure (RPKI)),
RFC6493 (The Resource Public Key Infrastructure (RPKI) Ghostbusters Record)
RFC6810 (The Resource Public Key Infrastructure (RPKI) to Router Protocol).
RFC 6490 Resource Public Key Infrastructure (RPKI) Trust Anchor Locator
RFC 7730 Resource Public Key Infrastructure (RPKI) Trust Anchor Locator

RPSTIR is also compliant with the following works in pogress, SIDR work items that have not yet been published as final.

- draft-ietf-sidr-rfc6485bis-05.txt
  The Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure available at https://tools.ietf.org/html/draft-ietf-sidr-rfc6485bis-05

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

API Application Programming Interface. 5

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. 5

ASN Autonomous System Number
ASN is the number associated to a Autonomous System (AS). 5

ASN.1 Abstract Syntax Notation One
ASN.1 is a language for describing structured information. 5

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

BGPsec BGP Security
Additions to the BGP protocol to increase the security of the exchanged routing information. 5

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

BPKI Business Public Key Infrastructure. 5

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. 5

CMS Cryptographic Message Syntax
CMS is the IETF's standard for cryptographically protected messages. 5

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. 5

GUI Graphical User Interface. 5

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. 5

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. 5

IRBE Internet Registry Back End. 5

IRDB Internet Registry Data Base. 5

IRR Internet Routing Registry
The union of world-wide routing policy databases that use the Routing Policy Specification Language. 5

ISP Internet Service Provider. 5

ODBC Open Database Connectivity
ODBC is a standard programming language middleware API for accessing database management systems. 5

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. 5

RIR Regional Internet Registries
Regional Internet Registries (RIRs) manage, distribute, and register public Internet Number Resources within their respective regions. 5

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. 5

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

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. 5

RRDP RPKI Repository Delta Protocol. 5

SIDR Secure Inter-Domain Routing (Working Group)
IETF Working Group that worked on creating BGPSEC [8]. 5

SQL Structured Query Language
SQL is a query language used for managing data held in a relational database system. 5

ssh Secure Shell
SSH is a protocol for secure remote login and other secure network services over an insecure networks. 5

SSL Secure Sockets Layer
SSL is a protocol that provides communication security over the Internet. 5

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. 5

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. 5

YaML YAML Ain't Markup Language
: YaML is a human-readable data serialization format. 5

GLOSSARY OF TERMINOLOGY

Apache Apache is a commercial grade web server package. 5

Django Django is a free and open source web application framework written in Python, that encourages rapid development and clean, pragmatic design. 5

ghostbuster An RPKI signed object which contains contact information for a person responsible for the RPKI repository in which the object appears. 5

irdbd A sample implementation of an IR database daemon. 5

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. 5

MySQL a widely used and popular open source database package. 5

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. 5

PostgreSQL a powerful, open source object-relational database system, whose SQL implementation strongly conforms to the ANSI-SQL:2008 standard. 5

prefix a contiguous block of Internet addresses, called a prefix because all the addresses share the same initial bit pattern. 5

pubd The publication engine daemon. 5

rcynic The primary validation tool in the rpki.net package. 5

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. 5

rootd A separate daemon for handling the root of an RPKI certificate tree. 5

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. 5

rpki-rtr A protocol to deliver validated prefix origin data to routers. Described in RFC 6810 [2]. 5

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. 5

rpkic A command line interface to control rpkid and pubd. 5

rpkid The main RPKI certificate issuance daemon. 5

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. 5

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. 5

RTRlib RPKI RTR Client C Library
The RTRlib is an open-source C implementation of the RPKI/Router Protocol client [6]. 5

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. 5

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]. 5

X.509 an ITU-T standard for public key infrastructure (PKI) certificates and certificate revocation lists. 5

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. Reynolds and S. Kent (editors). Local Trust Anchor Management for the Resource Public Key Infrastructure. IETF SIDR Working Group Internet Draft, April 2013. `http://tools.ietf.org/html/draft-ietf-sidr-ltamgmt`.

[6] 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`.

[7] RIPE. Youtube hijacking: A ripe ncc ris case study. `http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study`.

[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/`.