Stream: Internet Engineering Task Force (IETF)
RFC: 9319
BCP: 185
Category: Best Current Practice
Published: October 2022
ISSN: 2070-1721
Authors: Y. Gilad, *Hebrew University of Jerusalem*; S. Goldberg, *Boston University*; K. Sriram, *USA NIST*; J. Snijders, *Fastly*
B. Maddison, *Workonline Communications*

# RFC 9319
# The Use of maxLength in the Resource Public Key Infrastructure (RPKI)

## Abstract

This document recommends ways to reduce the forged-origin hijack attack surface by prudently limiting the set of IP prefixes that are included in a Route Origin Authorization (ROA). One recommendation is to avoid using the maxLength attribute in ROAs except in some specific cases. The recommendations complement and extend those in RFC 7115. This document also discusses the creation of ROAs for facilitating the use of Distributed Denial of Service (DDoS) mitigation services. Considerations related to ROAs and RPKI-based Route Origin Validation (RPKI-ROV) in the context of destination-based Remotely Triggered Discard Route (RTDR) (elsewhere referred to as "Remotely Triggered Black Hole") filtering are also highlighted.

## Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9319.

## Copyright Notice

## Table of Contents

# 1. Introduction

The Resource Public Key Infrastructure (RPKI) [RFC6480] uses Route Origin Authorizations (ROAs) to create a cryptographically verifiable mapping from an IP prefix to a set of Autonomous Systems (ASes) that are authorized to originate that prefix. Each ROA contains a set of IP prefixes and the AS number of one of the ASes authorized to originate all the IP prefixes in the set [RFC6482]. The ROA is cryptographically signed by the party that holds a certificate for the set of IP prefixes.

The ROA format also supports a maxLength attribute. According to [RFC6482], "When present, the maxLength specifies the maximum length of the IP address prefix that the AS is authorized to advertise." Thus, rather than requiring the ROA to list each prefix that the AS is authorized to originate, the maxLength attribute provides a shorthand that authorizes an AS to originate a set of IP prefixes.

However, measurements of RPKI deployments have found that the use of the maxLength attribute in ROAs tends to lead to security problems. In particular, measurements taken in June 2017 showed that of the prefixes specified in ROAs that use the maxLength attribute, 84% were vulnerable to a forged-origin sub-prefix hijack [GSG17]. The forged-origin prefix or sub-prefix hijack involves inserting the legitimate AS as specified in the ROA as the origin AS in the AS_PATH; the hijack can be launched against any IP prefix/sub-prefix that has a ROA. Consider a prefix/sub-prefix that has a ROA that is unused (i.e., not announced in BGP by a legitimate AS). A forged-origin hijack involving such a prefix/sub-prefix can propagate widely throughout the Internet. On the other hand, if the prefix/sub-prefix were announced by the legitimate AS, then the propagation of the forged-origin hijack is somewhat limited because of its increased AS_PATH length relative to the legitimate announcement. Of course, forged-origin hijacks are harmful in both cases, but the extent of harm is greater for unannounced prefixes. See Section 3 for detailed discussion.

For this reason, this document recommends that, whenever possible, operators **SHOULD** use "minimal ROAs" that authorize only those IP prefixes that are actually originated in BGP, and no other prefixes. Further, it recommends ways to reduce the forged-origin attack surface by prudently limiting the address space that is included in ROAs. One recommendation is to avoid using the maxLength attribute in ROAs except in some specific cases. The recommendations complement and extend those in [RFC7115]. The document also discusses the creation of ROAs for facilitating the use of DDoS mitigation services. Considerations related to ROAs and RPKI-ROV in the context of destination-based Remotely Triggered Discard Route (RTDR) (elsewhere referred to as "Remotely Triggered Black Hole") filtering are also highlighted.

Please note that the term "RPKI-based Route Origin Validation" and the corresponding acronym "RPKI-ROV" that are used in this document mean the same as the term "Prefix Origin Validation" used in [RFC6811].

One ideal place to implement the ROA-related recommendations is in the user interfaces for configuring ROAs. Recommendations for implementors of such user interfaces are provided in Section 7.

The practices described in this document require no changes to the RPKI specifications and will not increase the number of signed ROAs in the RPKI because ROAs already support lists of IP prefixes [RFC6482].

### 1.1. Requirements

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

### 1.2. Documentation Prefixes

The documentation prefixes recommended in [RFC5737] are insufficient for use as example prefixes in this document. Therefore, this document uses the address space defined in [RFC1918] for constructing example prefixes.

Note that although the examples in this document are presented using IPv4 prefixes, all the analysis thereof and the recommendations made are equally valid for the equivalent IPv6 cases.

## 2. Suggested Reading

It is assumed that the reader understands BGP [RFC4271], RPKI [RFC6480], ROAs [RFC6482], RPKI-ROV [RFC6811], and BGPsec [RFC8205].

## 3. Forged-Origin Sub-Prefix Hijack

A detailed description and discussion of forged-origin sub-prefix hijacks are presented here, especially considering the case when the sub-prefix is not announced in BGP. The forged-origin sub-prefix hijack is relevant to a scenario in which:

(1) the RPKI [RFC6480] is deployed, and
(2) routers use RPKI-ROV to drop invalid routes [RFC6811], but
(3) BGPsec [RFC8205] (or any similar method to validate the truthfulness of the BGP AS_PATH attribute) is not deployed.

Note that this set of assumptions accurately describes a substantial and growing number of large Internet networks at the time of writing.

The forged-origin sub-prefix hijack [RFC7115] [GCHSS] is described here using a running example.

Consider the IP prefix 192.168.0.0/16, which is allocated to an organization that also operates AS 64496. In BGP, AS 64496 originates the IP prefix 192.168.0.0/16 as well as its sub-prefix 192.168.225.0/24. Therefore, the RPKI should contain a ROA authorizing AS 64496 to originate these two IP prefixes.

Suppose, however, the organization issues and publishes a ROA including a maxLength value of 24:

> ROA:(192.168.0.0/16-24, AS 64496)

We refer to the above as a "loose ROA" since it authorizes AS 64496 to originate any sub-prefix of 192.168.0.0/16 up to and including length /24, rather than only those prefixes that are intended to be announced in BGP.

Because AS 64496 only originates two prefixes in BGP (192.168.0.0/16 and 192.168.225.0/24), all other prefixes authorized by the loose ROA (for instance, 192.168.0.0/24) are vulnerable to the following forged-origin sub-prefix hijack [RFC7115] [GCHSS]:

> The hijacker AS 64511 sends a BGP announcement "192.168.0.0/24: AS 64511, AS 64496", falsely claiming that AS 64511 is a neighbor of AS 64496 and that AS 64496 originates the IP prefix 192.168.0.0/24. In fact, the IP prefix 192.168.0.0/24 is not originated by AS 64496.
>
> The hijacker's BGP announcement is valid according to the RPKI since the ROA (192.168.0.0/16-24, AS 64496) authorizes AS 64496 to originate BGP routes for 192.168.0.0/24.
>
> Because AS 64496 does not actually originate a route for 192.168.0.0/24, the hijacker's route is the only route for 192.168.0.0/24. Longest-prefix-match routing ensures that the hijacker's route to the sub-prefix 192.168.0.0/24 is always preferred over the legitimate route to 192.168.0.0/16 originated by AS 64496.

Thus, the hijacker's route propagates through the Internet, and traffic destined for IP addresses in 192.168.0.0/24 will be delivered to the hijacker.

The forged-origin sub-prefix hijack would have failed if a minimal ROA as described in Section 5 was used instead of the loose ROA. In this example, a minimal ROA would be:

> ROA:(192.168.0.0/16, 192.168.225.0/24, AS 64496)

This ROA is "minimal" because it includes only those IP prefixes that AS 64496 originates in BGP, but no other IP prefixes [RFC6907].

The minimal ROA renders AS 64511's BGP announcement invalid because:

(1) this ROA "covers" the attacker's announcement (since 192.168.0.0/24 is a sub-prefix of 192.168.0.0/16), and

(2) there is no ROA "matching" the attacker's announcement (there is no ROA for AS 64511 and IP prefix 192.168.0.0/24) [RFC6811].

If routers ignore invalid BGP announcements, the minimal ROA above ensures that the sub-prefix hijack will fail.

Thus, if a minimal ROA had been used, the attacker would be forced to launch a forged-origin prefix hijack in order to attract traffic as follows:

> The hijacker AS 64511 sends a BGP announcement "192.168.0.0/16: AS 64511, AS 64496", falsely claiming that AS 64511 is a neighbor of AS 64496.

This forged-origin prefix hijack is significantly less damaging than the forged-origin sub-prefix hijack:

> AS 64496 legitimately originates 192.168.0.0/16 in BGP, so the hijacker AS 64511 is not presenting the only route to 192.168.0.0/16.
>
> Moreover, the path originated by AS 64511 is one hop longer than the path originated by the legitimate origin AS 64496.

As discussed in [LSG16], this means that the hijacker will attract less traffic than it would have in the forged-origin sub-prefix hijack where the hijacker presents the only route to the hijacked sub-prefix.

In summary, a forged-origin sub-prefix hijack has the same impact as a regular sub-prefix hijack, despite the increased AS_PATH length of the illegitimate route. A forged-origin sub-prefix hijack is also more damaging than the forged-origin prefix hijack.

## 4. Measurements of the RPKI

Network measurements taken in June 2017 showed that 12% of the IP prefixes authorized in ROAs have a maxLength value longer than their prefix length. Of these, the vast majority (84%) were non-minimal, as they included sub-prefixes that are not announced in BGP by the legitimate AS and were thus vulnerable to forged-origin sub-prefix hijacks. See [GSG17] for details.

These measurements suggest that operators commonly misconfigure the maxLength attribute and unwittingly open themselves up to forged-origin sub-prefix hijacks. That is, they are exposing a much larger attack surface for forged-origin hijacks than necessary.

## 5. Recommendations about Minimal ROAs and maxLength

Operators **SHOULD** use minimal ROAs whenever possible. A minimal ROA contains only those IP prefixes that are actually originated by an AS in BGP and no other IP prefixes. See Section 3 for an example.

In general, operators **SHOULD** avoid using the maxLength attribute in their ROAs, since its inclusion will usually make the ROA non-minimal.

One such exception may be when all more specific prefixes permitted by the maxLength value are actually announced by the AS in the ROA. Another exception is where: (a) the maxLength value is substantially larger compared to the specified prefix length in the ROA, and (b) a large number of more specific prefixes in that range are announced by the AS in the ROA. In practice, this case should occur rarely (if at all). Operator discretion is necessary in this case.

This practice requires no changes to the RPKI specifications and need not increase the number of signed ROAs in the RPKI because ROAs already support lists of IP prefixes [RFC6482]. See [GSG17] for further discussion of why this practice will have minimal impact on the performance of the RPKI ecosystem.

Operators that implement these recommendations and have existing ROAs published in the RPKI system **MUST** perform a review of such objects, especially where they make use of the maxLength attribute, to ensure that the set of included prefixes is "minimal" with respect to the current BGP origination and routing policies. Published ROAs **MUST** be replaced as necessary. Such an exercise **MUST** be repeated whenever the operator makes changes to either policy.

## 5.1. Facilitating Ad Hoc Routing Changes and DDoS Mitigation

Operational requirements may require that a route for an IP prefix be originated on an ad hoc basis, with little or no prior warning. An example of such a situation arises when an operator wishes to make use of DDoS mitigation services that use BGP to redirect traffic via a "scrubbing center".

In order to ensure that such ad hoc routing changes are effective, a ROA validating the new route should exist. However, a difficulty arises due to the fact that newly created objects in the RPKI are made visible to relying parties considerably more slowly than routing updates in BGP.

Ideally, it would not be necessary to pre-create the ROA, which validates the ad hoc route, and instead create it "on the fly" as required. However, this is practical only if the latency imposed by the propagation of RPKI data is guaranteed to be within acceptable limits in the circumstances. For time-critical interventions such as responding to a DDoS attack, this is unlikely to be the case.

Thus, the ROA in question will usually need to be created well in advance of the routing intervention, but such a ROA will be non-minimal, since it includes an IP prefix that is sometimes (but not always) originated in BGP.

In this case, the ROA **SHOULD** only include:

(1) the set of IP prefixes that are always originated in BGP, and
(2) the set of IP prefixes that are sometimes, but not always, originated in BGP.

The ROA **SHOULD NOT** include any IP prefixes that the operator knows will not be originated in BGP. In general, the ROA **SHOULD NOT** make use of the maxLength attribute unless doing so has no impact on the set of included prefixes.

The running example is now extended to illustrate one situation where it is not possible to issue a minimal ROA.

Consider the following scenario prior to the deployment of RPKI. Suppose AS 64496 announced 192.168.0.0/16 and has a contract with a DDoS mitigation service provider that holds AS 64500. Further, assume that the DDoS mitigation service contract applies to all IP addresses covered by 192.168.0.0/22. When a DDoS attack is detected and reported by AS 64496, AS 64500 immediately originates 192.168.0.0/22, thus attracting all the DDoS traffic to itself. The traffic is scrubbed at AS 64500 and then sent back to AS 64496 over a backhaul link. Notice that, during a DDoS attack, the DDoS mitigation service provider AS 64500 originates a /22 prefix that is longer than AS 64496's /16 prefix, so all the traffic (destined to addresses in 192.168.0.0/22) that normally goes to AS 64496 goes to AS 64500 instead. In some deployments, the origination of the /22 route is performed by AS 64496 and announced only to AS 64500, which then announces transit for that prefix. This variation does not change the properties considered here.

First, suppose the RPKI only had the minimal ROA for AS 64496, as described in Section 3. However, if there is no ROA authorizing AS 64500 to announce the /22 prefix, then the DDoS mitigation (and traffic scrubbing) scheme would not work. That is, if AS 64500 originates the /22 prefix in BGP during DDoS attacks, the announcement would be invalid [RFC6811].

Therefore, the RPKI should have two ROAs: one for AS 64496 and one for AS 64500.

ROA:(192.168.0.0/16, 192.168.225.0/24, AS 64496)

ROA:(192.168.0.0/22, AS 64500)

Neither ROA uses the maxLength attribute, but the second ROA is not "minimal" because it contains a /22 prefix that is not originated by anyone in BGP during normal operations. The /22 prefix is only originated by AS 64500 as part of its DDoS mitigation service during a DDoS attack.

Notice, however, that this scheme does not come without risks. Namely, all IP addresses in 192.168.0.0/22 are vulnerable to a forged-origin sub-prefix hijack during normal operations when the /22 prefix is not originated. (The hijacker AS 64511 would send the BGP announcement "192.168.0.0/22: AS 64511, AS 64500", falsely claiming that AS 64511 is a neighbor of AS 64500 and falsely claiming that AS 64500 originates 192.168.0.0/22.)

In some situations, the DDoS mitigation service at AS 64500 might want to limit the amount of DDoS traffic that it attracts and scrubs. Suppose that a DDoS attack only targets IP addresses in 192.168.0.0/24. Then, the DDoS mitigation service at AS 64500 only wants to attract the traffic designated for the /24 prefix that is under attack, but not the entire /22 prefix. To allow for this, the RPKI should have two ROAs: one for AS 64496 and one for AS 64500.

ROA:(192.168.0.0/16, 192.168.225.0/24, AS 64496)

ROA:(192.168.0.0/22-24, AS 64500)

The second ROA uses the maxLength attribute because it is designed to explicitly enable AS 64500 to originate any /24 sub-prefix of 192.168.0.0/22.

As before, the second ROA is not "minimal" because it contains prefixes that are not originated by anyone in BGP during normal operations. Also, all IP addresses in 192.168.0.0/22 are vulnerable to a forged-origin sub-prefix hijack during normal operations when the /22 prefix is not originated.

The use of the maxLength attribute in this second ROA also comes with additional risk. While it permits the DDoS mitigation service at AS 64500 to originate prefix 192.168.0.0/24 during a DDoS attack in that space, it also makes the other /24 prefixes covered by the /22 prefix (i.e., 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24) vulnerable to forged-origin sub-prefix attacks.

### 5.2. Defensive De-aggregation in Response to Prefix Hijacks

When responding to certain classes of prefix hijack (in particular, the forged-origin sub-prefix hijack described above), it may be desirable for the victim to perform "defensive de-aggregation", i.e., to begin originating more-specific prefixes in order to compete with the hijack routes for selection as the best path in networks that are not performing RPKI-ROV [RFC6811].

In topologies where at least one AS on every path between the victim and hijacker filters RPKI-ROV invalid prefixes, it may be the case that the existence of a minimal ROA issued by the victim prevents the defensive more-specific prefixes from being propagated to the networks topologically close to the attacker, thus hampering the effectiveness of this response.

Nevertheless, this document recommends that, where possible, network operators publish minimal ROAs even in the face of this risk. This is because:

- Minimal ROAs offer the best possible protection against the immediate impact of such an attack, rendering the need for such a response less likely;
- Increasing RPKI-ROV adoption by network operators will, over time, decrease the size of the neighborhoods in which this risk exists; and
- Other methods for reducing the size of such neighborhoods are available to potential victims, such as establishing direct External BGP (EBGP) adjacencies with networks from whom the defensive routes would otherwise be hidden.

## 6. Considerations for RTDR Filtering Scenarios

Considerations related to ROAs and RPKI-ROV [RFC6811] for the case of destination-based RTDR (elsewhere referred to as "Remotely Triggered Black Hole") filtering are addressed here. In RTDR filtering, highly specific prefixes (greater than /24 in IPv4 and greater than /48 in IPv6, or possibly even /32 in IPv4 and /128 in IPv6) are announced in BGP. These announcements are tagged with the well-known BGP community defined by [RFC7999]. For the reasons set out above, it is obviously not desirable to use a large maxLength value or include any such highly specific prefixes in the ROAs to accommodate destination-based RTDR filtering.

As a result, RPKI-ROV [RFC6811] is a poor fit for the validation of RTDR routes. Specification of new procedures to address this use case through the use of the RPKI is outside the scope of this document.

Therefore:

- Operators **SHOULD NOT** create non-minimal ROAs (by either creating additional ROAs or using the maxLength attribute) for the purpose of advertising RTDR routes; and
- Operators providing a means for operators of neighboring autonomous systems to advertise RTDR routes via BGP **MUST NOT** make the creation of non-minimal ROAs a pre-requisite for its use.

## 7. User Interface Design Recommendations

Most operator interaction with the RPKI system when creating or modifying ROAs will occur via a user interface that abstracts the underlying encoding, signing, and publishing operations.

This document recommends that designers and/or providers of such user interfaces **SHOULD** provide warnings to draw the user's attention to the risks of creating non-minimal ROAs in general and using the maxLength attribute in particular.

Warnings provided by such a system may vary in nature from generic warnings based purely on the inclusion of the maxLength attribute to customised guidance based on the observable BGP routing policy of the operator in question. The choices made in this respect are expected to be dependent on the target user audience of the implementation.

## 8. Operational Considerations

The recommendations specified in this document (in particular, those in Section 5) involve trade-offs between operational agility and security.

Operators adopting the recommended practice of issuing minimal ROAs will, by definition, need to make changes to their existing set of issued ROAs in order to effect changes to the set of prefixes that are originated in BGP.

Even in the case of routing changes that are planned in advance, existing procedures may need to be updated to incorporate changes to issued ROAs and may require additional time allowed for those changes to propagate.

Operators are encouraged to carefully review the issues highlighted (especially those in Sections 5.1 and 5.2) in light of their specific operational requirements. Failure to do so could, in the worst case, result in a self-inflicted denial of service.

The recommendations made in Section 5 are likely to be more onerous for operators utilising large IP address space allocations from which many more-specific advertisements are made in BGP. Operators of such networks are encouraged to seek opportunities to automate the required procedures in order to minimise manual operational burden.

## 9. Security Considerations

This document makes recommendations regarding the use of RPKI-ROV as defined in [RFC6811] and, as such, introduces no additional security considerations beyond those specified therein.

## 10. IANA Considerations

This document has no IANA actions.

## 11. References

### 11.1. Normative References

**[RFC1918]** Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

**[RFC2119]** Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

**[RFC4271]** Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

**[RFC6480]** Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

**[RFC6482]** Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

**[RFC6811]** Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

**[RFC7115]** Bush, R., "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 7115, DOI 10.17487/RFC7115, January 2014, <https://www.rfc-editor.org/info/rfc7115>.

**[RFC8174]** Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

### 11.2. Informative References

**[GCHSS]** Gilad, Y., Cohen, A., Herzberg, A., Schapira, M., and H. Shulman, "Are We There Yet? On RPKI's Deployment and Security", NDSS 2017, February 2017, <https://eprint.iacr.org/2016/1010.pdf>.

**[GSG17]** Gilad, Y., Sagga, O., and S. Goldberg, "MaxLength Considered Harmful to the RPKI", CoNEXT '17, DOI 10.1145/3143361.3143363, December 2017, <https://eprint.iacr.org/2016/1015.pdf>.

**[LSG16]** Lychev, R., Shapira, M., and S. Goldberg, "Rethinking security for internet routing", Communications of the ACM, DOI 10.1145/2896817, October 2016, <http://cacm.acm.org/magazines/2016/10/207763-rethinking-security-for-internet-routing/>.

**[RFC5737]** Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", RFC 5737, DOI 10.17487/RFC5737, January 2010, <https://www.rfc-editor.org/info/rfc5737>.

**[RFC6907]** Manderson, T., Sriram, K., and R. White, "Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties", RFC 6907, DOI 10.17487/RFC6907, March 2013, <https://www.rfc-editor.org/info/rfc6907>.

**[RFC7999]** King, T., Dietzel, C., Snijders, J., Doering, G., and G. Hankins, "BLACKHOLE Community", RFC 7999, DOI 10.17487/RFC7999, October 2016, <https://www.rfc-editor.org/info/rfc7999>.

**[RFC8205]** Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

## Acknowledgments

The authors would like to thank the following people for their review and contributions to this document: Omar Sagga and Aris Lambrianidis. Thanks are also due to Matthias Waehlisch, Ties de Kock, Amreesh Phokeer, Éric Vyncke, Alvaro Retana, John Scudder, Roman Danyliw, Andrew Alston, and Murray Kucherawy for comments and suggestions, to Roni Even for the Gen-ART review, to Jean Mahoney for the ART-ART review, to Acee Lindem for the Routing Area Directorate review, and to Sean Turner for the Security Area Directorate review.

## Authors' Addresses

**Yossi Gilad**
Hebrew University of Jerusalem
Rothburg Family Buildings
Edmond J. Safra Campus
Jerusalem 9190416
Israel
Email: yossigi@cs.huji.ac.il

**Sharon Goldberg**
Boston University
111 Cummington St, MCS135
Boston, MA 02215
United States of America
Email: goldbe@cs.bu.edu

**Kotikalapudi Sriram**
USA National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
United States of America
Email: kotikalapudi.sriram@nist.gov

**Job Snijders**
Fastly
Amsterdam
Netherlands
Email: job@fastly.com

**Ben Maddison**
Workonline Communications
114 West St
Johannesburg
2196
South Africa
Email: benm@workonline.africa