TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 01/10 pp 1–12
DOI: 10.26599/TST.2018.9010025
Volume 23, Number 1, February 2018

RISP: An RPKI-Based Inter-AS Source Protection Mechanism

Yihao Jia, Ying Liu, Gang Ren*, and Lin He

Abstract: IP source address spoofing is regarded as one of the most prevalent components when launching an anonymous invasion, especially a Distributed Denial-of-Service (DDoS) attack. Although Source Address Validations (SAVs) at the access network level are standardized by the Internet Engineering Task Force (IETF), SAV at the inter-Autonomous System (AS) level still remains an important issue. To prevent routing hijacking, the IETF is constructing a Resource Public Key Infrastructure (RPKI) as a united trust anchor to secure interdomain routing. In this study, we creatively use the RPKI to support inter-AS SAV and propose an RPKI-based Inter-AS Source Protection (RISP) mechanism. According to the trust basis provided by the RPKI, RISP offers ASes a more credible source-oriented protection for the IP addresses they own and remains independent of the RPKI. Based on the experiments with real Internet topology, RISP not only provides better incentives, but also improves efficacy and economizes bandwidth with a modest resource consumption.

Key words: IP spoofing; source address validation; inter-AS; RPKI; DDoS

1 Introduction

The Distributed Denial-of-Service (DDoS)[1] attack is the most prevalent weapon[2] used to destroy the availability of any Internet-based service[3]. IP spoofing, which is the most critical dependency of a DDoS attack, is the core challenge faced by us. Theoretically, IP spoofing can be divided into two types: d-DDoS for "d"estination-orientated and s-DDoS for "s"ource-orientated attacks[4]. The d-DDoS may attack the target with arbitrary source addresses to simply remain anonymous, whereas the s-DDoS, which is also defined as a reflection attack, sends packets with the target's source addresses to innocent destination hosts, whose replies may then flood the target. In most cases, it is the "source" that suffers the most from IP spoofing attacks. Taking the network time protocol based reflection attack in 2014[5] as an example, to form the 400-Gbps extensive convergence flooding with amplifying traffic, it is the source, not the destination that acts as the assault target. Therefore, the deficiency of source protection for IP address holders should be the main reason leading to such reflection scenarios.

The Source Address Validation Architecture (SAVA)[6] is the most recent and intense research topic in this field. SAVA divides the mission into three levels with different granularities: the access network, intra-Autonomous System (AS), and inter-AS. The first two levels focus on the validation of the packets that originate in the AS, whereas the last level considers the packets originating from other ASes. Despite standardization at the access network level[7] is effectively conducted by the Internet Engineering Task Force (IETF) Source Address Validation Improvements (SAVI) working group, IP spoofing cannot be eradicated only by internal defense methods. Although methods like Ingress/Egress Filtering (IEF)[8] are cost-effective, it cannot prevent IP spoofing unless globe deployment. Therefore, inter-AS SAV is still indispensable against IP spoofing, because it is the only and last defense to prevent IP spoofing from outside of an AS according to SAVA architecture.

The Resource Public Key Infrastructure (RPKI)[9], the major trust anchor of the Internet promoted by IETF Secure InterDomain Routing (SIDR) working group,

• Yihao Jia, Ying Liu, Gang Ren, and Lin He are with the Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China. E-mail: rengang@cernet.edu.cn.
∗ To whom correspondence should be addressed.
Manuscript received: 2017-07-16; accepted: 2017-09-17

is constructed to solve the problem of authenticity of routing origination. The first application of RPKI—Route Origination Authorization (ROA)[10]—naturally provides a built-in stipulation where ASes can be the hosts for a given IP prefix. Therefore, we envision that a data source security for inter-AS SAV will also indirectly benefit from the RPKI system.

In this study, by probing the substance of RPKI, we creatively integrated inter-AS SAV into RPKI and propose RPKI-based Inter-AS Source Protection (RISP). RISP simplifies the logic of inter-AS SAV by decoupling its function, making the system focus on the validation while RPKI focuses on the rest. Through analysis, such a reciprocal attribute provides inter-AS SAV a more concise and modularized structure; this improves the filtering efficiency of traditional methods. To the best of our knowledge, this is the first study that tries to solve inter-AS SAV within the RPKI architecture. The key contributions of this paper can be summarized as follows:

(1) **Decoupled Structure:** RISP is an RPKI-based and RPKI-decoupled method. RISP adequately leverages the trust basis provided by RPKI and works well in the partial deployment of RPKI.

(2) **Source-Oriented Protection:** By valuing "protections" over "validation", RISP provides deployer ASes a more credible protection for the IP addresses they own, triggering decent incentives for themselves.

(3) **Filtering Efficiency:** RISP benefits from the power-law theorem of the Internet to a large extent, achieving high defensive performance with only a small deployment rate.

Through mathematical analysis and related experiments, it is shown that RISP provides deployer ASes decent incentives with a modest resource consumption, and improves performance and saves bandwidth over a typical cryptography-based method.

The rest of this paper is organized as follows: Section 2 describes the related studies. Section 3 describes RISP in detail. Section 4 presents the evaluation of RISP. Section 5 discusses security issues. Section 6 provides the conclusions of this study.

2 Related Studies

2.1 Inter-AS SAV

Inter-AS SAV methodologies implemented at Internet routers can be primarily classified into two types: routing-based validation and labeling-based validation. Routing-based validations verify source addresses by restricting the feasible incoming interfaces for each IP space according to the routing information. However, in most cases, routing-based validations neglect the benefits for deployed ASes themselves, resulting in weak incentives in deployment. Besides, in practice, false positives are another challenge for routing-based methods because of the dynamics of interdomain routing. A labeling-based validation usually involves cryptography, and it verifies the source address using an exclusive customized label. Although these methods introduce extra cost in validating these cryptographic labels, they offer the deployers higher incentives and flexibility even if these ASes are nonadjacent. Challenges for this method mainly include the optimizations of the labeling algorithm and key distribution. In this regard, a labeling-based validation usually presents a trade-off between flexibility and complexity.

In this section, we present the main technologies used for each type of methods to pinpoint both the characteristics and lessons that should be taken away.

2.1.1 Routing-based validation

Source Address Validity Enforcement (SAVE)[11], on the behalf of this type of method, attempts to provide a new protocol to notify each router the potential incoming interfaces for each source address space. However, SAVE only works if it is completely deployed, lacking mechanisms for partial deployment.

Unlike SAVE that depends on collaboration between numerous ASes, InterDomain Packet Filters (IDPF)[12] deployers construct a validation table by individually backward prediction from BGP update messages. Although IDPF acts as a classical representative inheriting the ideology of DPF[13], the possible false negatives are one of the main flaws of this method because of interdomain asymmetry routing.

Another defense technology with a valuable efficacy is the unicast Reverse Path Forwarding (uRPF)[14]. uRPF utilizes the forwarding table as the filter rules for source validation, exhibiting a high potency when deploying at the edge of the Internet. Despite that stub-AS occupies more than 85% of the entire interdomain units[15], the asymmetrical routing makes it impractical and unrealistic to deploy at the core of the Internet.

2.1.2 Labeling-based validation

Hop-Count Filtering (HCF)[16] utilizes the Time To Live (TTL) value as an inherent label of each packet. On the assumption of HCF, the hops of each two hosts are relatively stable, therefore the destination

can easily drop packets carrying an odd TTL value for a given source. Nevertheless, the TTL value remains variable due to dynamic routing; this makes it full of challenging for a traffic crossing domains. Worse, network intermediate nodes may not inspect the correctness of a TTL value, thus attackers can modify the TTL value easily to bypass such a defense.

Spoofing Prevention Mechanism (SPM)[17] is a typical representative to verify a packet source by its related label. In the control plane, the ASes that execute the method negotiate the key privately as the generator of the label. Then in the data plane, the packet that is sent to the ASes, who also belongs to the SPM alliance, would be tagged with an extra label by the key at the source AS border router and checked at the destination router. Essentially, SPM is an End-End verification technology; therefore, the filtering packets merely at the destination AS mean that the bandwidth can still be consumed in the interdomain area by the attackers' invalid flows. Besides, the key negotiation overhead during the inter-AS area would be colossal once the SPM is used for a large scale range.

2.2 RPKI overview

RPKI is an infrastructure designed to prevent the hijacking of inter-AS routing. By accessing the RPKI system, AS border routers can obtain the legitimate ASes list for each IP prefix, and then a BGP update that declares this IP prefix for other ASes would be considered as a hijack and subsequently dropped by these routers.

RPKI has two major components: repository and relying party. On one side, each Internet Number Resource (INR) holder with AS Numbers (ASNs) and IP addresses may maintain an isolated repository. Certificates and objects would be placed in these repositories. Certificates indicate the ownership of the INRs, whereas objects describe their usable range. For routing security, ROA is the object that assigns the original ASes for each IP prefix. On the other side, the relying parties in different places of the world would synchronize the data from all repositories and verify their validity. Subsequently, verification materials would be generated to feed routers that are willing to secure routing.

At present, RPKI has been standardized by more than dozens of RFCs in "SIDR", and RPKI-based innovations such as paper[15] also attract much attention in both research and industrial fields. Although the deployment ratio of RPKI has not reached 10% in five regional Internet registries at the moment, it is considered to be the ultimate solution for interdomain routing security and expected to mature gradually.

3 RISP

As indicated, RPKI provides an anchor for which ASes can announce the BGP update for a given IP prefix, so that malicious ASes cannot hijack the IP spaces that do not belong to them. However, if this scenario is looked at from another perspective, RPKI offers the bindings between ASNs and IP prefixes. In other words, RPKI indicates that the packets using a particular source address can only be sent from these designated ASes. In this regard, RPKI may also play an important role in inter-AS SAV.

This section describes in detail the theory of RISP, a labeling-based validation method. As learned from previous studies, inter-AS SAV usually involves a trade-off between flexibility and complexity. Therefore, at the end of this section, it is explained how RISP achieves decent incentives by valuing "protection" over "validation", and why RISP achieves a more reasonable balance compared to other methods. For conciseness, we denote the AS that enables RISP by RAS; the set of RASes is denoted by RISP alliance and the legacy ASes are denoted by LAS hereafter.

3.1 Architecture

Figure 1 shows the decoupled design of RISP. In such an architecture, both the RPKI repository and relying party play the same role as that in routing security, whereas a **logically centralized** but **practically distributed** center—RISP Alliance Center (RAC)—is introduced in the interdomain area. Besides, an RISP server is required for each RAS. Border routers of these RASes should also be equipped with modules that support inter-AS SAV.

Basically, each RISP server of the RAS would register a symmetric key to RACs and install it in all border routers, and then for the traffic that originates to and from the AS, labels would be tagged on these packets using such symmetric keys. By combining the data from RPKI and RISP servers, a validation rule would be formed in RACs. Subsequently, border

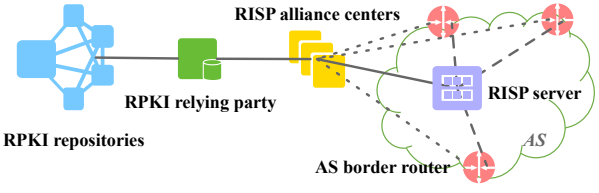


Fig. 1 RISP architecture.

routers of the RASes would adopt the rule to detect inter-AS spoofing by validating the packet carrying the labels, i.e., RAC, on one hand, acts as a service provider of inter-AS SAV, feeding RASes border routers on the validation rule to prevent spoofing; on the other hand, similar to a normal client of the RPKI system, the RAC absorbs the essential data from the relying parties to generate the rule. Foundational functions of these new entities are described below.

3.1.1 RISP server

An RISP server is more like a controller in each deployed AS. On one side, it connects to all the border routers of the RAS to install the basic configuration and symmetric key. On the other side, it registers with the RACs to declare the symmetric key that the AS uses. In addition, such functions can be supported by the RISP server if a reregistration is needed due to some security emergency.

3.1.2 RAC

The **logically centralized** RAC is regarded as the key distribution platform. In practice, similar to the roots of DNS, mirroring of the RAC is advised to reduce potential single point failure. Figure 2 shows the logical structure of the RAC. Two major materials are pulled from the RPKI relying party: "IP-ASN" mapping and "RPKI router public key". The access control module would use the public key to guarantee the security of communication, while both "IP-ASN" mapping and the registration data would be combined to create the validation rule of RISP. Border routers that belong to the RASes would be authorized to access the rule and prevent spoofing.

3.1.3 RAS border router

Both RISP server and RAC would feed the border router to support the RISP validation. Figure 3 shows the structure of the RAS border router. The RISP server would install a symmetric key and local IP space on the border routers; the label engine can tag the packets and source differentiator can distinguish the traffic according to them. The RAC would provide routers with the validation rule, so that the spoofing traffic that uses the source address belonging to RASes would be filtered.

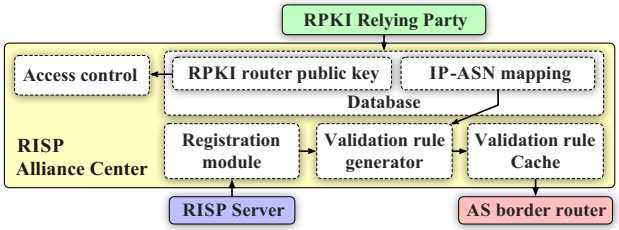


Fig. 2 RAC structure.

3.2 Control plane design

Primarily, RPKI implementation was assumed as the preparation of the RISP deployers, i.e., as a prerequisite, the IP address and ASN holders of RASes should issue the ROAs and RPKI router certificates at their own or upper repositories. Each RISP server of the RAS would register a symmetric key at the RAC, and an "ASN-symmetric key" list will be generated at the registration module of RAC. By combining the mapping of "IP-ASN" and "ASN-symmetric key" using "ASN" as the associated key, a table of "IP-ASN-symmetric key", as shown in Fig. 4, is available at the RAC as the validation rule of RISP. The registration information should be synced among different mirrors of the RAC, so that the RISP servers can register to the nearest mirror. Finally, the RAS border routers would periodically fetch the RISP validation rule from the nearest mirror of the RAC.

Notably, the IP address pertaining the ROA may refer to a variable length of the IP prefix, rather than a fixed length. Although the flexible IP prefix length can prevent hijacking, which "benefits" from the rule of longest prefix matched routing, inter-AS SAV still should protect the IP space of a given AS to the maximum possible extent. Therefore, the combination of two such maps should use the minimum length of the IP prefix for a larger protection space of each RAS.

Besides, to secure the communication of registration and validation rule fetch, a Transport Layer Security (TLS) session with advanced encryption and bilateral identity verification is indispensable for protecting the data from interception. For the identity authentication

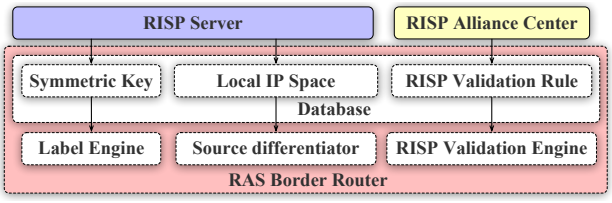


Fig. 3 RAS border router structure.

RISP Validation Rule		
IP	ASN	Symmetric Key
37.12.*.*/16	13 122	d42b2f1a3b12…
2001:2f35:*/48	370	1d43f1a3b25c…
…	…	…

Fig. 4 RISP validation rule.

of the RAC, an RISP root certificate can either be released from an out-band method or preset at the RAS border routers operation system. For registration, RISP servers should provide the signature so that the RAC can reject the invalid ASes based on the "RPKI router public key". For validation rule fetch, the RAC should first identify the AS border routers based on the "RPKI router public key", and subsequently check whether the AS they belong to has registered in the RISP alliance as an RAS. Only AS border routers with an RPKI router certificate and belong to a registered RAS can fetch the rule.

3.3 Data plane design

The data plane logic, as shown in Fig. 5, can be divided into two parts: one for the inflowing traffic, and the other for the outflowing traffic. Notably, it is assumed that all the border routers of the RASes have completed all processes of the control plane described above.

3.3.1 Basic ingress filtering

Inflowing traffic using the source address of deployed ASes themselves should be filtered out. For basic ingress filtering, RAS border routers should inspect the source address of all inflowing traffic and drop those using their own address as the source. Considering that there is no reason why the packets belonging to this AS would originate from others, the inflowing traffic with its own source address can be undoubtedly regarded as IP spoofing.

3.3.2 Labeling

For traffic outflowing from the RASes, RAS border routers should label the packets with source address belonging to their own AS. Considering that RASes already execute the basic ingress filtering at first, packets with the source address of themselves must come from their own users or devices. The content of the label is an exclusive Message Authentication Code (MAC) calculated by the symmetric key owned by the RAS. Such labels would be carried in an extension field of the IP header and treated as the identifier of the packet validity.

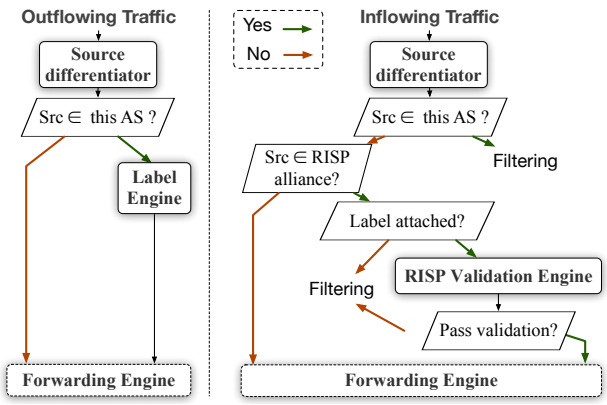


Fig. 5 Processing logic for data plane traffic.

3.3.3 Validation

Besides, for inflowing traffic using the RASes' source address, validity can be identified by the labels carried by these packets. Packets carrying no labels can only be sent from spoofed senders and should be directly filtered out. According to the validation rule obtained from the control plane, the MAC sequence can be calculated by the validation engine. Traffic whose label is inconsistent with the calculation result can be regarded as spoofing, and hence, must be dropped.

3.4 Label design

According to the design of the label, three details should be defined clearly in practical realization.

3.4.1 Labeling extension field

The design of the extension field in IPv4 and IPv6 is quite different. For all the fields in the header of IPv4, referencing the scheme of previous studies such as SPM, "Identification" (16-bit), and "Fragment Offset" (13-bit) could be the most suitable ones for sequence rewriting. First, they are immutable during routing, i.e., the sequence of these fields would not change when passing through the routers that forwarded the packets. Moreover, only about 0.06% of the packets on the Internet are truly fragmented[18]; hence, such collateral damages may be worthy because damages from IP spoofing may surpass those caused by fragmenting. In addition, considering that compatibility with IPv4 will no longer be the focus of the IETF[19], such a collateral damage could be another incentive for IPv6 migration.

For IPv6, owing to the great scalability supported by the IPv6 extension header, any new semantic for IP layer could be presented in a more logical way with a high compatibility. To find a field that satisfies inter-AS SAV the best, we propose an exclusive "RISP extension header" that can only be recognized by RAS border routers at interdomain areas. As the IETF suggests, an assumption should be made that the extension header is automatically ignored by intermediate devices that do not recognize it, including receivers. Besides, the extra 8 bytes introduced by the extension header may exceed the IPv6 Maximum Transmission Unit (MTU) of the external link negotiated before; hence, the border

router should announce a new MTU value that is 8 bytes smaller than the "packet too big" ICMPv6 message.

3.4.2 Labeling algorithm

The algorithm used to calculate the MAC sequence can be flexibly substituted if a more advanced or efficient method is available. In this paper, we recommend the widely acknowledged *AES-CMAC* algorithm[20]: *cmac=AES-CMAC(key, msg)* owing to its high security and extensive high-speed hardware implementations. The *msg* is the bit sequence with a fixed field of the original header that would not change during the interdomain forwarding, and we recommend the source and destination address as the *msg* as the trade-off between security and efficiency. Considering that it is authenticity rather than confidentiality that RISP focuses on, the truncation from 128-bit to 32-bit (IPv6) or 29-bit (IPv4) is acceptable for the RISP system to lower the bandwidth occupation.

3.4.3 Key update

Notice that RISP requires RASes to refresh the key periodically to maintain security. Therefore, a cryptography-secure pseudo-random number generation algorithm[21] could be used to further reduce the complexity of the key update step. Then, to realize such an auto-update, the seed, update algorithm, issue time, updating cycle, expiration time, and calculation algorithm should be stated clearly during the registration for each RAS, and the update could be conducted at RASes locally to reduce the communication burden on RACs. Besides, once a rule is stolen, a key reregistration is needed to resecure the system. Each time a reregistration is submitted to RACs, a notice must be sent to all RASes' RISP servers, and the RISP servers would inform all their border routers to reload the rule from the nearest RAC. It is emphasized that, to remove potential false positives during updating, periodic time synchronization among RACs is necessary to avoid any inconsistency, and for each RAS, a buffer time is indispensable before and after the key update.

3.5 Property summary

Before moving to the evaluation, we briefly describe a few advantageous properties that RISP possesses.

3.5.1 RPKI decoupling

Architecturally, RPKI can support the interdomain security of both routing and SAV. For inter-AS routing, RPKI remains the same as its original design, whereas for inter-AS SAV, RPKI is a part of the RISP and helps RACs produce the validation rule. In this regard, RISP can be regarded as a potential power user of RPKI under such a decoupled structure. Besides, multiplexing the already existing trust anchor allows RISP to avoid potential redundancy, and such a relationship between RPKI and RISP could also be considered as an accelerator to stimulate RPKI's deployment, which may, in turn, promote a positive cycle of the deployment of other security facilities at the inter-AS level.

3.5.2 Source-oriented protection

For an individual AS, spoofing defense has been treated as "protection", and hence, the primary concern of these deployed ASes is to what extent the mechanism can prevent addresses belonging to oneself being used by others. Therefore, RISP is highly designed as a "source-oriented" method to provide deployers the capability against potential s-DDoS attack involving reflection. Therefore, such a source-oriented defense makes RISP more like a "protection" mechanism, rather than a "validation" mechanism. In this regard, RISP can provide deployers more incentives for deploying this method.

3.5.3 On-path filtering

RISP could be regarded as the complementation of both "labeling" and "routing" based methods, with the advantages of each method. Unlike general "labeling-based" methods that filter packets at destination ASes, RISP changes the checking position to intermediate ASes during packet forwarding, reducing the burden of bandwidth and the possibility of attack convergence. In this regard, RISP makes a more "routing-based" approach; however, the cryptography-based labeling helps it avoid the intrinsic false positives of those mechanisms.

4 Evaluation

In this section, we evaluate RISP by "deployment incentives", performance, overhead, and false positives.

Most importantly, because we focus on the inter-AS scenario, as indicated earlier, methods that overemphasize the filtering effect usually ignore the incentives for AS deployers, and severely degrade the deployability for its practical implementation. In this regard, we consider "deployment incentives" as the most important and practical criterion for our evaluation. After that, to explore whether RISP

can provide good efficacy and a low error rate at reasonable costs, we studied the overall filtering performance, overheads, and false positives consulted from Ref. [22]. "Performance" is an empirically crucial criterion because it presents the effectiveness of IP spoofing prevention. Also, "overhead" is vital as well because it potentially affects, the feasibility whether a method can be practically accepted and implemented. Besides, notably ASes, in general, tend to provide the optimal service quality, and hence, methods with "false positives" are not allowed in practice.

To clearly elucidate the evaluation, we took the "incentive" metric as an elaborate example in the first evaluation part to disclose the theories adopted in these experiments. Evaluations of the performance obey the same model. Besides, because SPM is presented as a typical cryptography and labeling based method, we introduce it as the comparison in the analysis regarding the similar filtering mechanism and compatible assessment model consulted from Ref. [4]. For conciseness, we denoted the universal set of all the existing ASes by N and the set of all RASes by M with the number of n and m, respectively.

4.1 Deployment incentive

4.1.1 Mathematical analysis

The deployment incentive, which quantizes the desire of an LAS to be an RAS, is defined as the benefit of this implementing. Theoretically, we quantified the benefit as the "protection" they will gain in view of the reflection DDoS attack, i.e., whether the LAS can prevent their own IP addresses from being used by others.

Let $\mathrm{spf}(s, d, v)$ depict the spoofed traffic that originates from a source AS s to a destination AS d, taking IP addresses belonging to the victim AS v. Denoted by $F\{M, \mathrm{spf}(s, d, v)\}$, the result of whether AS v could be immune from a specific $\mathrm{spf}(s, d, v)$ under the protection of M, is given as follows:

$$F\{M, \mathrm{spf}(s, d, v)\} = \begin{cases} 1, & \text{if } M \text{ can filter } \mathrm{spf}(s, d, v); \\ 0, & \text{otherwise.} \end{cases}$$

Defining $\delta = \Delta\{M, \mathrm{spf}(s, d, v)\}$ as the benefits of the AS v's transformation from LAS to RAS,

$$\delta = F\{M \cup \{v\}, \mathrm{spf}(s, d, v)\} - F\{M, \mathrm{spf}(s, d, v)\}.$$

Because validation is executed for IP addresses belonging to RASes, an LAS cannot receive any protection from the RISP alliance M, i.e., $F\{M, \mathrm{spf}(s, d, v)\} = 0$. Thus, $\delta = F\{M \cup \{v\}, \mathrm{spf}(s, d, v)\}$. Hence $\delta = 1$ indicates that an LAS can benefit from the protection of a potential s-DDoS attack by deploying RISP, and $\delta = 0$ indicates that the LAS cannot filter such $\mathrm{spf}(s, d, v)$ by turning into an RAS.

p_i^{S}, p_i^{D}, and p_i^{V} are the independent probabilities of an AS i being the source AS, destination AS, or the victim AS, respectively, where $\forall i,\ 0 \leqslant p_i^{\mathrm{S}}, p_i^{\mathrm{D}}, p_i^{\mathrm{V}} \leqslant 1$, $\sum_i p_i^{\mathrm{S}} = \sum_i p_i^{\mathrm{D}} = \sum_i p_i^{\mathrm{V}} = 1$. Let $\mathrm{inc}(M, v)$ depict the incentives for an LAS v's transformation to RAS, so that the value of $\mathrm{inc}(M, v)$ can be derived as δ's weighted accumulation:

$$\mathrm{inc}(M, v) = \sum_{i,j} p_i^{\mathrm{S}} p_j^{\mathrm{D}} \Delta(M, \mathrm{spf}(s, d, v)).$$

$\mathrm{route}(s, d)$ is the AS sequence that $\mathrm{spf}(s, d, v)$ would be forwarded. Then, as the RISP mechanism executes, filtering would work at the first RAS in $\mathrm{route}(s, d)$, and spoofing traffic $\mathrm{spf}(s, d, v)$ can be filtered if $v \in \mathrm{RAS}$ and $\mathrm{route}(s, d) \cap M \neq \emptyset$. Therefore, $\delta = \Delta\{M, \mathrm{spf}(s, d, v)\} = 1$ if $\mathrm{route}(s, d) \cap \{M \cup \{v\}\} \neq \emptyset$, then $\mathrm{inc}(M, v)$ can be further defined as:

$$\mathrm{inc}(M, v) = \sum_{\mathrm{route}(i,j) \cap \{M \cup \{v\}\} \neq \emptyset} p_i^{\mathrm{S}}\, p_j^{\mathrm{D}}.$$

As the expression $\mathrm{inc}(M, v)$ indicated, the value of $\mathrm{inc}(M, v)$ monotonically increases as m increases, i.e., if $M_1 \subset M_2$, then $\mathrm{inc}(M_1, v) < \mathrm{inc}(M_2, v)$. In brief, if more LASes become RASes, the value of m would increase. In this case, the higher is the possibility of $\mathrm{spf}(s, d, v)$ transmitted by an RAS. Therefore, the benefits of RISP snowball for both RASes and the LASes deploying the technology.

To further express $\mathrm{inc}(M, v)$, traffic volume that is sent by (and to) each of the AS must be counted to imitate the real Internet environment. Unfortunately, the data described here are difficult to obtain. To approximate a real environment as much as possible, we adopt the widely applied "address equivalence" hypothesis in this research field. The address equivalence hypothesis assumes that the traffic shuttling from arbitrary IP addresses is undiscriminating, indicating that the traffic volume from different ASes is proportional to the address space they own. Under such assumptions, every routable address has the same probability of being the source, destination, and victim. Although this assumption is just an approximation, it is enough to appraise the efficacy of these methods to a certain extent.

To embody $\mathrm{inc}(M, v)$ in the address equivalence

hypothesis, we present the metric from a statistical angle. Let $g(x)$ denote the routable address space of AS_x; then for a specific source AS_s, spoofed traffic that employs v's addresses could be aimed at $n-1$ destinations. Thus, the aggregate spoofed flows from AS_s could be assumed to be $\lambda = g(s)\sum_{d\neq s} g(d)$. RISP can filter the traffic routing through M; hence, flows that could be filtered can be expressed as $\theta = g(s)\sum_{\mathrm{route}(s,\,d)\cap M\neq\emptyset} g(d)$. Therefore, total incentives $\mathrm{inc}(M, v)$ from RISP could be formalized as the weighted average of λ/θ as below:

$$\mathrm{inc}(M, v) = \frac{\sum_{s\in N}\left(g(s)\sum_{\mathrm{route}(s,\,d)\cap M\neq\emptyset} g(d)\right)}{\sum_{s\in N}\left(g(s)\sum_{d\neq s} g(d)\right)}.$$

4.1.2 Experiments and datasets

To verify the above theory, we measured the metric under different deployment ratios. Initially, we let $M = \emptyset$, and at each time point we randomly selected an LAS in M and calculated the incentives at this sampling point until all ASes were in M (random mode). We used the topology of the entire Internet with AS relationships from the CAIDA "AS Relationships" dataset on "2016-05-01"[23], and used the IP Mapping prefix-ASN from the CAIDA database "RouteViews Prefix to AS Mappings" from the same date[24]. Meanwhile, we used C-BGP[25] as a sophisticated simulator to find the route for any two ASes in the interdomain area.

4.1.3 Deployment strategy

Another question facing the implementation of this practice is that AS should be the initial RAS during the early stage of deployment. Because RISP filters packets during forwarding, the more important an AS in interdomain traffic transiting is, the more prominent it will be in the RISP system. Therefore, a crucial breakout for this question is to establish the AS that acts in this important role in interdomain traffic transiting.

Fortunately, the AS transit degree[26] proposed in Ref. [27] as a key metric for AS relationship detection embodies the characteristics sought by us. To recapitulate it in brief, the AS transit degree depicts the number of ASes that were observed receiving transit paths through a given AS. Therefore, in the second experiment, we always selected the LAS with the largest transit degree, instead of the random LAS, as our "Optimal" strategy.

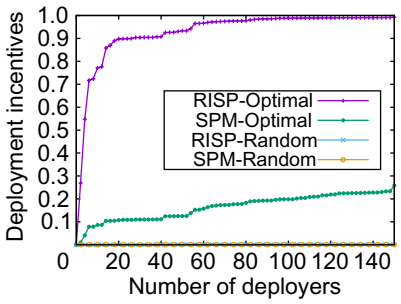
4.1.4 Results analysis

According to the results shown in Fig. 6, $\mathrm{inc}(M, v)$ is indeed a monotonic increasing function. Compared to the traditional cryptography method—SPM with a similar mathematical theory, it is reliable that RISP does go further in providing a better incentive. Theoretically, for $\mathrm{spf}(s, d, v)$ that $v \in M$, SPM can only filter packets for which $d \in M$, whereas RISP works once it flows through M. Therefore, the incentives of RISP will always exceed those in SPM within the same deployer set M. By concurrently drawing the SPM incentives at each sampling point, we find that although SPM obviously benefits from the "Optimal" selection mode, RISP may provide overwhelming superiority against this method in both the selection modes.

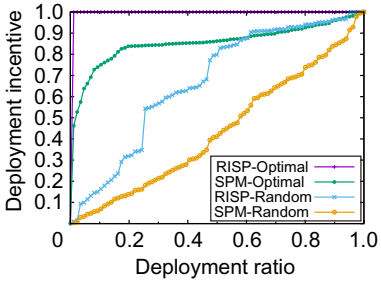
Besides, the results show that the incentives shown in Fig. 6b burst rapidly at the early deployment stage with more than 90% and 98% under only 61 and 120 deployers. In other words, almost all potential s-DDoS attacks that aim at an LAS, at such a sampling point, will be eliminated once an LAS uses RISP, i.e., RISP benefits from the power-law theorem of the Internet[28], and the extremely high initial incentives may trigger a virtuous circle if RASes are strategically selected.

4.2 Performance study

Based on the same mathematical theory and evaluation



(b) At early stage



(a) Whole deployment process

Fig. 6 Incentives along deployment.

model mentioned above, we studied the RISP's overall capability in preventing IP spoofing at the inter-AS level. In this subsection, we first simulated the filtering efficacy by drawing the proportion of global spoofing reduction. Then, by contrasting with the representative SPM, we show that RISP clearly improves the performance improvement and economizes the bandwidth.

4.2.1 Effectiveness

Figure 7a shows the global efficacy in IP spoofing prevention. Similar to our observations on the "incentive", the effectiveness of RISP surpasses that of SPM in both the "Random" and "Optimal" modes. In this regard, more spoofing traffic will be filtered in RISP under the unified deployment set. More importantly, according to the results in Fig. 7a, RISP filters out more than 70% of spoofed traffic with only 7% deployment in the "Optimal" mode, exhibiting a strong defense performance for the entire community.

4.2.2 Efficacy improvement

To find the amount of progress that has been made by using RISP, we computed the ratio of the spoofed traffic reduction between RISP and SPM under the unified deployment set. Figure 7b shows that RISP has a greater filtering capability than SPM in both the modes. However, an interesting phenomenon was observed: The progress in the "Optimal" mode is slightly lower than that in the "Random" mode. This is probably because the "Optimal" mode provides stronger performance improvements for SPM as well and narrows the gap between it and RISP.

4.2.3 Bandwidth economization

Another advantage of RISP is the improved bandwidth economy "borrowing" from the routing-based method. Unlike the spoofed traffic, which can only be filtered at the destination ASes under SPM, RISP filters packets on intermediate ASes as packets pass by. Therefore, even traffic that can be filtered effectively by SPM can be dropped earlier under the RISP system. To simulate the process economizing bandwidth, we simply extract the inter-AS hop count of the packets before they are filtered as an abstraction of the bandwidth utility.

As shown in Fig. 7c, the bandwidth economy improves as the number of deployers increases, reaching 68% in a global deployment scenario. While under the "Optimal" selection model, the value surges to 50% with only 500 RASes; more than half of the

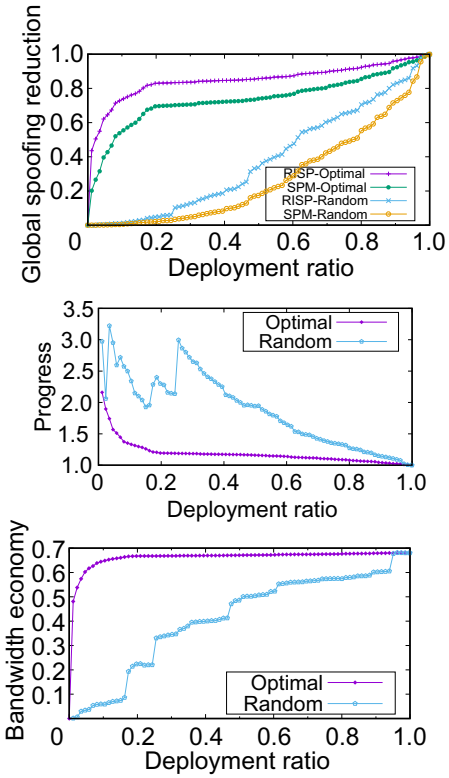


Fig. 7 a) Effectiveness; (b) Efficacy improvement; (c)Bandwidth economizing.

ASes should deploy RISP to achieve the equivalent performance with the "Random" model. Thus, RISP provides a dramatic bandwidth economy improvement compared to SPM, with rapid convergence if the "Optimal" model is executed.

4.3 Overhead

In this section, we estimate the overhead of RISP in both the control and data planes. In the control plane, the overhead cost mainly stems from the key distribution, while in the data plane, the overhead cost mainly stems from cryptography computation.

4.3.1 Key distribution

For a practical implementation, the biggest problem for SPM is the tremendous key negotiation overhead that increases along with the number of deployers.

Traditional key negotiation distributes the keys in a bilateral way, i.e., the overhead in that way would be $o(m^2)$. Unlike the traditional bilateral key negotiation, RISP deployers submit the keys to the logical center—RAC, and RAC acts as a unique key distribution platform for all deployers. Thus, the overhead of RISP for the control plane would be decreased from $o(m^2)$ to $o(m)$. Considering that the key rollover can be updated

periodically at local RASes automatically, the overhead of RISP is acceptable for practical deployment.

Attention should be paid to the fact that the unitive key distribution platform cannot provide equal security as the bilateral platform, and we regard it as the result of a trade-off between security and complexity. The security issues will be intensively discussed in the next section.

4.3.2 Cryptography computation

For the data plane, the overhead of RISP may stem from a table lookup and cryptography computation. Although packets belonging to LASes would not require any validation during interdomain forwarding, we focused on the validation computation to explore whether it would become a bottleneck practically. As indicated above, the cost of computation highly depends on the algorithm used, but we still evaluated that for *AES-CMAC* to explain the feasibility of cryptography. Owing to the high-speed hardware utilization of *AES-CMAC*, the implementations on ASIC and FPGA can already handle a maximum traffic throughput of around 2 Gbps per IP core[29]. Therefore, the throughput of tens of gigabits per second in the interdomain area is completely acceptable in view of the benefit they receive.

In addition, notably if we adopt the "Optimal" deployment model at this early stage, it may not be easy for RASes with a greater transit degree because of the huge traffic they transmit. Although the overhead of RISP is strictly limited in the above range, it is proportional to the traffic volume processed. Considering that ASes, especially that in Tier-1, are more likely to forward traffic of hundreds of gigabits per second, more hardware should be updated in supporting such a huge traffic they deliver.

4.4 False positives analysis

According to the filtering logic, the false positives of RISP can stem from the inconsistency of the validation rule. To avoid this inconsistency, we recommend reserving a one-minute time buffer in practice after the key rollover and key reregistration. Each time the key update is triggered, previous keys should be considered as valid during the buffer time zone. Besides, especially for key reregistration, new keys can be used only after that time zone. However, implementation in practice may have some instability caused by the practical situation, and the buffer time could be extended in the case of errors such as delays among different RAC mirrors.

5 Security Issues

This section analyzes three potential threats that RISP may face. For these threats, possible solutions or advices are proposed to narrow these attack spaces. To ensure a high-level security, AS reputation systems such as system in Ref. [30] could be introduced to dislodge maliciously deployed ASes. However, without the loss of generality, it is assumed that RASes that joined the RISP alliance would strictly observe the regulation of the design, and the operations of RPKI are stable as desired.

5.1 DDoS attacking

Although massive DDoS attacks can be significantly weakened if the source addresses are difficult to spoof due to the implementation of RISP, attacks that use a genuine source address from a gradually growing number of IoT devices may still be able to degrade the defense system to a certain degree.

5.1.1 RPKI orientated

DDoS attacks that aim at a relying party may not cause trouble because the "users" of RPKI may be configured with several alternatives; hence, the RAC can be quickly switched to a backup if the primary one is interrupted. Besides, DDoS attacks may also aim at RPKI repositories and their inner policies. However, the policies prepared for interdomain area are relatively stable in view of a downtime period.

5.1.2 RAC orientated

RACs may not be absolutely safe, even though a mirror technology is introduced in the RISP system. DDoS mitigation methods such as BGP Anycast may work to reduce the attacking space, and the security policy should be further considered during its realization. Fortunately, studies in the DDoS mitigation area are continuously active; technologies such as methods in Ref. [31] can be gradually introduced to defend against such attacks.

5.1.3 RAS orientated

Attackers may attempt to overwhelm the border routers of the target RAS with massive spurious labels, and networks may crash once the computation consumption is not affordable during the malicious flooding. However, it is easier for border routers to selectively pause the validation once the computation resources are completely depleted. Hence, DDoS attacks aiming at RASes still remain challenging.

5.2 Rule interception

Theoretically, communications involving RAC are all equipped with advanced encryption and bilateral authentication. Therefore, rule interception during communications is more about a practice problem, rather than a design issue. Besides, attackers may attempt to compromise the RAS border routers to steal the rule. To defend against such threats, border routers that enable RISP should be installed with strict security policy to protect themselves against such an invasion. Besides, a global rule update is obligatory once the rule is intercepted.

5.3 Brute force

The brute-force label forgery attack is expected to succeed in guessing the correct symmetric key after 2^{31} (IPv6) or 2^{28} (IPv4) attempts, therefore, a theoretically spoofed traffic may survive during the rekey period. However, the cost of such an attack seems prohibitive for most invasions. Attackers can be easily frustrated by expanding the bit sequence of the identifier label or simply by reducing the period of key rollover.

6 Conclusion

In this paper, we proposed an inter-AS SAV mechanism: RISP as a new application of RPKI. Architecturally, RISP adequately leverages the trust basis provided by RPKI and works well in RPKI's partial deployment. According to the source-oriented validation, RISP offers ASes a more credible protection for IP addresses they own, triggering decent incentives and increasing defense efficacy. Based on the experiments with real Internet topology, RISP avoids inherent false positives as well as relieves the burden of bandwidth with modest resource consumption.

Acknowledgment

This work was supported by the National Natural Science Foundation of China Nos. 61772307 and 61402257, the National Key Basic Research and Development (973) Program of China Nos. 2009CB320500 and 2009CB320501, and Tsinghua University Self-determined Project under grant No. 2014z21051.

References

[1] C. Rossow, Amplification Hell: Revisiting network protocols for DDoS abuse, in *Network and Distributed System Security Symposium (NDSS)*, San Diego, USA, CA, 2014.

[2] Arbor Networks and Google idea, DDoS visualization map, http://www.digitalattackmap.com/, 2017.

[3] D. Anstee, P. Bowen, C. Chui, and G. Sockrider, 12th worldwide infrastructure security report, 2017.

[4] B. Liu and J. Bi, Discs: A distributed collaboration system for inter-as spoofing defense, in *International Conference on Parallel Processing (ICPP)*, Beijing, China, 2015.

[5] M. Prince, Technical details behind a 400Gbps NTP amplification ddos attack, Cloudflare Inc, https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/, 2017.

[6] J. Wu, J. Bi, X. Li, G. Ren, M. Williams, and K. Xu, A Source Address Validation Architecture (SAVA) testbed and deployment experience, RFC 5210, June 2008.

[7] J. Wu, J. Bi, M. Bagnulo, F. Baker, and C. Vogt, Source Address Validation Improvement (SAVI) framework, RFC 7039, Oct. 2013.

[8] P. Ferguson, Network Ingress Filtering: DDoS attacks which employ IP source address spoofing, RFC 2827, May 2000.

[9] M. Lepinski and D. S. T. Kent, An infrastructure to support secure internet routing, RFC 6480, Feb. 2012.

[10] M. Lepinski, D. Kong, and S. Kent, A profile for Route Origin Authorizations (ROAs), RFC 6482, Feb. 2012.

[11] J. Li, J. Mirkovic, T. Ehrenkranz, M. Wang, P. Reiher, and L. Zhang, Learning the valid incoming direction of ip packets, *Computer Networks*, vol. 52, no. 2, pp. 399–417, 2008.

[12] Z. Duan, X. Yuan, and J. Chandrashekar, Constructing inter-domain packet filters to control IP spoofing based on BGP updates, in *International Conference on Computer Communications (INFOCOM)*, Barcelona, Spain, 2006.

[13] K. Park and H. Lee, On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets, *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 15–26, 2001.

[14] F. Baker and P. Savola, Ingress Filtering for Multihomed Networks, RFC 3704, Mar. 2004.

[15] A. Cohen, Y. Gilad, A. Herzberg, and M.Schapira, Jumpstarting BGP security with path-end validation, in *Special Interest Group on Data Communication (SIGCOMM)*, Florianpois, Brazil, 2016.

[16] C. Jin, H. Wang, and K. G. Shin, Defense against spoofed IP traffic using Hop-Count filtering, *IEEE/ACM Transactions on Networking*, vol. 15, pp. 40–53, 2007

[17] A. Bremler-Barr and H. Levy, Spoofing prevention method, in *Proceedings of IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 536–547, 2005.

[18] R. Beverly, A. Berger, Y. Hyun, K. Claffy, Understanding the efficacy of deployed internet source address validation filtering, in *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference*, pp. 356–369, 2009.

[19] L. Howard, IETF: End Work on IPv4, Internet-Draft draft-ietf-sunset4-ipv6-ietf-00, Internet Engineering Task Force, Mar. 2017, Work in Progress.

[20] J. Lee and R. Poovendran, The AES-CMAC algorithm, RFC 4493, June 2006.

[21] M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudorandom bits, *SIAM Journal on Computing*, vol. 13, no. 4, pp. 850–864, 1984.
[22] J. Mirkovic and E. Kissel, Comparative evaluation of spoofing defenses, *IEEE Trans. Dependable Sec. Comput,*, vol. 8, pp. 218–232, 2011.
[23] AS-relationships, http://data.caida.org/datasets/as-relationships, 2017.
[24] Prefix-to-AS-Mappings, http://data.caida.org/datasets/routing, 2017.
[25] B. Quoitin and S. Uhlig, Modeling the routing of an autonomous system with c-bgp, *IEEE Network*, vol. 19, no. 6, pp. 12–19, 2005.
[26] AS rank by transit degree, http://as-rank.caida.org, 2017.
[27] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and K. Claffy, AS relationships, customer cones, and validation, in *Proceedings of the Conference on Internet Measurement*, pp. 243–256, 2013.
[28] M. Faloutsos, P. Faloutsos, and C. Faloutsos, On power-law relationships of the internet topology, *ACM SIGCOMM Computer Communication Review*, vol. 29, pp. 251–262, 1999.
[29] AES-cores, http://www.heliontech.com/aes.htm, 2017.
[30] M. Konte, R. Perdisci, and N. Feamster, Aswatch: An AS reputation system to expose bulletproof hosting ases, *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 625–638, 2015.
[31] S. Mansfield-Devine, DDoS: Threats and mitigation, *Network Security*, vol. 2011, no. 12, pp. 5–12, 2011.

Yihao Jia is currently a PhD candidate at Institute for Network Sciences and Cyberspace, Tsinghua University, China. His research interests include network architecture and protocol design. He received the bachelor degree in network engineering from University of Electronic Science and Technology of China in 2014.

Ying Liu received the MS degree in computer science and the PhD degree in applied mathematics from Xidian University, China in 1998 and 2001, respectively. She is currently an associate professor at Tsinghua University, China. Her major research interests include network architecture design, next generation Internet architecture, and routing algorithm and protocol.

Gang Ren received the PhD degree in computer system architecture from Tsinghua University, China in 2009. He is currently an assistant professor at Tsinghua University, China. His major research interests include network architecture design, next generation Internet architecture, and network security.

Lin He is currently a Ph.D. candidate at Institute for Network Sciences and Cyberspace, Tsinghua University, China. His research interests include network architecture design, IPv6 address generation and management, and network protocol design.