Analyzing Inconsistency of RPKI Cache Servers and Impact on BGP

X-CHECK

Samir Al-Sheikh, Matthias Wählisch

{samir.al-sheikh, m.waehlisch}@fu-berlin.de

Freie Universität Berlin, Institut für Informatik, Germany

Freie Universität Berlin

Introduction

- RPKI is major framework to secure BGP
- Helps to prevent Prefix Hijacking
- Route Origin Authorization (ROA) objects in distributed repositories
- Crypto offloaded to cache servers
- Objective 1: Measurement method for live and historical analysis
- Objective 2: Develop tools

Background: RPKI

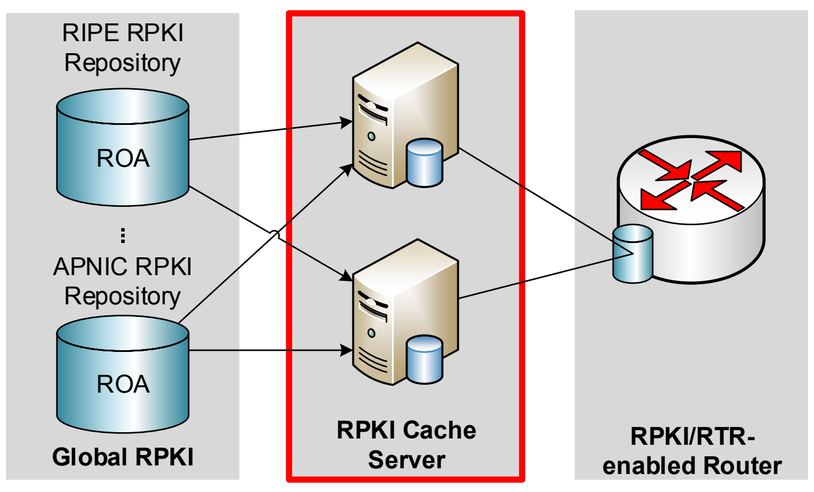
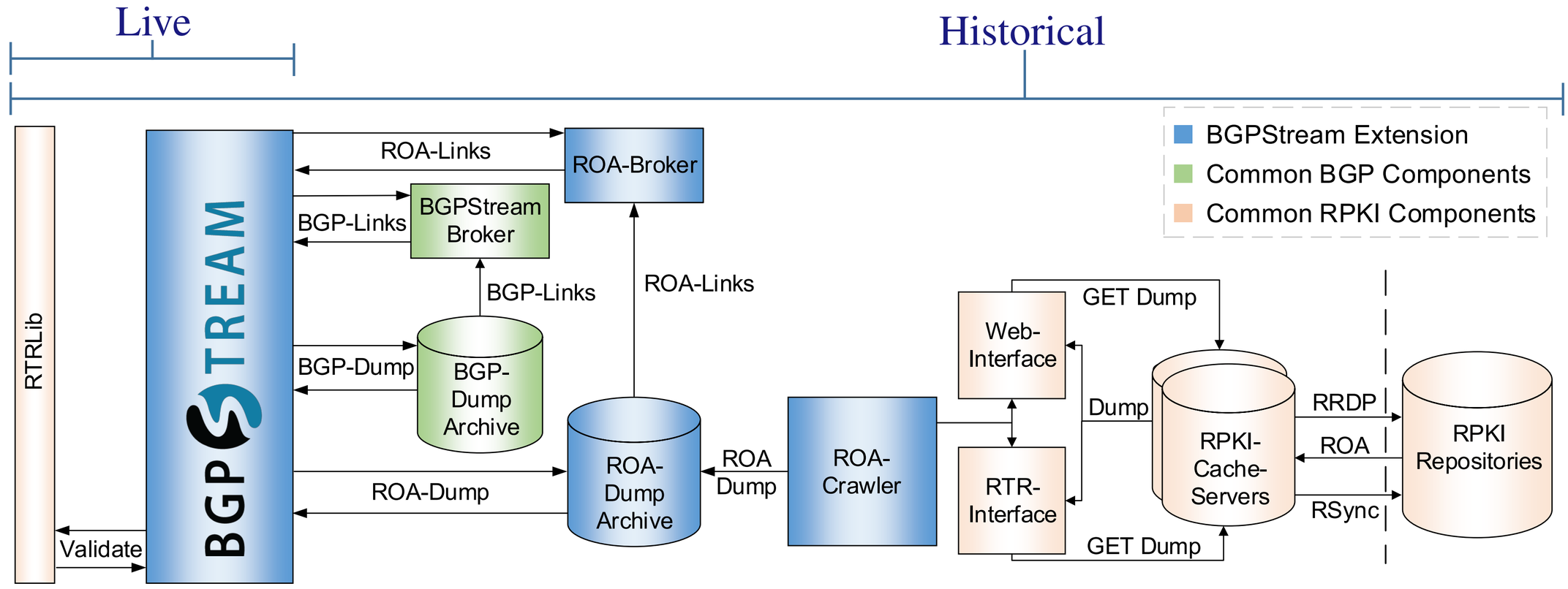


Fig. 1: Resource Public Key Infrastructure

Research Questions & Challenges

- Are RPKI Cache Servers consistent?
- Which reasons cause inconsistency?
- Does inconsistency impact BGP validation?
- Build a long-term ROA data archive
- Different time resolution of RPKI and BGP data
- Extend BGPStream to support BGP *and* RPKI analysis

Measurement Infrastructure and Extension of BGPStream



Cache consistency

- Beacon Delay - Propagation delay of ROA Beacons (i.e., periodically changing ROA data) visible at different cache servers
- Differences per RIR - Relative number of different prefix entries, compared between all cache servers
- Impact on BGP - RPKI origin validation of BGP updates based on ROA data of different cache servers

Preliminary Results