Segment Level Authentication: Combating Internet Source Spoofing

Ming Li*, Matti Siekkinen*, Sasu Tarkoma*, Antti Ylä-Jääski*, Yong Cui†

*Department of Computer Science and Engineering
Helsinki University of Technology
FI-02015, Espoo, Finland
{ming.li, matti.siekkinen, sasu.tarkoma, antti.yla-Jaaski}@tkk.fi

†Department of Computer Science and Technology
Tsinghua University
100084, Beijing, China
cuiyong@mail.tsinghua.edu.cn

Abstract—**This paper presents SLA (Segment Level Authentication), a transport segment level solution designed to prevent both of the intra-domain and inter-domain source spoofing. SLA is based on public key cryptography authentication. It enables intermediate network nodes the ability to validate the packet authenticity by verifying authentication information carried in packets. Although public key cryptography is computationally intensive and induces the traffic overhead, SLA leverages FPGA (Field Programmable Gate Array) based ECC (Elliptic Curve Cryptography) hardware cryptography accelerator to decrease the computation and traffic overhead. SLA provides incremental deployment and offers incentives for both of hosts and ASes. We find that the SLA is feasible for Gigabit links and can effectively mitigate source spoofing in both of intra-domain and inter-domain networks.**

Keywords-source spoofing; authentication; certificate; public key cryptography

I. Introduction

By masquerading as other hosts, attackers hide their true identities and locations, causing the source IP address based filtering less effective and allowing attackers to gain unauthorized access to computers or networks. Reflector DDoS (Distributed Denial-of-Service) attacks [1] and TCP SYN flooding attacks [2] are popular vectors of source spoofing based attacks. Although compromised hosts are increasingly using their real source addresses, recent studies [3] indicate IP spoofing is still a common phenomenon.

In this paper, we propose SLA (Segment Level Authentication), an authentication scheme aiming to mitigate intra-domain and inter-domain source spoofing. SLA uses a two-class public key cryptography system, to authenticate the origin of IP packets by adding necessary authentication information (named SLA tag) in packets and allows en route entities to verify the packets. In order to decrease the computation cost, SLA leverages the hardware cryptography accelerator implemented by FPGA (Field Programmable Gate Array) which can generate and verify digital signatures at Gbps speed.

Our work is motivated by two goals. The first is to provide two-class, i.e., intra-domain and inter-domain, source authentications to the Internet, prioritizing the traffic that can prove its origin. The second goal is to facilitate the deployment by employing a deployable design which does not require major revision of the existing Internet but offers more security benefits and incentives.

The remainder of the paper is organized as follows. In Section 2, we discuss the related work. Section 3 presents the design of SLA. In Section 4, we analyze the deployment issues. Security and performance are analyzed in Section 5 and Section 6 respectively. We conclude the article in Section 7.

II. Related Work

IPSec [4] is a traditional end-to-end or end-to-middle security solution which is also useful to prevent source spoofing. But it cannot solve it on the scale of the whole Internet. First, it requires a globally trusted PKI. Such a PKI cannot be deployed in near future. Next, it does not allow routers to identify a spoofed packet until it arrives at its destination. Thus, spoofed packets are always able to consume the network resources before they are detected.

In SPM [5], each packet leaving its source AS (Autonomous System) network is tagged with a key shared by the source and destination ASes. After arriving at the destination AS, the key is verified and removed. SPM offers good spoofing mitigation, but it does not allow intermediate ASes to assist in filtering spoofed packets. Thus spoofed traffic is still able to reach the target AS.

TCP MD5 Option [6] uses signature to secure the BGP [7] session by protecting the TCP connection between BGP border routers. It can be extended to prevent source spoofing by binding the shared secret keys with host IP addresses. But it can only protect TCP traffic without protection of UDP traffic; and it lacks a reliable and scalable mechanism to distribute the secret keys.

SAVE [8] is a route-based filtering approach, allowing each router to build an incoming table to filter the packets coming from unexpected interfaces. But it is only effective with full deployment and lacks a mechanism to secure the control messages themselves.

PLA [9] enables every network node to verify the authenticity of every IP packet. This approach has the adoptability benefit of enabling every network node to independently authenticate the source of every packet. But it requires a per-host globally trusted PKI (Public Key Infrastructure) which cannot be deployed in near future.

Ingress Filtering [10] runs on border routers of a network to filter packets whose source addresses are out of its address space. If a network deploys it, it cannot prevent other malicious hosts outside of its network from spoofing its addresses.

In Passport [11], each upgraded AS border router stamps MACs (Message Authentication Codes) on outbound packets. The authentication of the packet is bound to a specific AS path. Intermediate ASes forward suspect spoofed packets with best effort in order to avoid false positives. Only the destination AS can discard the spoofed packets. Thus, legitimate traffic still needs to compete for bandwidth with the spoofed traffic.

978-1-4244-7755-5/10/$26.00 ©2010 IEEE

III. SLA DESIGN

A. Overview

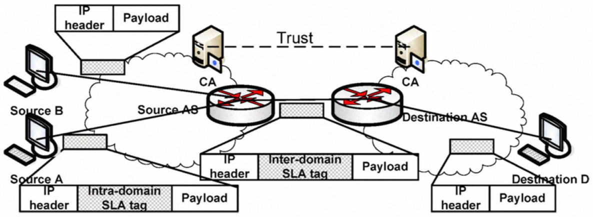


Figure 1. A simplified SLA deployment

The basic idea behind SLA is that when public key cryptography is used, only the owner of the private key can sign over the messages, but every entity having the corresponding public key can verify the messages. SLA ensures the authenticity of a packet by adding a SLA tag in it.

SLA is a complete source spoofing prevention solution providing both of intra-domain and inter-domain packet authentications. Figure 1 shows how SLA works at a high level. The SLA architecture consists of three components: hosts, AS border routers and CAs (Certificate Authorities). Each upgraded host holds a local CA issued certificate to bind its IP address with its public key; and each upgraded AS border router shares its local CA's certificate which binds its AS number with its public key.

Within the administrative boundary of an AS, an intra-domain certificate is used to authenticate the source of a packet to the granularity of its original host. Each upgraded host inserts intra-domain SLA tags into its packets as a proof of their origin. The border router holding each upgraded host's certificate verifies the SLA packets to prevent intra-domain spoofing. An inter-domain certificate is used to authenticate the source of a packet to the granularity of its original AS. Among inter-domain AS networks, each upgraded source AS inserts inter-domain SLA tags into its outbound packets as a proof of their origin. The en route upgraded ASes holding the source AS's certificate verify the packets. If any of the verification fails, the packet will be discarded immediately.

B. Certificates Distribution

After obtaining an IP address, a host may use TLS [12] to communicate with its local CA to obtain an intra-domain certificate binding its current IP address with a public key.

Every AS obtains an inter-domain certificate from a globally trusted CA and leverages BGP update messages to advertise its inter-domain certificate to other ASes. When obtaining the certificates advertised by other ASes, an AS border router sends them to its local CA for verification. The local CA validates a certificate by checking its certificate chain. If a received certificate is invalid, the border router ignores it.

The basic format of a certificate is shown in Figure 2. The mandatory fields include:

- Subject's public key: the public key of a host or an AS.
- IP address: the IP address of an upgraded host.
- ASN: the autonomous system number of an AS.
- Issuer: the IP address of the upper layer CA to allow nodes to contact it for verification.
- Signature algorithm: the cryptography algorithms used in signature calculation.
- Certificate signature: the signature signed by the certificate issuer.

Subject' public key (163 bits)
IP address (128 bits)
AS number (16 bits)
Issuer (128 bits)
Signature algorithm (16 bits)
Certificate signature (326 bits)

Figure 2. Mandatory fields of a certificate

C. Stamping and Verification

SLA uses two types of SLA tags: Intra-domain SLA tag and inter-domain SLA tag. Intra-domain SLA tag ensures the source address of an upgraded host cannot be used by other hosts within the same AS. Inter-domain SLA tag guarantees there is no host in other ASes able to spoof the address space of any upgraded AS.

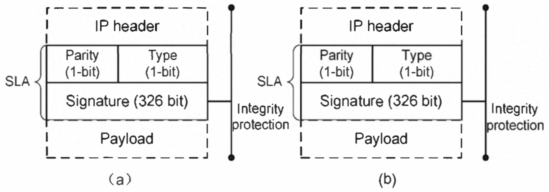


Figure 3. SLA tag formats

SLA tag is located between transport and IP protocols. Figure 3 illustrates two types of SLA tag format: (a) intra-domain SLA tag; and (b) inter-domain SLA tag. They all contain three fields: a public key signature signed by its source host or source AS, a parity bit (explained in subsection D), and a type bit. The public key signature is calculated over the transport header, data payload, and transport pseudo-header (contains the source address, destination address, protocol, and transport segment length). Thus the transport header, IP addresses, and data payload are all under the authentication protection. The type bit is set by the source AS to indicate whether a SLA packet is verified in its source AS. We explain the usage of it in the stamping and verification procedure as follows.

As depicted in Figure 1, for simplification, we assume the source and destination ASes are connected directly and have both upgraded. How to deal with legacy ASes is discussed in section 4. Host A and host B are upgraded and legacy hosts respectively. When host A sends a SLA packet to host D, the basic processing procedure within the source AS is:

1) Host A stamps an intra-domain SLA tag in the packet.
2) When the packet leaves its source AS, the border router looks up its intra-domain certificate indicated by its source address and uses the matched certificate to verify the SLA tag. If the verification succeeds, it replaces the intra-domain SLA tag with an inter-domain SLA tag and forwards it to the destination AS.

When host B sends a legacy packet to host D, the basic processing procedure within the source AS is:

1) After receiving the packet, the source AS border router checks whether the source address belongs to its

978-1-4244-7755-5/10/$26.00 ©2010 IEEE

address space. If not, the border router discards the packet. This design is borrowed from the Ingress Filtering [10].

2) The border router checks whether the packet should carry an intra-domain SLA tag. If the host has upgraded, legacy packets carrying that source address will be discarded.
3) The source border router stamps an inter-domain SLA tag in the packet and forwards it to the destination AS.

When the two packets arrive at the destination AS, the border router looks up their corresponding inter-domain certificates indicated by their source addresses and verifies the SLA tags using the matched certificates. If the verification fails, it discards the packets. Otherwise, it strips off the SLA tags and forwards the packets to host D.

D. Re-certificates

An intra-domain certificate may be valid on the order of minutes or hours depending on the address allocation and security policy. Before the certificate expires, a host should apply for a new certificate from the local CA using its previous certified certificate. After renewing a certificate, the local CA informs the border routers in the local AS about the updated certificate. After the old certificate expires, the border routers use the corresponding new certificate to verify the SLA packets sent from the host.

To improve security, inter-domain certificates should be updated periodically, e.g., on the order of a few weeks or months. To advertise the renewed certificate, an AS sends BGP update messages piggybacking the new certificate. The routing advertisement will arrive at other ASes asynchronously. If we assume BGP takes one hour to converge (We use the same assumption as Passport [11] does), from the start of the re-certificate process, verifying ASes should still use the old for a few extra hours to guarantee every other AS has received the new certificate.

Each AS maintains two certificates for each of other ASes. To identify the old and new certificates, SLA uses the parity bit. When an AS generates the signature part of the SLA tag, it uses the parity bit field of the SLA tag to indicate the parity of its current certificate. A verifying AS will use the newest obtained certificate as the current verifying certificate for that AS when it receives its packets carrying SLA tags whose parity bit is different from the recorded one.

E. Prioritization of the Verified Traffic

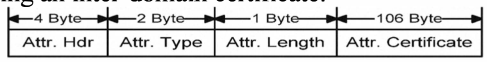
SLA employs the type bit in SLA tags to distinguish the two types of inter-domain SLA packets: 1) verified packets originally sent by upgraded hosts that can prove their origin in their source ASes, e.g., the packet sent from A to D in Figure 1; 2) unverified packets originally sent by legacy hosts that cannot prove their origin in their source ASes, e.g., the packet sent from B to D in Figure 1. SLA grants different forwarding priority to the verified and unverified packets as well as legacy packets. A verifying AS recognizes the traffic by checking the type bit in the SLA tag. An inter-domain SLA packet with the type bit set is a verified packet; an inter-domain SLA packet with the type bit unset is an unverified packet; a packet without SLA tag is a legacy packet.

How to prioritize different types of traffic is up to the AS to define its queue policy. One possible option is that a verifying AS uses three weighted queues, allocating limited bandwidth to unverified and legacy traffic.

IV. Deployment

A. Inter-operation with Legacy Entities

Upgraded ASes use the optional and transitive path attributes of BGP to piggyback the inter-domain certificates to distribute them among ASes. Legacy ASes do not process the optional and transitive path attributes but just include them in the routing advertisements and propagate them to their neighbor ASes. Figure 4 shows a BGP update message piggybacking an inter-domain certificate.



4 Byte	2 Byte	1 Byte	106 Byte
Attr. Hdr	Attr. Type	Attr. Length	Attr. Certificate

Figure 4. Certificates paggybacked in a BGP AS path attribute

B. Middle Deployment Mode of Inter-domain SLA Tag

Inter-domain SLA is deployed in the middle of the network. When both a source AS and a destination AS have upgraded, the border router at the source AS stamps an inter-domain SLA tag in a packet and the border router at the destination AS strips off the SLA tag. If the destination AS has not deployed SLA, an upgraded source AS can still use inter-domain SLA tags as long as there are other en route upgraded ASes which can still verify the SLA packets. An AS border router can obtain the AS path information from BGP to construct a network topology of the network. Each upgraded AS is able to recognize other upgraded ASes according to whether they hold inter-domain certificates or not. Thus, each AS knows the upgraded ASes on the path toward the destination in advance. In this case, the last upgraded AS on the path strips off the SLA tag.

C. Incentive and Incremental Deployment of SLA

SLA offers benefit to early adopters. First of all, as long as an AS upgrades, its address space cannot be spoofed by other ASes. Some ASes whose address space is often forged by other networks would like to deploy SLA to protect itself from false accusation. Secondly, a packet can get higher forwarding treatment if it can prove its origin to a finer granularity.

SLA also supports incremental deployment, requiring no full deployment overnight. In the early phase of deployment, Inter-domain SLA may be adopted by a few mutual trusted ASes for coarse grained traffic authentication, access control or firewall applications. These ASes can also incrementally deploy intra-domain SLA to protect their end-hosts from source spoofing within the same AS.

V. Security

The heart of SLA is the public key cryptography using a NIST recommended 163-bit ECC (Elliptic Curve Cryptography) [13] public key cryptography on Koblitz Curves. It is computationally infeasible to break it within a short time with low cost.

The inter-domain certificates are distributed across ASes. Each AS will verify their received certificates by inquiring its local CA. Even if an attacker can successfully hijack a certificate announcement and replace the certificate, the receiving AS will detect and ignore it.

In an upgraded AS network, if a host is compromised, it cannot spoof the addresses of upgraded hosts within the same AS but can only spoof the addresses of no upgraded hosts which is an incentive for end-hosts to deploy SLA to prevent its address from spoofing.

If a border router of an upgraded AS is compromised, the worst source spoofing damage it can cause is stamping every outbound packet with an inter-domain SLA tag with the type bit set. But the attackers are limited to spoof addresses of their own AS network. Fighting against compromised hosts using valid SLA tags is out of the scope in this paper.

VI. Performance Analysis

A. *SLA Tag Computation Overhead*

The public key cryptography processing overhead is high. While software implementations cannot meet the performance requirements, hardware cryptography accelerator is a promising solution. FPGA is an attractive alternative for implementing cryptography algorithms because of its performance and flexibility. We refer to the performance of FPGA based hardware cryptography accelerator to demonstrate its feasibility to be used in SLA.

To decrease the computation and traffic overhead, SLA uses ECC on NIST K-163 Koblitz curve for signature generation and verification because of its relatively small key and signature size. An optimized simulation using parallel processing for performing ECC public key operations has been made based on an Altera Stratix Π 180C3 FPGA board [14]. When optimized for throughput, it achieves 645,160 signature generations per second with a latency of 16.36 us per generation and 283,092 signature verifications per second with a latency of 24.28 us per verification. If we assume the average size of an IP packet is about 6000 bits [15], then the accelerator could generate and verify SLA traffic with the speed of about 3.87 Gbps and 1.7 Gbps respectively, which is efficient enough for edge routers. And we believe legacy traffic will occupy most of the traffic in the backbone network. 1.7 Gbps may be able to handle the NPLA traffic.

B. *Memory and Traffic Overhead*

SLA maintains per-AS inter-domain certificate information. According to [16], there are less than 32K ASes. A complete inter-domain certificate occupies 98 bytes extra memory. Thus, the memory overhead of two inter-domain certificates per-AS is about 6.3MB for each AS border router. In addition, a source AS border router needs to maintain the intra-domain certificates. The local CA maintains all the necessary information and border routers only store the certificate information of only online hosts. In this paper, we assume an individual AS has no more than 320K online hosts. Based on this assumption, the memory overhead is around 63MB for a source AS border router. Thus, the maximum memory overhead for an AS border router is about 70MB, which is not a big cost for the modern routers.

As shown in Figure 3, a SLA tag has a 41-byte fixed traffic overhead. We assume the average size of an IP packet is 6000 bits (750 bytes) [15]. SLA headers add about 5.5% bandwidth overhead to legacy IP traffic. Such overhead is not critical for the rapid growth of the available bandwidth of the Internet.

VII. Conclusion

In this paper, we treat each AS as a trust and fate-sharing unit which prevents the intra-domain source spoofing action as a local security issue and inter-domain source spoofing action as a global security issue. We propose SLA to provide a two-class authentication scheme to solve the source spoofing on the Internet. By granting high forwarding priority to the traffic that can prove its origin, SLA provides incentives to be deployed. In addition to the security related benefits and incentives, performance considerations of public key operations are crucial in convincing ISPs to adopt and deploy SLA. Our analysis of employing hardware cryptographic accelerator in SLA indicates that it is feasible to process the SLA traffic generation and verification at gigabit speed.

Acknowledgment

This work was supported in part by the Academy of Finland (no. 135230), NordicHIP project funded by Nordunet3 programme, and NSFC (no. 60911130511, 60873252).

References

[1] D. Piscitellod. Anatomy of a DNS DDoS amplification attack. http://www.watchguard.com/infocenter/editorial/41649.asp, 2006

[2] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage. Inferring internet Denial-of-Service activity. ACM Transactions on Computer Systems, vol. 24, no. 2, May 2006.

[3] T. Ehrenkranz and J. Li. 2009. On the state of IP spoofing defense. ACM Transactions on Internet Technology, Vol. 9, No.2, Article 6, May.

[4] S. Kent and K. Seo. Security architecture for the Internet Protocol. RFC 4301, The Internet Engineering Task Force, December 2005.

[5] A. Bremler-Barr and H. Levy. Spoofing prevention method. In Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (InfoCom), 2005.

[6] A. Heffernan, Protection of BGP Sessions Via the TCP Md5 Signature Option. RFC 2385, The Internet Engineering Task Force, 1998.

[7] Y. Rekhter, T. Li, and S. Hares. A Border Gateway Protocol 4 (BGP-4). RFC 4271, 2006.

[8] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang. SAVE: Source Address Validity Enforcement. In IEEE INFOCOM, 2002.

[9] C. Candolin, J. Lundberg, and H. Kari. Packet level authentication in military networks. In Proc. 6th Australian Information Warfare & IT Security Conf., Geelong, Australia, Nov. 2005.

[10] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing. RFC 2827, May 2000.

[11] X. Liu, X. Yang, D. Wetherall, and A. Li. Passport: Secure and Adoptable Source Authentication. In Proceedings of the 5th USENIX NSDI, April 2008.

[12] P. Eronen. The Transport Layer Security (TLS) protocol Version 1.2. RFC 5246, The Internet Engineering Task Force, August 2008.

[13] A. Menezes, Elliptic Curve Cryptosystems. CryptoBytes, Vol.1 No.2, Summer 1995.

[14] K. U. Järvinen and J. O. Skyttä. High-Speed Elliptic Curve Cryptography Accelerator for Koblitz Curves. In Proceedings of the 16th IEEE Symposium on Fieldprogrammable Custom Computing Machines, FCCM 2008.

[15] W. John and S. Tafvelin. Analysis of internet backbone traffic and header anomalies observed. In Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, New York, USA, 2007

[16] RouteViewsProject. http://www.routeviews.org/ [Accessed 12th Dec 2009].