Inter-Domain Routing Validator Based Spoofing Defence System

Lei Wang, Tianbing Xia, Jennifer Seberry
School of Computer Science and Software Engineering
University of Wollongong
Wollongong, NSW, Australia
Email: lw941, txia, jennie@uow.edu.au

***Abstract*—IP spoofing remains a problem today in the Internet. In this paper, a new system called Inter-Domain Routing Validator Based Spoofing Defence System (SDS) for filtering spoofed IP packets is proposed . SDS uses efficient symmetric key message authentication code (UMAC) as its tag to verify that a source IP address is valid. Different ASes border routers obtain a shared key via the Inter-Domain Routing Validator (IRV) servers which will manage the secret keys and exchange keys among different ASes via security communication channel. SDS is efficient, secure and easy to cooperate with other defence mechanisms.**

I. Introduction

Internet Protocol (IP) [1] is the foundation of the Internet. Packets sent using the IP protocol include the IP address of the sending host. The recipient who replies to the sender using this address is not verified by the protocol. The IP protocol specifies no method for validating the authenticity of the packet's source. This implies that the attacker can forge the source address. This is a well-known problem and has been well described in [2]. Sending IP packets with forged source address is known as IP Spoofing and could be used by attackers for several purposes. IP spoofing remains a popular method to launch Distributed Denial of Service (DDoS) attacks [3] which cost millions of dollars to online companies. Unfortunately, this attack is difficult to stop because hackers are able to hide their IP address by IP Spoofing, so it is often impossible to identify their location. On the other hand, an attacker can access a sensitive computer or a network by making it appear that a malicious message has come from a trusted machine by spoofing the IP address of that machine.

Many solutions have been proposed to detect IP spoofing. Most of them are based on filtering packets, based on the IP source address and the incoming interface [4]. In this paper, we present an alternative solution to the Inter-domain Routing Validator (IRV) [5] based spoofing defence system (SDS) which is a router based packet marking solution. Unfortunately, like any other router based solutions, the efficiency of the system depends on the number of participating routers. It is impossible that every router on the Internet participate in the system and different Internet Service Providers (ISPs) deploy the same method. Thus, the collaboration with different systems is considered in our system. IRV is a new protocol which acts as a companion to Border Gateway Protocol 4 (BGP) [6] and solves some BGP security issues, see more details in [5].

The idea of SDS comes from packet marking system, such as SPM, passport. Packet marking seems to be the most efficient method to solve IP spoofing problem. Most of these systems depend on BGP message e.g. BGP UPDATE message, unfortunately, this is insecure. SDS based on secure BGP (IRV-BGP) which is more secure than others.

The structure of this paper is as follows: In section II we present a detailed description of the architecture of SDS and it's benefits. We conclude our work and present a future plan in section III.

II. The Spoofing Defence System

The purpose of our system is to provide an authentic source identifier which can be used by the network to identify the spoofing packet. To enable the Spoofing Defence System (SDS) some participating Autonomous Systems (ASes) are required to mark the outgoing packets with keyed Message Authentication Code, and verify the authenticity of the MAC on incoming packets.

A. Overview

Our proposed system is essentially a packet marking system. In the SDS architecture a MAC is added to each packet, to validate that the packet is not spoofed. *Figure 1* shows how SDS works at a high level. When a packet leaves its source AS, the border router (R) of AS stamps one MAC for next AS on the path into its header. Each MAC is computed using a secret key shared between each AS on the path. E.g. AS1 and AS2, AS2 and AS3...

When the packet enters the next AS on the path, the border router verifies the MAC value using the secret key shared with the previous AS. A correct MAC can only be produced by the current AS which shared the secret key with the previous AS. If the MAC verifies, it is sufficient to show that the packet comes from the source AS indicated by its source address, and the border router will generate a new MAC to overwrite the valid one. The new secret key is shared between current AS and next AS. Otherwise, it is a spoofed packet. The packet with an invalid MAC is discarded at the current AS. We chose to discard spoofed packets because that spoofed packets will not further consume network resources, such as bandwidth. This is an important feature of SDS, especially under DDoS attack.

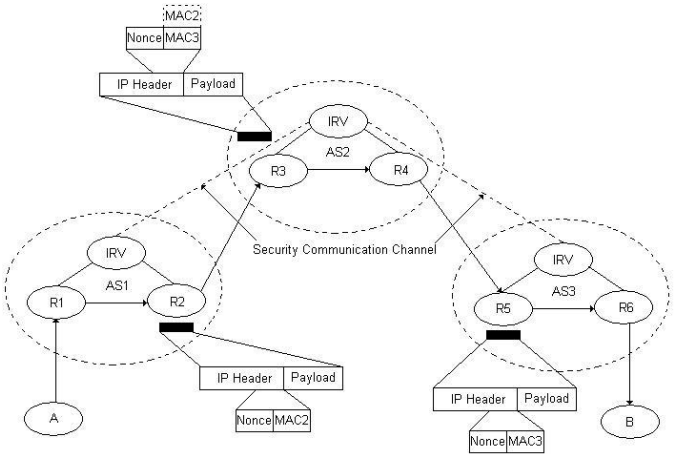

Fig. 1. A high level overview of spoofing defence system

Thus, the spoofed packet will never reach the destination. The MAC generation process only happens at the initial time, once a communication is established between source and destination then there is no requirement to generate a new MAC and share a new secret key between ASes on the path. The MAC is added into the packet by current border router, the next router just compares the MAC value with the previous packet. The time required to verify each packet and share the secret key is saved.

The stamping and verification processes could also be written as following steps:

Step 1: Border router of ASi computes MAC *(src, dst, len, IP ID, ASi num, ASi+1 num, payload[0,7])* using the secret key shared between ASi and ASi+1. It then stamps MAC into IP opinion field as part of IP header in the packet which will be sent to the ASi+1. **Note:** The MAC is computed only once (The MAC value never change in the same path), the following packets are added to the same MAC in the IP opinion field till communication finish.

Step 2: Border router of ASi+1 verifies the MAC in the IP opinion field of the packet received from ASi.

-if the MAC value is correct, ASi+1 repeats **step 1**. The border router will replace the MAC in the IP opinion field. Then the new packet will be send to the next AS on the path. **Note:** The first time verification needs to recompute the MAC value. After that, the MAC value is only compared with the first packet MAC value from the ASi till communication is finished.

-else discard the packet: the source address must have been spoofed.

B. Deployment and Implementation

The role of the keyed Message Authentication Code (MAC) is to verify that the source address of a packet is not spoofed. The IP layer is the largest common protocol of the Internet, all Internet protocols run over it. Thus, adding the MAC to the IP header allows SDS to capture any spoofing attack over any Internet protocol, such as TCP, UDP or other protocols.

For the ease of deployment and implementation of SDS, the MAC can be placed in the IP option field in the IP header. Most of router-based systems use ID field in the IP header. This obviously may lead to problems to cooperate with other IP spoofing defence techniques like SPM [7] and StackPi [8]. Another disadvantage in using the IP ID field is that the IP ID field length is only 16-bit, which is insecure under off-line cryptanalysis attack. Thus, we use IP option field and MAC in SDS to avoid these problems.

1) The Message Authentication Code(MAC): Obviously, SDS can be implemented via digital signatures. A source signs its packets, and routers validate the digital signatures with the source's public key. We discard this approach as digital signatures are computationally expensive to generate and verify. Instead, SDS uses an efficient symmetric key MAC (UMAC) [9] as its signature. Our design uses UMAC because of its high speed. UMAC takes a nonce as its input, so we generate a random number into the 32-bit nonce field and use it together with the 16-bit IP Identification to generate a 48-bit nonce for UMAC computation. A border router of an AS stamps a MAC for the next AS on the path to the destination. Each MAC is computed using the key which is 128-bit, shares with the next AS on the path. These secret keys are exchanged between ASes as described in subsection *The Key*. The MAC computed for the next AS covers the source address, the destination address, the IP ID, the packet length field of the IP header, current and next AS number and the first 8 bytes of packet payload. In *Figure 1*, when a packet from host A to host B leaves AS1 to AS2, the border router R2 of AS1 computes MAC2 *(src, dst, len, IP ID, AS1 num, AS2 num, payload[0,7])*. *Figure 2* shows a possible SDS header format used in our implementation. Our design uses a 64-bit MAC for each AS hop. A border router stamps/replaces a SDS header for a packet with a valid source address, and discards the spoofed packet otherwise.

Fig. 2. Possible header format of spoofing defence system in IPv4 [1]

2) The key: Exchanging key information between routers is required in our system. It is important in our system to make sure that the key exchange is secure. Some IP spoofing defence systems exchange secret keys on BGP, such as Passport [10], this is obviously insecure due to various BGP security issues such as prefix hijacking.

BGP has three major weaknesses [11]. The first weakness is there is no mechanism to check the integrity, freshness and source authenticity of BGP message. Second, BGP doesn't

offer any mechanism to verify the authenticity of an address prefix and an AS origination of this prefix in the routing system. Last, the BGP protocol doesn't provide any way to guarantee that the attributes of a BGP UPDATE message are correct. The lack of security concepts in BGP leaves it vulnerable to several types of control plane attacks [12]. There are several suggestions to secure BGP by adding certificate keys to BGP announcements to validate them. In secure BGP, there are two basic methods of keys distribution been suggested and under consideration of the Internet Engineering Task Force (IETF). The first one is the central method where the organization of IP registries (ARIN, APNIC, RIPE) are in charge of distributing the keys. The second one is the IRV (Inter-domain Routing Validator) method that uses distributed server (IRV) in each AS to manage the key distribution. We use the second method the same as is to be used in SPM [7] to distribute and manage the secret key. Note, the keys distributed here are not the keys we used in SDS. Those distributed keys are used for BGP authentication and verification, see more details in [5].

We use one central server in each AS to manage the secret key. IRV is a new architecture used to solve security issues in BGP. That is, the IRV is used to validate BGP data and acquire additional routing information relevant to an AS. IPSec or TLS can be used to ensure the integrity and authenticity. We assume that the security communication channel has already been established before key exchange. In SDS, the IRV selects and exchanges the secret key for different ASes border routers, e.g. *Figure 1* shows how the IRV exchanges the secret key via IPSec for different ASes. We believe the IRV provides better security in partial deployments, which is important for the success of SDS. Consider the implementation of IRV, it must be simple, robust, and built on widely deployed technology. Obviously, HTTP easily fulfills these requirements, our system implements IRV as a web-based service. Many well known security solutions provide security to web-based services such as SSL/TLS and IPSec. Hence, ASes are free to implement IRV security as is appropriate for their environment.

3) Benefit of SDS: We use an efficient symmetric key MAC (UMAC) [9] in SDS. The UMAC with 128-bit keys is computationally infeasible to break. In spoofing attack, the attacker might try to guess a valid SDS header by sending packets. Because a SDS header has 64-bit MAC value, the attacker have to send at lease 2^{63} packets to guess the correct one. The time that the attacker takes exceeds the period of UMAC renew. It is obviously easy to cooperate with other defence mechanisms such as SPM [7], because we use the IP option field when most of them are using the IP ID field. Key distributing is needed in IRV-BGP as we mentioned in the previous section. The IRV system is a *independent* system, i.e. it is possible to configure the routing system to prevent malicious hosts from injecting routing packets. For instance, two adjacent routers authorize each other before they set up communication. When this kind of communication is established, routers can then forward and process routing packets with the highest priority. Normal data traffic cannot congest the routing channel.

For better security, domains need to periodically change the secret keys. This requires periodic update of new secret key pairs, which can happen at a large time scale. SDS conjunction with BGP UPDATE message to renew its secret key pairs. Rapid rekeying prevents an attacker form replaying a SDS packet.

III. Conclusion and future work

In this paper, we proposed a new approach to the IP spoofing defence called Inter-Domain Routing Validator Based Spoofing Defence System (SDS). The approach effectively filters the spoofing packet. SDS is efficient, secure and easy to cooperate with other defence mechanism. SDS uses efficient symmetric key message authentication code (UMAC) as its *digital signature* to verify that IP packet has not been spoofed. Different ASes border routers obtain shared keys via IRV servers which will manage the secret keys and exchange keys between different ASes via security communication channel such as using IPSec to establish the security communication channel between IRV servers. SDS is deployable because the computational cost for SDS header generation, validation and key exchange is affordable.

Several issues of SDS were not discussed in this paper. They will be investigated and reported in the near future. In the future, we are planning to prove the deployment performance of SDS using simulation studies. It would be interesting to examine that real cooperate performance with other defence mechanisms such as Ingress/engress filter, SPM in the network.

References

[1] J. Postel, "Internet Protocol," *DARPA INTERNET PROGRAM, RFC0791*, 1981.

[2] S. M. Bellovin, "A Look Back at 'Security Problems in the TCP/IP Protocol Suite'," *20th Annual Computer Security Applications Conference (ACSAC)*, 2004.

[3] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed Denial of Service Attacks," *In IEEE International Conference on Systems, Man, and Cybernetics*, pp. 2275–2280, 2000.

[4] T. Ehrenkranz and J. Li, "On the State of IP Spoofing Defense," *ACM Transactions on Internet Technology*, vol. 9, no. 2, 2009.

[5] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin, "Working Around BGP: An Incremental Approch to Improving Security and Accuracy of Interdomain Routing," *in Proceedings of Network and Distributed System Security Symposium, San Diego, CA*, 2003.

[6] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," *The Internet Society, RFC4271*, 2006.

[7] A. Bremler-Barr and H. Levy, "Spoofing Prevention Method," *in Proceedings - IEEE INFOCOM*, pp. 536–547, 2005.

[8] A. Yaar, A. Perring, and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP Spoofing defense," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 1853–1863, 2006.

[9] T. Krovetz, "UMAC: Message Authentication Code using Universal Hashing," *The Internet Society, RFC4418*, 2006.

[10] X. Liu, A. Li, X. Yang, and D. Wetherall, "Passport: Secure and adoptable source authentication," *in Proceedings of USENIX Symposium on Networked Systems Design and Implementation*, 2008.

[11] S. Murphy, "BGP Security Vulnerabilities Analysis," *The Internet Society, RFC4272*, 2006.

[12] J. Israr, M. Guennoun, and H. T. Mouftah, "Mitigating IP Spoofing by Validating BGP Routes Updates," *IJCSNS International Journal of Computer Science and Network Security*, pp. 71–76, 2009.