2012 IEEE 11th International Symposium on Network Computing and Applications

A Multi-Fence Countermeasure Based Inter-domain Source Address Validation Method

Jie Li[*,2,3], Jun Bi [†,1,3], Jianping Wu [‡,1,2,3], Wei Zhang[§,2,3]
[1] Network Research Center, Tsinghua University, Beijing, China
[2] Dept. Computer Science & Technology,Tsinghua University, Beijing, China
[3] Tsinghua National Laboratory for Information Science & Technology (TNList), Beijing, China
[*] jieli@csnet1.cs.tsinghua.edu.cn, [†] junbi@tsinghua.edu.cn, [‡] jianping@cernet.edu.cn,[§] zw@netarchlab.tsinghua.edu.cn

***Abstract*—The functional deficiency of the Internet architecture enables attackers the ability to easily to spoof IP source address. The traditional signature-and-verification based anti-spoofing methods are often limited by essential process based on an explicit analysis and process of the IP header and does not adapt to incremental deployment. This paper designs a multi-fence countermeasure based inter-domain source address validation method named VIP. By employing intelligent originating information label and extended MPLS based cloud and network, VIP enables lightweight-label-based packet forwarding and validation. And VIP offers gains in efficiency by reducing the load on both forwarding tables and validation processing without negative influences and complex operations on de facto networks. In addition to enhanced scalability, VIP may facilitate incremental deployment in the long run.**

Keywords- extended MPLS; inter-domain; IP source address validation; network security

I. INTRODUCTION

The Internet architecture includes no explicit notion of packet-level authenticity, which enables attackers the ability to easily to spoof IP source address. By masquerading as a different source, an attacker can stage attacks that undermine the security of fundamental Internet applications and redirect blame, and even induce millions of dollars of financial losses. Research reports by Arbor Networks [1] and CERT [2] show that spoofing-based attacks have now become an everyday occurrence and the Internet that has been plagued by the exponential rise of attacks and offensives increasing in both scale and frequency over recent years.

With varying levels of success, many researchers and operational networks have implemented source address validation good common practices: [3] and [4] are classical examples to defend against source spoofing. In practice however, the implementation of the method presented in [3] is not DoS/DDoS resilient in the key-update process and cannot be used for anti-spoofing of smaller granularities [4]. The method in [4] is derived from and improves upon [3] and is more effective and secure. However, this method makes all deployed autonomous systems (AS) of the trust alliance (TA) maintain a full-mesh and two-way of state machine (SM): when implemented on a large scale, this approach leads to a heavy management cost on validation rules and introduces extra delay on verifying packets. And the reliability and efficiency of the methods proposed in [3] and [4] are often limited by essential forwarding and validation mechanisms based on an explicit analysis and process of the IP header. This paper proposes an efficient and secure mechanism to verify the source of a packet, called VIP: an extension-MPLS-based, inter-domain authenticated source address validation solution.

Our method addresses efficiency by addressing the implications that routers can authenticate the source of a packet at high-speed based on the extended Multi-protocol Label Switching protocol (MPLS [5]) networks without any changes to the de facto topological structure and inter-domain routing protocol(s). Our solution addresses security by the use of multi-fence mechanisms (the integrating design of internal-oriented constraint prevention, external-oriented suppression prevention, and validation). This makes it impossible to send traffic with bogus IP source address and to trigger impersonation attacks. Moreover, in contrast to the methods in [3, 4], VIP is more resilient to changes in the network topology and changes in the route from source to destination and requires no special operations at intermediate nodes and end hosts.

II. DESIGN PRINCIPLE OF VIP

VIP advocates an intelligent, light-weighted *OIL* (originating information label) based extended MPLS network without negative influences on networks and can provide a way to enable trustworthy and efficient source authentication.

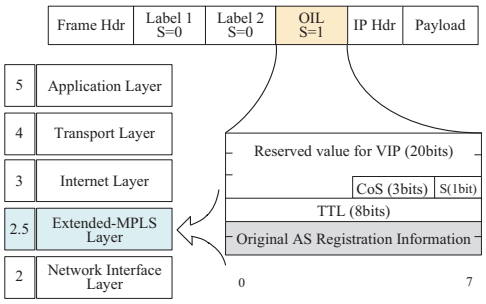

Figure 1. Location and format of the OIL label.

A. Basic Design

We propose a special globally unique MPLS label called a source identifier label, or simply an *OIL*. It is encapsulated in the MPLS layer header as shown in Fig. 1. The OIL is

This work was supported by National Science Foundation of China under Grant 61073172, Program for New Century Excellent Talents in University, Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20090002110026,and National Basic Research Program ("973" Program) of China under Grant 2009CB320501.

978-0-7695-4773-2/12 $26.00 © 2012 IEEE
DOI 10.1109/NCA.2012.20

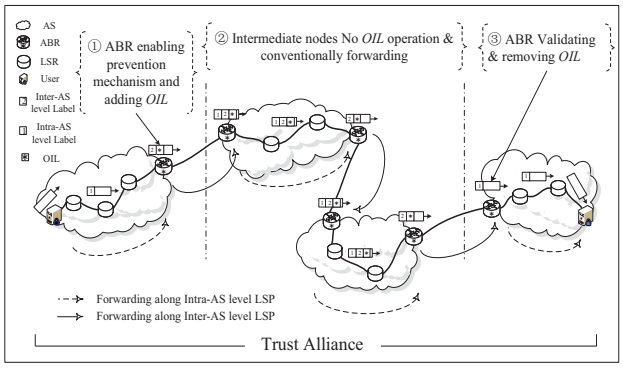

Figure 2. A demonstration of forwarding and validating in VIP.

only used for identifying the origin and validating the authenticity of IP source address rather than using for forwarding. Architecturally speaking, VIP can support a hierarchical MPLS label stack which is used to achieve nesting in packet networks; the OIL is located at the bottom of this type of label stack. We refer to the AS enabled OIL as the extended-MPLS AS. In accordance with real world network situations, VIP makes adjacent extended-MPLS ASes consist of the TA as members and establish cooperatively the multi-domain extended-MPLS network, in light of flexibly choosing different strategies such as routing policy, network topology, data communication frequency, economic strategy and subordinate relations and so on. Relying on the extended-MPLS network within the scope of the TA, routers residing in each extended-MPLS AS perform path computations to create the intra-domain level Label Switched Path (LSP) whereby packets can be quickly transported to the domain border across multiple routers within the extended-MPLS AS. Moreover, different extended-MPLS ASes also consult and assign MPLS forwarding label to set up the inter-domain level LSP that carries packets quickly to span multiple domains. In this way, VIP adheres to nest separate intra-domain level LSPs and inter-domain level LSPs into one 2-level hierarchical end-to-end LSP from source domain to destination domain within the scope of TA. During the labeled packets forwarding along the end-to-end LSP from source to destination, the OIL is added by the AS border router (ABR) residing in source domain ensuring the functionality of identifying the origin, and removed by the ABR belonging to the destination domain through the ability to validate the authenticity of IP source address. With leveraging the extended-MPLS label, VIP enables label-driven routing, forwarding and validating to achieve the goal that no further IP header analysis and authentication needs to be done by subsequent routers; in this way our approach reduces both forwarding tables and validation processing load. VIP focuses on enforcing the routing and forwarding to a high-speed level and further ensuring the functionality of light-weight and efficiently authenticating the source of a packet to the granularity of the origin AS without negative influence and complex operations on de facto networks.

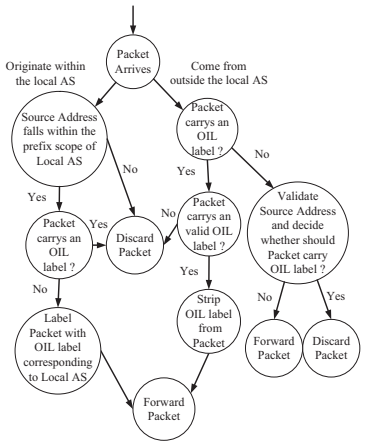

Figure 3. Flow chart of the packets validating process.

B. *Multi-fence Validating Mechanisms*

At first, labeled packets are forwarded to the source domain border along the intra-domain LSP and the ABR enables the first level prevention mechanism by verifying the source of these incoming packets according to the validation rules. This aims to filter the illegitimate packets and guarantee the initial authenticity, i.e. *the internal-oriented constraint process*; then, the ABR removes the intra-domain label and adds the OIL on the bottom and the inter-domain label on the top of label stack in the legitimate packet, and delivers all legitimate packets to downstream neighboring extended-MPLS AS according to the inter-domain LSP. Thus, the ABR enables the second level prevention mechanism by embedding the OILs into the packets. This aims to prevent local AS' prefixes from being spoofed from outside the local AS and enhance the trustworthiness of source, i.e. *the external-oriented suppression process*. When packets reach their neighboring extended-MPLS AS, the ABR swaps the inter-domain level label and adds a specified local intra-domain level label at the top of the label stack and transits labeled packets along the local intra-domain LSP toward the border that connects to the next downstream extended-MPLS AS en route. During the process of forwarding labeled packets, the intermediate Label Switched Router (LSR) simply implements the conventional MPLS forwarding. In this fashion, as long as the packets transit several intermediate extended-MPLS ASes, the ABRs and LSRs allocated to these ASes continue to complete the label operation on the top of label stack from source to destination, and do not need deal with the OIL. Finally, when the packets reach the destination AS, the ABR verifies and removes the OILs still encapsulated at the bottom of the label stack by checking validation rules, i.e. *the destination validation process*, which accomplishes the whole process of source validation (Fig. 2).

VIP enables the spoof-proof mechanism of the OIL-specific information from the end hosts as well as legacy networks outside. If a packet labeled with a bogus OIL is sent to the ABR either from inside an extended-MPLS AS network or from an outside legacy AS network, the ABR

automatically drops it. Meanwhile, when extended-MPLS ASes receive general packets from legacy ASes outside the TA, VIP implements the conventional validation process to validate the authenticity of the source address that relies on the mapping between the source address and the corresponding source AS. Figure 3 depicts the validating process at an ABR.

C. Validation Rules Generating and Updating

VIP piggybacks the OIL exchange on BGP routing advertisements to generate validation rules, and relies on BGP update messages for periodically updating OIL-specific information. Thus, VIP gains the benefit that the security of generating and updating the validation rules is bound to BGP routing security. Additionally, extended-MPLS ASes do initially need to register separately their OILs to the TA Registration Center (TRC) in order to bind OIL_i to the original extended-MPLS AS_i; this is needed to provide the basis for authenticating to other peer ASes among the TA network. Through sharing their own Diffie-Hellman public-private key-pairs $<d_i, r_i>$, extended-MPLS AS and TRC can build TCP secure channels that maintain the ability to keep the interaction of the OIL information secret from attackers. With the routing advertisements carrying the OIL-specific information arriving in neighboring extended-MPLS ASes, the ABRs that lie in these ASes can authenticate the received OILs by inquiring TRC by using the secure channel mechanism so that they can further establish the validation rules (Fig. 4.).

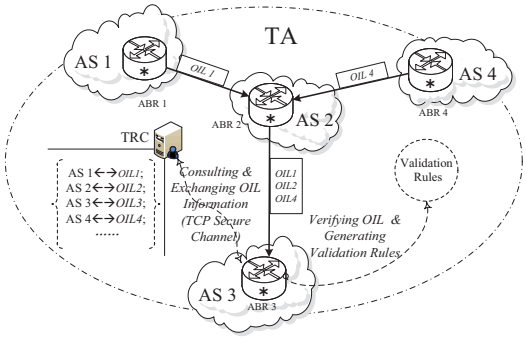

Figure 4. Illustration of generating validation rules.

D. Benefits and Incentives of VIP

Compared with [3, 4], in the context of the analysis below we are in a position to further evaluate the desirable benefits and incentives of the VIP as follow:

- *Overhead*: With the mechanism of label-based forwarding and validating, VIP dramatically improves the transmission efficiency compared to traditional IP header-based mechanisms. And VIP reduces the processing load of both forwarding tables and validation.
- *Scalability*: VIP gains inherently scalable capabilities from the distribution of the OIL within the routing system, and can be bootstrapped without much out-of-band communication or manual configuration. And VIP avoids making major configuration changes to legacy routers and ensures no negative effect on de facto inter-domain routing protocols.
- *Deployment Incentive*: VIP makes all intermediate LSRs do not need to deploy the validation rules and have no validation configurations and operations. Furthermore, VIP constructs the connection-oriented extended-MPLS network to easily enable source-based fair resource allocation. OIL and the Diffie-Hellman value can be carried in an optional and transitive BGP path attribute.
- *Security Concerns*: In VIP, the extended-MPLS offers the same security as traditional MPLS. Meanwhile, the VIP-compliant ABR can cryptographically compute the secret and unique OIL by covering the original AS registration information [6]. Moreover, OIL-specific information is processed and removed from the ABR before packets arrive at end hosts. Thus, VIP ensures the spoof-proof of the OIL-specific information from the end hosts and compromised ABRs on its own. VIP can also periodically update the OILs.

III. EXPERIMENTAL EVALUATION

Based on experimental analysis, we evaluate the advantages of VIP on the optimization of validation costs over the methods presented in [4].

A. Experiment I. The cost evaluation on validation rules generating and updating

SSFNet Simulator was used to implement VIP and evaluate the cost on generating and updating validation rules. For simulation purposes, the maximum number of member ASes is set to a relatively high 40,000 in accordance with the report in [9]. Here, we denote symbolic expression N as the size of TA networks and d as maximum degree of the member AS. Considering the comparative analysis of the Internet AS-level topologies [10], we adopt separately 3 groups AS-level experiment topologies: $\{N=59, d=13\}$,$\{N=113, d=21\}$,$\{N=259, d=26\}$ to evaluate the optimization of cost on generating validation rules on ABR. In addition, we also select different 4 groups topologies: $\{N \in [1, 40{,}000], d=626\}$,$\{N \in [1, 40{,}000], d=1333\}$,$\{N \in [1, 40{,}000], d=2657\}$ to evaluate the optimization of cost on updating validation rules. From the results shown in Fig. 5, we can see that, as the TA scales up, the cost on generating validation rules is increased by $O(N^2)$ in [4], which approaches zero in VIP during the generating process.

As shown in Fig. 6, the cost of updating validation rules is also far less than those in [4], and the increasing function of the cost evolves approximately into linear fit function. The optimization is quite obvious and space complexity is reduced to a feasible level of $O(N)$ from the $O(N^2)$

B. Experiment II. The cost evaluation on packet validating

Supported by the project of the National Basic Research Program of China (973 Program), Tsinghua University develops and implements a trustworthy Internet infrastructure SAVA [8] to figure out the difficult issues of

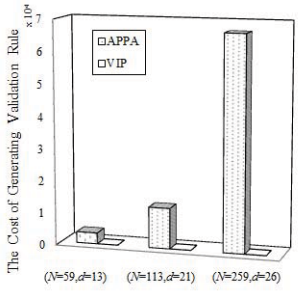

Figure 5. The cost of generating validation rules

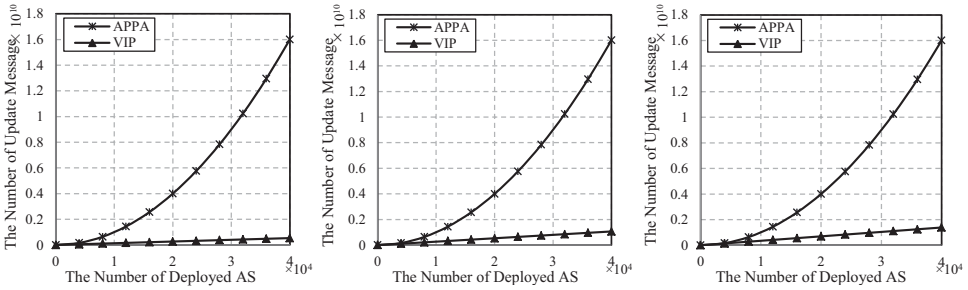

Figure 6. The cost evaluation on validation rules updating.

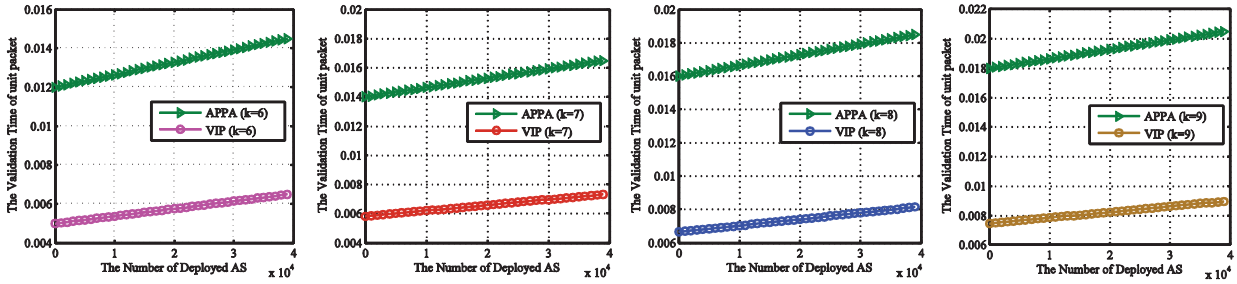

Figure 7. The cost on packet validating in VIP.

authenticating address access. So far, the SAVA prototype system based on authenticated IPv6 source address validation architecture has been deployed and tested on CERNET2, and one document eventually became RFC5210. With the development of this project, many research institutes, ISPs and equipment manufacturers have become involved. These members are all designated with more than 225 globally unique AS Nums, which provided an ideal network environment for our experiments II. Based on traffic data collected from the Aladdin Network Manage System in NOC of CNGI-CERNET2, we constructed the China Next Generation Internet-CERNET2 TA (CNGI-CERNET2 TA), which enables the multi-AS and extended-MPLS network environment. According to the real situation of 25+ member ASes in CNGI-CERNET2 TA, we construct and select 4 different member ASes (Beijing Edge Node, Shanghai Edge Node, Xiamen Edge Node, Hefei Edge Node) to be the experimental data acquisition and analysis nodes to verify our proposed VIP. In experiment, we design and evaluate respectively four cross-domain communication scenarios: {k=6},{k=7},{k=8},{k=9}, considering the hop count (k), the number of hops a given packet passes through along the LSP from source AS to destination AS within the TA. Compared to [4] and other relative methods, we see that VIP can provide an efficient way to reduce packet validation costs and even the minimum rate of reduction can already achieve 57.14%, and average to 57.85% shown in Fig. 7. Experimental results show that VIP is more effective, safe and proves the designed schemes to be feasible.

IV. CONCLUSION

Compared with the method in [4] and other relative solutions, VIP focuses on ensuring the functionality of source address validation based on inter-domain extended-MPLS networks. VIP is adept at flexibly enabling label-driven forwarding and, particularly, validation. VIP finally offers a way to reduce both forwarding tables and validation processing loads. By using the lightweight OIL system and hierarchical end-to-end LSPs based on the extended-MPLS network, VIP offers high-speed forwarding and furthers the functionality of source authentication to the granularity of the origin AS under the precondition of ensuring inter-domain high-speed communications. Our experimental results show that even when implemented on large scale networks, VIP can achieve the effectiveness, simplicity, and optimization of costs on packet validation.

REFERENCES

[1] "Network Infrastructure Security Report", Arbor Networks. 2011.

[2] "CERT Research Annual Report", Carnegie Mellon University's Computer Emergency Response Team, Sep. 23, 2011.

[3] A. Bremler-Barr and H. Levy, "Spoofing prevention method," In Proc IEEE INFOCOM, Washington, 2005,pp.536-547.

[4] Y. Shen, J. Bi, J. Wu and Q. Liu, "A Two-Level Source Address Spoofing Prevention based on Automatic Signature and Verification Mechanism", In: Proc IEEE ISCC, Marrakech, 2008,pp.392-397.

[5] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture," IETF-RFC, RFC3031, January, 2001.

[6] D. Meyer, J. Schmitz, C. Orange, M. Prior, C. Alaettinoglu, "Using RPSL in Practice," IETF-RFC, RFC2650, August 1999.

[7] J. Wu, G. Ren, X. Li, "Source address validation: architecture and protocol design", Proc. of the 15th IEEE ICNP, Beijing, China, 2007.

[8] J. Wu, J. Bi, X. Li, G. Ren etc.,"A Source Address Validation Architecture Testbed and Experiences," IETF-RFC5210, June, 2008.

[9] BGP Routing Table Analysis Reports, http://bgpupdates.potaroo.net/.

[10] Comparative Analysis of the Internet AS-Level Topologies: Master Comparison.http://www.caida.org.