Computer Networks 80 (2015) 1–26

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A survey on the recent efforts of the Internet Standardization Body for securing inter-domain routing

M.S. Siddiqui [a,b,*], D. Montero [a], R. Serral-Gracià [a], X. Masip-Bruin [b], M. Yannuzzi [a]

[a] *Networking and Information Technology Lab (NetIT Lab), Technical University of Catalonia (UPC), Spain*
[b] *Advanced Network Architectures Lab (CRAAX), Technical University of Catalonia (UPC), Spain*

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form 22 January 2015
Accepted 27 January 2015
Available online 3 February 2015

Keywords:
BGP
Security
BGPSEC
Routing
Internet
Inter-domain

ABSTRACT

The Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol in the Internet, thus it plays a crucial role in current communications. Unfortunately, it was conceived without any internal security mechanism, and hence is prone to a number of vulnerabilities and attacks that can result in large scale outages in the Internet. In light of this, securing BGP has been an active research area since its adoption. Several security strategies, ranging from a complete replacement of the protocol up to the addition of new features in it were proposed, but only minor tweaks have found the pathway to be adopted. More recently, the IETF Secure Inter-Domain Routing (SIDR) Working Group (WG) has put forward several recommendations to secure BGP. In this paper, we survey the efforts of the SIDR WG including, the Resource Public Key Infrastructure (RPKI), Route Origin Authorizations (ROAs), and BGP Security (BGPSEC), for securing the BGP protocol. We also discuss the post SIDR inter-domain routing unresolved security challenges along with the deployment and adoption challenges of SIDR's proposals. Furthermore, we shed light on future research directions in managing the broader security issues in inter-domain routing. The paper is targeted to readers from the academic and industrial communities that are not only interested in an updated article accounting for the recent developments made by the Internet standardization body toward securing BGP (i.e., by the IETF), but also for an analytical discussion about their pros and cons, including promising research lines as well.

1. Introduction

The Border Gateway Protocol (BGP) is the protocol used for exchanging reachability information in the inter-domain arena of the Internet. Unfortunately, it is widely accepted that the current version of BGP (version 4, usually denoted as BGP-4), does not provide any performance or security guarantees [1]. The intrinsic assumption of trust on the information exchanged between Autonomous Systems (AS) through the BGP protocol does not stand realistic anymore, as a number of day-to-day social as well as business applications, such as telephony, online-banking, and stock trading, increasingly rely on the Internet. The heavy reliance on such mission critical applications has played a vital role in motivating the increased interest in improving the security of the Internet. BGP has always been an interesting topic for the research community mainly due to several concerns related to its convergence [2–10], its churn [11–13], its limitations in terms of traffic engineering [14–17], policies [18–25], documented anomalies

[*] Corresponding author at: Networking and Information Technology Lab (NetIT Lab), Technical University of Catalonia (UPC), Spain. Tel.: +34 938967294.

E-mail addresses: siddiqui@ac.upc.edu (M.S. Siddiqui), dmontero@ac.upc.edu (D. Montero), rserral@ac.upc.edu (R. Serral-Gracià), xmasip@ac.upc.edu (X. Masip-Bruin), yannuzzi@ac.upc.edu (M. Yannuzzi).

http://dx.doi.org/10.1016/j.comnet.2015.01.017
1389-1286/© 2015 Elsevier B.V. All rights reserved.

[26–31], and other issues [32–40], but the recent large scale outages in the Internet acted as a catalyst for reviving the research focus toward its security [41–53].

The security issues in BGP arise from the implicit trust among BGP speakers, paving the way for a number of vulnerabilities and attacks. Furthermore, due to the complex way that BGP operates, it is hard to distinguish between a malicious attack and the unfortunate result of a misconfiguration. The misconfiguration in BGP is a regular occurrence, some of which have caused internationally noticeable Internet service disruptions in the past [54], as well as recently [55,56]. In fact, BGP is not a very complicated protocol, but the way it is operated in practice, that is, allowing flexible policies while maintaining global scalability, makes it intricate [57].

One of the main security problems of BGP is traffic hijacking, which occurs due to false IP prefix origination or false route propagation. The false IP prefix origination refers to the scenario when an AS advertises an IP prefix as its owner where in fact it is not. In 2008, the diversion of Youtube traffic toward an ISP in Pakistan caused unavailability of Youtube for several hours for almost the entire Internet, and this is just one of the several incidents occurring every year [56]. The false route propagation refers to the scenario where an AS manipulates the AS-path information, not related to itself, to influence the decision process of route selection on other ASes. In April 2010, one of the telecommunications companies in China allegedly hijacked 15% of the entire Internet traffic for about 15 min, by announcing routes belonging to other ISPs [58].

Another apparently simple but complex security problem regarding BGP that has caused large scale disruption in Internet service is referred to as a “route leak”. A route leak is a policy related anomaly that occurs when a route is not advertised according to the business relationship or the link classification—we will exemplify and delve into this issue along the paper (cf. Section 2.4). For instance, in February 2012, a misconfiguration at a multi-homed ISP leaked all its internal routes to one of its providers, including the routes from other providers, causing a national level disruption in Internet service in Australia [55].

In light of this, the improvement of BGP security has been an active research area since its adoption. There are detailed best practices and recommendations [59], which can be used as a first line of defense in mitigating the BGP anomalies, but even after such countermeasures, BGP remains vulnerable to some major attacks related to the authenticity and integrity of the exchanged information, stemming from the implicit trust model and the lack of intrinsic security mechanisms in BGP. As a result, several security mechanisms and protocols have been proposed during the past decade or so [60–81], suggesting from small changes up to the complete replacement of the BGP protocol. Despite these efforts, only minor tweaks have finally reached an operational status in practice. In this context, the Secure Inter-Domain Routing (SIDR) [82], an IETF [84] Working Group (WG), has put forward several recommendations which have gained interest from industry as well as from the research community. Indeed, a couple of the recommendations have already been adopted by regional Internet registries [85,86] and several providers.

In this paper, we particularly examine the SIDR’s contributions for securing BGP, including the Resource Public Key Infrastructure (RPKI) [87], Route Origin Authorizations (ROAs) [88] and BGPSEC [89], in light of the well-known set of BGP attacks. We also discuss the unresolved security vulnerabilities and considerations for BGP in the presence of SIDR’s solutions. SIDR’s recommended solutions do not attempt to address an important set of security anomalies, specifically, the policy related attacks [83]. Most of the existing proposals—including SIDR’s—approach BGP security from an operational perspective, and do not take into consideration the business policies among the ASes for securing BGP. This is mainly because the ASes keep the information regarding their relationships and routing policies with other ASes confidential, which makes the mitigation of policy related attacks, such as route leaks, a challenging problem. Then, we discuss the excess baggage of SIDR’s solution in terms of software, hardware and changes required to the current version of the BGP protocol. We also look at the deployment and adoption challenges of the SIDR’s solution. Although some of SIDR’s security recommendations are already in testing phase, the BGPSEC protocol is facing resistance because apart from requiring hardware upgrades on the routers it requires syntactical and operational changes in the BGP protocol as well. In this regard, it is crucial to explore different ways by which a proposed security mechanism could be integrated while avoiding collateral burden and fatal entropy to the existing inter-domain routing system. In this paper, we also discuss the proposition of decoupling or outsourcing the security requirements away from the protocol itself.

The rest of the paper is organized as follows. In Section 2, we present a brief overview about the AS polices in inter-domain routing and illustrate some of the main security vulnerabilities of the BGP-4 protocol. Section 3 compares the design principles of SIDR WG recommendations with earlier proposed solutions. We survey the contributions made by SIDR in Section 4. In Section 5, we examine SIDR’s contributions with respect to the BGP vulnerabilities described earlier, and discuss about their pros and cons. Section 6 discusses the potential of outsourcing inter-domain routing security chores; and finally, Section 7 concludes the paper.

2. Major vulnerabilities of BGP

The blind trust with which two neighboring BGP speakers accept the exchanged information gives rise to vulnerabilities that can be exploited in different ways. Besides, given the complex operation of BGP, a number of BGP anomalies can even occur due to misconfigurations rather than to malicious intent. In a nutshell, the attacks in BGP can be broadly classified into three categories, namely, false information exchange attacks (e.g., false IP prefix origination and false BGP update), BGP protocol manipulation attacks (e.g., Route Flap Damping and Minimum Route Advertisement Interval attacks [43,90]), and AS policy violations attacks (e.g., route leaks). It is important highlighting that the focus of this paper is not on the BGP attacks