Working Group 6: Secure BGP Deployment

14 March 2013

Andy T Ogielski, Renesys
Jennifer Rexford, Princeton
WG 6 Co-Chairs

Working Group 6: Secure BGP Deployment

WG Description: The Border Gateway Protocol (BGP) is used for inter-domain routing on the Internet. BGP relies on mutual trust among operators of gateway routers to ensure the integrity of the Internet routing infrastructure. Over the years, this trust has been compromised on a number of occasions, both accidentally and maliciously, revealing fundamental weaknesses of this critical infrastructure.

This Working Group will recommend the framework for industry regarding incremental adoption of secure routing procedures and protocols based on existing work in industry and research. The framework will include specific technical procedures and protocols. The framework will be proposed in a way suitable for opt-in by Internet Service Providers (ISPs) in order to create incentives for a wider scale, incremental ISP deployment of secure BGP protocols and practices in a market-driven, cost-effective manner.

Duration: August 2011 – March 2013

CSRIC III
Communications Security, Reliability and Interoperability Council

Working Group 6 – Participants

Name (Affiliation)	Name (Affiliation)
Shane Amante (Level3)	Doug Maughan (DHS S&T)
Daniel Awduche (Verizon)	Danny McPherson (Verisign)
Ron Bonica (Juniper)	Doug Montgomery (NIST)
Jay Borkenhagen (AT&T)	Christopher Morrow (Google)
Belinda Carpenter (Sprint)	Sandra Murphy (SPARTA)
Martin Dolly (ATIS/AT&T)	Mats Nilsson (ATIS/Ericsson)
Mike Geller (ATIS/Cisco)	Andy Ogielski (Renesys), co-chair
Sharon Goldberg (Boston University)	Eric Osterweil (Verisign Labs)
Adam Golodner (Cisco)	Mary Retka (Century Link)
John Griffin (TeleComm Systems)	Jennifer Rexford (Princeton), co-chair
Kyle Hambright (Las Vegas Metro Police)	Isil Sebuktekin (Applied Comm Sciences)
Lars Harvey (Internet Identity)	Ted Seely (Sprint)
Michael Kelsen (Time Warner Cable)	Greg Sharp (Internet Identity)
Ed Kern (Cisco)	Tony Tauber (Comcast)
Padma Krishnaswamy (Batelle)	David Ward (Cisco)
Eric Lent (Comcast)	William Wells (TeleComm Systems)

Interdomain Routing

- **Interdomain routing** is fundamental for operation of the Internet (the “Inter” in Internet).

- **BGP *protocol* is simple**
  - BGP routers relay messages to neighbors about routes
  - Routes are constructed hop-by-hop, beyond the originator’s control

- **BGP *policy* is complex & there is no global coordination**
  - Local policies for accepting, rejecting and propagating routes
  - **This is good**: Great flexibility to support business objectives
  - **This is bad**: Vulnerability to propagating bogus routes

CSRIC III
Communications Security, Reliability and Interoperability Council

Scope of this Report

- **Fundamental notion in all BGP security solutions:**
  - How to distinguish "legitimate routes" from "bogus routes"
  - Legitimate means *"consistent with published routing policy specifications" aka "the Ground Truth"*

- **Secure BGP deployment :** To add to BGP, or to its operation, mechanisms preventing propagation of routes with bogus attributes

- **Specific focus**
  - Focus on solutions sufficiently advanced in IETF standards & available for wider incremental deployment - RPKI
  - Interesting proposals in early stages were not adequately addressed due to time constraints (e.g., DNSSEC-based)

CSRIC III
Communications Security, Reliability and Interoperability Council

How Common are BGP Security Incidents?

- **Too common for comfort**, but note that most of the time BGP operates quite robustly.
  - Incident detection is imperfect without the Ground Truth.
  - Most investigated is Bogus Origin AS (route hijacking). On average several confirmed incidents per month, more possible. Typical incident durations: minutes to hours.
  - Bogus AS_PATH – large number of “obviously wrong” routes observed, but impact on reachability not obvious nor analyzed. No research on prevalence of other bogus attributes.

CSRIC III
Communications Security, Reliability and Interoperability Council

Recommendations

1. Improve record keeping for Internet number resources (IP addresses, AS Numbers) owners. Recommend a PKI-based routing policy publication & management.

2. Be careful and do no harm: Recommend cautious, staged deployment of RPKI origin validation.

3. RPKI opens new attack surfaces and means of abuse. Prevent this. Recommend transparency of operation.

4. Improve BGP security metrics and measurements, track participation in the RPKI and measure if it works.

CSRIC III
Communications Security, Reliability and Interoperability Council

While unanimity in recommendations was an objective from the outset, the conclusions of the report are not necessarily shared by all group members.

Recommendation 1: Need Ground Truth

Improve databases of IP address holders and their routing policies

Security of inter-domain routing relies on accurate information who is authorized to route what, where and when.

- Improve Internet Routing Registries (IRRs) used today in BCP.
- Use cryptographic identity management systems such as Resource Public Key Infrastructure (RPKI) for number resource certificates and Route Origin Authorizations (ROAs).
- Establish a single global “root of trust” for the RPKI.
- Experiment with alternative origin authorization systems.

CSRIC III
Communications Security, Reliability and Interoperability Council

Recommendation 2: Caution with RPKI

Cautious, staged deployment of RPKI origin validation:

•AS Operators should retain autonomy in setting their routing policies, including if and how to use the RPKI data.

- AS operators should start by using RPKI data as one of several ingredients in detecting suspicious routes. It is too early to tell how well RPKI will behave in wider deployment.
- Any future *fully automated* use of RPKI data in filtering "invalid" routes should come only after AS operators are highly confident in the reliability and timeliness of the RPKI data.

CSRIC III
Communications Security, Reliability and Interoperability Council

Recommendation 3: Risks Inherent in RPKI

RPKI opens new attack surfaces and failure modes.

RPKI design obscures information about ownership of number resources. Some remedies were added, but are optional.

- We recommend that every RPKI repository employ accurate and effective human contact information for all certificates and ROAs. Errors and misconfigurations are inevitable, and may significantly impact reachability.
- We recommend that corresponding authorities keep their IP address allocation records up to date and synchronized with corresponding RPKI records to remedy the decoupling of identities of resource holders from RPKI.

CSRIC III
Communications Security, Reliability and Interoperability Council

Recommendation 3: Risks Inherent in RPKI

RPKI enables new means for denial of service by state actors.

Recommend transparency of operation for abuse prevention and diagnosis.

- WG 6 found vulnerability of RPKI to selective denial of service to targeted networks by Certificate Authorities, without ISP participation.
- We recommend that RPKI operators make available tools to detect erroneous and expiring certificates, and all changes.
- RPKI operators should allow open access to the RPKI records and permit general dissemination of the data and derived results (e.g., lists of validated origins).

CSRIC III
Communications Security, Reliability and Interoperability Council

Recommendation 4: Security metrics

Recommend to use metrics to track BGP security evolution

- Quantitative analysis of BGP monitoring data is crucial for informing decisions about which security solutions to deploy and which to reject.
- The BGP security community (network operators and R&D) should track changes in frequency and severity of security incidents to validate new solutions.
- As RPKI deployments proceed, the community should track participation in the RPKI and gauge its effectiveness in preventing the spread of bogus routes.

CSRIC III
Communications Security, Reliability and Interoperability Council

Suggestions for further study

- New attack surfaces opened up by new systemic dependencies between RPKI components and BGP operation, their effects on international enterprises and critical infrastructure networks.
- Systematic comparison of RPKI to DNSSEC based solutions
- Holistic approach towards securing of all BGP route attributes and routing policy registries.
- Performance scaling of RPKI and other BGP security solutions with the expected growth of “Internet of things” and IPv6, with millions to billions of networks in global routing tables.

END OF PRESENTATION

CSRIC III
Communications Security, Reliability and Interoperability Council