Chain-of-Trust Packet Marking

Otávio A. S. Carpinteiro, Phyllipe L. Francisco, Pablo M. Oliveira, Edmilson M. Moreira

Research Group on Systems and Computer Engineering
Federal University of Itajubá, 37500–903, Itajubá, MG, Brazil
Emails: {otavio,phyllipe,pablo,edmarmo}@unifei.edu.br

***Abstract*—This paper proposes a new deterministic traceback method — chain-of-trust packet marking (CTPM). CTPM establishes a chain of trust composed of the border routers of the autonomous systems (ASes). It makes use of a new IPv6 extension header — the traceback extension header (TEH) — which extends the datagram size in 168 bytes at most. The TEH contains encrypted marks which trace the path taken by each IPv6 datagram from its origin to the destination. The computational load on the border routers, as well as the network latency generated by CTPM will be measured and evaluated in future studies.**

***Keywords*-packet marking; IPv6 traceback; IPv6 extension header; network security.packet marking; IPv6 traceback; IPv6 extension header; network security.**

I. Introduction

One of the serious security shortfalls of the Internet today is failure to correctly identify the point of origin and the path taken by packets. The IPv6 source address of the packet can be easily forged by miscreants. The technique of forging source addresses is known as IP spoofing. The methods for fighting IP spoofing can be divided into two large areas — prevention and traceback [1].

Prevention methods seek to filter spoofed packets before they reach their destination and therefore seek to prevent the attack or minimize its effects. The methods proposed by Lee et al. [2], Liu et al. [3], and Shue et al. [1] are amongst the prevention methods.

Prevention methods have three serious disadvantages. Firstly, they may not recognize legitimate packets, and may therefore discard them [1]. Secondly, they require cooperation between different autonomous systems (ASes) on the Internet, requiring information exchange between them, and consequently requiring them to incur extra costs with storage and bandwidth resources. Thirdly, in filtering spoofed packets, they prevent not only the detection of the real perpetrator of the attack but also the obtainment of means of proving that he/she actually committed the attack. Thus, perpetrators continue to launch successive attacks on the Internet, unduly consuming its resources without being identified, held responsible and potentially penalized.

Traceback methods seek to identify the source of spoofed packets and therefore seek to identify the origin (or origins) of the attack. The best-known methods are probabilistic packet marking (PPM) and deterministic packet marking (DPM). The methods proposed by Savage et al. [4], and Goodrich [5] are amongst the PPM methods. The methods proposed by Belenky and Ansari [6], Xiang et al. [7], and Sun et al. [8] are amongst the DPM methods.

PPM methods proposed in the literature have some disadvantages. Firstly, they require large amounts of packets for correct reconstruction of the path between the origin and the destination of traffic. Secondly, they require the destination (or victim) to have significant computational resources in order to correctly identify the path taken by the packets. Thirdly, they fail to define protocols for the reliable exchange of keys between routers when making use of encryption or of hash functions. Finally, PPM methods cannot trace emails with spam content or distributed denial of service (DDoS) attacks.

DPM methods proposed in the literature also have some disadvantages. Firstly, they require the recipient (or victim) to know IP addresses of interfaces of border routers of the ASes to identify the source of the packets. Secondly, they require the recipient (or victim) to know which ASes deploy DPM and which do not. Thirdly, they do not specify any policy for the Internet service providers (ISPs) to deploy DPM either gradually or not. Finally, DPM methods do not propose any mark authentication scheme in order to guarantee the validity of the marks.

This paper proposes a new deterministic traceback method — chain-of-trust packet marking (CTPM). CTPM establishes a chain of trust composed of the border routers of the autonomous systems (ASes). It makes use of a new IPv6 extension header — the traceback extension header (TEH).

The paper is divided into six sections. Sections II and III describes the TEH and CTPM, respectively. Section IV details the future implementations through which CTPM will be evaluated. Section V presents the benefits of CTPM and Section VI concludes the paper.

II. Description of TEH

CTPM modifies neither the IPv6 header nor any of the existing IPv6 extension headers. CTPM just adds the new TEH to the IPv6 datagram. If the hop-by-hop options extension header is present in the datagram, the TEH must immediately follow it. Otherwise, the TEH must immediately follow the IPv6 header.

The creation of the new TEH header is necessary as none of the six existing IPv6 extension headers are currently processed exclusively by the border routers. The TEH is composed of the

 ISBN: 978-1-61208-450-3

two usual fields of any IPv6 extension header — next header (NH) and header length (HL) — [9], a padding field and the chain-of-trust mark (CTM). It is presented in Figure 1a.

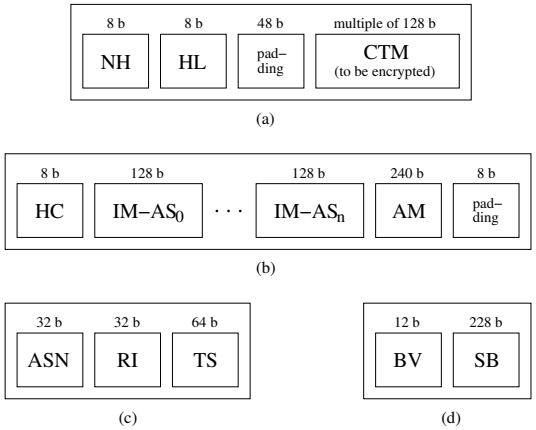

Figure 1. (a) traceback extension header (TEH); (b) chain-of-trust mark (CTM); (c) identification mark (IM); (d) autentication mark (AM) — b: bit(s)

CTM is composed of the hop count (HC) field, one or more identification marks (IM), an authentication mark (AM), and a padding field. It is presented in Figure 1b.

The HC indicates how many ASes the packet has passed through, and consequently, indicates how many IMs exist in the TEH. The IM is composed of three fields — autonomous system number (ASN), router interface (RI), and timestamp (TS). It is presented in Figure 1c.

The purpose of the ASN field is to globally identify an AS [10] through which the packet has passed. The RI field indicates the interface of the router through which the packet entered the AS. The 32 bits of the field can be used in the most convenient way for each AS. The TS field indicates the date on which the packet entered the AS. The date is represented in terms of Unix/Posix time.

The AM is composed of two fields — bit values (BV) and selected bits (SB). It is presented in Figure 1d. The purpose of the BV field is to store the value of 12 bits, selected randomly, of the datagram. The SB field identifies the position, in the datagram, of each selected bit.

Mark spoofing reduces the effectiveness of packet marking. Therefore, the use of encryption is necessary [2]. The operations community resists the use of any type of encryption on the Internet, mainly because of the costs involved [11]. However, the cost of encryption in this proposal can be largely offset by the cutting of costs with network appliances, caused by the reduction of garbage that currently circulates on the Internet.

The CTM size is always a multiple value of 128 bits. It is encrypted by the advanced encryption standard (AES) algorithm using a 128-bit key. In the vast majority of cases, the AS path does not exceed 8 hops [12]. Thus, the TEH can usually reach the maximum size of 168 (1 + 1 + 6 + 32 + 8 * 16) bytes. This size represents 13% of 1280 bytes — maximum transmission unit (MTU) garanteed by the network infrastructure [13]. Therefore, upon its creation, the IPv6 datagram must have a maximum size of 1112 bytes in order to circulate on the Internet without path MTU discovery [14].

III. Description of the CTPM method

In CTPM, marks are created and manipulated by border routers of the ASes which the packet traverses. They are stored in the TEH. Thus, each AS which a packet traverses can identify the path taken by the packet to reach it.

The AES key is shared only between the interface of the border router of an AS with its respective peer interface of the border router of the neighbouring AS. The keys could be established and exchanged by the two border routers through border gateway protocol (BGP) update messages. However, for safety reasons and to keep CTPM independent from BGP, CTPM will use Diffie-Hellman key exchange to establish and exchange AES keys. It will also use certificates of a public-key infrastructure (PKI), such as PKIX [15], to validate public keys. The AES keys must be changed periodically (every 60 days, for example).

Figure 2 illustrates the CTPM method by means of an example. In the example, there are 3 ASes — AS_0, AS_1 and AS_2 — each with two border routers. A packet is sent from the source computer to the destination (or victim) computer.

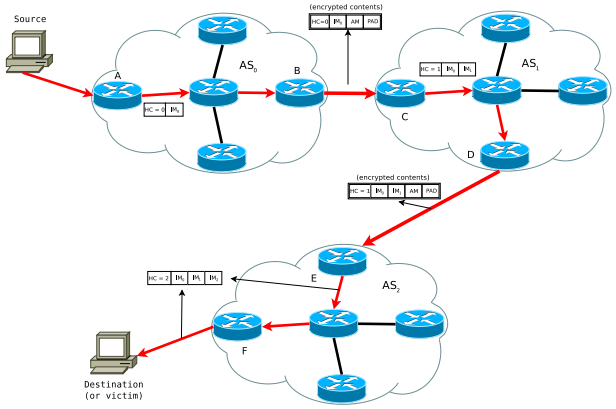

Figure 2. The chain-of-trust packet marking (CTPM) method

Upon receiving the packet sent by the source computer (administered by AS_0), border router A creates the TEH with HC value equal to 0 and with an IM of AS_0. The packet travels inside AS_0. Finally, upon receiving the packet, border router B adds the AM and padding fields to CTM. The CTM is then encrypted and TEH is rebuilt.

Upon receiving the packet sent by border router B, border router C decrypts the CTM and checks the AM, HC, and ASN fields. If the values of the three fields are valid, the packet processing continues. The AM and padding fields are then removed, the HC value is incremented, the IM of AS_1 is added to CTM, and TEH is rebuilt. The packet travels within AS_1. Finally, upon receiving the packet, border router D adds the AM and padding fields to CTM. The CTM is then encrypted and TEH is rebuilt.

 ISBN: 978-1-61208-450-3

Upon receiving the packet sent by border router D, border router E decrypts the CTM and checks the AM, HC, and ASN fields. If the values of the three fields are valid, the packet processing continues. The AM and padding fields are then removed, the HC value is incremented, the IM of AS_2 is added to CTM, and TEH is rebuilt. The packet travels within AS_2. Finally, upon receiving the packet, border router F removes the TEH from the packet, and sends the latter to the destination (or victim) computer. If required, border router F may save the packet header and TEH for offline analysis.

It is important to emphasize the fact that border router B trusts router A as they are both administered by AS_0. In turn, border router C trusts router B as both AS_0 and AS_1 know through which interfaces B and C are connected. They also know the AES key that they use to encrypt and decrypt the CTM fields of the TEH of the packets. In addition, both ASes exchange the AES key in a reliable manner via a PKI certificate. Successively, border router D trusts router C, router E trusts router D, and router F trusts router E. Thus, the CTPM method builds and makes use of a chain of trust in which its chain rings are border routers.

As may be seen from Figure 2, the gateway of the source computer is administered by AS_0. So, AS_0 is responsible for the traffic of the computer and it is up to AS_0 to take measures to avoid propagating malicious traffic coming from the computer. CTPM is intended to be incrementally deployed from the major carriers down to the ASes. Disincentives can also be applied, after deployment deadlines, by deployers for non-deployers as a mechanism to drive deployment.

IV. Future performance evaluation

Two CTPM implementations will be developed. The first will implement a Linux kernel module to extend the TCP/IPv6 stack. In the second, the CTM field will be encrypted and decrypted in field-programmable gate array (FPGA) hardware. The extra computational load on the border routers and extra network latency generated by CTPM will be measured and evaluated. These evaluations aim to verify the computational feasibility of CTPM and to give the ASes an idea of the extra investment required in network appliances if the CTPM method is adopted on the Internet.

V. Benefits of CTPM

The adoption of the CTPM produces several benefits for Internet security. The main benefit is the possibility of knowing the precise origin of each packet that circulates on the Internet. The sources of spam emails, which produce more than 70% of the global traffic of messages [16], can thus be identified and eliminated. Moreover, sources of attacks and malware can also be identified and fought.

Another benefit arises from the possibility of knowing the precise path, from origin to destination, of each packet that circulates on the Internet. CTPM can thus assist in both the correction of misconfigurations of BGP in order to ensure that each AS control- and data-plane paths match [17], and in the identification of bad actors in the routing system [18].

VI. Conclusions and future work

This paper proposes the new chain-of-trust packet marking (CTPM) method. CTPM establishes a chain of trust composed of the border routers of the autonomous systems (ASes). It makes use of the new IPv6 traceback extension header (TEH). The TEH contains encrypted marks that trace the path taken by each packet from its origin to the destination. Although the marks are created and manipulated only by the border routers, they do not allow the identification of internal topologies of the networks of the ASes traversed by the packet. The extra computational costs and network latency generated by CTPM will be measured and evaluated. These evaluations aim to verify the computational feasibility of CTPM and to give the ASes an idea of the extra investment required in network appliances if the CTPM method is adopted on the Internet.

Acknowledgment

This research is supported by CNPq and CAPES, Brazil.

References

[1] C. A. Shue, M. Gupta, and M. P. Davy, “Packet forwarding with source verification,” Computer Networks, vol. 52, 2008, pp. 1567–1582.

[2] H. Lee, M. Kwon, G. Hasker, and A. Perrig, “BASE: An incrementally deployable mechanism for viable IP spoofing prevention,” in Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2007, pp. 20–31.

[3] X. Liu, A. Li, X. Yang, and D. Wetherall, “Passport: secure and adoptable source authentication,” in Proceedings of the USENIX Symposium on Networked Systems Design (NSDI), 2008, pp. 365–378.

[4] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Network support for IP traceback,” Transactions on Networking, vol. 9, no. 3, 2001, pp. 226–237.

[5] M. T. Goodrich, “Probabilistic packet marking for large-scale IP traceback,” Transactions on Networking, vol. 16, no. 1, 2008, pp. 15–24.

[6] A. Belenky and N. Ansari, “On deterministic packet marking,” Computer Networks, vol. 51, 2007, pp. 2677–2700.

[7] Y. Xiang, W. Zhou, and M. Guo, “Flexible deterministic packet marking: an IP traceback system to find the real source of attacks,” Transactions on Parallel and Distributed Systems, vol. 20, no. 4, 2009, pp. 567–580.

[8] Y. Sun, C. Zhang, S. Meng, and K. Lu, “Modified deterministic packet marking for DDoS attack traceback in IPv6 network,” in Proceedings of the IEEE International Conference on Computer and Information Technology, 2011, pp. 245–248.

[9] RFC 6564, Internet Engineering Task Force, 2012, available at http://tools.ietf.org/html/rfc6564 [retrieved: January, 2016].

[10] RFC 6793, Internet Engineering Task Force, 2012, available at http://tools.ietf.org/html/rfc6793 [retrieved: January, 2016].

[11] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford, “A survey of BGP security issues and solutions,” Proceedings of the IEEE, vol. 98, no. 1, 2010, pp. 100–122.

[12] Z. Gao and N. Ansari, “A practical and robust inter-domain marking scheme for IP traceback,” Computer Networks, vol. 51, 2007, pp. 732–750.

[13] RFC 2460, Internet Engineering Task Force, 1998, available at http://tools.ietf.org/html/rfc2460 [retrieved: January, 2016].

[14] RFC 1981, Internet Engineering Task Force, 1996, available at http://tools.ietf.org/html/rfc1981 [retrieved: January, 2016].

[15] Public-key infrastructure based on the X.509 protocol, Internet Engineering Task Force, available at http://datatracker.ietf.org/wg/pkix/documents/ [retrieved: January, 2016].

[16] Spam, Kaspersky Lab, available at http://www.kaspersky.com/about/news/spam [retrieved: January, 2016].

[17] S. Goldberg, S. Halevi, A. D. Jaggard, V. Ramachandran, and R. N. Wright, “Rationality and traffic attraction: incentives for honest path announcements in BGP,” in Proceedings of the ACM SIGCOMM Conference on Data Communication, 2008, pp. 267–278.

[18] G. Huston, M. Rossi, and G. Armitage, “Securing BGP — A literature survey,” Comm. Surveys & Tutorials, vol. 13, no. 2, 2011, pp. 199–222.

 ISBN: 978-1-61208-450-3